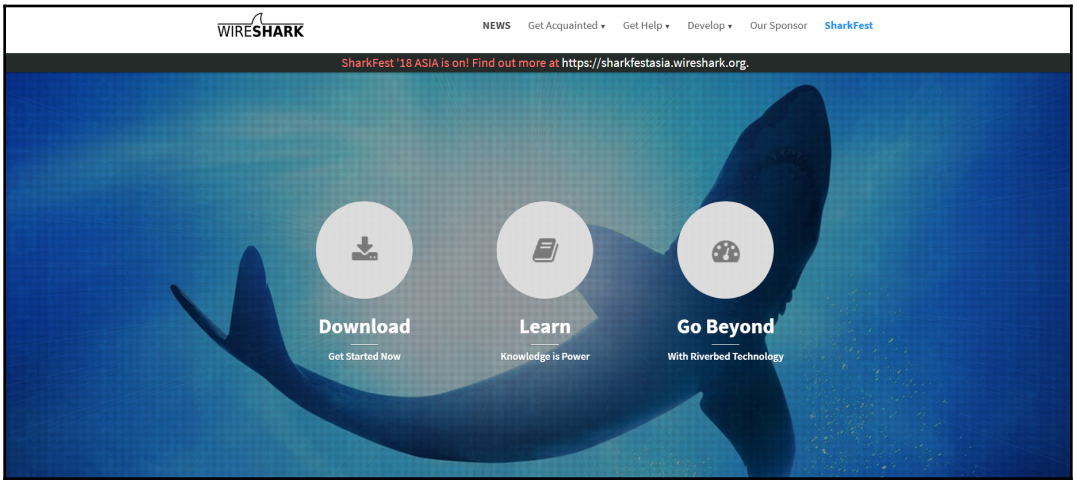
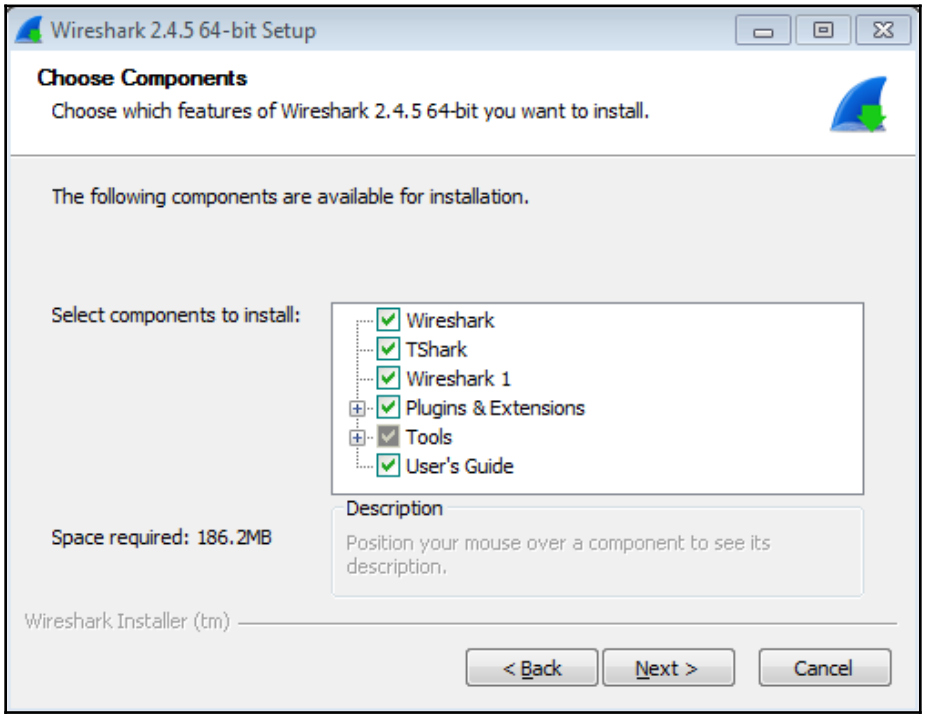
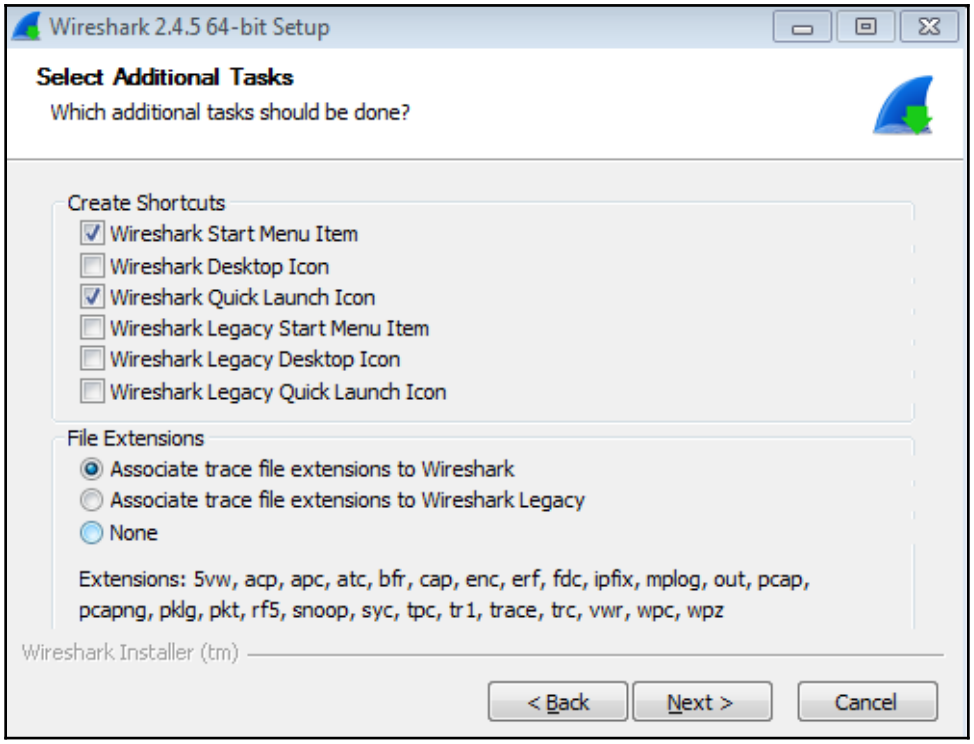
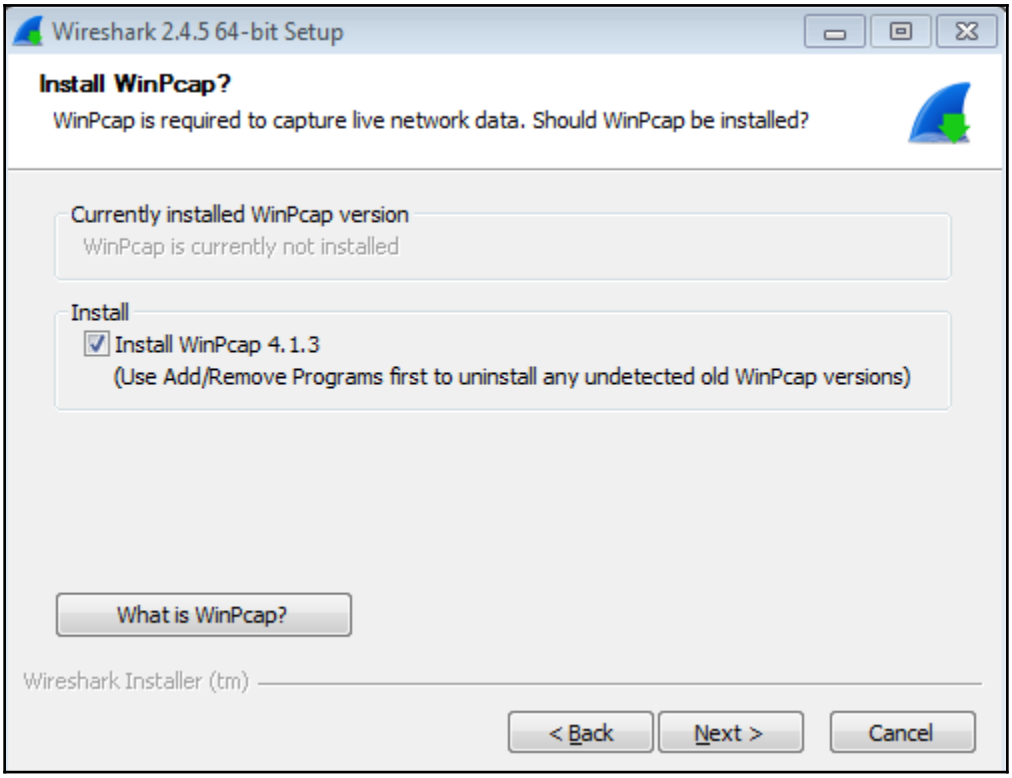
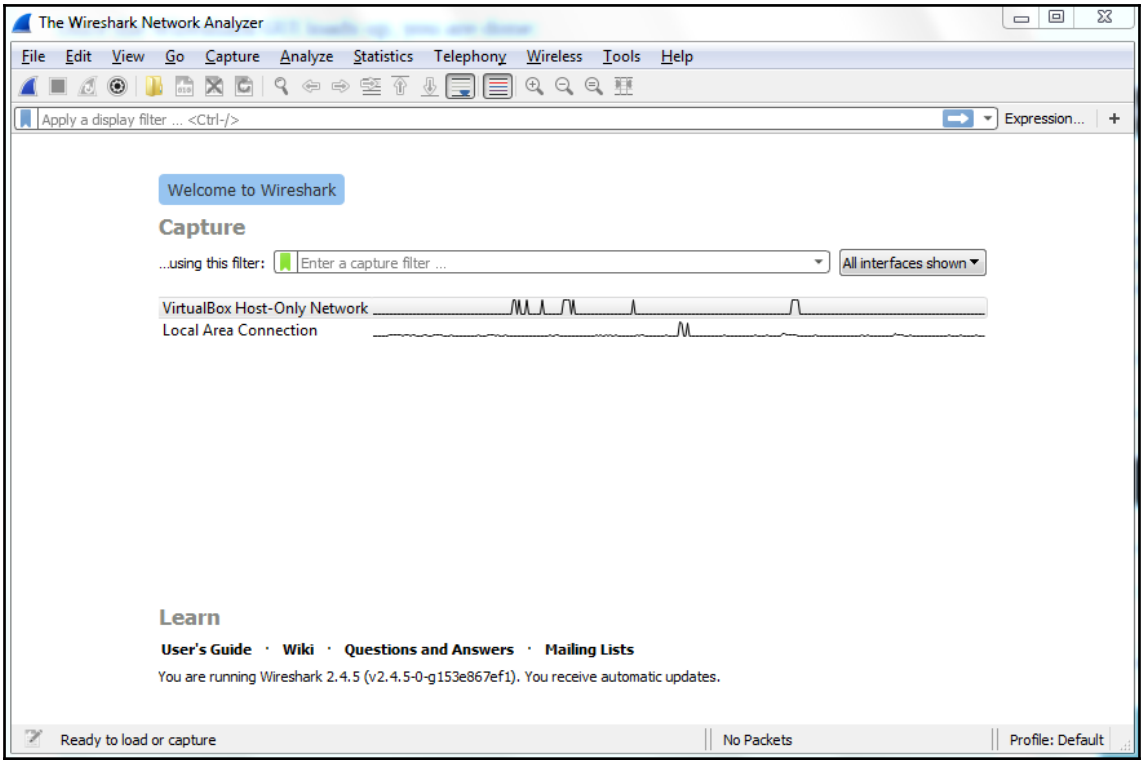
Chapter 01: Installing Wireshark 2

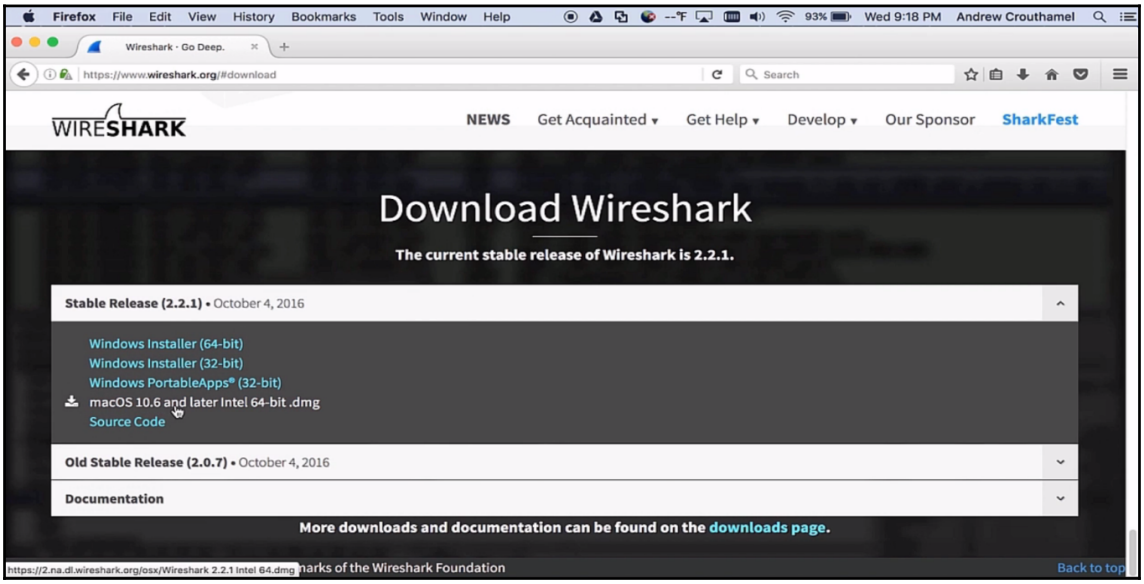


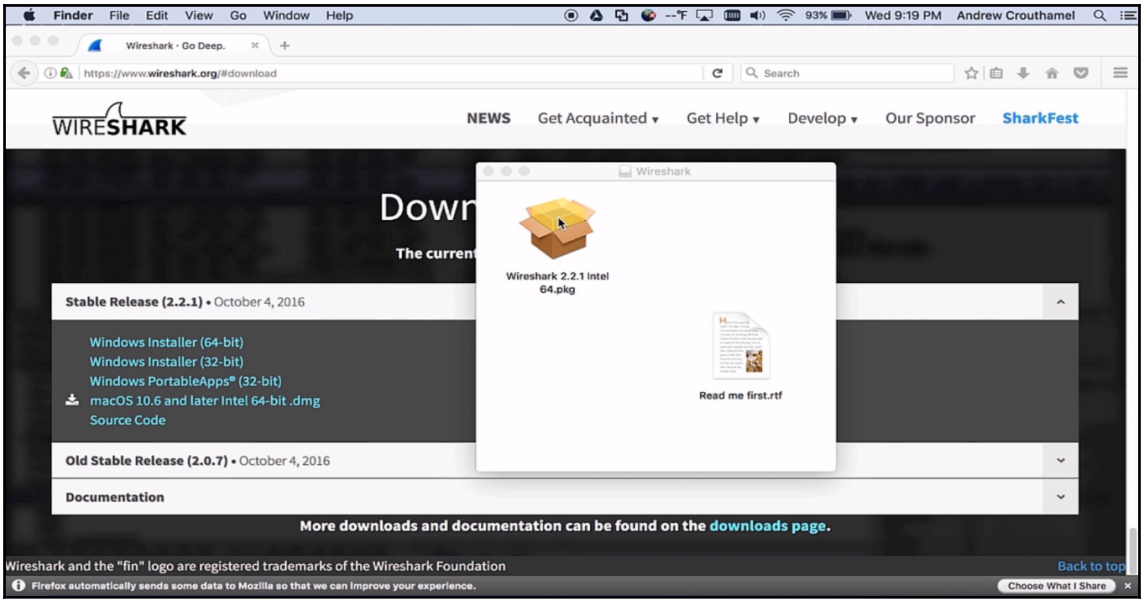



Wireshark 2.4.5 64-bit Setup
Select Additional Tasks
Which additional tasks should be done?
Create Shortcuts
Wireshark Start Menu Item
Wireshark Desktop Icon
Wireshark Quick Launch Icon
Wireshark Legacy Start Menu Item
Wireshark Legacy Desktop Icon
Wireshark Legacy Quick Launch Icon
File Extensions
Associate trace file extensions to Wireshark
Associate trace file extensions to Wireshark Legacy
None
Extensions: 5vw, acp, apc, atc, bfr, cap, enc, erf, fdc, ipfix, mplog, out, pcap, pcapng, pklg, pkt, rf5, snoop, syc, tpc, tr1, trace, trc, vwr, wpc, wpz
Wireshark Installer (tm)
< Back
Next >
Cancel

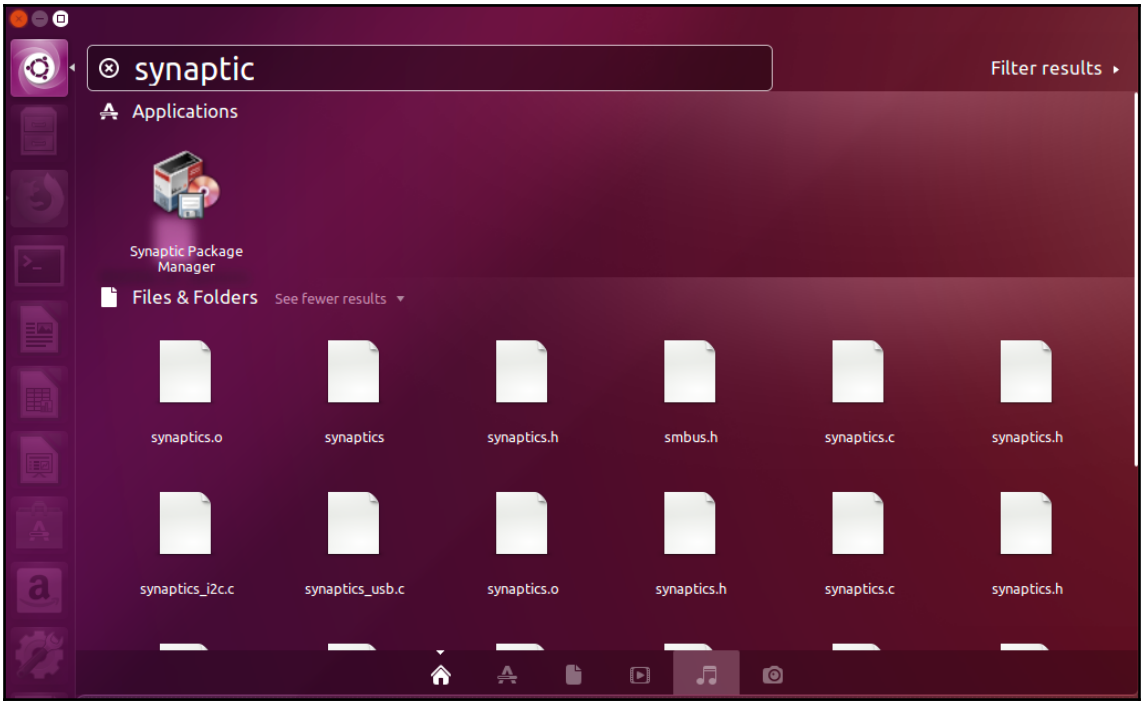

Wireshark 2.4.5 64-bit Setup
Install WinPcap?
WinPcap is required to capture live network data. Should WinPcap be installed?
Currently installed WinPcap version
WinPcap is currently not installed
Install
Install WinPcap 4.1.3
(Use Add/Remove Programs first to uninstall any undetected old WinPcap versions)
What is WinPcap?
Wireshark Installer (tm)
< Back
Next >
Cancel

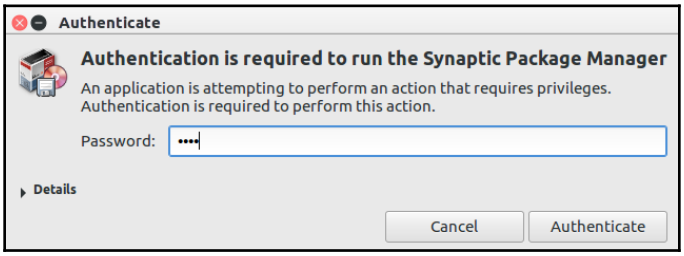

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
VirtualBox Host-Only Network
Local Area Connection
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.5 (v2.4.5-0-g153e867ef1). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

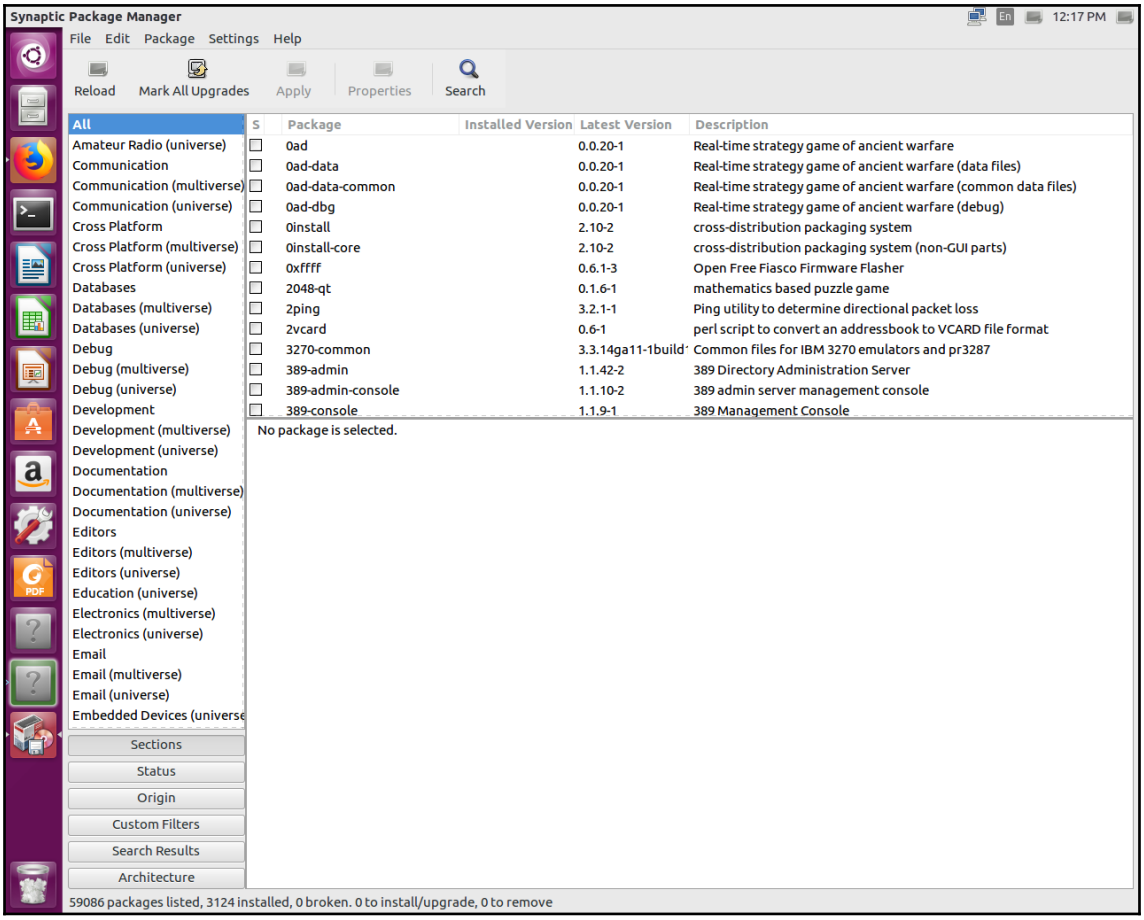

Firefox File Edit View History Bookmarks Tools Window Help
Wed 9:18 PM Andrew Crouthamel
Wireshark · Go Deep.
https://www.wireshark.org/#download
Search
WIRESHARK
NEWS Get Acquainted Get Help Develop Our Sponsor SharkFest
Download Wireshark
The current stable release of Wireshark is 2.2.1.
Stable Release (2.2.1) • October 4, 2016
Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS 10.6 and later Intel 64-bit .dmg
Source Code
Old Stable Release (2.0.7) • October 4, 2016
Documentation
More downloads and documentation can be found on the downloads page.
https://2.na.dl.wireshark.org/osx/Wireshark 2.2.1 Intel 64.dmg
narks of the Wireshark Foundation
Back to top

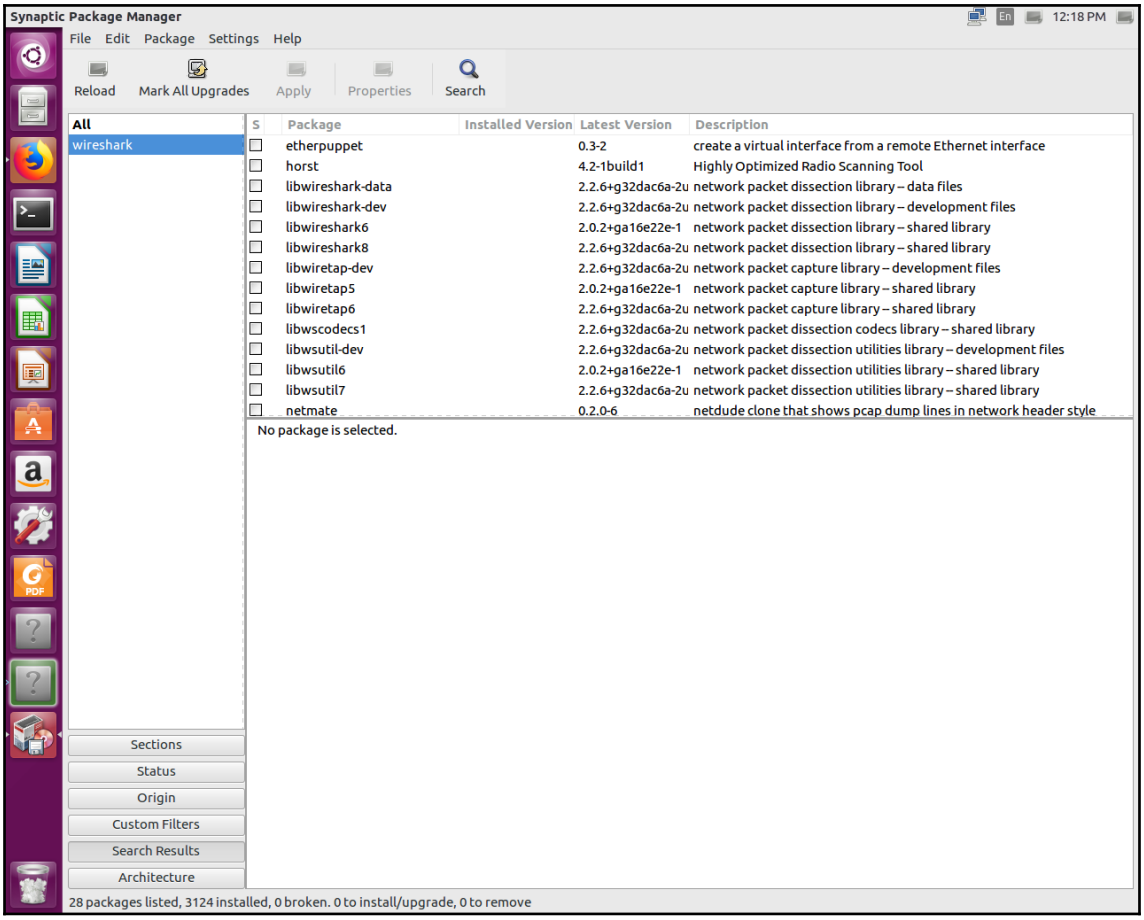

Finder File Edit View Go Window Help
Wireshark · Go Deep.
https://www.wireshark.org/#download
WIRESHARK
NEWS
Get Acquainted
Get Help
Develop
Our Sponsor
SharkFest
Wireshark
Wireshark 2.2.1 Intel 64.pkg
Read me first.rtf
Stable Release (2.2.1) • October 4, 2016
Windows Installer (64-bit)
Windows Installer (32-bit)
Windows PortableApps® (32-bit)
macOS 10.6 and later Intel 64-bit .dmg
Source Code
Old Stable Release (2.0.7) • October 4, 2016
Documentation
More downloads and documentation can be found on the downloads page.
Wireshark and the "fin" logo are registered trademarks of the Wireshark Foundation
Back to top
Firefox automatically sends some data to Mozilla so that we can improve your experience.
Choose What I Share

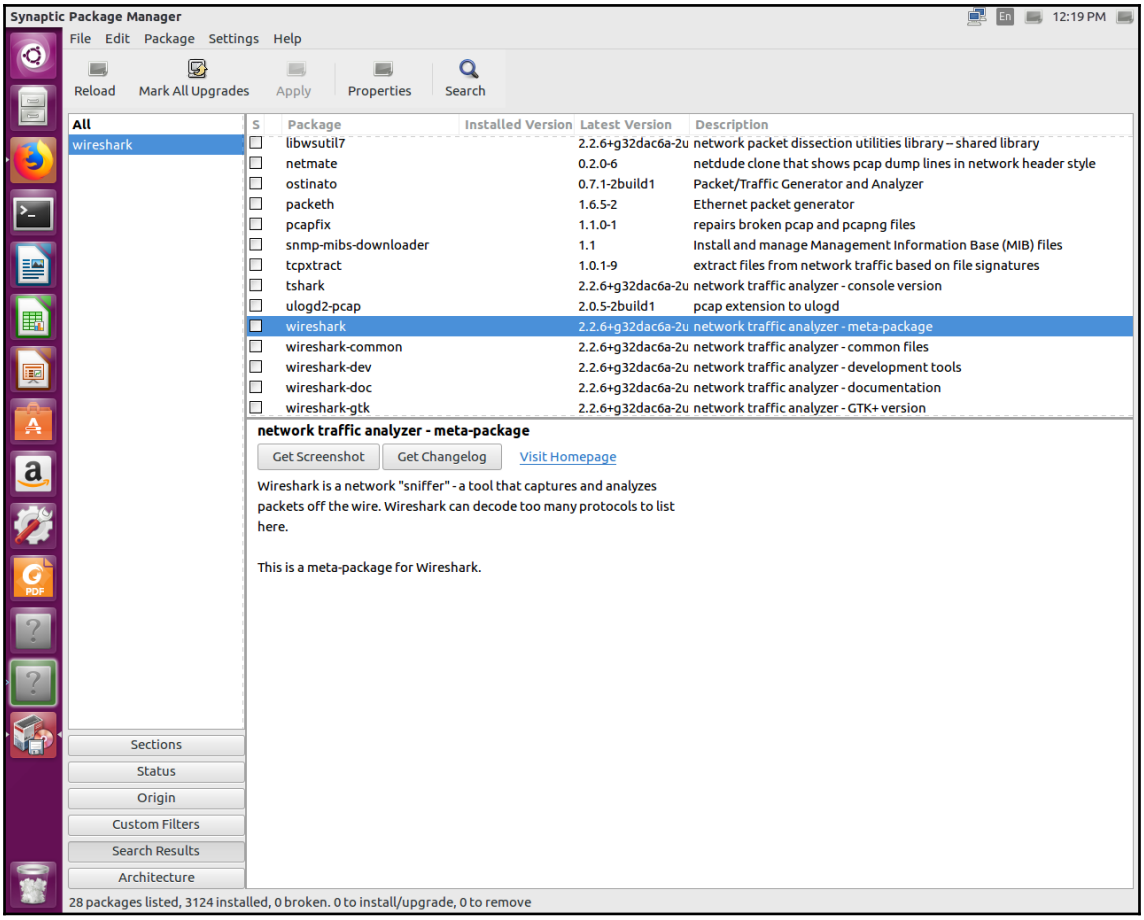

Applications
Smart Switch
SonicWA...nect.app
Stasis.app
Steam.app
Stickies.app
StrongVPN.app
System P...nces.app
TeamViewer.app
TextEdit.app
Time Machine.app
TorBrowser.app
unetbootin.app
Unity
Utilities
uTorrent.app
Visual St...ode.app
VMware Fusion.app
vSSH Lite.app
Wireshark.app
Zenmap.app
zoom.us.app
Open in Finder

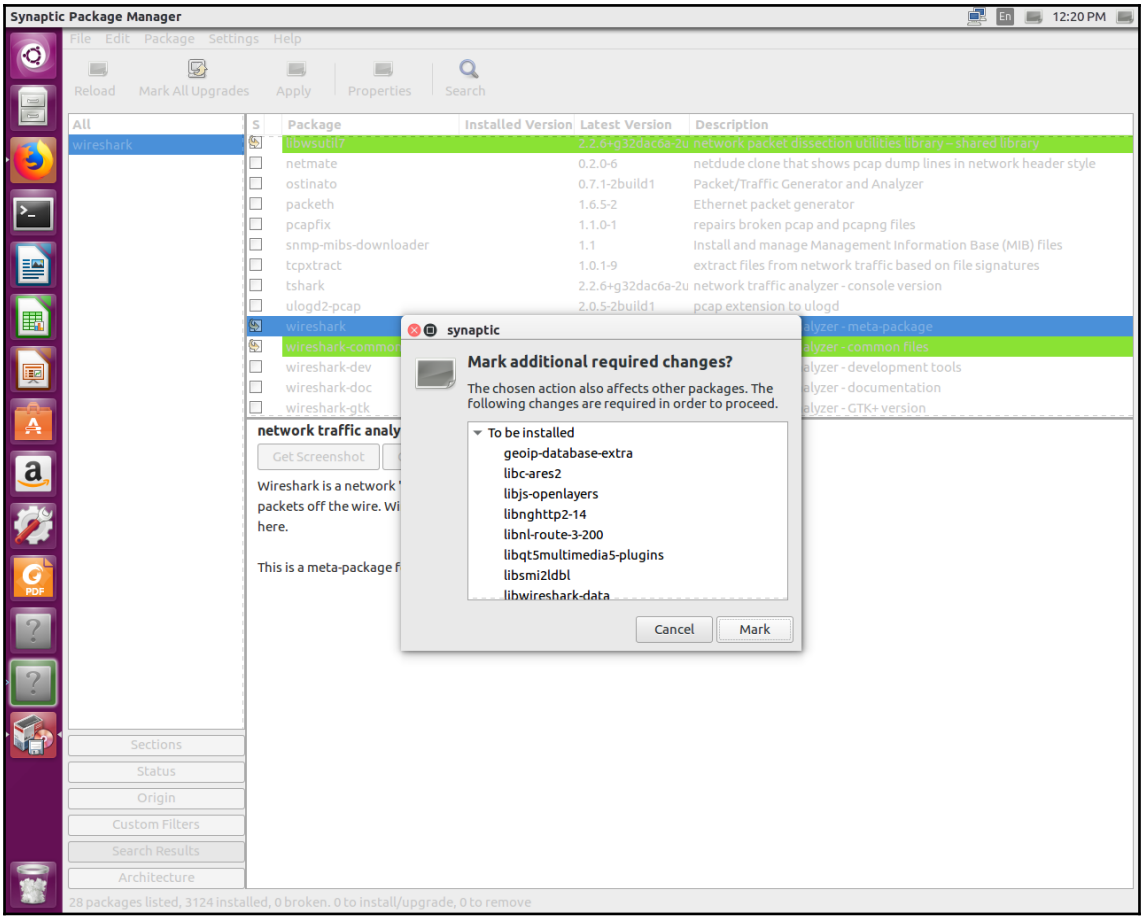

synaptic
Filter results
Applications
Synaptic Package Manager
Files & Folders
See fewer results
synaptics.o
synaptics
synaptics.h
smbus.h
synaptics.c
synaptics.h
synaptics_i2c.c
synaptics_usb.c
synaptics.o
synaptics.h
synaptics.c
synaptics.h

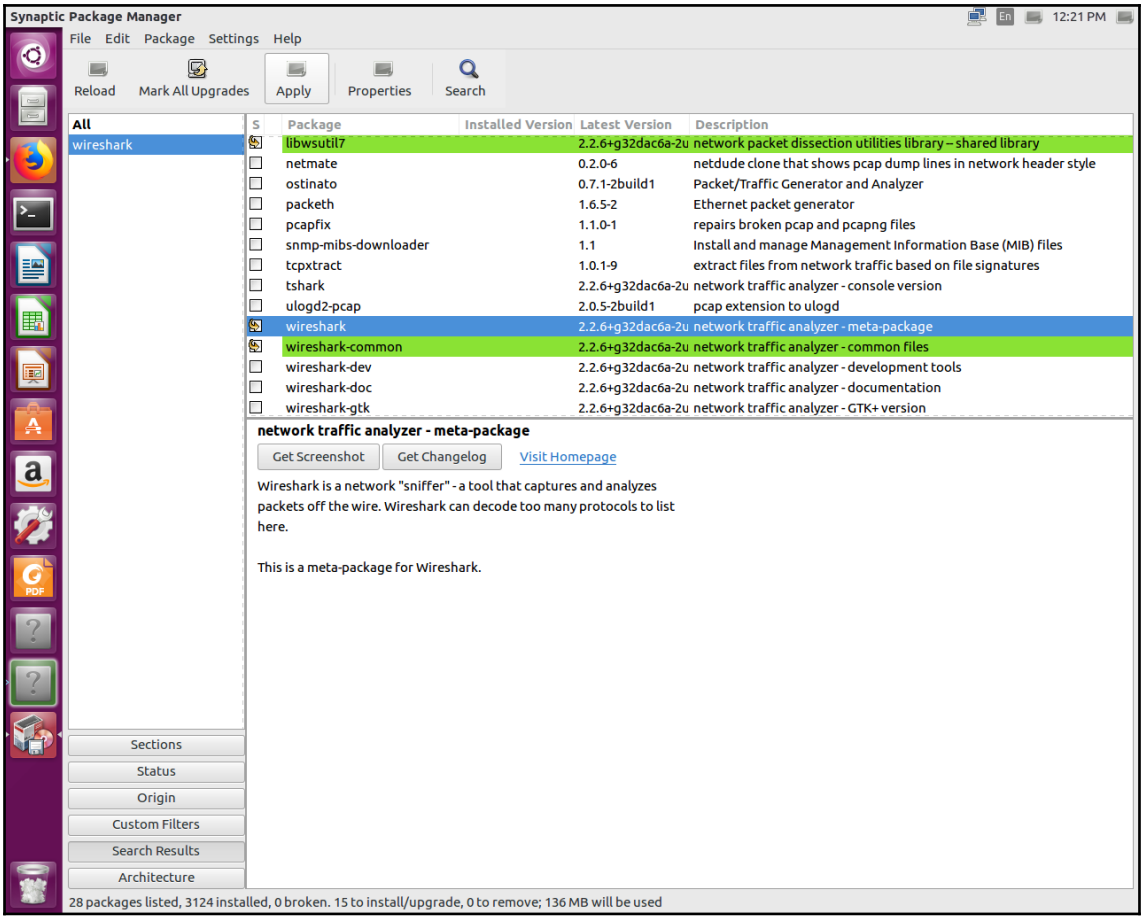

Authenticate
Authentication is required to run the Synaptic Package Manager
An application is attempting to perform an action that requires privileges.
Authentication is required to perform this action.
Password:
Details
Cancel
Authenticate

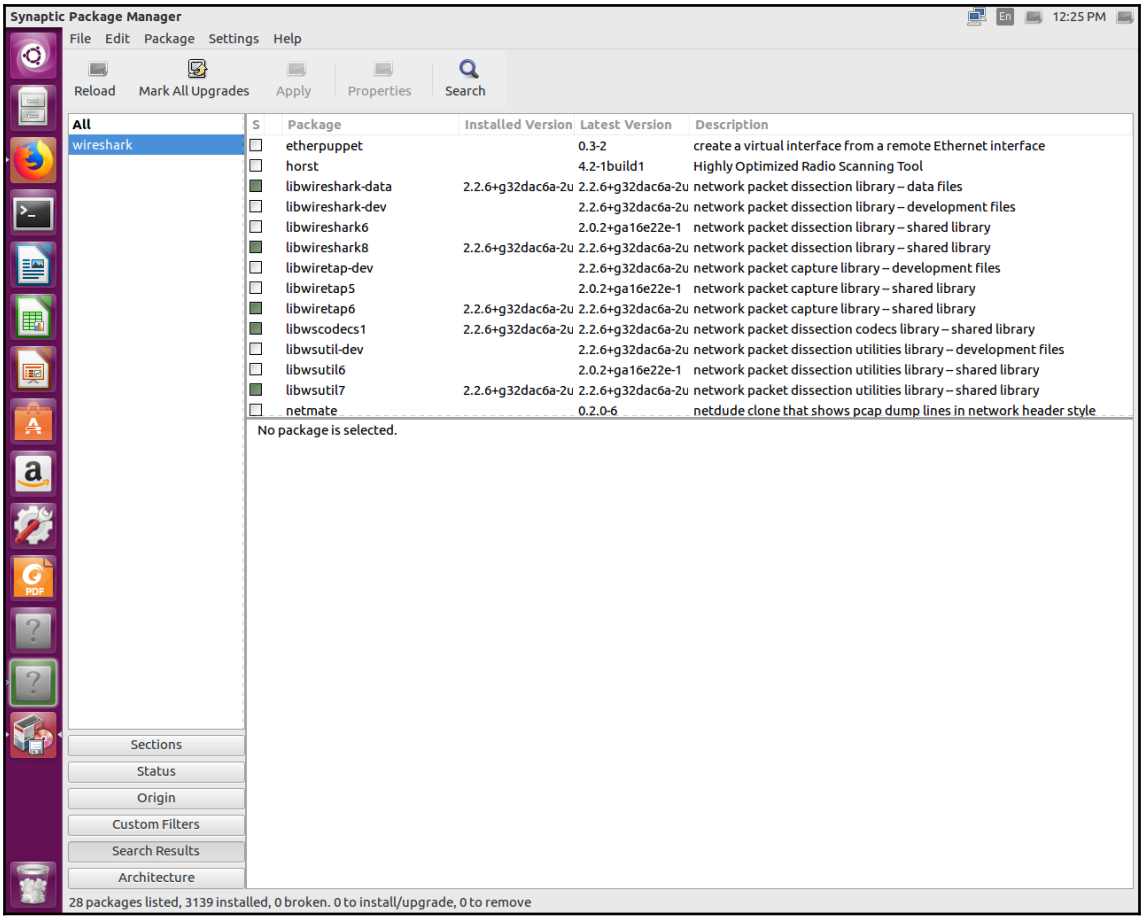

Synaptic Package Manager
12:17 PM
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Search
All
Amateur Radio (universe)
Communication
Communication (multiverse)
Communication (universe)
Cross Platform
Cross Platform (multiverse)
Cross Platform (universe)
Databases
Databases (multiverse)
Databases (universe)
Debug
Debug (multiverse)
Debug (universe)
Development
Development (multiverse)
Development (universe)
Documentation
Documentation (multiverse)
Documentation (universe)
Editors
Editors (multiverse)
Editors (universe)
Education (universe)
Electronics (multiverse)
Electronics (universe)
Email
Email (multiverse)
Email (universe)
Embedded Devices (universe
Sections
Status
Origin
Custom Filters
Search Results
Architecture
S
Package
Installed Version
Latest Version
Description
0ad 0.0.20-1 Real-time strategy game of ancient warfare
0ad-data 0.0.20-1 Real-time strategy game of ancient warfare (data files)
0ad-data-common 0.0.20-1 Real-time strategy game of ancient warfare (common data files)
0ad-dbg 0.0.20-1 Real-time strategy game of ancient warfare (debug)
0install 2.10-2 cross-distribution packaging system
0install-core 2.10-2 cross-distribution packaging system (non-GUI parts)
0xffff 0.6.1-3 Open Free Fiasco Firmware Flasher
2048-qt 0.1.6-1 mathematics based puzzle game
2ping 3.2.1-1 Ping utility to determine directional packet loss
2vcard 0.6-1 perl script to convert an addressbook to VCARD file format
3270-common 3.3.14ga11-1build Common files for IBM 3270 emulators and pr3287
389-admin 1.1.42-2 389 Directory Administration Server
389-admin-console 1.1.10-2 389 admin server management console
389-console 1.1.9-1 389 Management Console
No package is selected.
59086 packages listed, 3124 installed, 0 broken. 0 to install/upgrade, 0 to remove


Synaptic Package Manager
12:18 PM
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Search
All
wireshark
S Package Installed Version Latest Version Description
etherpuppet 0.3-2 create a virtual interface from a remote Ethernet interface
horst 4.2-1build1 Highly Optimized Radio Scanning Tool
libwireshark-data 2.2.6+g32dac6a-2u network packet dissection library – data files
libwireshark-dev 2.2.6+g32dac6a-2u network packet dissection library – development files
libwireshark6 2.0.2+ga16e22e-1 network packet dissection library – shared library
libwireshark8 2.2.6+g32dac6a-2u network packet dissection library – shared library
libwiretap-dev 2.2.6+g32dac6a-2u network packet capture library – development files
libwiretap5 2.0.2+ga16e22e-1 network packet capture library – shared library
libwiretap6 2.2.6+g32dac6a-2u network packet capture library – shared library
libwscodecs1 2.2.6+g32dac6a-2u network packet dissection codecs library – shared library
libwsutil-dev 2.2.6+g32dac6a-2u network packet dissection utilities library – development files
libwsutil6 2.0.2+ga16e22e-1 network packet dissection utilities library – shared library
libwsutil7 2.2.6+g32dac6a-2u network packet dissection utilities library – shared library
netmate 0.2.0-6 netdude clone that shows pcap dump lines in network header style
No package is selected.
Sections
Status
Origin
Custom Filters
Search Results
Architecture
28 packages listed, 3124 installed, 0 broken. 0 to install/upgrade, 0 to remove

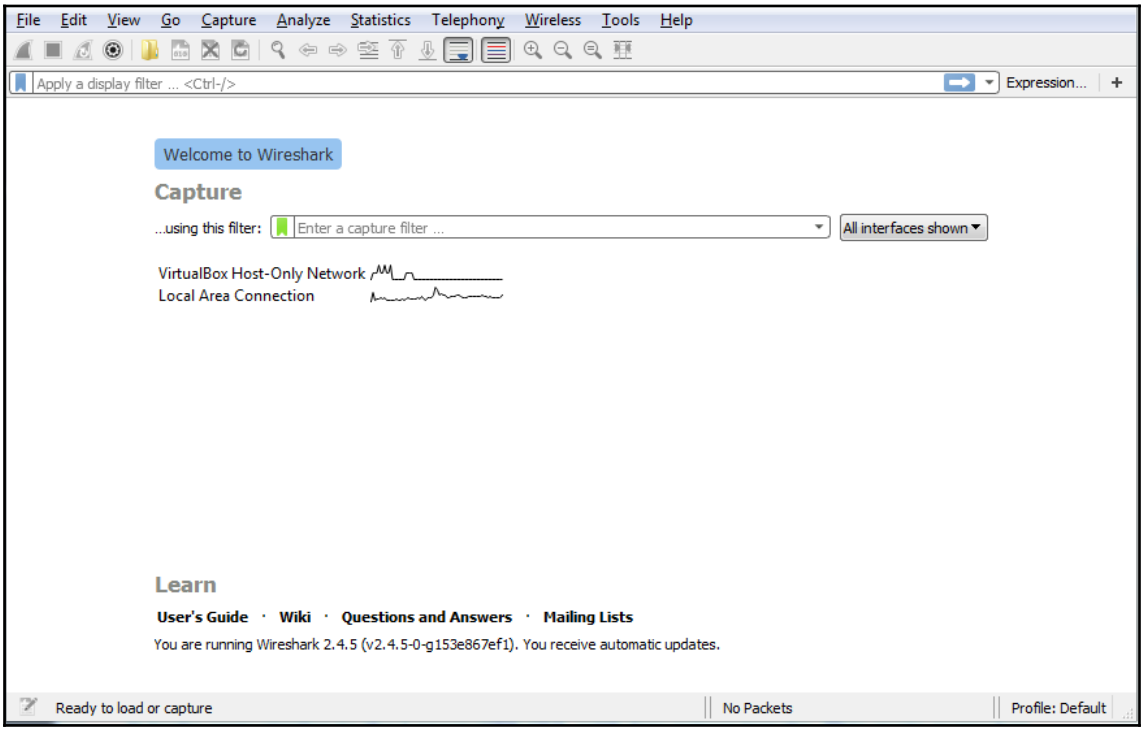

Synaptic Package Manager
12:19 PM
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Search
All
wireshark
S Package Installed Version Latest Version Description
libwsutil7 2.2.6+g32dac6a-2u network packet dissection utilities library – shared library
netmate 0.2.0-6 netdude clone that shows pcap dump lines in network header style
ostinato 0.7.1-2build1 Packet/Traffic Generator and Analyzer
packeth 1.6.5-2 Ethernet packet generator
pcapfix 1.1.0-1 repairs broken pcap and pcapng files
snmp-mibs-downloader 1.1 Install and manage Management Information Base (MIB) files
tcpxtract 1.0.1-9 extract files from network traffic based on file signatures
tshark 2.2.6+g32dac6a-2u network traffic analyzer - console version
ulogd2-pcap 2.0.5-2build1 pcap extension to ulogd
wireshark 2.2.6+g32dac6a-2u network traffic analyzer - meta-package
wireshark-common 2.2.6+g32dac6a-2u network traffic analyzer - common files
wireshark-dev 2.2.6+g32dac6a-2u network traffic analyzer - development tools
wireshark-doc 2.2.6+g32dac6a-2u network traffic analyzer - documentation
wireshark-gtk 2.2.6+g32dac6a-2u network traffic analyzer - GTK+ version
network traffic analyzer - meta-package
Get Screenshot
Get Changelog
Visit Homepage
Wireshark is a network "sniffer" - a tool that captures and analyzes packets off the wire. Wireshark can decode too many protocols to list here.
This is a meta-package for Wireshark.
Sections
Status
Origin
Custom Filters
Search Results
Architecture
28 packages listed, 3124 installed, 0 broken. 0 to install/upgrade, 0 to remove

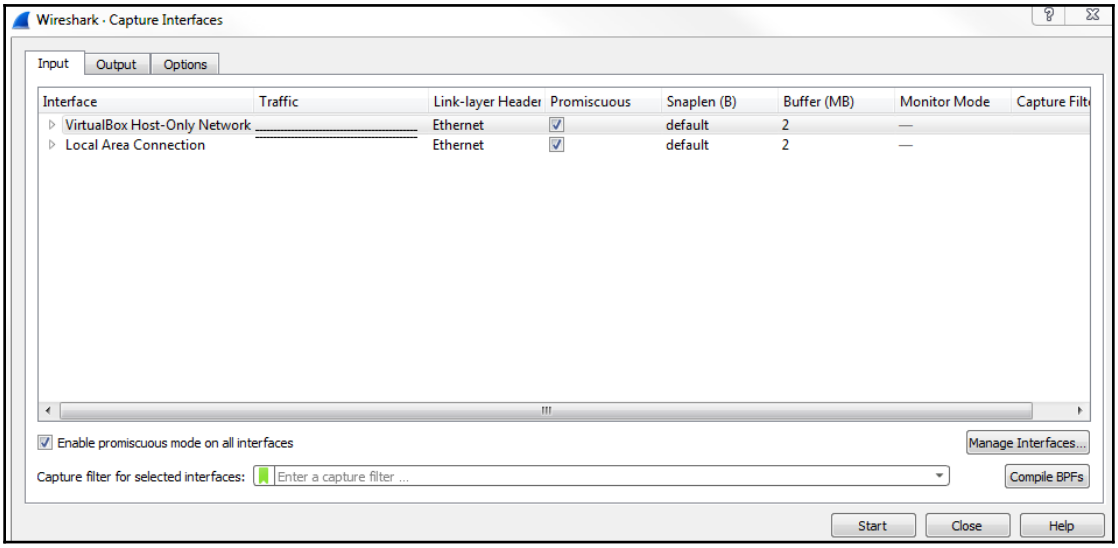

Synaptic Package Manager
12:20 PM
File Edit Package Settings Help
Reload Mark All Upgrades Apply Properties Search
All
wireshark
S Package Installed Version Latest Version Description
libwsutil7 2.2.6+g32dac6a-2u network packet dissection utilities library – shared library
netmate 0.2.0-6 netdude clone that shows pcap dump lines in network header style
ostinato 0.7.1-2build1 Packet/Traffic Generator and Analyzer
packeth 1.6.5-2 Ethernet packet generator
pcapfix 1.1.0-1 repairs broken pcap and pcapng files
snmp-mibs-downloader 1.1 Install and manage Management Information Base (MIB) files
tcpxtract 1.0.1-9 extract files from network traffic based on file signatures
tshark 2.2.6+g32dac6a-2u network traffic analyzer - console version
ulogd2-pcap 2.0.5-2build1 pcap extension to ulogd
wireshark
wireshark-common
wireshark-dev
wireshark-doc
wireshark-gtk
alyzer - meta-package
alyzer - common files
alyzer - development tools
alyzer - documentation
alyzer - GTK+ version
network traffic analy
Get Screenshot
Wireshark is a network
packets off the wire. Wi
here.
This is a meta-package f
synaptic
Mark additional required changes?
The chosen action also affects other packages. The following changes are required in order to proceed.
To be installed
geoip-database-extra
libc-ares2
libjs-openlayers
libnghttp2-14
libnl-route-3-200
libqt5multimedia5-plugins
libsmi2ldbl
libwireshark-data
Cancel
Mark
Sections
Status
Origin
Custom Filters
Search Results
Architecture
28 packages listed, 3124 installed, 0 broken. 0 to install/upgrade, 0 to remove

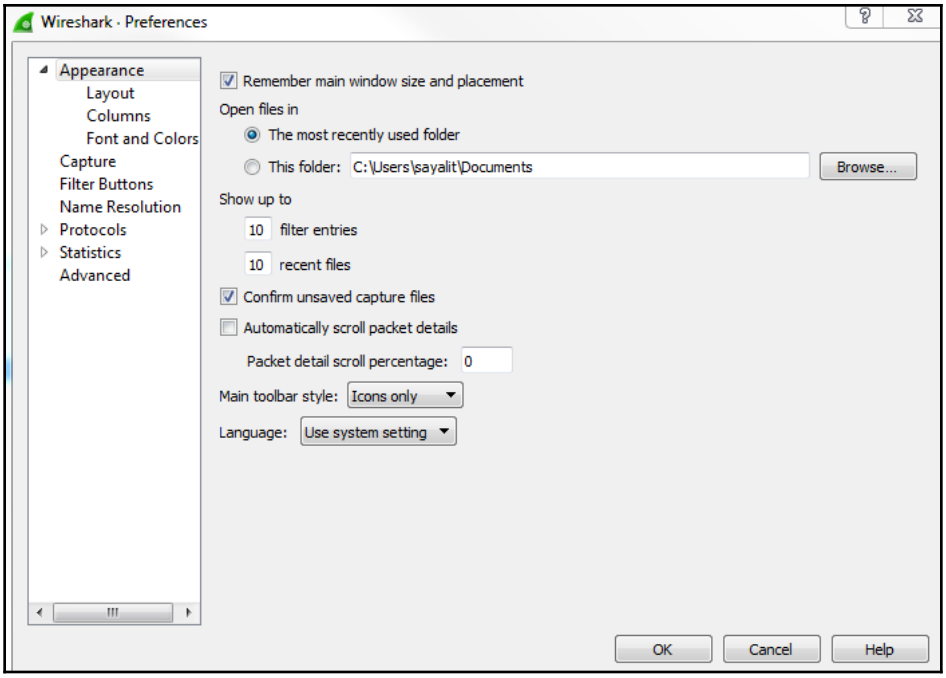

Synaptic Package Manager
12:21 PM
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Search
All
wireshark
S Package Installed Version Latest Version Description
libwsutil7 2.2.6+g32dac6a-2u network packet dissection utilities library – shared library
netmate 0.2.0-6 netdude clone that shows pcap dump lines in network header style
ostinato 0.7.1-2build1 Packet/Traffic Generator and Analyzer
packeth 1.6.5-2 Ethernet packet generator
pcapfix 1.1.0-1 repairs broken pcap and pcapng files
snmp-mibs-downloader 1.1 Install and manage Management Information Base (MIB) files
tcpxtract 1.0.1-9 extract files from network traffic based on file signatures
tshark 2.2.6+g32dac6a-2u network traffic analyzer - console version
ulogd2-pcap 2.0.5-2build1 pcap extension to ulogd
wireshark 2.2.6+g32dac6a-2u network traffic analyzer - meta-package
wireshark-common 2.2.6+g32dac6a-2u network traffic analyzer - common files
wireshark-dev 2.2.6+g32dac6a-2u network traffic analyzer - development tools
wireshark-doc 2.2.6+g32dac6a-2u network traffic analyzer - documentation
wireshark-gtk 2.2.6+g32dac6a-2u network traffic analyzer - GTK+ version
network traffic analyzer - meta-package
Get Screenshot
Get Changelog
Visit Homepage
Wireshark is a network "sniffer" - a tool that captures and analyzes packets off the wire. Wireshark can decode too many protocols to list here.
This is a meta-package for Wireshark.
Sections
Status
Origin
Custom Filters
Search Results
Architecture
28 packages listed, 3124 installed, 0 broken. 15 to install/upgrade, 0 to remove; 136 MB will be used

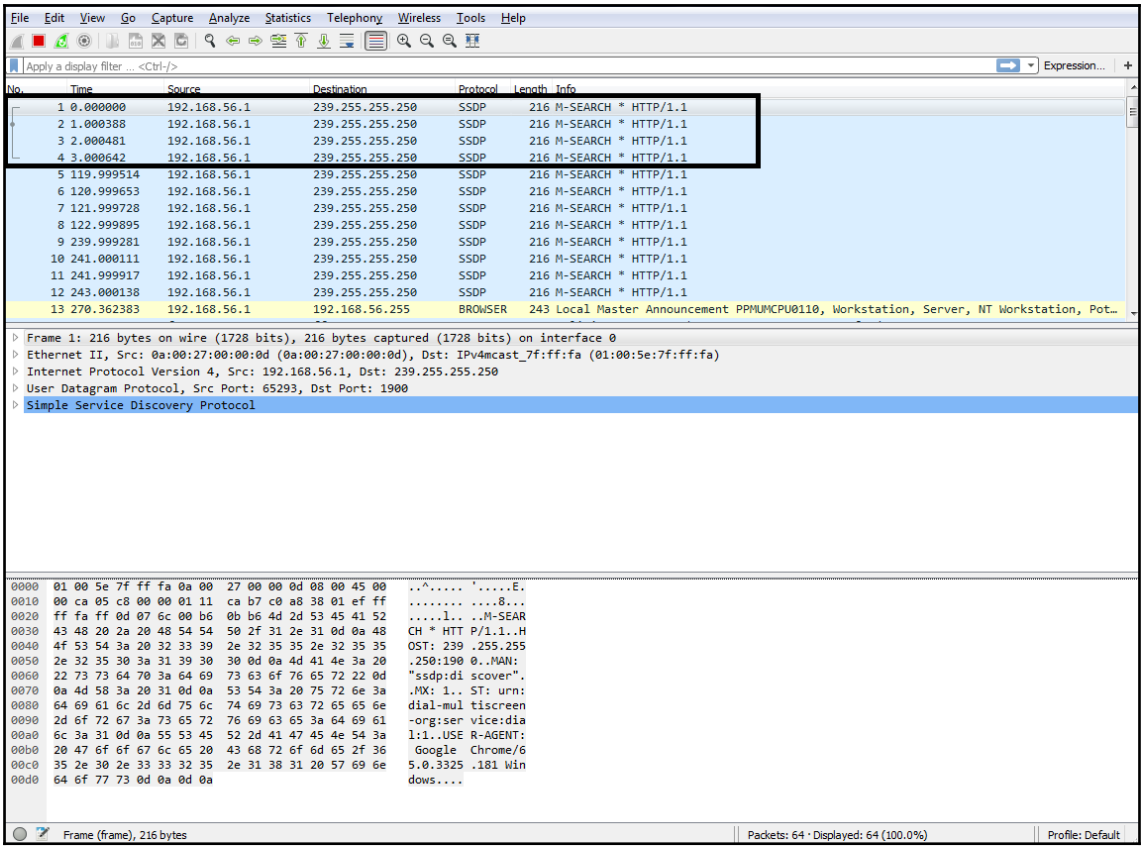

Synaptic Package Manager
12:25 PM
File Edit Package Settings Help
Reload
Mark All Upgrades
Apply
Properties
Search
All
wireshark
S Package Installed Version Latest Version Description
etherpuppet 0.3-2 create a virtual interface from a remote Ethernet interface
horst 4.2-1build1 Highly Optimized Radio Scanning Tool
libwireshark-data 2.2.6+g32dac6a-2u 2.2.6+g32dac6a-2u network packet dissection library – data files
libwireshark-dev 2.2.6+g32dac6a-2u network packet dissection library – development files
libwireshark6 2.0.2+ga16e22e-1 network packet dissection library – shared library
libwireshark8 2.2.6+g32dac6a-2u 2.2.6+g32dac6a-2u network packet dissection library – shared library
libwiretap-dev 2.2.6+g32dac6a-2u network packet capture library – development files
libwiretap5 2.0.2+ga16e22e-1 network packet capture library – shared library
libwiretap6 2.2.6+g32dac6a-2u 2.2.6+g32dac6a-2u network packet capture library – shared library
libwscodecs1 2.2.6+g32dac6a-2u 2.2.6+g32dac6a-2u network packet dissection codecs library – shared library
libwsutil-dev 2.2.6+g32dac6a-2u network packet dissection utilities library – development files
libwsutil6 2.0.2+ga16e22e-1 network packet dissection utilities library – shared library
libwsutil7 2.2.6+g32dac6a-2u 2.2.6+g32dac6a-2u network packet dissection utilities library – shared library
netmate 0.2.0-6 netdude clone that shows pcap dump lines in network header style
No package is selected.
Sections
Status
Origin
Custom Filters
Search Results
Architecture
28 packages listed, 3139 installed, 0 broken. 0 to install/upgrade, 0 to remove

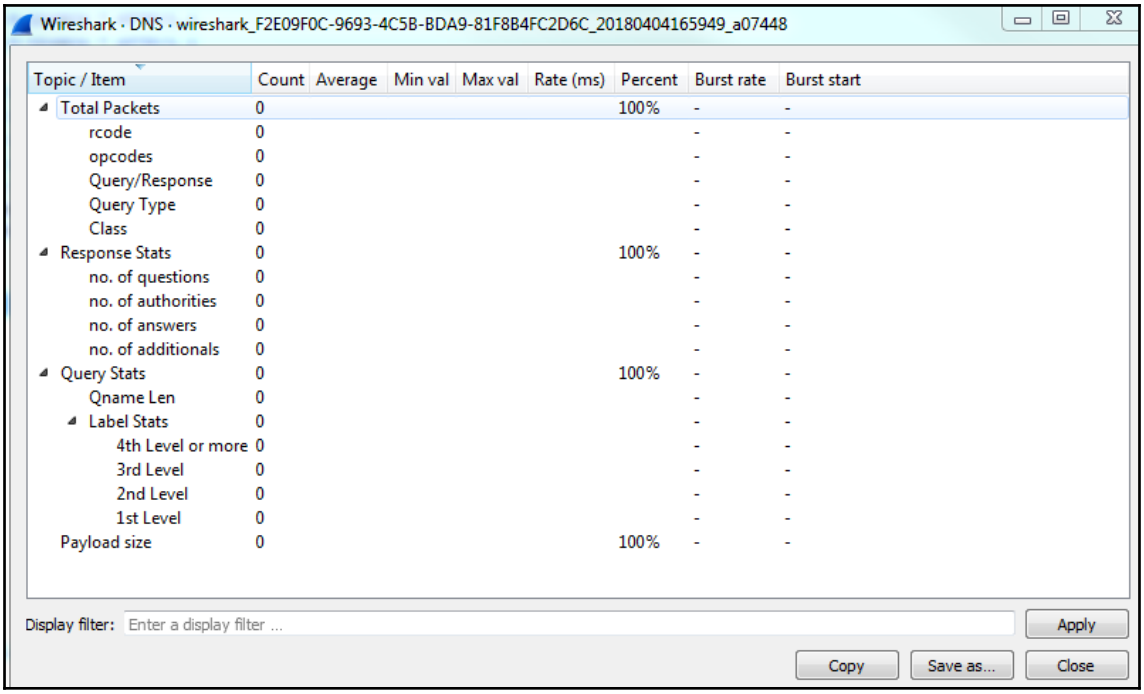
Chapter 02: Getting Started with Wireshark

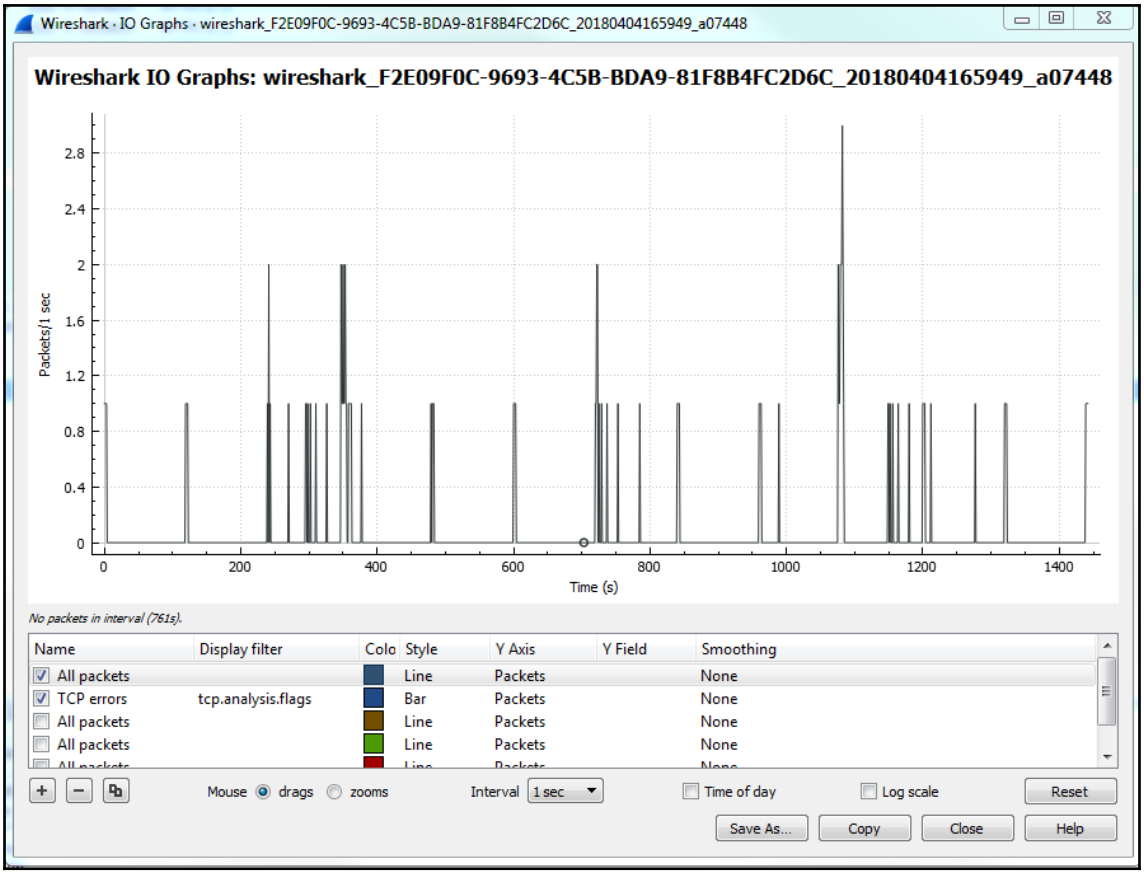


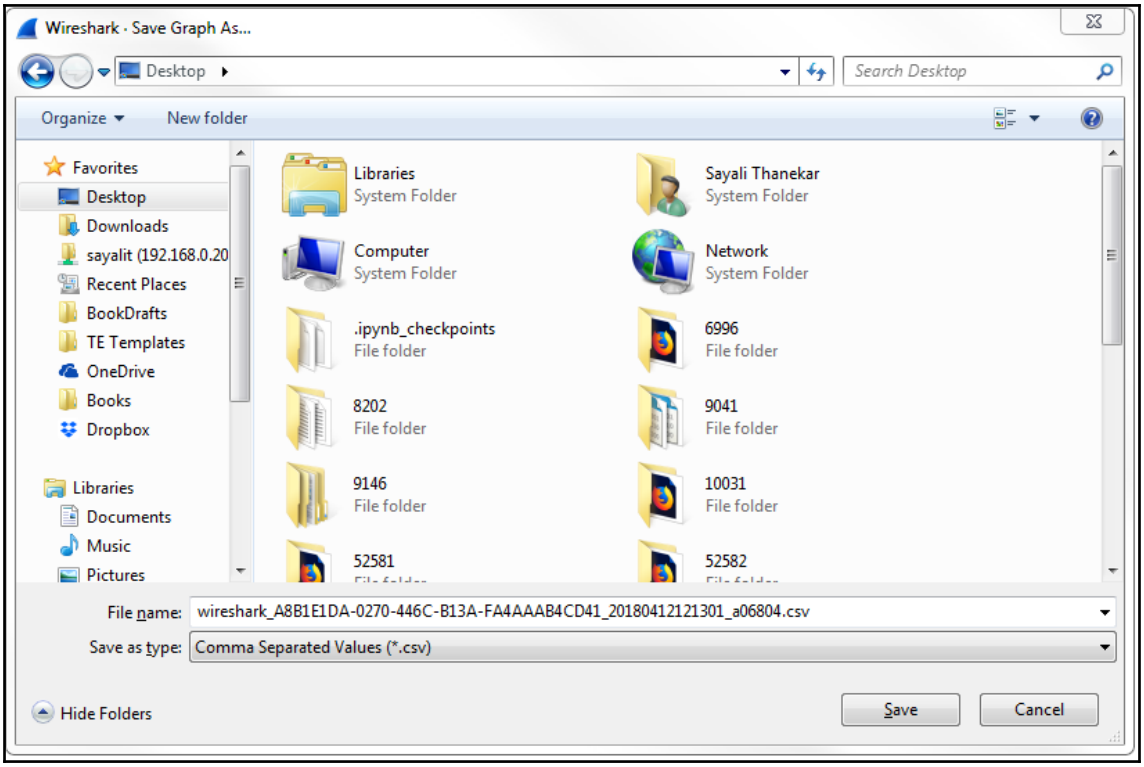

Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promiscuous
Snaplen (B)
Buffer (MB)
Monitor Mode
Capture Filt
VirtualBox Host-Only Network
Ethernet
default
2
Local Area Connection
Ethernet
default
2
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Close
Help

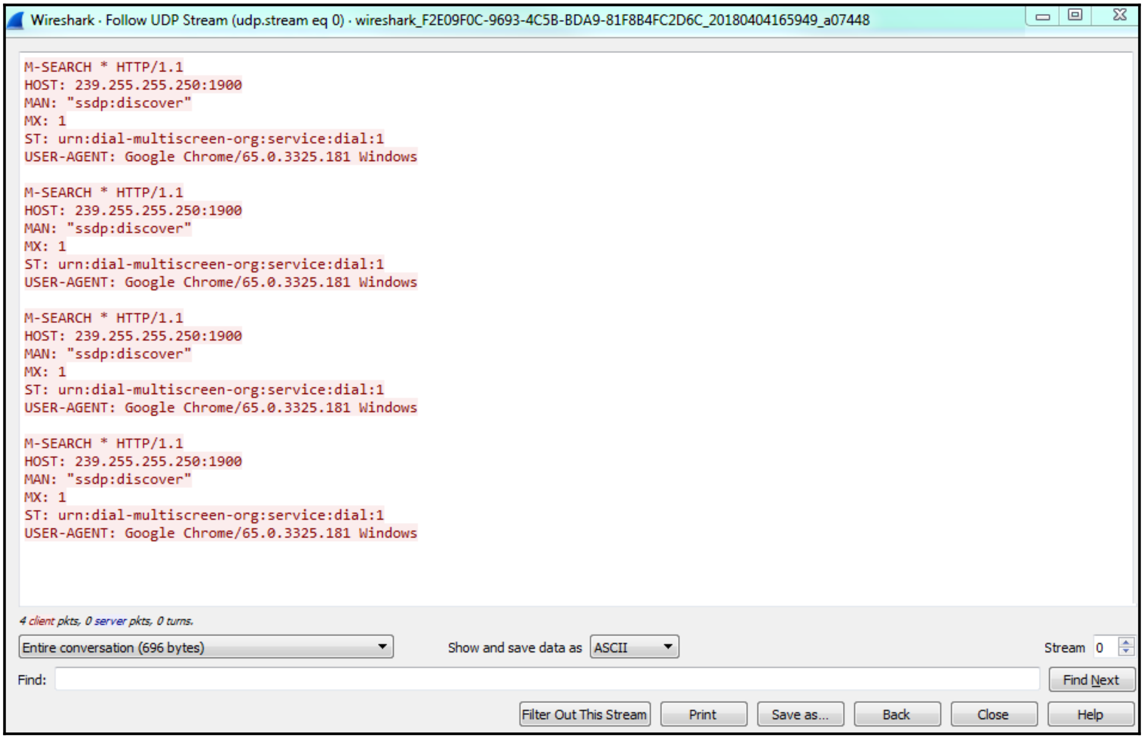

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Remember main window size and placement
Open files in
The most recently used folder
This folder:
C:\Users\sayalit\Documents
Browse...
Show up to
10
filter entries
10
recent files
Confirm unsaved capture files
Automatically scroll packet details
Packet detail scroll percentage:
0
Main toolbar style:
Icons only
Language:
Use system setting
OK
Cancel
Help

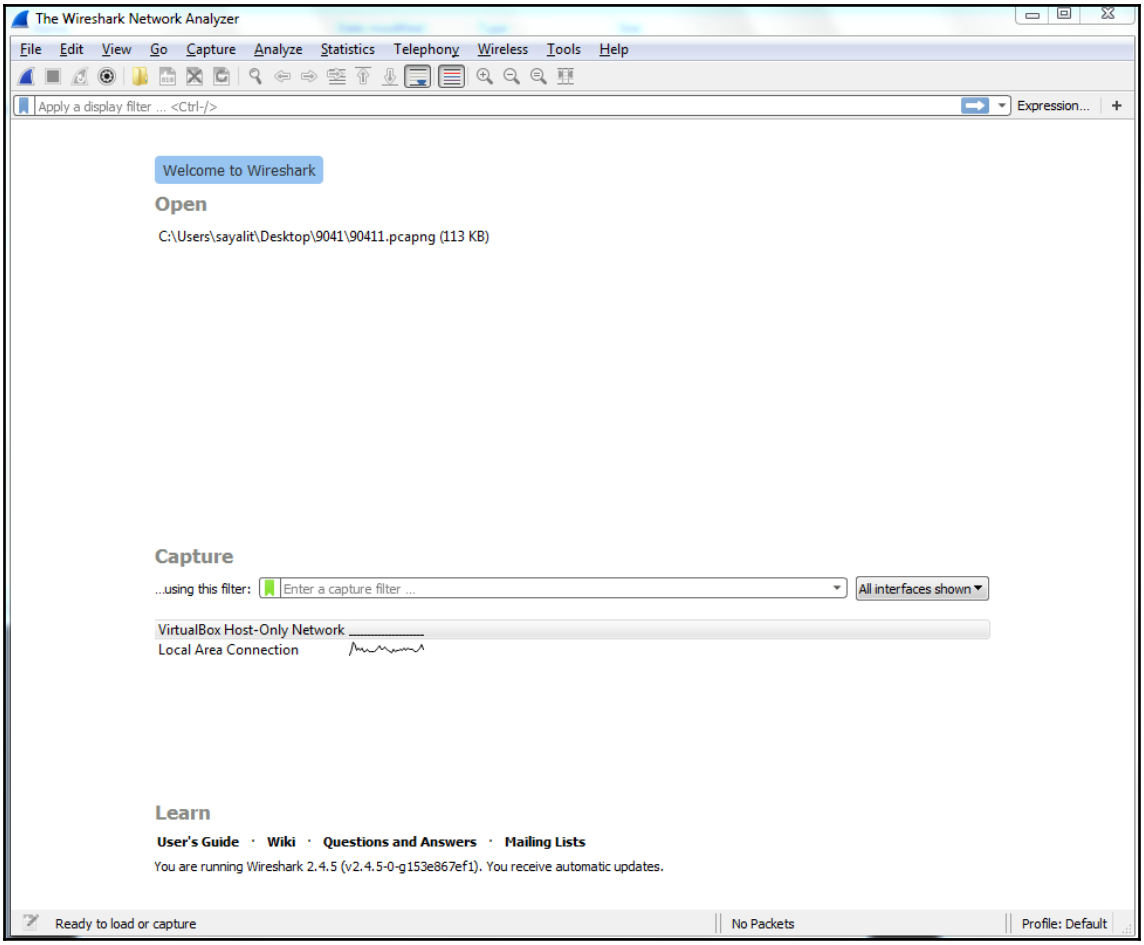

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 1.000388 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
3 2.000481 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
4 3.000642 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5 119.999514 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
6 120.999653 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
7 121.999728 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
8 122.999895 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
9 239.999281 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
10 241.000111 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
11 241.999917 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
12 243.000138 192.168.56.1 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
13 270.362383 192.168.56.1 192.168.56.255 BROWSER 243 Local Master Announcement PPMUMCPU0110, Workstation, Server, NT Workstation, Pot…
Frame 1: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: 0a:00:27:00:00:0d (0a:00:27:00:00:0d), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 65293, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa 0a 00 27 00 00 0d 08 00 45 00 ..^..... '.....E.
0010 00 ca 05 c8 00 00 01 11 ca b7 c0 a8 38 01 ef ff ....8...
0020 ff fa ff 0d 07 6c 00 b6 0b b6 4d 2d 53 45 41 52 .....l.. ..M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1.. ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-mul tiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:ser vice:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a l:1..USE R-AGENT:
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 36 Google Chrome/6
00c0 35 2e 30 2e 33 33 32 35 2e 31 38 31 20 57 69 6e 5.0.3325 .181 Win
00d0 64 6f 77 73 0d 0a 0d 0a dows....
Frame (frame), 216 bytes
Packets: 64 · Displayed: 64 (100.0%)
Profile: Default

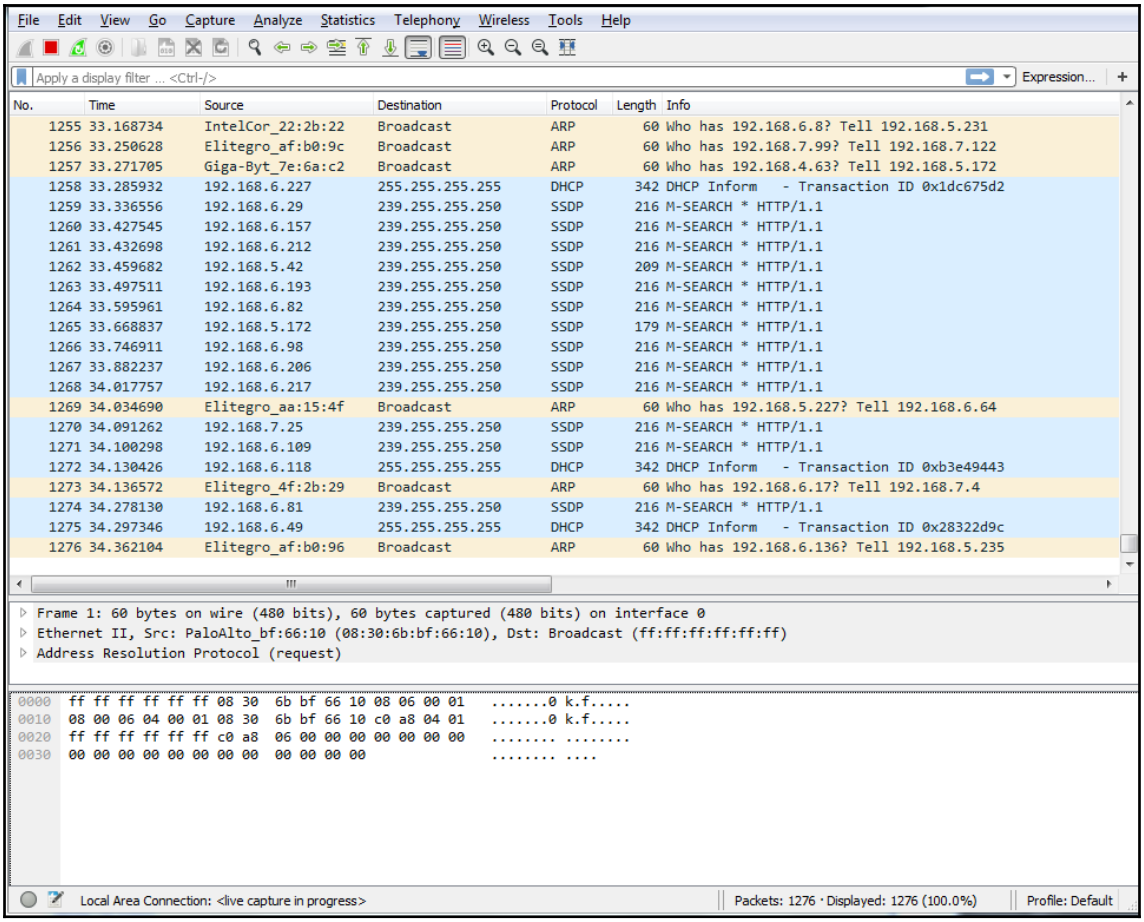

Wireshark · DNS · wireshark_F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C_20180404165949_a07448
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
Total Packets 0 100% - -
rcode 0 - -
opcodes 0 - -
Query/Response 0 - -
Query Type 0 - -
Class 0 - -
Response Stats 0 100% - -
no. of questions 0 - -
no. of authorities 0 - -
no. of answers 0 - -
no. of additionals 0 - -
Query Stats 0 100% - -
Qname Len 0 - -
Label Stats 0 - -
4th Level or more 0 - -
3rd Level 0 - -
2nd Level 0 - -
1st Level 0 - -
Payload size 0 100% - -
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

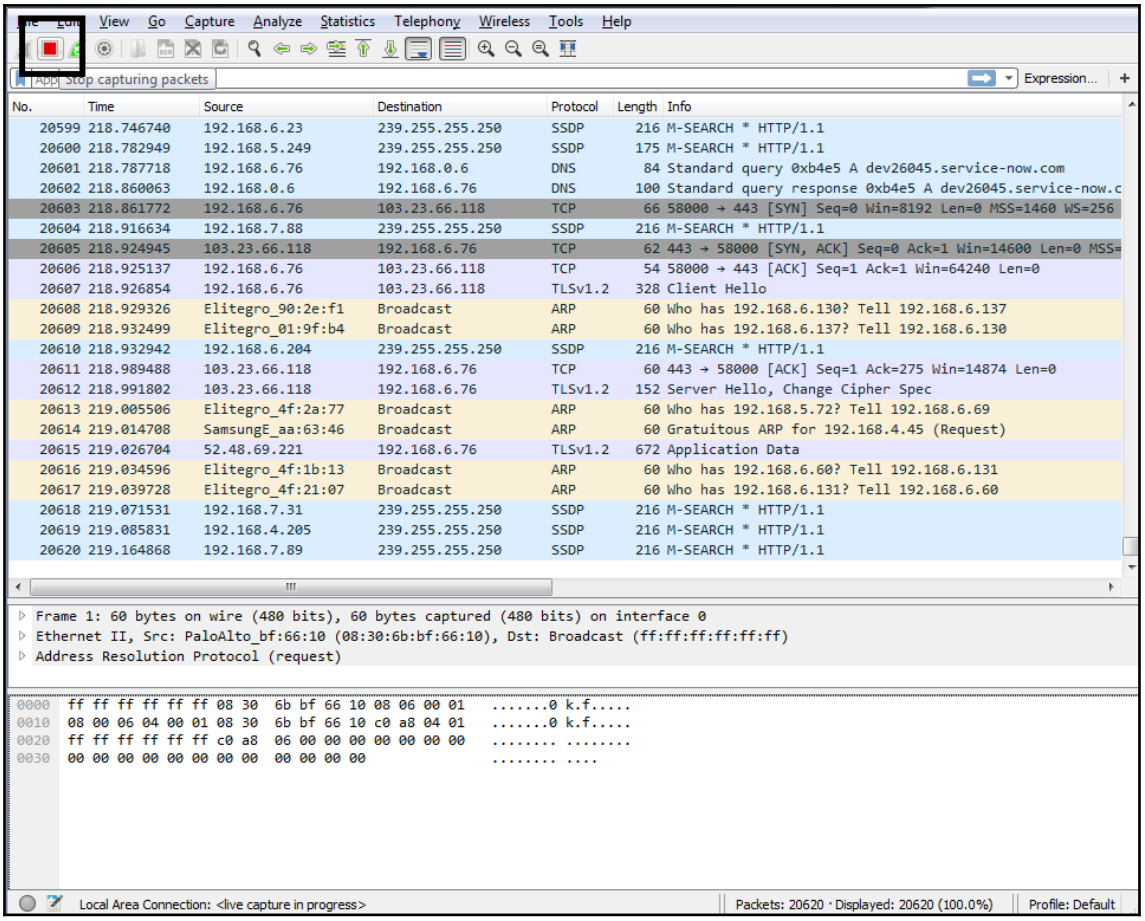

Wireshark · IO Graphs · wireshark_F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C_20180404165949_a07448
Wireshark IO Graphs: wireshark_F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C_20180404165949_a07448
Packets/1 sec
Time (s)
No packets in interval (761s).
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
TCP errors
tcp.analysis.flags
Bar
Packets
None
All packets
Line
Packets
None
All packets
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

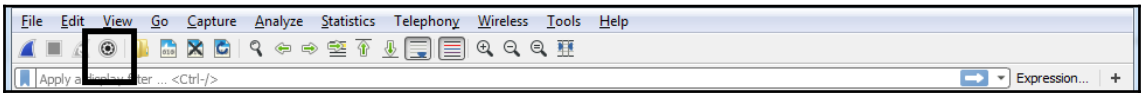

Wireshark · Save Graph As...
Desktop
Search Desktop
Organize
New folder
Favorites
Desktop
Downloads
sayalit (192.168.0.20
Recent Places
BookDrafts
TE Templates
OneDrive
Books
Dropbox
Libraries
Documents
Music
Pictures
Libraries
System Folder
Sayali Thanekar
System Folder
Computer
System Folder
Network
System Folder
.ipynb_checkpoints
File folder
6996
File folder
8202
File folder
9041
File folder
9146
File folder
10031
File folder
52581
52582
File name:
wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180412121301_a06804.csv
Save as type:
Comma Separated Values (*.csv)
Hide Folders
Save
Cancel

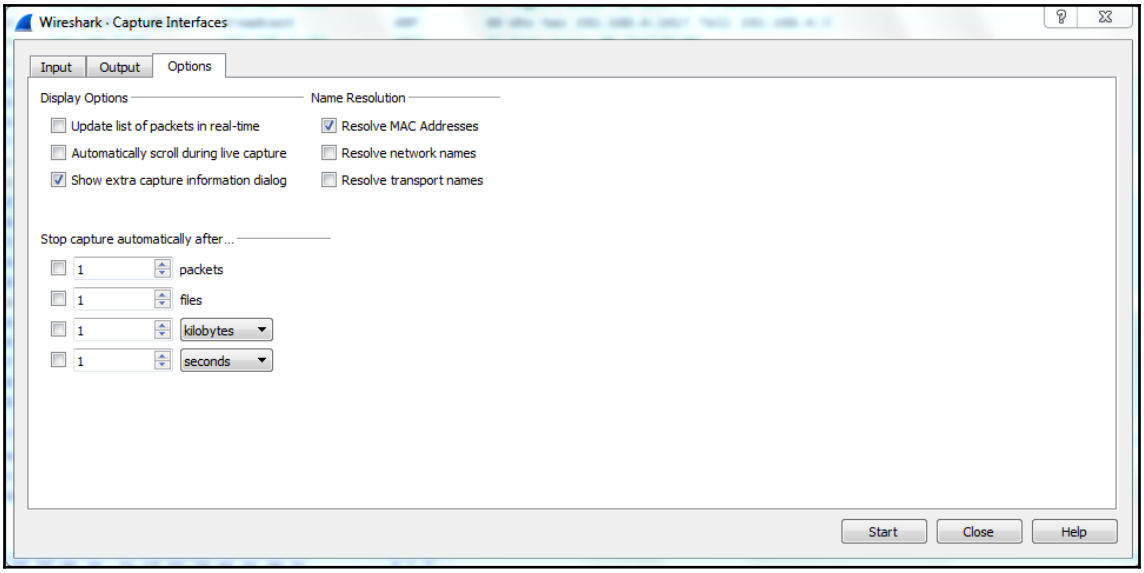

Wireshark · Follow UDP Stream (udp.stream eq 0) · wireshark_F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C_20180404165949_a07448
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/65.0.3325.181 Windows
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/65.0.3325.181 Windows
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/65.0.3325.181 Windows
M-SEARCH * HTTP/1.1
HOST: 239.255.255.250:1900
MAN: "ssdp:discover"
MX: 1
ST: urn:dial-multiscreen-org:service:dial:1
USER-AGENT: Google Chrome/65.0.3325.181 Windows
4 client pkts, 0 server pkts, 0 turns.
Entire conversation (696 bytes)
Show and save data as
ASCII
Stream
0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

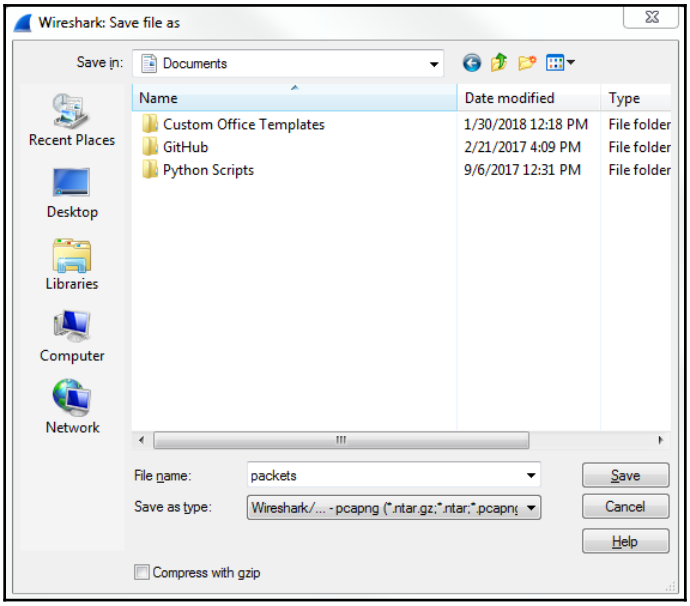

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open
C:\Users\sayalit\Desktop\9041\90411.pcapng (113 KB)
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
VirtualBox Host-Only Network
Local Area Connection
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.5 (v2.4.5-0-g153e867ef1). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

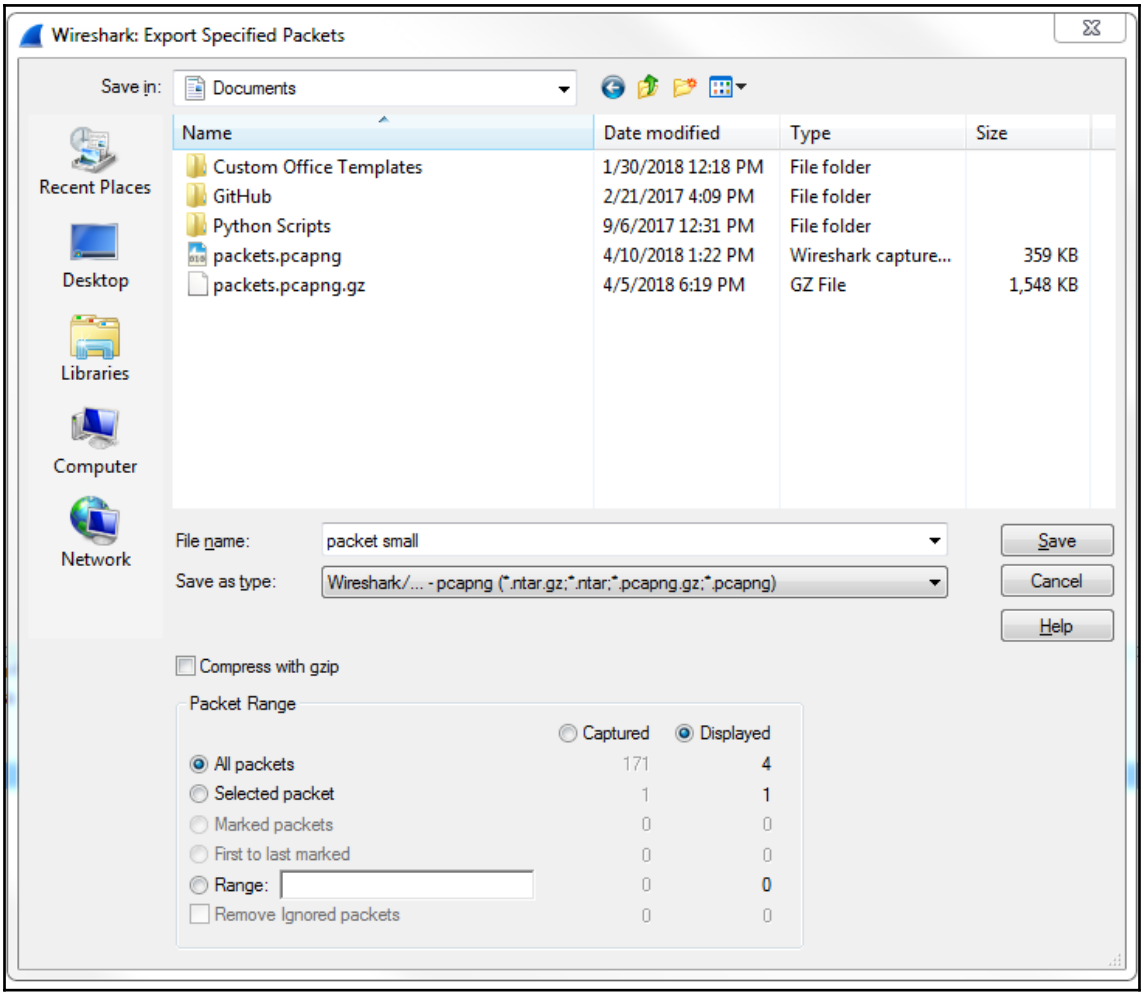

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1255 33.168734 IntelCor_22:2b:22 Broadcast ARP 60 Who has 192.168.6.8? Tell 192.168.5.231
1256 33.250628 Elitegro_af:b0:9c Broadcast ARP 60 Who has 192.168.7.99? Tell 192.168.7.122
1257 33.271705 Giga-Byt_7e:6a:c2 Broadcast ARP 60 Who has 192.168.4.63? Tell 192.168.5.172
1258 33.285932 192.168.6.227 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x1dc675d2
1259 33.336556 192.168.6.29 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1260 33.427545 192.168.6.157 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1261 33.432698 192.168.6.212 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1262 33.459682 192.168.5.42 239.255.255.250 SSDP 209 M-SEARCH * HTTP/1.1
1263 33.497511 192.168.6.193 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1264 33.595961 192.168.6.82 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1265 33.668837 192.168.5.172 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
1266 33.746911 192.168.6.98 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1267 33.882237 192.168.6.206 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1268 34.017757 192.168.6.217 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1269 34.034690 Elitegro_aa:15:4f Broadcast ARP 60 Who has 192.168.5.227? Tell 192.168.6.64
1270 34.091262 192.168.7.25 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1271 34.100298 192.168.6.109 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1272 34.130426 192.168.6.118 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0xb3e49443
1273 34.136572 Elitegro_4f:2b:29 Broadcast ARP 60 Who has 192.168.6.17? Tell 192.168.7.4
1274 34.278130 192.168.6.81 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1275 34.297346 192.168.6.49 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x28322d9c
1276 34.362104 Elitegro_af:b0:96 Broadcast ARP 60 Who has 192.168.6.136? Tell 192.168.5.235
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: PaloAlto_bf:66:10 (08:30:6b:bf:66:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 30 6b bf 66 10 08 06 00 01 .....0 k.f.....
0010 08 00 06 04 00 01 08 30 6b bf 66 10 c0 a8 04 01 .....0 k.f.....
0020 ff ff ff ff ff ff c0 a8 06 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
Local Area Connection: <live capture in progress>
Packets: 1276 · Displayed: 1276 (100.0%)
Profile: Default

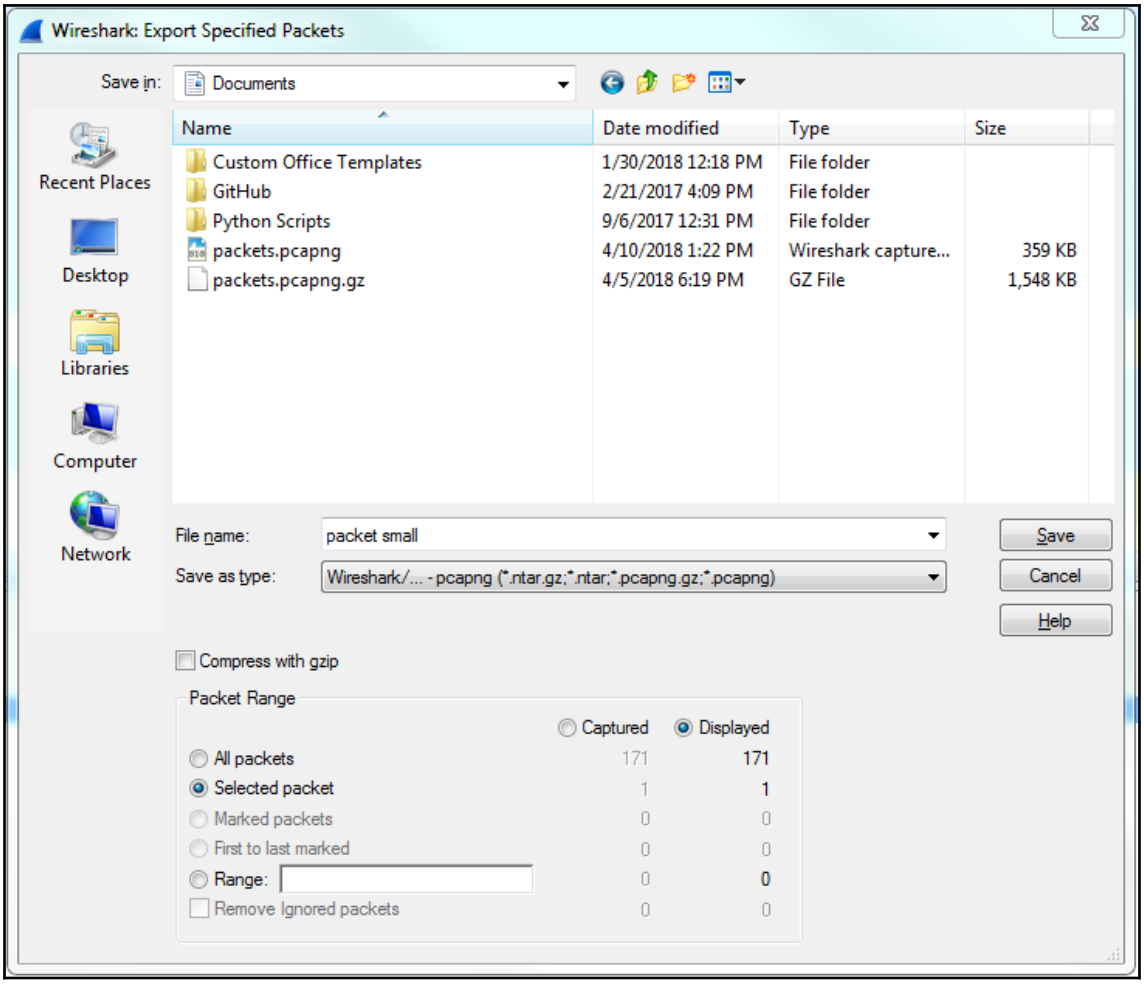

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Stop capturing packets
Expression...
No. Time Source Destination Protocol Length Info
20599 218.746740 192.168.6.23 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
20600 218.782949 192.168.5.249 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
20601 218.787718 192.168.6.76 192.168.0.6 DNS 84 Standard query 0xb4e5 A dev26045.service-now.com
20602 218.860063 192.168.0.6 192.168.6.76 DNS 100 Standard query response 0xb4e5 A dev26045.service-now.c
20603 218.861772 192.168.6.76 103.23.66.118 TCP 66 58000 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
20604 218.916634 192.168.7.88 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
20605 218.924945 103.23.66.118 192.168.6.76 TCP 62 443 → 58000 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=
20606 218.925137 192.168.6.76 103.23.66.118 TCP 54 58000 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
20607 218.926854 192.168.6.76 103.23.66.118 TLSv1.2 328 Client Hello
20608 218.929326 Elitegro_90:2e:f1 Broadcast ARP 60 Who has 192.168.6.130? Tell 192.168.6.137
20609 218.932499 Elitegro_01:9f:b4 Broadcast ARP 60 Who has 192.168.6.137? Tell 192.168.6.130
20610 218.932942 192.168.6.204 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
20611 218.989488 103.23.66.118 192.168.6.76 TCP 60 443 → 58000 [ACK] Seq=1 Ack=275 Win=14874 Len=0
20612 218.991802 103.23.66.118 192.168.6.76 TLSv1.2 152 Server Hello, Change Cipher Spec
20613 219.005506 Elitegro_4f:2a:77 Broadcast ARP 60 Who has 192.168.5.72? Tell 192.168.6.69
20614 219.014708 SamsungE_aa:63:46 Broadcast ARP 60 Gratuitous ARP for 192.168.4.45 (Request)
20615 219.026704 52.48.69.221 192.168.6.76 TLSv1.2 672 Application Data
20616 219.034596 Elitegro_4f:1b:13 Broadcast ARP 60 Who has 192.168.6.60? Tell 192.168.6.131
20617 219.039728 Elitegro_4f:21:07 Broadcast ARP 60 Who has 192.168.6.131? Tell 192.168.6.60
20618 219.071531 192.168.7.31 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
20619 219.085831 192.168.4.205 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
20620 219.164868 192.168.7.89 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: PaloAlto_bf:66:10 (08:30:6b:bf:66:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff 08 30 6b bf 66 10 08 06 00 01 ....0 k.f.....
0010 08 00 06 04 00 01 08 30 6b bf 66 10 c0 a8 04 01 ....0 k.f.....
0020 ff ff ff ff ff ff c0 a8 06 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....
Local Area Connection: <live capture in progress>
Packets: 20620 · Displayed: 20620 (100.0%)
Profile: Default

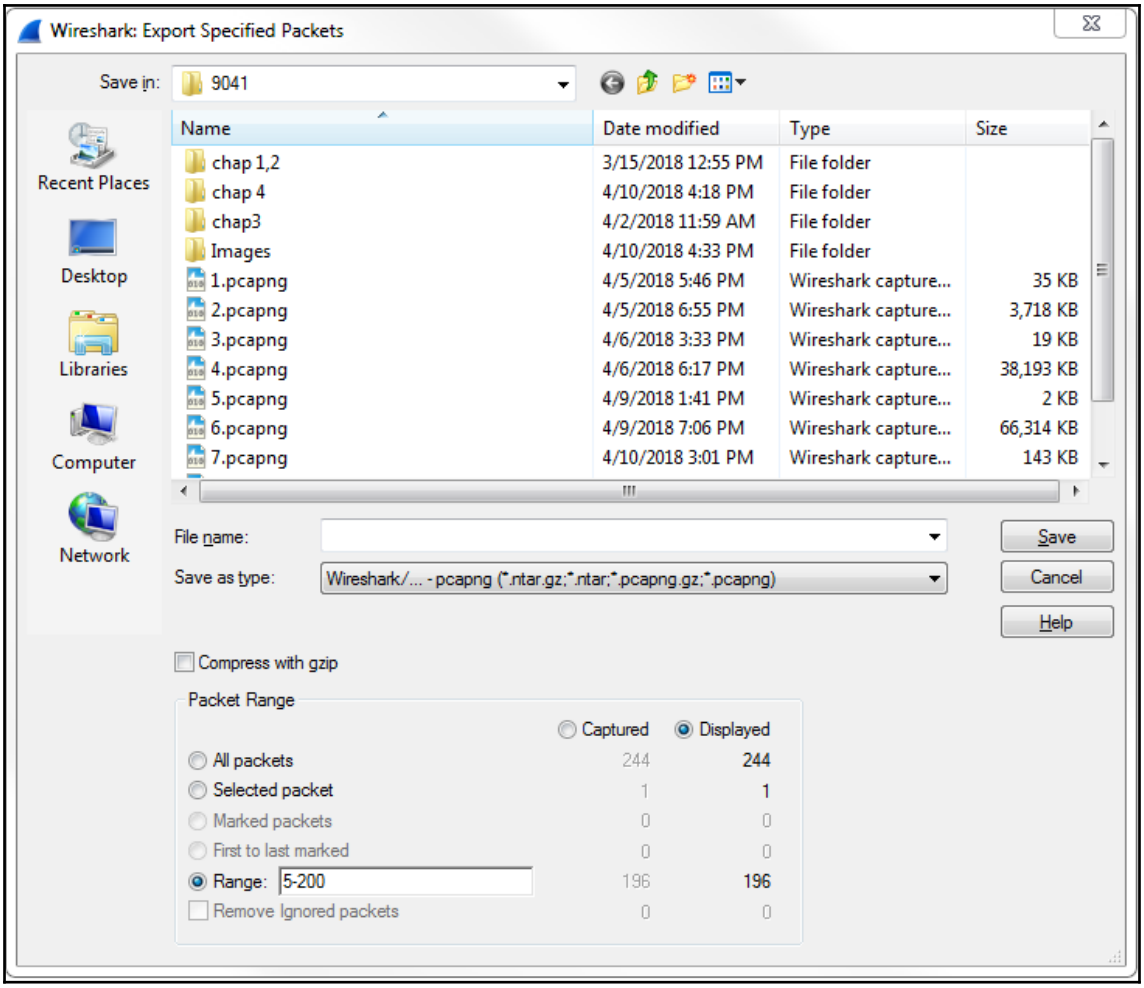

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...

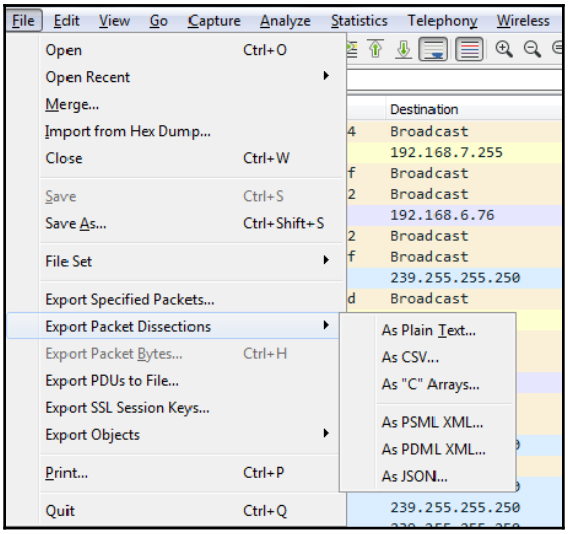

Wireshark · Capture Interfaces
Input
Output
Options
Display Options
Update list of packets in real-time
Automatically scroll during live capture
Show extra capture information dialog
Name Resolution
Resolve MAC Addresses
Resolve network names
Resolve transport names
Stop capture automatically after...
1
packets
1
files
1
kilobytes
1
seconds
Start
Close
Help

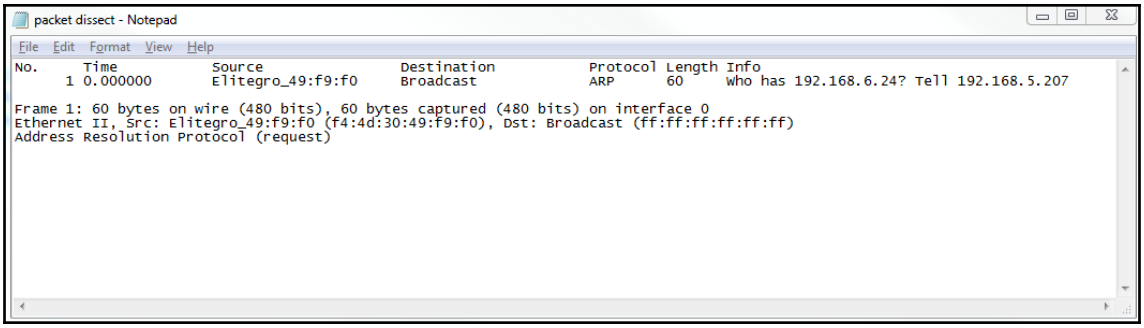

Wireshark: Save file as
Save in:
Documents
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
Custom Office Templates
1/30/2018 12:18 PM
File folder
GitHub
2/21/2017 4:09 PM
File folder
Python Scripts
9/6/2017 12:31 PM
File folder
File name:
packets
Save as type:
Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng
Save
Cancel
Help
Compress with gzip

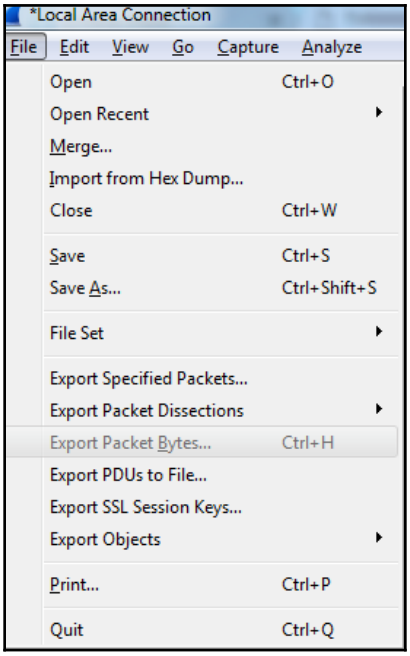

Wireshark: Export Specified Packets
Save in:
Documents
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
Size
Custom Office Templates
1/30/2018 12:18 PM
File folder
GitHub
2/21/2017 4:09 PM
File folder
Python Scripts
9/6/2017 12:31 PM
File folder
packets.pcapng
4/10/2018 1:22 PM
Wireshark capture...
359 KB
packets.pcapng.gz
4/5/2018 6:19 PM
GZ File
1,548 KB
File name:
packet small
Save as type:
Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)
Save
Cancel
Help
Compress with gzip
Packet Range
Captured
Displayed
All packets
171
4
Selected packet
1
1
Marked packets
0
0
First to last marked
0
0
Range:
0
0
Remove Ignored packets
0
0

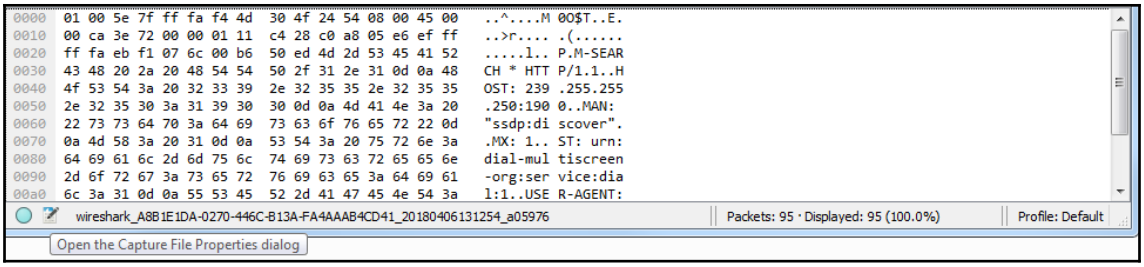

Wireshark: Export Specified Packets
Save in:
Documents
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
Size
Custom Office Templates
1/30/2018 12:18 PM
File folder
GitHub
2/21/2017 4:09 PM
File folder
Python Scripts
9/6/2017 12:31 PM
File folder
packets.pcapng
4/10/2018 1:22 PM
Wireshark capture...
359 KB
packets.pcapng.gz
4/5/2018 6:19 PM
GZ File
1,548 KB
File name:
packet small
Save as type:
Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)
Save
Cancel
Help
Compress with gzip
Packet Range
Captured
Displayed
All packets
171
171
Selected packet
1
1
Marked packets
0
0
First to last marked
0
0
Range:
0
0
Remove Ignored packets
0
0

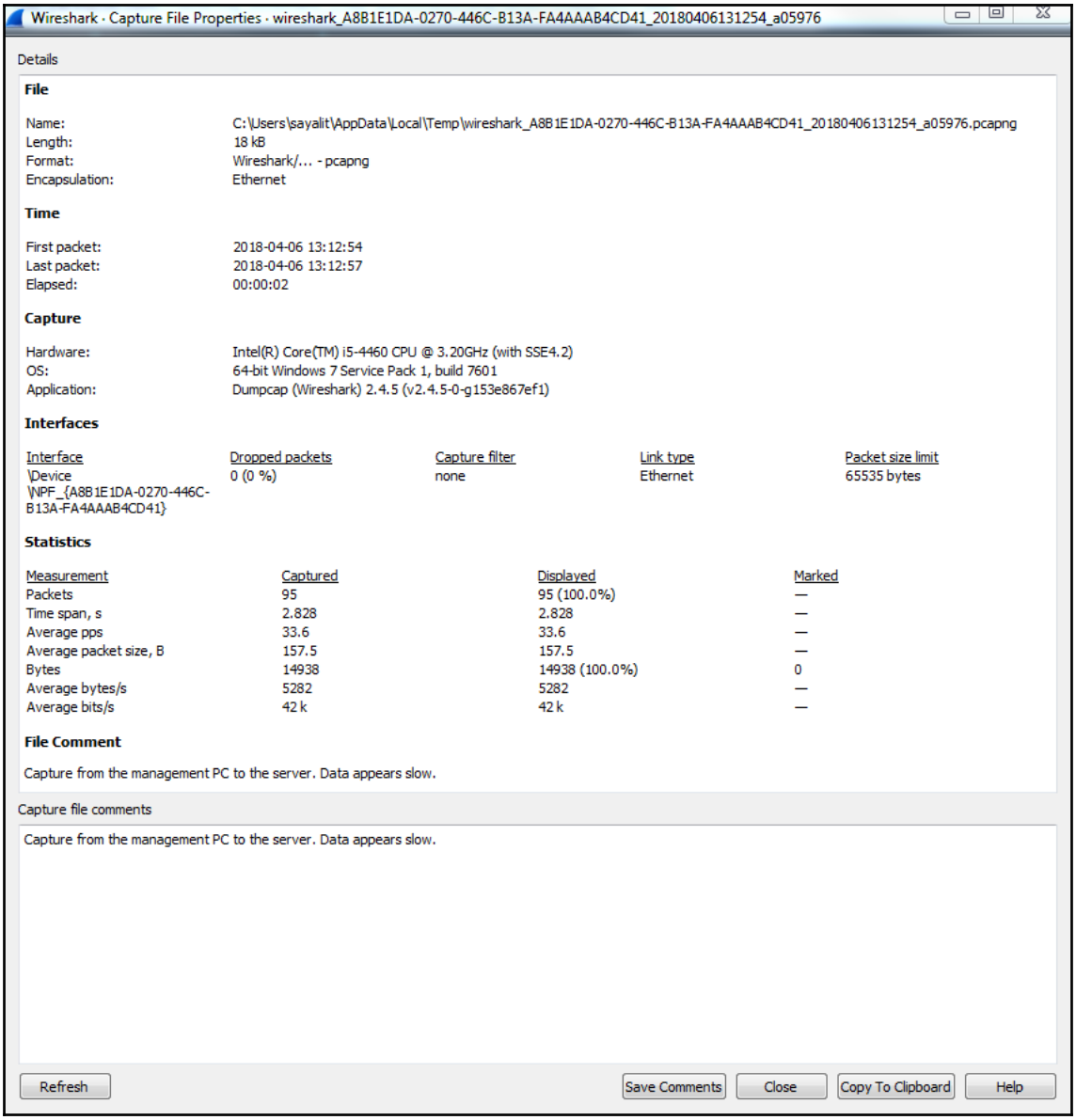

Wireshark: Export Specified Packets
Save in:
9041
Recent Places
Desktop
Libraries
Computer
Network
Name
Date modified
Type
Size
chap 1,2
3/15/2018 12:55 PM
File folder
chap 4
4/10/2018 4:18 PM
File folder
chap3
4/2/2018 11:59 AM
File folder
Images
4/10/2018 4:33 PM
File folder
1.pcapng
4/5/2018 5:46 PM
Wireshark capture...
35 KB
2.pcapng
4/5/2018 6:55 PM
Wireshark capture...
3,718 KB
3.pcapng
4/6/2018 3:33 PM
Wireshark capture...
19 KB
4.pcapng
4/6/2018 6:17 PM
Wireshark capture...
38,193 KB
5.pcapng
4/9/2018 1:41 PM
Wireshark capture...
2 KB
6.pcapng
4/9/2018 7:06 PM
Wireshark capture...
66,314 KB
7.pcapng
4/10/2018 3:01 PM
Wireshark capture...
143 KB
File name:
Save as type:
Wireshark/... - pcapng (*.ntar.gz;*.ntar;*.pcapng.gz;*.pcapng)
Save
Cancel
Help
Compress with gzip
Packet Range
Captured
Displayed
All packets
244
244
Selected packet
1
1
Marked packets
0
0
First to last marked
0
0
Range:
5-200
196
196
Remove Ignored packets
0
0

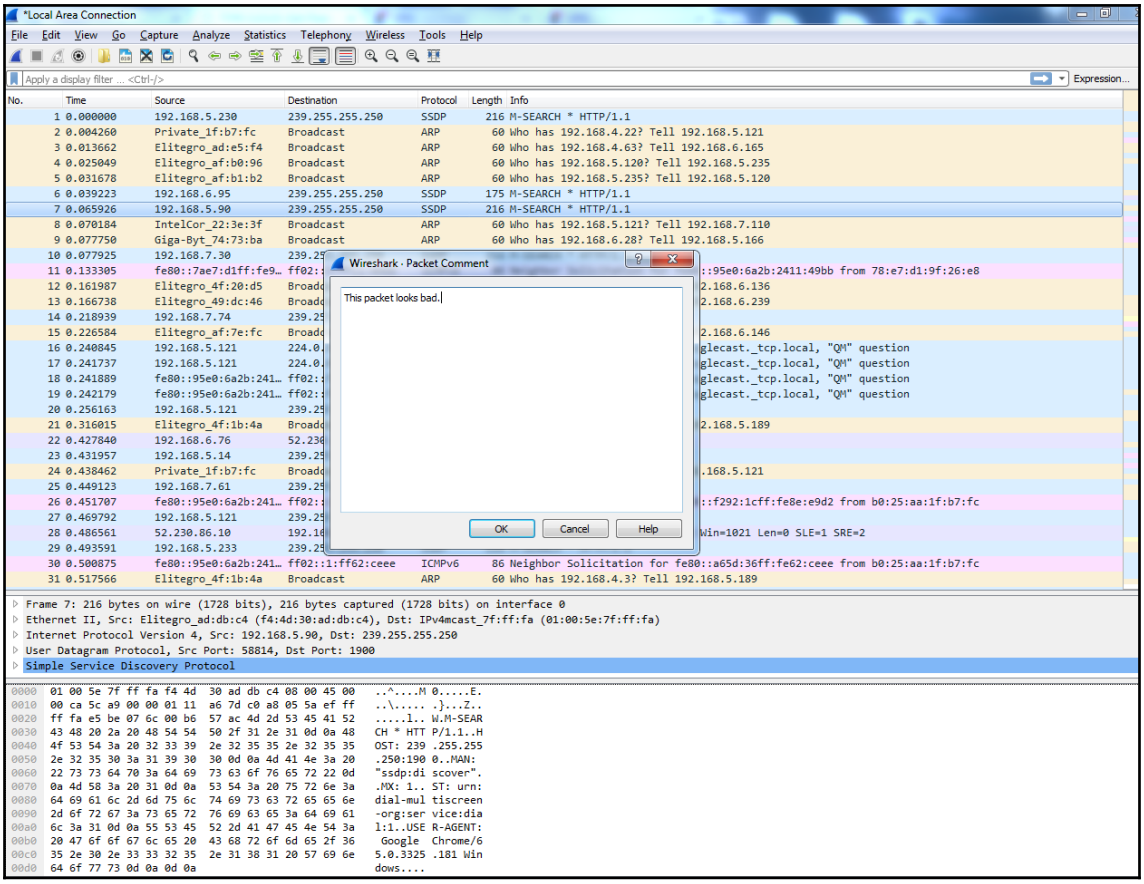

File Edit View Go Capture Analyze Statistics Telephony Wireless
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q
As Plain Text...
As CSV...
As "C" Arrays...
As PSML XML...
As PDML XML...
As JSON...
Destination
Broadcast
192.168.7.255
Broadcast
Broadcast
192.168.6.76
Broadcast
Broadcast
239.255.255.250
Broadcast
239.255.255.250

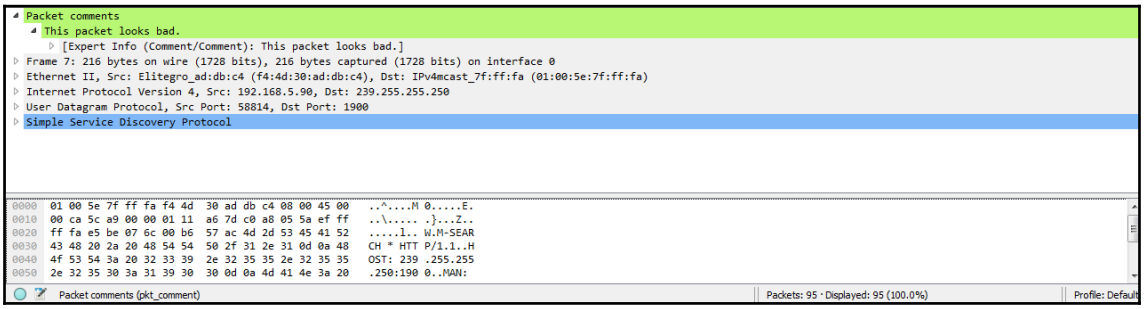

packet dissect - Notepad
File Edit Format View Help
No. Time Source Destination Protocol Length Info
1 0.000000 Elitegro_49:f9:f0 Broadcast ARP 60 Who has 192.168.6.24? Tell 192.168.5.207
Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Elitegro_49:f9:f0 (f4:4d:30:49:f9:f0), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)

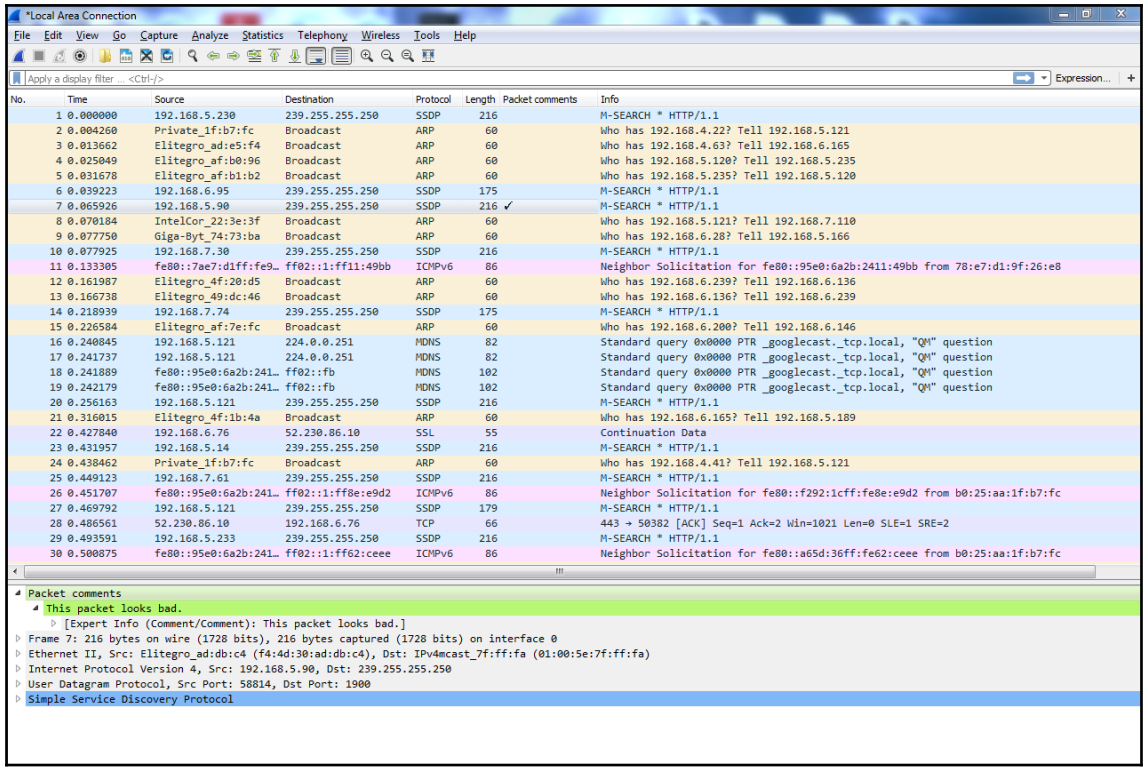

*Local Area Connection
File Edit View Go Capture Analyze
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+H
Export PDUs to File...
Export SSL Session Keys...
Export Objects
Print... Ctrl+P
Quit Ctrl+Q

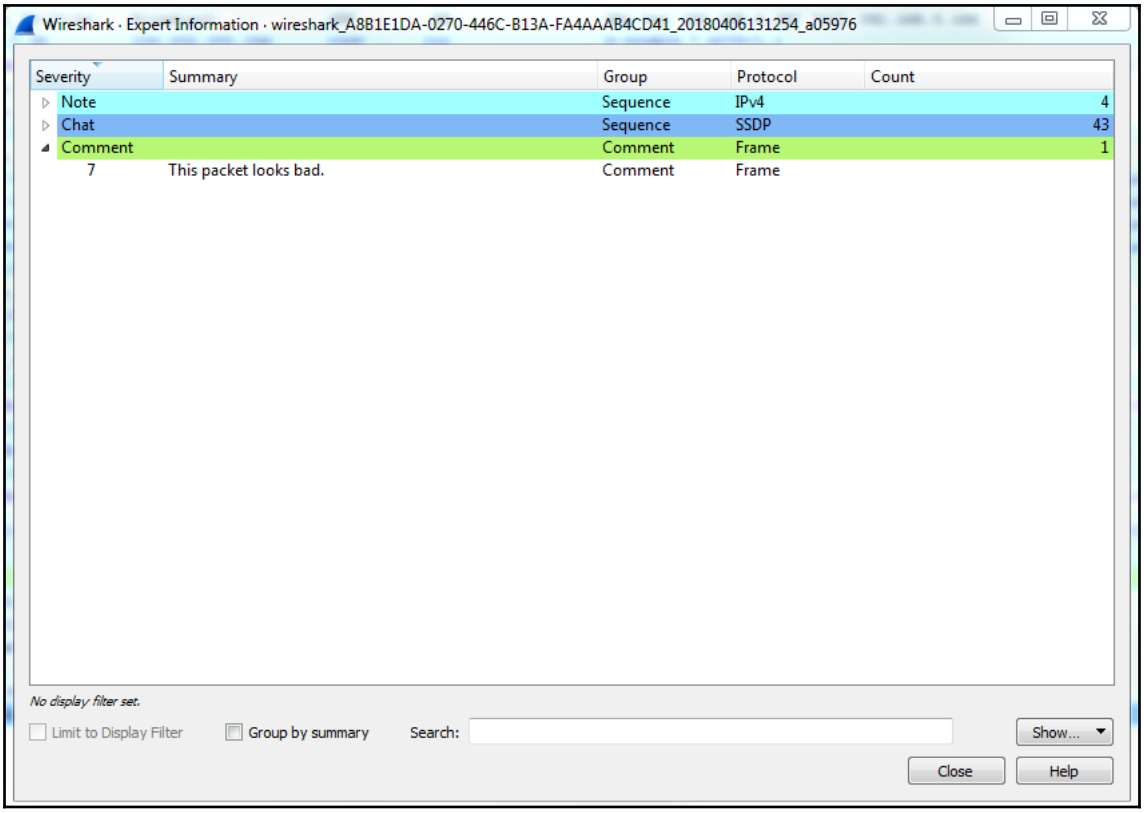

0000 01 00 5e 7f ff fa f4 4d 30 4f 24 54 08 00 45 00 ..^....M 0O$T..E.
0010 00 ca 3e 72 00 00 01 11 c4 28 c0 a8 05 e6 ef ff ..>r.... .(......
0020 ff fa eb f1 07 6c 00 b6 50 ed 4d 2d 53 45 41 52 .....l.. P.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1.. ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-mul tiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:ser vice:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a l:1..USE R-AGENT:
wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976
Packets: 95 · Displayed: 95 (100.0%)
Profile: Default
Open the Capture File Properties dialog

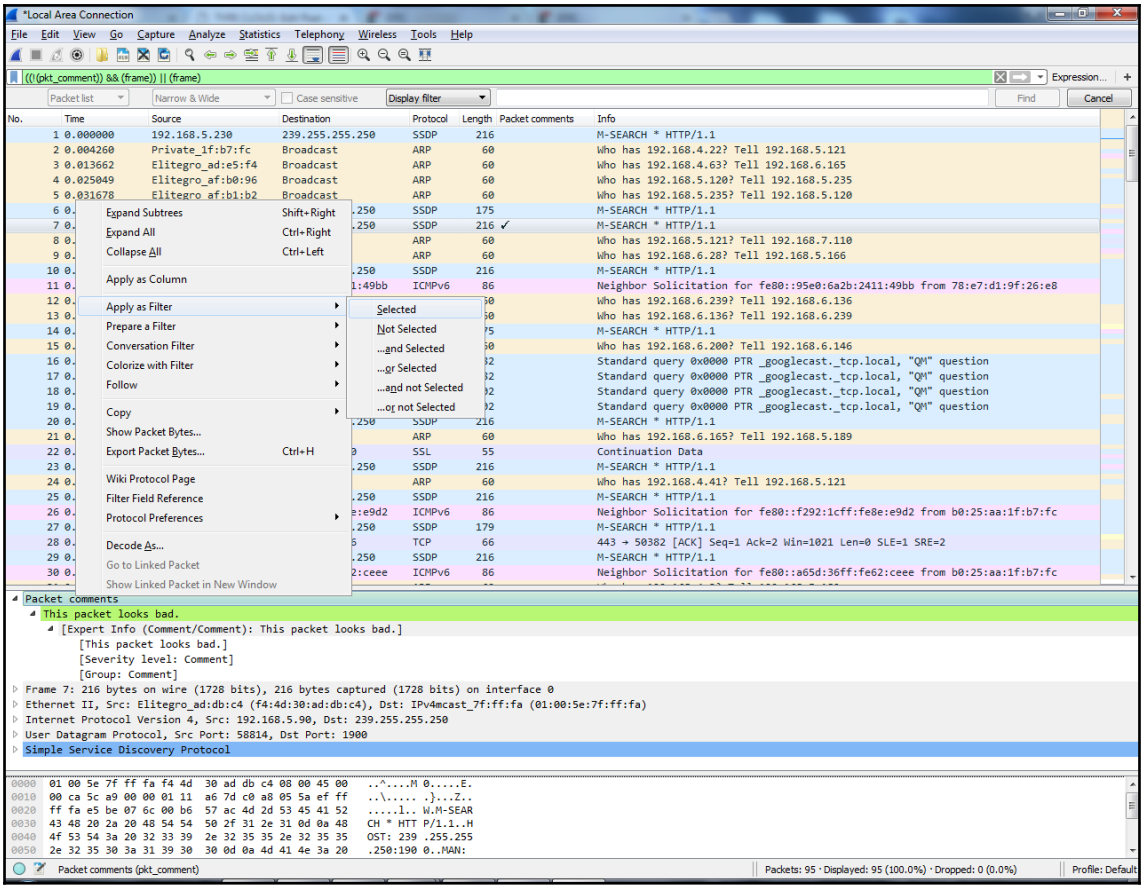

Wireshark · Capture File Properties · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976
Details
File
Name: C:\Users\sayalit\AppData\Local\Temp\wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976.pcapng
Length: 18 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2018-04-06 13:12:54
Last packet: 2018-04-06 13:12:57
Elapsed: 00:00:02
Capture
Hardware: Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz (with SSE4.2)
OS: 64-bit Windows 7 Service Pack 1, build 7601
Application: Dumpcap (Wireshark) 2.4.5 (v2.4.5-0-g153e867ef1)
Interfaces
Interface: \Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41}
Dropped packets: 0 (0 %)
Capture filter: none
Link type: Ethernet
Packet size limit: 65535 bytes
Statistics
Measurement | Captured | Displayed | Marked
Packets | 95 | 95 (100.0%) | —
Time span, s | 2.828 | 2.828 | —
Average pps | 33.6 | 33.6 | —
Average packet size, B | 157.5 | 157.5 | —
Bytes | 14938 | 14938 (100.0%) | 0
Average bytes/s | 5282 | 5282 | —
Average bits/s | 42 k | 42 k | —
File Comment
Capture from the management PC to the server. Data appears slow.
Capture file comments
Capture from the management PC to the server. Data appears slow.
Refresh
Save Comments
Close
Copy To Clipboard
Help

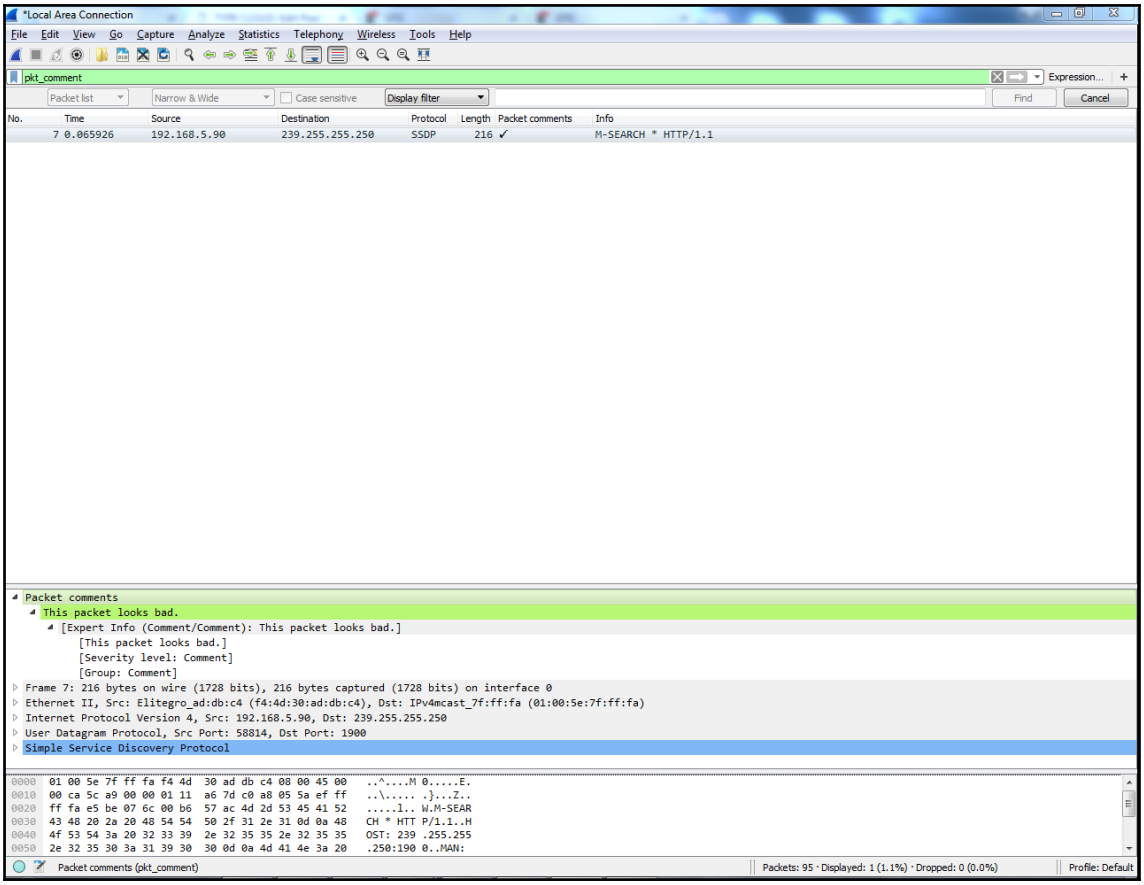

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.5.230 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 0.004260 Private_1f:b7:fc Broadcast ARP 60 Who has 192.168.4.22? Tell 192.168.5.121
3 0.013662 Elitegro_ad:e5:f4 Broadcast ARP 60 Who has 192.168.4.63? Tell 192.168.6.165
4 0.025049 Elitegro_af:b0:96 Broadcast ARP 60 Who has 192.168.5.120? Tell 192.168.5.235
5 0.031678 Elitegro_af:b1:b2 Broadcast ARP 60 Who has 192.168.5.235? Tell 192.168.5.120
6 0.039223 192.168.6.95 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
7 0.065926 192.168.5.90 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
8 0.070184 IntelCor_22:3e:3f Broadcast ARP 60 Who has 192.168.5.121? Tell 192.168.7.110
9 0.077750 Giga-Byt_74:73:ba Broadcast ARP 60 Who has 192.168.6.28? Tell 192.168.5.166
10 0.077925 192.168.7.30 239.25
11 0.133305 fe80::7ae7:d1ff:fe9… ff02::
12 0.161987 Elitegro_4f:20:d5 Broadc
13 0.166738 Elitegro_49:dc:46 Broadc
14 0.218939 192.168.7.74 239.25
15 0.226584 Elitegro_af:7e:fc Broadc
16 0.240845 192.168.5.121 224.0.
17 0.241737 192.168.5.121 224.0.
18 0.241889 fe80::95e0:6a2b:241… ff02::
19 0.242179 fe80::95e0:6a2b:241… ff02::
20 0.256163 192.168.5.121 239.25
21 0.316015 Elitegro_4f:1b:4a Broadc
22 0.427840 192.168.6.76 52.236
23 0.431957 192.168.5.14 239.25
24 0.438462 Private_1f:b7:fc Broadc
25 0.449123 192.168.7.61 239.25
26 0.451707 fe80::95e0:6a2b:241… ff02::
27 0.469792 192.168.5.121 239.25
28 0.486561 52.230.86.10 192.16
29 0.493591 192.168.5.233 239.25
30 0.500875 fe80::95e0:6a2b:241… ff02::1:ff62:ceee ICMPv6 86 Neighbor Solicitation for fe80::a65d:36ff:fe62:ceee from b0:25:aa:1f:b7:fc
31 0.517566 Elitegro_4f:1b:4a Broadcast ARP 60 Who has 192.168.4.3? Tell 192.168.5.189
Wireshark · Packet Comment
This packet looks bad.
OK Cancel Help
::95e0:6a2b:2411:49bb from 78:e7:d1:9f:26:e8
2.168.6.136
2.168.6.239
2.168.6.146
glecast._tcp.local, "QM" question
glecast._tcp.local, "QM" question
glecast._tcp.local, "QM" question
glecast._tcp.local, "QM" question
2.168.5.189
.168.5.121
::f292:1cff:fe8e:e9d2 from b0:25:aa:1f:b7:fc
Win=1021 Len=0 SLE=1 SRE=2
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa f4 4d 30 ad db c4 08 00 45 00 ..^....M 0.....E.
0010 00 ca 5c a9 00 00 01 11 a6 7d c0 a8 05 5a ef ff ..\..... .}...Z..
0020 ff fa e5 be 07 6c 00 b6 57 ac 4d 2d 53 45 41 52 .....l.. W.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d "ssdp:di scover".
0070 0a 4d 58 3a 20 31 0d 0a 53 54 3a 20 75 72 6e 3a .MX: 1.. ST: urn:
0080 64 69 61 6c 2d 6d 75 6c 74 69 73 63 72 65 65 6e dial-mul tiscreen
0090 2d 6f 72 67 3a 73 65 72 76 69 63 65 3a 64 69 61 -org:ser vice:dia
00a0 6c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a l:1..USE R-AGENT:
00b0 20 47 6f 6f 67 6c 65 20 43 68 72 6f 6d 65 2f 36 Google Chrome/6
00c0 35 2e 30 2e 33 33 32 35 2e 31 38 31 20 57 69 6e 5.0.3325 .181 Win
00d0 64 6f 77 73 0d 0a 0d 0a dows....

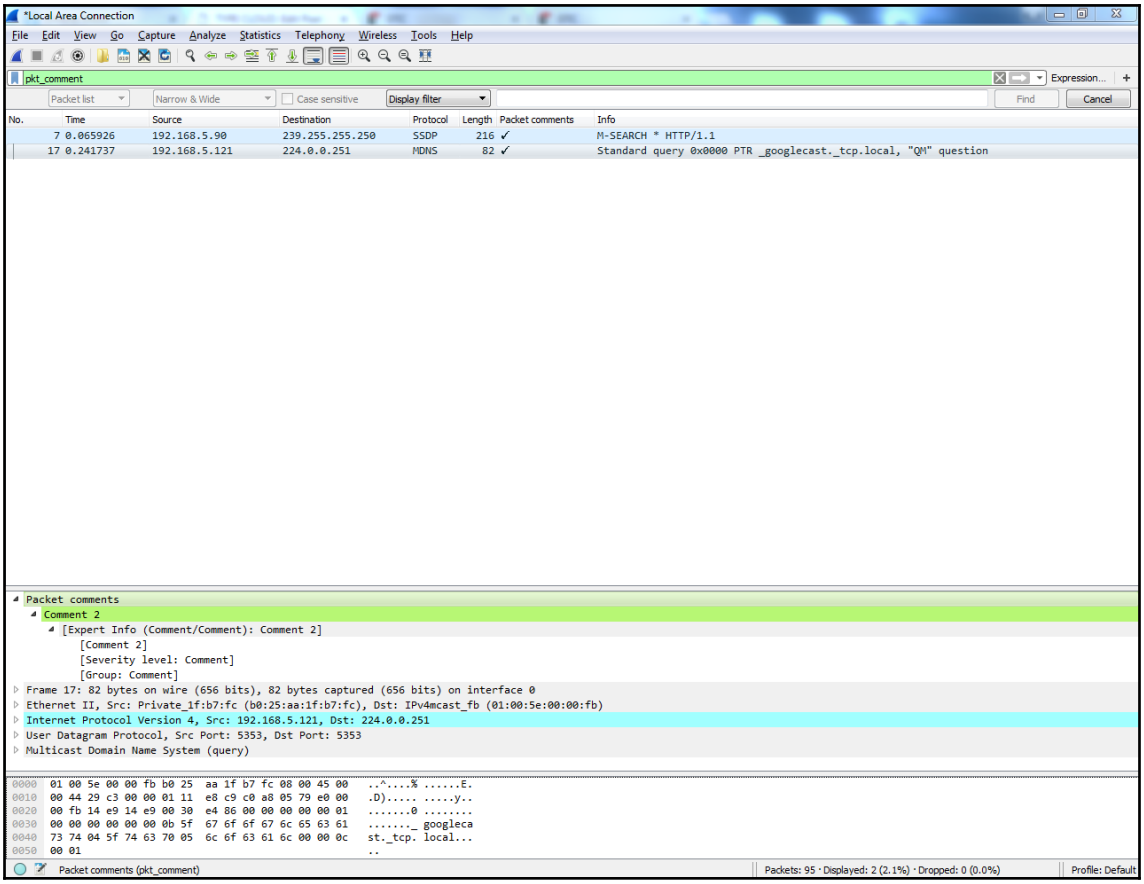

Packet comments
This packet looks bad.
[Expert Info (Comment/Comment): This packet looks bad.]
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa f4 4d 30 ad db c4 08 00 45 00 ..^....M 0.....E.
0010 00 ca 5c a9 00 00 01 11 a6 7d c0 a8 05 5a ef ff ..\..... .}...Z..
0020 ff fa e5 be 07 6c 00 b6 57 ac 4d 2d 53 45 41 52 .....l.. W.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
Packet comments (pkt_comment)
Packets: 95 · Displayed: 95 (100.0%)
Profile: Default

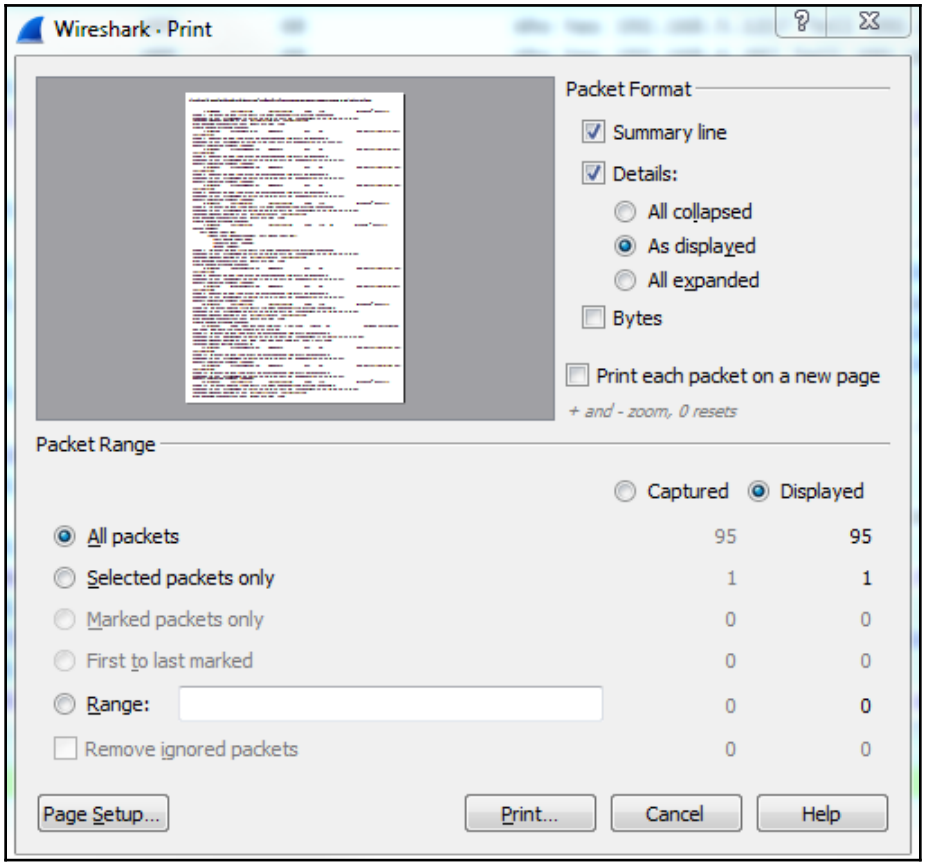

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Packet comments Info
1 0.000000 192.168.5.230 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 0.004260 Private_1f:b7:fc Broadcast ARP 60 Who has 192.168.4.22? Tell 192.168.5.121
3 0.013662 Elitegro_ad:e5:f4 Broadcast ARP 60 Who has 192.168.4.63? Tell 192.168.6.165
4 0.025049 Elitegro_af:b0:96 Broadcast ARP 60 Who has 192.168.5.120? Tell 192.168.5.235
5 0.031678 Elitegro_af:b1:b2 Broadcast ARP 60 Who has 192.168.5.235? Tell 192.168.5.120
6 0.039223 192.168.6.95 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
7 0.065926 192.168.5.90 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
8 0.070184 IntelCor_22:3e:3f Broadcast ARP 60 Who has 192.168.5.121? Tell 192.168.7.110
9 0.077750 Giga-Byt_74:73:ba Broadcast ARP 60 Who has 192.168.6.28? Tell 192.168.5.166
10 0.077925 192.168.7.30 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
11 0.133305 fe80::7ae7:d1ff:fe9… ff02::1:ff11:49bb ICMPv6 86 Neighbor Solicitation for fe80::95e0:6a2b:2411:49bb from 78:e7:d1:9f:26:e8
12 0.161987 Elitegro_4f:20:d5 Broadcast ARP 60 Who has 192.168.6.239? Tell 192.168.6.136
13 0.166738 Elitegro_49:dc:46 Broadcast ARP 60 Who has 192.168.6.136? Tell 192.168.6.239
14 0.218939 192.168.7.74 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
15 0.226584 Elitegro_af:7e:fc Broadcast ARP 60 Who has 192.168.6.200? Tell 192.168.6.146
16 0.240845 192.168.5.121 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
17 0.241737 192.168.5.121 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
18 0.241889 fe80::95e0:6a2b:241… ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
19 0.242179 fe80::95e0:6a2b:241… ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
20 0.256163 192.168.5.121 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
21 0.316015 Elitegro_4f:1b:4a Broadcast ARP 60 Who has 192.168.6.165? Tell 192.168.5.189
22 0.427840 192.168.6.76 52.230.86.10 SSL 55 Continuation Data
23 0.431957 192.168.5.14 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
24 0.438462 Private_1f:b7:fc Broadcast ARP 60 Who has 192.168.4.41? Tell 192.168.5.121
25 0.449123 192.168.7.61 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
26 0.451707 fe80::95e0:6a2b:241… ff02::1:ff8e:e9d2 ICMPv6 86 Neighbor Solicitation for fe80::f292:1cff:fe8e:e9d2 from b0:25:aa:1f:b7:fc
27 0.469792 192.168.5.121 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
28 0.486561 52.230.86.10 192.168.6.76 TCP 66 443 → 50382 [ACK] Seq=1 Ack=2 Win=1021 Len=0 SLE=1 SRE=2
29 0.493591 192.168.5.233 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
30 0.500875 fe80::95e0:6a2b:241… ff02::1:ff62:ceee ICMPv6 86 Neighbor Solicitation for fe80::a65d:36ff:fe62:ceee from b0:25:aa:1f:b7:fc
Packet comments
This packet looks bad.
[Expert Info (Comment/Comment): This packet looks bad.]
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol

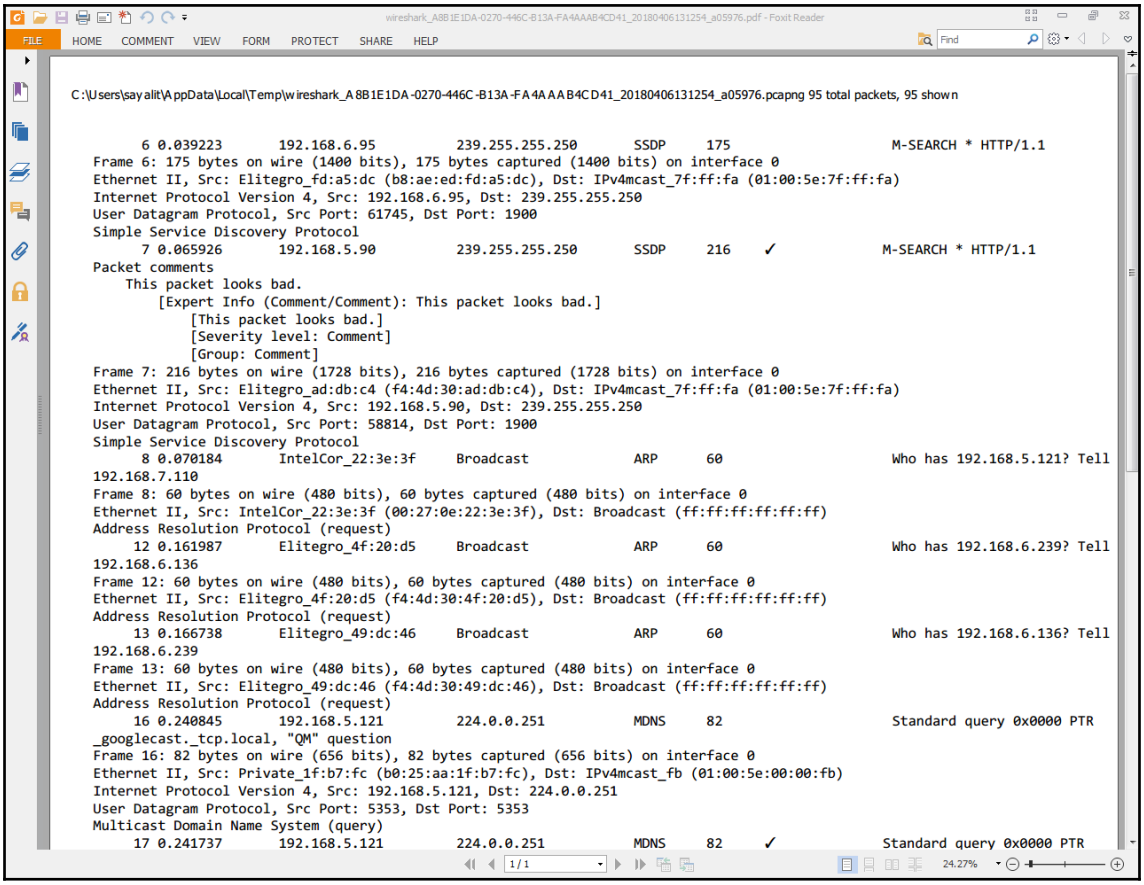

Wireshark · Expert Information · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976
Severity
Summary
Group
Protocol
Count
Note
Sequence
IPv4
4
Chat
Sequence
SSDP
43
Comment
Comment
Frame
1
7
This packet looks bad.
Comment
Frame
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

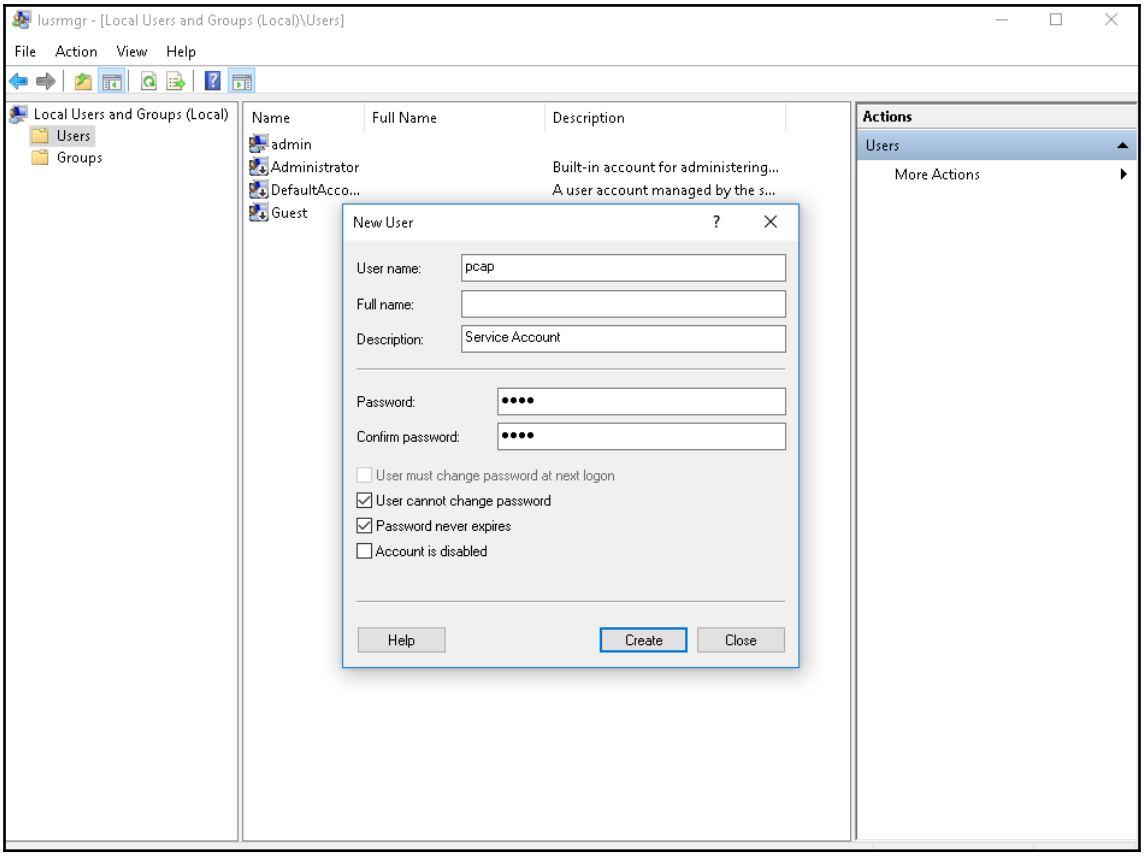

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(((pkt_comment)) && (frame)) || (frame)
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel
No. Time Source Destination Protocol Length Packet comments Info
1 0.000000 192.168.5.230 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 0.004260 Private_1f:b7:fc Broadcast ARP 60 Who has 192.168.4.22? Tell 192.168.5.121
3 0.013662 Elitegro_ad:e5:f4 Broadcast ARP 60 Who has 192.168.4.63? Tell 192.168.6.165
4 0.025049 Elitegro_af:b0:96 Broadcast ARP 60 Who has 192.168.5.120? Tell 192.168.5.235
5 0.031678 Elitegro_af:b1:b2 Broadcast ARP 60 Who has 192.168.5.235? Tell 192.168.5.120
6 0. .250 SSDP 175 M-SEARCH * HTTP/1.1
7 0. .250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
8 0. ARP 60 Who has 192.168.5.121? Tell 192.168.7.110
9 0. ARP 60 Who has 192.168.6.28? Tell 192.168.5.166
10 0. .250 SSDP 216 M-SEARCH * HTTP/1.1
11 0. 1:49bb ICMPv6 86 Neighbor Solicitation for fe80::95e0:6a2b:2411:49bb from 78:e7:d1:9f:26:e8
12 0. Who has 192.168.6.239? Tell 192.168.6.136
13 0. Who has 192.168.6.136? Tell 192.168.6.239
14 0. M-SEARCH * HTTP/1.1
15 0. Who has 192.168.6.200? Tell 192.168.6.146
16 0. Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
17 0. Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
18 0. Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
19 0. Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
20 0. .250 SSDP 216 M-SEARCH * HTTP/1.1
21 0. ARP 60 Who has 192.168.6.165? Tell 192.168.5.189
22 0. 0 SSL 55 Continuation Data
23 0. .250 SSDP 216 M-SEARCH * HTTP/1.1
24 0. ARP 60 Who has 192.168.4.41? Tell 192.168.5.121
25 0. .250 SSDP 216 M-SEARCH * HTTP/1.1
26 0. e:e9d2 ICMPv6 86 Neighbor Solicitation for fe80::f292:1cff:fe8e:e9d2 from b0:25:aa:1f:b7:fc
27 0. .250 SSDP 179 M-SEARCH * HTTP/1.1
28 0. 5 TCP 66 443 → 50382 [ACK] Seq=1 Ack=2 Win=1021 Len=0 SLE=1 SRE=2
29 0. .250 SSDP 216 M-SEARCH * HTTP/1.1
30 0. 2:ceee ICMPv6 86 Neighbor Solicitation for fe80::a65d:36ff:fe62:ceee from b0:25:aa:1f:b7:fc
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Packet comments
This packet looks bad.
[Expert Info (Comment/Comment): This packet looks bad.]
[This packet looks bad.]
[Severity level: Comment]
[Group: Comment]
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa f4 4d 30 ad db c4 08 00 45 00 ..^....M 0.....E.
0010 00 ca 5c a9 00 00 01 11 a6 7d c0 a8 05 5a ef ff ..\..... .}...Z..
0020 ff fa e5 be 07 6c 00 b6 57 ac 4d 2d 53 45 41 52 .....l.. W.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
Packet comments (pkt_comment)
Packets: 95 · Displayed: 95 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

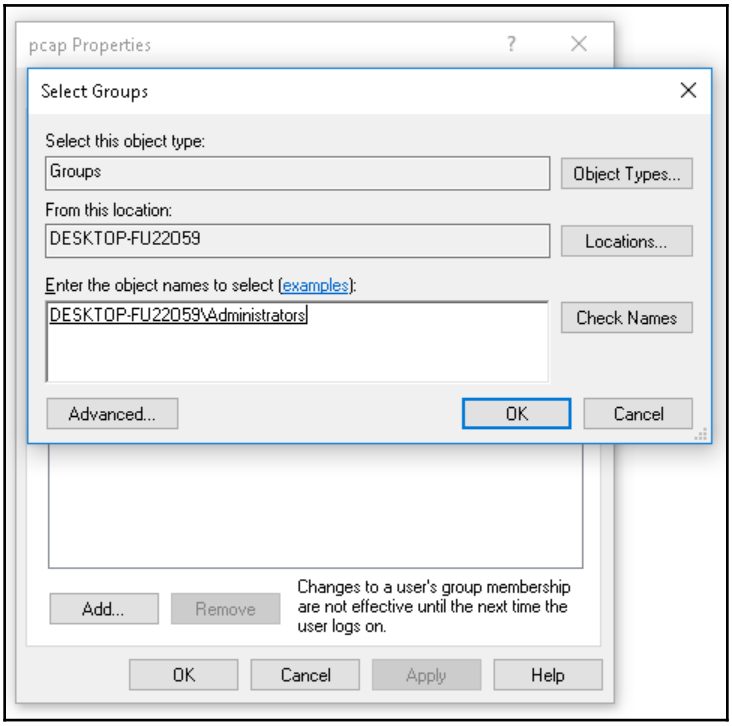

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pkt_comment
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel
No. Time Source Destination Protocol Length Packet comments Info
7 0.065926 192.168.5.90 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
Packet comments
This packet looks bad.
[Expert Info (Comment/Comment): This packet looks bad.]
[This packet looks bad.]
[Severity level: Comment]
[Group: Comment]
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol
0000 01 00 5e 7f ff fa f4 4d 30 ad db c4 08 00 45 00 ..^....M 0.....E.
0010 00 ca 5c a9 00 00 01 11 a6 7d c0 a8 05 5a ef ff ..\..... .}...Z..
0020 ff fa e5 be 07 6c 00 b6 57 ac 4d 2d 53 45 41 52 .....l.. W.M-SEAR
0030 43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48 CH * HTT P/1.1..H
0040 4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35 OST: 239 .255.255
0050 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 .250:190 0..MAN:
Packet comments (pkt_comment)
Packets: 95 · Displayed: 1 (1.1%) · Dropped: 0 (0.0%)
Profile: Default

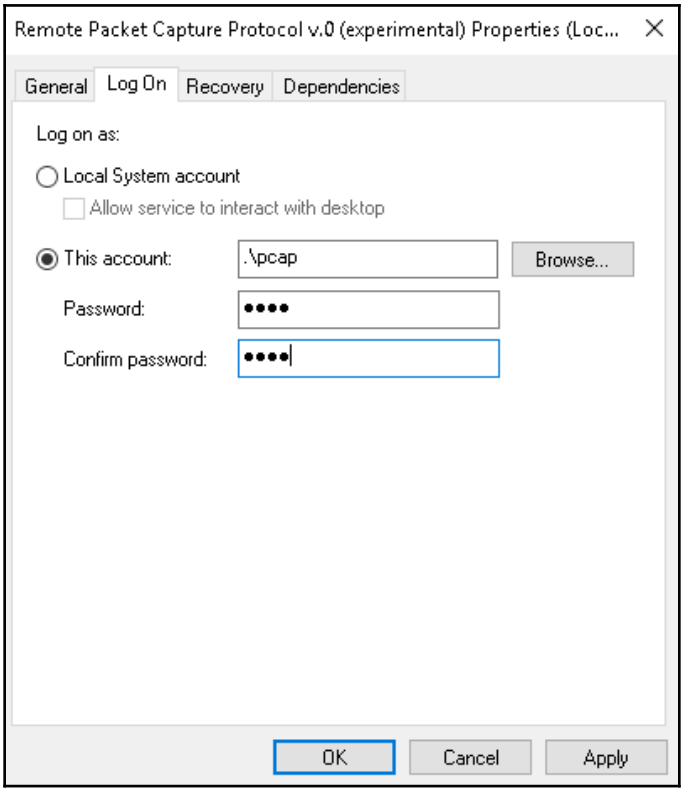

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pkt_comment
Expression...
Packet list
Narrow & Wide
Case sensitive
Display filter
Find
Cancel
No. Time Source Destination Protocol Length Packet comments Info
7 0.065926 192.168.5.90 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
17 0.241737 192.168.5.121 224.0.0.251 MDNS 82 ✓ Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
Packet comments
Comment 2
[Expert Info (Comment/Comment): Comment 2]
[Comment 2]
[Severity level: Comment]
[Group: Comment]
Frame 17: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: Private_1f:b7:fc (b0:25:aa:1f:b7:fc), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.5.121, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
0000 01 00 5e 00 00 fb b0 25 aa 1f b7 fc 08 00 45 00 ..^....% ......E.
0010 00 44 29 c3 00 00 01 11 e8 c9 c0 a8 05 79 e0 00 .D)..... .....y..
0020 00 fb 14 e9 14 e9 00 30 e4 86 00 00 00 00 00 01 ....0 ....
0030 00 00 00 00 00 00 0b 5f 67 6f 6f 67 6c 65 63 61 ...._ googleca
0040 73 74 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 0c st._tcp. local...
0050 00 01 ..
Packet comments (pkt_comment)
Packets: 95 · Displayed: 2 (2.1%) · Dropped: 0 (0.0%)
Profile: Default

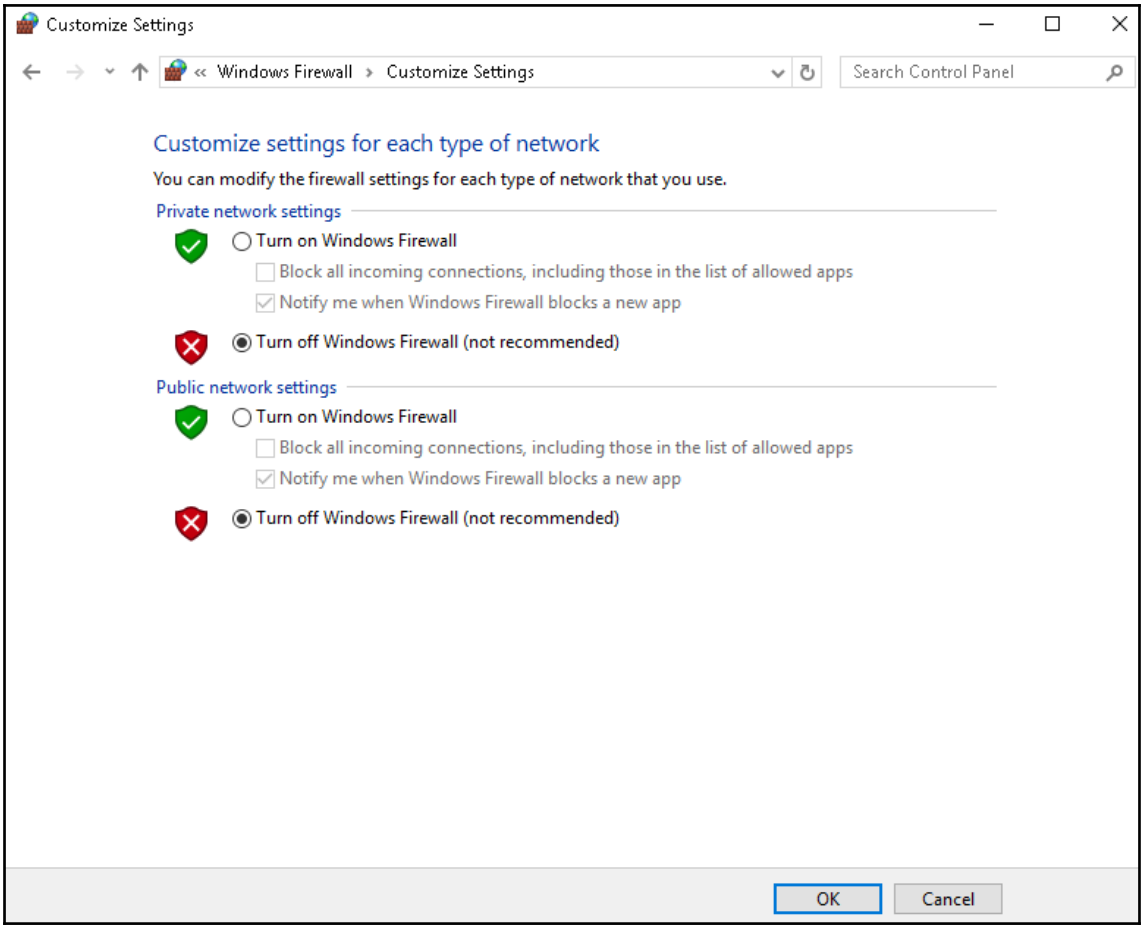

Wireshark · Print
Packet Format
Summary line
Details:
All collapsed
As displayed
All expanded
Bytes
Print each packet on a new page
+ and - zoom, 0 resets
Packet Range
Captured
Displayed
All packets 95 95
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0
Page Setup...
Print...
Cancel
Help

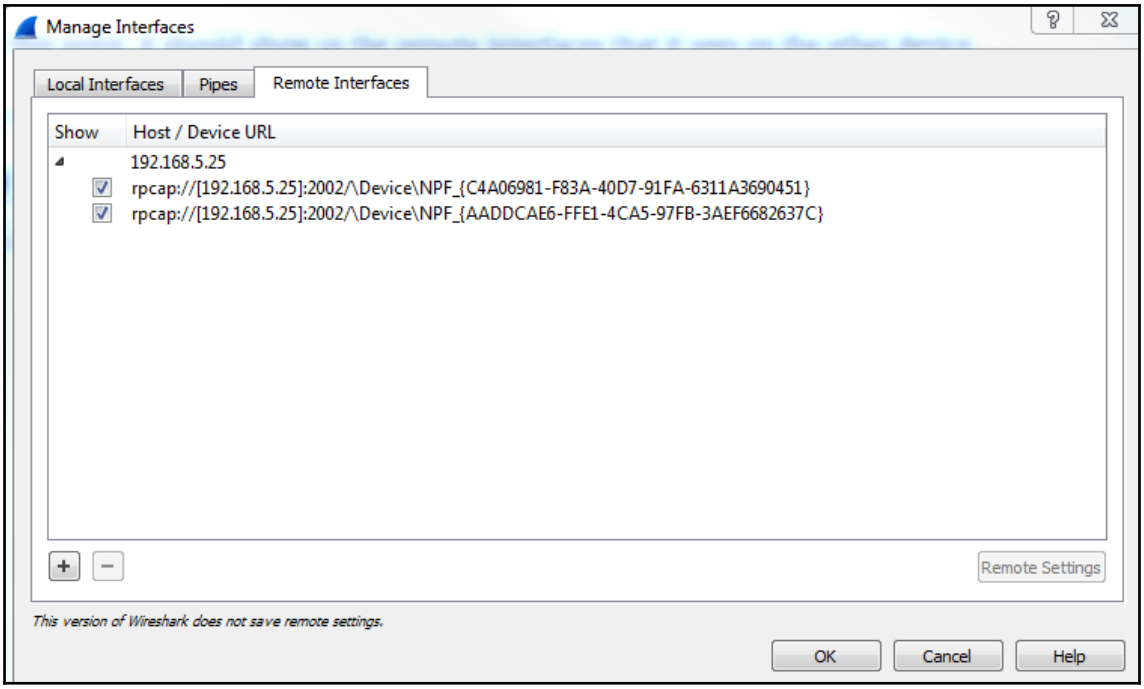

wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976.pdf - Foxit Reader
FILE HOME COMMENT VIEW FORM PROTECT SHARE HELP
Find
C:\Users\sayalit\AppData\Local\Temp\wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180406131254_a05976.pcapng 95 total packets, 95 shown
6 0.039223 192.168.6.95 239.255.255.250 SSDP 175 M-SEARCH * HTTP/1.1
Frame 6: 175 bytes on wire (1400 bits), 175 bytes captured (1400 bits) on interface 0
Ethernet II, Src: Elitegro_fd:a5:dc (b8:ae:ed:fd:a5:dc), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.6.95, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 61745, Dst Port: 1900
Simple Service Discovery Protocol
7 0.065926 192.168.5.90 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
Packet comments
This packet looks bad.
[Expert Info (Comment/Comment): This packet looks bad.]
[This packet looks bad.]
[Severity level: Comment]
[Group: Comment]
Frame 7: 216 bytes on wire (1728 bits), 216 bytes captured (1728 bits) on interface 0
Ethernet II, Src: Elitegro_ad:db:c4 (f4:4d:30:ad:db:c4), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
Internet Protocol Version 4, Src: 192.168.5.90, Dst: 239.255.255.250
User Datagram Protocol, Src Port: 58814, Dst Port: 1900
Simple Service Discovery Protocol
8 0.070184 IntelCor_22:3e:3f Broadcast ARP 60 Who has 192.168.5.121? Tell 192.168.7.110
Frame 8: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: IntelCor_22:3e:3f (00:27:0e:22:3e:3f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
12 0.161987 Elitegro_4f:20:d5 Broadcast ARP 60 Who has 192.168.6.239? Tell 192.168.6.136
Frame 12: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Elitegro_4f:20:d5 (f4:4d:30:4f:20:d5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
13 0.166738 Elitegro_49:dc:46 Broadcast ARP 60 Who has 192.168.6.136? Tell 192.168.6.239
Frame 13: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Elitegro_49:dc:46 (f4:4d:30:49:dc:46), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
16 0.240845 192.168.5.121 224.0.0.251 MDNS 82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
Frame 16: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
Ethernet II, Src: Private_1f:b7:fc (b0:25:aa:1f:b7:fc), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
Internet Protocol Version 4, Src: 192.168.5.121, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (query)
17 0.241737 192.168.5.121 224.0.0.251 MDNS 82 ✓ Standard query 0x0000 PTR
1 / 1
24.27%

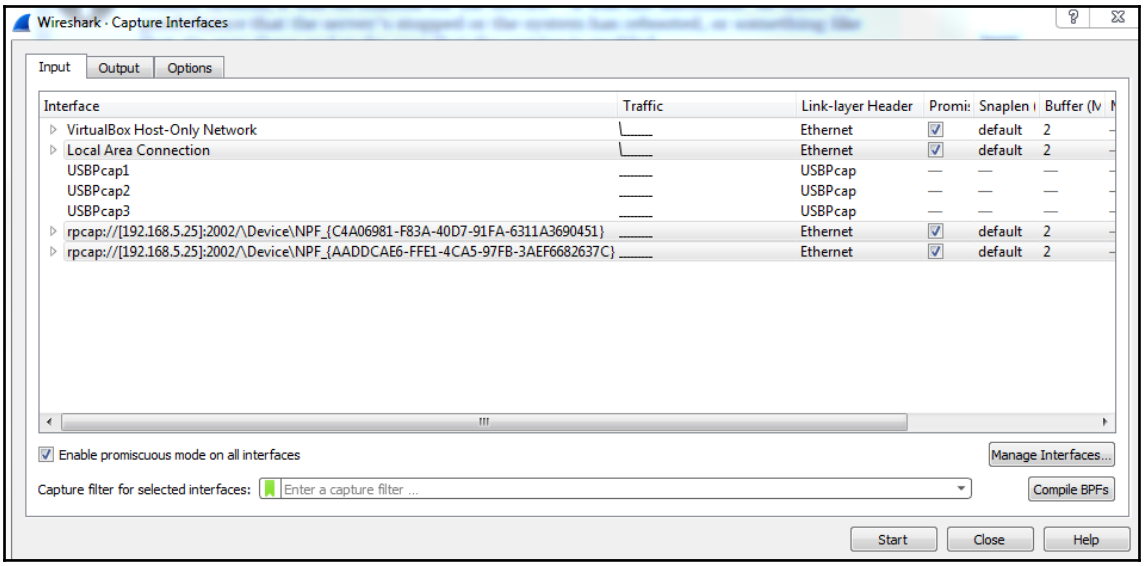

lusrmgr - [Local Users and Groups (Local)\Users]
File Action View Help
Local Users and Groups (Local)
Users
Groups
Name
Full Name
Description
admin
Administrator
Built-in account for administering...
DefaultAcco...
A user account managed by the s...
Guest
New User
User name:
pcap
Full name:
Description:
Service Account
Password:
Confirm password:
User must change password at next logon
User cannot change password
Password never expires
Account is disabled
Help
Create
Close
Actions
Users
More Actions


pcap Properties
Select Groups
Select this object type:
Groups
Object Types...
From this location:
DESKTOP-FU22059
Locations...
Enter the object names to select (examples):
DESKTOP-FU22059\Administrators
Check Names
Advanced...
OK
Cancel
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help

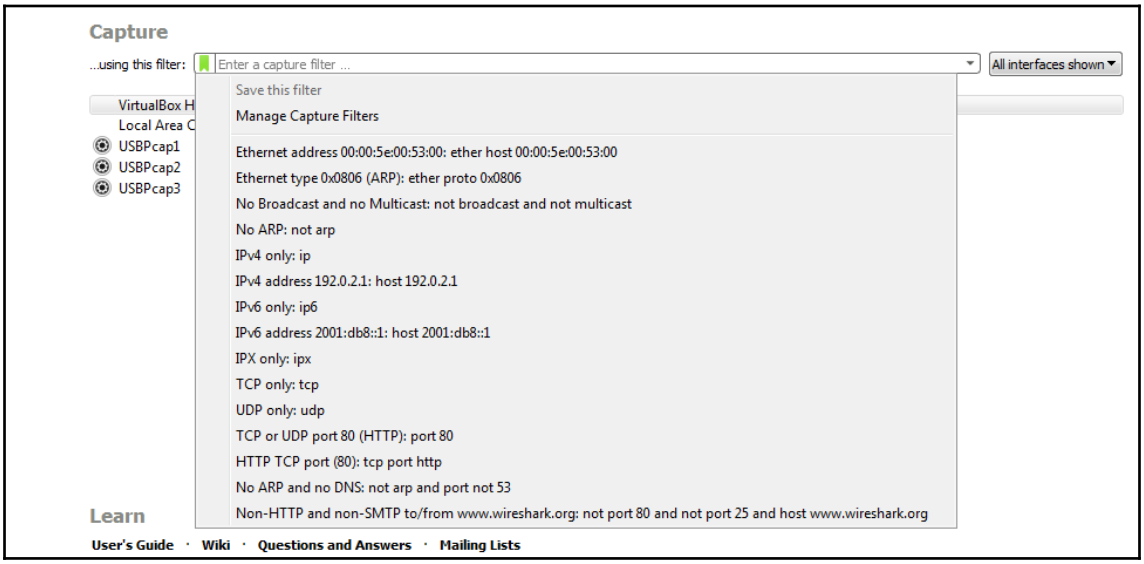

Remote Packet Capture Protocol v.0 (experimental) Properties (Loc...
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
.\pcap
Browse...
Password:
Confirm password:
OK
Cancel
Apply

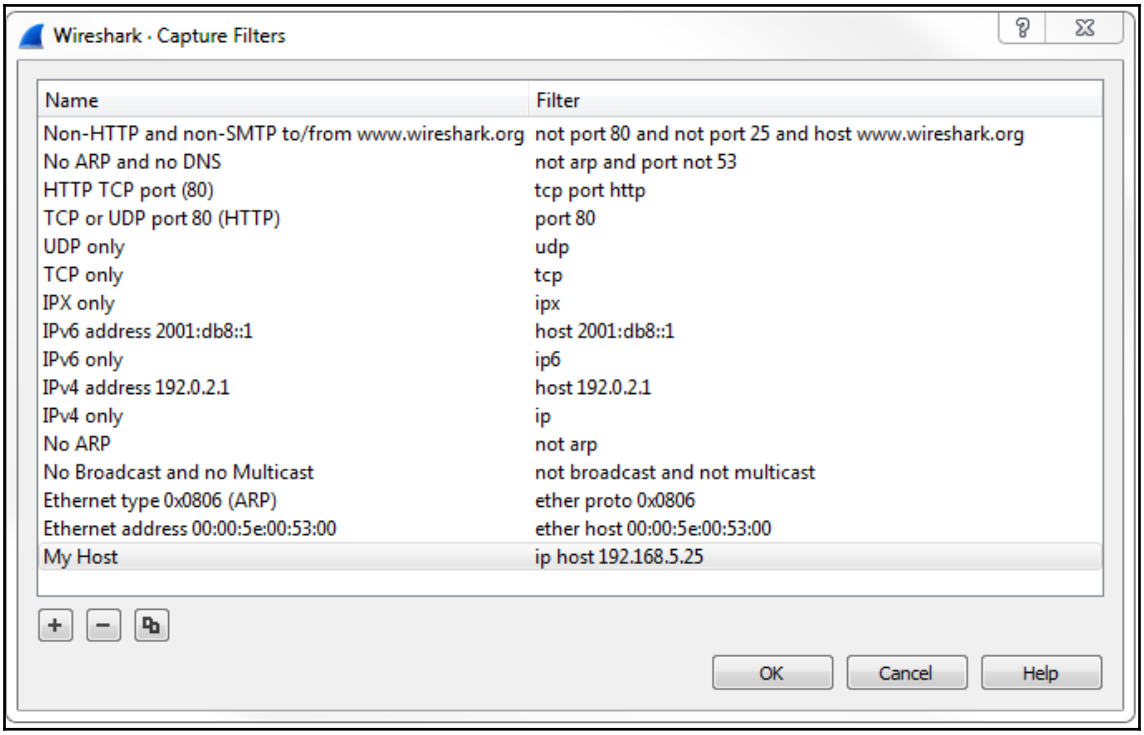

Customize Settings
« Windows Firewall › Customize Settings
Search Control Panel
Customize settings for each type of network
You can modify the firewall settings for each type of network that you use.
Private network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
Public network settings
Turn on Windows Firewall
Block all incoming connections, including those in the list of allowed apps
Notify me when Windows Firewall blocks a new app
Turn off Windows Firewall (not recommended)
OK
Cancel

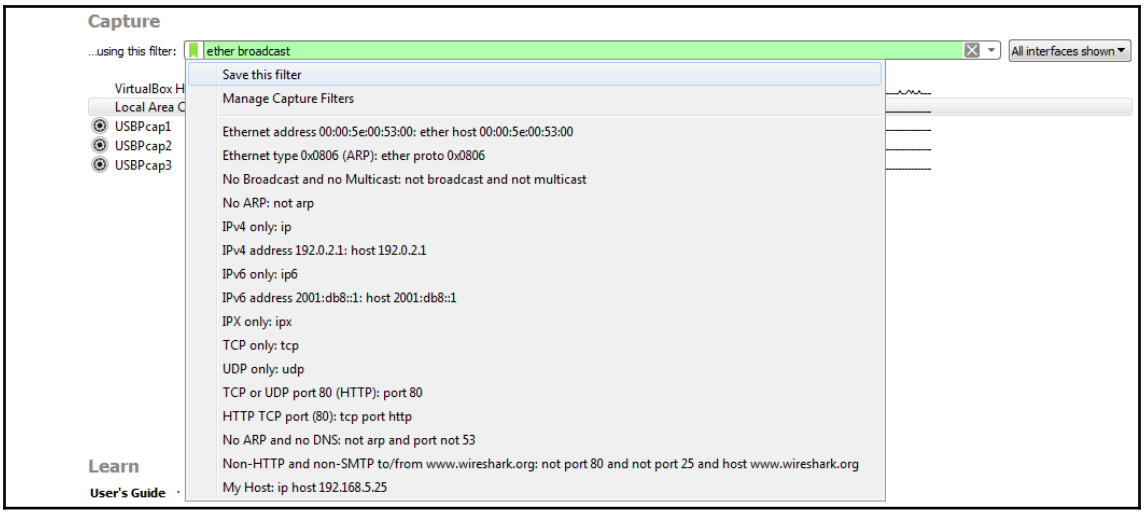

Manage Interfaces
Local Interfaces
Pipes
Remote Interfaces
Show
Host / Device URL
192.168.5.25
rpcap://[192.168.5.25]:2002/\Device\NPF_{C4A06981-F83A-40D7-91FA-6311A3690451}
rpcap://[192.168.5.25]:2002/\Device\NPF_{AADDCAE6-FFE1-4CA5-97FB-3AEF6682637C}
Remote Settings
This version of Wireshark does not save remote settings.
OK
Cancel
Help

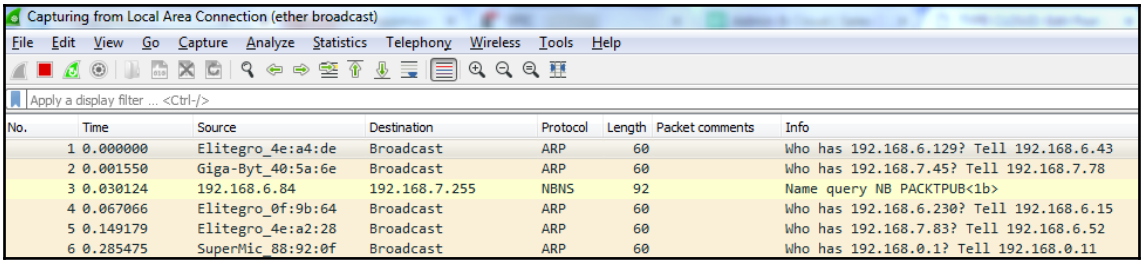

Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promi
Snaplen
Buffer (M
VirtualBox Host-Only Network
Local Area Connection
USBPcap1
USBPcap2
USBPcap3
rpcap://[192.168.5.25]:2002/\Device\NPF_{C4A06981-F83A-40D7-91FA-6311A3690451}
rpcap://[192.168.5.25]:2002/\Device\NPF_{AADDCAE6-FFE1-4CA5-97FB-3AEF6682637C}
Ethernet
USBPcap
default
2
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Close
Help

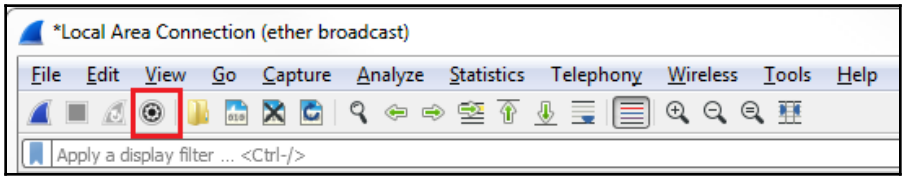
Chapter 03: Filtering Traffic

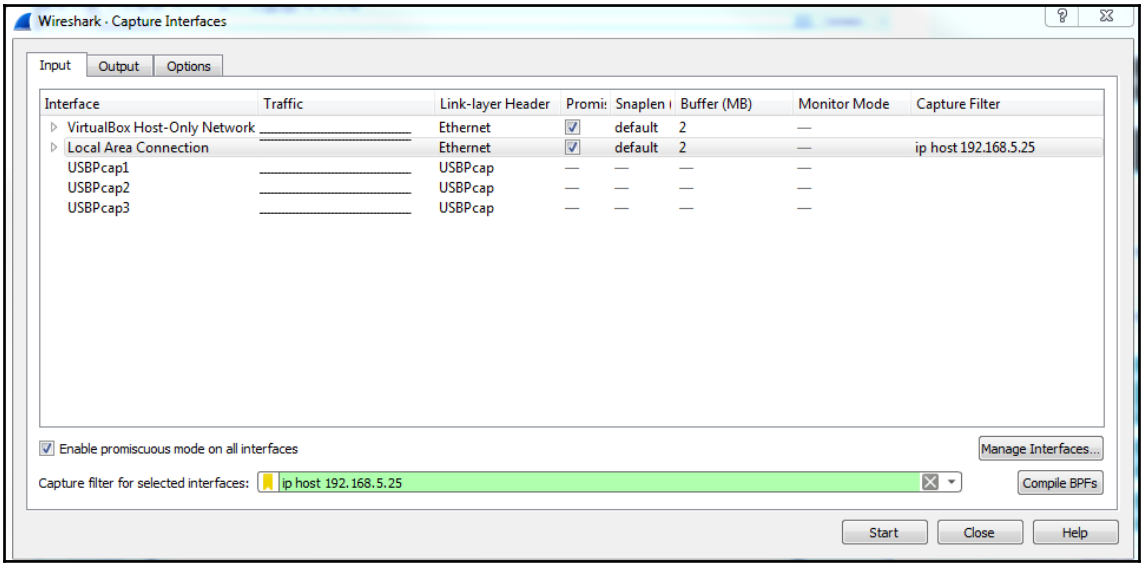


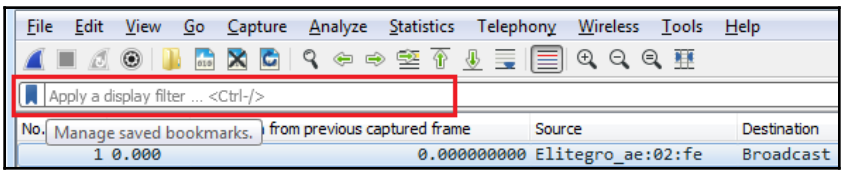

Wireshark · Capture Filters
Name
Filter
Non-HTTP and non-SMTP to/from www.wireshark.org
not port 80 and not port 25 and host www.wireshark.org
No ARP and no DNS
not arp and port not 53
HTTP TCP port (80)
tcp port http
TCP or UDP port 80 (HTTP)
port 80
UDP only
udp
TCP only
tcp
IPX only
ipx
IPv6 address 2001:db8::1
host 2001:db8::1
IPv6 only
ip6
IPv4 address 192.0.2.1
host 192.0.2.1
IPv4 only
ip
No ARP
not arp
No Broadcast and no Multicast
not broadcast and not multicast
Ethernet type 0x0806 (ARP)
ether proto 0x0806
Ethernet address 00:00:5e:00:53:00
ether host 00:00:5e:00:53:00
My Host
ip host 192.168.5.25
OK
Cancel
Help

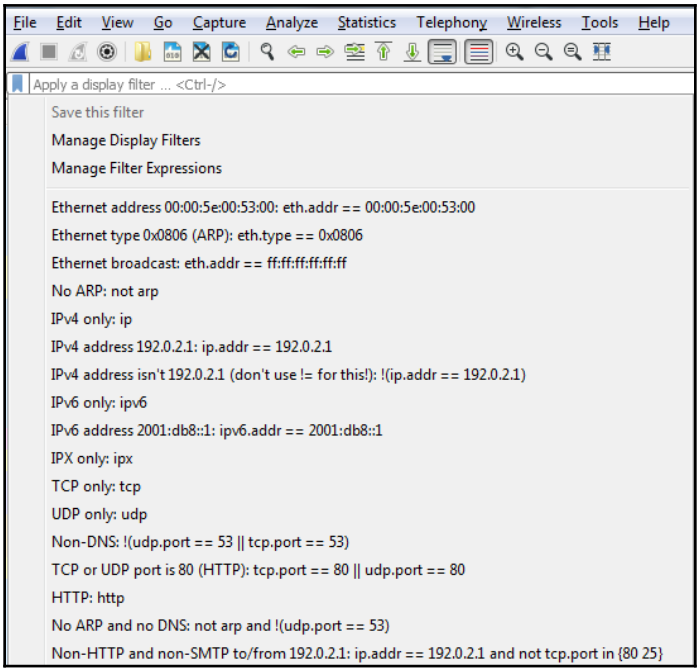

Capture
...using this filter:
ether broadcast
All interfaces shown
Save this filter
Manage Capture Filters
Ethernet address 00:00:5e:00:53:00: ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): ether proto 0x0806
No Broadcast and no Multicast: not broadcast and not multicast
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: host 192.0.2.1
IPv6 only: ip6
IPv6 address 2001:db8::1: host 2001:db8::1
IPX only: ipx
TCP only: tcp
UDP only: udp
TCP or UDP port 80 (HTTP): port 80
HTTP TCP port (80): tcp port http
No ARP and no DNS: not arp and port not 53
Non-HTTP and non-SMTP to/from www.wireshark.org: not port 80 and not port 25 and host www.wireshark.org
My Host: ip host 192.168.5.25
VirtualBox H
Local Area C
USBPcap1
USBPcap2
USBPcap3
Learn
User's Guide

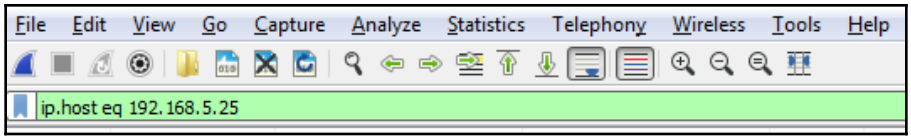

Capturing from Local Area Connection (ether broadcast)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Packet comments Info
1 0.000000 Elitegro_4e:a4:de Broadcast ARP 60 Who has 192.168.6.129? Tell 192.168.6.43
2 0.001550 Giga-Byt_40:5a:6e Broadcast ARP 60 Who has 192.168.7.45? Tell 192.168.7.78
3 0.030124 192.168.6.84 192.168.7.255 NBNS 92 Name query NB PACKTPUB<1b>
4 0.067066 Elitegro_0f:9b:64 Broadcast ARP 60 Who has 192.168.6.230? Tell 192.168.6.15
5 0.149179 Elitegro_4e:a2:28 Broadcast ARP 60 Who has 192.168.7.83? Tell 192.168.6.52
6 0.285475 SuperMic_88:92:0f Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11

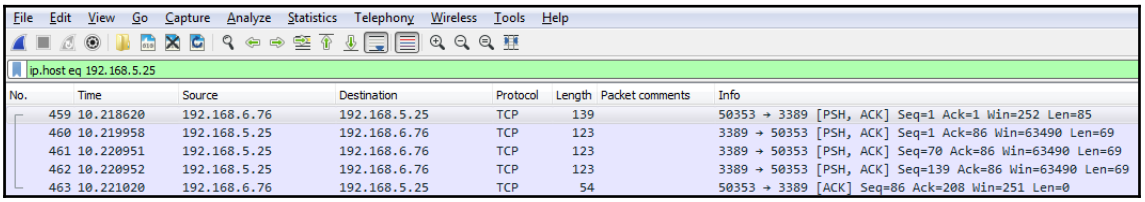

*Local Area Connection (ether broadcast)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

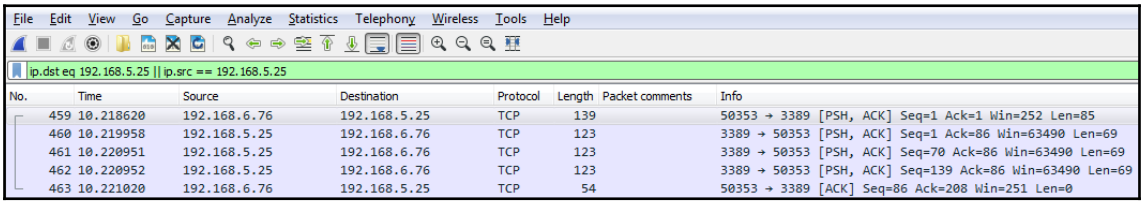

Wireshark · Capture Interfaces
Input Output Options
Interface Traffic Link-layer Header Promi Snaplen Buffer (MB) Monitor Mode Capture Filter
VirtualBox Host-Only Network Ethernet default 2
Local Area Connection Ethernet default 2 ip host 192.168.5.25
USBPcap1 USBPcap
USBPcap2 USBPcap
USBPcap3 USBPcap
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: ip host 192.168.5.25
Compile BPFs
Start Close Help

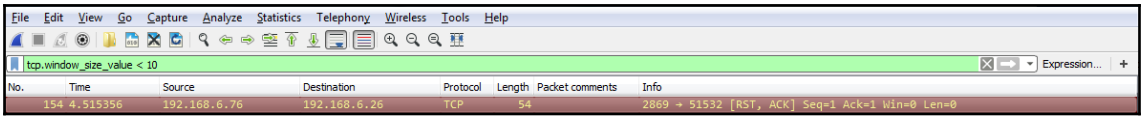

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Manage saved bookmarks.
No. from previous captured frame Source Destination
1 0.000 0.000000000 Elitegro_ae:02:fe Broadcast

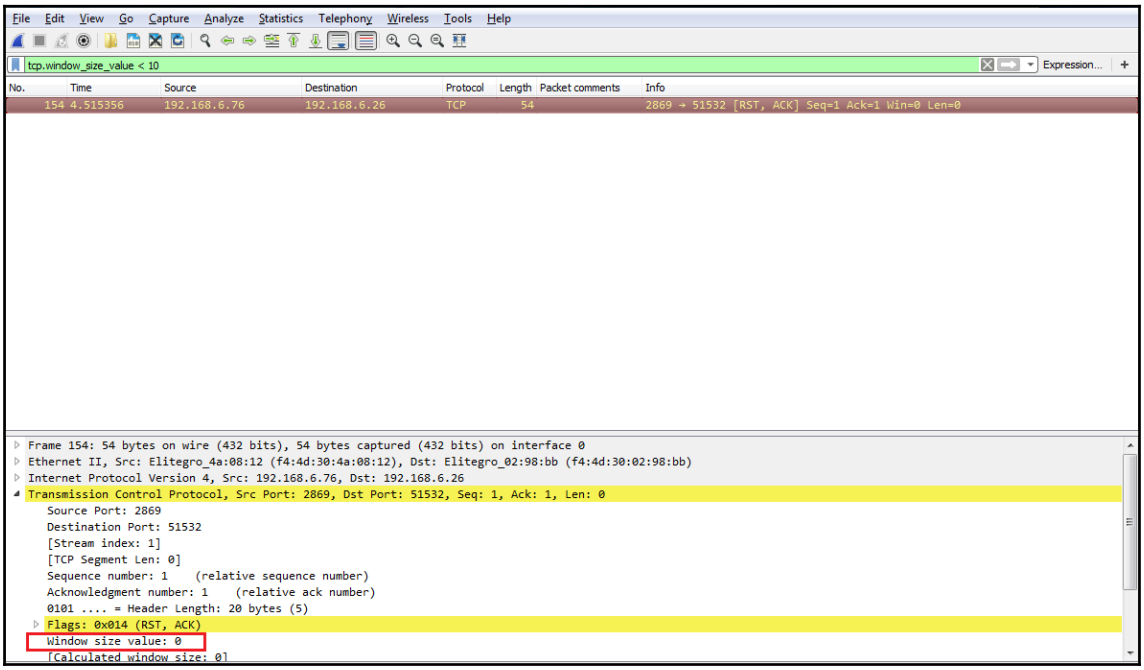

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Save this filter
Manage Display Filters
Manage Filter Expressions
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1 (don't use != for this!): !(ip.addr == 192.0.2.1)
IPv6 only: ipv6
IPv6 address 2001:db8::1: ipv6.addr == 2001:db8::1
IPX only: ipx
TCP only: tcp
UDP only: udp
Non-DNS: !(udp.port == 53 || tcp.port == 53)
TCP or UDP port is 80 (HTTP): tcp.port == 80 || udp.port == 80
HTTP: http
No ARP and no DNS: not arp and !(udp.port == 53)
Non-HTTP and non-SMTP to/from 192.0.2.1: ip.addr == 192.0.2.1 and not tcp.port in {80 25}

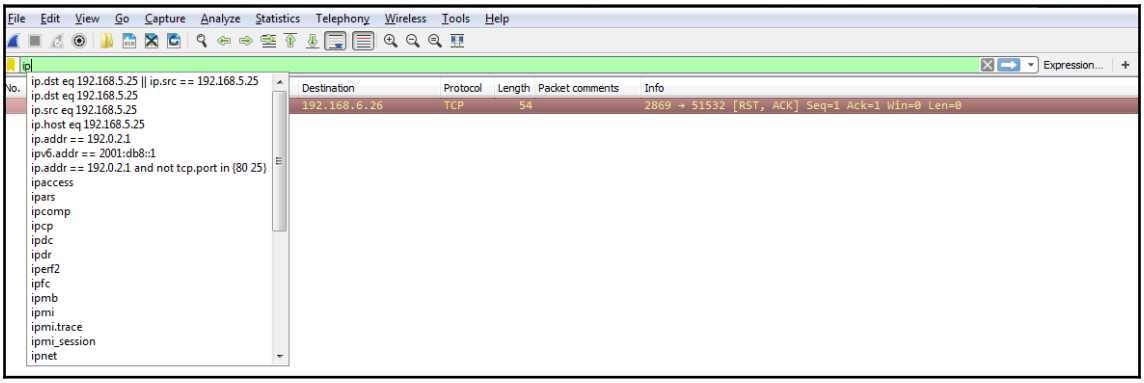

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.host eq 192.168.5.25

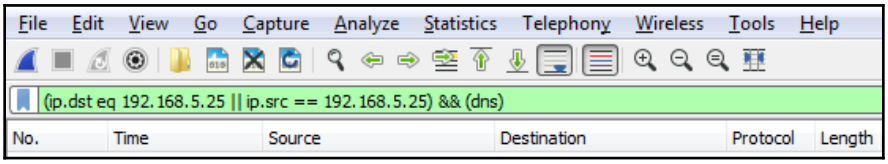

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.host eq 192.168.5.25
No. Time Source Destination Protocol Length Packet comments Info
459 10.218620 192.168.6.76 192.168.5.25 TCP 139 50353 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=85
460 10.219958 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=1 Ack=86 Win=63490 Len=69
461 10.220951 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=70 Ack=86 Win=63490 Len=69
462 10.220952 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=139 Ack=86 Win=63490 Len=69
463 10.221020 192.168.6.76 192.168.5.25 TCP 54 50353 → 3389 [ACK] Seq=86 Ack=208 Win=251 Len=0

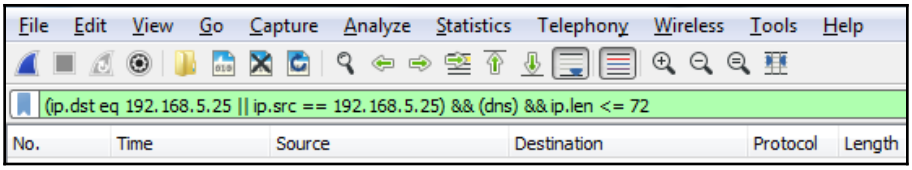

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.dst eq 192.168.5.25 || ip.src == 192.168.5.25
No. Time Source Destination Protocol Length Packet comments Info
459 10.218620 192.168.6.76 192.168.5.25 TCP 139 50353 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=85
460 10.219958 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=1 Ack=86 Win=63490 Len=69
461 10.220951 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=70 Ack=86 Win=63490 Len=69
462 10.220952 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=139 Ack=86 Win=63490 Len=69
463 10.221020 192.168.6.76 192.168.5.25 TCP 54 50353 → 3389 [ACK] Seq=86 Ack=208 Win=251 Len=0

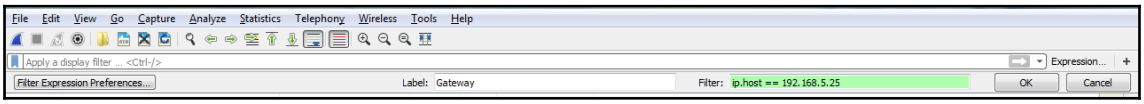

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.window_size_value < 10
Expression...
No. Time Source Destination Protocol Length Packet comments Info
154 4.515356 192.168.6.76 192.168.6.26 TCP 54 2869 → 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

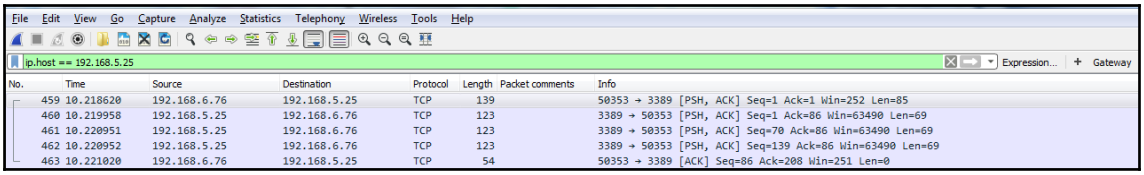

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.window_size_value < 10
Expression...
No. Time Source Destination Protocol Length Packet comments Info
154 4.515356 192.168.6.76 192.168.6.26 TCP 54 2869 → 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
Frame 154: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Elitegro_4a:08:12 (f4:4d:30:4a:08:12), Dst: Elitegro_02:98:bb (f4:4d:30:02:98:bb)
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 192.168.6.26
Transmission Control Protocol, Src Port: 2869, Dst Port: 51532, Seq: 1, Ack: 1, Len: 0
Source Port: 2869
Destination Port: 51532
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x014 (RST, ACK)
Window size value: 0
[Calculated window size: 0]

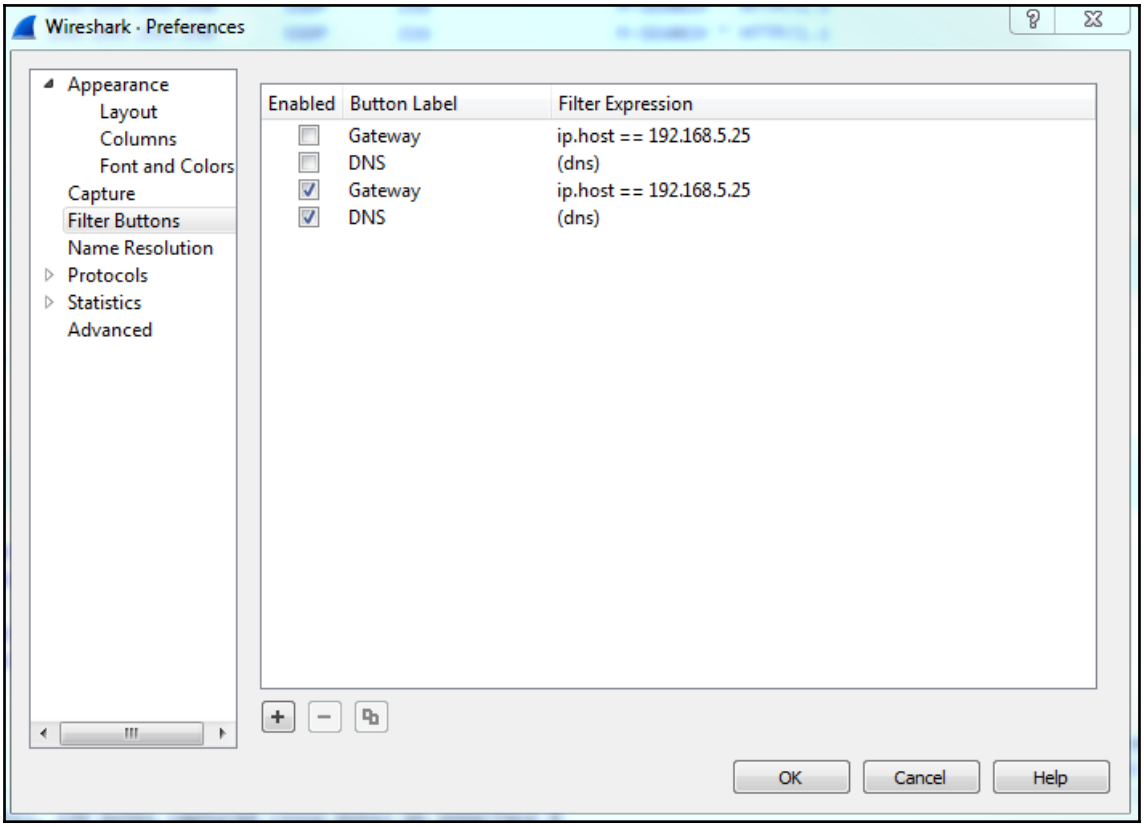

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip
Expression...
No.
ip.dst eq 192.168.5.25 || ip.src == 192.168.5.25
ip.dst eq 192.168.5.25
ip.src eq 192.168.5.25
ip.host eq 192.168.5.25
ip.addr == 192.0.2.1
ipv6.addr == 2001:db8::1
ip.addr == 192.0.2.1 and not tcp.port in {80 25}
ipaccess
ipars
ipcomp
ipcp
ipdc
ipdr
iperf2
ipfc
ipmb
ipmi
ipmi.trace
ipmi_session
ipnet
Destination Protocol Length Packet comments Info
192.168.6.26 TCP 54 2869 → 51532 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

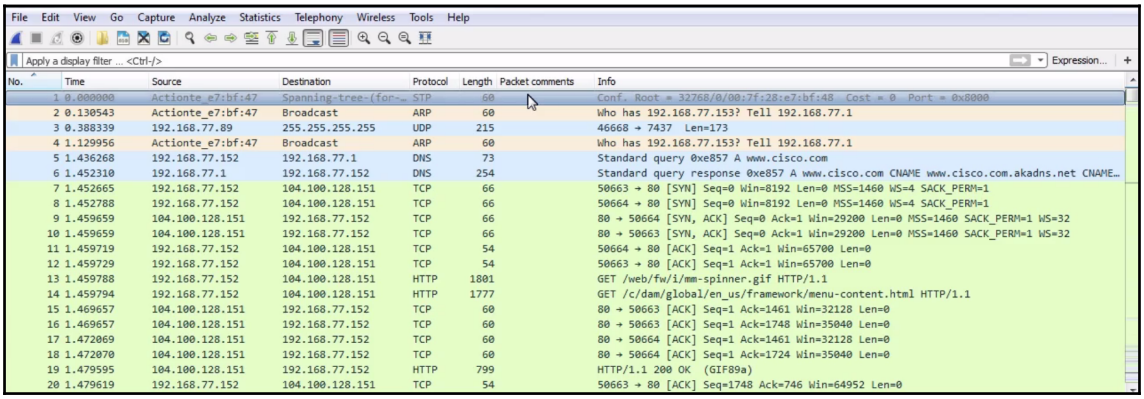

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst eq 192.168.5.25 || ip.src == 192.168.5.25) && (dns)
No. Time Source Destination Protocol Length

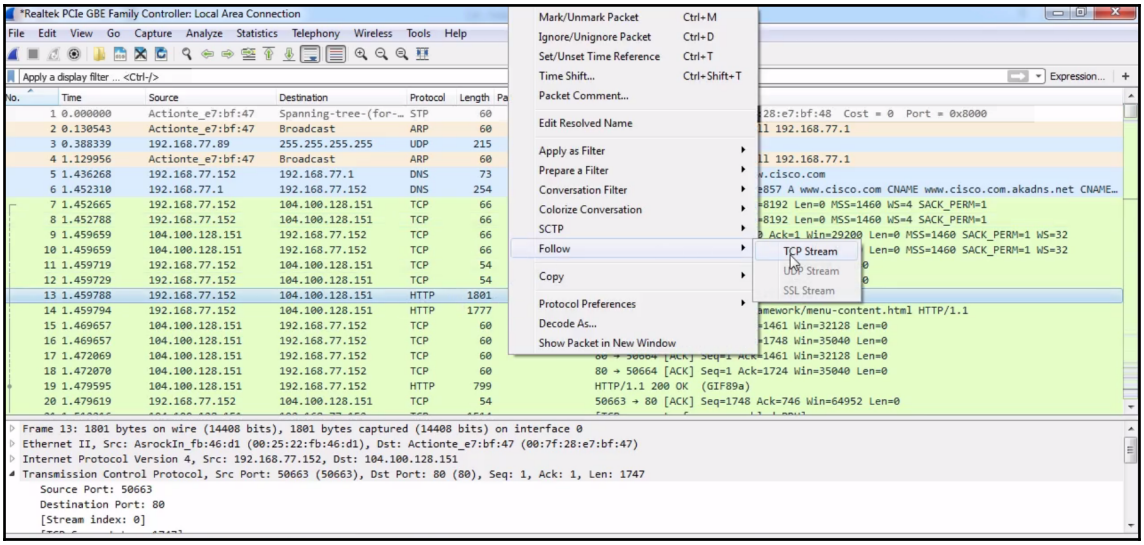

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.dst eq 192.168.5.25 || ip.src == 192.168.5.25) && (dns) && ip.len <= 72
No. Time Source Destination Protocol Length

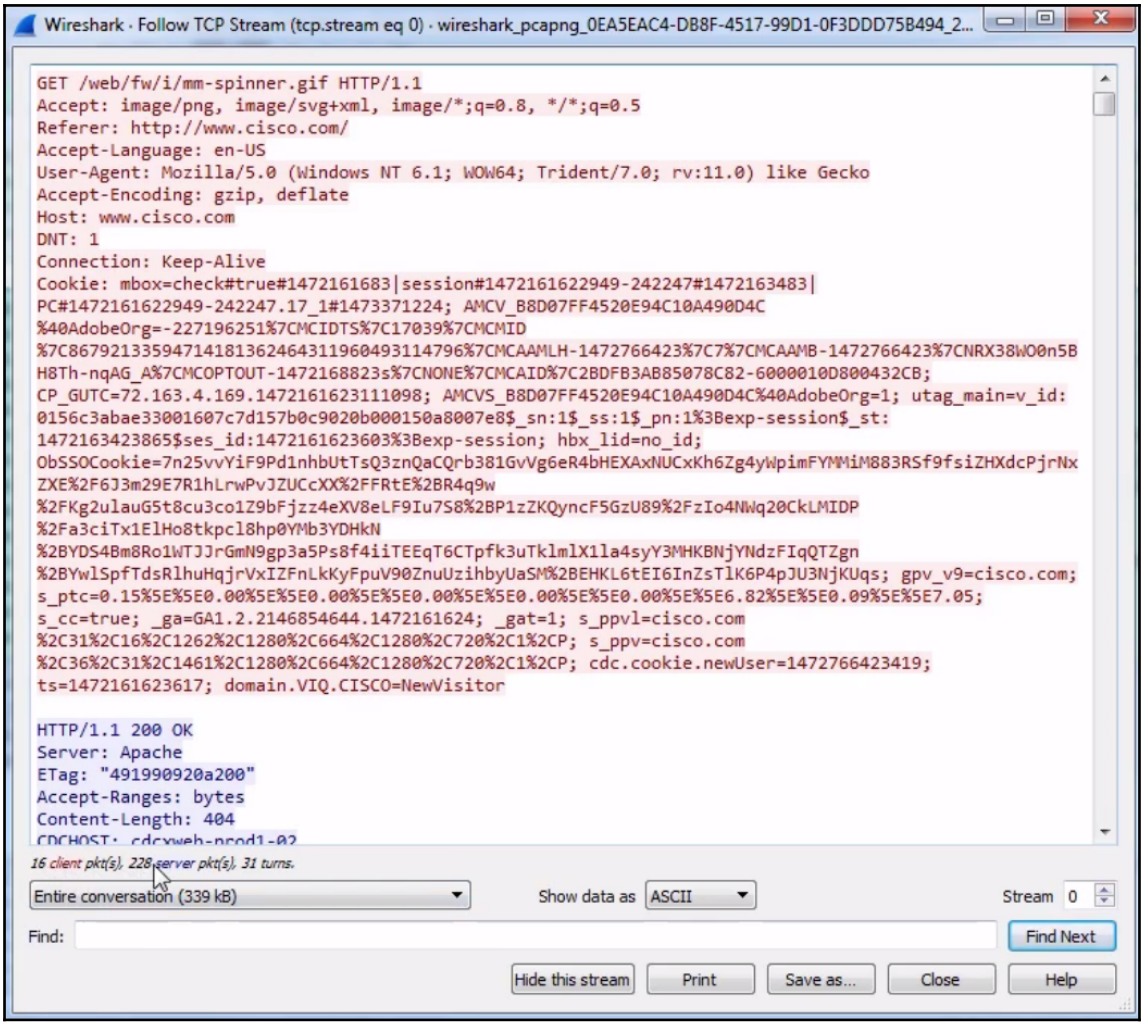

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Filter Expression Preferences...
Label: Gateway
Filter: ip.host == 192.168.5.25
OK
Cancel

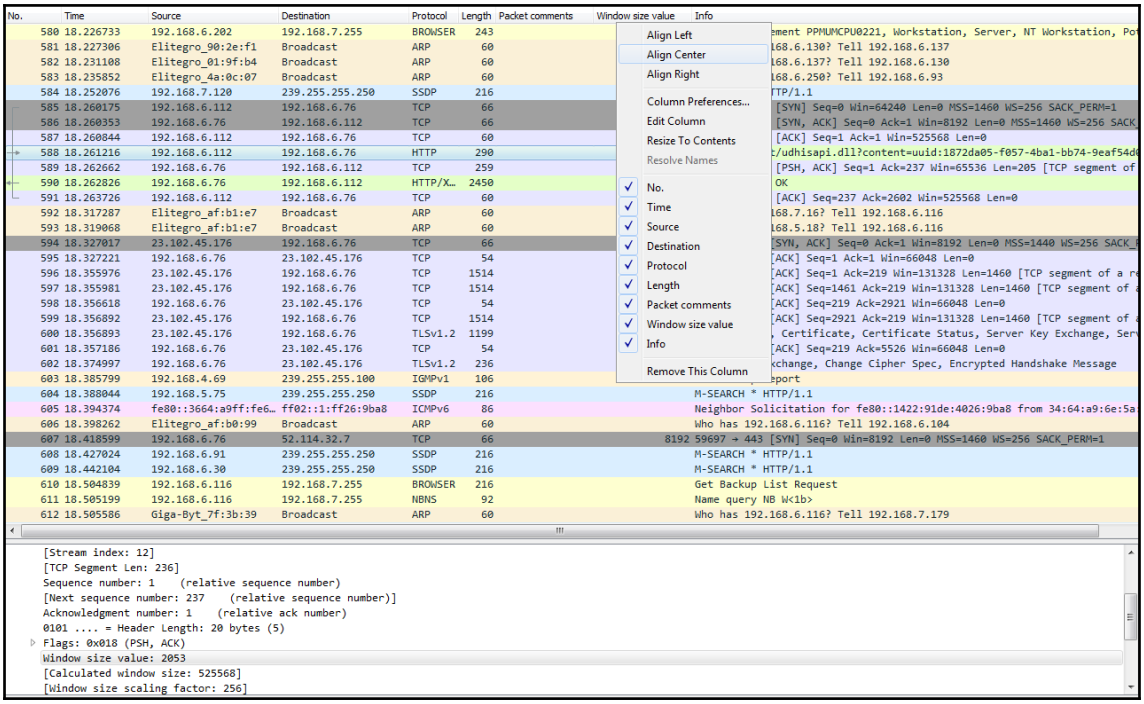

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.host == 192.168.5.25
Expression...
Gateway
No. Time Source Destination Protocol Length Packet comments Info
459 10.218620 192.168.6.76 192.168.5.25 TCP 139 50353 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=252 Len=85
460 10.219958 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=1 Ack=86 Win=63490 Len=69
461 10.220951 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=70 Ack=86 Win=63490 Len=69
462 10.220952 192.168.5.25 192.168.6.76 TCP 123 3389 → 50353 [PSH, ACK] Seq=139 Ack=86 Win=63490 Len=69
463 10.221020 192.168.6.76 192.168.5.25 TCP 54 50353 → 3389 [ACK] Seq=86 Ack=208 Win=251 Len=0

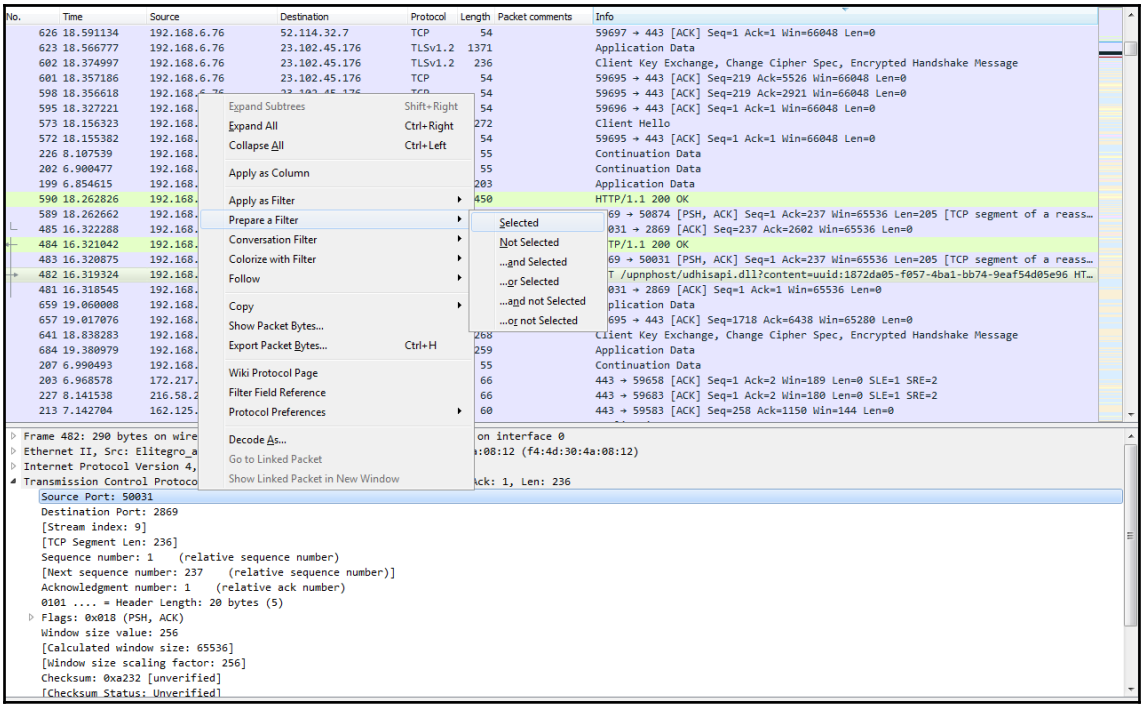

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Enabled
Button Label
Filter Expression
Gateway
ip.host == 192.168.5.25
DNS
(dns)
Gateway
ip.host == 192.168.5.25
DNS
(dns)
OK
Cancel
Help

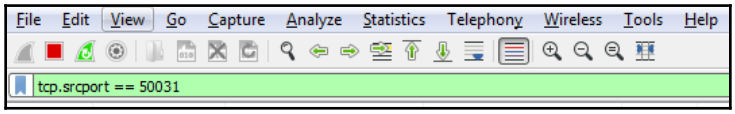

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Packet comments Info
1 0.000000 Actionte_e7:bf:47 Spanning-tree-(for-... STP 60 Conf. Root = 32768/0/00:7f:28:e7:bf:48 Cost = 0 Port = 0x8000
2 0.130543 Actionte_e7:bf:47 Broadcast ARP 60 Who has 192.168.77.153? Tell 192.168.77.1
3 0.388339 192.168.77.89 255.255.255.255 UDP 215 46668 → 7437 Len=173
4 1.129956 Actionte_e7:bf:47 Broadcast ARP 60 Who has 192.168.77.153? Tell 192.168.77.1
5 1.436268 192.168.77.152 192.168.77.1 DNS 73 Standard query 0xe857 A www.cisco.com
6 1.452310 192.168.77.1 192.168.77.152 DNS 254 Standard query response 0xe857 A www.cisco.com CNAME www.cisco.com.akadns.net CNAME...
7 1.452665 192.168.77.152 104.100.128.151 TCP 66 50663 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8 1.452788 192.168.77.152 104.100.128.151 TCP 66 50664 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
9 1.459659 104.100.128.151 192.168.77.152 TCP 66 80 → 50664 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=32
10 1.459659 104.100.128.151 192.168.77.152 TCP 66 80 → 50663 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=32
11 1.459719 192.168.77.152 104.100.128.151 TCP 54 50664 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
12 1.459729 192.168.77.152 104.100.128.151 TCP 54 50663 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
13 1.459788 192.168.77.152 104.100.128.151 HTTP 1801 GET /web/fw/i/mm-spinner.gif HTTP/1.1
14 1.459794 192.168.77.152 104.100.128.151 HTTP 1777 GET /c/dam/global/en_us/framework/menu-content.html HTTP/1.1
15 1.469657 104.100.128.151 192.168.77.152 TCP 60 80 → 50663 [ACK] Seq=1 Ack=1461 Win=32128 Len=0
16 1.469657 104.100.128.151 192.168.77.152 TCP 60 80 → 50663 [ACK] Seq=1 Ack=1748 Win=35040 Len=0
17 1.472069 104.100.128.151 192.168.77.152 TCP 60 80 → 50664 [ACK] Seq=1 Ack=1461 Win=32128 Len=0
18 1.472070 104.100.128.151 192.168.77.152 TCP 60 80 → 50664 [ACK] Seq=1 Ack=1724 Win=35040 Len=0
19 1.479595 104.100.128.151 192.168.77.152 HTTP 799 HTTP/1.1 200 OK (GIF89a)
20 1.479619 192.168.77.152 104.100.128.151 TCP 54 50663 → 80 [ACK] Seq=1748 Ack=746 Win=64952 Len=0

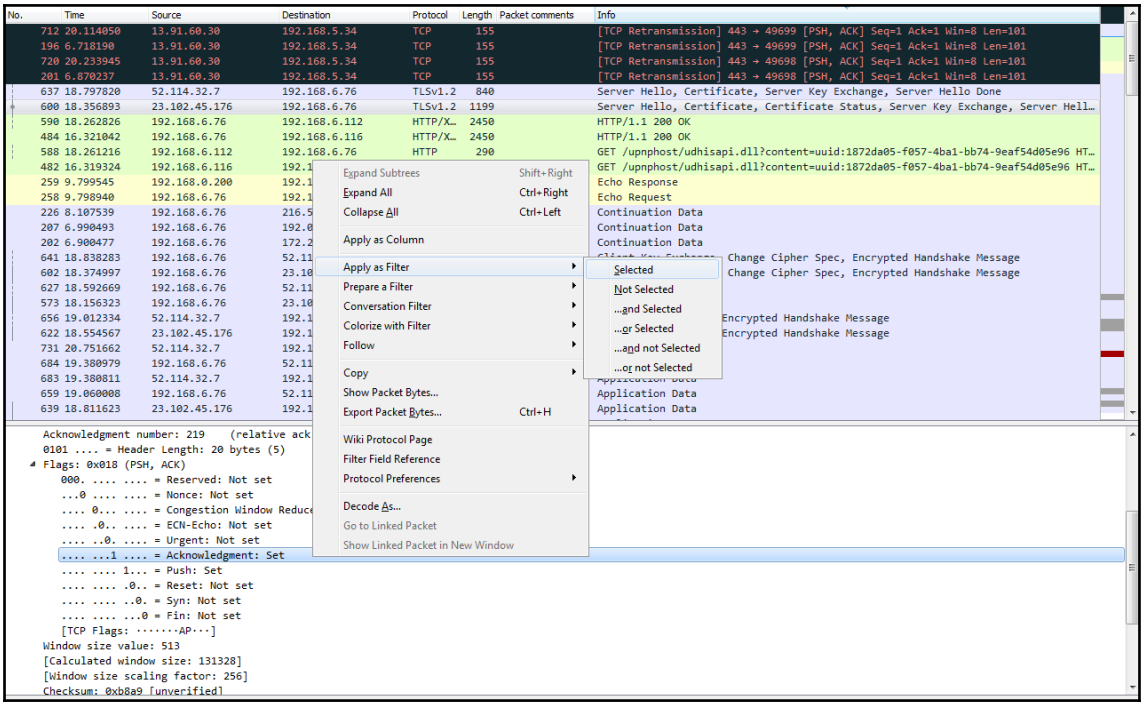

*Realtek PCIe GBE Family Controller: Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length
1 0.000000 Actionte_e7:bf:47 Spanning-tree-(for-... STP 60
2 0.130543 Actionte_e7:bf:47 Broadcast ARP 60
3 0.388339 192.168.77.89 255.255.255.255 UDP 215
4 1.129956 Actionte_e7:bf:47 Broadcast ARP 60
5 1.436268 192.168.77.152 192.168.77.1 DNS 73
6 1.452310 192.168.77.1 192.168.77.152 DNS 254
7 1.452665 192.168.77.152 104.100.128.151 TCP 66
8 1.452788 192.168.77.152 104.100.128.151 TCP 66
9 1.459659 104.100.128.151 192.168.77.152 TCP 66
10 1.459659 104.100.128.151 192.168.77.152 TCP 66
11 1.459719 192.168.77.152 104.100.128.151 TCP 54
12 1.459729 192.168.77.152 104.100.128.151 TCP 54
13 1.459788 192.168.77.152 104.100.128.151 HTTP 1801
14 1.459794 192.168.77.152 104.100.128.151 HTTP 1777
15 1.469657 104.100.128.151 192.168.77.152 TCP 60
16 1.469657 104.100.128.151 192.168.77.152 TCP 60
17 1.472069 104.100.128.151 192.168.77.152 TCP 60
18 1.472070 104.100.128.151 192.168.77.152 TCP 60
19 1.479595 104.100.128.151 192.168.77.152 HTTP 799
20 1.479619 192.168.77.152 104.100.128.151 TCP 54
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment...
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP/1.1 200 OK (GIF89a)
Frame 13: 1801 bytes on wire (14408 bits), 1801 bytes captured (14408 bits) on interface 0
Ethernet II, Src: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1), Dst: Actionte_e7:bf:47 (00:7f:28:e7:bf:47)
Internet Protocol Version 4, Src: 192.168.77.152, Dst: 104.100.128.151
Transmission Control Protocol, Src Port: 50663 (50663), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1747
Source Port: 50663
Destination Port: 80
[Stream index: 0]

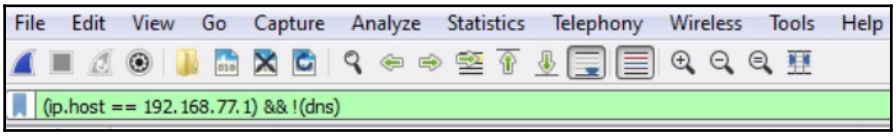

Wireshark · Follow TCP Stream (tcp.stream eq 0) · wireshark_pcapng_0EA5EAC4-DB8F-4517-99D1-0F3DDD75B494_2...
GET /web/fw/i/mm-spinner.gif HTTP/1.1
Accept: image/png, image/svg+xml, image/*;q=0.8, */*;q=0.5
Referer: http://www.cisco.com/
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: www.cisco.com
DNT: 1
Connection: Keep-Alive
Cookie: mbox=check#true#1472161683|session#1472161622949-242247#1472163483|
PC#1472161622949-242247.17_1#1473371224; AMCV_B8D07FF4520E94C10A490D4C
%40AdobeOrg=-227196251%7CMCIDTS%7C17039%7CMCMID
%7C86792133594714181362464311960493114796%7CMCAAMLH-1472766423%7C7%7CMCAAMB-1472766423%7CNRX38WO0n5B
H8Th-nqAG_A%7CMCOPTOUT-1472168823s%7CNONE%7CMCAID%7C2BDFB3AB85078C82-6000010D800432CB;
CP_GUTC=72.163.4.169.1472161623111098; AMCVS_B8D07FF4520E94C10A490D4C%40AdobeOrg=1; utag_main=v_id:
0156c3abae33001607c7d157b0c9020b000150a8007e8$_sn:1$_ss:1$_pn:1%3Bexp-session$_st:
1472163423865$ses_id:1472161623603%3Bexp-session; hbx_lid=no_id;
ObSSOCookie=7n25vvYiF9Pd1nhbUtTsQ3znQaCQrb381GvVg6eR4bHEXAxNUCxKh6Zg4yWpimFYMMiM883RSf9fsiZHXdcPjrNx
ZXE%2F6J3m29E7R1hLrwPvJZUCcXX%2FFRtE%2BR4q9w
%2FKg2ulauG5t8cu3co1Z9bFjzz4eXV8eLF9Iu7S8%2BP1zZKQyncF5GzU89%2FzIo4NWq20CkLMIDP
%2Fa3ciTx1ElHo8tkpcl8hp0YMb3YDHkN
%2BYDS4Bm8Ro1WTJJrGmN9gp3a5Ps8f4iiTEEqT6CTpfk3uTklmlX1la4syY3MHKBNjYNdzFIqQTZgn
%2BYwlSpfTdsRlhuHqjrVxIZFnLkKyFpuV90ZnuUzihbyUaSM%2BEHKL6tEI6InZsTlK6P4pJU3NjKUqs; gpv_v9=cisco.com;
s_ptc=0.15%5E%5E0.00%5E%5E0.00%5E%5E0.00%5E%5E0.00%5E%5E0.00%5E%5E6.82%5E%5E0.09%5E%5E7.05;
s_cc=true; _ga=GA1.2.2146854644.1472161624; _gat=1; s_ppvl=cisco.com
%2C31%2C16%2C1262%2C1280%2C664%2C1280%2C720%2C1%2CP; s_ppv=cisco.com
%2C36%2C31%2C1461%2C1280%2C664%2C1280%2C720%2C1%2CP; cdc.cookie.newUser=1472766423419;
ts=1472161623617; domain.VIQ.CISCO=NewVisitor
HTTP/1.1 200 OK
Server: Apache
ETag: "491990920a200"
Accept-Ranges: bytes
Content-Length: 404
16 client pkt(s), 228 server pkt(s), 31 turns.
Entire conversation (339 kB)
Show data as
ASCII
Stream
0
Find:
Find Next
Hide this stream
Print
Save as...
Close
Help


No. Time Source Destination Protocol Length Packet comments Window size value Info
580 18.226733 192.168.6.202 192.168.7.255 BROWSER 243 ement PPMUMCPU0221, Workstation, Server, NT Workstation, Po
581 18.227306 Elitegro_90:2e:f1 Broadcast ARP 60 168.6.130? Tell 192.168.6.137
582 18.231108 Elitegro_01:9f:b4 Broadcast ARP 60 168.6.137? Tell 192.168.6.130
583 18.235852 Elitegro_4a:0c:07 Broadcast ARP 60 168.6.250? Tell 192.168.6.93
584 18.252076 192.168.7.120 239.255.255.250 SSDP 216 TTP/1.1
585 18.260175 192.168.6.112 192.168.6.76 TCP 66 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
586 18.260353 192.168.6.76 192.168.6.112 TCP 66 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK
587 18.260844 192.168.6.112 192.168.6.76 TCP 60 [ACK] Seq=1 Ack=1 Win=525568 Len=0
588 18.261216 192.168.6.112 192.168.6.76 HTTP 290 t/udhisapi.dll?content=uuid:1872da05-f057-4ba1-bb74-9eaf54d
589 18.262662 192.168.6.76 192.168.6.112 TCP 259 [PSH, ACK] Seq=1 Ack=237 Win=65536 Len=205 [TCP segment of
590 18.262826 192.168.6.76 192.168.6.112 HTTP/X... 2450 OK
591 18.263726 192.168.6.112 192.168.6.76 TCP 60 [ACK] Seq=237 Ack=2602 Win=525568 Len=0
592 18.317287 Elitegro_af:b1:e7 Broadcast ARP 60 168.7.16? Tell 192.168.6.116
593 18.319068 Elitegro_af:b1:e7 Broadcast ARP 60 168.5.18? Tell 192.168.6.116
594 18.327017 23.102.45.176 192.168.6.76 TCP 66 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=256 SACK_
595 18.327221 192.168.6.76 23.102.45.176 TCP 54 [ACK] Seq=1 Ack=1 Win=66048 Len=0
596 18.355976 23.102.45.176 192.168.6.76 TCP 1514 [ACK] Seq=1 Ack=219 Win=131328 Len=1460 [TCP segment of a r
597 18.355981 23.102.45.176 192.168.6.76 TCP 1514 [ACK] Seq=1461 Ack=219 Win=131328 Len=1460 [TCP segment of
598 18.356618 192.168.6.76 23.102.45.176 TCP 54 [ACK] Seq=219 Ack=2921 Win=66048 Len=0
599 18.356892 23.102.45.176 192.168.6.76 TCP 1514 [ACK] Seq=2921 Ack=219 Win=131328 Len=1460 [TCP segment of
600 18.356893 23.102.45.176 192.168.6.76 TLSv1.2 1199 , Certificate, Certificate Status, Server Key Exchange, Ser
601 18.357186 192.168.6.76 23.102.45.176 TCP 54 [ACK] Seq=219 Ack=5526 Win=66048 Len=0
602 18.374997 192.168.6.76 23.102.45.176 TLSv1.2 236 xchange, Change Cipher Spec, Encrypted Handshake Message
603 18.385799 192.168.4.69 239.255.255.100 IGMPv1 106 eport
604 18.388044 192.168.5.75 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
605 18.394374 fe80::3664:a9ff:fe6... ff02::1:ff26:9ba8 ICMPv6 86 Neighbor Solicitation for fe80::1422:91de:4026:9ba8 from 34:64:a9:6e:5a
606 18.398262 Elitegro_af:b0:99 Broadcast ARP 60 Who has 192.168.6.116? Tell 192.168.6.104
607 18.418599 192.168.6.76 52.114.32.7 TCP 66 8192 59697 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
608 18.427024 192.168.6.91 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
609 18.442104 192.168.6.30 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
610 18.504839 192.168.6.116 192.168.7.255 BROWSER 216 Get Backup List Request
611 18.505199 192.168.6.116 192.168.7.255 NBNS 92 Name query NB W<1b>
612 18.505586 Giga-Byt_7f:3b:39 Broadcast ARP 60 Who has 192.168.6.116? Tell 192.168.7.179
Align Left
Align Center
Align Right
Column Preferences...
Edit Column
Resize To Contents
Resolve Names
No.
Time
Source
Destination
Protocol
Length
Packet comments
Window size value
Info
Remove This Column
[Stream index: 12]
[TCP Segment Len: 236]
Sequence number: 1 (relative sequence number)
[Next sequence number: 237 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 2053
[Calculated window size: 525568]
[Window size scaling factor: 256]

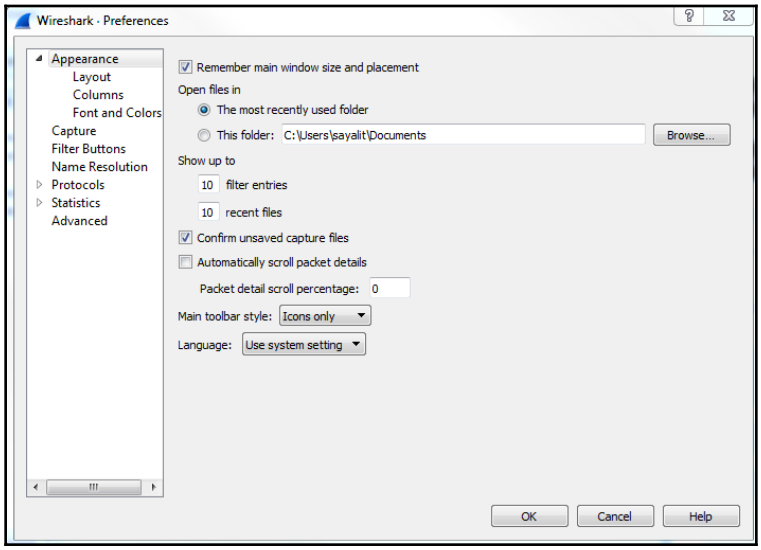

No. Time Source Destination Protocol Length Packet comments Info
626 18.591134 192.168.6.76 52.114.32.7 TCP 54 59697 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
623 18.566777 192.168.6.76 23.102.45.176 TLSv1.2 1371 Application Data
602 18.374997 192.168.6.76 23.102.45.176 TLSv1.2 236 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
601 18.357186 192.168.6.76 23.102.45.176 TCP 54 59695 → 443 [ACK] Seq=219 Ack=5526 Win=66048 Len=0
598 18.356618 54 59695 → 443 [ACK] Seq=219 Ack=2921 Win=66048 Len=0
595 18.327221 54 59696 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
573 18.156323 272 Client Hello
572 18.155382 54 59695 → 443 [ACK] Seq=1 Ack=1 Win=66048 Len=0
226 8.107539 55 Continuation Data
202 6.900477 55 Continuation Data
199 6.854615 203 Application Data
590 18.262826 450 HTTP/1.1 200 OK
589 18.262662 69 → 50874 [PSH, ACK] Seq=1 Ack=237 Win=65536 Len=205 [TCP segment of a reass…
485 16.322288 031 → 2869 [ACK] Seq=237 Ack=2602 Win=65536 Len=0
484 16.321042 TP/1.1 200 OK
483 16.320875 69 → 50031 [PSH, ACK] Seq=1 Ack=237 Win=65536 Len=205 [TCP segment of a reass…
482 16.319324 T /upnphost/udhisapi.dll?content=uuid:1872da05-f057-4ba1-bb74-9eaf54d05e96 HT…
481 16.318545 031 → 2869 [ACK] Seq=1 Ack=1 Win=65536 Len=0
659 19.060008 plication Data
657 19.017076 695 → 443 [ACK] Seq=1718 Ack=6438 Win=65280 Len=0
641 18.838283 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
684 19.380979 259 Application Data
207 6.990493 55 Continuation Data
203 6.968578 66 443 → 59658 [ACK] Seq=1 Ack=2 Win=189 Len=0 SLE=1 SRE=2
227 8.141538 66 443 → 59683 [ACK] Seq=1 Ack=2 Win=180 Len=0 SLE=1 SRE=2
213 7.142704 60 443 → 59583 [ACK] Seq=258 Ack=1150 Win=144 Len=0
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Frame 482: 290 bytes on wire on interface 0
Ethernet II, Src: Elitegro_a :08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4,
Transmission Control Protoco ck: 1, Len: 236
Source Port: 50031
Destination Port: 2869
[Stream index: 9]
[TCP Segment Len: 236]
Sequence number: 1 (relative sequence number)
[Next sequence number: 237 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 256
[Calculated window size: 65536]
[Window size scaling factor: 256]
Checksum: 0xa232 [unverified]
[Checksum Status: Unverified]

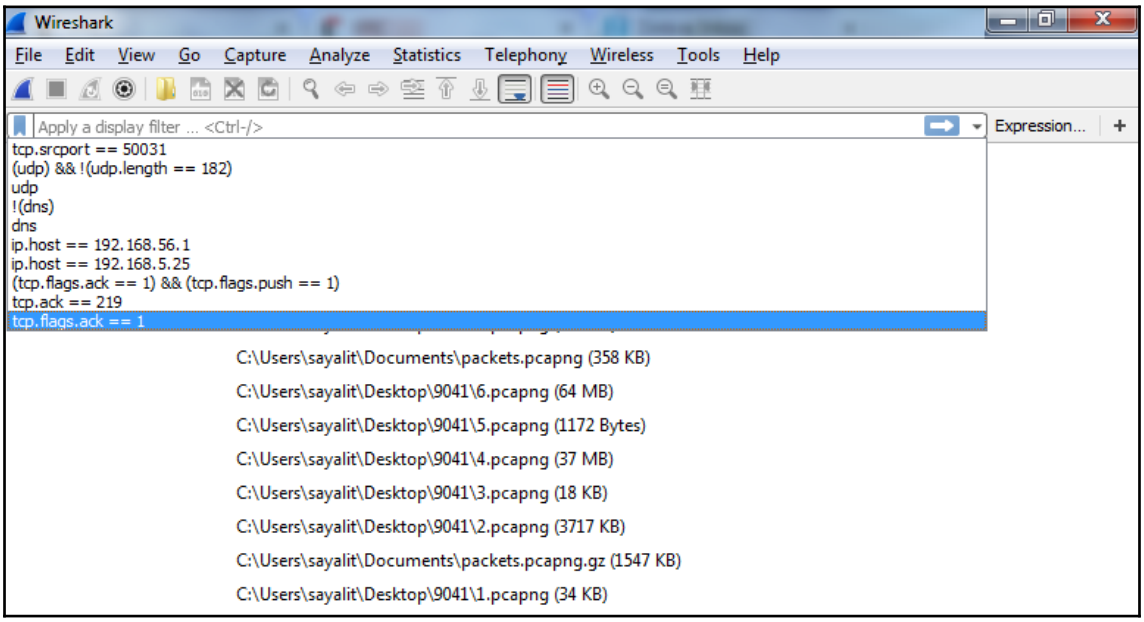

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.srcport == 50031

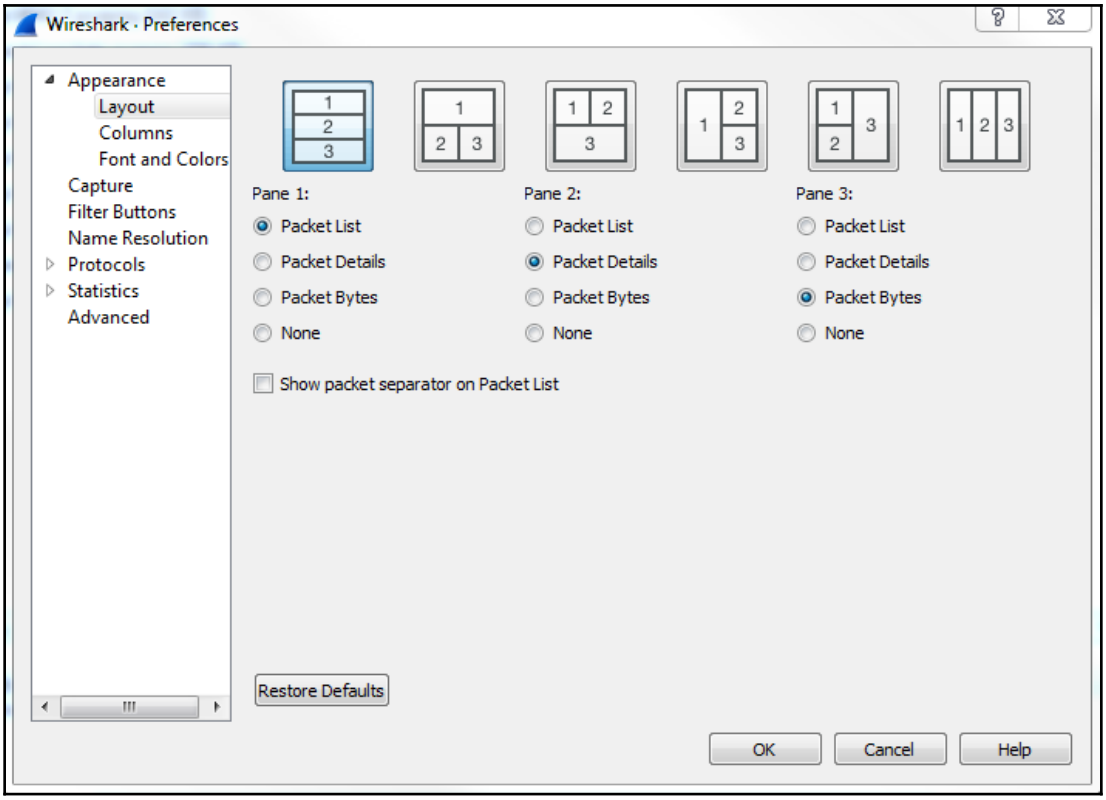

No. Time Source Destination Protocol Length Packet comments Info
712 20.114050 13.91.60.30 192.168.5.34 TCP 155 [TCP Retransmission] 443 → 49699 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
196 6.718190 13.91.60.30 192.168.5.34 TCP 155 [TCP Retransmission] 443 → 49699 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
720 20.233945 13.91.60.30 192.168.5.34 TCP 155 [TCP Retransmission] 443 → 49698 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
201 6.870237 13.91.60.30 192.168.5.34 TCP 155 [TCP Retransmission] 443 → 49698 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
637 18.797820 52.114.32.7 192.168.6.76 TLSv1.2 840 Server Hello, Certificate, Server Key Exchange, Server Hello Done
600 18.356893 23.102.45.176 192.168.6.76 TLSv1.2 1199 Server Hello, Certificate, Certificate Status, Server Key Exchange, Server Hell…
590 18.262826 192.168.6.76 192.168.6.112 HTTP/X… 2450 HTTP/1.1 200 OK
484 16.321042 192.168.6.76 192.168.6.116 HTTP/X… 2450 HTTP/1.1 200 OK
588 18.261216 192.168.6.112 192.168.6.76 HTTP 290 GET /upnphost/udhisapi.dll?content=uuid:1872da05-f057-4ba1-bb74-9eaf54d05e96 HT…
482 16.319324 192.168.6.116 192.1 GET /upnphost/udhisapi.dll?content=uuid:1872da05-f057-4ba1-bb74-9eaf54d05e96 HT…
259 9.799545 192.168.0.200 192.1 Echo Response
258 9.798940 192.168.6.76 192.1 Echo Request
226 8.107539 192.168.6.76 216.5 Continuation Data
207 6.990493 192.168.6.76 192.0 Continuation Data
202 6.900477 192.168.6.76 172.2 Continuation Data
641 18.838283 192.168.6.76 52.11 Change Cipher Spec, Encrypted Handshake Message
602 18.374997 192.168.6.76 23.10 Change Cipher Spec, Encrypted Handshake Message
627 18.592669 192.168.6.76 52.11
573 18.156323 192.168.6.76 23.10
656 19.012334 52.114.32.7 192.1 Encrypted Handshake Message
622 18.554567 23.102.45.176 192.1 Encrypted Handshake Message
731 20.751662 52.114.32.7 192.1
684 19.380979 192.168.6.76 52.11
683 19.380811 52.114.32.7 192.1
659 19.060008 192.168.6.76 52.11 Application Data
639 18.811623 23.102.45.176 192.1 Application Data
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
Acknowledgment number: 219 (relative ack
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduce
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 1... = Push: Set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····AP···]
Window size value: 513
[Calculated window size: 131328]
[Window size scaling factor: 256]
Checksum: 0xb8a9 [unverified]

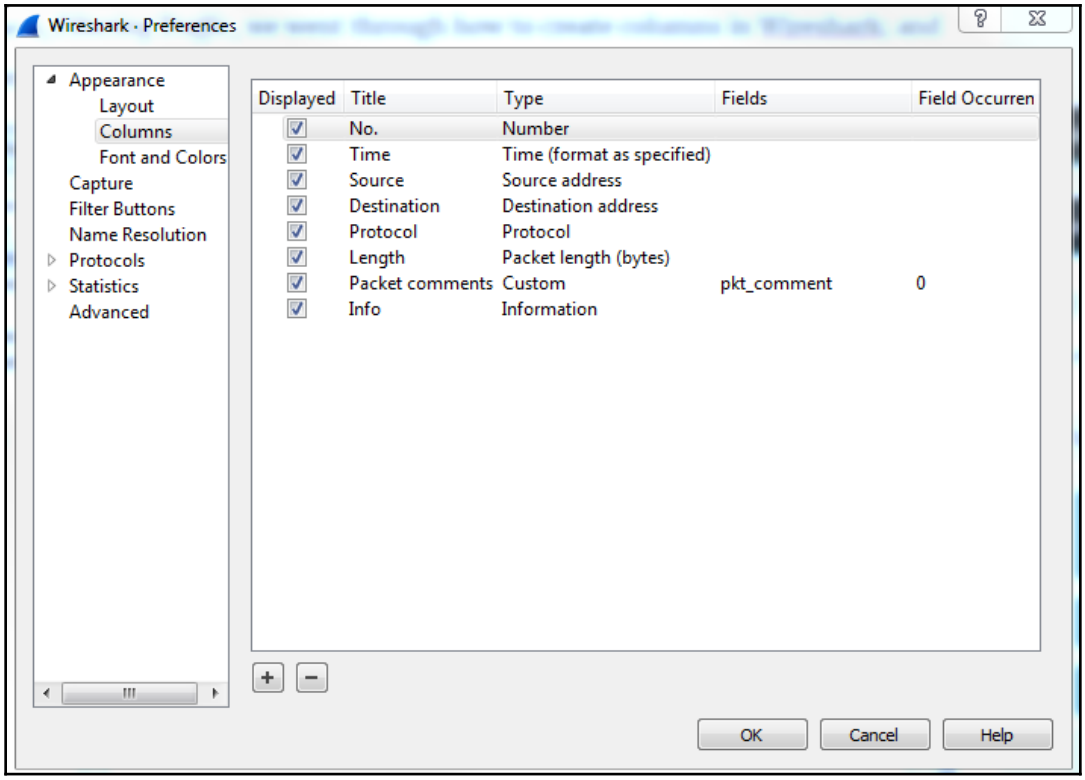

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
(ip.host == 192.168.77.1) && !(dns)

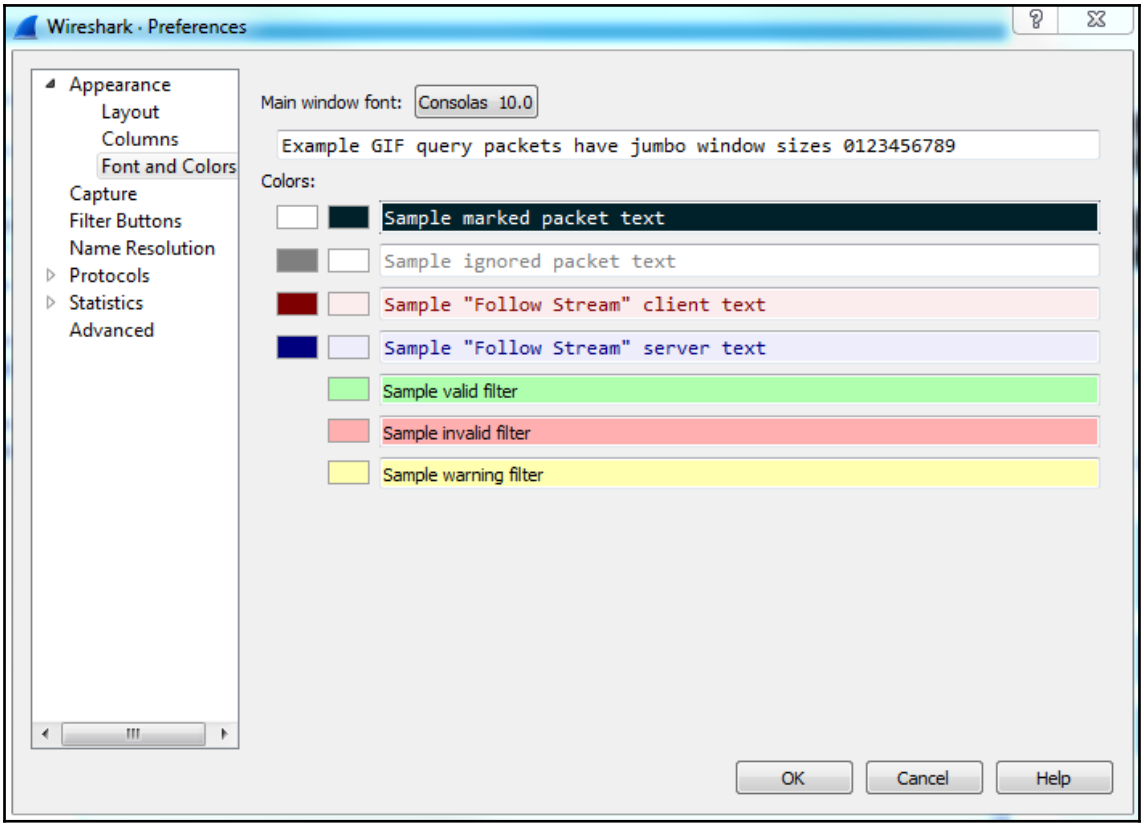
Chapter 04: Customizing Wireshark

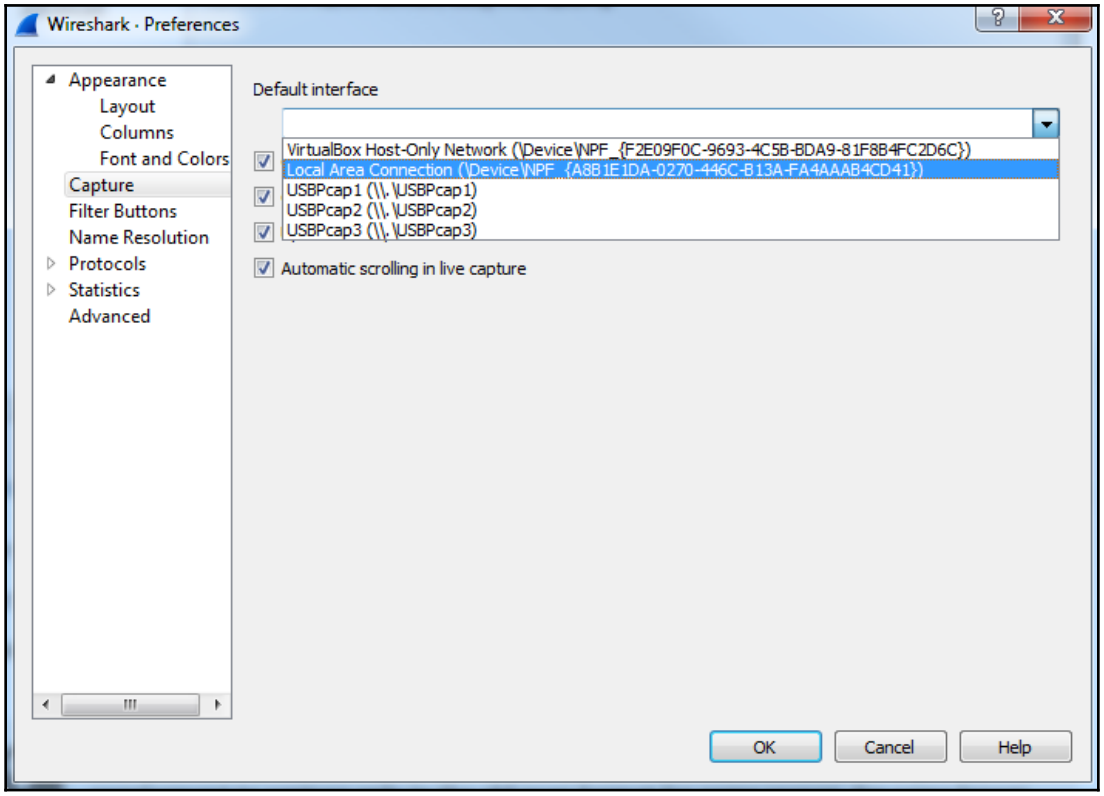


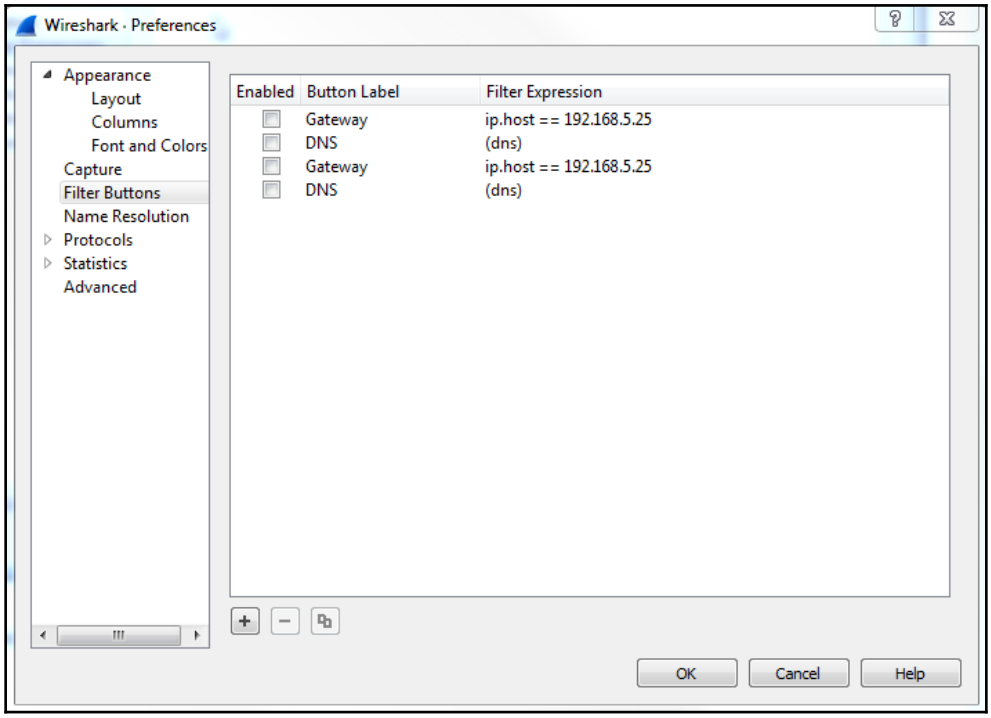


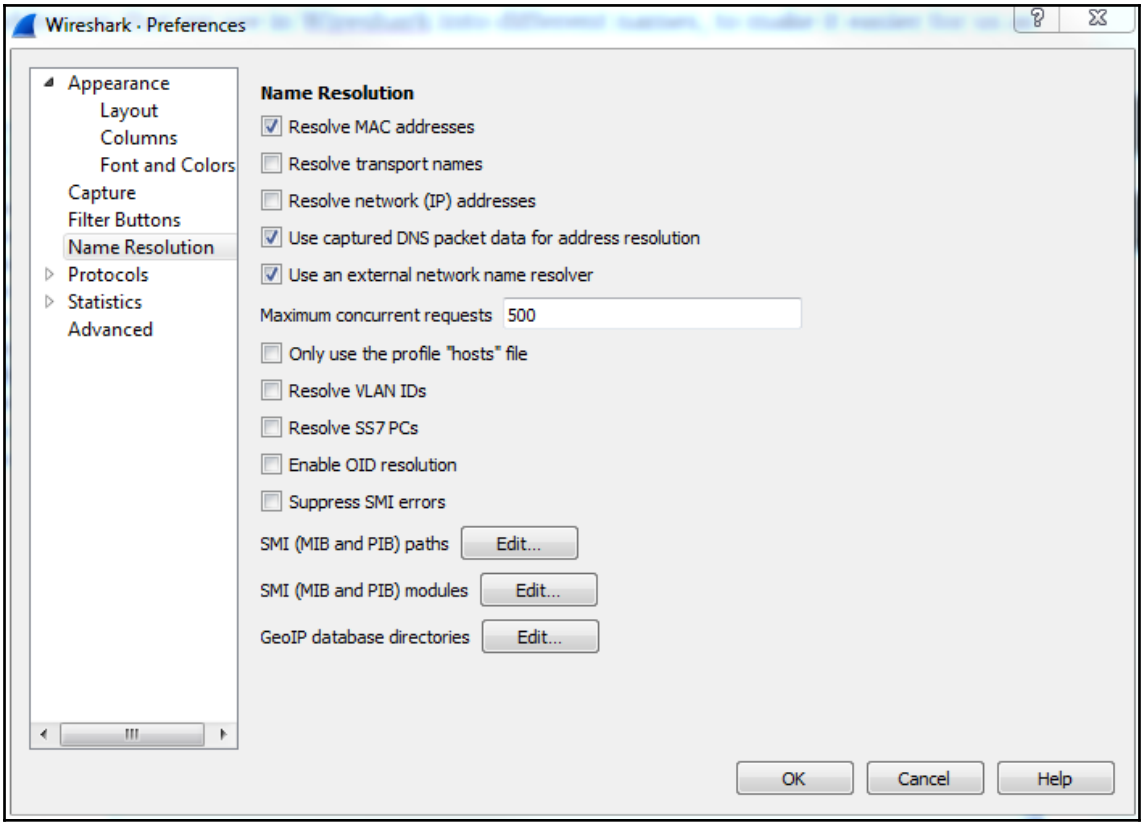

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Pane 1:
Packet List
Packet Details
Packet Bytes
None
Pane 2:
Packet List
Packet Details
Packet Bytes
None
Pane 3:
Packet List
Packet Details
Packet Bytes
None
Show packet separator on Packet List
Restore Defaults
OK
Cancel
Help

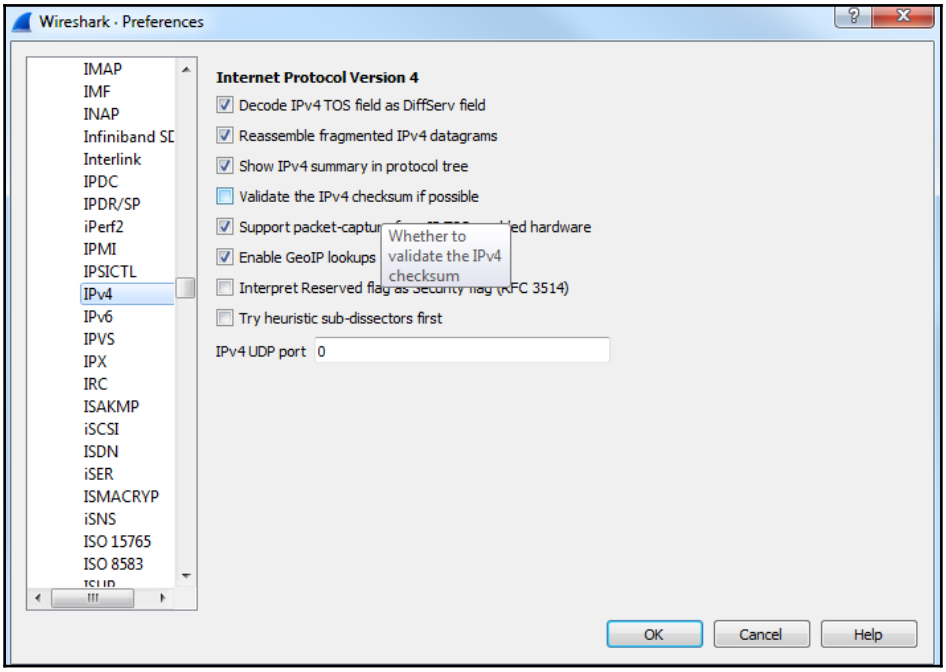

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Displayed
Title
Type
Fields
Field Occurren
No.
Number
Time
Time (format as specified)
Source
Source address
Destination
Destination address
Protocol
Protocol
Length
Packet length (bytes)
Packet comments
Custom
pkt_comment
0
Info
Information
OK
Cancel
Help

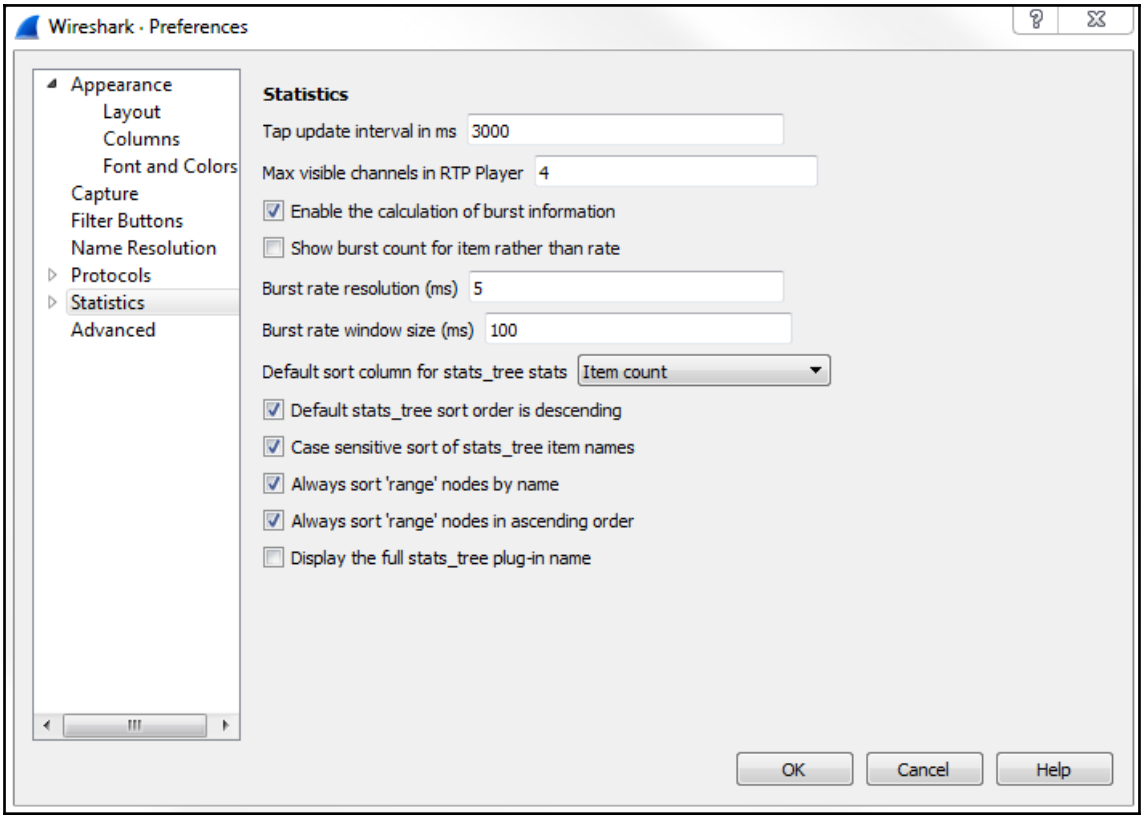

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Main window font:
Consolas 10.0
Example GIF query packets have jumbo window sizes 0123456789
Colors:
Sample marked packet text
Sample ignored packet text
Sample "Follow Stream" client text
Sample "Follow Stream" server text
Sample valid filter
Sample invalid filter
Sample warning filter
OK
Cancel
Help

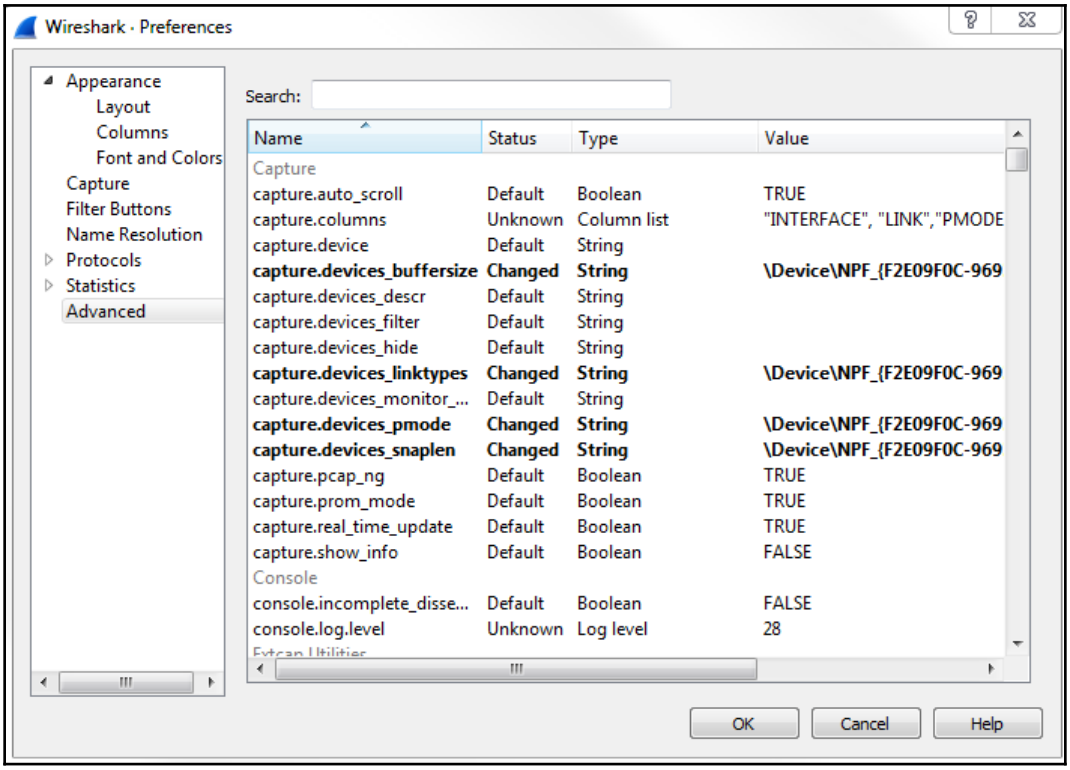

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Default interface
VirtualBox Host-Only Network (\Device\NPF_{F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C})
Local Area Connection (\Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41})
USBPcap1 (\\.\USBPcap1)
USBPcap2 (\\.\USBPcap2)
USBPcap3 (\\.\USBPcap3)
Automatic scrolling in live capture
OK
Cancel
Help

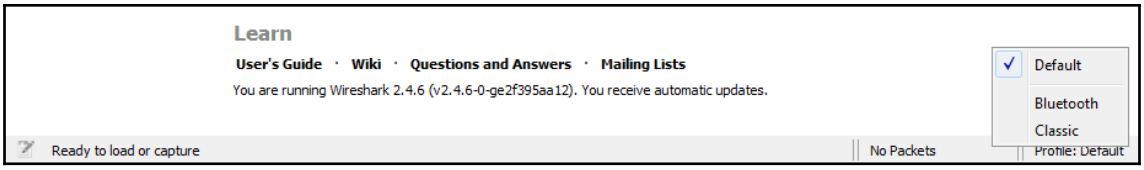

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Enabled
Button Label
Filter Expression
Gateway
ip.host == 192.168.5.25
DNS
(dns)
Gateway
ip.host == 192.168.5.25
DNS
(dns)
OK
Cancel
Help

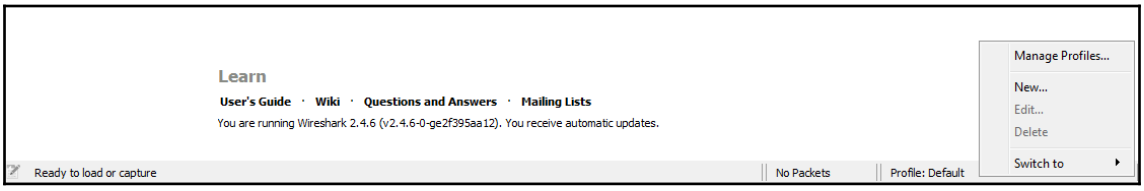

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Name Resolution
Resolve MAC addresses
Resolve transport names
Resolve network (IP) addresses
Use captured DNS packet data for address resolution
Use an external network name resolver
Maximum concurrent requests
500
Only use the profile "hosts" file
Resolve VLAN IDs
Resolve SS7 PCs
Enable OID resolution
Suppress SMI errors
SMI (MIB and PIB) paths
Edit...
SMI (MIB and PIB) modules
Edit...
GeoIP database directories
Edit...
OK
Cancel
Help

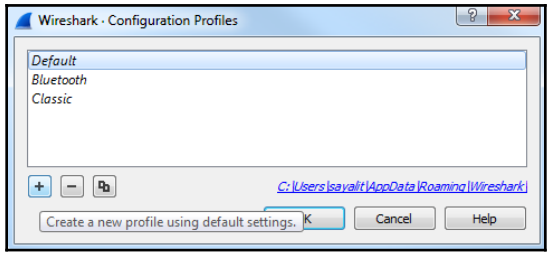

Wireshark · Preferences
IMAP
IMF
INAP
Infiniband SD
Interlink
IPDC
IPDR/SP
iPerf2
IPMI
IPSICTL
IPv4
IPv6
IPVS
IPX
IRC
ISAKMP
iSCSI
ISDN
iSER
ISMACRYP
iSNS
ISO 15765
ISO 8583
Internet Protocol Version 4
Decode IPv4 TOS field as DiffServ field
Reassemble fragmented IPv4 datagrams
Show IPv4 summary in protocol tree
Validate the IPv4 checksum if possible
Support packet-captur ed hardware
Enable GeoIP lookups
Whether to validate the IPv4 checksum
Interpret Reserved flag as Security flag (RFC 3514)
Try heuristic sub-dissectors first
IPv4 UDP port 0
OK
Cancel
Help

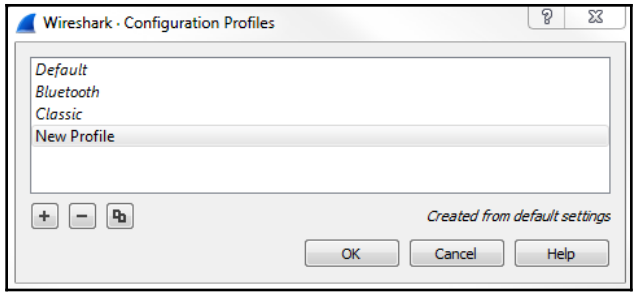

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Statistics
Tap update interval in ms 3000
Max visible channels in RTP Player 4
Enable the calculation of burst information
Show burst count for item rather than rate
Burst rate resolution (ms) 5
Burst rate window size (ms) 100
Default sort column for stats_tree stats Item count
Default stats_tree sort order is descending
Case sensitive sort of stats_tree item names
Always sort 'range' nodes by name
Always sort 'range' nodes in ascending order
Display the full stats_tree plug-in name
OK
Cancel
Help

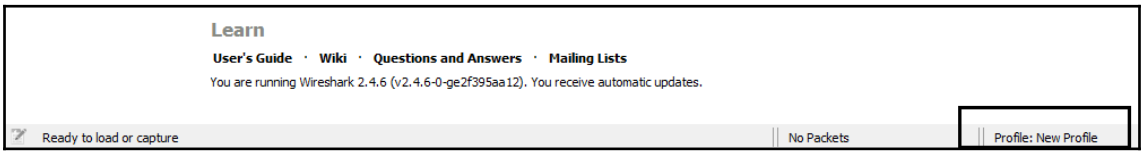

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Search:
Name
Status
Type
Value
Capture
capture.auto_scroll
Default
Boolean
TRUE
capture.columns
Unknown
Column list
"INTERFACE", "LINK","PMODE
capture.device
Default
String
capture.devices_buffersize
Changed
String
\Device\NPF_{F2E09F0C-969
capture.devices_descr
Default
String
capture.devices_filter
Default
String
capture.devices_hide
Default
String
capture.devices_linktypes
Changed
String
\Device\NPF_{F2E09F0C-969
capture.devices_monitor_...
Default
String
capture.devices_pmode
Changed
String
\Device\NPF_{F2E09F0C-969
capture.devices_snaplen
Changed
String
\Device\NPF_{F2E09F0C-969
capture.pcap_ng
Default
Boolean
TRUE
capture.prom_mode
Default
Boolean
TRUE
capture.real_time_update
Default
Boolean
TRUE
capture.show_info
Default
Boolean
FALSE
Console
console.incomplete_disse...
Default
Boolean
FALSE
console.log.level
Unknown
Log level
28
OK
Cancel
Help

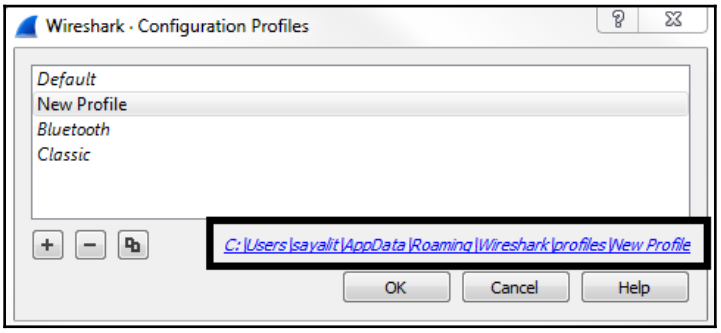

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395aa12). You receive automatic updates.
Default
Bluetooth
Classic
Ready to load or capture
No Packets
Profile: Default

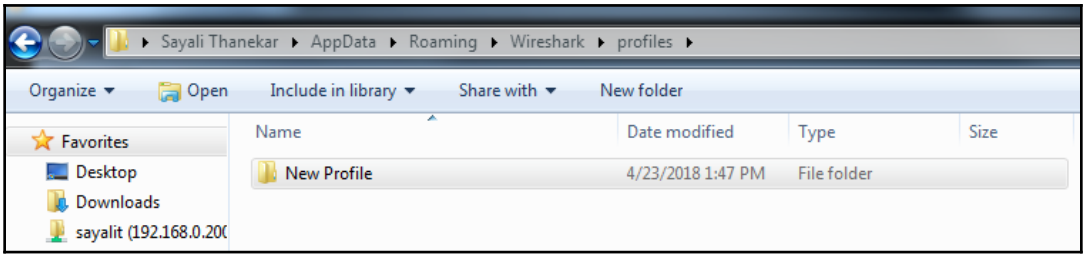

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395aa12). You receive automatic updates.
Manage Profiles...
New...
Edit...
Delete
Switch to
Ready to load or capture
No Packets
Profile: Default

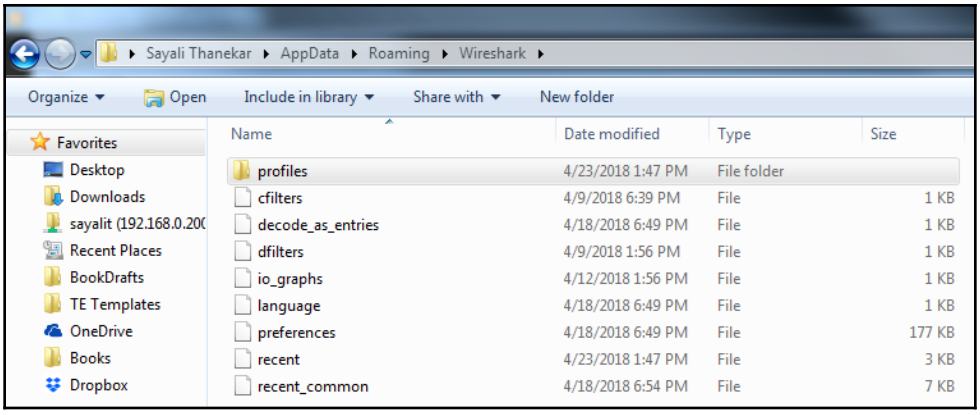

Wireshark · Configuration Profiles
Default
Bluetooth
Classic
C:\Users\sayalit\AppData\Roaming\Wireshark\
Create a new profile using default settings.
Cancel
Help

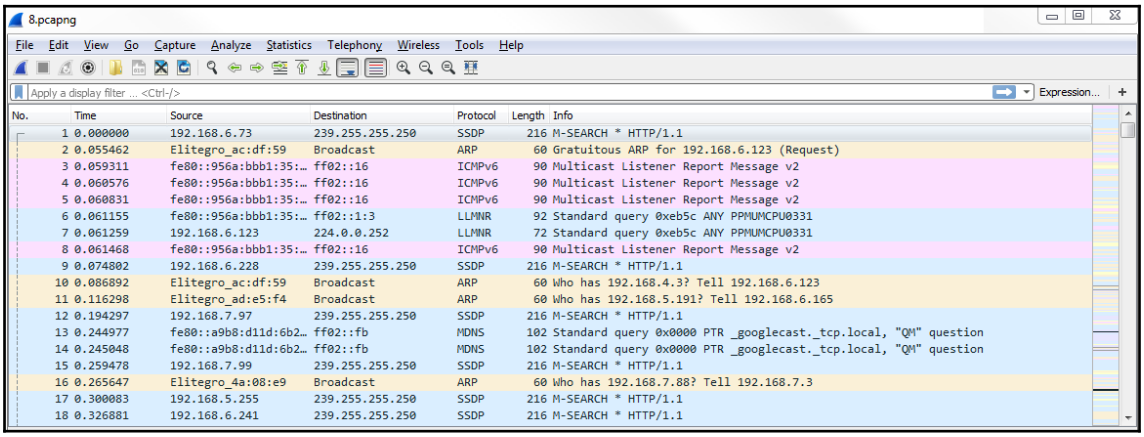

Wireshark · Configuration Profiles
Default
Bluetooth
Classic
New Profile
Created from default settings
OK
Cancel
Help

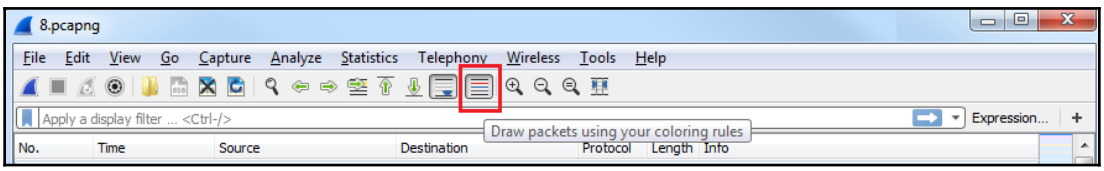

Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395aa12). You receive automatic updates.
Ready to load or capture
No Packets
Profile: New Profile

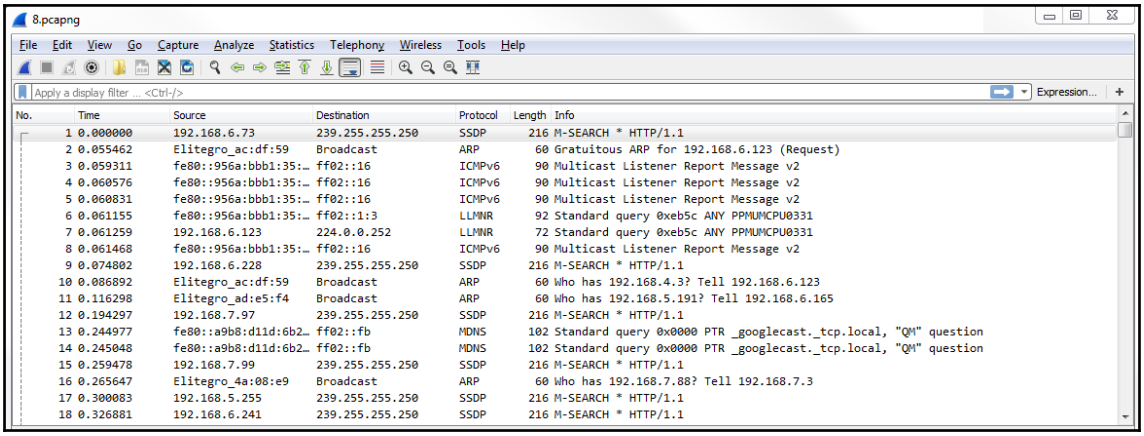

Wireshark · Configuration Profiles
Default
New Profile
Bluetooth
Classic
C:\Users\sayalit\AppData\Roaming\Wireshark\profiles\New Profile
OK
Cancel
Help

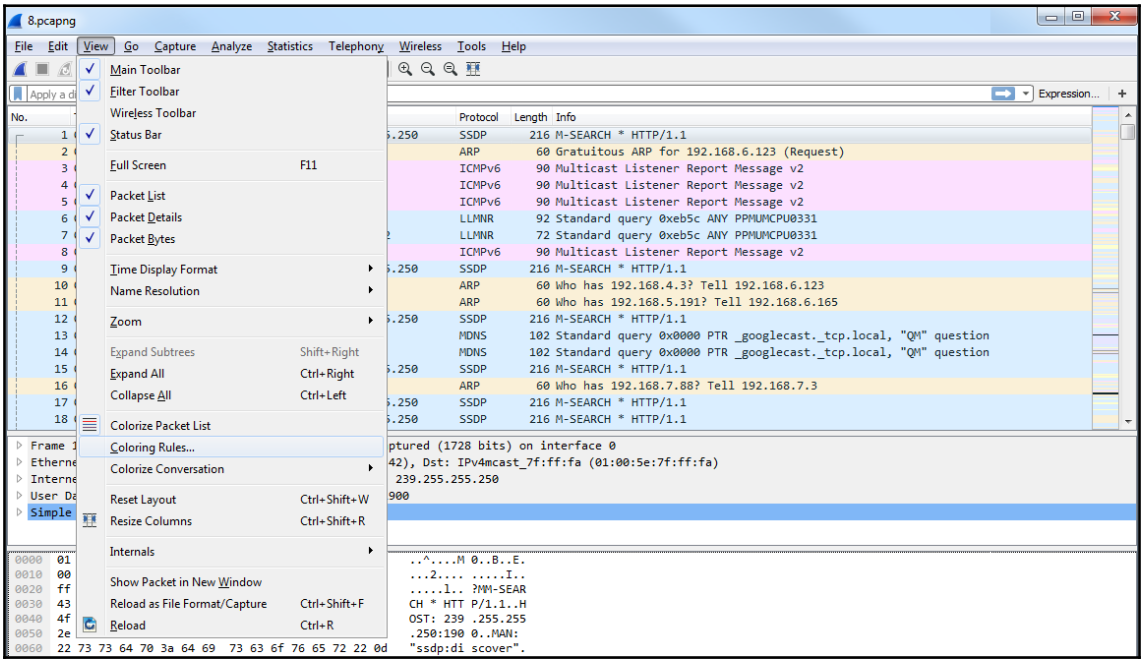

Sayali Thanekar ▸ AppData ▸ Roaming ▸ Wireshark ▸ profiles ▸
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
sayalit (192.168.0.20(
Name
Date modified
Type
Size
New Profile
4/23/2018 1:47 PM
File folder

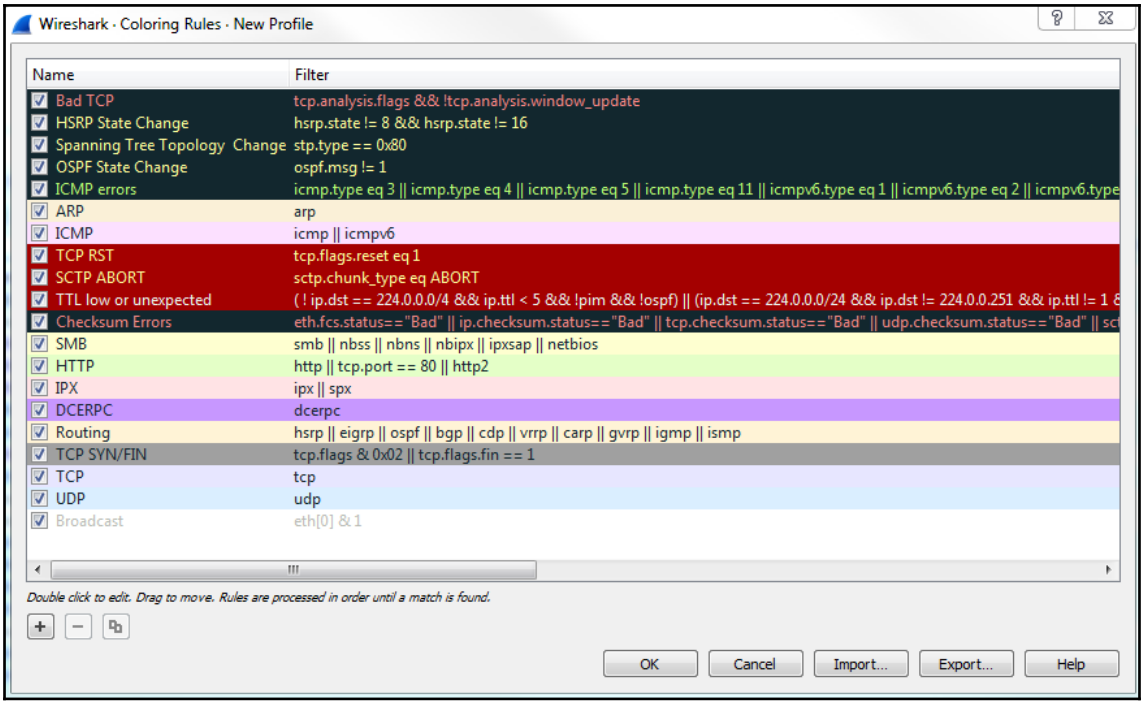

Sayali Thanekar ▸ AppData ▸ Roaming ▸ Wireshark ▸
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
sayalit (192.168.0.20(
Recent Places
BookDrafts
TE Templates
OneDrive
Books
Dropbox
Name
Date modified
Type
Size
profiles 4/23/2018 1:47 PM File folder
cfilters 4/9/2018 6:39 PM File 1 KB
decode_as_entries 4/18/2018 6:49 PM File 1 KB
dfilters 4/9/2018 1:56 PM File 1 KB
io_graphs 4/12/2018 1:56 PM File 1 KB
language 4/18/2018 6:49 PM File 1 KB
preferences 4/18/2018 6:49 PM File 177 KB
recent 4/23/2018 1:47 PM File 3 KB
recent_common 4/18/2018 6:54 PM File 7 KB

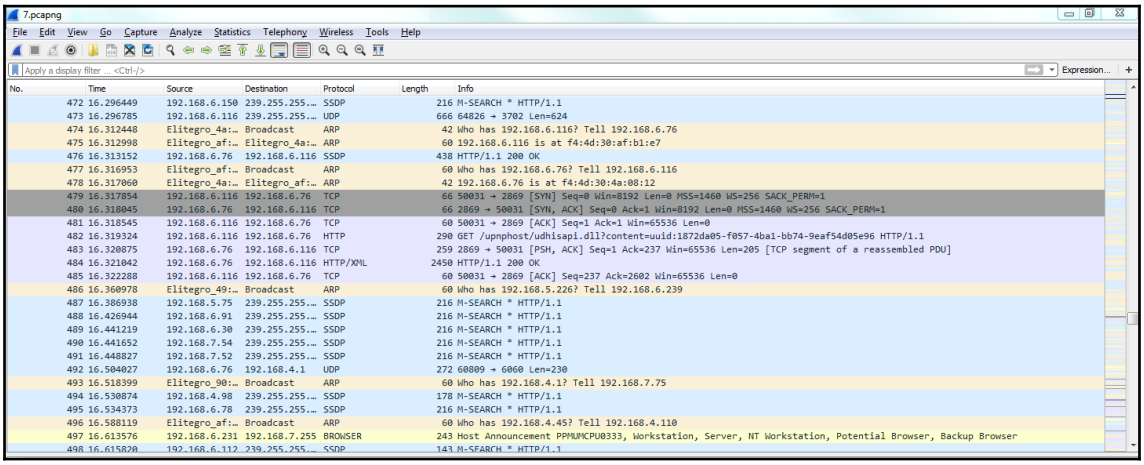

8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.6.73 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 0.055462 Elitegro_ac:df:59 Broadcast ARP 60 Gratuitous ARP for 192.168.6.123 (Request)
3 0.059311 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
4 0.060576 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.060831 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
6 0.061155 fe80::956a:bbb1:35:... ff02::1:3 LLMNR 92 Standard query 0xeb5c ANY PPMUMCPU0331
7 0.061259 192.168.6.123 224.0.0.252 LLMNR 72 Standard query 0xeb5c ANY PPMUMCPU0331
8 0.061468 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
9 0.074802 192.168.6.228 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
10 0.086892 Elitegro_ac:df:59 Broadcast ARP 60 Who has 192.168.4.3? Tell 192.168.6.123
11 0.116298 Elitegro_ad:e5:f4 Broadcast ARP 60 Who has 192.168.5.191? Tell 192.168.6.165
12 0.194297 192.168.7.97 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
13 0.244977 fe80::a9b8:d11d:6b2... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
14 0.245048 fe80::a9b8:d11d:6b2... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
15 0.259478 192.168.7.99 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16 0.265647 Elitegro_4a:08:e9 Broadcast ARP 60 Who has 192.168.7.88? Tell 192.168.7.3
17 0.300083 192.168.5.255 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
18 0.326881 192.168.6.241 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1

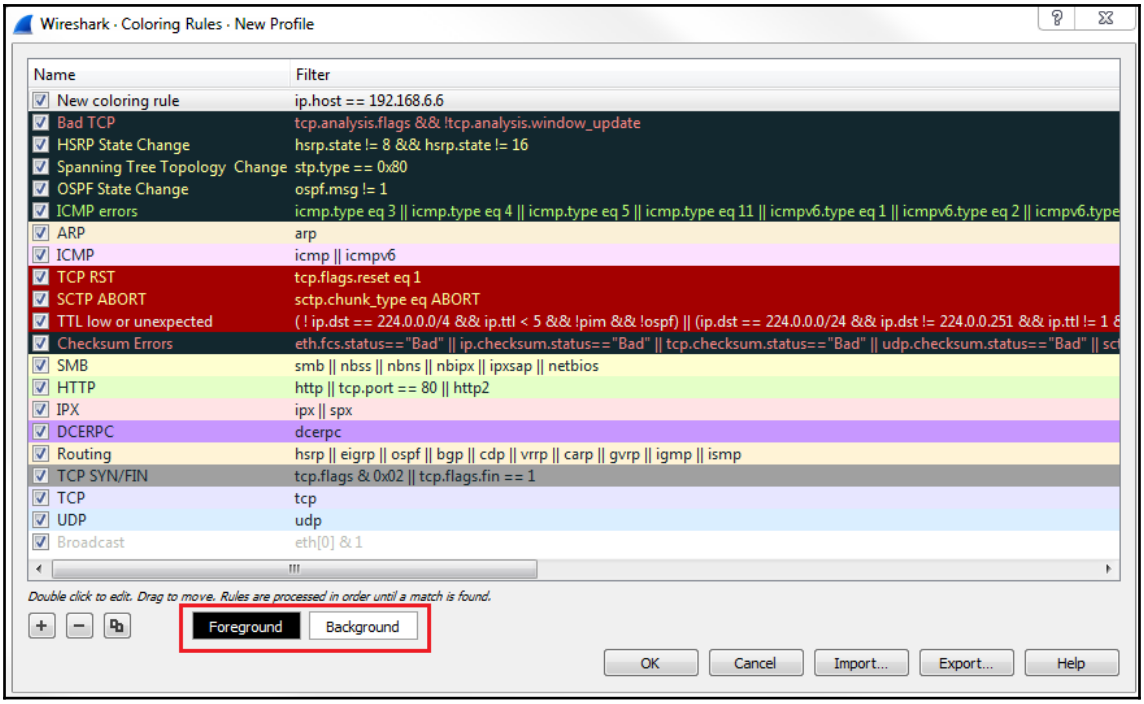

8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Draw packets using your coloring rules
No. Time Source Destination Protocol Length Info

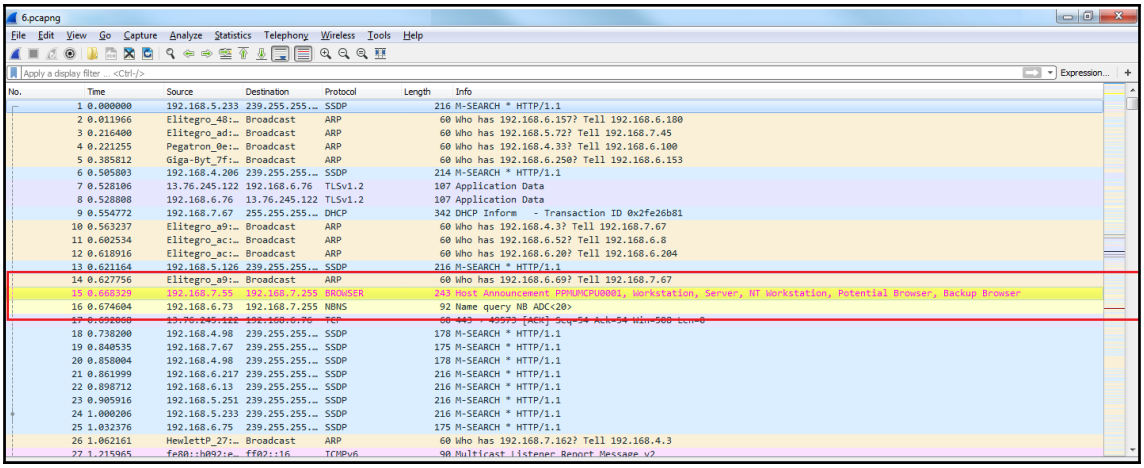

8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.6.73 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2 0.055462 Elitegro_ac:df:59 Broadcast ARP 60 Gratuitous ARP for 192.168.6.123 (Request)
3 0.059311 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
4 0.060576 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
5 0.060831 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
6 0.061155 fe80::956a:bbb1:35:... ff02::1:3 LLMNR 92 Standard query 0xeb5c ANY PPMUMCPU0331
7 0.061259 192.168.6.123 224.0.0.252 LLMNR 72 Standard query 0xeb5c ANY PPMUMCPU0331
8 0.061468 fe80::956a:bbb1:35:... ff02::16 ICMPv6 90 Multicast Listener Report Message v2
9 0.074802 192.168.6.228 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
10 0.086892 Elitegro_ac:df:59 Broadcast ARP 60 Who has 192.168.4.3? Tell 192.168.6.123
11 0.116298 Elitegro_ad:e5:f4 Broadcast ARP 60 Who has 192.168.5.191? Tell 192.168.6.165
12 0.194297 192.168.7.97 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
13 0.244977 fe80::a9b8:d11d:6b2... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
14 0.245048 fe80::a9b8:d11d:6b2... ff02::fb MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
15 0.259478 192.168.7.99 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
16 0.265647 Elitegro_4a:08:e9 Broadcast ARP 60 Who has 192.168.7.88? Tell 192.168.7.3
17 0.300083 192.168.5.255 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
18 0.326881 192.168.6.241 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1

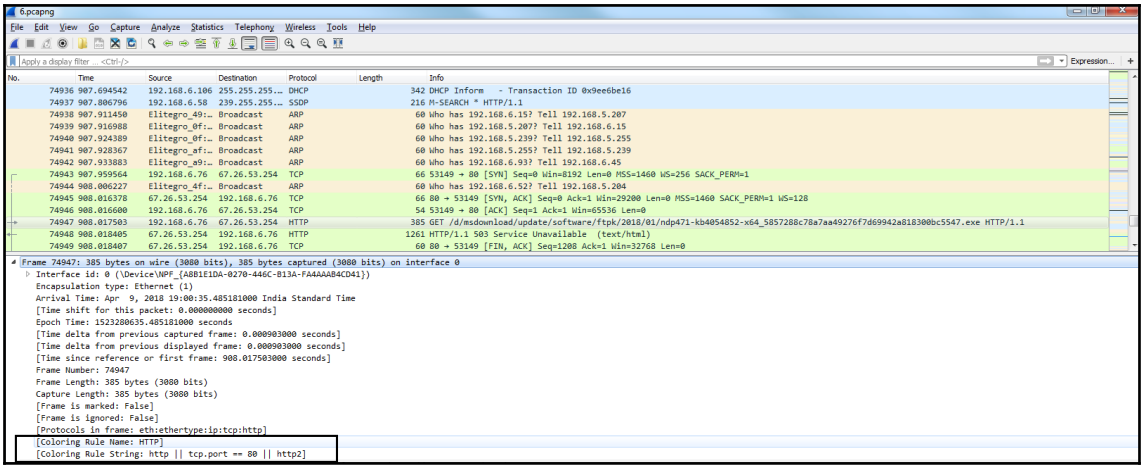

8.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Expression...
Protocol Length Info
SSDP 216 M-SEARCH * HTTP/1.1
ARP 60 Gratuitous ARP for 192.168.6.123 (Request)
ICMPv6 90 Multicast Listener Report Message v2
ICMPv6 90 Multicast Listener Report Message v2
ICMPv6 90 Multicast Listener Report Message v2
LLMNR 92 Standard query 0xeb5c ANY PPMUMCPU0331
LLMNR 72 Standard query 0xeb5c ANY PPMUMCPU0331
ICMPv6 90 Multicast Listener Report Message v2
SSDP 216 M-SEARCH * HTTP/1.1
ARP 60 Who has 192.168.4.3? Tell 192.168.6.123
ARP 60 Who has 192.168.5.191? Tell 192.168.6.165
SSDP 216 M-SEARCH * HTTP/1.1
MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
MDNS 102 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
SSDP 216 M-SEARCH * HTTP/1.1
ARP 60 Who has 192.168.7.88? Tell 192.168.7.3
SSDP 216 M-SEARCH * HTTP/1.1
SSDP 216 M-SEARCH * HTTP/1.1
Frame 1
Ethernet
Internet
User Da
Simple
ptured (1728 bits) on interface 0
42), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
239.255.255.250
900
0000 01
0010 00
0020 ff
0030 43
0040 4f
0050 2e
0060 22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d
..^....M 0..B..E.
...2.... .....I..
.....l.. ?MM-SEAR
CH * HTT P/1.1..H
OST: 239 .255.255
.250:190 0..MAN:
"ssdp:di scover".

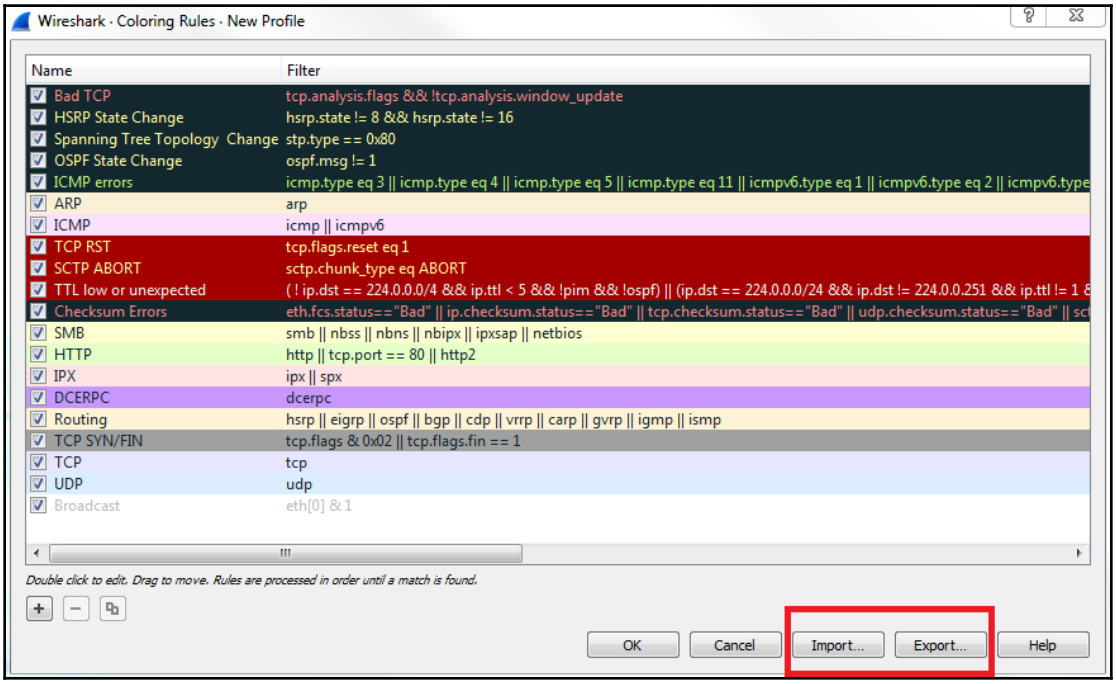

Wireshark · Coloring Rules · New Profile
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sc
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
OK
Cancel
Import...
Export...
Help

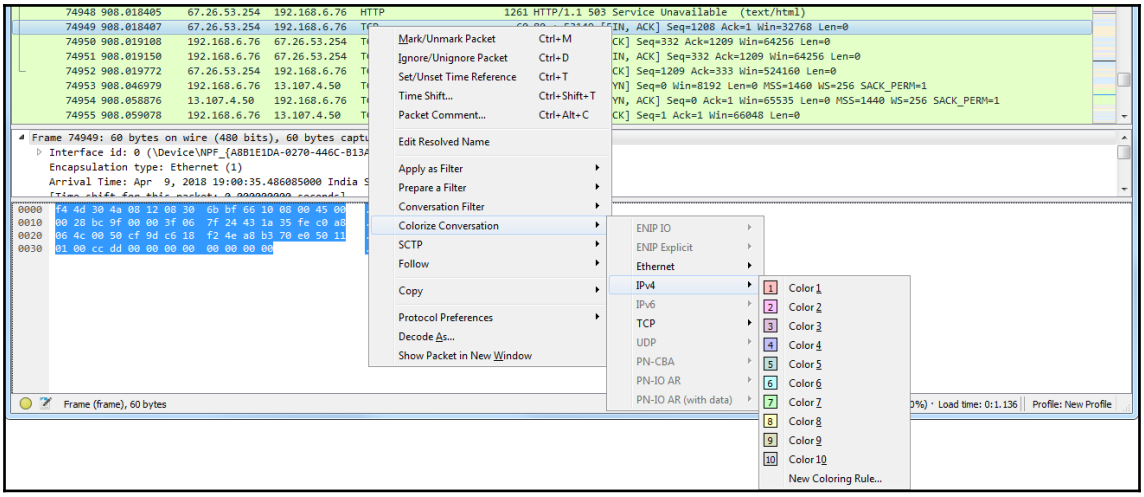

7.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
472 16.296449 192.168.6.150 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
473 16.296785 192.168.6.116 239.255.255.... UDP 666 64826 → 3702 Len=624
474 16.312448 Elitegro_4a:... Broadcast ARP 42 Who has 192.168.6.116? Tell 192.168.6.76
475 16.312998 Elitegro_af:... Elitegro_4a:... ARP 60 192.168.6.116 is at f4:4d:30:af:b1:e7
476 16.313152 192.168.6.76 192.168.6.116 SSDP 438 HTTP/1.1 200 OK
477 16.316953 Elitegro_af:... Broadcast ARP 60 Who has 192.168.6.76? Tell 192.168.6.116
478 16.317060 Elitegro_4a:... Elitegro_af:... ARP 42 192.168.6.76 is at f4:4d:30:4a:08:12
479 16.317854 192.168.6.116 192.168.6.76 TCP 66 50031 → 2869 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
480 16.318045 192.168.6.76 192.168.6.116 TCP 66 2869 → 50031 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
481 16.318545 192.168.6.116 192.168.6.76 TCP 60 50031 → 2869 [ACK] Seq=1 Ack=1 Win=65536 Len=0
482 16.319324 192.168.6.116 192.168.6.76 HTTP 290 GET /upnphost/udhisapi.dll?content=uuid:1872da05-f057-4ba1-bb74-9eaf54d05e96 HTTP/1.1
483 16.320875 192.168.6.76 192.168.6.116 TCP 259 2869 → 50031 [PSH, ACK] Seq=1 Ack=237 Win=65536 Len=205 [TCP segment of a reassembled PDU]
484 16.321042 192.168.6.76 192.168.6.116 HTTP/XML 2450 HTTP/1.1 200 OK
485 16.322288 192.168.6.116 192.168.6.76 TCP 60 50031 → 2869 [ACK] Seq=237 Ack=2602 Win=65536 Len=0
486 16.360978 Elitegro_49:... Broadcast ARP 60 Who has 192.168.5.226? Tell 192.168.6.239
487 16.386938 192.168.5.75 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
488 16.426944 192.168.6.91 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
489 16.441219 192.168.6.30 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
490 16.441652 192.168.7.54 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
491 16.448827 192.168.7.52 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
492 16.504027 192.168.6.76 192.168.4.1 UDP 272 60809 → 6060 Len=230
493 16.518399 Elitegro_90:... Broadcast ARP 60 Who has 192.168.4.1? Tell 192.168.7.75
494 16.530874 192.168.4.98 239.255.255.... SSDP 178 M-SEARCH * HTTP/1.1
495 16.534373 192.168.6.78 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
496 16.588119 Elitegro_af:... Broadcast ARP 60 Who has 192.168.4.45? Tell 192.168.4.110
497 16.613576 192.168.6.231 192.168.7.255 BROWSER 243 Host Announcement PPMUMCPU0333, Workstation, Server, NT Workstation, Potential Browser, Backup Browser
498 16.615820 192.168.6.112 239.255.255.... SSDP 143 M-SEARCH * HTTP/1.1

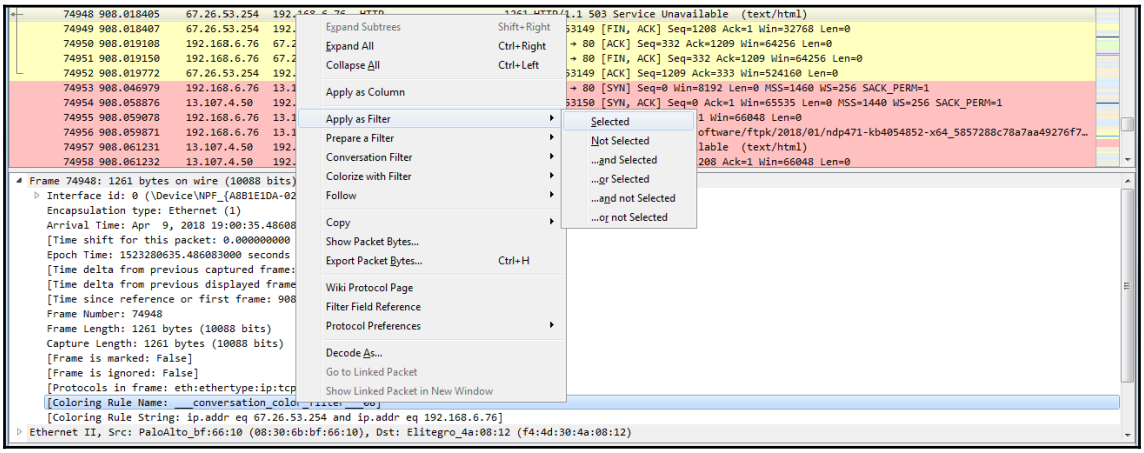

Wireshark · Coloring Rules · New Profile
Name
Filter
New coloring rule
ip.host == 192.168.6.6
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sc
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
Foreground
Background
OK
Cancel
Import...
Export...
Help

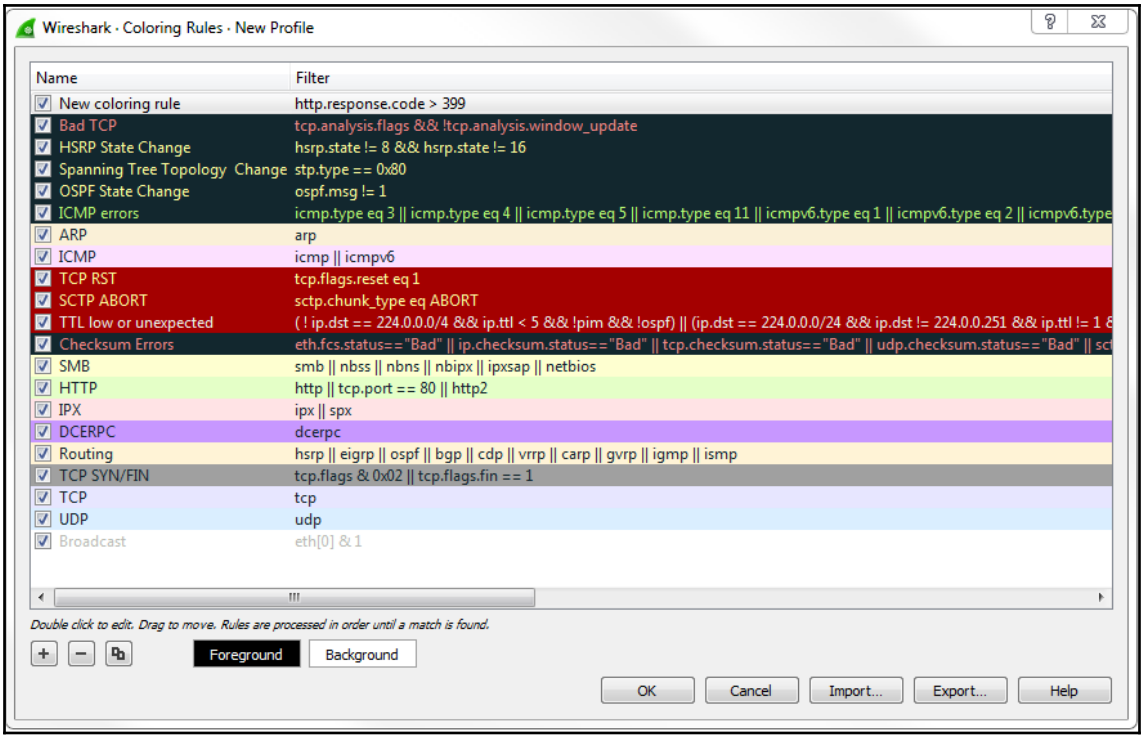

6.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.5.233 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
2 0.011966 Elitegro_48:... Broadcast ARP 60 Who has 192.168.6.157? Tell 192.168.6.180
3 0.216400 Elitegro_ad:... Broadcast ARP 60 Who has 192.168.5.72? Tell 192.168.7.45
4 0.221255 Pegatron_0e:... Broadcast ARP 60 Who has 192.168.4.33? Tell 192.168.6.100
5 0.385812 Giga-Byt_7f:... Broadcast ARP 60 Who has 192.168.6.250? Tell 192.168.6.153
6 0.505803 192.168.4.206 239.255.255.... SSDP 214 M-SEARCH * HTTP/1.1
7 0.528106 13.76.245.122 192.168.6.76 TLSv1.2 107 Application Data
8 0.528808 192.168.6.76 13.76.245.122 TLSv1.2 107 Application Data
9 0.554772 192.168.7.67 255.255.255.... DHCP 342 DHCP Inform - Transaction ID 0x2fe26b81
10 0.563237 Elitegro_a9:... Broadcast ARP 60 Who has 192.168.4.3? Tell 192.168.7.67
11 0.602534 Elitegro_ac:... Broadcast ARP 60 Who has 192.168.6.52? Tell 192.168.6.8
12 0.618916 Elitegro_ac:... Broadcast ARP 60 Who has 192.168.6.20? Tell 192.168.6.204
13 0.621164 192.168.5.126 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
14 0.627756 Elitegro_a9:... Broadcast ARP 60 Who has 192.168.6.69? Tell 192.168.7.67
15 0.668329 192.168.7.55 192.168.7.255 BROWSER 243 Host Announcement PPMUMCPU0001, Workstation, Server, NT Workstation, Potential Browser, Backup Browser
16 0.674604 192.168.6.73 192.168.7.255 NBNS 92 Name query NB ADC<20>
17 0.692060 13.76.245.122 192.168.6.76 TCP 60 443 → 49979 [ACK] Seq=54 Ack=54 Win=500 Len=0
18 0.738200 192.168.4.98 239.255.255.... SSDP 178 M-SEARCH * HTTP/1.1
19 0.840535 192.168.7.67 239.255.255.... SSDP 175 M-SEARCH * HTTP/1.1
20 0.858004 192.168.4.98 239.255.255.... SSDP 178 M-SEARCH * HTTP/1.1
21 0.861999 192.168.6.217 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
22 0.898712 192.168.6.13 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
23 0.905916 192.168.5.251 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
24 1.000206 192.168.5.233 239.255.255.... SSDP 216 M-SEARCH * HTTP/1.1
25 1.032376 192.168.6.75 239.255.255.... SSDP 175 M-SEARCH * HTTP/1.1
26 1.062161 HewlettP_27:... Broadcast ARP 60 Who has 192.168.7.162? Tell 192.168.4.3
27 1.215965 fe80::b092:e... ff02::16 ICMPv6 90 Multicast Listener Report Message v2

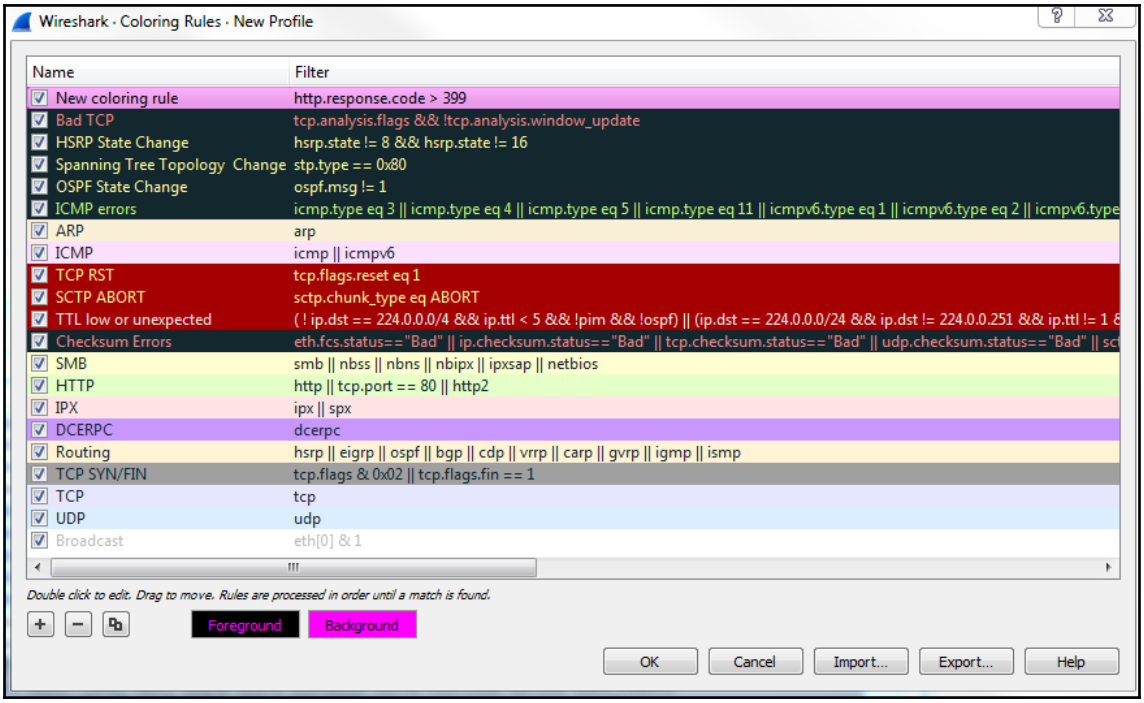

6.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
74936 907.694542 192.168.6.106 255.255.255... DHCP 342 DHCP Inform - Transaction ID 0x9ee6be16
74937 907.806796 192.168.6.58 239.255.255... SSDP 216 M-SEARCH * HTTP/1.1
74938 907.911450 Elitegro_49:... Broadcast ARP 60 Who has 192.168.6.15? Tell 192.168.5.207
74939 907.916988 Elitegro_0f:... Broadcast ARP 60 Who has 192.168.5.20? Tell 192.168.6.15
74940 907.924389 Elitegro_0f:... Broadcast ARP 60 Who has 192.168.5.239? Tell 192.168.5.255
74941 907.928367 Elitegro_af:... Broadcast ARP 60 Who has 192.168.5.255? Tell 192.168.5.239
74942 907.933883 Elitegro_e9:... Broadcast ARP 60 Who has 192.168.6.93? Tell 192.168.6.45
74943 907.959564 192.168.6.76 67.26.53.254 TCP 66 53149 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
74944 908.006227 Elitegro_4f:... Broadcast ARP 60 Who has 192.168.6.52? Tell 192.168.5.204
74945 908.016378 67.26.53.254 192.168.6.76 TCP 66 80 → 53149 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128
74946 908.016600 192.168.6.76 67.26.53.254 TCP 54 53149 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
74947 908.017503 192.168.6.76 67.26.53.254 HTTP 385 GET /d/msdownload/update/software/ftpk/2018/01/ndp471-kb4054852-x64_5857288c78a7aa49276f7d69942a818300bc5547.exe HTTP/1.1
74948 908.018405 67.26.53.254 192.168.6.76 HTTP 1261 HTTP/1.1 503 Service Unavailable (text/html)
74949 908.018407 67.26.53.254 192.168.6.76 TCP 60 80 → 53149 [FIN, ACK] Seq=1208 Ack=1 Win=32768 Len=0
Frame 74947: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits) on interface 0
Interface id: 0 (\Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41})
Encapsulation type: Ethernet (1)
Arrival Time: Apr 9, 2018 19:00:35.485181000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1523280635.485181000 seconds
[Time delta from previous captured frame: 0.000903000 seconds]
[Time delta from previous displayed frame: 0.000903000 seconds]
[Time since reference or first frame: 908.017503000 seconds]
Frame Number: 74947
Frame Length: 385 bytes (3080 bits)
Capture Length: 385 bytes (3080 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http]
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]

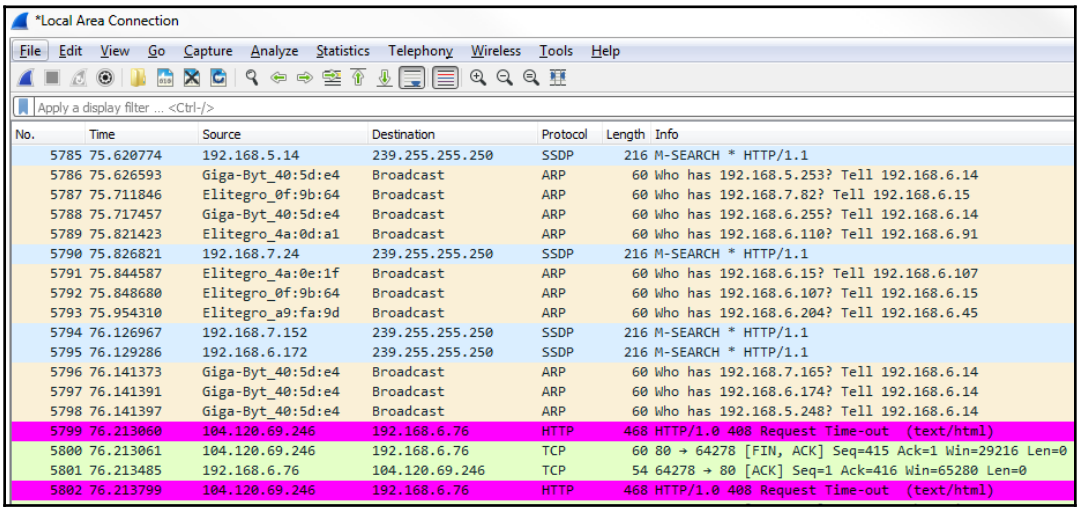

Wireshark · Coloring Rules · New Profile
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sc
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
OK
Cancel
Import...
Export...
Help

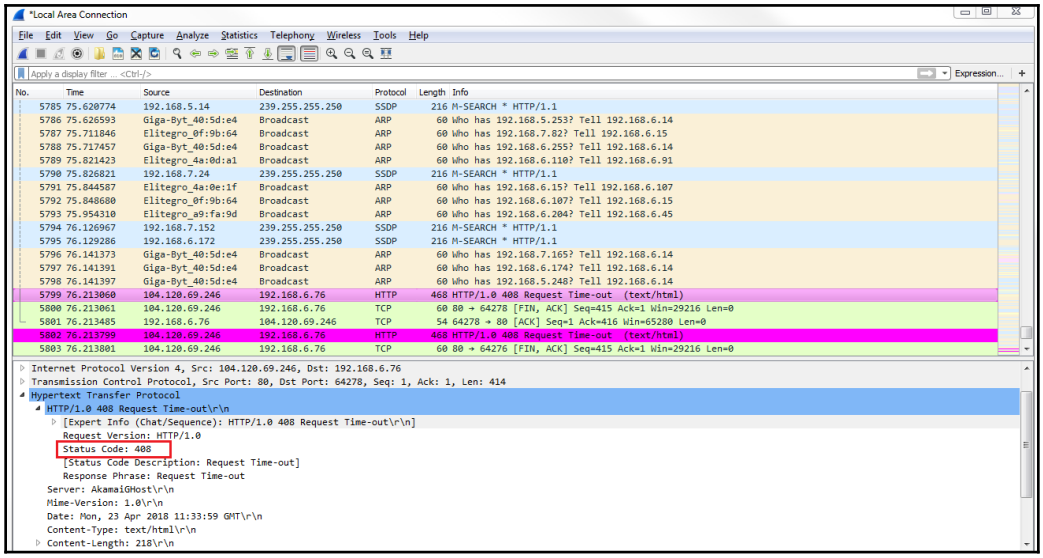

Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
ENIP IO
ENIP Explicit
Ethernet
IPv4
IPv6
TCP
UDP
PN-CBA
PN-IO AR
PN-IO AR (with data)
Color 1
Color 2
Color 3
Color 4
Color 5
Color 6
Color 7
Color 8
Color 9
Color 10
New Coloring Rule...

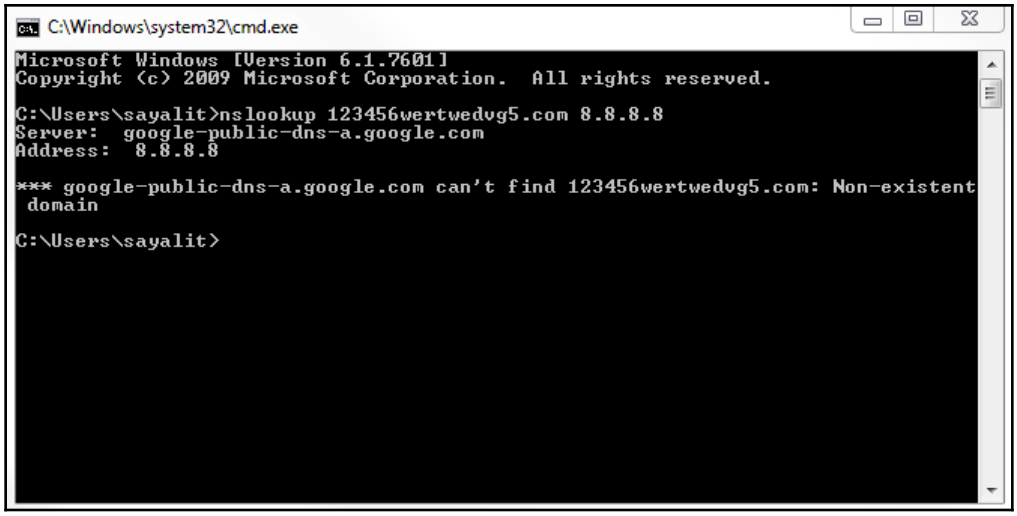

Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

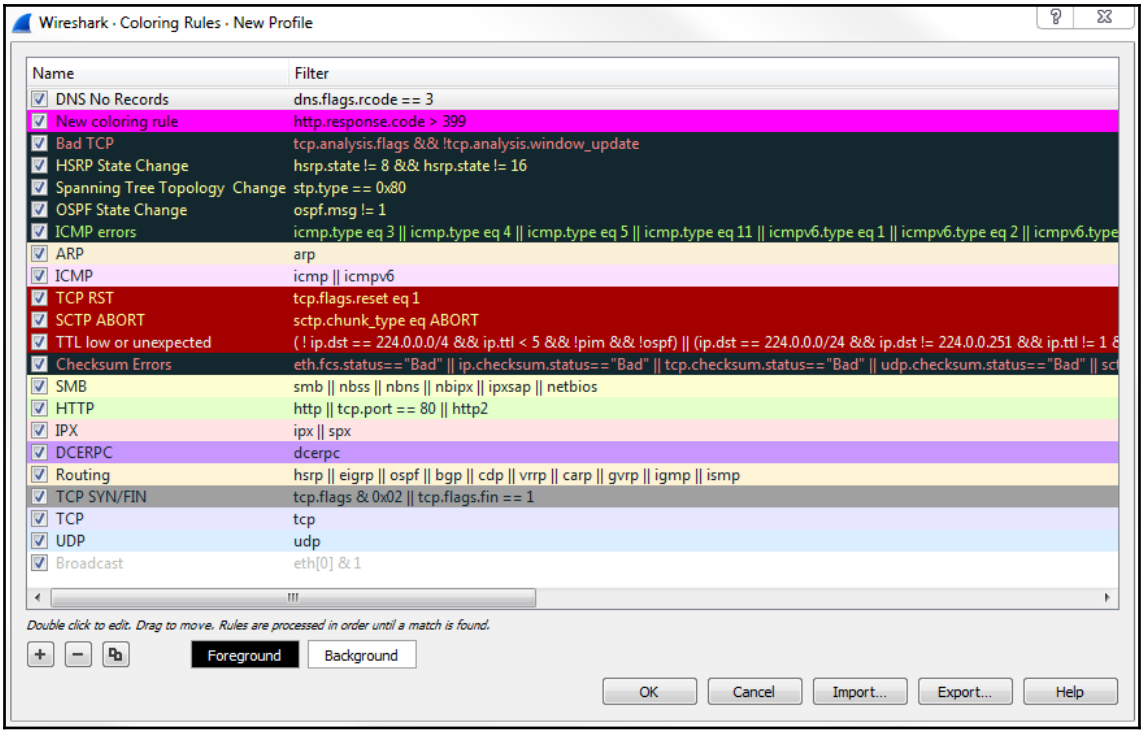

Wireshark · Coloring Rules · New Profile
Name
Filter
New coloring rule
http.response.code > 399
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sct
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
Foreground
Background
OK
Cancel
Import...
Export...
Help

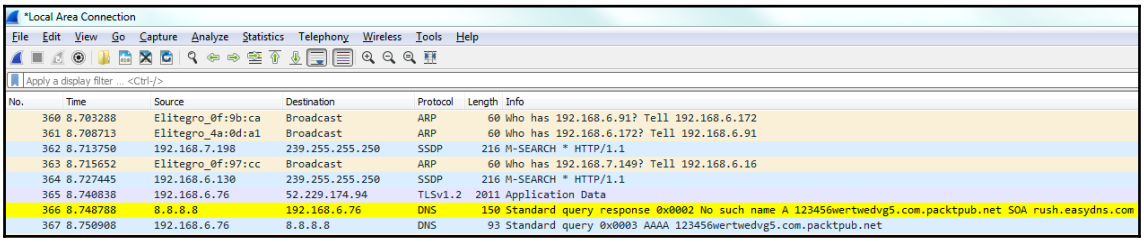

Wireshark · Coloring Rules · New Profile
Name
Filter
New coloring rule
http.response.code > 399
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sc
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
Foreground
Background
OK
Cancel
Import...
Export...
Help

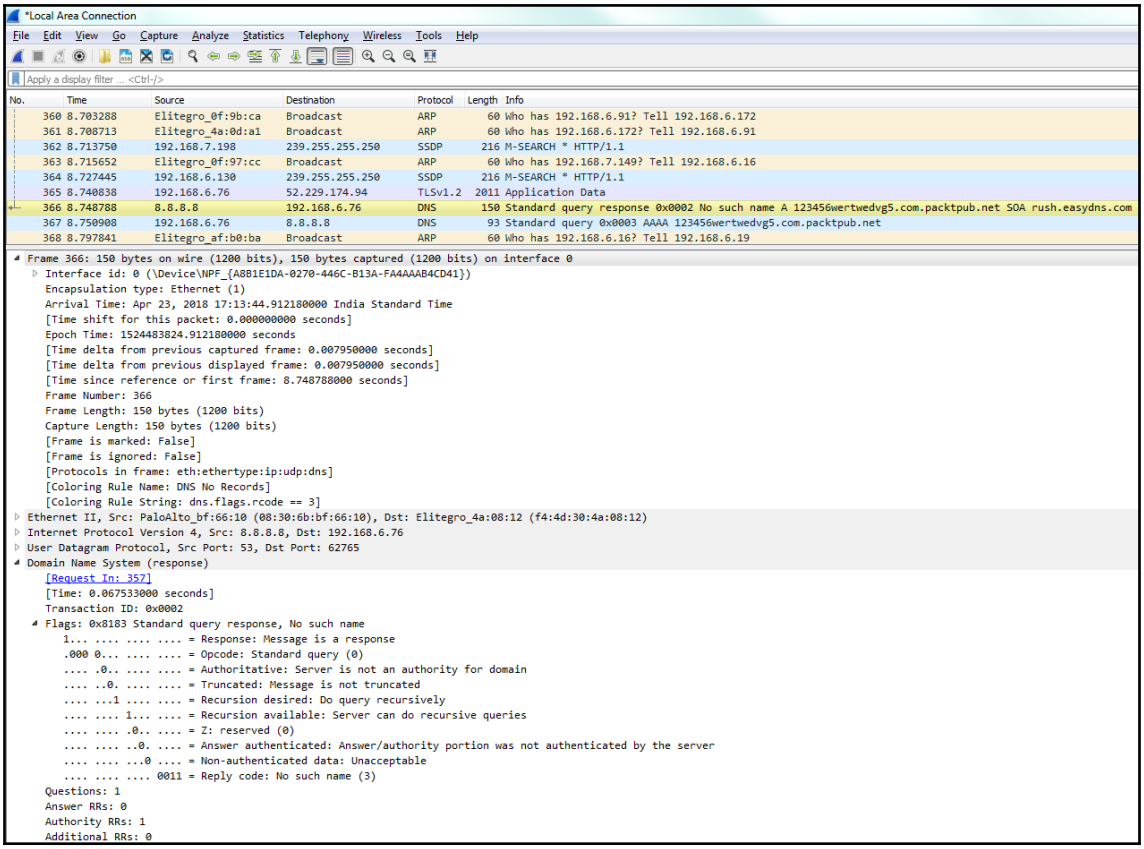

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
5785 75.620774 192.168.5.14 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5786 75.626593 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.5.253? Tell 192.168.6.14
5787 75.711846 Elitegro_0f:9b:64 Broadcast ARP 60 Who has 192.168.7.82? Tell 192.168.6.15
5788 75.717457 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.6.255? Tell 192.168.6.14
5789 75.821423 Elitegro_4a:0d:a1 Broadcast ARP 60 Who has 192.168.6.110? Tell 192.168.6.91
5790 75.826821 192.168.7.24 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5791 75.844587 Elitegro_4a:0e:1f Broadcast ARP 60 Who has 192.168.6.15? Tell 192.168.6.107
5792 75.848680 Elitegro_0f:9b:64 Broadcast ARP 60 Who has 192.168.6.107? Tell 192.168.6.15
5793 75.954310 Elitegro_a9:fa:9d Broadcast ARP 60 Who has 192.168.6.204? Tell 192.168.6.45
5794 76.126967 192.168.7.152 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5795 76.129286 192.168.6.172 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5796 76.141373 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.7.165? Tell 192.168.6.14
5797 76.141391 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.6.174? Tell 192.168.6.14
5798 76.141397 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.5.248? Tell 192.168.6.14
5799 76.213060 104.120.69.246 192.168.6.76 HTTP 468 HTTP/1.0 408 Request Time-out (text/html)
5800 76.213061 104.120.69.246 192.168.6.76 TCP 60 80 → 64278 [FIN, ACK] Seq=415 Ack=1 Win=29216 Len=0
5801 76.213485 192.168.6.76 104.120.69.246 TCP 54 64278 → 80 [ACK] Seq=1 Ack=416 Win=65280 Len=0
5802 76.213799 104.120.69.246 192.168.6.76 HTTP 468 HTTP/1.0 408 Request Time-out (text/html)


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
5785 75.620774 192.168.5.14 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5786 75.626593 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.5.253? Tell 192.168.6.14
5787 75.711846 Elitegro_0f:9b:64 Broadcast ARP 60 Who has 192.168.7.82? Tell 192.168.6.15
5788 75.717457 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.6.255? Tell 192.168.6.14
5789 75.821423 Elitegro_4a:0d:a1 Broadcast ARP 60 Who has 192.168.6.110? Tell 192.168.6.91
5790 75.826821 192.168.7.24 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5791 75.844587 Elitegro_4a:0e:1f Broadcast ARP 60 Who has 192.168.6.15? Tell 192.168.6.107
5792 75.848680 Elitegro_0f:9b:64 Broadcast ARP 60 Who has 192.168.6.107? Tell 192.168.6.15
5793 75.954310 Elitegro_a9:fa:9d Broadcast ARP 60 Who has 192.168.6.204? Tell 192.168.6.45
5794 76.126967 192.168.7.152 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5795 76.129286 192.168.6.172 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5796 76.141373 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.7.165? Tell 192.168.6.14
5797 76.141391 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.6.174? Tell 192.168.6.14
5798 76.141397 Giga-Byt_40:5d:e4 Broadcast ARP 60 Who has 192.168.5.248? Tell 192.168.6.14
5799 76.213060 104.120.69.246 192.168.6.76 HTTP 468 HTTP/1.0 408 Request Time-out (text/html)
5800 76.213061 104.120.69.246 192.168.6.76 TCP 60 80 → 64278 [FIN, ACK] Seq=415 Ack=1 Win=29216 Len=0
5801 76.213485 192.168.6.76 104.120.69.246 TCP 54 64278 → 80 [ACK] Seq=1 Ack=416 Win=65280 Len=0
5802 76.213799 104.120.69.246 192.168.6.76 HTTP 468 HTTP/1.0 408 Request Time-out (text/html)
5803 76.213801 104.120.69.246 192.168.6.76 TCP 60 80 → 64276 [FIN, ACK] Seq=415 Ack=1 Win=29216 Len=0
Internet Protocol Version 4, Src: 104.120.69.246, Dst: 192.168.6.76
Transmission Control Protocol, Src Port: 80, Dst Port: 64278, Seq: 1, Ack: 1, Len: 414
Hypertext Transfer Protocol
HTTP/1.0 408 Request Time-out\r\n
[Expert Info (Chat/Sequence): HTTP/1.0 408 Request Time-out\r\n]
Request Version: HTTP/1.0
Status Code: 408
[Status Code Description: Request Time-out]
Response Phrase: Request Time-out
Server: AkamaiGHost\r\n
Mime-Version: 1.0\r\n
Date: Mon, 23 Apr 2018 11:33:59 GMT\r\n
Content-Type: text/html\r\n
Content-Length: 218\r\n

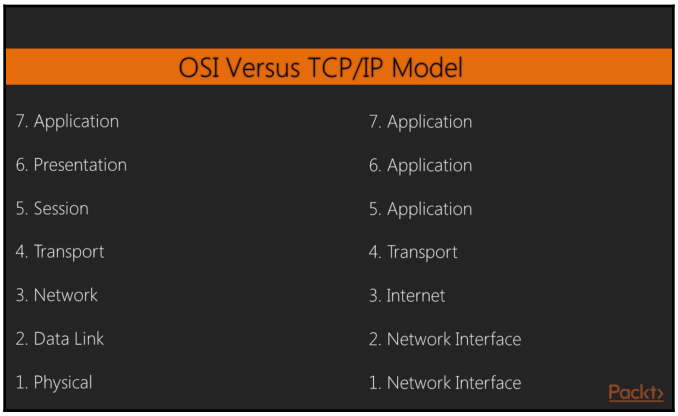

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\sayalit>nslookup 123456wertwedvg5.com 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8
*** google-public-dns-a.google.com can't find 123456wertwedvg5.com: Non-existent domain
C:\Users\sayalit>

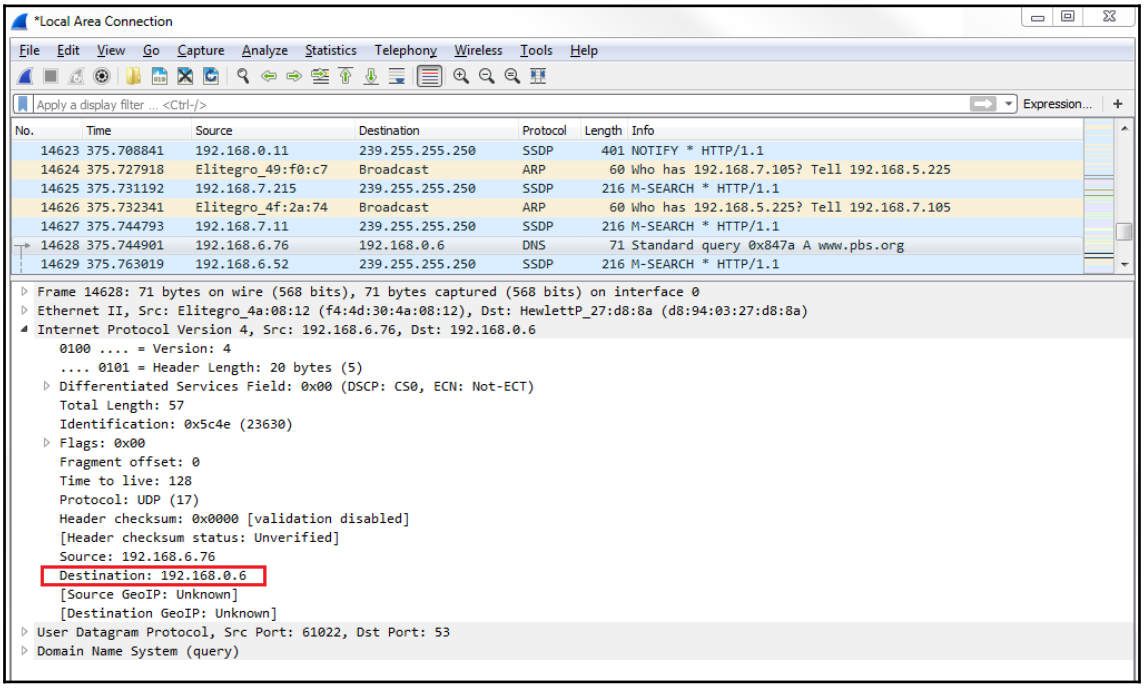

Wireshark · Coloring Rules · New Profile
Name
Filter
DNS No Records
dns.flags.rcode == 3
New coloring rule
http.response.code > 399
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type
ARP
arp
ICMP
icmp || icmpv6
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
TTL low or unexpected
(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) || (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 &
Checksum Errors
eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad" || sc
SMB
smb || nbss || nbns || nbipx || ipxsap || netbios
HTTP
http || tcp.port == 80 || http2
IPX
ipx || spx
DCERPC
dcerpc
Routing
hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
TCP SYN/FIN
tcp.flags & 0x02 || tcp.flags.fin == 1
TCP
tcp
UDP
udp
Broadcast
eth[0] & 1
Double click to edit. Drag to move. Rules are processed in order until a match is found.
Foreground
Background
OK
Cancel
Import...
Export...
Help

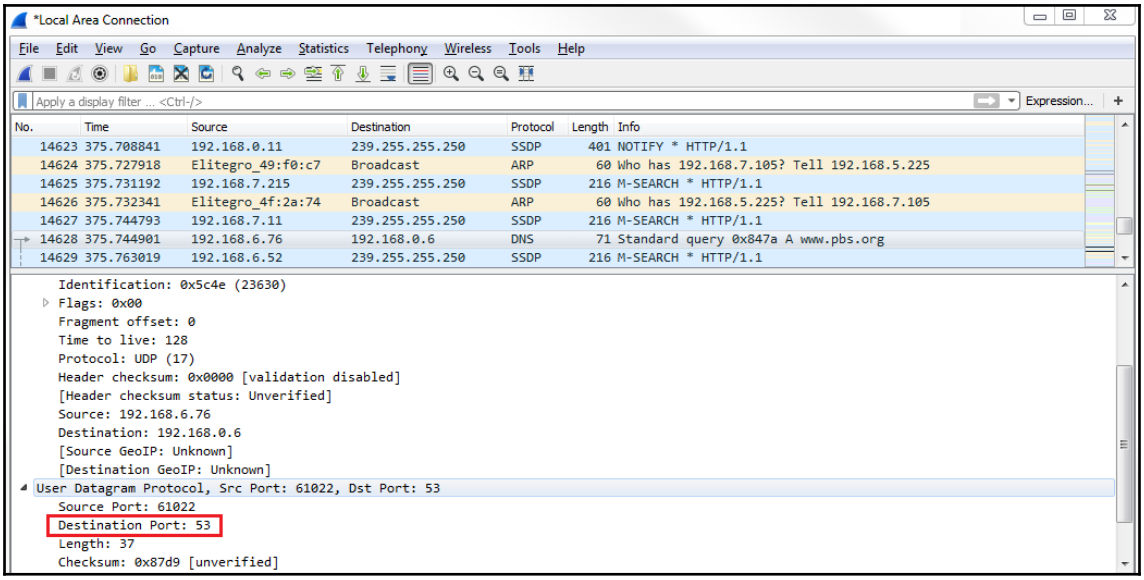

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
360 8.703288 Elitegro_0f:9b:ca Broadcast ARP 60 Who has 192.168.6.91? Tell 192.168.6.172
361 8.708713 Elitegro_4a:0d:a1 Broadcast ARP 60 Who has 192.168.6.172? Tell 192.168.6.91
362 8.713750 192.168.7.198 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
363 8.715652 Elitegro_0f:97:cc Broadcast ARP 60 Who has 192.168.7.149? Tell 192.168.6.16
364 8.727445 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
365 8.740838 192.168.6.76 52.229.174.94 TLSv1.2 2011 Application Data
366 8.748788 8.8.8.8 192.168.6.76 DNS 150 Standard query response 0x0002 No such name A 123456wertwedvg5.com.packtpub.net SOA rush.easydns.com
367 8.750908 192.168.6.76 8.8.8.8 DNS 93 Standard query 0x0003 AAAA 123456wertwedvg5.com.packtpub.net

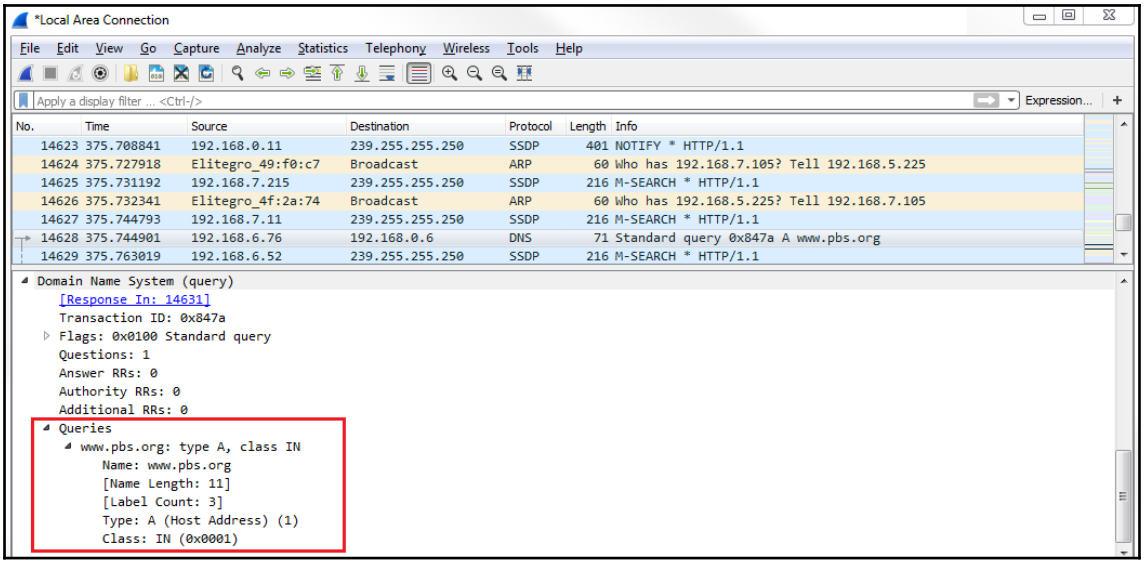

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
360 8.703288 Elitegro_0f:9b:ca Broadcast ARP 60 Who has 192.168.6.91? Tell 192.168.6.172
361 8.708713 Elitegro_4a:0d:a1 Broadcast ARP 60 Who has 192.168.6.172? Tell 192.168.6.91
362 8.713750 192.168.7.198 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
363 8.715652 Elitegro_0f:97:cc Broadcast ARP 60 Who has 192.168.7.149? Tell 192.168.6.16
364 8.727445 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
365 8.740838 192.168.6.76 52.229.174.94 TLSv1.2 2011 Application Data
366 8.748788 8.8.8.8 192.168.6.76 DNS 150 Standard query response 0x0002 No such name A 123456wertwedvg5.com.packtpub.net SOA rush.easydns.com
367 8.750908 192.168.6.76 8.8.8.8 DNS 93 Standard query 0x0003 AAAA 123456wertwedvg5.com.packtpub.net
368 8.797841 Elitegro_af:b0:ba Broadcast ARP 60 Who has 192.168.6.16? Tell 192.168.6.19
Frame 366: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Interface id: 0 (\Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41})
Encapsulation type: Ethernet (1)
Arrival Time: Apr 23, 2018 17:13:44.912180000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1524483824.912180000 seconds
[Time delta from previous captured frame: 0.007950000 seconds]
[Time delta from previous displayed frame: 0.007950000 seconds]
[Time since reference or first frame: 8.748788000 seconds]
Frame Number: 366
Frame Length: 150 bytes (1200 bits)
Capture Length: 150 bytes (1200 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:udp:dns]
[Coloring Rule Name: DNS No Records]
[Coloring Rule String: dns.flags.rcode == 3]
Ethernet II, Src: PaloAlto_bf:66:10 (08:30:6b:bf:66:10), Dst: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.6.76
User Datagram Protocol, Src Port: 53, Dst Port: 62765
Domain Name System (response)
[Request In: 357]
[Time: 0.067533000 seconds]
Transaction ID: 0x0002
Flags: 0x8183 Standard query response, No such name
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0011 = Reply code: No such name (3)
Questions: 1
Answer RRs: 0
Authority RRs: 1
Additional RRs: 0

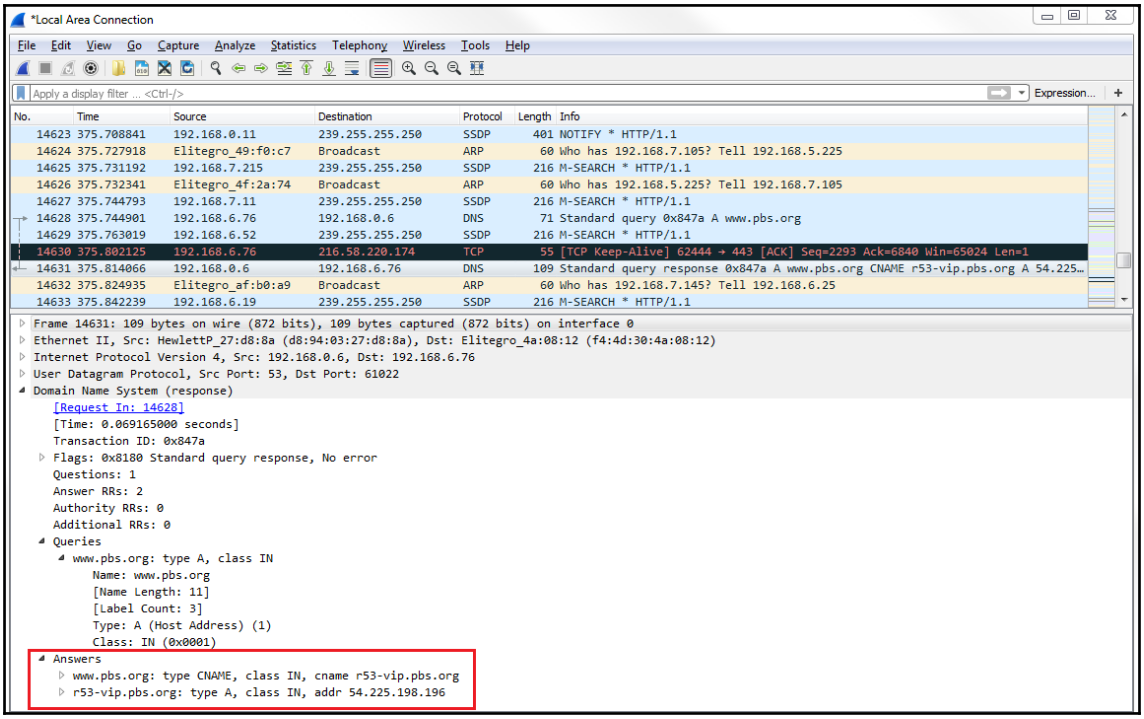
Chapter 05: Statistics

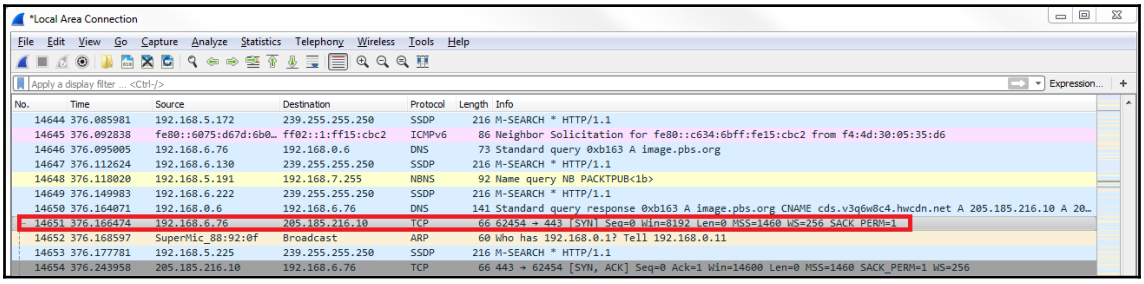


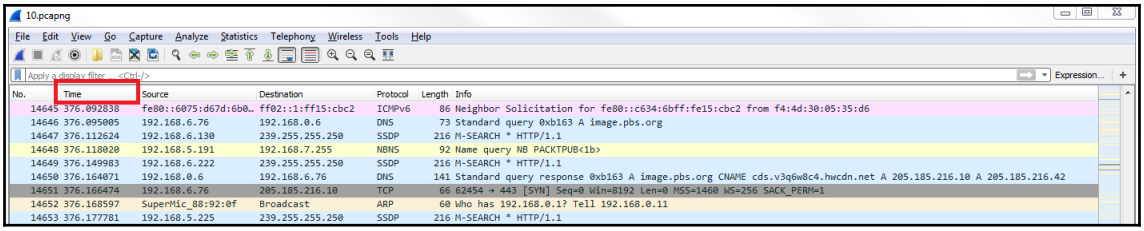


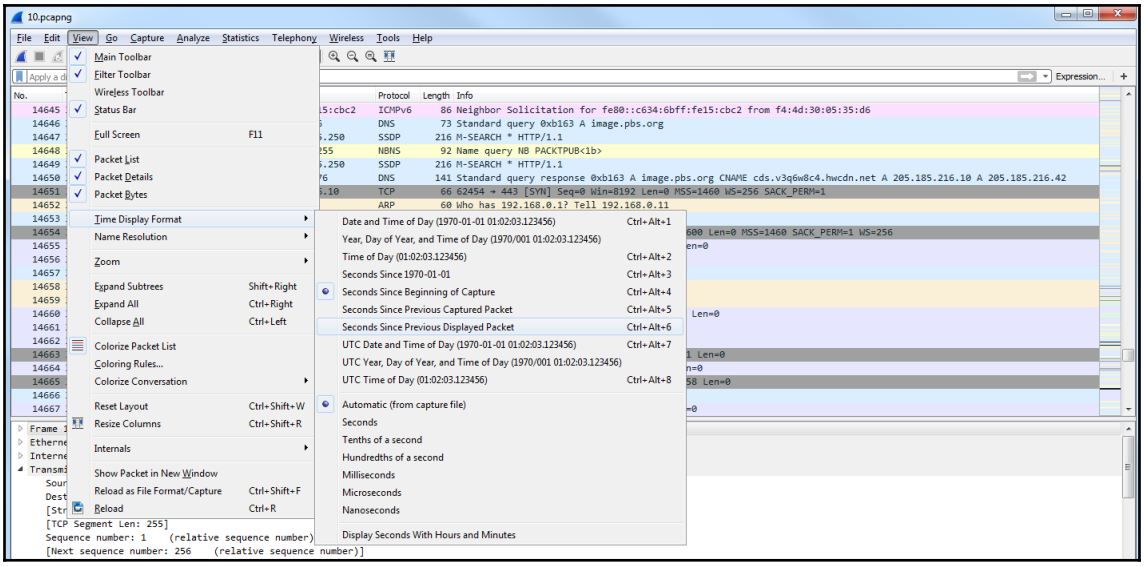

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14623 375.708841 192.168.0.11 239.255.255.250 SSDP 401 NOTIFY * HTTP/1.1
14624 375.727918 Elitegro_49:f0:c7 Broadcast ARP 60 Who has 192.168.7.105? Tell 192.168.5.225
14625 375.731192 192.168.7.215 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14626 375.732341 Elitegro_4f:2a:74 Broadcast ARP 60 Who has 192.168.5.225? Tell 192.168.7.105
14627 375.744793 192.168.7.11 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14628 375.744901 192.168.6.76 192.168.0.6 DNS 71 Standard query 0x847a A www.pbs.org
14629 375.763019 192.168.6.52 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Identification: 0x5c4e (23630)
Flags: 0x00
Fragment offset: 0
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.6.76
Destination: 192.168.0.6
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 61022, Dst Port: 53
Source Port: 61022
Destination Port: 53
Length: 37
Checksum: 0x87d9 [unverified]

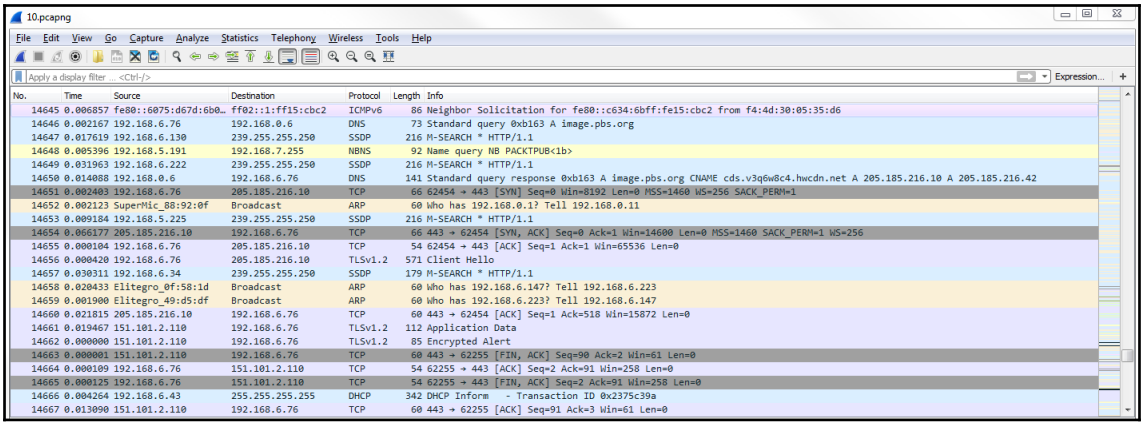

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14623 375.708841 192.168.0.11 239.255.255.250 SSDP 401 NOTIFY * HTTP/1.1
14624 375.727918 Elitegro_49:f0:c7 Broadcast ARP 60 Who has 192.168.7.105? Tell 192.168.5.225
14625 375.731192 192.168.7.215 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14626 375.732341 Elitegro_4f:2a:74 Broadcast ARP 60 Who has 192.168.5.225? Tell 192.168.7.105
14627 375.744793 192.168.7.11 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14628 375.744901 192.168.6.76 192.168.0.6 DNS 71 Standard query 0x847a A www.pbs.org
14629 375.763019 192.168.6.52 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Domain Name System (query)
[Response In: 14631]
Transaction ID: 0x847a
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.pbs.org: type A, class IN
Name: www.pbs.org
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)

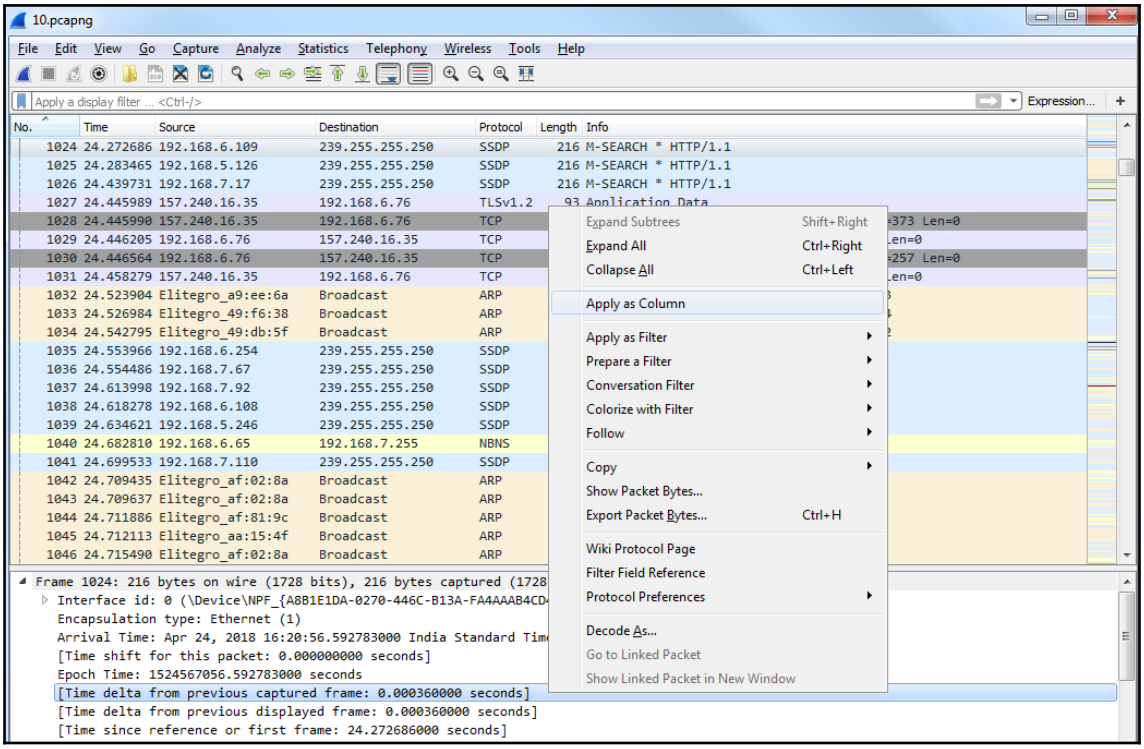

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14623 375.708841 192.168.0.11 239.255.255.250 SSDP 401 NOTIFY * HTTP/1.1
14624 375.727918 Elitegro_49:f0:c7 Broadcast ARP 60 Who has 192.168.7.105? Tell 192.168.5.225
14625 375.731192 192.168.7.215 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14626 375.732341 Elitegro_4f:2a:74 Broadcast ARP 60 Who has 192.168.5.225? Tell 192.168.7.105
14627 375.744793 192.168.7.11 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14628 375.744901 192.168.6.76 192.168.0.6 DNS 71 Standard query 0x847a A www.pbs.org
14629 375.763019 192.168.6.52 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14630 375.802125 192.168.6.76 216.58.220.174 TCP 55 [TCP Keep-Alive] 62444 → 443 [ACK] Seq=2293 Ack=6840 Win=65024 Len=1
14631 375.814066 192.168.0.6 192.168.6.76 DNS 109 Standard query response 0x847a A www.pbs.org CNAME r53-vip.pbs.org A 54.225...
14632 375.824935 Elitegro_af:b0:a9 Broadcast ARP 60 Who has 192.168.7.145? Tell 192.168.6.25
14633 375.842239 192.168.6.19 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
Frame 14631: 109 bytes on wire (872 bits), 109 bytes captured (872 bits) on interface 0
Ethernet II, Src: HewlettP_27:d8:8a (d8:94:03:27:d8:8a), Dst: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4, Src: 192.168.0.6, Dst: 192.168.6.76
User Datagram Protocol, Src Port: 53, Dst Port: 61022
Domain Name System (response)
[Request In: 14628]
[Time: 0.069165000 seconds]
Transaction ID: 0x847a
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
Queries
www.pbs.org: type A, class IN
Name: www.pbs.org
[Name Length: 11]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.pbs.org: type CNAME, class IN, cname r53-vip.pbs.org
r53-vip.pbs.org: type A, class IN, addr 54.225.198.196

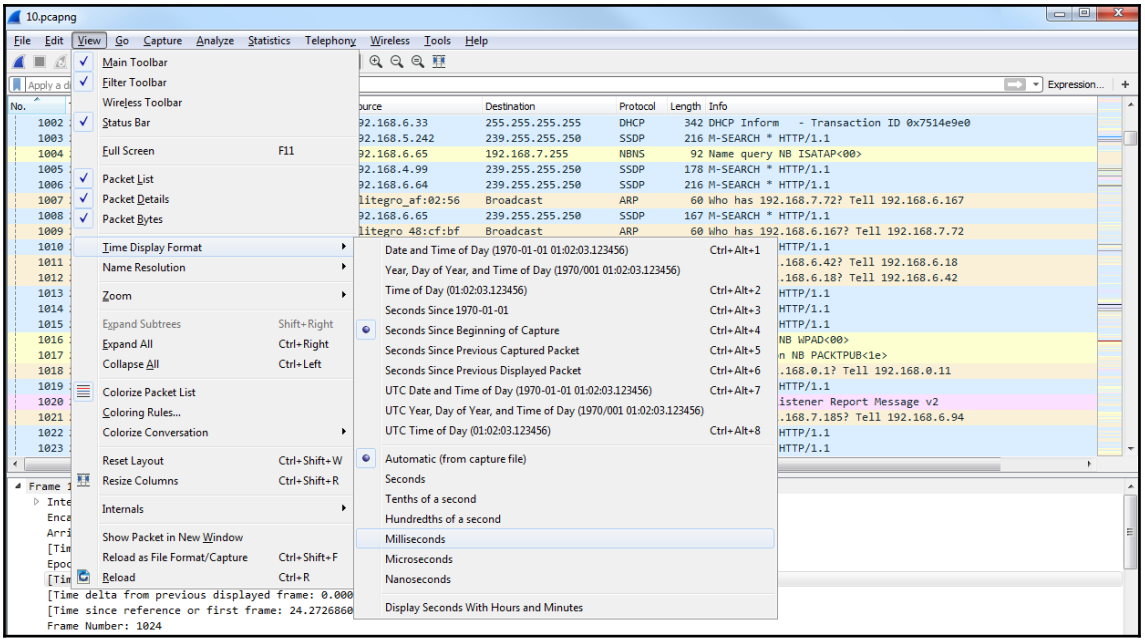

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14644 376.085981 192.168.5.172 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14645 376.092838 fe80::6075:d67d:6b0... ff02::1:ff15:cbc2 ICMPv6 86 Neighbor Solicitation for fe80::c634:6bff:fe15:cbc2 from f4:4d:30:05:35:d6
14646 376.095005 192.168.6.76 192.168.0.6 DNS 73 Standard query 0xb163 A image.pbs.org
14647 376.112624 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14648 376.118020 192.168.5.191 192.168.7.255 NBNS 92 Name query NB PACKTPUB<1b>
14649 376.149983 192.168.6.222 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14650 376.164071 192.168.0.6 192.168.6.76 DNS 141 Standard query response 0xb163 A image.pbs.org CNAME cds.v3q6w8c4.hwcdn.net A 205.185.216.10 A 20...
14651 376.166474 192.168.6.76 205.185.216.10 TCP 66 62454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14652 376.168597 SuperMic_88:92:0f Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11
14653 376.177781 192.168.5.225 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14654 376.243958 205.185.216.10 192.168.6.76 TCP 66 443 → 62454 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256

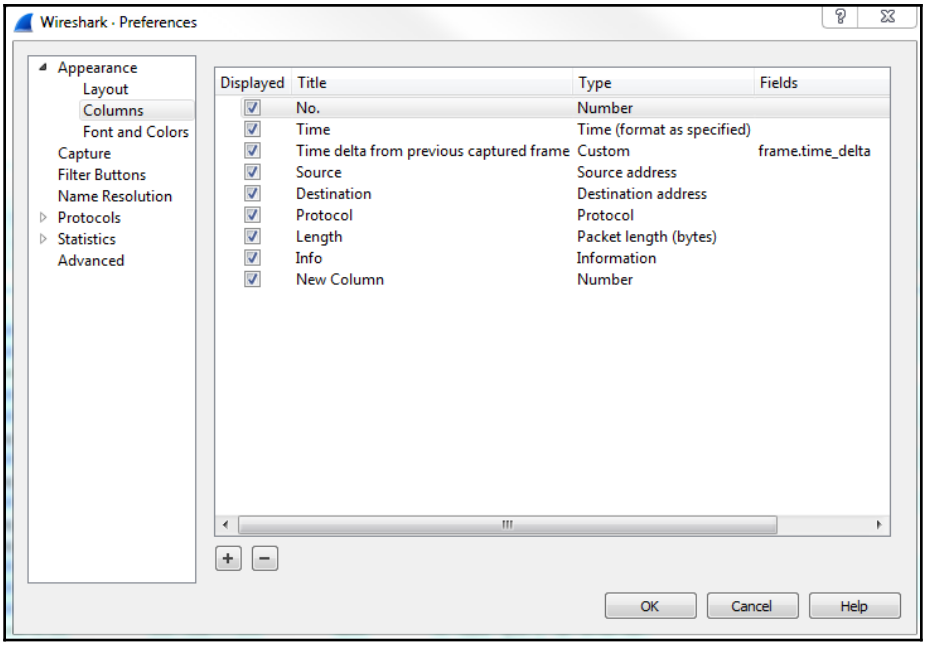

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
14645 376.092838 fe80::6075:d67d:6b0... ff02::1:ff15:cbc2 ICMPv6 86 Neighbor Solicitation for fe80::c634:6bff:fe15:cbc2 from f4:4d:30:05:35:d6
14646 376.095005 192.168.6.76 192.168.0.6 DNS 73 Standard query 0xb163 A image.pbs.org
14647 376.112624 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14648 376.118020 192.168.5.191 192.168.7.255 NBNS 92 Name query NB PACKTPUB<1b>
14649 376.149983 192.168.6.222 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14650 376.164071 192.168.0.6 192.168.6.76 DNS 141 Standard query response 0xb163 A image.pbs.org CNAME cds.v3q6w8c4.hwcdn.net A 205.185.216.10 A 205.185.216.42
14651 376.166474 192.168.6.76 205.185.216.10 TCP 66 62454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14652 376.168597 SuperMic_88:92:0f Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11
14653 376.177781 192.168.5.225 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1

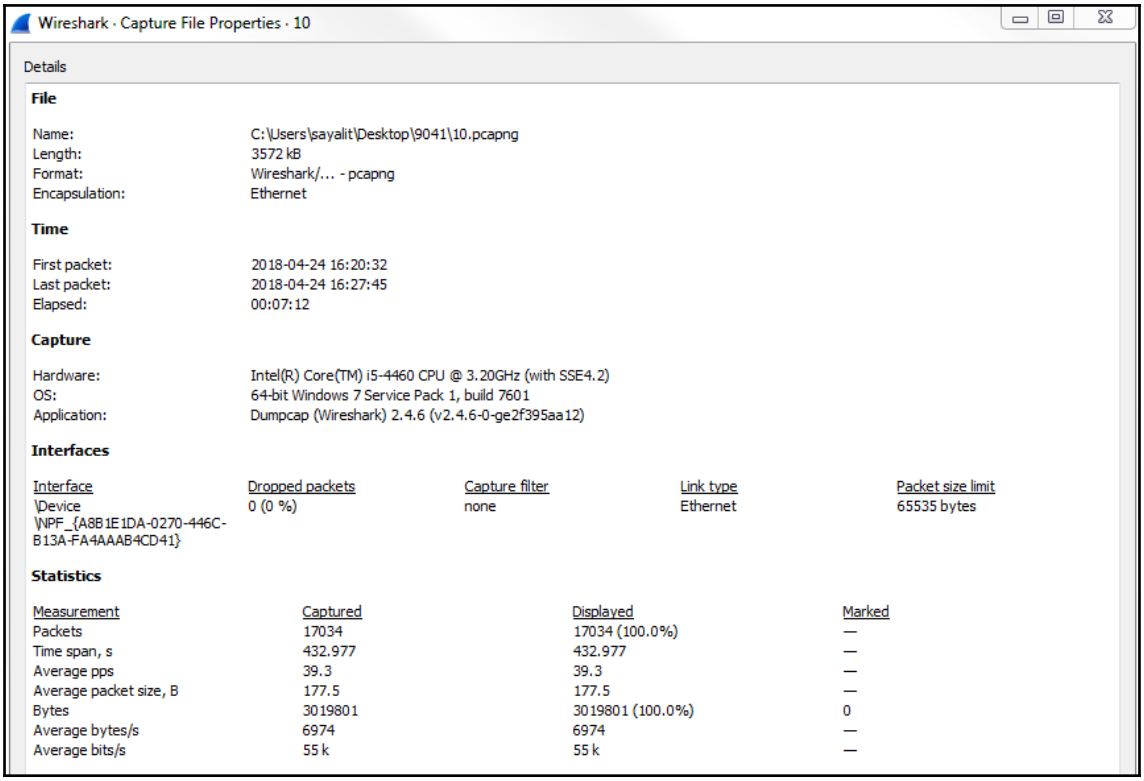

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
[TCP Segment Len: 255]
Sequence number: 1 (relative sequence number)
[Next sequence number: 256 (relative sequence number)]

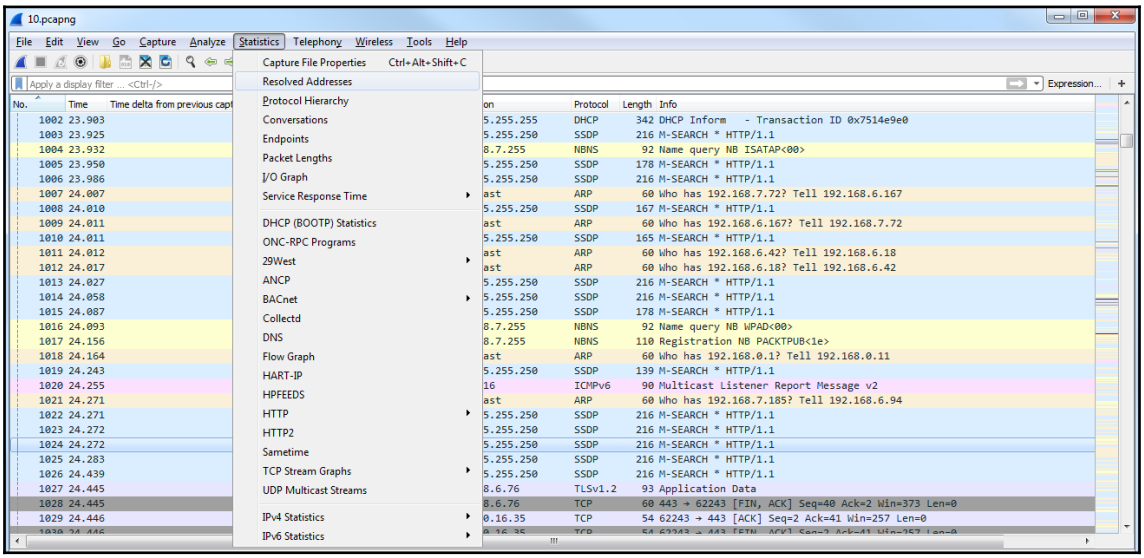

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
14645 0.006857 fe80::6075:d67d:6b0… ff02::1:ff15:cbc2 ICMPv6 86 Neighbor Solicitation for fe80::c634:6bff:fe15:cbc2 from f4:4d:30:05:35:d6
14646 0.002167 192.168.6.76 192.168.0.6 DNS 73 Standard query 0xb163 A image.pbs.org
14647 0.017619 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14648 0.005396 192.168.5.191 192.168.7.255 NBNS 92 Name query NB PACKTPUB<1b>
14649 0.031963 192.168.6.222 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14650 0.014088 192.168.0.6 192.168.6.76 DNS 141 Standard query response 0xb163 A image.pbs.org CNAME cds.v3q6w8c4.hwcdn.net A 205.185.216.10 A 205.185.216.42
14651 0.002403 192.168.6.76 205.185.216.10 TCP 66 62454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14652 0.002123 SuperMic_88:92:0f Broadcast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11
14653 0.009184 192.168.5.225 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14654 0.066177 205.185.216.10 192.168.6.76 TCP 66 443 → 62454 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
14655 0.000104 192.168.6.76 205.185.216.10 TCP 54 62454 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
14656 0.000420 192.168.6.76 205.185.216.10 TLSv1.2 571 Client Hello
14657 0.030311 192.168.6.34 239.255.255.250 SSDP 179 M-SEARCH * HTTP/1.1
14658 0.020433 Elitegro_0f:58:1d Broadcast ARP 60 Who has 192.168.6.147? Tell 192.168.6.223
14659 0.001900 Elitegro_49:d5:df Broadcast ARP 60 Who has 192.168.6.223? Tell 192.168.6.147
14660 0.021815 205.185.216.10 192.168.6.76 TCP 60 443 → 62454 [ACK] Seq=1 Ack=518 Win=15872 Len=0
14661 0.019467 151.101.2.110 192.168.6.76 TLSv1.2 112 Application Data
14662 0.000000 151.101.2.110 192.168.6.76 TLSv1.2 85 Encrypted Alert
14663 0.000001 151.101.2.110 192.168.6.76 TCP 60 443 → 62255 [FIN, ACK] Seq=90 Ack=2 Win=61 Len=0
14664 0.000109 192.168.6.76 151.101.2.110 TCP 54 62255 → 443 [ACK] Seq=2 Ack=91 Win=258 Len=0
14665 0.000125 192.168.6.76 151.101.2.110 TCP 54 62255 → 443 [FIN, ACK] Seq=2 Ack=91 Win=258 Len=0
14666 0.004264 192.168.6.43 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x2375c39a
14667 0.013090 151.101.2.110 192.168.6.76 TCP 60 443 → 62255 [ACK] Seq=91 Ack=3 Win=61 Len=0

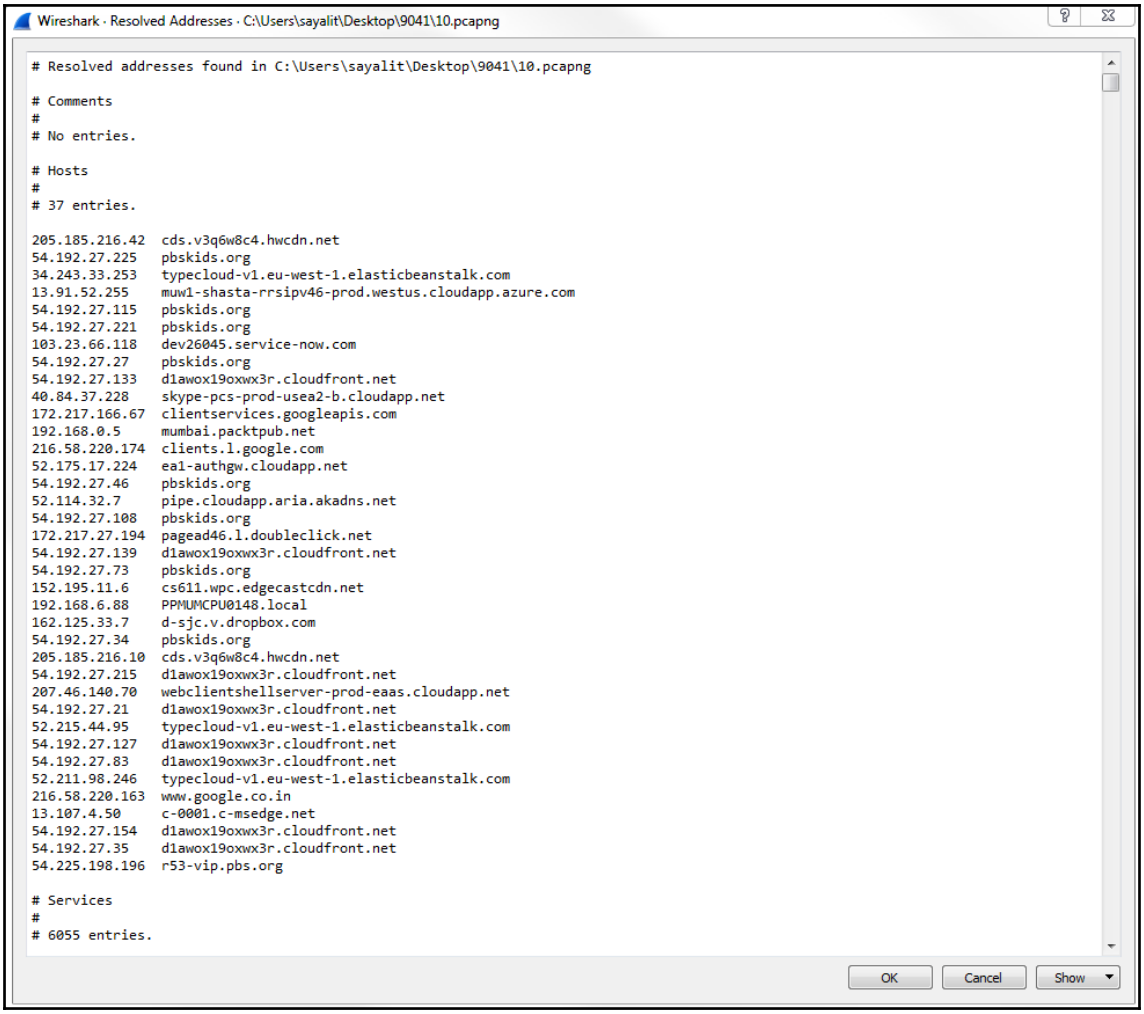

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1024 24.272686 192.168.6.109 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1025 24.283465 192.168.5.126 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1026 24.439731 192.168.7.17 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1027 24.445989 157.240.16.35 192.168.6.76 TLSv1.2 93 Application Data
1028 24.445990 157.240.16.35 192.168.6.76 TCP
1029 24.446205 192.168.6.76 157.240.16.35 TCP
1030 24.446564 192.168.6.76 157.240.16.35 TCP
1031 24.458279 157.240.16.35 192.168.6.76 TCP
1032 24.523904 Elitegro_a9:ee:6a Broadcast ARP
1033 24.526984 Elitegro_49:f6:38 Broadcast ARP
1034 24.542795 Elitegro_49:db:5f Broadcast ARP
1035 24.553966 192.168.6.254 239.255.255.250 SSDP
1036 24.554486 192.168.7.67 239.255.255.250 SSDP
1037 24.613998 192.168.7.92 239.255.255.250 SSDP
1038 24.618278 192.168.6.108 239.255.255.250 SSDP
1039 24.634621 192.168.5.246 239.255.255.250 SSDP
1040 24.682810 192.168.6.65 192.168.7.255 NBNS
1041 24.699533 192.168.7.110 239.255.255.250 SSDP
1042 24.709435 Elitegro_af:02:8a Broadcast ARP
1043 24.709637 Elitegro_af:02:8a Broadcast ARP
1044 24.711886 Elitegro_af:81:9c Broadcast ARP
1045 24.712113 Elitegro_aa:15:4f Broadcast ARP
1046 24.715490 Elitegro_af:02:8a Broadcast ARP
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Frame 1024: 216 bytes on wire (1728 bits), 216 bytes captured (1728
Interface id: 0 (\Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD
Encapsulation type: Ethernet (1)
Arrival Time: Apr 24, 2018 16:20:56.592783000 India Standard Tim
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1524567056.592783000 seconds
[Time delta from previous captured frame: 0.000360000 seconds]
[Time delta from previous displayed frame: 0.000360000 seconds]
[Time since reference or first frame: 24.272686000 seconds]

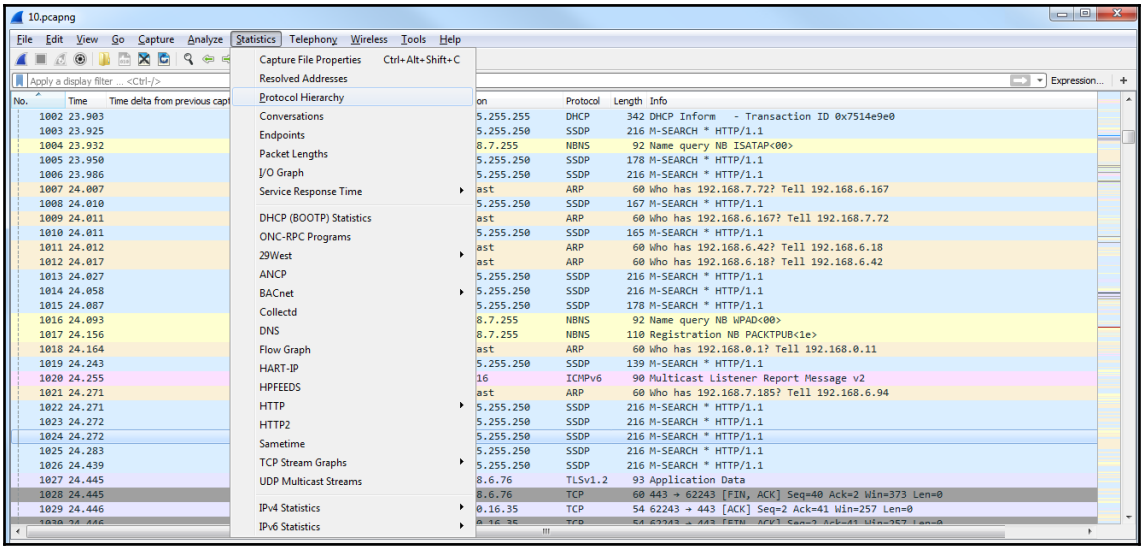

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Full Screen F11
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout Ctrl+Shift+W
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload as File Format/Capture Ctrl+Shift+F
Reload Ctrl+R
Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) Ctrl+Alt+2
Seconds Since 1970-01-01 Ctrl+Alt+3
Seconds Since Beginning of Capture Ctrl+Alt+4
Seconds Since Previous Captured Packet Ctrl+Alt+5
Seconds Since Previous Displayed Packet Ctrl+Alt+6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) Ctrl+Alt+7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) Ctrl+Alt+8
Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Microseconds
Nanoseconds
Display Seconds With Hours and Minutes
Destination Protocol Length Info
192.168.6.33 255.255.255.255 DHCP 342 DHCP Inform - Transaction ID 0x7514e9e0
192.168.5.242 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
192.168.6.65 192.168.7.255 NBNS 92 Name query NB ISATAP<00>
192.168.4.99 239.255.255.250 SSDP 178 M-SEARCH * HTTP/1.1
192.168.6.64 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
litegro_af:02:56 Broadcast ARP 60 Who has 192.168.7.72? Tell 192.168.6.167
192.168.6.65 239.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
litegro 48:cf:bf Broadcast ARP 60 Who has 192.168.6.167? Tell 192.168.7.72
[Time delta from previous displayed frame: 0.000
[Time since reference or first frame: 24.2726860
Frame Number: 1024

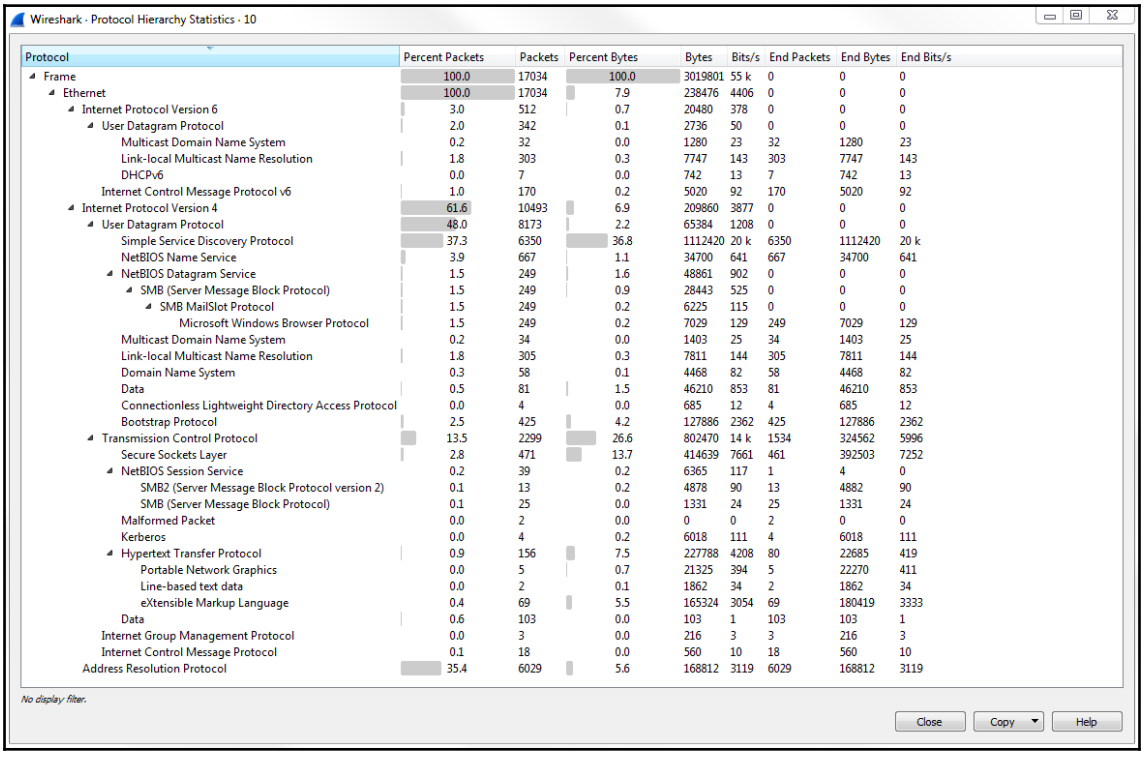

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Buttons
Name Resolution
Protocols
Statistics
Advanced
Displayed Title Type Fields
No. Number
Time Time (format as specified)
Time delta from previous captured frame Custom frame.time_delta
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
New Column Number
OK Cancel Help

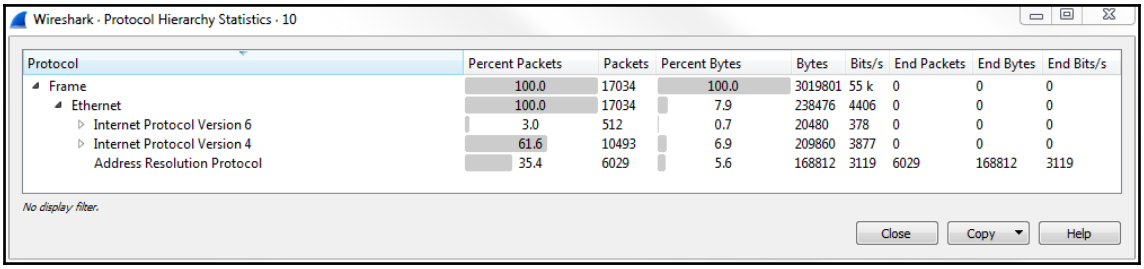

Wireshark · Capture File Properties · 10
Details
File
Name: C:\Users\sayalit\Desktop\9041\10.pcapng
Length: 3572 kB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Time
First packet: 2018-04-24 16:20:32
Last packet: 2018-04-24 16:27:45
Elapsed: 00:07:12
Capture
Hardware: Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz (with SSE4.2)
OS: 64-bit Windows 7 Service Pack 1, build 7601
Application: Dumpcap (Wireshark) 2.4.6 (v2.4.6-0-ge2f395aa12)
Interfaces
Interface Dropped packets Capture filter Link type Packet size limit
\Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41} 0 (0 %) none Ethernet 65535 bytes
Statistics
Measurement Captured Displayed Marked
Packets 17034 17034 (100.0%) —
Time span, s 432.977 432.977 —
Average pps 39.3 39.3 —
Average packet size, B 177.5 177.5 —
Bytes 3019801 3019801 (100.0%) 0
Average bytes/s 6974 6974 —
Average bits/s 55 k 55 k —

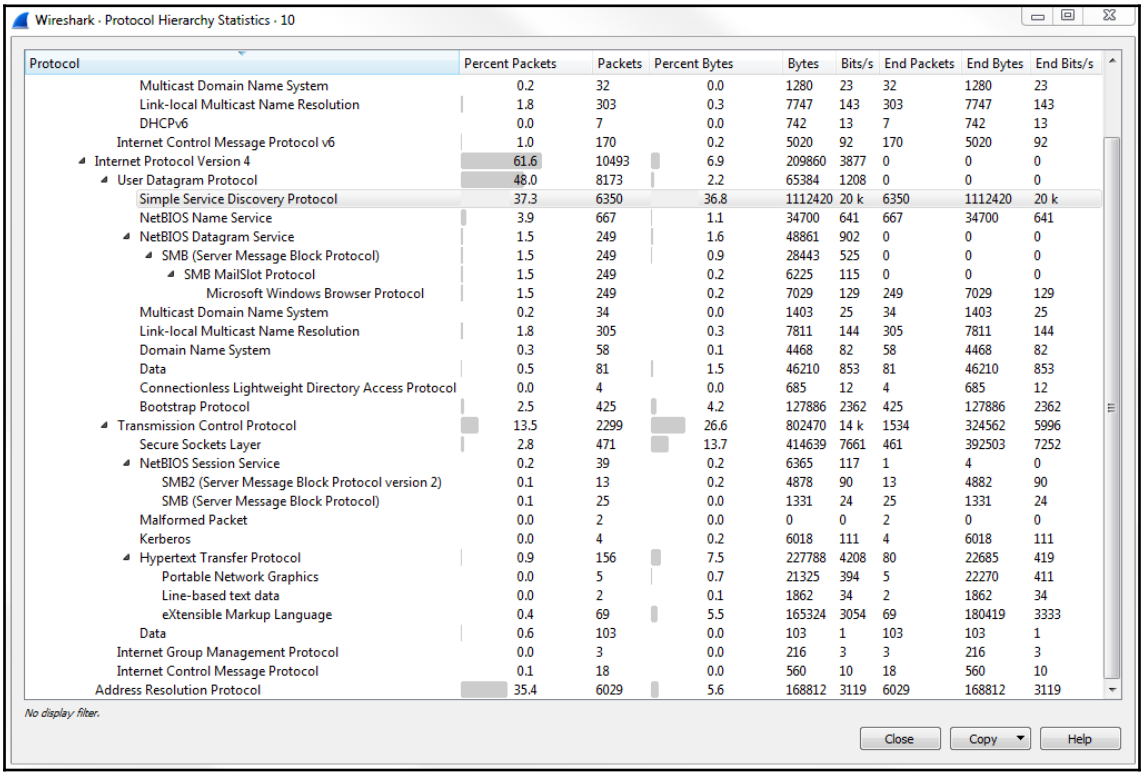

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics

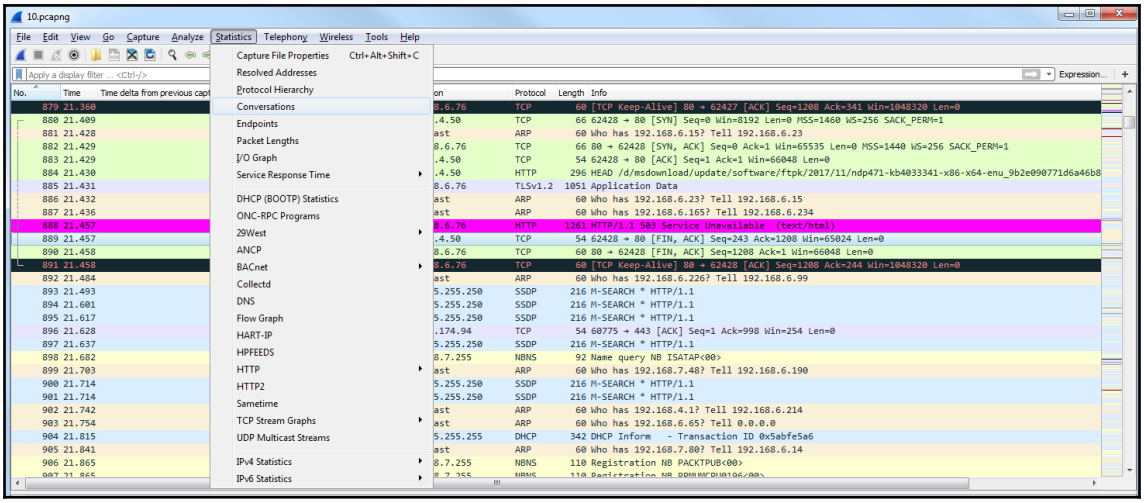

Wireshark · Resolved Addresses · C:\Users\sayalit\Desktop\9041\10.pcapng
Resolved addresses found in C:\Users\sayalit\Desktop\9041\10.pcapng
Comments
#
No entries.
Hosts
#
37 entries.
205.185.216.42 cds.v3q6w8c4.hwcdn.net
54.192.27.225 pbskids.org
34.243.33.253 typecloud-v1.eu-west-1.elasticbeanstalk.com
13.91.52.255 muw1-shasta-rrsipv46-prod.westus.cloudapp.azure.com
54.192.27.115 pbskids.org
54.192.27.221 pbskids.org
103.23.66.118 dev26045.service-now.com
54.192.27.27 pbskids.org
54.192.27.133 d1awox19oxwx3r.cloudfront.net
40.84.37.228 skype-pcs-prod-usea2-b.cloudapp.net
172.217.166.67 clientservices.googleapis.com
192.168.0.5 mumbai.packtpub.net
216.58.220.174 clients.l.google.com
52.175.17.224 ea1-authgw.cloudapp.net
54.192.27.46 pbskids.org
52.114.32.7 pipe.cloudapp.aria.akadns.net
54.192.27.108 pbskids.org
172.217.27.194 pagead46.l.doubleclick.net
54.192.27.139 d1awox19oxwx3r.cloudfront.net
54.192.27.73 pbskids.org
152.195.11.6 cs611.wpc.edgecastcdn.net
192.168.6.88 PPMUMCPU0148.local
162.125.33.7 d-sjc.v.dropbox.com
54.192.27.34 pbskids.org
205.185.216.10 cds.v3q6w8c4.hwcdn.net
54.192.27.215 d1awox19oxwx3r.cloudfront.net
207.46.140.70 webclientshellserver-prod-eaas.cloudapp.net
54.192.27.21 d1awox19oxwx3r.cloudfront.net
52.215.44.95 typecloud-v1.eu-west-1.elasticbeanstalk.com
54.192.27.127 d1awox19oxwx3r.cloudfront.net
54.192.27.83 d1awox19oxwx3r.cloudfront.net
52.211.98.246 typecloud-v1.eu-west-1.elasticbeanstalk.com
216.58.220.163 www.google.co.in
13.107.4.50 c-0001.c-msedge.net
54.192.27.154 d1awox19oxwx3r.cloudfront.net
54.192.27.35 d1awox19oxwx3r.cloudfront.net
54.225.198.196 r53-vip.pbs.org
Services
#
6055 entries.
OK
Cancel
Show

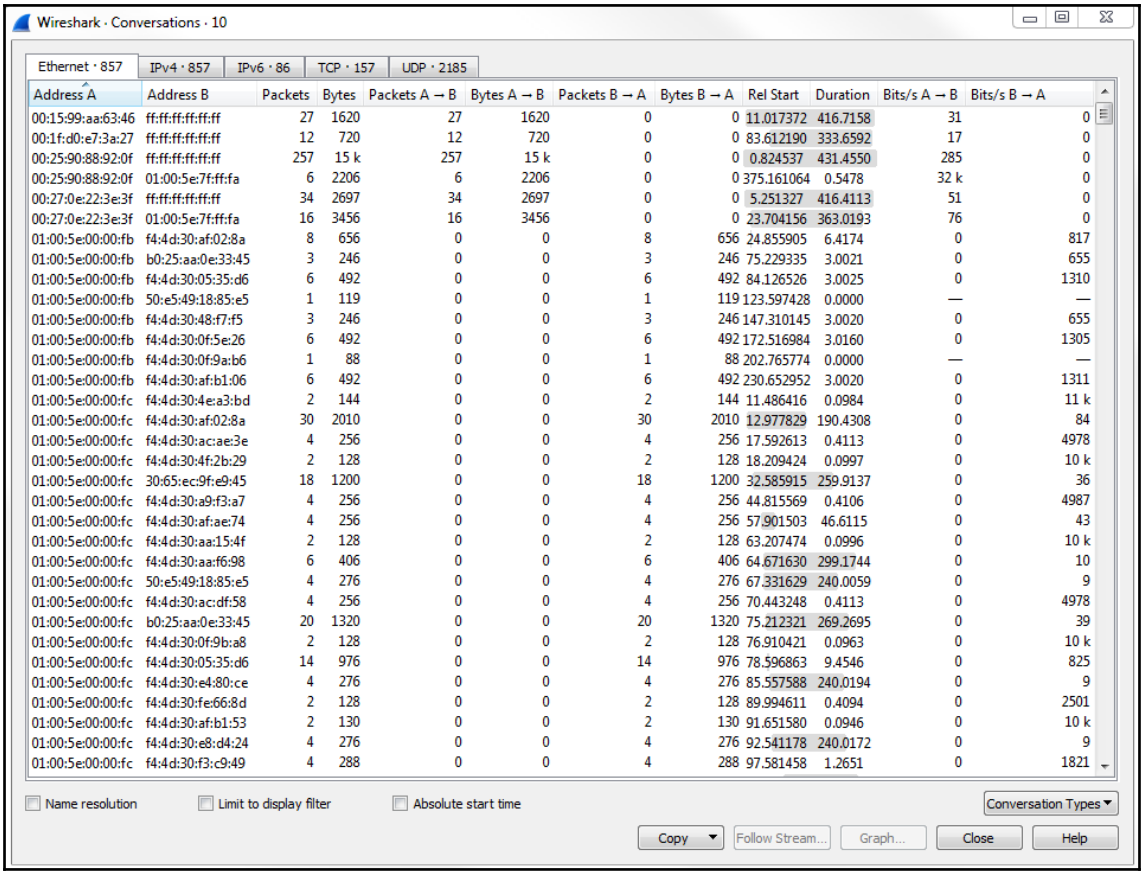

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous capt on Protocol Length Info
1002 23.903 5.255.255 DHCP 342 DHCP Inform - Transaction ID 0x7514e9e0
1003 23.925 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1004 23.932 8.7.255 NBNS 92 Name query NB ISATAP<00>
1005 23.950 5.255.250 SSDP 178 M-SEARCH * HTTP/1.1
1006 23.986 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1007 24.007 ast ARP 60 Who has 192.168.7.72? Tell 192.168.6.167
1008 24.010 5.255.250 SSDP 167 M-SEARCH * HTTP/1.1
1009 24.011 ast ARP 60 Who has 192.168.6.167? Tell 192.168.7.72
1010 24.011 5.255.250 SSDP 165 M-SEARCH * HTTP/1.1
1011 24.012 ast ARP 60 Who has 192.168.6.42? Tell 192.168.6.18
1012 24.017 ast ARP 60 Who has 192.168.6.18? Tell 192.168.6.42
1013 24.027 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1014 24.058 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1015 24.087 5.255.250 SSDP 178 M-SEARCH * HTTP/1.1
1016 24.093 8.7.255 NBNS 92 Name query NB WPAD<00>
1017 24.156 8.7.255 NBNS 110 Registration NB PACKTPUB<1e>
1018 24.164 ast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11
1019 24.243 5.255.250 SSDP 139 M-SEARCH * HTTP/1.1
1020 24.255 16 ICMPv6 90 Multicast Listener Report Message v2
1021 24.271 ast ARP 60 Who has 192.168.7.185? Tell 192.168.6.94
1022 24.271 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1023 24.272 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1024 24.272 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1025 24.283 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1026 24.439 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
1027 24.445 8.6.76 TLSv1.2 93 Application Data
1028 24.445 8.6.76 TCP 60 443 → 62243 [FIN, ACK] Seq=40 Ack=2 Win=373 Len=0
1029 24.446 0.16.35 TCP 54 62243 → 443 [ACK] Seq=2 Ack=41 Win=257 Len=0

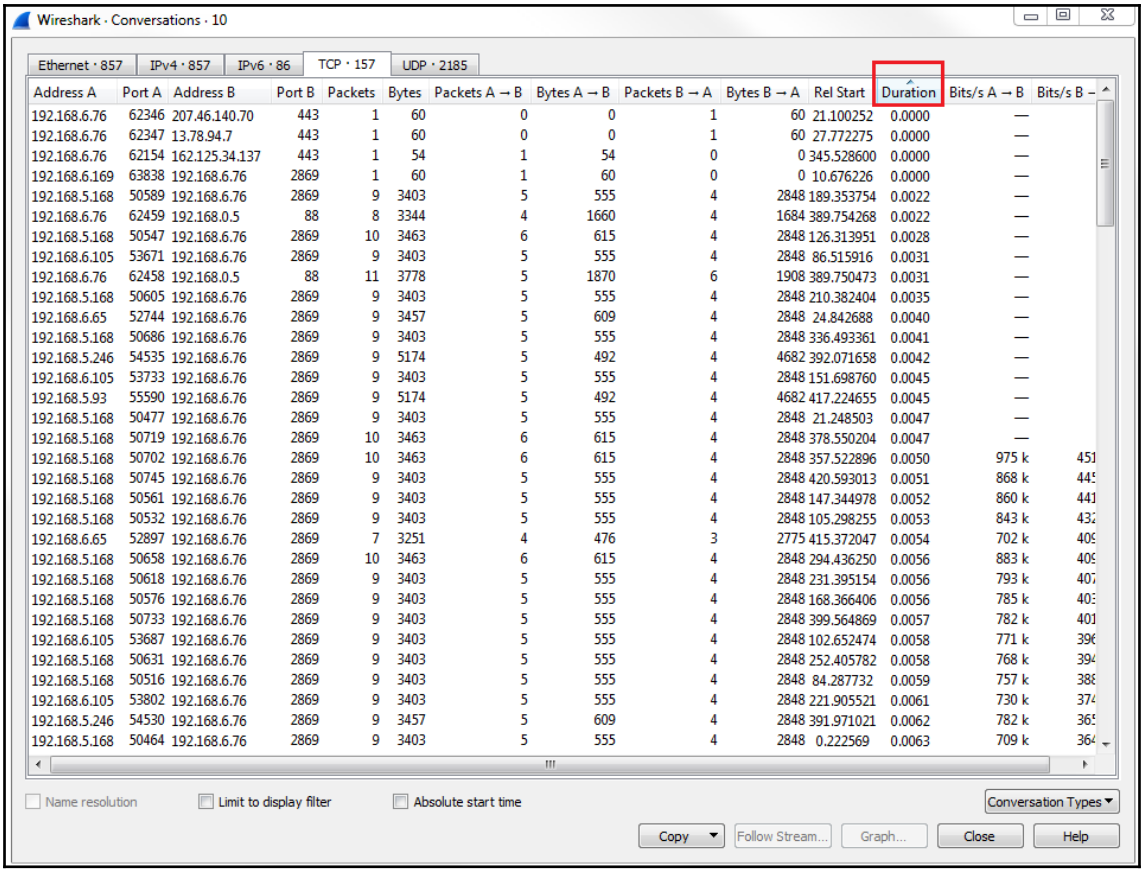

Wireshark · Protocol Hierarchy Statistics · 10
Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets End Bytes End Bits/s
Frame 100.0 17034 100.0 3019801 55 k 0 0 0
Ethernet 100.0 17034 7.9 238476 4406 0 0 0
Internet Protocol Version 6 3.0 512 0.7 20480 378 0 0 0
User Datagram Protocol 2.0 342 0.1 2736 50 0 0 0
Multicast Domain Name System 0.2 32 0.0 1280 23 32 1280 23
Link-local Multicast Name Resolution 1.8 303 0.3 7747 143 303 7747 143
DHCPv6 0.0 7 0.0 742 13 7 742 13
Internet Control Message Protocol v6 1.0 170 0.2 5020 92 170 5020 92
Internet Protocol Version 4 61.6 10493 6.9 209860 3877 0 0 0
User Datagram Protocol 48.0 8173 2.2 65384 1208 0 0 0
Simple Service Discovery Protocol 37.3 6350 36.8 1112420 20 k 6350 1112420 20 k
NetBIOS Name Service 3.9 667 1.1 34700 641 667 34700 641
NetBIOS Datagram Service 1.5 249 1.6 48861 902 0 0 0
SMB (Server Message Block Protocol) 1.5 249 0.9 28443 525 0 0 0
SMB MailSlot Protocol 1.5 249 0.2 6225 115 0 0 0
Microsoft Windows Browser Protocol 1.5 249 0.2 7029 129 249 7029 129
Multicast Domain Name System 0.2 34 0.0 1403 25 34 1403 25
Link-local Multicast Name Resolution 1.8 305 0.3 7811 144 305 7811 144
Domain Name System 0.3 58 0.1 4468 82 58 4468 82
Data 0.5 81 1.5 46210 853 81 46210 853
Connectionless Lightweight Directory Access Protocol 0.0 4 0.0 685 12 4 685 12
Bootstrap Protocol 2.5 425 4.2 127886 2362 425 127886 2362
Transmission Control Protocol 13.5 2299 26.6 802470 14 k 1534 324562 5996
Secure Sockets Layer 2.8 471 13.7 414639 7661 461 392503 7252
NetBIOS Session Service 0.2 39 0.2 6365 117 1 4 0
SMB2 (Server Message Block Protocol version 2) 0.1 13 0.2 4878 90 13 4882 90
SMB (Server Message Block Protocol) 0.1 25 0.0 1331 24 25 1331 24
Malformed Packet 0.0 2 0.0 0 0 2 0 0
Kerberos 0.0 4 0.2 6018 111 4 6018 111
Hypertext Transfer Protocol 0.9 156 7.5 227788 4208 80 22685 419
Portable Network Graphics 0.0 5 0.7 21325 394 5 22270 411
Line-based text data 0.0 2 0.1 1862 34 2 1862 34
eXtensible Markup Language 0.4 69 5.5 165324 3054 69 180419 3333
Data 0.6 103 0.0 103 1 103 103 1
Internet Group Management Protocol 0.0 3 0.0 216 3 3 216 3
Internet Control Message Protocol 0.1 18 0.0 560 10 18 560 10
Address Resolution Protocol 35.4 6029 5.6 168812 3119 6029 168812 3119
No display filter.
Close
Copy
Help


Wireshark · Protocol Hierarchy Statistics · 10
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
Frame 100.0 17034 100.0 3019801 55 k 0 0 0
Ethernet 100.0 17034 7.9 238476 4406 0 0 0
Internet Protocol Version 6 3.0 512 0.7 20480 378 0 0 0
Internet Protocol Version 4 61.6 10493 6.9 209860 3877 0 0 0
Address Resolution Protocol 35.4 6029 5.6 168812 3119 6029 168812 3119
No display filter.
Close
Copy
Help

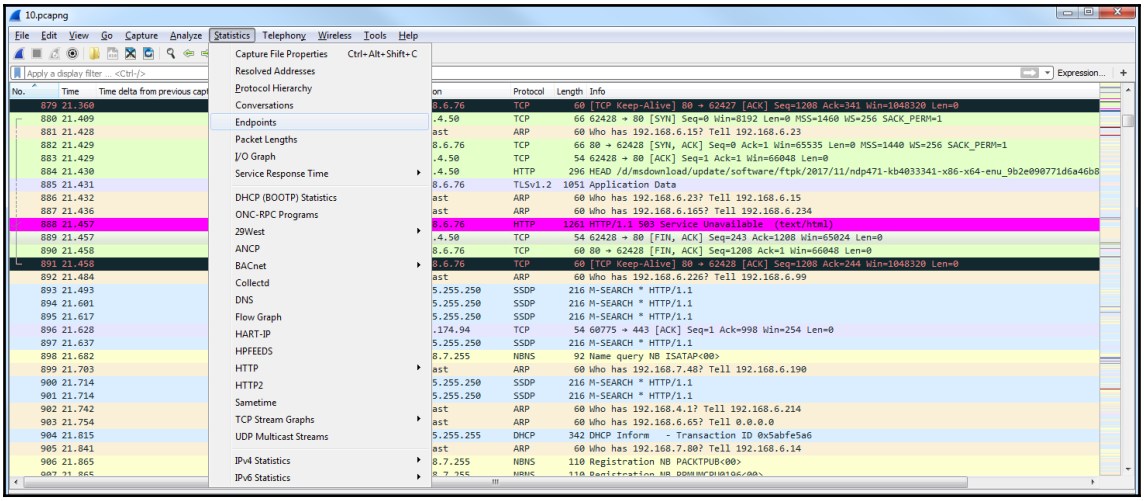

Wireshark · Protocol Hierarchy Statistics · 10
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
Multicast Domain Name System 0.2 32 0.0 1280 23 32 1280 23
Link-local Multicast Name Resolution 1.8 303 0.3 7747 143 303 7747 143
DHCPv6 0.0 7 0.0 742 13 7 742 13
Internet Control Message Protocol v6 1.0 170 0.2 5020 92 170 5020 92
Internet Protocol Version 4 61.6 10493 6.9 209860 3877 0 0 0
User Datagram Protocol 48.0 8173 2.2 65384 1208 0 0 0
Simple Service Discovery Protocol 37.3 6350 36.8 1112420 20 k 6350 1112420 20 k
NetBIOS Name Service 3.9 667 1.1 34700 641 667 34700 641
NetBIOS Datagram Service 1.5 249 1.6 48861 902 0 0 0
SMB (Server Message Block Protocol) 1.5 249 0.9 28443 525 0 0 0
SMB MailSlot Protocol 1.5 249 0.2 6225 115 0 0 0
Microsoft Windows Browser Protocol 1.5 249 0.2 7029 129 249 7029 129
Multicast Domain Name System 0.2 34 0.0 1403 25 34 1403 25
Link-local Multicast Name Resolution 1.8 305 0.3 7811 144 305 7811 144
Domain Name System 0.3 58 0.1 4468 82 58 4468 82
Data 0.5 81 1.5 46210 853 81 46210 853
Connectionless Lightweight Directory Access Protocol 0.0 4 0.0 685 12 4 685 12
Bootstrap Protocol 2.5 425 4.2 127886 2362 425 127886 2362
Transmission Control Protocol 13.5 2299 26.6 802470 14 k 1534 324562 5996
Secure Sockets Layer 2.8 471 13.7 414639 7661 461 392503 7252
NetBIOS Session Service 0.2 39 0.2 6365 117 1 4 0
SMB2 (Server Message Block Protocol version 2) 0.1 13 0.2 4878 90 13 4882 90
SMB (Server Message Block Protocol) 0.1 25 0.0 1331 24 25 1331 24
Malformed Packet 0.0 2 0.0 0 0 2 0 0
Kerberos 0.0 4 0.2 6018 111 4 6018 111
Hypertext Transfer Protocol 0.9 156 7.5 227788 4208 80 22685 419
Portable Network Graphics 0.0 5 0.7 21325 394 5 22270 411
Line-based text data 0.0 2 0.1 1862 34 2 1862 34
eXtensible Markup Language 0.4 69 5.5 165324 3054 69 180419 3333
Data 0.6 103 0.0 103 1 103 103 1
Internet Group Management Protocol 0.0 3 0.0 216 3 3 216 3
Internet Control Message Protocol 0.1 18 0.0 560 10 18 560 10
Address Resolution Protocol 35.4 6029 5.6 168812 3119 6029 168812 3119
No display filter.
Close
Copy
Help

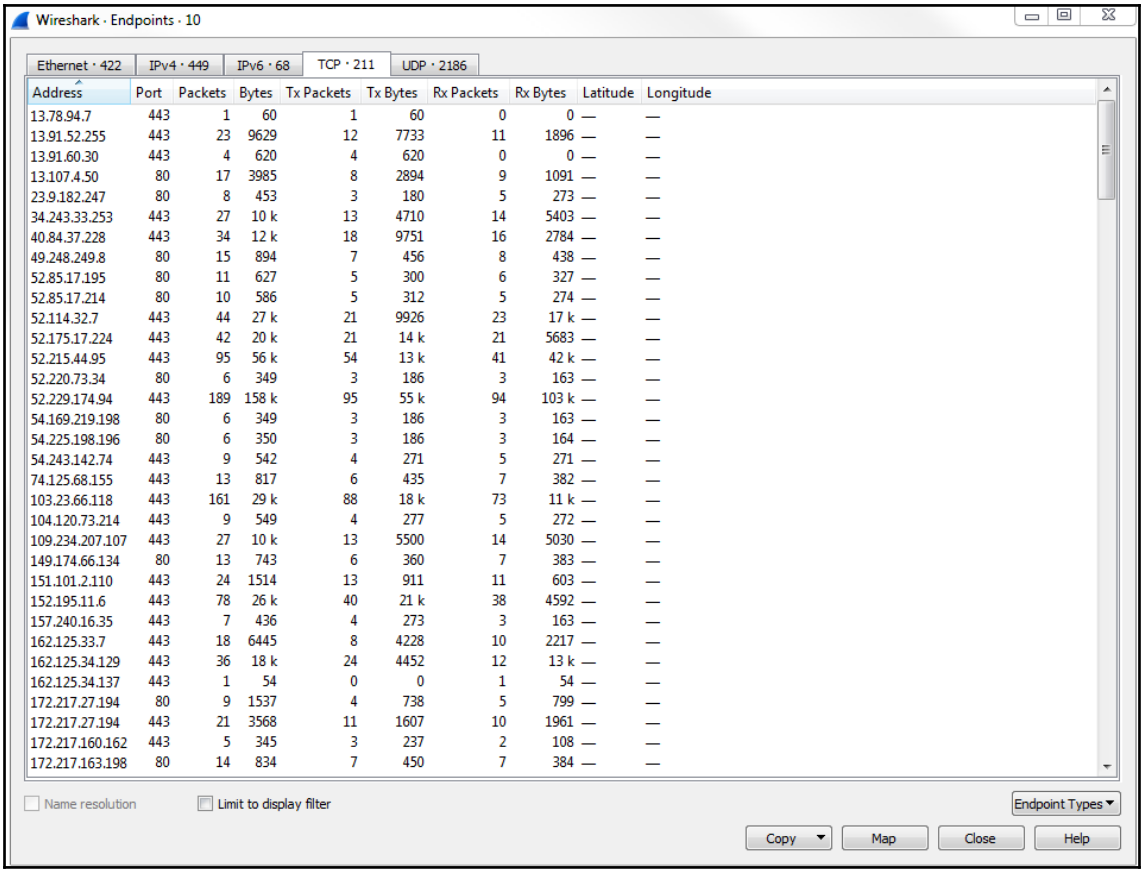

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous capt on Protocol Length Info
879 21.360 8.6.76 TCP 60 [TCP Keep-Alive] 80 → 62427 [ACK] Seq=1208 Ack=341 Win=1048320 Len=0
880 21.409 .4.50 TCP 66 62428 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
881 21.428 ast ARP 60 Who has 192.168.6.15? Tell 192.168.6.23
882 21.429 8.6.76 TCP 66 80 → 62428 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
883 21.429 .4.50 TCP 54 62428 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
884 21.430 .4.50 HTTP 296 HEAD /d/msdownload/update/software/ftpk/2017/11/ndp471-kb4033341-x86-x64-enu_9b2e090771d6a46b8
885 21.431 8.6.76 TLSv1.2 1051 Application Data
886 21.432 ast ARP 60 Who has 192.168.6.23? Tell 192.168.6.15
887 21.436 ast ARP 60 Who has 192.168.6.165? Tell 192.168.6.234
888 21.457 8.6.76 HTTP 1261 HTTP/1.1 503 Service Unavailable (text/html)
889 21.457 .4.50 TCP 54 62428 → 80 [FIN, ACK] Seq=243 Ack=1208 Win=65024 Len=0
890 21.458 8.6.76 TCP 60 80 → 62428 [FIN, ACK] Seq=1208 Ack=1 Win=66048 Len=0
891 21.458 8.6.76 TCP 60 [TCP Keep-Alive] 80 → 62428 [ACK] Seq=1208 Ack=244 Win=1048320 Len=0
892 21.484 ast ARP 60 Who has 192.168.6.226? Tell 192.168.6.99
893 21.493 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
894 21.601 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
895 21.617 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
896 21.628 .174.94 TCP 54 60775 → 443 [ACK] Seq=1 Ack=998 Win=254 Len=0
897 21.637 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
898 21.682 8.7.255 NBNS 92 Name query NB ISATAP<00>
899 21.703 ast ARP 60 Who has 192.168.7.48? Tell 192.168.6.190
900 21.714 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
901 21.714 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
902 21.742 ast ARP 60 Who has 192.168.4.1? Tell 192.168.6.214
903 21.754 ast ARP 60 Who has 192.168.6.65? Tell 0.0.0.0
904 21.815 5.255.255 DHCP 342 DHCP Inform - Transaction ID 0x5abfe5a6
905 21.841 ast ARP 60 Who has 192.168.7.80? Tell 192.168.6.14
906 21.865 8.7.255 NBNS 110 Registration NB PACKTPUB<00>


Wireshark · Conversations · 10
Ethernet · 857
IPv4 · 857
IPv6 · 86
TCP · 157
UDP · 2185
Address A
Address B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
00:15:99:aa:63:46 ff:ff:ff:ff:ff:ff 27 1620 27 1620 0 0 11.017372 416.7158 31 0
00:1f:d0:e7:3a:27 ff:ff:ff:ff:ff:ff 12 720 12 720 0 0 83.612190 333.6592 17 0
00:25:90:88:92:0f ff:ff:ff:ff:ff:ff 257 15 k 257 15 k 0 0 0.824537 431.4550 285 0
00:25:90:88:92:0f 01:00:5e:7f:ff:fa 6 2206 6 2206 0 0 375.161064 0.5478 32 k 0
00:27:0e:22:3e:3f ff:ff:ff:ff:ff:ff 34 2697 34 2697 0 0 5.251327 416.4113 51 0
00:27:0e:22:3e:3f 01:00:5e:7f:ff:fa 16 3456 16 3456 0 0 23.704156 363.0193 76 0
01:00:5e:00:00:fb f4:4d:30:af:02:8a 8 656 0 0 8 656 24.855905 6.4174 0 817
01:00:5e:00:00:fb b0:25:aa:0e:33:45 3 246 0 0 3 246 75.229335 3.0021 0 655
01:00:5e:00:00:fb f4:4d:30:05:35:d6 6 492 0 0 6 492 84.126526 3.0025 0 1310
01:00:5e:00:00:fb 50:e5:49:18:85:e5 1 119 0 0 1 119 123.597428 0.0000 — —
01:00:5e:00:00:fb f4:4d:30:48:f7:f5 3 246 0 0 3 246 147.310145 3.0020 0 655
01:00:5e:00:00:fb f4:4d:30:0f:5e:26 6 492 0 0 6 492 172.516984 3.0160 0 1305
01:00:5e:00:00:fb f4:4d:30:0f:9a:b6 1 88 0 0 1 88 202.765774 0.0000 — —
01:00:5e:00:00:fb f4:4d:30:af:b1:06 6 492 0 0 6 492 230.652952 3.0020 0 1311
01:00:5e:00:00:fc f4:4d:30:4e:a3:bd 2 144 0 0 2 144 11.486416 0.0984 0 11 k
01:00:5e:00:00:fc f4:4d:30:af:02:8a 30 2010 0 0 30 2010 12.977829 190.4308 0 84
01:00:5e:00:00:fc f4:4d:30:ac:ae:3e 4 256 0 0 4 256 17.592613 0.4113 0 4978
01:00:5e:00:00:fc f4:4d:30:4f:2b:29 2 128 0 0 2 128 18.209424 0.0997 0 10 k
01:00:5e:00:00:fc 30:65:ec:9f:e9:45 18 1200 0 0 18 1200 32.585915 259.9137 0 36
01:00:5e:00:00:fc f4:4d:30:a9:f3:a7 4 256 0 0 4 256 44.815569 0.4106 0 4987
01:00:5e:00:00:fc f4:4d:30:af:ae:74 4 256 0 0 4 256 57.901503 46.6115 0 43
01:00:5e:00:00:fc f4:4d:30:aa:15:4f 2 128 0 0 2 128 63.207474 0.0996 0 10 k
01:00:5e:00:00:fc f4:4d:30:aa:f6:98 6 406 0 0 6 406 64.671630 299.1744 0 10
01:00:5e:00:00:fc 50:e5:49:18:85:e5 4 276 0 0 4 276 67.331629 240.0059 0 9
01:00:5e:00:00:fc f4:4d:30:ac:df:58 4 256 0 0 4 256 70.443248 0.4113 0 4978
01:00:5e:00:00:fc b0:25:aa:0e:33:45 20 1320 0 0 20 1320 75.212321 269.2695 0 39
01:00:5e:00:00:fc f4:4d:30:0f:9b:a8 2 128 0 0 2 128 76.910421 0.0963 0 10 k
01:00:5e:00:00:fc f4:4d:30:05:35:d6 14 976 0 0 14 976 78.596863 9.4546 0 825
01:00:5e:00:00:fc f4:4d:30:e4:80:ce 4 276 0 0 4 276 85.557588 240.0194 0 9
01:00:5e:00:00:fc f4:4d:30:fe:66:8d 2 128 0 0 2 128 89.994611 0.4094 0 2501
01:00:5e:00:00:fc f4:4d:30:af:b1:53 2 130 0 0 2 130 91.651580 0.0946 0 10 k
01:00:5e:00:00:fc f4:4d:30:e8:d4:24 4 276 0 0 4 276 92.541178 240.0172 0 9
01:00:5e:00:00:fc f4:4d:30:f3:c9:49 4 288 0 0 4 288 97.581458 1.2651 0 1821
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

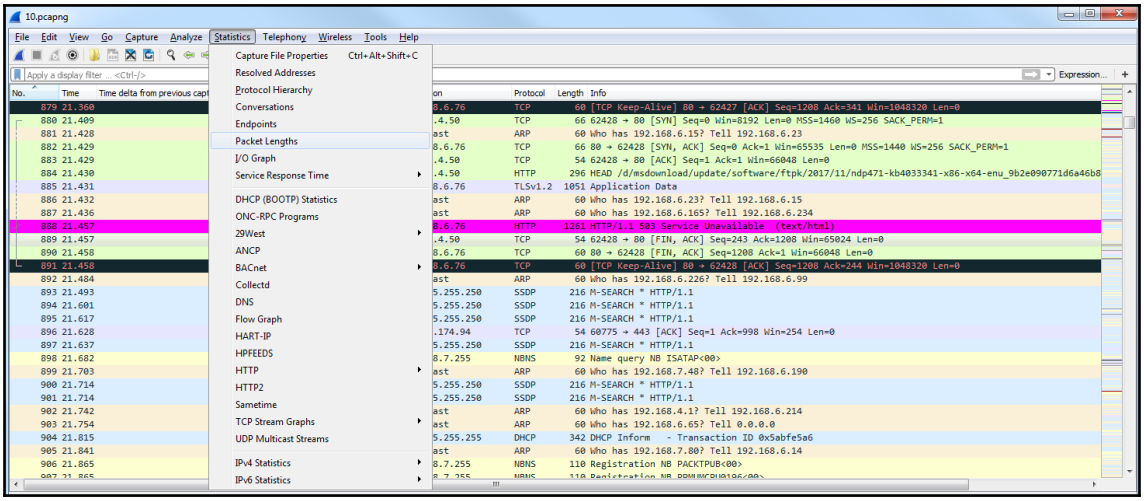


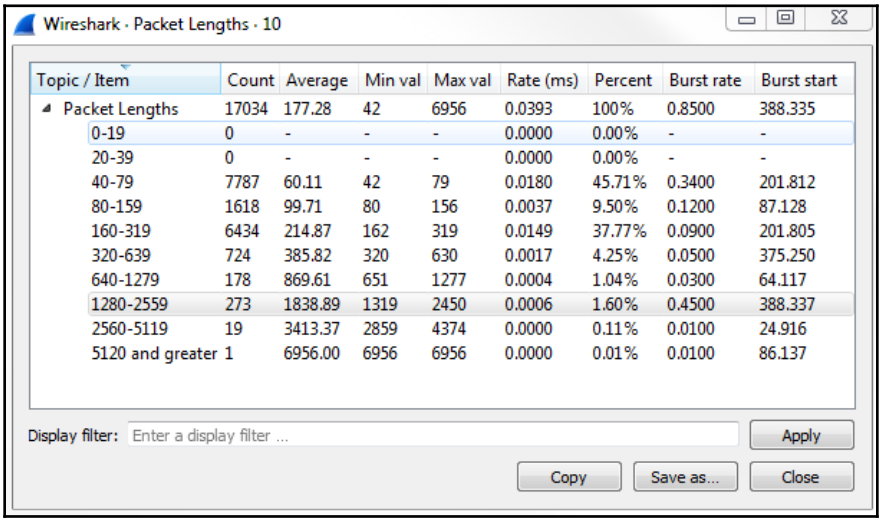
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.6.76	62346	207.46.140.70	443	1	60	0	0	1	60	21.100252	0.0000	—	
192.168.6.76	62347	13.78.94.7	443	1	60	0	0	1	60	27.772275	0.0000	—	
192.168.6.76	62154	162.125.34.137	443	1	54	1	54	0	0	345.528600	0.0000	—	
192.168.6.169	63838	192.168.6.76	2869	1	60	1	60	0	0	10.676226	0.0000	—	
192.168.5.168	50589	192.168.6.76	2869	9	3403	5	555	4	2848	189.353754	0.0022	—	
192.168.6.76	62459	192.168.0.5	88	8	3344	4	1660	4	1684	389.754268	0.0022	—	
192.168.5.168	50547	192.168.6.76	2869	10	3463	6	615	4	2848	126.313951	0.0028	—	
192.168.6.105	53671	192.168.6.76	2869	9	3403	5	555	4	2848	86.515916	0.0031	—	
192.168.6.76	62458	192.168.0.5	88	11	3778	5	1870	6	1908	389.750473	0.0031	—	
192.168.5.168	50605	192.168.6.76	2869	9	3403	5	555	4	2848	210.382404	0.0035	—	
192.168.6.65	52744	192.168.6.76	2869	9	3457	5	609	4	2848	24.842688	0.0040	—	
192.168.5.168	50686	192.168.6.76	2869	9	3403	5	555	4	2848	336.493361	0.0041	—	
192.168.5.246	54535	192.168.6.76	2869	9	5174	5	492	4	4682	392.071658	0.0042	—	
192.168.6.105	53733	192.168.6.76	2869	9	3403	5	555	4	2848	151.698760	0.0045	—	
192.168.5.93	55590	192.168.6.76	2869	9	5174	5	492	4	4682	417.224655	0.0045	—	
192.168.5.168	50477	192.168.6.76	2869	9	3403	5	555	4	2848	21.248503	0.0047	—	
192.168.5.168	50719	192.168.6.76	2869	10	3463	6	615	4	2848	378.550204	0.0047	—	
192.168.5.168	50702	192.168.6.76	2869	10	3463	6	615	4	2848	357.522896	0.0050	975 k	451
192.168.5.168	50745	192.168.6.76	2869	9	3403	5	555	4	2848	420.593013	0.0051	868 k	445
192.168.5.168	50561	192.168.6.76	2869	9	3403	5	555	4	2848	147.344978	0.0052	860 k	441
192.168.5.168	50532	192.168.6.76	2869	9	3403	5	555	4	2848	105.298255	0.0053	843 k	432
192.168.6.65	52897	192.168.6.76	2869	7	3251	4	476	3	2775	415.372047	0.0054	702 k	409
192.168.5.168	50658	192.168.6.76	2869	10	3463	6	615	4	2848	294.436250	0.0056	883 k	409
192.168.5.168	50618	192.168.6.76	2869	9	3403	5	555	4	2848	231.395154	0.0056	793 k	407
192.168.5.168	50576	192.168.6.76	2869	9	3403	5	555	4	2848	168.366406	0.0056	785 k	403
192.168.5.168	50733	192.168.6.76	2869	9	3403	5	555	4	2848	399.564869	0.0057	782 k	401
192.168.6.105	53687	192.168.6.76	2869	9	3403	5	555	4	2848	102.652474	0.0058	771 k	396
192.168.5.168	50631	192.168.6.76	2869	9	3403	5	555	4	2848	252.405782	0.0058	768 k	394
192.168.5.168	50516	192.168.6.76	2869	9	3403	5	555	4	2848	84.287732	0.0059	757 k	388
192.168.6.105	53802	192.168.6.76	2869	9	3403	5	555	4	2848	221.905521	0.0061	730 k	374
192.168.5.246	54530	192.168.6.76	2869	9	3457	5	609	4	2848	391.971021	0.0062	782 k	365
192.168.5.168	50464	192.168.6.76	2869	9	3403	5	555	4	2848	0.222569	0.0063	709 k	364

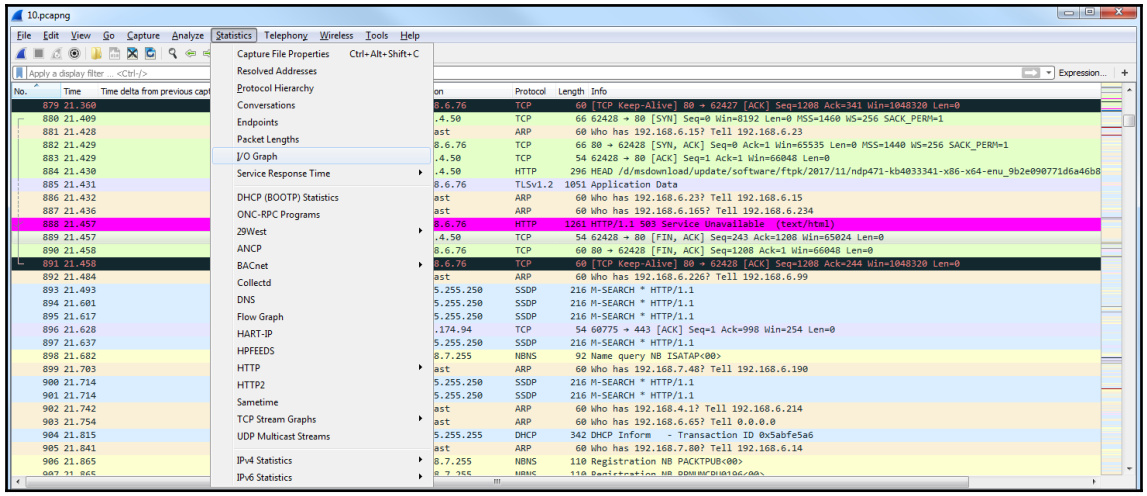

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous capt ion Protocol Length Info
879 21.360 8.6.76 TCP 60 [TCP Keep-Alive] 80 → 62427 [ACK] Seq=1208 Ack=341 Win=1048320 Len=0
880 21.409 .4.50 TCP 66 62428 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
881 21.428 ast ARP 60 Who has 192.168.6.15? Tell 192.168.6.23
882 21.429 8.6.76 TCP 66 80 → 62428 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
883 21.429 .4.50 TCP 54 62428 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
884 21.430 .4.50 HTTP 296 HEAD /d/msdownload/update/software/ftpk/2017/11/ndp471-kb4033341-x86-x64-enu_9b2e090771d6a46b8
885 21.431 8.6.76 TLSv1.2 1051 Application Data
886 21.432 ast ARP 60 Who has 192.168.6.23? Tell 192.168.6.15
887 21.436 ast ARP 60 Who has 192.168.6.165? Tell 192.168.6.234
888 21.457 8.6.76 HTTP 1261 HTTP/1.1 503 Service Unavailable (text/html)
889 21.457 .4.50 TCP 54 62428 → 80 [FIN, ACK] Seq=243 Ack=1208 Win=65024 Len=0
890 21.458 8.6.76 TCP 60 80 → 62428 [FIN, ACK] Seq=1208 Ack=1 Win=66048 Len=0
891 21.458 8.6.76 TCP 60 [TCP Keep-Alive] 80 → 62428 [ACK] Seq=1208 Ack=244 Win=1048320 Len=0
892 21.484 ast ARP 60 Who has 192.168.6.226? Tell 192.168.6.99
893 21.493 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
894 21.601 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
895 21.617 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
896 21.628 .174.94 TCP 54 60775 → 443 [ACK] Seq=1 Ack=998 Win=254 Len=0
897 21.637 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
898 21.682 8.7.255 NBNS 92 Name query NB ISATAP<00>
899 21.703 ast ARP 60 Who has 192.168.7.48? Tell 192.168.6.190
900 21.714 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
901 21.714 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
902 21.742 ast ARP 60 Who has 192.168.4.1? Tell 192.168.6.214
903 21.754 ast ARP 60 Who has 192.168.6.65? Tell 0.0.0.0
904 21.815 5.255.255 DHCP 342 DHCP Inform - Transaction ID 0x5abfe5a6
905 21.841 ast ARP 60 Who has 192.168.7.80? Tell 192.168.6.14
906 21.865 8.7.255 NBNS 110 Registration NB PACKTPUB<00>

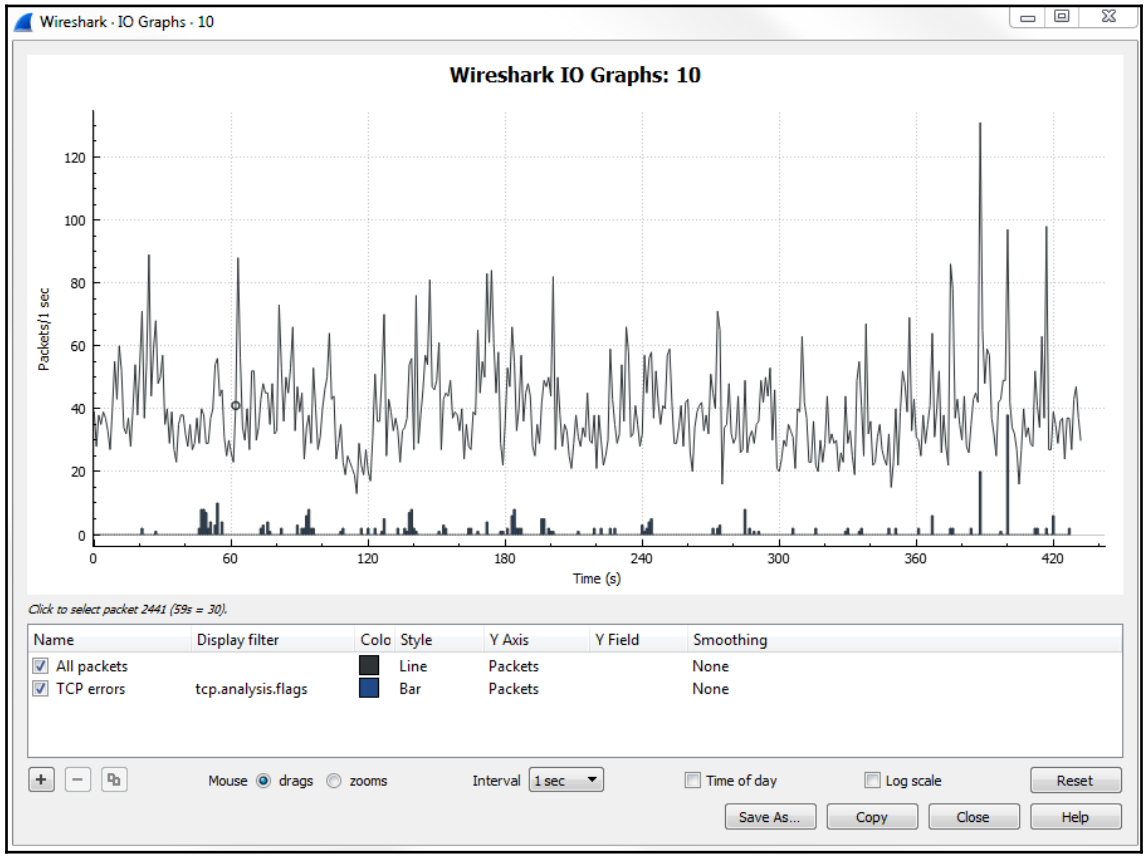


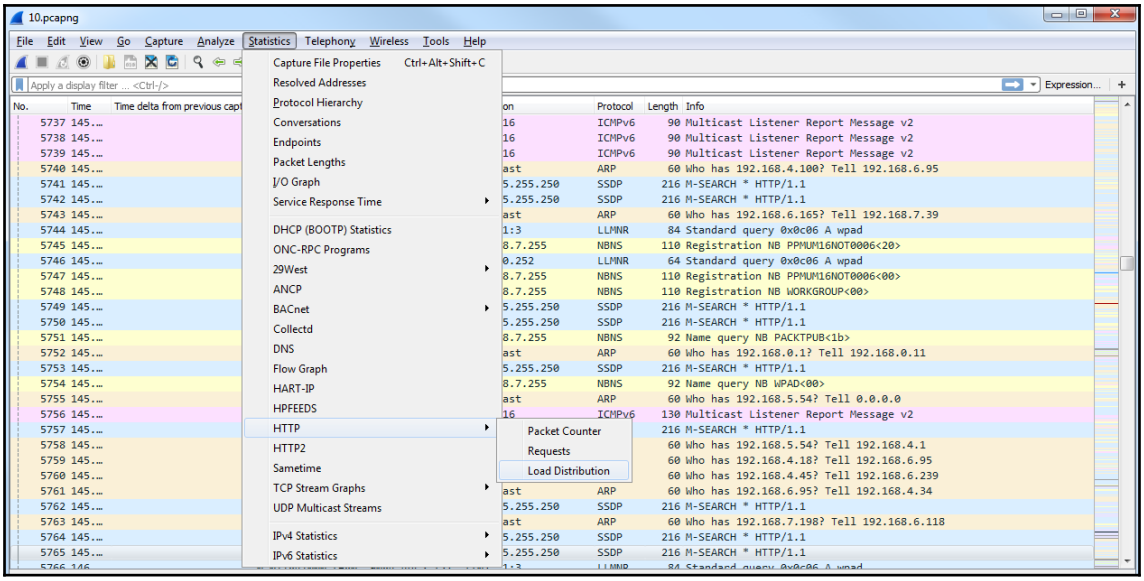
Address	Port	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Latitude	Longitude
13.78.94.7	443	1	60	1	60	0	0	—	—
13.91.52.255	443	23	9629	12	7733	11	1896	—	—
13.91.60.30	443	4	620	4	620	0	0	—	—
13.107.4.50	80	17	3985	8	2894	9	1091	—	—
23.9.182.247	80	8	453	3	180	5	273	—	—
34.243.33.253	443	27	10 k	13	4710	14	5403	—	—
40.84.37.228	443	34	12 k	18	9751	16	2784	—	—
49.248.249.8	80	15	894	7	456	8	438	—	—
52.85.17.195	80	11	627	5	300	6	327	—	—
52.85.17.214	80	10	586	5	312	5	274	—	—
52.114.32.7	443	44	27 k	21	9926	23	17 k	—	—
52.175.17.224	443	42	20 k	21	14 k	21	5683	—	—
52.215.44.95	443	95	56 k	54	13 k	41	42 k	—	—
52.220.73.34	80	6	349	3	186	3	163	—	—
52.229.174.94	443	189	158 k	95	55 k	94	103 k	—	—
54.169.219.198	80	6	349	3	186	3	163	—	—
54.225.198.196	80	6	350	3	186	3	164	—	—
54.243.142.74	443	9	542	4	271	5	271	—	—
74.125.68.155	443	13	817	6	435	7	382	—	—
103.23.66.118	443	161	29 k	88	18 k	73	11 k	—	—
104.120.73.214	443	9	549	4	277	5	272	—	—
109.234.207.107	443	27	10 k	13	5500	14	5030	—	—
149.174.66.134	80	13	743	6	360	7	383	—	—
151.101.2.110	443	24	1514	13	911	11	603	—	—
152.195.11.6	443	78	26 k	40	21 k	38	4592	—	—
157.240.16.35	443	7	436	4	273	3	163	—	—
162.125.33.7	443	18	6445	8	4228	10	2217	—	—
162.125.34.129	443	36	18 k	24	4452	12	13 k	—	—
162.125.34.137	443	1	54	0	0	1	54	—	—
172.217.27.194	80	9	1537	4	738	5	799	—	—
172.217.27.194	443	21	3568	11	1607	10	1961	—	—
172.217.160.162	443	5	345	3	237	2	108	—	—
172.217.163.198	80	14	834	7	450	7	384	—	—

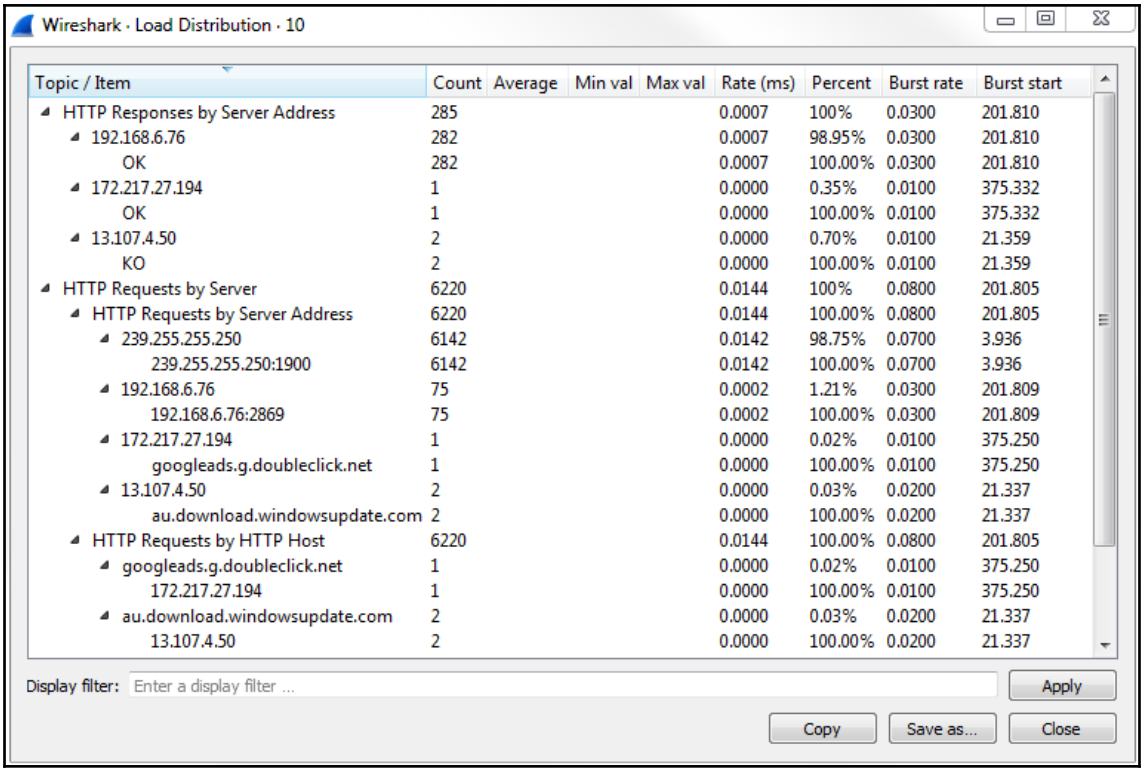

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics

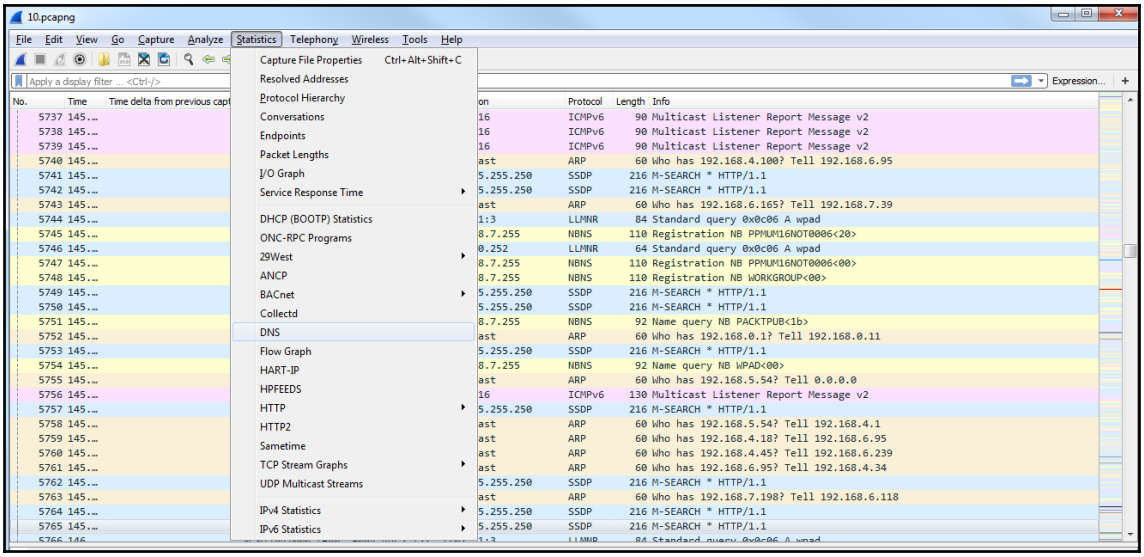

Wireshark · Packet Lengths · 10
Topic / Item Count Average Min val Max val Rate (ms) Percent Burst rate Burst start
Packet Lengths 17034 177.28 42 6956 0.0393 100% 0.8500 388.335
0-19 0 - - - 0.0000 0.00% - -
20-39 0 - - - 0.0000 0.00% - -
40-79 7787 60.11 42 79 0.0180 45.71% 0.3400 201.812
80-159 1618 99.71 80 156 0.0037 9.50% 0.1200 87.128
160-319 6434 214.87 162 319 0.0149 37.77% 0.0900 201.805
320-639 724 385.82 320 630 0.0017 4.25% 0.0500 375.250
640-1279 178 869.61 651 1277 0.0004 1.04% 0.0300 64.117
1280-2559 273 1838.89 1319 2450 0.0006 1.60% 0.4500 388.337
2560-5119 19 3413.37 2859 4374 0.0000 0.11% 0.0100 24.916
5120 and greater 1 6956.00 6956 6956 0.0000 0.01% 0.0100 86.137
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

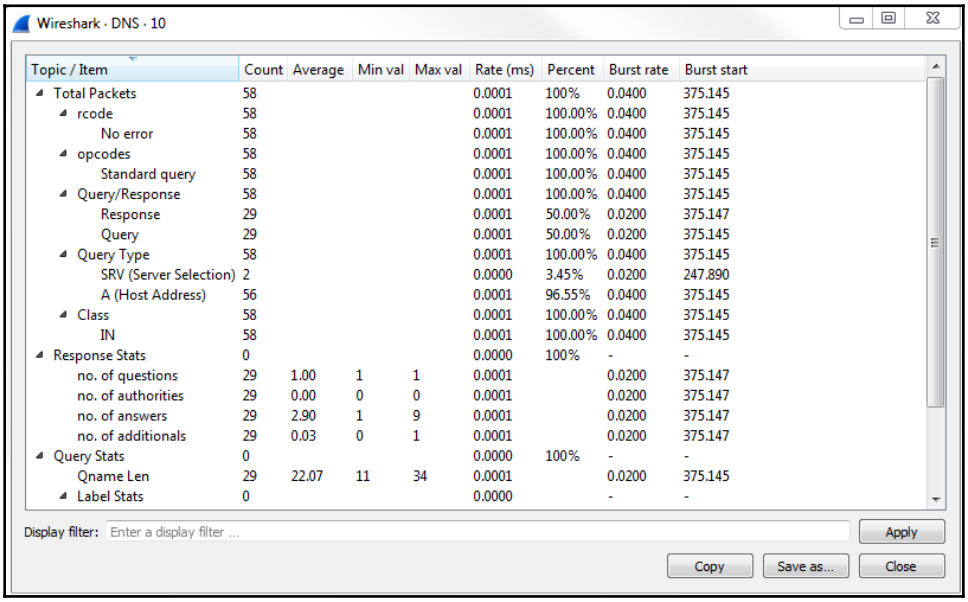

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics

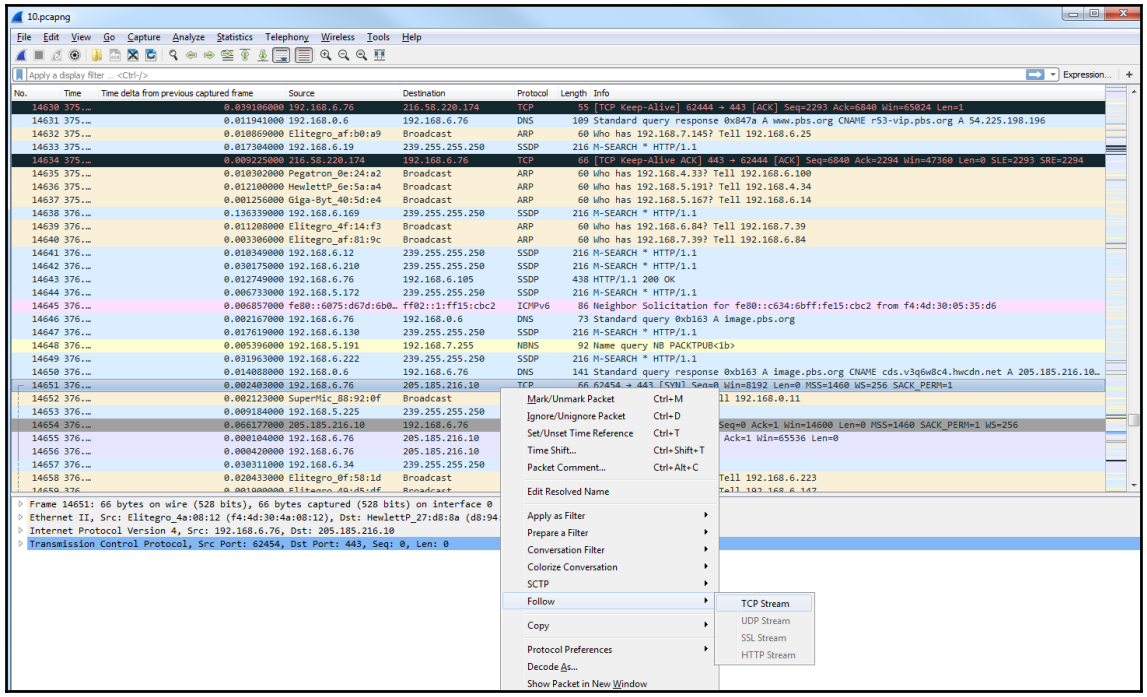

Wireshark · IO Graphs · 10
Wireshark IO Graphs: 10
Packets/1 sec
Time (s)
Click to select packet 2441 (59s = 30).
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
TCP errors
tcp.analysis.flags
Bar
Packets
None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

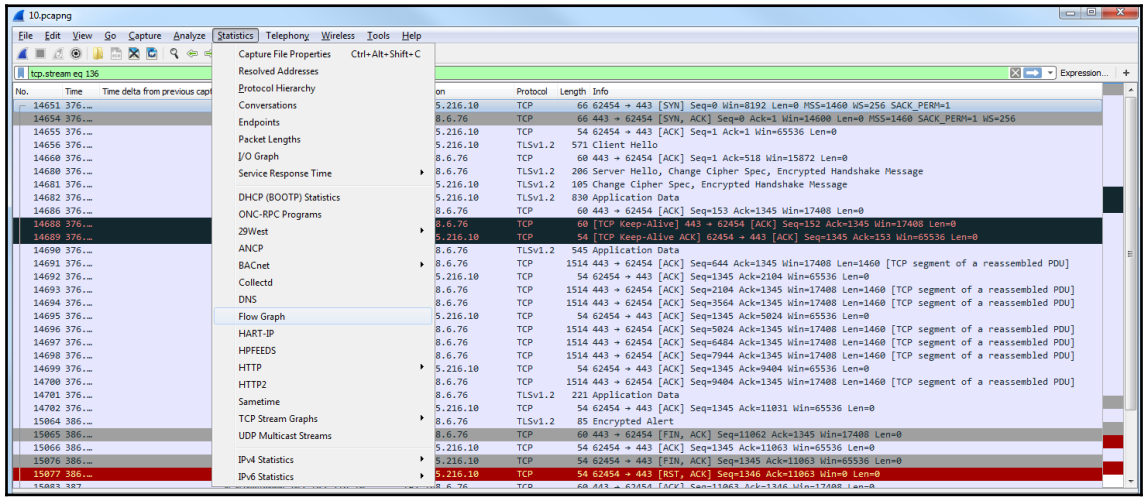

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Packet Counter
Requests
Load Distribution

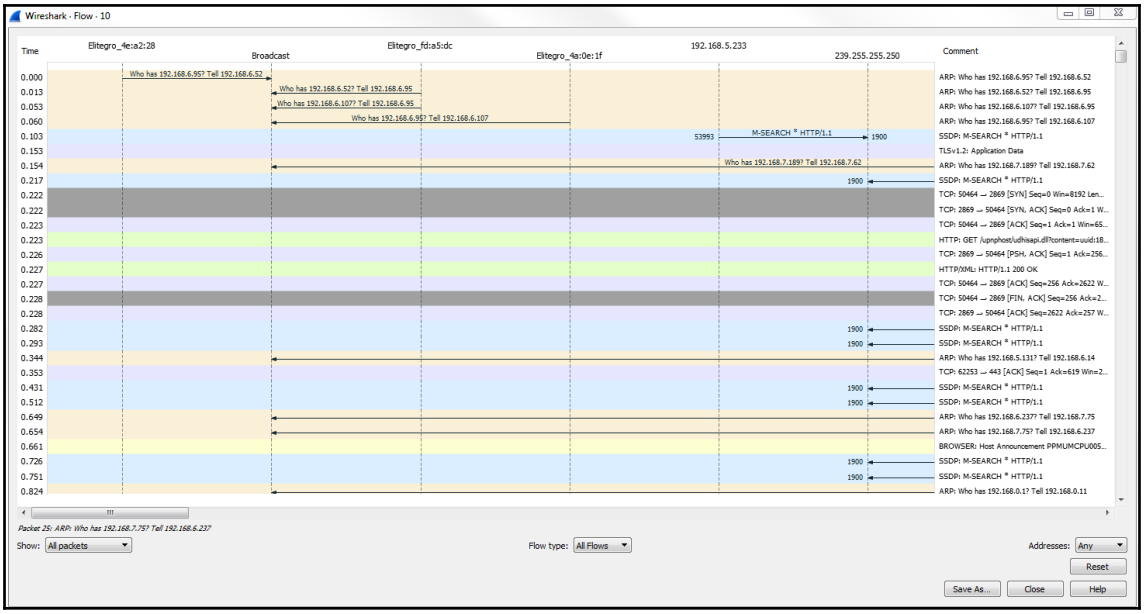

Wireshark · Load Distribution · 10
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
HTTP Responses by Server Address 285 0.0007 100% 0.0300 201.810
192.168.6.76 282 0.0007 98.95% 0.0300 201.810
OK 282 0.0007 100.00% 0.0300 201.810
172.217.27.194 1 0.0000 0.35% 0.0100 375.332
OK 1 0.0000 100.00% 0.0100 375.332
13.107.4.50 2 0.0000 0.70% 0.0100 21.359
KO 2 0.0000 100.00% 0.0100 21.359
HTTP Requests by Server 6220 0.0144 100% 0.0800 201.805
HTTP Requests by Server Address 6220 0.0144 100.00% 0.0800 201.805
239.255.255.250 6142 0.0142 98.75% 0.0700 3.936
239.255.255.250:1900 6142 0.0142 100.00% 0.0700 3.936
192.168.6.76 75 0.0002 1.21% 0.0300 201.809
192.168.6.76:2869 75 0.0002 100.00% 0.0300 201.809
172.217.27.194 1 0.0000 0.02% 0.0100 375.250
googleads.g.doubleclick.net 1 0.0000 100.00% 0.0100 375.250
13.107.4.50 2 0.0000 0.03% 0.0200 21.337
au.download.windowsupdate.com 2 0.0000 100.00% 0.0200 21.337
HTTP Requests by HTTP Host 6220 0.0144 100.00% 0.0800 201.805
googleads.g.doubleclick.net 1 0.0000 0.02% 0.0100 375.250
172.217.27.194 1 0.0000 100.00% 0.0100 375.250
au.download.windowsupdate.com 2 0.0000 0.03% 0.0200 21.337
13.107.4.50 2 0.0000 100.00% 0.0200 21.337
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

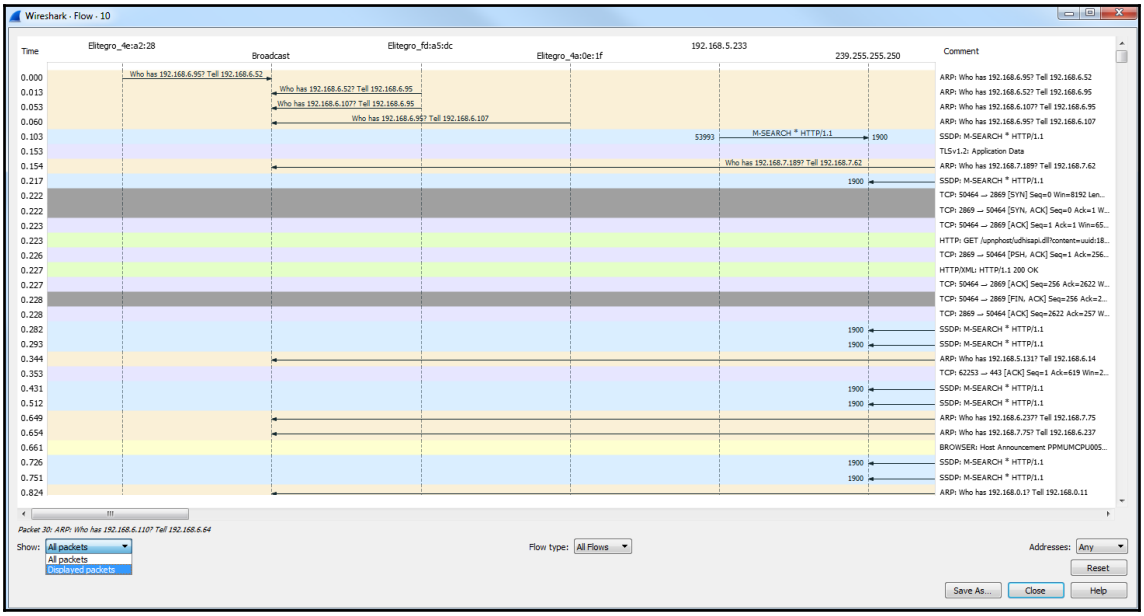

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous capt on Protocol Length Info
5737 145.... 16 ICMPv6 90 Multicast Listener Report Message v2
5738 145.... 16 ICMPv6 90 Multicast Listener Report Message v2
5739 145.... 16 ICMPv6 90 Multicast Listener Report Message v2
5740 145.... ast ARP 60 Who has 192.168.4.100? Tell 192.168.6.95
5741 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5742 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5743 145.... ast ARP 60 Who has 192.168.6.165? Tell 192.168.7.39
5744 145.... 1:3 LLMNR 84 Standard query 0x0c06 A wpad
5745 145.... 8.7.255 NBNS 110 Registration NB PPMUM16NOT0006<20>
5746 145.... 0.252 LLMNR 64 Standard query 0x0c06 A wpad
5747 145.... 8.7.255 NBNS 110 Registration NB PPMUM16NOT0006<00>
5748 145.... 8.7.255 NBNS 110 Registration NB WORKGROUP<00>
5749 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5750 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5751 145.... 8.7.255 NBNS 92 Name query NB PACKTPUB<1b>
5752 145.... ast ARP 60 Who has 192.168.0.1? Tell 192.168.0.11
5753 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5754 145.... 8.7.255 NBNS 92 Name query NB WPAD<00>
5755 145.... ast ARP 60 Who has 192.168.5.54? Tell 0.0.0.0
5756 145.... 16 ICMPv6 130 Multicast Listener Report Message v2
5757 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5758 145.... ast ARP 60 Who has 192.168.5.54? Tell 192.168.4.1
5759 145.... ast ARP 60 Who has 192.168.4.18? Tell 192.168.6.95
5760 145.... ast ARP 60 Who has 192.168.4.45? Tell 192.168.6.239
5761 145.... ast ARP 60 Who has 192.168.6.95? Tell 192.168.4.34
5762 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5763 145.... ast ARP 60 Who has 192.168.7.198? Tell 192.168.6.118
5764 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5765 145.... 5.255.250 SSDP 216 M-SEARCH * HTTP/1.1

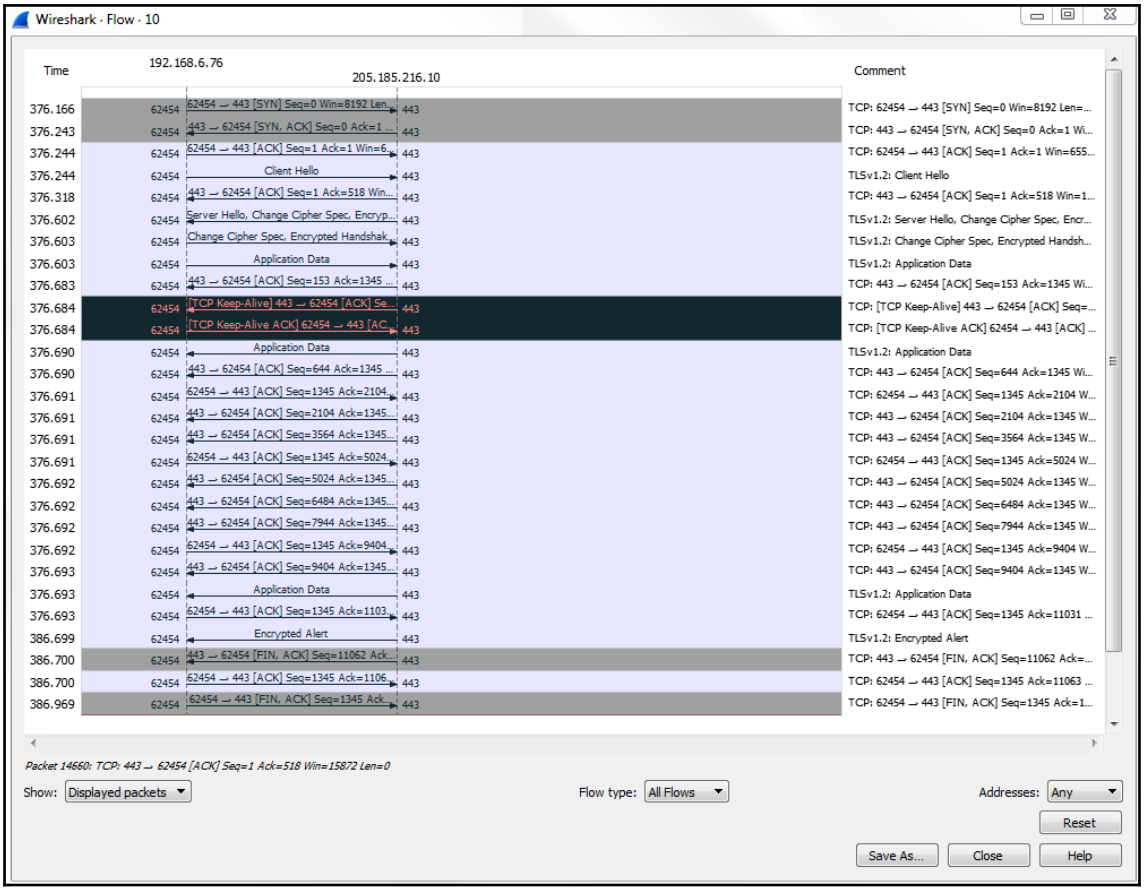

Wireshark · DNS · 10
Topic / Item Count Average Min val Max val Rate (ms) Percent Burst rate Burst start
Total Packets 58 0.0001 100% 0.0400 375.145
rcode 58 0.0001 100.00% 0.0400 375.145
No error 58 0.0001 100.00% 0.0400 375.145
opcodes 58 0.0001 100.00% 0.0400 375.145
Standard query 58 0.0001 100.00% 0.0400 375.145
Query/Response 58 0.0001 100.00% 0.0400 375.145
Response 29 0.0001 50.00% 0.0200 375.147
Query 29 0.0001 50.00% 0.0200 375.145
Query Type 58 0.0001 100.00% 0.0400 375.145
SRV (Server Selection) 2 0.0000 3.45% 0.0200 247.890
A (Host Address) 56 0.0001 96.55% 0.0400 375.145
Class 58 0.0001 100.00% 0.0400 375.145
IN 58 0.0001 100.00% 0.0400 375.145
Response Stats 0 0.0000 100% - -
no. of questions 29 1.00 1 1 0.0001 0.0200 375.147
no. of authorities 29 0.00 0 0 0.0001 0.0200 375.147
no. of answers 29 2.90 1 9 0.0001 0.0200 375.147
no. of additionals 29 0.03 0 1 0.0001 0.0200 375.147
Query Stats 0 0.0000 100% - -
Qname Len 29 22.07 11 34 0.0001 0.0200 375.145
Label Stats 0 0.0000 - -
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

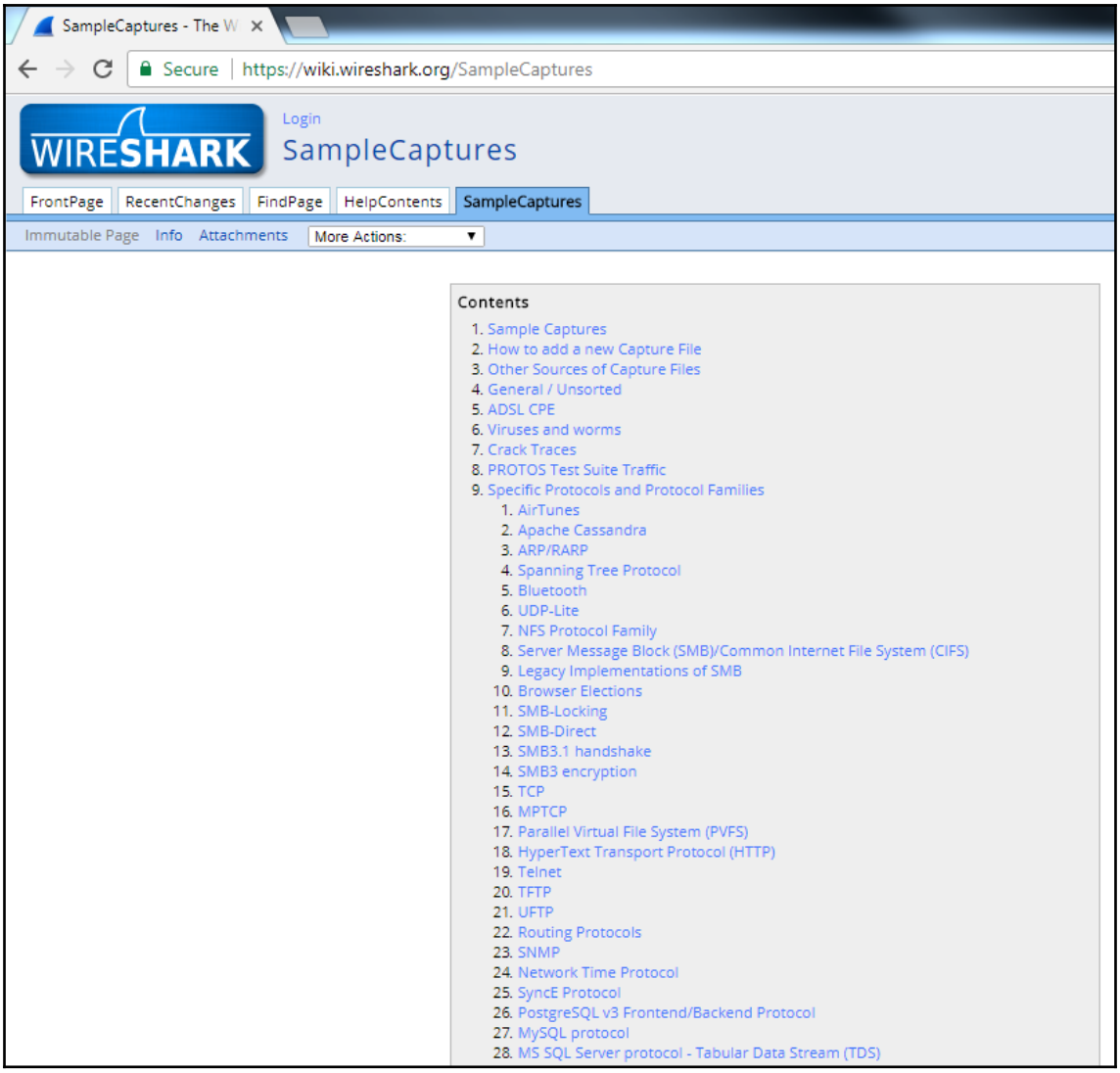

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
Protocol Preferences
Decode As...
Show Packet in New Window
TCP Stream
UDP Stream
SSL Stream
HTTP Stream

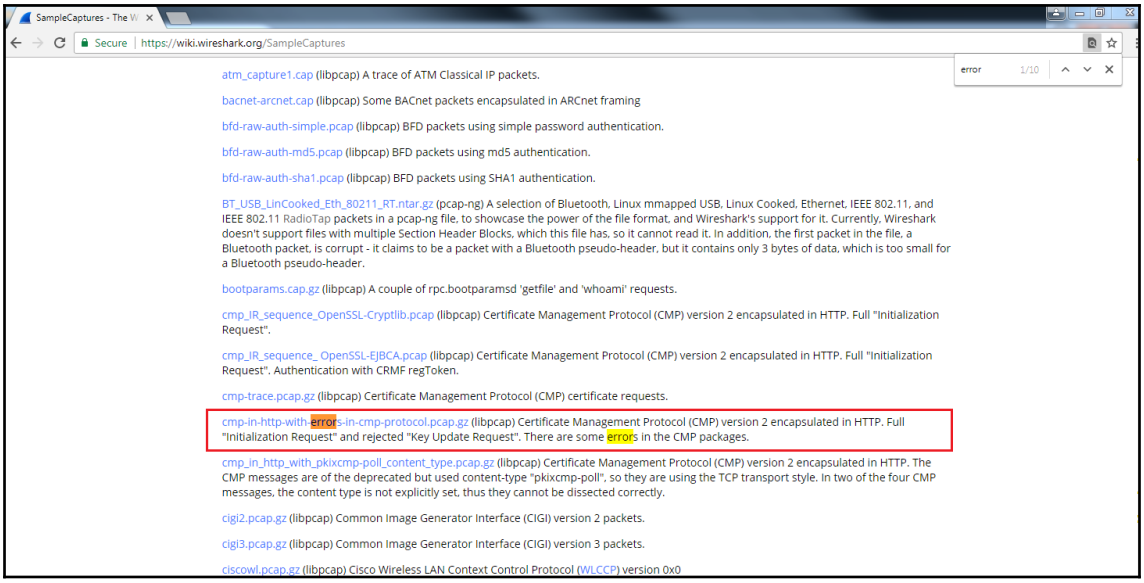

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics

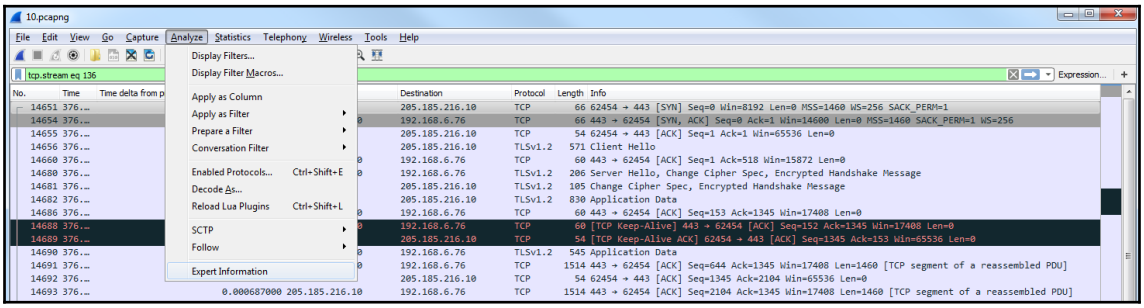

Wireshark · Flow · 10
Time
Elitegro_4e:a2:28
Broadcast
Elitegro_fd:a5:dc
Elitegro_4a:0e:1f
192.168.5.233
239.255.255.250
Comment
Who has 192.168.6.95? Tell 192.168.6.52
Who has 192.168.6.52? Tell 192.168.6.95
Who has 192.168.6.107? Tell 192.168.6.95
Who has 192.168.6.95? Tell 192.168.6.107
53993
M-SEARCH * HTTP/1.1
1900
Who has 192.168.7.189? Tell 192.168.7.62
Packet 25: ARP: Who has 192.168.7.75? Tell 192.168.6.237
Show: All packets
Flow type: All Flows
Addresses: Any
Reset
Save As...
Close
Help

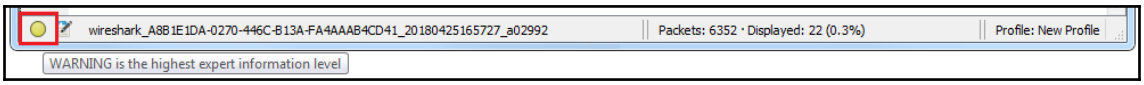

Wireshark · Flow · 10
Time
Elitegro_4e:a2:28
Broadcast
Elitegro_fd:a5:dc
Elitegro_4a:0e:1f
192.168.5.233
239.255.255.250
Comment
Who has 192.168.6.95? Tell 192.168.6.52
Who has 192.168.6.52? Tell 192.168.6.95
Who has 192.168.6.107? Tell 192.168.6.95
Who has 192.168.6.95? Tell 192.168.6.107
53993
M-SEARCH * HTTP/1.1
1900
Who has 192.168.7.189? Tell 192.168.7.62
Packet 30: ARP: Who has 192.168.6.110? Tell 192.168.6.64
Show: All packets
All packets
Displayed packets
Flow type: All Flows
Addresses: Any
Reset
Save As...
Close
Help

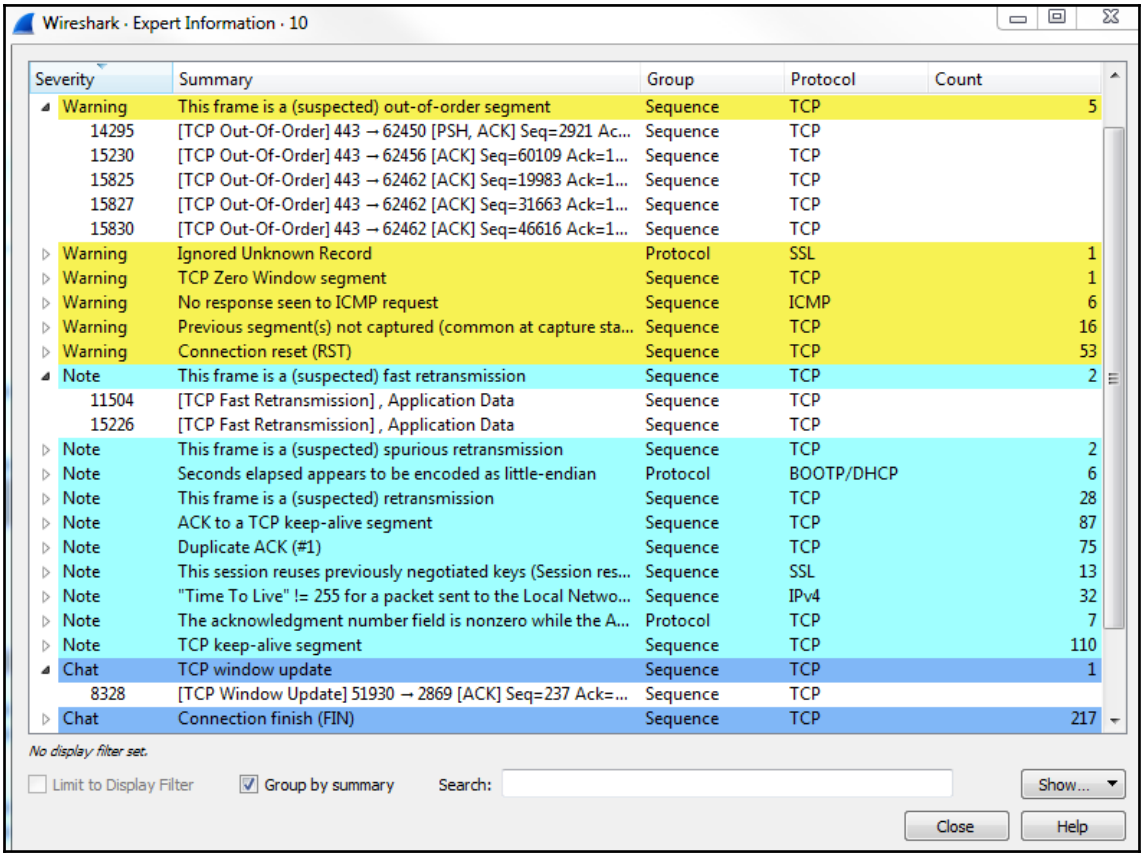

Wireshark · Flow · 10
Time
192.168.6.76
205.185.216.10
Comment
376.166 62454 62454 → 443 [SYN] Seq=0 Win=8192 Len... 443 TCP: 62454 → 443 [SYN] Seq=0 Win=8192 Len=...
376.243 62454 443 → 62454 [SYN, ACK] Seq=0 Ack=1 ... 443 TCP: 443 → 62454 [SYN, ACK] Seq=0 Ack=1 Wi...
376.244 62454 62454 → 443 [ACK] Seq=1 Ack=1 Win=6... 443 TCP: 62454 → 443 [ACK] Seq=1 Ack=1 Win=655...
376.244 62454 Client Hello 443 TLSv1.2: Client Hello
376.318 62454 443 → 62454 [ACK] Seq=1 Ack=518 Win... 443 TCP: 443 → 62454 [ACK] Seq=1 Ack=518 Win=1...
376.602 62454 Server Hello, Change Cipher Spec, Encryp... 443 TLSv1.2: Server Hello, Change Cipher Spec, Encr...
376.603 62454 Change Cipher Spec, Encrypted Handshak... 443 TLSv1.2: Change Cipher Spec, Encrypted Handsh...
376.603 62454 Application Data 443 TLSv1.2: Application Data
376.683 62454 443 → 62454 [ACK] Seq=153 Ack=1345 ... 443 TCP: 443 → 62454 [ACK] Seq=153 Ack=1345 Wi...
376.684 62454 [TCP Keep-Alive] 443 → 62454 [ACK] Se... 443 TCP: [TCP Keep-Alive] 443 → 62454 [ACK] Seq=...
376.684 62454 [TCP Keep-Alive ACK] 62454 → 443 [AC... 443 TCP: [TCP Keep-Alive ACK] 62454 → 443 [ACK] ...
376.690 62454 Application Data 443 TLSv1.2: Application Data
376.690 62454 443 → 62454 [ACK] Seq=644 Ack=1345 ... 443 TCP: 443 → 62454 [ACK] Seq=644 Ack=1345 Wi...
376.691 62454 62454 → 443 [ACK] Seq=1345 Ack=2104... 443 TCP: 62454 → 443 [ACK] Seq=1345 Ack=2104 W...
376.691 62454 443 → 62454 [ACK] Seq=2104 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=2104 Ack=1345 W...
376.691 62454 443 → 62454 [ACK] Seq=3564 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=3564 Ack=1345 W...
376.691 62454 62454 → 443 [ACK] Seq=1345 Ack=5024... 443 TCP: 62454 → 443 [ACK] Seq=1345 Ack=5024 W...
376.692 62454 443 → 62454 [ACK] Seq=5024 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=5024 Ack=1345 W...
376.692 62454 443 → 62454 [ACK] Seq=6484 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=6484 Ack=1345 W...
376.692 62454 443 → 62454 [ACK] Seq=7944 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=7944 Ack=1345 W...
376.692 62454 62454 → 443 [ACK] Seq=1345 Ack=9404... 443 TCP: 62454 → 443 [ACK] Seq=1345 Ack=9404 W...
376.693 62454 443 → 62454 [ACK] Seq=9404 Ack=1345... 443 TCP: 443 → 62454 [ACK] Seq=9404 Ack=1345 W...
376.693 62454 Application Data 443 TLSv1.2: Application Data
376.693 62454 62454 → 443 [ACK] Seq=1345 Ack=1103... 443 TCP: 62454 → 443 [ACK] Seq=1345 Ack=11031 ...
386.699 62454 Encrypted Alert 443 TLSv1.2: Encrypted Alert
386.700 62454 443 → 62454 [FIN, ACK] Seq=11062 Ack... 443 TCP: 443 → 62454 [FIN, ACK] Seq=11062 Ack=...
386.700 62454 62454 → 443 [ACK] Seq=1345 Ack=1106... 443 TCP: 62454 → 443 [ACK] Seq=1345 Ack=11063 ...
386.969 62454 62454 → 443 [FIN, ACK] Seq=1345 Ack... 443 TCP: 62454 → 443 [FIN, ACK] Seq=1345 Ack=1...
Packet 14660: TCP: 443 → 62454 [ACK] Seq=1 Ack=518 Win=15872 Len=0
Show: Displayed packets
Flow type: All Flows
Addresses: Any
Reset
Save As...
Close
Help

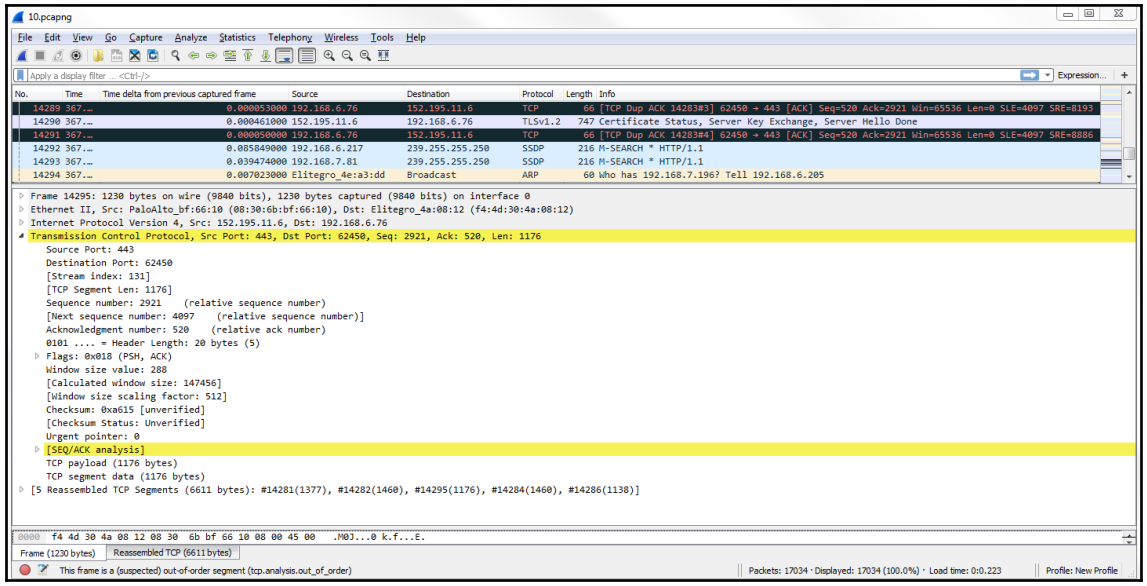

SampleCaptures - The W
Secure
https://wiki.wireshark.org/SampleCaptures
WIRESHARK
Login
SampleCaptures
FrontPage
RecentChanges
FindPage
HelpContents
SampleCaptures
Immutable Page
Info
Attachments
More Actions:
Contents
1. Sample Captures
2. How to add a new Capture File
3. Other Sources of Capture Files
4. General / Unsorted
5. ADSL CPE
6. Viruses and worms
7. Crack Traces
8. PROTOS Test Suite Traffic
9. Specific Protocols and Protocol Families
1. AirTunes
2. Apache Cassandra
3. ARP/RARP
4. Spanning Tree Protocol
5. Bluetooth
6. UDP-Lite
7. NFS Protocol Family
8. Server Message Block (SMB)/Common Internet File System (CIFS)
9. Legacy Implementations of SMB
10. Browser Elections
11. SMB-Locking
12. SMB-Direct
13. SMB3.1 handshake
14. SMB3 encryption
15. TCP
16. MPTCP
17. Parallel Virtual File System (PVFS)
18. HyperText Transport Protocol (HTTP)
19. Telnet
20. TFTP
21. UFTP
22. Routing Protocols
23. SNMP
24. Network Time Protocol
25. SyncE Protocol
26. PostgreSQL v3 Frontend/Backend Protocol
27. MySQL protocol
28. MS SQL Server protocol - Tabular Data Stream (TDS)

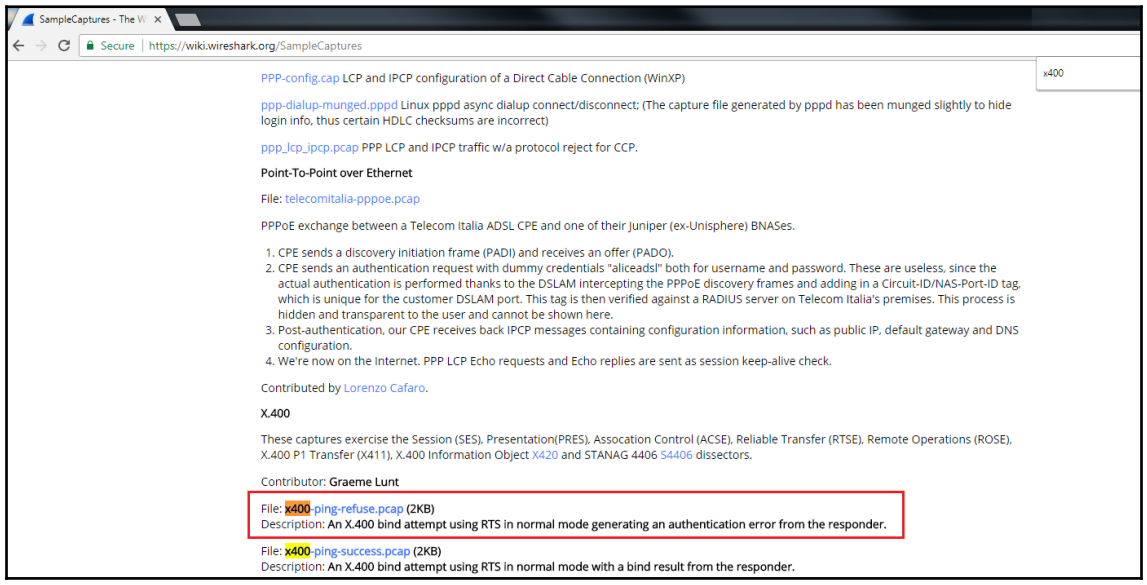

SampleCaptures - The W
Secure | https://wiki.wireshark.org/SampleCaptures
error 1/10
atm_capture1.cap (libpcap) A trace of ATM Classical IP packets.
bacnet-arcnet.cap (libpcap) Some BACnet packets encapsulated in ARCnet framing
bfd-raw-auth-simple.pcap (libpcap) BFD packets using simple password authentication.
bfd-raw-auth-md5.pcap (libpcap) BFD packets using md5 authentication.
bfd-raw-auth-sha1.pcap (libpcap) BFD packets using SHA1 authentication.
BT_USB_LinCooked_Eth_80211_RT.ntar.gz (pcap-ng) A selection of Bluetooth, Linux mmapped USB, Linux Cooked, Ethernet, IEEE 802.11, and IEEE 802.11 RadioTap packets in a pcap-ng file, to showcase the power of the file format, and Wireshark's support for it. Currently, Wireshark doesn't support files with multiple Section Header Blocks, which this file has, so it cannot read it. In addition, the first packet in the file, a Bluetooth packet, is corrupt - it claims to be a packet with a Bluetooth pseudo-header, but it contains only 3 bytes of data, which is too small for a Bluetooth pseudo-header.
bootparams.cap.gz (libpcap) A couple of rpc.bootparamsd 'getfile' and 'whoami' requests.
cmp_IR_sequence_OpenSSL-Cryptlib.pcap (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request".
cmp_IR_sequence_ OpenSSL-EJBCA.pcap (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request". Authentication with CRMF regToken.
cmp-trace.pcap.gz (libpcap) Certificate Management Protocol (CMP) certificate requests.
cmp-in-http-with-errors-in-cmp-protocol.pcap.gz (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. Full "Initialization Request" and rejected "Key Update Request". There are some errors in the CMP packages.
cmp_in_http_with_pkixcmp-poll_content_type.pcap.gz (libpcap) Certificate Management Protocol (CMP) version 2 encapsulated in HTTP. The CMP messages are of the deprecated but used content-type "pkixcmp-poll", so they are using the TCP transport style. In two of the four CMP messages, the content type is not explicitly set, thus they cannot be dissected correctly.
cigi2.pcap.gz (libpcap) Common Image Generator Interface (CIGI) version 2 packets.
cigi3.pcap.gz (libpcap) Common Image Generator Interface (CIGI) version 3 packets.
ciscowl.pcap.gz (libpcap) Cisco Wireless LAN Context Control Protocol (WLCCP) version 0x0

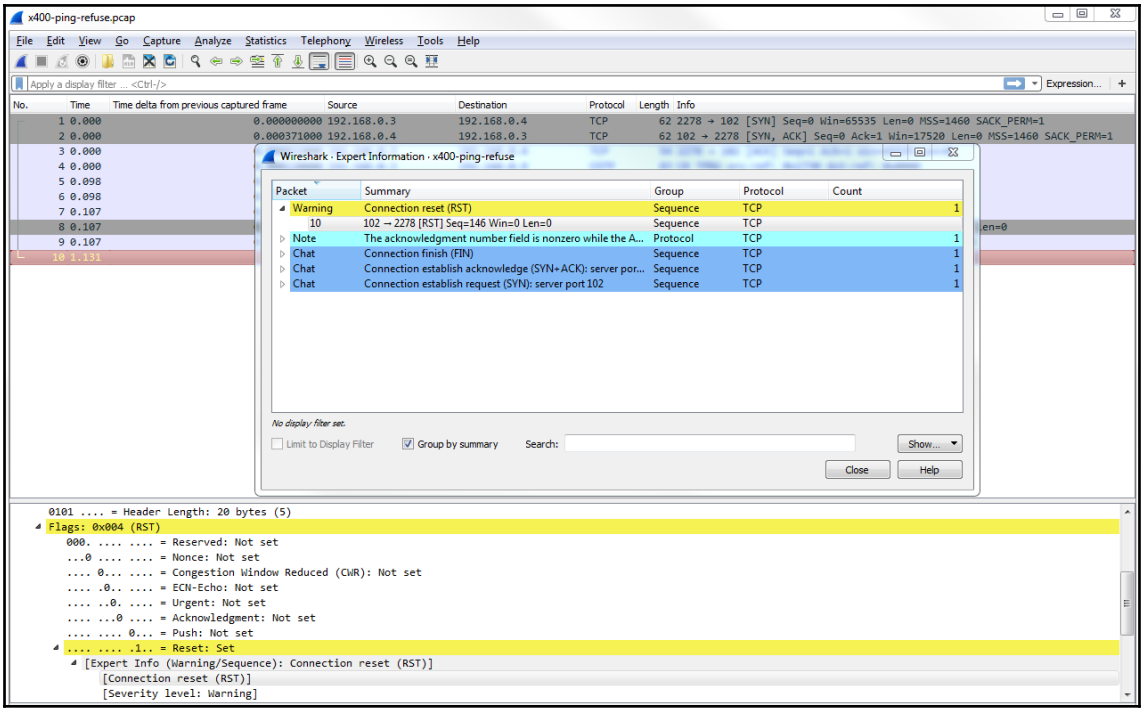

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Enabled Protocols... Ctrl+Shift+E
Decode As...
Reload Lua Plugins Ctrl+Shift+L
SCTP
Follow
Expert Information
tcp.stream eq 136
Expression...
No. Time Time delta from p Destination Protocol Length Info
14651 376... 205.185.216.10 TCP 66 62454 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
14654 376... 192.168.6.76 TCP 66 443 → 62454 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=256
14655 376... 205.185.216.10 TCP 54 62454 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
14656 376... 205.185.216.10 TLSv1.2 571 Client Hello
14660 376... 192.168.6.76 TCP 60 443 → 62454 [ACK] Seq=1 Ack=518 Win=15872 Len=0
14680 376... 192.168.6.76 TLSv1.2 206 Server Hello, Change Cipher Spec, Encrypted Handshake Message
14681 376... 205.185.216.10 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
14682 376... 205.185.216.10 TLSv1.2 830 Application Data
14686 376... 192.168.6.76 TCP 60 443 → 62454 [ACK] Seq=153 Ack=1345 Win=17408 Len=0
14688 376... 192.168.6.76 TCP 60 [TCP Keep-Alive] 443 → 62454 [ACK] Seq=152 Ack=1345 Win=17408 Len=0
14689 376... 205.185.216.10 TCP 54 [TCP Keep-Alive ACK] 62454 → 443 [ACK] Seq=1345 Ack=153 Win=65536 Len=0
14690 376... 192.168.6.76 TLSv1.2 545 Application Data
14691 376... 192.168.6.76 TCP 1514 443 → 62454 [ACK] Seq=644 Ack=1345 Win=17408 Len=1460 [TCP segment of a reassembled PDU]
14692 376... 205.185.216.10 TCP 54 62454 → 443 [ACK] Seq=1345 Ack=2104 Win=65536 Len=0
14693 376... 0.000687000 205.185.216.10 192.168.6.76 TCP 1514 443 → 62454 [ACK] Seq=2104 Ack=1345 Win=17408 Len=1460 [TCP segment of a reassembled PDU]


wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180425165727_a02992
Packets: 6352 · Displayed: 22 (0.3%)
Profile: New Profile
WARNING is the highest expert information level

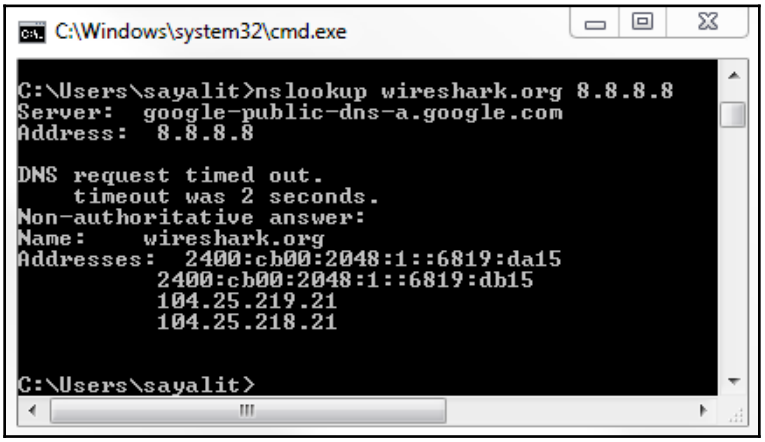

Wireshark · Expert Information · 10
Severity
Summary
Group
Protocol
Count
Warning
This frame is a (suspected) out-of-order segment
Sequence
TCP
5
14295
[TCP Out-Of-Order] 443 → 62450 [PSH, ACK] Seq=2921 Ac...
Sequence
TCP
15230
[TCP Out-Of-Order] 443 → 62456 [ACK] Seq=60109 Ack=1...
Sequence
TCP
15825
[TCP Out-Of-Order] 443 → 62462 [ACK] Seq=19983 Ack=1...
Sequence
TCP
15827
[TCP Out-Of-Order] 443 → 62462 [ACK] Seq=31663 Ack=1...
Sequence
TCP
15830
[TCP Out-Of-Order] 443 → 62462 [ACK] Seq=46616 Ack=1...
Sequence
TCP
Warning
Ignored Unknown Record
Protocol
SSL
1
Warning
TCP Zero Window segment
Sequence
TCP
1
Warning
No response seen to ICMP request
Sequence
ICMP
6
Warning
Previous segment(s) not captured (common at capture sta...
Sequence
TCP
16
Warning
Connection reset (RST)
Sequence
TCP
53
Note
This frame is a (suspected) fast retransmission
Sequence
TCP
2
11504
[TCP Fast Retransmission] , Application Data
Sequence
TCP
15226
[TCP Fast Retransmission] , Application Data
Sequence
TCP
Note
This frame is a (suspected) spurious retransmission
Sequence
TCP
2
Note
Seconds elapsed appears to be encoded as little-endian
Protocol
BOOTP/DHCP
6
Note
This frame is a (suspected) retransmission
Sequence
TCP
28
Note
ACK to a TCP keep-alive segment
Sequence
TCP
87
Note
Duplicate ACK (#1)
Sequence
TCP
75
Note
This session reuses previously negotiated keys (Session res...
Sequence
SSL
13
Note
"Time To Live" != 255 for a packet sent to the Local Netwo...
Sequence
IPv4
32
Note
The acknowledgment number field is nonzero while the A...
Protocol
TCP
7
Note
TCP keep-alive segment
Sequence
TCP
110
Chat
TCP window update
Sequence
TCP
1
8328
[TCP Window Update] 51930 → 2869 [ACK] Seq=237 Ack=...
Sequence
TCP
Chat
Connection finish (FIN)
Sequence
TCP
217
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

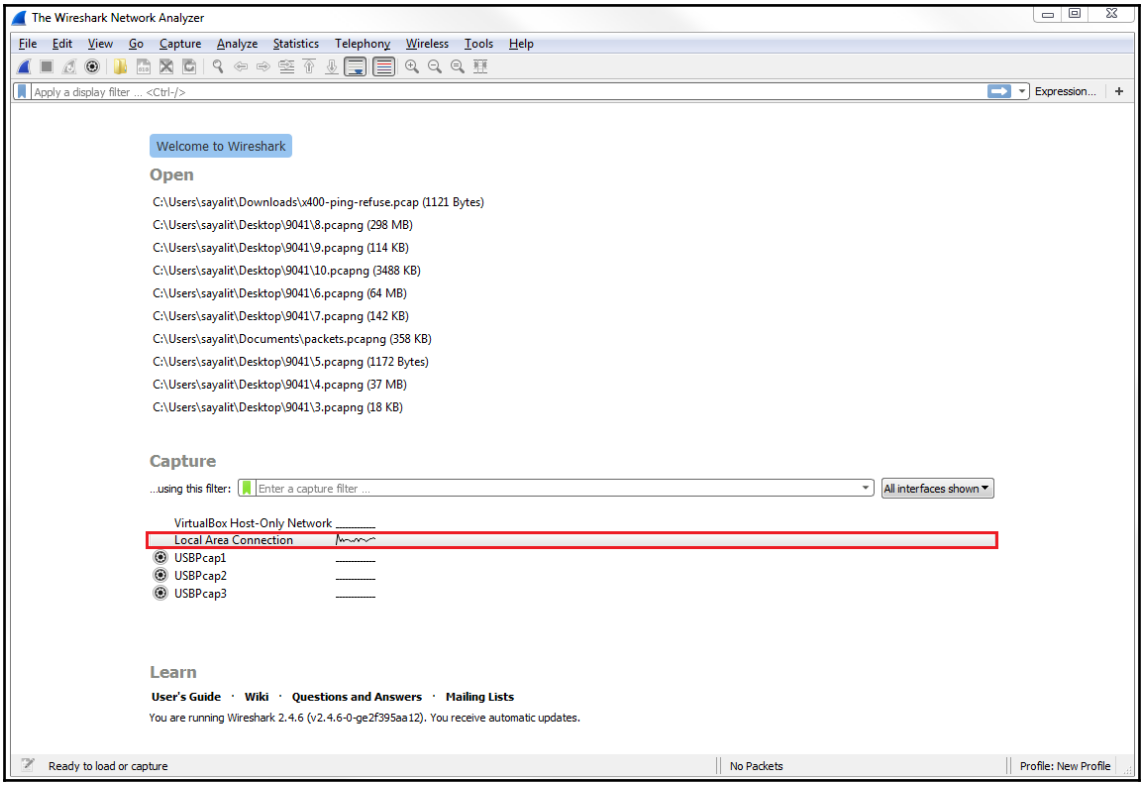

10.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
14289 367... 0.000053000 192.168.6.76 152.195.11.6 TCP 66 [TCP Dup ACK 14283#3] 62450 → 443 [ACK] Seq=520 Ack=2921 Win=65536 Len=0 SLE=4097 SRE=8193
14290 367... 0.000461000 152.195.11.6 192.168.6.76 TLSv1.2 747 Certificate Status, Server Key Exchange, Server Hello Done
14291 367... 0.000050000 192.168.6.76 152.195.11.6 TCP 66 [TCP Dup ACK 14283#4] 62450 → 443 [ACK] Seq=520 Ack=2921 Win=65536 Len=0 SLE=4097 SRE=8886
14292 367... 0.085849000 192.168.6.217 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14293 367... 0.039474000 192.168.7.81 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
14294 367... 0.007023000 Elitegro_4e:a3:dd Broadcast ARP 60 Who has 192.168.7.196? Tell 192.168.6.205
Frame 14295: 1230 bytes on wire (9840 bits), 1230 bytes captured (9840 bits) on interface 0
Ethernet II, Src: PaloAlto_bf:66:10 (08:30:6b:bf:66:10), Dst: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4, Src: 152.195.11.6, Dst: 192.168.6.76
Transmission Control Protocol, Src Port: 443, Dst Port: 62450, Seq: 2921, Ack: 520, Len: 1176
Source Port: 443
Destination Port: 62450
[Stream index: 131]
[TCP Segment Len: 1176]
Sequence number: 2921 (relative sequence number)
[Next sequence number: 4097 (relative sequence number)]
Acknowledgment number: 520 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x018 (PSH, ACK)
Window size value: 288
[Calculated window size: 147456]
[Window size scaling factor: 512]
Checksum: 0xa615 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
TCP payload (1176 bytes)
TCP segment data (1176 bytes)
[5 Reassembled TCP Segments (6611 bytes): #14281(1377), #14282(1460), #14295(1176), #14284(1460), #14286(1138)]
0000 f4 4d 30 4a 08 12 08 30 6b bf 66 10 08 00 45 00 .M0J...0 k.f...E.
Frame (1230 bytes) Reassembled TCP (6611 bytes)
This frame is a (suspected) out-of-order segment (tcp.analysis.out_of_order)
Packets: 17034 · Displayed: 17034 (100.0%) · Load time: 0:0.223
Profile: New Profile

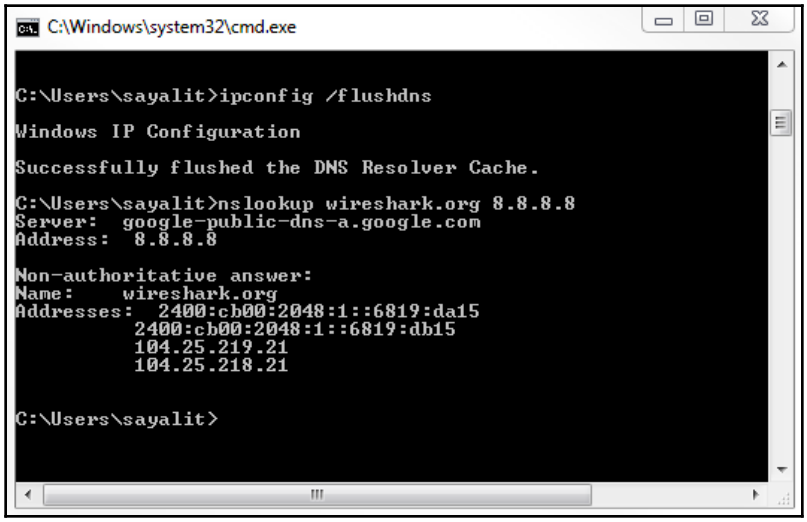

SampleCaptures - The W
Secure https://wiki.wireshark.org/SampleCaptures
x400
PPP-config.cap LCP and IPCP configuration of a Direct Cable Connection (WinXP)
ppp-dialup-munged.pppd Linux pppd async dialup connect/disconnect; (The capture file generated by pppd has been munged slightly to hide login info, thus certain HDLC checksums are incorrect)
ppp_lcp_ipcp.pcap PPP LCP and IPCP traffic w/a protocol reject for CCP.
Point-To-Point over Ethernet
File: telecomitalia-pppoe.pcap
PPPoE exchange between a Telecom Italia ADSL CPE and one of their Juniper (ex-Unisphere) BNASes.
1. CPE sends a discovery initiation frame (PADI) and receives an offer (PADO).
2. CPE sends an authentication request with dummy credentials "aliceadsl" both for username and password. These are useless, since the actual authentication is performed thanks to the DSLAM intercepting the PPPoE discovery frames and adding in a Circuit-ID/NAS-Port-ID tag, which is unique for the customer DSLAM port. This tag is then verified against a RADIUS server on Telecom Italia's premises. This process is hidden and transparent to the user and cannot be shown here.
3. Post-authentication, our CPE receives back IPCP messages containing configuration information, such as public IP, default gateway and DNS configuration.
4. We're now on the Internet. PPP LCP Echo requests and Echo replies are sent as session keep-alive check.
Contributed by Lorenzo Cafaro.
X.400
These captures exercise the Session (SES), Presentation(PRES), Association Control (ACSE), Reliable Transfer (RTSE), Remote Operations (ROSE), X.400 P1 Transfer (X411), X.400 Information Object X420 and STANAG 4406 S4406 dissectors.
Contributor: Graeme Lunt
File: x400-ping-refuse.pcap (2KB)
Description: An X.400 bind attempt using RTS in normal mode generating an authentication error from the responder.
File: x400-ping-success.pcap (2KB)
Description: An X.400 bind attempt using RTS in normal mode with a bind result from the responder.

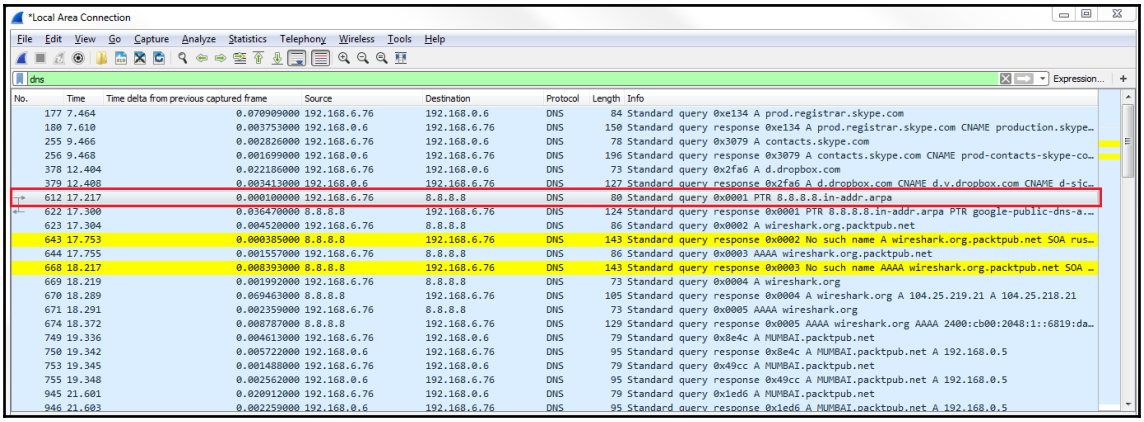

x400-ping-refuse.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
1 0.000 0.000000000 192.168.0.3 192.168.0.4 TCP 62 2278 → 102 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
2 0.000 0.000371000 192.168.0.4 192.168.0.3 TCP 62 102 → 2278 [SYN, ACK] Seq=0 Ack=1 Win=17520 Len=0 MSS=1460 SACK_PERM=1
3 0.000
4 0.000
5 0.098
6 0.098
7 0.107
8 0.107
9 0.107
10 1.131
Wireshark · Expert Information · x400-ping-refuse
Packet Summary Group Protocol Count
Warning Connection reset (RST) Sequence TCP 1
10 102 → 2278 [RST] Seq=146 Win=0 Len=0 Sequence TCP
Note The acknowledgment number field is nonzero while the A... Protocol TCP 1
Chat Connection finish (FIN) Sequence TCP 1
Chat Connection establish acknowledge (SYN+ACK): server por... Sequence TCP 1
Chat Connection establish request (SYN): server port 102 Sequence TCP 1
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help
0101 .... = Header Length: 20 bytes (5)
Flags: 0x004 (RST)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .1.. = Reset: Set
[Expert Info (Warning/Sequence): Connection reset (RST)]
[Connection reset (RST)]
[Severity level: Warning]

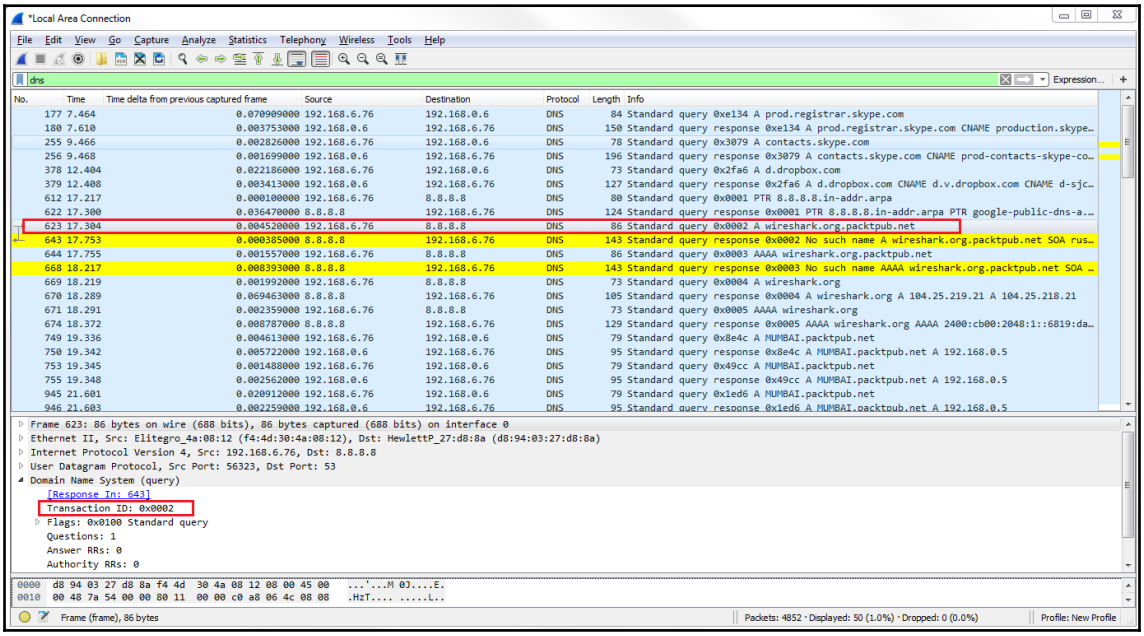
Chapter 06: Introductory Analysis

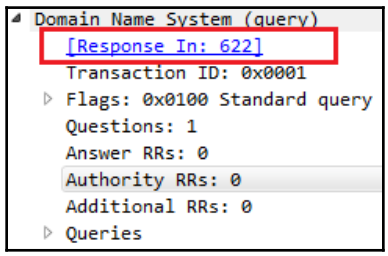


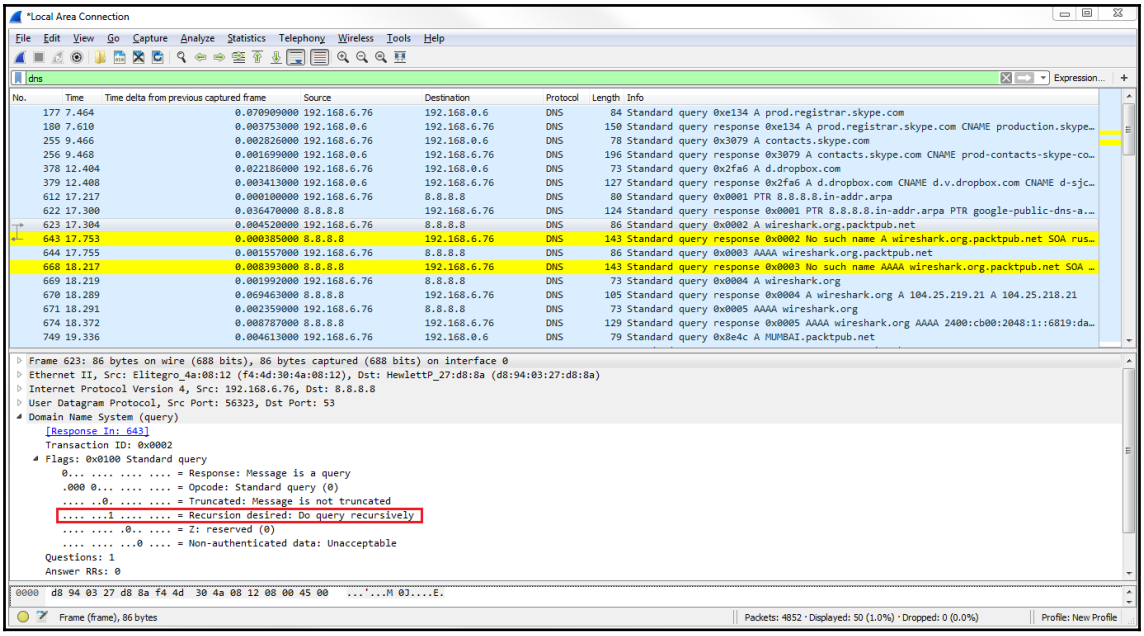

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open
C:\Users\sayalit\Downloads\x400-ping-refuse.pcap (1121 Bytes)
C:\Users\sayalit\Desktop\9041\8.pcapng (298 MB)
C:\Users\sayalit\Desktop\9041\9.pcapng (114 KB)
C:\Users\sayalit\Desktop\9041\10.pcapng (3488 KB)
C:\Users\sayalit\Desktop\9041\6.pcapng (64 MB)
C:\Users\sayalit\Desktop\9041\7.pcapng (142 KB)
C:\Users\sayalit\Documents\packets.pcapng (358 KB)
C:\Users\sayalit\Desktop\9041\5.pcapng (1172 Bytes)
C:\Users\sayalit\Desktop\9041\4.pcapng (37 MB)
C:\Users\sayalit\Desktop\9041\3.pcapng (18 KB)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
VirtualBox Host-Only Network
Local Area Connection
USBPcap1
USBPcap2
USBPcap3
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.4.6 (v2.4.6-0-ge2f395aa12). You receive automatic updates.
Ready to load or capture
No Packets
Profile: New Profile

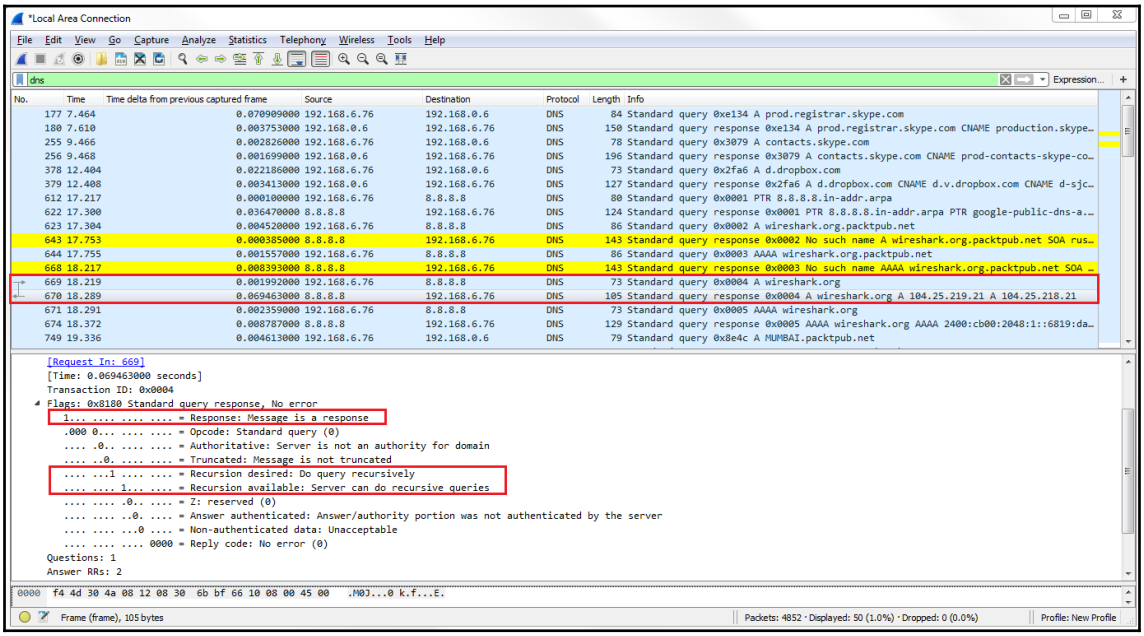

C:\Windows\system32\cmd.exe
C:\Users\sayalit>ipconfig /flushdns
Windows IP Configuration
Successfully flushed the DNS Resolver Cache.
C:\Users\sayalit>nslookup wireshark.org 8.8.8.8
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name: wireshark.org
Addresses: 2400:cb00:2048:1::6819:da15
2400:cb00:2048:1::6819:db15
104.25.219.21
104.25.218.21
C:\Users\sayalit>


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
177 7.464 0.070909000 192.168.6.76 192.168.0.6 DNS 84 Standard query 0xe134 A prod.registrar.skype.com
180 7.610 0.003753000 192.168.0.6 192.168.6.76 DNS 150 Standard query response 0xe134 A prod.registrar.skype.com CNAME production.skype…
255 9.466 0.002826000 192.168.6.76 192.168.0.6 DNS 78 Standard query 0x3079 A contacts.skype.com
256 9.468 0.001699000 192.168.0.6 192.168.6.76 DNS 196 Standard query response 0x3079 A contacts.skype.com CNAME prod-contacts-skype-co…
378 12.404 0.022186000 192.168.6.76 192.168.0.6 DNS 73 Standard query 0x2fa6 A d.dropbox.com
379 12.408 0.003413000 192.168.0.6 192.168.6.76 DNS 127 Standard query response 0x2fa6 A d.dropbox.com CNAME d.v.dropbox.com CNAME d-sjc…
612 17.217 0.000100000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
622 17.300 0.036470000 8.8.8.8 192.168.6.76 DNS 124 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.…
623 17.304 0.004520000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0002 A wireshark.org.packtpub.net
643 17.753 0.000385000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0002 No such name A wireshark.org.packtpub.net SOA rus…
644 17.755 0.001557000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0003 AAAA wireshark.org.packtpub.net
668 18.217 0.008393000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0003 No such name AAAA wireshark.org.packtpub.net SOA …
669 18.219 0.001992000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0004 A wireshark.org
670 18.289 0.069463000 8.8.8.8 192.168.6.76 DNS 105 Standard query response 0x0004 A wireshark.org A 104.25.219.21 A 104.25.218.21
671 18.291 0.002359000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0005 AAAA wireshark.org
674 18.372 0.008787000 8.8.8.8 192.168.6.76 DNS 129 Standard query response 0x0005 AAAA wireshark.org AAAA 2400:cb00:2048:1::6819:da…
749 19.336 0.004613000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x8e4c A MUMBAI.packtpub.net
750 19.342 0.005722000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x8e4c A MUMBAI.packtpub.net A 192.168.0.5
753 19.345 0.001488000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x49cc A MUMBAI.packtpub.net
755 19.348 0.002562000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x49cc A MUMBAI.packtpub.net A 192.168.0.5
945 21.601 0.020912000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x1ed6 A MUMBAI.packtpub.net
946 21.603 0.002259000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x1ed6 A MUMBAI.packtpub.net A 192.168.0.5


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
177 7.464 0.070909000 192.168.6.76 192.168.0.6 DNS 84 Standard query 0xe134 A prod.registrar.skype.com
180 7.610 0.003753000 192.168.0.6 192.168.6.76 DNS 150 Standard query response 0xe134 A prod.registrar.skype.com CNAME production.skype…
255 9.466 0.002826000 192.168.6.76 192.168.0.6 DNS 78 Standard query 0x3079 A contacts.skype.com
256 9.468 0.001699000 192.168.0.6 192.168.6.76 DNS 196 Standard query response 0x3079 A contacts.skype.com CNAME prod-contacts-skype-co…
378 12.404 0.022186000 192.168.6.76 192.168.0.6 DNS 73 Standard query 0x2fa6 A d.dropbox.com
379 12.408 0.003413000 192.168.0.6 192.168.6.76 DNS 127 Standard query response 0x2fa6 A d.dropbox.com CNAME d.v.dropbox.com CNAME d-sjc…
612 17.217 0.000100000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
622 17.300 0.036470000 8.8.8.8 192.168.6.76 DNS 124 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.…
623 17.304 0.004520000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0002 A wireshark.org.packtpub.net
643 17.753 0.000385000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0002 No such name A wireshark.org.packtpub.net SOA rus…
644 17.755 0.001557000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0003 AAAA wireshark.org.packtpub.net
668 18.217 0.008393000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0003 No such name AAAA wireshark.org.packtpub.net SOA …
669 18.219 0.001992000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0004 A wireshark.org
670 18.289 0.069463000 8.8.8.8 192.168.6.76 DNS 105 Standard query response 0x0004 A wireshark.org A 104.25.219.21 A 104.25.218.21
671 18.291 0.002359000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0005 AAAA wireshark.org
674 18.372 0.008787000 8.8.8.8 192.168.6.76 DNS 129 Standard query response 0x0005 AAAA wireshark.org AAAA 2400:cb00:2048:1::6819:da…
749 19.336 0.004613000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x8e4c A MUMBAI.packtpub.net
750 19.342 0.005722000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x8e4c A MUMBAI.packtpub.net A 192.168.0.5
753 19.345 0.001488000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x49cc A MUMBAI.packtpub.net
755 19.348 0.002562000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x49cc A MUMBAI.packtpub.net A 192.168.0.5
945 21.601 0.020912000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x1ed6 A MUMBAI.packtpub.net
946 21.603 0.002259000 192.168.0.6 192.168.6.76 DNS 95 Standard query response 0x1ed6 A MUMBAI.packtpub.net A 192.168.0.5
Frame 623: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Elitegro_4a:08:12 (f4:4d:30:4a:08:12), Dst: HewlettP_27:d8:8a (d8:94:03:27:d8:8a)
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 56323, Dst Port: 53
Domain Name System (query)
[Response In: 643]
Transaction ID: 0x0002
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
0000 d8 94 03 27 d8 8a f4 4d 30 4a 08 12 08 00 45 00 ...'...M 0J....E.
0010 00 48 7a 54 00 00 80 11 00 00 c0 a8 06 4c 08 08 .HzT.... .....L..
Frame (frame), 86 bytes
Packets: 4852 · Displayed: 50 (1.0%) · Dropped: 0 (0.0%)
Profile: New Profile


Domain Name System (query)
[Response In: 622]
Transaction ID: 0x0001
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries

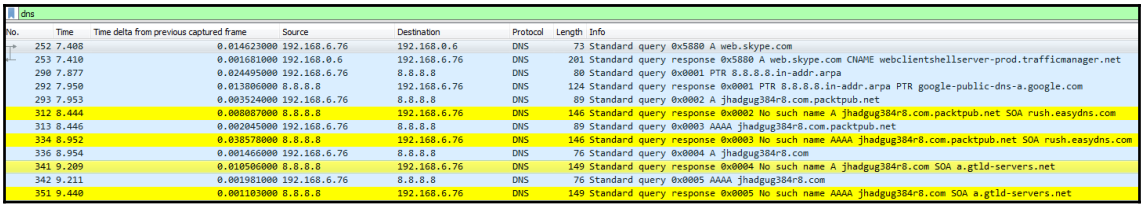

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
177 7.464 0.070909000 192.168.6.76 192.168.0.6 DNS 84 Standard query 0xe134 A prod.registrar.skype.com
180 7.610 0.003753000 192.168.0.6 192.168.6.76 DNS 150 Standard query response 0xe134 A prod.registrar.skype.com CNAME production.skype...
255 9.466 0.002826000 192.168.6.76 192.168.0.6 DNS 78 Standard query 0x3079 A contacts.skype.com
256 9.468 0.001699000 192.168.0.6 192.168.6.76 DNS 196 Standard query response 0x3079 A contacts.skype.com CNAME prod-contacts-skype-co...
378 12.404 0.022186000 192.168.6.76 192.168.0.6 DNS 73 Standard query 0x2fa6 A d.dropbox.com
379 12.408 0.003413000 192.168.0.6 192.168.6.76 DNS 127 Standard query response 0x2fa6 A d.dropbox.com CNAME d.v.dropbox.com CNAME d-sjc...
612 17.217 0.000100000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
622 17.300 0.036470000 8.8.8.8 192.168.6.76 DNS 124 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a...
623 17.304 0.004520000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0002 A wireshark.org.packtpub.net
643 17.753 0.000385000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0002 No such name A wireshark.org.packtpub.net SOA rus...
644 17.755 0.001557000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0003 AAAA wireshark.org.packtpub.net
668 18.217 0.008393000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0003 No such name AAAA wireshark.org.packtpub.net SOA ...
669 18.219 0.001992000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0004 A wireshark.org
670 18.289 0.069463000 8.8.8.8 192.168.6.76 DNS 105 Standard query response 0x0004 A wireshark.org A 104.25.219.21 A 104.25.218.21
671 18.291 0.002359000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0005 AAAA wireshark.org
674 18.372 0.008787000 8.8.8.8 192.168.6.76 DNS 129 Standard query response 0x0005 AAAA wireshark.org AAAA 2400:cb00:2048:1::6819:da...
749 19.336 0.004613000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x8e4c A MUMBAI.packtpub.net
Frame 623: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: Elitegro_4a:08:12 (f4:4d:30:4a:08:12), Dst: HewlettP_27:d8:8a (d8:94:03:27:d8:8a)
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 56323, Dst Port: 53
Domain Name System (query)
[Response In: 643]
Transaction ID: 0x0002
Flags: 0x0100 Standard query
0... .... = Response: Message is a query
.000 0... .... = Opcode: Standard query (0)
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... .0.. .... = Z: reserved (0)
....0 .... = Non-authenticated data: Unacceptable
Questions: 1
Answer RRs: 0
0000 d8 94 03 27 d8 8a f4 4d 30 4a 08 12 08 00 45 00 ...'...M 0J....E.
Frame (frame), 86 bytes
Packets: 4852 · Displayed: 50 (1.0%) · Dropped: 0 (0.0%)
Profile: New Profile

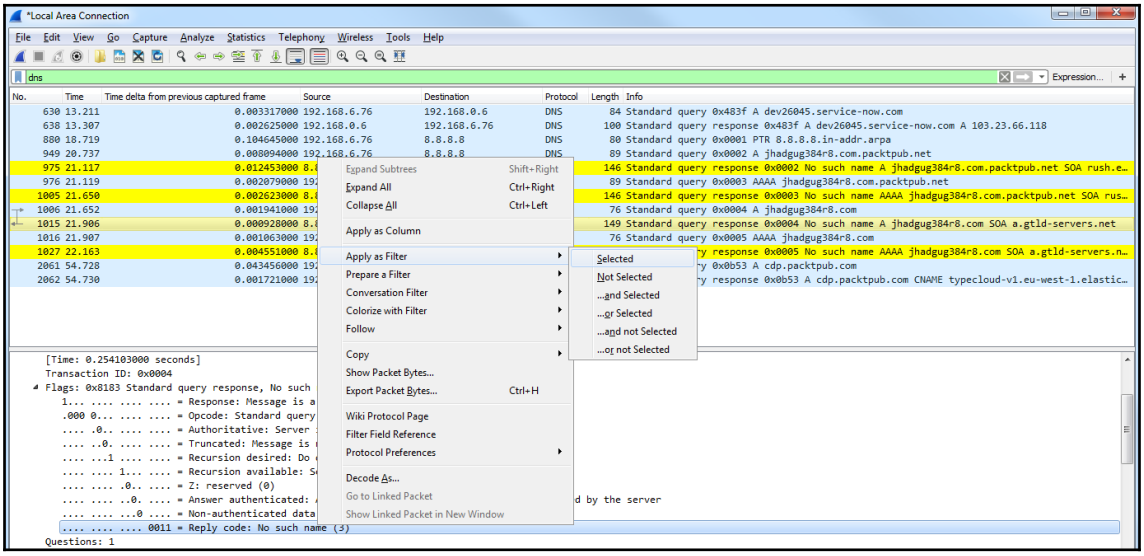

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
177 7.464 0.070909000 192.168.6.76 192.168.0.6 DNS 84 Standard query 0xe134 A prod.registrar.skype.com
180 7.610 0.003753000 192.168.0.6 192.168.6.76 DNS 150 Standard query response 0xe134 A prod.registrar.skype.com CNAME production.skype...
255 9.466 0.002826000 192.168.6.76 192.168.0.6 DNS 78 Standard query 0x3079 A contacts.skype.com
256 9.468 0.001699000 192.168.0.6 192.168.6.76 DNS 196 Standard query response 0x3079 A contacts.skype.com CNAME prod-contacts-skype-co...
378 12.404 0.022186000 192.168.6.76 192.168.0.6 DNS 73 Standard query 0x2fa6 A d.dropbox.com
379 12.408 0.003413000 192.168.0.6 192.168.6.76 DNS 127 Standard query response 0x2fa6 A d.dropbox.com CNAME d.v.dropbox.com CNAME d-sjc...
612 17.217 0.000100000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
622 17.300 0.036470000 8.8.8.8 192.168.6.76 DNS 124 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a...
623 17.304 0.004520000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0002 A wireshark.org.packtpub.net
643 17.753 0.000385000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0002 No such name A wireshark.org.packtpub.net SOA rus...
644 17.755 0.001557000 192.168.6.76 8.8.8.8 DNS 86 Standard query 0x0003 AAAA wireshark.org.packtpub.net
668 18.217 0.008393000 8.8.8.8 192.168.6.76 DNS 143 Standard query response 0x0003 No such name AAAA wireshark.org.packtpub.net SOA ...
669 18.219 0.001992000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0004 A wireshark.org
670 18.289 0.069463000 8.8.8.8 192.168.6.76 DNS 105 Standard query response 0x0004 A wireshark.org A 104.25.219.21 A 104.25.218.21
671 18.291 0.002359000 192.168.6.76 8.8.8.8 DNS 73 Standard query 0x0005 AAAA wireshark.org
674 18.372 0.008787000 8.8.8.8 192.168.6.76 DNS 129 Standard query response 0x0005 AAAA wireshark.org AAAA 2400:cb00:2048:1::6819:da...
749 19.336 0.004613000 192.168.6.76 192.168.0.6 DNS 79 Standard query 0x8e4c A MUMBAI.packtpub.net
[Request In: 669]
[Time: 0.069463000 seconds]
Transaction ID: 0x0004
Flags: 0x8180 Standard query response, No error
1... .... = Response: Message is a response
.000 0... .... = Opcode: Standard query (0)
.... .0.. .... = Authoritative: Server is not an authority for domain
.... ..0. .... = Truncated: Message is not truncated
....1 .... = Recursion desired: Do query recursively
.... 1... .... = Recursion available: Server can do recursive queries
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated: Answer/authority portion was not authenticated by the server
....0 .... = Non-authenticated data: Unacceptable
.... 0000 = Reply code: No error (0)
Questions: 1
Answer RRs: 2
0000 f4 4d 30 4a 08 12 08 30 6b bf 66 10 08 00 45 00 .M0J...0 k.f...E.
Frame (frame), 105 bytes
Packets: 4852 · Displayed: 50 (1.0%) · Dropped: 0 (0.0%)
Profile: New Profile

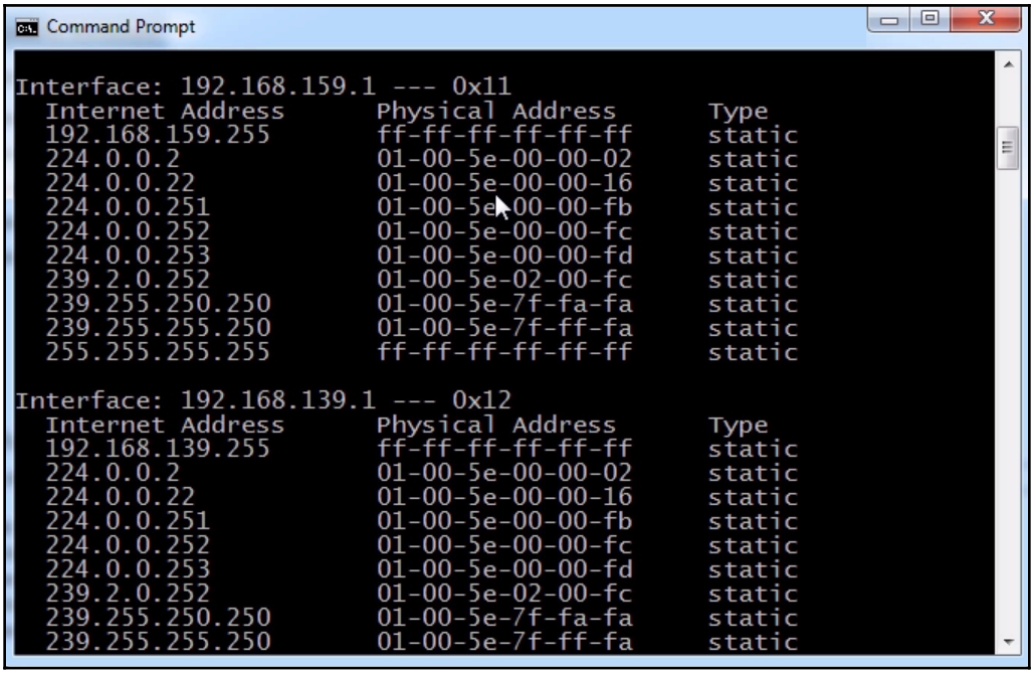
```
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
```

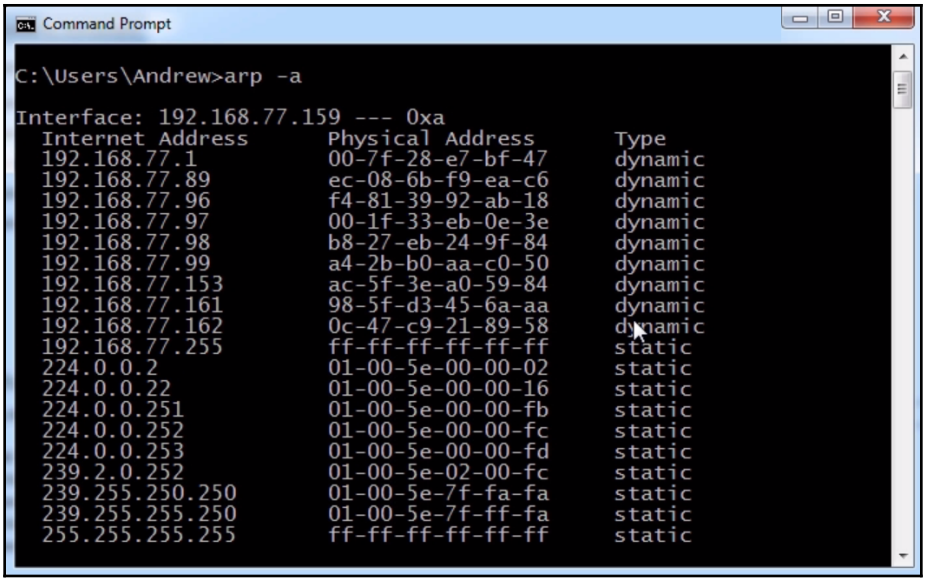
```
▲ Queries
  ▲ wireshark.org: type A, class IN
      Name: wireshark.org
      [Name Length: 13]
      [Label Count: 2]
      Type: A (Host Address) (1)
      Class: IN (0x0001)
▲ Answers
  ▲ wireshark.org: type A, class IN, addr 104.25.219.21
      Name: wireshark.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 299
      Data length: 4
      Address: 104.25.219.21
  ▲ wireshark.org: type A, class IN, addr 104.25.218.21
      Name: wireshark.org
      Type: A (Host Address) (1)
      Class: IN (0x0001)
      Time to live: 299
      Data length: 4
      Address: 104.25.218.21
```

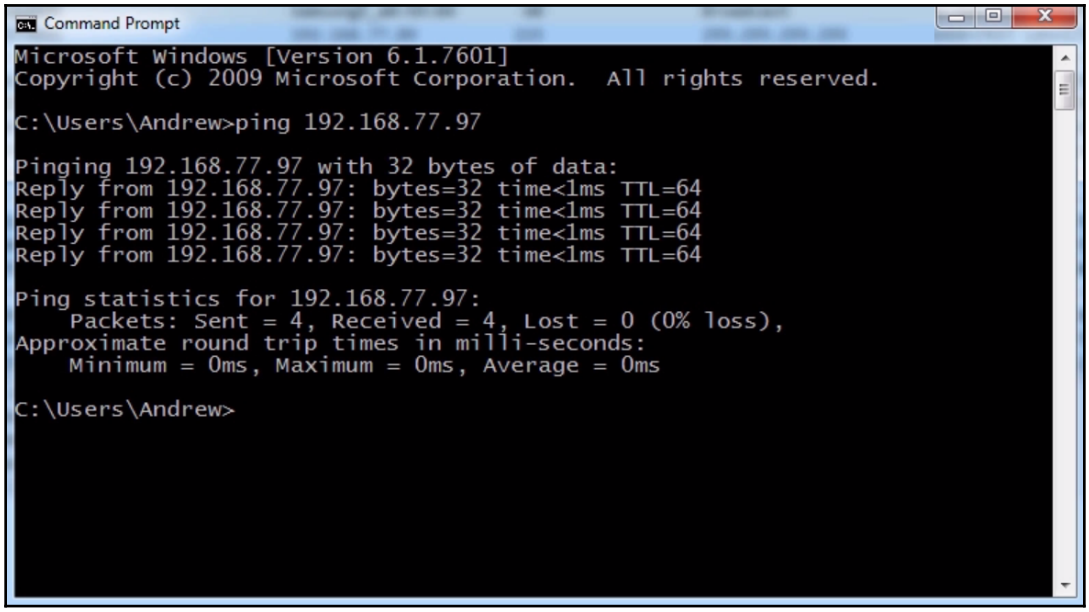
```
C:\Users\sayalit>nslookup jhadgug384r8.com 8.8.8.8
```

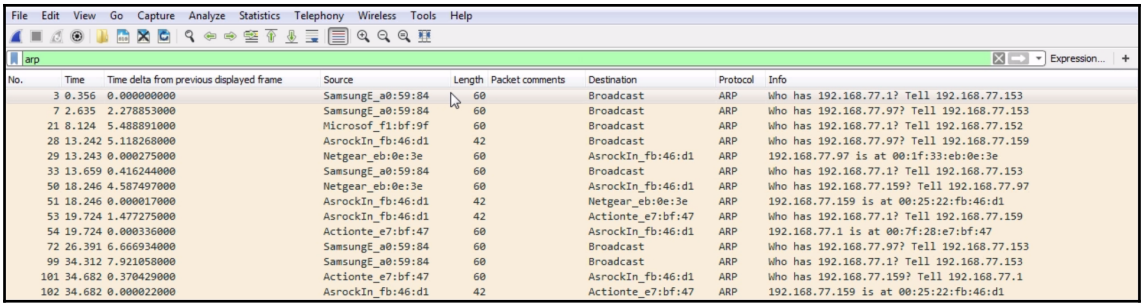

dns
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
252 7.408 0.014623000 192.168.6.76 192.168.0.6 DNS 73 Standard query 0x5880 A web.skype.com
253 7.410 0.001681000 192.168.0.6 192.168.6.76 DNS 201 Standard query response 0x5880 A web.skype.com CNAME webclientshellserver-prod.trafficmanager.net
290 7.877 0.024495000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
292 7.950 0.013806000 8.8.8.8 192.168.6.76 DNS 124 Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns-a.google.com
293 7.953 0.003524000 192.168.6.76 8.8.8.8 DNS 89 Standard query 0x0002 A jhadgug384r8.com.packtpub.net
312 8.444 0.008087000 8.8.8.8 192.168.6.76 DNS 146 Standard query response 0x0002 No such name A jhadgug384r8.com.packtpub.net SOA rush.easydns.com
313 8.446 0.002045000 192.168.6.76 8.8.8.8 DNS 89 Standard query 0x0003 AAAA jhadgug384r8.com.packtpub.net
334 8.952 0.038578000 8.8.8.8 192.168.6.76 DNS 146 Standard query response 0x0003 No such name AAAA jhadgug384r8.com.packtpub.net SOA rush.easydns.com
336 8.954 0.001466000 192.168.6.76 8.8.8.8 DNS 76 Standard query 0x0004 A jhadgug384r8.com
341 9.209 0.010506000 8.8.8.8 192.168.6.76 DNS 149 Standard query response 0x0004 No such name A jhadgug384r8.com SOA a.gtld-servers.net
342 9.211 0.001981000 192.168.6.76 8.8.8.8 DNS 76 Standard query 0x0005 AAAA jhadgug384r8.com
351 9.440 0.001103000 8.8.8.8 192.168.6.76 DNS 149 Standard query response 0x0005 No such name AAAA jhadgug384r8.com SOA a.gtld-servers.net

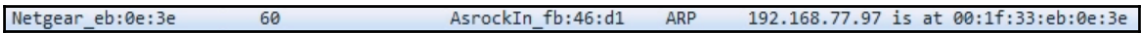

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
630 13.211 0.003317000 192.168.6.76 192.168.0.6 DNS 84 Standard query 0x483f A dev26045.service-now.com
638 13.307 0.002625000 192.168.0.6 192.168.6.76 DNS 100 Standard query response 0x483f A dev26045.service-now.com A 103.23.66.118
880 18.719 0.104645000 192.168.6.76 8.8.8.8 DNS 80 Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
949 20.737 0.008094000 192.168.6.76 8.8.8.8 DNS 89 Standard query 0x0002 A jhadgug384r8.com.packtpub.net
975 21.117 0.012453000 8.8
976 21.119 0.002079000 19
1005 21.650 0.002623000 8.8
1006 21.652 0.001941000 19
1015 21.906 0.000928000 8.8
1016 21.907 0.001063000 19
1027 22.163 0.004551000 8.8
2061 54.728 0.043456000 19
2062 54.730 0.001721000 19
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
[Time: 0.254103000 seconds]
Transaction ID: 0x0004
Flags: 0x8183 Standard query response, No such
1... .... = Response: Message is a
.000 0... .... = Opcode: Standard query
.... .0.. .... = Authoritative: Server
.... ..0. .... = Truncated: Message is
....1 .... = Recursion desired: Do
.... 1... .... = Recursion available: S
.... .0.. .... = Z: reserved (0)
....0. .... = Answer authenticated:
....0 .... = Non-authenticated data
.... 0011 = Reply code: No such name (3)
Questions: 1

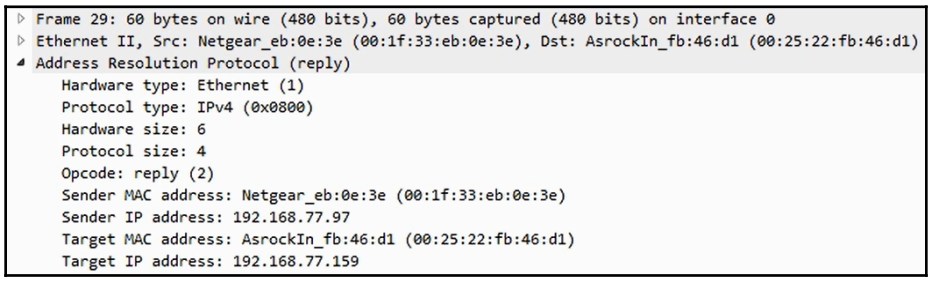

Command Prompt
Interface: 192.168.159.1 --- 0x11
Internet Address Physical Address Type
192.168.159.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
224.0.0.253 01-00-5e-00-00-fd static
239.2.0.252 01-00-5e-02-00-fc static
239.255.250.250 01-00-5e-7f-fa-fa static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 192.168.139.1 --- 0x12
Internet Address Physical Address Type
192.168.139.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
224.0.0.253 01-00-5e-00-00-fd static
239.2.0.252 01-00-5e-02-00-fc static
239.255.250.250 01-00-5e-7f-fa-fa static
239.255.255.250 01-00-5e-7f-ff-fa static

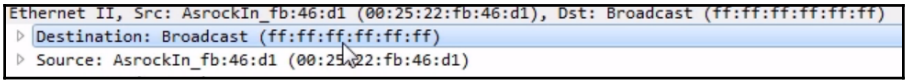

Command Prompt
C:\Users\Andrew>arp -a
Interface: 192.168.77.159 --- 0xa
Internet Address Physical Address Type
192.168.77.1 00-7f-28-e7-bf-47 dynamic
192.168.77.89 ec-08-6b-f9-ea-c6 dynamic
192.168.77.96 f4-81-39-92-ab-18 dynamic
192.168.77.97 00-1f-33-eb-0e-3e dynamic
192.168.77.98 b8-27-eb-24-9f-84 dynamic
192.168.77.99 a4-2b-b0-aa-c0-50 dynamic
192.168.77.153 ac-5f-3e-a0-59-84 dynamic
192.168.77.161 98-5f-d3-45-6a-aa dynamic
192.168.77.162 0c-47-c9-21-89-58 dynamic
192.168.77.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
224.0.0.253 01-00-5e-00-00-fd static
239.2.0.252 01-00-5e-02-00-fc static
239.255.250.250 01-00-5e-7f-fa-fa static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static

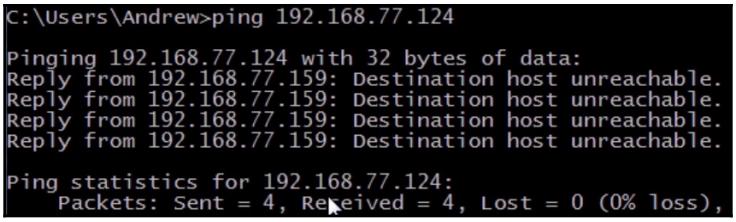

Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Andrew>ping 192.168.77.97
Pinging 192.168.77.97 with 32 bytes of data:
Reply from 192.168.77.97: bytes=32 time<1ms TTL=64
Reply from 192.168.77.97: bytes=32 time<1ms TTL=64
Reply from 192.168.77.97: bytes=32 time<1ms TTL=64
Reply from 192.168.77.97: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.77.97:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Andrew>

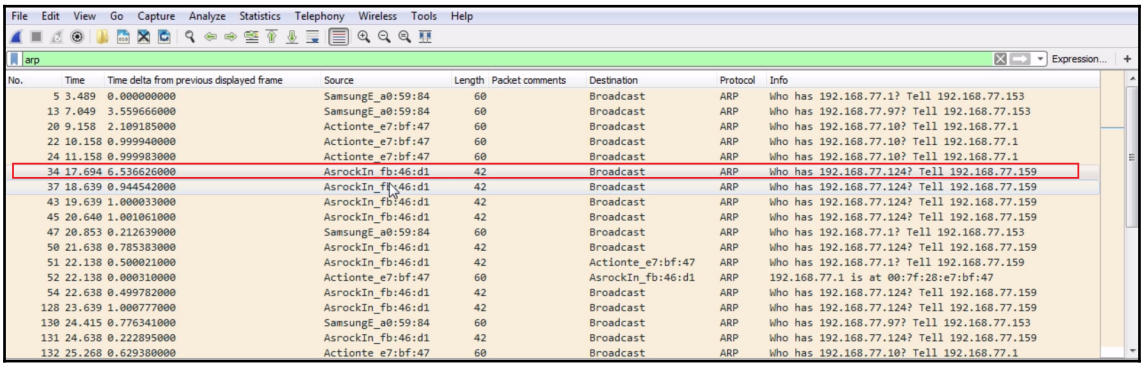

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
3 0.356 0.000000000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
7 2.635 2.278853000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.153
21 8.124 5.488891000 Microsof_f1:bf:9f 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.152
28 13.242 5.118268000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.159
29 13.243 0.000275000 Netgear_eb:0e:3e 60 AsrockIn_fb:46:d1 ARP 192.168.77.97 is at 00:1f:33:eb:0e:3e
33 13.659 0.416244000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
50 18.246 4.587497000 Netgear_eb:0e:3e 60 AsrockIn_fb:46:d1 ARP Who has 192.168.77.159? Tell 192.168.77.97
51 18.246 0.000017000 AsrockIn_fb:46:d1 42 Netgear_eb:0e:3e ARP 192.168.77.159 is at 00:25:22:fb:46:d1
53 19.724 1.477275000 AsrockIn_fb:46:d1 42 Actionte_e7:bf:47 ARP Who has 192.168.77.1? Tell 192.168.77.159
54 19.724 0.000336000 Actionte_e7:bf:47 60 AsrockIn_fb:46:d1 ARP 192.168.77.1 is at 00:7f:28:e7:bf:47
72 26.391 6.666934000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.153
99 34.312 7.921058000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
101 34.682 0.370429000 Actionte_e7:bf:47 60 AsrockIn_fb:46:d1 ARP Who has 192.168.77.159? Tell 192.168.77.1
102 34.682 0.000022000 AsrockIn_fb:46:d1 42 Actionte_e7:bf:47 ARP 192.168.77.159 is at 00:25:22:fb:46:d1

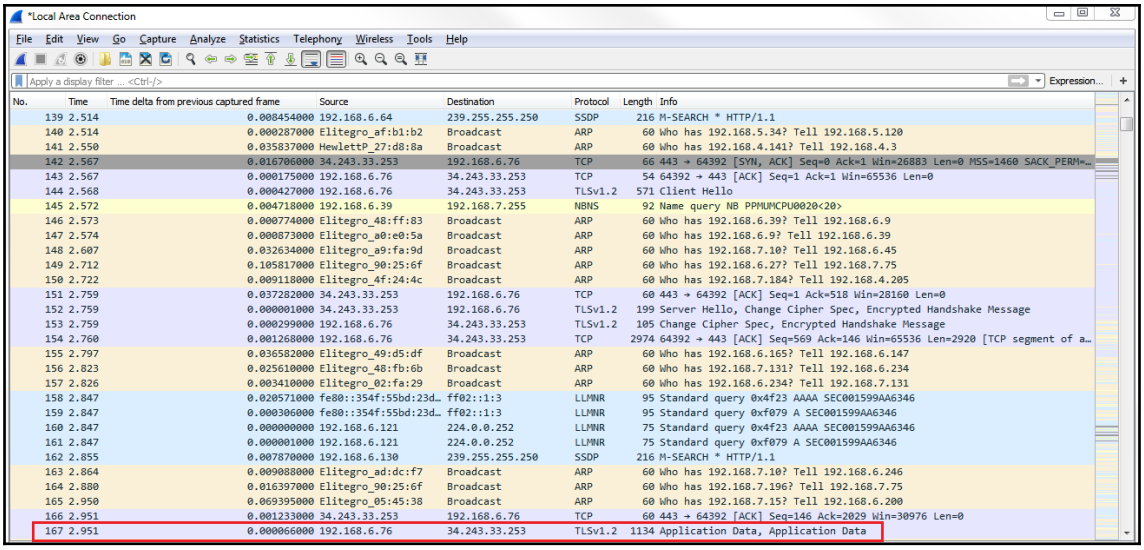

Netgear_eb:0e:3e 60 AsrockIn_fb:46:d1 ARP 192.168.77.97 is at 00:1f:33:eb:0e:3e


Frame 29: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Netgear_eb:0e:3e (00:1f:33:eb:0e:3e), Dst: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1)
Address Resolution Protocol (reply)
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (2)
Sender MAC address: Netgear_eb:0e:3e (00:1f:33:eb:0e:3e)
Sender IP address: 192.168.77.97
Target MAC address: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1)
Target IP address: 192.168.77.159


Ethernet II, Src: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Source: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1)


C:\Users\Andrew>ping 192.168.77.124
Pinging 192.168.77.124 with 32 bytes of data:
Reply from 192.168.77.159: Destination host unreachable.
Reply from 192.168.77.159: Destination host unreachable.
Reply from 192.168.77.159: Destination host unreachable.
Reply from 192.168.77.159: Destination host unreachable.
Ping statistics for 192.168.77.124:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

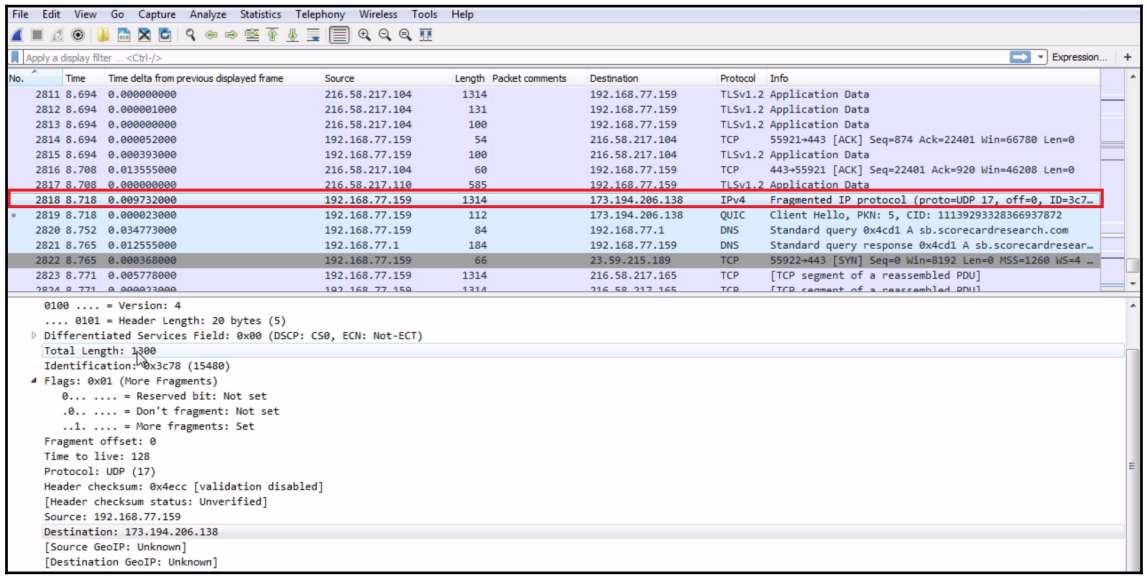

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
5 3.489 0.000000000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
13 7.049 3.559666000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.153
20 9.158 2.109185000 Actionte_e7:bf:47 60 Broadcast ARP Who has 192.168.77.10? Tell 192.168.77.1
22 10.158 0.999940000 Actionte_e7:bf:47 60 Broadcast ARP Who has 192.168.77.10? Tell 192.168.77.1
24 11.158 0.999983000 Actionte_e7:bf:47 60 Broadcast ARP Who has 192.168.77.10? Tell 192.168.77.1
34 17.694 6.536626000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
37 18.639 0.944542000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
43 19.639 1.000033000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
45 20.640 1.001061000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
47 20.853 0.212639000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
50 21.638 0.785383000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
51 22.138 0.500021000 AsrockIn_fb:46:d1 42 Actionte_e7:bf:47 ARP Who has 192.168.77.1? Tell 192.168.77.159
52 22.138 0.000310000 Actionte_e7:bf:47 60 AsrockIn_fb:46:d1 ARP 192.168.77.1 is at 00:7f:28:e7:bf:47
54 22.638 0.499782000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
128 23.639 1.000777000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
130 24.415 0.776341000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.153
131 24.638 0.222895000 AsrockIn_fb:46:d1 42 Broadcast ARP Who has 192.168.77.124? Tell 192.168.77.159
132 25.268 0.629380000 Actionte_e7:bf:47 60 Broadcast ARP Who has 192.168.77.10? Tell 192.168.77.1

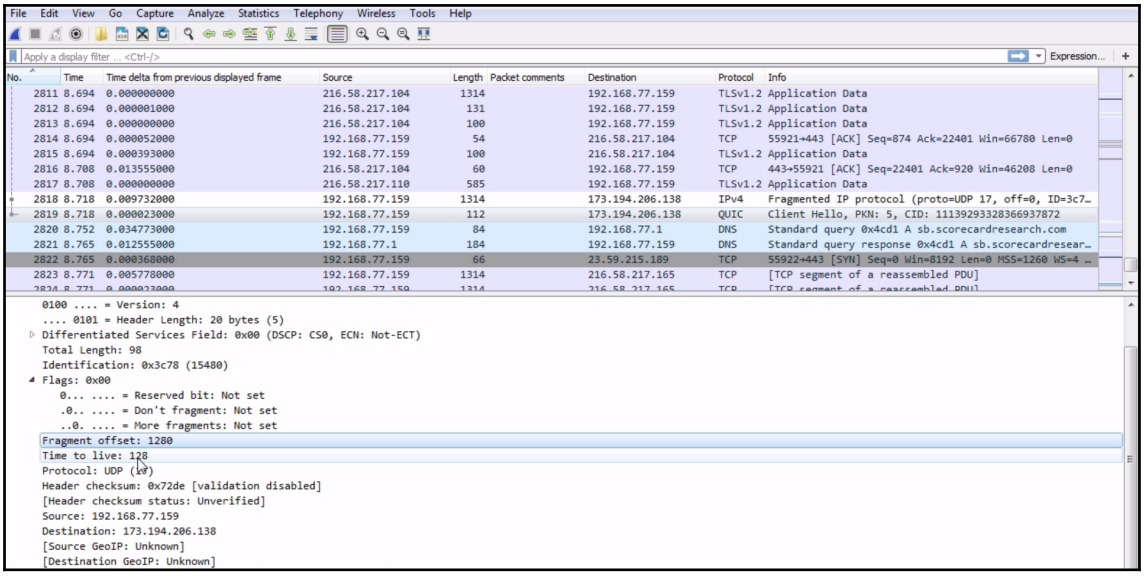

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
139 2.514 0.008454000 192.168.6.64 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
140 2.514 0.000287000 Elitegro_af:b1:b2 Broadcast ARP 60 Who has 192.168.5.34? Tell 192.168.5.120
141 2.550 0.035837000 HewlettP_27:d8:8a Broadcast ARP 60 Who has 192.168.4.141? Tell 192.168.4.3
142 2.567 0.016706000 34.243.33.253 192.168.6.76 TCP 66 443 → 64392 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0 MSS=1460 SACK_PERM=…
143 2.567 0.000175000 192.168.6.76 34.243.33.253 TCP 54 64392 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
144 2.568 0.000427000 192.168.6.76 34.243.33.253 TLSv1.2 571 Client Hello
145 2.572 0.004718000 192.168.6.39 192.168.7.255 NBNS 92 Name query NB PPMUMCPU0020<20>
146 2.573 0.000774000 Elitegro_48:ff:83 Broadcast ARP 60 Who has 192.168.6.39? Tell 192.168.6.9
147 2.574 0.000873000 Elitegro_a0:e0:5a Broadcast ARP 60 Who has 192.168.6.9? Tell 192.168.6.39
148 2.607 0.032634000 Elitegro_a9:fa:9d Broadcast ARP 60 Who has 192.168.7.10? Tell 192.168.6.45
149 2.712 0.105817000 Elitegro_90:25:6f Broadcast ARP 60 Who has 192.168.6.27? Tell 192.168.7.75
150 2.722 0.009118000 Elitegro_4f:24:4c Broadcast ARP 60 Who has 192.168.7.184? Tell 192.168.4.205
151 2.759 0.037282000 34.243.33.253 192.168.6.76 TCP 60 443 → 64392 [ACK] Seq=1 Ack=518 Win=28160 Len=0
152 2.759 0.000001000 34.243.33.253 192.168.6.76 TLSv1.2 199 Server Hello, Change Cipher Spec, Encrypted Handshake Message
153 2.759 0.000299000 192.168.6.76 34.243.33.253 TLSv1.2 105 Change Cipher Spec, Encrypted Handshake Message
154 2.760 0.001268000 192.168.6.76 34.243.33.253 TCP 2974 64392 → 443 [ACK] Seq=569 Ack=146 Win=65536 Len=2920 [TCP segment of a…
155 2.797 0.036582000 Elitegro_49:d5:df Broadcast ARP 60 Who has 192.168.6.165? Tell 192.168.6.147
156 2.823 0.025610000 Elitegro_48:fb:6b Broadcast ARP 60 Who has 192.168.7.131? Tell 192.168.6.234
157 2.826 0.003410000 Elitegro_02:fa:29 Broadcast ARP 60 Who has 192.168.6.234? Tell 192.168.7.131
158 2.847 0.020571000 fe80::354f:55bd:23d… ff02::1:3 LLMNR 95 Standard query 0x4f23 AAAA SEC001599AA6346
159 2.847 0.000306000 fe80::354f:55bd:23d… ff02::1:3 LLMNR 95 Standard query 0xf079 A SEC001599AA6346
160 2.847 0.000000000 192.168.6.121 224.0.0.252 LLMNR 75 Standard query 0x4f23 AAAA SEC001599AA6346
161 2.847 0.000001000 192.168.6.121 224.0.0.252 LLMNR 75 Standard query 0xf079 A SEC001599AA6346
162 2.855 0.007870000 192.168.6.130 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
163 2.864 0.009088000 Elitegro_ad:dc:f7 Broadcast ARP 60 Who has 192.168.7.10? Tell 192.168.6.246
164 2.880 0.016397000 Elitegro_90:25:6f Broadcast ARP 60 Who has 192.168.7.196? Tell 192.168.7.75
165 2.950 0.069395000 Elitegro_05:45:38 Broadcast ARP 60 Who has 192.168.7.15? Tell 192.168.6.200
166 2.951 0.001233000 34.243.33.253 192.168.6.76 TCP 60 443 → 64392 [ACK] Seq=146 Ack=2029 Win=30976 Len=0
167 2.951 0.000066000 192.168.6.76 34.243.33.253 TLSv1.2 1134 Application Data, Application Data

```
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 34.243.33.253
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 1120
    Identification: 0x2ddf (11743)
  ▷ Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.6.76
    Destination: 34.243.33.253
```

```
Flags: 0x4000, Don't fragment
    0... .... .... .... = Reserved bit: Not set
    .1.. .... .... .... = Don't fragment: Set
    ..0. .... .... .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment offset: 0
```

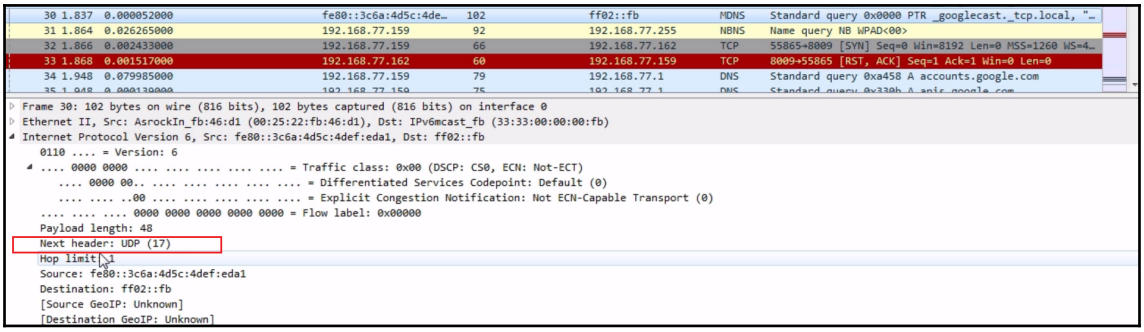
```
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.6.76
Destination: 34.243.33.253
```

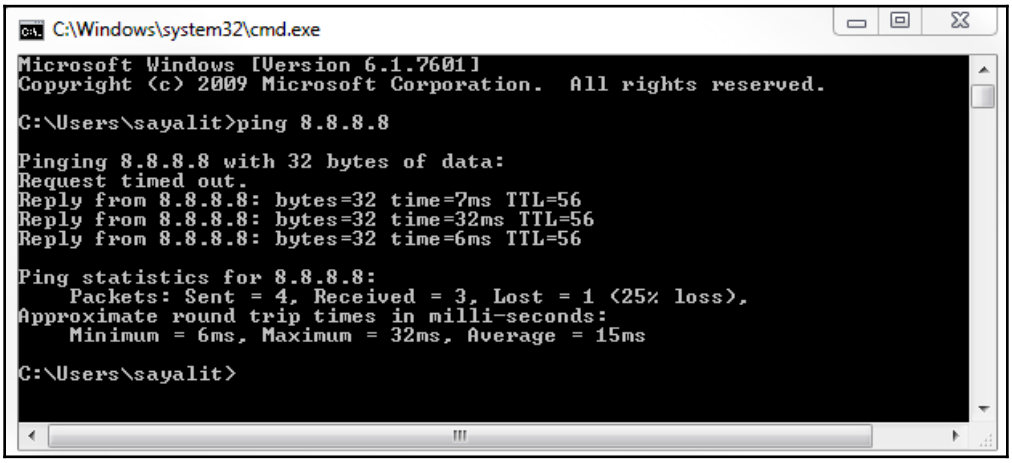


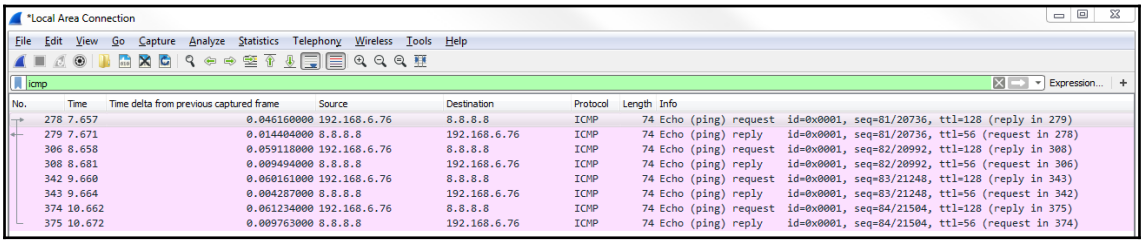



```
[2 IPv4 Fragments (1358 bytes): #2818(1280), #2819(78)]
    [Frame: 2818, payload: 0-1279 (1280 bytes)]
    [Frame: 2819, payload: 1280-1357 (78 bytes)]
    [Fragment count: 2]
    [Reassembled IPv4 length: 1358]
```

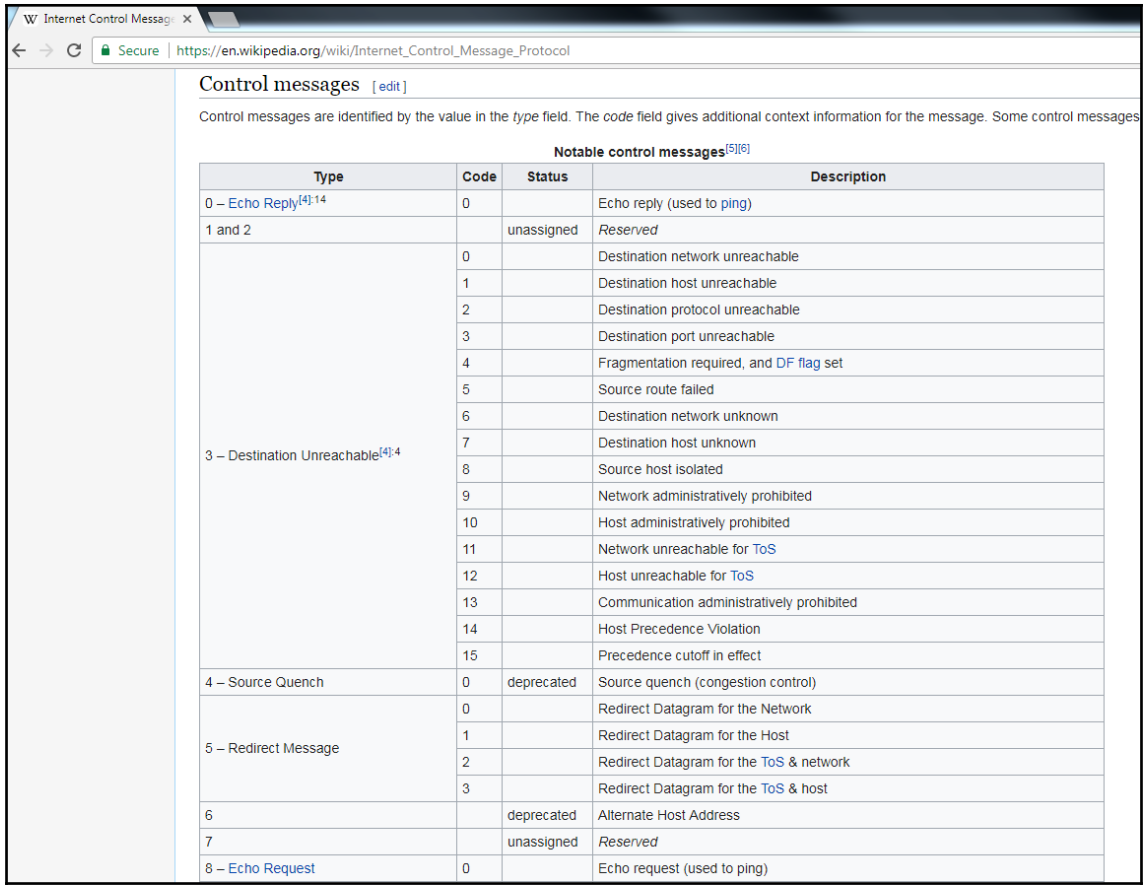
```
Flags: 0x01 (More Fragments)
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..1. .... = More fragments: Set
  Fragment offset: 0
  Time to live: 128
  Protocol: UDP (17)
  Header checksum: 0x4ecc [validation disabled]
  [Header checksum status: Unverified]
  Source: 192.168.77.159
  Destination: 173.194.206.138
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  Reassembled IPv4 in frame: 2819
```


30 1.837 0.000052000 fe80::3c6a:4d5c:4de… 102 ff02::fb MDNS Standard query 0x0000 PTR _googlecast._tcp.local, "…
31 1.864 0.026265000 192.168.77.159 92 192.168.77.255 NBNS Name query NB WPAD<00>
32 1.866 0.002433000 192.168.77.159 66 192.168.77.162 TCP 55865+8009 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4…
33 1.868 0.001517000 192.168.77.162 60 192.168.77.159 TCP 8009+55865 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
34 1.948 0.079985000 192.168.77.159 79 192.168.77.1 DNS Standard query 0xa458 A accounts.google.com
Frame 30: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
Ethernet II, Src: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1), Dst: IPv6mcast_fb (33:33:00:00:00:fb)
Internet Protocol Version 6, Src: fe80::3c6a:4d5c:4def:eda1, Dst: ff02::fb
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0000 00.. .... = Differentiated Services Codepoint: Default (0)
....00 .... = Explicit Congestion Notification: Not ECN-Capable Transport (0)
.... 0000 0000 0000 0000 0000 = Flow label: 0x00000
Payload length: 48
Next header: UDP (17)
Hop limit: 1
Source: fe80::3c6a:4d5c:4def:eda1
Destination: ff02::fb
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\sayalit>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Reply from 8.8.8.8: bytes=32 time=7ms TTL=56
Reply from 8.8.8.8: bytes=32 time=32ms TTL=56
Reply from 8.8.8.8: bytes=32 time=6ms TTL=56
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 6ms, Maximum = 32ms, Average = 15ms
C:\Users\sayalit>


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression…
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
278 7.657 0.046160000 192.168.6.76 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (reply in 279)
279 7.671 0.014404000 8.8.8.8 192.168.6.76 ICMP 74 Echo (ping) reply id=0x0001, seq=81/20736, ttl=56 (request in 278)
306 8.658 0.059118000 192.168.6.76 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=82/20992, ttl=128 (reply in 308)
308 8.681 0.009494000 8.8.8.8 192.168.6.76 ICMP 74 Echo (ping) reply id=0x0001, seq=82/20992, ttl=56 (request in 306)
342 9.660 0.060161000 192.168.6.76 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=83/21248, ttl=128 (reply in 343)
343 9.664 0.004287000 8.8.8.8 192.168.6.76 ICMP 74 Echo (ping) reply id=0x0001, seq=83/21248, ttl=56 (request in 342)
374 10.662 0.061234000 192.168.6.76 8.8.8.8 ICMP 74 Echo (ping) request id=0x0001, seq=84/21504, ttl=128 (reply in 375)
375 10.672 0.009763000 8.8.8.8 192.168.6.76 ICMP 74 Echo (ping) reply id=0x0001, seq=84/21504, ttl=56 (request in 374)

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d0a [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 81 (0x0051)
    Sequence number (LE): 20736 (0x5100)
    [Response frame: 279]
  ▷ Data (32 bytes)
```



Internet Control Messag

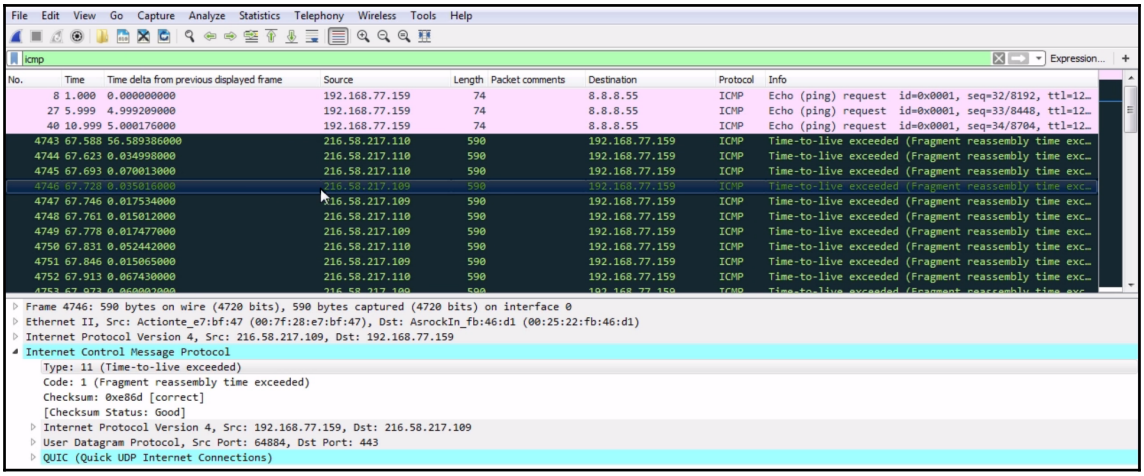
Secure | https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

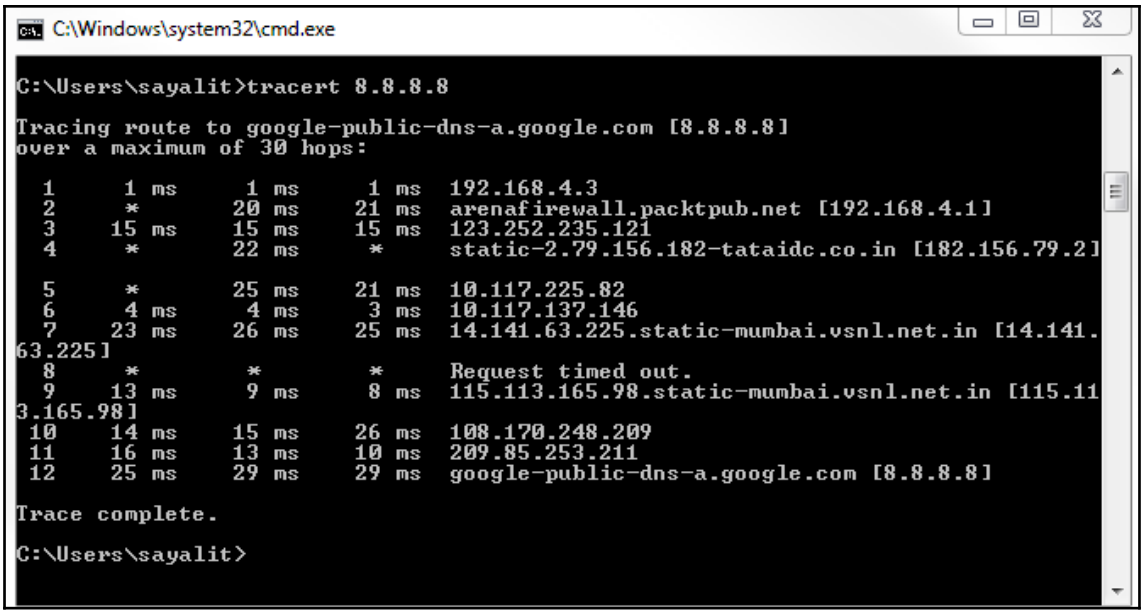
Control messages [edit]

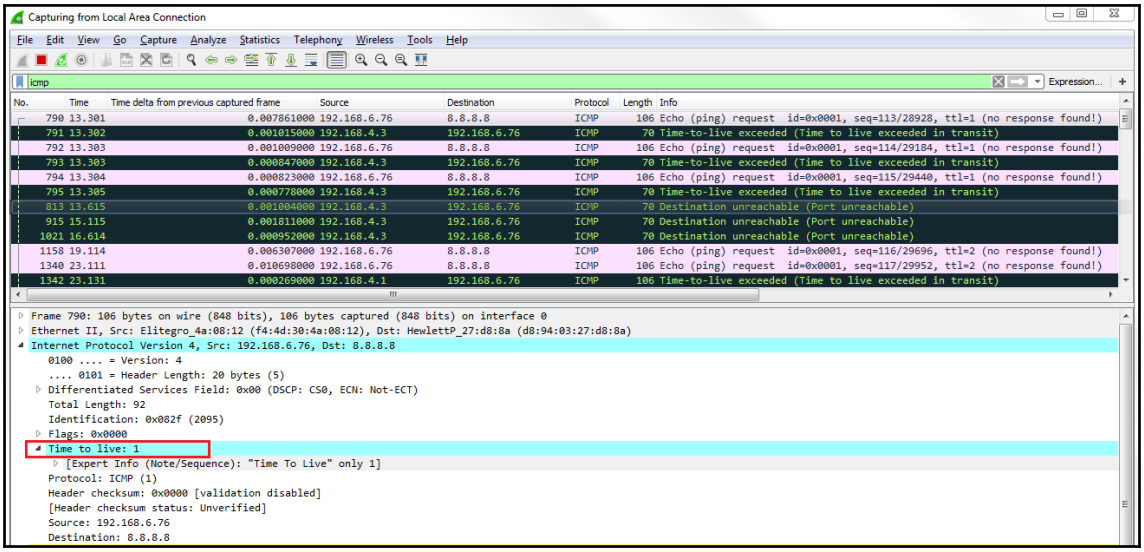
Control messages are identified by the value in the *type* field. The *code* field gives additional context information for the message. Some control messages

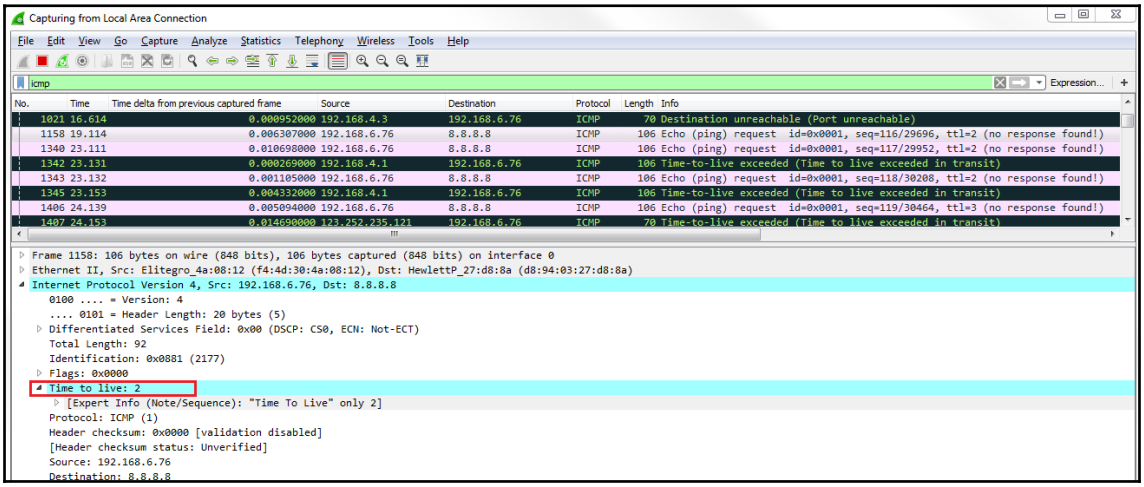
Notable control messages[5][6]

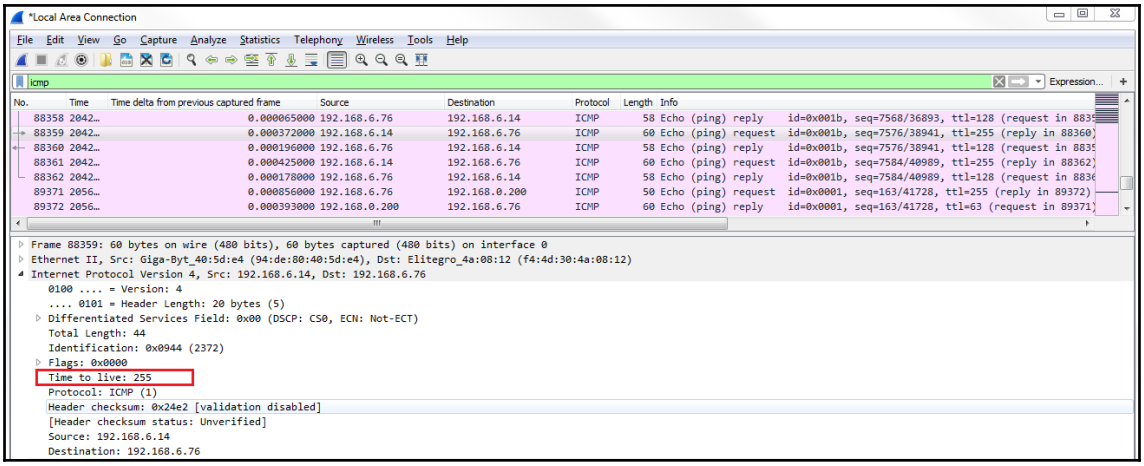
Type	Code	Status	Description
0 – Echo Reply[4]:14	0		Echo reply (used to ping)
1 and 2		unassigned	*Reserved*
3 – Destination Unreachable[4]:4	0		Destination network unreachable
	1		Destination host unreachable
	2		Destination protocol unreachable
	3		Destination port unreachable
	4		Fragmentation required, and DF flag set
	5		Source route failed
	6		Destination network unknown
	7		Destination host unknown
	8		Source host isolated
	9		Network administratively prohibited
	10		Host administratively prohibited
	11		Network unreachable for ToS
	12		Host unreachable for ToS
	13		Communication administratively prohibited
	14		Host Precedence Violation
	15		Precedence cutoff in effect
4 – Source Quench	0	deprecated	Source quench (congestion control)
5 – Redirect Message	0		Redirect Datagram for the Network
	1		Redirect Datagram for the Host
	2		Redirect Datagram for the ToS & network
	3		Redirect Datagram for the ToS & host
6		deprecated	Alternate Host Address
7		unassigned	*Reserved*
8 – Echo Request	0		Echo request (used to ping)


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
8 1.000 0.000000000 192.168.77.159 74 8.8.8.55 ICMP Echo (ping) request id=0x0001, seq=32/8192, ttl=12…
27 5.999 4.999209000 192.168.77.159 74 8.8.8.55 ICMP Echo (ping) request id=0x0001, seq=33/8448, ttl=12…
40 10.999 5.000176000 192.168.77.159 74 8.8.8.55 ICMP Echo (ping) request id=0x0001, seq=34/8704, ttl=12…
4743 67.588 56.589386000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4744 67.623 0.034998000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4745 67.693 0.070013000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4746 67.728 0.035016000 216.58.217.109 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4747 67.746 0.017534000 216.58.217.109 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4748 67.761 0.015012000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4749 67.778 0.017477000 216.58.217.109 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4750 67.831 0.052442000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4751 67.846 0.015065000 216.58.217.109 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
4752 67.913 0.067430000 216.58.217.110 590 192.168.77.159 ICMP Time-to-live exceeded (Fragment reassembly time exc…
Frame 4746: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
Ethernet II, Src: Actionte_e7:bf:47 (00:7f:28:e7:bf:47), Dst: AsrockIn_fb:46:d1 (00:25:22:fb:46:d1)
Internet Protocol Version 4, Src: 216.58.217.109, Dst: 192.168.77.159
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 1 (Fragment reassembly time exceeded)
Checksum: 0xe86d [correct]
[Checksum Status: Good]
Internet Protocol Version 4, Src: 192.168.77.159, Dst: 216.58.217.109
User Datagram Protocol, Src Port: 64884, Dst Port: 443
QUIC (Quick UDP Internet Connections)

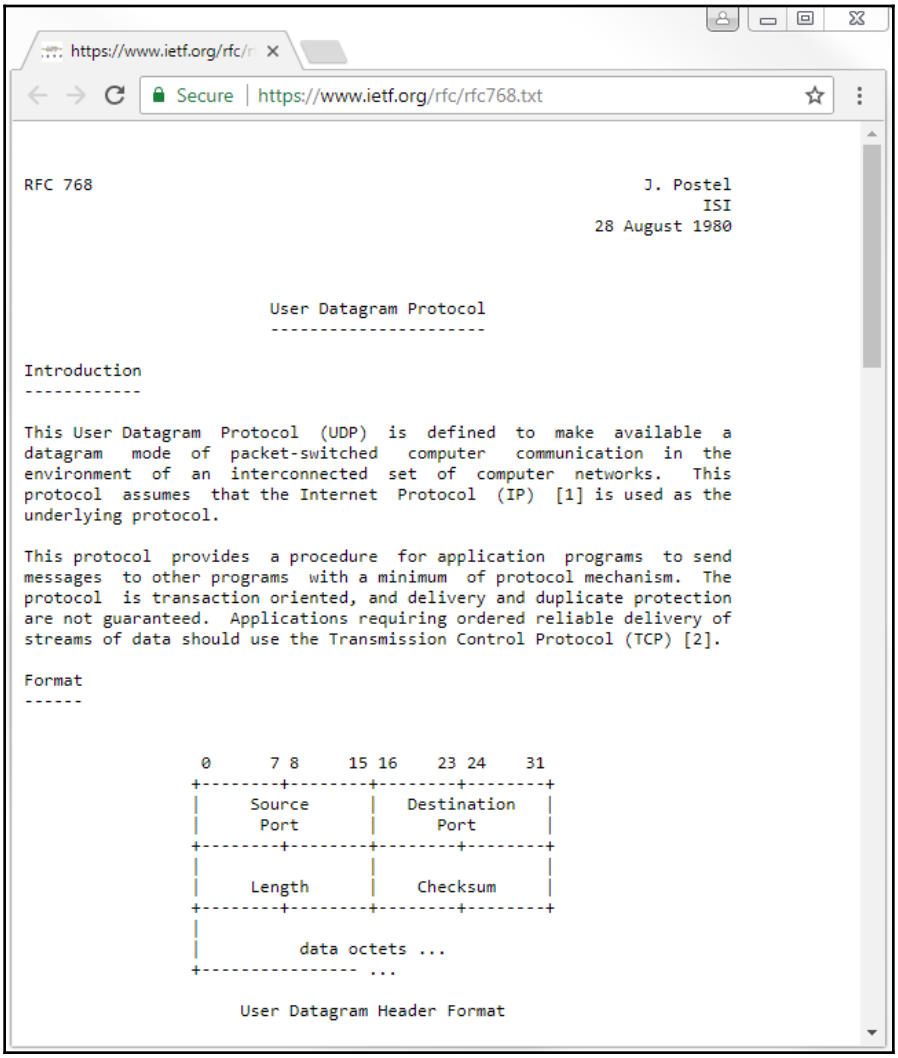

C:\Windows\system32\cmd.exe
C:\Users\sayalit>tracert 8.8.8.8
Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
1 1 ms 1 ms 1 ms 192.168.4.3
2 * 20 ms 21 ms arenafirewall.packtpub.net [192.168.4.1]
3 15 ms 15 ms 15 ms 123.252.235.121
4 * 22 ms * static-2.79.156.182-tataidc.co.in [182.156.79.2]
5 * 25 ms 21 ms 10.117.225.82
6 4 ms 4 ms 3 ms 10.117.137.146
7 23 ms 26 ms 25 ms 14.141.63.225.static-mumbai.vsnl.net.in [14.141.63.225]
8 * * * Request timed out.
9 13 ms 9 ms 8 ms 115.113.165.98.static-mumbai.vsnl.net.in [115.113.165.98]
10 14 ms 15 ms 26 ms 108.170.248.209
11 16 ms 13 ms 10 ms 209.85.253.211
12 25 ms 29 ms 29 ms google-public-dns-a.google.com [8.8.8.8]
Trace complete.
C:\Users\sayalit>


Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
790 13.301 0.007861000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=113/28928, ttl=1 (no response found!)
791 13.302 0.001015000 192.168.4.3 192.168.6.76 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
792 13.303 0.001009000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=114/29184, ttl=1 (no response found!)
793 13.303 0.000847000 192.168.4.3 192.168.6.76 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
794 13.304 0.000823000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=115/29440, ttl=1 (no response found!)
795 13.305 0.000778000 192.168.4.3 192.168.6.76 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
813 13.615 0.001004000 192.168.4.3 192.168.6.76 ICMP 70 Destination unreachable (Port unreachable)
915 15.115 0.001811000 192.168.4.3 192.168.6.76 ICMP 70 Destination unreachable (Port unreachable)
1021 16.614 0.000952000 192.168.4.3 192.168.6.76 ICMP 70 Destination unreachable (Port unreachable)
1158 19.114 0.006307000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=116/29696, ttl=2 (no response found!)
1340 23.111 0.010698000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=117/29952, ttl=2 (no response found!)
1342 23.131 0.000269000 192.168.4.1 192.168.6.76 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
Frame 790: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: Elitegro_4a:08:12 (f4:4d:30:4a:08:12), Dst: HewlettP_27:d8:8a (d8:94:03:27:d8:8a)
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x082f (2095)
Flags: 0x0000
Time to live: 1
[Expert Info (Note/Sequence): "Time To Live" only 1]
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.6.76
Destination: 8.8.8.8


Capturing from Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
1021 16.614 0.000952000 192.168.4.3 192.168.6.76 ICMP 70 Destination unreachable (Port unreachable)
1158 19.114 0.006307000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=116/29696, ttl=2 (no response found!)
1340 23.111 0.010698000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=117/29952, ttl=2 (no response found!)
1342 23.131 0.000269000 192.168.4.1 192.168.6.76 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
1343 23.132 0.001105000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=118/30208, ttl=2 (no response found!)
1345 23.153 0.004332000 192.168.4.1 192.168.6.76 ICMP 106 Time-to-live exceeded (Time to live exceeded in transit)
1406 24.139 0.005094000 192.168.6.76 8.8.8.8 ICMP 106 Echo (ping) request id=0x0001, seq=119/30464, ttl=3 (no response found!)
1407 24.153 0.014690000 123.252.235.121 192.168.6.76 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
Frame 1158: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: Elitegro_4a:08:12 (f4:4d:30:4a:08:12), Dst: HewlettP_27:d8:8a (d8:94:03:27:d8:8a)
Internet Protocol Version 4, Src: 192.168.6.76, Dst: 8.8.8.8
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 92
Identification: 0x0881 (2177)
Flags: 0x0000
Time to live: 2
[Expert Info (Note/Sequence): "Time To Live" only 2]
Protocol: ICMP (1)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.6.76
Destination: 8.8.8.8


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Info
88358 2042... 0.000065000 192.168.6.76 192.168.6.14 ICMP 58 Echo (ping) reply id=0x001b, seq=7568/36893, ttl=128 (request in 8835
88359 2042... 0.000372000 192.168.6.14 192.168.6.76 ICMP 60 Echo (ping) request id=0x001b, seq=7576/38941, ttl=255 (reply in 88360)
88360 2042... 0.000196000 192.168.6.76 192.168.6.14 ICMP 58 Echo (ping) reply id=0x001b, seq=7576/38941, ttl=128 (request in 8835
88361 2042... 0.000425000 192.168.6.14 192.168.6.76 ICMP 60 Echo (ping) request id=0x001b, seq=7584/40989, ttl=255 (reply in 88362)
88362 2042... 0.000178000 192.168.6.76 192.168.6.14 ICMP 58 Echo (ping) reply id=0x001b, seq=7584/40989, ttl=128 (request in 8836
89371 2056... 0.000856000 192.168.6.76 192.168.0.200 ICMP 50 Echo (ping) request id=0x0001, seq=163/41728, ttl=255 (reply in 89372)
89372 2056... 0.000393000 192.168.0.200 192.168.6.76 ICMP 60 Echo (ping) reply id=0x0001, seq=163/41728, ttl=63 (request in 89371)
Frame 88359: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: Giga-Byt_40:5d:e4 (94:de:80:40:5d:e4), Dst: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4, Src: 192.168.6.14, Dst: 192.168.6.76
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 44
Identification: 0x0944 (2372)
Flags: 0x0000
Time to live: 255
Protocol: ICMP (1)
Header checksum: 0x24e2 [validation disabled]
[Header checksum status: Unverified]
Source: 192.168.6.14
Destination: 192.168.6.76

Chapter 07: Network Protocol Analysis



https://www.ietf.org/rfc/r

Secure | https://www.ietf.org/rfc/rfc768.txt

RFC 768

J. Postel
ISI
28 August 1980

User Datagram Protocol

Introduction

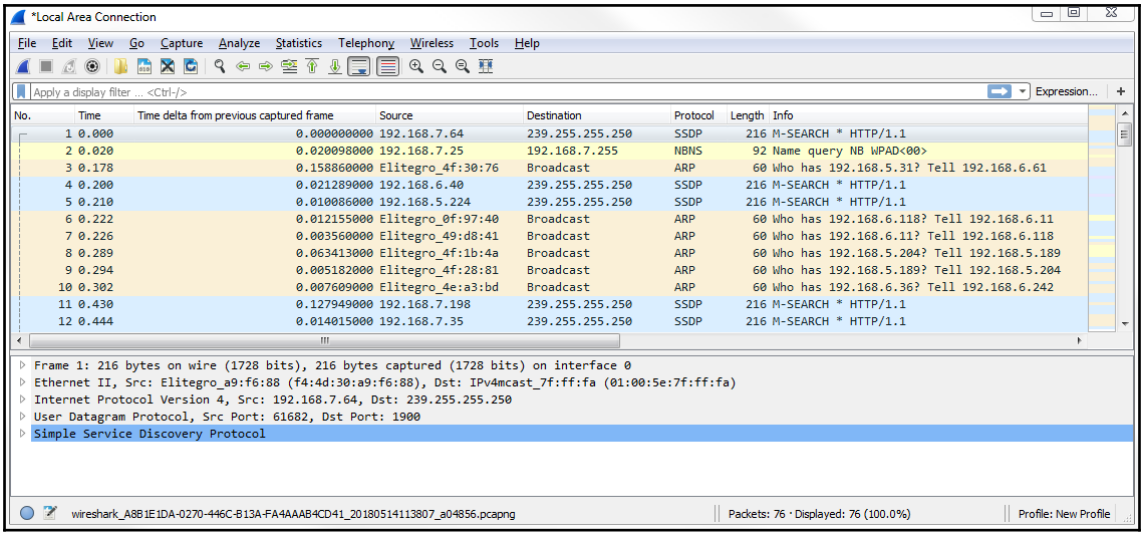
This User Datagram Protocol (UDP) is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) [1] is used as the underlying protocol.

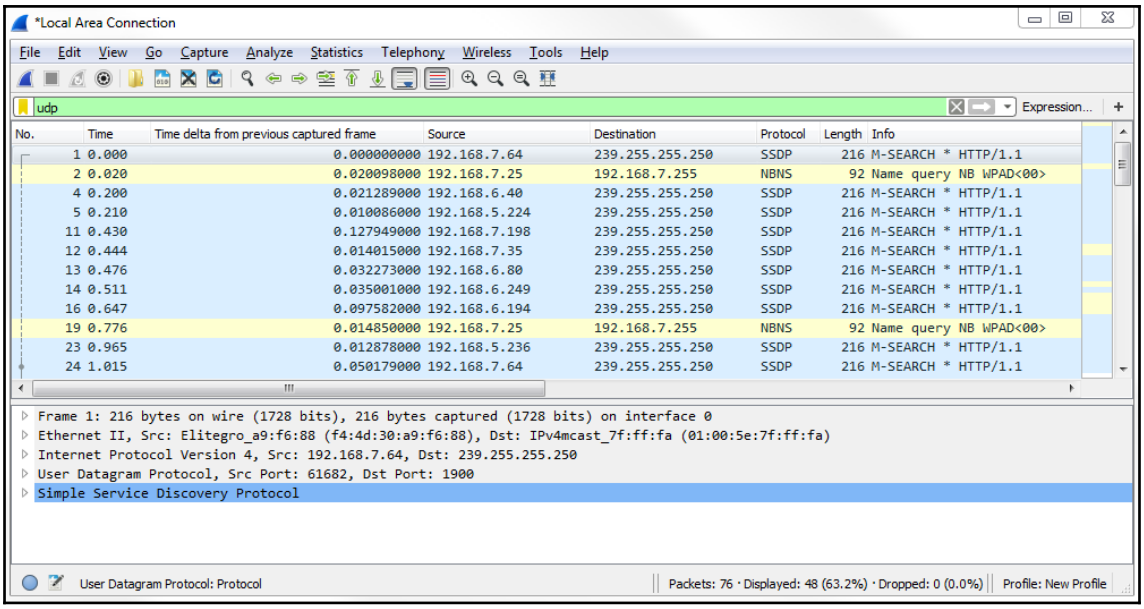
This protocol provides a procedure for application programs to send messages to other programs with a minimum of protocol mechanism. The protocol is transaction oriented, and delivery and duplicate protection are not guaranteed. Applications requiring ordered reliable delivery of streams of data should use the Transmission Control Protocol (TCP) [2].

Format

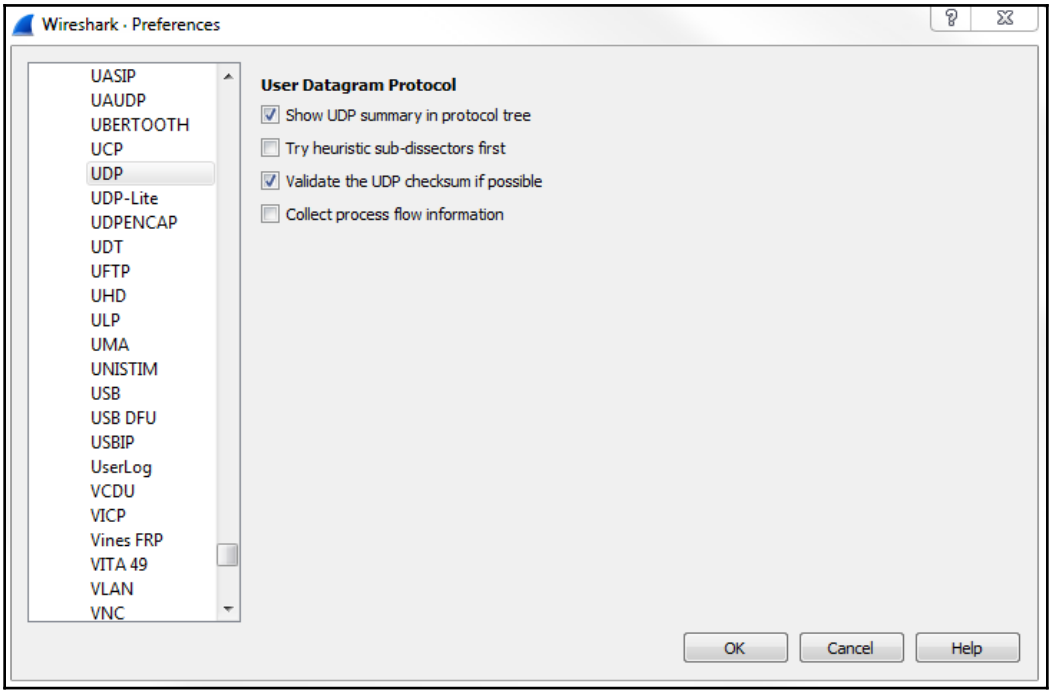
```
 0      7 8     15 16    23 24    31
+--------+--------+--------+--------+
|     Source      |   Destination   |
|      Port       |      Port       |
+--------+--------+--------+--------+
|                 |                 |
|     Length      |    Checksum     |
+--------+--------+--------+--------+
|
|          data octets ...
+---------------- ...
```

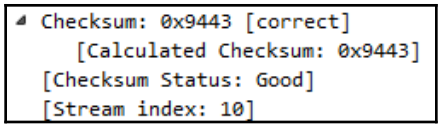
User Datagram Header Format

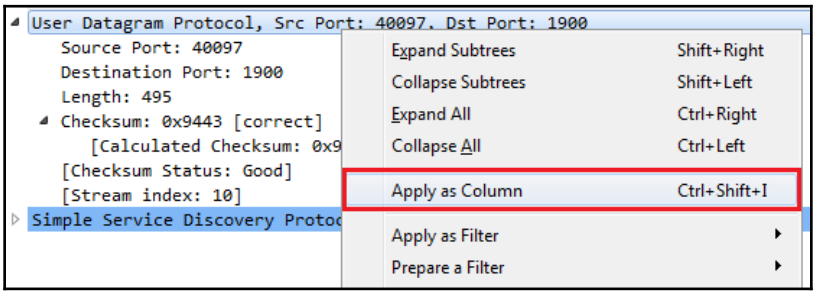


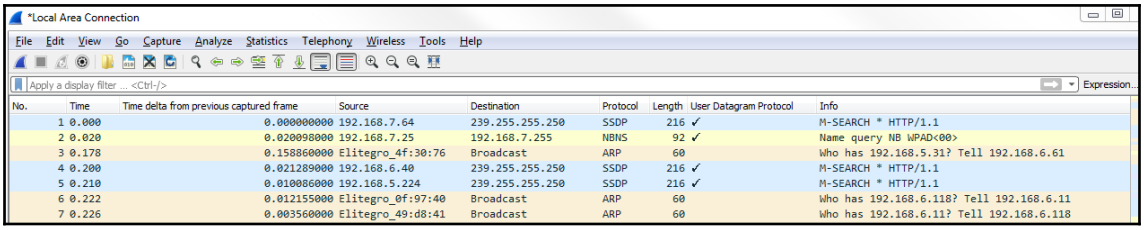


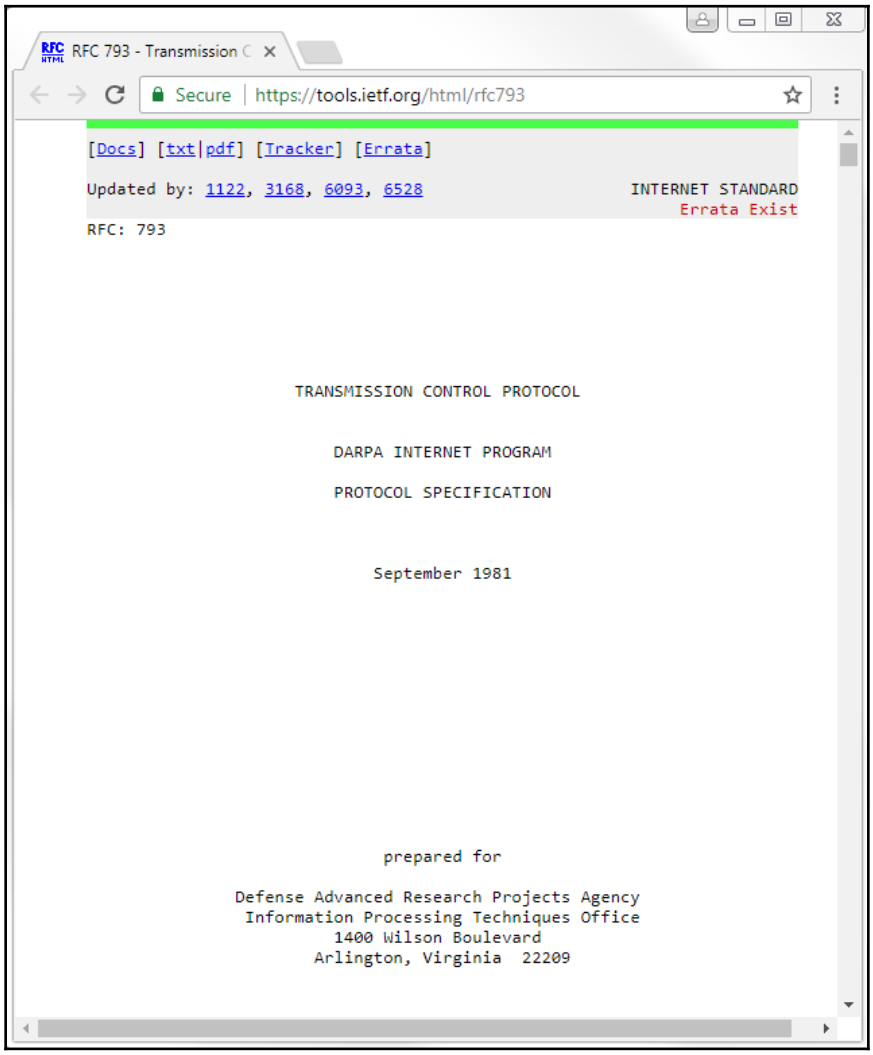

```
User Datagram Protocol, Src Port: 61682, Dst Port: 1900
    Source Port: 61682
    Destination Port: 1900
    Length: 182
    Checksum: 0x4b86 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
```

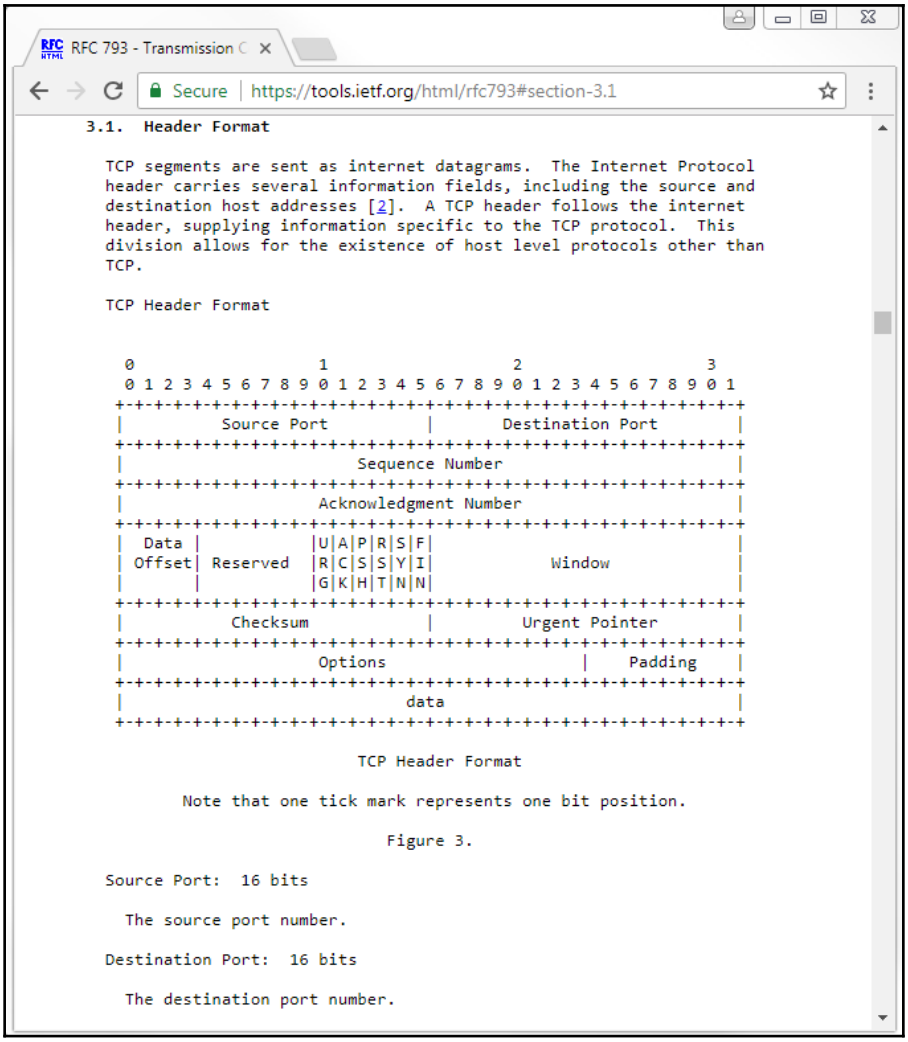

Wireshark · Preferences
UASIP
UAUDP
UBERTOOTH
UCP
UDP
UDP-Lite
UDPENCAP
UDT
UFTP
UHD
ULP
UMA
UNISTIM
USB
USB DFU
USBIP
UserLog
VCDU
VICP
Vines FRP
VITA 49
VLAN
VNC
User Datagram Protocol
Show UDP summary in protocol tree
Try heuristic sub-dissectors first
Validate the UDP checksum if possible
Collect process flow information
OK
Cancel
Help


Checksum: 0x9443 [correct]
[Calculated Checksum: 0x9443]
[Checksum Status: Good]
[Stream index: 10]


User Datagram Protocol, Src Port: 40097, Dst Port: 1900
Source Port: 40097
Destination Port: 1900
Length: 495
Checksum: 0x9443 [correct]
[Calculated Checksum: 0x9
[Checksum Status: Good]
[Stream index: 10]
Simple Service Discovery Protoc
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length User Datagram Protocol Info
1 0.000 0.000000000 192.168.7.64 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
2 0.020 0.020098000 192.168.7.25 192.168.7.255 NBNS 92 ✓ Name query NB WPAD<00>
3 0.178 0.158860000 Elitegro_4f:30:76 Broadcast ARP 60 Who has 192.168.5.31? Tell 192.168.6.61
4 0.200 0.021289000 192.168.6.40 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
5 0.210 0.010086000 192.168.5.224 239.255.255.250 SSDP 216 ✓ M-SEARCH * HTTP/1.1
6 0.222 0.012155000 Elitegro_0f:97:40 Broadcast ARP 60 Who has 192.168.6.118? Tell 192.168.6.11
7 0.226 0.003560000 Elitegro_49:d8:41 Broadcast ARP 60 Who has 192.168.6.11? Tell 192.168.6.118


RFC 793 - Transmission C
Secure https://tools.ietf.org/html/rfc793
[Docs] [txt|pdf] [Tracker] [Errata]
Updated by: 1122, 3168, 6093, 6528
INTERNET STANDARD
Errata Exist
RFC: 793
TRANSMISSION CONTROL PROTOCOL
DARPA INTERNET PROGRAM
PROTOCOL SPECIFICATION
September 1981
prepared for
Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209



3.1. Header Format

TCP segments are sent as internet datagrams. The Internet Protocol header carries several information fields, including the source and destination host addresses [2]. A TCP header follows the internet header, supplying information specific to the TCP protocol. This division allows for the existence of host level protocols other than TCP.

TCP Header Format

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          Source Port          |       Destination Port        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                        Sequence Number                        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Acknowledgment Number                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Data |           |U|A|P|R|S|F|                               |
 | Offset| Reserved  |R|C|S|S|Y|I|            Window             |
 |       |           |G|K|H|T|N|N|                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           Checksum            |         Urgent Pointer        |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                    Options                    |    Padding    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                             data                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TCP Header Format

Note that one tick mark represents one bit position.

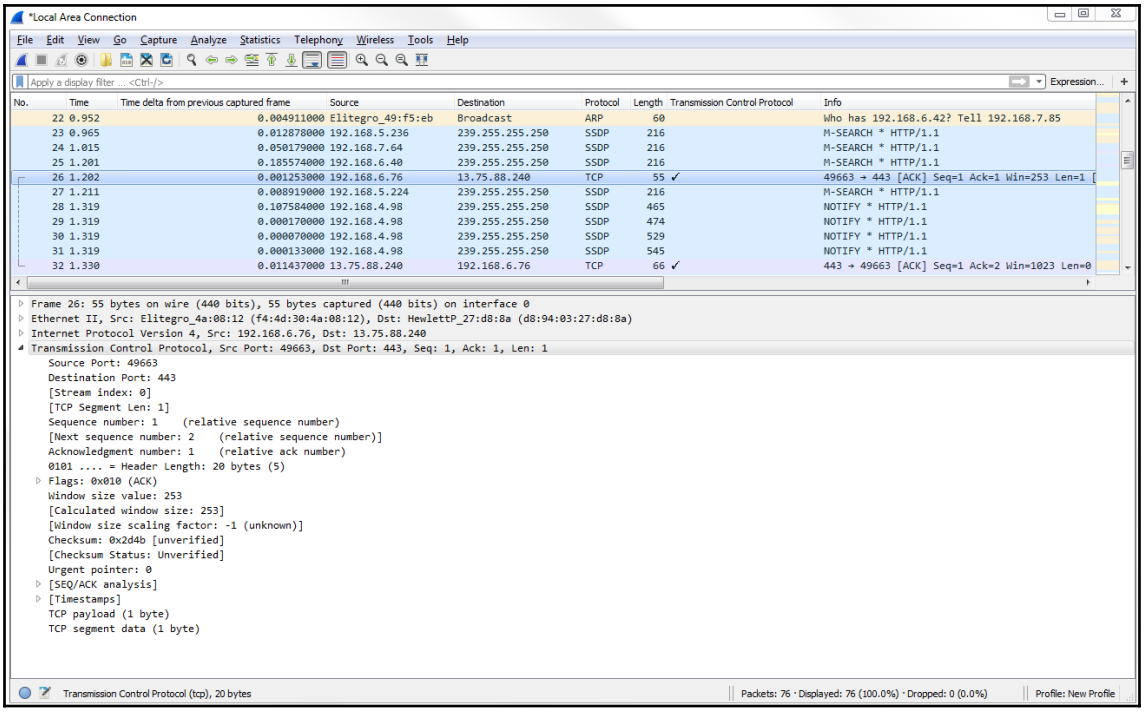
Figure 3.

Source Port: 16 bits

The source port number.

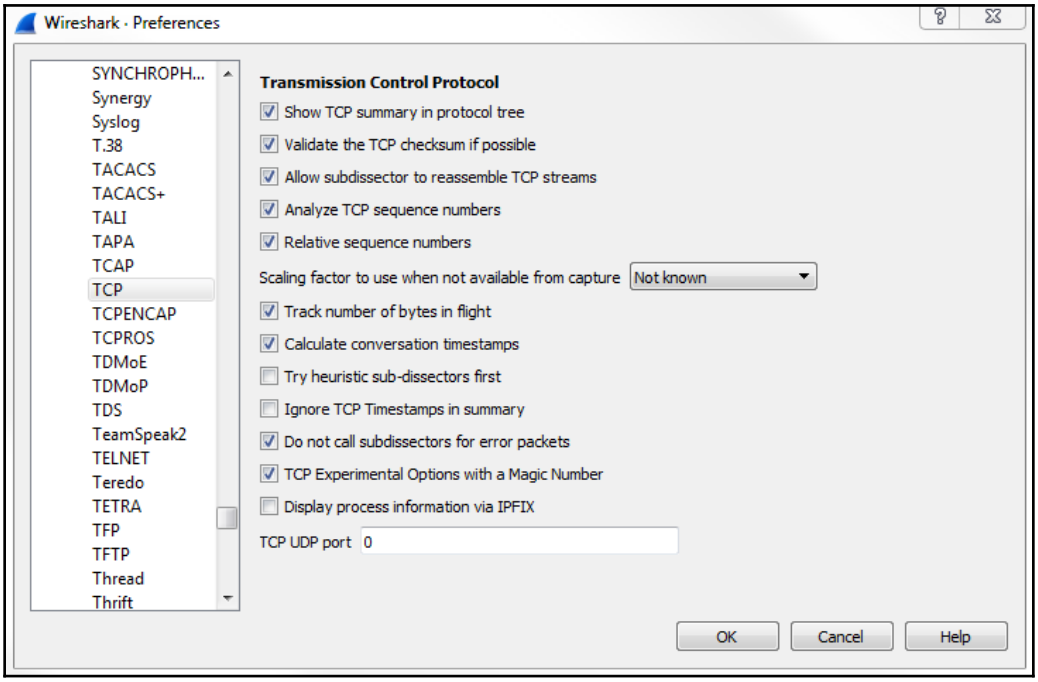
Destination Port: 16 bits

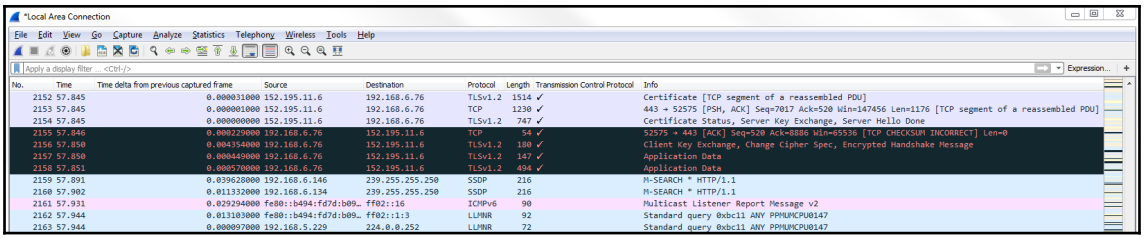
The destination port number.

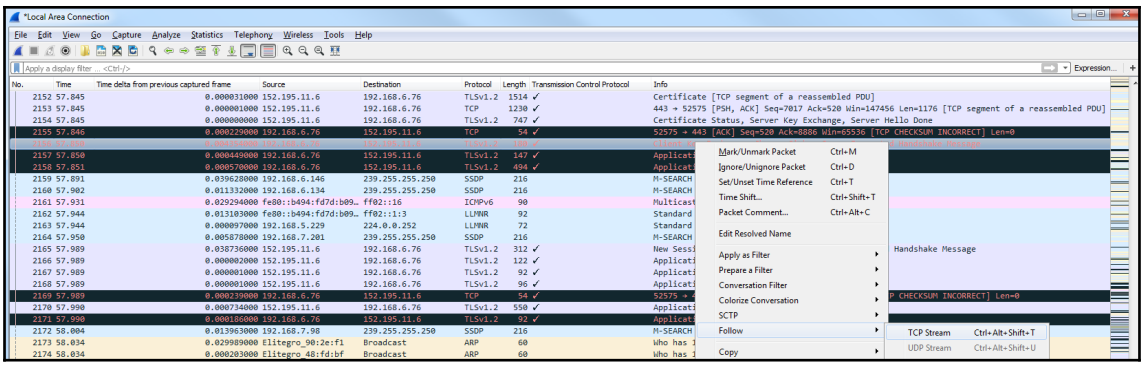


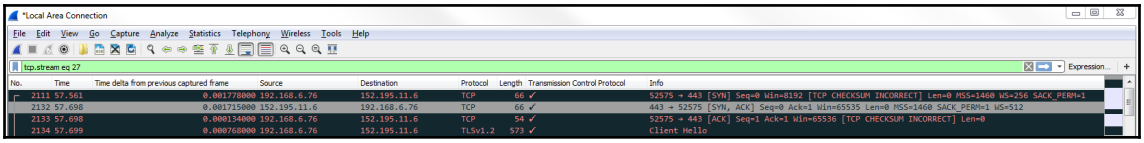

```
Flags: 0x010 (ACK)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Nonce: Not set
    .... 0... .... = Congestion Window Reduced (CWR): Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...1 .... = Acknowledgment: Set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ·····A····]
```

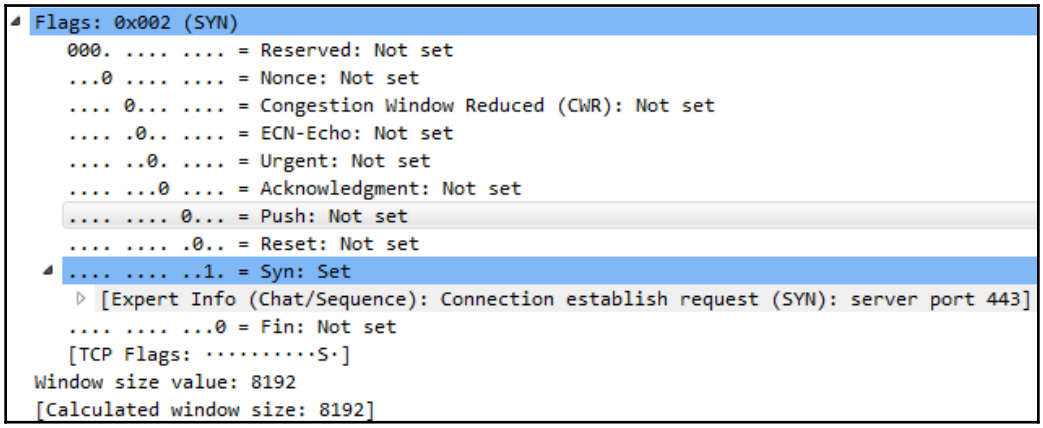
```
  Window size value: 253
  [Calculated window size: 253]
  [Window size scaling factor: -1 (unknown)]
  Checksum: 0x2d4b [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
▷ [SEQ/ACK analysis]
```

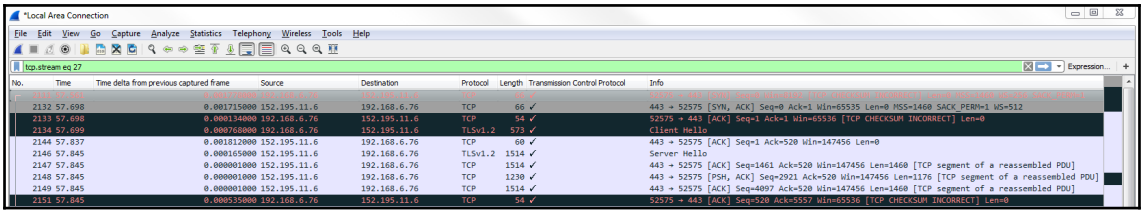

Wireshark · Preferences
SYNCHROPH...
Synergy
Syslog
T.38
TACACS
TACACS+
TALI
TAPA
TCAP
TCP
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TELNET
Teredo
TETRA
TFP
TFTP
Thread
Thrift
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Analyze TCP sequence numbers
Relative sequence numbers
Scaling factor to use when not available from capture
Not known
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port
0
OK
Cancel
Help

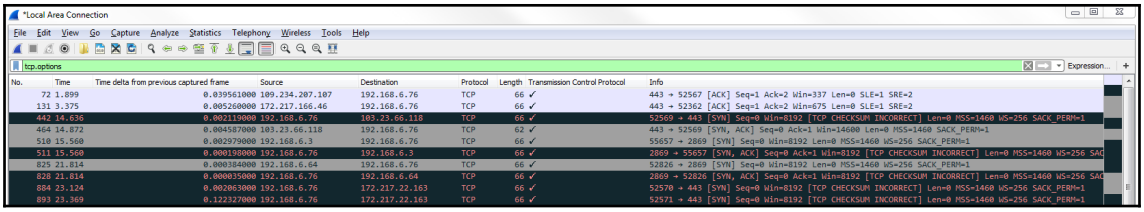

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
2152 57.845 0.000031000 152.195.11.6 192.168.6.76 TLSv1.2 1514 ✓ Certificate [TCP segment of a reassembled PDU]
2153 57.845 0.000001000 152.195.11.6 192.168.6.76 TCP 1230 ✓ 443 → 52575 [PSH, ACK] Seq=7017 Ack=520 Win=147456 Len=1176 [TCP segment of a reassembled PDU]
2154 57.845 0.000000000 152.195.11.6 192.168.6.76 TLSv1.2 747 ✓ Certificate Status, Server Key Exchange, Server Hello Done
2155 57.846 0.000229000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 → 443 [ACK] Seq=520 Ack=8886 Win=65536 [TCP CHECKSUM INCORRECT] Len=0
2156 57.850 0.004354000 192.168.6.76 152.195.11.6 TLSv1.2 180 ✓ Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2157 57.850 0.000449000 192.168.6.76 152.195.11.6 TLSv1.2 147 ✓ Application Data
2158 57.851 0.000570000 192.168.6.76 152.195.11.6 TLSv1.2 494 ✓ Application Data
2159 57.891 0.039628000 192.168.6.146 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2160 57.902 0.011332000 192.168.6.134 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
2161 57.931 0.029294000 fe80::b494:fd7d:b09… ff02::16 ICMPv6 90 Multicast Listener Report Message v2
2162 57.944 0.013103000 fe80::b494:fd7d:b09… ff02::1:3 LLMNR 92 Standard query 0xbc11 ANY PPMUMCPU0147
2163 57.944 0.000097000 192.168.5.229 224.0.0.252 LLMNR 72 Standard query 0xbc11 ANY PPMUMCPU0147


*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
2152 57.845 0.000031000 152.195.11.6 192.168.6.76 TLSv1.2 1514 ✓ Certificate [TCP segment of a reassembled PDU]
2153 57.845 0.000001000 152.195.11.6 192.168.6.76 TCP 1230 ✓ 443 → 52575 [PSH, ACK] Seq=7017 Ack=520 Win=147456 Len=1176 [TCP segment of a reassembled PDU]
2154 57.845 0.000000000 152.195.11.6 192.168.6.76 TLSv1.2 747 ✓ Certificate Status, Server Key Exchange, Server Hello Done
2155 57.846 0.000229000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 → 443 [ACK] Seq=520 Ack=8886 Win=65536 [TCP CHECKSUM INCORRECT] Len=0
2157 57.850 0.000449000 192.168.6.76 152.195.11.6 TLSv1.2 147 ✓
2158 57.851 0.000570000 192.168.6.76 152.195.11.6 TLSv1.2 494 ✓
2159 57.891 0.039628000 192.168.6.146 239.255.255.250 SSDP 216
2160 57.902 0.011332000 192.168.6.134 239.255.255.250 SSDP 216
2161 57.931 0.029294000 fe80::b494:fd7d:b09… ff02::16
2162 57.944 0.013103000 fe80::b494:fd7d:b09… ff02::1:3
2163 57.944 0.000097000 192.168.5.229 224.0.0.252
2164 57.950 0.005878000 192.168.7.201 239.255.255.250 SSDP 216 M-SEARCH
2165 57.989 0.038736000 152.195.11.6 192.168.6.76 TLSv1.2 312 ✓ New Sessi
2166 57.989 0.000002000 152.195.11.6 192.168.6.76 TLSv1.2 122 ✓ Applicati
2167 57.989 0.000001000 152.195.11.6 192.168.6.76 TLSv1.2 92 ✓ Applicati
2168 57.989 0.000001000 152.195.11.6 192.168.6.76 TLSv1.2 96 ✓ Applicati
2169 57.989 0.000239000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 →
2170 57.990 0.000734000 152.195.11.6 192.168.6.76 TLSv1.2 550 ✓ Applicati
2171 57.990 0.000186000 192.168.6.76 152.195.11.6 TLSv1.2 92 ✓ Applicati
2172 58.004 0.013963000 192.168.7.98 239.255.255.250 SSDP 216 M-SEARCH
2173 58.034 0.029980000 Elitegro_90:2e:f1 Broadcast ARP 60 Who has
2174 58.034 0.000203000 Elitegro_48:fd:bf Broadcast ARP 60 Who has
Mark/Unmark Packet Ctrl+M
Ignore/Unignore Packet Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comment... Ctrl+Alt+C
Edit Resolved Name
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
Handshake Message
P CHECKSUM INCORRECT] Len=0

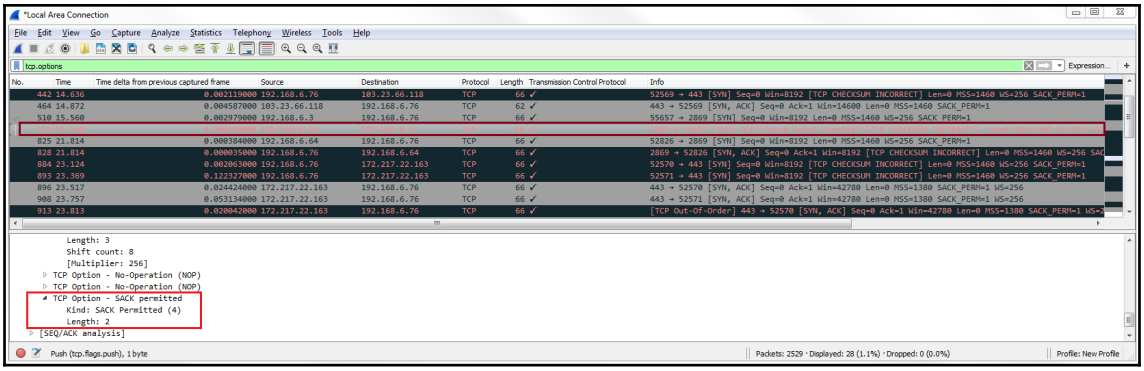

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 27
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
2111 57.561 0.001778000 192.168.6.76 152.195.11.6 TCP 66 ✓ 52575 → 443 [SYN] Seq=0 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SACK_PERM=1
2132 57.698 0.001715000 152.195.11.6 192.168.6.76 TCP 66 ✓ 443 → 52575 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
2133 57.698 0.000134000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 → 443 [ACK] Seq=1 Ack=1 Win=65536 [TCP CHECKSUM INCORRECT] Len=0
2134 57.699 0.000768000 192.168.6.76 152.195.11.6 TLSv1.2 573 ✓ Client Hello

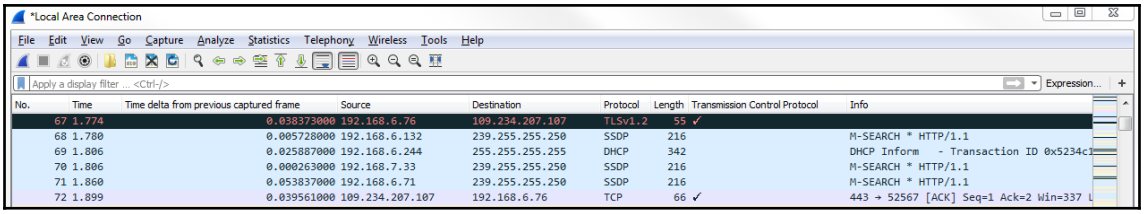

Flags: 0x002 (SYN)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....0 .... = Acknowledgment: Not set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....1. = Syn: Set
[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 443]
....0 = Fin: Not set
[TCP Flags: ··········S·]
Window size value: 8192
[Calculated window size: 8192]

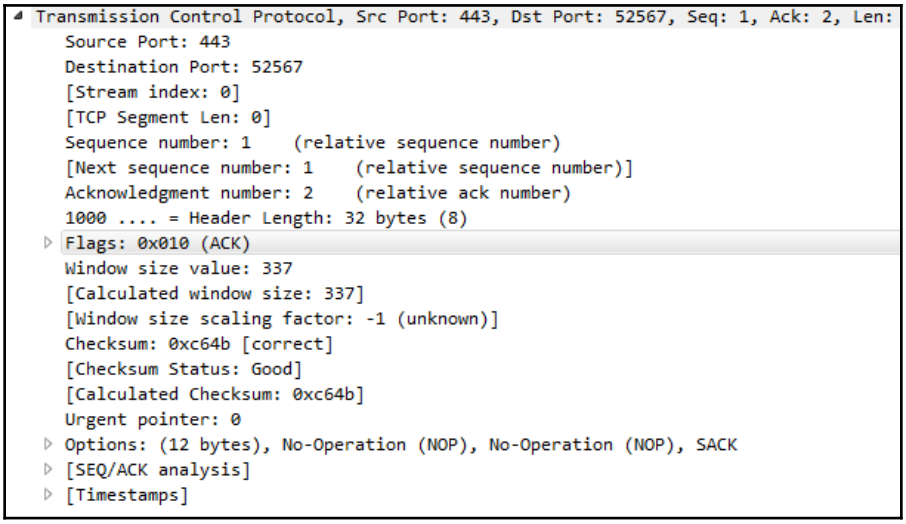

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 27
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
2132 57.698 0.001715000 152.195.11.6 192.168.6.76 TCP 66 ✓ 443 → 52575 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
2133 57.698 0.000134000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 → 443 [ACK] Seq=1 Ack=1 Win=65536 [TCP CHECKSUM INCORRECT] Len=0
2134 57.699 0.000768000 192.168.6.76 152.195.11.6 TLSv1.2 573 ✓ Client Hello
2144 57.837 0.001812000 152.195.11.6 192.168.6.76 TCP 60 ✓ 443 → 52575 [ACK] Seq=1 Ack=520 Win=147456 Len=0
2146 57.845 0.000165000 152.195.11.6 192.168.6.76 TLSv1.2 1514 ✓ Server Hello
2147 57.845 0.000001000 152.195.11.6 192.168.6.76 TCP 1514 ✓ 443 → 52575 [ACK] Seq=1461 Ack=520 Win=147456 Len=1460 [TCP segment of a reassembled PDU]
2148 57.845 0.000001000 152.195.11.6 192.168.6.76 TCP 1230 ✓ 443 → 52575 [PSH, ACK] Seq=2921 Ack=520 Win=147456 Len=1176 [TCP segment of a reassembled PDU]
2149 57.845 0.000001000 152.195.11.6 192.168.6.76 TCP 1514 ✓ 443 → 52575 [ACK] Seq=4097 Ack=520 Win=147456 Len=1460 [TCP segment of a reassembled PDU]
2151 57.845 0.000535000 192.168.6.76 152.195.11.6 TCP 54 ✓ 52575 → 443 [ACK] Seq=520 Ack=5557 Win=65536 [TCP CHECKSUM INCORRECT] Len=0

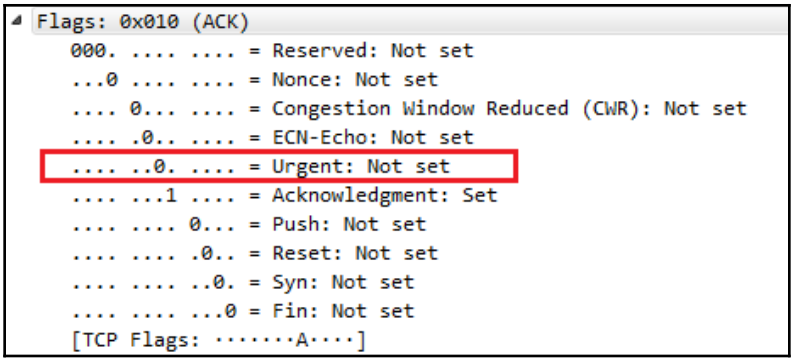

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.options
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
72 1.899 0.039561000 109.234.207.107 192.168.6.76 TCP 66 ✓ 443 → 52567 [ACK] Seq=1 Ack=2 Win=337 Len=0 SLE=1 SRE=2
131 3.375 0.005260000 172.217.166.46 192.168.6.76 TCP 66 ✓ 443 → 52362 [ACK] Seq=1 Ack=2 Win=675 Len=0 SLE=1 SRE=2
442 14.636 0.002119000 192.168.6.76 103.23.66.118 TCP 66 ✓ 52569 → 443 [SYN] Seq=0 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SACK_PERM=1
464 14.872 0.004587000 103.23.66.118 192.168.6.76 TCP 62 ✓ 443 → 52569 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
510 15.560 0.002979000 192.168.6.3 192.168.6.76 TCP 66 ✓ 55657 → 2869 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
511 15.560 0.000198000 192.168.6.76 192.168.6.3 TCP 66 ✓ 2869 → 55657 [SYN, ACK] Seq=0 Ack=1 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SAC
825 21.814 0.000384000 192.168.6.64 192.168.6.76 TCP 66 ✓ 52826 → 2869 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
828 21.814 0.000035000 192.168.6.76 192.168.6.64 TCP 66 ✓ 2869 → 52826 [SYN, ACK] Seq=0 Ack=1 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SAC
884 23.124 0.002063000 192.168.6.76 172.217.22.163 TCP 66 ✓ 52570 → 443 [SYN] Seq=0 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SACK_PERM=1
893 23.369 0.122327000 192.168.6.76 172.217.22.163 TCP 66 ✓ 52571 → 443 [SYN] Seq=0 Win=8192 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=256 SACK_PERM=1

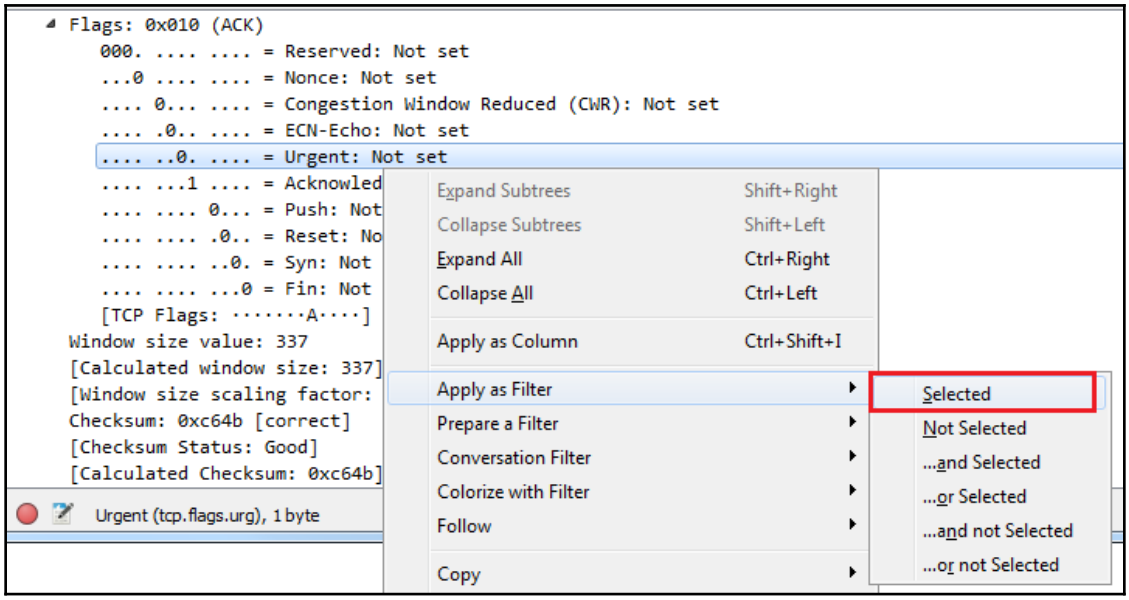
```
▲ TCP Option - Window scale: 8 (multiply by 256)
      Kind: Window Scale (3)
      Length: 3
      Shift count: 8
      [Multiplier: 256]
▷ TCP Option - No-Operation (NOP)
▷ TCP Option - No-Operation (NOP)
▲ TCP Option - SACK permitted
      Kind: SACK Permitted (4)
      Length: 2
```

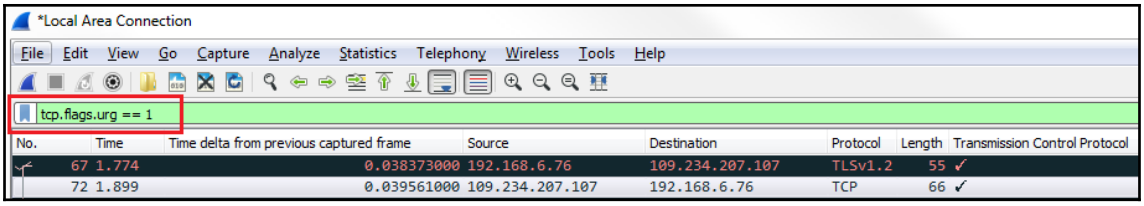


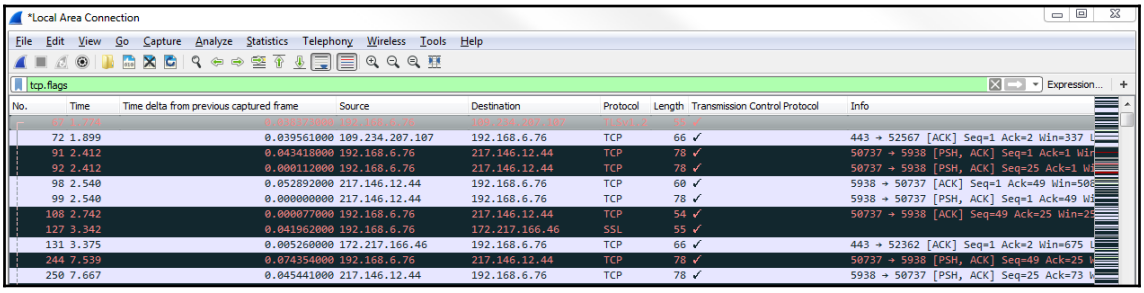


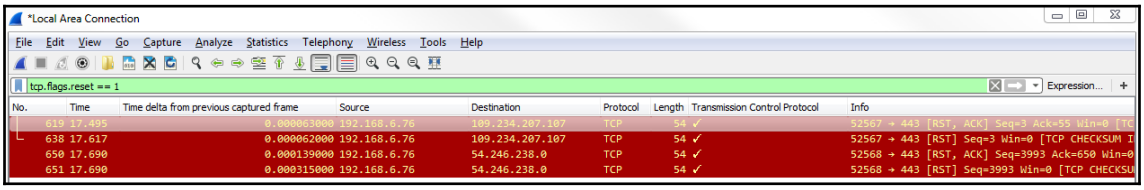

Transmission Control Protocol, Src Port: 443, Dst Port: 52567, Seq: 1, Ack: 2, Len:
Source Port: 443
Destination Port: 52567
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 2 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 337
[Calculated window size: 337]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xc64b [correct]
[Checksum Status: Good]
[Calculated Checksum: 0xc64b]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
[SEQ/ACK analysis]
[Timestamps]

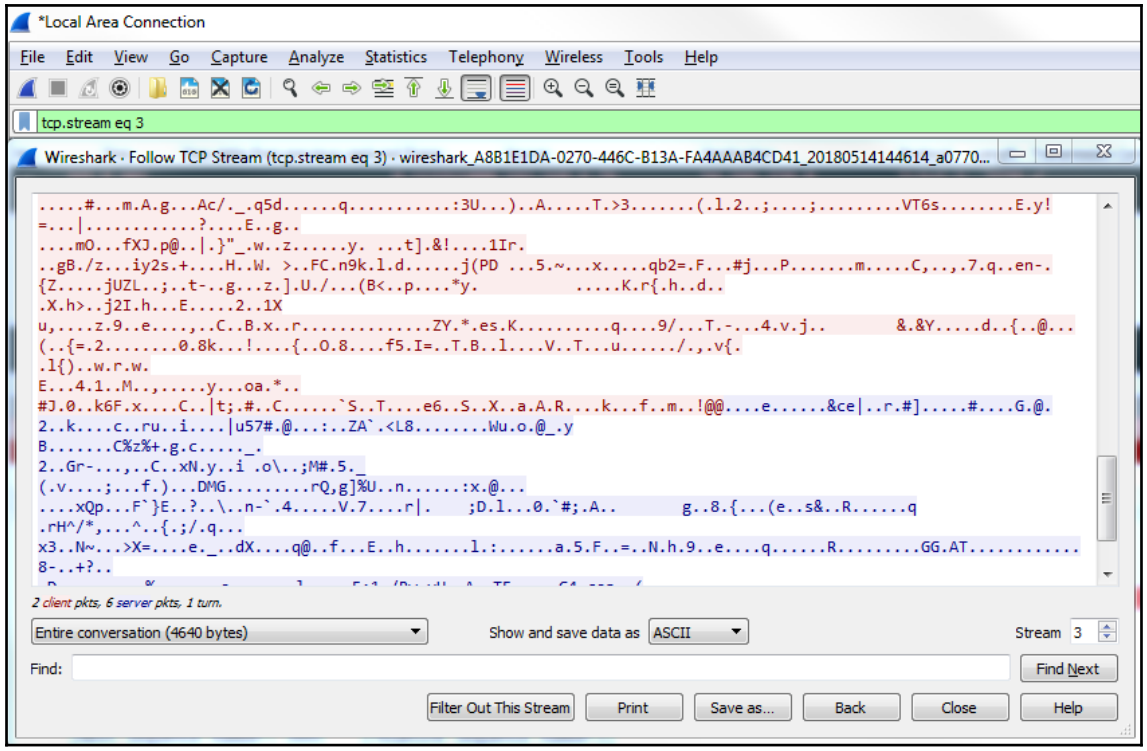

Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A····]

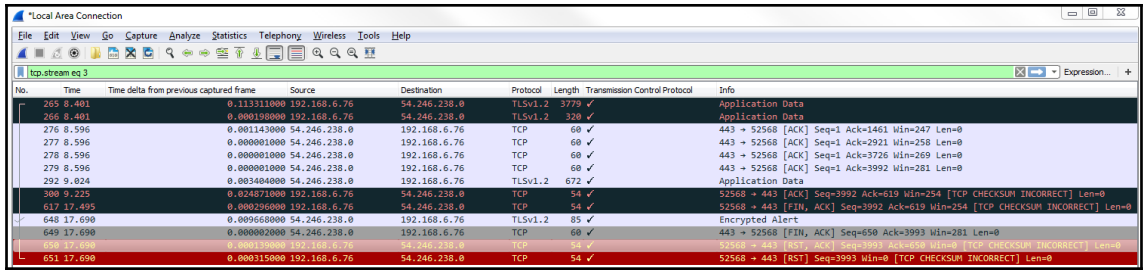

Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowled
.... 0... = Push: Not
.... .0.. = Reset: No
....0. = Syn: Not
....0 = Fin: Not
[TCP Flags: ·····A····]
Window size value: 337
[Calculated window size: 337]
[Window size scaling factor:
Checksum: 0xc64b [correct]
[Checksum Status: Good]
[Calculated Checksum: 0xc64b]
Urgent (tcp.flags.urg), 1 byte
Expand Subtrees Shift+Right
Collapse Subtrees Shift+Left
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

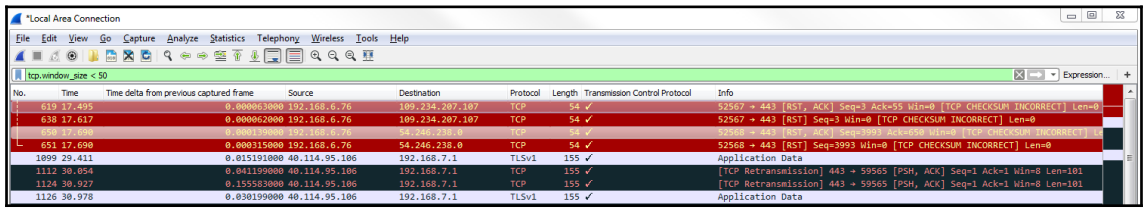

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.urg == 1
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol
67 1.774 0.038373000 192.168.6.76 109.234.207.107 TLSv1.2 55 ✓
72 1.899 0.039561000 109.234.207.107 192.168.6.76 TCP 66 ✓

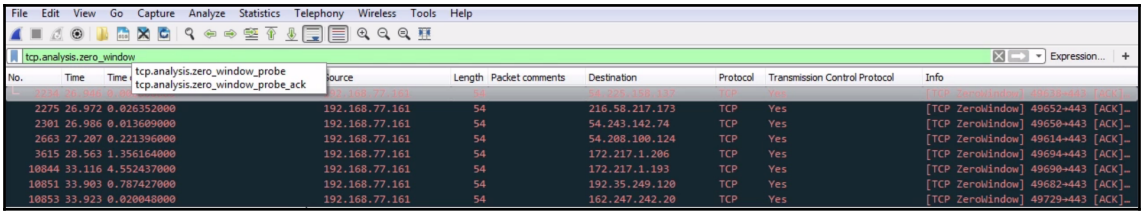

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
72 1.899 0.039561000 109.234.207.107 192.168.6.76 TCP 66 ✓ 443 → 52567 [ACK] Seq=1 Ack=2 Win=337
91 2.412 0.043418000 192.168.6.76 217.146.12.44 TCP 78 ✓ 50737 → 5938 [PSH, ACK] Seq=1 Ack=1
92 2.412 0.000112000 192.168.6.76 217.146.12.44 TCP 78 ✓ 50737 → 5938 [PSH, ACK] Seq=25 Ack=1
98 2.540 0.052892000 217.146.12.44 192.168.6.76 TCP 60 ✓ 5938 → 50737 [ACK] Seq=1 Ack=49 Win=
99 2.540 0.000000000 217.146.12.44 192.168.6.76 TCP 78 ✓ 5938 → 50737 [PSH, ACK] Seq=1 Ack=49
108 2.742 0.000077000 192.168.6.76 217.146.12.44 TCP 54 ✓ 50737 → 5938 [ACK] Seq=49 Ack=25 Win=
127 3.342 0.041962000 192.168.6.76 172.217.166.46 SSL 55 ✓
131 3.375 0.005260000 172.217.166.46 192.168.6.76 TCP 66 ✓ 443 → 52362 [ACK] Seq=1 Ack=2 Win=675
244 7.539 0.074354000 192.168.6.76 217.146.12.44 TCP 78 ✓ 50737 → 5938 [PSH, ACK] Seq=49 Ack=25
250 7.667 0.045441000 217.146.12.44 192.168.6.76 TCP 78 ✓ 5938 → 50737 [PSH, ACK] Seq=25 Ack=73

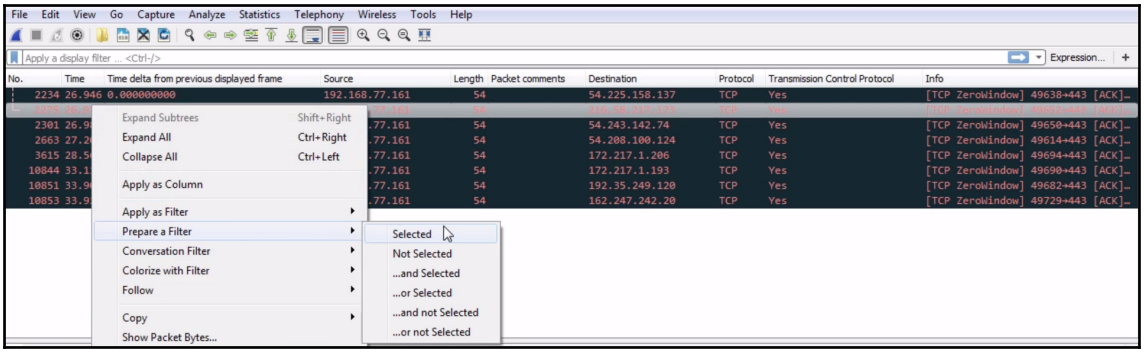

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.flags.reset == 1
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
619 17.495 0.000063000 192.168.6.76 109.234.207.107 TCP 54 ✓ 52567 → 443 [RST, ACK] Seq=3 Ack=55 Win=0
638 17.617 0.000062000 192.168.6.76 109.234.207.107 TCP 54 ✓ 52567 → 443 [RST] Seq=3 Win=0 [TCP CHECKSUM
650 17.690 0.000139000 192.168.6.76 54.246.238.0 TCP 54 ✓ 52568 → 443 [RST, ACK] Seq=3993 Ack=650 Win=0
651 17.690 0.000315000 192.168.6.76 54.246.238.0 TCP 54 ✓ 52568 → 443 [RST] Seq=3993 Win=0 [TCP CHECKSU

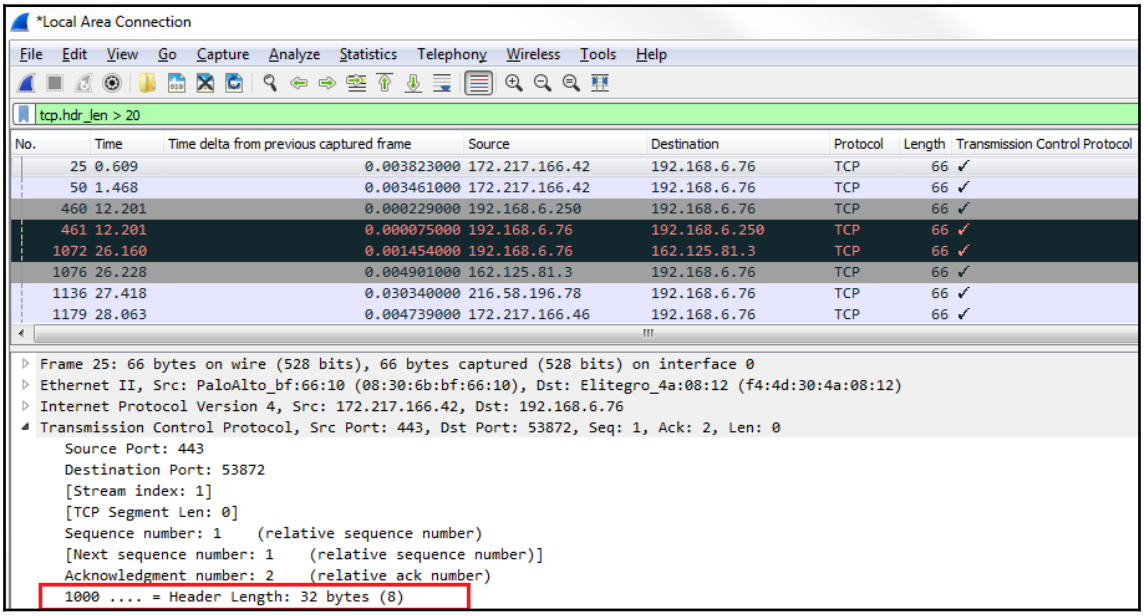

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 3
Wireshark · Follow TCP Stream (tcp.stream eq 3) · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514144614_a0770...
2 client pkts, 6 server pkts, 1 turn.
Entire conversation (4640 bytes)
Show and save data as ASCII
Stream 3
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

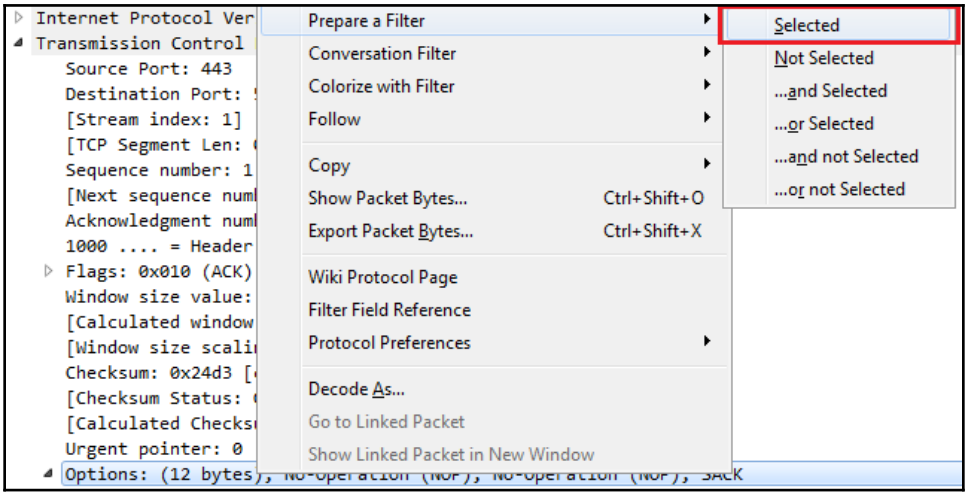

*Local Area Connection
tcp.stream eq 3
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
265 8.401 0.113311000 192.168.6.76 54.246.238.0 TLSv1.2 3779 Application Data
266 8.401 0.000198000 192.168.6.76 54.246.238.0 TLSv1.2 320 Application Data
276 8.596 0.001143000 54.246.238.0 192.168.6.76 TCP 60 443 → 52568 [ACK] Seq=1 Ack=1461 Win=247 Len=0
277 8.596 0.000001000 54.246.238.0 192.168.6.76 TCP 60 443 → 52568 [ACK] Seq=1 Ack=2921 Win=258 Len=0
278 8.596 0.000001000 54.246.238.0 192.168.6.76 TCP 60 443 → 52568 [ACK] Seq=1 Ack=3726 Win=269 Len=0
279 8.596 0.000001000 54.246.238.0 192.168.6.76 TCP 60 443 → 52568 [ACK] Seq=1 Ack=3992 Win=281 Len=0
292 9.024 0.003404000 54.246.238.0 192.168.6.76 TLSv1.2 672 Application Data
300 9.225 0.024871000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [ACK] Seq=3992 Ack=619 Win=254 [TCP CHECKSUM INCORRECT] Len=0
617 17.495 0.000296000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [FIN, ACK] Seq=3992 Ack=619 Win=254 [TCP CHECKSUM INCORRECT] Len=0
648 17.690 0.009668000 54.246.238.0 192.168.6.76 TLSv1.2 85 Encrypted Alert
649 17.690 0.000002000 54.246.238.0 192.168.6.76 TCP 60 443 → 52568 [FIN, ACK] Seq=650 Ack=3993 Win=281 Len=0
650 17.690 0.000139000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [RST, ACK] Seq=3993 Ack=650 Win=0 [TCP CHECKSUM INCORRECT] Len=0
651 17.690 0.000315000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [RST] Seq=3993 Win=0 [TCP CHECKSUM INCORRECT] Len=0

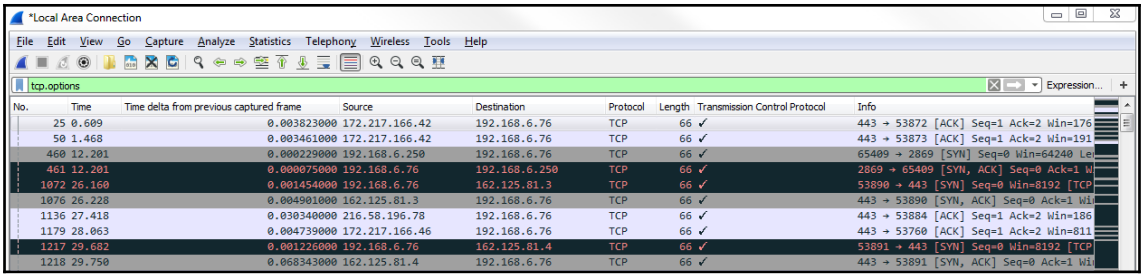

*Local Area Connection
tcp.window_size < 50
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
619 17.495 0.000063000 192.168.6.76 109.234.207.107 TCP 54 52567 → 443 [RST, ACK] Seq=3 Ack=55 Win=0 [TCP CHECKSUM INCORRECT] Len=0
638 17.617 0.000062000 192.168.6.76 109.234.207.107 TCP 54 52567 → 443 [RST] Seq=3 Win=0 [TCP CHECKSUM INCORRECT] Len=0
650 17.690 0.000139000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [RST, ACK] Seq=650 Win=0 [TCP CHECKSUM INCORRECT] Len=0
651 17.690 0.000315000 192.168.6.76 54.246.238.0 TCP 54 52568 → 443 [RST] Seq=3993 Win=0 [TCP CHECKSUM INCORRECT] Len=0
1099 29.411 0.015191000 40.114.95.106 192.168.7.1 TLSv1 155 Application Data
1112 30.054 0.041199000 40.114.95.106 192.168.7.1 TCP 155 [TCP Retransmission] 443 → 59565 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
1124 30.927 0.155583000 40.114.95.106 192.168.7.1 TCP 155 [TCP Retransmission] 443 → 59565 [PSH, ACK] Seq=1 Ack=1 Win=8 Len=101
1126 30.978 0.030199000 40.114.95.106 192.168.7.1 TLSv1 155 Application Data

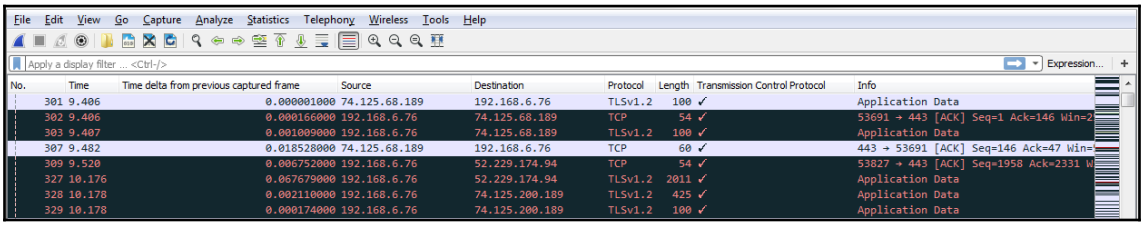

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.analysis.zero_window
tcp.analysis.zero_window_probe
tcp.analysis.zero_window_probe_ack
Expression...
No. Time Source Length Packet comments Destination Protocol Transmission Control Protocol Info
2275 26.972 0.026352000 192.168.77.161 54 216.58.217.173 TCP Yes [TCP ZeroWindow] 49652→443 [ACK]…
2301 26.986 0.013609000 192.168.77.161 54 54.243.142.74 TCP Yes [TCP ZeroWindow] 49650→443 [ACK]…
2663 27.207 0.221396000 192.168.77.161 54 54.208.100.124 TCP Yes [TCP ZeroWindow] 49614→443 [ACK]…
3615 28.563 1.356164000 192.168.77.161 54 172.217.1.206 TCP Yes [TCP ZeroWindow] 49694→443 [ACK]…
10844 33.116 4.552437000 192.168.77.161 54 172.217.1.193 TCP Yes [TCP ZeroWindow] 49690→443 [ACK]…
10851 33.903 0.787427000 192.168.77.161 54 192.35.249.120 TCP Yes [TCP ZeroWindow] 49682→443 [ACK]…
10853 33.923 0.020048000 192.168.77.161 54 162.247.242.20 TCP Yes [TCP ZeroWindow] 49729→443 [ACK]…

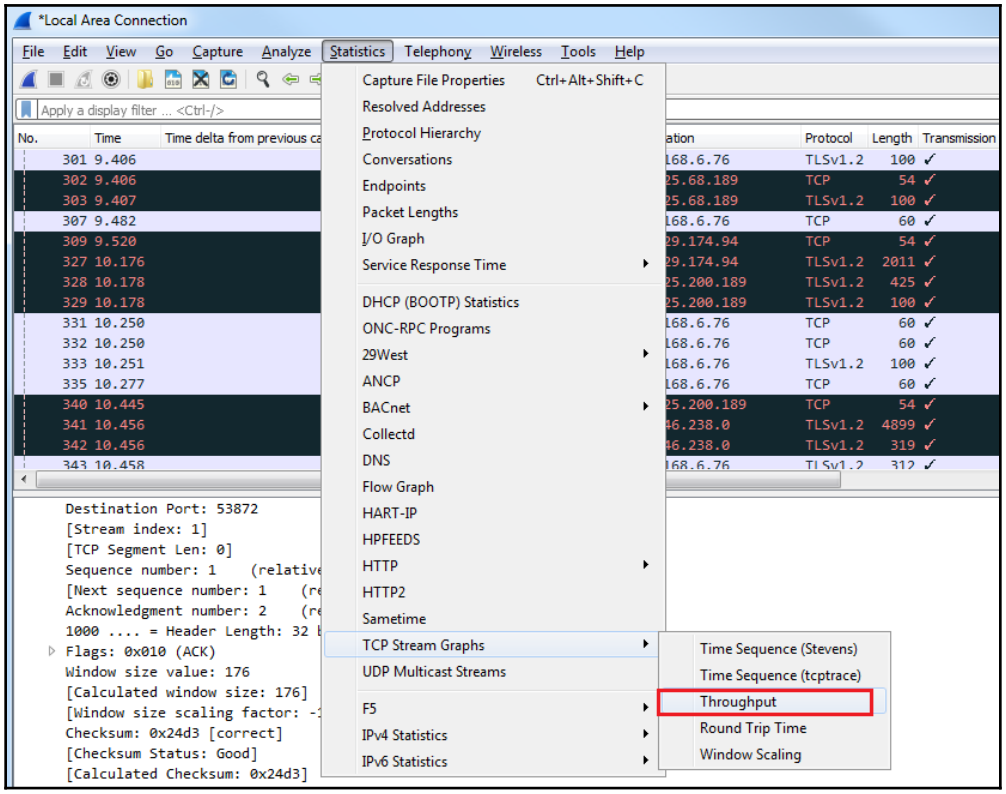

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Transmission Control Protocol Info
2234 26.946 0.000000000 192.168.77.161 54 54.225.158.137 TCP Yes [TCP ZeroWindow] 49638→443 [ACK]…
2301 26.9 .77.161 54 54.243.142.74 TCP Yes [TCP ZeroWindow] 49650→443 [ACK]…
2663 27.2 .77.161 54 54.208.100.124 TCP Yes [TCP ZeroWindow] 49614→443 [ACK]…
3615 28.5 .77.161 54 172.217.1.206 TCP Yes [TCP ZeroWindow] 49694→443 [ACK]…
10844 33.1 .77.161 54 172.217.1.193 TCP Yes [TCP ZeroWindow] 49690→443 [ACK]…
10851 33.9 .77.161 54 192.35.249.120 TCP Yes [TCP ZeroWindow] 49682→443 [ACK]…
10853 33.9 .77.161 54 162.247.242.20 TCP Yes [TCP ZeroWindow] 49729→443 [ACK]…
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

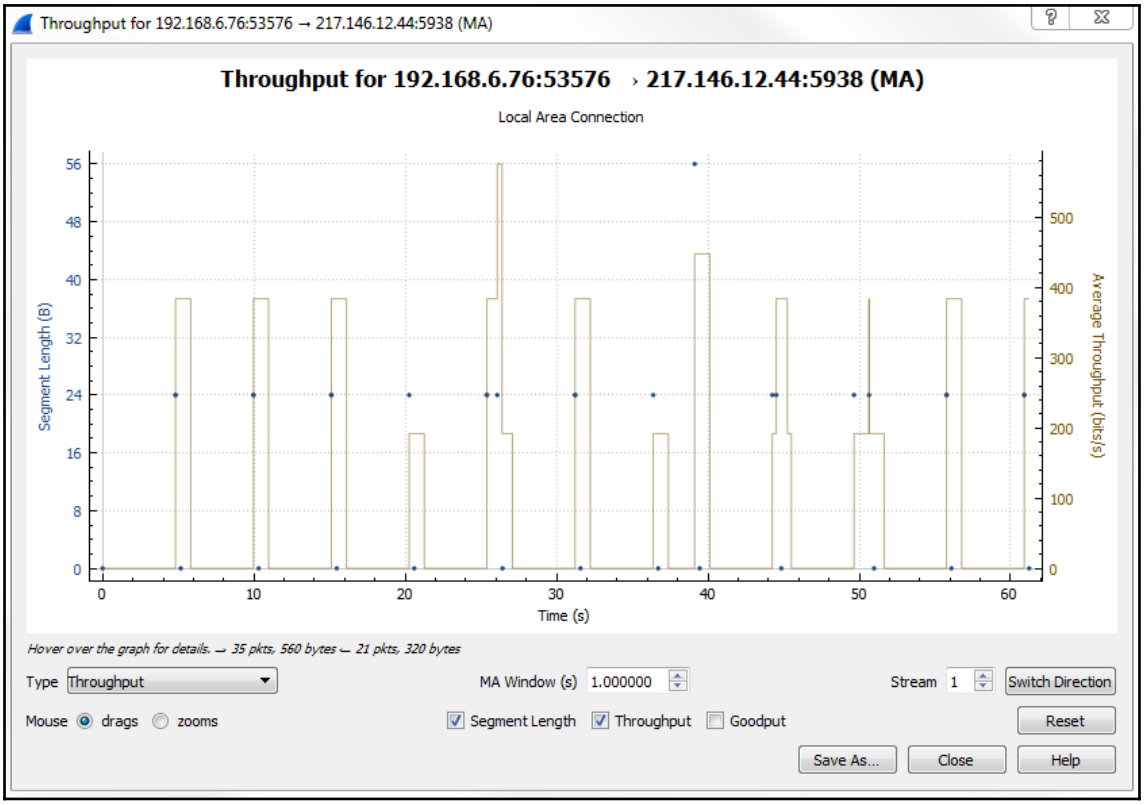

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.hdr_len > 20
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol
25 0.609 0.003823000 172.217.166.42 192.168.6.76 TCP 66 ✓
50 1.468 0.003461000 172.217.166.42 192.168.6.76 TCP 66 ✓
460 12.201 0.000229000 192.168.6.250 192.168.6.76 TCP 66 ✓
461 12.201 0.000075000 192.168.6.76 192.168.6.250 TCP 66 ✓
1072 26.160 0.001454000 192.168.6.76 162.125.81.3 TCP 66 ✓
1076 26.228 0.004901000 162.125.81.3 192.168.6.76 TCP 66 ✓
1136 27.418 0.030340000 216.58.196.78 192.168.6.76 TCP 66 ✓
1179 28.063 0.004739000 172.217.166.46 192.168.6.76 TCP 66 ✓
Frame 25: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PaloAlto_bf:66:10 (08:30:6b:bf:66:10), Dst: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Internet Protocol Version 4, Src: 172.217.166.42, Dst: 192.168.6.76
Transmission Control Protocol, Src Port: 443, Dst Port: 53872, Seq: 1, Ack: 2, Len: 0
Source Port: 443
Destination Port: 53872
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 2 (relative ack number)
1000 .... = Header Length: 32 bytes (8)

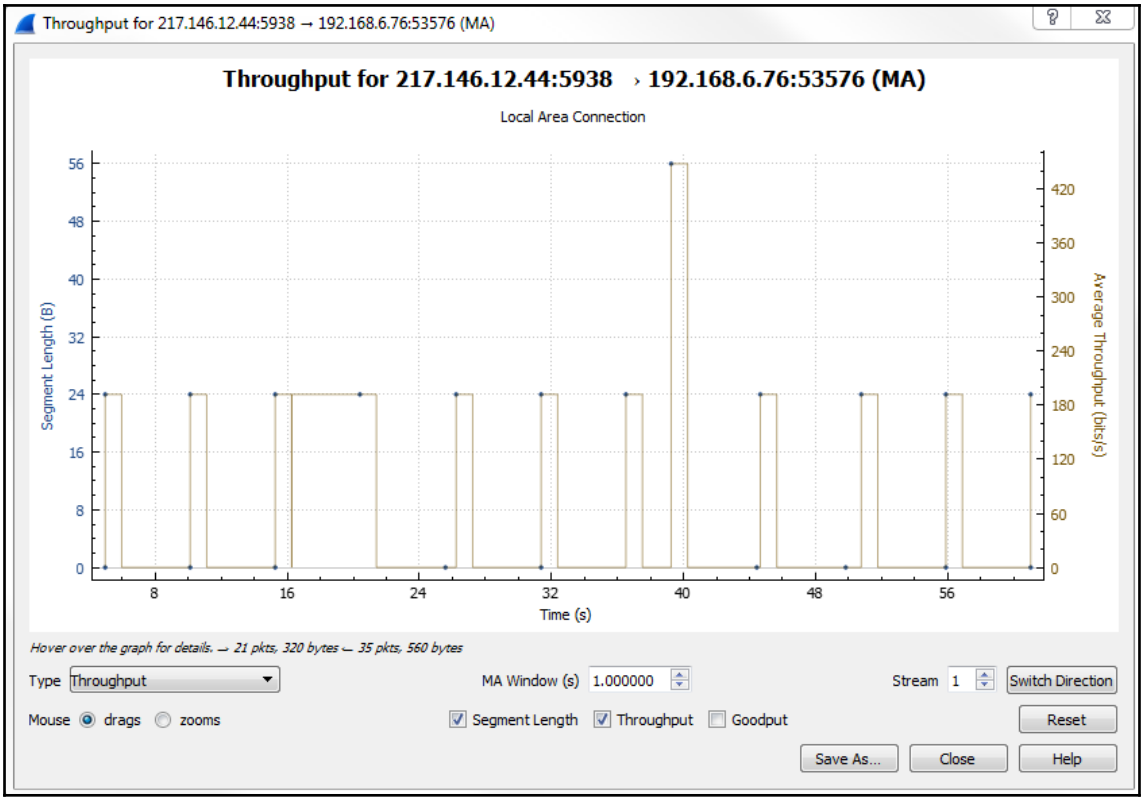

Internet Protocol Ver
Transmission Control
Source Port: 443
Destination Port:
[Stream index: 1]
[TCP Segment Len:
Sequence number: 1
[Next sequence numl
Acknowledgment numl
1000 .... = Header
Flags: 0x010 (ACK)
Window size value:
[Calculated window
[Window size scali
Checksum: 0x24d3 [
[Checksum Status:
[Calculated Checks
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), SACK
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

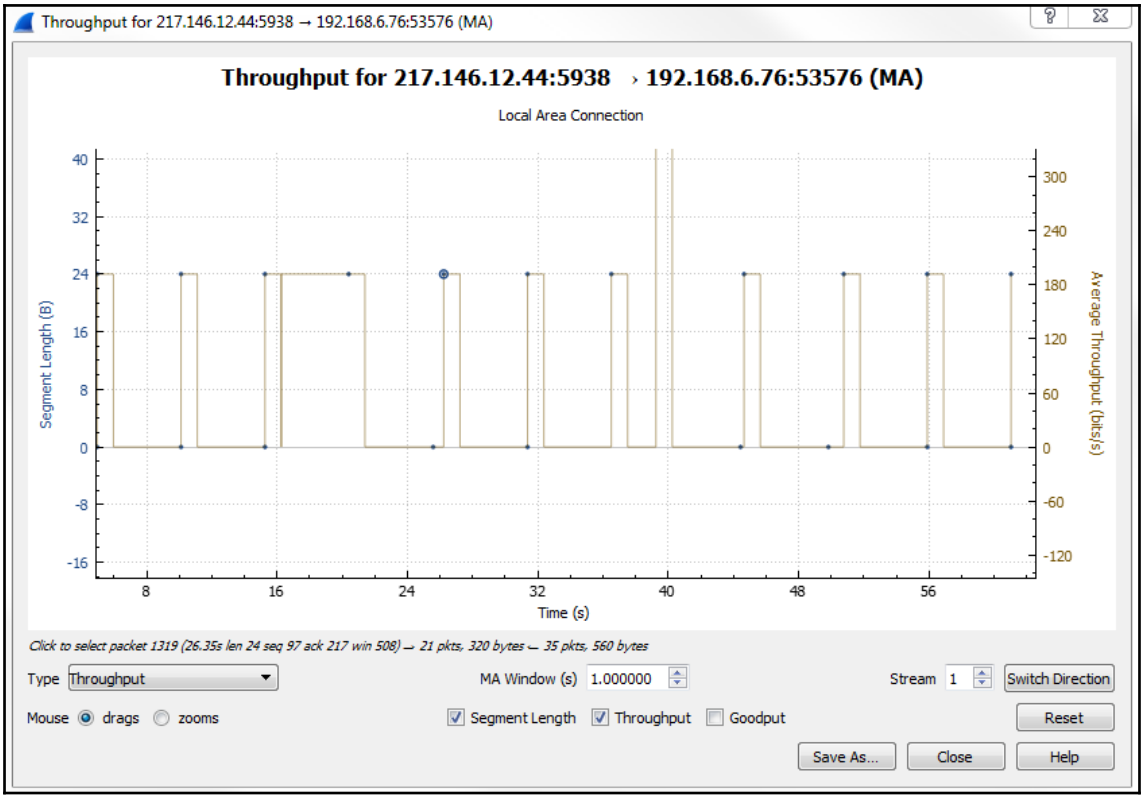

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.options
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
25 0.609 0.003823000 172.217.166.42 192.168.6.76 TCP 66 ✓ 443 → 53872 [ACK] Seq=1 Ack=2 Win=176
50 1.468 0.003461000 172.217.166.42 192.168.6.76 TCP 66 ✓ 443 → 53873 [ACK] Seq=1 Ack=2 Win=191
460 12.201 0.000229000 192.168.6.250 192.168.6.76 TCP 66 ✓ 65409 → 2869 [SYN] Seq=0 Win=64240 Le
461 12.201 0.000075000 192.168.6.76 192.168.6.250 TCP 66 ✓ 2869 → 65409 [SYN, ACK] Seq=0 Ack=1 W
1072 26.160 0.001454000 192.168.6.76 162.125.81.3 TCP 66 ✓ 53890 → 443 [SYN] Seq=0 Win=8192 [TCP
1076 26.228 0.004901000 162.125.81.3 192.168.6.76 TCP 66 ✓ 443 → 53890 [SYN, ACK] Seq=0 Ack=1 Wi
1136 27.418 0.030340000 216.58.196.78 192.168.6.76 TCP 66 ✓ 443 → 53884 [ACK] Seq=1 Ack=2 Win=186
1179 28.063 0.004739000 172.217.166.46 192.168.6.76 TCP 66 ✓ 443 → 53760 [ACK] Seq=1 Ack=2 Win=811
1217 29.682 0.001226000 192.168.6.76 162.125.81.4 TCP 66 ✓ 53891 → 443 [SYN] Seq=0 Win=8192 [TCP
1218 29.750 0.068343000 162.125.81.4 192.168.6.76 TCP 66 ✓ 443 → 53891 [SYN, ACK] Seq=0 Ack=1 Wi

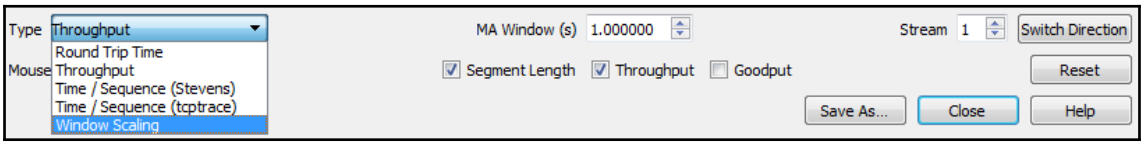

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
301 9.406 0.000001000 74.125.68.189 192.168.6.76 TLSv1.2 100 ✓ Application Data
302 9.406 0.000166000 192.168.6.76 74.125.68.189 TCP 54 ✓ 53691 → 443 [ACK] Seq=1 Ack=146 Win=2
303 9.407 0.001009000 192.168.6.76 74.125.68.189 TLSv1.2 100 ✓ Application Data
307 9.482 0.018528000 74.125.68.189 192.168.6.76 TCP 60 ✓ 443 → 53691 [ACK] Seq=146 Ack=47 Win=
309 9.520 0.006752000 192.168.6.76 52.229.174.94 TCP 54 ✓ 53827 → 443 [ACK] Seq=1958 Ack=2331 W
327 10.176 0.067679000 192.168.6.76 52.229.174.94 TLSv1.2 2011 ✓ Application Data
328 10.178 0.002110000 192.168.6.76 74.125.200.189 TLSv1.2 425 ✓ Application Data
329 10.178 0.000174000 192.168.6.76 74.125.200.189 TLSv1.2 100 ✓ Application Data

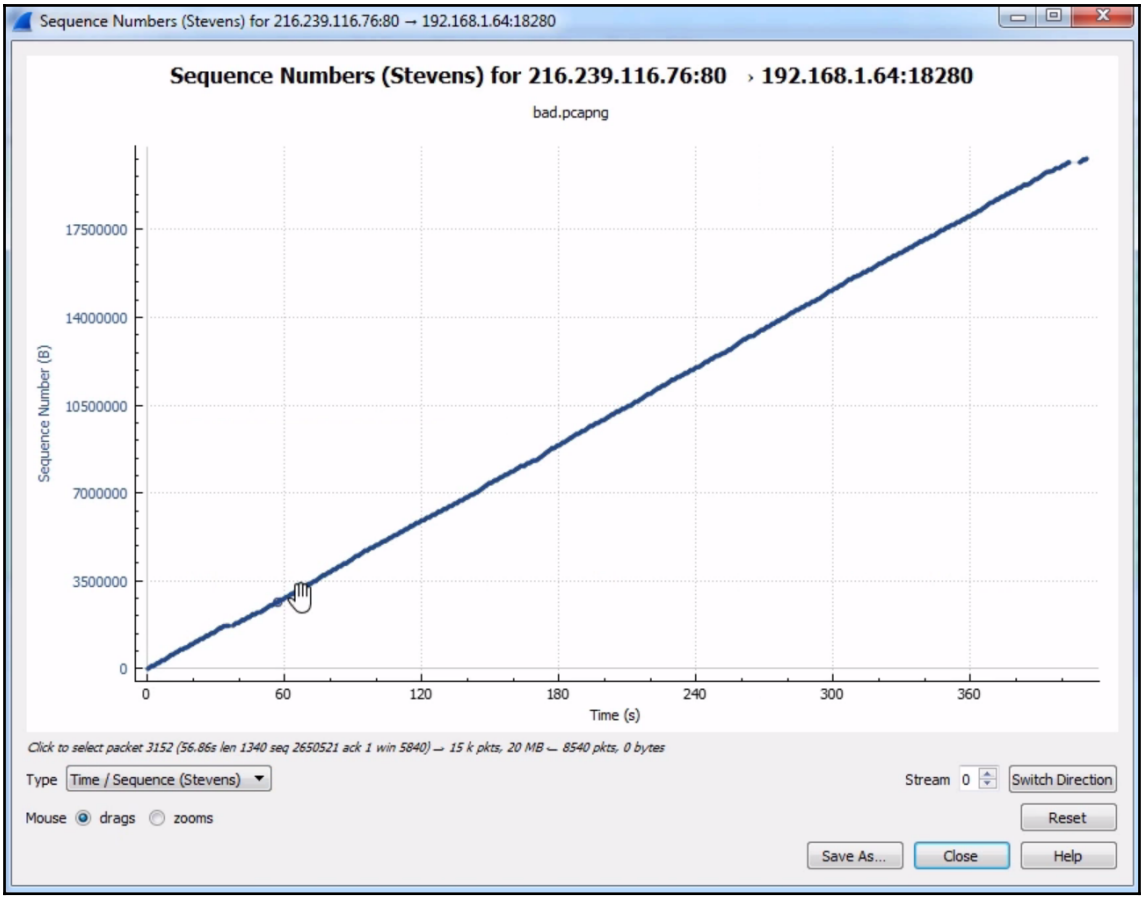

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Time delta from previous ca ation Protocol Length Transmission
301 9.406 168.6.76 TLSv1.2 100
302 9.406 25.68.189 TCP 54
303 9.407 25.68.189 TLSv1.2 100
307 9.482 168.6.76 TCP 60
309 9.520 29.174.94 TCP 54
327 10.176 29.174.94 TLSv1.2 2011
328 10.178 25.200.189 TLSv1.2 425
329 10.178 25.200.189 TLSv1.2 100
331 10.250 168.6.76 TCP 60
332 10.250 168.6.76 TCP 60
333 10.251 168.6.76 TLSv1.2 100
335 10.277 168.6.76 TCP 60
340 10.445 25.200.189 TCP 54
341 10.456 46.238.0 TLSv1.2 4899
342 10.456 46.238.0 TLSv1.2 319
343 10.458 168.6.76 TLSv1.2 312
Destination Port: 53872
[Stream index: 1]
[TCP Segment Len: 0]
Sequence number: 1 (relative
[Next sequence number: 1 (re
Acknowledgment number: 2 (re
1000 .... = Header Length: 32 b
Flags: 0x010 (ACK)
Window size value: 176
[Calculated window size: 176]
[Window size scaling factor: -1
Checksum: 0x24d3 [correct]
[Checksum Status: Good]
[Calculated Checksum: 0x24d3]
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
F5
IPv4 Statistics
IPv6 Statistics
Time Sequence (Stevens)
Time Sequence (tcptrace)
Throughput
Round Trip Time
Window Scaling

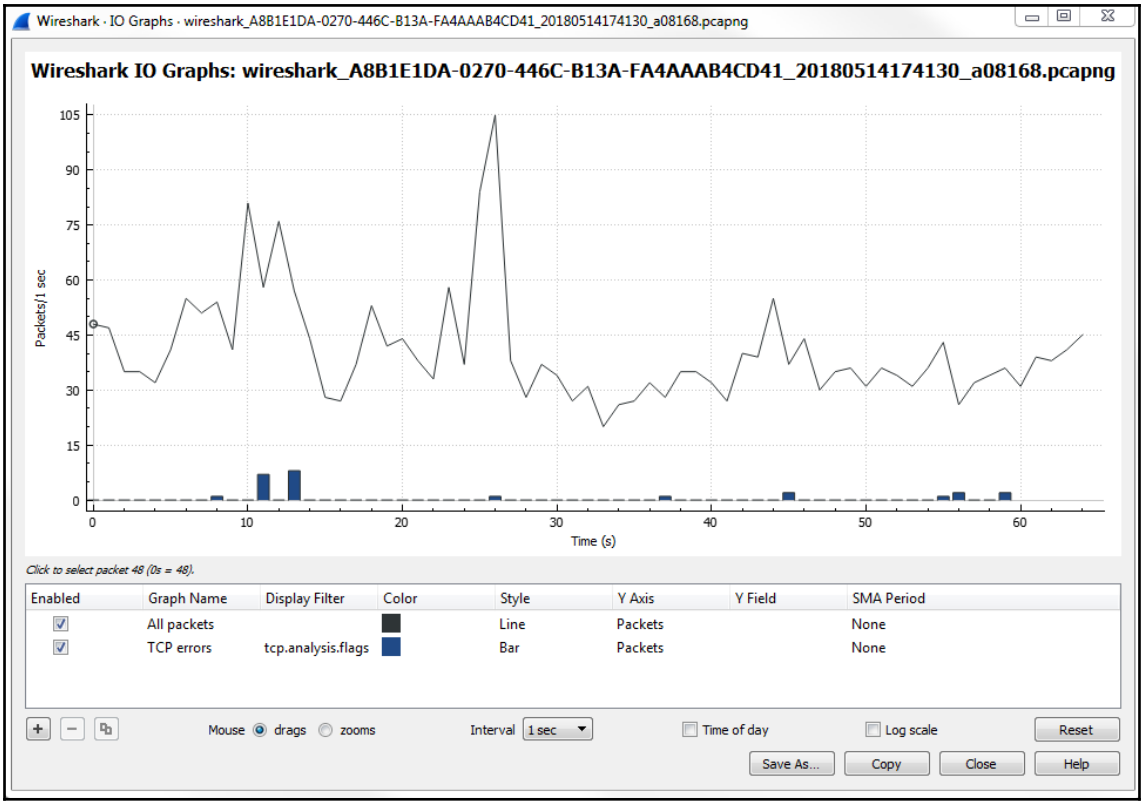

Throughput for 192.168.6.76:53576 → 217.146.12.44:5938 (MA)
Throughput for 192.168.6.76:53576 › 217.146.12.44:5938 (MA)
Local Area Connection
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Hover over the graph for details. ⇀ 35 pkts, 560 bytes ↽ 21 pkts, 320 bytes
Type Throughput
MA Window (s) 1.000000
Stream 1
Switch Direction
Mouse drags zooms
Segment Length
Throughput
Goodput
Reset
Save As...
Close
Help

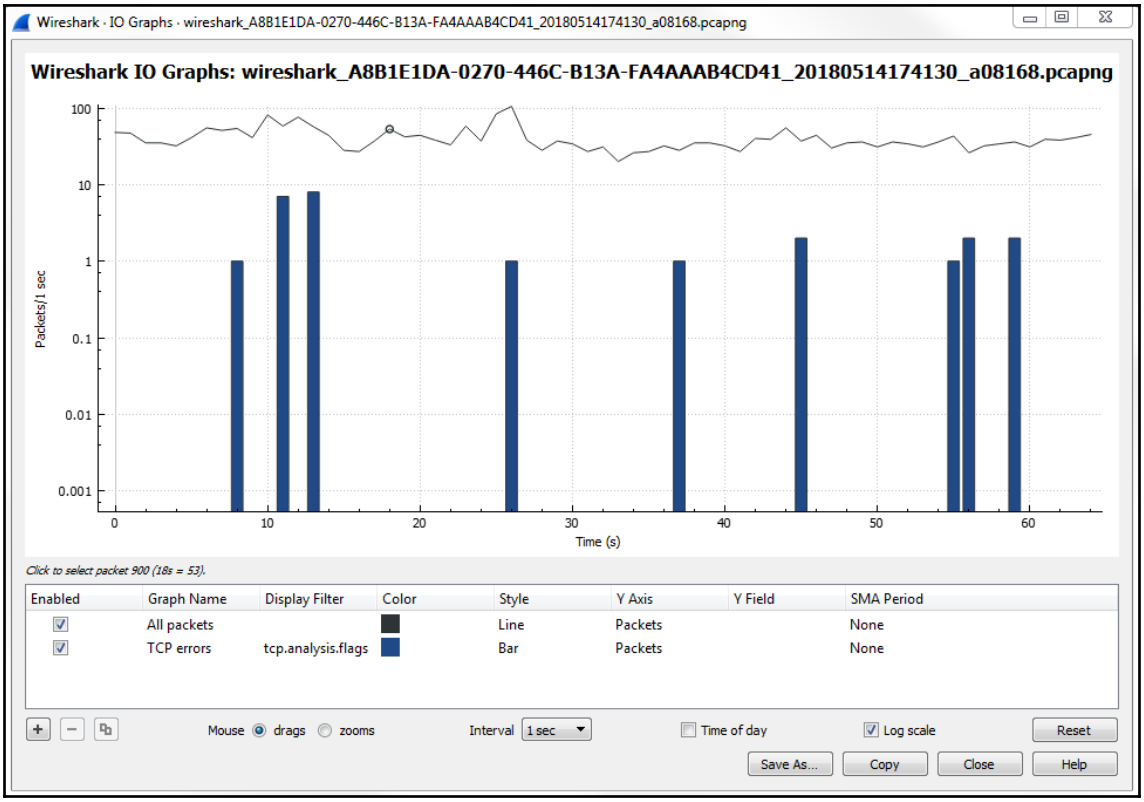

Throughput for 217.146.12.44:5938 → 192.168.6.76:53576 (MA)
Throughput for 217.146.12.44:5938 › 192.168.6.76:53576 (MA)
Local Area Connection
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Hover over the graph for details. → 21 pkts, 320 bytes ← 35 pkts, 560 bytes
Type Throughput
MA Window (s) 1.000000
Stream 1
Switch Direction
Mouse drags zooms
Segment Length
Throughput
Goodput
Reset
Save As...
Close
Help

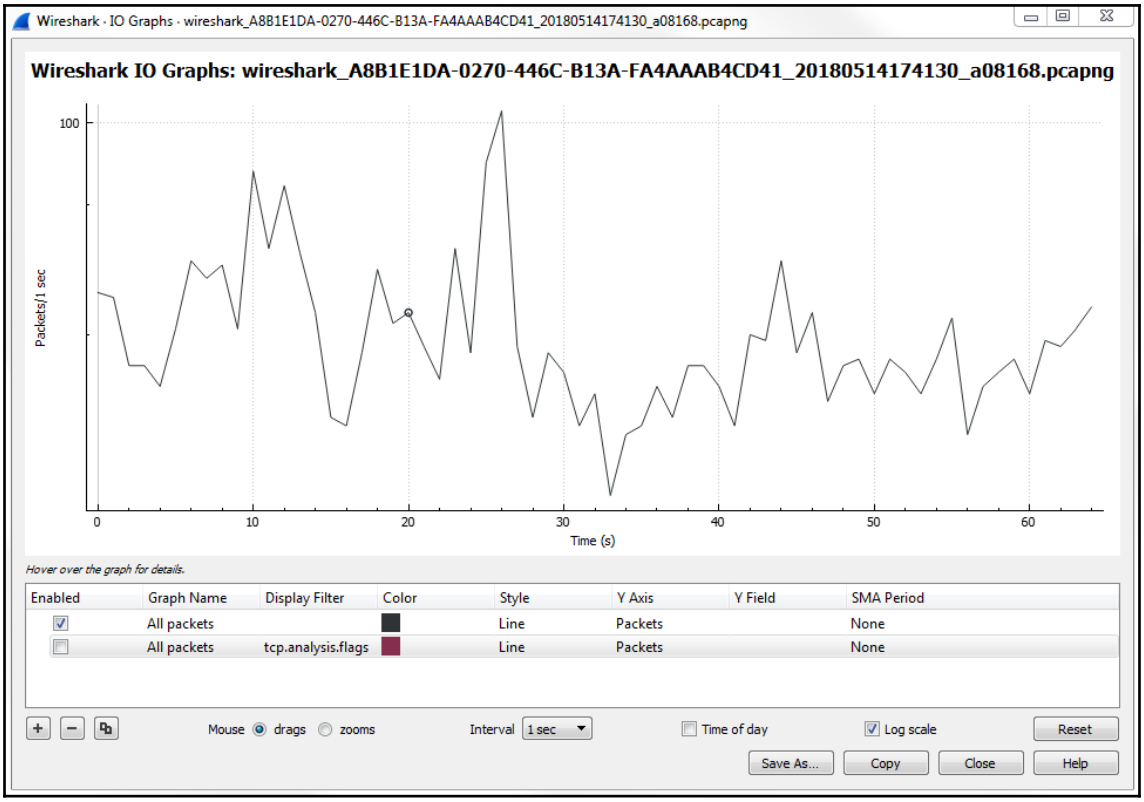

Throughput for 217.146.12.44:5938 → 192.168.6.76:53576 (MA)
Throughput for 217.146.12.44:5938 › 192.168.6.76:53576 (MA)
Local Area Connection
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Click to select packet 1319 (26.35s len 24 seq 97 ack 217 win 508) → 21 pkts, 320 bytes ← 35 pkts, 560 bytes
Type Throughput
MA Window (s) 1.000000
Stream 1
Switch Direction
Mouse drags zooms
Segment Length
Throughput
Goodput
Reset
Save As...
Close
Help

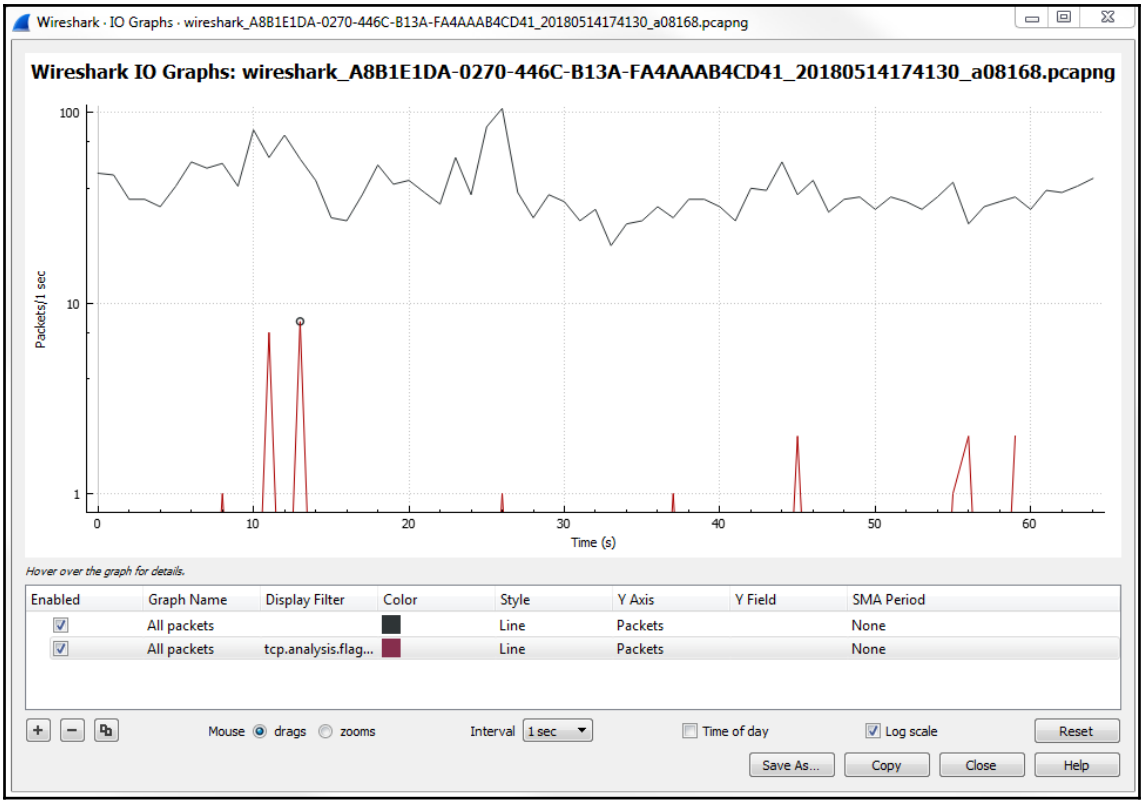

Type Throughput
Round Trip Time
Throughput
Time / Sequence (Stevens)
Time / Sequence (tcptrace)
Window Scaling
MA Window (s) 1.000000
Stream 1
Switch Direction
Mouse
Segment Length
Throughput
Goodput
Reset
Save As...
Close
Help


Sequence Numbers (Stevens) for 216.239.116.76:80 → 192.168.1.64:18280
Sequence Numbers (Stevens) for 216.239.116.76:80 › 192.168.1.64:18280
bad.pcapng
Sequence Number (B)
17500000
14000000
10500000
7000000
3500000
0
0
60
120
180
240
300
360
Time (s)
Click to select packet 3152 (56.86s len 1340 seq 2650521 ack 1 win 5840) ⇀ 15 k pkts, 20 MB ↽ 8540 pkts, 0 bytes
Type
Time / Sequence (Stevens)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

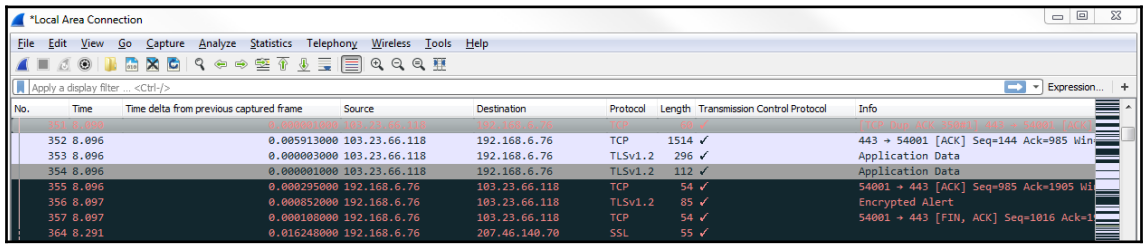

Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Packets/1 sec
105
90
75
60
45
30
15
0
0
10
20
30
40
50
60
Time (s)
Click to select packet 48 (0s = 48).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
TCP errors
tcp.analysis.flags
Bar
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

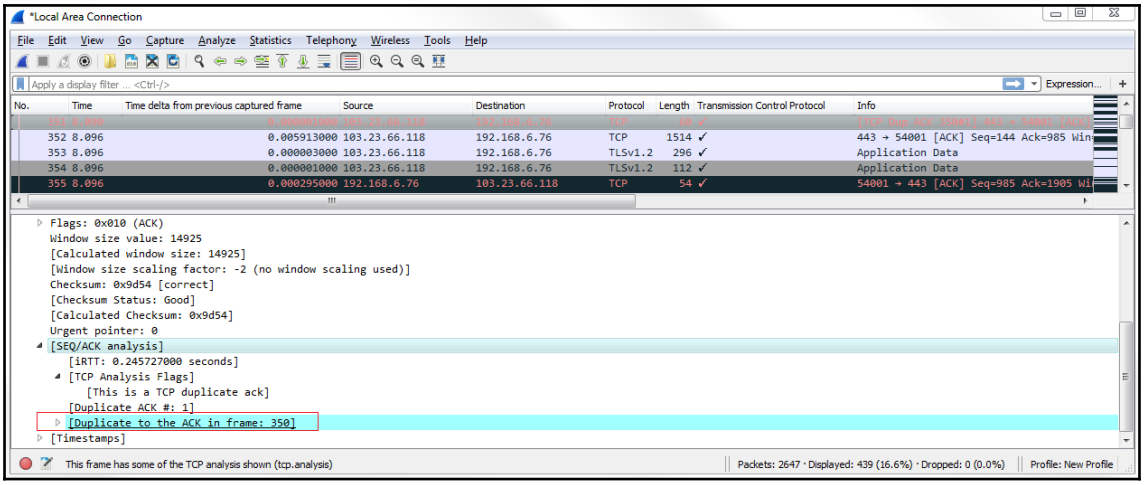

Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Packets/1 sec
100
10
1
0.1
0.01
0.001
0
10
20
30
40
50
60
Time (s)
Click to select packet 900 (18s = 53).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
TCP errors
tcp.analysis.flags
Bar
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

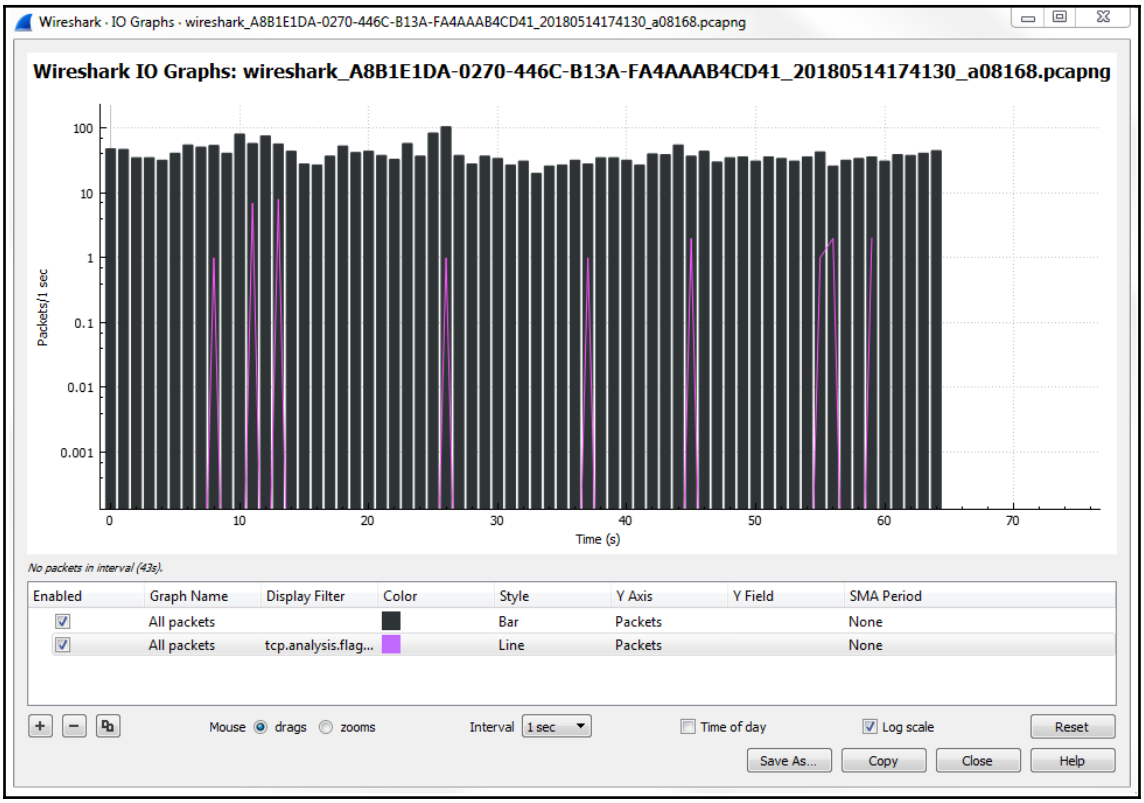

Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
100
Packets/1 sec
0
10
20
30
40
50
60
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
All packets
tcp.analysis.flags
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help


Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
100
10
1
Packets/1 sec
0
10
20
30
40
50
60
Time (s)
Hover over the graph for details.
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
All packets
tcp.analysis.flag...
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

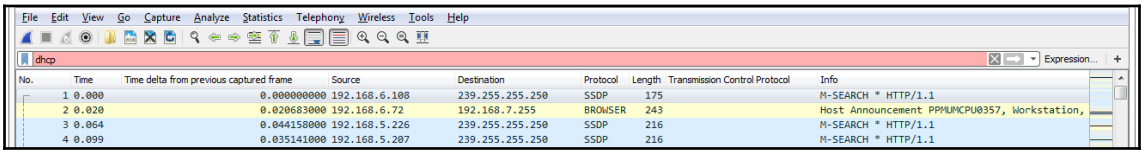

Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Packets/1 sec
100
10
1
0.1
0.01
0.001
0
10
20
30
40
50
60
Time (s)
No packets in interval (0s).
Enabled
Graph Name
Display Filter
Color
Style
Y Axis
Y Field
SMA Period
All packets
Line
Packets
None
All packets
tcp.analysis.flag...
Bar
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

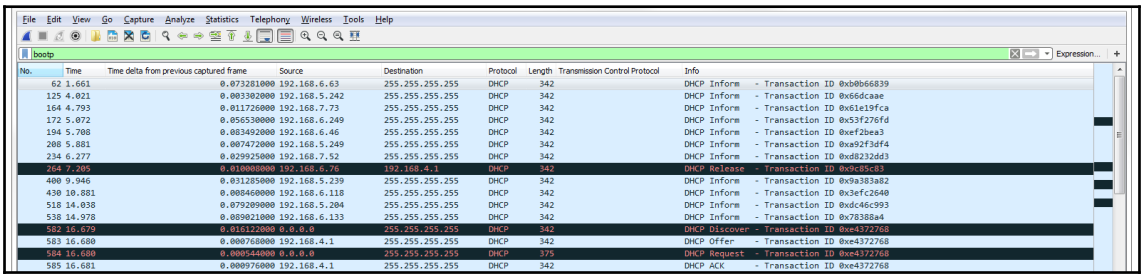

*Local Area Connection
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Expression...
No.
Time
Time delta from previous captured frame
Source
Destination
Protocol
Length
Transmission Control Protocol
Info
352 8.096 0.005913000 103.23.66.118 192.168.6.76 TCP 1514 ✓ 443 → 54001 [ACK] Seq=144 Ack=985 Win
353 8.096 0.000003000 103.23.66.118 192.168.6.76 TLSv1.2 296 ✓ Application Data
354 8.096 0.000001000 103.23.66.118 192.168.6.76 TLSv1.2 112 ✓ Application Data
355 8.096 0.000295000 192.168.6.76 103.23.66.118 TCP 54 ✓ 54001 → 443 [ACK] Seq=985 Ack=1905 Wi
356 8.097 0.000852000 192.168.6.76 103.23.66.118 TLSv1.2 85 ✓ Encrypted Alert
357 8.097 0.000108000 192.168.6.76 103.23.66.118 TCP 54 ✓ 54001 → 443 [FIN, ACK] Seq=1016 Ack=1
364 8.291 0.016248000 192.168.6.76 207.46.140.70 SSL 55 ✓

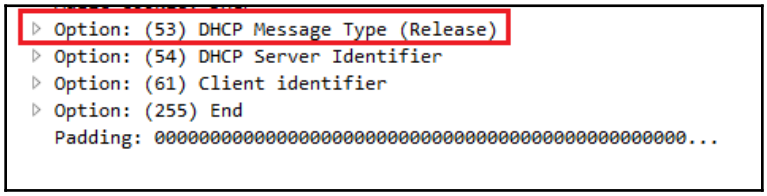

*Local Area Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
352 8.096 0.005913000 103.23.66.118 192.168.6.76 TCP 1514 443 → 54001 [ACK] Seq=144 Ack=985 Win
353 8.096 0.000003000 103.23.66.118 192.168.6.76 TLSv1.2 296 Application Data
354 8.096 0.000001000 103.23.66.118 192.168.6.76 TLSv1.2 112 Application Data
355 8.096 0.000295000 192.168.6.76 103.23.66.118 TCP 54 54001 → 443 [ACK] Seq=985 Ack=1905 Wi
Flags: 0x010 (ACK)
Window size value: 14925
[Calculated window size: 14925]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x9d54 [correct]
[Checksum Status: Good]
[Calculated Checksum: 0x9d54]
Urgent pointer: 0
[SEQ/ACK analysis]
[iRTT: 0.245727000 seconds]
[TCP Analysis Flags]
[This is a TCP duplicate ack]
[Duplicate ACK #: 1]
[Duplicate to the ACK in frame: 350]
[Timestamps]
This frame has some of the TCP analysis shown (tcp.analysis)
Packets: 2647 · Displayed: 439 (16.6%) · Dropped: 0 (0.0%)
Profile: New Profile

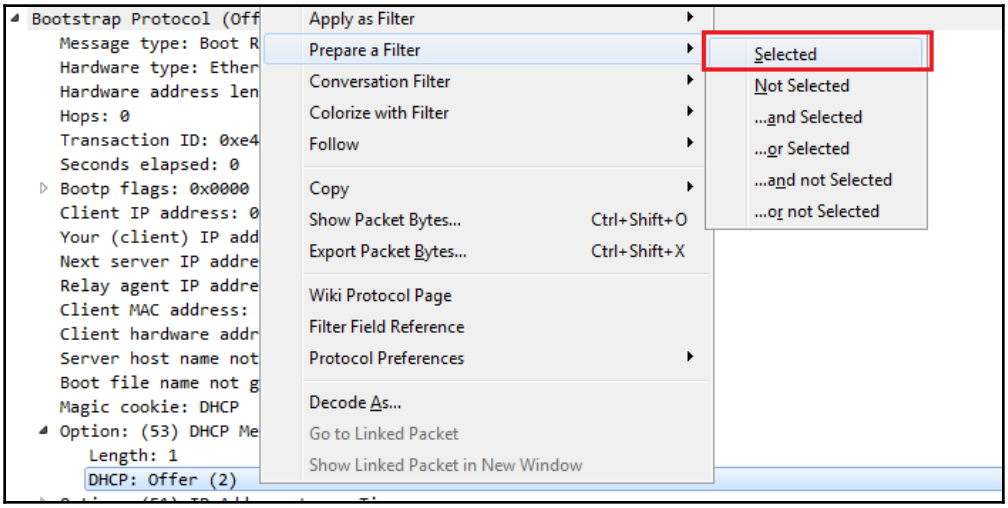

Wireshark · IO Graphs · wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Wireshark IO Graphs: wireshark_A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41_20180514174130_a08168.pcapng
Packets/1 sec
100
10
1
0.1
0.01
0.001
0
10
20
30
40
50
60
70
Time (s)
No packets in interval (43s).
Enabled Graph Name Display Filter Color Style Y Axis Y Field SMA Period
All packets Bar Packets None
All packets tcp.analysis.flag... Line Packets None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

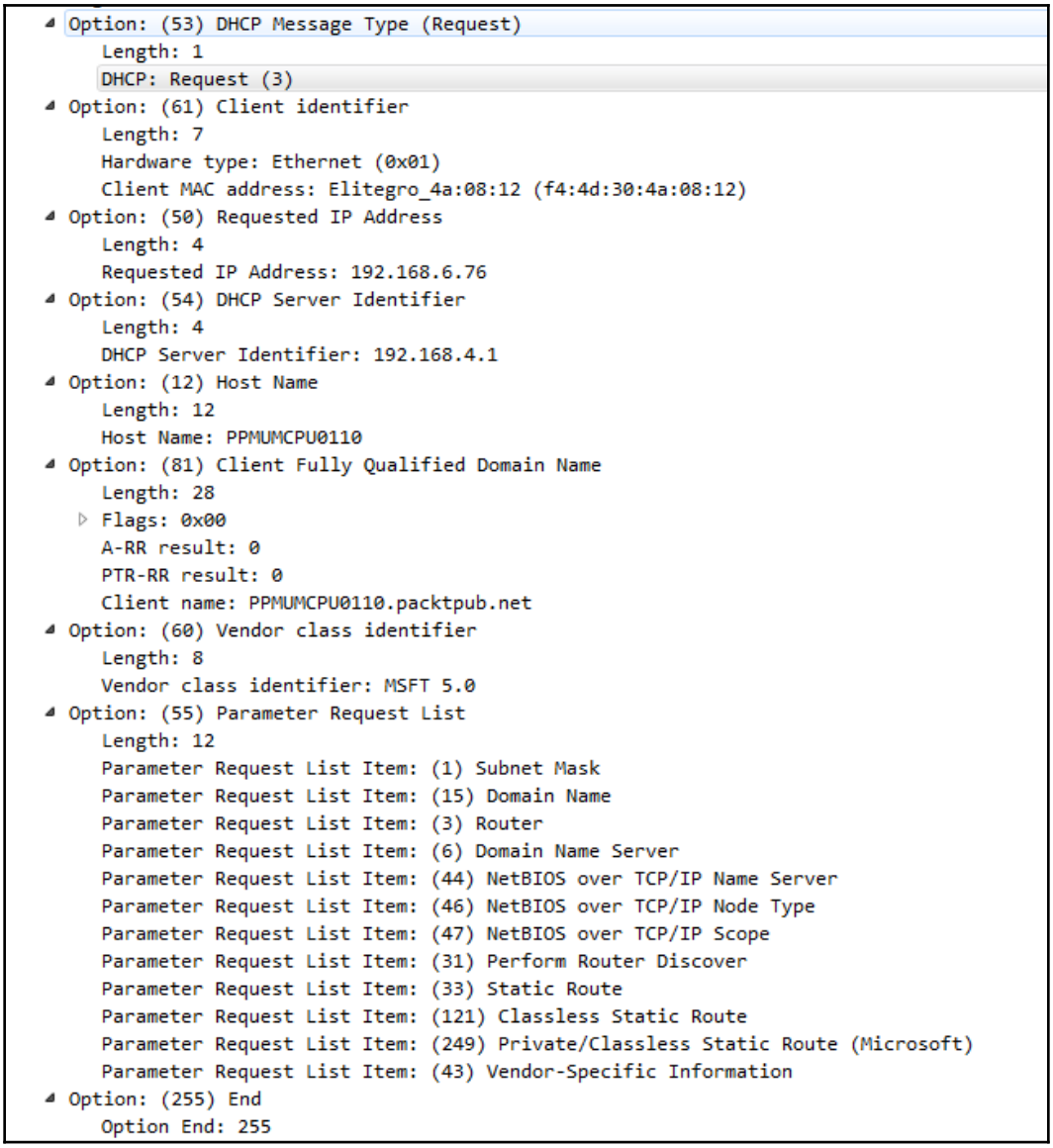
Chapter 08: Application Protocol Analysis I

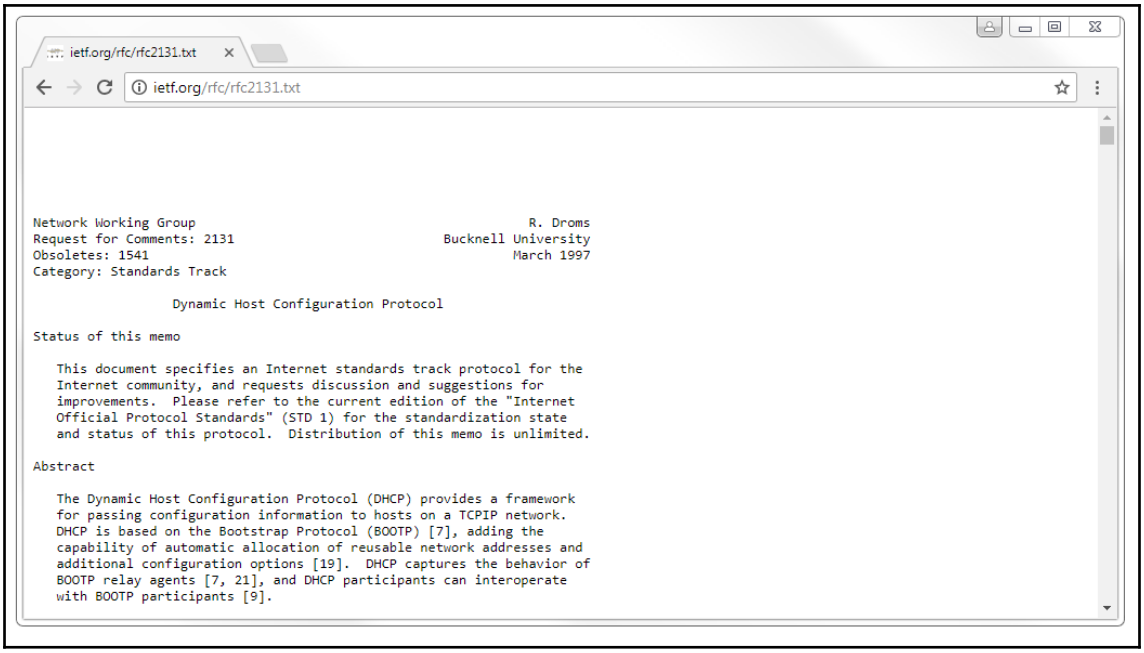






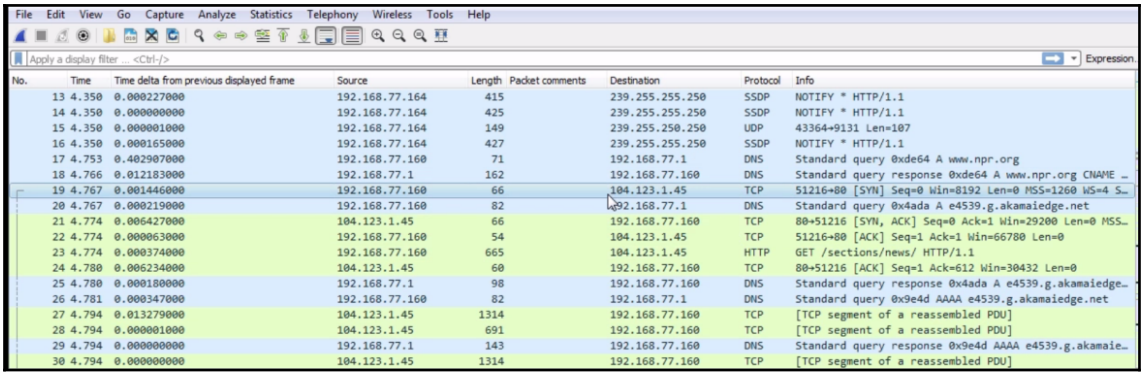


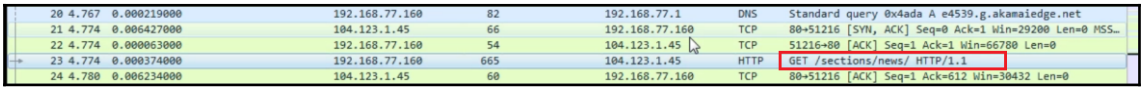

Option: (53) DHCP Message Type (Request)
Length: 1
DHCP: Request (3)
Option: (61) Client identifier
Length: 7
Hardware type: Ethernet (0x01)
Client MAC address: Elitegro_4a:08:12 (f4:4d:30:4a:08:12)
Option: (50) Requested IP Address
Length: 4
Requested IP Address: 192.168.6.76
Option: (54) DHCP Server Identifier
Length: 4
DHCP Server Identifier: 192.168.4.1
Option: (12) Host Name
Length: 12
Host Name: PPMUMCPU0110
Option: (81) Client Fully Qualified Domain Name
Length: 28
Flags: 0x00
A-RR result: 0
PTR-RR result: 0
Client name: PPMUMCPU0110.packtpub.net
Option: (60) Vendor class identifier
Length: 8
Vendor class identifier: MSFT 5.0
Option: (55) Parameter Request List
Length: 12
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (3) Router
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
Parameter Request List Item: (31) Perform Router Discover
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (43) Vendor-Specific Information
Option: (255) End
Option End: 255

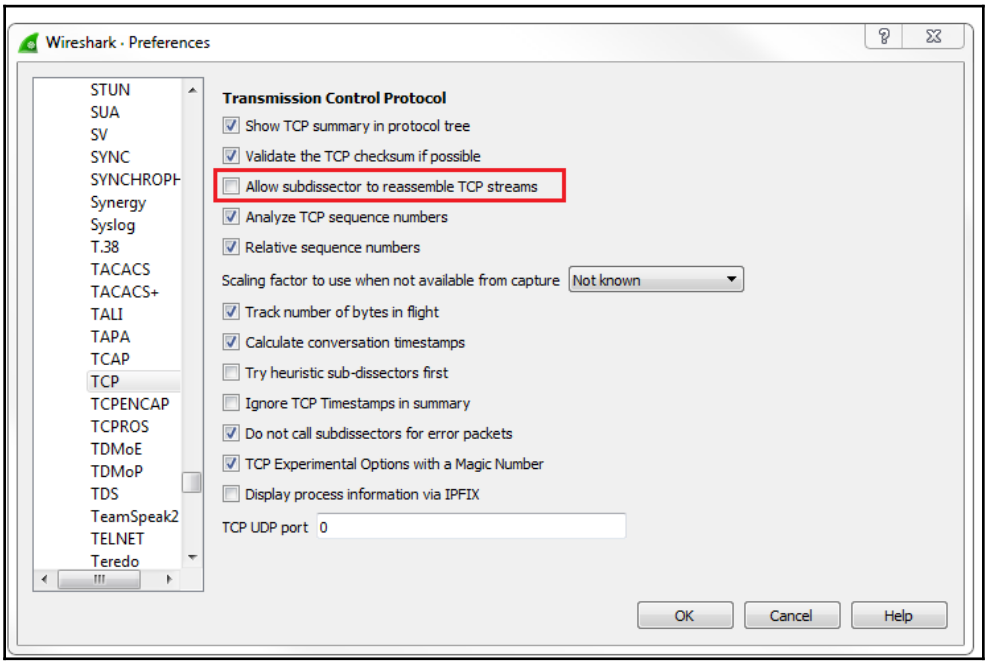


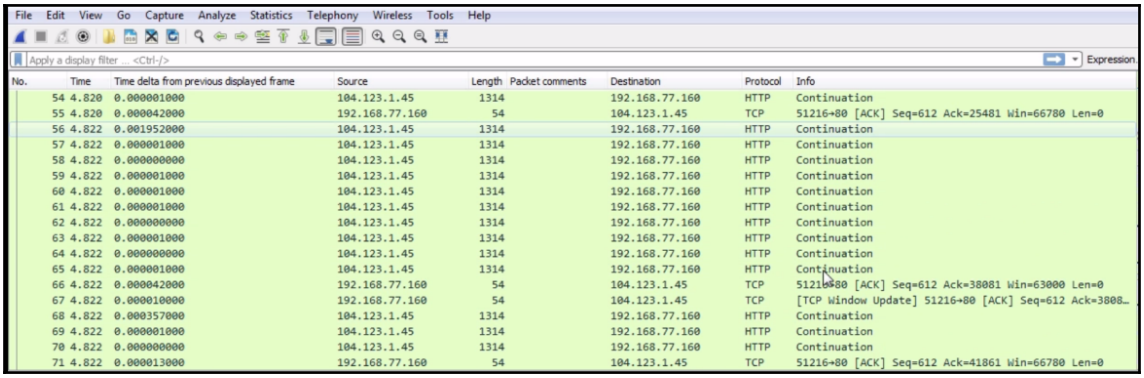
62	1.661	0.073281000	192.168.6.63	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xb0b66839
125	4.021	0.003302000	192.168.5.242	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x66dcaae
164	4.793	0.011726000	192.168.7.73	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x61e19fca
172	5.072	0.056530000	192.168.6.249	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x53f276fd
194	5.708	0.083492000	192.168.6.46	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0xef2bea3

```
▲ Option: (55) Parameter Request List
    Length: 13
    Parameter Request List Item: (1) Subnet Mask
    Parameter Request List Item: (15) Domain Name
    Parameter Request List Item: (3) Router
    Parameter Request List Item: (6) Domain Name Server
    Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
    Parameter Request List Item: (46) NetBIOS over TCP/IP Node Type
    Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
    Parameter Request List Item: (31) Perform Router Discover
    Parameter Request List Item: (33) Static Route
    Parameter Request List Item: (121) Classless Static Route
    Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
    Parameter Request List Item: (43) Vendor-Specific Information
    Parameter Request List Item: (252) Private/Proxy autodiscovery
```

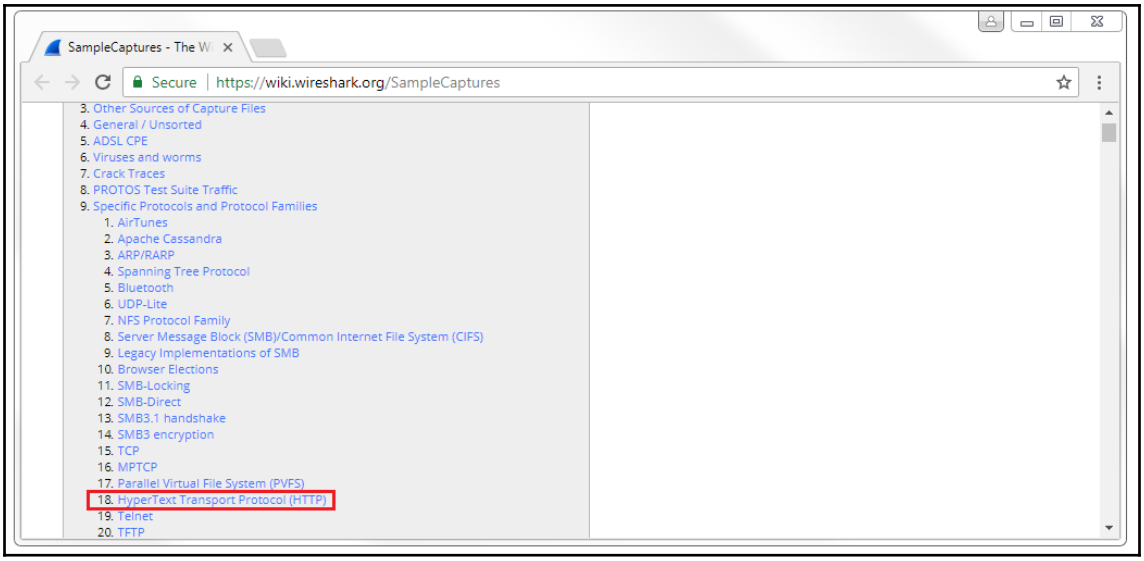

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
13 4.350 0.000227000 192.168.77.164 415 239.255.255.250 SSDP NOTIFY * HTTP/1.1
14 4.350 0.000000000 192.168.77.164 425 239.255.255.250 SSDP NOTIFY * HTTP/1.1
15 4.350 0.000001000 192.168.77.164 149 239.255.250.250 UDP 43364→9131 Len=107
16 4.350 0.000165000 192.168.77.164 427 239.255.255.250 SSDP NOTIFY * HTTP/1.1
17 4.753 0.402907000 192.168.77.160 71 192.168.77.1 DNS Standard query 0xde64 A www.npr.org
18 4.766 0.012183000 192.168.77.1 162 192.168.77.160 DNS Standard query response 0xde64 A www.npr.org CNAME …
19 4.767 0.001446000 192.168.77.160 66 104.123.1.45 TCP 51216→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=4 S…
20 4.767 0.000219000 192.168.77.160 82 192.168.77.1 DNS Standard query 0x4ada A e4539.g.akamaiedge.net
21 4.774 0.006427000 104.123.1.45 66 192.168.77.160 TCP 80→51216 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS…
22 4.774 0.000063000 192.168.77.160 54 104.123.1.45 TCP 51216→80 [ACK] Seq=1 Ack=1 Win=66780 Len=0
23 4.774 0.000374000 192.168.77.160 665 104.123.1.45 HTTP GET /sections/news/ HTTP/1.1
24 4.780 0.006234000 104.123.1.45 60 192.168.77.160 TCP 80→51216 [ACK] Seq=1 Ack=612 Win=30432 Len=0
25 4.780 0.000180000 192.168.77.1 98 192.168.77.160 DNS Standard query response 0x4ada A e4539.g.akamaiedge…
26 4.781 0.000347000 192.168.77.160 82 192.168.77.1 DNS Standard query 0x9e4d AAAA e4539.g.akamaiedge.net
27 4.794 0.013279000 104.123.1.45 1314 192.168.77.160 TCP [TCP segment of a reassembled PDU]
28 4.794 0.000001000 104.123.1.45 691 192.168.77.160 TCP [TCP segment of a reassembled PDU]
29 4.794 0.000000000 192.168.77.1 143 192.168.77.160 DNS Standard query response 0x9e4d AAAA e4539.g.akamaie…
30 4.794 0.000000000 104.123.1.45 1314 192.168.77.160 TCP [TCP segment of a reassembled PDU]

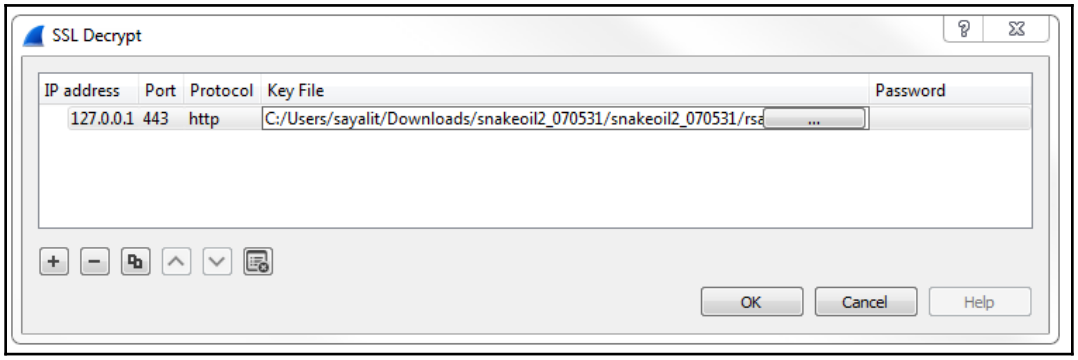

20 4.767 0.000219000 192.168.77.160 82 192.168.77.1 DNS Standard query 0x4ada A e4539.g.akamaiedge.net
21 4.774 0.006427000 104.123.1.45 66 192.168.77.160 TCP 80→51216 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS…
22 4.774 0.000063000 192.168.77.160 54 104.123.1.45 TCP 51216→80 [ACK] Seq=1 Ack=1 Win=66780 Len=0
23 4.774 0.000374000 192.168.77.160 665 104.123.1.45 HTTP GET /sections/news/ HTTP/1.1
24 4.780 0.006234000 104.123.1.45 60 192.168.77.160 TCP 80→51216 [ACK] Seq=1 Ack=612 Win=30432 Len=0

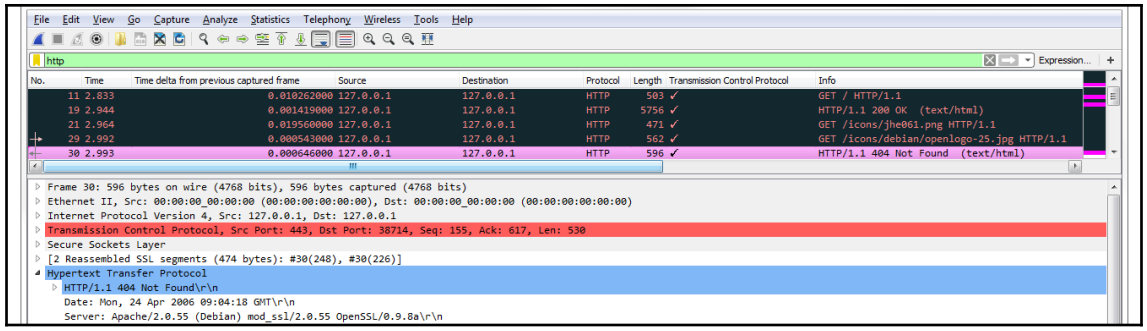

Wireshark · Preferences
STUN
SUA
SV
SYNC
SYNCHROPH
Synergy
Syslog
T.38
TACACS
TACACS+
TALI
TAPA
TCAP
TCP
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TELNET
Teredo
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Analyze TCP sequence numbers
Relative sequence numbers
Scaling factor to use when not available from capture
Not known
Track number of bytes in flight
Calculate conversation timestamps
Try heuristic sub-dissectors first
Ignore TCP Timestamps in summary
Do not call subdissectors for error packets
TCP Experimental Options with a Magic Number
Display process information via IPFIX
TCP UDP port
0
OK
Cancel
Help

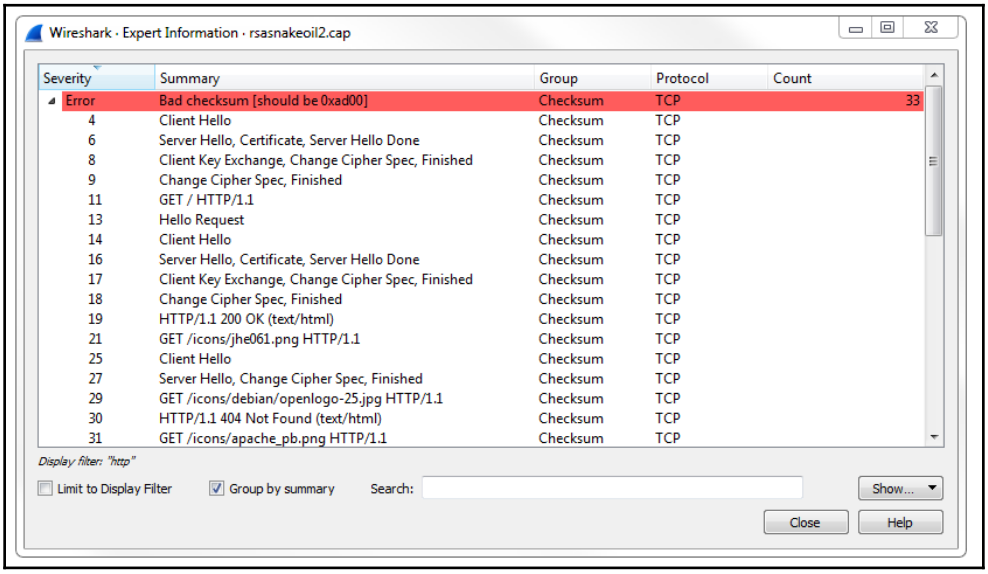

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
54 4.820 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
55 4.820 0.000042000 192.168.77.160 54 104.123.1.45 TCP 51216→80 [ACK] Seq=612 Ack=25481 Win=66780 Len=0
56 4.822 0.001952000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
57 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
58 4.822 0.000000000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
59 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
60 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
61 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
62 4.822 0.000000000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
63 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
64 4.822 0.000000000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
65 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
66 4.822 0.000042000 192.168.77.160 54 104.123.1.45 TCP 51216→80 [ACK] Seq=612 Ack=38081 Win=63000 Len=0
67 4.822 0.000010000 192.168.77.160 54 104.123.1.45 TCP [TCP Window Update] 51216→80 [ACK] Seq=612 Ack=3808…
68 4.822 0.000357000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
69 4.822 0.000001000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
70 4.822 0.000000000 104.123.1.45 1314 192.168.77.160 HTTP Continuation
71 4.822 0.000013000 192.168.77.160 54 104.123.1.45 TCP 51216→80 [ACK] Seq=612 Ack=41861 Win=66780 Len=0

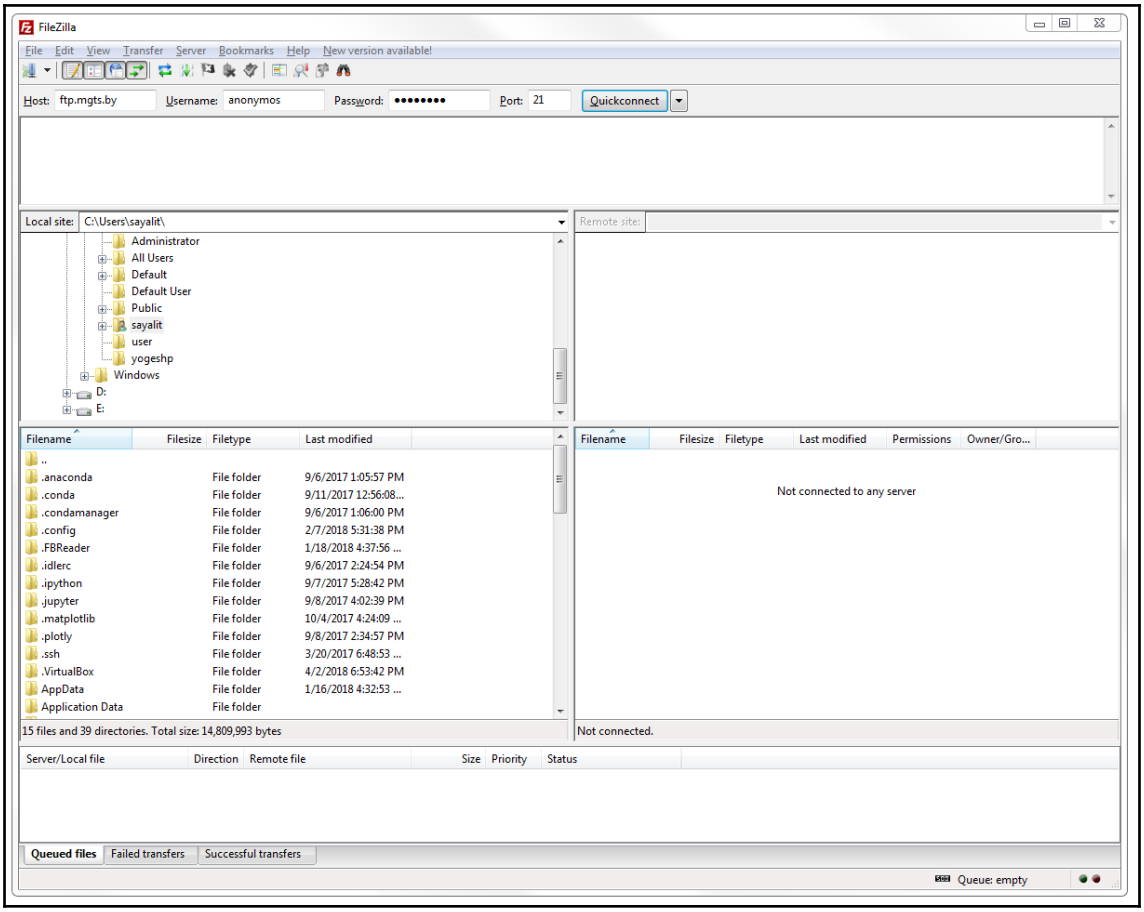

Line-based text data: text/html
[truncated]<!doctype html><html class="no-js" lang="en"><head><script type="text/javascript">(window.NREUM||(NREUM={})).loader_config={xpid:"UwcOV1NACwcHVlFbAw=="};window.NR

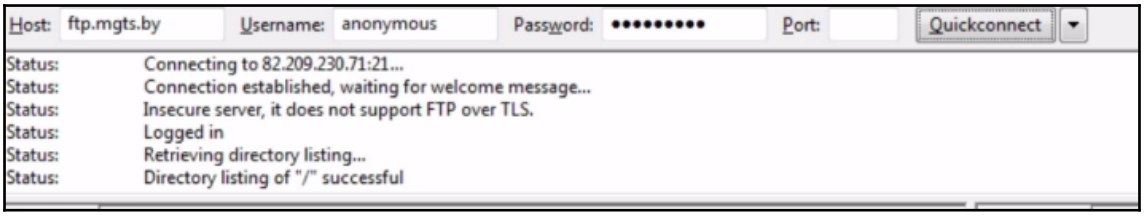

SampleCaptures - The W
Secure | https://wiki.wireshark.org/SampleCaptures
3. Other Sources of Capture Files
4. General / Unsorted
5. ADSL CPE
6. Viruses and worms
7. Crack Traces
8. PROTOS Test Suite Traffic
9. Specific Protocols and Protocol Families
1. AirTunes
2. Apache Cassandra
3. ARP/RARP
4. Spanning Tree Protocol
5. Bluetooth
6. UDP-Lite
7. NFS Protocol Family
8. Server Message Block (SMB)/Common Internet File System (CIFS)
9. Legacy Implementations of SMB
10. Browser Elections
11. SMB-Locking
12. SMB-Direct
13. SMB3.1 handshake
14. SMB3 encryption
15. TCP
16. MPTCP
17. Parallel Virtual File System (PVFS)
18. HyperText Transport Protocol (HTTP)
19. Telnet
20. TFTP

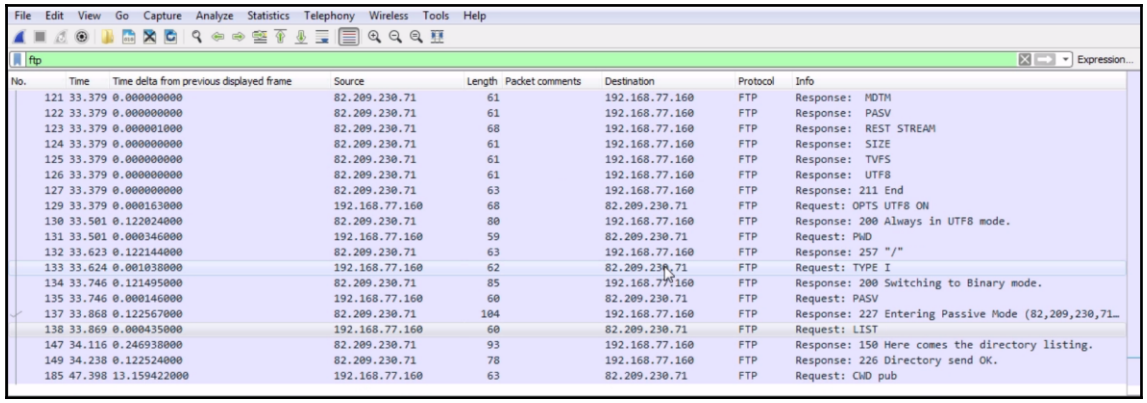

SSL Decrypt
IP address
Port
Protocol
Key File
Password
127.0.0.1 443 http C:/Users/sayalit/Downloads/snakeoil2_070531/snakeoil2_070531/rsa ...
OK
Cancel
Help


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
11 2.833 0.010262000 127.0.0.1 127.0.0.1 HTTP 503 ✓ GET / HTTP/1.1
19 2.944 0.001419000 127.0.0.1 127.0.0.1 HTTP 5756 ✓ HTTP/1.1 200 OK (text/html)
21 2.964 0.019560000 127.0.0.1 127.0.0.1 HTTP 471 ✓ GET /icons/jhe061.png HTTP/1.1
29 2.992 0.000543000 127.0.0.1 127.0.0.1 HTTP 562 ✓ GET /icons/debian/openlogo-25.jpg HTTP/1.1
30 2.993 0.000646000 127.0.0.1 127.0.0.1 HTTP 596 ✓ HTTP/1.1 404 Not Found (text/html)
Frame 30: 596 bytes on wire (4768 bits), 596 bytes captured (4768 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 443, Dst Port: 38714, Seq: 155, Ack: 617, Len: 530
Secure Sockets Layer
[2 Reassembled SSL segments (474 bytes): #30(248), #30(226)]
Hypertext Transfer Protocol
HTTP/1.1 404 Not Found\r\n
Date: Mon, 24 Apr 2006 09:04:18 GMT\r\n
Server: Apache/2.0.55 (Debian) mod_ssl/2.0.55 OpenSSL/0.9.8a\r\n

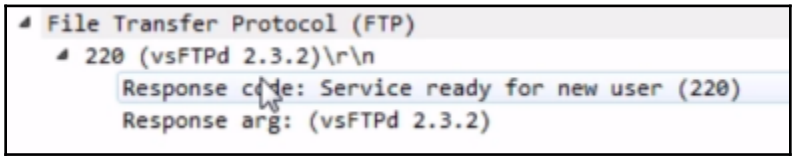

Wireshark · Expert Information · rsasnakeoil2.cap
Severity Summary Group Protocol Count
Error Bad checksum [should be 0xad00] Checksum TCP 33
4 Client Hello Checksum TCP
6 Server Hello, Certificate, Server Hello Done Checksum TCP
8 Client Key Exchange, Change Cipher Spec, Finished Checksum TCP
9 Change Cipher Spec, Finished Checksum TCP
11 GET / HTTP/1.1 Checksum TCP
13 Hello Request Checksum TCP
14 Client Hello Checksum TCP
16 Server Hello, Certificate, Server Hello Done Checksum TCP
17 Client Key Exchange, Change Cipher Spec, Finished Checksum TCP
18 Change Cipher Spec, Finished Checksum TCP
19 HTTP/1.1 200 OK (text/html) Checksum TCP
21 GET /icons/jhe061.png HTTP/1.1 Checksum TCP
25 Client Hello Checksum TCP
27 Server Hello, Change Cipher Spec, Finished Checksum TCP
29 GET /icons/debian/openlogo-25.jpg HTTP/1.1 Checksum TCP
30 HTTP/1.1 404 Not Found (text/html) Checksum TCP
31 GET /icons/apache_pb.png HTTP/1.1 Checksum TCP
Display filter: "http"
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

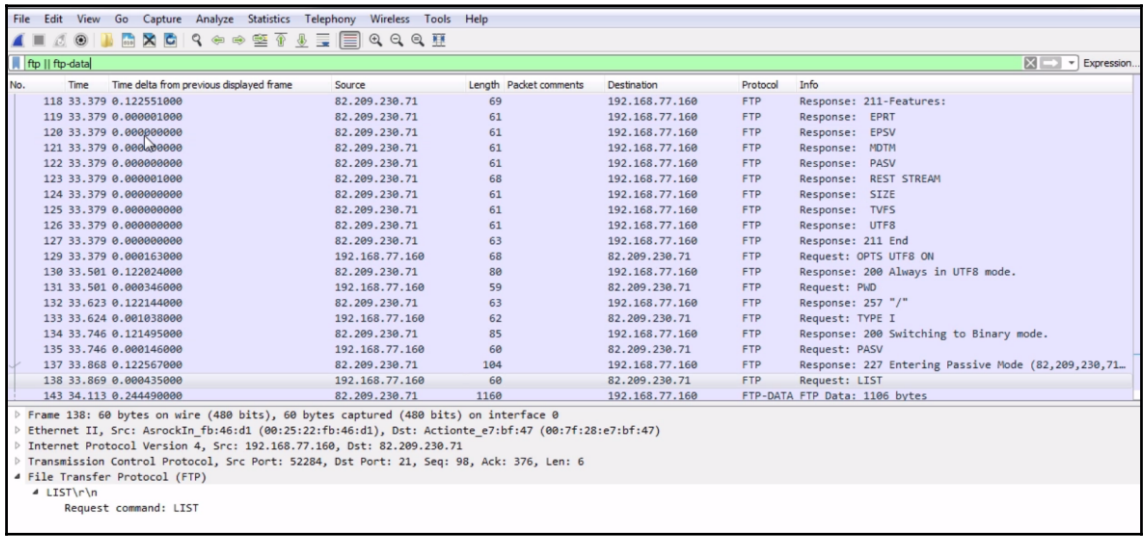

FileZilla
File Edit View Transfer Server Bookmarks Help New version available!
Host: ftp.mgts.by Username: anonymos Password: •••••••• Port: 21 Quickconnect
Local site: C:\Users\sayalit\
Administrator
All Users
Default
Default User
Public
sayalit
user
yogeshp
Windows
D:
E:
Remote site:
Filename Filesize Filetype Last modified
.. File folder
.anaconda File folder 9/6/2017 1:05:57 PM
.conda File folder 9/11/2017 12:56:08...
.condamanager File folder 9/6/2017 1:06:00 PM
.config File folder 2/7/2018 5:31:38 PM
.FBReader File folder 1/18/2018 4:37:56 ...
.idlerc File folder 9/6/2017 2:24:54 PM
.ipython File folder 9/7/2017 5:28:42 PM
.jupyter File folder 9/8/2017 4:02:39 PM
.matplotlib File folder 10/4/2017 4:24:09 ...
.plotly File folder 9/8/2017 2:34:57 PM
.ssh File folder 3/20/2017 6:48:53 ...
.VirtualBox File folder 4/2/2018 6:53:42 PM
AppData File folder 1/16/2018 4:32:53 ...
Application Data File folder
15 files and 39 directories. Total size: 14,809,993 bytes
Filename Filesize Filetype Last modified Permissions Owner/Gro...
Not connected to any server
Not connected.
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers
Queue: empty


Host: ftp.mgts.by Username: anonymous Password: •••••••••• Port: Quickconnect
Status: Connecting to 82.209.230.71:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful



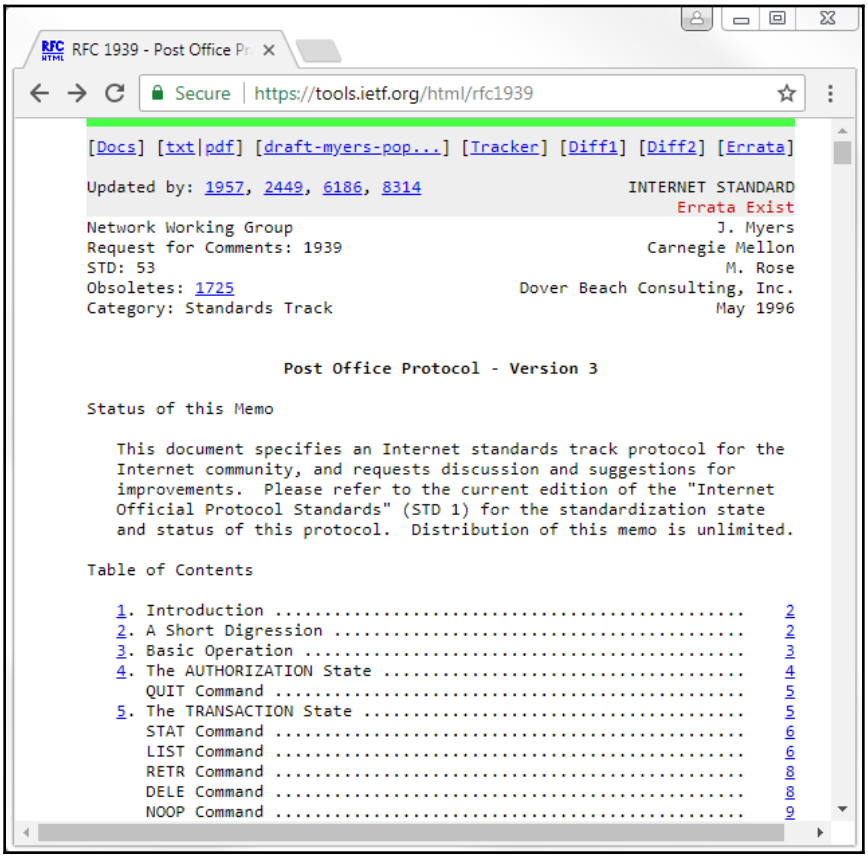
No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
121	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: MDTM
122	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: PASV
123	33.379	0.000001000	82.209.230.71	68		192.168.77.160	FTP	Response: REST STREAM
124	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: SIZE
125	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: TVFS
126	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: UTF8
127	33.379	0.000000000	82.209.230.71	63		192.168.77.160	FTP	Response: 211 End
129	33.379	0.000163000	192.168.77.160	68		82.209.230.71	FTP	Request: OPTS UTF8 ON
130	33.501	0.122024000	82.209.230.71	80		192.168.77.160	FTP	Response: 200 Always in UTF8 mode.
131	33.501	0.000346000	192.168.77.160	59		82.209.230.71	FTP	Request: PWD
132	33.623	0.122144000	82.209.230.71	63		192.168.77.160	FTP	Response: 257 "/"
133	33.624	0.001038000	192.168.77.160	62		82.209.230.71	FTP	Request: TYPE I
134	33.746	0.121495000	82.209.230.71	85		192.168.77.160	FTP	Response: 200 Switching to Binary mode.
135	33.746	0.000146000	192.168.77.160	60		82.209.230.71	FTP	Request: PASV
137	33.868	0.122567000	82.209.230.71	104		192.168.77.160	FTP	Response: 227 Entering Passive Mode (82,209,230,71…
138	33.869	0.000435000	192.168.77.160	60		82.209.230.71	FTP	Request: LIST
147	34.116	0.246938000	82.209.230.71	93		192.168.77.160	FTP	Response: 150 Here comes the directory listing.
149	34.238	0.122524000	82.209.230.71	78		192.168.77.160	FTP	Response: 226 Directory send OK.
185	47.398	13.159422000	192.168.77.160	63		82.209.230.71	FTP	Request: CWD pub

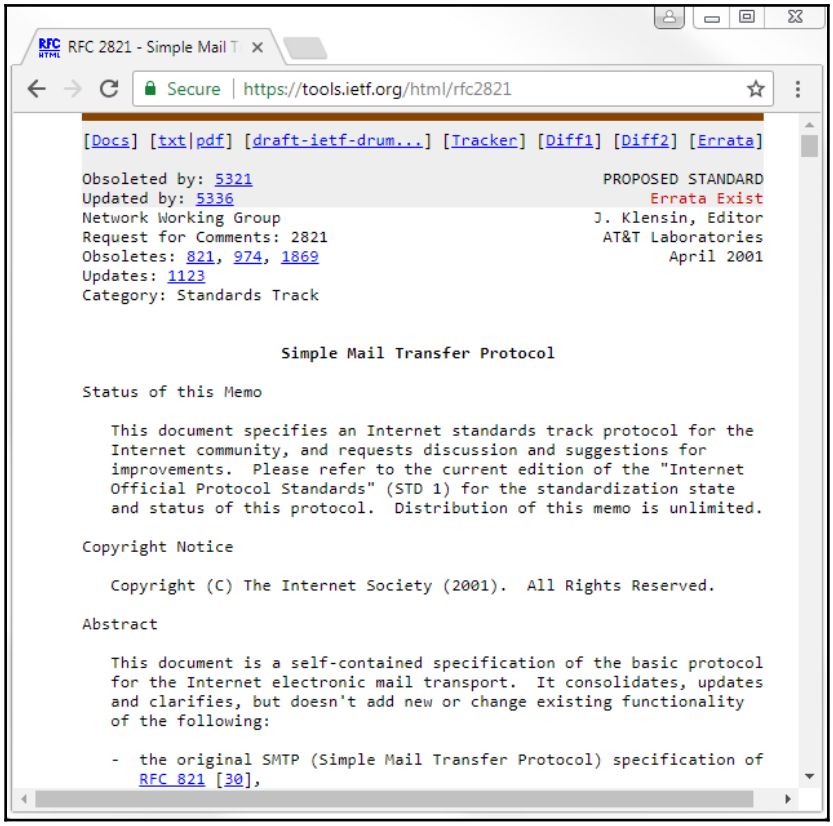


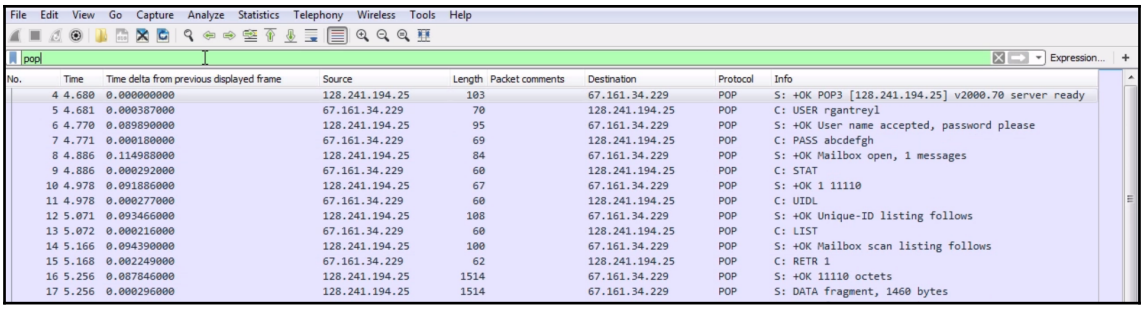


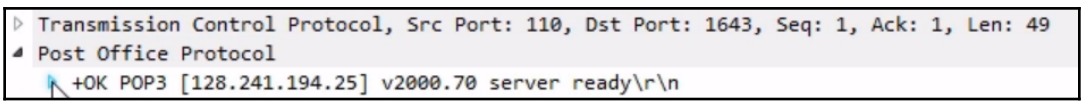
No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
118	33.379	0.122551000	82.209.230.71	69		192.168.77.160	FTP	Response: 211-Features:
119	33.379	0.000001000	82.209.230.71	61		192.168.77.160	FTP	Response: EPRT
120	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: EPSV
121	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: MDTM
122	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: PASV
123	33.379	0.000001000	82.209.230.71	68		192.168.77.160	FTP	Response: REST STREAM
124	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: SIZE
125	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: TVFS
126	33.379	0.000000000	82.209.230.71	61		192.168.77.160	FTP	Response: UTF8
127	33.379	0.000000000	82.209.230.71	63		192.168.77.160	FTP	Response: 211 End
129	33.379	0.000163000	192.168.77.160	68		82.209.230.71	FTP	Request: OPTS UTF8 ON
130	33.501	0.122024000	82.209.230.71	80		192.168.77.160	FTP	Response: 200 Always in UTF8 mode.
131	33.501	0.000346000	192.168.77.160	59		82.209.230.71	FTP	Request: PWD
132	33.623	0.122144000	82.209.230.71	63		192.168.77.160	FTP	Response: 257 "/"
133	33.624	0.001038000	192.168.77.160	62		82.209.230.71	FTP	Request: TYPE I
134	33.746	0.121495000	82.209.230.71	85		192.168.77.160	FTP	Response: 200 Switching to Binary mode.
135	33.746	0.000146000	192.168.77.160	60		82.209.230.71	FTP	Request: PASV
137	33.868	0.122567000	82.209.230.71	104		192.168.77.160	FTP	Response: 227 Entering Passive Mode (82,209,230,71…
138	33.869	0.000435000	192.168.77.160	60		82.209.230.71	FTP	Request: LIST
143	34.113	0.244490000	82.209.230.71	1160		192.168.77.160	FTP-DATA	FTP Data: 1106 bytes

Chapter 09: Application Protocol Analysis II




RFC 2821 - Simple Mail T
Secure | https://tools.ietf.org/html/rfc2821
[Docs] [txt|pdf] [draft-ietf-drum...] [Tracker] [Diff1] [Diff2] [Errata]
Obsoleted by: 5321
Updated by: 5336
Network Working Group
Request for Comments: 2821
Obsoletes: 821, 974, 1869
Updates: 1123
Category: Standards Track
PROPOSED STANDARD
Errata Exist
J. Klensin, Editor
AT&T Laboratories
April 2001
Simple Mail Transfer Protocol
Status of this Memo
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.
Copyright Notice
Copyright (C) The Internet Society (2001). All Rights Reserved.
Abstract
This document is a self-contained specification of the basic protocol for the Internet electronic mail transport. It consolidates, updates and clarifies, but doesn't add new or change existing functionality of the following:
- the original SMTP (Simple Mail Transfer Protocol) specification of RFC 821 [30],


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
pop
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
4 4.680 0.000000000 128.241.194.25 103 67.161.34.229 POP S: +OK POP3 [128.241.194.25] v2000.70 server ready
5 4.681 0.000387000 67.161.34.229 70 128.241.194.25 POP C: USER rgantreyl
6 4.770 0.089890000 128.241.194.25 95 67.161.34.229 POP S: +OK User name accepted, password please
7 4.771 0.000180000 67.161.34.229 69 128.241.194.25 POP C: PASS abcdefgh
8 4.886 0.114988000 128.241.194.25 84 67.161.34.229 POP S: +OK Mailbox open, 1 messages
9 4.886 0.000292000 67.161.34.229 60 128.241.194.25 POP C: STAT
10 4.978 0.091886000 128.241.194.25 67 67.161.34.229 POP S: +OK 1 11110
11 4.978 0.000277000 67.161.34.229 60 128.241.194.25 POP C: UIDL
12 5.071 0.093466000 128.241.194.25 108 67.161.34.229 POP S: +OK Unique-ID listing follows
13 5.072 0.000216000 67.161.34.229 60 128.241.194.25 POP C: LIST
14 5.166 0.094390000 128.241.194.25 100 67.161.34.229 POP S: +OK Mailbox scan listing follows
15 5.168 0.002249000 67.161.34.229 62 128.241.194.25 POP C: RETR 1
16 5.256 0.087846000 128.241.194.25 1514 67.161.34.229 POP S: +OK 11110 octets
17 5.256 0.000296000 128.241.194.25 1514 67.161.34.229 POP S: DATA fragment, 1460 bytes


Transmission Control Protocol, Src Port: 110, Dst Port: 1643, Seq: 1, Ack: 1, Len: 49
Post Office Protocol
+OK POP3 [128.241.194.25] v2000.70 server ready\r\n

4	4.680	4.593677000	128.241.194.25	103	67.161.34.229	POP	S: +OK POP3 [128.241.194.25] v2000.70 server ready
5	4.681	0.000387000	67.161.34.229	70	128.241.194.25	POP	C: USER rgantreyl
6	4.770	0.089890000	128.241.194.25	95	67.161.34.229	POP	S: +OK User name accepted, password please
7	4.771	0.000180000	67.161.34.229	69	128.241.194.25	POP	C: PASS abcdefgh
8	4.886	0.114988000	128.241.194.25	84	67.161.34.229	POP	S: +OK Mailbox open, 1 messages
9	4.886	0.000292000	67.161.34.229	60	128.241.194.25	POP	C: STAT
10	4.978	0.091886000	128.241.194.25	67	67.161.34.229	POP	S: +OK 1 11110
11	4.978	0.000277000	67.161.34.229	60	128.241.194.25	POP	C: UIDL
12	5.071	0.093466000	128.241.194.25	108	67.161.34.229	POP	S: +OK Unique-ID listing follows
13	5.072	0.000216000	67.161.34.229	60	128.241.194.25	POP	C: LIST
14	5.166	0.094390000	128.241.194.25	100	67.161.34.229	POP	S: +OK Mailbox scan listing follows
15	5.168	0.002249000	67.161.34.229	62	128.241.194.25	POP	C: RETR 1
16	5.256	0.087846000	128.241.194.25	1514	67.161.34.229	POP	S: +OK 11110 octets

```
Post Office Protocol
▲ +OK 11110 octets\r\n
    Response indicator: +OK
    Response description: 11110 octets
  Return-Path: bbelch@packet-level.com\r\n
  Received: from mx20.stngva01.us.mxservers.net (204.202.242.7)\r\n
  \tby mail11d.verio-web.com (RS ver 1.0.95vs) with SMTP id 3-0575327743\r\n
  \tfor <rgantreyl@packet-level.com>; Mon, 15 Jan 2007 16:49:06 -0500 (EST)\r\n
  Received: from mxw1100.verio-web.com [161.88.148.09] (EHLO GIGA)\r\n
  \tby mx20.stngva01.us.mxservers.net (mxl_mta-1.3.8-10p4) with ESMTP id d05fba54.2509.132.mx20.stngva01.us.mxservers.net;\r\n
```

16	5.256	0.087846000	128.241.194.25	1514	67.161.34.229	POP	S: +OK 11110 octets
17	5.256	0.000296000	128.241.194.25	1514	67.161.34.229	POP	S: DATA fragment, 1460 bytes
18	5.257	0.000025000	67.161.34.229	54	128.241.194.25	TCP	1643→110 [ACK] Seq=58 Ack=3154 Win=256960 Len=0
19	5.257	0.000240000	128.241.194.25	1230	67.161.34.229	POP	S: DATA fragment, 1176 bytes
20	5.258	0.001077000	128.241.194.25	1514	67.161.34.229	POP	S: DATA fragment, 1460 bytes
21	5.258	0.000017000	67.161.34.229	54	128.241.194.25	TCP	1643→110 [ACK] Seq=58 Ack=5790 Win=256960 Len=0
22	5.258	0.000302000	128.241.194.25	1514	67.161.34.229	POP	S: DATA fragment, 1460 bytes
23	5.259	0.000931000	128.241.194.25	1514	67.161.34.229	POP	S: DATA fragment, 1460 bytes
24	5.259	0.000023000	67.161.34.229	54	128.241.194.25	TCP	1643→110 [ACK] Seq=58 Ack=8710 Win=256960 Len=0
25	5.343	0.083831000	128.241.194.25	338	67.161.34.229	POP	S: DATA fragment, 284 bytes
26	5.351	0.007775000	128.241.194.25	1514	67.161.34.229	POP	S: DATA fragment, 1460 bytes
27	5.351	0.000039000	67.161.34.229	54	128.241.194.25	TCP	1643→110 [ACK] Seq=58 Ack=10454 Win=256960 Len=0
28	5.437	0.086159000	128.241.194.25	966	67.161.34.229	POP	S: DATA fragment, 912 bytes
29	5.562	0.125231000	67.161.34.229	54	128.241.194.25	TCP	1643→110 [ACK] Seq=58 Ack=11366 Win=256048 Len=0
30	8.371	2.809058000	67.161.34.229	62	128.241.194.25	POP	C: DELE 1
31	8.460	0.088840000	128.241.194.25	75	67.161.34.229	POP	S: +OK Message deleted

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression

No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
1	0.000	0.000000000	67.161.34.229	66		128.241.194.25	TCP	1650→25 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=4 …
2	0.088	0.088301000	128.241.194.25	66		67.161.34.229	TCP	25→1650 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS…
3	0.088	0.000055000	67.161.34.229	54		128.241.194.25	TCP	1650→25 [ACK] Seq=1 Ack=1 Win=256960 Len=0
4	4.683	4.594681000	128.241.194.25	163		67.161.34.229	SMTP	S: 220 mx100.stngva01.us.mxservers.net ESMTP mxl_m…
5	4.683	0.000270000	67.161.34.229	65		128.241.194.25	SMTP	C: EHLO Vaio
6	4.782	0.098716000	128.241.194.25	91		67.161.34.229	SMTP	S: 250 mx100.stngva01.us.mxservers.net
7	4.906	0.124529000	67.161.34.229	54		128.241.194.25	TCP	1650→25 [ACK] Seq=12 Ack=147 Win=256812 Len=0
8	4.995	0.088823000	128.241.194.25	82		67.161.34.229	SMTP	S: 250 SIZE 0 | 250 PIPELINING
9	4.995	0.000142000	67.161.34.229	95		128.241.194.25	SMTP	C: MAIL FROM: <breaddy16@packet-level.com>
10	5.096	0.100986000	128.241.194.25	69		67.161.34.229	SMTP	S: 250 Sender Ok
11	5.096	0.000363000	67.161.34.229	90		128.241.194.25	SMTP	C: RCPT TO: <bbelch@packet-level.com>
12	5.298	0.201889000	128.241.194.25	95		67.161.34.229	SMTP	S: 250 bbelch@packet-level.com ok (normal)
13	5.298	0.000243000	67.161.34.229	60		128.241.194.25	SMTP	C: DATA

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp Expression... +

No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
4	4.683	0.000000000	128.241.194.25	163		67.161.34.229	SMTP	S: 220 mx100.stngva01.us.mxservers.net ESMTP mxl_mta-1.3.…
5	4.683	0.000270000	67.161.34.229	65		128.241.194.25	SMTP	C: EHLO Vaio
6	4.782	0.098716000	128.241.194.25	91		67.161.34.229	SMTP	S: 250 mx100.stngva01.us.mxservers.net
8	4.995	0.213352000	128.241.194.25	82		67.161.34.229	SMTP	S: 250 SIZE 0 | 250 PIPELINING
9	4.995	0.000142000	67.161.34.229	95		128.241.194.25	SMTP	C: MAIL FROM: <breaddy16@packet-level.com>
10	5.096	0.100986000	128.241.194.25	69		67.161.34.229	SMTP	S: 250 Sender Ok

```
Simple Mail Transfer Protocol
  Response: 220 mx100.stngva01.us.mxservers.net ESMTP mxl_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:49:50 -0500 (EST); NO UCE\r\n
    Response code: <domain> Service ready (220)
    Response parameter: mx100.stngva01.us.mxservers.net ESMTP mxl_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:49:50 -0500 (EST); NO UCE
```

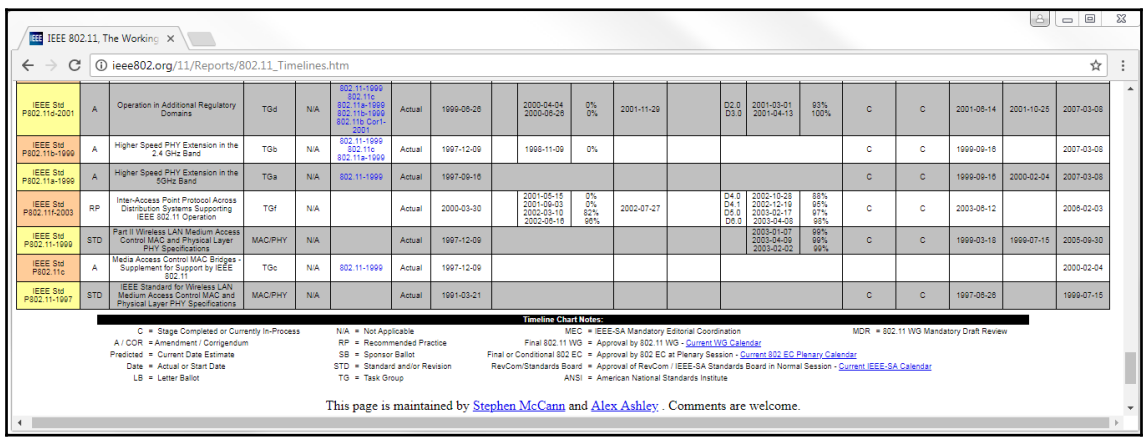
4	4.683	4.594681000	128.241.194.25	163	67.161.34.229	SMTP	S: 220 mx100.stngva01.us.mxservers.net ESMTP mxl_m…
5	4.683	0.000270000	67.161.34.229	65	128.241.194.25	SMTP	C: EHLO Vaio
6	4.782	0.098716000	128.241.194.25	91	67.161.34.229	SMTP	S: 25 mx100.stngva01.us.mxservers.net
7	4.906	0.124529000	67.161.34.229	54	128.241.194.25	TCP	1650→25 [ACK] Seq=12 Ack=147 Win=256812 Len=0
8	4.995	0.088823000	128.241.194.25	82	67.161.34.229	SMTP	S: 250 SIZE 0 | 250 PIPELINING

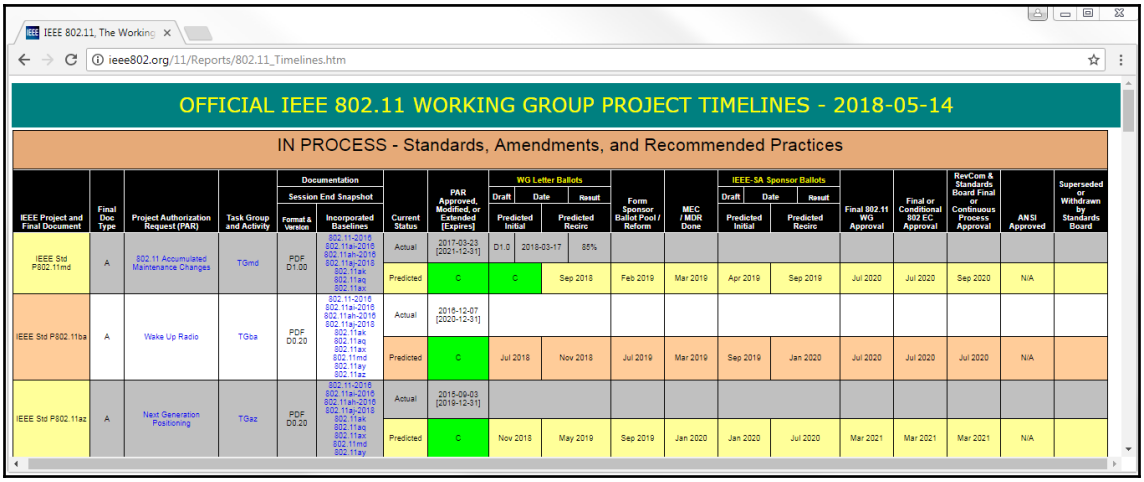
```
Simple Mail Transfer Protocol
  Response: 250-SIZE 0\r\n
    Response code: Requested mail action okay, completed (250)
    Response parameter: SIZE 0
  Response: 250 PIPELINING\r\n
    Response code: Requested mail action okay, completed (250)
    Response parameter: PIPELINING
```

9	4.995	0.000142000	67.161.34.229	95	128.241.194.25	SMTP	C: MAIL FROM: <breaddy16@packet-level.com>
10	5.096	0.100986000	128.241.194.25	69	67.161.34.229	SMTP	S: 250 Sender Ok
11	5.096	0.000363000	67.161.34.229	90	128.241.194.25	SMTP	C: RCPT TO: <bbelch@packet-level.com>
12	5.298	0.201889000	128.241.194.25	95	67.161.34.229	SMTP	S: 250 bbelch@packet-level.com ok (normal)

13	5.298	0.000243000	67.161.34.229	60	128.241.194.25	SMTP	C: DATA
14	5.385	0.086553000	128.241.194.25	100	67.161.34.229	SMTP	S: 354 Start mail input; end with <CRLF>.<CRLF>
15	5.396	0.011263000	67.161.34.229	1514	128.241.194.25	SMTP	C: DATA fragment, 1460 bytes
16	5.396	0.000025000	67.161.34.229	1514	128.241.194.25	SMTP	C: DATA fragment, 1460 bytes
17	5.396	0.000013000	67.161.34.229	1476	128.241.194.25	SMTP	C: DATA fragment, 1422 bytes
18	5.496	0.099800000	128.241.194.25	60	67.161.34.229	TCP	25→1650 [ACK] Seq=277 Ack=3015 Win=65535 Len=0
19	5.496	0.000022000	67.161.34.229	59	128.241.194.25	IMF	from: "Brian Readdy16" <breaddy16@packet-level.com…
20	5.500	0.004146000	128.241.194.25	60	67.161.34.229	TCP	25→1650 [ACK] Seq=277 Ack=4437 Win=64113 Len=0
21	5.718	0.217512000	128.241.194.25	60	67.161.34.229	TCP	25→1650 [ACK] Seq=277 Ack=4442 Win=64108 Len=0
22	6.360	0.642102000	128.241.194.25	102	67.161.34.229	SMTP	S: 250 0-0484658135 Message accepted for delivery

23	6.511	0.151263000	67.161.34.229	54	128.241.194.25	TCP	1650→25 [ACK] Seq=4442 Ack=325 Win=256636 Len=0
24	8.870	2.358602000	67.161.34.229	60	128.241.194.25	SMTP	C: QUIT
25	8.870	0.000120000	67.161.34.229	54	128.241.194.25	TCP	1650→25 [FIN, ACK] Seq=4448 Ack=325 Win=256636 Len…
26	8.958	0.087663000	128.241.194.25	128	67.161.34.229	SMTP	S: 221 mx100.stngva01.us.mxservers.net Service clo…
27	8.958	0.000044000	67.161.34.229	54	128.241.194.25	TCP	1650→25 [RST, ACK] Seq=4449 Ack=399 Win=0 Len=0
28	8.959	0.000951000	128.241.194.25	60	67.161.34.229	TCP	25→1650 [FIN, ACK] Seq=399 Ack=4448 Win=64102 Len=0





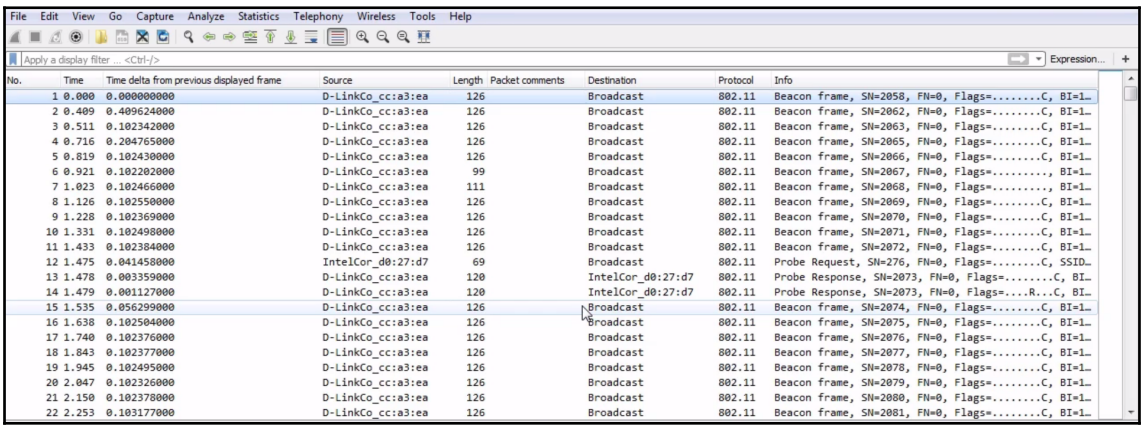
IEEE 802.11, The Working

ieee802.org/11/Reports/802.11_Timelines.htm

OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES - 2018-05-14

IN PROCESS - Standards, Amendments, and Recommended Practices

IEEE Project and Final Document	Final Doc Type	Project Authorization Request (PAR)	Task Group and Activity	Documentation: Session End Snapshot: Format & Version	Documentation: Session End Snapshot: Incorporated Baselines	Current Status	PAR Approved, Modified, or Extended [Expires]	WG Letter Ballots: Draft: Predicted Initial	WG Letter Ballots: Date: Predicted Recirc	WG Letter Ballots: Result: Predicted Recirc	Form Sponsor Ballot Pool / Reform	MEC / MDR Done	IEEE-SA Sponsor Ballots: Draft: Predicted Initial	IEEE-SA Sponsor Ballots: Date: Predicted Recirc	Final 802.11 WG Approval	Final or Conditional 802 EC Approval	RevCom & Standards Board Final or Continuous Process Approval	ANSI Approved	Superseded or Withdrawn by Standards Board
IEEE Std P802.11md	A	802.11 Accumulated Maintenance Changes	TGmd	PDF D1.00	802.11-2016 802.11ai-2016 802.11ah-2016 802.11aj-2018 802.11ax 802.11aq 802.11az	Actual	2017-03-23 [2021-12-31]	D1.0	2018-03-17	85%									
						Predicted	C	C		Sep 2018	Feb 2019	Mar 2019	Apr 2019	Sep 2019	Jul 2020	Jul 2020	Sep 2020	N/A	
IEEE Std P802.11ba	A	Wake Up Radio	TGba	PDF D0.20	802.11-2016 802.11ai-2016 802.11ah-2016 802.11aj-2018 802.11ax 802.11aq 802.11ax 802.11md 802.11ay 802.11az	Actual	2016-12-07 [2020-12-31]												
						Predicted	C	Jul 2018	Nov 2018		Jul 2019	Mar 2019	Sep 2019	Jan 2020	Jul 2020	Jul 2020	Jul 2020	N/A	
IEEE Std P802.11az	A	Next Generation Positioning	TGaz	PDF D0.20	802.11-2016 802.11ai-2016 802.11ah-2016 802.11aj-2018 802.11ak 802.11aq 802.11ax 802.11md 802.11ay	Actual	2015-09-03 [2019-12-31]												
						Predicted	C	Nov 2018	May 2019		Sep 2019	Jan 2020	Jan 2020	Jul 2020	Mar 2021	Mar 2021	Mar 2021	N/A	

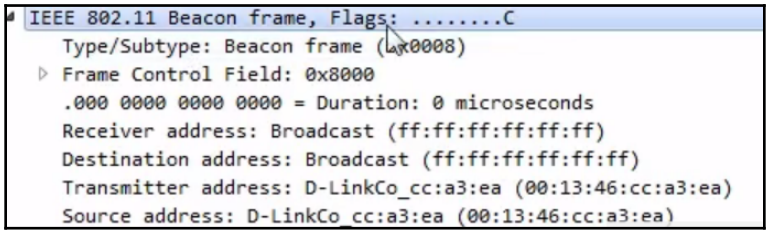


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

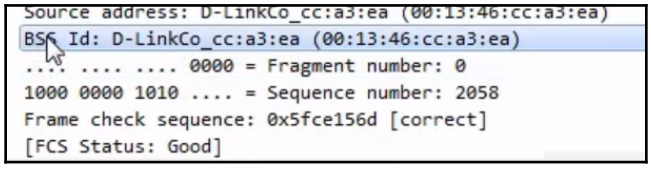
Apply a display filter ... <Ctrl-/>

Expression...

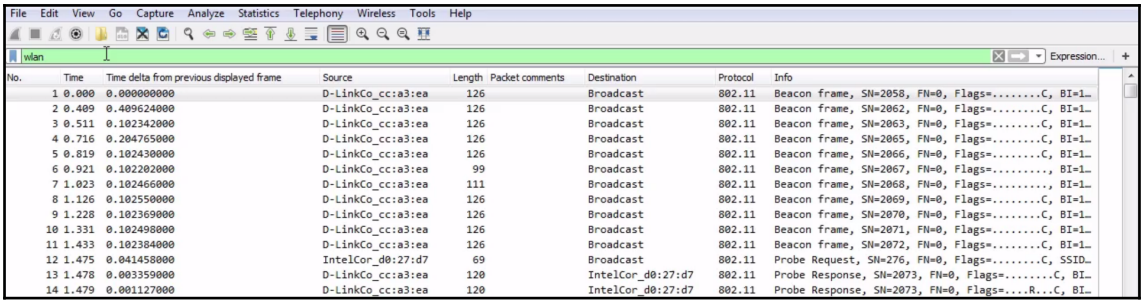
No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
1	0.000	0.000000000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2058, FN=0, Flags=.....C, BI=1…
2	0.409	0.409624000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2062, FN=0, Flags=.....C, BI=1…
3	0.511	0.102342000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2063, FN=0, Flags=.....C, BI=1…
4	0.716	0.204765000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2065, FN=0, Flags=.....C, BI=1…
5	0.819	0.102430000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2066, FN=0, Flags=.....C, BI=1…
6	0.921	0.102202000	D-LinkCo_cc:a3:ea	99		Broadcast	802.11	Beacon frame, SN=2067, FN=0, Flags=....., BI=1…
7	1.023	0.102466000	D-LinkCo_cc:a3:ea	111		Broadcast	802.11	Beacon frame, SN=2068, FN=0, Flags=....., BI=1…
8	1.126	0.102550000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2069, FN=0, Flags=.....C, BI=1…
9	1.228	0.102369000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2070, FN=0, Flags=.....C, BI=1…
10	1.331	0.102498000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2071, FN=0, Flags=.....C, BI=1…
11	1.433	0.102384000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2072, FN=0, Flags=.....C, BI=1…
12	1.475	0.041458000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=276, FN=0, Flags=.....C, SSID…
13	1.478	0.003359000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2073, FN=0, Flags=.....C, BI…
14	1.479	0.001127000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2073, FN=0, Flags=....R...C, BI…
15	1.535	0.056299000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2074, FN=0, Flags=.....C, BI=1…
16	1.638	0.102504000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2075, FN=0, Flags=.....C, BI=1…
17	1.740	0.102376000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2076, FN=0, Flags=.....C, BI=1…
18	1.843	0.102377000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2077, FN=0, Flags=.....C, BI=1…
19	1.945	0.102495000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2078, FN=0, Flags=.....C, BI=1…
20	2.047	0.102326000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2079, FN=0, Flags=.....C, BI=1…
21	2.150	0.102378000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2080, FN=0, Flags=.....C, BI=1…
22	2.253	0.103177000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=2081, FN=0, Flags=.....C, BI=1…

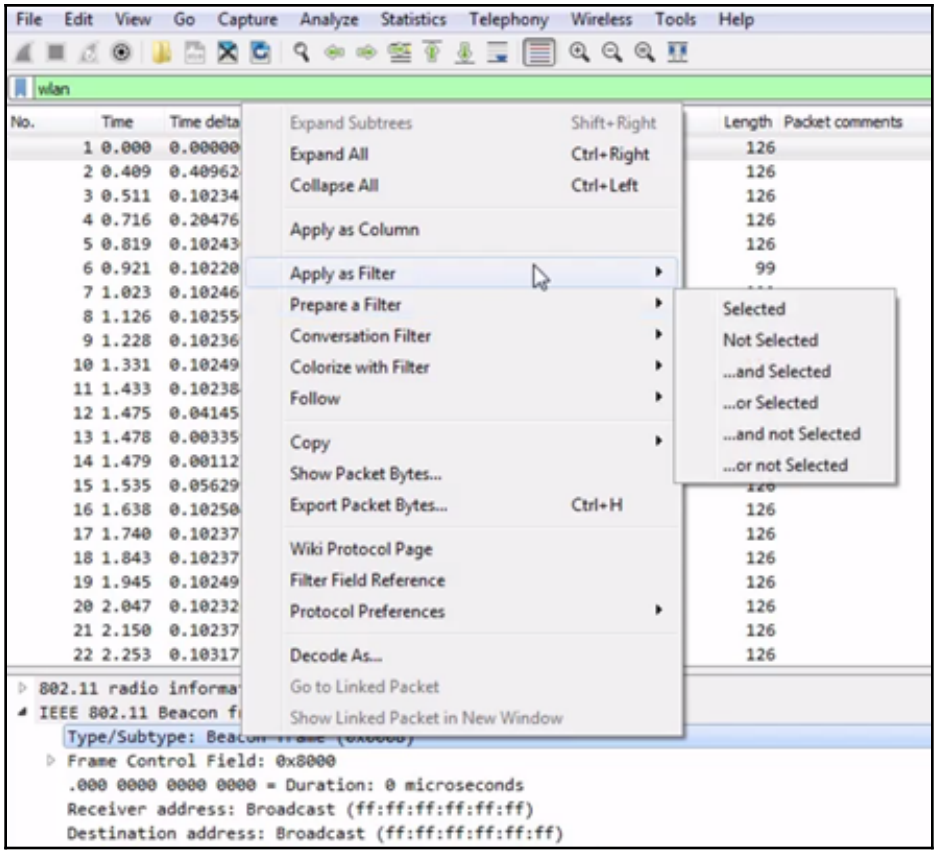


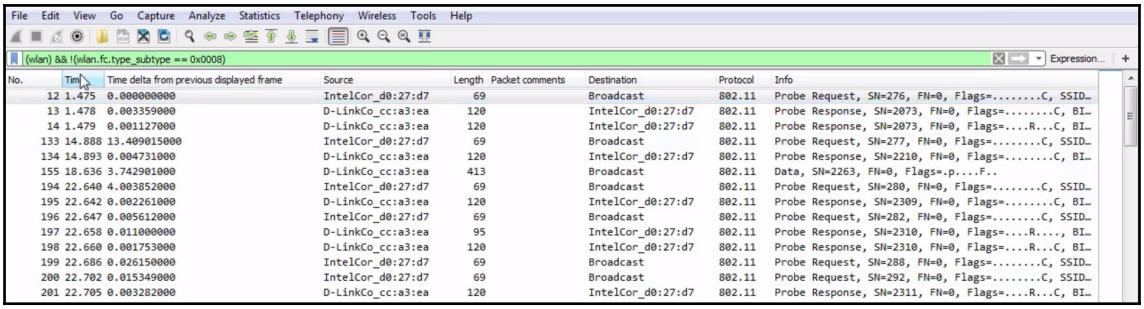
```
IEEE 802.11 Beacon frame, Flags: .....C
    Type/Subtype: Beacon frame (0x0008)
  ▷ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: D-LinkCo_cc:a3:ea (00:13:46:cc:a3:ea)
    Source address: D-LinkCo_cc:a3:ea (00:13:46:cc:a3:ea)
```



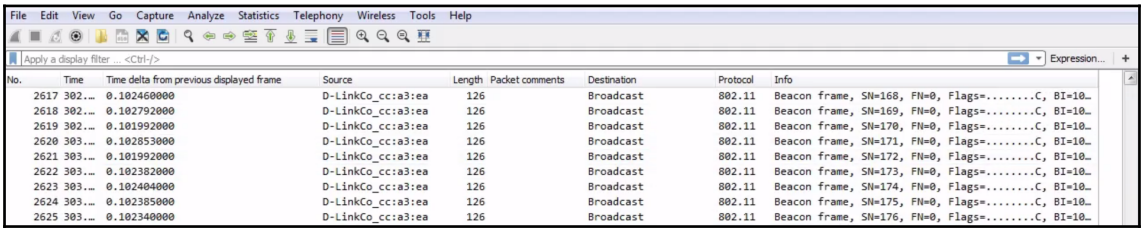
```
Source address: D-LinkCo_cc:a3:ea (00:13:46:cc:a3:ea)
BSS Id: D-LinkCo_cc:a3:ea (00:13:46:cc:a3:ea)
.... .... .... 0000 = Fragment number: 0
1000 0000 1010 .... = Sequence number: 2058
Frame check sequence: 0x5fce156d [correct]
[FCS Status: Good]
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
1 0.000 0.000000000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2058, FN=0, Flags=.....C, BI=1…
2 0.409 0.409624000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2062, FN=0, Flags=.....C, BI=1…
3 0.511 0.102342000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2063, FN=0, Flags=.....C, BI=1…
4 0.716 0.204765000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2065, FN=0, Flags=.....C, BI=1…
5 0.819 0.102430000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2066, FN=0, Flags=.....C, BI=1…
6 0.921 0.102202000 D-LinkCo_cc:a3:ea 99 Broadcast 802.11 Beacon frame, SN=2067, FN=0, Flags=....., BI=1…
7 1.023 0.102466000 D-LinkCo_cc:a3:ea 111 Broadcast 802.11 Beacon frame, SN=2068, FN=0, Flags=....., BI=1…
8 1.126 0.102550000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2069, FN=0, Flags=.....C, BI=1…
9 1.228 0.102369000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2070, FN=0, Flags=.....C, BI=1…
10 1.331 0.102498000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2071, FN=0, Flags=.....C, BI=1…
11 1.433 0.102384000 D-LinkCo_cc:a3:ea 126 Broadcast 802.11 Beacon frame, SN=2072, FN=0, Flags=.....C, BI=1…
12 1.475 0.041458000 IntelCor_d0:27:d7 69 Broadcast 802.11 Probe Request, SN=276, FN=0, Flags=.....C, SSID…
13 1.478 0.003359000 D-LinkCo_cc:a3:ea 120 IntelCor_d0:27:d7 802.11 Probe Response, SN=2073, FN=0, Flags=.....C, BI…
14 1.479 0.001127000 D-LinkCo_cc:a3:ea 120 IntelCor_d0:27:d7 802.11 Probe Response, SN=2073, FN=0, Flags=....R...C, BI…

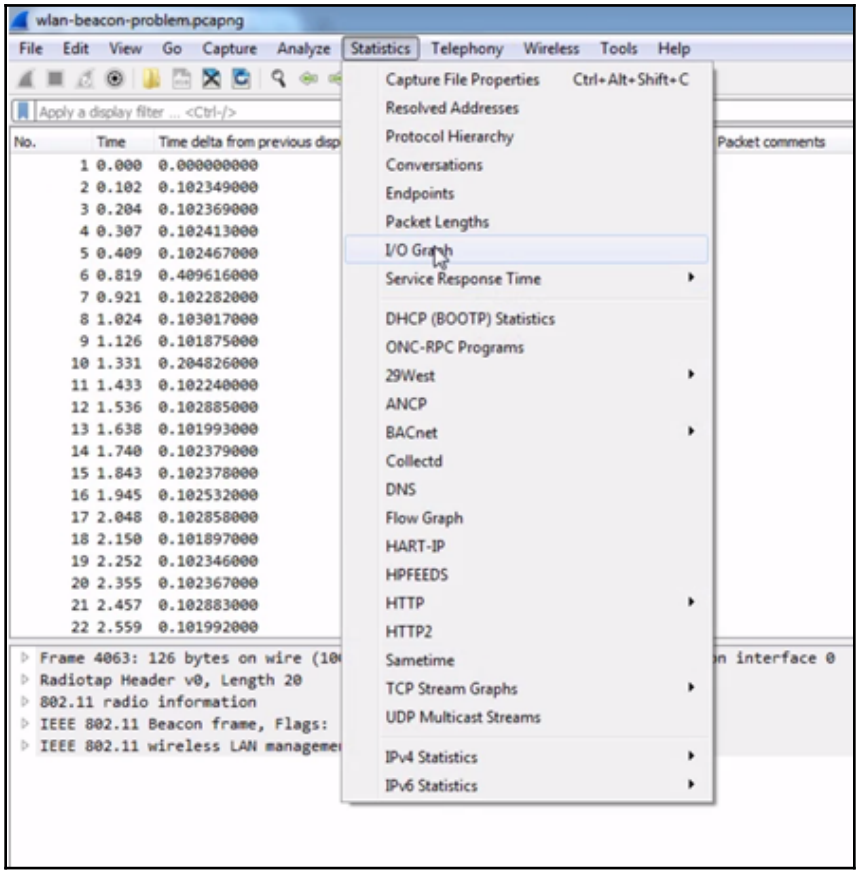

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
wlan
No. Time Time delta
Length Packet comments
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
Show Packet Bytes...
Export Packet Bytes... Ctrl+H
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As...
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
802.11 radio informa
IEEE 802.11 Beacon f
Type/Subtype: Beacon frame
Frame Control Field: 0x8000
.000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)

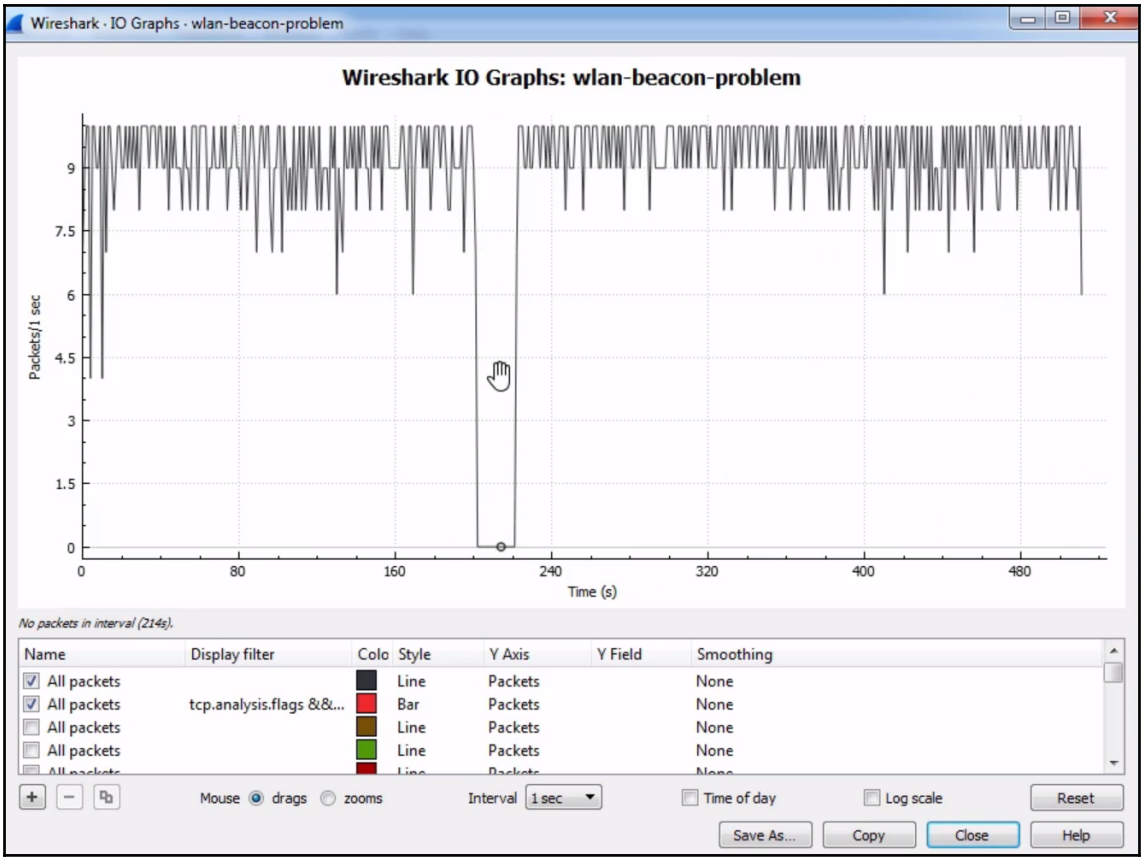


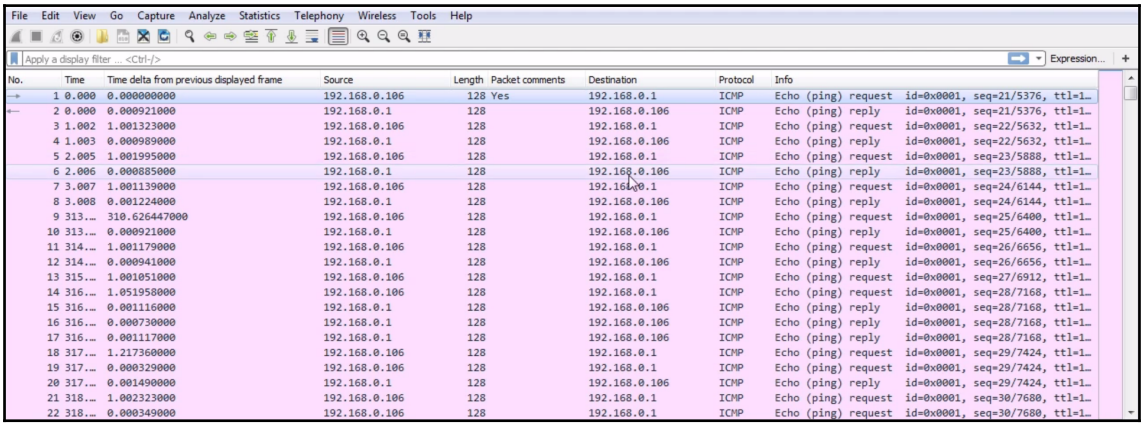
No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
12	1.475	0.000000000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=276, FN=0, Flags=........C, SSID…
13	1.478	0.003359000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2073, FN=0, Flags=........C, BI…
14	1.479	0.001127000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2073, FN=0, Flags=....R...C, BI…
133	14.888	13.409015000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=277, FN=0, Flags=........C, SSID…
134	14.893	0.004731000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2210, FN=0, Flags=........C, BI…
155	18.636	3.742901000	D-LinkCo_cc:a3:ea	413		Broadcast	802.11	Data, SN=2263, FN=0, Flags=.p....F..
194	22.640	4.003852000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=280, FN=0, Flags=........C, SSID…
195	22.642	0.002261000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2309, FN=0, Flags=........C, BI…
196	22.647	0.005612000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=282, FN=0, Flags=........C, SSID…
197	22.658	0.011000000	D-LinkCo_cc:a3:ea	95		IntelCor_d0:27:d7	802.11	Probe Response, SN=2310, FN=0, Flags=....R...., BI…
198	22.660	0.001753000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2310, FN=0, Flags=....R...C, BI…
199	22.686	0.026150000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=288, FN=0, Flags=........C, SSID…
200	22.702	0.015349000	IntelCor_d0:27:d7	69		Broadcast	802.11	Probe Request, SN=292, FN=0, Flags=........C, SSID…
201	22.705	0.003282000	D-LinkCo_cc:a3:ea	120		IntelCor_d0:27:d7	802.11	Probe Response, SN=2311, FN=0, Flags=....R...C, BI…

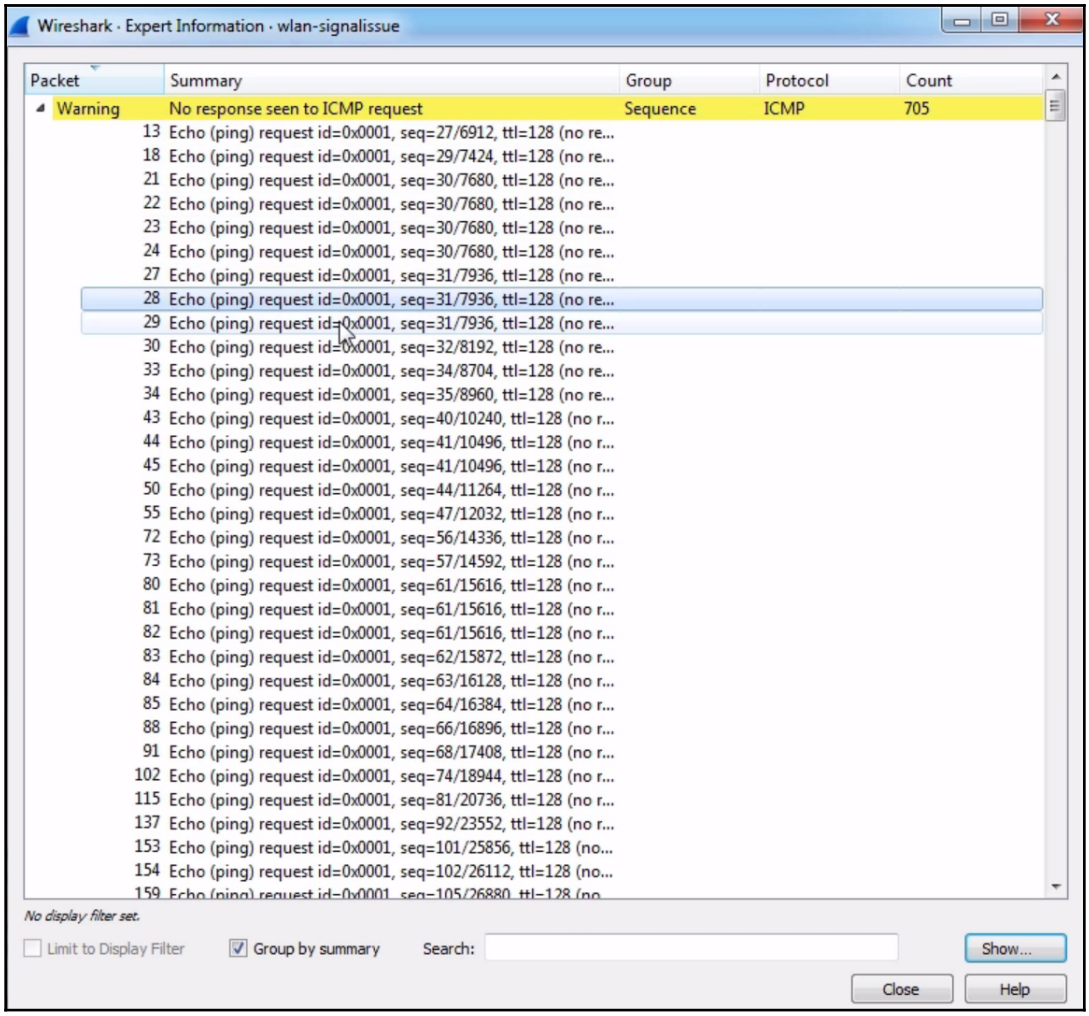


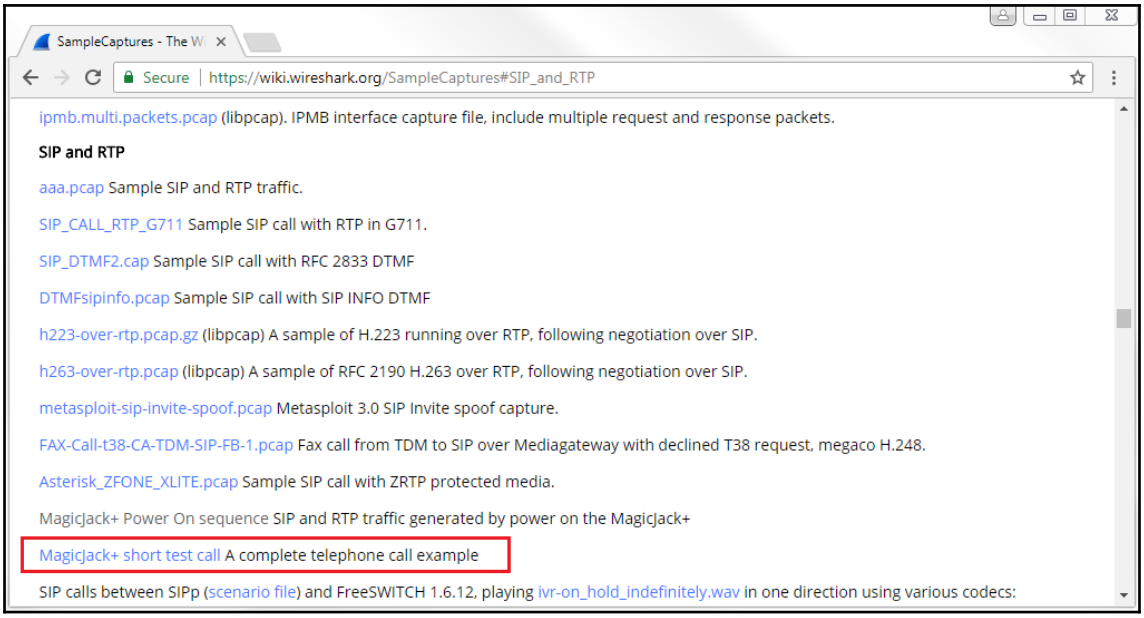
No.	Time	Time delta from previous displayed frame	Source	Length	Packet comments	Destination	Protocol	Info
2617	302.…	0.102460000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=168, FN=0, Flags=........C, BI=10…
2618	302.…	0.102792000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=169, FN=0, Flags=........C, BI=10…
2619	302.…	0.101992000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=170, FN=0, Flags=........C, BI=10…
2620	303.…	0.102853000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=171, FN=0, Flags=........C, BI=10…
2621	303.…	0.101992000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=172, FN=0, Flags=........C, BI=10…
2622	303.…	0.102382000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=173, FN=0, Flags=........C, BI=10…
2623	303.…	0.102404000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=174, FN=0, Flags=........C, BI=10…
2624	303.…	0.102385000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=175, FN=0, Flags=........C, BI=10…
2625	303.…	0.102340000	D-LinkCo_cc:a3:ea	126		Broadcast	802.11	Beacon frame, SN=176, FN=0, Flags=........C, BI=10…

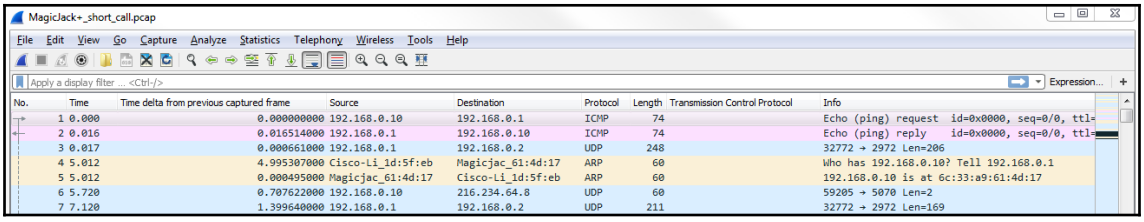

wlan-beacon-problem.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Time delta from previous disp
1 0.000 0.000000000
2 0.102 0.102349000
3 0.204 0.102369000
4 0.307 0.102413000
5 0.409 0.102467000
6 0.819 0.409616000
7 0.921 0.102282000
8 1.024 0.103017000
9 1.126 0.101875000
10 1.331 0.204826000
11 1.433 0.102240000
12 1.536 0.102885000
13 1.638 0.101993000
14 1.740 0.102379000
15 1.843 0.102378000
16 1.945 0.102532000
17 2.048 0.102858000
18 2.150 0.101897000
19 2.252 0.102346000
20 2.355 0.102367000
21 2.457 0.102883000
22 2.559 0.101992000
Packet comments
Frame 4063: 126 bytes on wire (10
Radiotap Header v0, Length 20
802.11 radio information
IEEE 802.11 Beacon frame, Flags:
IEEE 802.11 wireless LAN manageme
n interface 0
Capture File Properties Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
IPv4 Statistics
IPv6 Statistics

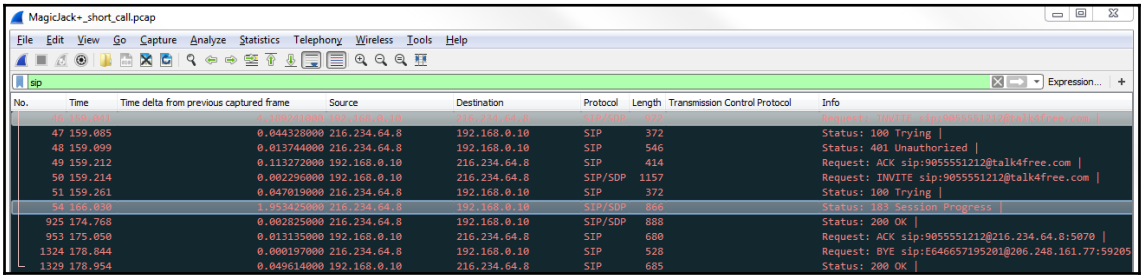

Wireshark · IO Graphs · wlan-beacon-problem
Wireshark IO Graphs: wlan-beacon-problem
Packets/1 sec
Time (s)
No packets in interval (214s).
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
tcp.analysis.flags &&...
Bar
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

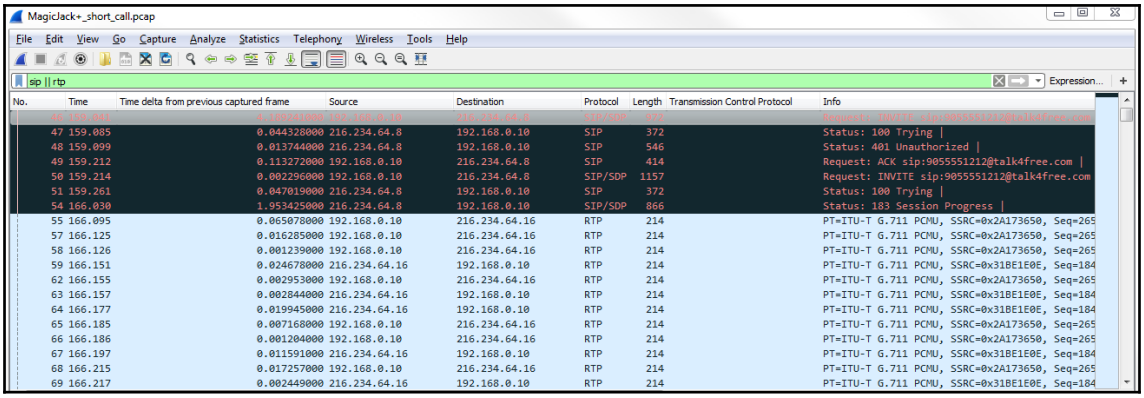

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
1 0.000 0.000000000 192.168.0.106 128 Yes 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=21/5376, ttl=1...
2 0.000 0.000921000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=21/5376, ttl=1...
3 1.002 1.001323000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=22/5632, ttl=1...
4 1.003 0.000989000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=22/5632, ttl=1...
5 2.005 1.001995000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=23/5888, ttl=1...
6 2.006 0.000885000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=23/5888, ttl=1...
7 3.007 1.001139000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=24/6144, ttl=1...
8 3.008 0.001224000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=24/6144, ttl=1...
9 313.... 310.626447000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=25/6400, ttl=1...
10 313.... 0.000921000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=25/6400, ttl=1...
11 314.... 1.001179000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=26/6656, ttl=1...
12 314.... 0.000941000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=26/6656, ttl=1...
13 315.... 1.001051000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=27/6912, ttl=1...
14 316.... 1.051958000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=28/7168, ttl=1...
15 316.... 0.001116000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=28/7168, ttl=1...
16 316.... 0.000730000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=28/7168, ttl=1...
17 316.... 0.001117000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=28/7168, ttl=1...
18 317.... 1.217360000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=29/7424, ttl=1...
19 317.... 0.000329000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=29/7424, ttl=1...
20 317.... 0.001490000 192.168.0.1 128 192.168.0.106 ICMP Echo (ping) reply id=0x0001, seq=29/7424, ttl=1...
21 318.... 1.002323000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=30/7680, ttl=1...
22 318.... 0.000349000 192.168.0.106 128 192.168.0.1 ICMP Echo (ping) request id=0x0001, seq=30/7680, ttl=1...

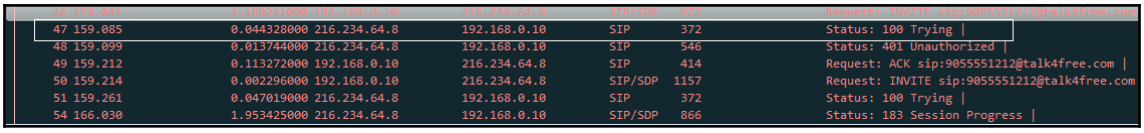

Wireshark · Expert Information · wlan-signalissue
Packet
Summary
Group
Protocol
Count
Warning
No response seen to ICMP request
Sequence
ICMP
705
13 Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (no re...
18 Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (no re...
21 Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no re...
22 Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no re...
23 Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no re...
24 Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (no re...
27 Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (no re...
28 Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (no re...
29 Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (no re...
30 Echo (ping) request id=0x0001, seq=32/8192, ttl=128 (no re...
33 Echo (ping) request id=0x0001, seq=34/8704, ttl=128 (no re...
34 Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (no re...
43 Echo (ping) request id=0x0001, seq=40/10240, ttl=128 (no r...
44 Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (no r...
45 Echo (ping) request id=0x0001, seq=41/10496, ttl=128 (no r...
50 Echo (ping) request id=0x0001, seq=44/11264, ttl=128 (no r...
55 Echo (ping) request id=0x0001, seq=47/12032, ttl=128 (no r...
72 Echo (ping) request id=0x0001, seq=56/14336, ttl=128 (no r...
73 Echo (ping) request id=0x0001, seq=57/14592, ttl=128 (no r...
80 Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (no r...
81 Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (no r...
82 Echo (ping) request id=0x0001, seq=61/15616, ttl=128 (no r...
83 Echo (ping) request id=0x0001, seq=62/15872, ttl=128 (no r...
84 Echo (ping) request id=0x0001, seq=63/16128, ttl=128 (no r...
85 Echo (ping) request id=0x0001, seq=64/16384, ttl=128 (no r...
88 Echo (ping) request id=0x0001, seq=66/16896, ttl=128 (no r...
91 Echo (ping) request id=0x0001, seq=68/17408, ttl=128 (no r...
102 Echo (ping) request id=0x0001, seq=74/18944, ttl=128 (no r...
115 Echo (ping) request id=0x0001, seq=81/20736, ttl=128 (no r...
137 Echo (ping) request id=0x0001, seq=92/23552, ttl=128 (no r...
153 Echo (ping) request id=0x0001, seq=101/25856, ttl=128 (no...
154 Echo (ping) request id=0x0001, seq=102/26112, ttl=128 (no...
159 Echo (ping) request id=0x0001, seq=105/26880, ttl=128 (no
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

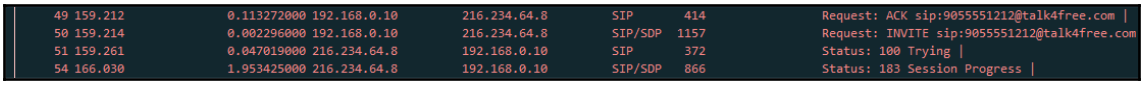

SampleCaptures - The W
Secure
https://wiki.wireshark.org/SampleCaptures#SIP_and_RTP
ipmb.multi.packets.pcap (libpcap). IPMB interface capture file, include multiple request and response packets.
SIP and RTP
aaa.pcap Sample SIP and RTP traffic.
SIP_CALL_RTP_G711 Sample SIP call with RTP in G711.
SIP_DTMF2.cap Sample SIP call with RFC 2833 DTMF
DTMFsipinfo.pcap Sample SIP call with SIP INFO DTMF
h223-over-rtp.pcap.gz (libpcap) A sample of H.223 running over RTP, following negotiation over SIP.
h263-over-rtp.pcap (libpcap) A sample of RFC 2190 H.263 over RTP, following negotiation over SIP.
metasploit-sip-invite-spoof.pcap Metasploit 3.0 SIP Invite spoof capture.
FAX-Call-t38-CA-TDM-SIP-FB-1.pcap Fax call from TDM to SIP over Mediagateway with declined T38 request, megaco H.248.
Asterisk_ZFONE_XLITE.pcap Sample SIP call with ZRTP protected media.
MagicJack+ Power On sequence SIP and RTP traffic generated by power on the MagicJack+
MagicJack+ short test call A complete telephone call example
SIP calls between SIPp (scenario file) and FreeSWITCH 1.6.12, playing ivr-on_hold_indefinitely.wav in one direction using various codecs:

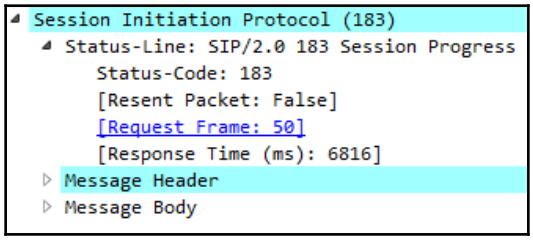

MagicJack+_short_call.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
1 0.000 0.000000000 192.168.0.10 192.168.0.1 ICMP 74 Echo (ping) request id=0x0000, seq=0/0, ttl=
2 0.016 0.016514000 192.168.0.1 192.168.0.10 ICMP 74 Echo (ping) reply id=0x0000, seq=0/0, ttl=
3 0.017 0.000661000 192.168.0.1 192.168.0.2 UDP 248 32772 → 2972 Len=206
4 5.012 4.995307000 Cisco-Li_1d:5f:eb Magicjac_61:4d:17 ARP 60 Who has 192.168.0.10? Tell 192.168.0.1
5 5.012 0.000495000 Magicjac_61:4d:17 Cisco-Li_1d:5f:eb ARP 60 192.168.0.10 is at 6c:33:a9:61:4d:17
6 5.720 0.707622000 192.168.0.10 216.234.64.8 UDP 60 59205 → 5070 Len=2
7 7.120 1.399640000 192.168.0.1 192.168.0.2 UDP 211 32772 → 2972 Len=169

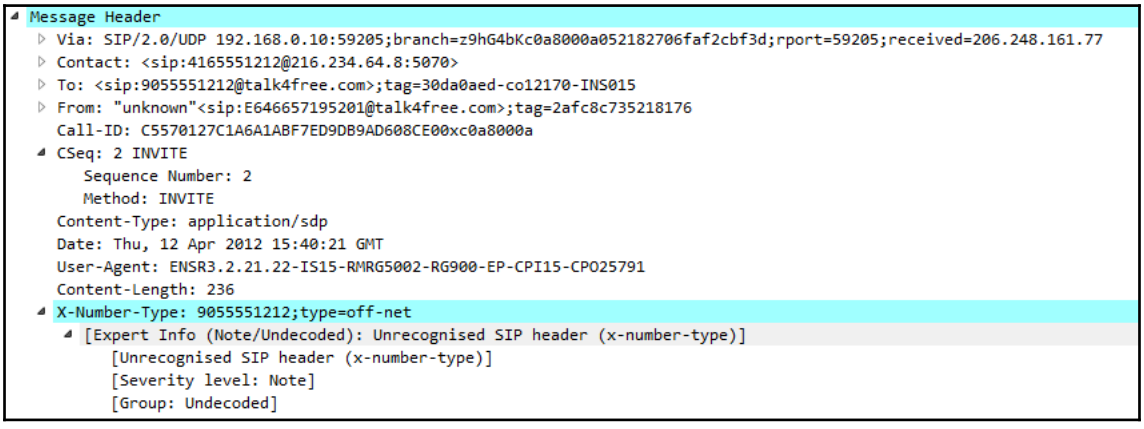

MagicJack+_short_call.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
47 159.085 0.044328000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
48 159.099 0.013744000 216.234.64.8 192.168.0.10 SIP 546 Status: 401 Unauthorized |
49 159.212 0.113272000 192.168.0.10 216.234.64.8 SIP 414 Request: ACK sip:9055551212@talk4free.com |
50 159.214 0.002296000 192.168.0.10 216.234.64.8 SIP/SDP 1157 Request: INVITE sip:9055551212@talk4free.com |
51 159.261 0.047019000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
54 166.030 1.953425000 216.234.64.8 192.168.0.10 SIP/SDP 866 Status: 183 Session Progress |
925 174.768 0.002825000 216.234.64.8 192.168.0.10 SIP/SDP 888 Status: 200 OK |
953 175.050 0.013135000 192.168.0.10 216.234.64.8 SIP 680 Request: ACK sip:9055551212@216.234.64.8:5070 |
1324 178.844 0.000197000 216.234.64.8 192.168.0.10 SIP 528 Request: BYE sip:E646657195201@206.248.161.77:59205
1329 178.954 0.049614000 192.168.0.10 216.234.64.8 SIP 685 Status: 200 OK |

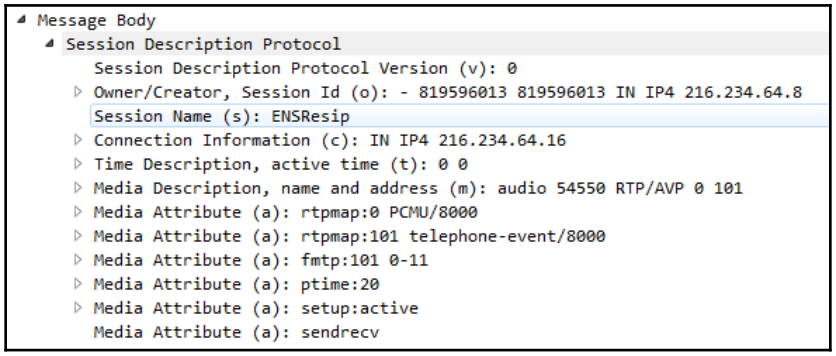

MagicJack+_short_call.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
sip || rtp
Expression...
No. Time Time delta from previous captured frame Source Destination Protocol Length Transmission Control Protocol Info
47 159.085 0.044328000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
48 159.099 0.013744000 216.234.64.8 192.168.0.10 SIP 546 Status: 401 Unauthorized |
49 159.212 0.113272000 192.168.0.10 216.234.64.8 SIP 414 Request: ACK sip:9055551212@talk4free.com |
50 159.214 0.002296000 192.168.0.10 216.234.64.8 SIP/SDP 1157 Request: INVITE sip:9055551212@talk4free.com
51 159.261 0.047019000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
54 166.030 1.953425000 216.234.64.8 192.168.0.10 SIP/SDP 866 Status: 183 Session Progress |
55 166.095 0.065078000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
57 166.125 0.016285000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
58 166.126 0.001239000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
59 166.151 0.024678000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
62 166.155 0.002953000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
63 166.157 0.002844000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
64 166.177 0.019945000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
65 166.185 0.007168000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
66 166.186 0.001204000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
67 166.197 0.011591000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
68 166.215 0.017257000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
69 166.217 0.002449000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184

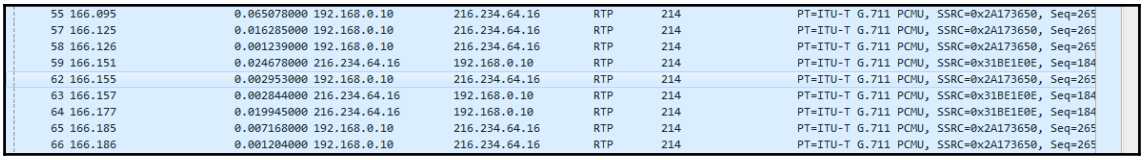

47 159.085 0.044328000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
48 159.099 0.013744000 216.234.64.8 192.168.0.10 SIP 546 Status: 401 Unauthorized |
49 159.212 0.113272000 192.168.0.10 216.234.64.8 SIP 414 Request: ACK sip:9055551212@talk4free.com |
50 159.214 0.002296000 192.168.0.10 216.234.64.8 SIP/SDP 1157 Request: INVITE sip:9055551212@talk4free.com
51 159.261 0.047019000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
54 166.030 1.953425000 216.234.64.8 192.168.0.10 SIP/SDP 866 Status: 183 Session Progress |

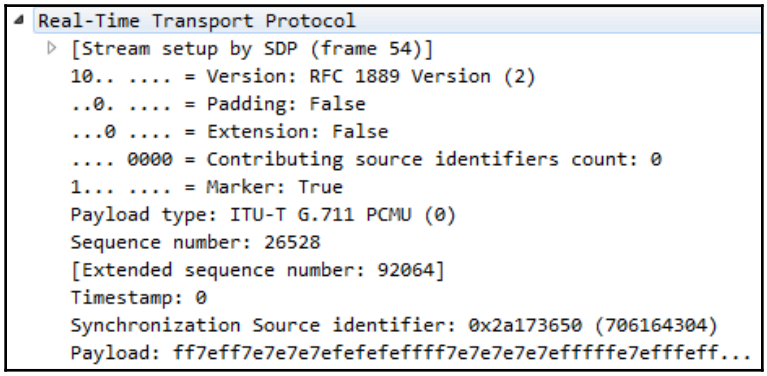

49 159.212 0.113272000 192.168.0.10 216.234.64.8 SIP 414 Request: ACK sip:9055551212@talk4free.com |
50 159.214 0.002296000 192.168.0.10 216.234.64.8 SIP/SDP 1157 Request: INVITE sip:9055551212@talk4free.com
51 159.261 0.047019000 216.234.64.8 192.168.0.10 SIP 372 Status: 100 Trying |
54 166.030 1.953425000 216.234.64.8 192.168.0.10 SIP/SDP 866 Status: 183 Session Progress |

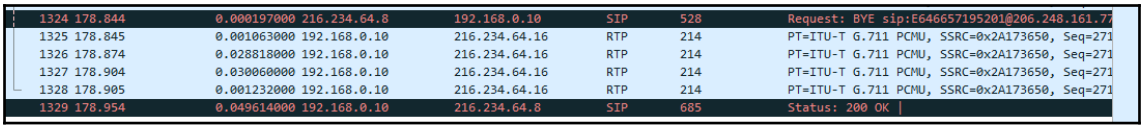

Session Initiation Protocol (183)
Status-Line: SIP/2.0 183 Session Progress
Status-Code: 183
[Resent Packet: False]
[Request Frame: 50]
[Response Time (ms): 6816]
Message Header
Message Body

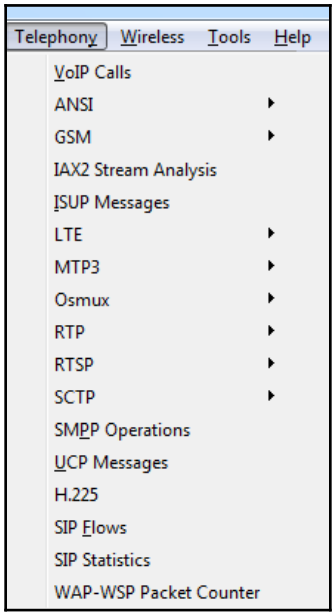

Message Header
Via: SIP/2.0/UDP 192.168.0.10:59205;branch=z9hG4bKc0a8000a052182706faf2cbf3d;rport=59205;received=206.248.161.77
Contact: <sip:4165551212@216.234.64.8:5070>
To: <sip:9055551212@talk4free.com>;tag=30da0aed-co12170-INS015
From: "unknown"<sip:E646657195201@talk4free.com>;tag=2afc8c735218176
Call-ID: C5570127C1A6A1ABF7ED9DB9AD608CE00xc0a8000a
CSeq: 2 INVITE
Sequence Number: 2
Method: INVITE
Content-Type: application/sdp
Date: Thu, 12 Apr 2012 15:40:21 GMT
User-Agent: ENSR3.2.21.22-IS15-RMRG5002-RG900-EP-CPI15-CPO25791
Content-Length: 236
X-Number-Type: 9055551212;type=off-net
[Expert Info (Note/Undecoded): Unrecognised SIP header (x-number-type)]
[Unrecognised SIP header (x-number-type)]
[Severity level: Note]
[Group: Undecoded]

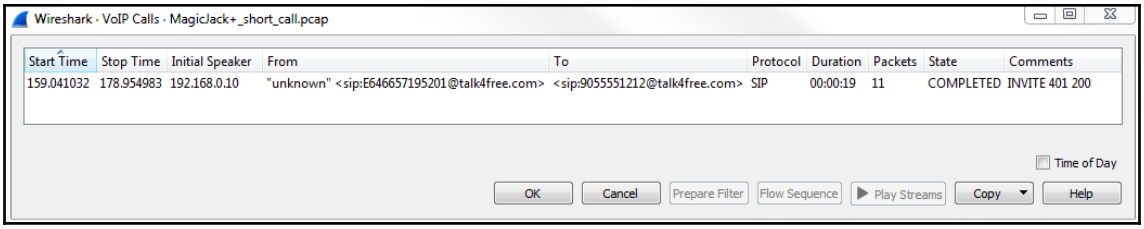

Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): - 819596013 819596013 IN IP4 216.234.64.8
Session Name (s): ENSResip
Connection Information (c): IN IP4 216.234.64.16
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 54550 RTP/AVP 0 101
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): fmtp:101 0-11
Media Attribute (a): ptime:20
Media Attribute (a): setup:active
Media Attribute (a): sendrecv

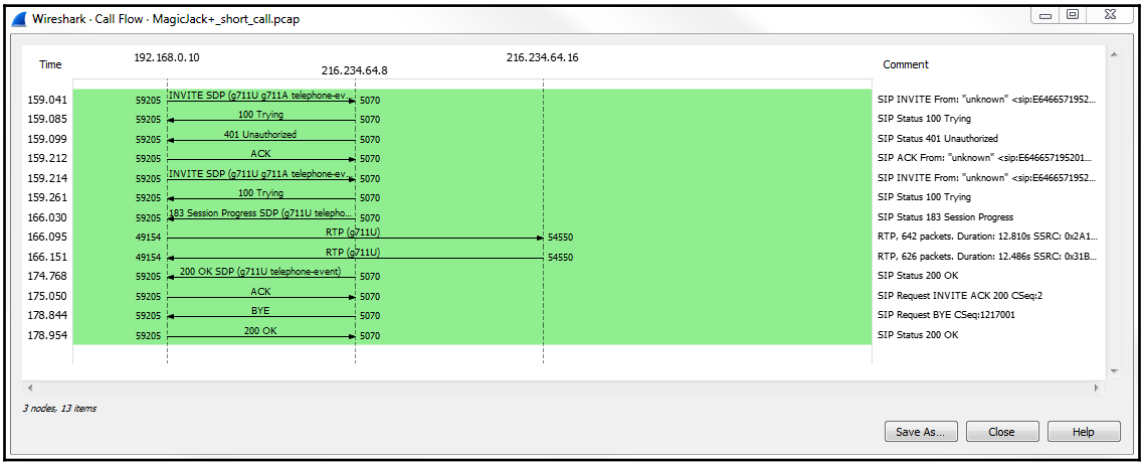

55 166.095 0.065078000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
57 166.125 0.016285000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
58 166.126 0.001239000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
59 166.151 0.024678000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
62 166.155 0.002953000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
63 166.157 0.002844000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
64 166.177 0.019945000 216.234.64.16 192.168.0.10 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x31BE1E0E, Seq=184
65 166.185 0.007168000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265
66 166.186 0.001204000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=265

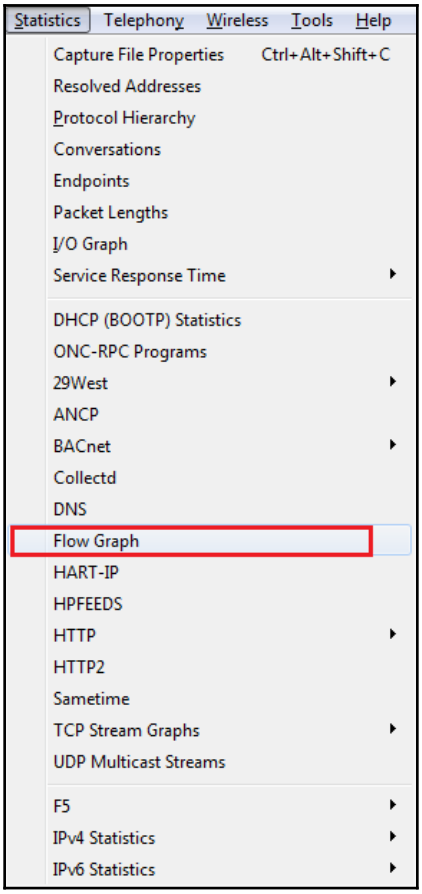

Real-Time Transport Protocol
[Stream setup by SDP (frame 54)]
10.. .... = Version: RFC 1889 Version (2)
..0. .... = Padding: False
...0 .... = Extension: False
.... 0000 = Contributing source identifiers count: 0
1... .... = Marker: True
Payload type: ITU-T G.711 PCMU (0)
Sequence number: 26528
[Extended sequence number: 92064]
Timestamp: 0
Synchronization Source identifier: 0x2a173650 (706164304)
Payload: ff7eff7e7e7e7efefefefffff7e7e7e7e7effffe7efffeff...

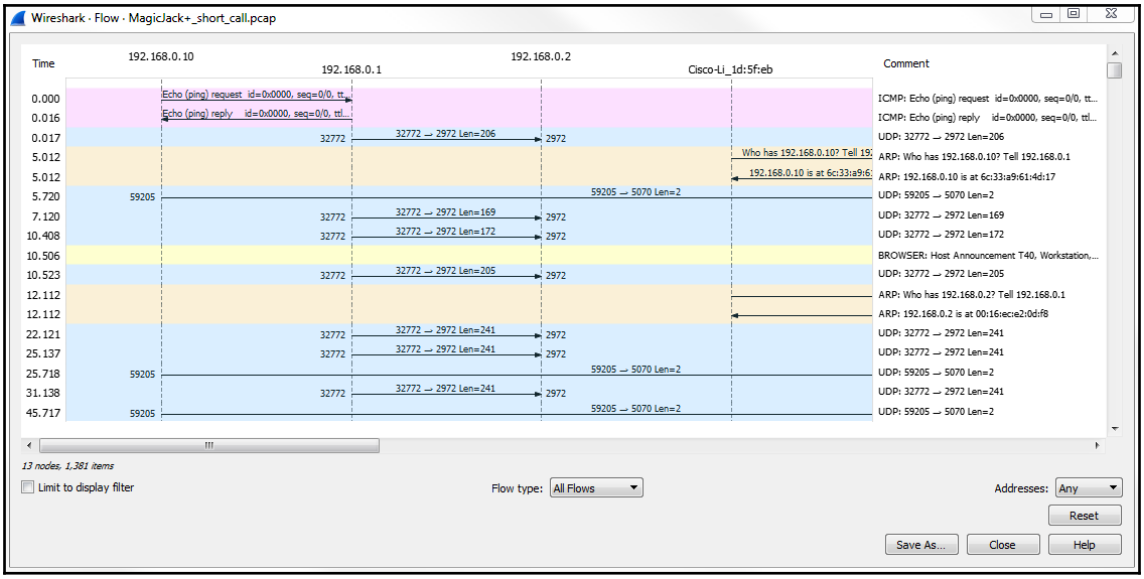

1324 178.844 0.000197000 216.234.64.8 192.168.0.10 SIP 528 Request: BYE sip:E646657195201@206.248.161.77
1325 178.845 0.001063000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=271
1326 178.874 0.028818000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=271
1327 178.904 0.030060000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=271
1328 178.905 0.001232000 192.168.0.10 216.234.64.16 RTP 214 PT=ITU-T G.711 PCMU, SSRC=0x2A173650, Seq=271
1329 178.954 0.049614000 192.168.0.10 216.234.64.8 SIP 685 Status: 200 OK

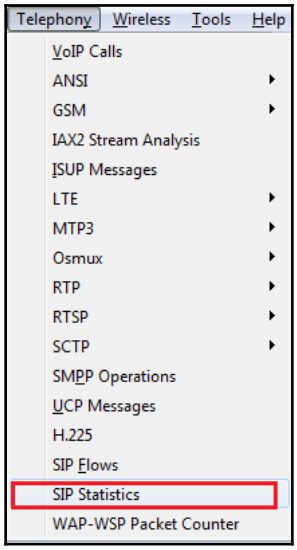

Telephony
Wireless
Tools
Help
VoIP Calls
ANSI
GSM
IAX2 Stream Analysis
ISUP Messages
LTE
MTP3
Osmux
RTP
RTSP
SCTP
SMPP Operations
UCP Messages
H.225
SIP Flows
SIP Statistics
WAP-WSP Packet Counter

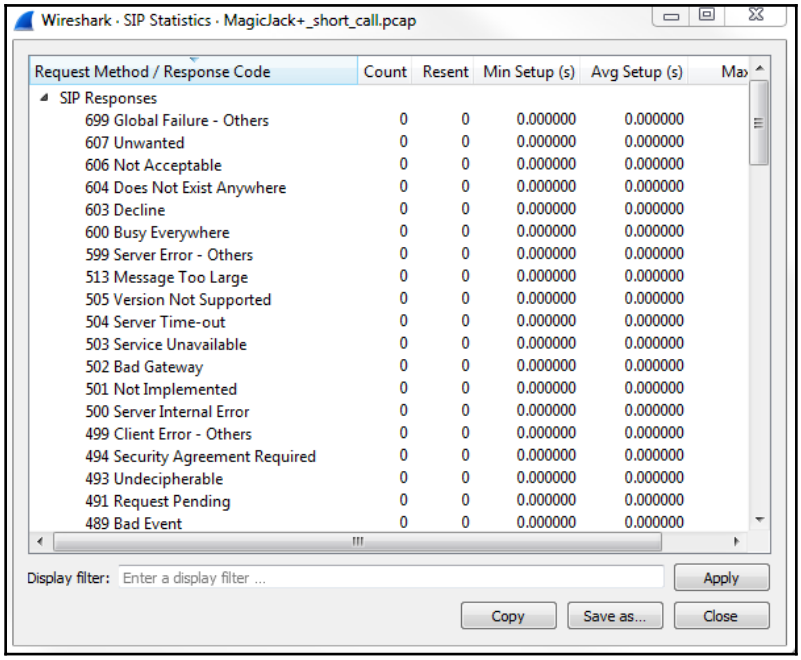

Wireshark · VoIP Calls · MagicJack+_short_call.pcap
Start Time
Stop Time
Initial Speaker
From
To
Protocol
Duration
Packets
State
Comments
159.041032
178.954983
192.168.0.10
"unknown" <sip:E646657195201@talk4free.com>
<sip:9055551212@talk4free.com>
SIP
00:00:19
11
COMPLETED
INVITE 401 200
Time of Day
OK
Cancel
Prepare Filter
Flow Sequence
Play Streams
Copy
Help

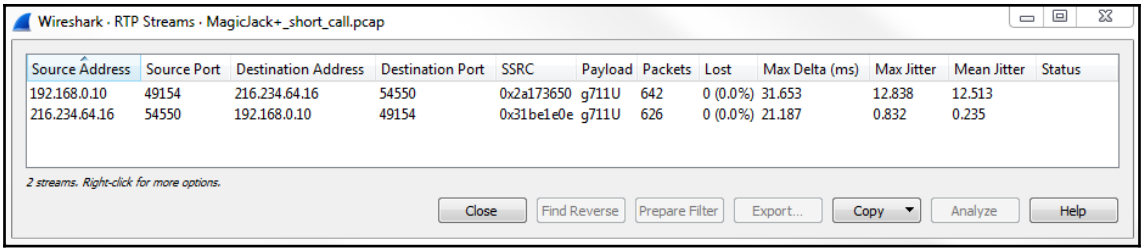

Wireshark · Call Flow · MagicJack+_short_call.pcap
Time
192.168.0.10
216.234.64.8
216.234.64.16
Comment
159.041 59205 INVITE SDP (g711U g711A telephone-ev... 5070 SIP INVITE From: "unknown" <sip:E6466571952...
159.085 59205 100 Trying 5070 SIP Status 100 Trying
159.099 59205 401 Unauthorized 5070 SIP Status 401 Unauthorized
159.212 59205 ACK 5070 SIP ACK From: "unknown" <sip:E646657195201...
159.214 59205 INVITE SDP (g711U g711A telephone-ev... 5070 SIP INVITE From: "unknown" <sip:E6466571952...
159.261 59205 100 Trying 5070 SIP Status 100 Trying
166.030 59205 183 Session Progress SDP (g711U telepho... 5070 SIP Status 183 Session Progress
166.095 49154 RTP (g711U) 54550 RTP, 642 packets. Duration: 12.810s SSRC: 0x2A1...
166.151 49154 RTP (g711U) 54550 RTP, 626 packets. Duration: 12.486s SSRC: 0x31B...
174.768 59205 200 OK SDP (g711U telephone-event) 5070 SIP Status 200 OK
175.050 59205 ACK 5070 SIP Request INVITE ACK 200 CSeq:2
178.844 59205 BYE 5070 SIP Request BYE CSeq:1217001
178.954 59205 200 OK 5070 SIP Status 200 OK
3 nodes, 13 items
Save As...
Close
Help

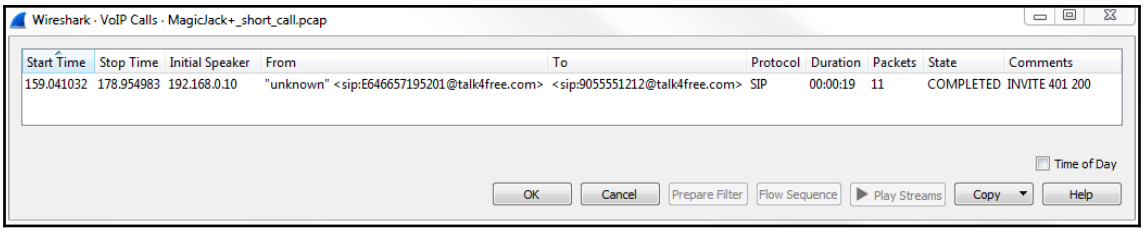

Statistics
Telephony
Wireless
Tools
Help
Capture File Properties
Ctrl+Alt+Shift+C
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
BACnet
Collectd
DNS
Flow Graph
HART-IP
HPFEEDS
HTTP
HTTP2
Sametime
TCP Stream Graphs
UDP Multicast Streams
F5
IPv4 Statistics
IPv6 Statistics

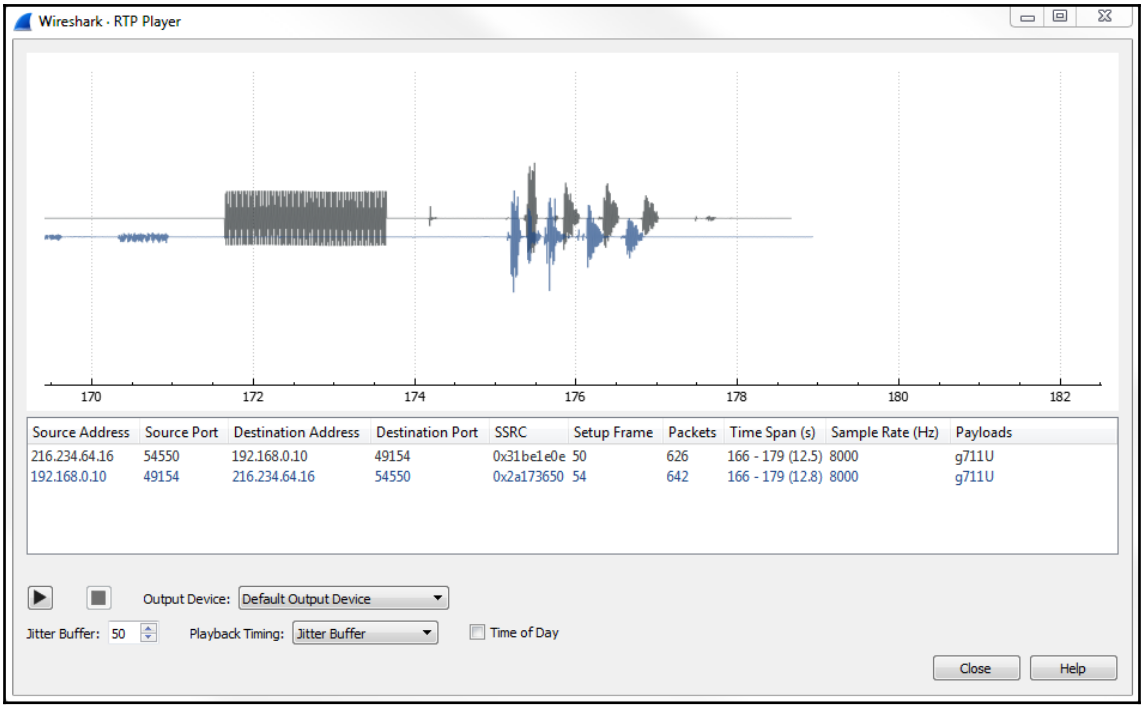

Wireshark · Flow · MagicJack+_short_call.pcap
Time
192.168.0.10
192.168.0.1
192.168.0.2
Cisco-Li_1d:5f:eb
Comment
0.000 Echo (ping) request id=0x0000, seq=0/0, tt...
0.016 Echo (ping) reply id=0x0000, seq=0/0, ttl...
0.017 32772 → 2972 Len=206
5.012 Who has 192.168.0.10? Tell 192.168.0.1
5.012 192.168.0.10 is at 6c:33:a9:61:4d:17
5.720 59205 → 5070 Len=2
7.120 32772 → 2972 Len=169
10.408 32772 → 2972 Len=172
10.506 BROWSER: Host Announcement T40, Workstation,...
10.523 32772 → 2972 Len=205
12.112 ARP: Who has 192.168.0.2? Tell 192.168.0.1
12.112 ARP: 192.168.0.2 is at 00:16:ec:e2:0d:f8
22.121 32772 → 2972 Len=241
25.137 32772 → 2972 Len=241
25.718 59205 → 5070 Len=2
31.138 32772 → 2972 Len=241
45.717 59205 → 5070 Len=2
13 nodes, 1,381 items
Limit to display filter
Flow type: All Flows
Addresses: Any
Reset
Save As...
Close
Help

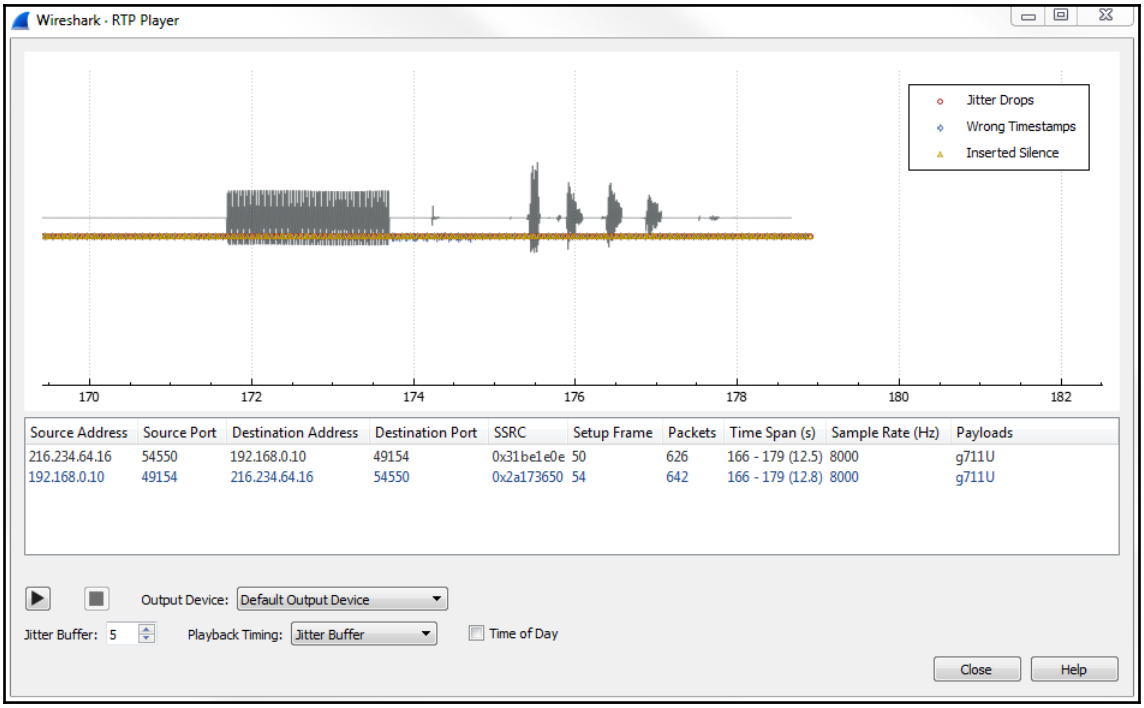

Telephony
Wireless
Tools
Help
VoIP Calls
ANSI
GSM
IAX2 Stream Analysis
ISUP Messages
LTE
MTP3
Osmux
RTP
RTSP
SCTP
SMPP Operations
UCP Messages
H.225
SIP Flows
SIP Statistics
WAP-WSP Packet Counter

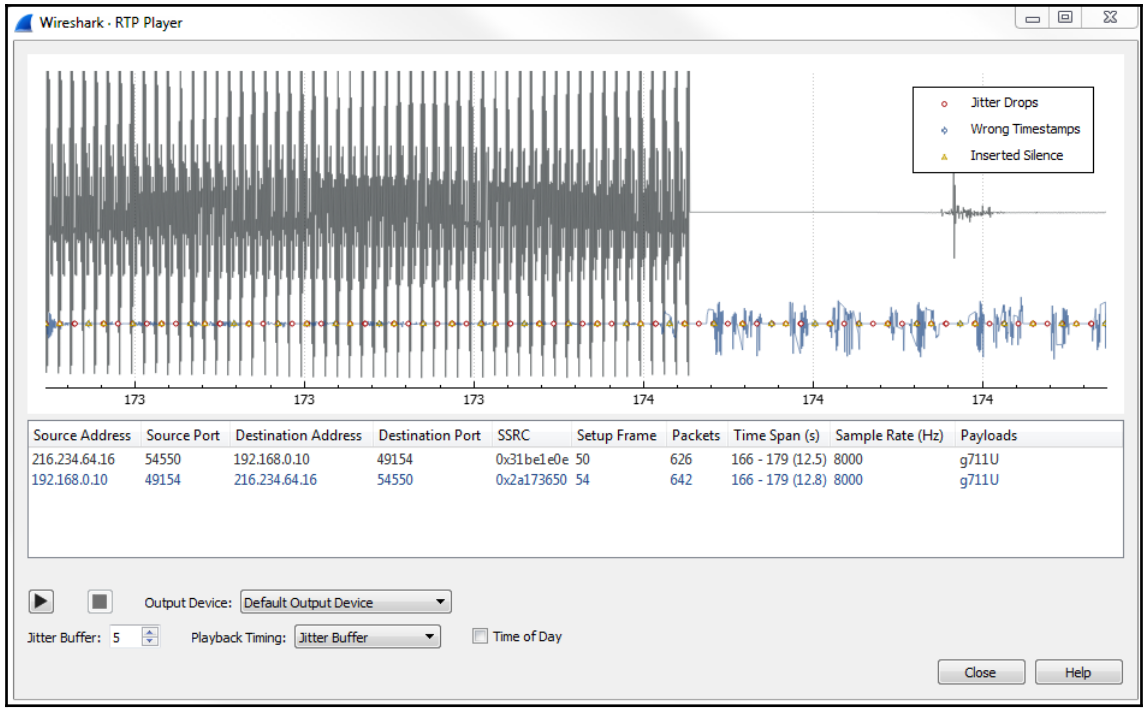

Wireshark · SIP Statistics · MagicJack+_short_call.pcap
Request Method / Response Code
Count
Resent
Min Setup (s)
Avg Setup (s)
Max
SIP Responses
699 Global Failure - Others 0 0 0.000000 0.000000
607 Unwanted 0 0 0.000000 0.000000
606 Not Acceptable 0 0 0.000000 0.000000
604 Does Not Exist Anywhere 0 0 0.000000 0.000000
603 Decline 0 0 0.000000 0.000000
600 Busy Everywhere 0 0 0.000000 0.000000
599 Server Error - Others 0 0 0.000000 0.000000
513 Message Too Large 0 0 0.000000 0.000000
505 Version Not Supported 0 0 0.000000 0.000000
504 Server Time-out 0 0 0.000000 0.000000
503 Service Unavailable 0 0 0.000000 0.000000
502 Bad Gateway 0 0 0.000000 0.000000
501 Not Implemented 0 0 0.000000 0.000000
500 Server Internal Error 0 0 0.000000 0.000000
499 Client Error - Others 0 0 0.000000 0.000000
494 Security Agreement Required 0 0 0.000000 0.000000
493 Undecipherable 0 0 0.000000 0.000000
491 Request Pending 0 0 0.000000 0.000000
489 Bad Event 0 0 0.000000 0.000000
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

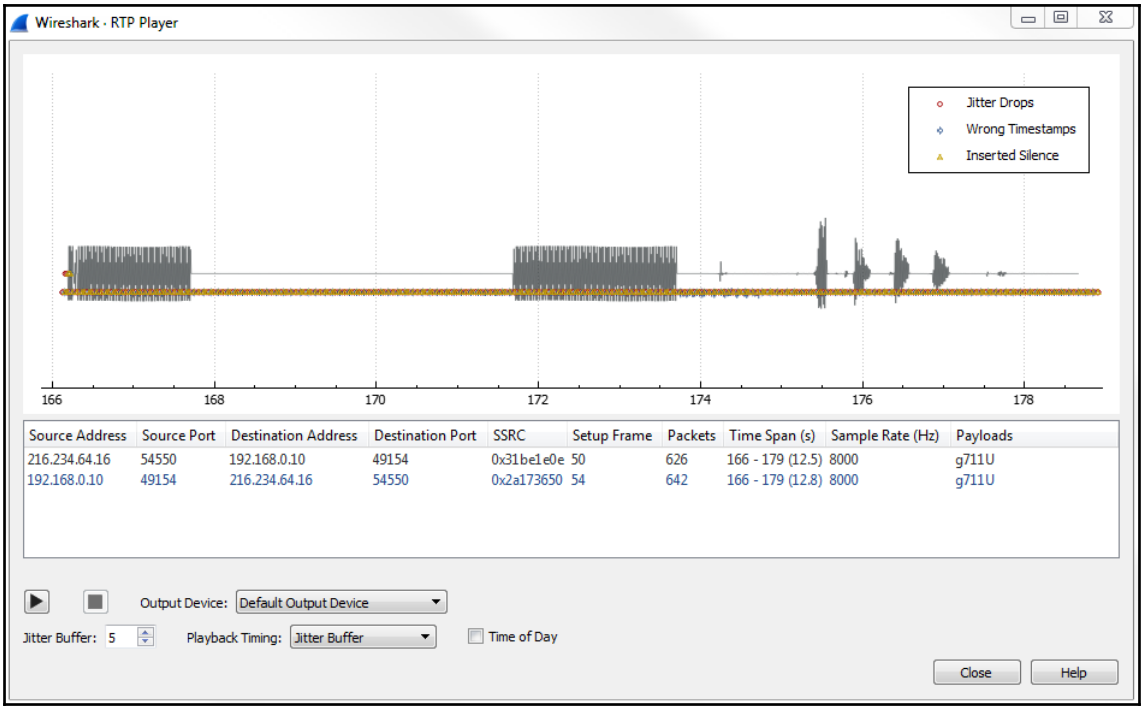

Wireshark · RTP Streams · MagicJack+_short_call.pcap
Source Address
Source Port
Destination Address
Destination Port
SSRC
Payload
Packets
Lost
Max Delta (ms)
Max Jitter
Mean Jitter
Status
192.168.0.10 49154 216.234.64.16 54550 0x2a173650 g711U 642 0 (0.0%) 31.653 12.838 12.513
216.234.64.16 54550 192.168.0.10 49154 0x31be1e0e g711U 626 0 (0.0%) 21.187 0.832 0.235
2 streams. Right-click for more options.
Close
Find Reverse
Prepare Filter
Export...
Copy
Analyze
Help


Wireshark · VoIP Calls · MagicJack+_short_call.pcap
Start Time
Stop Time
Initial Speaker
From
To
Protocol
Duration
Packets
State
Comments
159.041032 178.954983 192.168.0.10 "unknown" <sip:E646657195201@talk4free.com> <sip:9055551212@talk4free.com> SIP 00:00:19 11 COMPLETED INVITE 401 200
Time of Day
OK
Cancel
Prepare Filter
Flow Sequence
Play Streams
Copy
Help

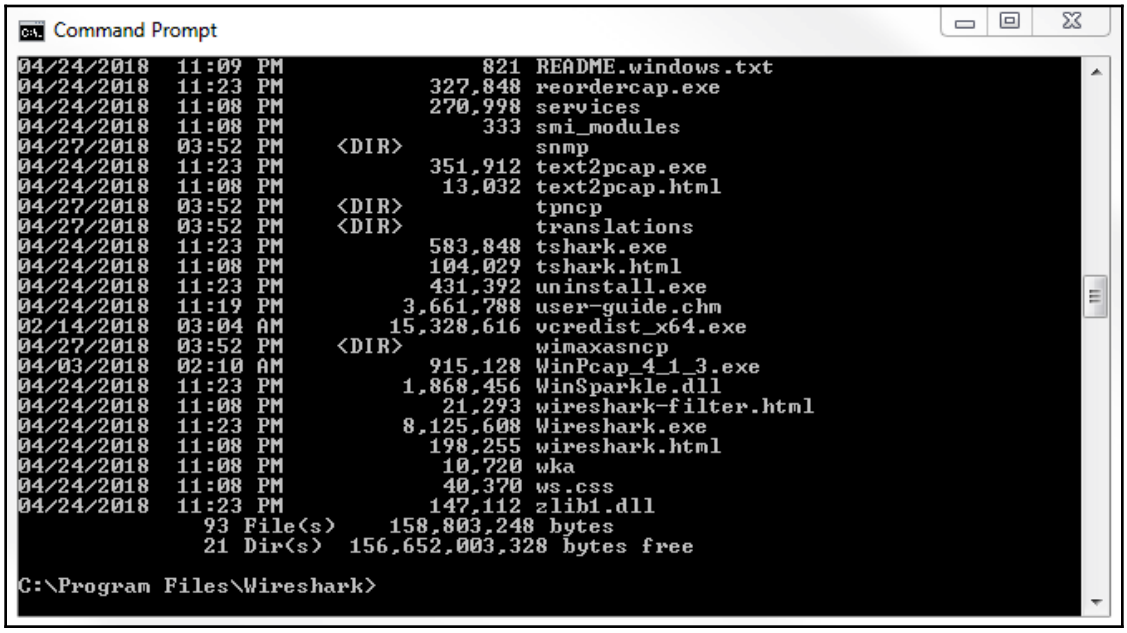

Wireshark · RTP Player
170
172
174
176
178
180
182
Source Address Source Port Destination Address Destination Port SSRC Setup Frame Packets Time Span (s) Sample Rate (Hz) Payloads
216.234.64.16 54550 192.168.0.10 49154 0x31be1e0e 50 626 166 - 179 (12.5) 8000 g711U
192.168.0.10 49154 216.234.64.16 54550 0x2a173650 54 642 166 - 179 (12.8) 8000 g711U
Output Device: Default Output Device
Jitter Buffer: 50
Playback Timing: Jitter Buffer
Time of Day
Close
Help

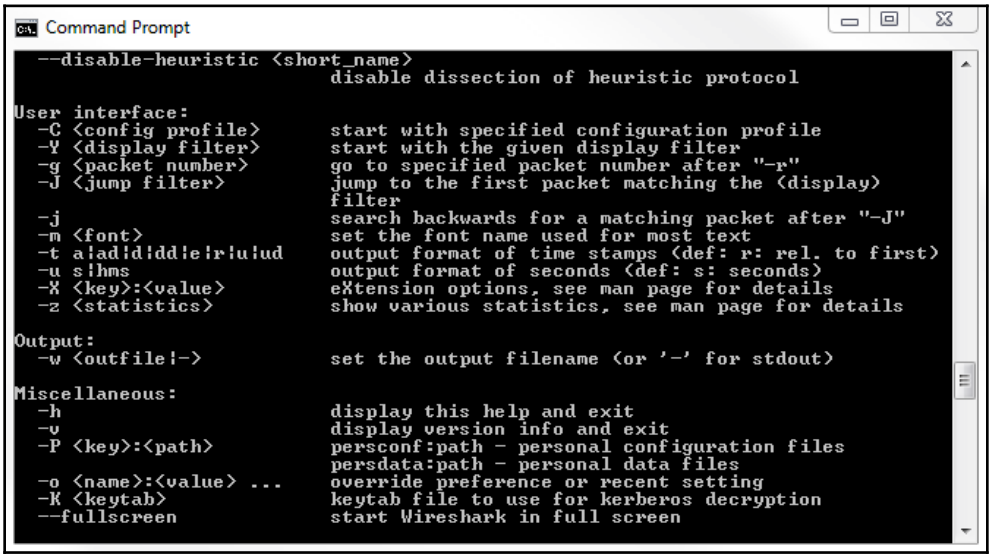

Wireshark · RTP Player
Jitter Drops
Wrong Timestamps
Inserted Silence
170
172
174
176
178
180
182
Source Address Source Port Destination Address Destination Port SSRC Setup Frame Packets Time Span (s) Sample Rate (Hz) Payloads
216.234.64.16 54550 192.168.0.10 49154 0x31be1e0e 50 626 166 - 179 (12.5) 8000 g711U
192.168.0.10 49154 216.234.64.16 54550 0x2a173650 54 642 166 - 179 (12.8) 8000 g711U
Output Device: Default Output Device
Jitter Buffer: 5
Playback Timing: Jitter Buffer
Time of Day
Close
Help

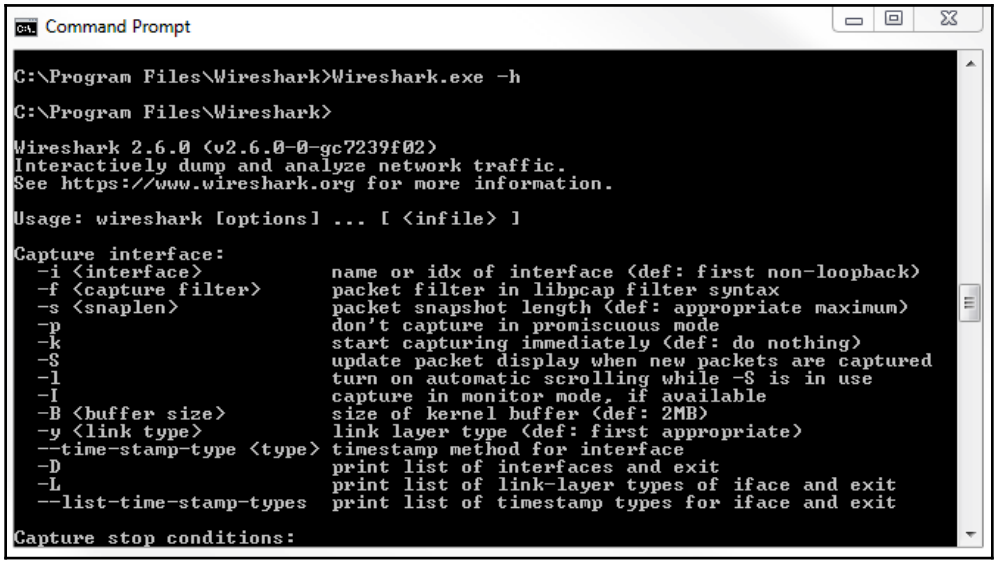

Wireshark · RTP Player
Jitter Drops
Wrong Timestamps
Inserted Silence
173
173
173
174
174
174
Source Address Source Port Destination Address Destination Port SSRC Setup Frame Packets Time Span (s) Sample Rate (Hz) Payloads
216.234.64.16 54550 192.168.0.10 49154 0x31be1e0e 50 626 166 - 179 (12.5) 8000 g711U
192.168.0.10 49154 216.234.64.16 54550 0x2a173650 54 642 166 - 179 (12.8) 8000 g711U
Output Device: Default Output Device
Jitter Buffer: 5
Playback Timing: Jitter Buffer
Time of Day
Close
Help

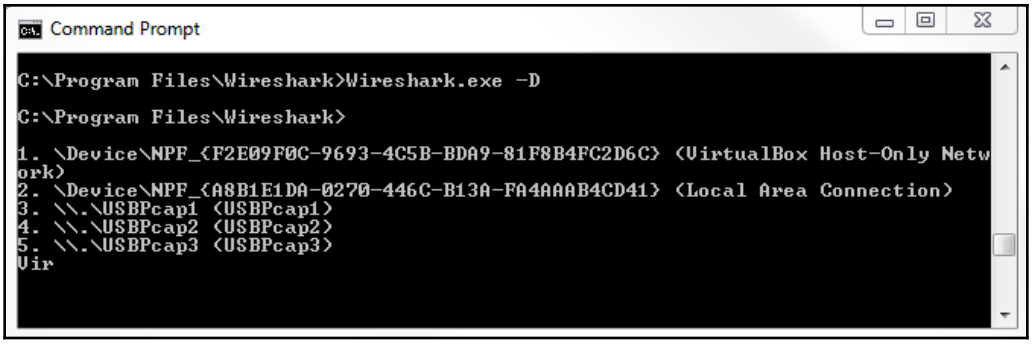

Wireshark · RTP Player
Jitter Drops
Wrong Timestamps
Inserted Silence
166
168
170
172
174
176
178
Source Address
Source Port
Destination Address
Destination Port
SSRC
Setup Frame
Packets
Time Span (s)
Sample Rate (Hz)
Payloads
216.234.64.16
54550
192.168.0.10
49154
0x31be1e0e
50
626
166 - 179 (12.5)
8000
g711U
192.168.0.10
49154
216.234.64.16
54550
0x2a173650
54
642
166 - 179 (12.8)
8000
g711U
Output Device:
Default Output Device
Jitter Buffer:
5
Playback Timing:
Jitter Buffer
Time of Day
Close
Help

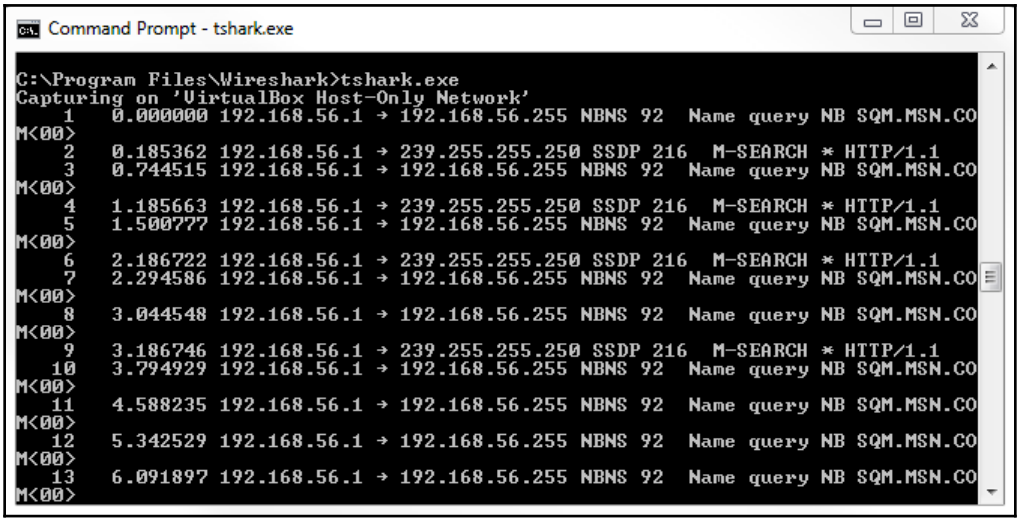
Chapter 10: Command-Line Tools

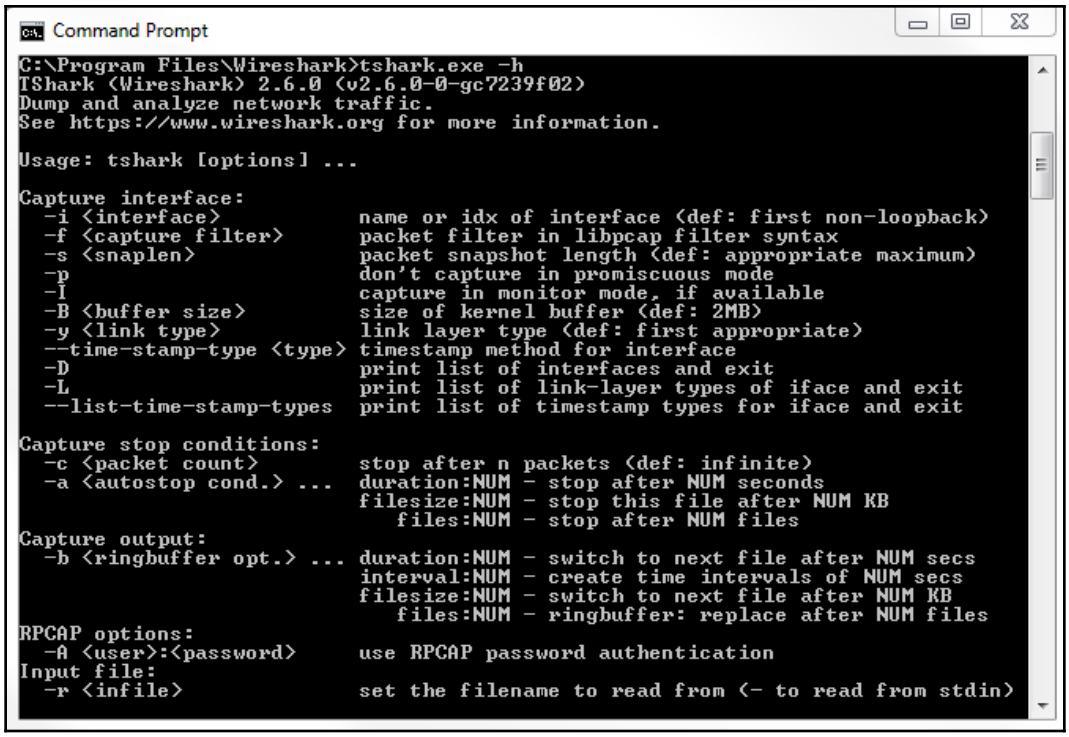


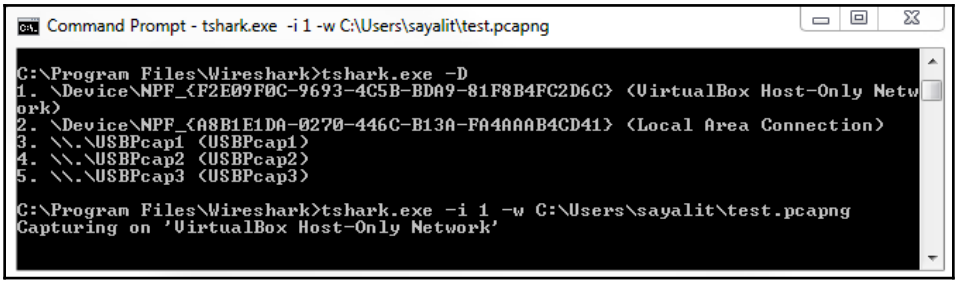


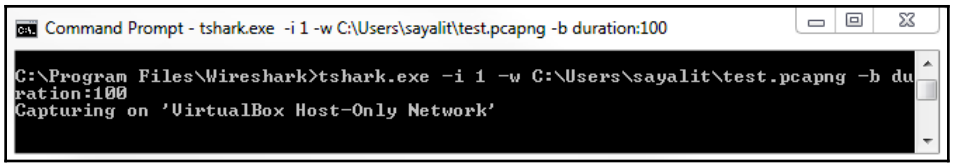

Command Prompt
C:\Program Files\Wireshark>Wireshark.exe -h
C:\Program Files\Wireshark>
Wireshark 2.6.0 (v2.6.0-0-gc7239f02)
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.
Usage: wireshark [options] ... [<infile>]
Capture interface:
-i <interface> name or idx of interface (def: first non-loopback)
-f <capture filter> packet filter in libpcap filter syntax
-s <snaplen> packet snapshot length (def: appropriate maximum)
-p don't capture in promiscuous mode
-k start capturing immediately (def: do nothing)
-S update packet display when new packets are captured
-l turn on automatic scrolling while -S is in use
-I capture in monitor mode, if available
-B <buffer size> size of kernel buffer (def: 2MB)
-y <link type> link layer type (def: first appropriate)
--time-stamp-type <type> timestamp method for interface
-D print list of interfaces and exit
-L print list of link-layer types of iface and exit
--list-time-stamp-types print list of timestamp types for iface and exit
Capture stop conditions:


Command Prompt
C:\Program Files\Wireshark>Wireshark.exe -D
C:\Program Files\Wireshark>
1. \Device\NPF_{F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C} (VirtualBox Host-Only Netw
ork)
2. \Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41} (Local Area Connection)
3. \\.\USBPcap1 (USBPcap1)
4. \\.\USBPcap2 (USBPcap2)
5. \\.\USBPcap3 (USBPcap3)
Vir


Command Prompt - tshark.exe
C:\Program Files\Wireshark>tshark.exe
Capturing on 'VirtualBox Host-Only Network'
1 0.000000 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
2 0.185362 192.168.56.1 → 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
3 0.744515 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
4 1.185663 192.168.56.1 → 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
5 1.500777 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
6 2.186722 192.168.56.1 → 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
7 2.294586 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
8 3.044548 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
9 3.186746 192.168.56.1 → 239.255.255.250 SSDP 216 M-SEARCH * HTTP/1.1
10 3.794929 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
11 4.588235 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
12 5.342529 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>
13 6.091897 192.168.56.1 → 192.168.56.255 NBNS 92 Name query NB SQM.MSN.CO
M<00>


Command Prompt
C:\Program Files\Wireshark>tshark.exe -h
TShark (Wireshark) 2.6.0 (v2.6.0-0-gc7239f02)
Dump and analyze network traffic.
See https://www.wireshark.org for more information.
Usage: tshark [options] ...
Capture interface:
-i <interface> name or idx of interface (def: first non-loopback)
-f <capture filter> packet filter in libpcap filter syntax
-s <snaplen> packet snapshot length (def: appropriate maximum)
-p don't capture in promiscuous mode
-I capture in monitor mode, if available
-B <buffer size> size of kernel buffer (def: 2MB)
-y <link type> link layer type (def: first appropriate)
--time-stamp-type <type> timestamp method for interface
-D print list of interfaces and exit
-L print list of link-layer types of iface and exit
--list-time-stamp-types print list of timestamp types for iface and exit
Capture stop conditions:
-c <packet count> stop after n packets (def: infinite)
-a <autostop cond.> ... duration:NUM - stop after NUM seconds
filesize:NUM - stop this file after NUM KB
files:NUM - stop after NUM files
Capture output:
-b <ringbuffer opt.> ... duration:NUM - switch to next file after NUM secs
interval:NUM - create time intervals of NUM secs
filesize:NUM - switch to next file after NUM KB
files:NUM - ringbuffer: replace after NUM files
RPCAP options:
-A <user>:<password> use RPCAP password authentication
Input file:
-r <infile> set the filename to read from (- to read from stdin)






```
andrew@ubuntu:~$ tcpdump --help
tcpdump version 4.7.4
libpcap version 1.7.4
OpenSSL 1.0.2g  1 Mar 2016
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqRStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z command ]
                [ -Z user ] [ expression ]
```

```
andrew@ubuntu:~$ man tcpdump
andrew@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:5a:28:8e
          inet addr:192.168.139.131  Bcast:192.168.139.255  Mask:255.255.255.0
          inet6 addr: fe80::ffe8:9443:3f8f:42d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:167879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75044 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:220455267 (220.4 MB)  TX bytes:4541715 (4.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:22103 (22.1 KB)  TX bytes:22103 (22.1 KB)
```

```
andrew@ubuntu:~$ ifconfig
ens33     Link encap:Ethernet  HWaddr 00:0c:29:5a:28:8e
          inet addr:192.168.139.131  Bcast:192.168.139.255  Mask:255.255.255.0
          inet6 addr: fe80::ffe8:9443:3f8f:42d0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:167879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75044 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:220455267 (220.4 MB)  TX bytes:4541715 (4.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:22103 (22.1 KB)  TX bytes:22103 (22.1 KB)

andrew@ubuntu:~$
andrew@ubuntu:~$ tcpdump
tcpdump: ens33: You don't have permission to capture on that device
(socket: Operation not permitted)
andrew@ubuntu:~$
```

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:167879 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75044 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:220455267 (220.4 MB)  TX bytes:4541715 (4.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:22103 (22.1 KB)  TX bytes:22103 (22.1 KB)

andrew@ubuntu:~$
andrew@ubuntu:~$ tcpdump
tcpdump: ens33: You don't have permission to capture on that device
(socket: Operation not permitted)
andrew@ubuntu:~$ sudo tcpdump
[sudo] password for andrew:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
```

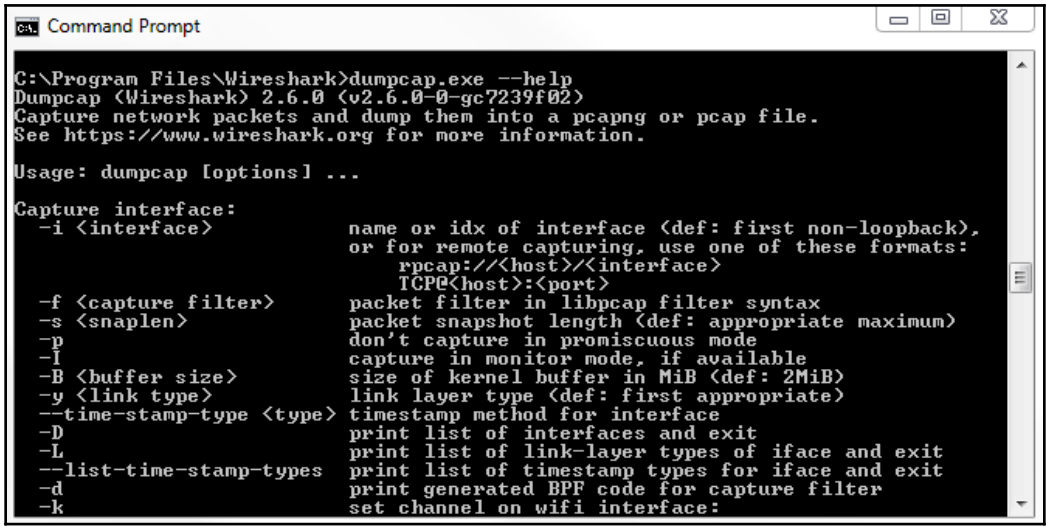
```
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:275 errors:0 dropped:0 overruns:0 frame:0
          TX packets:275 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:22103 (22.1 KB)  TX bytes:22103 (22.1 KB)

andrew@ubuntu:~$
andrew@ubuntu:~$ tcpdump
tcpdump: ens33: You don't have permission to capture on that device
(socket: Operation not permitted)
andrew@ubuntu:~$ sudo tcpdump
[sudo] password for andrew:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
andrew@ubuntu:~$ sudo tcpdump -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
```

```
andrew@ubuntu:~$ sudo tcpdump -i lo
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
18:59:45.040066 IP localhost > localhost: ICMP echo request, id 19418, seq 1, le
ngth 64
18:59:45.040078 IP localhost > localhost: ICMP echo reply, id 19418, seq 1, leng
th 64
18:59:46.039267 IP localhost > localhost: ICMP echo request, id 19418, seq 2, le
ngth 64
18:59:46.039278 IP localhost > localhost: ICMP echo re
th 64
18:59:47.039418 IP localhost > localhost: ICMP echo re
ngth 64
18:59:47.039429 IP localhost > localhost: ICMP echo re
th 64
18:59:48.039324 IP localhost > localhost: ICMP echo re
ngth 64
18:59:48.039334 IP localhost > localhost: ICMP echo re
th 64
```

```
andrew@ubuntu: ~
andrew@ubuntu:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.084 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.051 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.046 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.049 ms
```

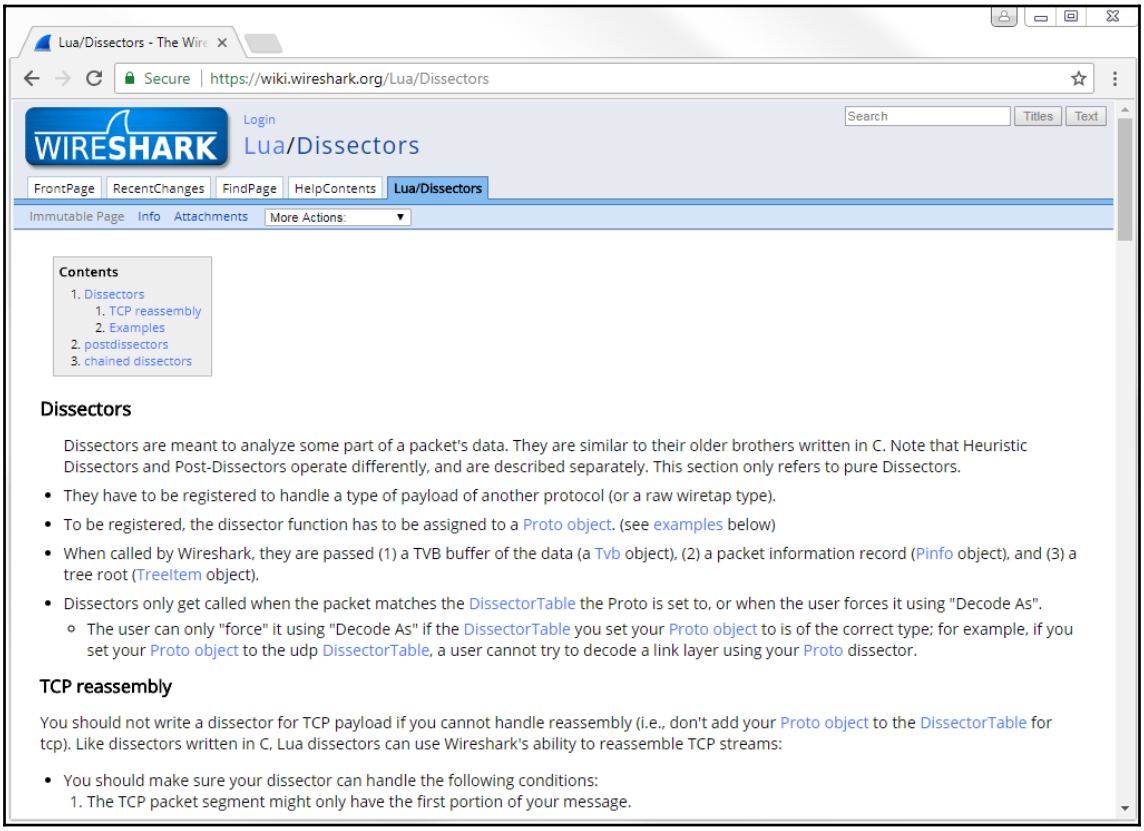
```
19:00:08.039088 IP localhost > localhost: ICMP echo request, id 19418, seq 24, l
ength 64
19:00:08.039102 IP localhost > localhost: ICMP echo reply, id 19418, seq 24, len
gth 64
19:00:09.039182 IP localhost > localhost: ICMP echo request, id 19418, seq 25, l
ength 64
19:00:09.039193 IP localhost > localhost: ICMP echo reply, id 19418, seq 25, len
gth 64
19:00:10.039226 IP localhost > localhost: ICMP echo request, id 19418, seq 26, l
ength 64
19:00:10.039237 IP localhost > localhost: ICMP echo reply, id 19418, seq 26, len
gth 64
19:00:11.039182 IP localhost > localhost: ICMP echo request, id 19418, seq 27, l
ength 64
19:00:11.039194 IP localhost > localhost: ICMP echo reply, id 19418, seq 27, len
gth 64
^C
54 packets captured
108 packets received by filter
0 packets dropped by kernel
andrew@ubuntu:~$ ls
Desktop    Downloads         Music     Public     test.pcap
Documents  examples.desktop  Pictures  Templates  Videos
andrew@ubuntu:~$
```

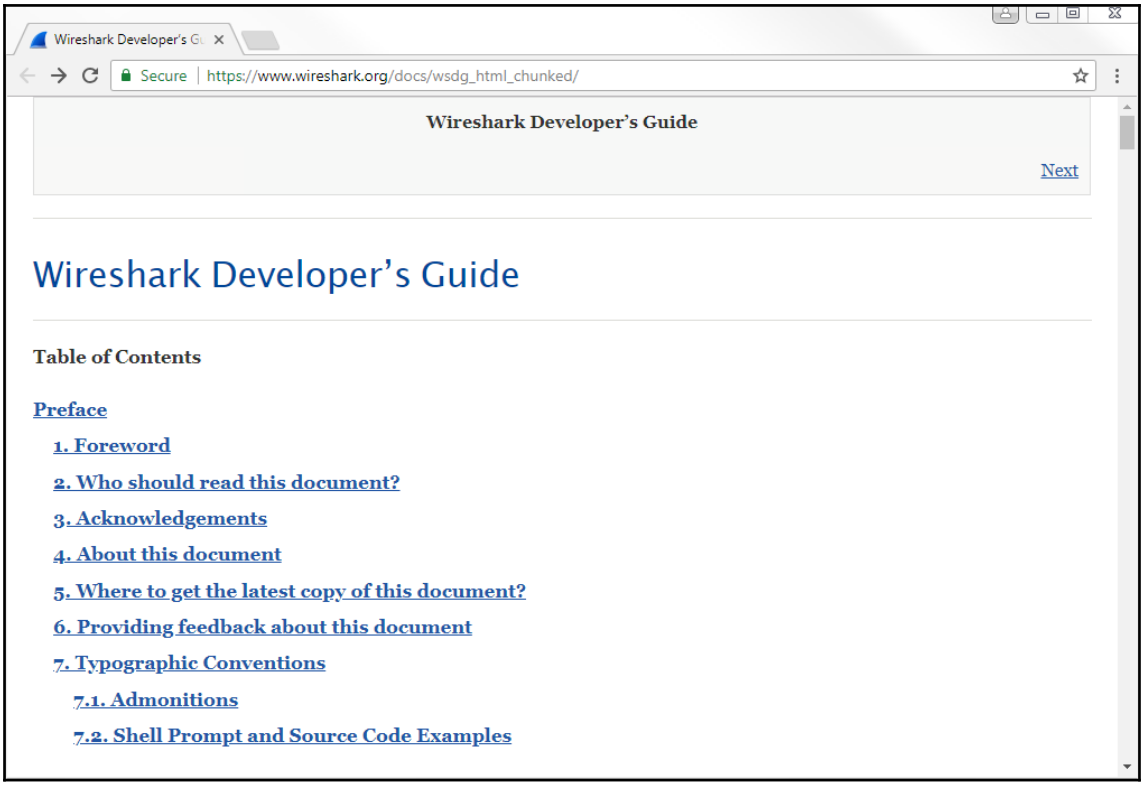
```
19:00:10.039237 IP localhost > localhost: ICMP echo reply, id 19418, seq 26, len
gth 64
19:00:11.039182 IP localhost > localhost: ICMP echo request, id 19418, seq 27, l
ength 64
19:00:11.039194 IP localhost > localhost: ICMP echo reply, id 19418, seq 27, len
gth 64
^C
54 packets captured
108 packets received by filter
0 packets dropped by kernel
andrew@ubuntu:~$ ls
Desktop    Downloads         Music     Public     test.pcap
Documents  examples.desktop  Pictures  Templates  Videos
andrew@ubuntu:~$ rm test.pcap
rm: remove write-protected regular file 'test.pcap'? yes
andrew@ubuntu:~$ ls
Desktop    Downloads         Music     Public     Videos
Documents  examples.desktop  Pictures  Templates
andrew@ubuntu:~$ sudo tcpdump -i lo -w test.pcap
tcpdump: listening on lo, link-type EN10MB (Ethernet), capture size 262144 bytes
^C32 packets captured
64 packets received by filter
0 packets dropped by kernel
andrew@ubuntu:~$ ls
```

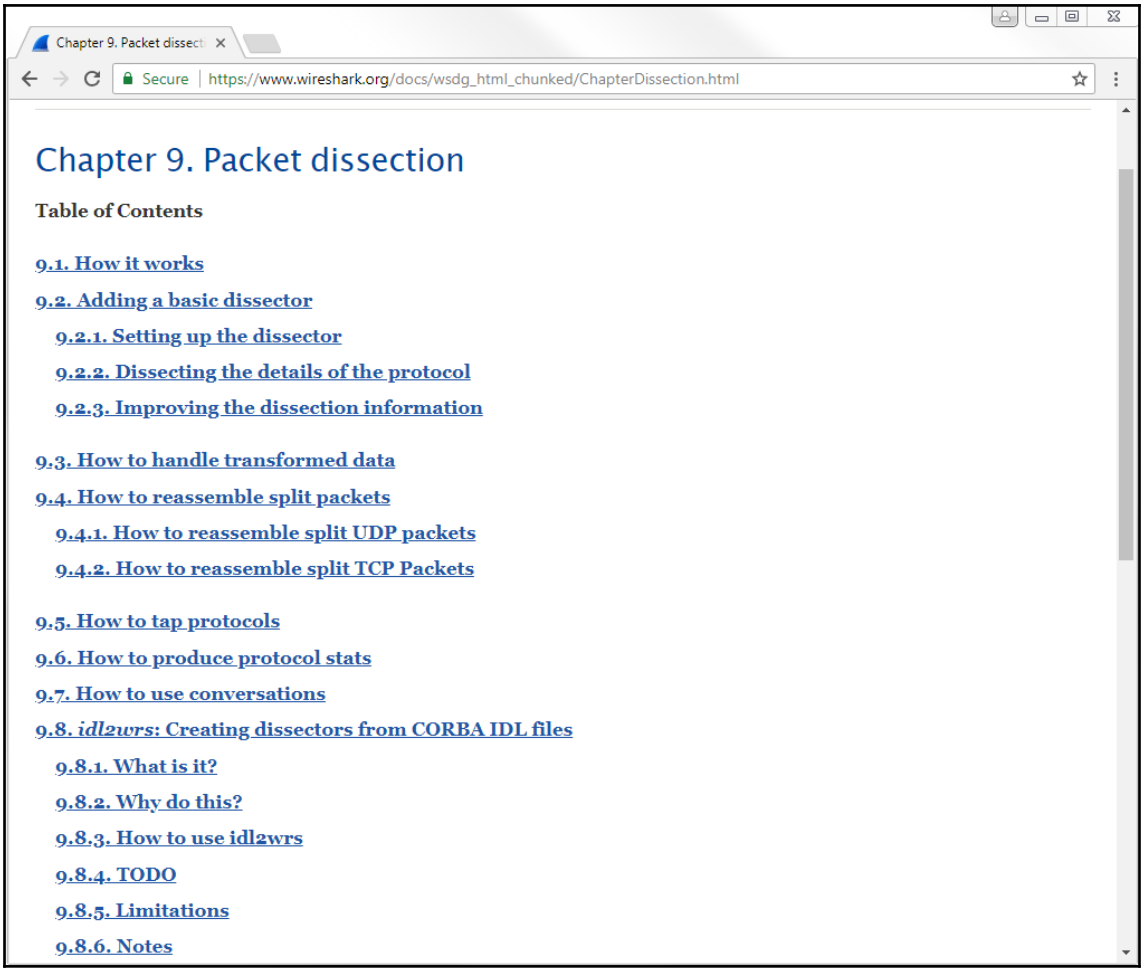

Command Prompt
C:\Program Files\Wireshark>dumpcap.exe --help
Dumpcap (Wireshark) 2.6.0 (v2.6.0-0-gc7239f02)
Capture network packets and dump them into a pcapng or pcap file.
See https://www.wireshark.org for more information.
Usage: dumpcap [options] ...
Capture interface:
-i <interface> name or idx of interface (def: first non-loopback),
or for remote capturing, use one of these formats:
rpcap://<host>/<interface>
TCP@<host>:<port>
-f <capture filter> packet filter in libpcap filter syntax
-s <snaplen> packet snapshot length (def: appropriate maximum)
-p don't capture in promiscuous mode
-I capture in monitor mode, if available
-B <buffer size> size of kernel buffer in MiB (def: 2MiB)
-y <link type> link layer type (def: first appropriate)
--time-stamp-type <type> timestamp method for interface
-D print list of interfaces and exit
-L print list of link-layer types of iface and exit
--list-time-stamp-types print list of timestamp types for iface and exit
-d print generated BPF code for capture filter
-k set channel on wifi interface:

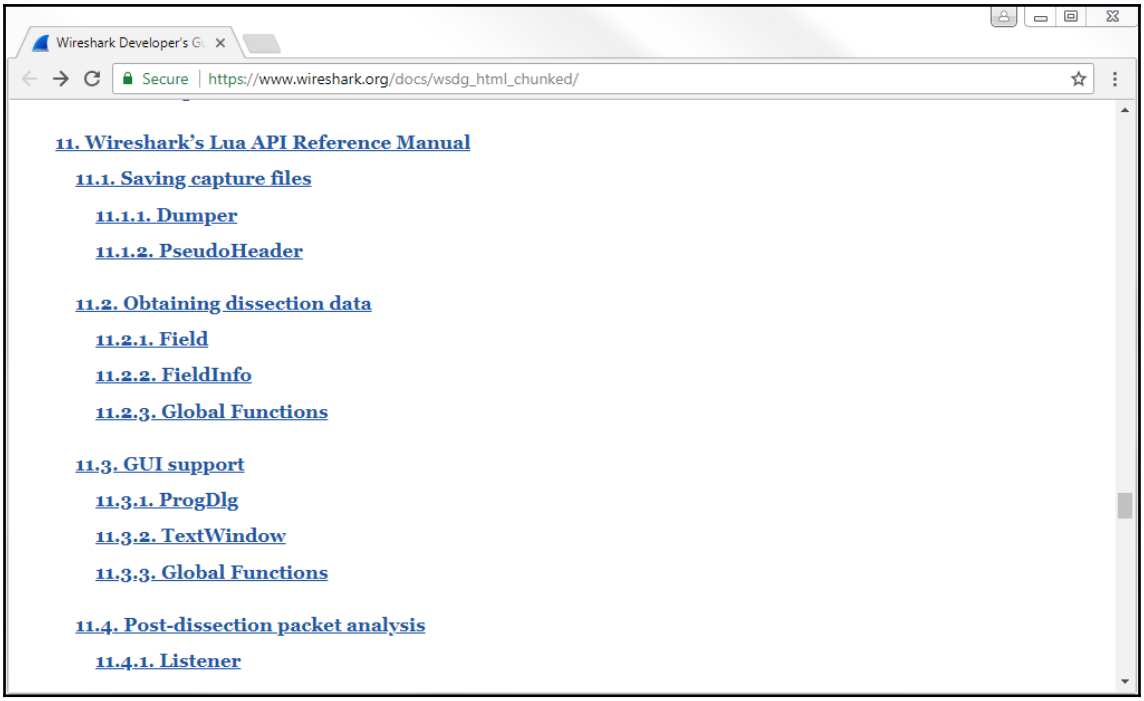

Command Prompt
C:\Program Files\Wireshark>dumpcap.exe -D
1. \Device\NPF_{F2E09F0C-9693-4C5B-BDA9-81F8B4FC2D6C} (VirtualBox Host-Only Network)
2. \Device\NPF_{A8B1E1DA-0270-446C-B13A-FA4AAAB4CD41} (Local Area Connection)
C:\Program Files\Wireshark>dumpcap.exe -i 1 -w C:\Users\sayalit\dump.pcap
Capturing on 'VirtualBox Host-Only Network'
File: C:\Users\sayalit\dump.pcap
Packets captured: 0
Packets received/dropped on interface 'VirtualBox Host-Only Network': 0/0 (pcap:0/dumpcap:0/flushed:0/ps_ifdrop:0) (0.0%)

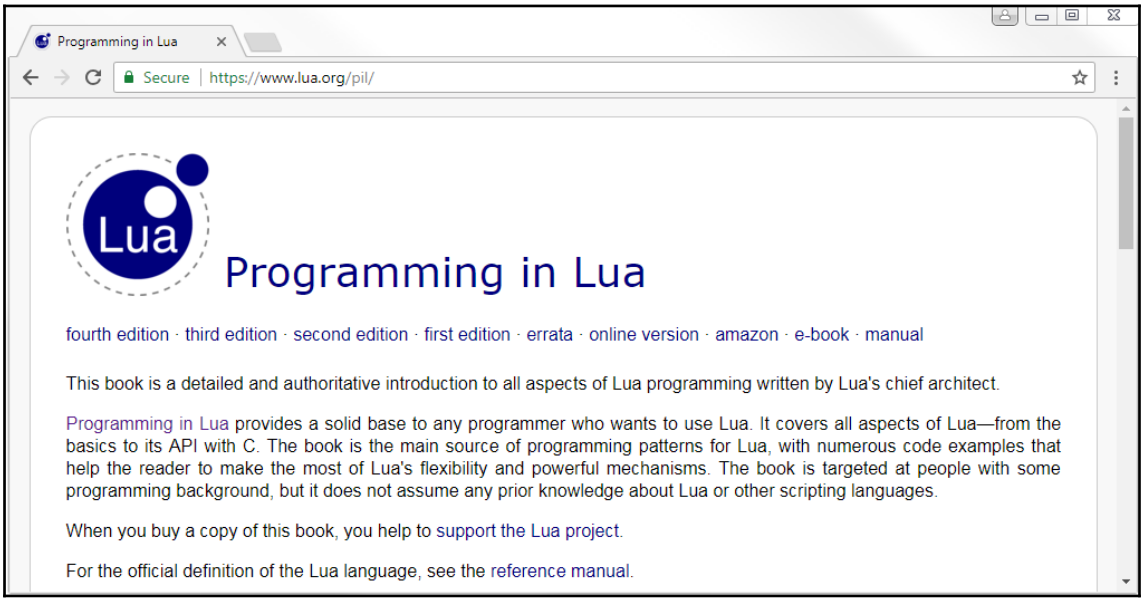
Chapter 11: A Troubleshooting Scenario

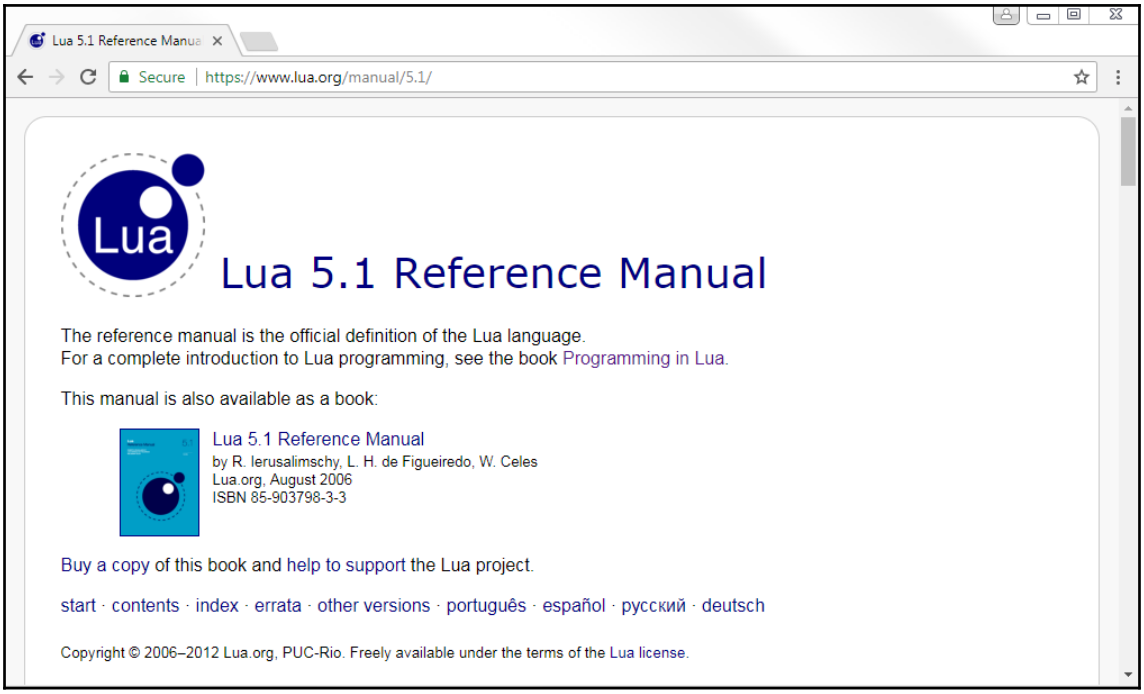


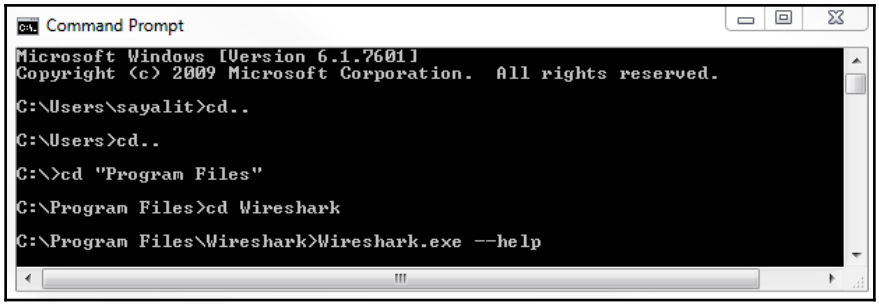

Wireshark Developer's G
Secure
https://www.wireshark.org/docs/wsdg_html_chunked/
Wireshark Developer's Guide
Next
Wireshark Developer's Guide
Table of Contents
Preface
1. Foreword
2. Who should read this document?
3. Acknowledgements
4. About this document
5. Where to get the latest copy of this document?
6. Providing feedback about this document
7. Typographic Conventions
7.1. Admonitions
7.2. Shell Prompt and Source Code Examples

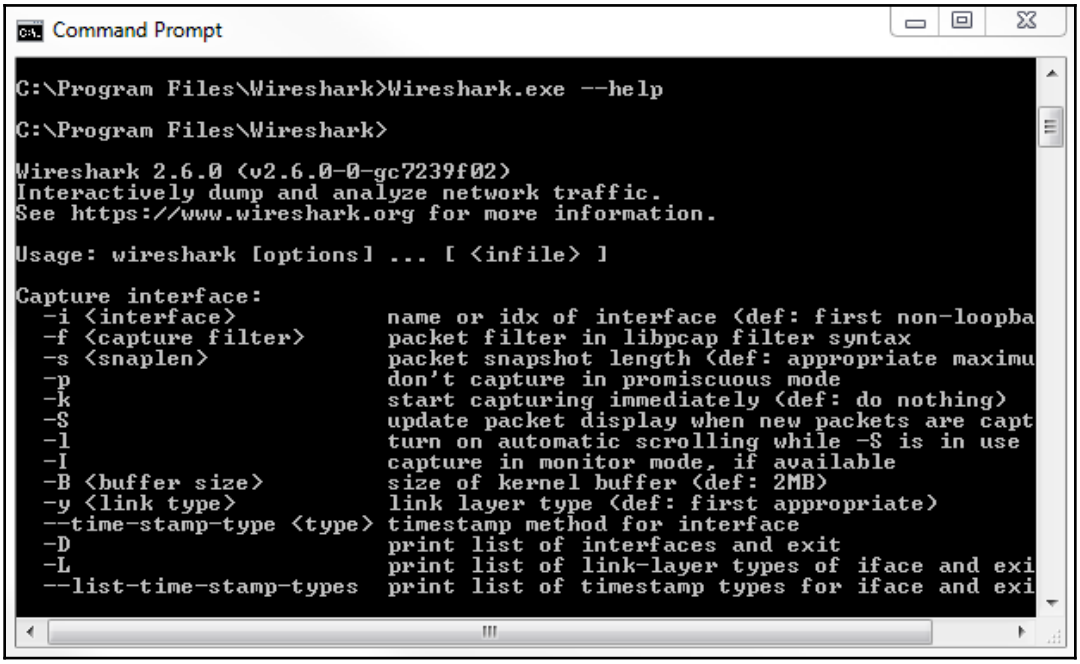

Chapter 9. Packet dissect
Secure | https://www.wireshark.org/docs/wsdg_html_chunked/ChapterDissection.html
Chapter 9. Packet dissection
Table of Contents
9.1. How it works
9.2. Adding a basic dissector
9.2.1. Setting up the dissector
9.2.2. Dissecting the details of the protocol
9.2.3. Improving the dissection information
9.3. How to handle transformed data
9.4. How to reassemble split packets
9.4.1. How to reassemble split UDP packets
9.4.2. How to reassemble split TCP Packets
9.5. How to tap protocols
9.6. How to produce protocol stats
9.7. How to use conversations
9.8. idl2wrs: Creating dissectors from CORBA IDL files
9.8.1. What is it?
9.8.2. Why do this?
9.8.3. How to use idl2wrs
9.8.4. TODO
9.8.5. Limitations
9.8.6. Notes

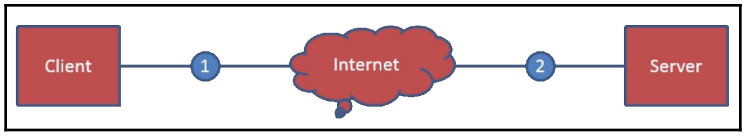

Wireshark Developer's G
Secure | https://www.wireshark.org/docs/wsdg_html_chunked/
11. Wireshark's Lua API Reference Manual
11.1. Saving capture files
11.1.1. Dumper
11.1.2. PseudoHeader
11.2. Obtaining dissection data
11.2.1. Field
11.2.2. FieldInfo
11.2.3. Global Functions
11.3. GUI support
11.3.1. ProgDlg
11.3.2. TextWindow
11.3.3. Global Functions
11.4. Post-dissection packet analysis
11.4.1. Listener

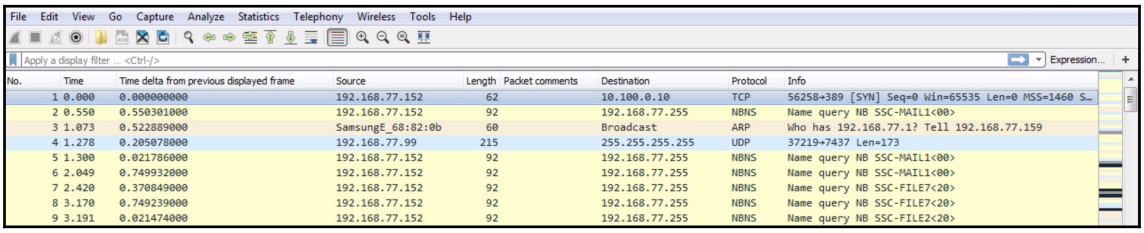

Programming in Lua
Secure | https://www.lua.org/pil/
Lua
Programming in Lua
fourth edition · third edition · second edition · first edition · errata · online version · amazon · e-book · manual
This book is a detailed and authoritative introduction to all aspects of Lua programming written by Lua's chief architect.
Programming in Lua provides a solid base to any programmer who wants to use Lua. It covers all aspects of Lua—from the basics to its API with C. The book is the main source of programming patterns for Lua, with numerous code examples that help the reader to make the most of Lua's flexibility and powerful mechanisms. The book is targeted at people with some programming background, but it does not assume any prior knowledge about Lua or other scripting languages.
When you buy a copy of this book, you help to support the Lua project.
For the official definition of the Lua language, see the reference manual.

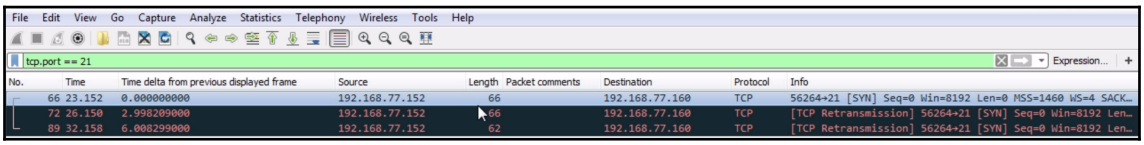

Lua 5.1 Reference Manual
Secure
https://www.lua.org/manual/5.1/
Lua
Lua 5.1 Reference Manual
The reference manual is the official definition of the Lua language.
For a complete introduction to Lua programming, see the book Programming in Lua.
This manual is also available as a book:
Lua 5.1 Reference Manual
by R. Ierusalimschy, L. H. de Figueiredo, W. Celes
Lua.org, August 2006
ISBN 85-903798-3-3
Buy a copy of this book and help to support the Lua project.
start · contents · index · errata · other versions · português · español · русский · deutsch
Copyright © 2006–2012 Lua.org, PUC-Rio. Freely available under the terms of the Lua license.

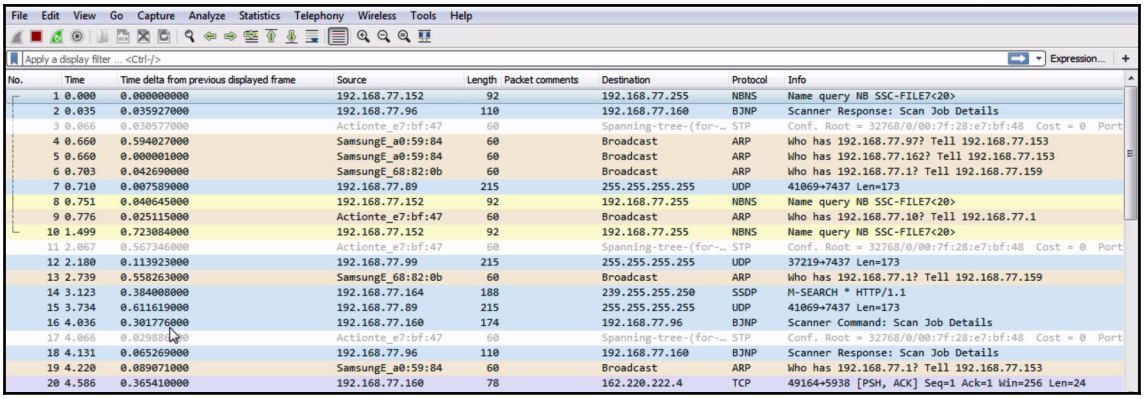

Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\sayalit>cd..
C:\Users>cd..
C:\>cd "Program Files"
C:\Program Files>cd Wireshark
C:\Program Files\Wireshark>Wireshark.exe --help

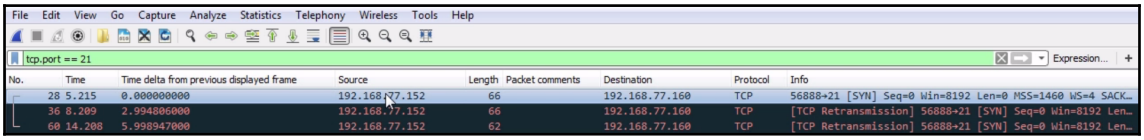

Command Prompt
C:\Program Files\Wireshark>Wireshark.exe --help
C:\Program Files\Wireshark>
Wireshark 2.6.0 (v2.6.0-0-gc7239f02)
Interactively dump and analyze network traffic.
See https://www.wireshark.org for more information.
Usage: wireshark [options] ... [<infile>]
Capture interface:
-i <interface> name or idx of interface (def: first non-loopba
-f <capture filter> packet filter in libpcap filter syntax
-s <snaplen> packet snapshot length (def: appropriate maximu
-p don't capture in promiscuous mode
-k start capturing immediately (def: do nothing)
-S update packet display when new packets are capt
-l turn on automatic scrolling while -S is in use
-I capture in monitor mode, if available
-B <buffer size> size of kernel buffer (def: 2MB)
-y <link type> link layer type (def: first appropriate)
--time-stamp-type <type> timestamp method for interface
-D print list of interfaces and exit
-L print list of link-layer types of iface and exi
--list-time-stamp-types print list of timestamp types for iface and exi

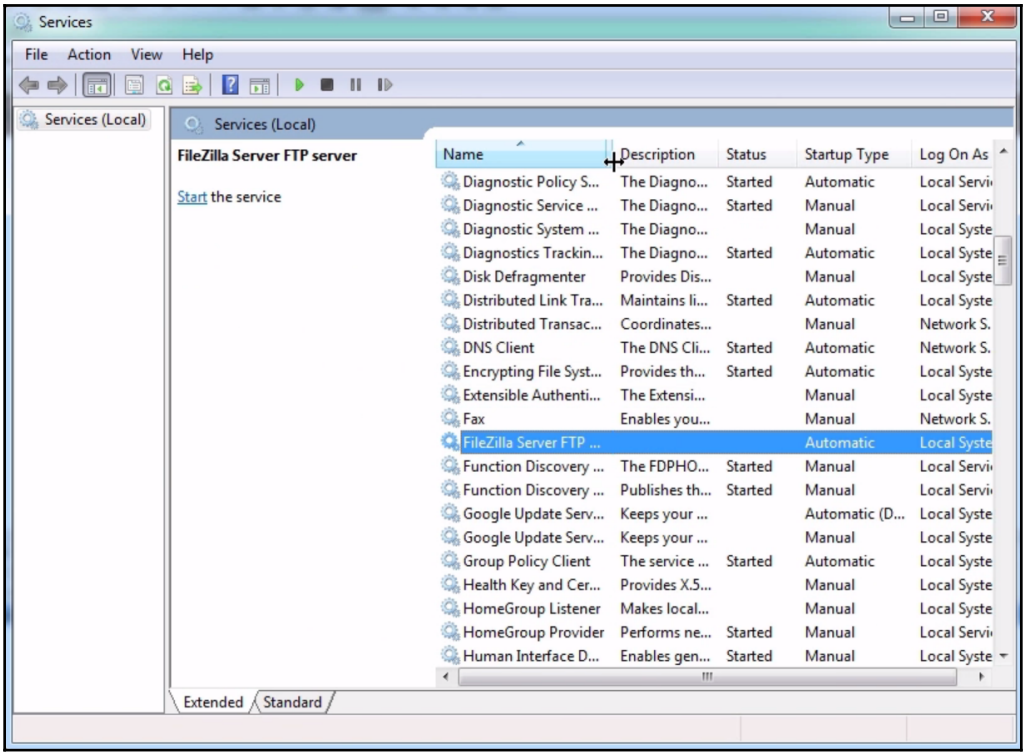

Client
1
Internet
2
Server

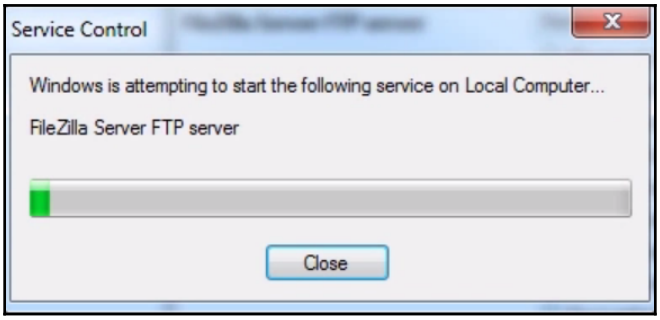

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
1 0.000 0.000000000 192.168.77.152 62 10.100.0.10 TCP 56258+389 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S…
2 0.550 0.550301000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-MAIL1<00>
3 1.073 0.522889000 SamsungE_68:82:0b 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.159
4 1.278 0.205078000 192.168.77.99 215 255.255.255.255 UDP 37219→7437 Len=173
5 1.300 0.021786000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-MAIL1<00>
6 2.049 0.749932000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-MAIL1<00>
7 2.420 0.370849000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE7<20>
8 3.170 0.749239000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE7<20>
9 3.191 0.021474000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE2<20>

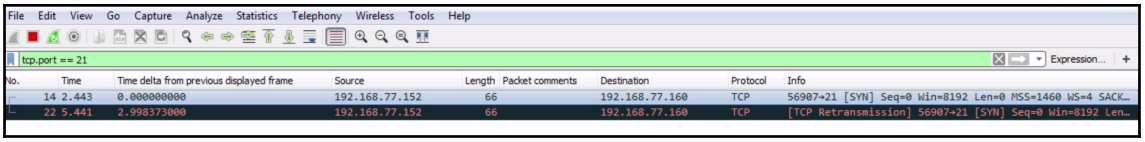

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
66 23.152 0.000000000 192.168.77.152 66 192.168.77.160 TCP 56264→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK…
72 26.150 2.998209000 192.168.77.152 66 192.168.77.160 TCP [TCP Retransmission] 56264→21 [SYN] Seq=0 Win=8192 Len…
89 32.158 6.008299000 192.168.77.152 62 192.168.77.160 TCP [TCP Retransmission] 56264→21 [SYN] Seq=0 Win=8192 Len…

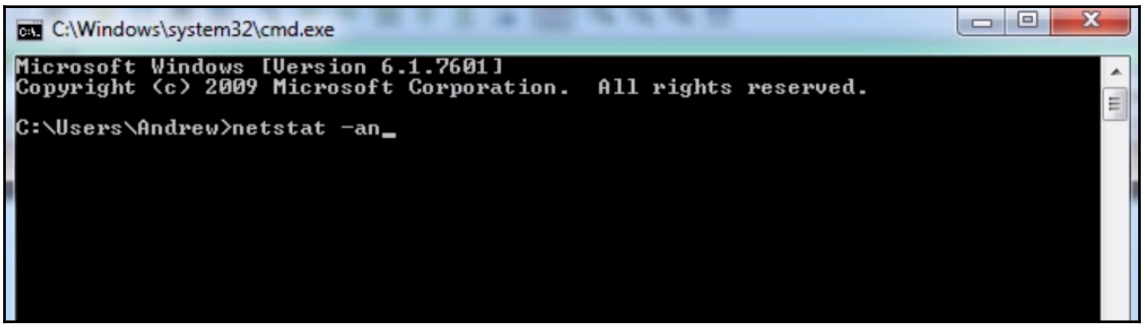

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
1 0.000 0.000000000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE7<20>
2 0.035 0.035927000 192.168.77.96 110 192.168.77.160 BJNP Scanner Response: Scan Job Details
3 0.066 0.030577000 Actionte_e7:bf:47 60 Spanning-tree-(for-... STP Conf. Root = 32768/0/00:7f:28:e7:bf:48 Cost = 0 Port
4 0.660 0.594027000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.97? Tell 192.168.77.153
5 0.660 0.000001000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.162? Tell 192.168.77.153
6 0.703 0.042690000 SamsungE_68:82:0b 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.159
7 0.710 0.007589000 192.168.77.89 215 255.255.255.255 UDP 41069→7437 Len=173
8 0.751 0.040645000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE7<20>
9 0.776 0.025115000 Actionte_e7:bf:47 60 Broadcast ARP Who has 192.168.77.10? Tell 192.168.77.1
10 1.499 0.723084000 192.168.77.152 92 192.168.77.255 NBNS Name query NB SSC-FILE7<20>
11 2.067 0.567346000 Actionte_e7:bf:47 60 Spanning-tree-(for-... STP Conf. Root = 32768/0/00:7f:28:e7:bf:48 Cost = 0 Port
12 2.180 0.113923000 192.168.77.99 215 255.255.255.255 UDP 37219→7437 Len=173
13 2.739 0.558263000 SamsungE_68:82:0b 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.159
14 3.123 0.384008000 192.168.77.164 188 239.255.255.250 SSDP M-SEARCH * HTTP/1.1
15 3.734 0.611619000 192.168.77.89 215 255.255.255.255 UDP 41069→7437 Len=173
16 4.036 0.301776000 192.168.77.160 174 192.168.77.96 BJNP Scanner Command: Scan Job Details
17 4.066 0.029884000 Actionte_e7:bf:47 60 Spanning-tree-(for-... STP Conf. Root = 32768/0/00:7f:28:e7:bf:48 Cost = 0 Port
18 4.131 0.065269000 192.168.77.96 110 192.168.77.160 BJNP Scanner Response: Scan Job Details
19 4.220 0.089071000 SamsungE_a0:59:84 60 Broadcast ARP Who has 192.168.77.1? Tell 192.168.77.153
20 4.586 0.365410000 192.168.77.160 78 162.220.222.4 TCP 49164→5938 [PSH, ACK] Seq=1 Ack=1 Win=256 Len=24

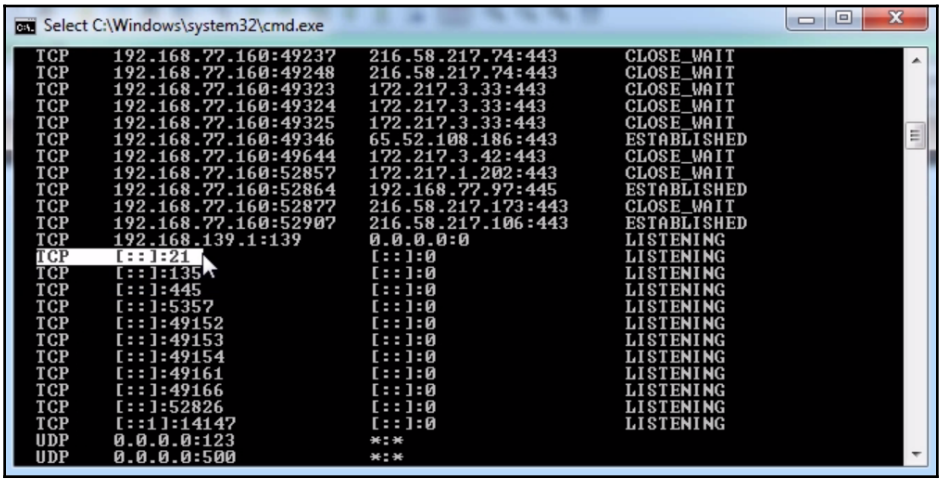

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
28 5.215 0.000000000 192.168.77.152 66 192.168.77.160 TCP 56888→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK...
36 8.209 2.994806000 192.168.77.152 66 192.168.77.160 TCP [TCP Retransmission] 56888→21 [SYN] Seq=0 Win=8192 Len...
60 14.208 5.998947000 192.168.77.152 62 192.168.77.160 TCP [TCP Retransmission] 56888→21 [SYN] Seq=0 Win=8192 Len...

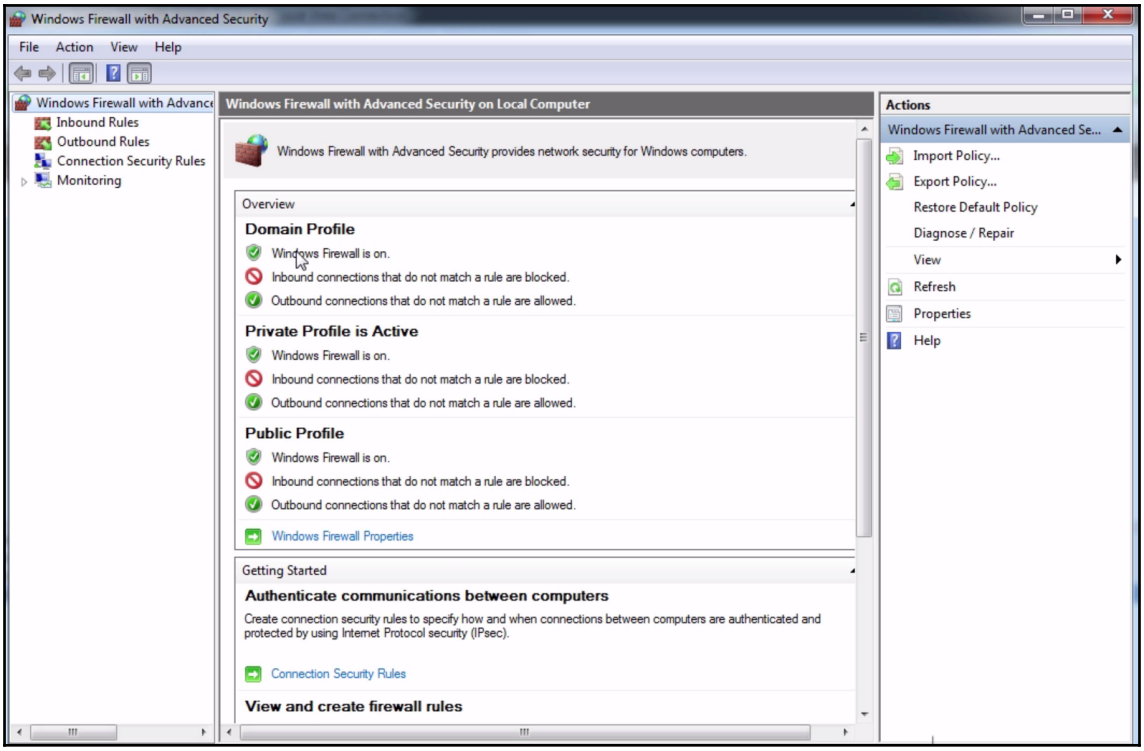

Services
File Action View Help
Services (Local)
Services (Local)
FileZilla Server FTP server
Start the service
Name Description Status Startup Type Log On As
Diagnostic Policy S... The Diagno... Started Automatic Local Servi
Diagnostic Service ... The Diagno... Started Manual Local Servi
Diagnostic System ... The Diagno... Manual Local Syste
Diagnostics Trackin... The Diagno... Started Automatic Local Syste
Disk Defragmenter Provides Dis... Manual Local Syste
Distributed Link Tra... Maintains li... Started Automatic Local Syste
Distributed Transac... Coordinates... Manual Network S.
DNS Client The DNS Cli... Started Automatic Network S.
Encrypting File Syst... Provides th... Started Automatic Local Syste
Extensible Authenti... The Extensi... Manual Local Syste
Fax Enables you... Manual Network S.
FileZilla Server FTP ... Automatic Local Syste
Function Discovery ... The FDPHO... Started Manual Local Servi
Function Discovery ... Publishes th... Started Manual Local Servi
Google Update Serv... Keeps your ... Automatic (D... Local Syste
Google Update Serv... Keeps your ... Manual Local Syste
Group Policy Client The service ... Started Automatic Local Syste
Health Key and Cer... Provides X.5... Manual Local Syste
HomeGroup Listener Makes local... Manual Local Syste
HomeGroup Provider Performs ne... Started Manual Local Servi
Human Interface D... Enables gen... Started Manual Local Syste
Extended Standard

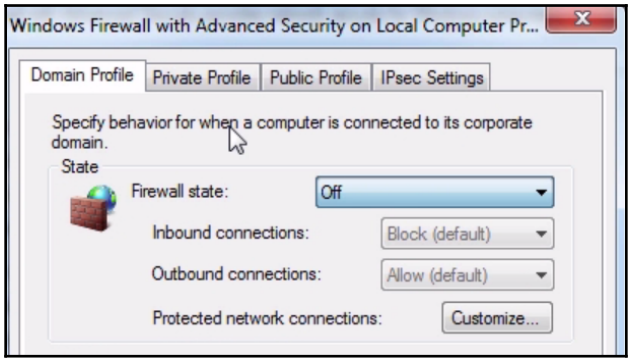

Service Control
Windows is attempting to start the following service on Local Computer...
FileZilla Server FTP server
Close

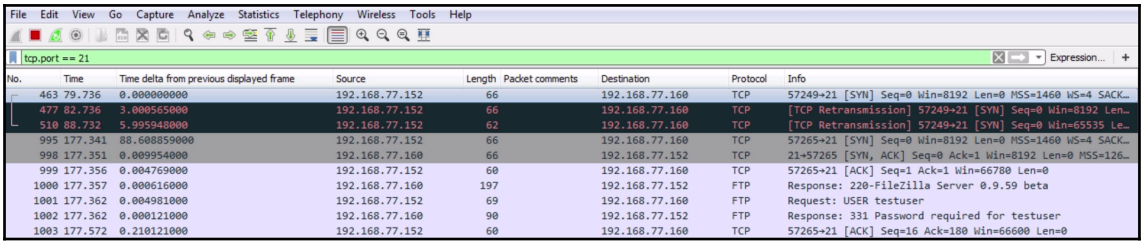

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
14 2.443 0.000000000 192.168.77.152 66 192.168.77.160 TCP 56907→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK…
22 5.441 2.998373000 192.168.77.152 66 192.168.77.160 TCP [TCP Retransmission] 56907→21 [SYN] Seq=0 Win=8192 Len…

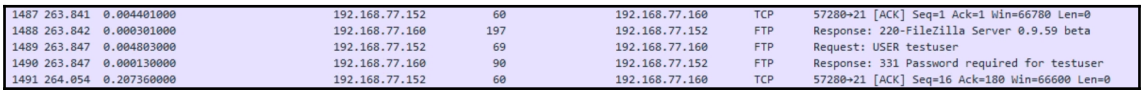

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Andrew>netstat -an

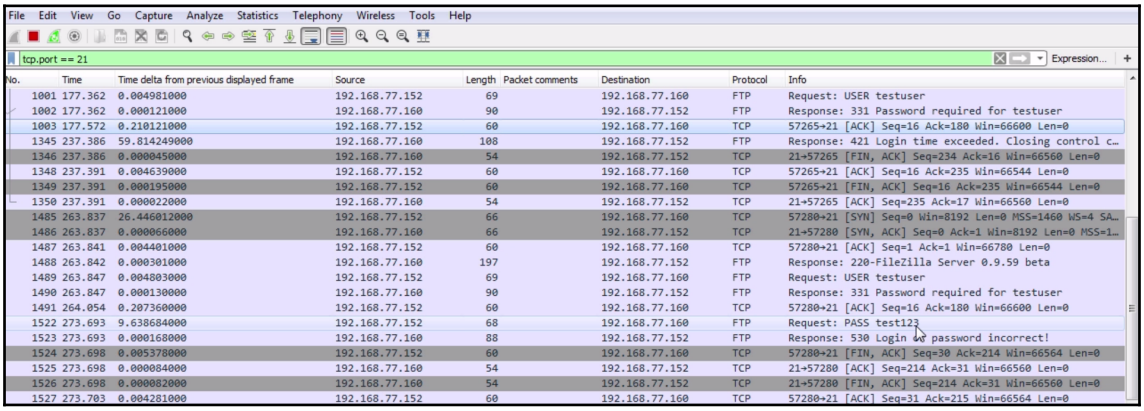

Select C:\Windows\system32\cmd.exe
TCP 192.168.77.160:49237 216.58.217.74:443 CLOSE_WAIT
TCP 192.168.77.160:49248 216.58.217.74:443 CLOSE_WAIT
TCP 192.168.77.160:49323 172.217.3.33:443 CLOSE_WAIT
TCP 192.168.77.160:49324 172.217.3.33:443 CLOSE_WAIT
TCP 192.168.77.160:49325 172.217.3.33:443 CLOSE_WAIT
TCP 192.168.77.160:49346 65.52.108.186:443 ESTABLISHED
TCP 192.168.77.160:49644 172.217.3.42:443 CLOSE_WAIT
TCP 192.168.77.160:52857 172.217.1.202:443 CLOSE_WAIT
TCP 192.168.77.160:52864 192.168.77.97:445 ESTABLISHED
TCP 192.168.77.160:52877 216.58.217.173:443 CLOSE_WAIT
TCP 192.168.77.160:52907 216.58.217.106:443 ESTABLISHED
TCP 192.168.139.1:139 0.0.0.0:0 LISTENING
TCP [::]:21 [::]:0 LISTENING
TCP [::]:135 [::]:0 LISTENING
TCP [::]:445 [::]:0 LISTENING
TCP [::]:5357 [::]:0 LISTENING
TCP [::]:49152 [::]:0 LISTENING
TCP [::]:49153 [::]:0 LISTENING
TCP [::]:49154 [::]:0 LISTENING
TCP [::]:49161 [::]:0 LISTENING
TCP [::]:49166 [::]:0 LISTENING
TCP [::]:52826 [::]:0 LISTENING
TCP [::1]:14147 [::]:0 LISTENING
UDP 0.0.0.0:123 *:*
UDP 0.0.0.0:500 *:*

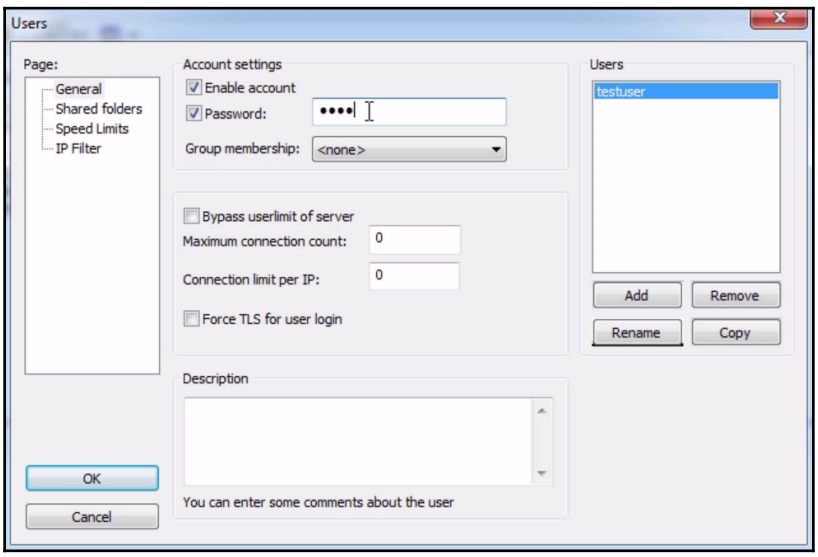

Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advanc
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Firewall with Advanced Security on Local Computer
Windows Firewall with Advanced Security provides network security for Windows computers.
Overview
Domain Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Private Profile is Active
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Public Profile
Windows Firewall is on.
Inbound connections that do not match a rule are blocked.
Outbound connections that do not match a rule are allowed.
Windows Firewall Properties
Getting Started
Authenticate communications between computers
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Connection Security Rules
View and create firewall rules
Actions
Windows Firewall with Advanced Se...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help


Windows Firewall with Advanced Security on Local Computer Pr...
Domain Profile
Private Profile
Public Profile
IPsec Settings
Specify behavior for when a computer is connected to its corporate domain.
State
Firewall state:
Off
Inbound connections:
Block (default)
Outbound connections:
Allow (default)
Protected network connections:
Customize...


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
463 79.736 0.000000000 192.168.77.152 66 192.168.77.160 TCP 57249→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK…
477 82.736 3.000565000 192.168.77.152 66 192.168.77.160 TCP [TCP Retransmission] 57249→21 [SYN] Seq=0 Win=8192 Len…
510 88.732 5.995948000 192.168.77.152 62 192.168.77.160 TCP [TCP Retransmission] 57249→21 [SYN] Seq=0 Win=65535 Le…
995 177.341 88.608859000 192.168.77.152 66 192.168.77.160 TCP 57265→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK…
998 177.351 0.009954000 192.168.77.160 66 192.168.77.152 TCP 21→57265 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=126…
999 177.356 0.004769000 192.168.77.152 60 192.168.77.160 TCP 57265→21 [ACK] Seq=1 Ack=1 Win=66780 Len=0
1000 177.357 0.000616000 192.168.77.160 197 192.168.77.152 FTP Response: 220-FileZilla Server 0.9.59 beta
1001 177.362 0.004981000 192.168.77.152 69 192.168.77.160 FTP Request: USER testuser
1002 177.362 0.000121000 192.168.77.160 90 192.168.77.152 FTP Response: 331 Password required for testuser
1003 177.572 0.210121000 192.168.77.152 60 192.168.77.160 TCP 57265→21 [ACK] Seq=16 Ack=180 Win=66600 Len=0


1487 263.841 0.004401000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [ACK] Seq=1 Ack=1 Win=66780 Len=0
1488 263.842 0.000301000 192.168.77.160 197 192.168.77.152 FTP Response: 220-FileZilla Server 0.9.59 beta
1489 263.847 0.004803000 192.168.77.152 69 192.168.77.160 FTP Request: USER testuser
1490 263.847 0.000130000 192.168.77.160 90 192.168.77.152 FTP Response: 331 Password required for testuser
1491 264.054 0.207360000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [ACK] Seq=16 Ack=180 Win=66600 Len=0


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 21
Expression...
No. Time Time delta from previous displayed frame Source Length Packet comments Destination Protocol Info
1001 177.362 0.004981000 192.168.77.152 69 192.168.77.160 FTP Request: USER testuser
1002 177.362 0.000121000 192.168.77.160 90 192.168.77.152 FTP Response: 331 Password required for testuser
1003 177.572 0.210121000 192.168.77.152 60 192.168.77.160 TCP 57265→21 [ACK] Seq=16 Ack=180 Win=66600 Len=0
1345 237.386 59.814249000 192.168.77.160 108 192.168.77.152 FTP Response: 421 Login time exceeded. Closing control c…
1346 237.386 0.000045000 192.168.77.160 54 192.168.77.152 TCP 21→57265 [FIN, ACK] Seq=234 Ack=16 Win=66560 Len=0
1348 237.391 0.004639000 192.168.77.152 60 192.168.77.160 TCP 57265→21 [ACK] Seq=16 Ack=235 Win=66544 Len=0
1349 237.391 0.000195000 192.168.77.152 60 192.168.77.160 TCP 57265→21 [FIN, ACK] Seq=16 Ack=235 Win=66544 Len=0
1350 237.391 0.000022000 192.168.77.160 54 192.168.77.152 TCP 21→57265 [ACK] Seq=235 Ack=17 Win=66560 Len=0
1485 263.837 26.446012000 192.168.77.152 66 192.168.77.160 TCP 57280→21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SA…
1486 263.837 0.000066000 192.168.77.160 66 192.168.77.152 TCP 21→57280 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1…
1487 263.841 0.004401000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [ACK] Seq=1 Ack=1 Win=66780 Len=0
1488 263.842 0.000301000 192.168.77.160 197 192.168.77.152 FTP Response: 220-FileZilla Server 0.9.59 beta
1489 263.847 0.004803000 192.168.77.152 69 192.168.77.160 FTP Request: USER testuser
1490 263.847 0.000130000 192.168.77.160 90 192.168.77.152 FTP Response: 331 Password required for testuser
1491 264.054 0.207360000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [ACK] Seq=16 Ack=180 Win=66600 Len=0
1522 273.693 9.638684000 192.168.77.152 68 192.168.77.160 FTP Request: PASS test123
1523 273.693 0.000168000 192.168.77.160 88 192.168.77.152 FTP Response: 530 Login or password incorrect!
1524 273.698 0.005378000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [FIN, ACK] Seq=30 Ack=214 Win=66564 Len=0
1525 273.698 0.000084000 192.168.77.160 54 192.168.77.152 TCP 21→57280 [ACK] Seq=214 Ack=31 Win=66560 Len=0
1526 273.698 0.000082000 192.168.77.160 54 192.168.77.152 TCP 21→57280 [FIN, ACK] Seq=214 Ack=31 Win=66560 Len=0
1527 273.703 0.004281000 192.168.77.152 60 192.168.77.160 TCP 57280→21 [ACK] Seq=31 Ack=215 Win=66564 Len=0


Users
Page:
General
Shared folders
Speed Limits
IP Filter
Account settings
Enable account
Password:
Group membership:
<none>
Bypass userlimit of server
Maximum connection count:
0
Connection limit per IP:
0
Force TLS for user login
Users
testuser
Add
Remove
Rename
Copy
Description
You can enter some comments about the user
OK
Cancel

1900	349.592	0.004447000	192.168.77.152	60	192.168.77.160	TCP	57297→21 [ACK] Seq=1 Ack=1 Win=66780 Len=0
1901	349.592	0.000323000	192.168.77.160	197	192.168.77.152	FTP	Response: 220-FileZilla Server 0.9.59 beta
1902	349.597	0.005048000	192.168.77.152	69	192.168.77.160	FTP	Request: USER testuser
1903	349.597	0.000157000	192.168.77.160	90	192.168.77.152	FTP	Response: 331 Password required for testuser
1904	349.602	0.004690000	192.168.77.152	68	192.168.77.160	FTP	Request: PASS test123
1905	349.602	0.000181000	192.168.77.160	69	192.168.77.152	FTP	Response: 230 Logged on
1906	349.607	0.004726000	192.168.77.152	60	192.168.77.160	FTP	Request: SYST
1907	349.607	0.000122000	192.168.77.160	86	192.168.77.152	FTP	Response: 215 UNIX emulated by FileZilla
1908	349.612	0.004662000	192.168.77.152	60	192.168.77.160	FTP	Request: FEAT
1909	349.612	0.000085000	192.168.77.160	176	192.168.77.152	FTP	Response: 211-Features:
1910	349.617	0.005108000	192.168.77.152	81	192.168.77.160	FTP	Request: CLNT WinSCP-release-5.9.3
1911	349.617	0.000094000	192.168.77.160	70	192.168.77.152	FTP	Response: 200 Don't care
1912	349.622	0.005037000	192.168.77.152	68	192.168.77.160	FTP	Request: OPTS UTF8 ON
1913	349.622	0.000122000	192.168.77.160	118	192.168.77.152	FTP	Response: 202 UTF8 mode is always enabled. No need t…
1914	349.704	0.081625000	192.168.77.152	60	192.168.77.160	FTP	Request: PWD

2182	412.503	2.462598000	192.168.77.152	60	192.168.77.160	TCP	57297→21 [FIN, ACK] Seq=121 Ack=669 Win=66112 Len=0
2183	412.503	0.000034000	192.168.77.160	54	192.168.77.152	TCP	21→57297 [ACK] Seq=669 Ack=122 Win=66560 Len=0
2184	412.503	0.000079000	192.168.77.160	54	192.168.77.152	TCP	21→57297 [FIN, ACK] Seq=669 Ack=122 Win=66560 Len=0
2185	412.508	0.004683000	192.168.77.152	60	192.168.77.160	TCP	57297→21 [ACK] Seq=122 Ack=670 Win=66112 Len=0