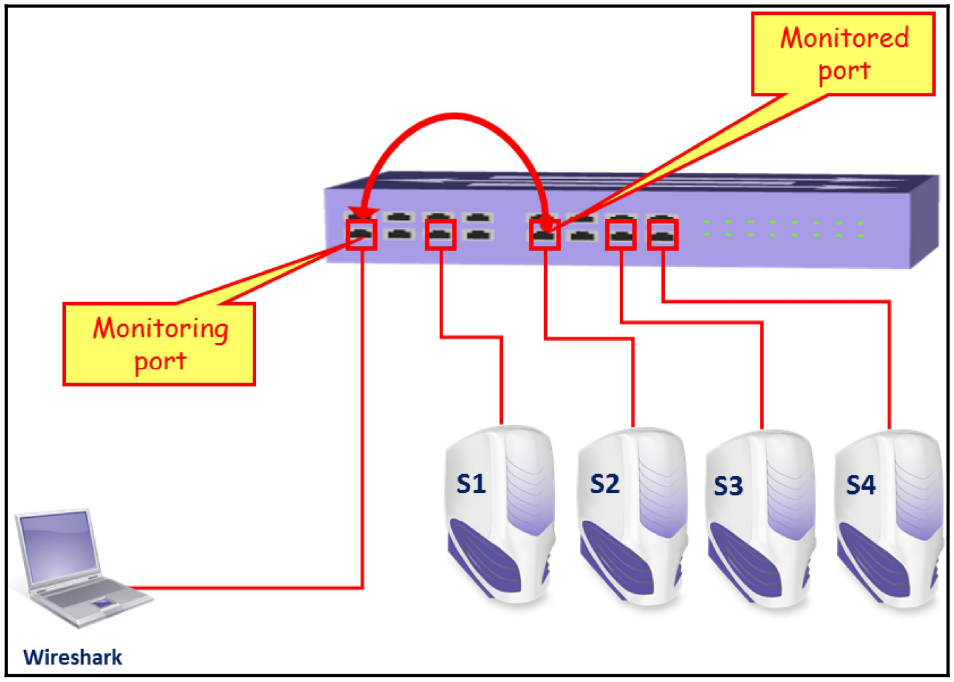
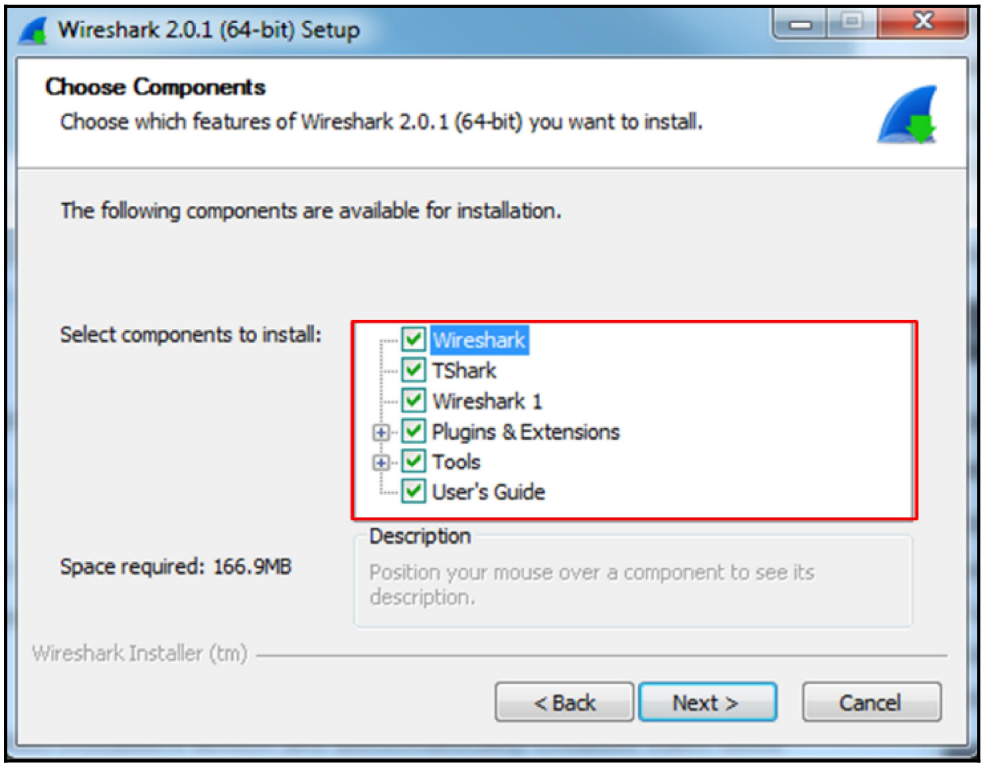
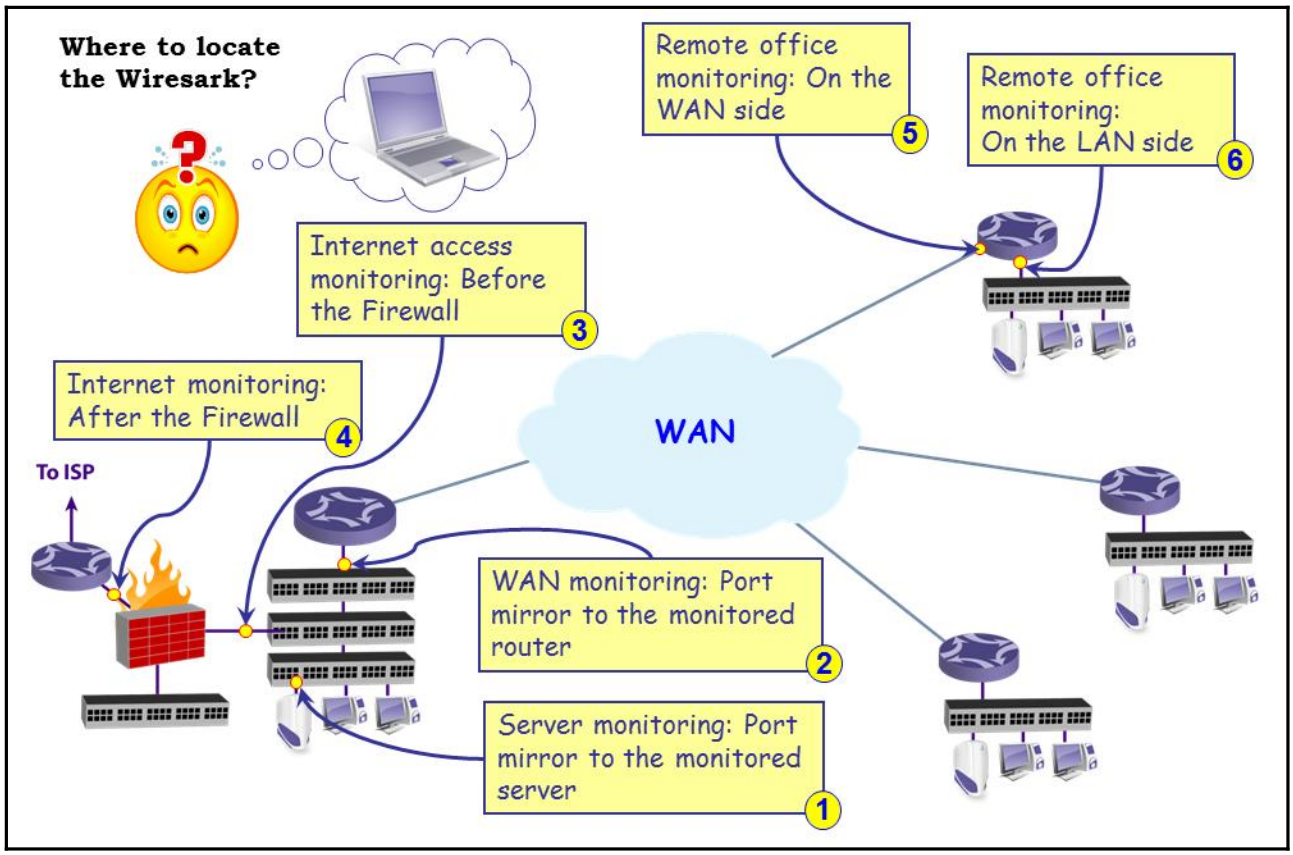
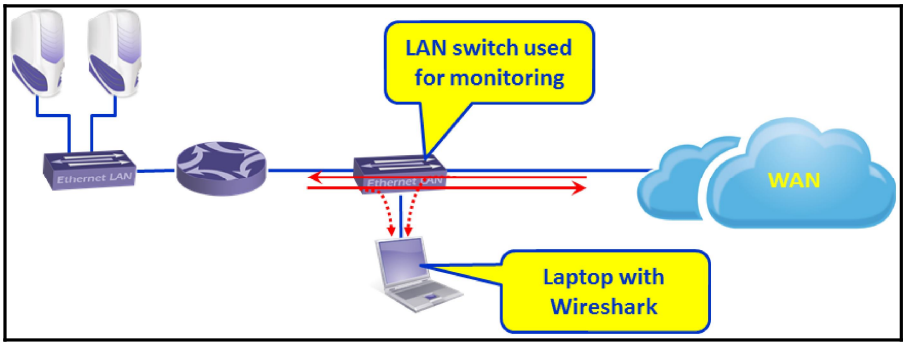
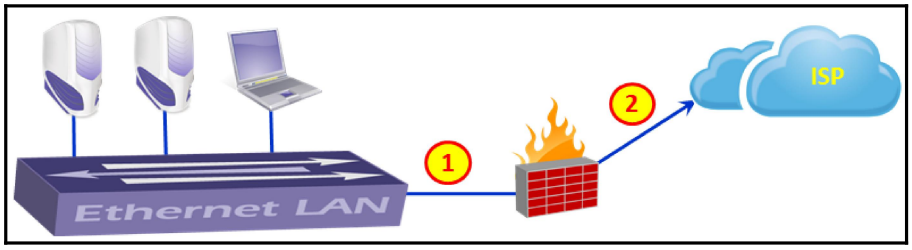
Chapter 1: Introduction to Wireshark Version 2

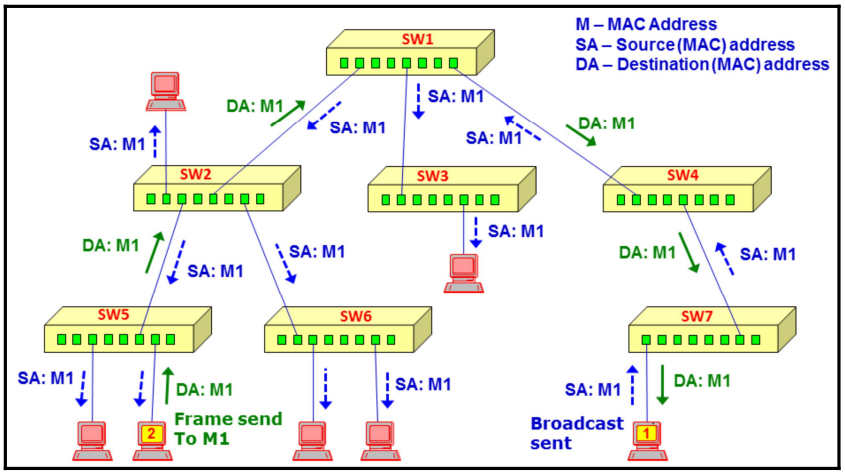


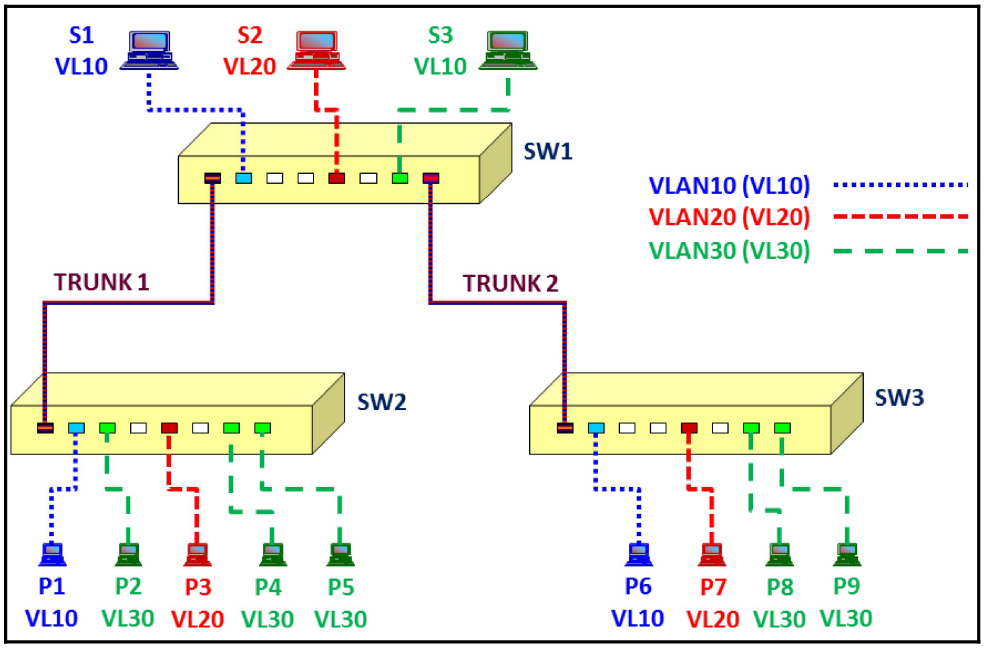

Wireshark 2.0.1 (64-bit) Setup
Choose Components
Choose which features of Wireshark 2.0.1 (64-bit) you want to install.
The following components are available for installation.
Select components to install:
Wireshark
TShark
Wireshark 1
Plugins & Extensions
Tools
User's Guide
Description
Position your mouse over a component to see its description.
Space required: 166.9MB
Wireshark Installer (tm)
< Back
Next >
Cancel

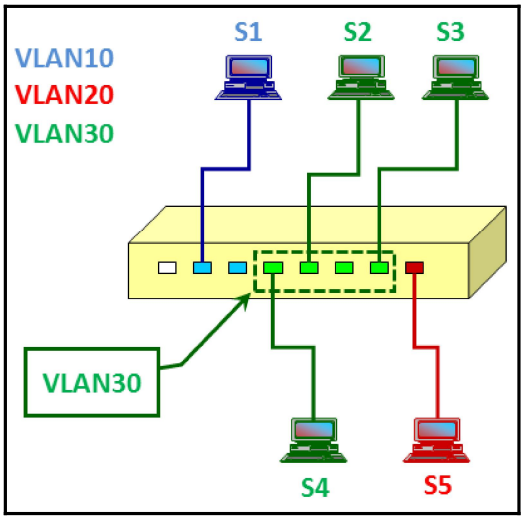

Where to locate the Wiresark?
Remote office monitoring: On the WAN side
5
Remote office monitoring: On the LAN side
6
Internet access monitoring: Before the Firewall
3
Internet monitoring: After the Firewall
4
To ISP
WAN
WAN monitoring: Port mirror to the monitored router
2
Server monitoring: Port mirror to the monitored server
1

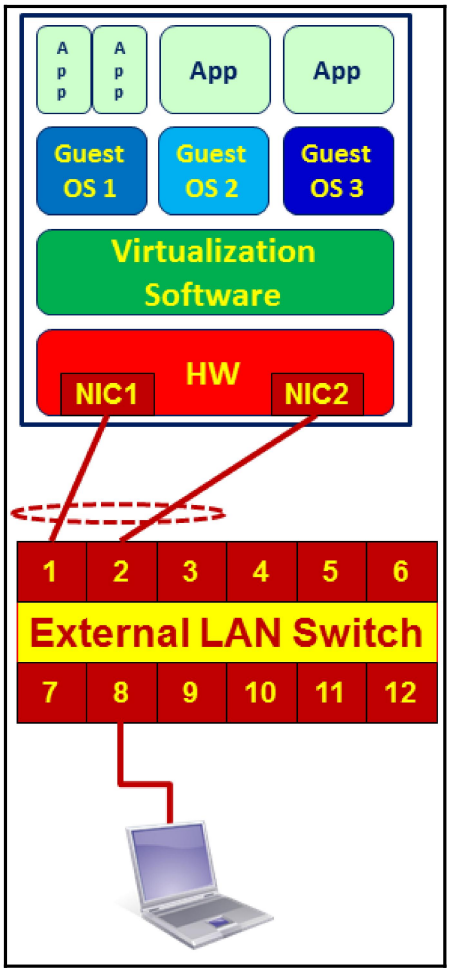

LAN switch used for monitoring
Ethernet LAN
WAN
Laptop with Wireshark

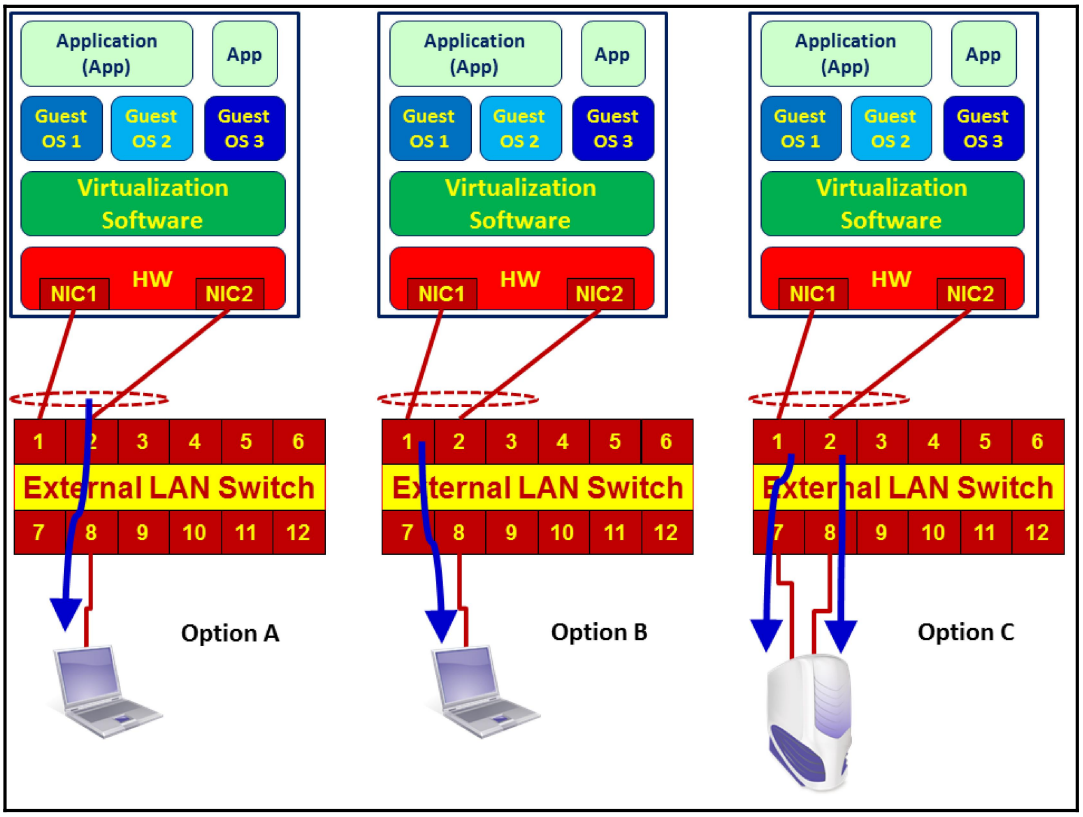

ISP
2
1
Ethernet LAN

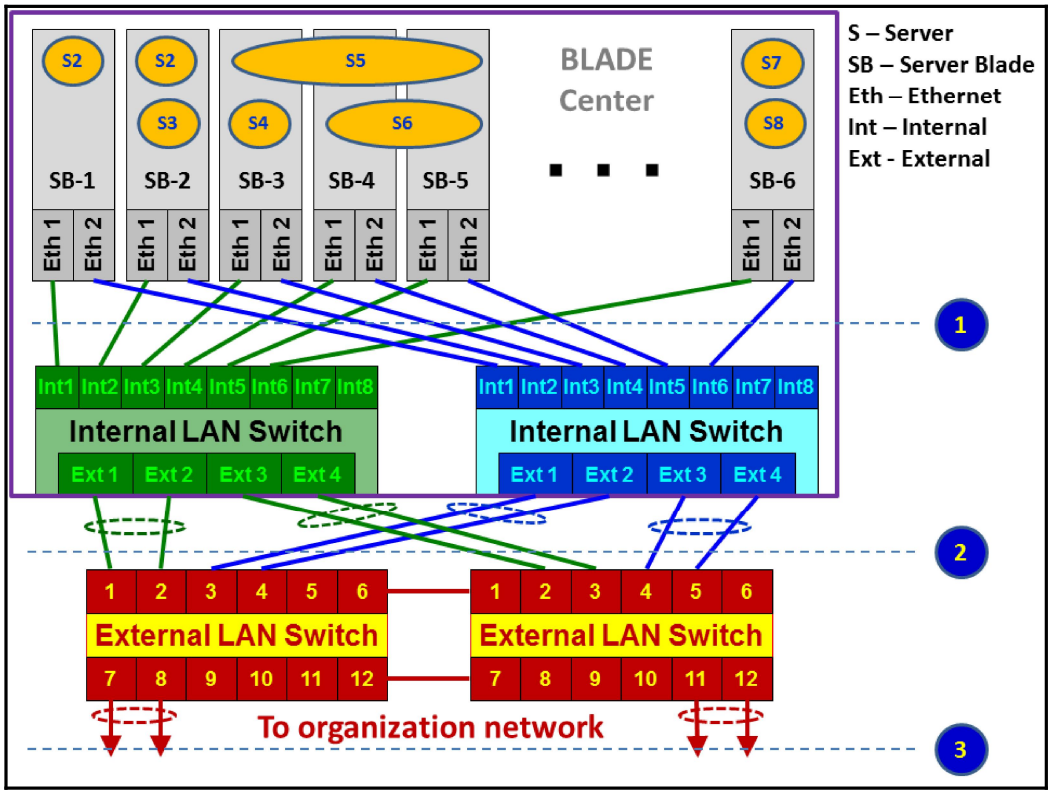

M – MAC Address
SA – Source (MAC) address
DA – Destination (MAC) address
SW1
SW2
SW3
SW4
SW5
SW6
SW7
DA: M1
SA: M1
Frame send
To M1
Broadcast
sent
1
2

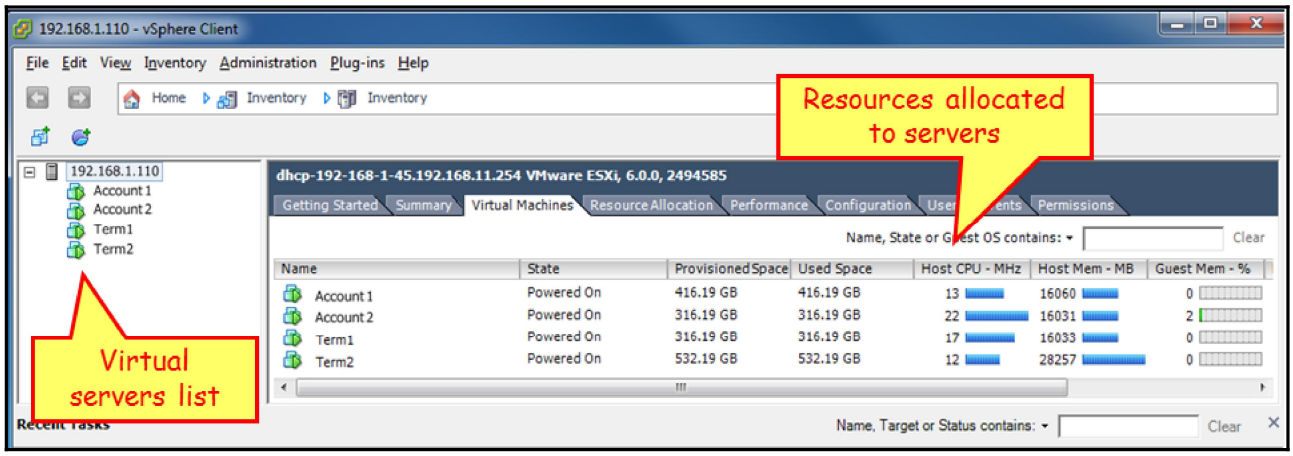

S1
VL10
S2
VL20
S3
VL10
SW1
VLAN10 (VL10)
VLAN20 (VL20)
VLAN30 (VL30)
TRUNK 1
TRUNK 2
SW2
SW3
P1
VL10
P2
VL30
P3
VL20
P4
VL30
P5
VL30
P6
VL10
P7
VL20
P8
VL30
P9
VL30

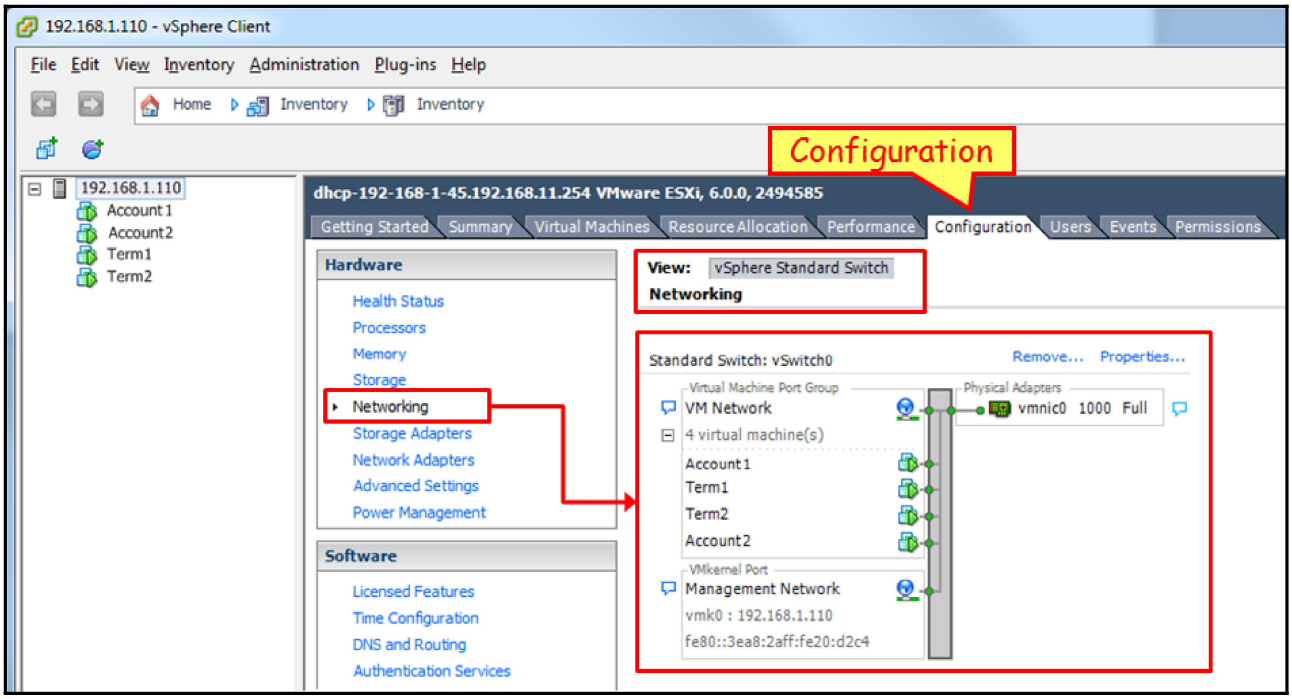

VLAN10
VLAN20
VLAN30
S1
S2
S3
VLAN30
S4
S5

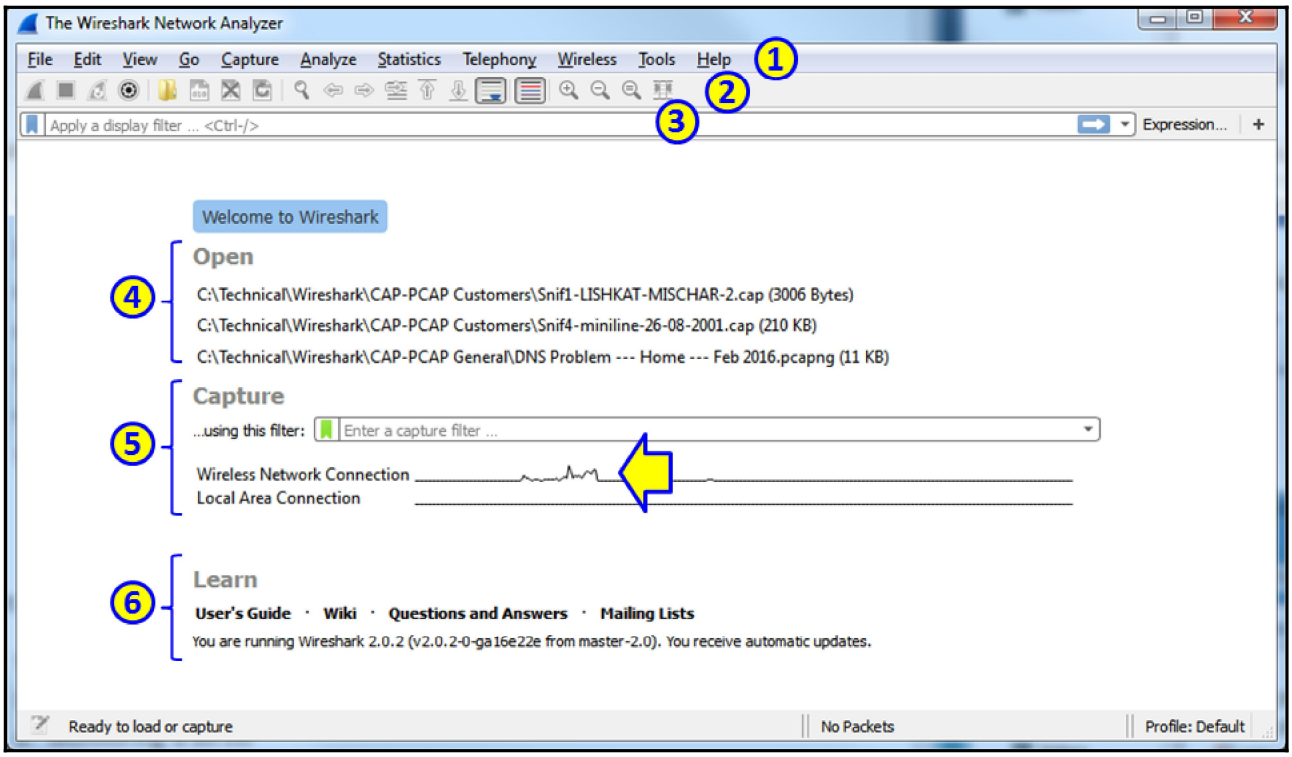

App
App
App
App
Guest OS 1
Guest OS 2
Guest OS 3
Virtualization Software
HW
NIC1
NIC2
1
2
3
4
5
6
External LAN Switch
7
8
9
10
11
12

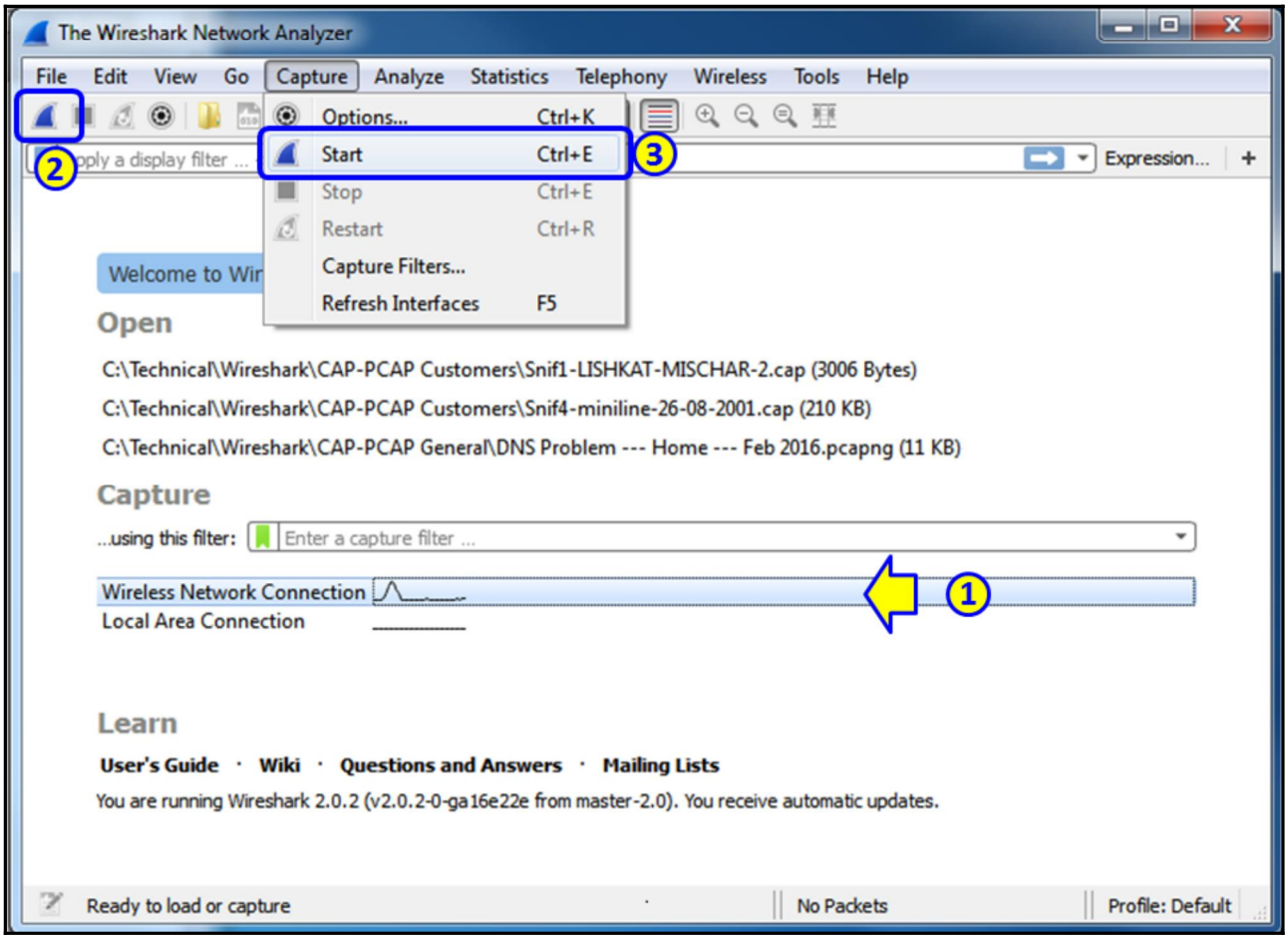

Application (App)
App
Guest OS 1
Guest OS 2
Guest OS 3
Virtualization Software
HW
NIC1
NIC2
1 2 3 4 5 6
External LAN Switch
7 8 9 10 11 12
Option A
Option B
Option C

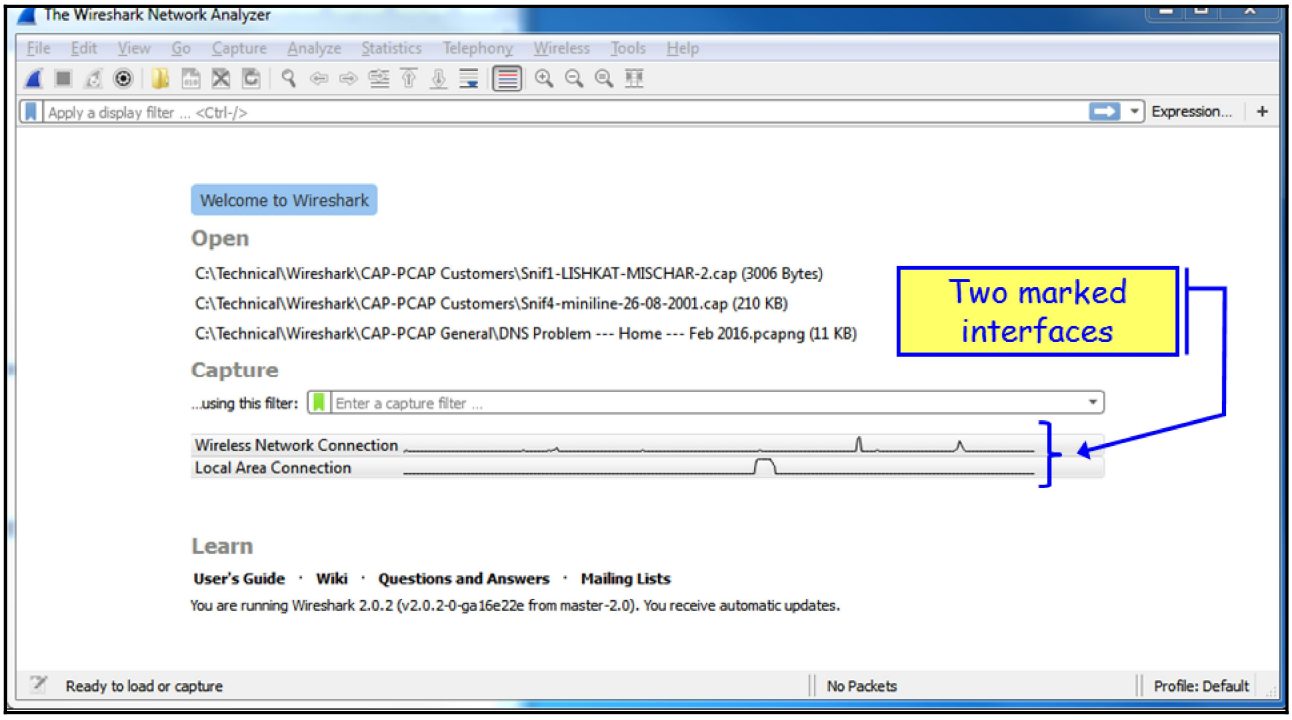

S – Server
SB – Server Blade
Eth – Ethernet
Int – Internal
Ext - External
BLADE Center
S2
S3
S5
S4
S6
S7
S8
SB-1
SB-2
SB-3
SB-4
SB-5
SB-6
Eth 1
Eth 2
1
Int1 Int2 Int3 Int4 Int5 Int6 Int7 Int8
Internal LAN Switch
Ext 1 Ext 2 Ext 3 Ext 4
2
1 2 3 4 5 6
7 8 9 10 11 12
External LAN Switch
To organization network
3

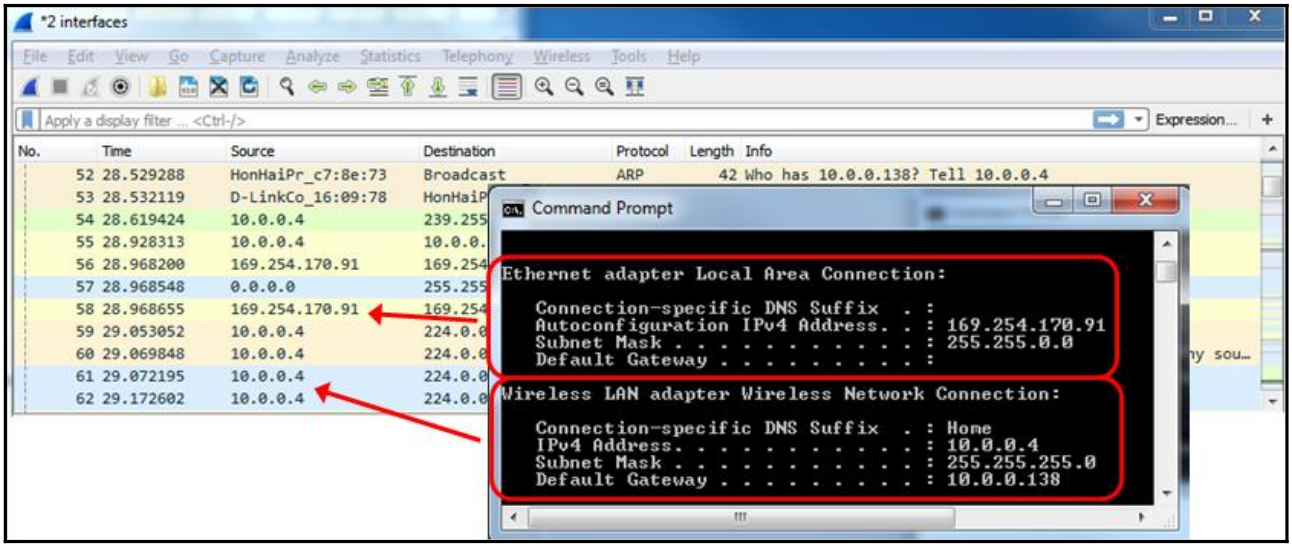

192.168.1.110 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
Resources allocated to servers
192.168.1.110
Account 1
Account 2
Term1
Term2
dhcp-192-168-1-45.192.168.11.254 VMware ESXi, 6.0.0, 2494585
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Permissions
Name State Provisioned Space Used Space Host CPU - MHz Host Mem - MB Guest Mem - %
Account 1 Powered On 416.19 GB 416.19 GB 13 16060 0
Account 2 Powered On 316.19 GB 316.19 GB 22 16031 2
Term1 Powered On 316.19 GB 316.19 GB 17 16033 0
Term2 Powered On 532.19 GB 532.19 GB 12 28257 0
Virtual servers list
Recent Tasks
Clear

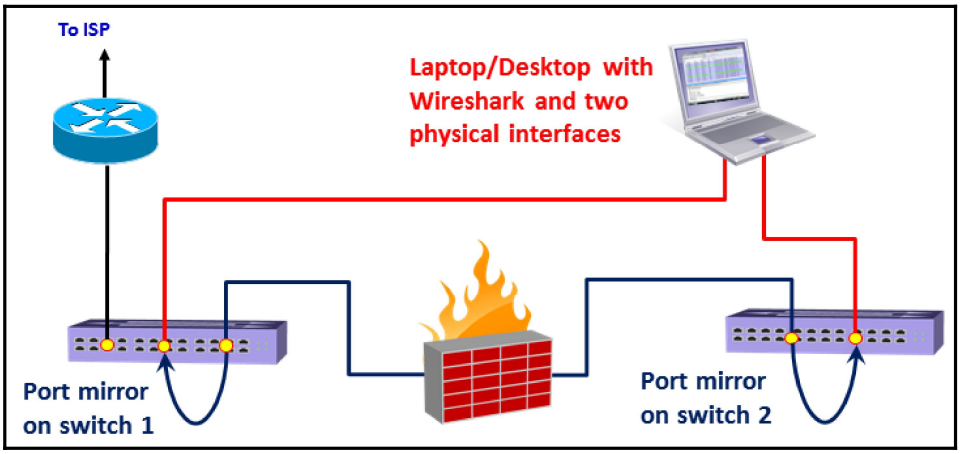

192.168.1.110 - vSphere Client
File Edit View Inventory Administration Plug-ins Help
Home Inventory Inventory
Configuration
192.168.1.110
Account1
Account2
Term1
Term2
dhcp-192-168-1-45.192.168.11.254 VMware ESXi, 6.0.0, 2494585
Getting Started Summary Virtual Machines Resource Allocation Performance Configuration Users Events Permissions
Hardware
Health Status
Processors
Memory
Storage
Networking
Storage Adapters
Network Adapters
Advanced Settings
Power Management
Software
Licensed Features
Time Configuration
DNS and Routing
Authentication Services
View: vSphere Standard Switch
Networking
Standard Switch: vSwitch0
Remove... Properties...
Virtual Machine Port Group
VM Network
4 virtual machine(s)
Account1
Term1
Term2
Account2
VMkernel Port
Management Network
vmk0 : 192.168.1.110
fe80::3ea8:2aff:fe20:d2c4
Physical Adapters
vmnic0 1000 Full

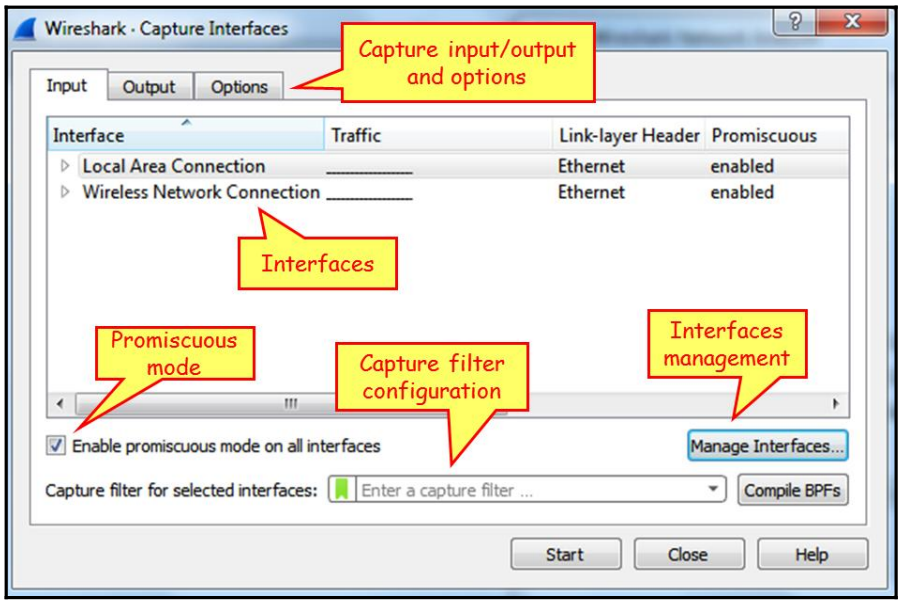

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
1
2
3
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
4
Open
C:\Technical\Wireshark\CAP-PCAP Customers\Snif1-LISHKAT-MISCHAR-2.cap (3006 Bytes)
C:\Technical\Wireshark\CAP-PCAP Customers\Snif4-miniline-26-08-2001.cap (210 KB)
C:\Technical\Wireshark\CAP-PCAP General\DNS Problem --- Home --- Feb 2016.pcapng (11 KB)
5
Capture
...using this filter: Enter a capture filter ...
Wireless Network Connection
Local Area Connection
6
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

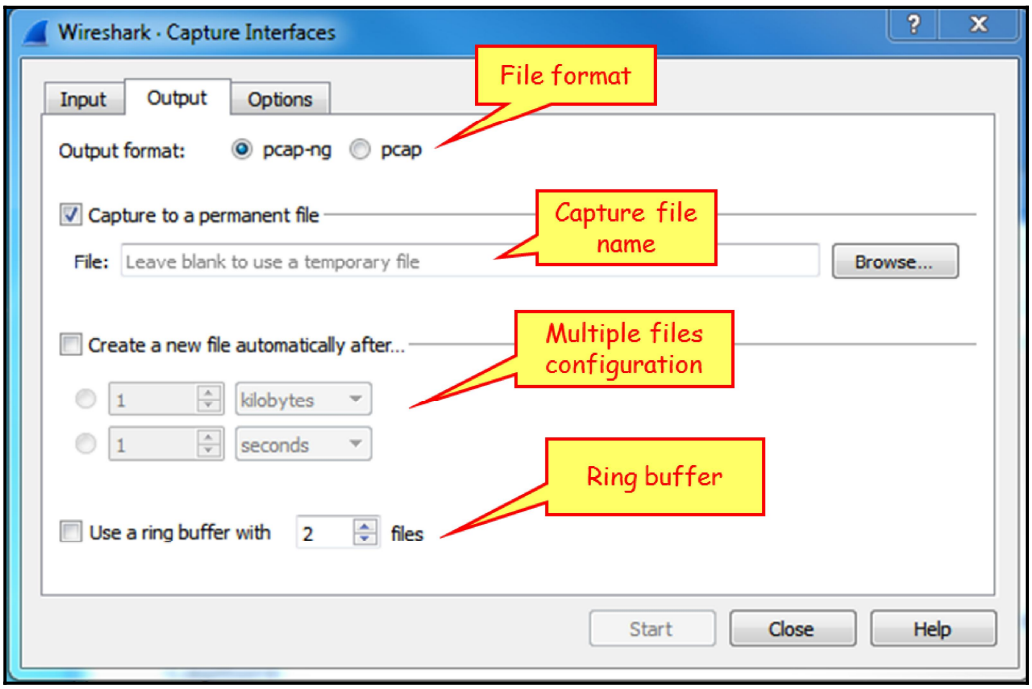

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Expression...
Welcome to Wir
Open
C:\Technical\Wireshark\CAP-PCAP Customers\Snif1-LISHKAT-MISCHAR-2.cap (3006 Bytes)
C:\Technical\Wireshark\CAP-PCAP Customers\Snif4-miniline-26-08-2001.cap (210 KB)
C:\Technical\Wireshark\CAP-PCAP General\DNS Problem --- Home --- Feb 2016.pcapng (11 KB)
Capture
...using this filter: Enter a capture filter ...
Wireless Network Connection
Local Area Connection
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default
1
2
3

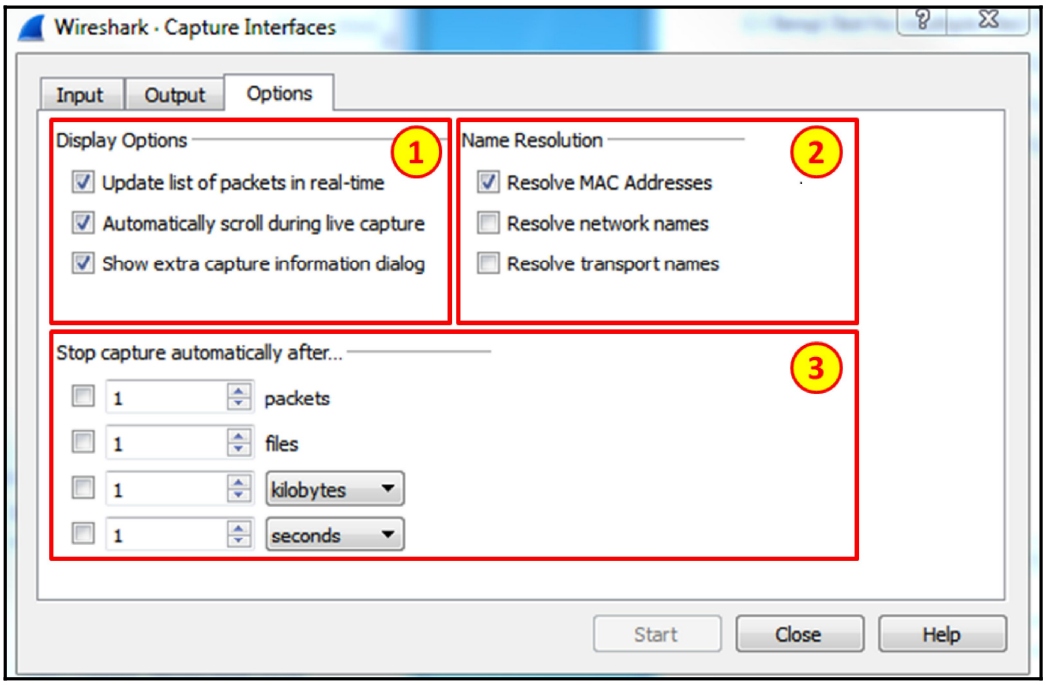

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Open
C:\Technical\Wireshark\CAP-PCAP Customers\Snif1-LISHKAT-MISCHAR-2.cap (3006 Bytes)
C:\Technical\Wireshark\CAP-PCAP Customers\Snif4-miniline-26-08-2001.cap (210 KB)
C:\Technical\Wireshark\CAP-PCAP General\DNS Problem --- Home --- Feb 2016.pcapng (11 KB)
Two marked interfaces
Capture
...using this filter:
Enter a capture filter ...
Wireless Network Connection
Local Area Connection
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.0.2 (v2.0.2-0-ga16e22e from master-2.0). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

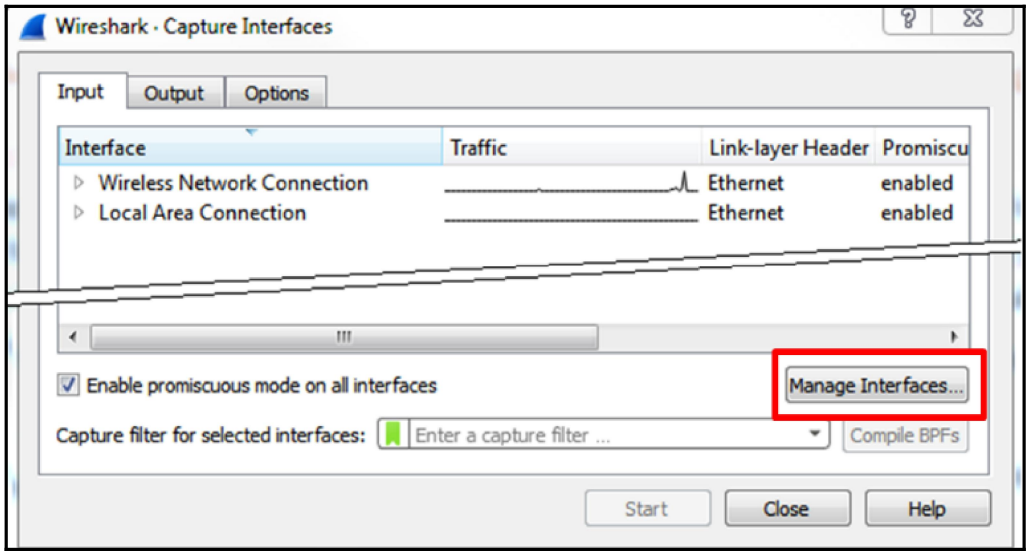

*2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
52 28.529288 HonHaiPr_c7:8e:73 Broadcast ARP 42 Who has 10.0.0.138? Tell 10.0.0.4
53 28.532119 D-LinkCo_16:09:78
54 28.619424 10.0.0.4
55 28.928313 10.0.0.4
56 28.968200 169.254.170.91
57 28.968548 0.0.0.0
58 28.968655 169.254.170.91
59 29.053052 10.0.0.4
60 29.069848 10.0.0.4
61 29.072195 10.0.0.4
62 29.172602 10.0.0.4
Command Prompt
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Autoconfiguration IPv4 Address. . : 169.254.170.91
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
Wireless LAN adapter Wireless Network Connection:
Connection-specific DNS Suffix . : Home
IPv4 Address. . . . . : 10.0.0.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.0.0.138

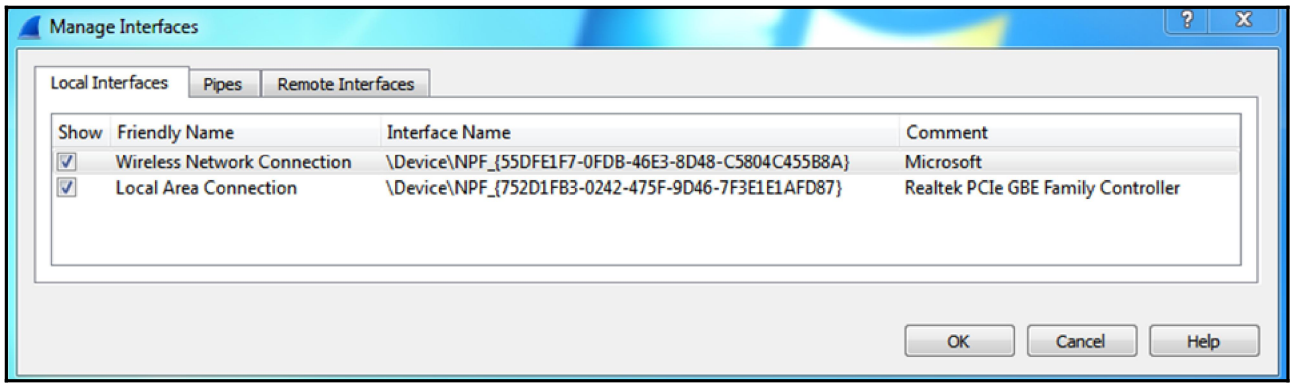

To ISP
Laptop/Desktop with Wireshark and two physical interfaces
Port mirror on switch 1
Port mirror on switch 2

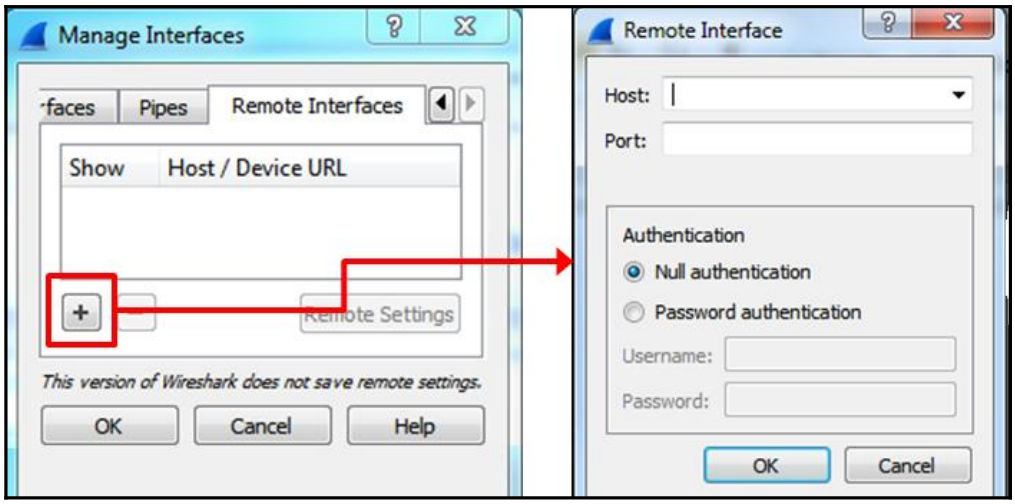

Wireshark · Capture Interfaces
Capture input/output and options
Input
Output
Options
Interface
Traffic
Link-layer Header
Promiscuous
Local Area Connection
Ethernet
enabled
Wireless Network Connection
Ethernet
enabled
Interfaces
Promiscuous mode
Capture filter configuration
Interfaces management
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Close
Help

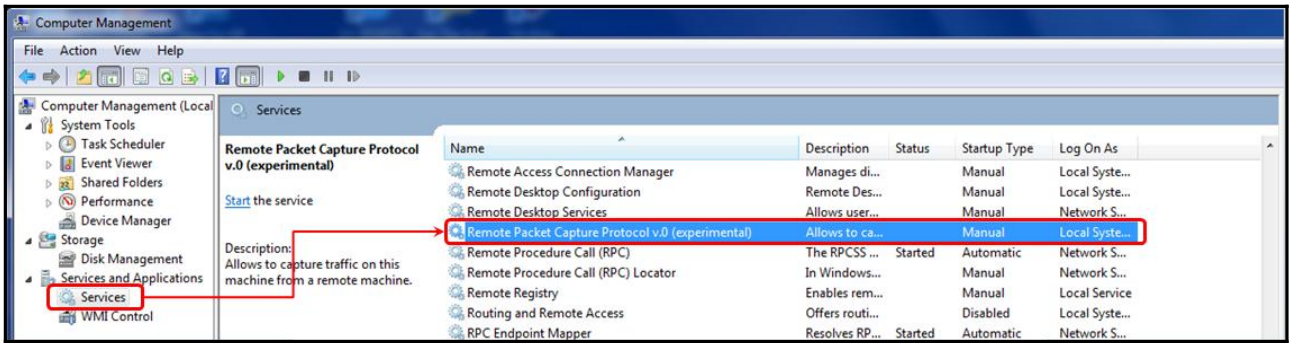

Wireshark · Capture Interfaces
Input
Output
Options
File format
Output format:
pcap-ng
pcap
Capture to a permanent file
Capture file name
File:
Leave blank to use a temporary file
Browse...
Create a new file automatically after...
Multiple files configuration
1
kilobytes
1
seconds
Ring buffer
Use a ring buffer with
2
files
Start
Close
Help

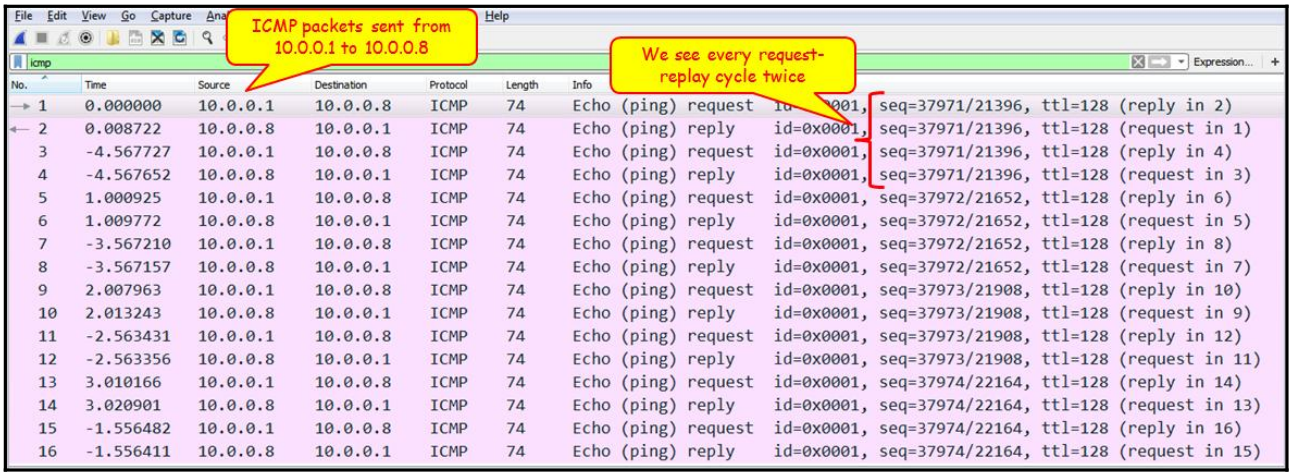

Wireshark · Capture Interfaces
Input
Output
Options
Display Options
1
Update list of packets in real-time
Automatically scroll during live capture
Show extra capture information dialog
Name Resolution
2
Resolve MAC Addresses
Resolve network names
Resolve transport names
Stop capture automatically after...
3
1
packets
1
files
1
kilobytes
1
seconds
Start
Close
Help

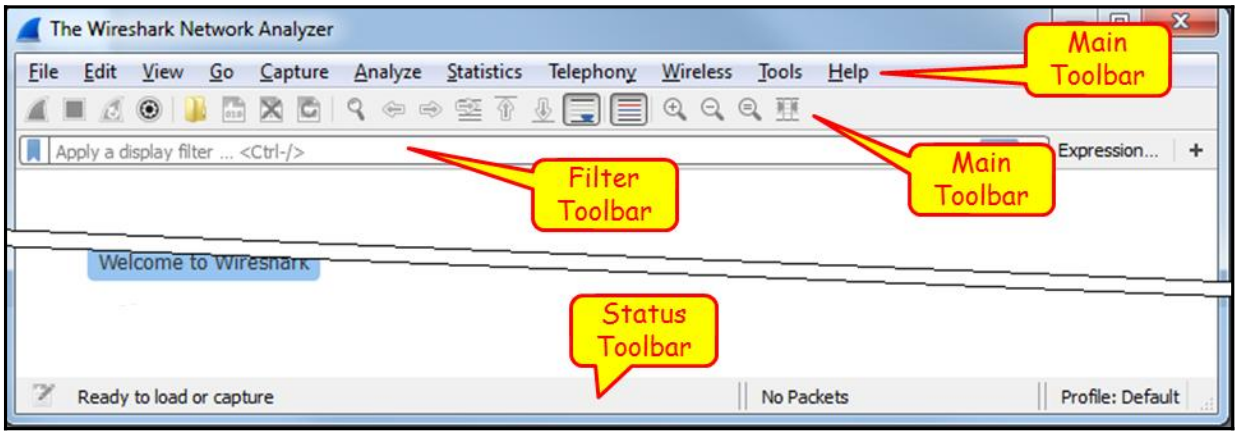

Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promiscu
Wireless Network Connection
Ethernet
enabled
Local Area Connection
Ethernet
enabled
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Close
Help

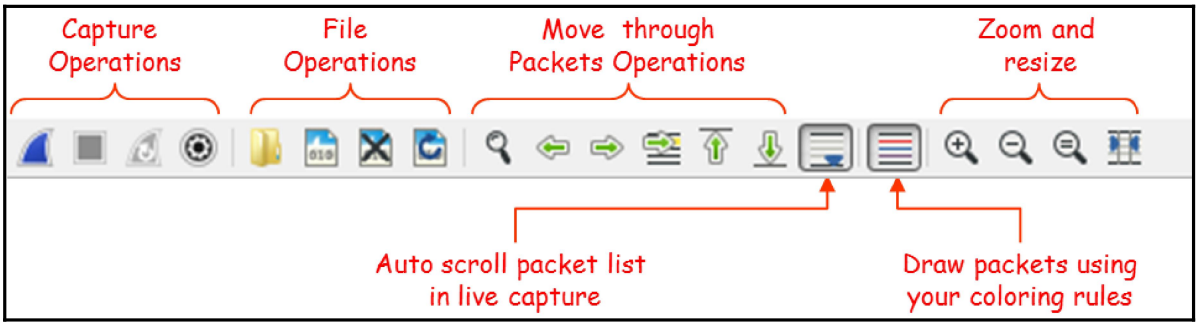

Manage Interfaces
Local Interfaces
Pipes
Remote Interfaces
Show
Friendly Name
Interface Name
Comment
Wireless Network Connection
\Device\NPF_{55DFE1F7-0FDB-46E3-8D48-C5804C455B8A}
Microsoft
Local Area Connection
\Device\NPF_{752D1FB3-0242-475F-9D46-7F3E1E1AFD87}
Realtek PCIe GBE Family Controller
OK
Cancel
Help

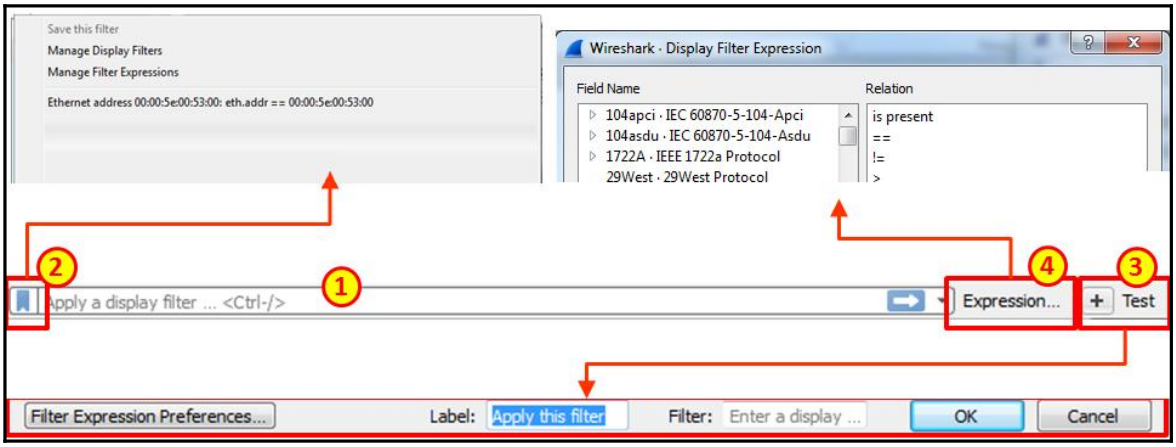

Manage Interfaces
faces
Pipes
Remote Interfaces
Show
Host / Device URL
Remote Settings
This version of Wireshark does not save remote settings.
OK
Cancel
Help
Remote Interface
Host:
Port:
Authentication
Null authentication
Password authentication
Username:
Password:
OK
Cancel

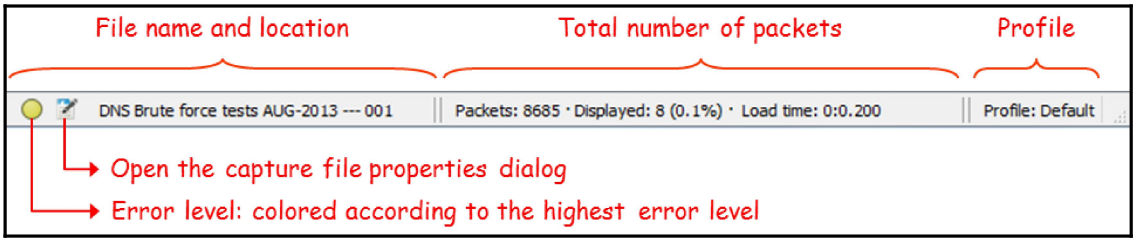

Computer Management
File Action View Help
Computer Management (Local
System Tools
Task Scheduler
Event Viewer
Shared Folders
Performance
Device Manager
Storage
Disk Management
Services and Applications
Services
WMI Control
Services
Remote Packet Capture Protocol v.0 (experimental)
Start the service
Description:
Allows to capture traffic on this machine from a remote machine.
Name
Description
Status
Startup Type
Log On As
Remote Access Connection Manager
Remote Desktop Configuration
Remote Desktop Services
Remote Packet Capture Protocol v.0 (experimental)
Remote Procedure Call (RPC)
Remote Procedure Call (RPC) Locator
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper


ICMP packets sent from 10.0.0.1 to 10.0.0.8
We see every request-replay cycle twice
icmp
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request seq=37971/21396, ttl=128 (reply in 2)
2 0.008722 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37971/21396, ttl=128 (request in 1)
3 -4.567727 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37971/21396, ttl=128 (reply in 4)
4 -4.567652 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37971/21396, ttl=128 (request in 3)
5 1.000925 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37972/21652, ttl=128 (reply in 6)
6 1.009772 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37972/21652, ttl=128 (request in 5)
7 -3.567210 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37972/21652, ttl=128 (reply in 8)
8 -3.567157 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37972/21652, ttl=128 (request in 7)
9 2.007963 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37973/21908, ttl=128 (reply in 10)
10 2.013243 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37973/21908, ttl=128 (request in 9)
11 -2.563431 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37973/21908, ttl=128 (reply in 12)
12 -2.563356 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37973/21908, ttl=128 (request in 11)
13 3.010166 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37974/22164, ttl=128 (reply in 14)
14 3.020901 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37974/22164, ttl=128 (request in 13)
15 -1.556482 10.0.0.1 10.0.0.8 ICMP 74 Echo (ping) request id=0x0001, seq=37974/22164, ttl=128 (reply in 16)
16 -1.556411 10.0.0.8 10.0.0.1 ICMP 74 Echo (ping) reply id=0x0001, seq=37974/22164, ttl=128 (request in 15)

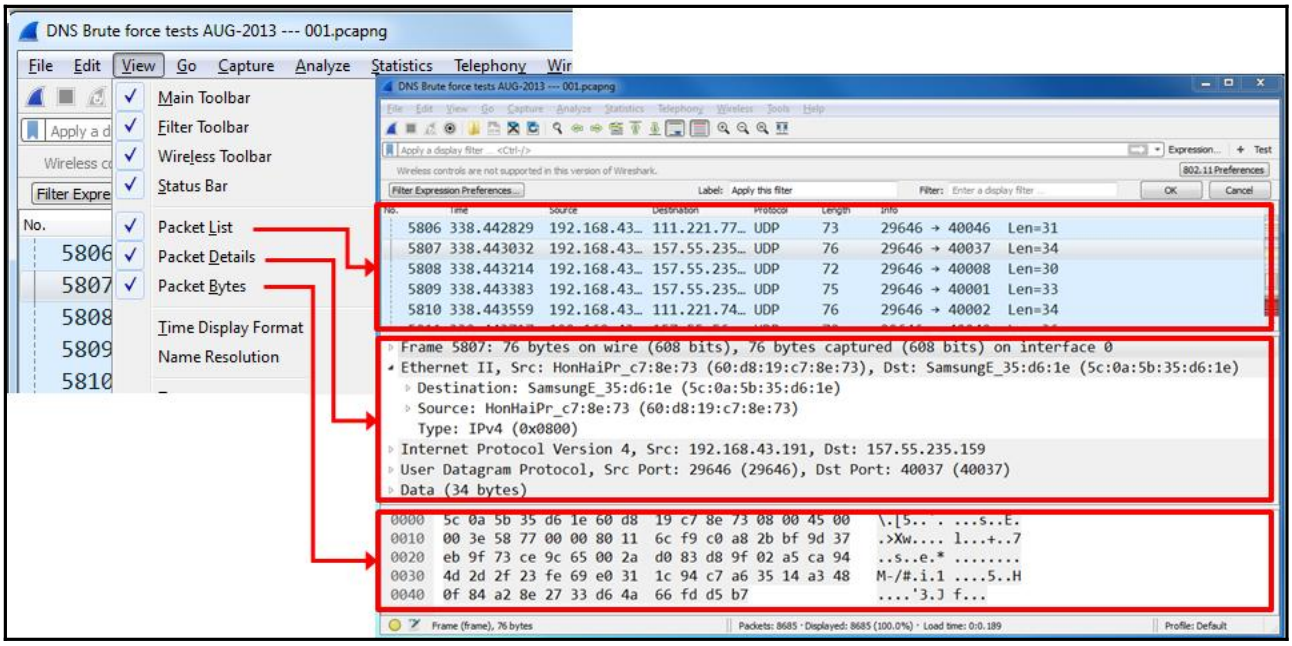

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Apply a display filter ... <Ctrl-/>
Expression...
Filter Toolbar
Main Toolbar
Welcome to Wireshark
Status Toolbar
Ready to load or capture
No Packets
Profile: Default

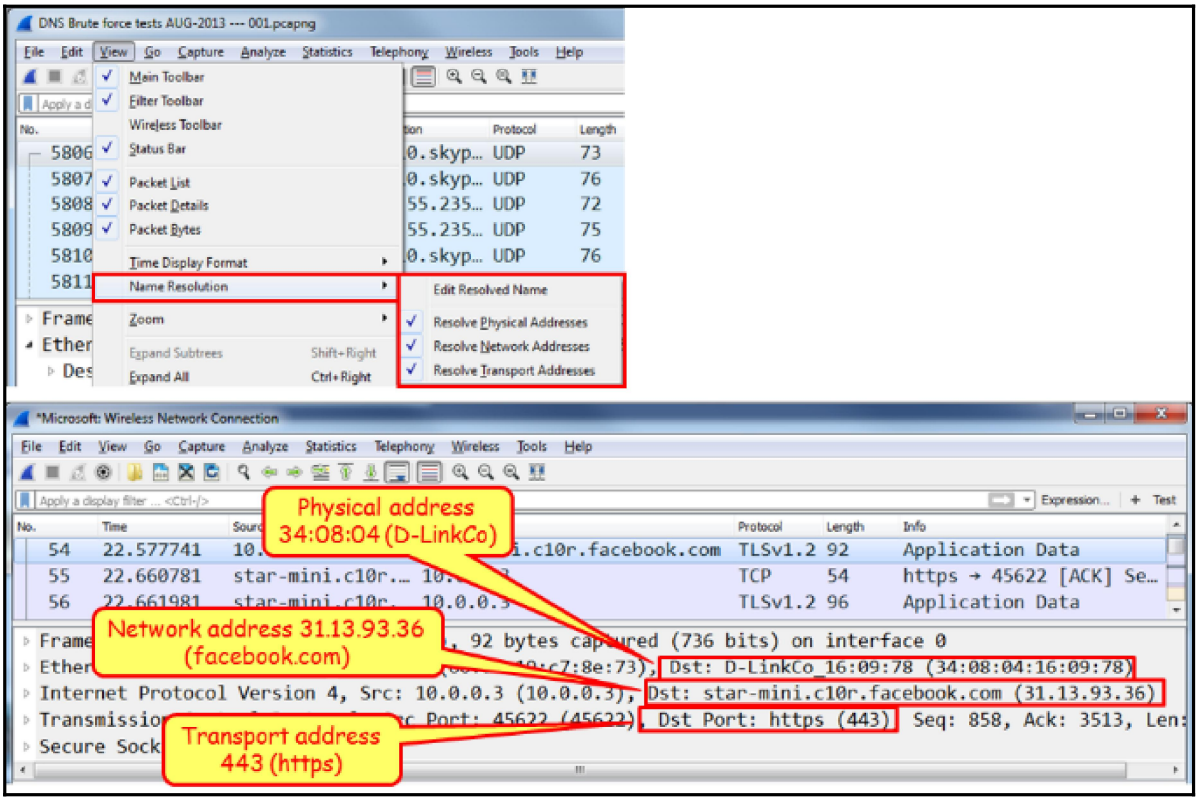

Capture Operations
File Operations
Move through Packets Operations
Zoom and resize
Auto scroll packet list in live capture
Draw packets using your coloring rules

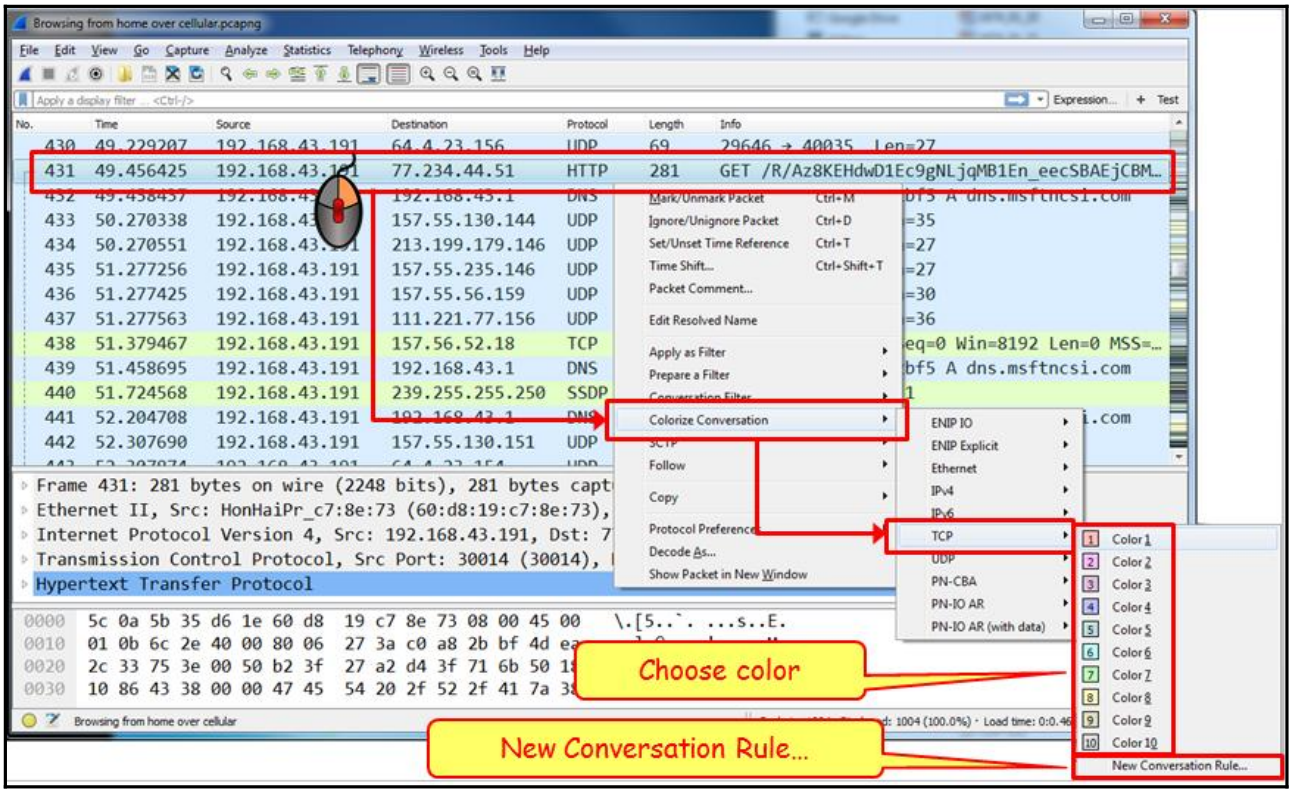

Save this filter
Manage Display Filters
Manage Filter Expressions
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Wireshark · Display Filter Expression
Field Name
Relation
104apci · IEC 60870-5-104-Apci
104asdu · IEC 60870-5-104-Asdu
1722A · IEEE 1722a Protocol
29West · 29West Protocol
is present
==
!=
>
2
1
Apply a display filter ... <Ctrl-/>
4
3
Expression...
Test
Filter Expression Preferences...
Label:
Apply this filter
Filter:
Enter a display ...
OK
Cancel

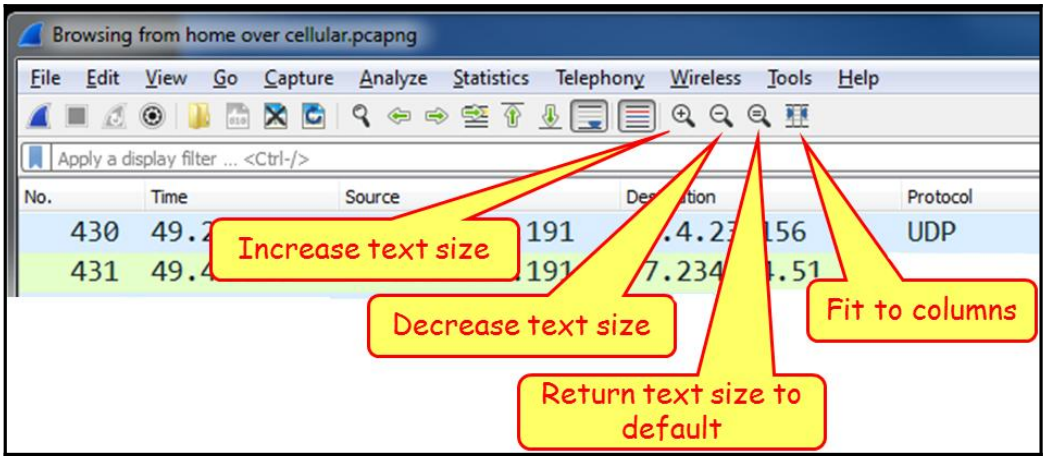

File name and location
Total number of packets
Profile
DNS Brute force tests AUG-2013 --- 001
Packets: 8685 · Displayed: 8 (0.1%) · Load time: 0:0.200
Profile: Default
Open the capture file properties dialog
Error level: colored according to the highest error level


DNS Brute force tests AUG-2013 --- 001.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Wireless Toolbar
Status Bar
Packet List
Packet Details
Packet Bytes
Time Display Format
Open the preferences configuration for Wireless LAN
802.11 Preferences
Wireless controls are not supported in this version of Wireshark.

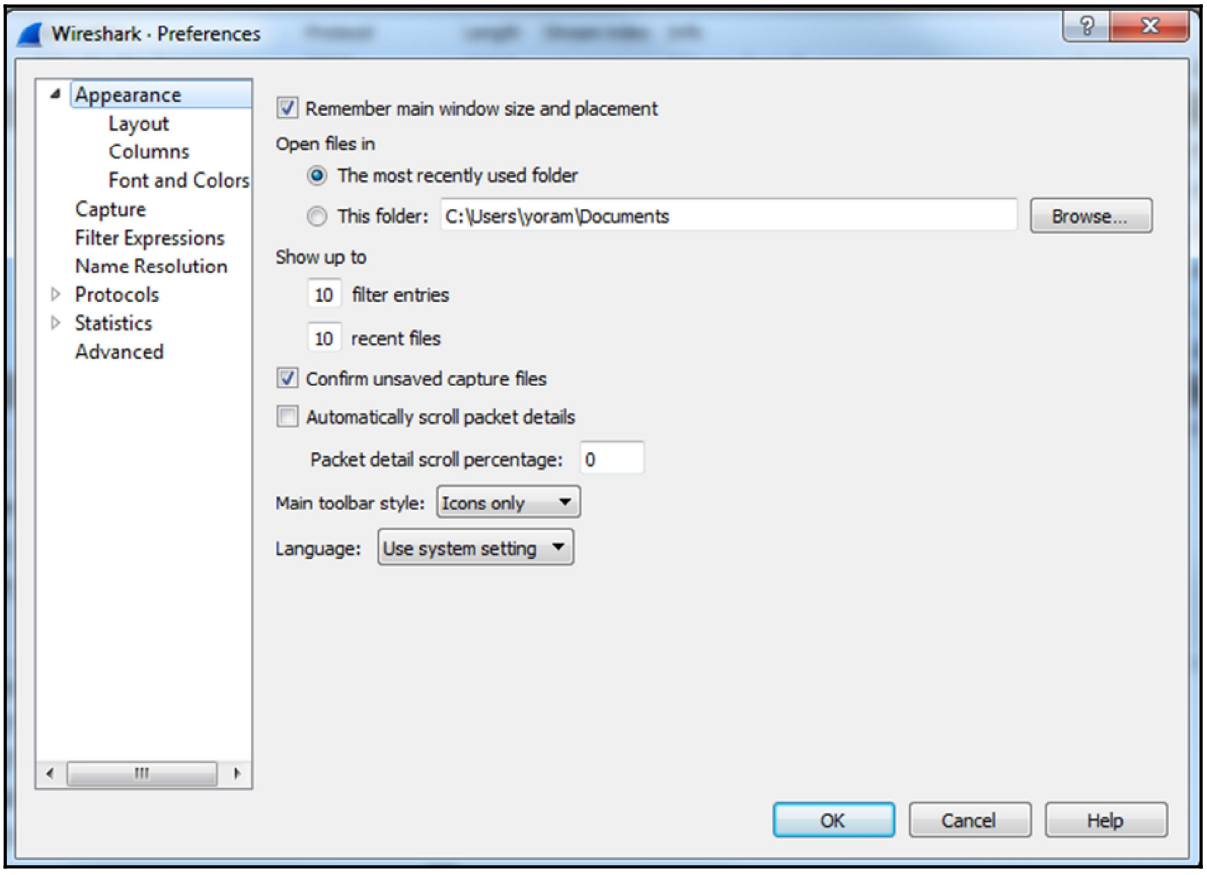

DNS Brute force tests AUG-2013 --- 001.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wir
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
5806 338.442829 192.168.43… 111.221.77… UDP 73 29646 → 40046 Len=31
5807 338.443032 192.168.43… 157.55.235… UDP 76 29646 → 40037 Len=34
5808 338.443214 192.168.43… 157.55.235… UDP 72 29646 → 40008 Len=30
5809 338.443383 192.168.43… 157.55.235… UDP 75 29646 → 40001 Len=33
5810 338.443559 192.168.43… 111.221.74… UDP 76 29646 → 40002 Len=34
Frame 5807: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface 0
Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: SamsungE_35:d6:1e (5c:0a:5b:35:d6:1e)
Destination: SamsungE_35:d6:1e (5c:0a:5b:35:d6:1e)
Source: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.191, Dst: 157.55.235.159
User Datagram Protocol, Src Port: 29646 (29646), Dst Port: 40037 (40037)
Data (34 bytes)
0000 5c 0a 5b 35 d6 1e 60 d8 19 c7 8e 73 08 00 45 00
0010 00 3e 58 77 00 00 80 11 6c f9 c0 a8 2b bf 9d 37
0020 eb 9f 73 ce 9c 65 00 2a d0 83 d8 9f 02 a5 ca 94
0030 4d 2d 2f 23 fe 69 e0 31 1c 94 c7 a6 35 14 a3 48
0040 0f 84 a2 8e 27 33 d6 4a 66 fd d5 b7

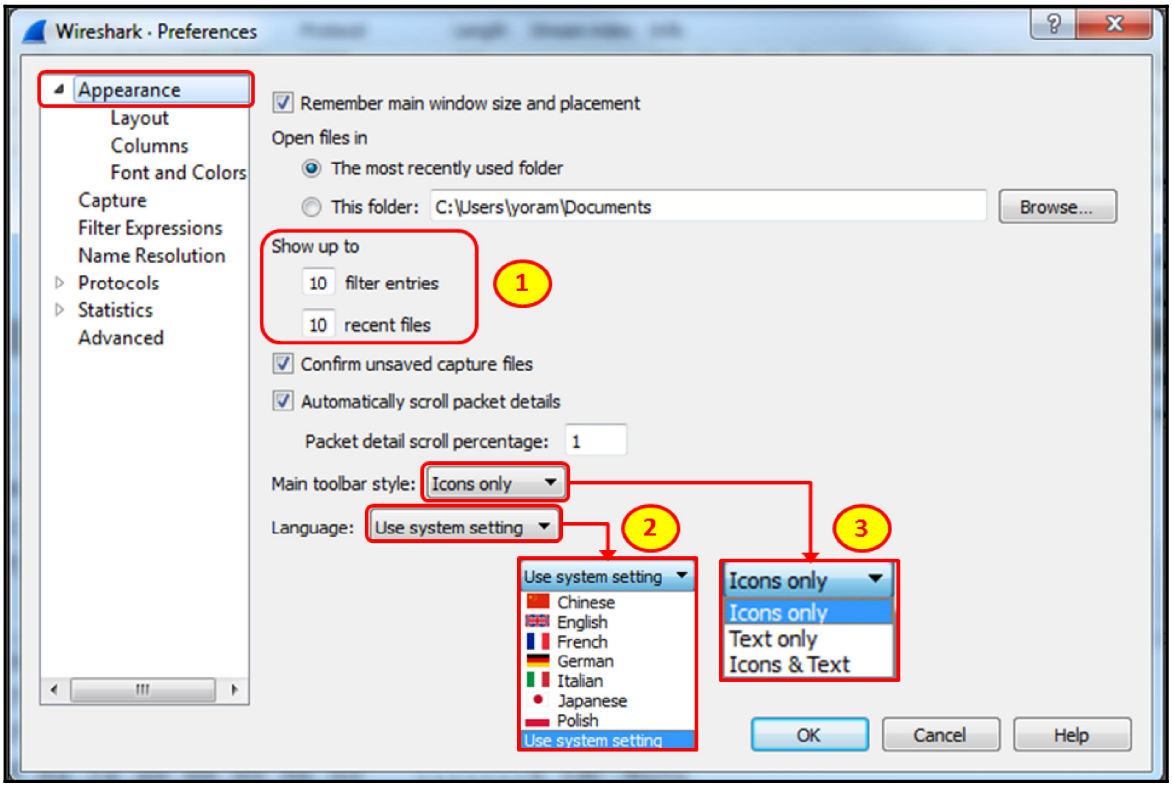

DNS Brute force tests AUG-2013 --- 001.pcapng
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Edit Resolved Name
Resolve Physical Addresses
Resolve Network Addresses
Resolve Transport Addresses
*Microsoft: Wireless Network Connection
Physical address 34:08:04 (D-LinkCo)
Network address 31.13.93.36 (facebook.com)
Transport address 443 (https)
54 22.577741 TLSv1.2 92 Application Data
55 22.660781 TCP 54 https → 45622 [ACK] Se…
56 TLSv1.2 96 Application Data
Dst: D-LinkCo_16:09:78 (34:08:04:16:09:78)
Dst: star-mini.c10r.facebook.com (31.13.93.36)
Dst Port: https (443) Seq: 858, Ack: 3513, Len:

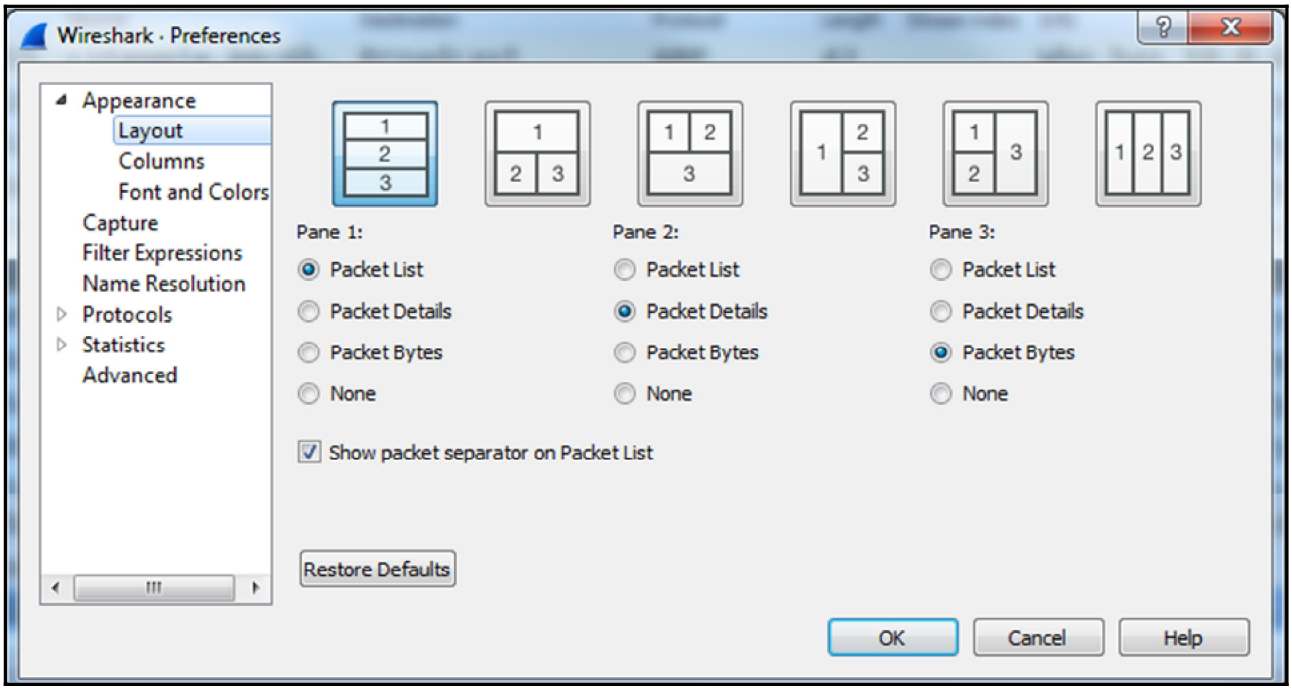

Choose color
New Conversation Rule...

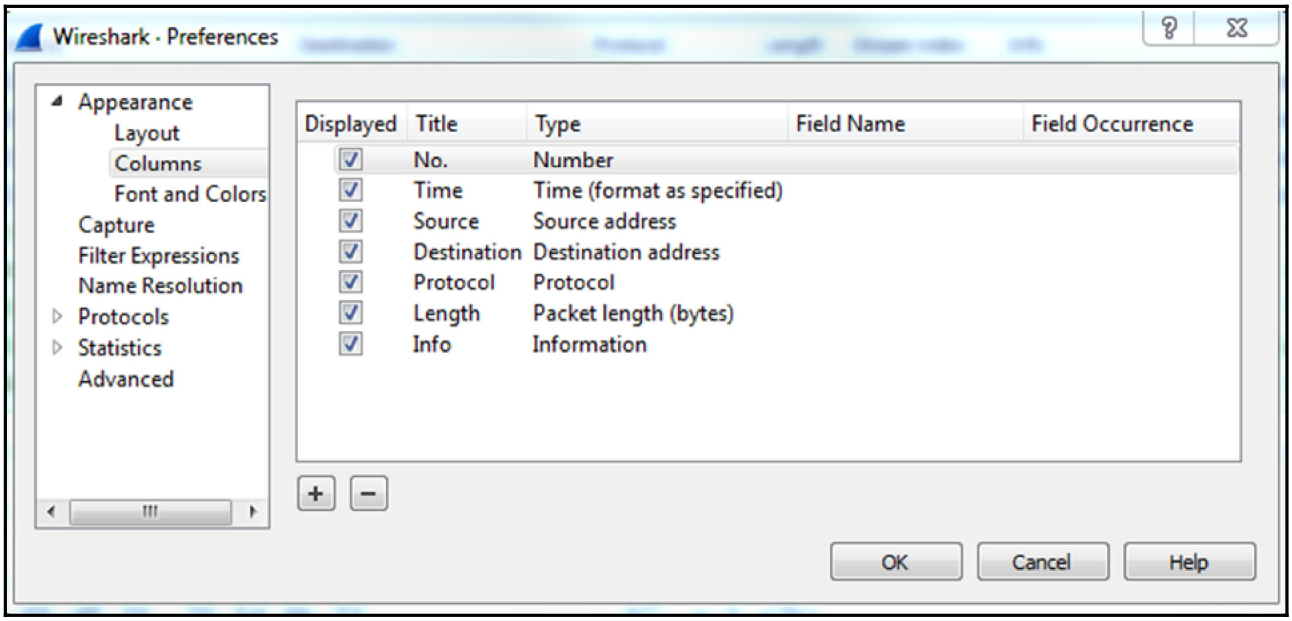

Increase text size
Decrease text size
Return text size to default
Fit to columns

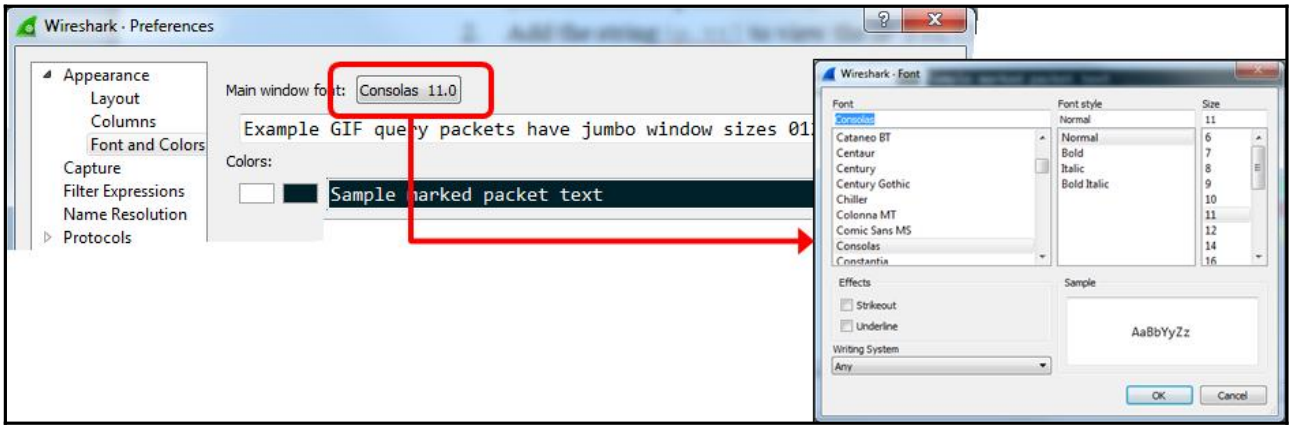
Chapter 2: Mastering Wireshark for Network Troubleshooting

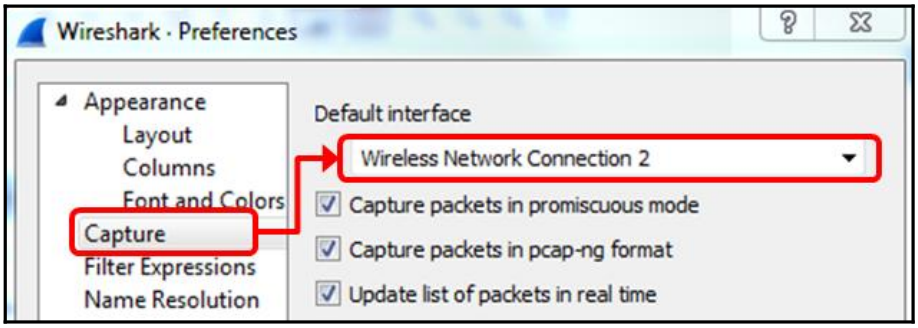


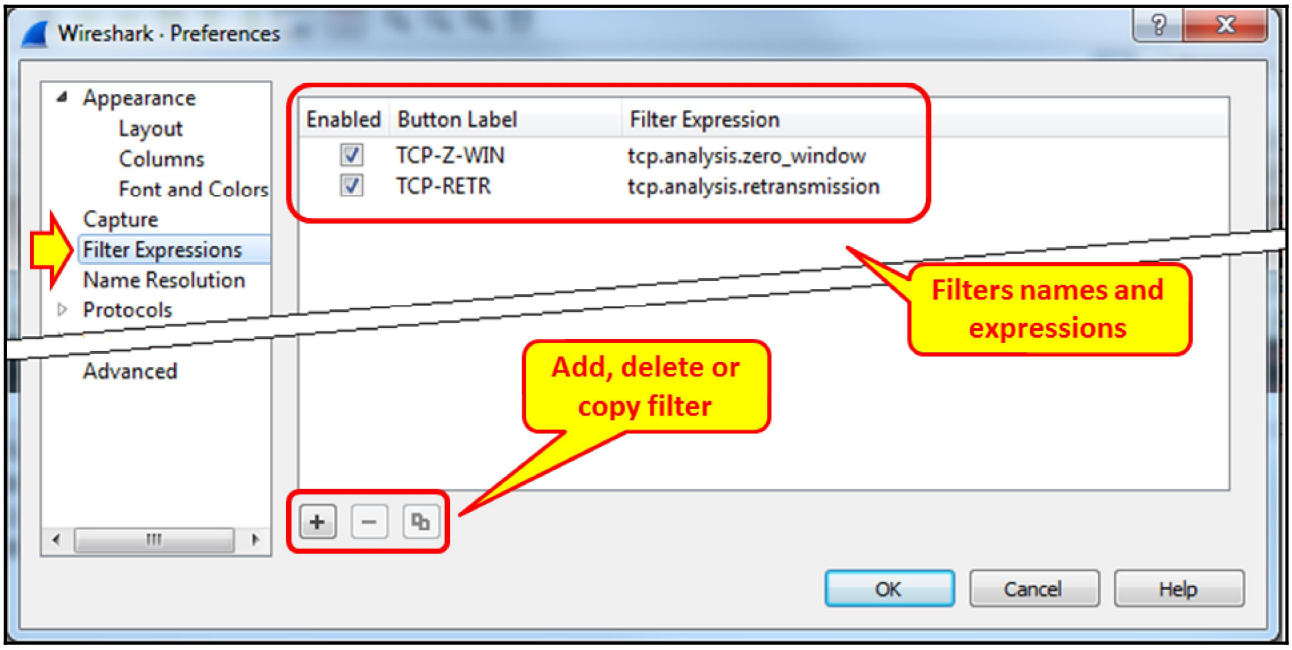

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Statistics
Advanced
Remember main window size and placement
Open files in
The most recently used folder
This folder: C:\Users\yoram\Documents
Browse...
Show up to
10 filter entries
10 recent files
1
Confirm unsaved capture files
Automatically scroll packet details
Packet detail scroll percentage: 1
Main toolbar style: Icons only
Language: Use system setting
2
3
Use system setting
Chinese
English
French
German
Italian
Japanese
Polish
Use system setting
Icons only
Icons only
Text only
Icons & Text
OK
Cancel
Help

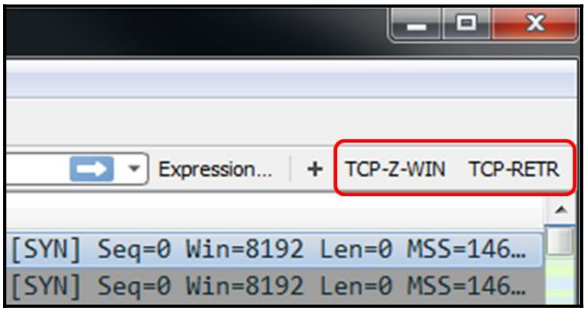

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Statistics
Advanced
Pane 1:
Packet List
Packet Details
Packet Bytes
None
Pane 2:
Packet List
Packet Details
Packet Bytes
None
Pane 3:
Packet List
Packet Details
Packet Bytes
None
Show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

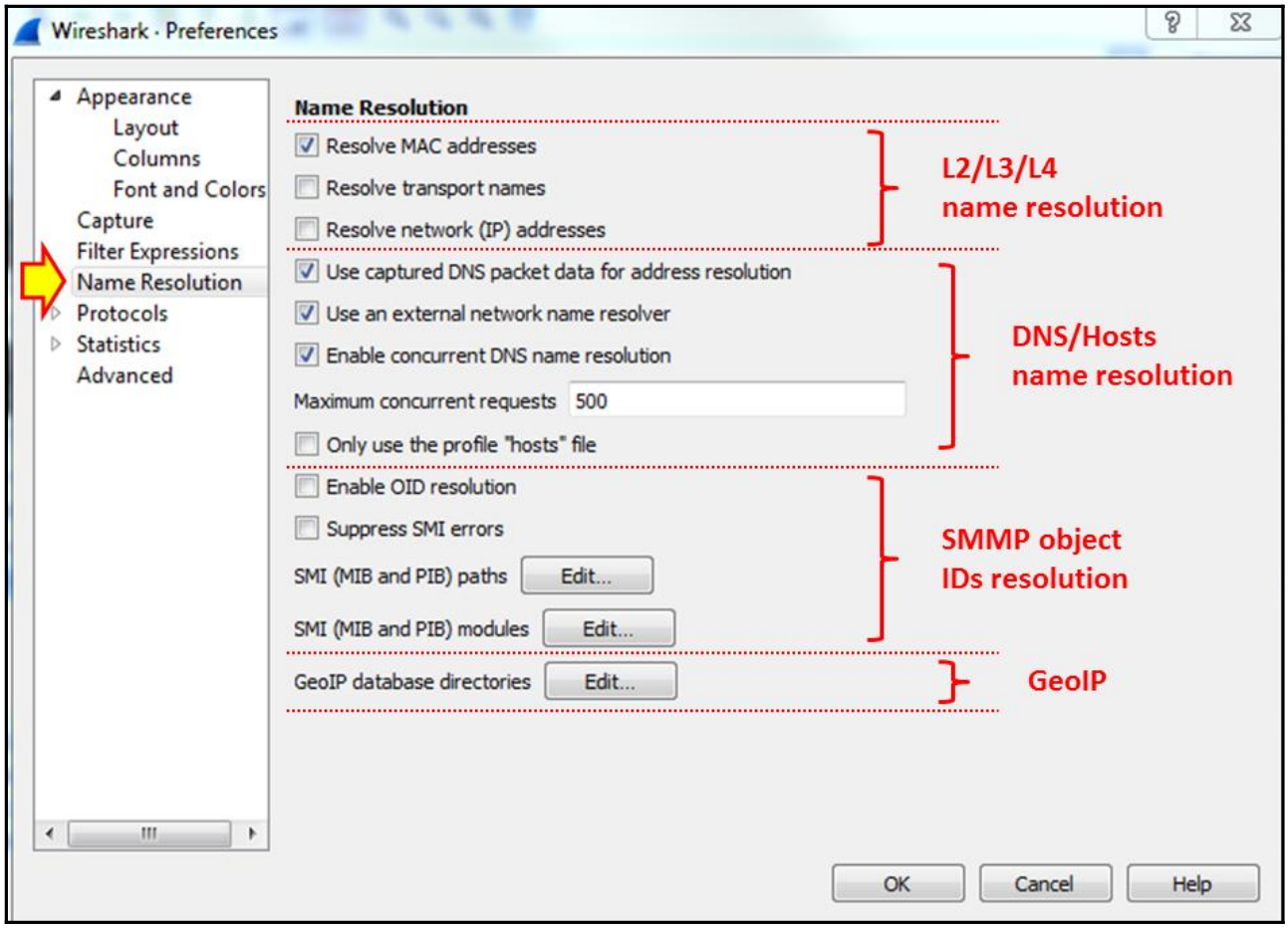

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Statistics
Advanced
Displayed
Title
Type
Field Name
Field Occurrence
No.
Number
Time
Time (format as specified)
Source
Source address
Destination
Destination address
Protocol
Protocol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

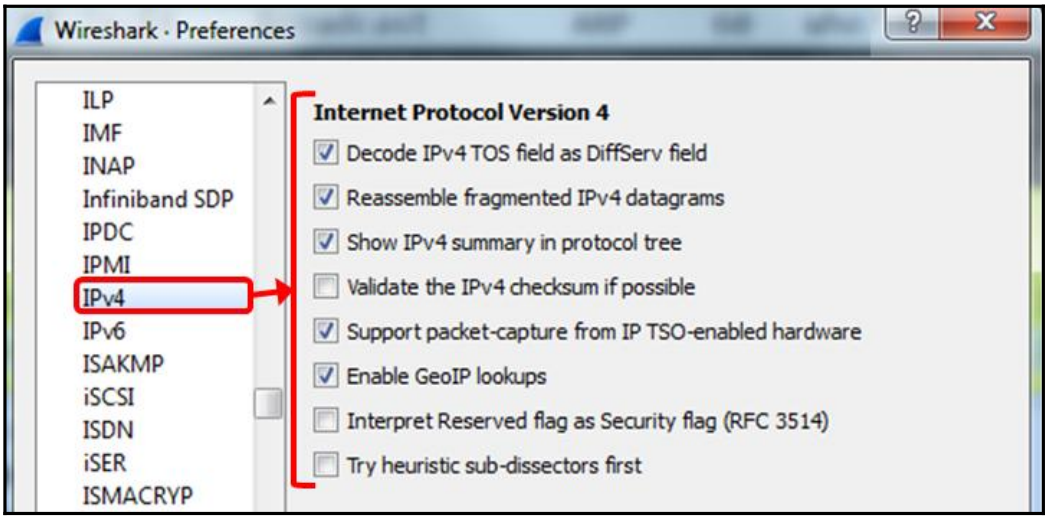

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Main window font:
Consolas 11.0
Colors:
Wireshark · Font
Font
Font style
Size
Effects
Strikeout
Underline
Writing System
Sample
AaBbYyZz
OK
Cancel

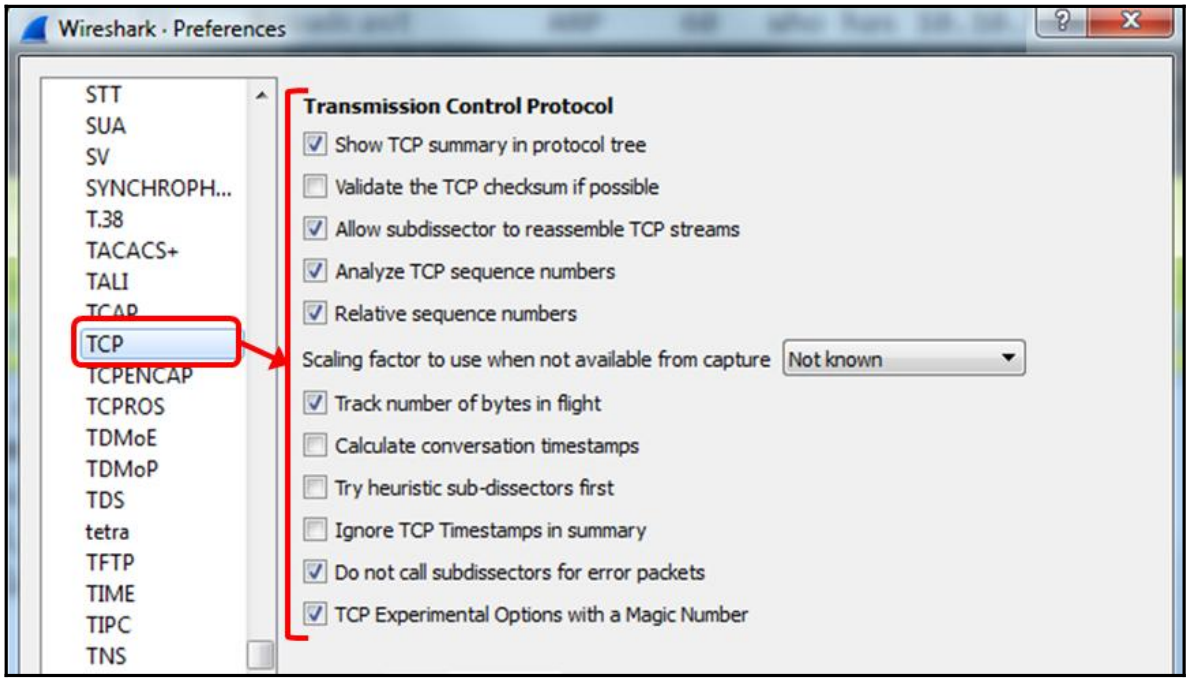

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Default interface
Wireless Network Connection 2
Capture packets in promiscuous mode
Capture packets in pcap-ng format
Update list of packets in real time

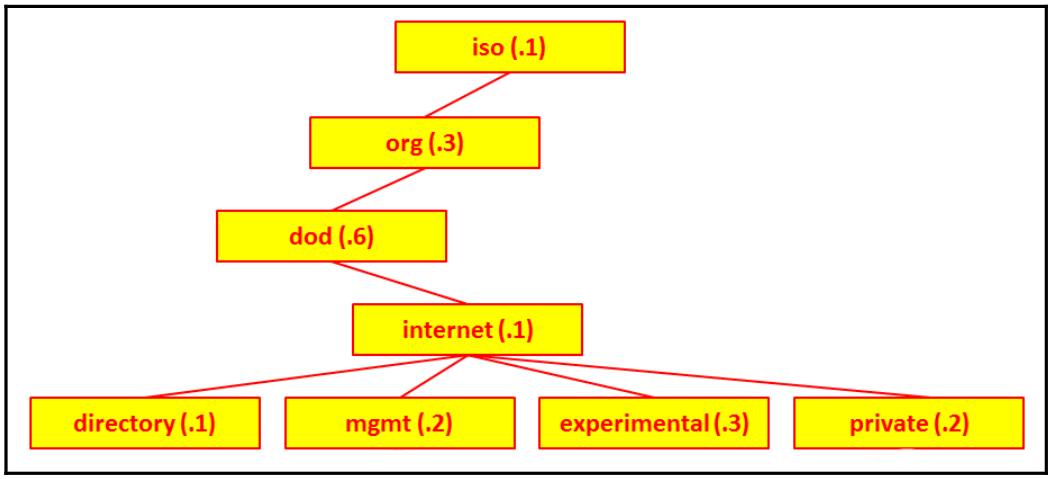

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Advanced
Enabled
Button Label
Filter Expression
TCP-Z-WIN
tcp.analysis.zero_window
TCP-RETR
tcp.analysis.retransmission
Filters names and expressions
Add, delete or copy filter
OK
Cancel
Help

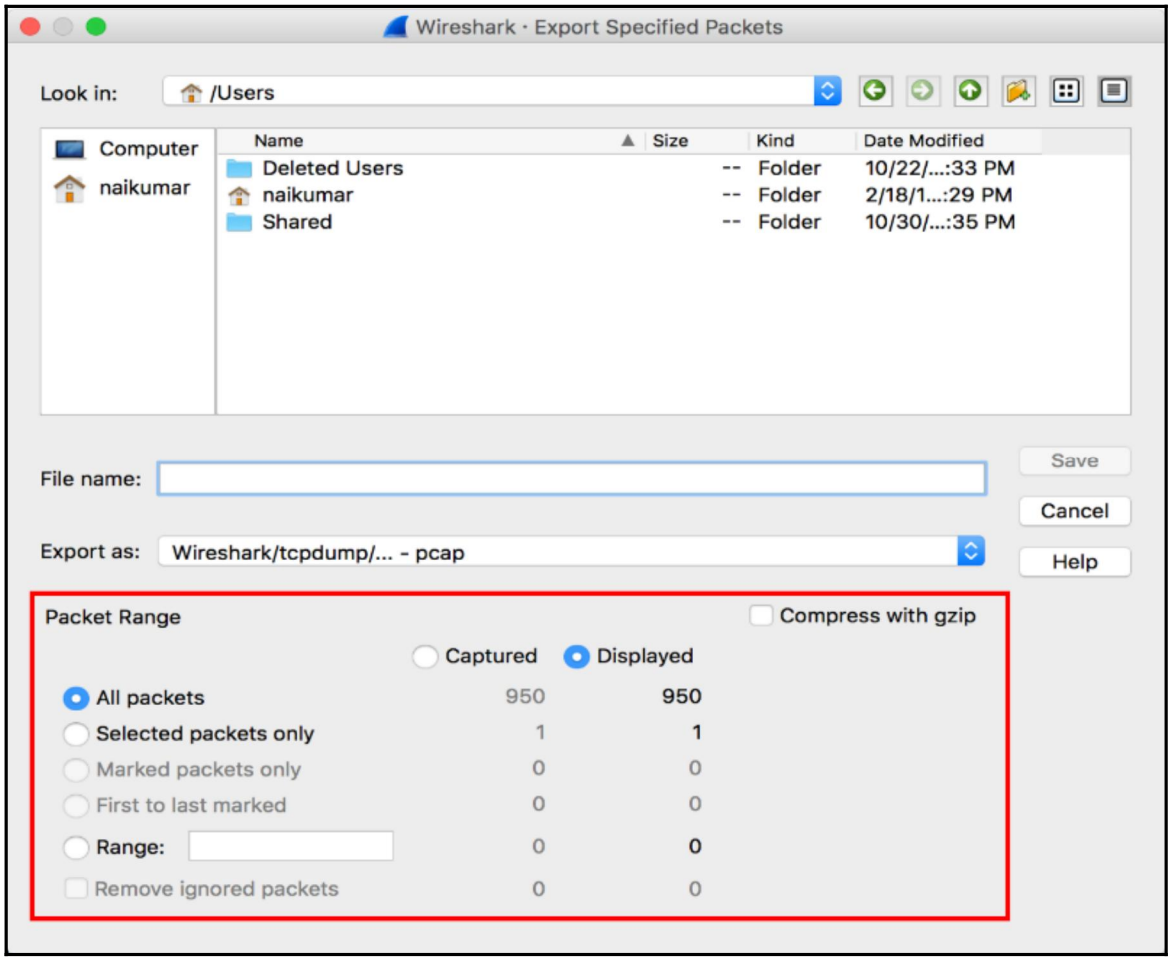

Expression...
TCP-Z-WIN
TCP-RETR
[SYN] Seq=0 Win=8192 Len=0 MSS=146...
[SYN] Seq=0 Win=8192 Len=0 MSS=146...

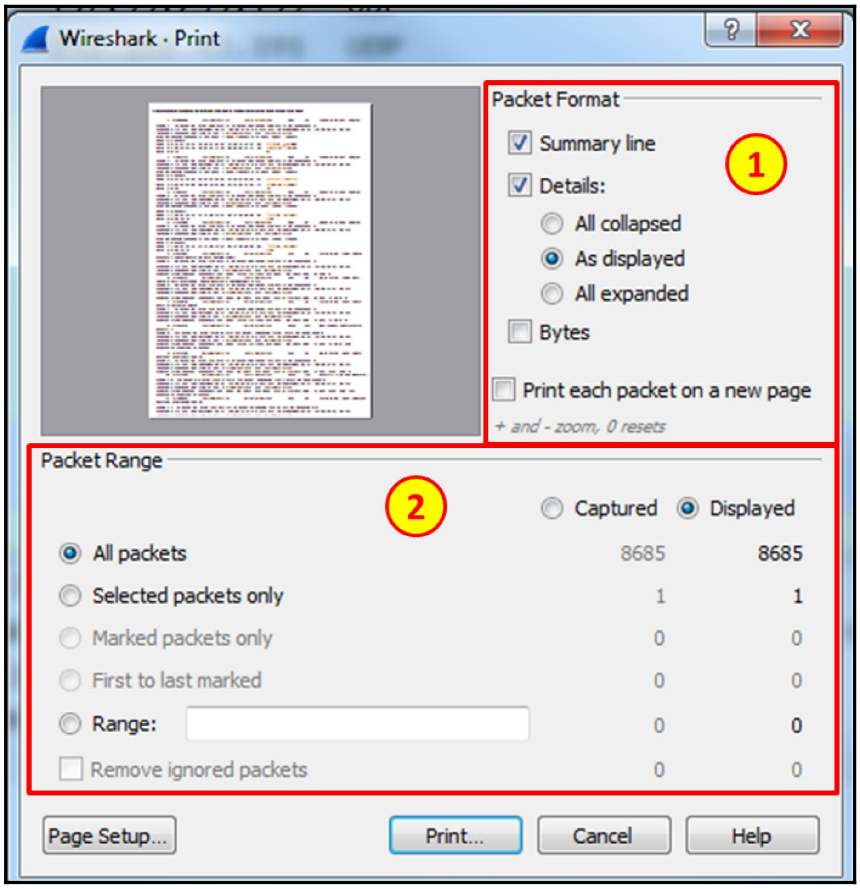

Wireshark · Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Protocols
Statistics
Advanced
Name Resolution
Resolve MAC addresses
Resolve transport names
Resolve network (IP) addresses
L2/L3/L4 name resolution
Use captured DNS packet data for address resolution
Use an external network name resolver
Enable concurrent DNS name resolution
Maximum concurrent requests
500
Only use the profile "hosts" file
DNS/Hosts name resolution
Enable OID resolution
Suppress SMI errors
SMI (MIB and PIB) paths
Edit...
SMI (MIB and PIB) modules
Edit...
SMMP object IDs resolution
GeoIP database directories
Edit...
GeoIP
OK
Cancel
Help


Wireshark · Preferences
ILP
IMF
INAP
Infiniband SDP
IPDC
IPMI
IPv4
IPv6
ISAKMP
iSCSI
ISDN
iSER
ISMACRYP
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-capture from IP TSO-enabled hardware
Enable GeoIP lookups
Interpret Reserved flag as Security flag (RFC 3514)
Try heuristic sub-dissectors first


Wireshark · Preferences
STT
SUA
SV
SYNCHROPH...
T.38
TACACS+
TALI
TCAP
TCP
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
tetra
TFTP
TIME
TIPC
TNS
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

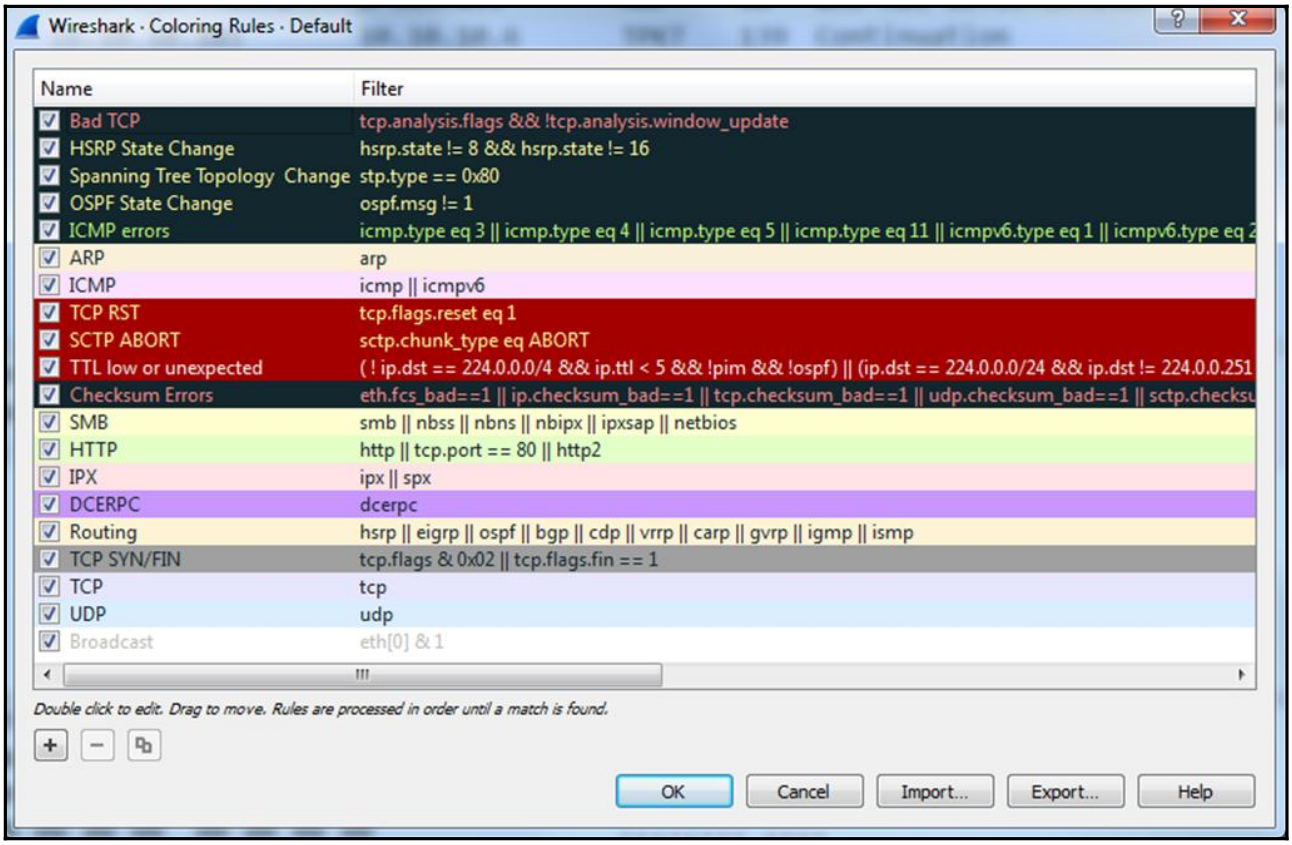

iso (.1)
org (.3)
dod (.6)
internet (.1)
directory (.1)
mgmt (.2)
experimental (.3)
private (.2)

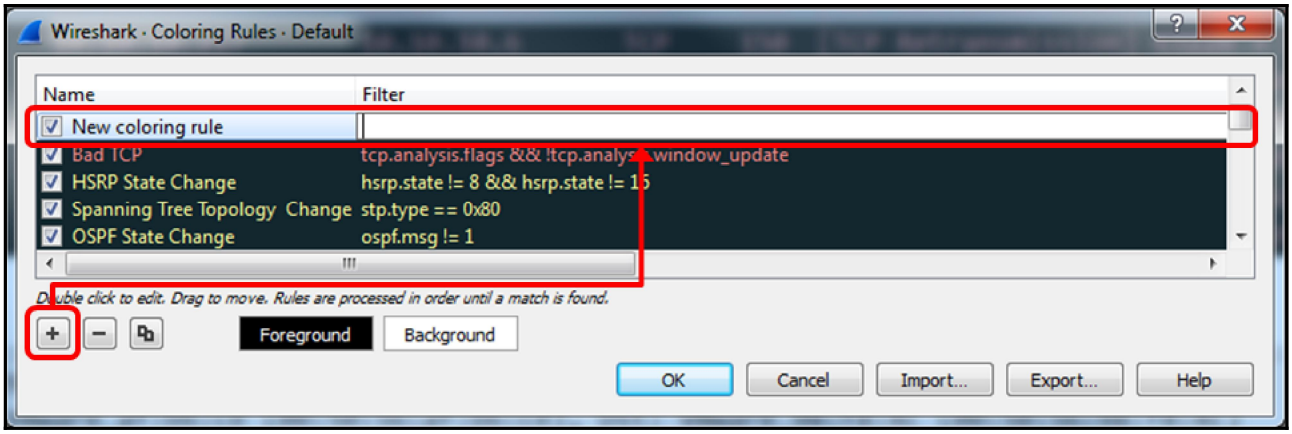

Wireshark · Export Specified Packets
Look in:
/Users
Computer
naikumar
Name
Size
Kind
Date Modified
Deleted Users -- Folder 10/22/...:33 PM
naikumar -- Folder 2/18/1...:29 PM
Shared -- Folder 10/30/...:35 PM
File name:
Save
Cancel
Export as:
Wireshark/tcpdump/... - pcap
Help
Packet Range
Compress with gzip
Captured
Displayed
All packets 950 950
Selected packets only 1 1
Marked packets only 0 0
First to last marked 0 0
Range: 0 0
Remove ignored packets 0 0

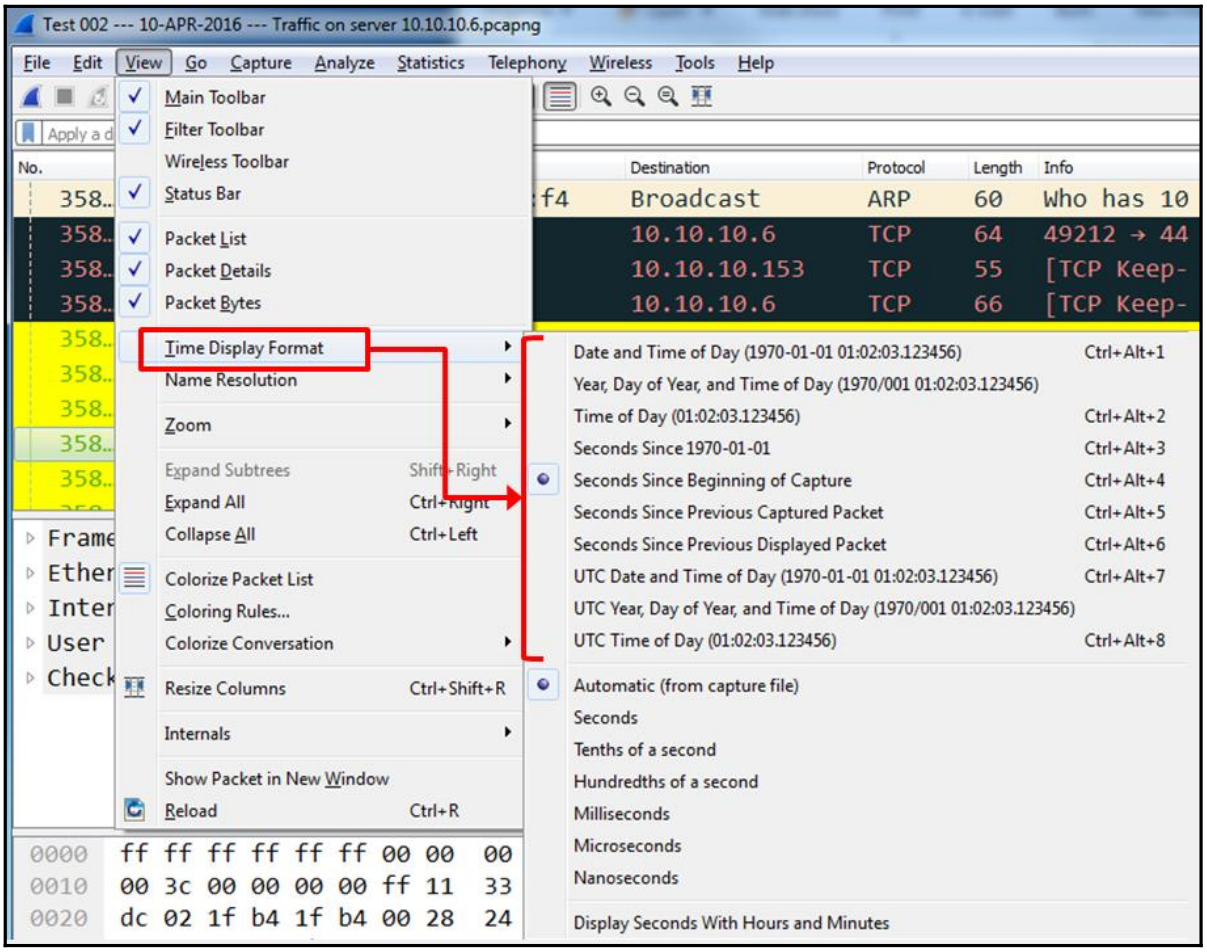


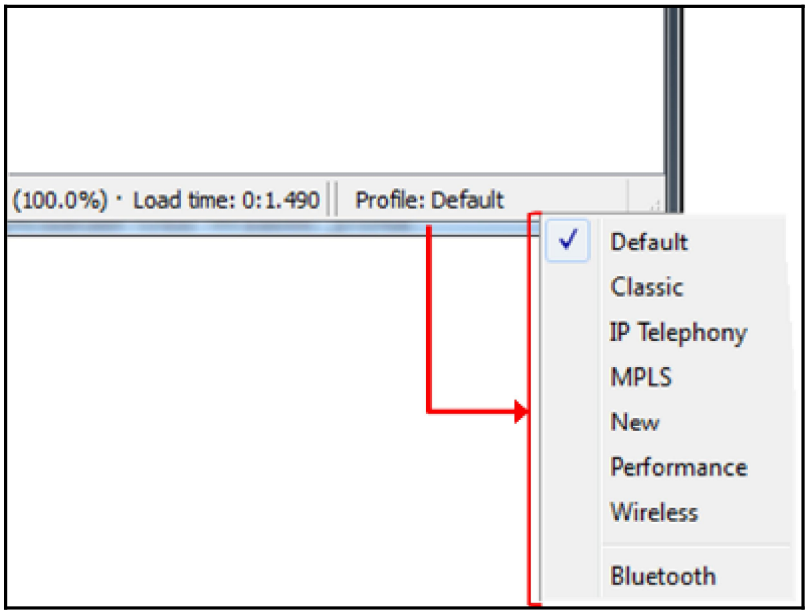
Wireshark | Authors | Folders | Plugins | Keyboard Shortcuts | License

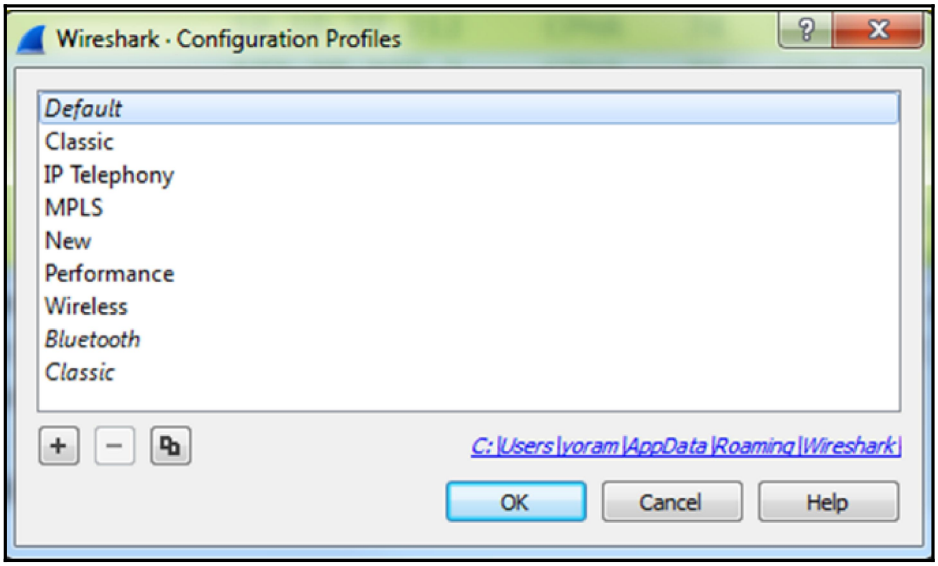
Name	Location	Typical Files
"File" dialogs	C:\Technical\Wireshark\CAP-PCAP Customers\	capture files
Temp	C:\Users\yoram\AppData\Local\Temp	untitled capture files
Personal configuration	C:\Users\yoram\AppData\Roaming\Wireshark\	*dfilters, preferences, ethers, ..*
Global configuration	C:\Program Files\Wireshark	*dfilters, preferences, manuf, ..*
System	C:\Program Files\Wireshark	*ethers, ipxnets*
Program	C:\Program Files\Wireshark	program files
Personal Plugins	C:\Users\yoram\AppDat...ing\Wireshark\plugins	dissector plugins
Global Plugins	C:\Program Files\Wireshark\plugins\2.0.2	dissector plugins
Extcap path	C:\Program Files\Wireshark\extcap	Extcap Plugins search path

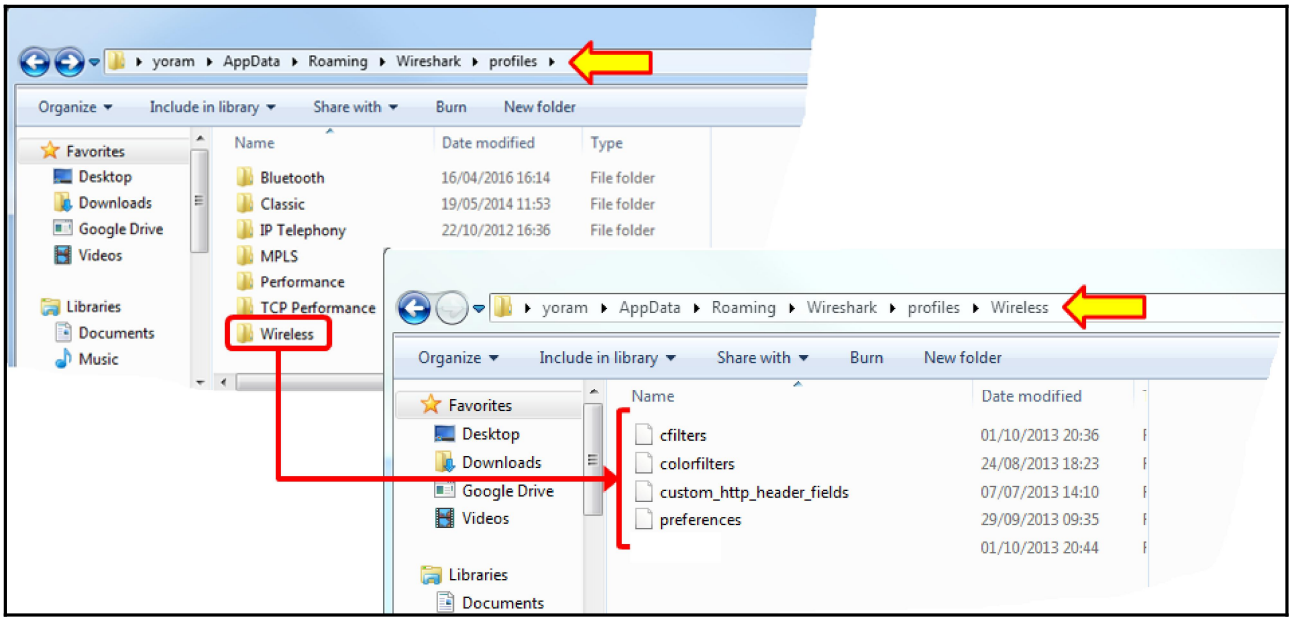

Wireshark · Coloring Rules · Default
Name
Filter
Bad TCP
tcp.analysis.flags && !tcp.analysis.window_update
HSRP State Change
hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 1
ICMP errors
icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2
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
Checksum Errors
eth.fcs_bad==1 || ip.checksum_bad==1 || tcp.checksum_bad==1 || udp.checksum_bad==1 || sctp.checksu
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


Wireshark · Coloring Rules · Default
Name
Filter
New coloring rule
Bad TCP
HSRP State Change
Spanning Tree Topology Change
stp.type == 0x80
OSPF State Change
ospf.msg != 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

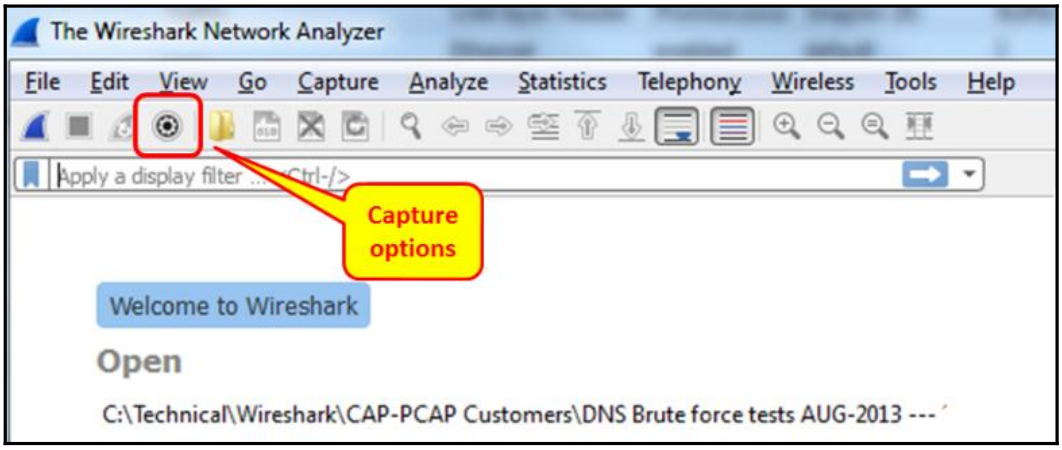

Test 002 --- 10-APR-2016 --- Traffic on server 10.10.10.6.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Main Toolbar
Filter Toolbar
Wireless Toolbar
Status Bar
Packet List
Packet Details
Packet Bytes
Time Display Format
Name Resolution
Zoom
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Colorize Packet List
Coloring Rules...
Colorize Conversation
Resize Columns Ctrl+Shift+R
Internals
Show Packet in New Window
Reload Ctrl+R
Destination Protocol Length Info
Broadcast ARP 60 Who has 10
10.10.10.6 TCP 64 49212 → 44
10.10.10.153 TCP 55 [TCP Keep-
10.10.10.6 TCP 66 [TCP Keep-
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
0000 ff ff ff ff ff ff 00 00 00
0010 00 3c 00 00 00 00 ff 11 33
0020 dc 02 1f b4 1f b4 00 28 24

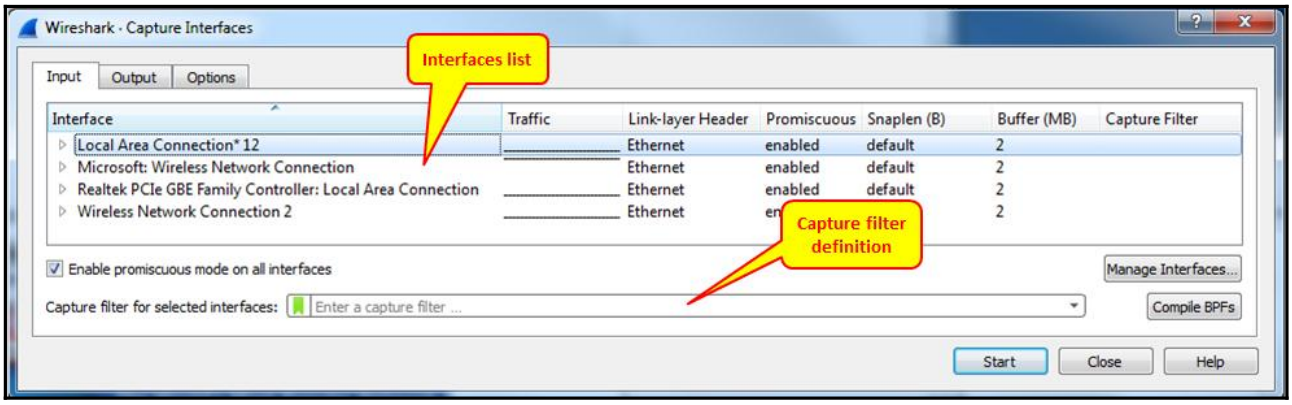

(100.0%) · Load time: 0:1.490
Profile: Default
Default
Classic
IP Telephony
MPLS
New
Performance
Wireless
Bluetooth

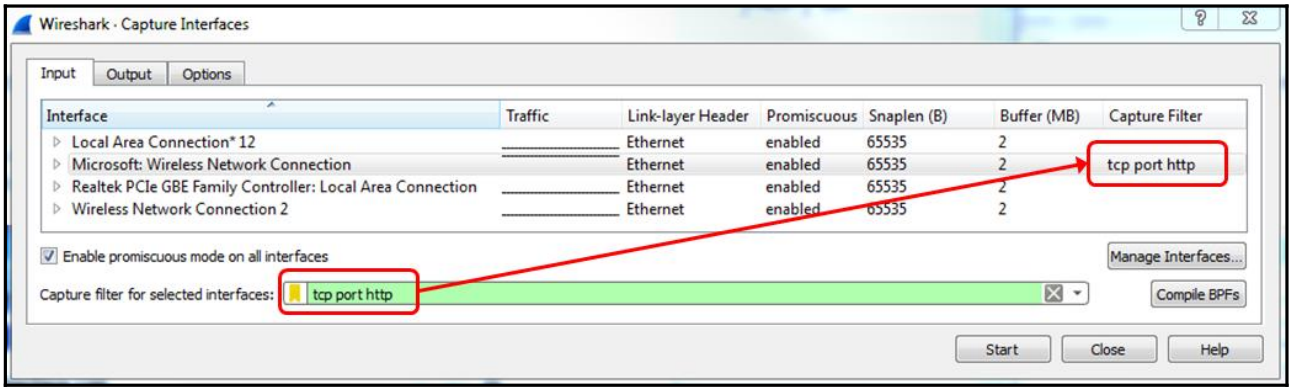

Wireshark · Configuration Profiles
Default
Classic
IP Telephony
MPLS
New
Performance
Wireless
Bluetooth
Classic
C:\Users\yoram\AppData\Roaming\Wireshark\
OK
Cancel
Help

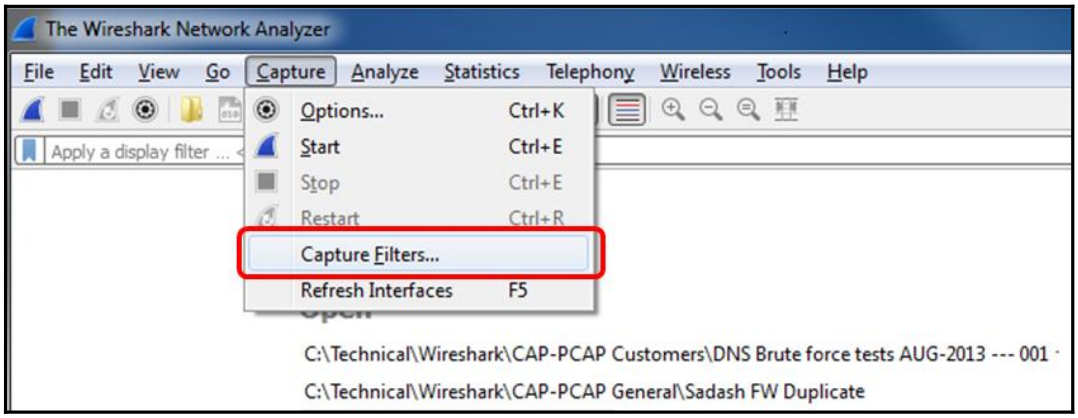

yoram ▸ AppData ▸ Roaming ▸ Wireshark ▸ profiles ▸
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Google Drive
Videos
Libraries
Documents
Music
Name
Date modified
Type
Bluetooth
16/04/2016 16:14
File folder
Classic
19/05/2014 11:53
File folder
IP Telephony
22/10/2012 16:36
File folder
MPLS
Performance
TCP Performance
Wireless
yoram ▸ AppData ▸ Roaming ▸ Wireshark ▸ profiles ▸ Wireless
Organize
Include in library
Share with
Burn
New folder
Favorites
Desktop
Downloads
Google Drive
Videos
Libraries
Documents
Name
Date modified
cfilters
01/10/2013 20:36
colorfilters
24/08/2013 18:23
custom_http_header_fields
07/07/2013 14:10
preferences
29/09/2013 09:35
01/10/2013 20:44

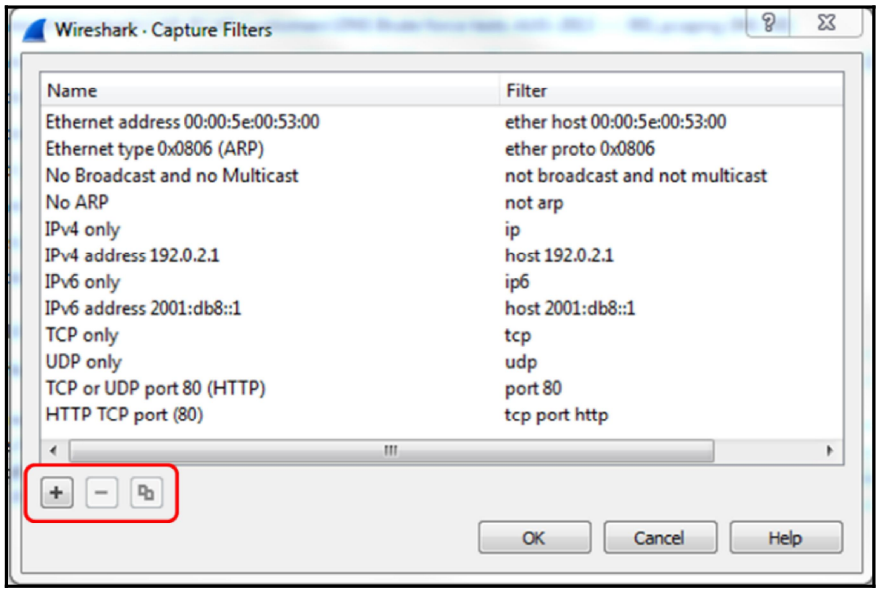
Chapter 3: Using Capture Filters

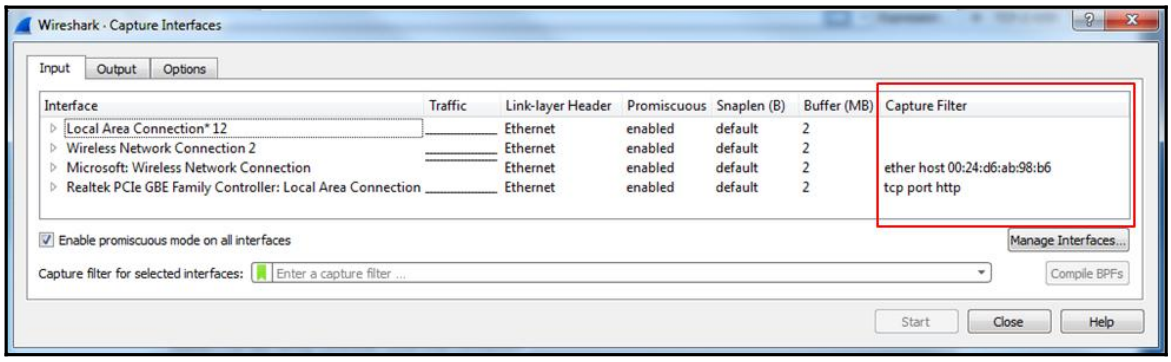


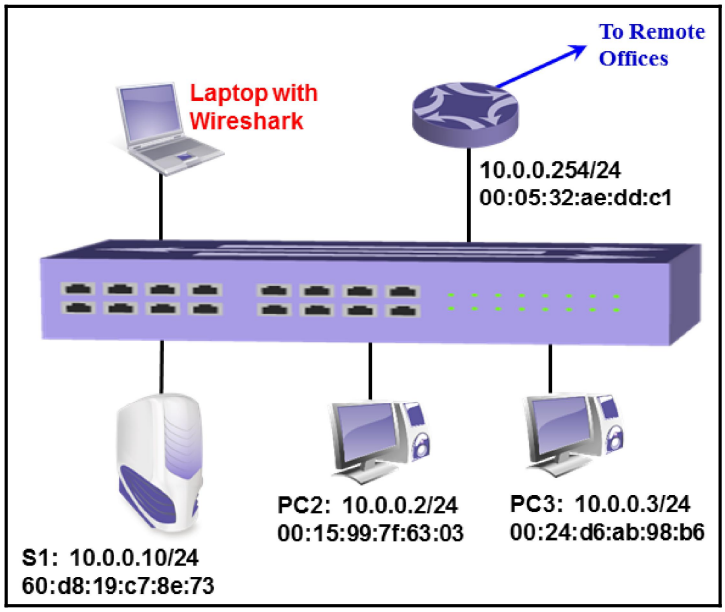


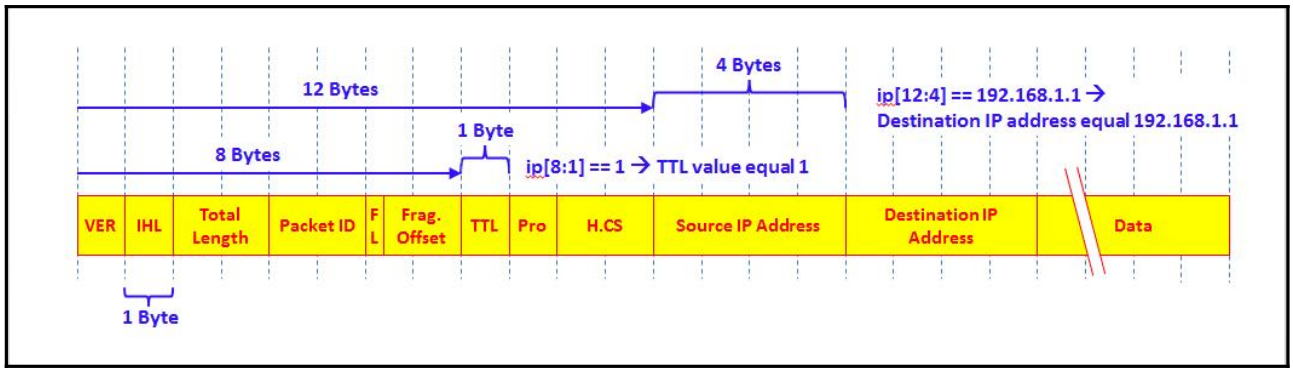


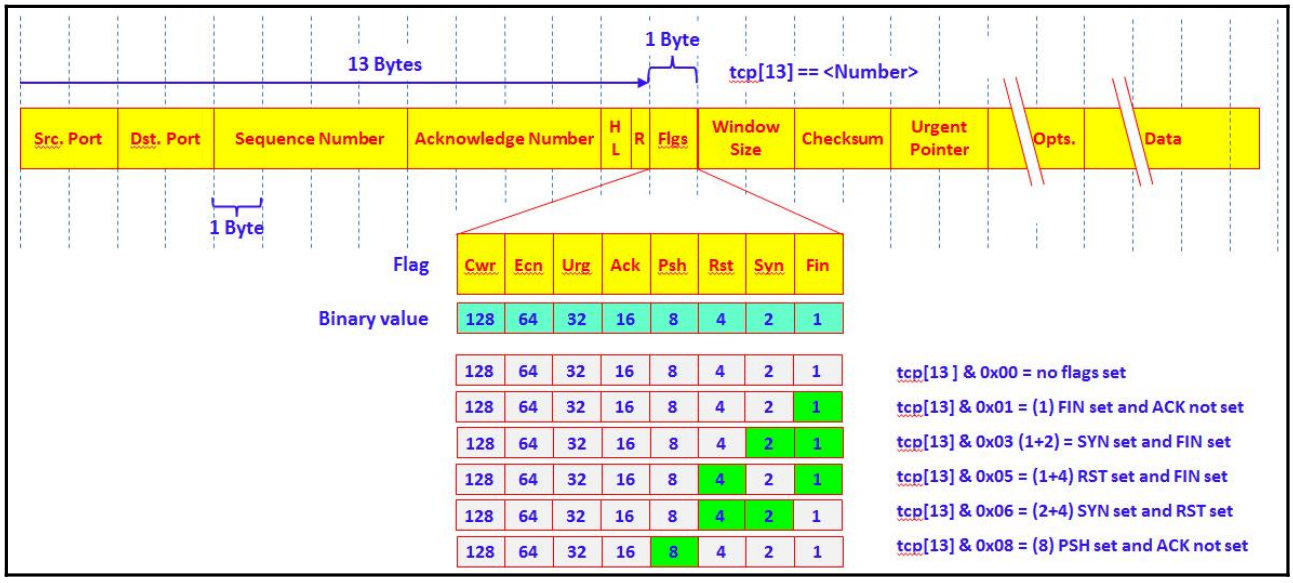

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Refresh Interfaces F5
Apply a display filter ...
C:\Technical\Wireshark\CAP-PCAP Customers\DNS Brute force tests AUG-2013 --- 001
C:\Technical\Wireshark\CAP-PCAP General\Sadash FW Duplicate

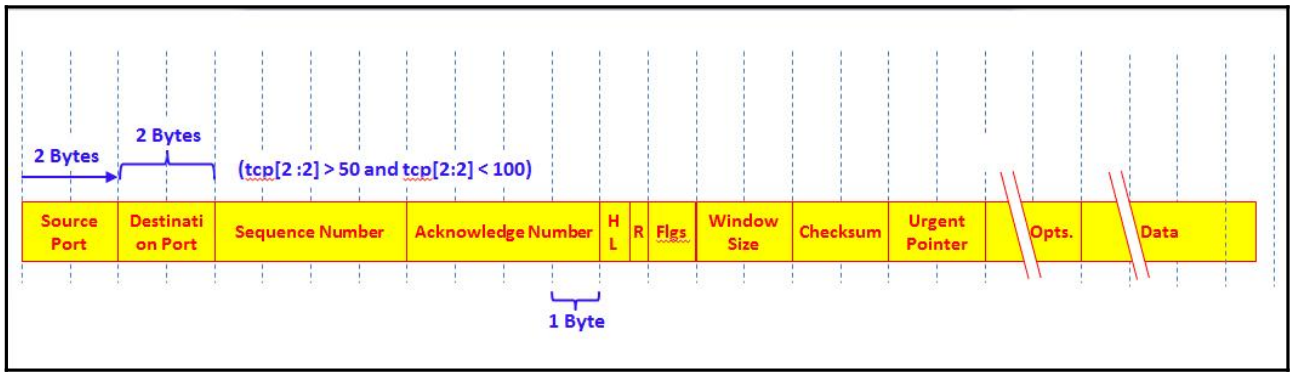

Wireshark · Capture Filters
Name
Filter
Ethernet address 00:00:5e:00:53:00
ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
ether proto 0x0806
No Broadcast and no Multicast
not broadcast and not multicast
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
host 192.0.2.1
IPv6 only
ip6
IPv6 address 2001:db8::1
host 2001:db8::1
TCP only
tcp
UDP only
udp
TCP or UDP port 80 (HTTP)
port 80
HTTP TCP port (80)
tcp port http
OK
Cancel
Help

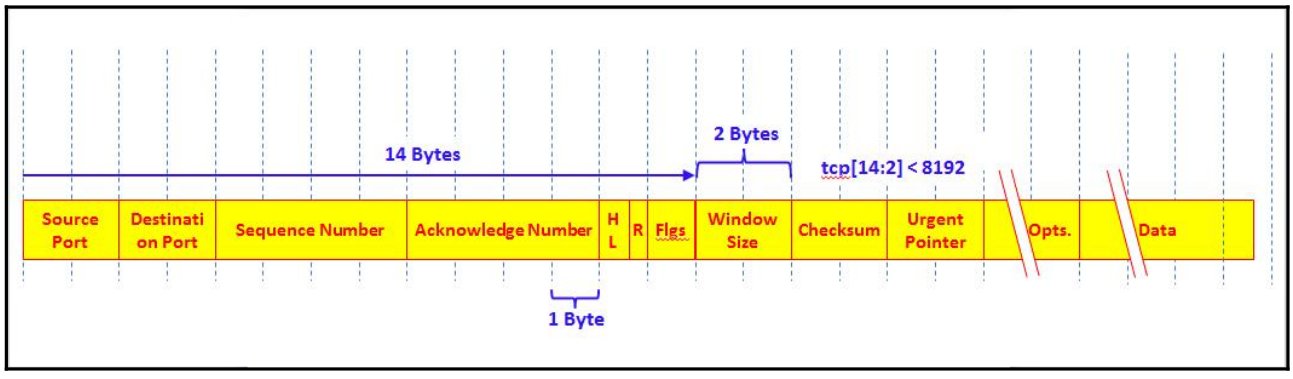

Wireshark · Capture Interfaces
Input
Output
Options
Interface
Traffic
Link-layer Header
Promiscuous
Snaplen (B)
Buffer (MB)
Capture Filter
Local Area Connection* 12
Ethernet
enabled
default
2
Wireless Network Connection 2
Ethernet
enabled
default
2
Microsoft: Wireless Network Connection
Ethernet
enabled
default
2
ether host 00:24:d6:ab:98:b6
Realtek PCIe GBE Family Controller: Local Area Connection
Ethernet
enabled
default
2
tcp port http
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces:
Enter a capture filter ...
Compile BPFs
Start
Close
Help


To Remote Offices
Laptop with Wireshark
10.0.0.254/24
00:05:32:ae:dd:c1
PC2: 10.0.0.2/24
00:15:99:7f:63:03
PC3: 10.0.0.3/24
00:24:d6:ab:98:b6
S1: 10.0.0.10/24
60:d8:19:c7:8e:73

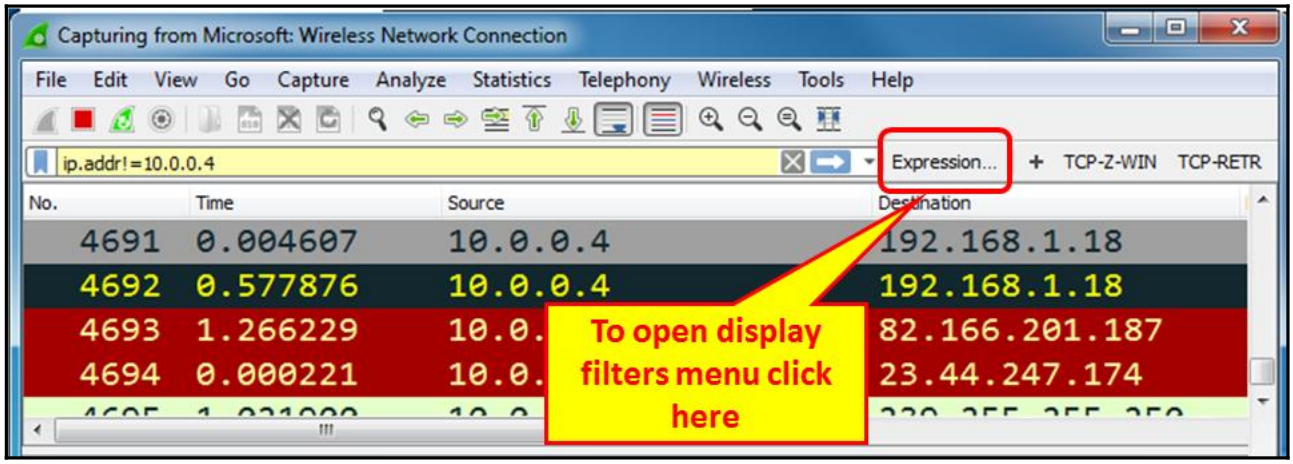

12 Bytes
4 Bytes
ip[12:4] == 192.168.1.1
Destination IP address equal 192.168.1.1
1 Byte
8 Bytes
ip[8:1] == 1 → TTL value equal 1
VER
IHL
Total Length
Packet ID
F L
Frag. Offset
TTL
Pro
H.CS
Source IP Address
Destination IP Address
Data
1 Byte

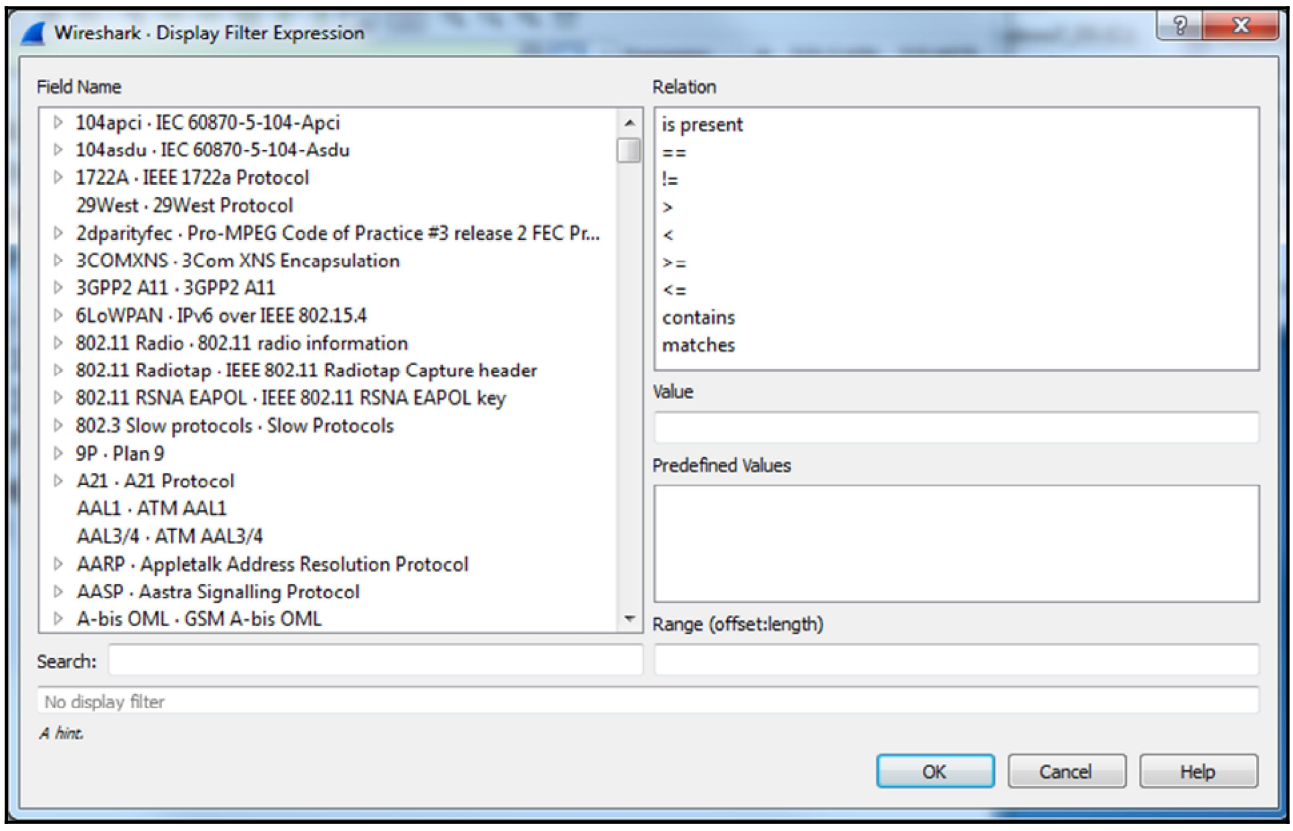

13 Bytes
1 Byte
tcp[13] == <Number>
Src. Port
Dst. Port
Sequence Number
Acknowledge Number
H L
R
Flgs
Window Size
Checksum
Urgent Pointer
Opts.
Data
1 Byte
Flag
Cwr Ecn Urg Ack Psh Rst Syn Fin
Binary value
128 64 32 16 8 4 2 1
tcp[13] & 0x00 = no flags set
tcp[13] & 0x01 = (1) FIN set and ACK not set
tcp[13] & 0x03 (1+2) = SYN set and FIN set
tcp[13] & 0x05 = (1+4) RST set and FIN set
tcp[13] & 0x06 = (2+4) SYN set and RST set
tcp[13] & 0x08 = (8) PSH set and ACK not set

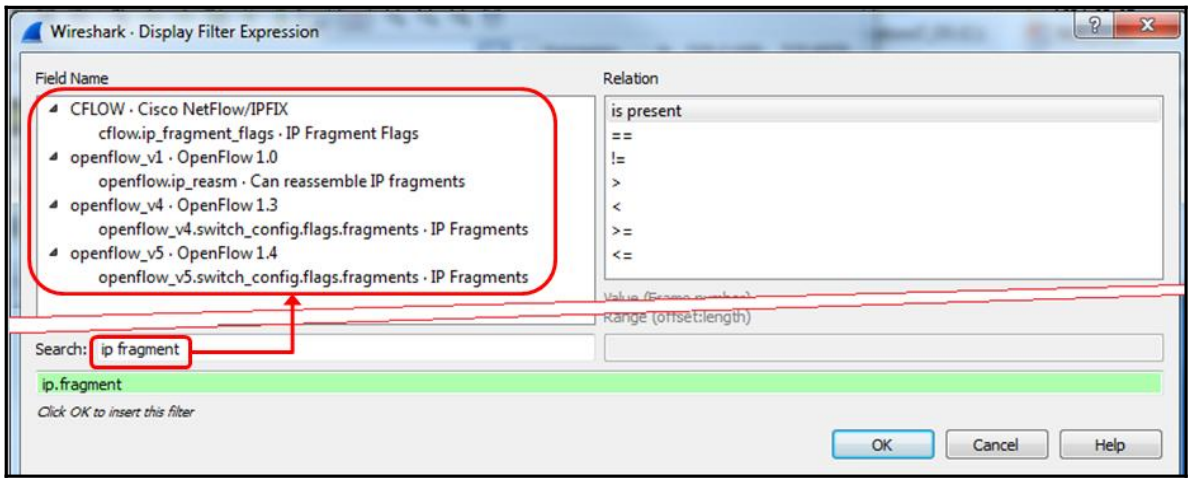

2 Bytes
2 Bytes
(tcp[2 :2] > 50 and tcp[2:2] < 100)
Source Port
Destinati on Port
Sequence Number
Acknowledge Number
H L
R
Flgs
Window Size
Checksum
Urgent Pointer
Opts.
Data
1 Byte

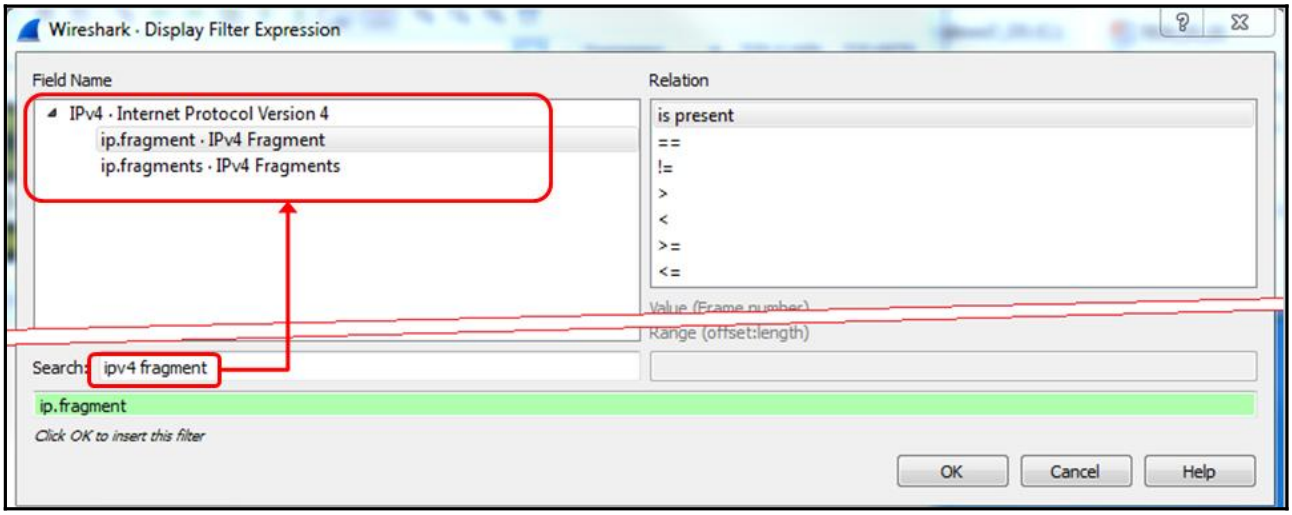

14 Bytes
2 Bytes
tcp[14:2] < 8192
Source Port
Destinati on Port
Sequence Number
Acknowledge Number
H L
R
Flgs
Window Size
Checksum
Urgent Pointer
Opts.
Data
1 Byte

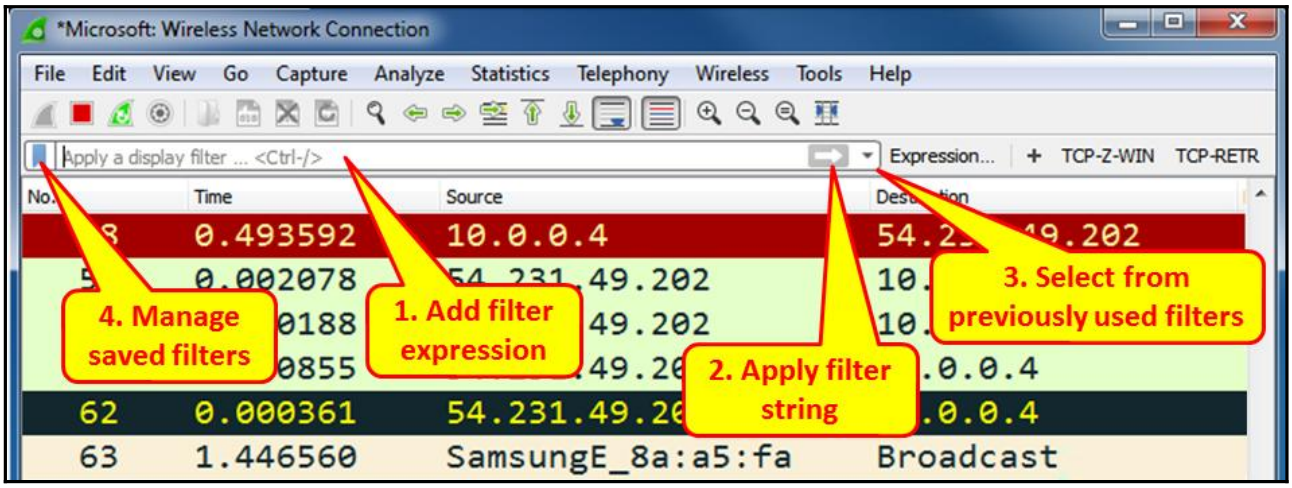
Chapter 4: Using Display Filters

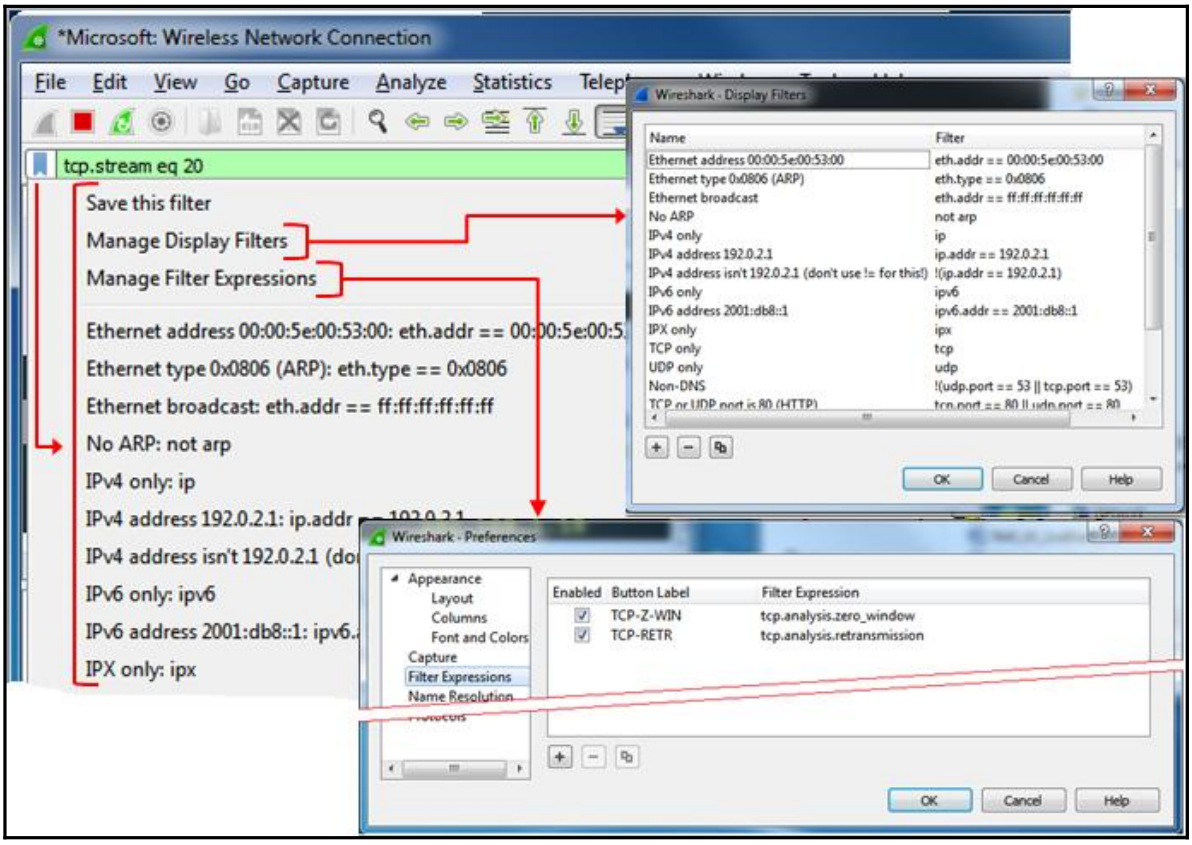


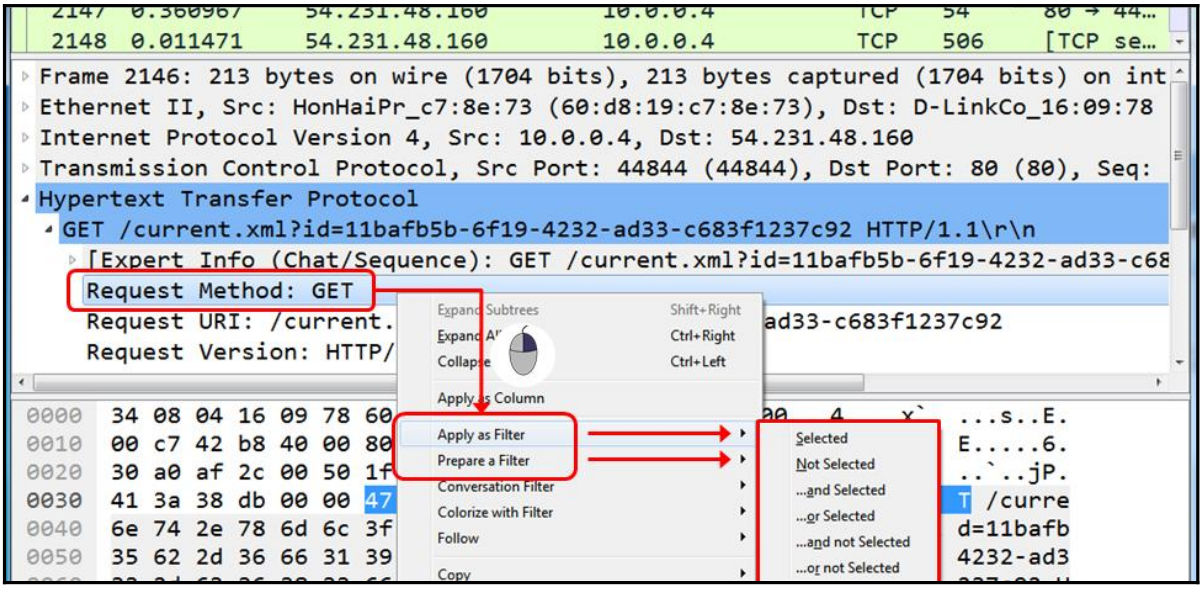


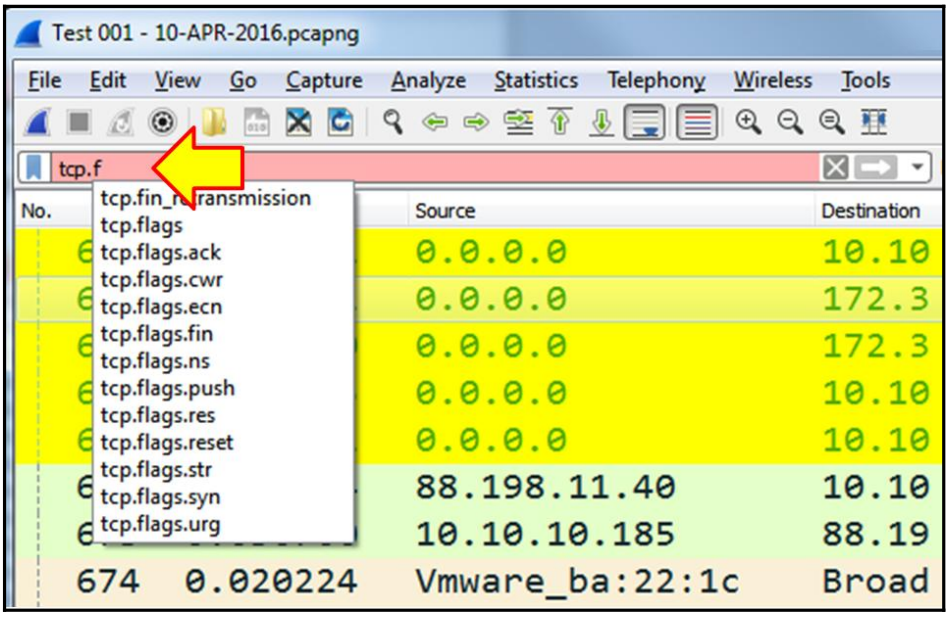

Wireshark · Display Filter Expression
Field Name
Relation
CFLOW · Cisco NetFlow/IPFIX
cflow.ip_fragment_flags · IP Fragment Flags
openflow_v1 · OpenFlow 1.0
openflow.ip_reasm · Can reassemble IP fragments
openflow_v4 · OpenFlow 1.3
openflow_v4.switch_config.flags.fragments · IP Fragments
openflow_v5 · OpenFlow 1.4
openflow_v5.switch_config.flags.fragments · IP Fragments
is present
==
!=
>
<
>=
<=
Range (offset:length)
Search: ip fragment
ip.fragment
Click OK to insert this filter
OK
Cancel
Help

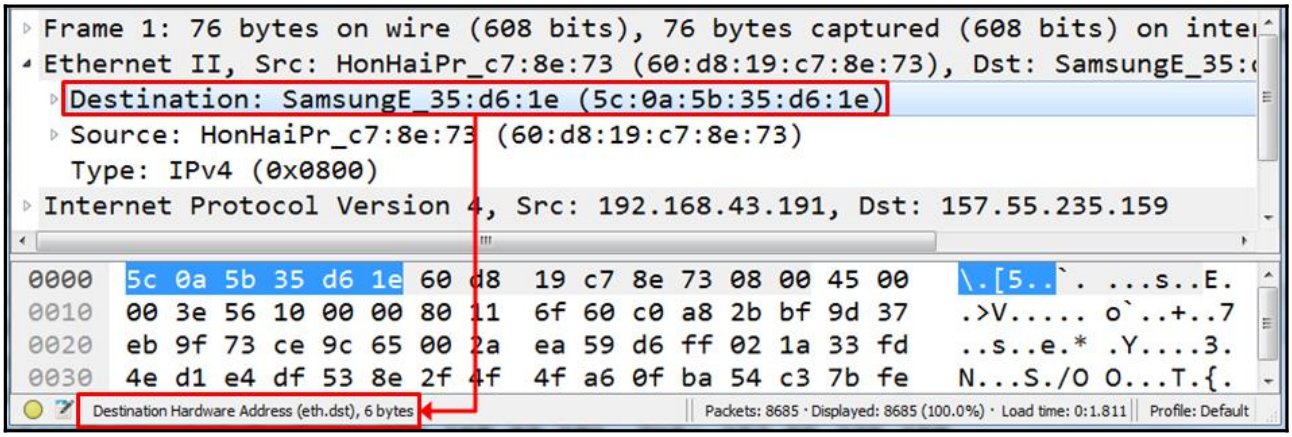

Wireshark · Display Filter Expression
Field Name
Relation
IPv4 · Internet Protocol Version 4
ip.fragment · IPv4 Fragment
ip.fragments · IPv4 Fragments
is present
==
!=
>
<
>=
<=
Range (offset:length)
Search: ipv4 fragment
ip.fragment
Click OK to insert this filter
OK
Cancel
Help

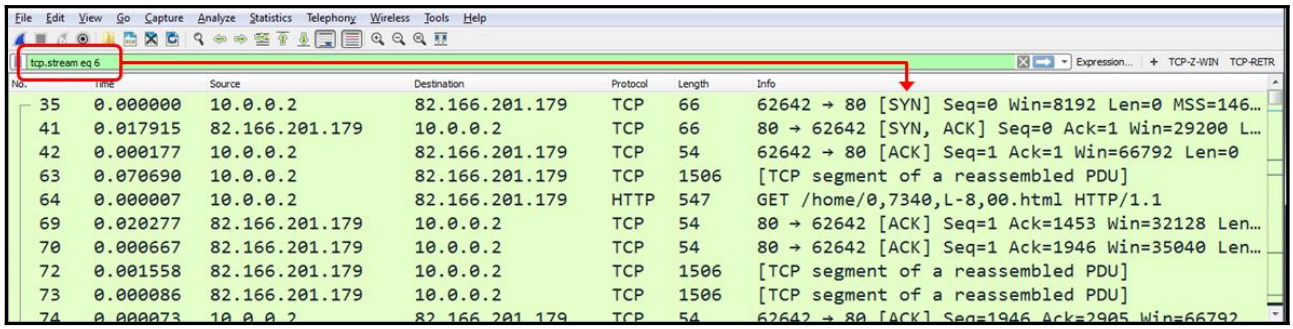

*Microsoft: Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
TCP-Z-WIN
TCP-RETR
No.
Time
Source
0.493592
10.0.0.4
0.002078
62
0.000361
63
1.446560
SamsungE_8a:a5:fa
Broadcast
4. Manage saved filters
1. Add filter expression
2. Apply filter string
3. Select from previously used filters

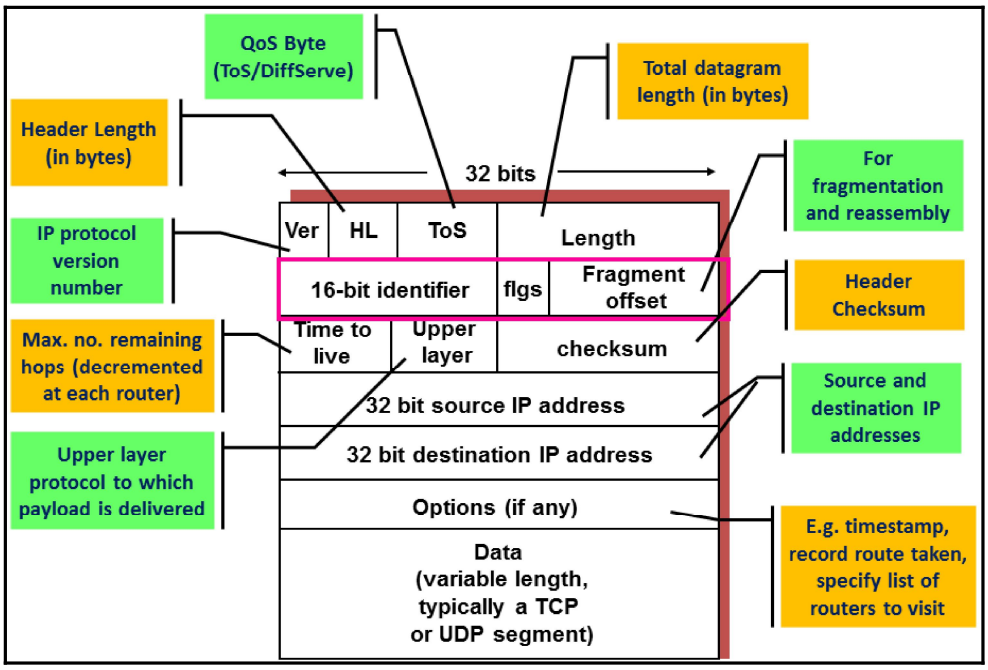

*Microsoft: Wireless Network Connection
File Edit View Go Capture Analyze Statistics
tcp.stream eq 20
Save this filter
Manage Display Filters
Manage Filter Expressions
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:5
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
No ARP: not arp
IPv4 only: ip
IPv4 address 192.0.2.1: ip.addr
IPv4 address isn't 192.0.2.1 (do
IPv6 only: ipv6
IPv6 address 2001:db8::1: ipv6.
IPX only: ipx
Wireshark - Display Filters
Name
Filter
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)
OK
Cancel
Help
Wireshark - Preferences
Appearance
Layout
Columns
Font and Colors
Capture
Filter Expressions
Name Resolution
Enabled
Button Label
Filter Expression
TCP-Z-WIN
tcp.analysis.zero_window
TCP-RETR
tcp.analysis.retransmission
OK
Cancel
Help

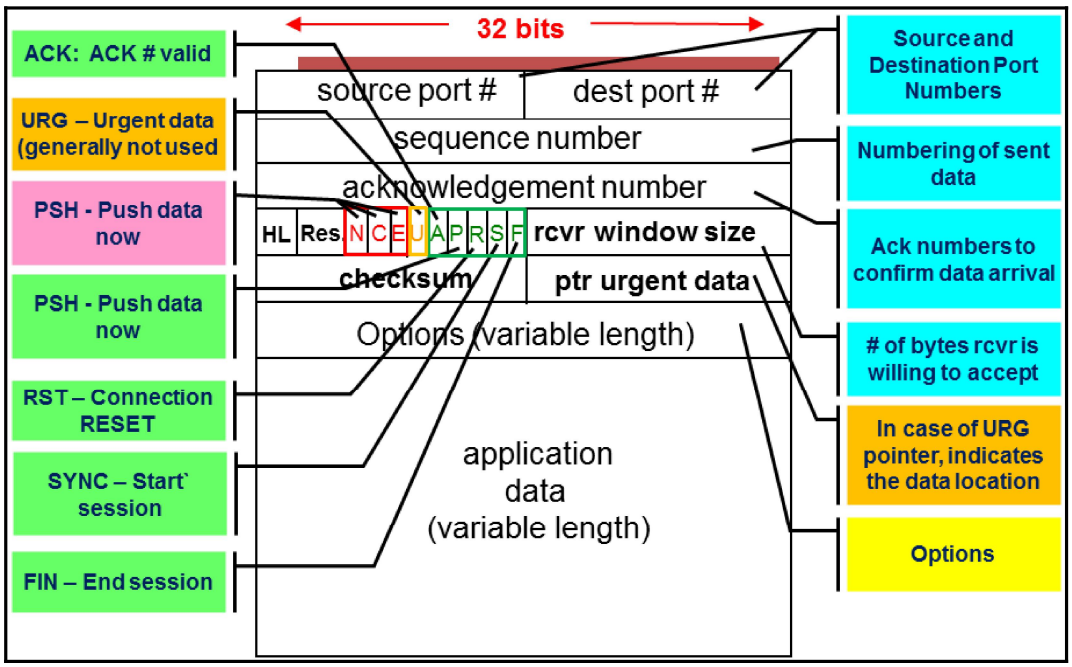

2148 0.011471 54.231.48.160 10.0.0.4 TCP 506 [TCP se…
Frame 2146: 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits) on int
Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: D-LinkCo_16:09:78
Internet Protocol Version 4, Src: 10.0.0.4, Dst: 54.231.48.160
Transmission Control Protocol, Src Port: 44844 (44844), Dst Port: 80 (80), Seq:
Hypertext Transfer Protocol
GET /current.xml?id=11bafb5b-6f19-4232-ad33-c683f1237c92 HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET /current.xml?id=11bafb5b-6f19-4232-ad33-c68
Request Method: GET
Request URI: /current.
Request Version: HTTP/
ad33-c683f1237c92
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse Ctrl+Left
Apply as Column
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
0000 34 08 04 16 09 78 60
0010 00 c7 42 b8 40 00 80
0020 30 a0 af 2c 00 50 1f
0030 41 3a 38 db 00 00 47
0040 6e 74 2e 78 6d 6c 3f
0050 35 62 2d 36 66 31 39
...s..E.
E.....6.
..`..jP.
T /curre
d=11bafb
4232-ad3

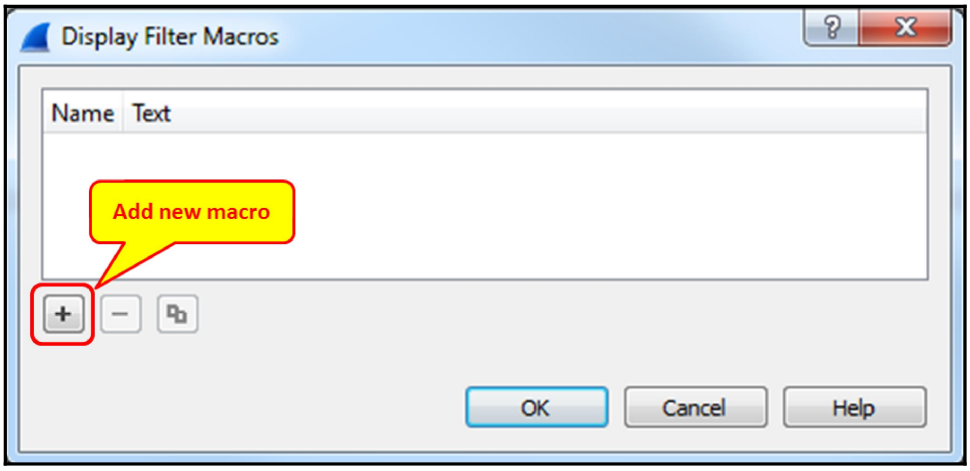

Test 001 - 10-APR-2016.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
tcp.f
tcp.fin_retransmission
tcp.flags
tcp.flags.ack
tcp.flags.cwr
tcp.flags.ecn
tcp.flags.fin
tcp.flags.ns
tcp.flags.push
tcp.flags.res
tcp.flags.reset
tcp.flags.str
tcp.flags.syn
tcp.flags.urg
No.
Source
Destination
0.0.0.0
10.10
0.0.0.0
172.3
0.0.0.0
172.3
0.0.0.0
10.10
0.0.0.0
10.10
88.198.11.40
10.10
10.10.10.185
88.19
674 0.020224
Vmware_ba:22:1c
Broad


Frame 1: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on inte
Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: SamsungE_35:
Destination: SamsungE_35:d6:1e (5c:0a:5b:35:d6:1e)
Source: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 192.168.43.191, Dst: 157.55.235.159
0000 5c 0a 5b 35 d6 1e 60 d8 19 c7 8e 73 08 00 45 00 \.[5..`. ...s..E.
0010 00 3e 56 10 00 00 80 11 6f 60 c0 a8 2b bf 9d 37 .>V..... o`..+..7
0020 eb 9f 73 ce 9c 65 00 2a ea 59 d6 ff 02 1a 33 fd ..s..e.* .Y....3.
0030 4e d1 e4 df 53 8e 2f 4f 4f a6 0f ba 54 c3 7b fe N...S./O O...T.{.
Destination Hardware Address (eth.dst), 6 bytes
Packets: 8685 · Displayed: 8685 (100.0%) · Load time: 0:1.811
Profile: Default

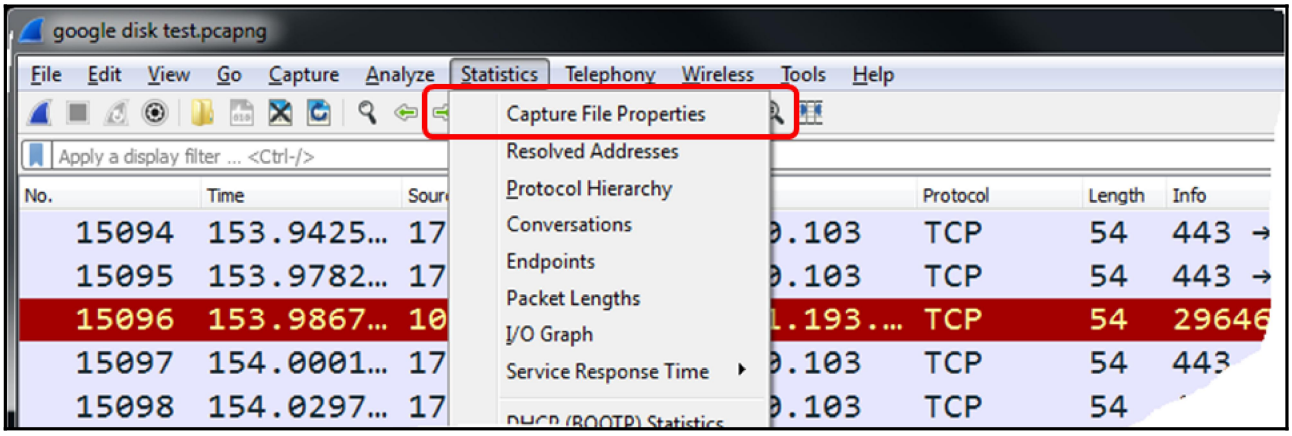

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 6
No. Time Source Destination Protocol Length Info
35 0.000000 10.0.0.2 82.166.201.179 TCP 66 62642 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146…
41 0.017915 82.166.201.179 10.0.0.2 TCP 66 80 → 62642 [SYN, ACK] Seq=0 Ack=1 Win=29200 L…
42 0.000177 10.0.0.2 82.166.201.179 TCP 54 62642 → 80 [ACK] Seq=1 Ack=1 Win=66792 Len=0
63 0.070690 10.0.0.2 82.166.201.179 TCP 1506 [TCP segment of a reassembled PDU]
64 0.000007 10.0.0.2 82.166.201.179 HTTP 547 GET /home/0,7340,L-8,00.html HTTP/1.1
69 0.020277 82.166.201.179 10.0.0.2 TCP 54 80 → 62642 [ACK] Seq=1 Ack=1453 Win=32128 Len…
70 0.000667 82.166.201.179 10.0.0.2 TCP 54 80 → 62642 [ACK] Seq=1 Ack=1946 Win=35040 Len…
72 0.001558 82.166.201.179 10.0.0.2 TCP 1506 [TCP segment of a reassembled PDU]
73 0.000086 82.166.201.179 10.0.0.2 TCP 1506 [TCP segment of a reassembled PDU]

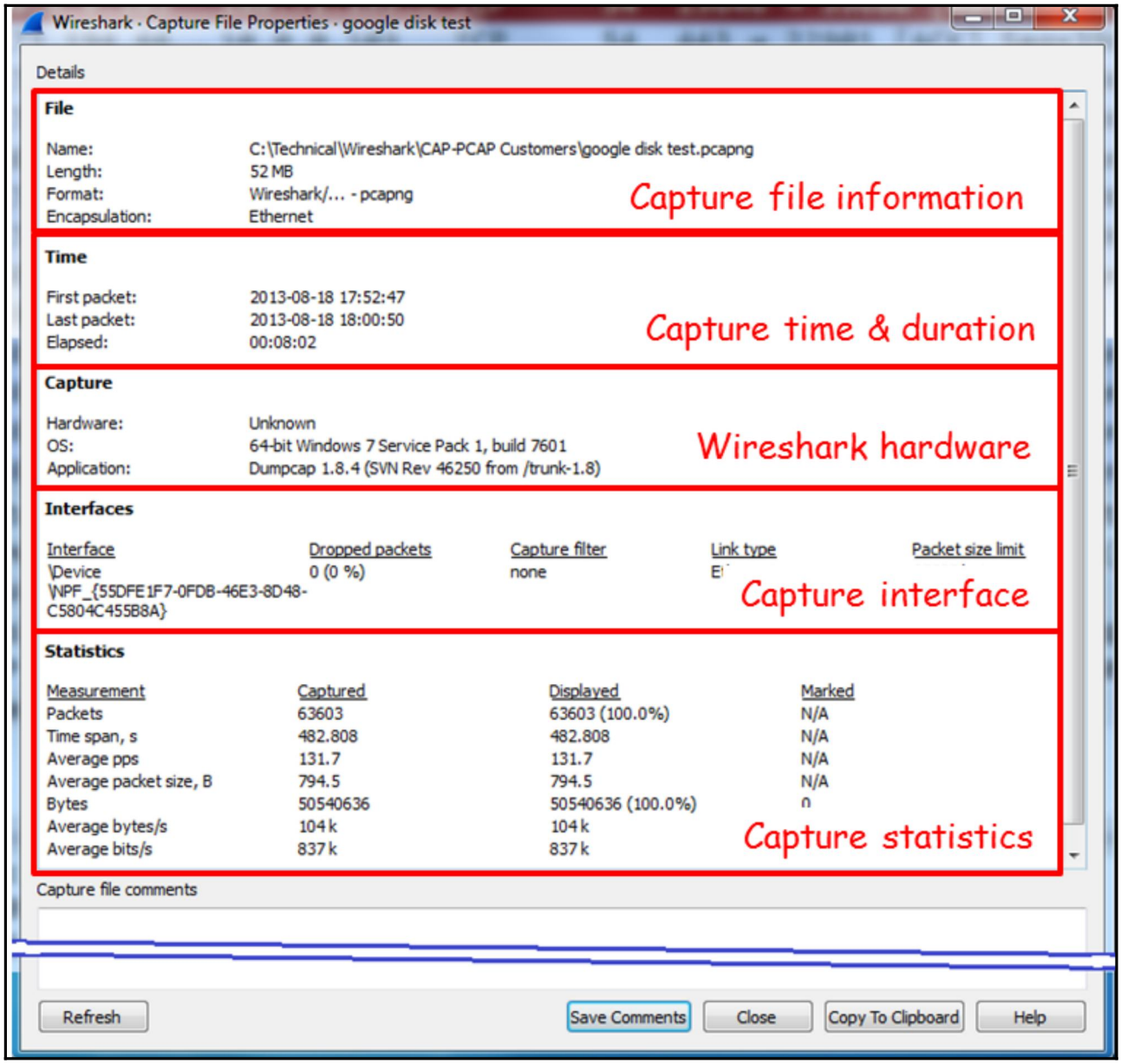

QoS Byte (ToS/DiffServe)
Total datagram length (in bytes)
Header Length (in bytes)
32 bits
For fragmentation and reassembly
IP protocol version number
Ver
HL
ToS
Length
16-bit identifier
flgs
Fragment offset
Header Checksum
Max. no. remaining hops (decremented at each router)
Time to live
Upper layer
checksum
Source and destination IP addresses
32 bit source IP address
Upper layer protocol to which payload is delivered
32 bit destination IP address
Options (if any)
E.g. timestamp, record route taken, specify list of routers to visit
Data (variable length, typically a TCP or UDP segment)

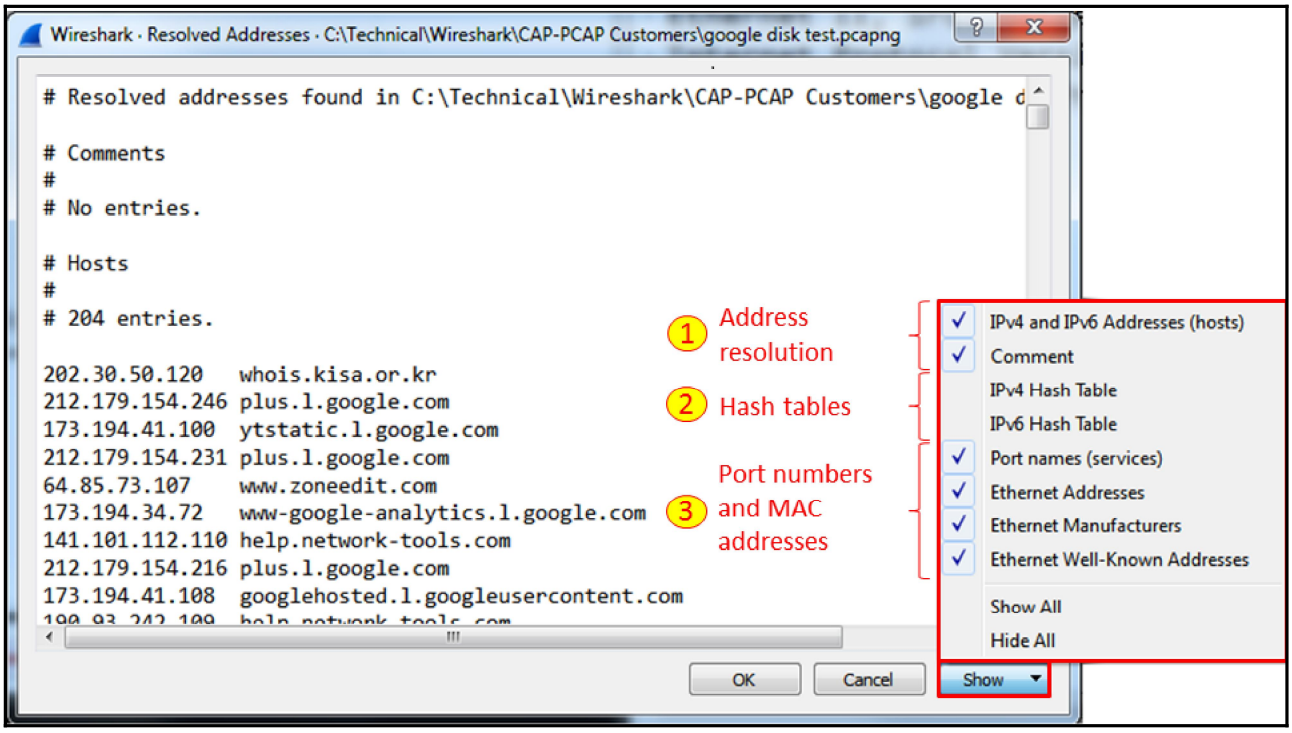

32 bits
ACK: ACK # valid
source port #
dest port #
Source and Destination Port Numbers
URG – Urgent data (generally not used
sequence number
Numbering of sent data
acknowledgement number
PSH - Push data now
HL
Res
N C E U A P R S F
rcvr window size
Ack numbers to confirm data arrival
checksum
ptr urgent data
PSH - Push data now
Options (variable length)
# of bytes rcvr is willing to accept
RST – Connection RESET
In case of URG pointer, indicates the data location
SYNC – Start` session
application data (variable length)
Options
FIN – End session

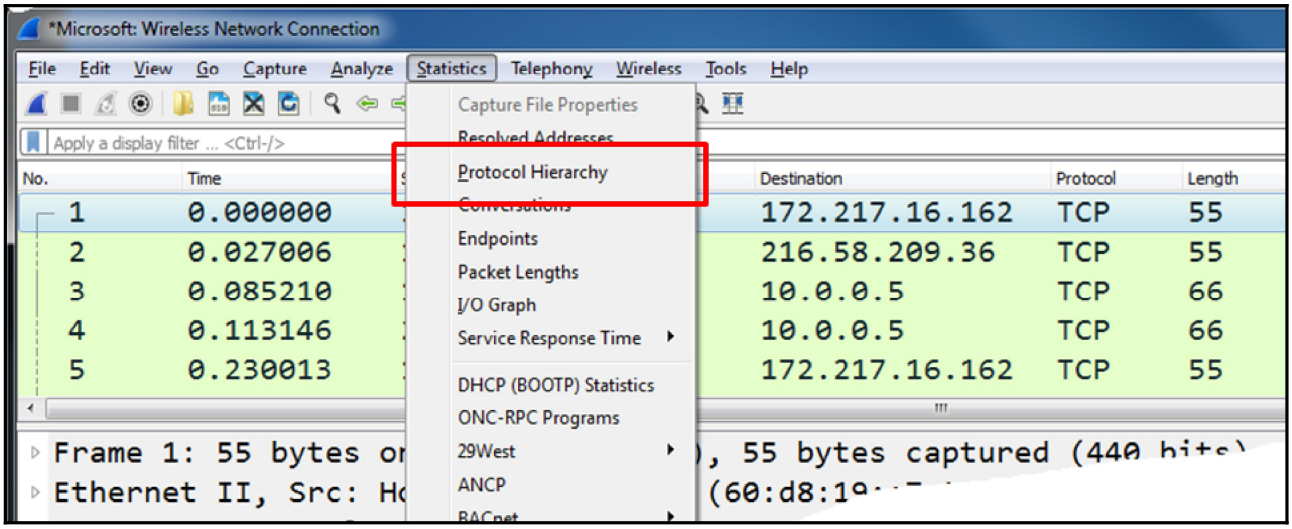

Display Filter Macros
Name
Text
Add new macro
OK
Cancel
Help

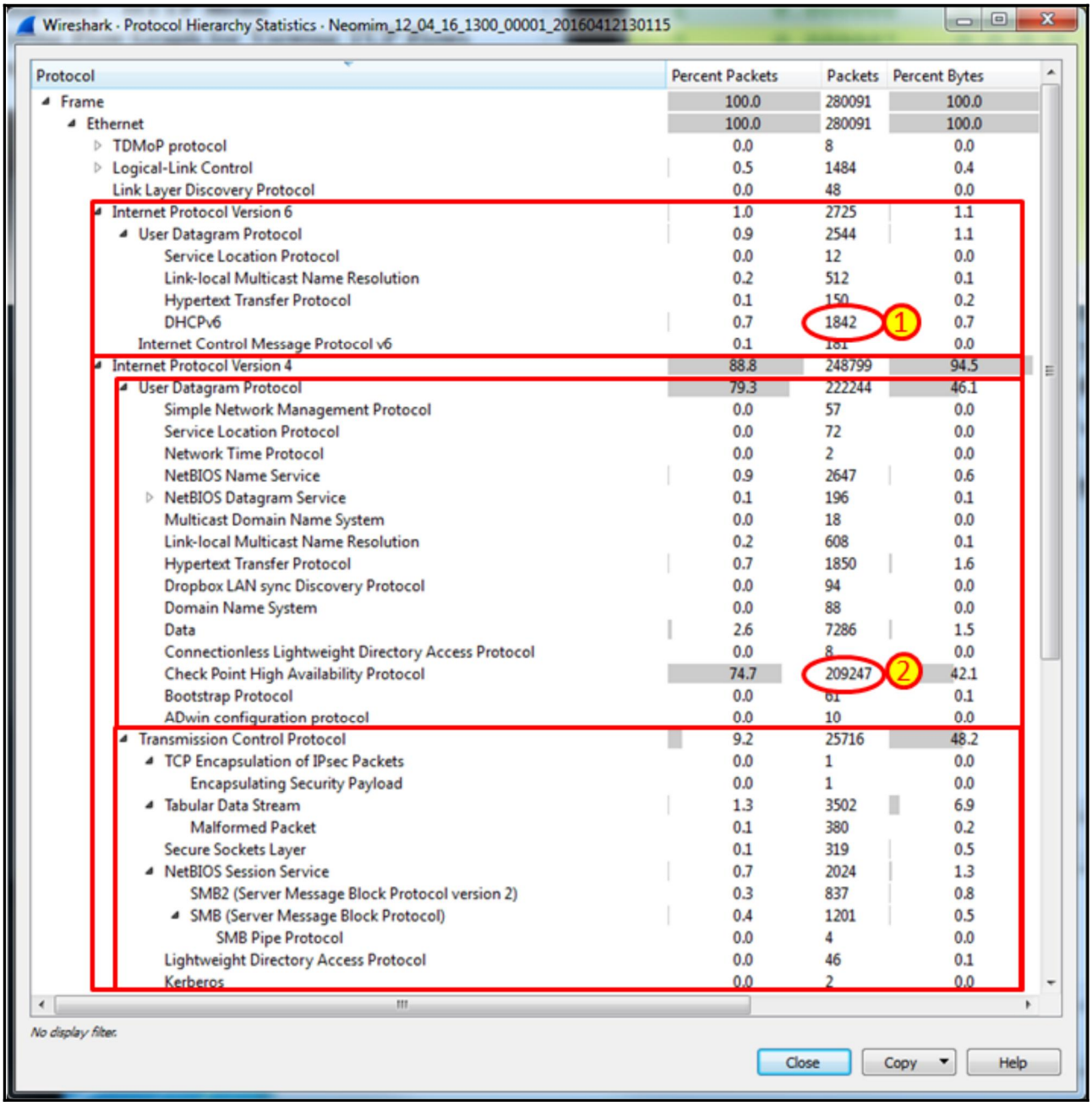
Chapter 5: Using Basic Statistics Tools

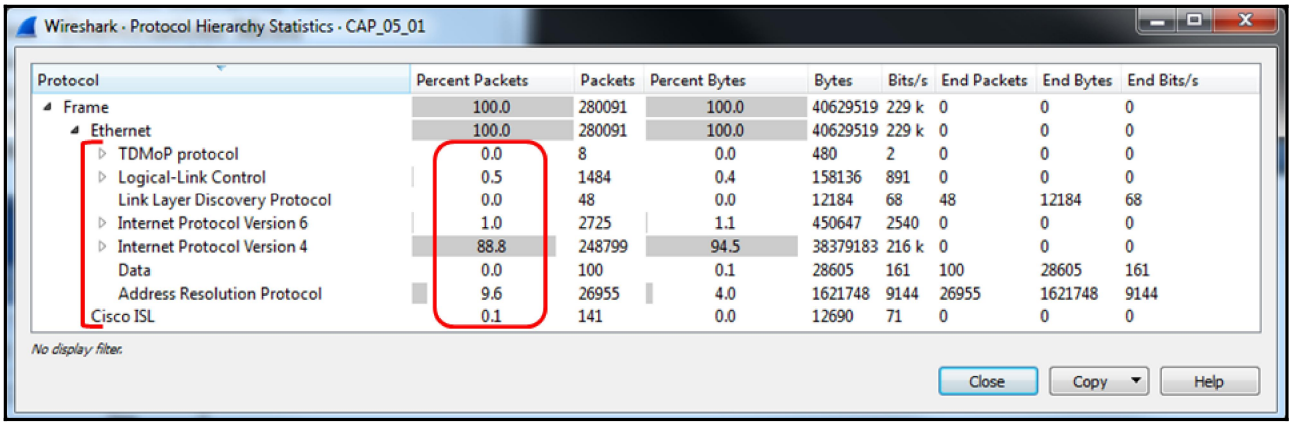


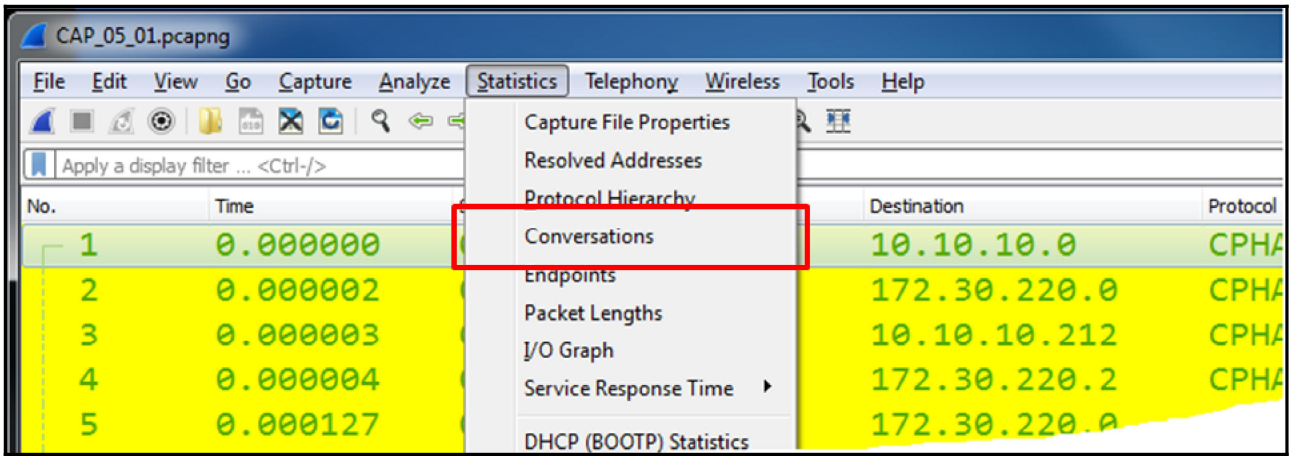

Wireshark · Capture File Properties · google disk test
Details
File
Name: C:\Technical\Wireshark\CAP-PCAP Customers\google disk test.pcapng
Length: 52 MB
Format: Wireshark/... - pcapng
Encapsulation: Ethernet
Capture file information
Time
First packet: 2013-08-18 17:52:47
Last packet: 2013-08-18 18:00:50
Elapsed: 00:08:02
Capture time & duration
Capture
Hardware: Unknown
OS: 64-bit Windows 7 Service Pack 1, build 7601
Application: Dumpcap 1.8.4 (SVN Rev 46250 from /trunk-1.8)
Wireshark hardware
Interfaces
Interface
Dropped packets
Capture filter
Link type
Packet size limit
\Device\NPF_{55DFE1F7-0FDB-46E3-8D48-C5804C455B8A}
0 (0 %)
none
Capture interface
Statistics
Measurement
Captured
Displayed
Marked
Packets 63603 63603 (100.0%) N/A
Time span, s 482.808 482.808 N/A
Average pps 131.7 131.7 N/A
Average packet size, B 794.5 794.5 N/A
Bytes 50540636 50540636 (100.0%) 0
Average bytes/s 104 k 104 k
Average bits/s 837 k 837 k
Capture statistics
Capture file comments
Refresh
Save Comments
Close
Copy To Clipboard
Help

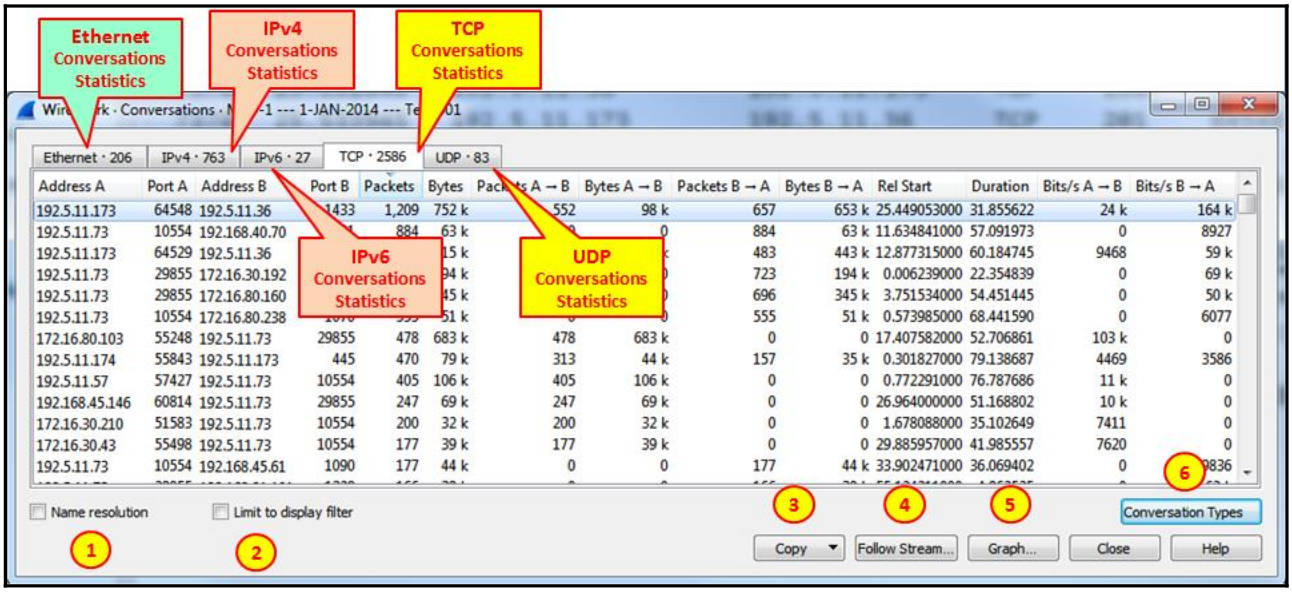

Wireshark · Resolved Addresses · C:\Technical\Wireshark\CAP-PCAP Customers\google disk test.pcapng
Resolved addresses found in C:\Technical\Wireshark\CAP-PCAP Customers\google d
Comments
#
No entries.
Hosts
#
204 entries.
202.30.50.120 whois.kisa.or.kr
212.179.154.246 plus.l.google.com
173.194.41.100 ytstatic.l.google.com
212.179.154.231 plus.l.google.com
64.85.73.107 www.zoneedit.com
173.194.34.72 www-google-analytics.l.google.com
141.101.112.110 help.network-tools.com
212.179.154.216 plus.l.google.com
173.194.41.108 googlehosted.l.googleusercontent.com
1 Address resolution
2 Hash tables
3 Port numbers and MAC addresses
IPv4 and IPv6 Addresses (hosts)
Comment
IPv4 Hash Table
IPv6 Hash Table
Port names (services)
Ethernet Addresses
Ethernet Manufacturers
Ethernet Well-Known Addresses
Show All
Hide All
OK
Cancel
Show

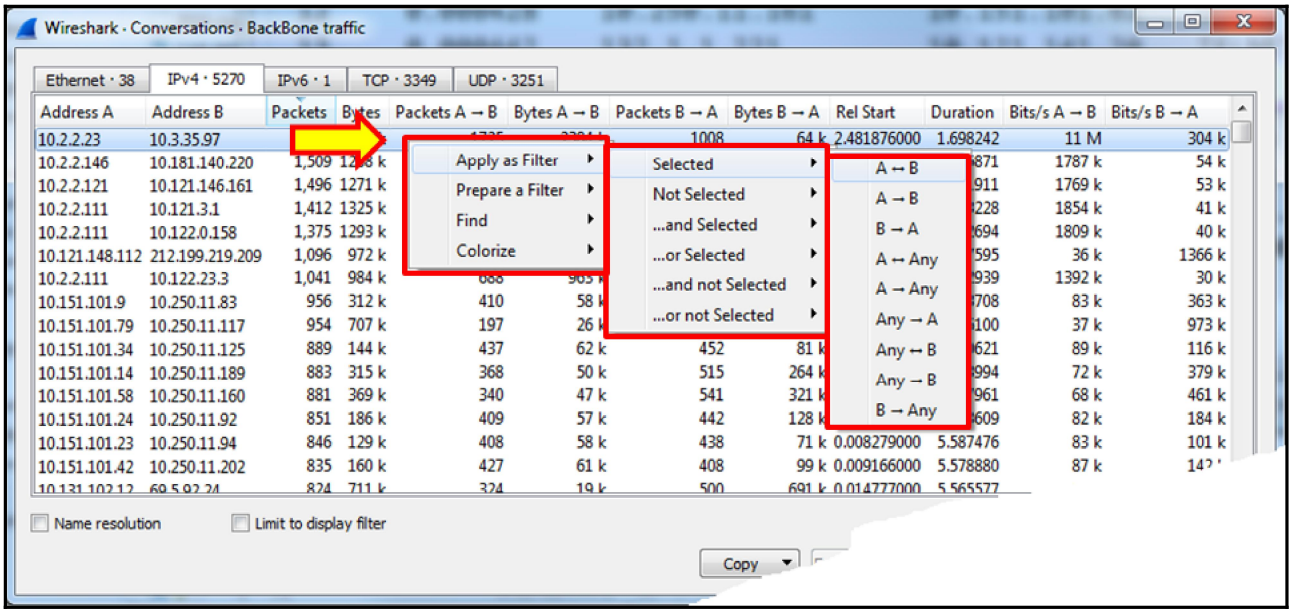

*Microsoft: Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
ONC-RPC Programs
29West
ANCP
Apply a display filter ... <Ctrl-/>
No. Time Destination Protocol Length
1 0.000000 172.217.16.162 TCP 55
2 0.027006 216.58.209.36 TCP 55
3 0.085210 10.0.0.5 TCP 66
4 0.113146 10.0.0.5 TCP 66
5 0.230013 172.217.16.162 TCP 55
Frame 1: 55 bytes
, 55 bytes captured (440
Ethernet II, Src:

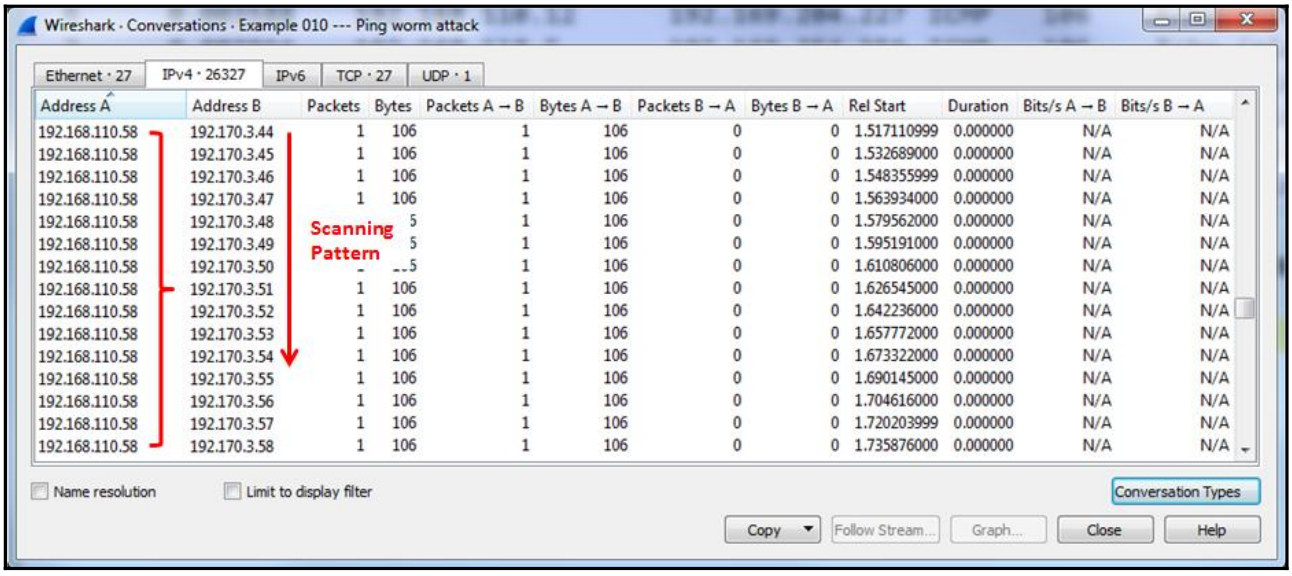

Wireshark · Protocol Hierarchy Statistics · Neomim_12_04_16_1300_00001_20160412130115
Protocol
Percent Packets
Packets
Percent Bytes
Frame 100.0 280091 100.0
Ethernet 100.0 280091 100.0
TDMoP protocol 0.0 8 0.0
Logical-Link Control 0.5 1484 0.4
Link Layer Discovery Protocol 0.0 48 0.0
Internet Protocol Version 6 1.0 2725 1.1
User Datagram Protocol 0.9 2544 1.1
Service Location Protocol 0.0 12 0.0
Link-local Multicast Name Resolution 0.2 512 0.1
Hypertext Transfer Protocol 0.1 150 0.2
DHCPv6 0.7 1842 0.7
Internet Control Message Protocol v6 0.1 181 0.0
Internet Protocol Version 4 88.8 248799 94.5
User Datagram Protocol 79.3 222244 46.1
Simple Network Management Protocol 0.0 57 0.0
Service Location Protocol 0.0 72 0.0
Network Time Protocol 0.0 2 0.0
NetBIOS Name Service 0.9 2647 0.6
NetBIOS Datagram Service 0.1 196 0.1
Multicast Domain Name System 0.0 18 0.0
Link-local Multicast Name Resolution 0.2 608 0.1
Hypertext Transfer Protocol 0.7 1850 1.6
Dropbox LAN sync Discovery Protocol 0.0 94 0.0
Domain Name System 0.0 88 0.0
Data 2.6 7286 1.5
Connectionless Lightweight Directory Access Protocol 0.0 8 0.0
Check Point High Availability Protocol 74.7 209247 42.1
Bootstrap Protocol 0.0 61 0.1
ADwin configuration protocol 0.0 10 0.0
Transmission Control Protocol 9.2 25716 48.2
TCP Encapsulation of IPsec Packets 0.0 1 0.0
Encapsulating Security Payload 0.0 1 0.0
Tabular Data Stream 1.3 3502 6.9
Malformed Packet 0.1 380 0.2
Secure Sockets Layer 0.1 319 0.5
NetBIOS Session Service 0.7 2024 1.3
SMB2 (Server Message Block Protocol version 2) 0.3 837 0.8
SMB (Server Message Block Protocol) 0.4 1201 0.5
SMB Pipe Protocol 0.0 4 0.0
Lightweight Directory Access Protocol 0.0 46 0.1
Kerberos 0.0 2 0.0
1
2
No display filter.
Close
Copy
Help

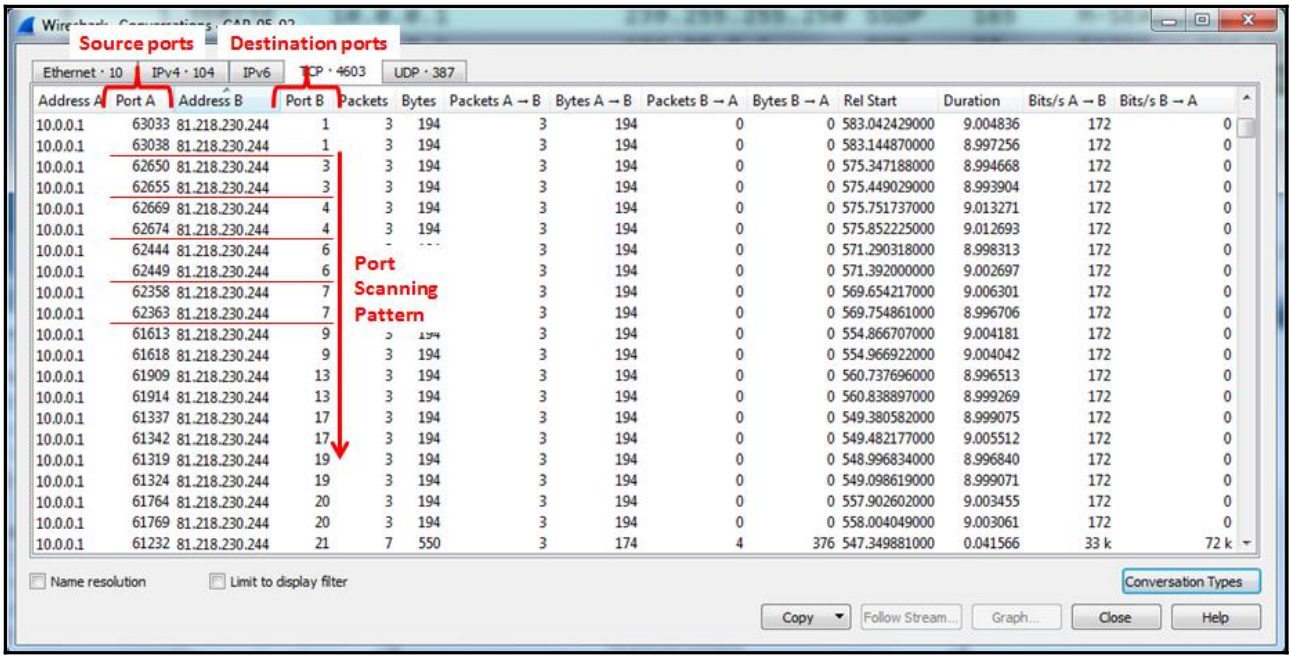

Wireshark · Protocol Hierarchy Statistics · CAP_05_01
Protocol
Percent Packets
Packets
Percent Bytes
Bytes
Bits/s
End Packets
End Bytes
End Bits/s
Frame 100.0 280091 100.0 40629519 229 k 0 0 0
Ethernet 100.0 280091 100.0 40629519 229 k 0 0 0
TDMoP protocol 0.0 8 0.0 480 2 0 0 0
Logical-Link Control 0.5 1484 0.4 158136 891 0 0 0
Link Layer Discovery Protocol 0.0 48 0.0 12184 68 48 12184 68
Internet Protocol Version 6 1.0 2725 1.1 450647 2540 0 0 0
Internet Protocol Version 4 88.8 248799 94.5 38379183 216 k 0 0 0
Data 0.0 100 0.1 28605 161 100 28605 161
Address Resolution Protocol 9.6 26955 4.0 1621748 9144 26955 1621748 9144
Cisco ISL 0.1 141 0.0 12690 71 0 0 0
No display filter.
Close
Copy
Help

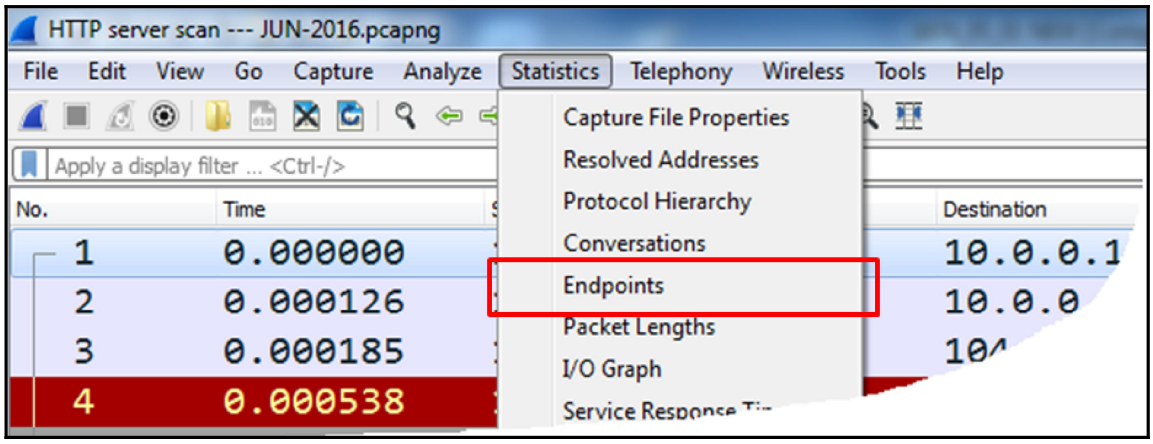

CAP_05_01.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Time
DHCP (BOOTP) Statistics
No. Time Destination Protocol
1 0.000000 10.10.10.0 CPHA
2 0.000002 172.30.220.0 CPHA
3 0.000003 10.10.10.212 CPHA
4 0.000004 172.30.220.2 CPHA
5 0.000127 172.30.220.0

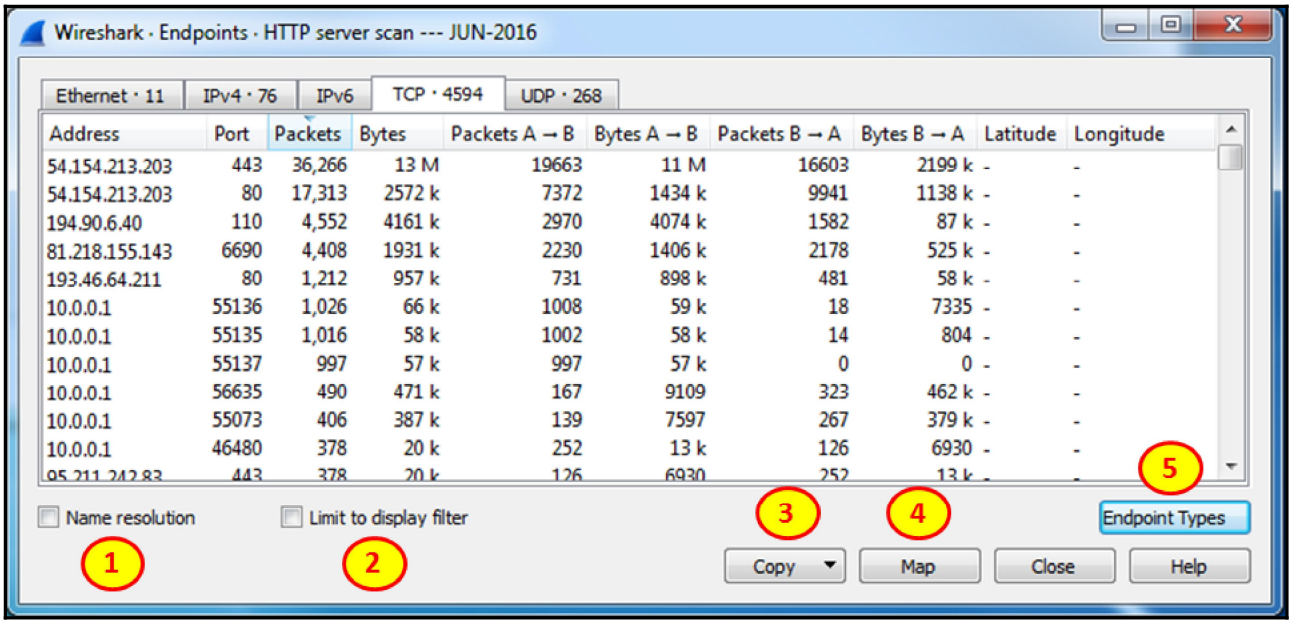

Ethernet Conversations Statistics
IPv4 Conversations Statistics
TCP Conversations Statistics
IPv6 Conversations Statistics
UDP Conversations Statistics
Ethernet · 206
IPv4 · 763
IPv6 · 27
TCP · 2586
UDP · 83
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
192.5.11.173 64548 192.5.11.36 1433 1,209 752 k 552 98 k 657 653 k 25.449053000 31.855622 24 k 164 k
192.5.11.73 10554 192.168.40.70 884 63 k 0 0 884 63 k 11.634841000 57.091973 0 8927
192.5.11.173 64529 192.5.11.36 483 443 k 12.877315000 60.184745 9468 59 k
192.5.11.73 29855 172.16.30.192 723 194 k 0.006239000 22.354839 0 69 k
192.5.11.73 29855 172.16.80.160 696 345 k 3.751534000 54.451445 0 50 k
192.5.11.73 10554 172.16.80.238 555 51 k 0.573985000 68.441590 0 6077
172.16.80.103 55248 192.5.11.73 29855 478 683 k 478 683 k 0 0 17.407582000 52.706861 103 k 0
192.5.11.174 55843 192.5.11.173 445 470 79 k 313 44 k 157 35 k 0.301827000 79.138687 4469 3586
192.5.11.57 57427 192.5.11.73 10554 405 106 k 405 106 k 0 0 0.772291000 76.787686 11 k 0
192.168.45.146 60814 192.5.11.73 29855 247 69 k 247 69 k 0 0 26.964000000 51.168802 10 k 0
172.16.30.210 51583 192.5.11.73 10554 200 32 k 200 32 k 0 0 1.678088000 35.102649 7411 0
172.16.30.43 55498 192.5.11.73 10554 177 39 k 177 39 k 0 0 29.885957000 41.985557 7620 0
192.5.11.73 10554 192.168.45.61 1090 177 44 k 0 0 177 44 k 33.902471000 36.069402 0 9836
Name resolution
Limit to display filter
1
2
3
4
5
6
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

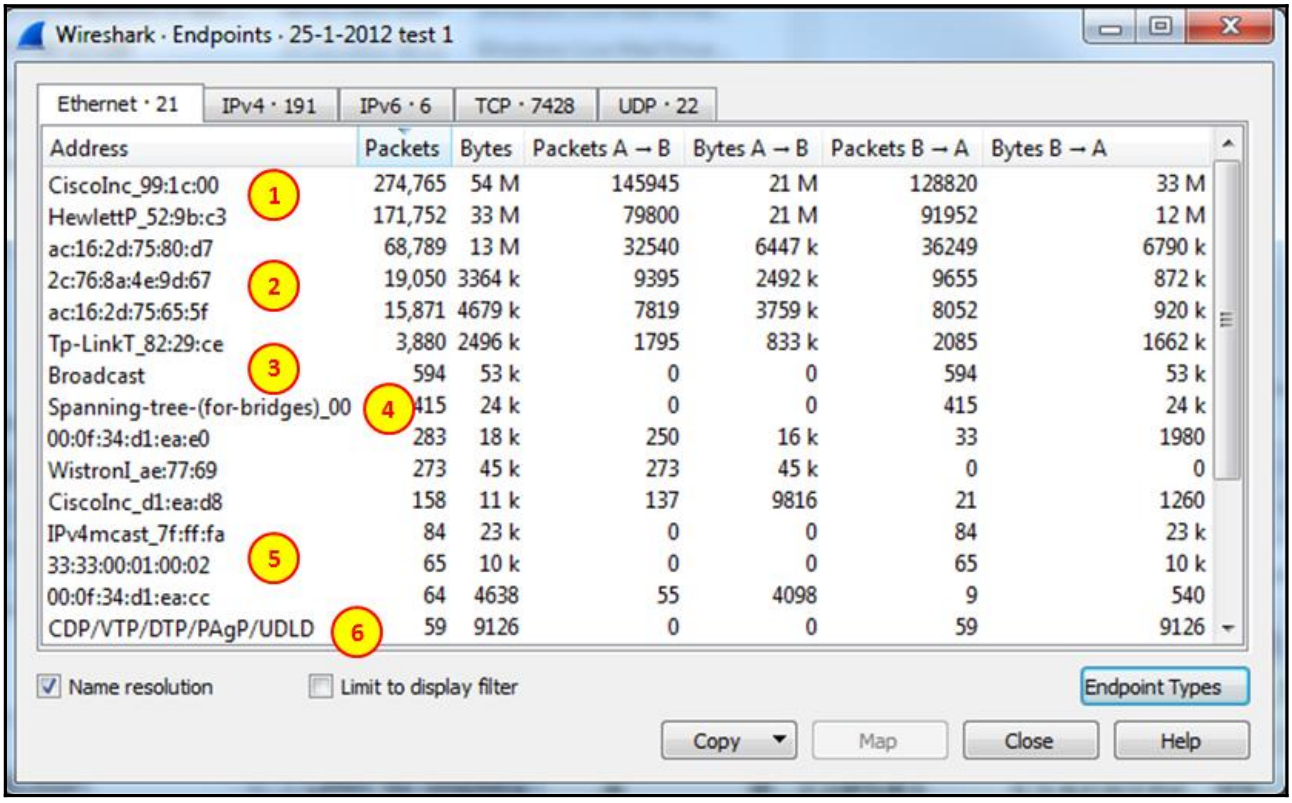

Wireshark · Conversations · BackBone traffic
Ethernet · 38
IPv4 · 5270
IPv6 · 1
TCP · 3349
UDP · 3251
Address A
Address B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
10.2.2.23 10.3.35.97 1008 64 k 2.481876000 1.698242 11 M 304 k
10.2.2.146 10.181.140.220 1,509 1248 k 1787 k 54 k
10.2.2.121 10.121.146.161 1,496 1271 k 1769 k 53 k
10.2.2.111 10.121.3.1 1,412 1325 k 1854 k 41 k
10.2.2.111 10.122.0.158 1,375 1293 k 1809 k 40 k
10.121.148.112 212.199.219.209 1,096 972 k 36 k 1366 k
10.2.2.111 10.122.23.3 1,041 984 k 1392 k 30 k
10.151.101.9 10.250.11.83 956 312 k 410 58 k 83 k 363 k
10.151.101.79 10.250.11.117 954 707 k 197 26 k 37 k 973 k
10.151.101.34 10.250.11.125 889 144 k 437 62 k 452 81 k 89 k 116 k
10.151.101.14 10.250.11.189 883 315 k 368 50 k 515 264 k 72 k 379 k
10.151.101.58 10.250.11.160 881 369 k 340 47 k 541 321 k 68 k 461 k
10.151.101.24 10.250.11.92 851 186 k 409 57 k 442 128 k 82 k 184 k
10.151.101.23 10.250.11.94 846 129 k 408 58 k 438 71 k 0.008279000 5.587476 83 k 101 k
10.151.101.42 10.250.11.202 835 160 k 427 61 k 408 99 k 0.009166000 5.578880 87 k
Apply as Filter
Prepare a Filter
Find
Colorize
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected
A ↔ B
A → B
B → A
A ↔ Any
A → Any
Any → A
Any ↔ B
Any → B
B → Any
Name resolution
Limit to display filter
Copy

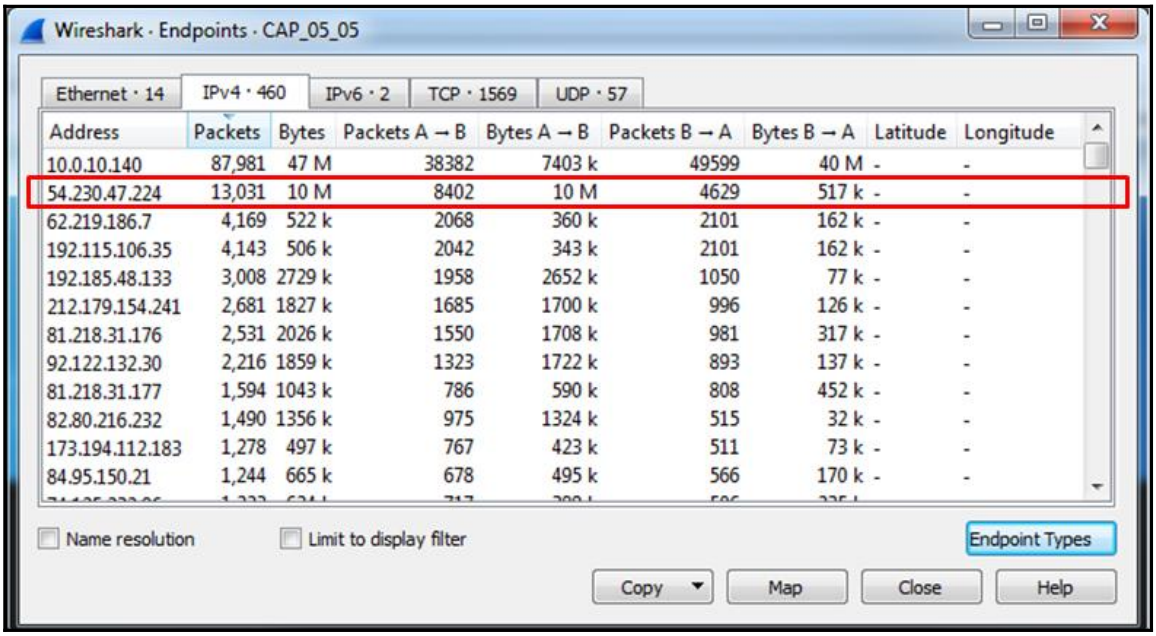

Wireshark · Conversations · Example 010 --- Ping worm attack
Ethernet · 27
IPv4 · 26327
IPv6
TCP · 27
UDP · 1
Address A
Address B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
192.168.110.58 192.170.3.44 1 106 1 106 0 0 1.517110999 0.000000 N/A N/A
192.168.110.58 192.170.3.45 1 106 1 106 0 0 1.532689000 0.000000 N/A N/A
192.168.110.58 192.170.3.46 1 106 1 106 0 0 1.548355999 0.000000 N/A N/A
192.168.110.58 192.170.3.47 1 106 1 106 0 0 1.563934000 0.000000 N/A N/A
192.168.110.58 192.170.3.48 1 106 1 106 0 0 1.579562000 0.000000 N/A N/A
192.168.110.58 192.170.3.49 1 106 1 106 0 0 1.595191000 0.000000 N/A N/A
192.168.110.58 192.170.3.50 1 106 1 106 0 0 1.610806000 0.000000 N/A N/A
192.168.110.58 192.170.3.51 1 106 1 106 0 0 1.626545000 0.000000 N/A N/A
192.168.110.58 192.170.3.52 1 106 1 106 0 0 1.642236000 0.000000 N/A N/A
192.168.110.58 192.170.3.53 1 106 1 106 0 0 1.657772000 0.000000 N/A N/A
192.168.110.58 192.170.3.54 1 106 1 106 0 0 1.673322000 0.000000 N/A N/A
192.168.110.58 192.170.3.55 1 106 1 106 0 0 1.690145000 0.000000 N/A N/A
192.168.110.58 192.170.3.56 1 106 1 106 0 0 1.704616000 0.000000 N/A N/A
192.168.110.58 192.170.3.57 1 106 1 106 0 0 1.720203999 0.000000 N/A N/A
192.168.110.58 192.170.3.58 1 106 1 106 0 0 1.735876000 0.000000 N/A N/A
Scanning Pattern
Name resolution
Limit to display filter
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

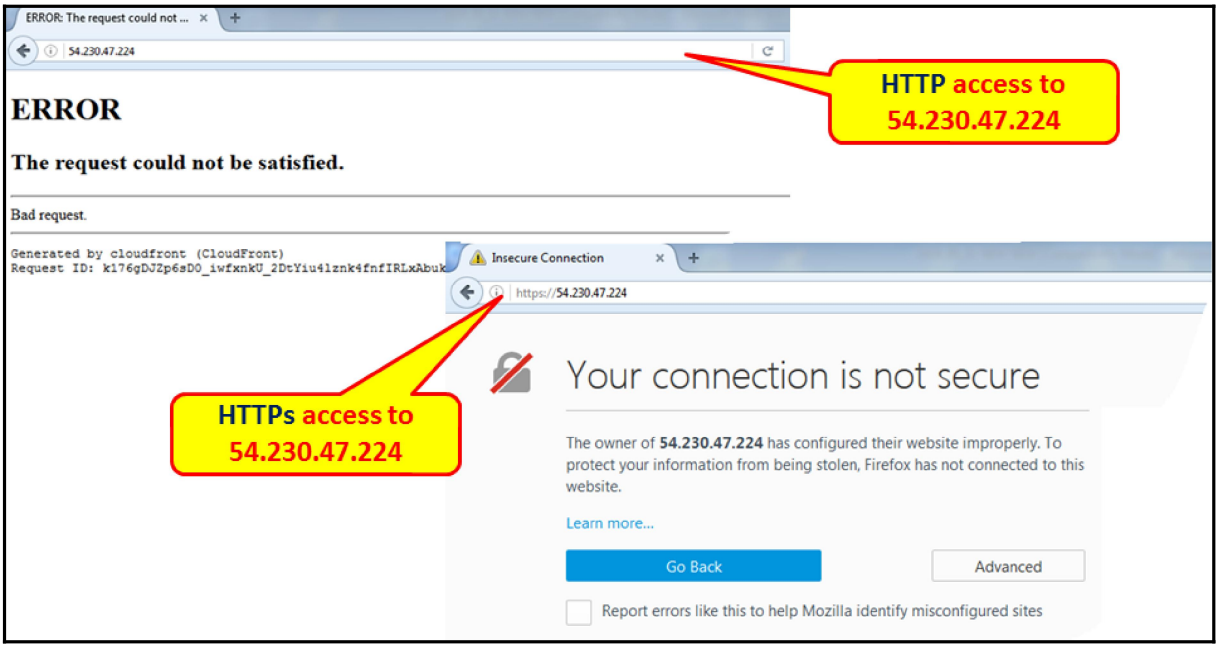

Source ports
Destination ports
Ethernet · 10
IPv4 · 104
IPv6
TCP · 4603
UDP · 387
Address A
Port A
Address B
Port B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
10.0.0.1 63033 81.218.230.244 1 3 194 3 194 0 0 583.042429000 9.004836 172 0
10.0.0.1 63038 81.218.230.244 1 3 194 3 194 0 0 583.144870000 8.997256 172 0
10.0.0.1 62650 81.218.230.244 3 3 194 3 194 0 0 575.347188000 8.994668 172 0
10.0.0.1 62655 81.218.230.244 3 3 194 3 194 0 0 575.449029000 8.993904 172 0
10.0.0.1 62669 81.218.230.244 4 3 194 3 194 0 0 575.751737000 9.013271 172 0
10.0.0.1 62674 81.218.230.244 4 3 194 3 194 0 0 575.852225000 9.012693 172 0
10.0.0.1 62444 81.218.230.244 6 3 194 3 194 0 0 571.290318000 8.998313 172 0
10.0.0.1 62449 81.218.230.244 6 3 194 3 194 0 0 571.392000000 9.002697 172 0
10.0.0.1 62358 81.218.230.244 7 3 194 3 194 0 0 569.654217000 9.006301 172 0
10.0.0.1 62363 81.218.230.244 7 3 194 3 194 0 0 569.754861000 8.996706 172 0
10.0.0.1 61613 81.218.230.244 9 3 194 3 194 0 0 554.866707000 9.004181 172 0
10.0.0.1 61618 81.218.230.244 9 3 194 3 194 0 0 554.966922000 9.004042 172 0
10.0.0.1 61909 81.218.230.244 13 3 194 3 194 0 0 560.737696000 8.996513 172 0
10.0.0.1 61914 81.218.230.244 13 3 194 3 194 0 0 560.838897000 8.999269 172 0
10.0.0.1 61337 81.218.230.244 17 3 194 3 194 0 0 549.380582000 8.999075 172 0
10.0.0.1 61342 81.218.230.244 17 3 194 3 194 0 0 549.482177000 9.005512 172 0
10.0.0.1 61319 81.218.230.244 19 3 194 3 194 0 0 548.996834000 8.996840 172 0
10.0.0.1 61324 81.218.230.244 19 3 194 3 194 0 0 549.098619000 8.999071 172 0
10.0.0.1 61764 81.218.230.244 20 3 194 3 194 0 0 557.902602000 9.003455 172 0
10.0.0.1 61769 81.218.230.244 20 3 194 3 194 0 0 558.004049000 9.003061 172 0
10.0.0.1 61232 81.218.230.244 21 7 550 3 174 4 376 547.349881000 0.041566 33 k 72 k
Port Scanning Pattern
Name resolution
Limit to display filter
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

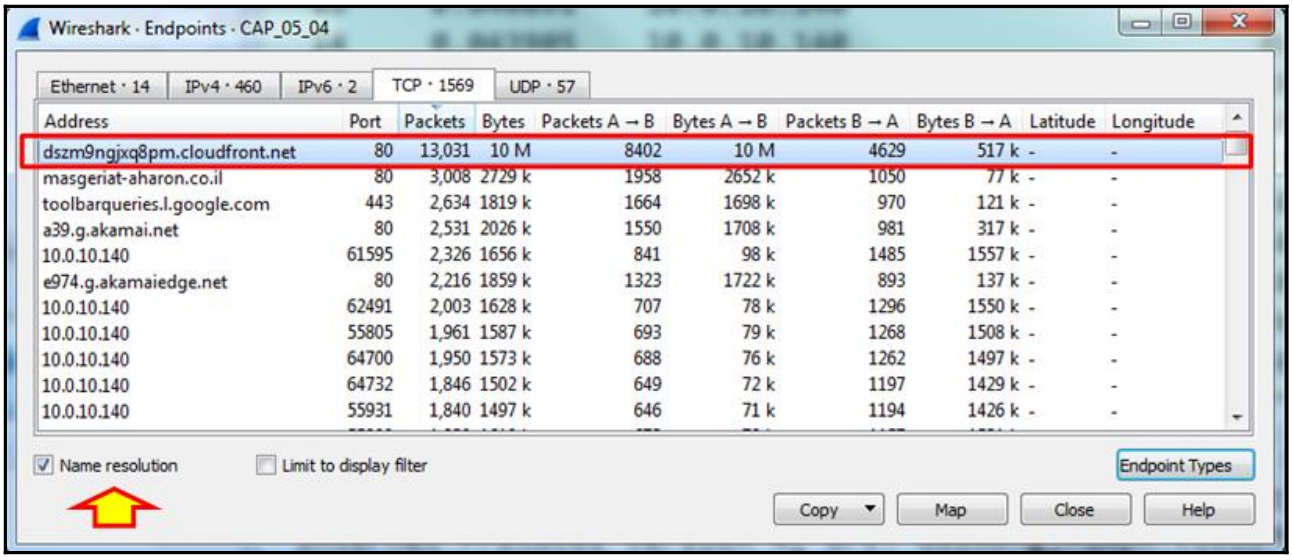

HTTP server scan --- JUN-2016.pcapng
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
No.
Time
Destination
1 0.000000 10.0.0.1
2 0.000126 10.0.0
3 0.000185 10
4 0.000538
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths
I/O Graph
Service Response Tim

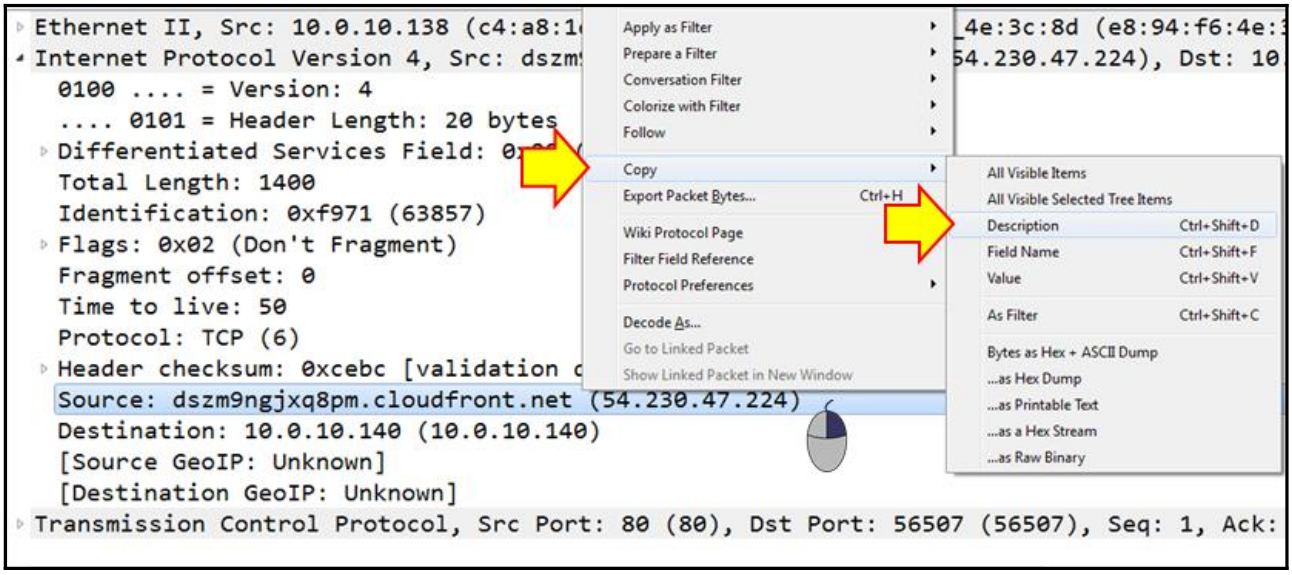

Wireshark · Endpoints · HTTP server scan --- JUN-2016
Ethernet · 11
IPv4 · 76
IPv6
TCP · 4594
UDP · 268
Address Port Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Latitude Longitude
54.154.213.203 443 36,266 13 M 19663 11 M 16603 2199 k - -
54.154.213.203 80 17,313 2572 k 7372 1434 k 9941 1138 k - -
194.90.6.40 110 4,552 4161 k 2970 4074 k 1582 87 k - -
81.218.155.143 6690 4,408 1931 k 2230 1406 k 2178 525 k - -
193.46.64.211 80 1,212 957 k 731 898 k 481 58 k - -
10.0.0.1 55136 1,026 66 k 1008 59 k 18 7335 - -
10.0.0.1 55135 1,016 58 k 1002 58 k 14 804 - -
10.0.0.1 55137 997 57 k 997 57 k 0 0 - -
10.0.0.1 56635 490 471 k 167 9109 323 462 k - -
10.0.0.1 55073 406 387 k 139 7597 267 379 k - -
10.0.0.1 46480 378 20 k 252 13 k 126 6930 - -
95.211.242.83 443 378 20 k 126 6930 252 13 k - -
Name resolution
Limit to display filter
1
2
3
4
5
Endpoint Types
Copy
Map
Close
Help

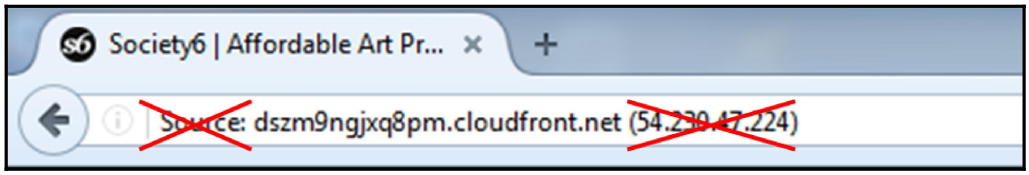

Wireshark · Endpoints · 25-1-2012 test 1
Ethernet · 21
IPv4 · 191
IPv6 · 6
TCP · 7428
UDP · 22
Address Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A
CiscoInc_99:1c:00 274,765 54 M 145945 21 M 128820 33 M
HewlettP_52:9b:c3 171,752 33 M 79800 21 M 91952 12 M
ac:16:2d:75:80:d7 68,789 13 M 32540 6447 k 36249 6790 k
2c:76:8a:4e:9d:67 19,050 3364 k 9395 2492 k 9655 872 k
ac:16:2d:75:65:5f 15,871 4679 k 7819 3759 k 8052 920 k
Tp-LinkT_82:29:ce 3,880 2496 k 1795 833 k 2085 1662 k
Broadcast 594 53 k 0 0 594 53 k
Spanning-tree-(for-bridges)_00 415 24 k 0 0 415 24 k
00:0f:34:d1:ea:e0 283 18 k 250 16 k 33 1980
WistronI_ae:77:69 273 45 k 273 45 k 0 0
CiscoInc_d1:ea:d8 158 11 k 137 9816 21 1260
IPv4mcast_7f:ff:fa 84 23 k 0 0 84 23 k
33:33:00:01:00:02 65 10 k 0 0 65 10 k
00:0f:34:d1:ea:cc 64 4638 55 4098 9 540
CDP/VTP/DTP/PAgP/UDLD 59 9126 0 0 59 9126
1
2
3
4
5
6
Name resolution
Limit to display filter
Endpoint Types
Copy
Map
Close
Help

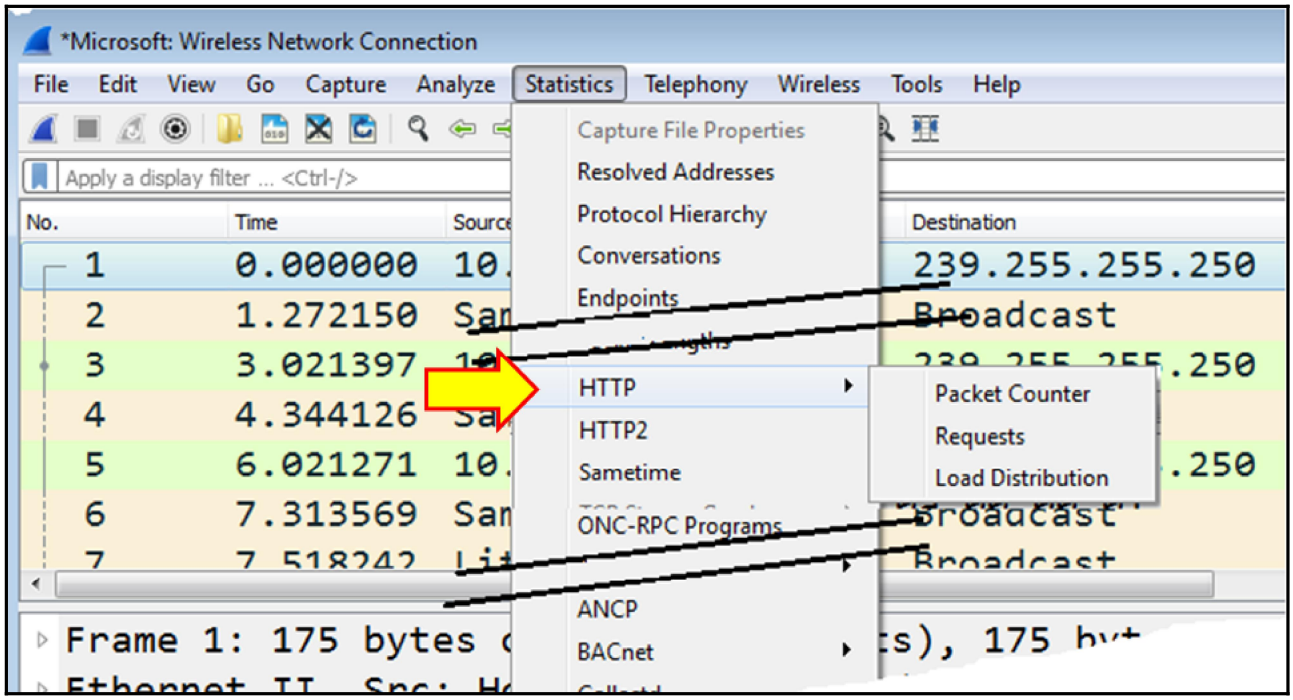

Wireshark · Endpoints · CAP_05_05
Ethernet · 14
IPv4 · 460
IPv6 · 2
TCP · 1569
UDP · 57
Address Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Latitude Longitude
10.0.10.140 87,981 47 M 38382 7403 k 49599 40 M - -
54.230.47.224 13,031 10 M 8402 10 M 4629 517 k - -
62.219.186.7 4,169 522 k 2068 360 k 2101 162 k - -
192.115.106.35 4,143 506 k 2042 343 k 2101 162 k - -
192.185.48.133 3,008 2729 k 1958 2652 k 1050 77 k - -
212.179.154.241 2,681 1827 k 1685 1700 k 996 126 k - -
81.218.31.176 2,531 2026 k 1550 1708 k 981 317 k - -
92.122.132.30 2,216 1859 k 1323 1722 k 893 137 k - -
81.218.31.177 1,594 1043 k 786 590 k 808 452 k - -
82.80.216.232 1,490 1356 k 975 1324 k 515 32 k - -
173.194.112.183 1,278 497 k 767 423 k 511 73 k - -
84.95.150.21 1,244 665 k 678 495 k 566 170 k - -
Name resolution
Limit to display filter
Endpoint Types
Copy
Map
Close
Help

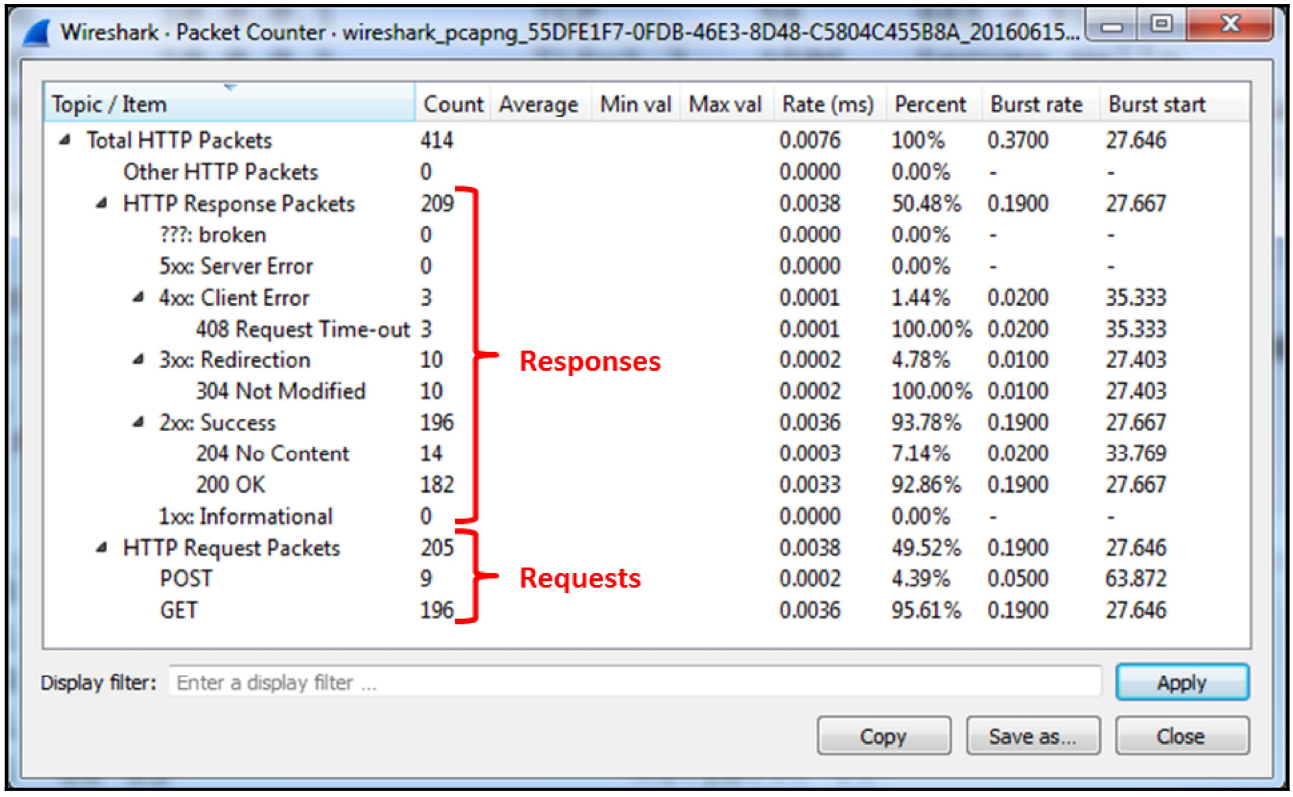

ERROR: The request could not ...
54.230.47.224
HTTP access to 54.230.47.224
ERROR
The request could not be satisfied.
Bad request.
Generated by cloudfront (CloudFront)
Request ID: k176gDJZp6sD0_iwfxnkU_2DtYiu4lznk4fnfIRLxAbuk
Insecure Connection
https://54.230.47.224
HTTPs access to 54.230.47.224
Your connection is not secure
The owner of 54.230.47.224 has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.
Learn more...
Go Back
Advanced
Report errors like this to help Mozilla identify misconfigured sites

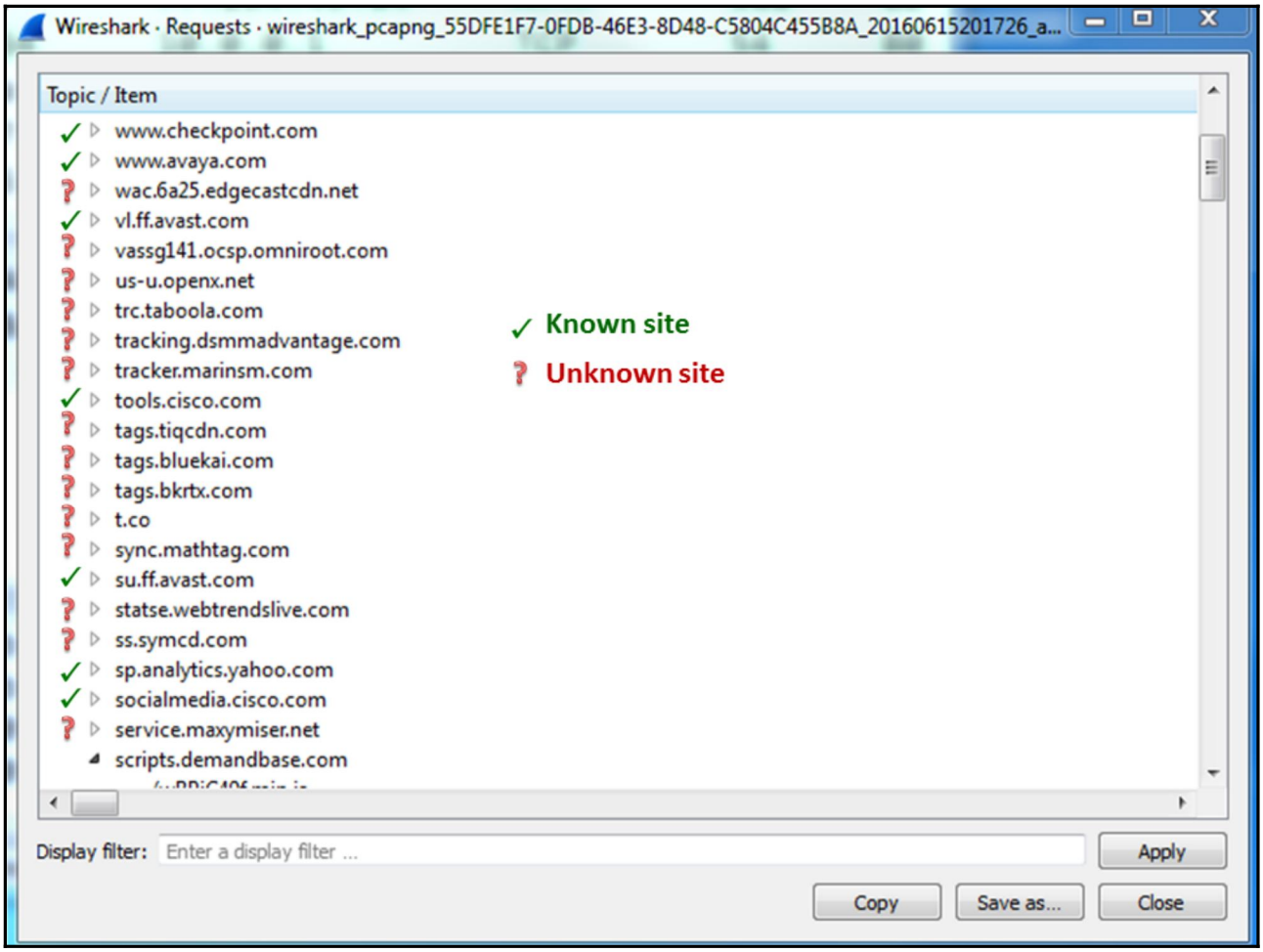

Wireshark · Endpoints · CAP_05_04
Ethernet · 14
IPv4 · 460
IPv6 · 2
TCP · 1569
UDP · 57
Address Port Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Latitude Longitude
dszm9ngjxq8pm.cloudfront.net 80 13,031 10 M 8402 10 M 4629 517 k - -
masgeriat-aharon.co.il 80 3,008 2729 k 1958 2652 k 1050 77 k - -
toolbarqueries.l.google.com 443 2,634 1819 k 1664 1698 k 970 121 k - -
a39.g.akamai.net 80 2,531 2026 k 1550 1708 k 981 317 k - -
10.0.10.140 61595 2,326 1656 k 841 98 k 1485 1557 k - -
e974.g.akamaiedge.net 80 2,216 1859 k 1323 1722 k 893 137 k - -
10.0.10.140 62491 2,003 1628 k 707 78 k 1296 1550 k - -
10.0.10.140 55805 1,961 1587 k 693 79 k 1268 1508 k - -
10.0.10.140 64700 1,950 1573 k 688 76 k 1262 1497 k - -
10.0.10.140 64732 1,846 1502 k 649 72 k 1197 1429 k - -
10.0.10.140 55931 1,840 1497 k 646 71 k 1194 1426 k - -
Name resolution
Limit to display filter
Endpoint Types
Copy
Map
Close
Help

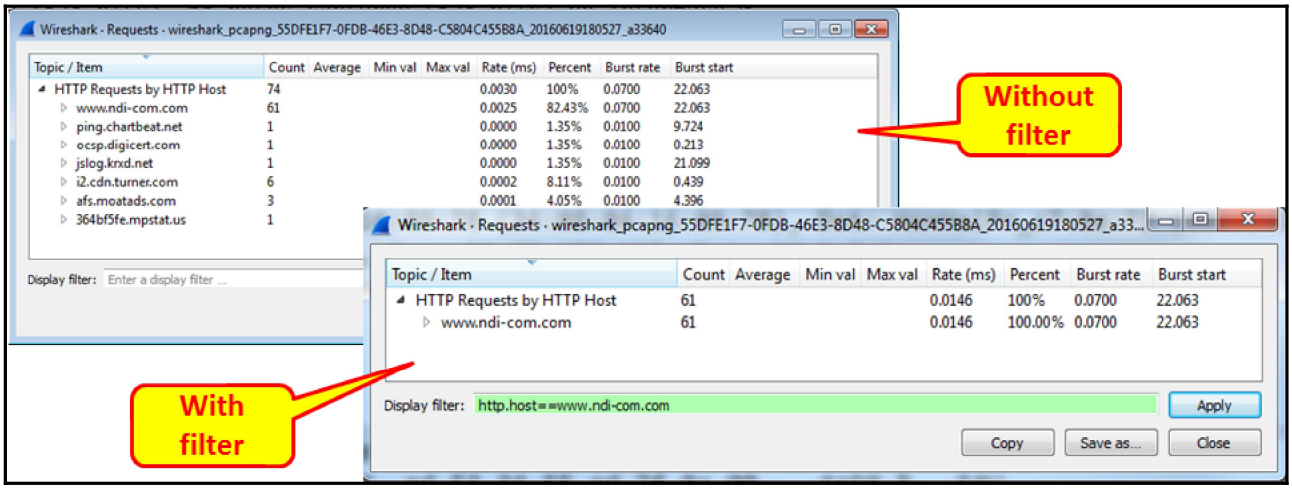

Ethernet II, Src: 10.0.10.138 (c4:a8:1
Internet Protocol Version 4, Src: dszm
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes
Differentiated Services Field:
Total Length: 1400
Identification: 0xf971 (63857)
Flags: 0x02 (Don't Fragment)
Fragment offset: 0
Time to live: 50
Protocol: TCP (6)
Header checksum: 0xcebc [validation
Source: dszm9ngjxq8pm.cloudfront.net (54.230.47.224)
Destination: 10.0.10.140 (10.0.10.140)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 80 (80), Dst Port: 56507 (56507), Seq: 1, Ack:
_4e:3c:8d (e8:94:f6:4e:
54.230.47.224), Dst: 10
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Copy
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
All Visible Items
All Visible Selected Tree Items
Description Ctrl+Shift+D
Field Name Ctrl+Shift+F
Value Ctrl+Shift+V
As Filter Ctrl+Shift+C
Bytes as Hex + ASCII Dump
...as Hex Dump
...as Printable Text
...as a Hex Stream
...as Raw Binary

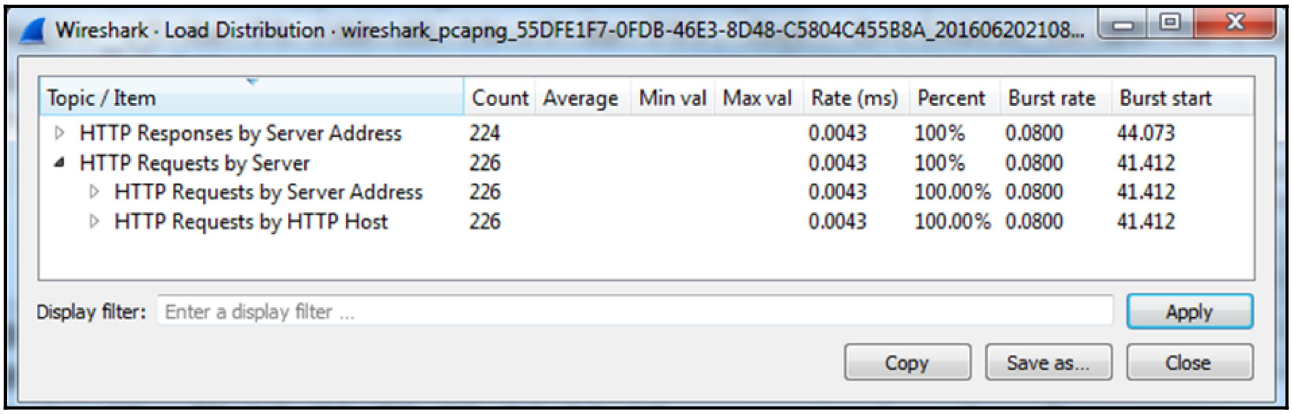

Society6 | Affordable Art Pr...
Source: dszm9ngjxq8pm.cloudfront.net (54.230.47.224)

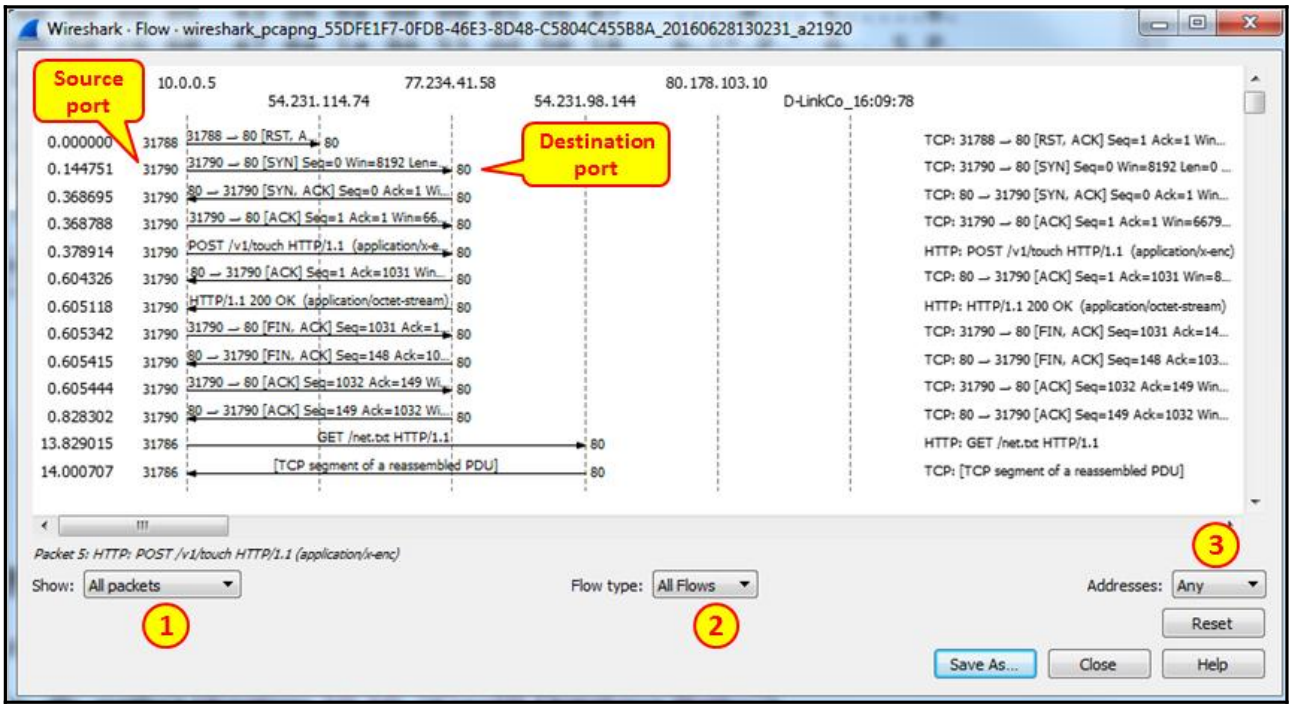

*Microsoft: Wireless Network Connection
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination
1 0.000000 239.255.255.250
2 1.272150 Broadcast
3 3.021397 .250
4 4.344126
5 6.021271 .250
6 7.313569 Broadcast
7 Broadcast
Frame 1: 175 bytes
Capture File Properties
Resolved Addresses
Protocol Hierarchy
Conversations
Endpoints
HTTP
HTTP2
Sametime
ONC-RPC Programs
ANCP
BACnet
Packet Counter
Requests
Load Distribution

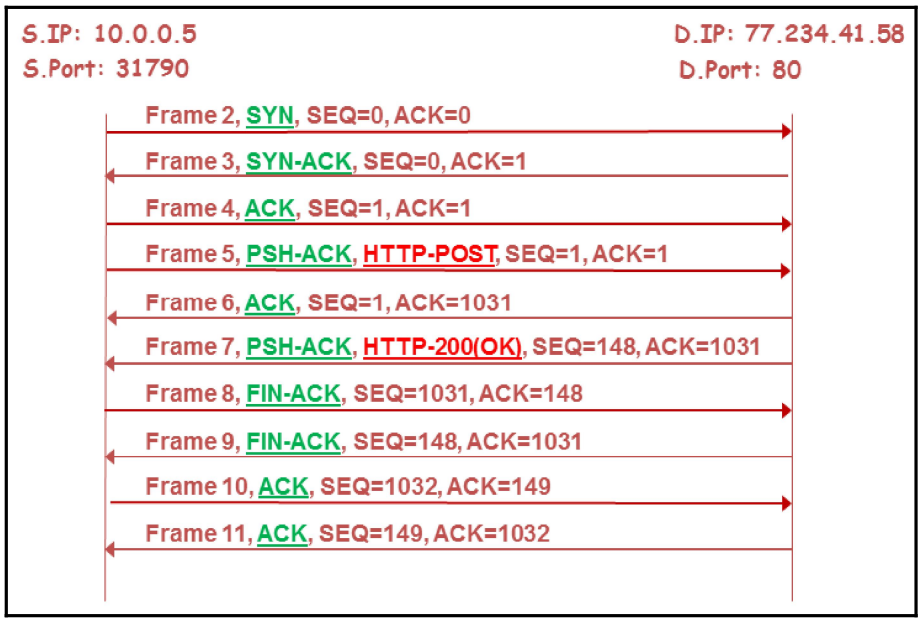

Wireshark · Packet Counter · wireshark_pcapng_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_20160615...
Topic / Item Count Average Min val Max val Rate (ms) Percent Burst rate Burst start
Total HTTP Packets 414 0.0076 100% 0.3700 27.646
Other HTTP Packets 0 0.0000 0.00% - -
HTTP Response Packets 209 0.0038 50.48% 0.1900 27.667
???: broken 0 0.0000 0.00% - -
5xx: Server Error 0 0.0000 0.00% - -
4xx: Client Error 3 0.0001 1.44% 0.0200 35.333
408 Request Time-out 3 0.0001 100.00% 0.0200 35.333
3xx: Redirection 10 0.0002 4.78% 0.0100 27.403
304 Not Modified 10 0.0002 100.00% 0.0100 27.403
2xx: Success 196 0.0036 93.78% 0.1900 27.667
204 No Content 14 0.0003 7.14% 0.0200 33.769
200 OK 182 0.0033 92.86% 0.1900 27.667
1xx: Informational 0 0.0000 0.00% - -
HTTP Request Packets 205 0.0038 49.52% 0.1900 27.646
POST 9 0.0002 4.39% 0.0500 63.872
GET 196 0.0036 95.61% 0.1900 27.646
Responses
Requests
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

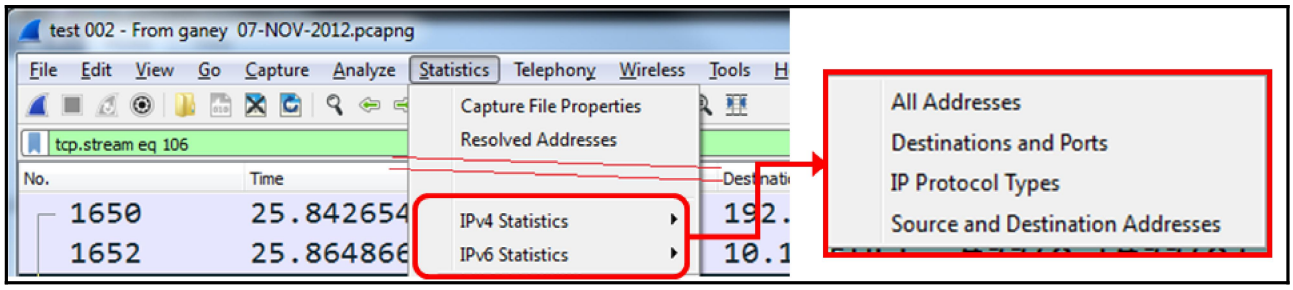

Wireshark · Requests · wireshark_pcapng_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_20160615201726_a...
Topic / Item
www.checkpoint.com
www.avaya.com
wac.6a25.edgecastcdn.net
vl.ff.avast.com
vassg141.ocsp.omniroot.com
us-u.openx.net
trc.taboola.com
tracking.dsmmadvantage.com
tracker.marinsm.com
tools.cisco.com
tags.tiqcdn.com
tags.bluekai.com
tags.bkrtx.com
t.co
sync.mathtag.com
su.ff.avast.com
statse.webtrendslive.com
ss.symcd.com
sp.analytics.yahoo.com
socialmedia.cisco.com
service.maxymiser.net
scripts.demandbase.com
Known site
Unknown site
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

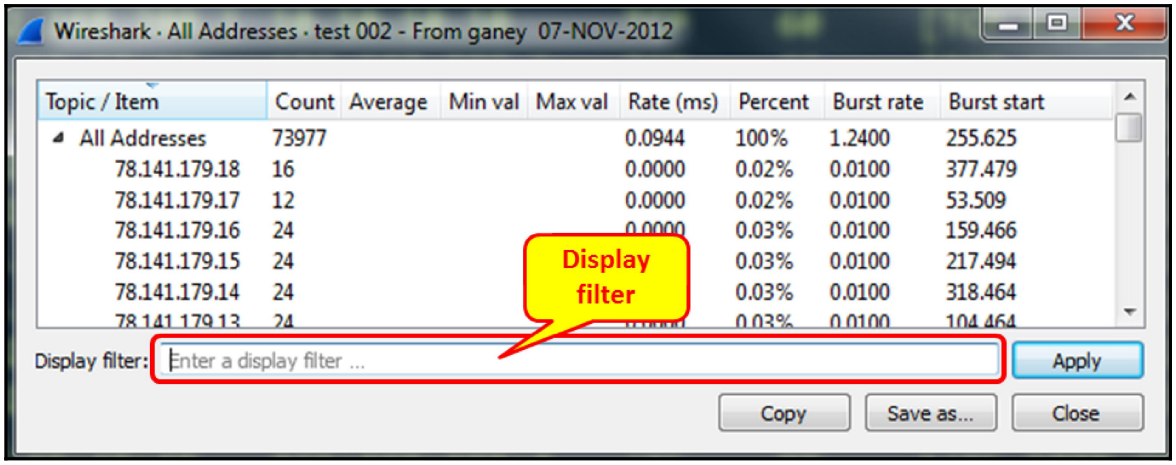

Without filter
With filter
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
HTTP Requests by HTTP Host
www.ndi-com.com
ping.chartbeat.net
ocsp.digicert.com
jslog.krxd.net
i2.cdn.turner.com
afs.moatads.com
364bf5fe.mpstat.us
Display filter:
http.host==www.ndi-com.com
Apply
Copy
Save as...
Close

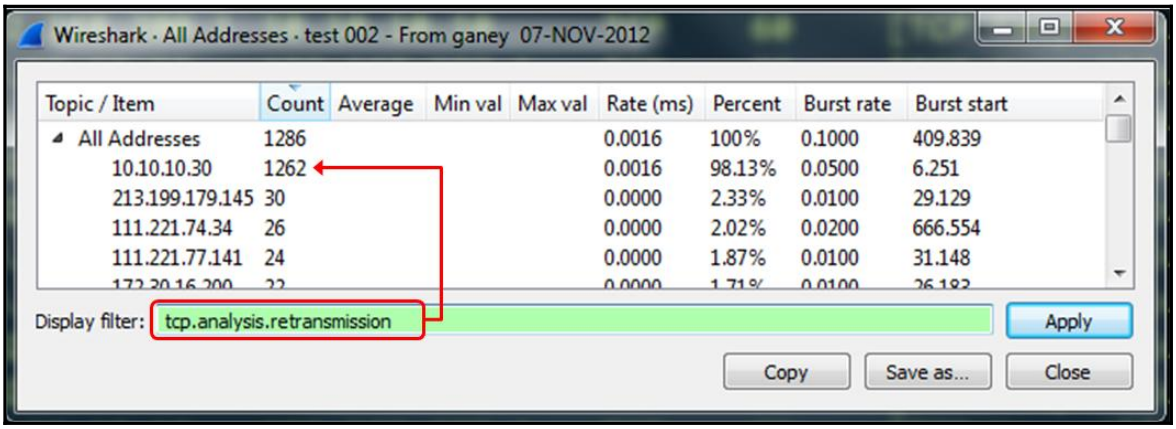

Wireshark · Load Distribution · wireshark_pcapng_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_201606202108...
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
HTTP Responses by Server Address 224 0.0043 100% 0.0800 44.073
HTTP Requests by Server 226 0.0043 100% 0.0800 41.412
HTTP Requests by Server Address 226 0.0043 100.00% 0.0800 41.412
HTTP Requests by HTTP Host 226 0.0043 100.00% 0.0800 41.412
Display filter:
Enter a display filter ...
Apply
Copy
Save as...
Close

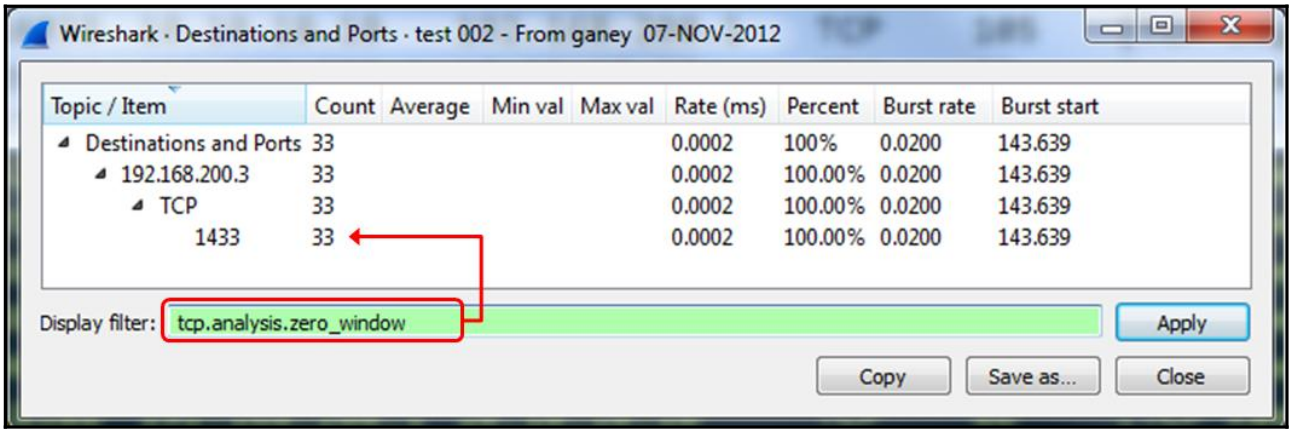

Wireshark · Flow · wireshark_pcapng_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_20160628130231_a21920
Source port
Destination port
10.0.0.5
54.231.114.74
77.234.41.58
54.231.98.144
80.178.103.10
D-LinkCo_16:09:78
0.000000 31788 → 80 [RST, A... 80 TCP: 31788 → 80 [RST, ACK] Seq=1 Ack=1 Win...
0.144751 31790 → 80 [SYN] Seq=0 Win=8192 Len=... 80 TCP: 31790 → 80 [SYN] Seq=0 Win=8192 Len=0 ...
0.368695 31790 80 → 31790 [SYN, ACK] Seq=0 Ack=1 Wi... 80 TCP: 80 → 31790 [SYN, ACK] Seq=0 Ack=1 Win...
0.368788 31790 → 80 [ACK] Seq=1 Ack=1 Win=66... 80 TCP: 31790 → 80 [ACK] Seq=1 Ack=1 Win=6679...
0.378914 31790 POST /v1/touch HTTP/1.1 (application/x-e... 80 HTTP: POST /v1/touch HTTP/1.1 (application/x-enc)
0.604326 31790 80 → 31790 [ACK] Seq=1 Ack=1031 Win... 80 TCP: 80 → 31790 [ACK] Seq=1 Ack=1031 Win=8...
0.605118 31790 HTTP/1.1 200 OK (application/octet-stream) 80 HTTP: HTTP/1.1 200 OK (application/octet-stream)
0.605342 31790 → 80 [FIN, ACK] Seq=1031 Ack=1... 80 TCP: 31790 → 80 [FIN, ACK] Seq=1031 Ack=14...
0.605415 31790 80 → 31790 [FIN, ACK] Seq=148 Ack=10... 80 TCP: 80 → 31790 [FIN, ACK] Seq=148 Ack=103...
0.605444 31790 → 80 [ACK] Seq=1032 Ack=149 Wi... 80 TCP: 31790 → 80 [ACK] Seq=1032 Ack=149 Win...
0.828302 31790 80 → 31790 [ACK] Seq=149 Ack=1032 Wi... 80 TCP: 80 → 31790 [ACK] Seq=149 Ack=1032 Win...
13.829015 31786 GET /net.txt HTTP/1.1 80 HTTP: GET /net.txt HTTP/1.1
14.000707 31786 [TCP segment of a reassembled PDU] 80 TCP: [TCP segment of a reassembled PDU]
Packet 5: HTTP: POST /v1/touch HTTP/1.1 (application/x-enc)
Show: All packets
Flow type: All Flows
Addresses: Any
1
2
3
Reset
Save As...
Close
Help


S.IP: 10.0.0.5
S.Port: 31790
D.IP: 77.234.41.58
D.Port: 80
Frame 2, SYN, SEQ=0, ACK=0
Frame 3, SYN-ACK, SEQ=0, ACK=1
Frame 4, ACK, SEQ=1, ACK=1
Frame 5, PSH-ACK, HTTP-POST, SEQ=1, ACK=1
Frame 6, ACK, SEQ=1, ACK=1031
Frame 7, PSH-ACK, HTTP-200(OK), SEQ=148, ACK=1031
Frame 8, FIN-ACK, SEQ=1031, ACK=148
Frame 9, FIN-ACK, SEQ=148, ACK=1031
Frame 10, ACK, SEQ=1032, ACK=149
Frame 11, ACK, SEQ=149, ACK=1032

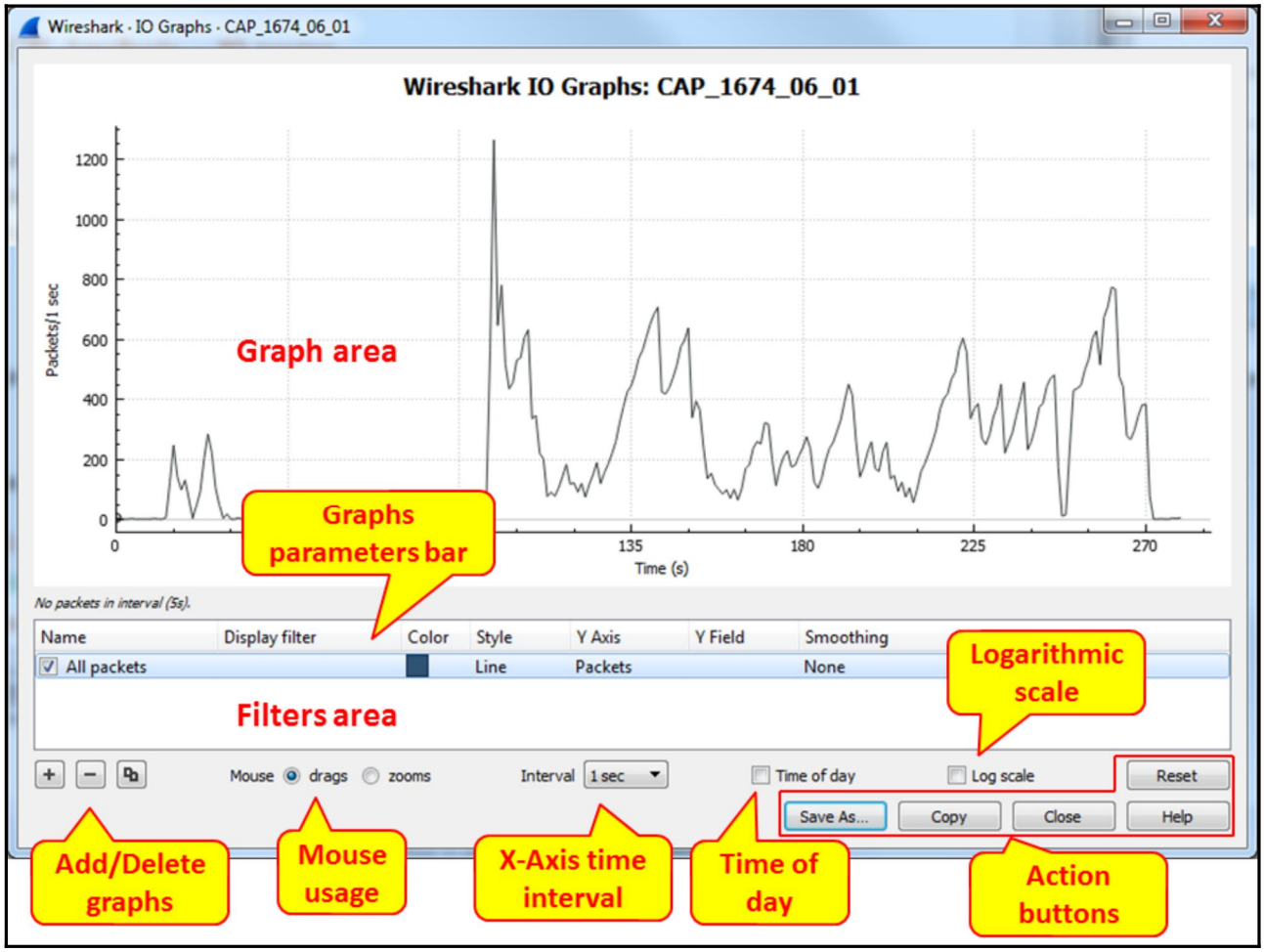

test 002 - From ganey 07-NOV-2012.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools H
tcp.stream eq 106
No. Time
1650 25.842654
1652 25.864866
Capture File Properties
Resolved Addresses
IPv4 Statistics
IPv6 Statistics
All Addresses
Destinations and Ports
IP Protocol Types
Source and Destination Addresses

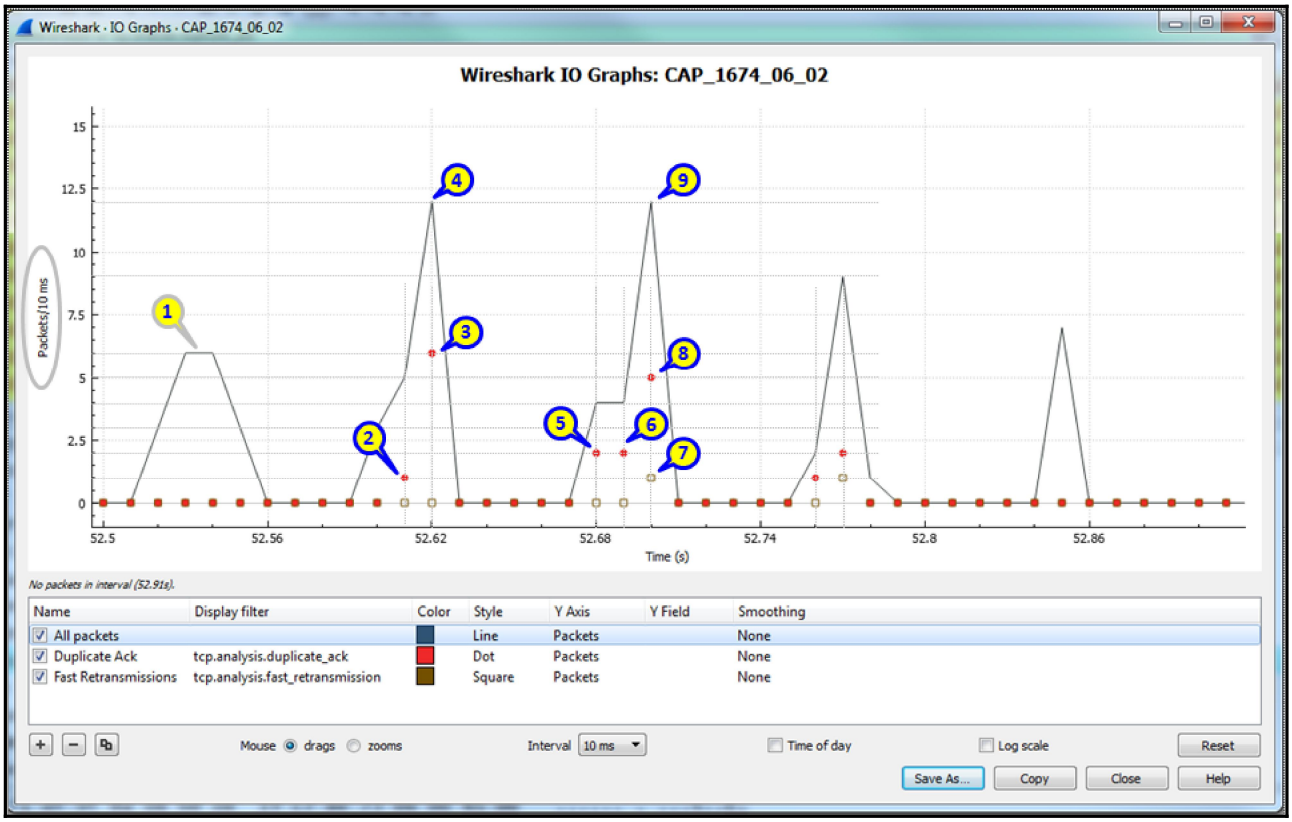

Wireshark · All Addresses · test 002 - From ganey 07-NOV-2012
Topic / Item Count Average Min val Max val Rate (ms) Percent Burst rate Burst start
All Addresses 73977 0.0944 100% 1.2400 255.625
78.141.179.18 16 0.0000 0.02% 0.0100 377.479
78.141.179.17 12 0.0000 0.02% 0.0100 53.509
78.141.179.16 24 0.03% 0.0100 159.466
78.141.179.15 24 0.03% 0.0100 217.494
78.141.179.14 24 0.03% 0.0100 318.464
Display filter
Display filter: Enter a display filter ...
Apply
Copy
Save as...
Close

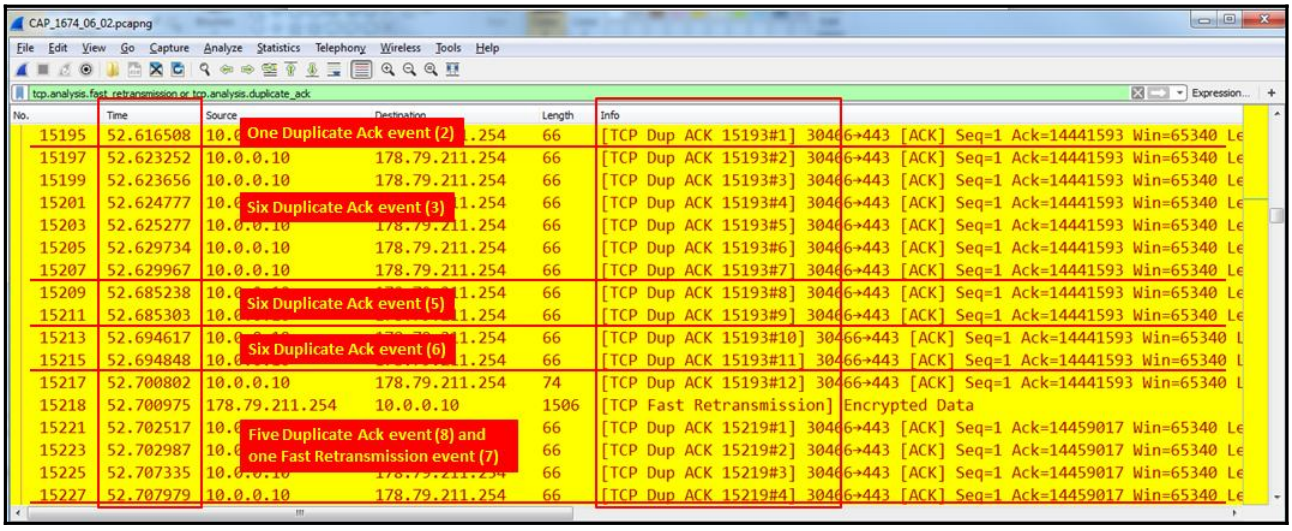

Wireshark · All Addresses · test 002 - From ganey 07-NOV-2012
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
All Addresses 1286 0.0016 100% 0.1000 409.839
10.10.10.30 1262 0.0016 98.13% 0.0500 6.251
213.199.179.145 30 0.0000 2.33% 0.0100 29.129
111.221.74.34 26 0.0000 2.02% 0.0200 666.554
111.221.77.141 24 0.0000 1.87% 0.0100 31.148
Display filter: tcp.analysis.retransmission
Apply
Copy
Save as...
Close

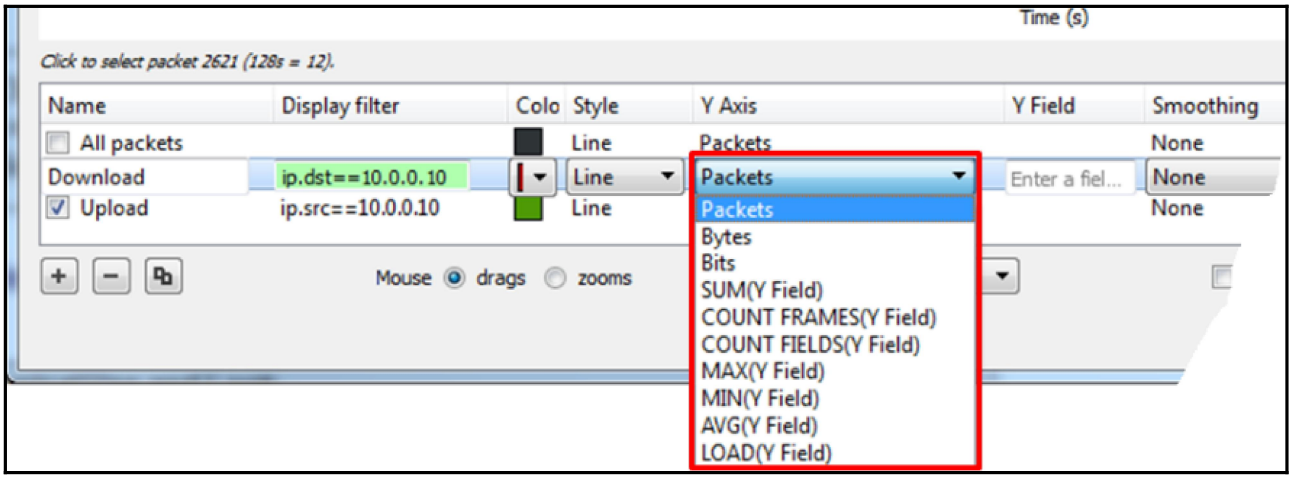

Wireshark · Destinations and Ports · test 002 - From ganey 07-NOV-2012
Topic / Item
Count
Average
Min val
Max val
Rate (ms)
Percent
Burst rate
Burst start
Destinations and Ports 33 0.0002 100% 0.0200 143.639
192.168.200.3 33 0.0002 100.00% 0.0200 143.639
TCP 33 0.0002 100.00% 0.0200 143.639
1433 33 0.0002 100.00% 0.0200 143.639
Display filter: tcp.analysis.zero_window
Apply
Copy
Save as...
Close

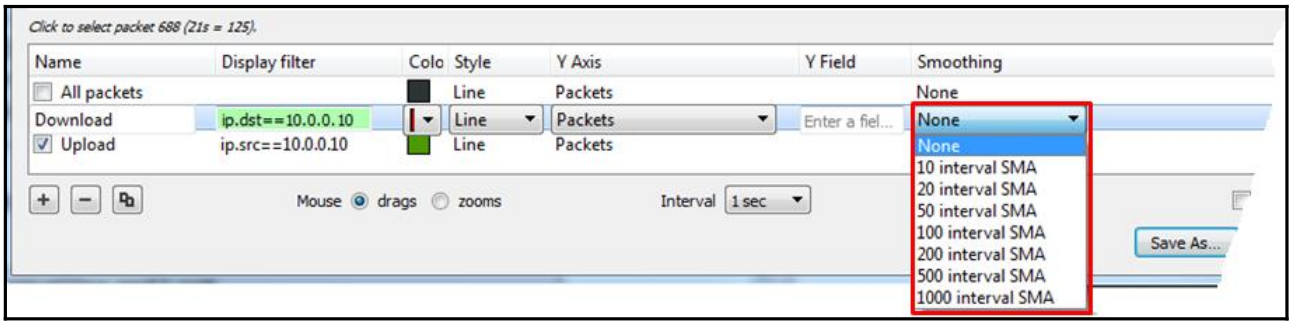
Chapter 6: Using Advanced Statistics Tools

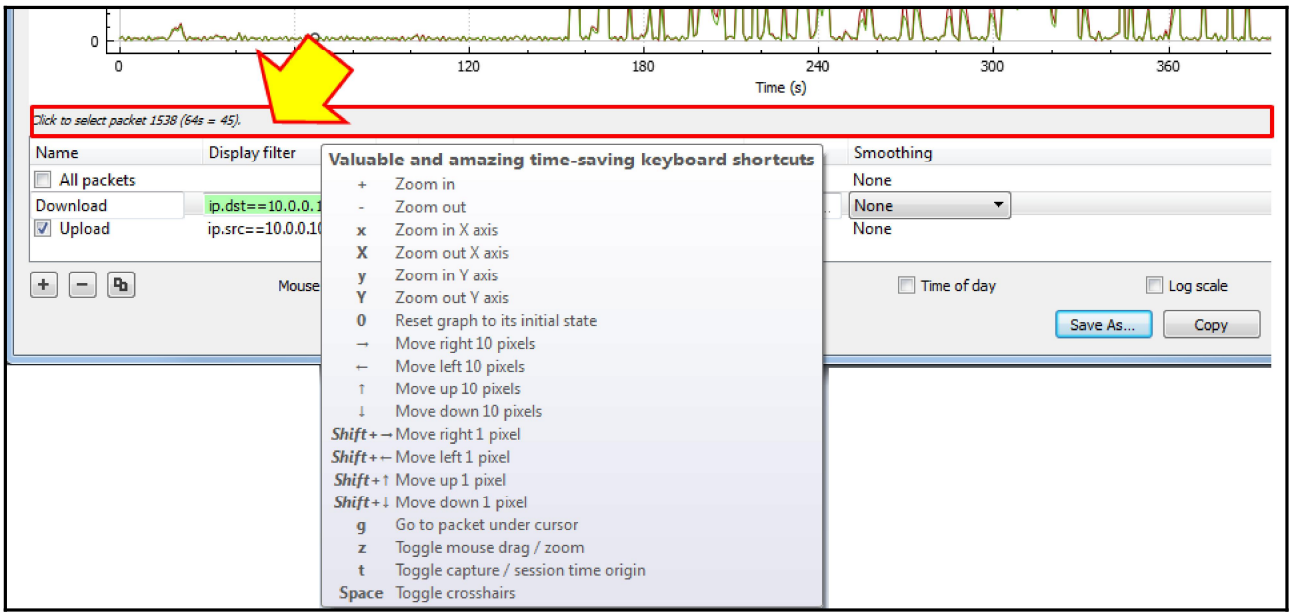


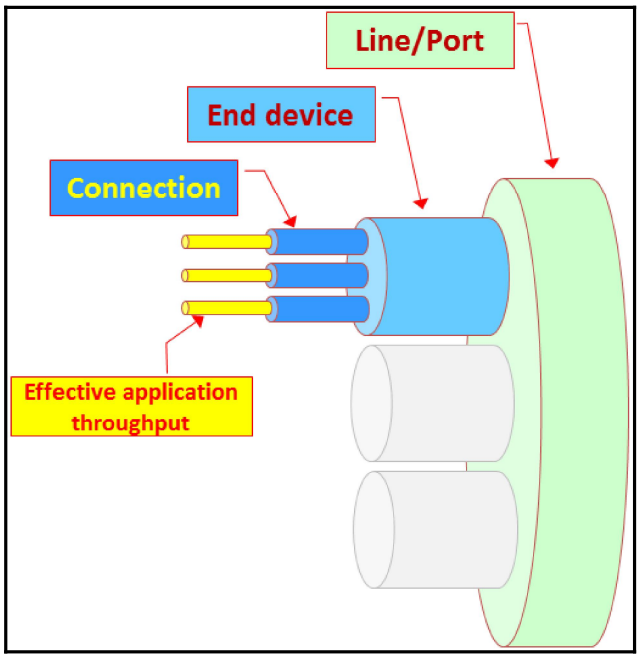

Wireshark · IO Graphs · CAP_1674_06_02
Wireshark IO Graphs: CAP_1674_06_02
Packets/10 ms
Time (s)
1
2
3
4
5
6
7
8
9
No packets in interval (52.91s).
Name
Display filter
Color
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
Duplicate Ack
tcp.analysis.duplicate_ack
Dot
Packets
None
Fast Retransmissions
tcp.analysis.fast_retransmission
Square
Packets
None
Mouse drags zooms
Interval 10 ms
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

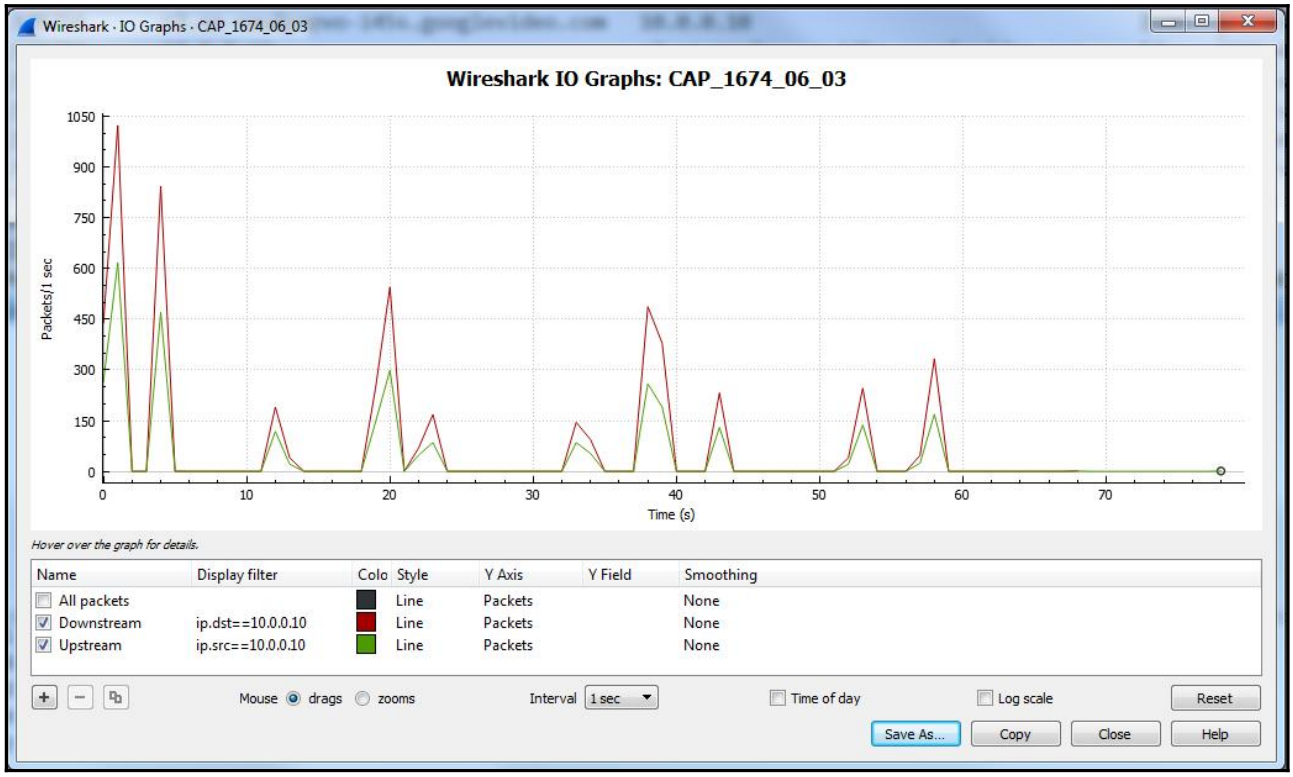

CAP_1674_06_02.pcapng
One Duplicate Ack event (2)
Six Duplicate Ack event (3)
Six Duplicate Ack event (5)
Six Duplicate Ack event (6)
Five Duplicate Ack event (8) and one Fast Retransmission event (7)
15195 52.616508 [TCP Dup ACK 15193#1] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15197 52.623252 10.0.0.10 178.79.211.254 66 [TCP Dup ACK 15193#2] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15199 52.623656 10.0.0.10 178.79.211.254 66 [TCP Dup ACK 15193#3] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15201 52.624777 66 [TCP Dup ACK 15193#4] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15203 52.625277 66 [TCP Dup ACK 15193#5] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15205 52.629734 10.0.0.10 178.79.211.254 66 [TCP Dup ACK 15193#6] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15207 52.629967 10.0.0.10 178.79.211.254 66 [TCP Dup ACK 15193#7] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15209 52.685238 66 [TCP Dup ACK 15193#8] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15211 52.685303 66 [TCP Dup ACK 15193#9] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15213 52.694617 66 [TCP Dup ACK 15193#10] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15215 52.694848 66 [TCP Dup ACK 15193#11] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15217 52.700802 10.0.0.10 178.79.211.254 74 [TCP Dup ACK 15193#12] 30466→443 [ACK] Seq=1 Ack=14441593 Win=65340
15218 52.700975 178.79.211.254 10.0.0.10 1506 [TCP Fast Retransmission] Encrypted Data
15221 52.702517 66 [TCP Dup ACK 15219#1] 30466→443 [ACK] Seq=1 Ack=14459017 Win=65340
15223 52.702987 66 [TCP Dup ACK 15219#2] 30466→443 [ACK] Seq=1 Ack=14459017 Win=65340
15225 52.707335 66 [TCP Dup ACK 15219#3] 30466→443 [ACK] Seq=1 Ack=14459017 Win=65340
15227 52.707979 10.0.0.10 178.79.211.254 66 [TCP Dup ACK 15219#4] 30466→443 [ACK] Seq=1 Ack=14459017 Win=65340

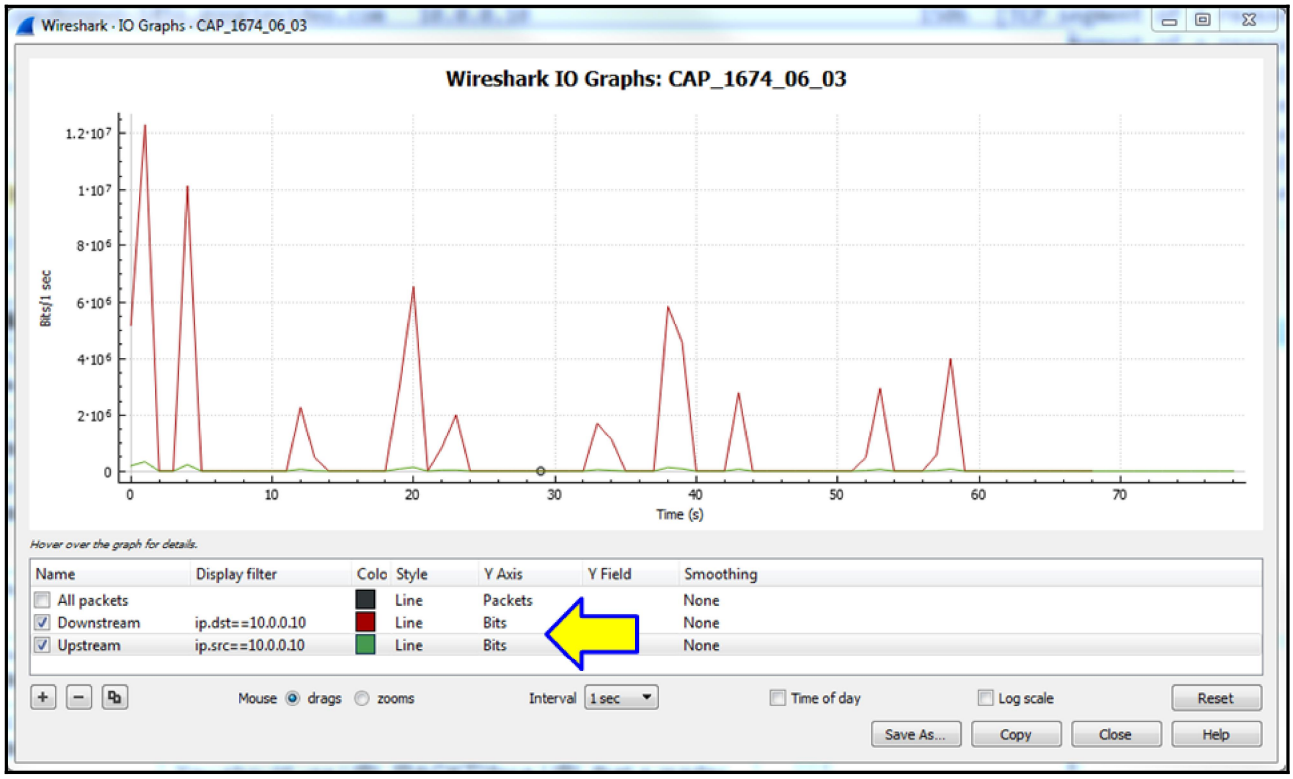

Time (s)
Click to select packet 2621 (128s = 12).
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
Download
ip.dst==10.0.0.10
Line
Packets
Enter a fiel...
None
Upload
ip.src==10.0.0.10
Line
None
Mouse
drags
zooms
Packets
Bytes
Bits
SUM(Y Field)
COUNT FRAMES(Y Field)
COUNT FIELDS(Y Field)
MAX(Y Field)
MIN(Y Field)
AVG(Y Field)
LOAD(Y Field)

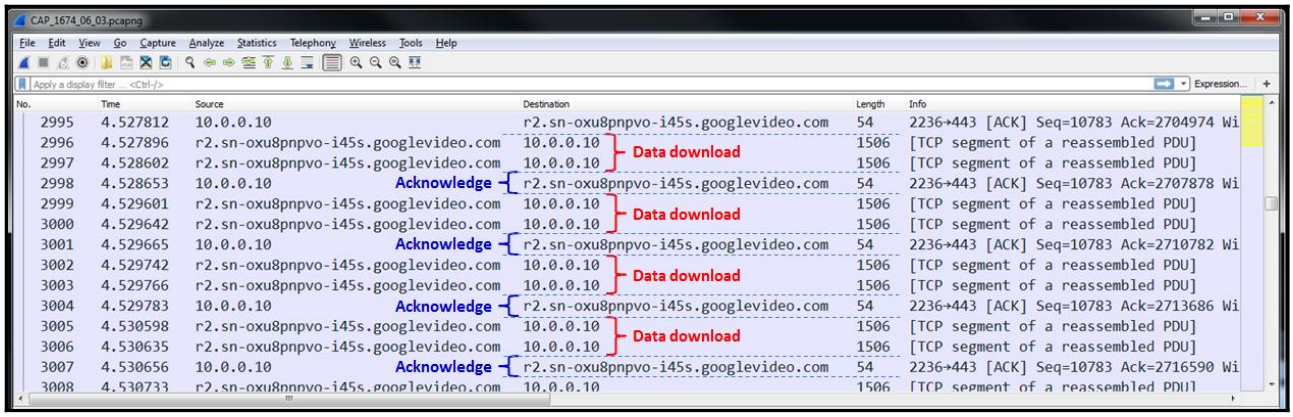

Click to select packet 688 (21s = 125).
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
Download
ip.dst==10.0.0.10
Line
Packets
Enter a fiel...
None
Upload
ip.src==10.0.0.10
Line
Packets
Mouse
drags
zooms
Interval
1 sec
Save As...
None
10 interval SMA
20 interval SMA
50 interval SMA
100 interval SMA
200 interval SMA
500 interval SMA
1000 interval SMA

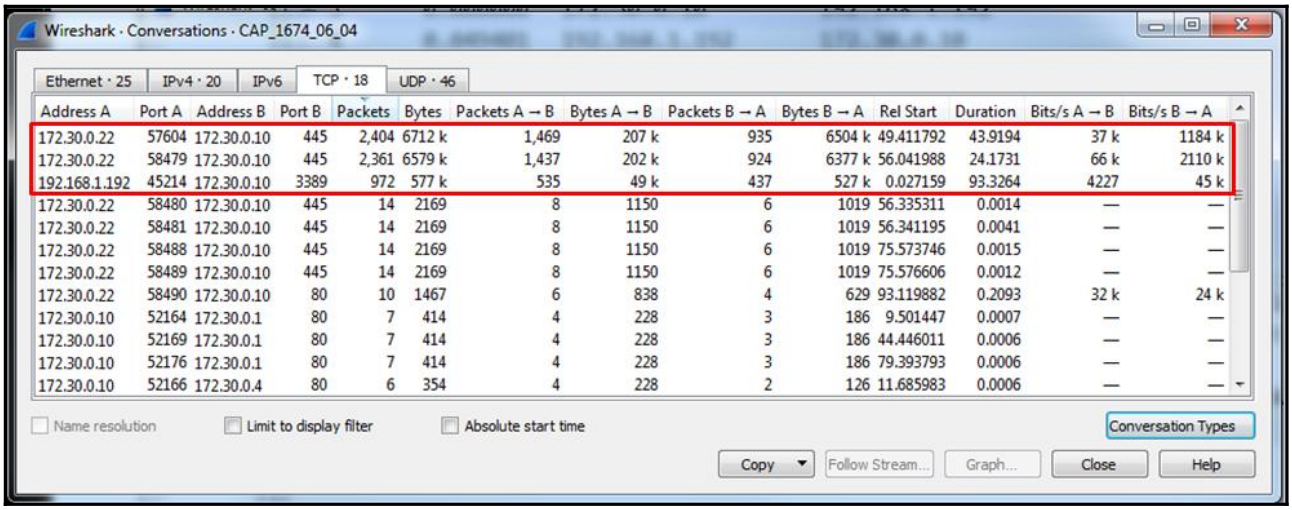

0
0
120
180
240
300
360
Time (s)
Click to select packet 1538 (64s = 45).
Name
Display filter
Smoothing
All packets
None
Download
None
Upload
None
Time of day
Log scale
Save As...
Copy
Valuable and amazing time-saving keyboard shortcuts
+ Zoom in
- Zoom out
x Zoom in X axis
X Zoom out X axis
y Zoom in Y axis
Y Zoom out Y axis
0 Reset graph to its initial state
→ Move right 10 pixels
← Move left 10 pixels
↑ Move up 10 pixels
↓ Move down 10 pixels
Shift+→ Move right 1 pixel
Shift+← Move left 1 pixel
Shift+↑ Move up 1 pixel
Shift+↓ Move down 1 pixel
g Go to packet under cursor
z Toggle mouse drag / zoom
t Toggle capture / session time origin
Space Toggle crosshairs

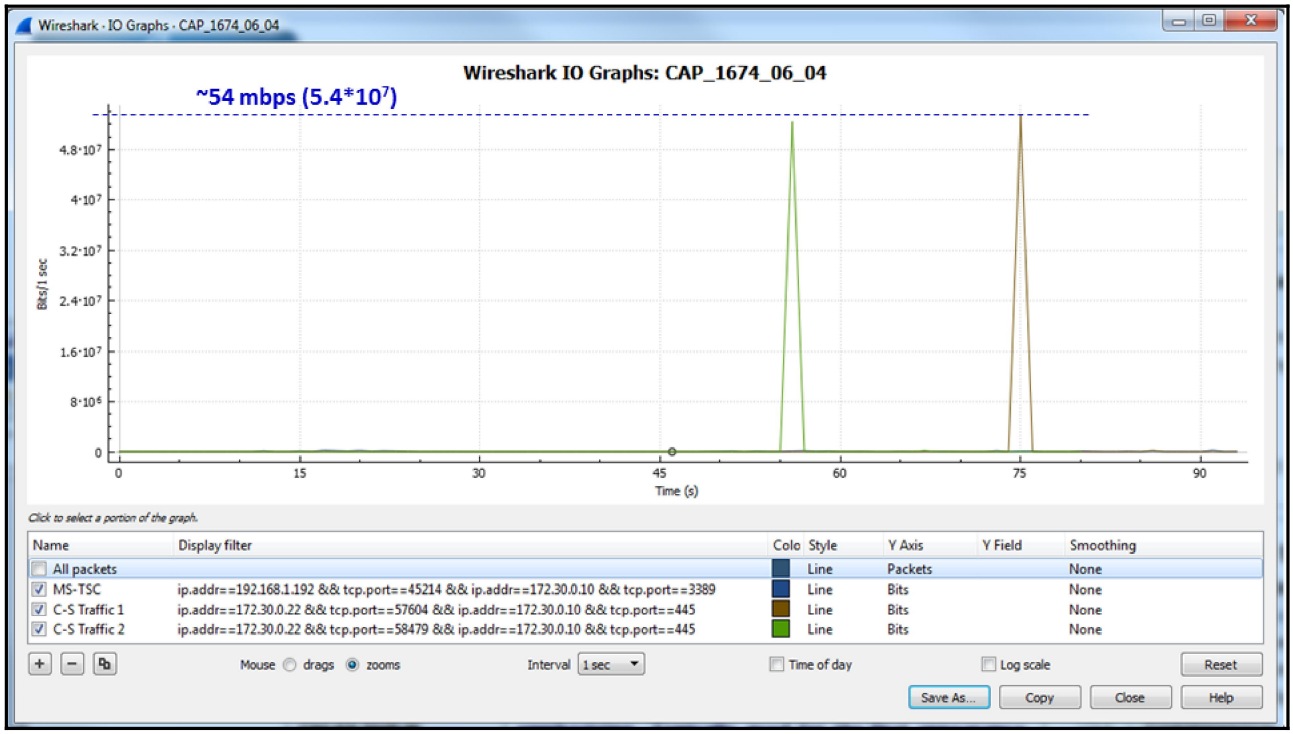

Line/Port
End device
Connection
Effective application throughput

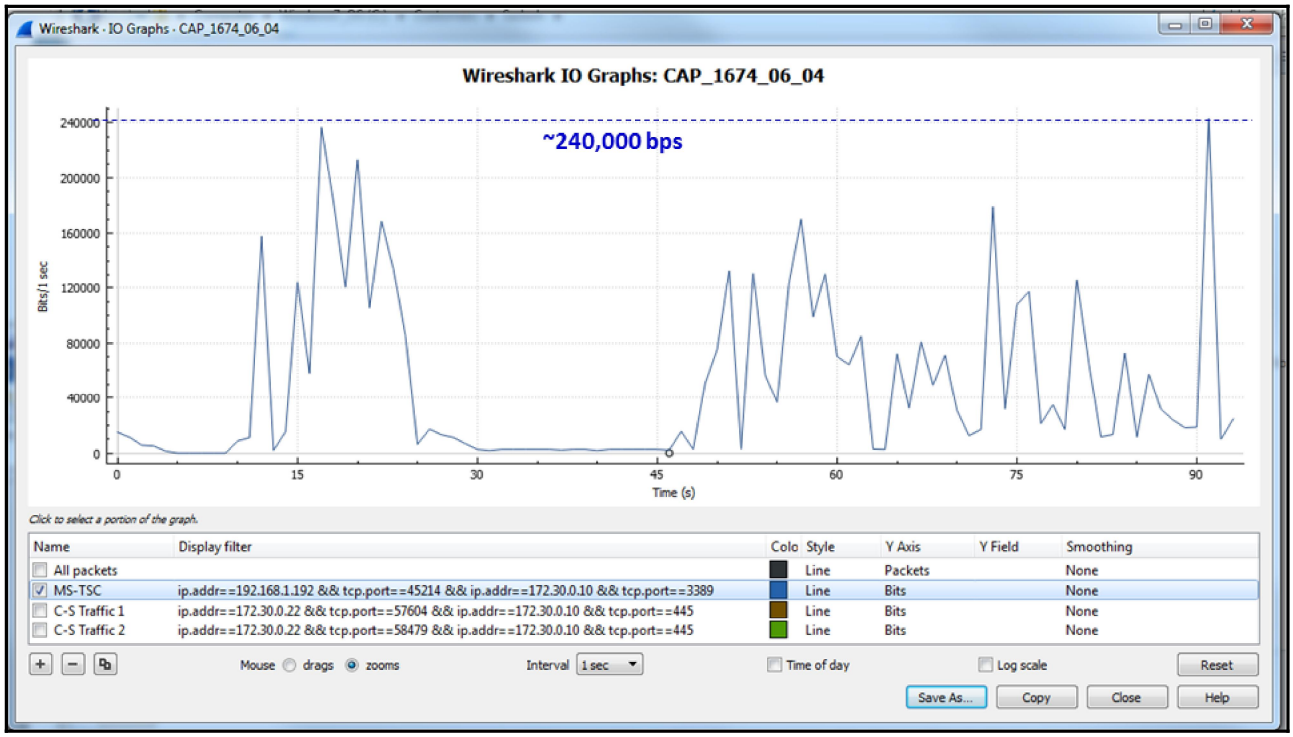

Wireshark · IO Graphs · CAP_1674_06_03
Wireshark IO Graphs: CAP_1674_06_03
Packets/1 sec
Time (s)
Hover over the graph for details.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
Downstream
ip.dst==10.0.0.10
Line
Packets
None
Upstream
ip.src==10.0.0.10
Line
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

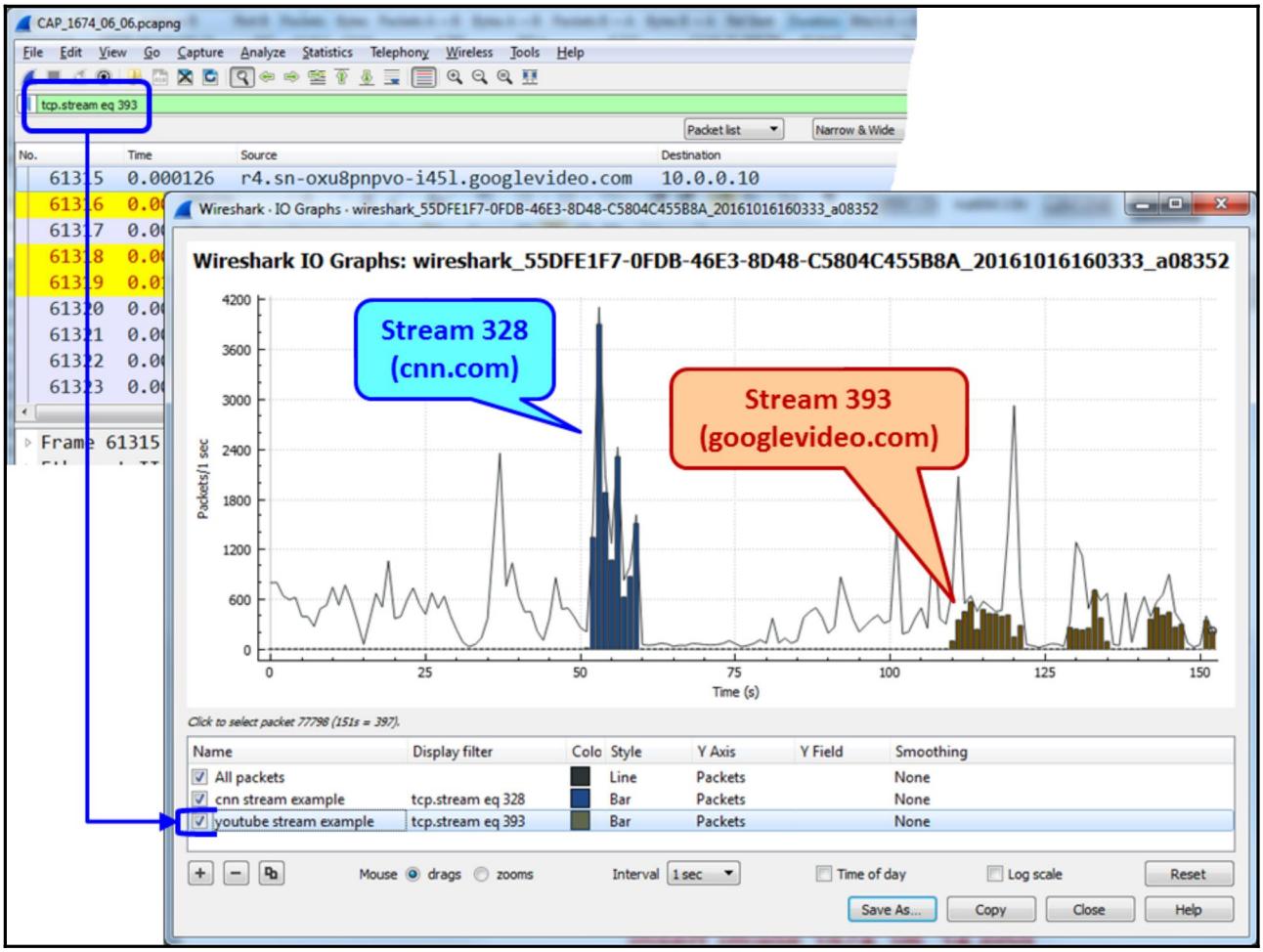

Wireshark · IO Graphs · CAP_1674_06_03
Wireshark IO Graphs: CAP_1674_06_03
Bits/1 sec
Time (s)
Hover over the graph for details.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
Downstream
ip.dst==10.0.0.10
Line
Bits
None
Upstream
ip.src==10.0.0.10
Line
Bits
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

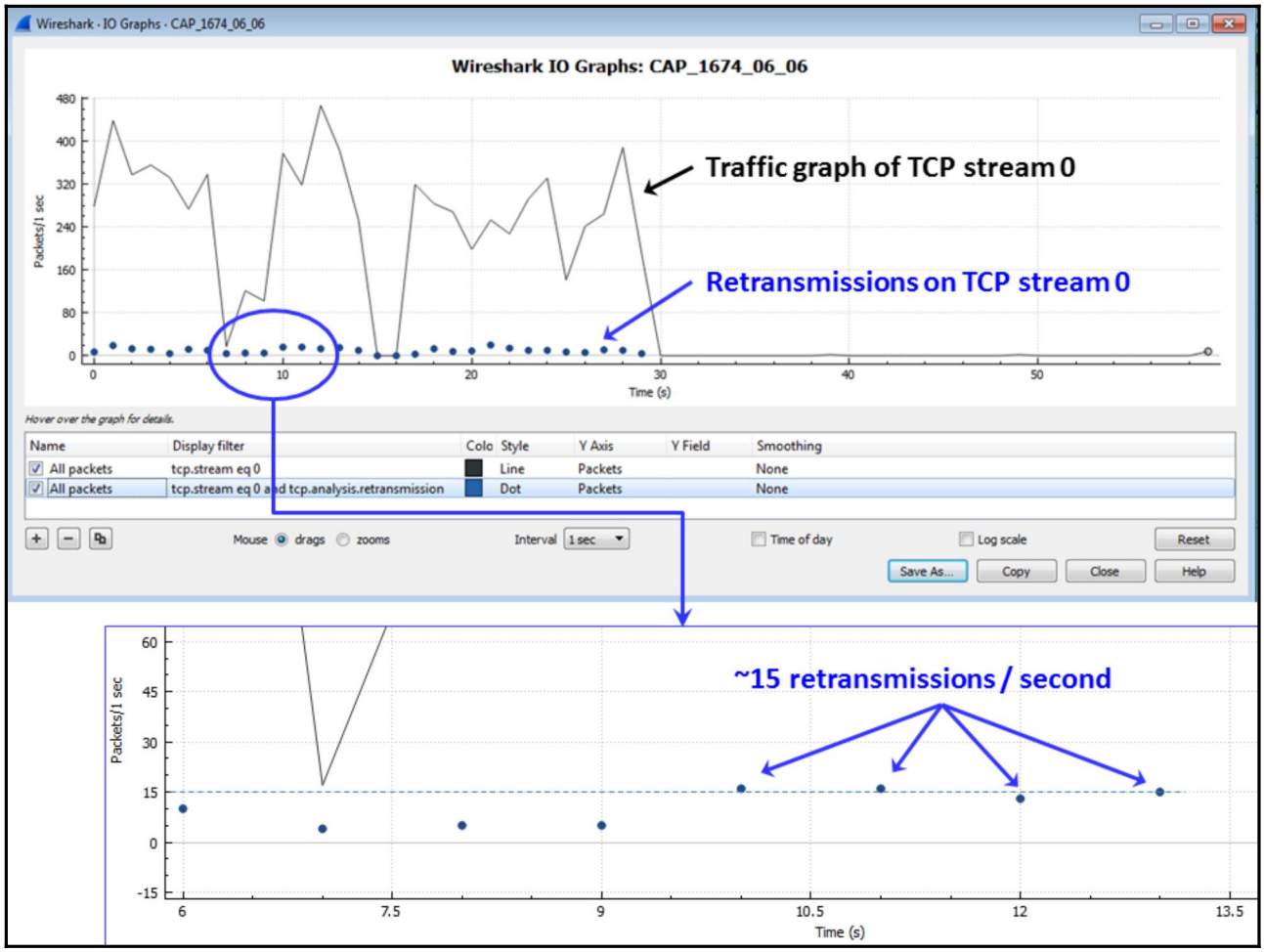

CAP_1674_06_03.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Length Info
2995 4.527812 10.0.0.10 r2.sn-oxu8pnpvo-i45s.googlevideo.com 54 2236→443 [ACK] Seq=10783 Ack=2704974 Wi
2996 4.527896 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
2997 4.528602 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
2998 4.528653 10.0.0.10 r2.sn-oxu8pnpvo-i45s.googlevideo.com 54 2236→443 [ACK] Seq=10783 Ack=2707878 Wi
2999 4.529601 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3000 4.529642 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3001 4.529665 10.0.0.10 r2.sn-oxu8pnpvo-i45s.googlevideo.com 54 2236→443 [ACK] Seq=10783 Ack=2710782 Wi
3002 4.529742 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3003 4.529766 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3004 4.529783 10.0.0.10 r2.sn-oxu8pnpvo-i45s.googlevideo.com 54 2236→443 [ACK] Seq=10783 Ack=2713686 Wi
3005 4.530598 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3006 4.530635 r2.sn-oxu8pnpvo-i45s.googlevideo.com 10.0.0.10 1506 [TCP segment of a reassembled PDU]
3007 4.530656 10.0.0.10 r2.sn-oxu8pnpvo-i45s.googlevideo.com 54 2236→443 [ACK] Seq=10783 Ack=2716590 Wi
Data download
Acknowledge
Data download
Acknowledge
Data download
Acknowledge
Data download

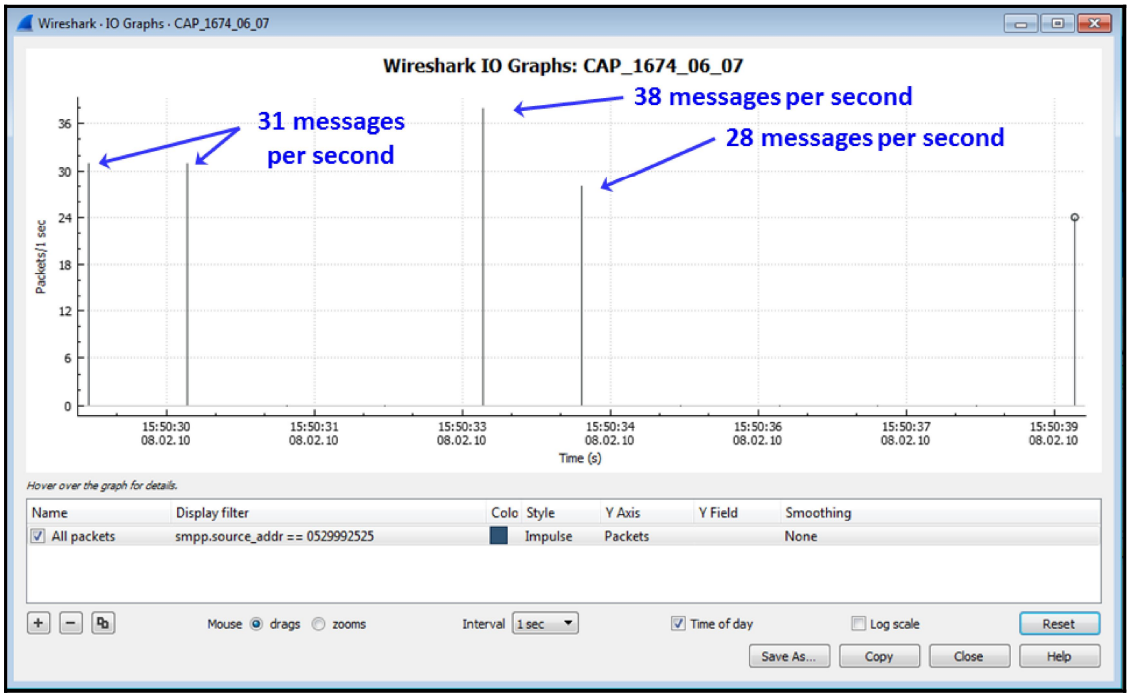

Wireshark · Conversations · CAP_1674_06_04
Ethernet · 25
IPv4 · 20
IPv6
TCP · 18
UDP · 46
Address A Port A Address B Port B Packets Bytes Packets A → B Bytes A → B Packets B → A Bytes B → A Rel Start Duration Bits/s A → B Bits/s B → A
172.30.0.22 57604 172.30.0.10 445 2,404 6712 k 1,469 207 k 935 6504 k 49.411792 43.9194 37 k 1184 k
172.30.0.22 58479 172.30.0.10 445 2,361 6579 k 1,437 202 k 924 6377 k 56.041988 24.1731 66 k 2110 k
192.168.1.192 45214 172.30.0.10 3389 972 577 k 535 49 k 437 527 k 0.027159 93.3264 4227 45 k
172.30.0.22 58480 172.30.0.10 445 14 2169 8 1150 6 1019 56.335311 0.0014 — —
172.30.0.22 58481 172.30.0.10 445 14 2169 8 1150 6 1019 56.341195 0.0041 — —
172.30.0.22 58488 172.30.0.10 445 14 2169 8 1150 6 1019 75.573746 0.0015 — —
172.30.0.22 58489 172.30.0.10 445 14 2169 8 1150 6 1019 75.576606 0.0012 — —
172.30.0.22 58490 172.30.0.10 80 10 1467 6 838 4 629 93.119882 0.2093 32 k 24 k
172.30.0.10 52164 172.30.0.1 80 7 414 4 228 3 186 9.501447 0.0007 — —
172.30.0.10 52169 172.30.0.1 80 7 414 4 228 3 186 44.446011 0.0006 — —
172.30.0.10 52176 172.30.0.1 80 7 414 4 228 3 186 79.393793 0.0006 — —
172.30.0.10 52166 172.30.0.4 80 6 354 4 228 2 126 11.685983 0.0006 — —
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

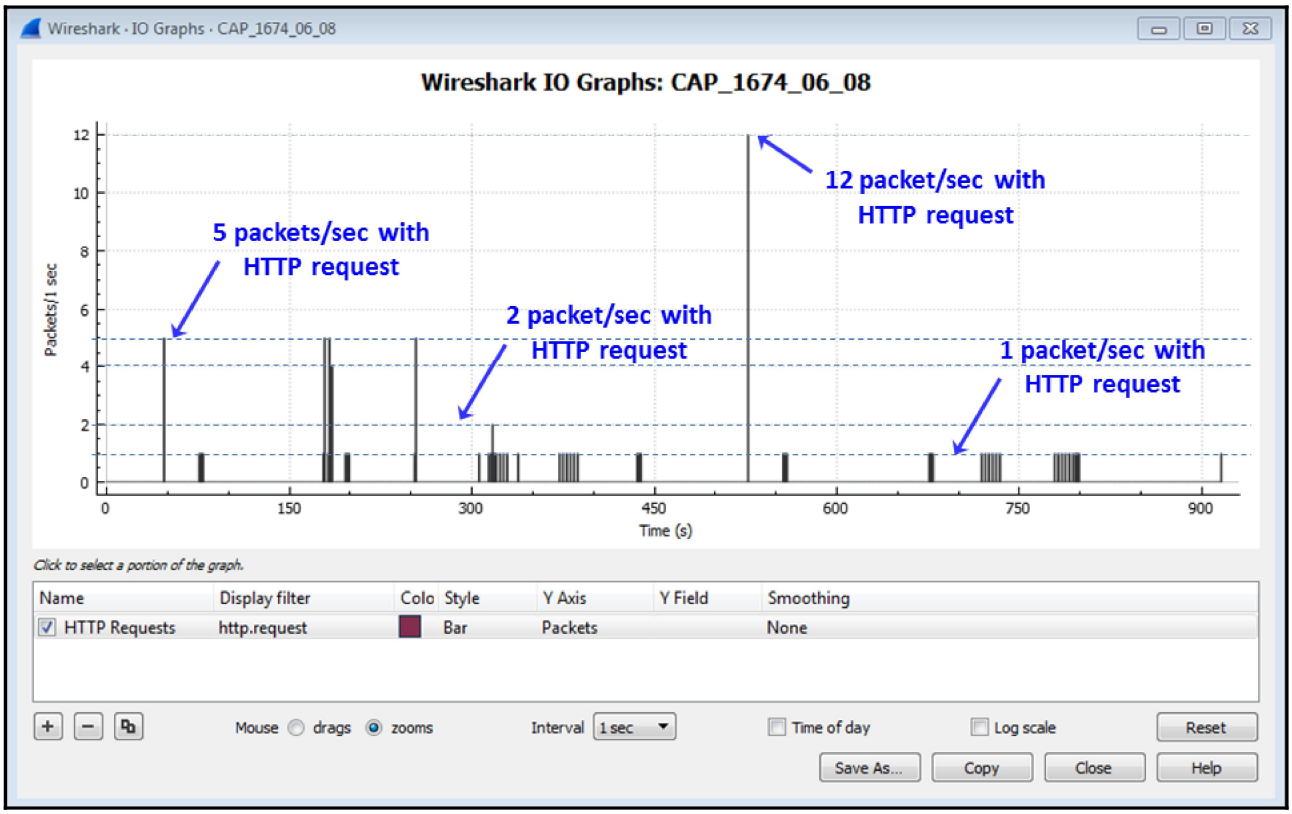

Wireshark · IO Graphs · CAP_1674_06_04
Wireshark IO Graphs: CAP_1674_06_04
~54 mbps (5.4*10^7)
4.8·10^7
4·10^7
3.2·10^7
2.4·10^7
1.6·10^7
8·10^6
0
Bits/1 sec
0
15
30
45
60
75
90
Time (s)
Click to select a portion of the graph.
Name Display filter Colo Style Y Axis Y Field Smoothing
All packets Line Packets None
MS-TSC ip.addr==192.168.1.192 && tcp.port==45214 && ip.addr==172.30.0.10 && tcp.port==3389 Line Bits None
C-S Traffic 1 ip.addr==172.30.0.22 && tcp.port==57604 && ip.addr==172.30.0.10 && tcp.port==445 Line Bits None
C-S Traffic 2 ip.addr==172.30.0.22 && tcp.port==58479 && ip.addr==172.30.0.10 && tcp.port==445 Line Bits None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help


Wireshark · IO Graphs · CAP_1674_06_04
Wireshark IO Graphs: CAP_1674_06_04
~240,000 bps
Bits/1 sec
240000
200000
160000
120000
80000
40000
0
0
15
30
45
60
75
90
Time (s)
Click to select a portion of the graph.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Line
Packets
None
MS-TSC
ip.addr==192.168.1.192 && tcp.port==45214 && ip.addr==172.30.0.10 && tcp.port==3389
Line
Bits
None
C-S Traffic 1
ip.addr==172.30.0.22 && tcp.port==57604 && ip.addr==172.30.0.10 && tcp.port==445
Line
Bits
None
C-S Traffic 2
ip.addr==172.30.0.22 && tcp.port==58479 && ip.addr==172.30.0.10 && tcp.port==445
Line
Bits
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

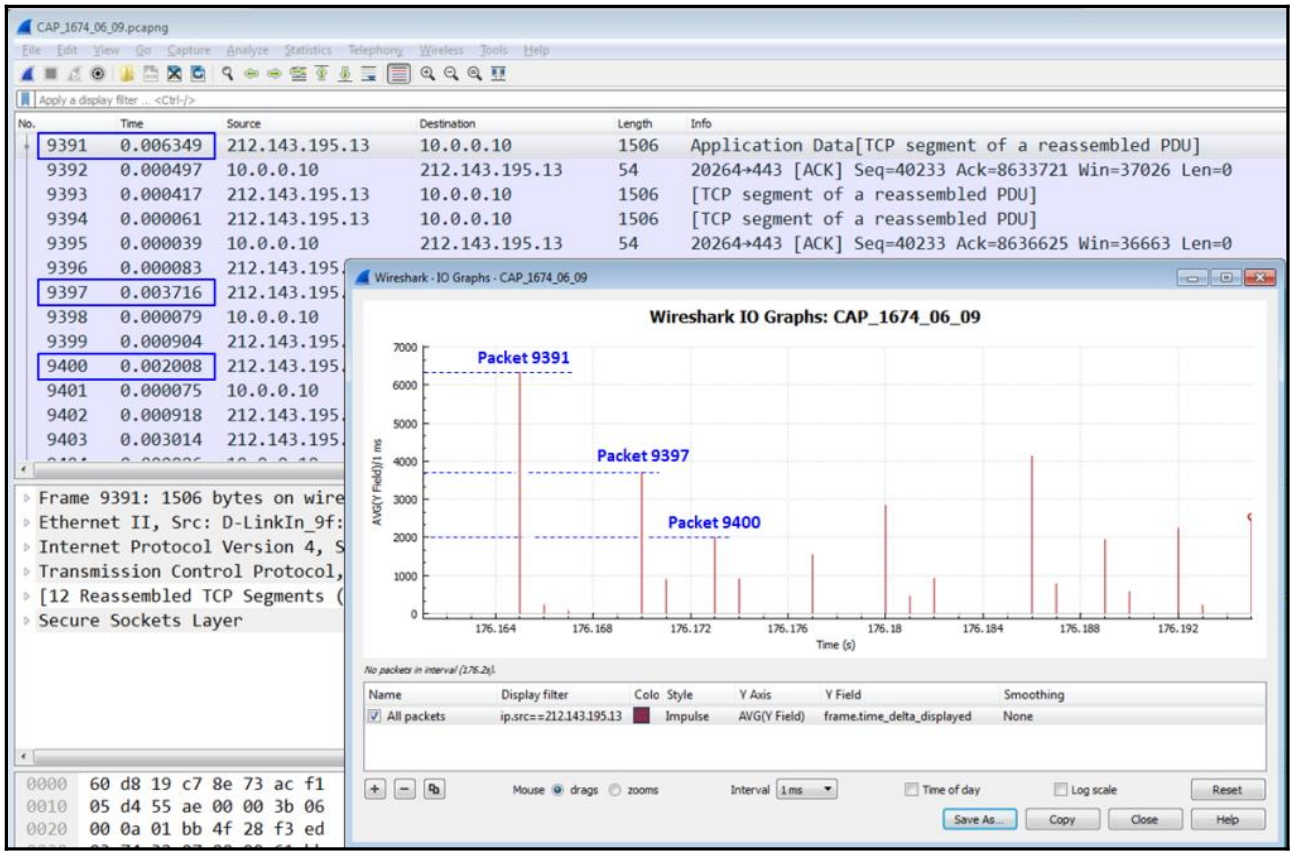

CAP_1674_06_06.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 393
Packet list
Narrow & Wide
No. Time Source Destination
61315 0.000126 r4.sn-oxu8pnpvo-i45l.googlevideo.com 10.0.0.10
Wireshark · IO Graphs · wireshark_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_20161016160333_a08352
Wireshark IO Graphs: wireshark_55DFE1F7-0FDB-46E3-8D48-C5804C455B8A_20161016160333_a08352
Stream 328 (cnn.com)
Stream 393 (googlevideo.com)
Packets/1 sec
Time (s)
Click to select packet 77798 (151s = 397).
Name Display filter Colo Style Y Axis Y Field Smoothing
All packets Line Packets None
cnn stream example tcp.stream eq 328 Bar Packets None
youtube stream example tcp.stream eq 393 Bar Packets None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

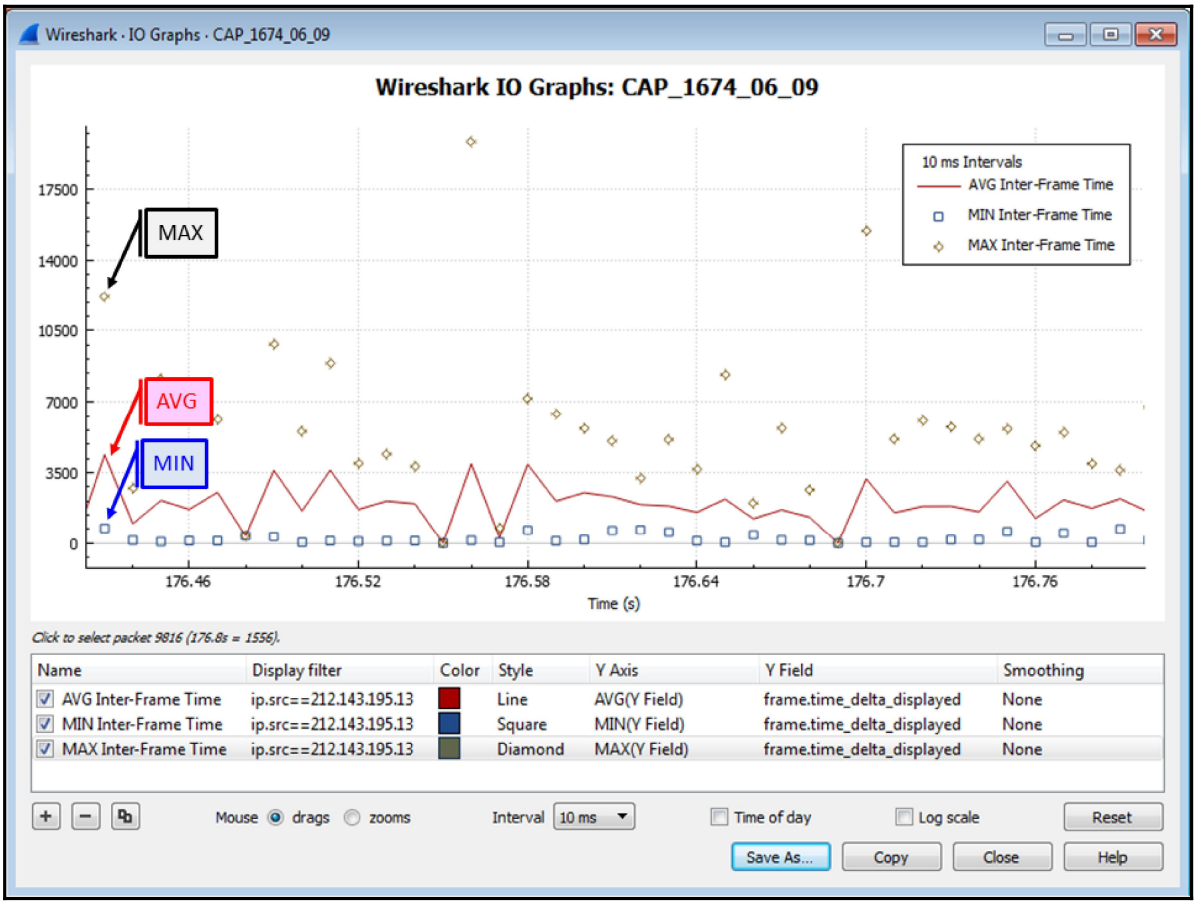

Wireshark · IO Graphs · CAP_1674_06_06
Wireshark IO Graphs: CAP_1674_06_06
Traffic graph of TCP stream 0
Retransmissions on TCP stream 0
Packets/1 sec
Time (s)
Hover over the graph for details.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
tcp.stream eq 0
Line
Packets
None
All packets
tcp.stream eq 0 and tcp.analysis.retransmission
Dot
Packets
None
Mouse drags zooms
Interval 1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help
~15 retransmissions / second
Packets/1 sec
Time (s)

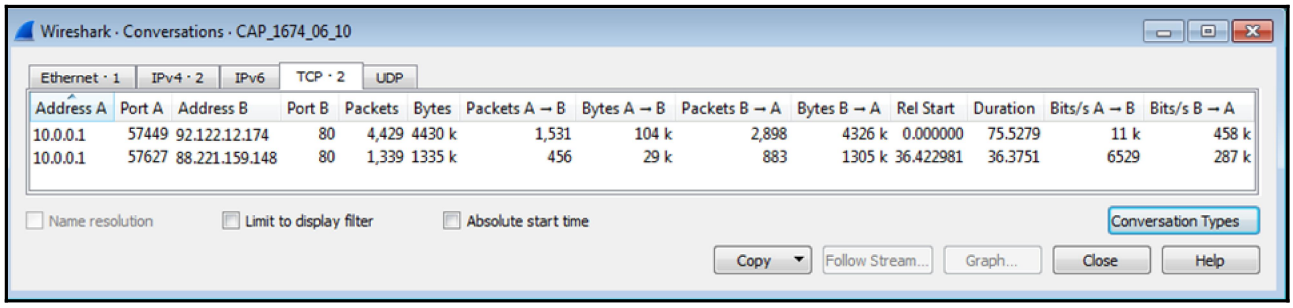

Wireshark · IO Graphs · CAP_1674_06_07
Wireshark IO Graphs: CAP_1674_06_07
31 messages per second
38 messages per second
28 messages per second
Packets/1 sec
Time (s)
Hover over the graph for details.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
smpp.source_addr == 0529992525
Impulse
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

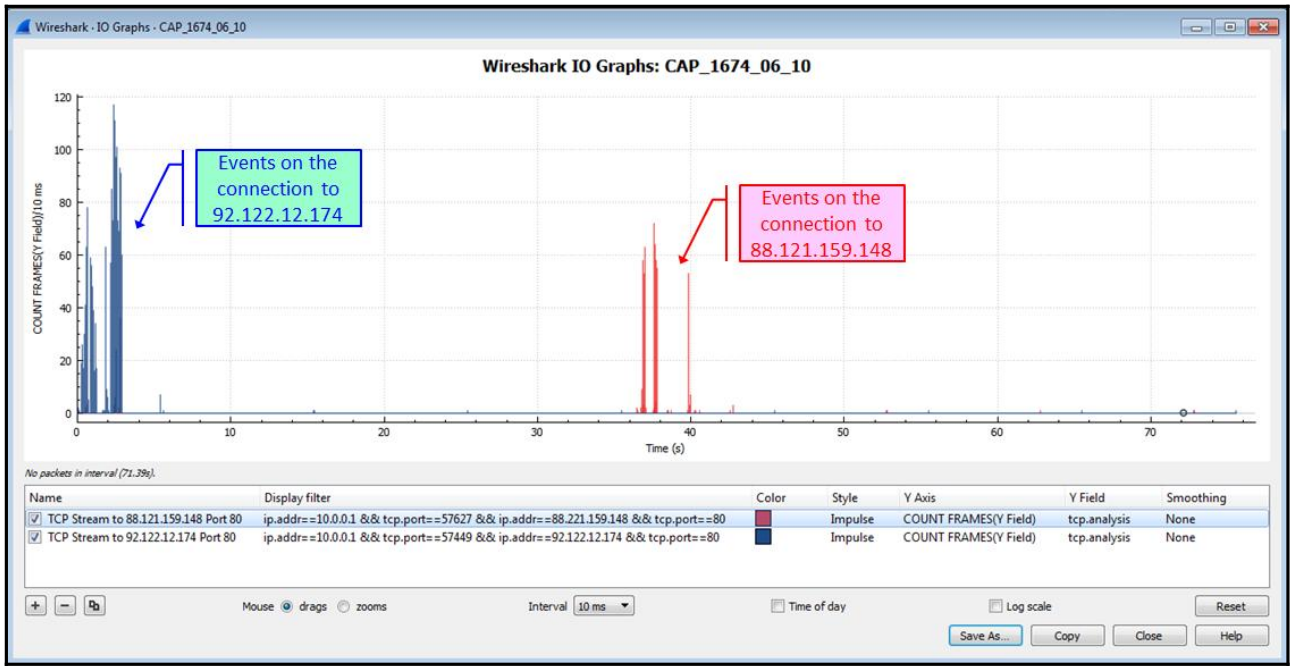

Wireshark · IO Graphs · CAP_1674_06_08
Wireshark IO Graphs: CAP_1674_06_08
5 packets/sec with HTTP request
2 packet/sec with HTTP request
12 packet/sec with HTTP request
1 packet/sec with HTTP request
Packets/1 sec
Time (s)
Click to select a portion of the graph.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
HTTP Requests
http.request
Bar
Packets
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

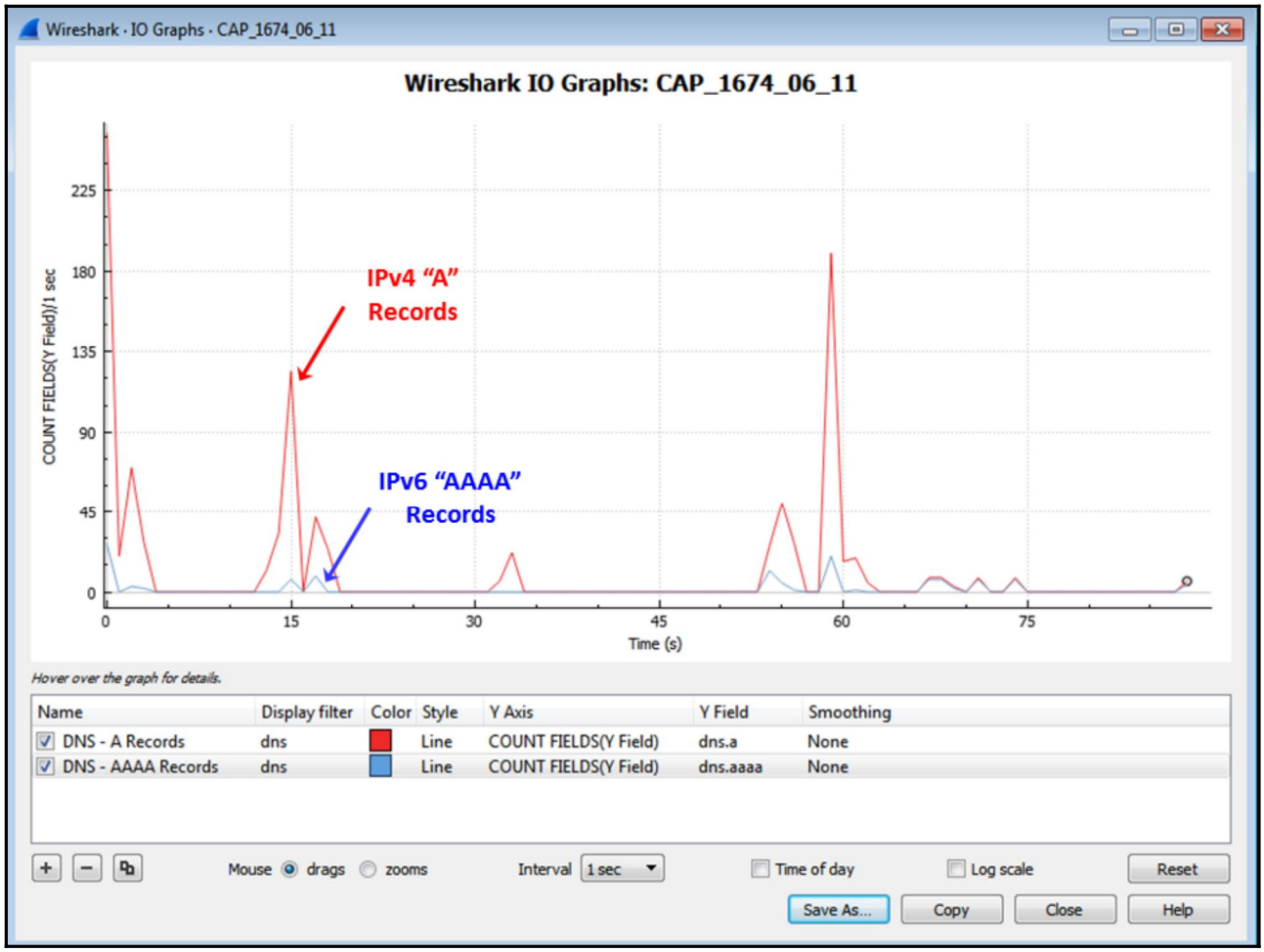

900
450
0
0
150
300
450
600
Time (s)
Hover over the graph for details.
Name
Display filter
Colo
Style
Y Axis
Y Field
Smoothing
All packets
Enter a display filt...
Line
Packets
Enter a field ...
None
Packets
Bytes
Bits
SUM(Y Field)
COUNT FRAMES(Y Field)
COUNT FIELDS(Y Field)
MAX(Y Field)
MIN(Y Field)
AVG(Y Field)
LOAD(Y Field)
Mouse
drags
zooms
Time of day
Save As...

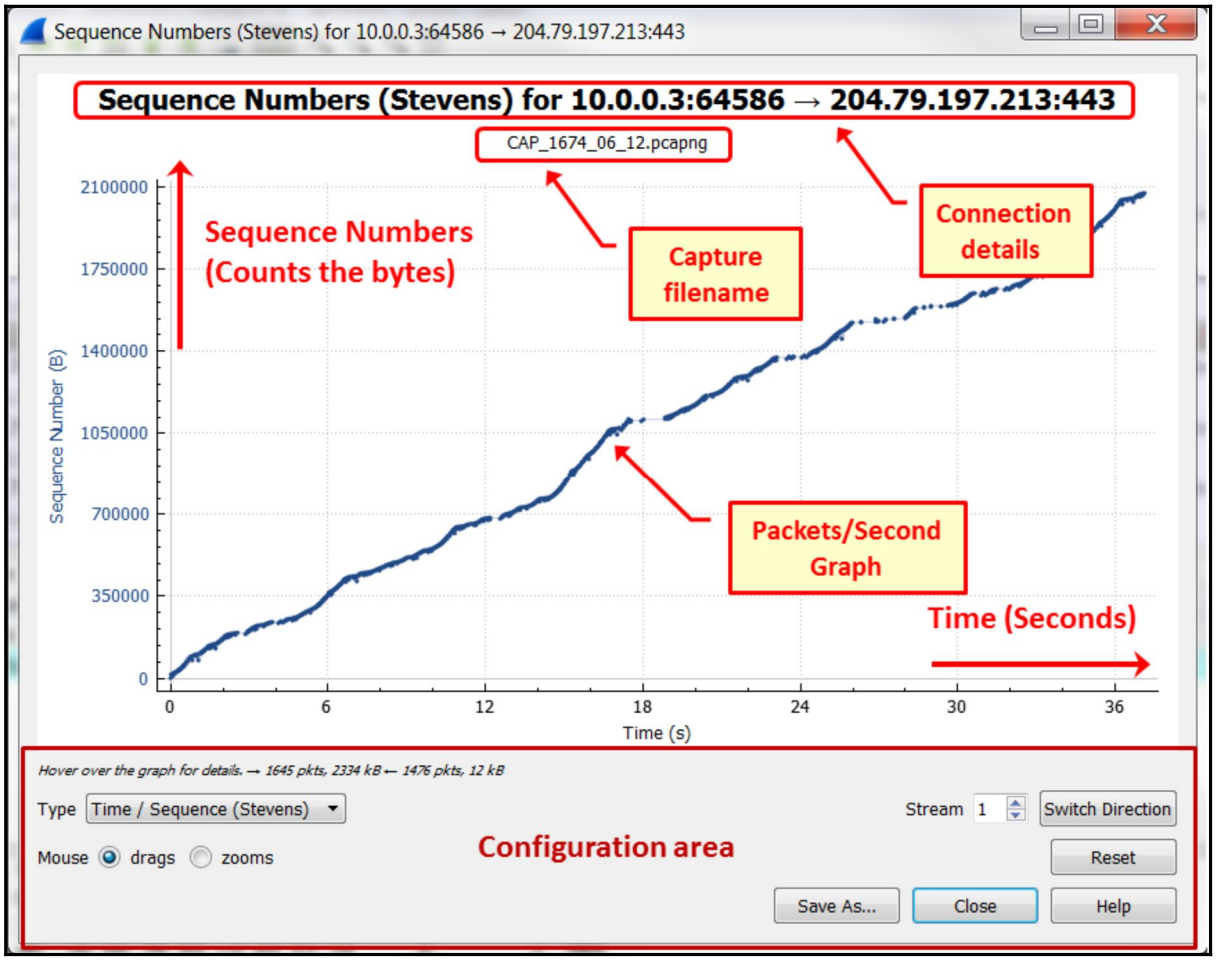

CAP_1674_06_09.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Length Info
9391 0.006349 212.143.195.13 10.0.0.10 1506 Application Data[TCP segment of a reassembled PDU]
9392 0.000497 10.0.0.10 212.143.195.13 54 20264→443 [ACK] Seq=40233 Ack=8633721 Win=37026 Len=0
9393 0.000417 212.143.195.13 10.0.0.10 1506 [TCP segment of a reassembled PDU]
9394 0.000061 212.143.195.13 10.0.0.10 1506 [TCP segment of a reassembled PDU]
9395 0.000039 10.0.0.10 212.143.195.13 54 20264→443 [ACK] Seq=40233 Ack=8636625 Win=36663 Len=0
9396 0.000083 212.143.195.
9397 0.003716 212.143.195.
9398 0.000079 10.0.0.10
9399 0.000904 212.143.195.
9400 0.002008 212.143.195.
9401 0.000075 10.0.0.10
9402 0.000918 212.143.195.
9403 0.003014 212.143.195.
Frame 9391: 1506 bytes on wire
Ethernet II, Src: D-LinkIn_9f:
Internet Protocol Version 4, S
Transmission Control Protocol,
[12 Reassembled TCP Segments (
Secure Sockets Layer
0000 60 d8 19 c7 8e 73 ac f1
0010 05 d4 55 ae 00 00 3b 06
0020 00 0a 01 bb 4f 28 f3 ed
Wireshark · IO Graphs · CAP_1674_06_09
Wireshark IO Graphs: CAP_1674_06_09
Packet 9391
Packet 9397
Packet 9400
AVG(Y Field)/1 ms
Time (s)
No packets in interval (176.2s).
Name Display filter Colo Style Y Axis Y Field Smoothing
All packets ip.src==212.143.195.13 Impulse AVG(Y Field) frame.time_delta_displayed None
Mouse drags zooms Interval 1 ms Time of day Log scale Reset
Save As... Copy Close Help

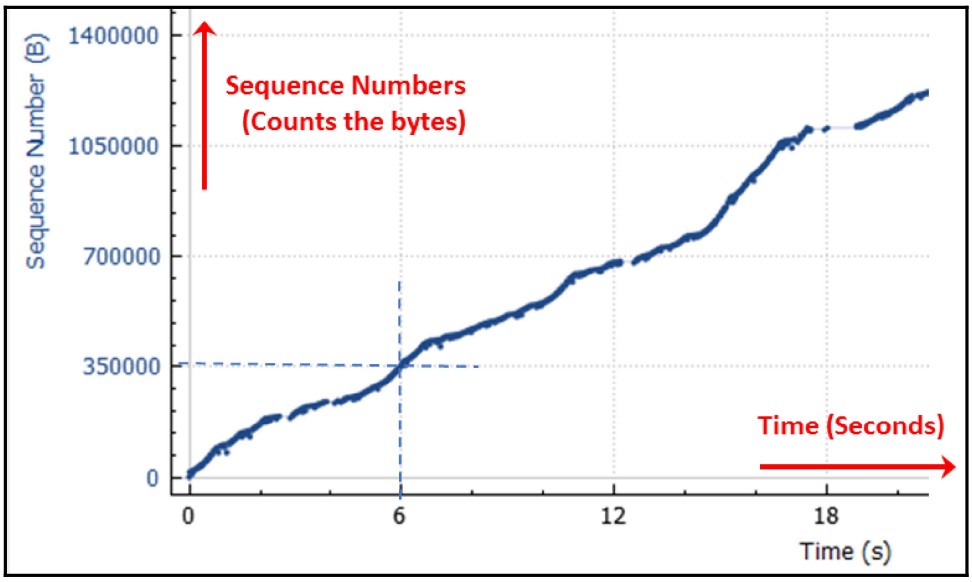

Wireshark · IO Graphs · CAP_1674_06_09
Wireshark IO Graphs: CAP_1674_06_09
10 ms Intervals
AVG Inter-Frame Time
MIN Inter-Frame Time
MAX Inter-Frame Time
MAX
AVG
MIN
17500
14000
10500
7000
3500
0
176.46
176.52
176.58
176.64
176.7
176.76
Time (s)
Click to select packet 9816 (176.8s = 1556).
Name
Display filter
Color
Style
Y Axis
Y Field
Smoothing
AVG Inter-Frame Time
ip.src==212.143.195.13
Line
AVG(Y Field)
frame.time_delta_displayed
None
MIN Inter-Frame Time
ip.src==212.143.195.13
Square
MIN(Y Field)
frame.time_delta_displayed
None
MAX Inter-Frame Time
ip.src==212.143.195.13
Diamond
MAX(Y Field)
frame.time_delta_displayed
None
Mouse
drags
zooms
Interval
10 ms
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

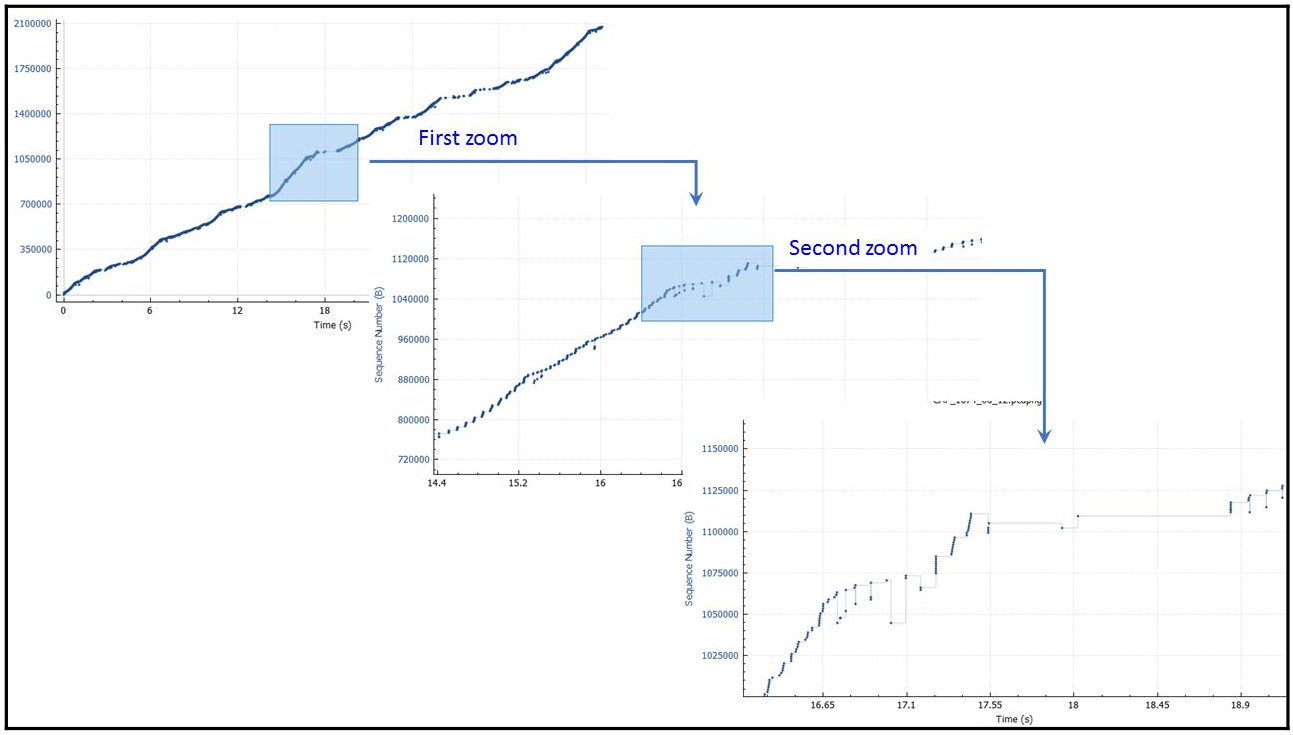

Wireshark · Conversations · CAP_1674_06_10
Ethernet · 1
IPv4 · 2
IPv6
TCP · 2
UDP
Address A
Port A
Address B
Port B
Packets
Bytes
Packets A → B
Bytes A → B
Packets B → A
Bytes B → A
Rel Start
Duration
Bits/s A → B
Bits/s B → A
10.0.0.1 57449 92.122.12.174 80 4,429 4430 k 1,531 104 k 2,898 4326 k 0.000000 75.5279 11 k 458 k
10.0.0.1 57627 88.221.159.148 80 1,339 1335 k 456 29 k 883 1305 k 36.422981 36.3751 6529 287 k
Name resolution
Limit to display filter
Absolute start time
Conversation Types
Copy
Follow Stream...
Graph...
Close
Help

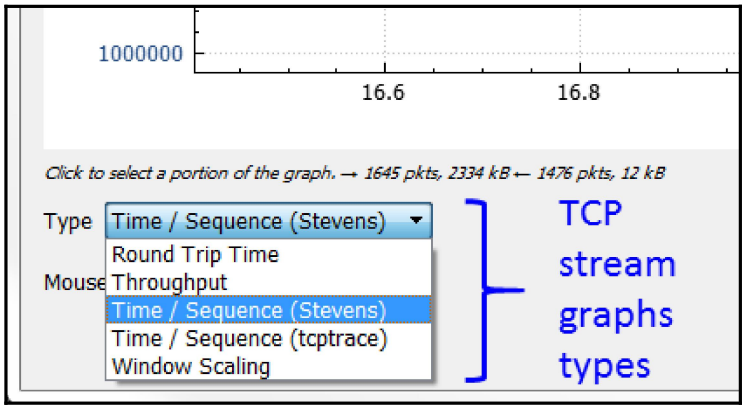

Wireshark · IO Graphs · CAP_1674_06_10
Wireshark IO Graphs: CAP_1674_06_10
Events on the connection to 92.122.12.174
Events on the connection to 88.121.159.148
COUNT FRAMES(Y Field)/10 ms
Time (s)
No packets in interval (71.39s).
Name
Display filter
Color
Style
Y Axis
Y Field
Smoothing
TCP Stream to 88.121.159.148 Port 80
ip.addr==10.0.0.1 && tcp.port==57627 && ip.addr==88.221.159.148 && tcp.port==80
Impulse
COUNT FRAMES(Y Field)
tcp.analysis
None
TCP Stream to 92.122.12.174 Port 80
ip.addr==10.0.0.1 && tcp.port==57449 && ip.addr==92.122.12.174 && tcp.port==80
Impulse
COUNT FRAMES(Y Field)
tcp.analysis
None
Mouse drags zooms
Interval 10 ms
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

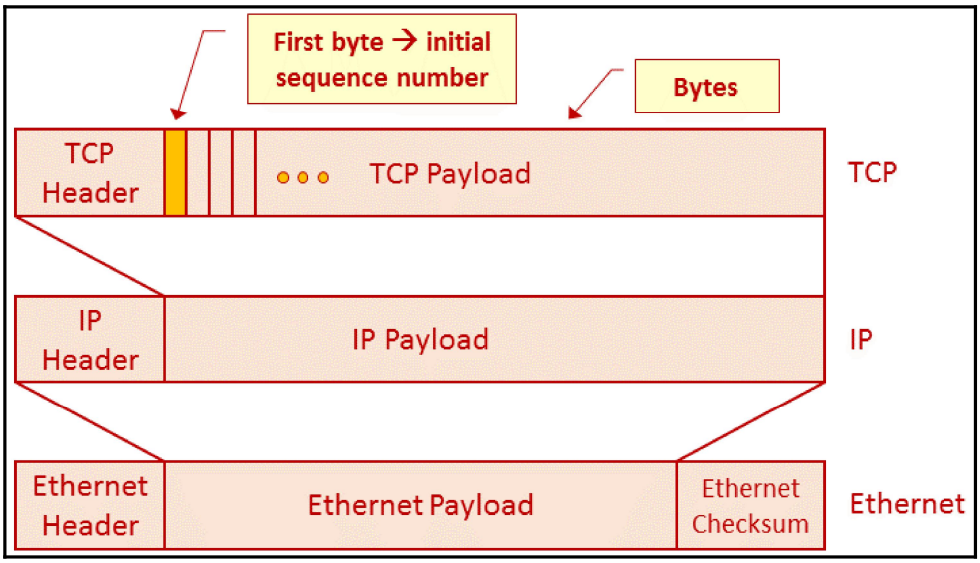

Wireshark · IO Graphs · CAP_1674_06_11
Wireshark IO Graphs: CAP_1674_06_11
COUNT FIELDS(Y Field)/1 sec
225
180
135
90
45
0
IPv4 "A" Records
IPv6 "AAAA" Records
0
15
30
45
60
75
Time (s)
Hover over the graph for details.
Name
Display filter
Color
Style
Y Axis
Y Field
Smoothing
DNS - A Records
dns
Line
COUNT FIELDS(Y Field)
dns.a
None
DNS - AAAA Records
dns
Line
COUNT FIELDS(Y Field)
dns.aaaa
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Save As...
Copy
Close
Help

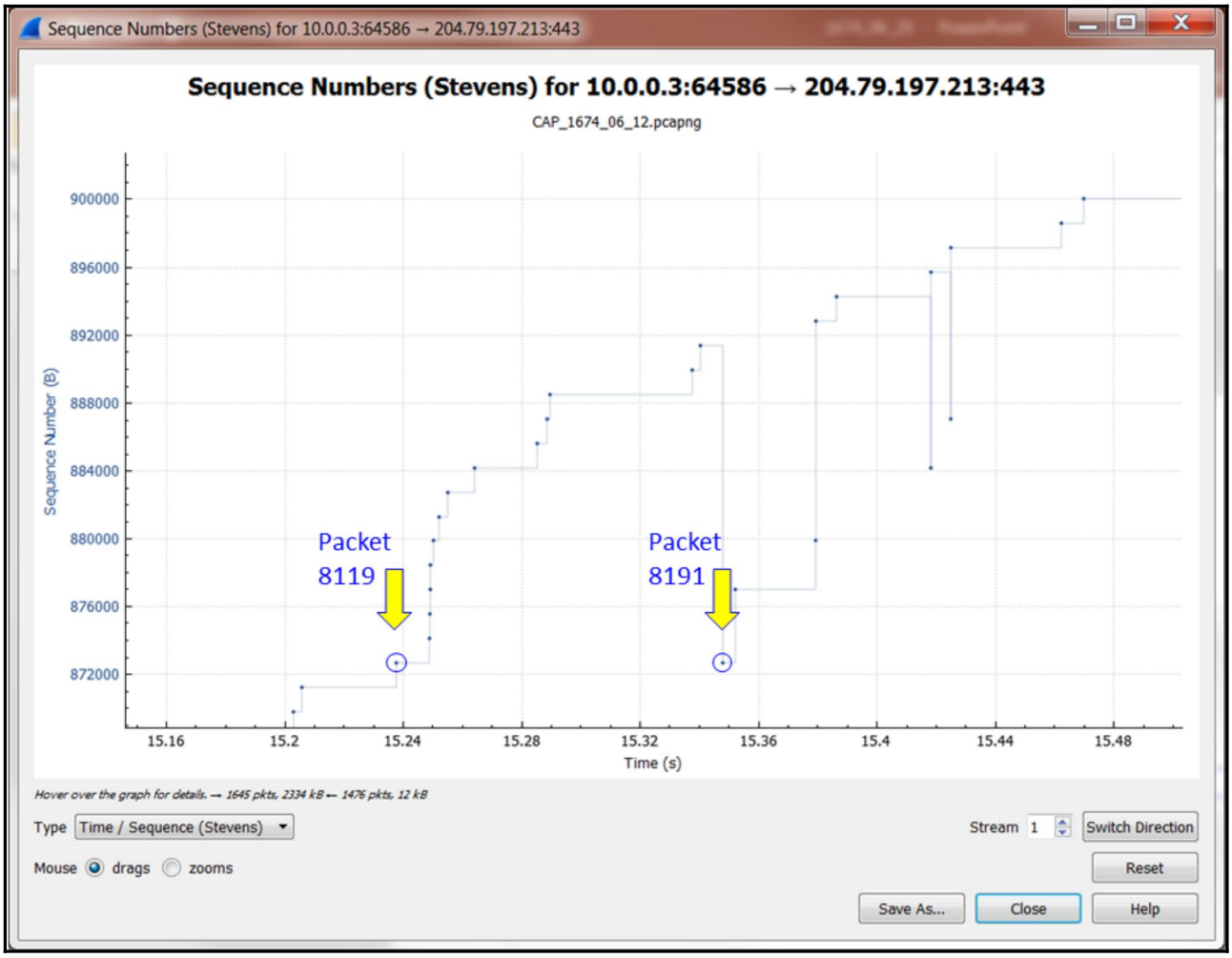

Sequence Numbers (Stevens) for 10.0.0.3:64586 → 204.79.197.213:443
Sequence Numbers (Stevens) for 10.0.0.3:64586 → 204.79.197.213:443
CAP_1674_06_12.pcapng
Sequence Numbers
(Counts the bytes)
Capture
filename
Connection
details
Packets/Second
Graph
Time (Seconds)
Sequence Number (B)
Time (s)
2100000
1750000
1400000
1050000
700000
350000
0
0
6
12
18
24
30
36
Hover over the graph for details. → 1645 pkts, 2334 kB ← 1476 pkts, 12 kB
Type
Time / Sequence (Stevens)
Stream
1
Switch Direction
Mouse
drags
zooms
Configuration area
Reset
Save As...
Close
Help

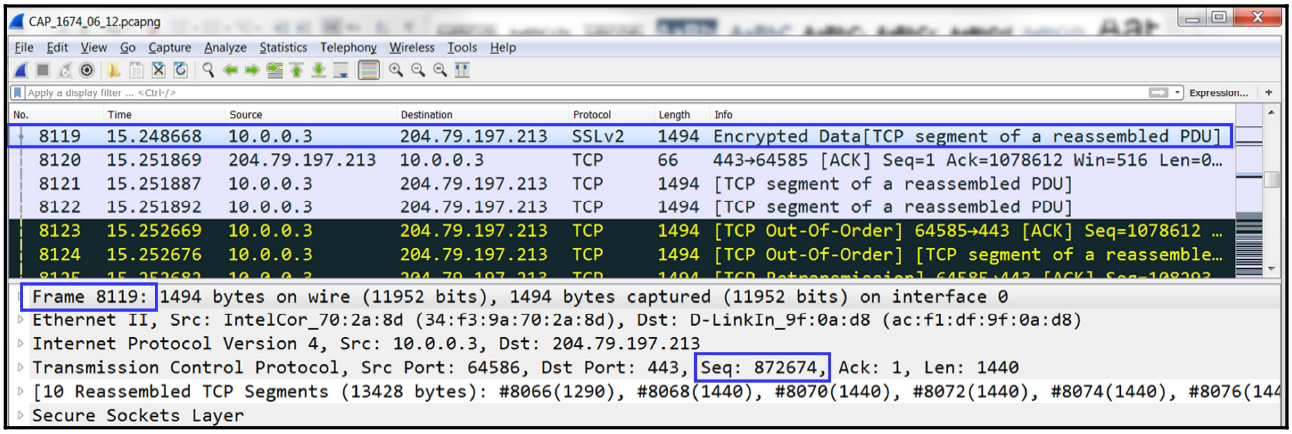

Sequence Number (B)
1400000
1050000
700000
350000
0
Sequence Numbers
(Counts the bytes)
Time (Seconds)
0
6
12
18
Time (s)

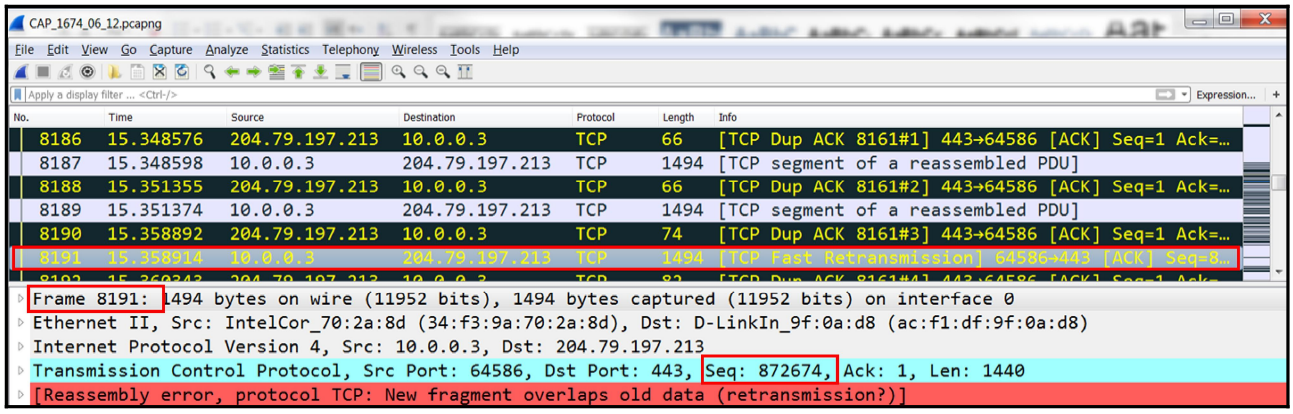

First zoom
Second zoom
Sequence Number (B)
Time (s)

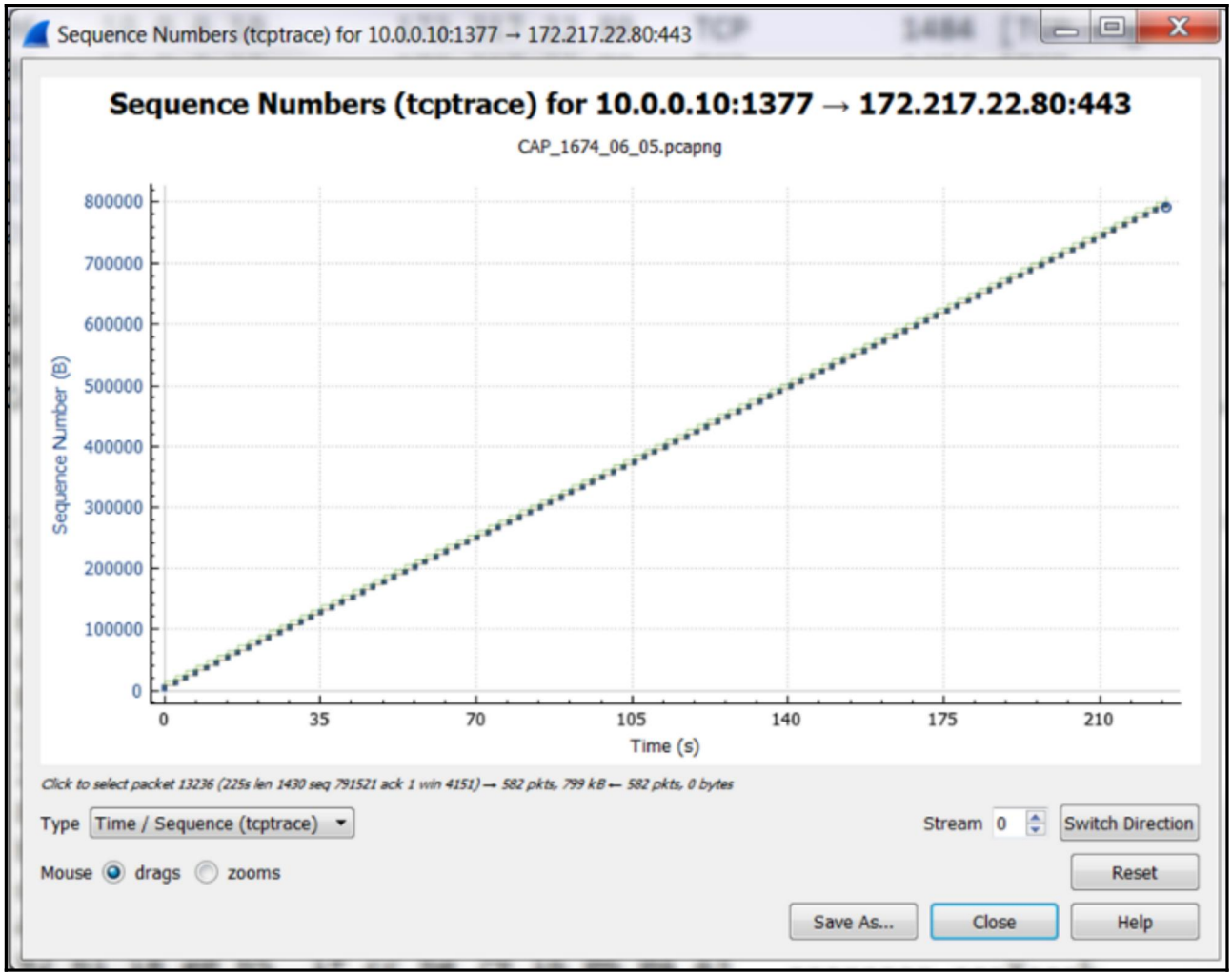

1000000
16.6
16.8
Click to select a portion of the graph. → 1645 pkts, 2334 kB ← 1476 pkts, 12 kB
Type
Time / Sequence (Stevens)
Round Trip Time
Mouse
Throughput
Time / Sequence (Stevens)
Time / Sequence (tcptrace)
Window Scaling
TCP
stream
graphs
types

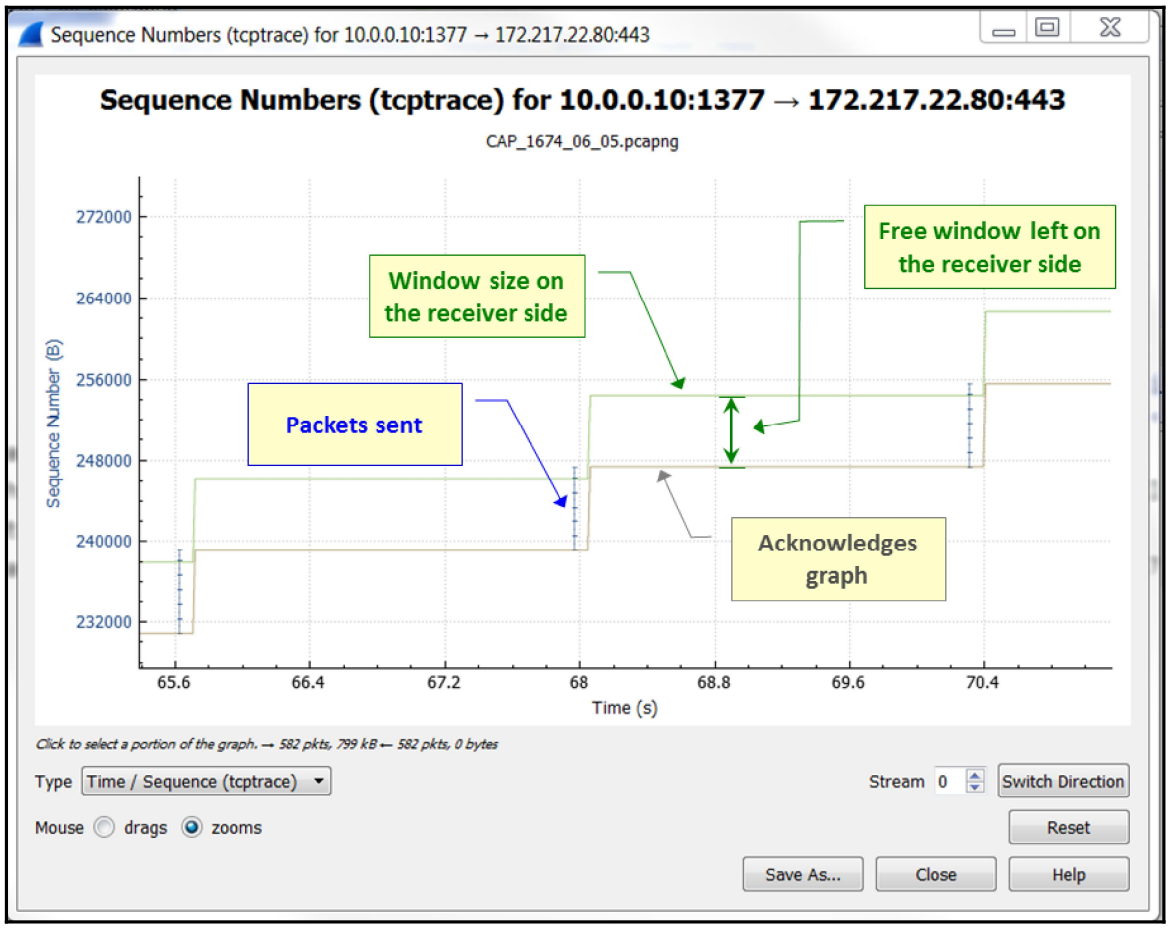

First byte → initial sequence number
Bytes
TCP Header
TCP Payload
TCP
IP Header
IP Payload
IP
Ethernet Header
Ethernet Payload
Ethernet Checksum
Ethernet

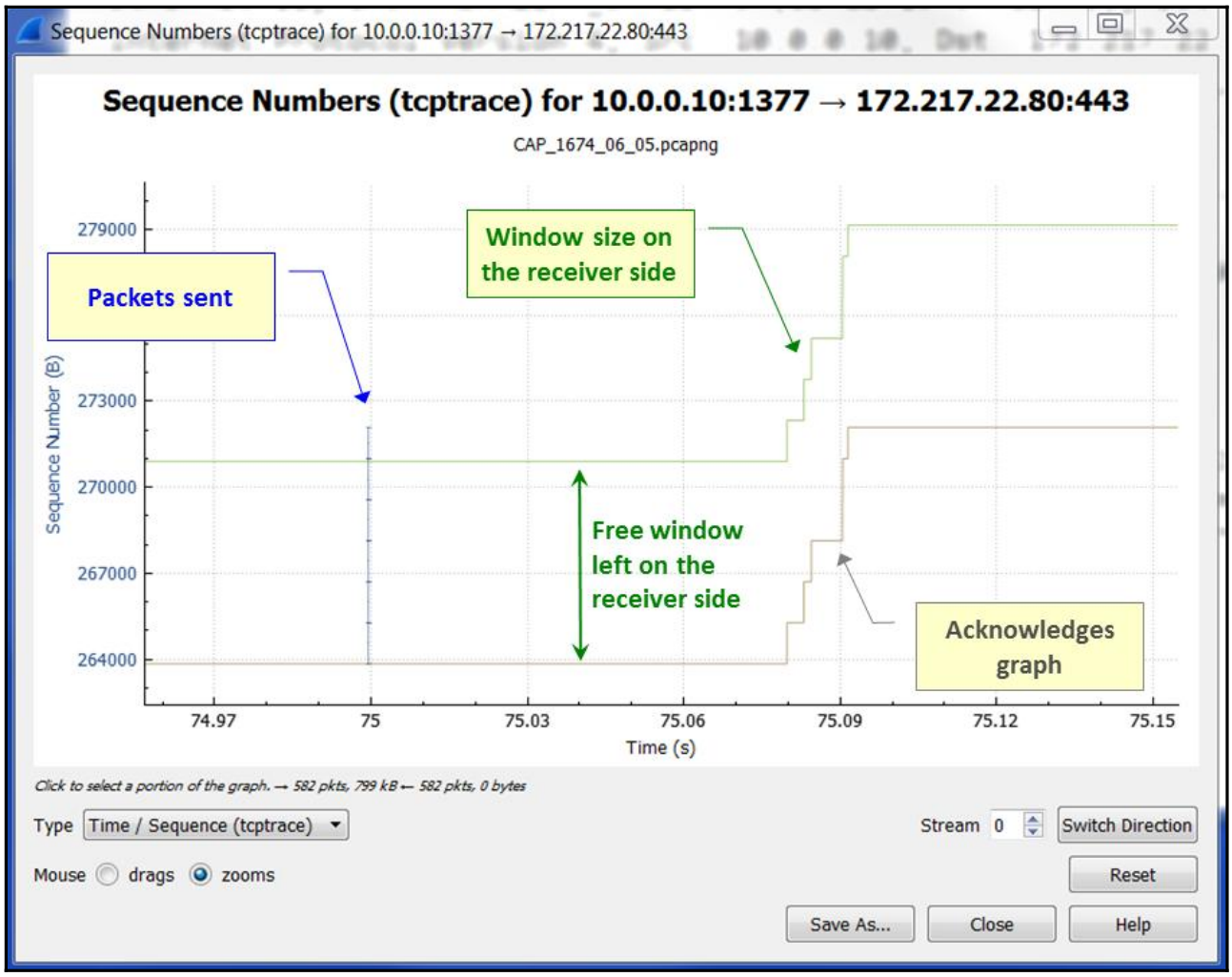

Sequence Numbers (Stevens) for 10.0.0.3:64586 → 204.79.197.213:443
Sequence Numbers (Stevens) for 10.0.0.3:64586 → 204.79.197.213:443
CAP_1674_06_12.pcapng
Sequence Number (B)
900000
896000
892000
888000
884000
880000
876000
872000
Packet 8119
Packet 8191
15.16
15.2
15.24
15.28
15.32
15.36
15.4
15.44
15.48
Time (s)
Hover over the graph for details. → 1645 pkts, 2334 kB ← 1476 pkts, 12 kB
Type
Time / Sequence (Stevens)
Stream
1
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

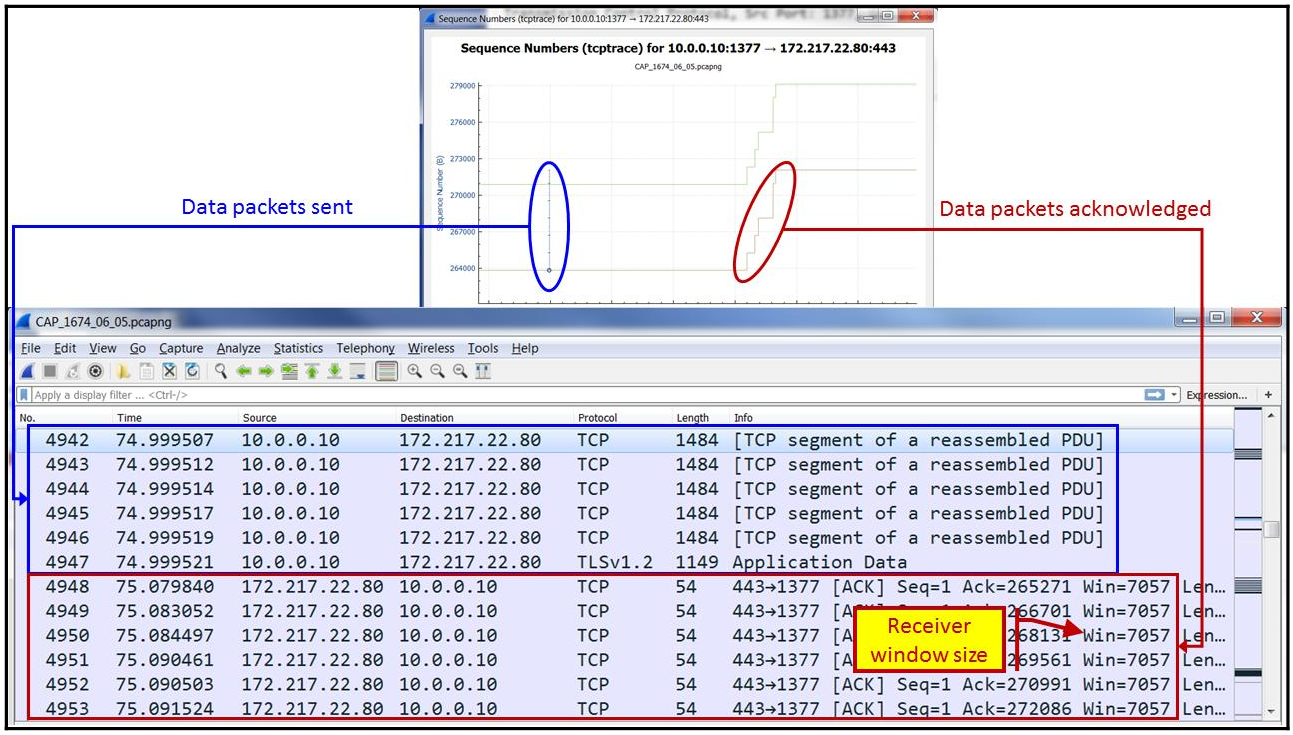

CAP_1674_06_12.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
No. Time Source Destination Protocol Length Info
8119 15.248668 10.0.0.3 204.79.197.213 SSLv2 1494 Encrypted Data[TCP segment of a reassembled PDU]
8120 15.251869 204.79.197.213 10.0.0.3 TCP 66 443→64585 [ACK] Seq=1 Ack=1078612 Win=516 Len=0…
8121 15.251887 10.0.0.3 204.79.197.213 TCP 1494 [TCP segment of a reassembled PDU]
8122 15.251892 10.0.0.3 204.79.197.213 TCP 1494 [TCP segment of a reassembled PDU]
8123 15.252669 10.0.0.3 204.79.197.213 TCP 1494 [TCP Out-Of-Order] 64585→443 [ACK] Seq=1078612 …
8124 15.252676 10.0.0.3 204.79.197.213 TCP 1494 [TCP Out-Of-Order] [TCP segment of a reassemble…
Frame 8119: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
Ethernet II, Src: IntelCor_70:2a:8d (34:f3:9a:70:2a:8d), Dst: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8)
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 204.79.197.213
Transmission Control Protocol, Src Port: 64586, Dst Port: 443, Seq: 872674, Ack: 1, Len: 1440
[10 Reassembled TCP Segments (13428 bytes): #8066(1290), #8068(1440), #8070(1440), #8072(1440), #8074(1440), #8076(144
Secure Sockets Layer

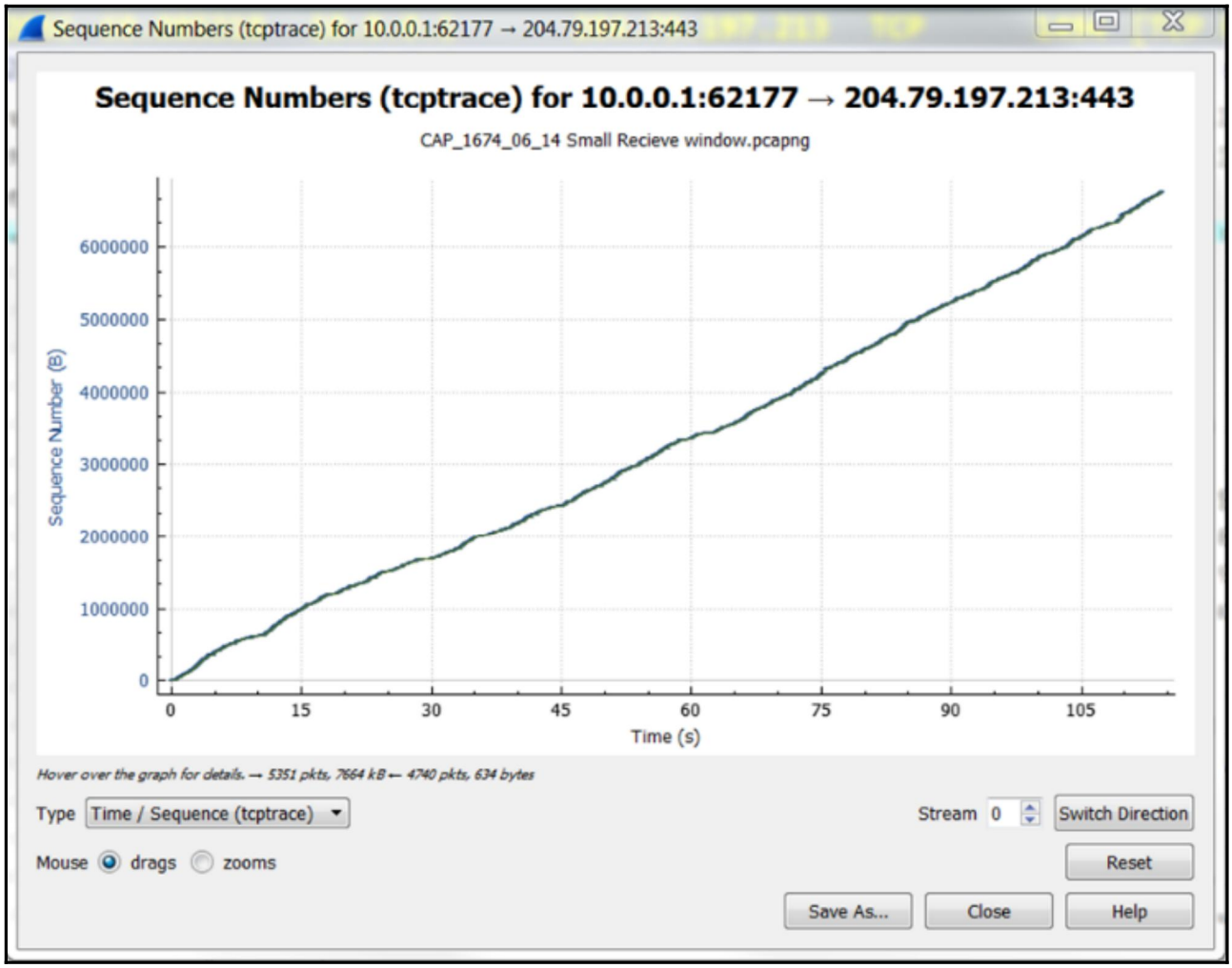

CAP_1674_06_12.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
8186 15.348576 204.79.197.213 10.0.0.3 TCP 66 [TCP Dup ACK 8161#1] 443→64586 [ACK] Seq=1 Ack=...
8187 15.348598 10.0.0.3 204.79.197.213 TCP 1494 [TCP segment of a reassembled PDU]
8188 15.351355 204.79.197.213 10.0.0.3 TCP 66 [TCP Dup ACK 8161#2] 443→64586 [ACK] Seq=1 Ack=...
8189 15.351374 10.0.0.3 204.79.197.213 TCP 1494 [TCP segment of a reassembled PDU]
8190 15.358892 204.79.197.213 10.0.0.3 TCP 74 [TCP Dup ACK 8161#3] 443→64586 [ACK] Seq=1 Ack=...
8191 15.358914 10.0.0.3 204.79.197.213 TCP 1494 [TCP Fast Retransmission] 64586→443 [ACK] Seq=8...
Frame 8191: 1494 bytes on wire (11952 bits), 1494 bytes captured (11952 bits) on interface 0
Ethernet II, Src: IntelCor_70:2a:8d (34:f3:9a:70:2a:8d), Dst: D-LinkIn_9f:0a:d8 (ac:f1:df:9f:0a:d8)
Internet Protocol Version 4, Src: 10.0.0.3, Dst: 204.79.197.213
Transmission Control Protocol, Src Port: 64586, Dst Port: 443, Seq: 872674, Ack: 1, Len: 1440
[Reassembly error, protocol TCP: New fragment overlaps old data (retransmission?)]

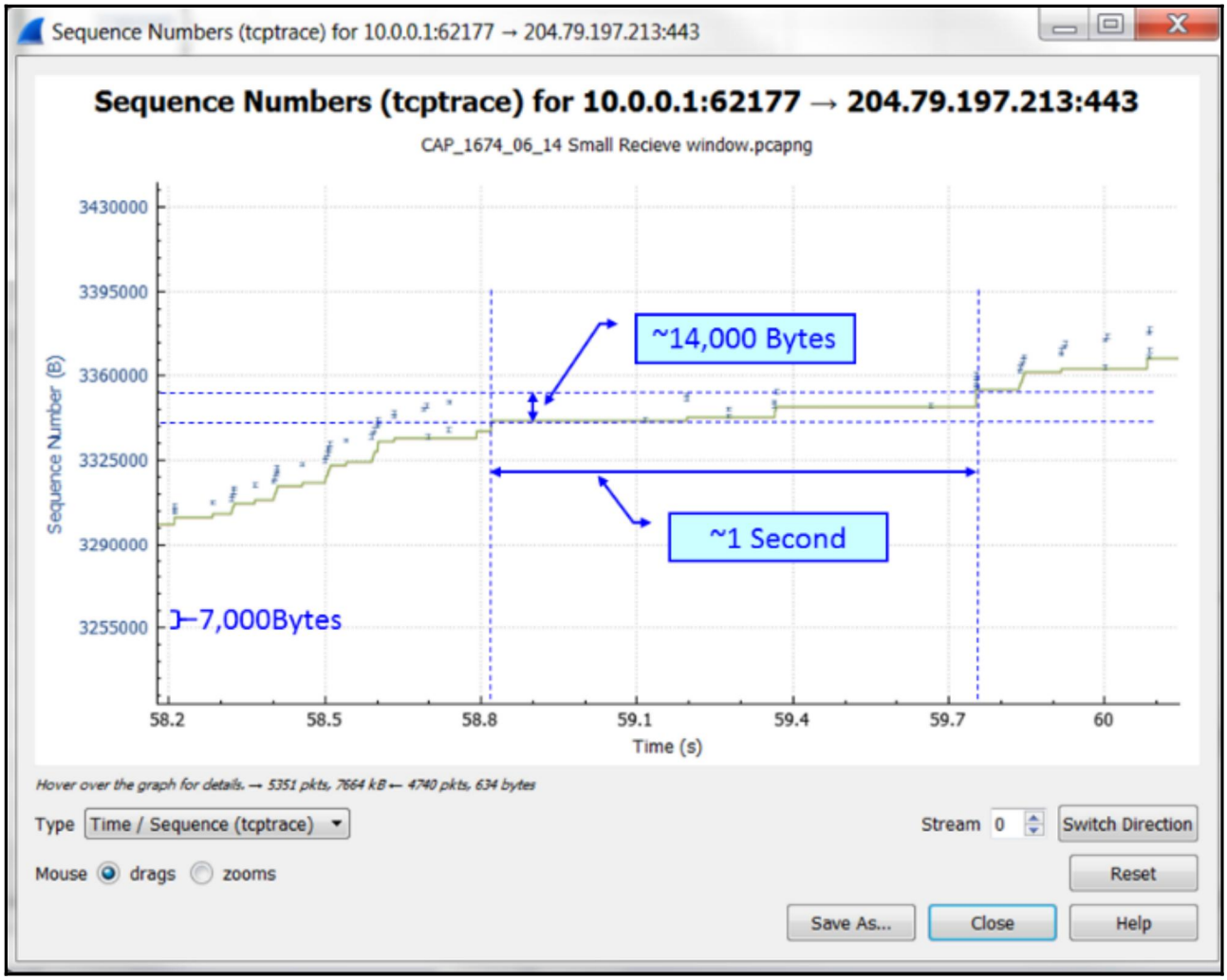

Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
CAP_1674_06_05.pcapng
Sequence Number (B)
800000
700000
600000
500000
400000
300000
200000
100000
0
0
35
70
105
140
175
210
Time (s)
Click to select packet 13236 (225s len 1430 seq 791521 ack 1 win 4151) → 582 pkts, 799 kB ← 582 pkts, 0 bytes
Type Time / Sequence (tcptrace)
Stream 0
Switch Direction
Mouse drags zooms
Reset
Save As...
Close
Help

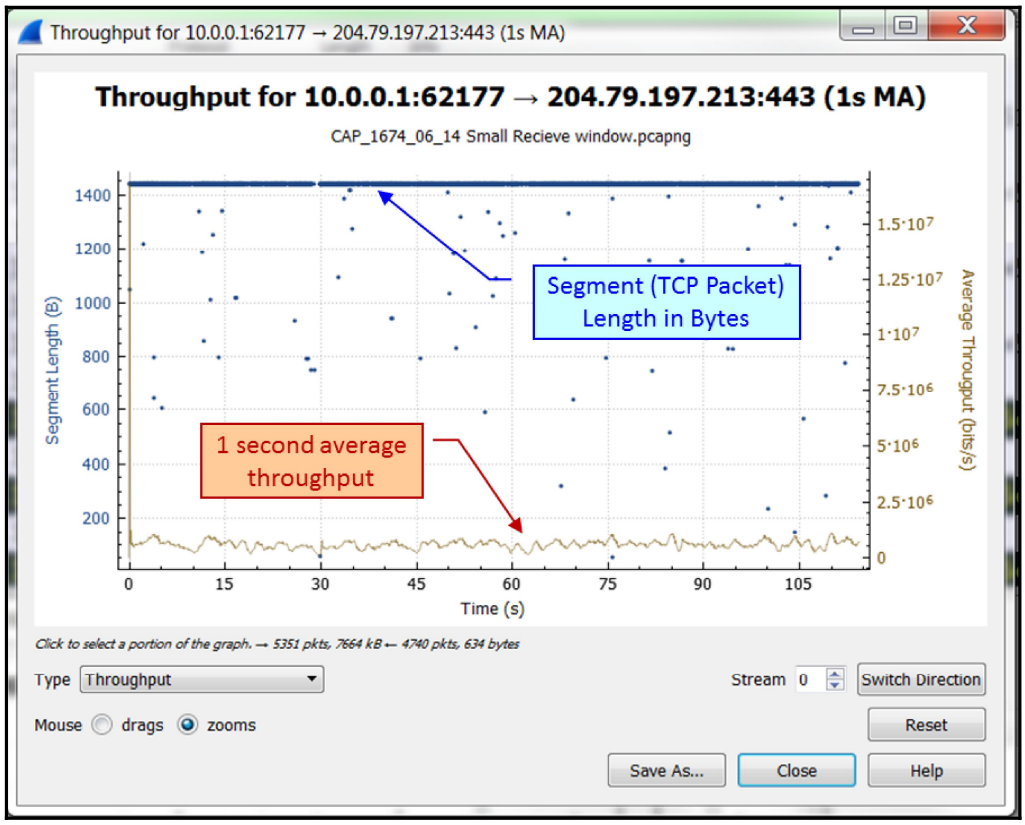

Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
CAP_1674_06_05.pcapng
Free window left on the receiver side
Window size on the receiver side
Packets sent
Acknowledges graph
Sequence Number (B)
272000
264000
256000
248000
240000
232000
65.6
66.4
67.2
68
68.8
69.6
70.4
Time (s)
Click to select a portion of the graph. → 582 pkts, 799 kB ← 582 pkts, 0 bytes
Type
Time / Sequence (tcptrace)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

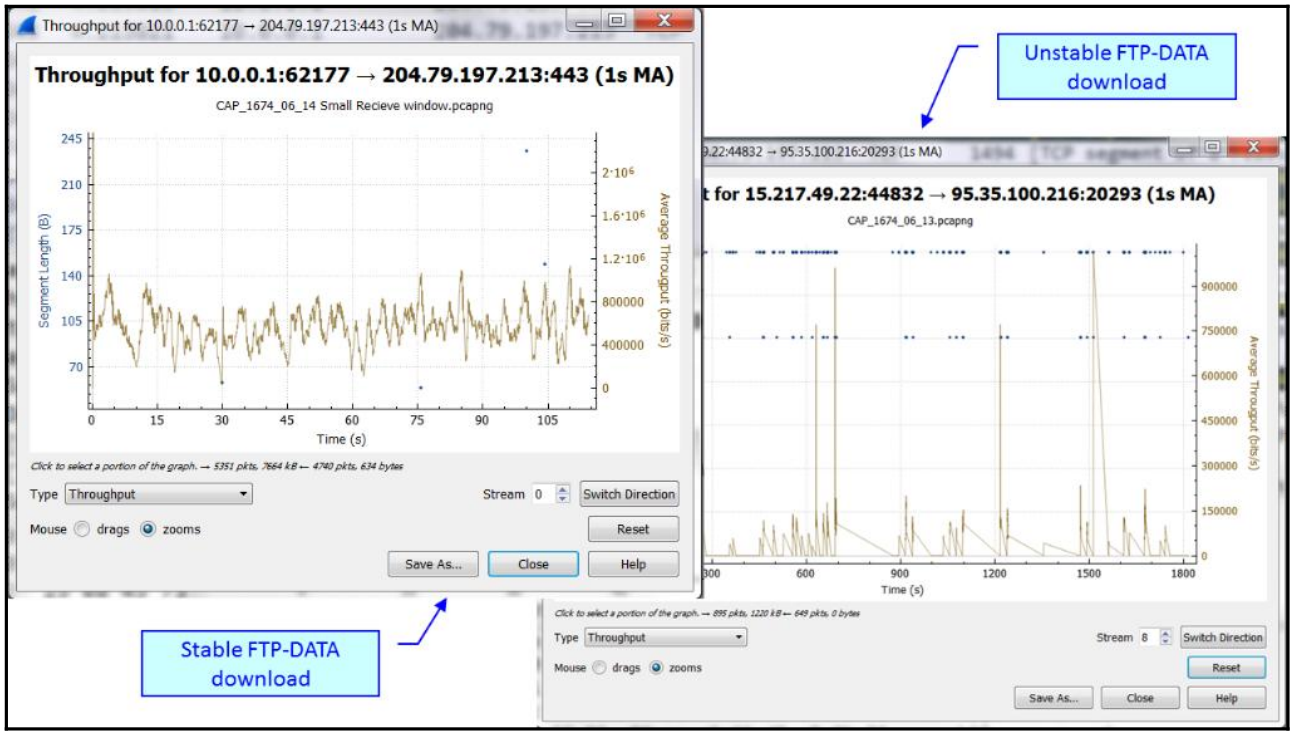

Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
CAP_1674_06_05.pcapng
Packets sent
Window size on the receiver side
Free window left on the receiver side
Acknowledges graph
Sequence Number (B)
279000
273000
270000
267000
264000
74.97
75
75.03
75.06
75.09
75.12
75.15
Time (s)
Click to select a portion of the graph. → 582 pkts, 799 kB ← 582 pkts, 0 bytes
Type
Time / Sequence (tcptrace)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

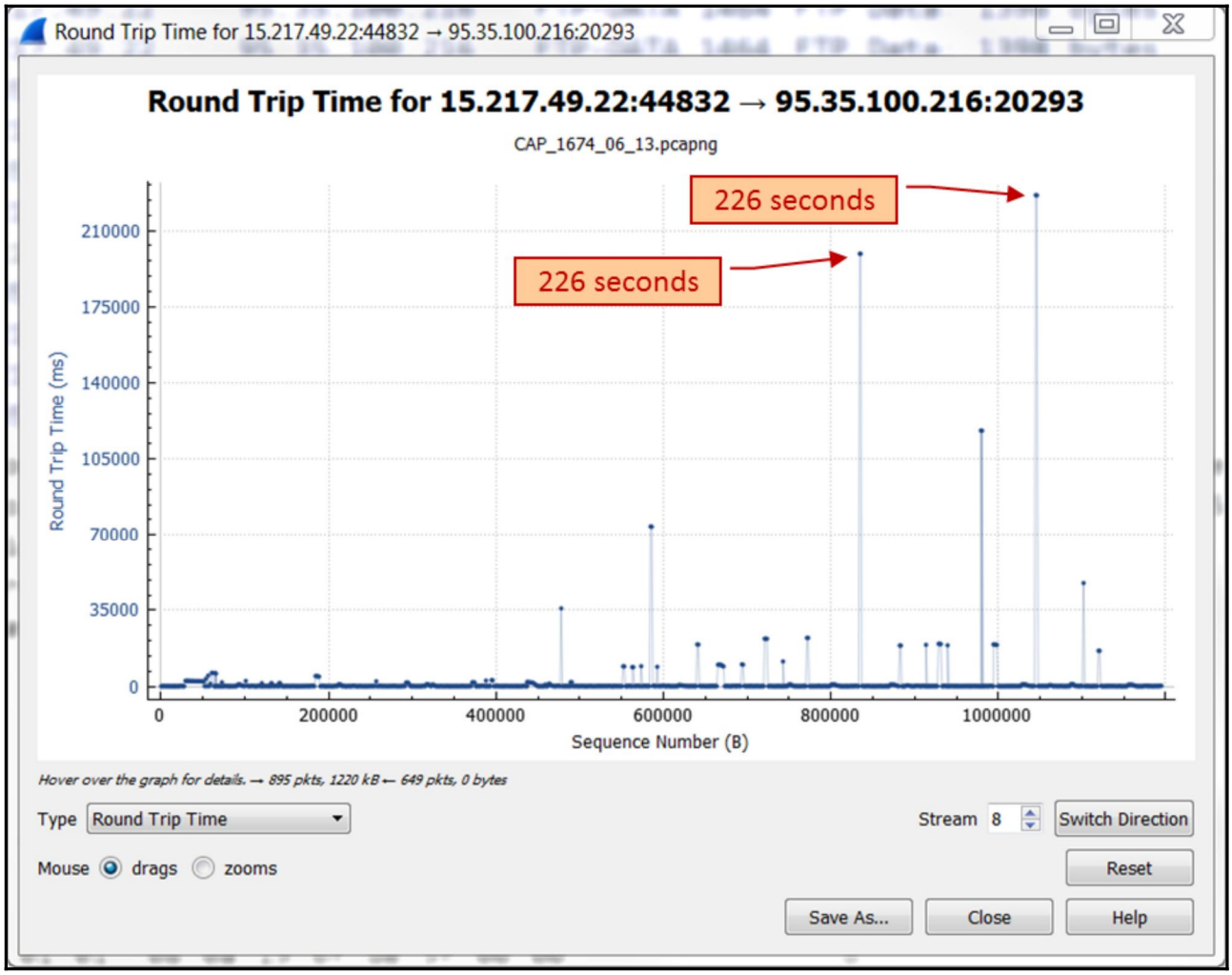

Sequence Numbers (tcptrace) for 10.0.0.10:1377 → 172.217.22.80:443
CAP_1674_06_05.pcapng
Data packets sent
Data packets acknowledged
Receiver window size
CAP_1674_06_05.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
4942 74.999507 10.0.0.10 172.217.22.80 TCP 1484 [TCP segment of a reassembled PDU]
4943 74.999512 10.0.0.10 172.217.22.80 TCP 1484 [TCP segment of a reassembled PDU]
4944 74.999514 10.0.0.10 172.217.22.80 TCP 1484 [TCP segment of a reassembled PDU]
4945 74.999517 10.0.0.10 172.217.22.80 TCP 1484 [TCP segment of a reassembled PDU]
4946 74.999519 10.0.0.10 172.217.22.80 TCP 1484 [TCP segment of a reassembled PDU]
4947 74.999521 10.0.0.10 172.217.22.80 TLSv1.2 1149 Application Data
4948 75.079840 172.217.22.80 10.0.0.10 TCP 54 443→1377 [ACK] Seq=1 Ack=265271 Win=7057 Len...
4949 75.083052 172.217.22.80 10.0.0.10 TCP 54 443→1377 [A 266701 Win=7057 Len...
4950 75.084497 172.217.22.80 10.0.0.10 TCP 54 443→1377 [A 268131 Win=7057 Len...
4951 75.090461 172.217.22.80 10.0.0.10 TCP 54 443→1377 [A 269561 Win=7057 Len...
4952 75.090503 172.217.22.80 10.0.0.10 TCP 54 443→1377 [ACK] Seq=1 Ack=270991 Win=7057 Len...
4953 75.091524 172.217.22.80 10.0.0.10 TCP 54 443→1377 [ACK] Seq=1 Ack=272086 Win=7057 Len...

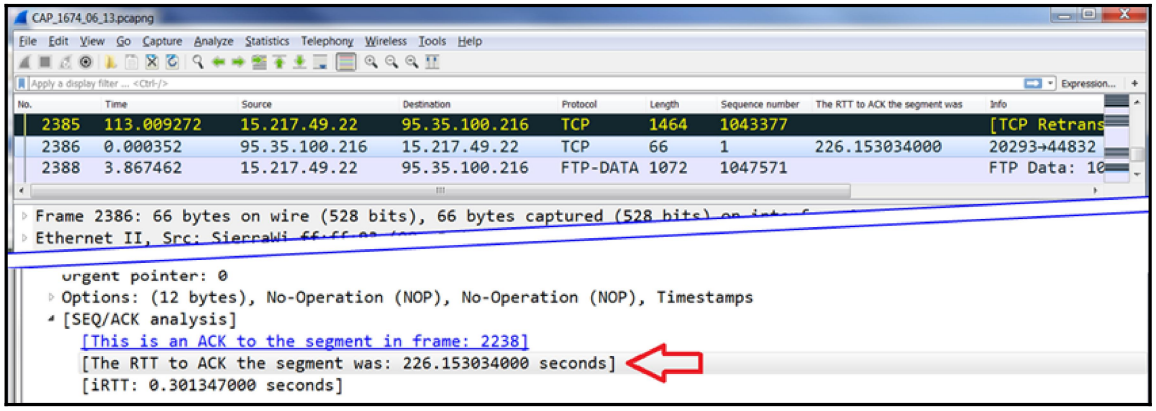

Sequence Numbers (tcptrace) for 10.0.0.1:62177 → 204.79.197.213:443
Sequence Numbers (tcptrace) for 10.0.0.1:62177 → 204.79.197.213:443
CAP_1674_06_14 Small Recieve window.pcapng
Sequence Number (B)
6000000
5000000
4000000
3000000
2000000
1000000
0
0
15
30
45
60
75
90
105
Time (s)
Hover over the graph for details. → 5351 pkts, 7664 kB ← 4740 pkts, 634 bytes
Type
Time / Sequence (tcptrace)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

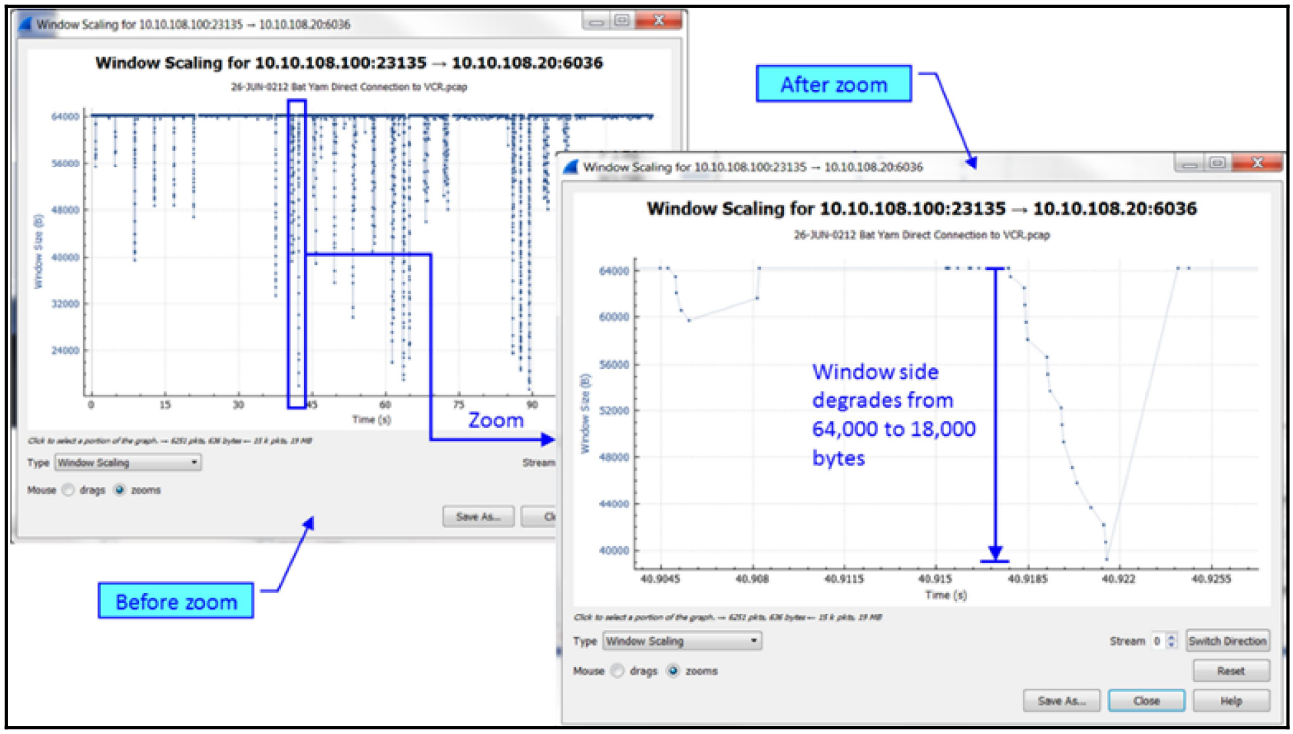

Sequence Numbers (tcptrace) for 10.0.0.1:62177 → 204.79.197.213:443
Sequence Numbers (tcptrace) for 10.0.0.1:62177 → 204.79.197.213:443
CAP_1674_06_14 Small Recieve window.pcapng
Sequence Number (B)
3430000
3395000
3360000
3325000
3290000
3255000
~14,000 Bytes
~1 Second
7,000Bytes
58.2
58.5
58.8
59.1
59.4
59.7
60
Time (s)
Hover over the graph for details. → 5351 pkts, 7664 kB ← 4740 pkts, 634 bytes
Type
Time / Sequence (tcptrace)
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help


Throughput for 10.0.0.1:62177 → 204.79.197.213:443 (1s MA)
Throughput for 10.0.0.1:62177 → 204.79.197.213:443 (1s MA)
CAP_1674_06_14 Small Recieve window.pcapng
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Segment (TCP Packet) Length in Bytes
1 second average throughput
Click to select a portion of the graph. → 5351 pkts, 7664 kB ← 4740 pkts, 634 bytes
Type
Throughput
Stream
0
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

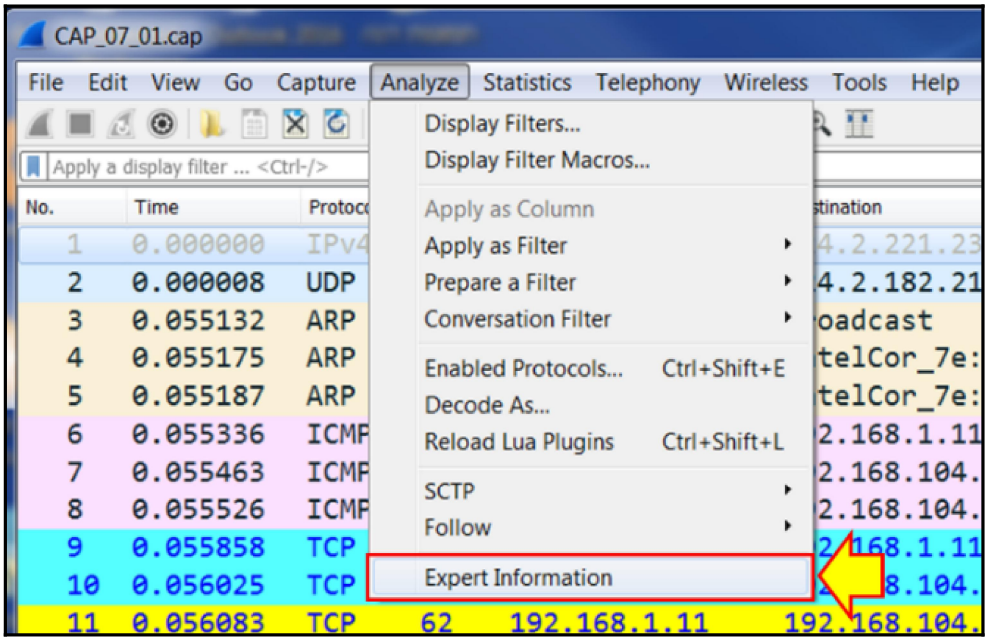

Throughput for 10.0.0.1:62177 → 204.79.197.213:443 (1s MA)
Throughput for 10.0.0.1:62177 → 204.79.197.213:443 (1s MA)
CAP_1674_06_14 Small Recieve window.pcapng
Segment Length (B)
Average Throughput (bits/s)
Time (s)
Type Throughput
Stream 0
Switch Direction
Mouse drags zooms
Reset
Save As...
Close
Help
Unstable FTP-DATA download
t for 15.217.49.22:44832 → 95.35.100.216:20293 (1s MA)
CAP_1674_06_13.pcapng
Stable FTP-DATA download

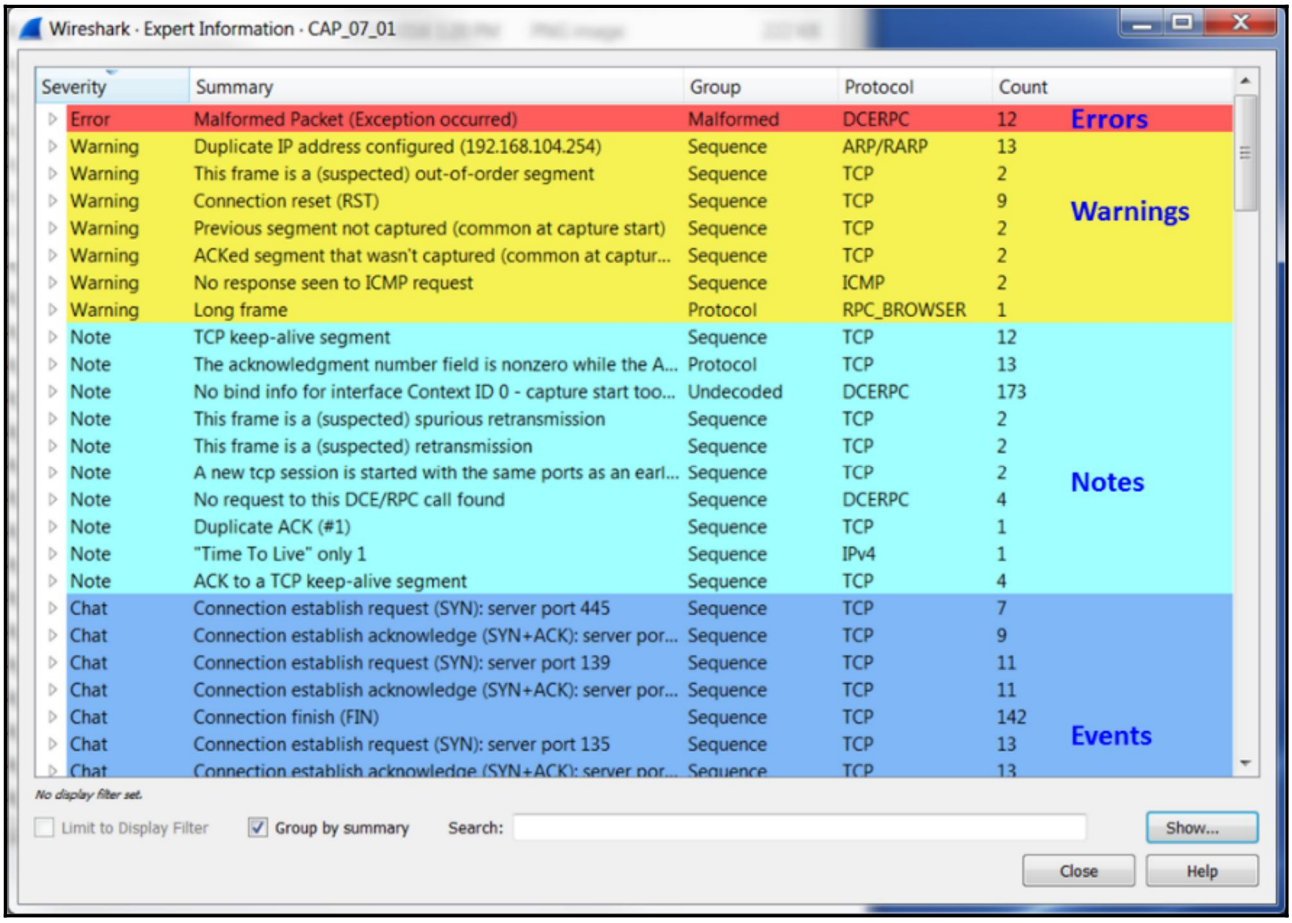

Round Trip Time for 15.217.49.22:44832 → 95.35.100.216:20293
Round Trip Time for 15.217.49.22:44832 → 95.35.100.216:20293
CAP_1674_06_13.pcapng
226 seconds
226 seconds
Round Trip Time (ms)
210000
175000
140000
105000
70000
35000
0
0
200000
400000
600000
800000
1000000
Sequence Number (B)
Hover over the graph for details. → 895 pkts, 1220 kB ← 649 pkts, 0 bytes
Type
Round Trip Time
Stream
8
Switch Direction
Mouse
drags
zooms
Reset
Save As...
Close
Help

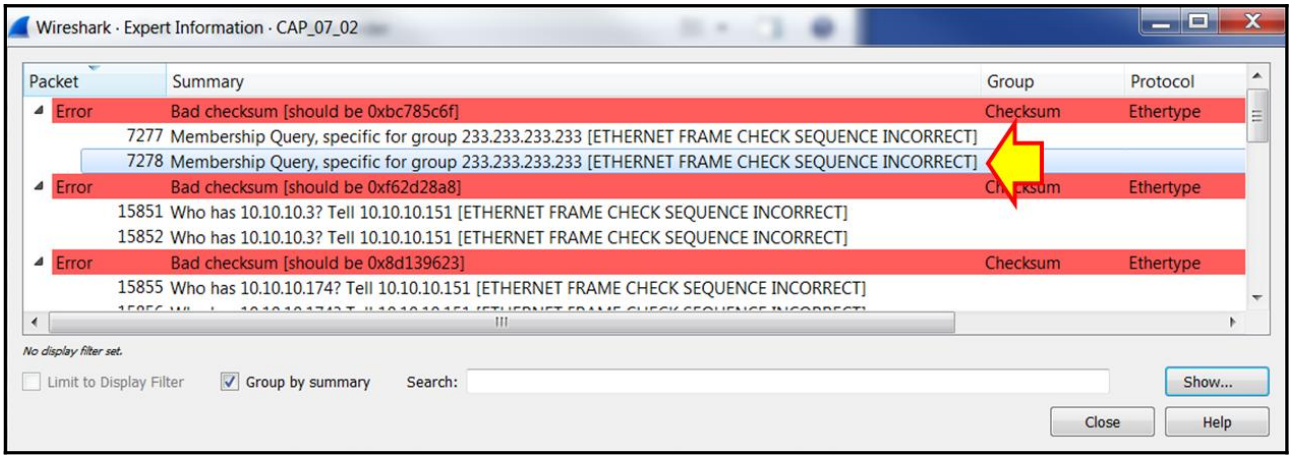

CAP_1674_06_13.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Sequence number The RTT to ACK the segment was Info
2385 113.009272 15.217.49.22 95.35.100.216 TCP 1464 1043377 [TCP Retrans
2386 0.000352 95.35.100.216 15.217.49.22 TCP 66 1 226.153034000 20293→44832
2388 3.867462 15.217.49.22 95.35.100.216 FTP-DATA 1072 1047571 FTP Data: 10
Frame 2386: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src:
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[SEQ/ACK analysis]
[This is an ACK to the segment in frame: 2238]
[The RTT to ACK the segment was: 226.153034000 seconds]
[iRTT: 0.301347000 seconds]

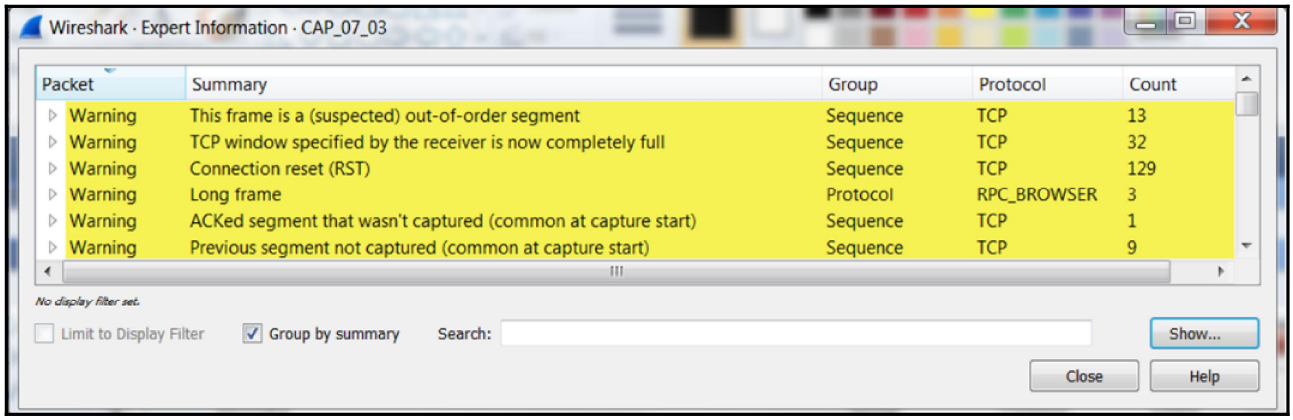

Window Scaling for 10.10.108.100:23135 → 10.10.108.20:6036
Window Scaling for 10.10.108.100:23135 → 10.10.108.20:6036
26-JUN-0212 Bat Yam Direct Connection to VCR.pcap
Window Size (B)
Time (s)
Zoom
After zoom
Before zoom
Window side degrades from 64,000 to 18,000 bytes
Type
Window Scaling
Mouse
drags
zooms
Stream
Switch Direction
Reset
Save As...
Close
Help

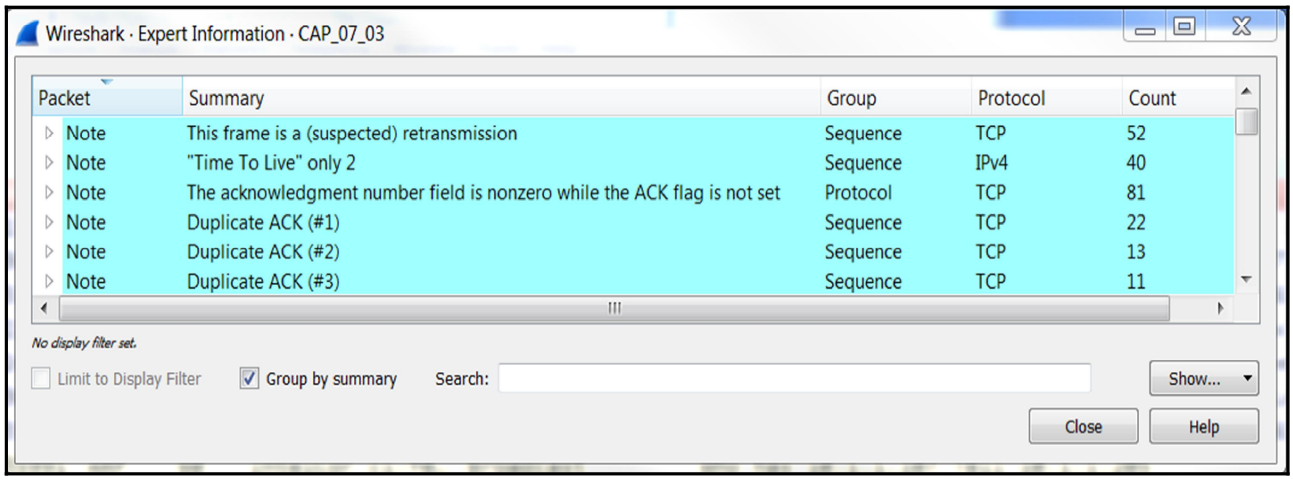
Chapter 7: Using the Expert System

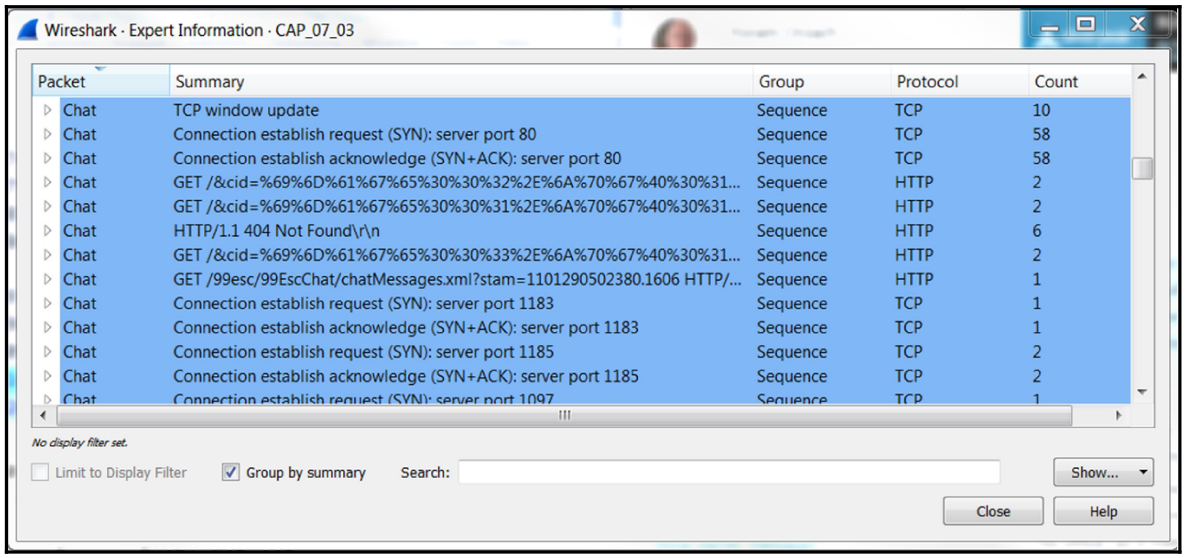


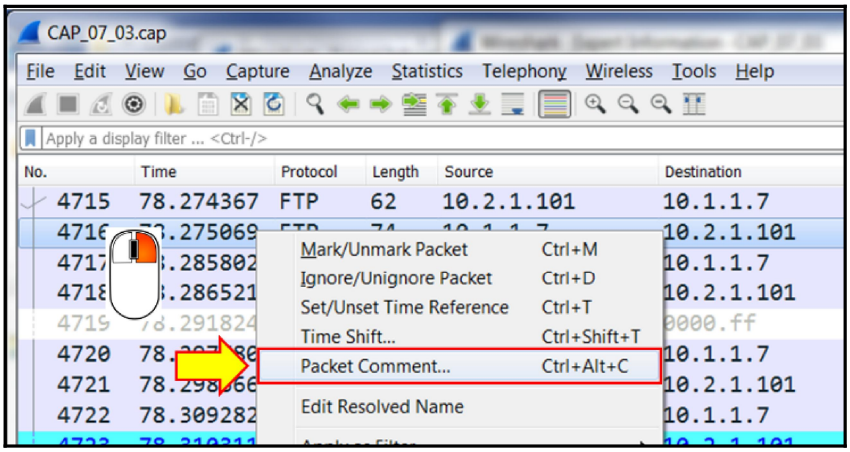

Wireshark · Expert Information · CAP_07_01
Severity
Summary
Group
Protocol
Count
Error Malformed Packet (Exception occurred) Malformed DCERPC 12
Errors
Warning Duplicate IP address configured (192.168.104.254) Sequence ARP/RARP 13
Warning This frame is a (suspected) out-of-order segment Sequence TCP 2
Warning Connection reset (RST) Sequence TCP 9
Warning Previous segment not captured (common at capture start) Sequence TCP 2
Warning ACKed segment that wasn't captured (common at captur... Sequence TCP 2
Warning No response seen to ICMP request Sequence ICMP 2
Warning Long frame Protocol RPC_BROWSER 1
Warnings
Note TCP keep-alive segment Sequence TCP 12
Note The acknowledgment number field is nonzero while the A... Protocol TCP 13
Note No bind info for interface Context ID 0 - capture start too... Undecoded DCERPC 173
Note This frame is a (suspected) spurious retransmission Sequence TCP 2
Note This frame is a (suspected) retransmission Sequence TCP 2
Note A new tcp session is started with the same ports as an earl... Sequence TCP 2
Note No request to this DCE/RPC call found Sequence DCERPC 4
Note Duplicate ACK (#1) Sequence TCP 1
Note "Time To Live" only 1 Sequence IPv4 1
Note ACK to a TCP keep-alive segment Sequence TCP 4
Notes
Chat Connection establish request (SYN): server port 445 Sequence TCP 7
Chat Connection establish acknowledge (SYN+ACK): server por... Sequence TCP 9
Chat Connection establish request (SYN): server port 139 Sequence TCP 11
Chat Connection establish acknowledge (SYN+ACK): server por... Sequence TCP 11
Chat Connection finish (FIN) Sequence TCP 142
Chat Connection establish request (SYN): server port 135 Sequence TCP 13
Events
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

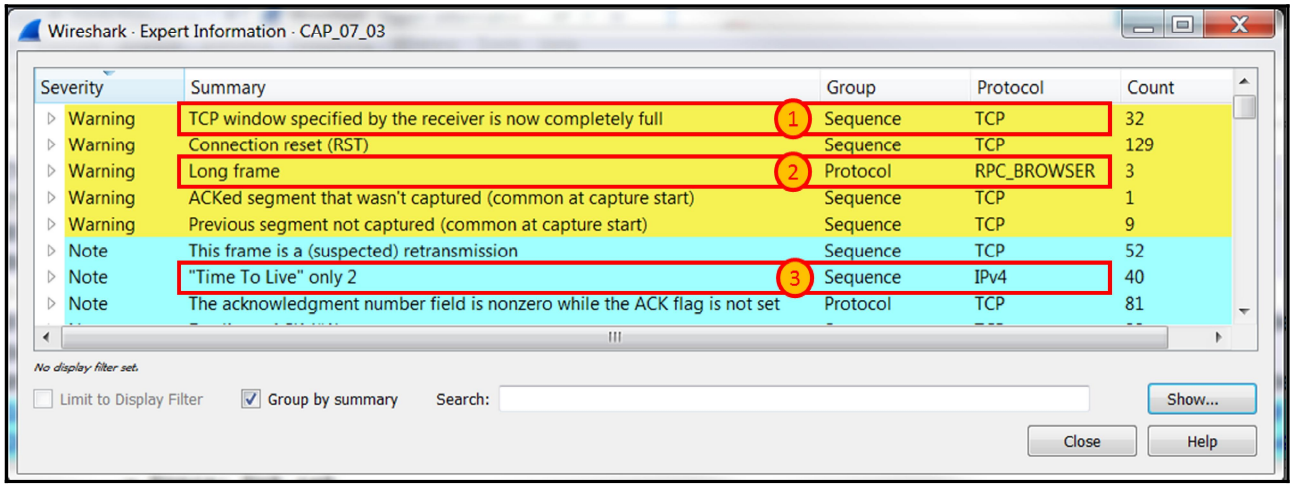

Wireshark · Expert Information · CAP_07_02
Packet
Summary
Group
Protocol
Error Bad checksum [should be 0xbc785c6f] Checksum Ethertype
7277 Membership Query, specific for group 233.233.233.233 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
7278 Membership Query, specific for group 233.233.233.233 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
Error Bad checksum [should be 0xf62d28a8] Ethertype
15851 Who has 10.10.10.3? Tell 10.10.10.151 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
15852 Who has 10.10.10.3? Tell 10.10.10.151 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
Error Bad checksum [should be 0x8d139623] Checksum Ethertype
15855 Who has 10.10.10.174? Tell 10.10.10.151 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

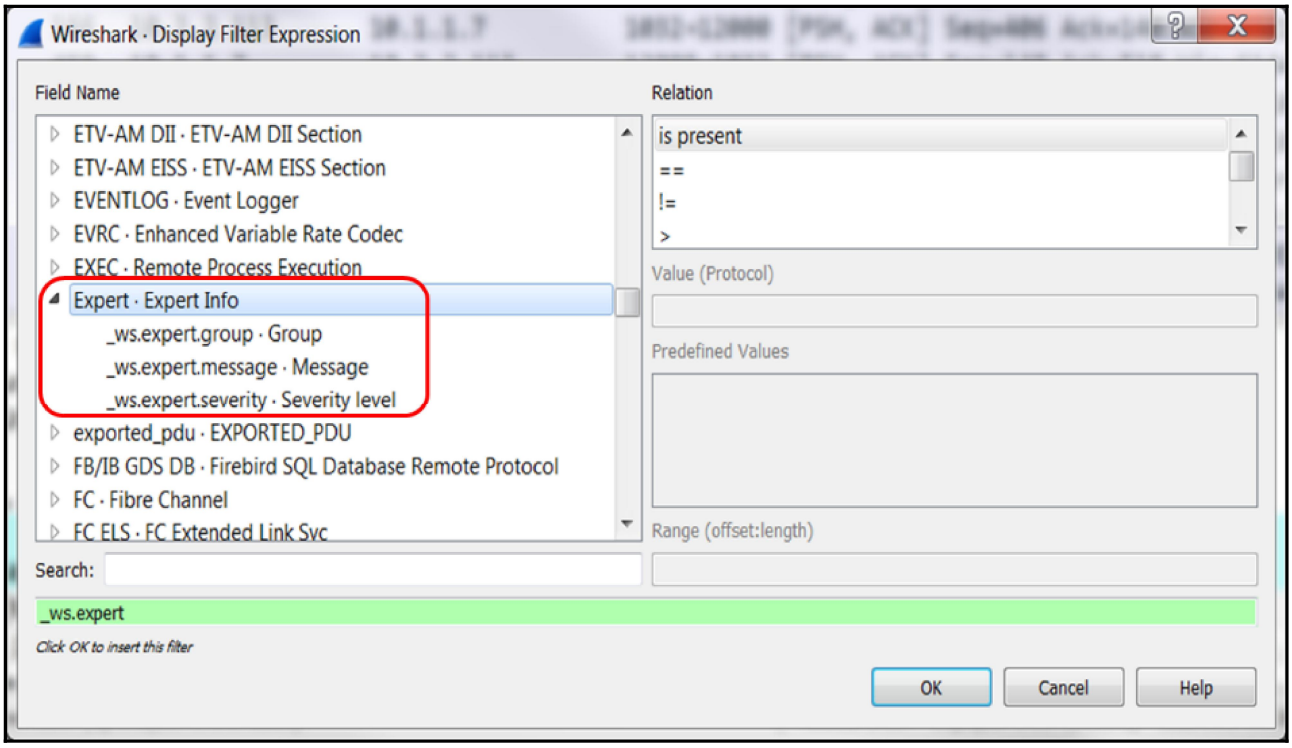

Wireshark · Expert Information · CAP_07_03
Packet
Summary
Group
Protocol
Count
Warning
This frame is a (suspected) out-of-order segment
Sequence
TCP
13
Warning
TCP window specified by the receiver is now completely full
Sequence
TCP
32
Warning
Connection reset (RST)
Sequence
TCP
129
Warning
Long frame
Protocol
RPC_BROWSER
3
Warning
ACKed segment that wasn't captured (common at capture start)
Sequence
TCP
1
Warning
Previous segment not captured (common at capture start)
Sequence
TCP
9
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

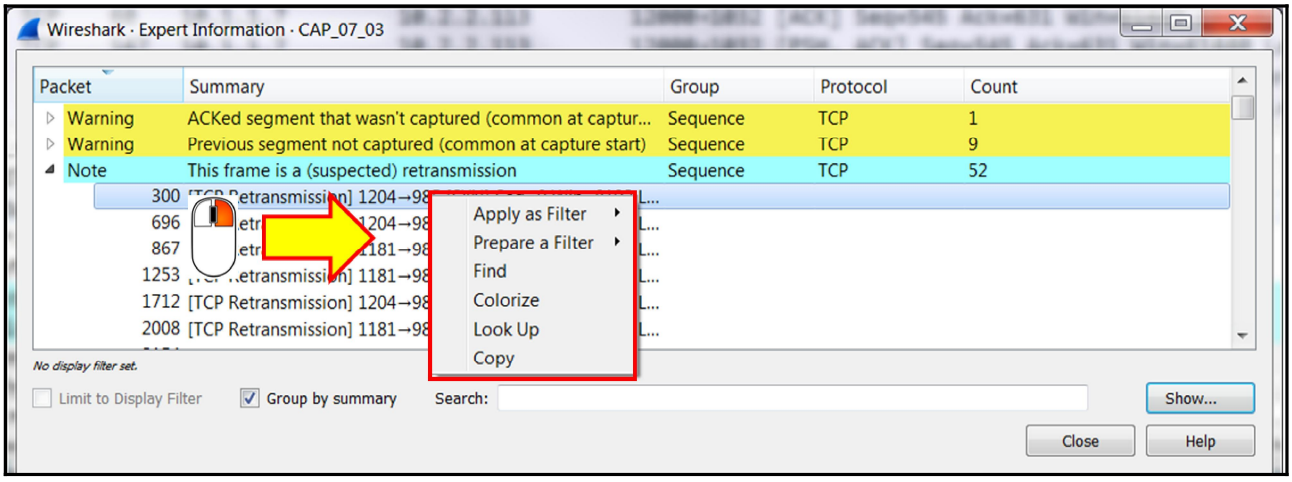

Wireshark · Expert Information · CAP_07_03
Packet
Summary
Group
Protocol
Count
Note
This frame is a (suspected) retransmission
Sequence
TCP
52
Note
"Time To Live" only 2
Sequence
IPv4
40
Note
The acknowledgment number field is nonzero while the ACK flag is not set
Protocol
TCP
81
Note
Duplicate ACK (#1)
Sequence
TCP
22
Note
Duplicate ACK (#2)
Sequence
TCP
13
Note
Duplicate ACK (#3)
Sequence
TCP
11
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

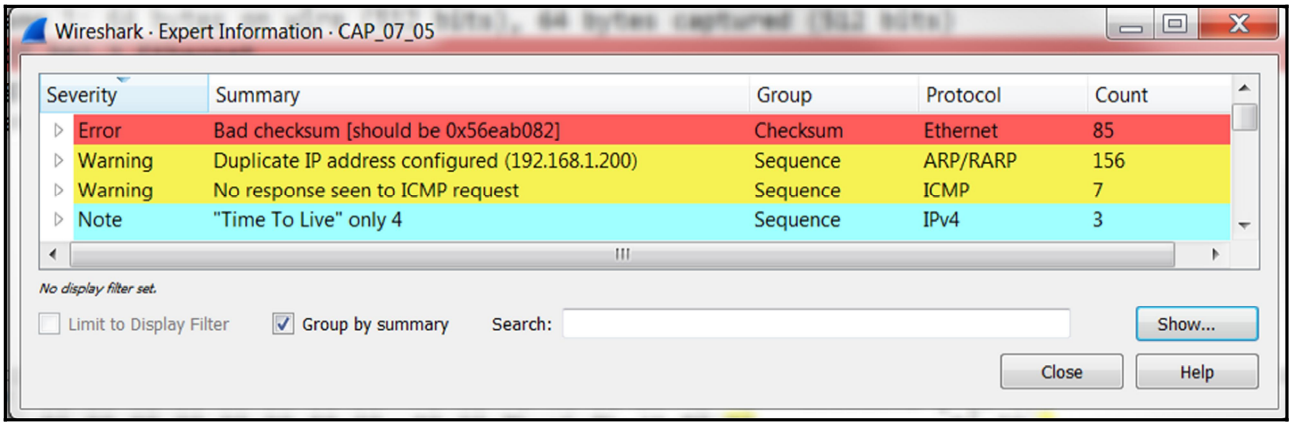

Wireshark · Expert Information · CAP_07_03
Packet
Summary
Group
Protocol
Count
Chat
TCP window update
Sequence
TCP
10
Chat
Connection establish request (SYN): server port 80
Sequence
TCP
58
Chat
Connection establish acknowledge (SYN+ACK): server port 80
Sequence
TCP
58
Chat
GET /&cid=%69%6D%61%67%65%30%30%32%2E%6A%70%67%40%30%31...
Sequence
HTTP
2
Chat
GET /&cid=%69%6D%61%67%65%30%30%31%2E%6A%70%67%40%30%31...
Sequence
HTTP
2
Chat
HTTP/1.1 404 Not Found\r\n
Sequence
HTTP
6
Chat
GET /&cid=%69%6D%61%67%65%30%30%33%2E%6A%70%67%40%30%31...
Sequence
HTTP
2
Chat
GET /99esc/99EscChat/chatMessages.xml?stam=1101290502380.1606 HTTP/...
Sequence
HTTP
1
Chat
Connection establish request (SYN): server port 1183
Sequence
TCP
1
Chat
Connection establish acknowledge (SYN+ACK): server port 1183
Sequence
TCP
1
Chat
Connection establish request (SYN): server port 1185
Sequence
TCP
2
Chat
Connection establish acknowledge (SYN+ACK): server port 1185
Sequence
TCP
2
Chat
Connection establish request (SYN): server port 1097
Sequence
TCP
1
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

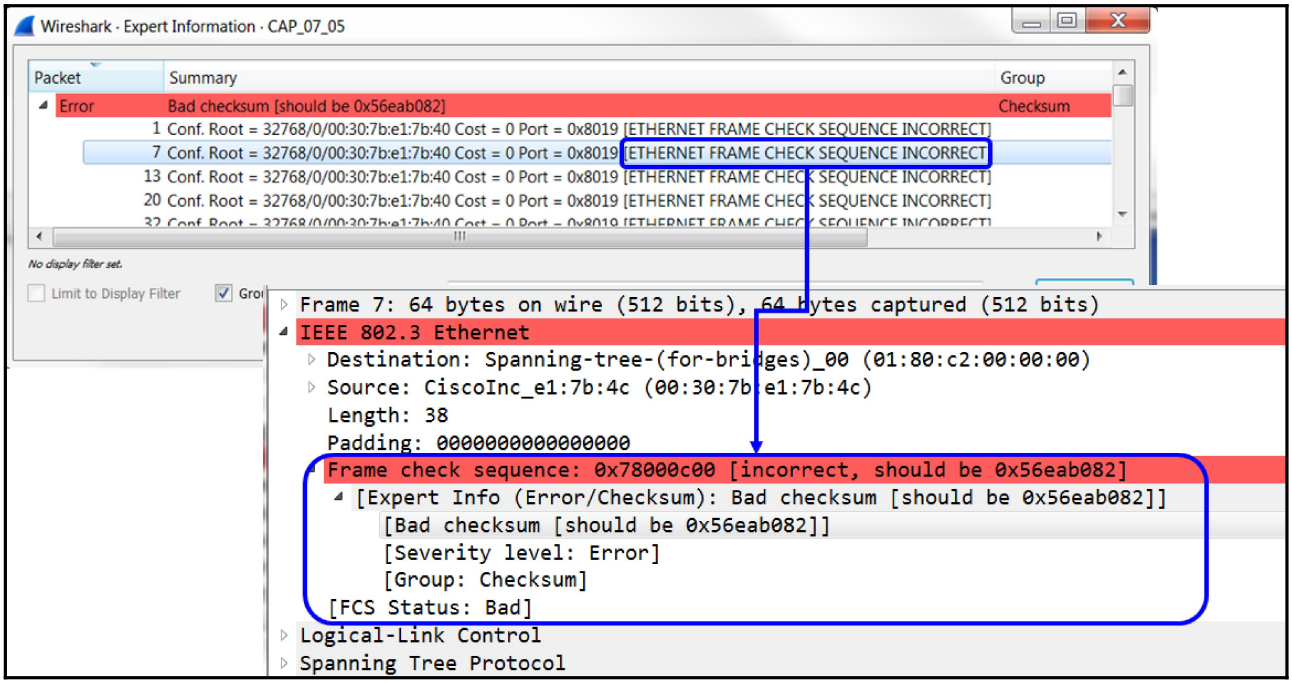

CAP_07_03.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Protocol Length Source Destination
4715 78.274367 FTP 62 10.2.1.101 10.1.1.7
4716 10.2.1.101
4717 10.1.1.7
4718 10.2.1.101
4719 0000.ff
4720 10.1.1.7
4721 10.2.1.101
4722 78.309282 10.1.1.7
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

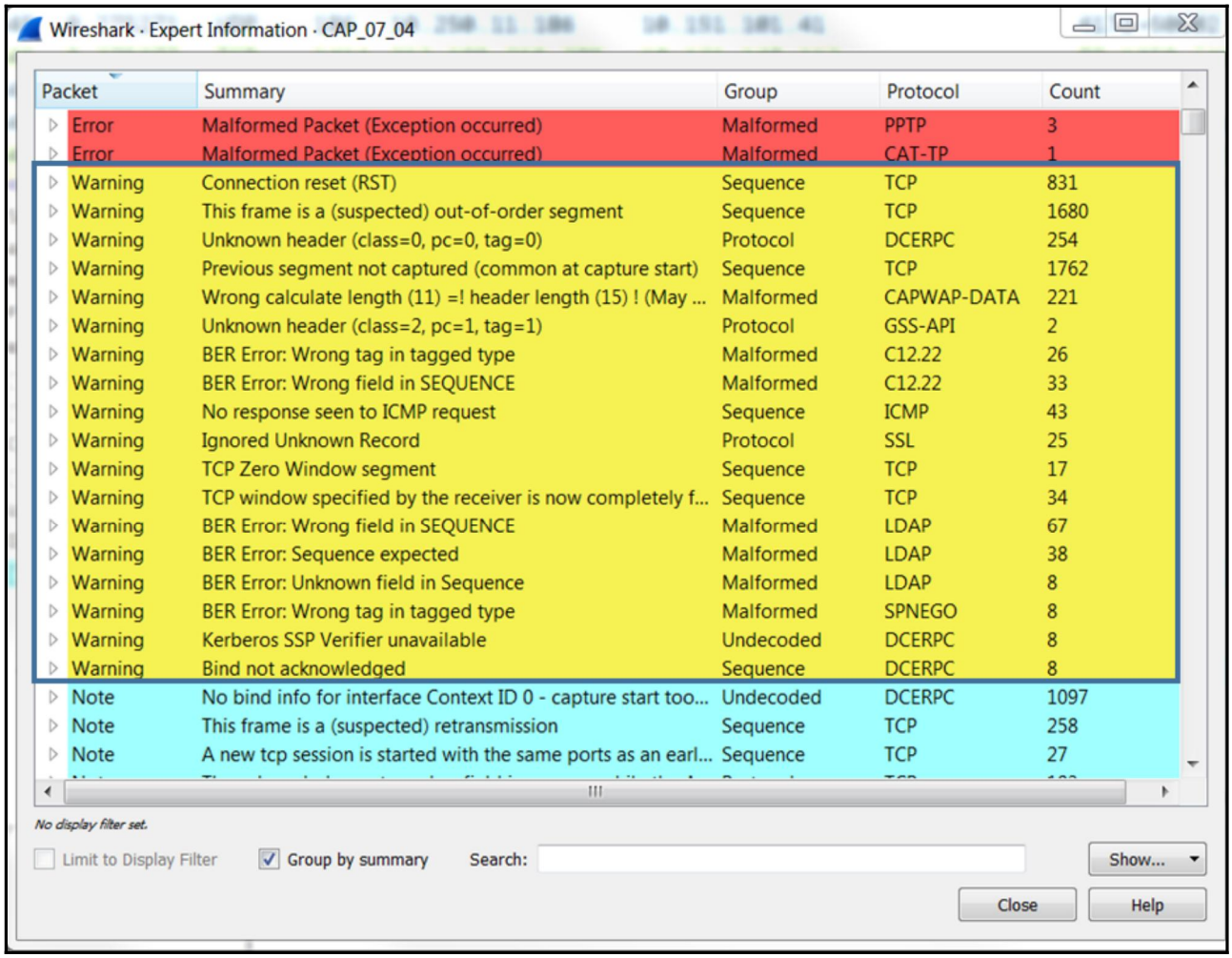

Wireshark · Expert Information · CAP_07_03
Severity Summary Group Protocol Count
Warning TCP window specified by the receiver is now completely full 1 Sequence TCP 32
Warning Connection reset (RST) Sequence TCP 129
Warning Long frame 2 Protocol RPC_BROWSER 3
Warning ACKed segment that wasn't captured (common at capture start) Sequence TCP 1
Warning Previous segment not captured (common at capture start) Sequence TCP 9
Note This frame is a (suspected) retransmission Sequence TCP 52
Note "Time To Live" only 2 3 Sequence IPv4 40
Note The acknowledgment number field is nonzero while the ACK flag is not set Protocol TCP 81
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

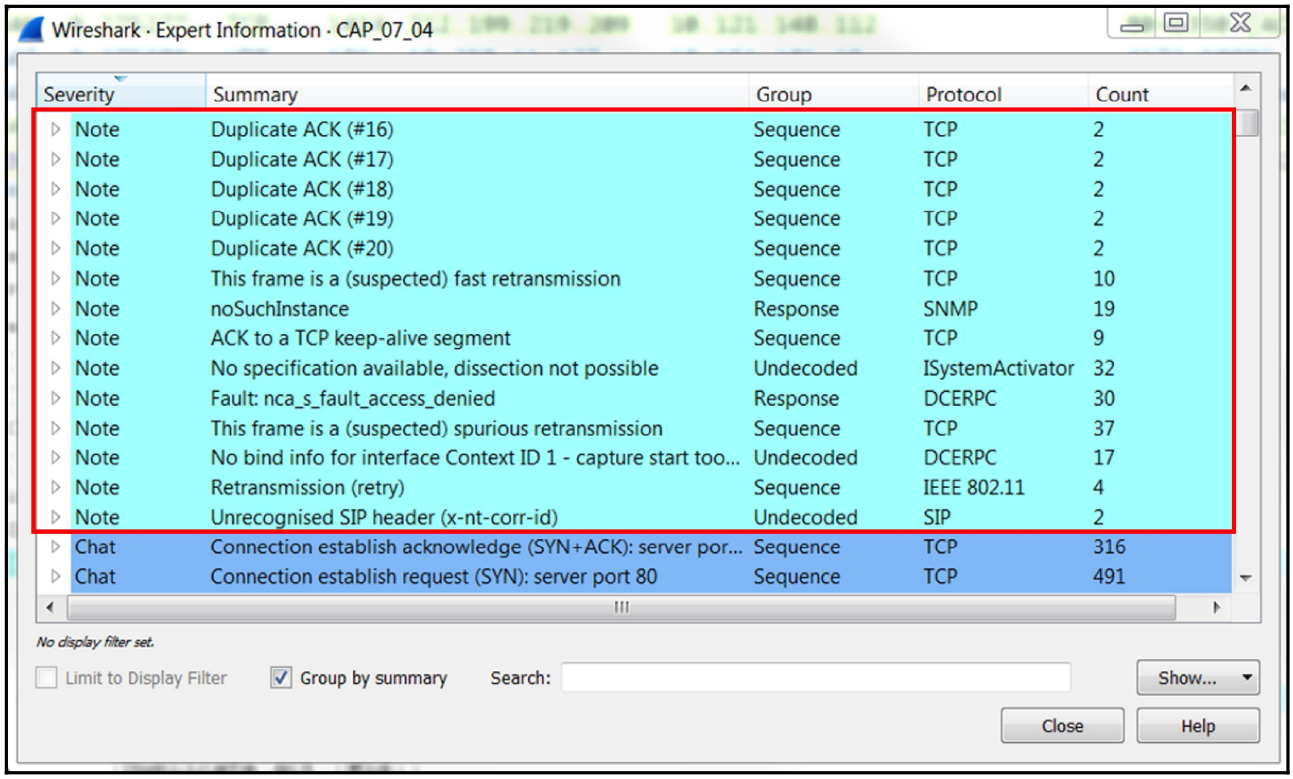

Wireshark · Display Filter Expression
Field Name
Relation
ETV-AM DII · ETV-AM DII Section
ETV-AM EISS · ETV-AM EISS Section
EVENTLOG · Event Logger
EVRC · Enhanced Variable Rate Codec
EXEC · Remote Process Execution
Expert · Expert Info
_ws.expert.group · Group
_ws.expert.message · Message
_ws.expert.severity · Severity level
exported_pdu · EXPORTED_PDU
FB/IB GDS DB · Firebird SQL Database Remote Protocol
FC · Fibre Channel
FC ELS · FC Extended Link Svc
is present
==
!=
>
Value (Protocol)
Predefined Values
Range (offset:length)
Search:
_ws.expert
Click OK to insert this filter
OK
Cancel
Help


Wireshark · Expert Information · CAP_07_03
Packet
Summary
Group
Protocol
Count
Warning
ACKed segment that wasn't captured (common at captur...
Sequence
TCP
1
Warning
Previous segment not captured (common at capture start)
Sequence
TCP
9
Note
This frame is a (suspected) retransmission
Sequence
TCP
52
300
696
867
1253
1712 [TCP Retransmission] 1204→98
2008 [TCP Retransmission] 1181→98
Apply as Filter
Prepare a Filter
Find
Colorize
Look Up
Copy
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

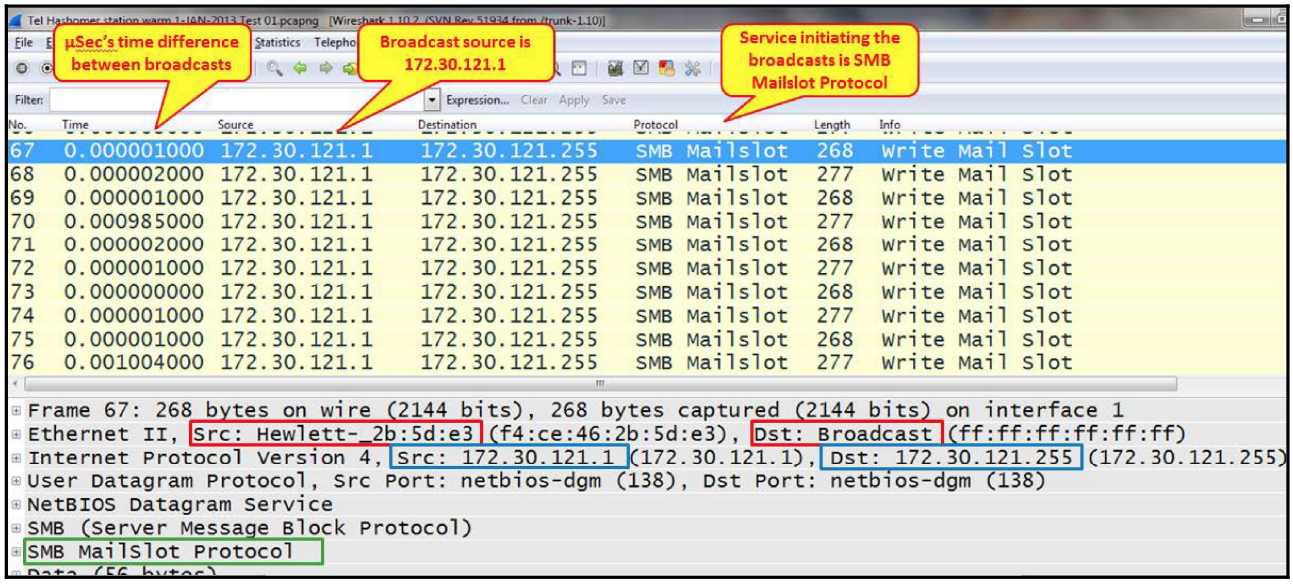

Wireshark · Expert Information · CAP_07_05
Severity
Summary
Group
Protocol
Count
Error
Bad checksum [should be 0x56eab082]
Checksum
Ethernet
85
Warning
Duplicate IP address configured (192.168.1.200)
Sequence
ARP/RARP
156
Warning
No response seen to ICMP request
Sequence
ICMP
7
Note
"Time To Live" only 4
Sequence
IPv4
3
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

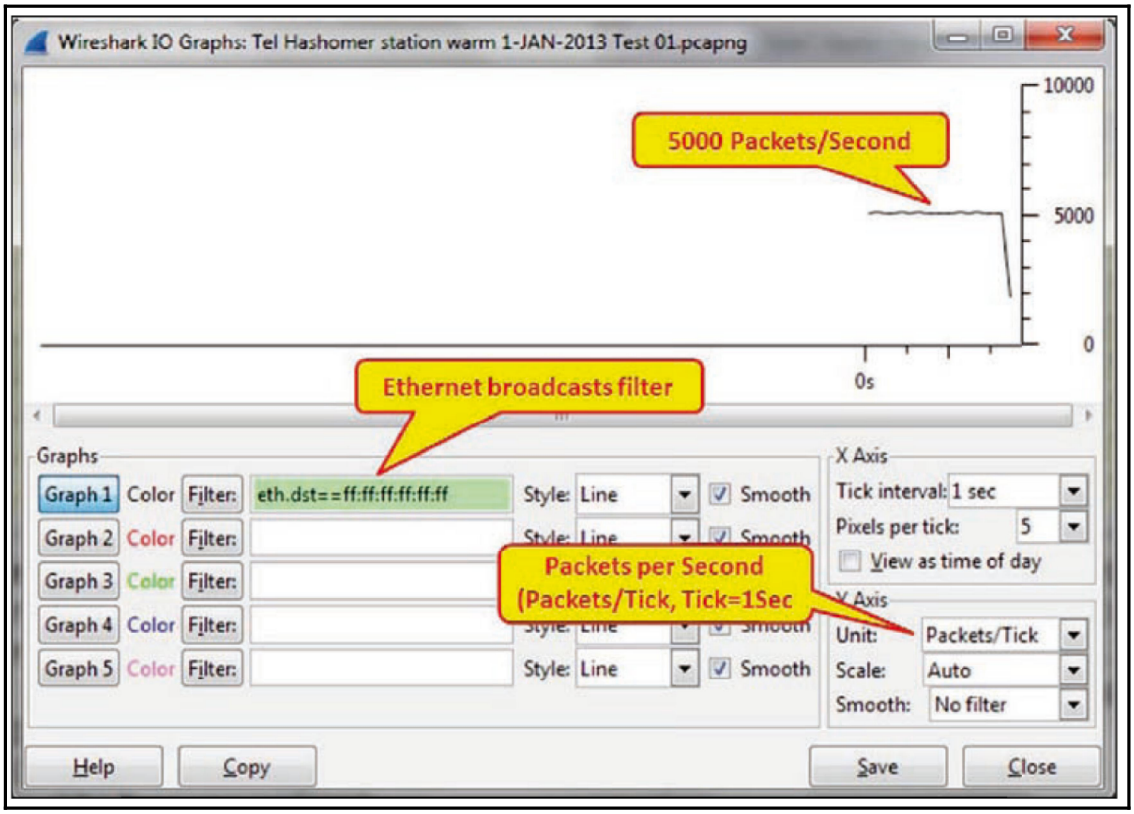

Wireshark · Expert Information · CAP_07_05
Packet
Summary
Group
Error
Bad checksum [should be 0x56eab082]
Checksum
1 Conf. Root = 32768/0/00:30:7b:e1:7b:40 Cost = 0 Port = 0x8019 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
7 Conf. Root = 32768/0/00:30:7b:e1:7b:40 Cost = 0 Port = 0x8019 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
13 Conf. Root = 32768/0/00:30:7b:e1:7b:40 Cost = 0 Port = 0x8019 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
20 Conf. Root = 32768/0/00:30:7b:e1:7b:40 Cost = 0 Port = 0x8019 [ETHERNET FRAME CHECK SEQUENCE INCORRECT]
No display filter set.
Limit to Display Filter
Frame 7: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
IEEE 802.3 Ethernet
Destination: Spanning-tree-(for-bridges)_00 (01:80:c2:00:00:00)
Source: CiscoInc_e1:7b:4c (00:30:7b:e1:7b:4c)
Length: 38
Padding: 0000000000000000
Frame check sequence: 0x78000c00 [incorrect, should be 0x56eab082]
[Expert Info (Error/Checksum): Bad checksum [should be 0x56eab082]]
[Bad checksum [should be 0x56eab082]]
[Severity level: Error]
[Group: Checksum]
[FCS Status: Bad]
Logical-Link Control
Spanning Tree Protocol

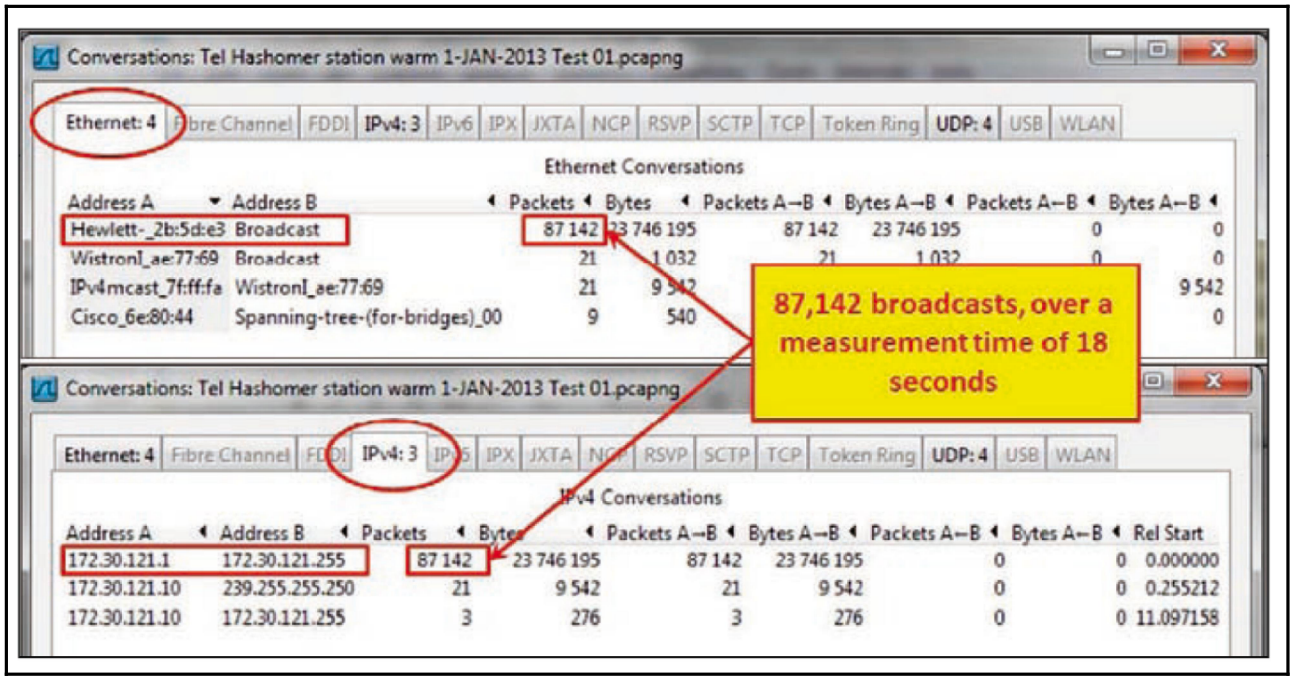

Wireshark · Expert Information · CAP_07_04
Packet
Summary
Group
Protocol
Count
Error Malformed Packet (Exception occurred) Malformed PPTP 3
Error Malformed Packet (Exception occurred) Malformed CAT-TP 1
Warning Connection reset (RST) Sequence TCP 831
Warning This frame is a (suspected) out-of-order segment Sequence TCP 1680
Warning Unknown header (class=0, pc=0, tag=0) Protocol DCERPC 254
Warning Previous segment not captured (common at capture start) Sequence TCP 1762
Warning Wrong calculate length (11) =! header length (15) ! (May ... Malformed CAPWAP-DATA 221
Warning Unknown header (class=2, pc=1, tag=1) Protocol GSS-API 2
Warning BER Error: Wrong tag in tagged type Malformed C12.22 26
Warning BER Error: Wrong field in SEQUENCE Malformed C12.22 33
Warning No response seen to ICMP request Sequence ICMP 43
Warning Ignored Unknown Record Protocol SSL 25
Warning TCP Zero Window segment Sequence TCP 17
Warning TCP window specified by the receiver is now completely f... Sequence TCP 34
Warning BER Error: Wrong field in SEQUENCE Malformed LDAP 67
Warning BER Error: Sequence expected Malformed LDAP 38
Warning BER Error: Unknown field in Sequence Malformed LDAP 8
Warning BER Error: Wrong tag in tagged type Malformed SPNEGO 8
Warning Kerberos SSP Verifier unavailable Undecoded DCERPC 8
Warning Bind not acknowledged Sequence DCERPC 8
Note No bind info for interface Context ID 0 - capture start too... Undecoded DCERPC 1097
Note This frame is a (suspected) retransmission Sequence TCP 258
Note A new tcp session is started with the same ports as an earl... Sequence TCP 27
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

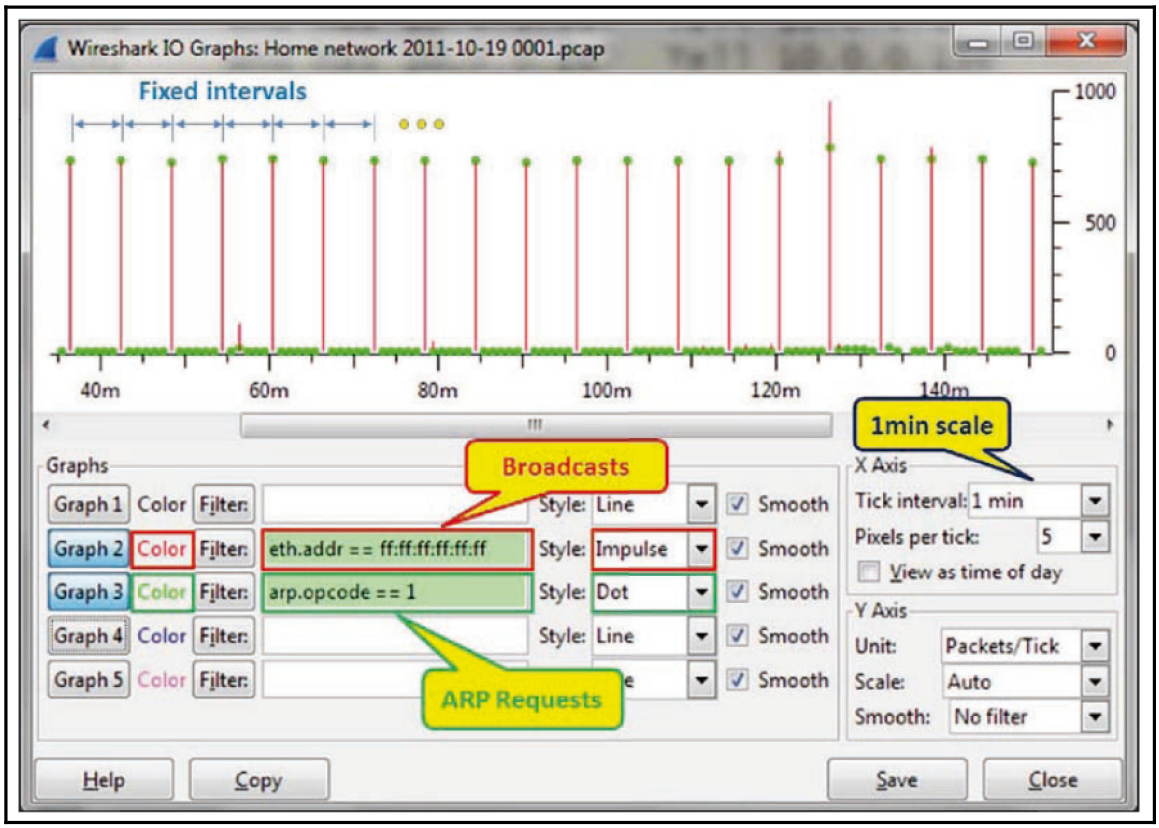

Wireshark · Expert Information · CAP_07_04
Severity
Summary
Group
Protocol
Count
Note
Duplicate ACK (#16)
Sequence
TCP
2
Note
Duplicate ACK (#17)
Sequence
TCP
2
Note
Duplicate ACK (#18)
Sequence
TCP
2
Note
Duplicate ACK (#19)
Sequence
TCP
2
Note
Duplicate ACK (#20)
Sequence
TCP
2
Note
This frame is a (suspected) fast retransmission
Sequence
TCP
10
Note
noSuchInstance
Response
SNMP
19
Note
ACK to a TCP keep-alive segment
Sequence
TCP
9
Note
No specification available, dissection not possible
Undecoded
ISystemActivator
32
Note
Fault: nca_s_fault_access_denied
Response
DCERPC
30
Note
This frame is a (suspected) spurious retransmission
Sequence
TCP
37
Note
No bind info for interface Context ID 1 - capture start too...
Undecoded
DCERPC
17
Note
Retransmission (retry)
Sequence
IEEE 802.11
4
Note
Unrecognised SIP header (x-nt-corr-id)
Undecoded
SIP
2
Chat
Connection establish acknowledge (SYN+ACK): server por...
Sequence
TCP
316
Chat
Connection establish request (SYN): server port 80
Sequence
TCP
491
No display filter set.
Limit to Display Filter
Group by summary
Search:
Show...
Close
Help

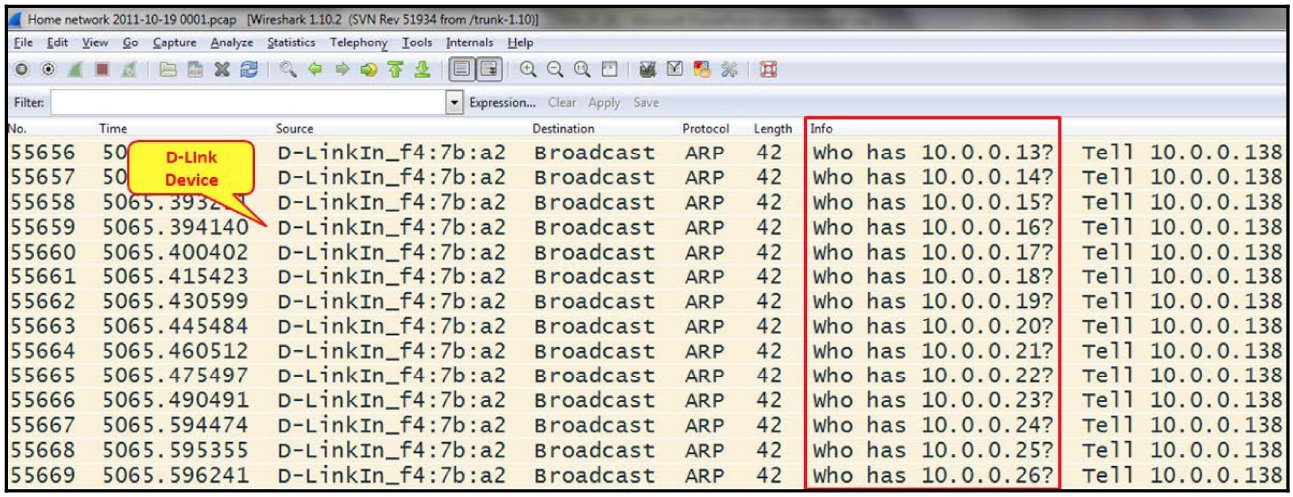
Chapter 8: Ethernet and LAN Switching

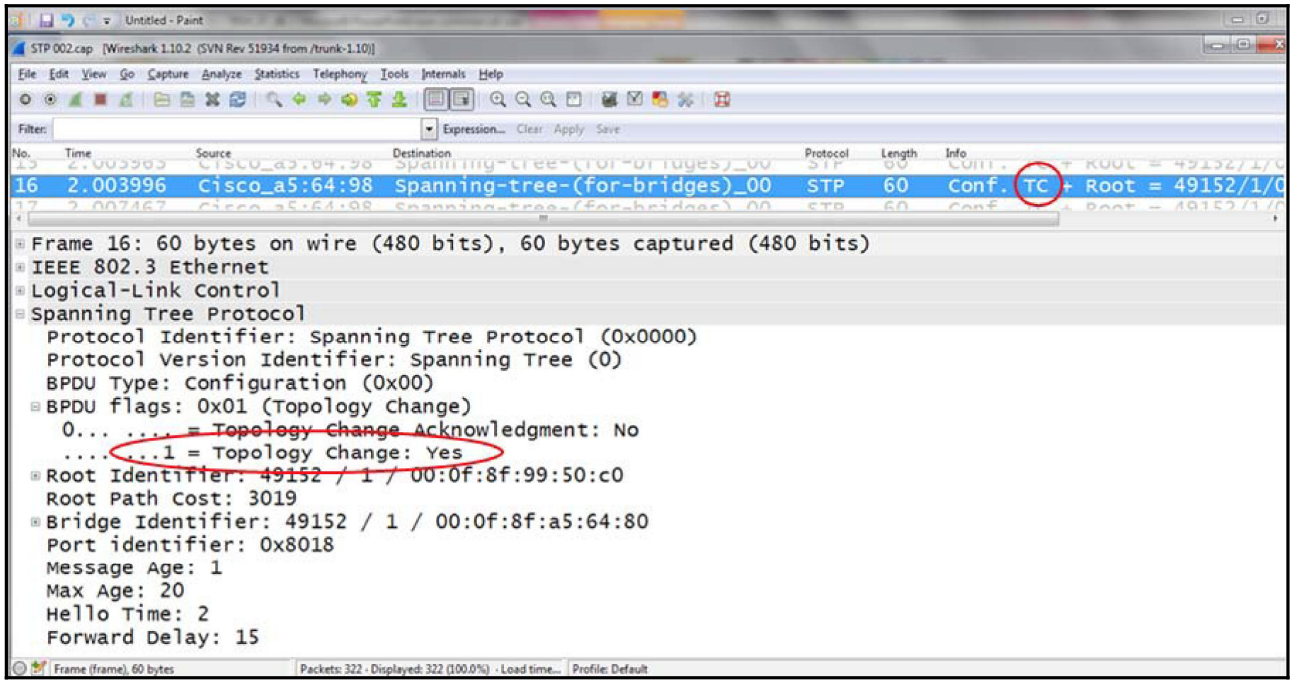


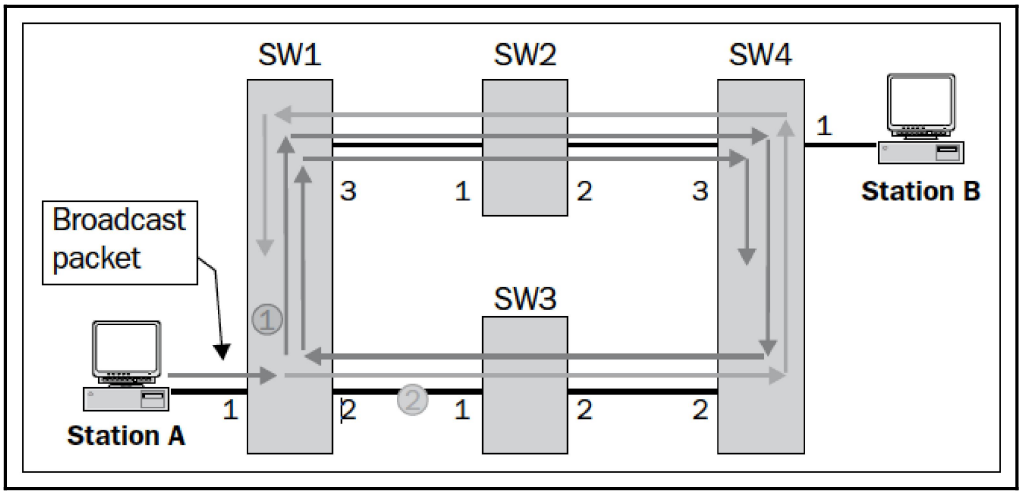


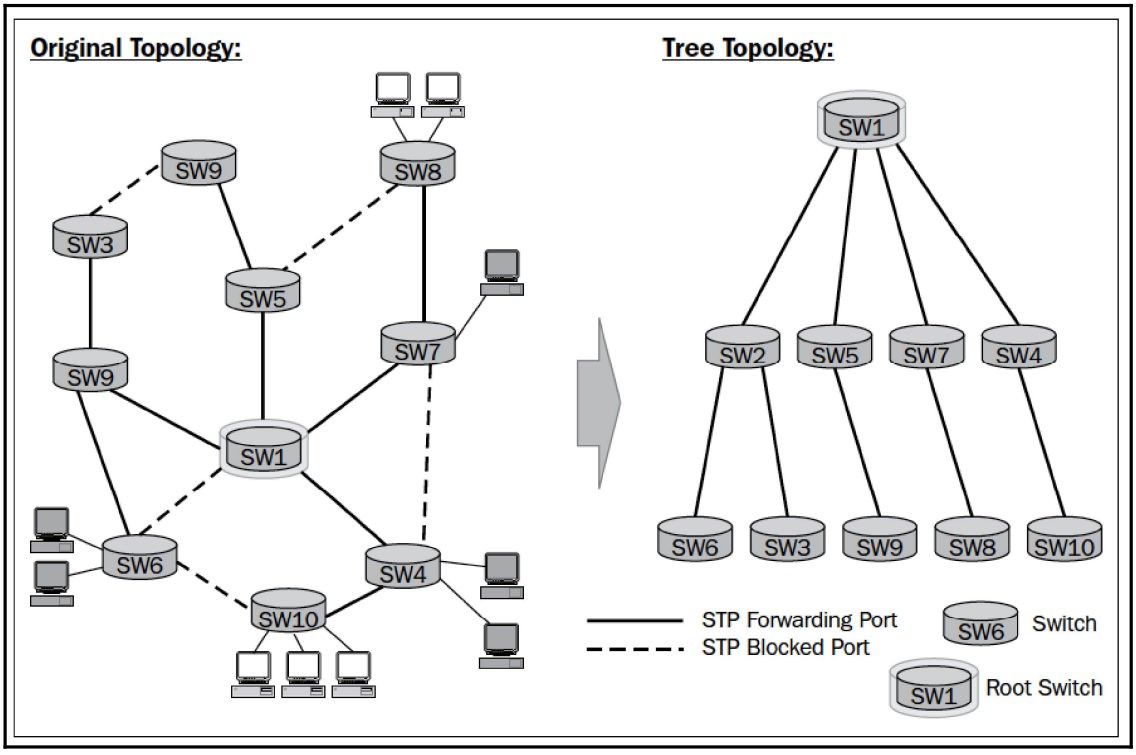

Conversations: Tel Hashomer station warm 1-JAN-2013 Test 01.pcapng
Ethernet: 4
Fibre Channel
FDDI
IPv4: 3
IPv6
IPX
JXTA
NCP
RSVP
SCTP
TCP
Token Ring
UDP: 4
USB
WLAN
Ethernet Conversations
Address A
Address B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
Hewlett-_2b:5d:e3
Broadcast
87 142
23 746 195
87 142
23 746 195
0
0
Wistronl_ae:77:69
Broadcast
21
1 032
21
1 032
0
0
IPv4mcast_7f:ff:fa
Wistronl_ae:77:69
21
9 542
9 542
Cisco_6e:80:44
Spanning-tree-(for-bridges)_00
9
540
0
87,142 broadcasts, over a measurement time of 18 seconds
Conversations: Tel Hashomer station warm 1-JAN-2013 Test 01.pcapng
IPv4 Conversations
Address A
Address B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
Rel Start
172.30.121.1
172.30.121.255
87 142
23 746 195
87 142
23 746 195
0
0
0.000000
172.30.121.10
239.255.255.250
21
9 542
21
9 542
0
0
0.255212
172.30.121.10
172.30.121.255
3
276
3
276
0
0
11.097158

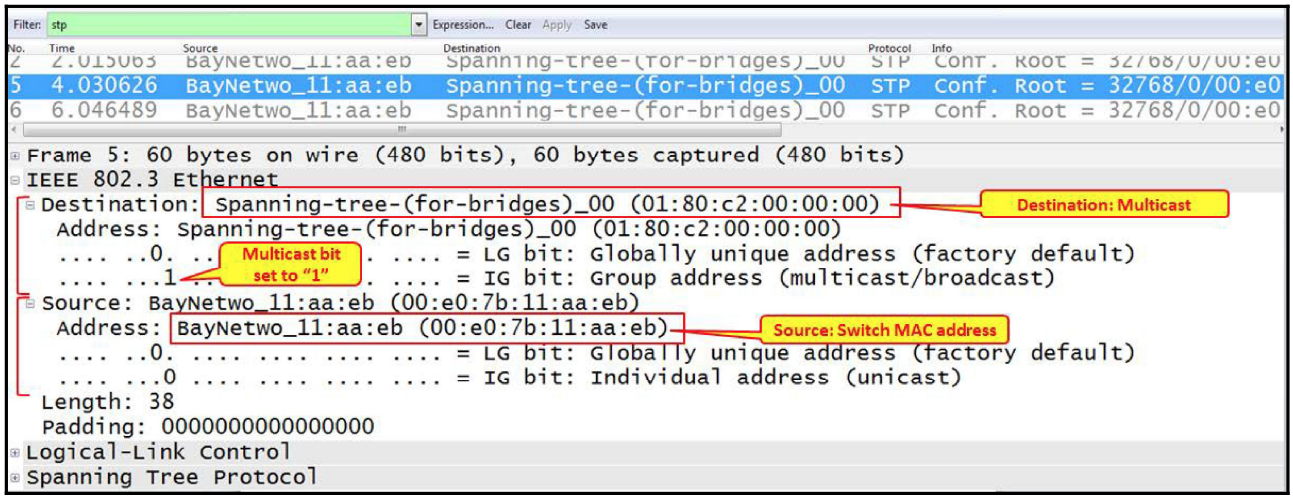

Wireshark IO Graphs: Home network 2011-10-19 0001.pcap
Fixed intervals
1000
500
0
40m
60m
80m
100m
120m
140m
1min scale
Broadcasts
ARP Requests
Graphs
Graph 1
Color
Filter:
Style:
Line
Smooth
Graph 2
Color
Filter:
eth.addr == ff:ff:ff:ff:ff:ff
Style:
Impulse
Smooth
Graph 3
Color
Filter:
arp.opcode == 1
Style:
Dot
Smooth
Graph 4
Color
Filter:
Style:
Line
Smooth
Graph 5
Color
Filter:
Smooth
X Axis
Tick interval:
1 min
Pixels per tick:
5
View as time of day
Y Axis
Unit:
Packets/Tick
Scale:
Auto
Smooth:
No filter
Help
Copy
Save
Close

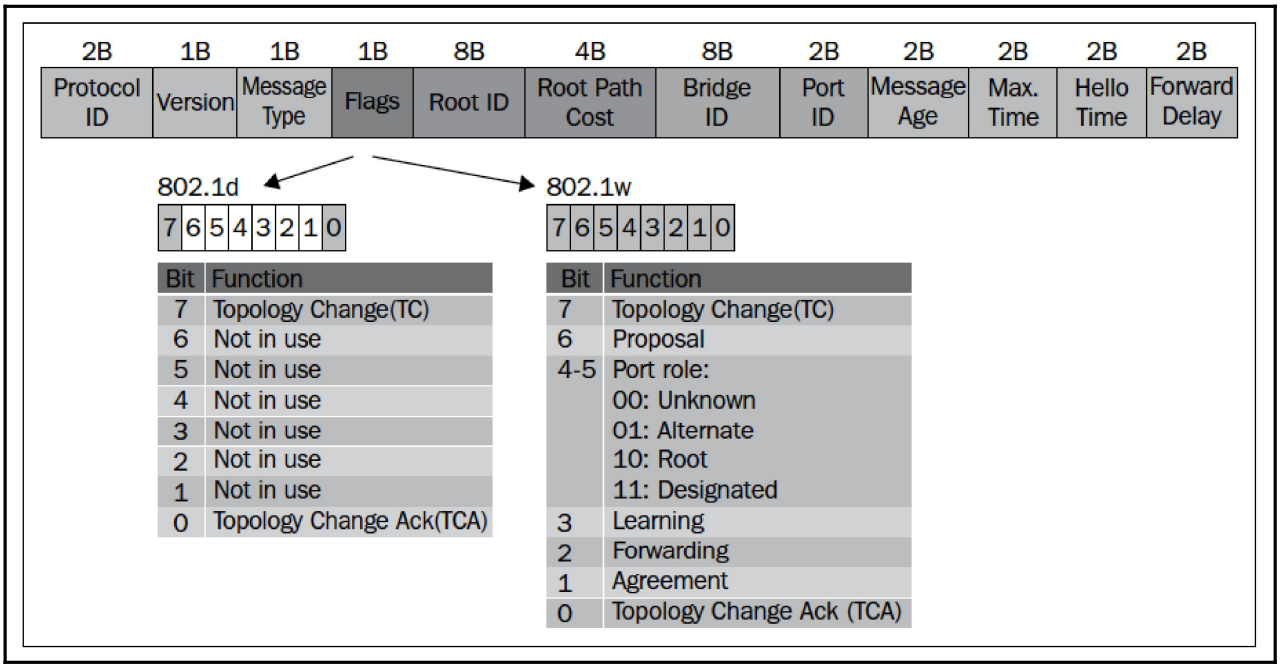

Home network 2011-10-19 0001.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
D-Link Device
55656 50 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.13? Tell 10.0.0.138
55657 50 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.14? Tell 10.0.0.138
55658 5065.393 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.15? Tell 10.0.0.138
55659 5065.394140 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.16? Tell 10.0.0.138
55660 5065.400402 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.17? Tell 10.0.0.138
55661 5065.415423 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.18? Tell 10.0.0.138
55662 5065.430599 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.19? Tell 10.0.0.138
55663 5065.445484 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.20? Tell 10.0.0.138
55664 5065.460512 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.21? Tell 10.0.0.138
55665 5065.475497 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.22? Tell 10.0.0.138
55666 5065.490491 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.23? Tell 10.0.0.138
55667 5065.594474 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.24? Tell 10.0.0.138
55668 5065.595355 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.25? Tell 10.0.0.138
55669 5065.596241 D-LinkIn_f4:7b:a2 Broadcast ARP 42 Who has 10.0.0.26? Tell 10.0.0.138


Untitled - Paint
STP 002.cap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
16 2.003996 Cisco_a5:64:98 Spanning-tree-(for-bridges)_00 STP 60 Conf. TC + Root = 49152/1/0
Frame 16: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Spanning Tree (0)
BPDU Type: Configuration (0x00)
BPDU flags: 0x01 (Topology Change)
0... .... = Topology Change Acknowledgment: No
....1 = Topology Change: Yes
Root Identifier: 49152 / 1 / 00:0f:8f:99:50:c0
Root Path Cost: 3019
Bridge Identifier: 49152 / 1 / 00:0f:8f:a5:64:80
Port identifier: 0x8018
Message Age: 1
Max Age: 20
Hello Time: 2
Forward Delay: 15
Frame (frame), 60 bytes
Packets: 322 · Displayed: 322 (100.0%) · Load time...
Profile: Default


SW1
SW2
SW4
SW3
Broadcast packet
Station A
Station B
1
2
3

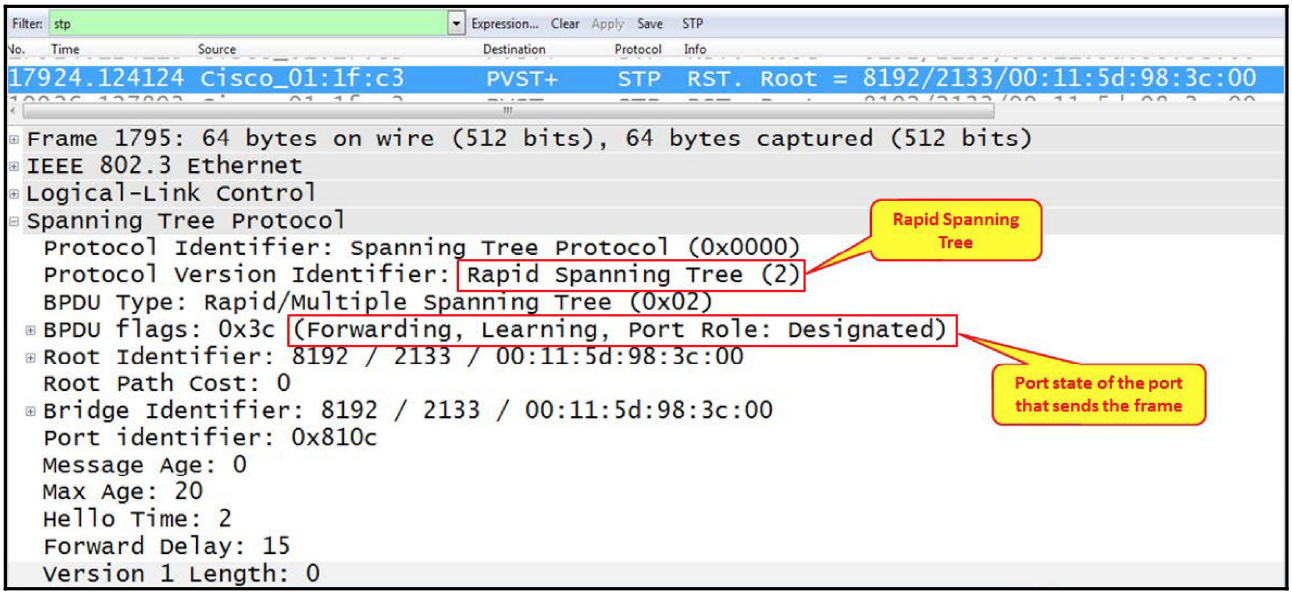

Original Topology:
Tree Topology:
SW1
SW2
SW3
SW4
SW5
SW6
SW7
SW8
SW9
SW10
STP Forwarding Port
STP Blocked Port
Switch
Root Switch

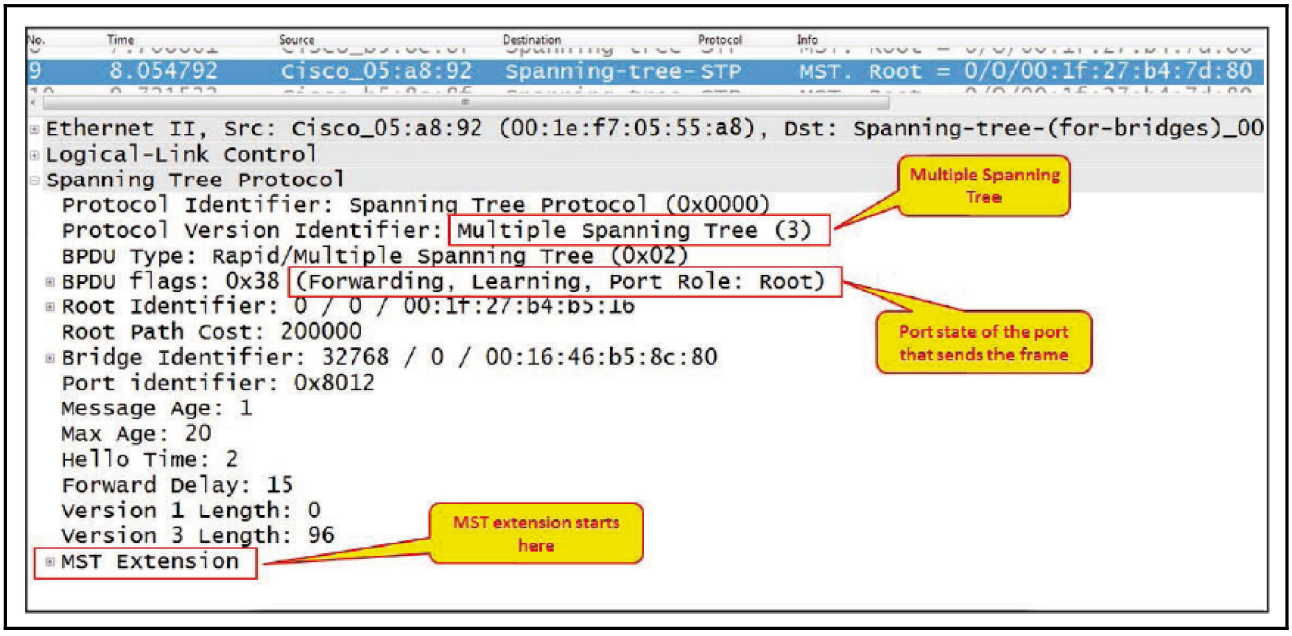


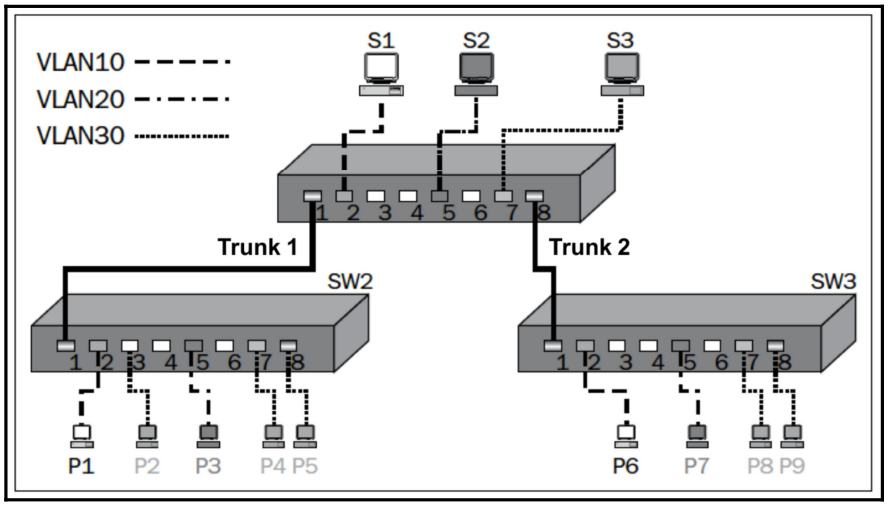


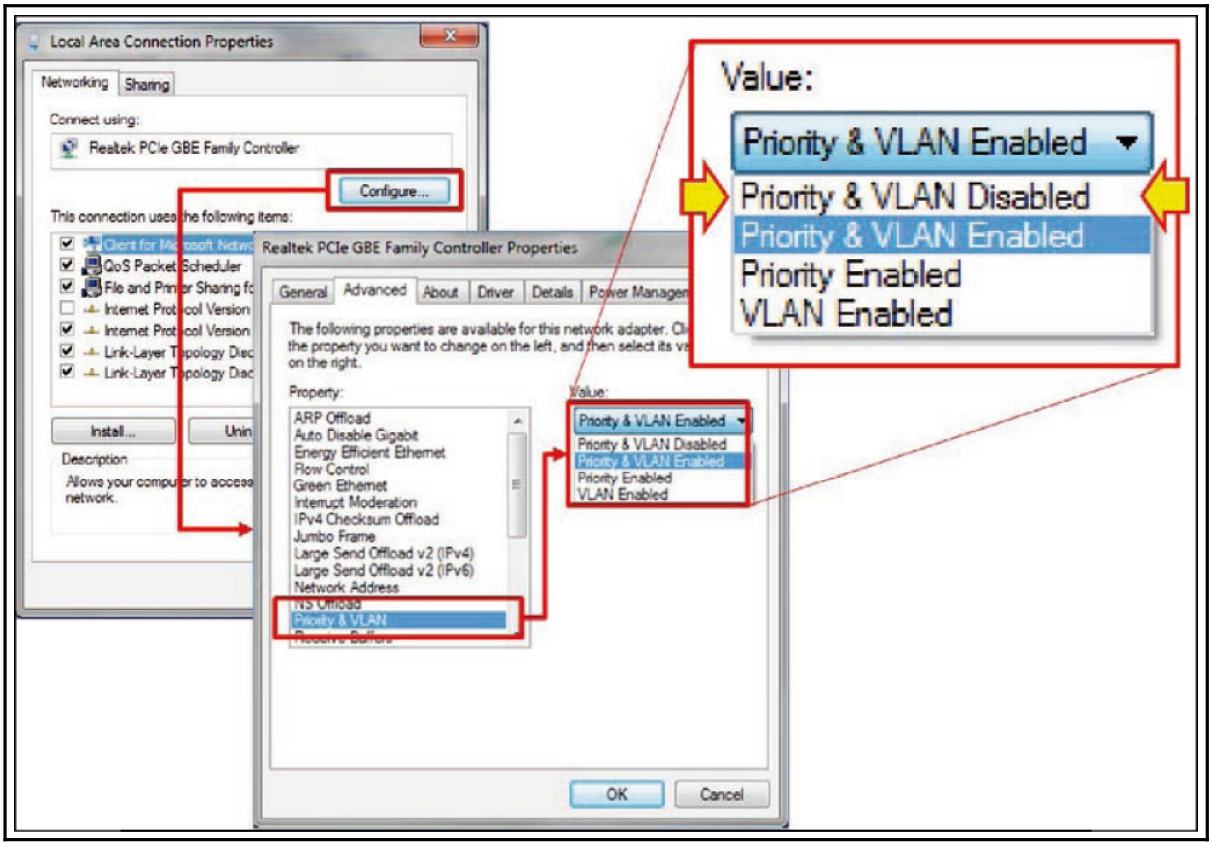
Bit	Function
7	Topology Change(TC)
6	Not in use
5	Not in use
4	Not in use
3	Not in use
2	Not in use
1	Not in use
0	Topology Change Ack(TCA)

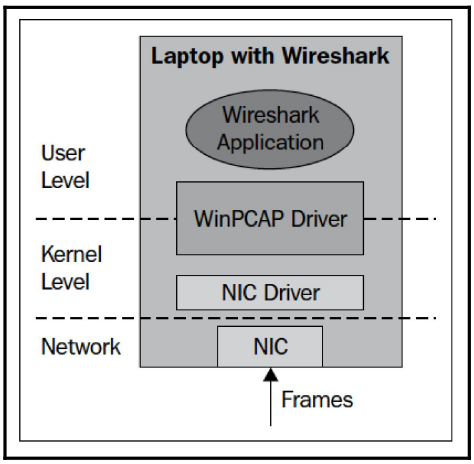
Bit	Function
7	Topology Change(TC)
6	Proposal
4-5	Port role: 00: Unknown 01: Alternate 10: Root 11: Designated
3	Learning
2	Forwarding
1	Agreement
0	Topology Change Ack (TCA)

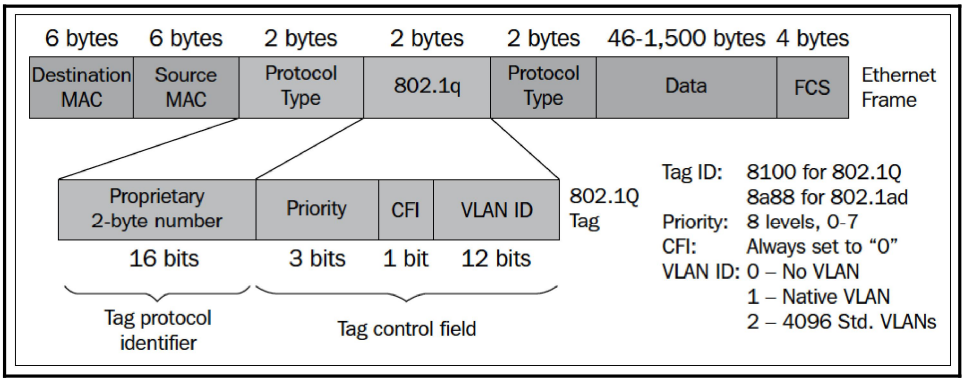

Filter: stp
Expression... Clear Apply Save STP
No. Time Source Destination Protocol Info
17924.124124 Cisco_01:1f:c3 PVST+ STP RST. Root = 8192/2133/00:11:5d:98:3c:00
Frame 1795: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
IEEE 802.3 Ethernet
Logical-Link Control
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Rapid Spanning Tree (2)
BPDU Type: Rapid/Multiple Spanning Tree (0x02)
BPDU flags: 0x3c (Forwarding, Learning, Port Role: Designated)
Root Identifier: 8192 / 2133 / 00:11:5d:98:3c:00
Root Path Cost: 0
Bridge Identifier: 8192 / 2133 / 00:11:5d:98:3c:00
Port identifier: 0x810c
Message Age: 0
Max Age: 20
Hello Time: 2
Forward Delay: 15
Version 1 Length: 0
Rapid Spanning Tree
Port state of the port that sends the frame

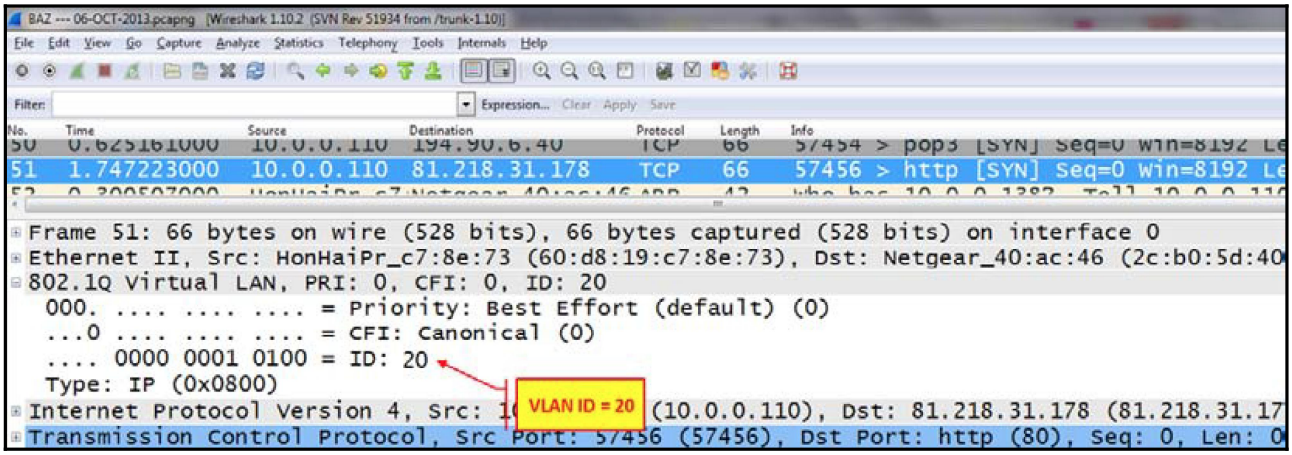

No. Time Source Destination Protocol Info
9 8.054792 Cisco_05:a8:92 Spanning-tree-STP MST. Root = 0/0/00:1f:27:b4:7d:80
Ethernet II, Src: Cisco_05:a8:92 (00:1e:f7:05:55:a8), Dst: Spanning-tree-(for-bridges)_00
Logical-Link Control
Spanning Tree Protocol
Protocol Identifier: Spanning Tree Protocol (0x0000)
Protocol Version Identifier: Multiple Spanning Tree (3)
BPDU Type: Rapid/Multiple Spanning Tree (0x02)
BPDU flags: 0x38 (Forwarding, Learning, Port Role: Root)
Root Identifier: 0 / 0 / 00:1f:27:b4:b5:16
Root Path Cost: 200000
Bridge Identifier: 32768 / 0 / 00:16:46:b5:8c:80
Port identifier: 0x8012
Message Age: 1
Max Age: 20
Hello Time: 2
Forward Delay: 15
Version 1 Length: 0
Version 3 Length: 96
MST Extension
Multiple Spanning Tree
Port state of the port that sends the frame
MST extension starts here


VLAN10
VLAN20
VLAN30
S1
S2
S3
1 2 3 4 5 6 7 8
Trunk 1
Trunk 2
SW2
SW3
1 2 3 4 5 6 7 8
1 2 3 4 5 6 7 8
P1 P2 P3 P4 P5
P6 P7 P8 P9

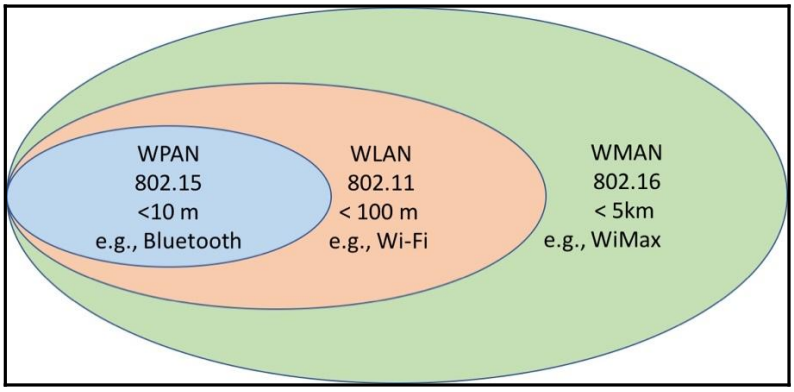

Local Area Connection Properties
Networking
Sharing
Connect using:
Realtek PCIe GBE Family Controller
Configure...
This connection uses the following items:
QoS Packet Scheduler
Internet Protocol Version
Internet Protocol Version
Link-Layer Topology Disc
Link-Layer Topology Disc
Install...
Description
Realtek PCIe GBE Family Controller Properties
General
Advanced
About
Driver
Details
Power Manage
The following properties are available for this network adapter.
the property you want to change on the left, and then select its v
on the right.
Property:
ARP Offload
Auto Disable Gigabit
Energy Efficient Ethernet
Flow Control
Green Ethernet
Interrupt Moderation
IPv4 Checksum Offload
Jumbo Frame
Large Send Offload v2 (IPv4)
Large Send Offload v2 (IPv6)
Network Address
Priority & VLAN
Value:
Priority & VLAN Enabled
Priority & VLAN Disabled
Priority & VLAN Enabled
Priority Enabled
VLAN Enabled
OK
Cancel
Value:
Priority & VLAN Enabled
Priority & VLAN Disabled
Priority & VLAN Enabled
Priority Enabled
VLAN Enabled

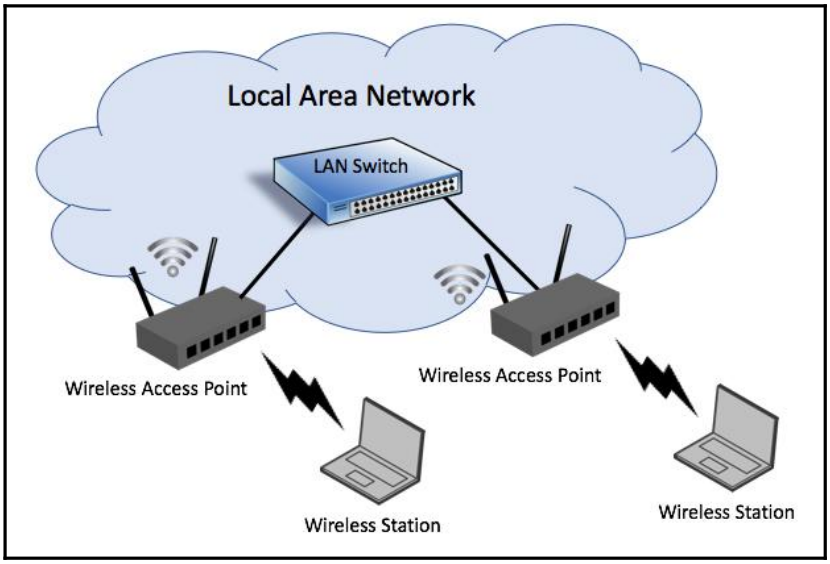

Laptop with Wireshark
Wireshark Application
User Level
WinPCAP Driver
Kernel Level
NIC Driver
Network
NIC
Frames

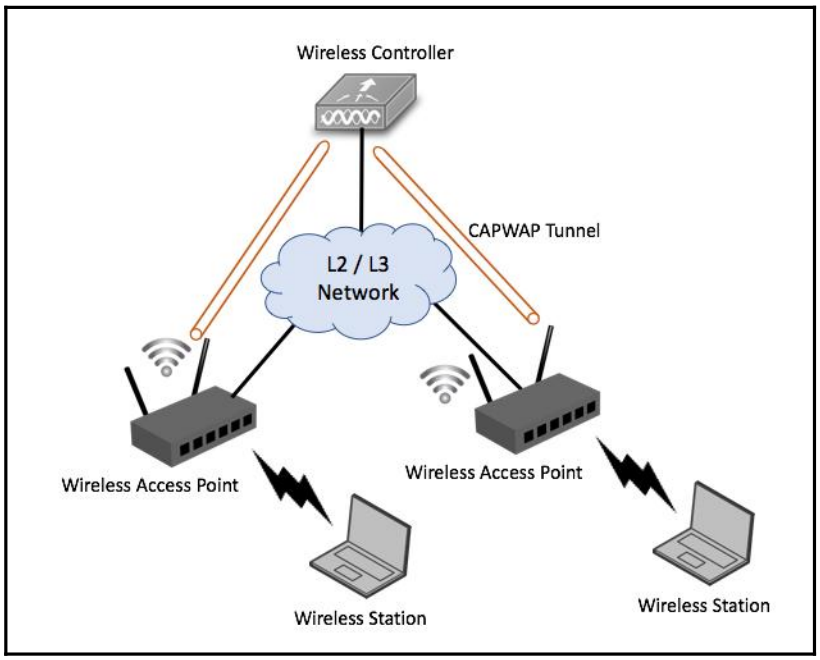

6 bytes
6 bytes
2 bytes
2 bytes
2 bytes
46-1,500 bytes
4 bytes
Destination MAC
Source MAC
Protocol Type
802.1q
Protocol Type
Data
FCS
Ethernet Frame
Proprietary 2-byte number
Priority
CFI
VLAN ID
802.1Q Tag
16 bits
3 bits
1 bit
12 bits
Tag protocol identifier
Tag control field
Tag ID: 8100 for 802.1Q
8a88 for 802.1ad
Priority: 8 levels, 0-7
CFI: Always set to "0"
VLAN ID: 0 – No VLAN
1 – Native VLAN
2 – 4096 Std. VLANs

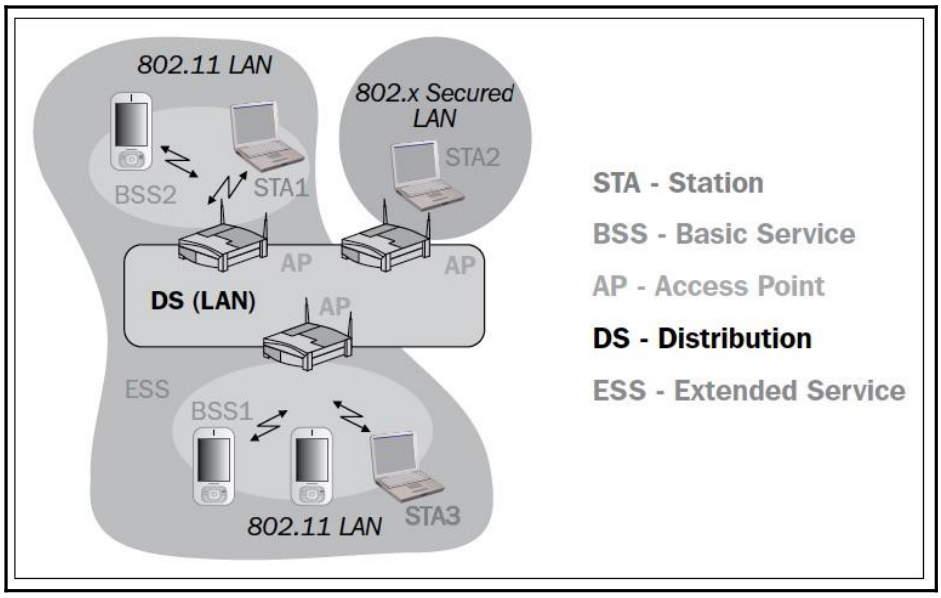

BAZ --- 06-OCT-2013.pcapng [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
51 1.747223000 10.0.0.110 81.218.31.178 TCP 66 57456 > http [SYN] Seq=0 Win=8192 Le
Frame 51: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: Netgear_40:ac:46 (2c:b0:5d:40
802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
000. .... = Priority: Best Effort (default) (0)
...0 .... = CFI: Canonical (0)
.... 0000 0001 0100 = ID: 20
Type: IP (0x0800)
VLAN ID = 20
Internet Protocol Version 4, Src: 10.0.0.110 (10.0.0.110), Dst: 81.218.31.178 (81.218.31.17
Transmission Control Protocol, Src Port: 57456 (57456), Dst Port: http (80), Seq: 0, Len: 0

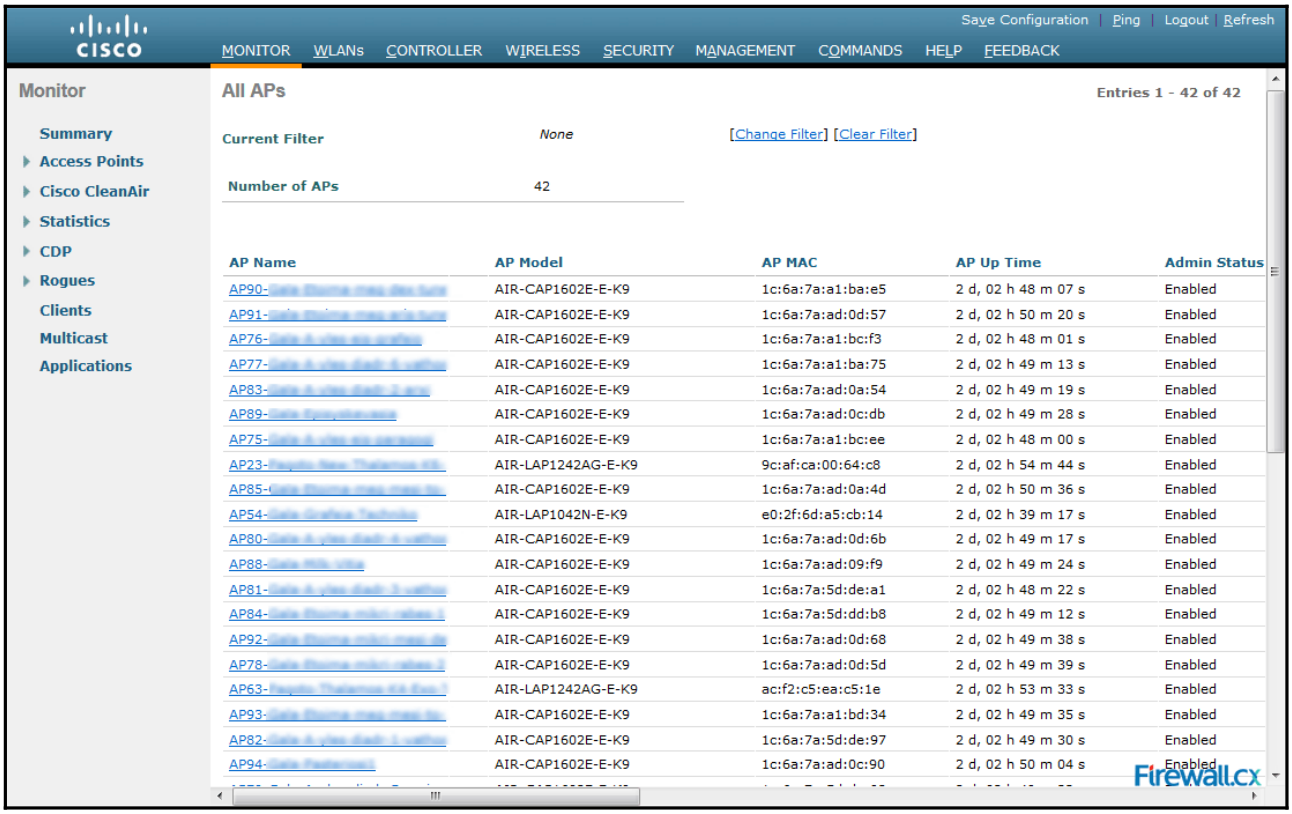
Chapter 9: Wireless LAN

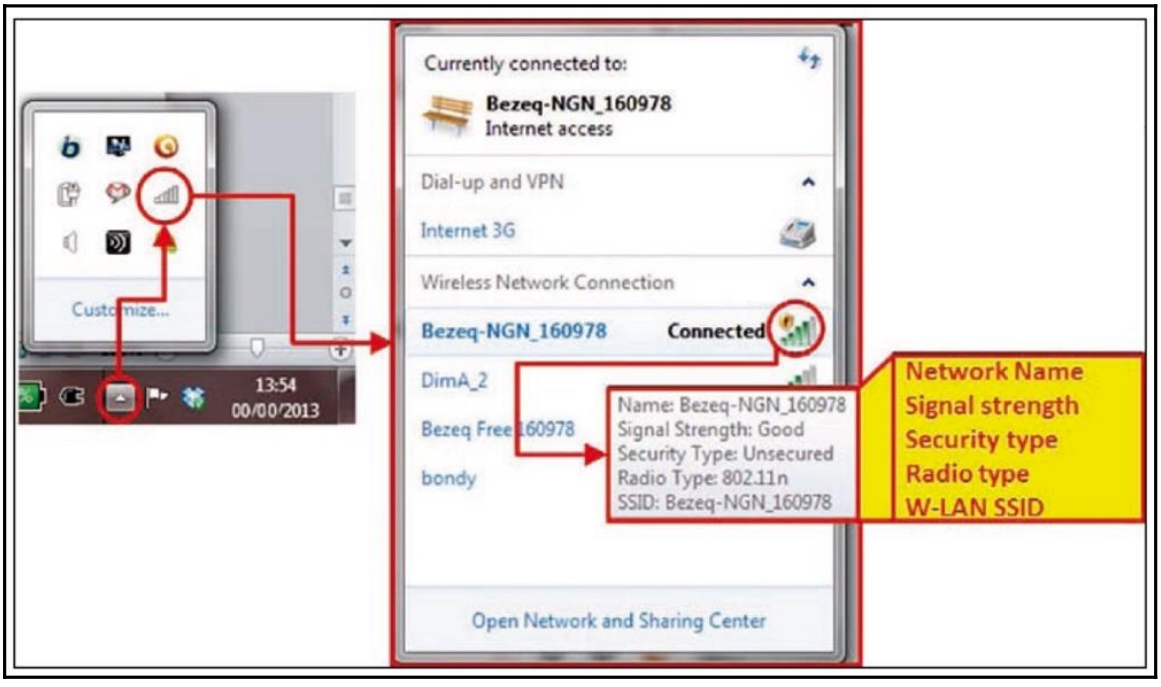


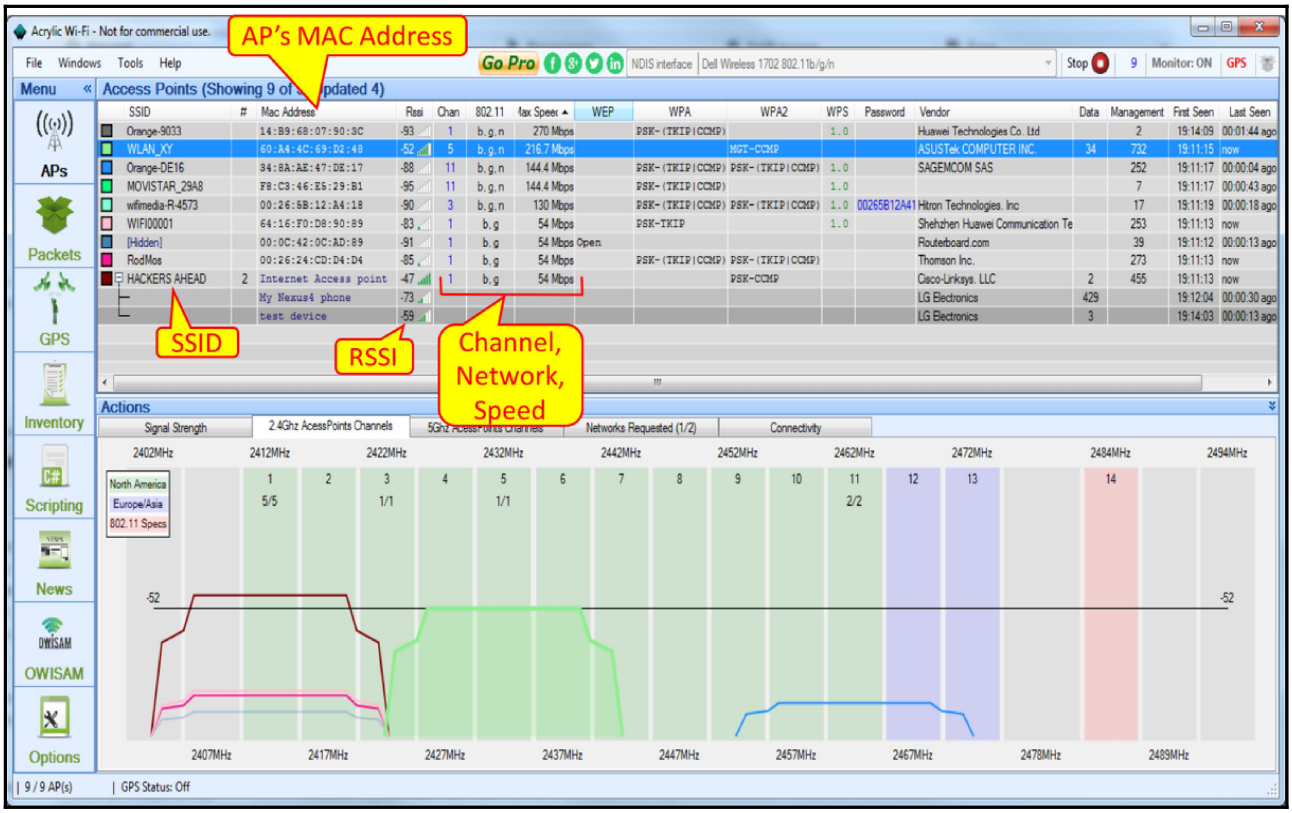



Wireless Controller
CAPWAP Tunnel
L2 / L3
Network
Wireless Access Point
Wireless Access Point
Wireless Station
Wireless Station


802.11 LAN
802.x Secured
LAN
STA2
BSS2
STA1
AP
AP
DS (LAN)
AP
ESS
BSS1
802.11 LAN
STA3
STA - Station
BSS - Basic Service
AP - Access Point
DS - Distribution
ESS - Extended Service

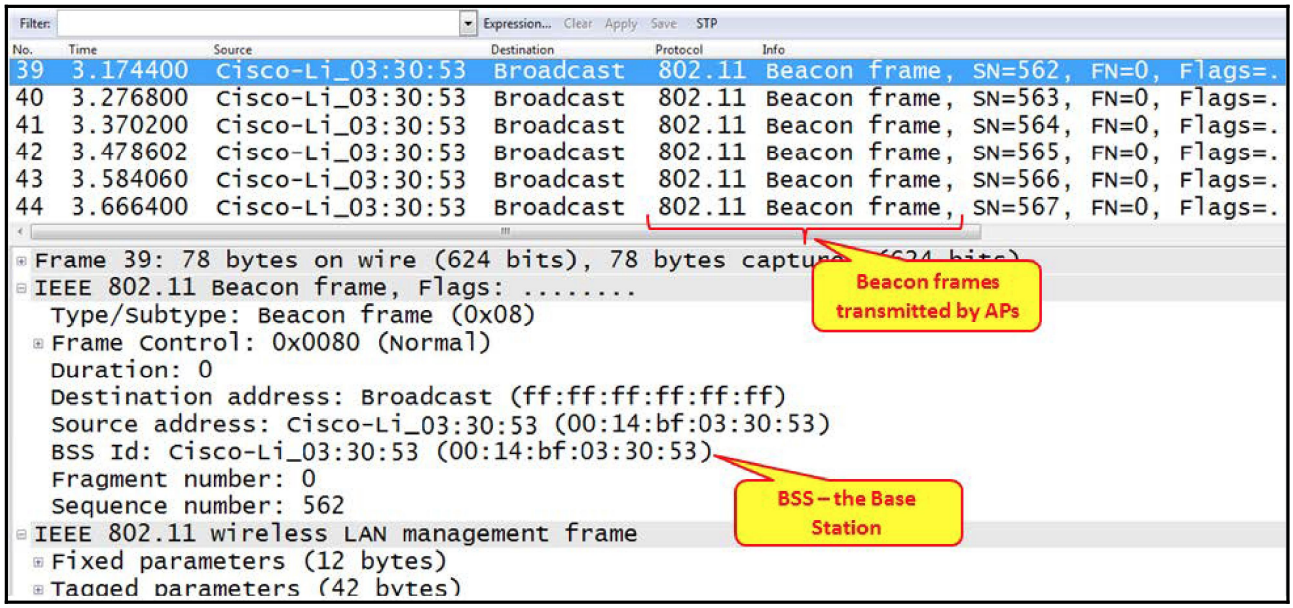

Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Monitor
Summary
Access Points
Cisco CleanAir
Statistics
CDP
Rogues
Clients
Multicast
Applications
All APs
Entries 1 - 42 of 42
Current Filter None [Change Filter] [Clear Filter]
Number of APs 42
AP Name AP Model AP MAC AP Up Time Admin Status
AP90- AIR-CAP1602E-E-K9 1c:6a:7a:a1:ba:e5 2 d, 02 h 48 m 07 s Enabled
AP91- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0d:57 2 d, 02 h 50 m 20 s Enabled
AP76- AIR-CAP1602E-E-K9 1c:6a:7a:a1:bc:f3 2 d, 02 h 48 m 01 s Enabled
AP77- AIR-CAP1602E-E-K9 1c:6a:7a:a1:ba:75 2 d, 02 h 49 m 13 s Enabled
AP83- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0a:54 2 d, 02 h 49 m 19 s Enabled
AP89- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0c:db 2 d, 02 h 49 m 28 s Enabled
AP75- AIR-CAP1602E-E-K9 1c:6a:7a:a1:bc:ee 2 d, 02 h 48 m 00 s Enabled
AP23- AIR-LAP1242AG-E-K9 9c:af:ca:00:64:c8 2 d, 02 h 54 m 44 s Enabled
AP85- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0a:4d 2 d, 02 h 50 m 36 s Enabled
AP54- AIR-LAP1042N-E-K9 e0:2f:6d:a5:cb:14 2 d, 02 h 39 m 17 s Enabled
AP80- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0d:6b 2 d, 02 h 49 m 17 s Enabled
AP88- AIR-CAP1602E-E-K9 1c:6a:7a:ad:09:f9 2 d, 02 h 49 m 24 s Enabled
AP81- AIR-CAP1602E-E-K9 1c:6a:7a:5d:de:a1 2 d, 02 h 48 m 22 s Enabled
AP84- AIR-CAP1602E-E-K9 1c:6a:7a:5d:dd:b8 2 d, 02 h 49 m 12 s Enabled
AP92- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0d:68 2 d, 02 h 49 m 38 s Enabled
AP78- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0d:5d 2 d, 02 h 49 m 39 s Enabled
AP63- AIR-LAP1242AG-E-K9 ac:f2:c5:ea:c5:1e 2 d, 02 h 53 m 33 s Enabled
AP93- AIR-CAP1602E-E-K9 1c:6a:7a:a1:bd:34 2 d, 02 h 49 m 35 s Enabled
AP82- AIR-CAP1602E-E-K9 1c:6a:7a:5d:de:97 2 d, 02 h 49 m 30 s Enabled
AP94- AIR-CAP1602E-E-K9 1c:6a:7a:ad:0c:90 2 d, 02 h 50 m 04 s Enabled
Firewall.cx

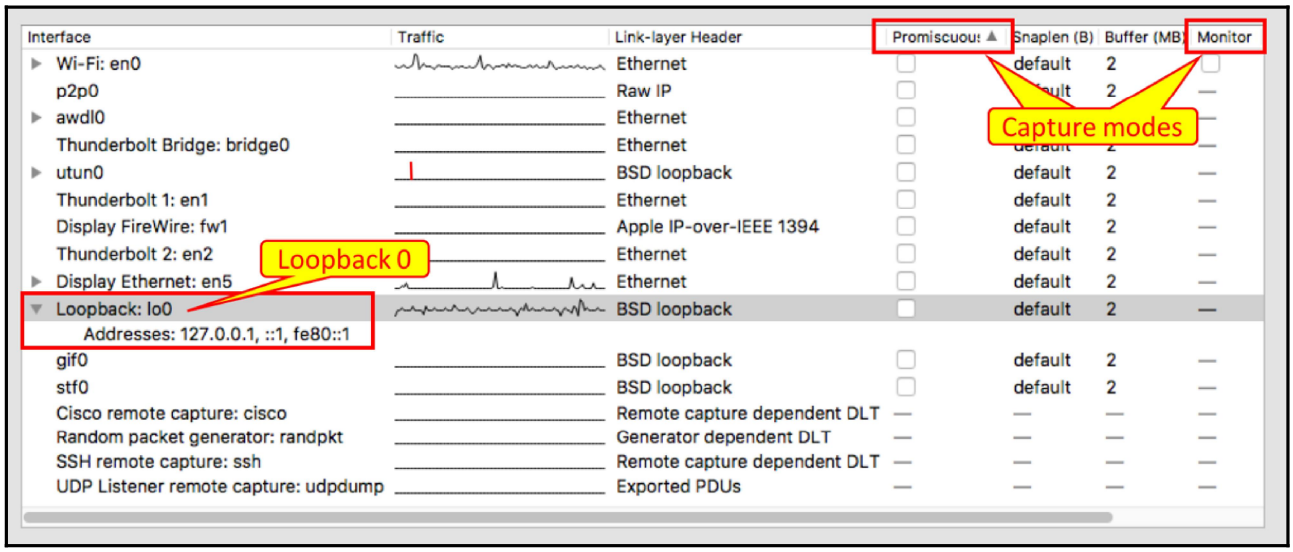

Currently connected to:
Bezeq-NGN_160978
Internet access
Dial-up and VPN
Internet 3G
Wireless Network Connection
Bezeq-NGN_160978 Connected
DimA_2
Bezeq Free 160978
bondy
Open Network and Sharing Center
Customize...
13:54
00/00/2013
Name: Bezeq-NGN_160978
Signal Strength: Good
Security Type: Unsecured
Radio Type: 802.11n
SSID: Bezeq-NGN_160978
Network Name
Signal strength
Security type
Radio type
W-LAN SSID

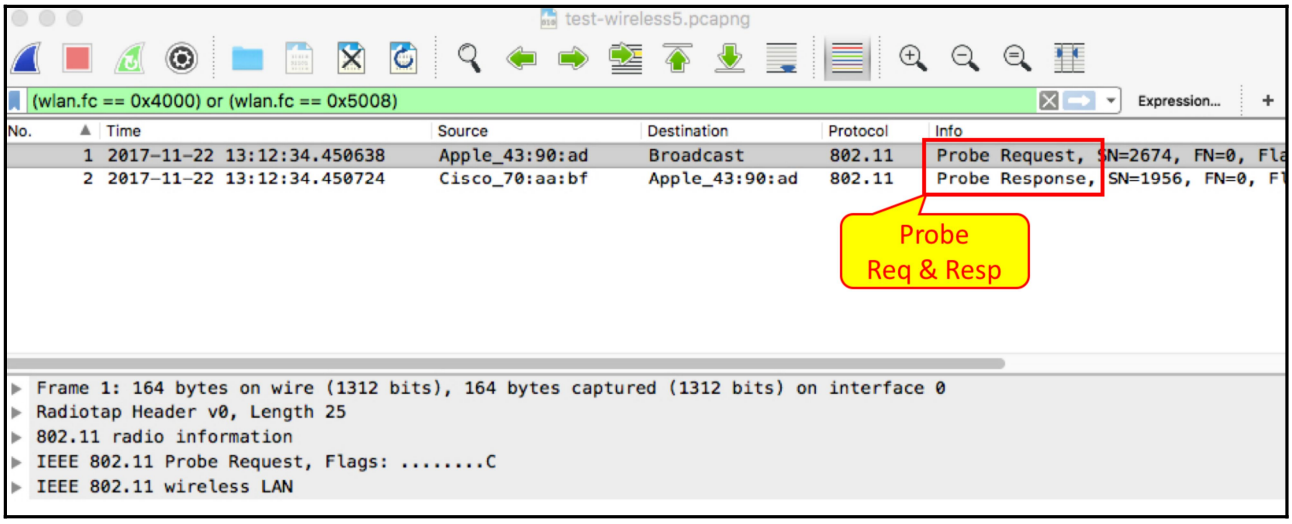

AP's MAC Address
SSID
RSSI
Channel, Network, Speed

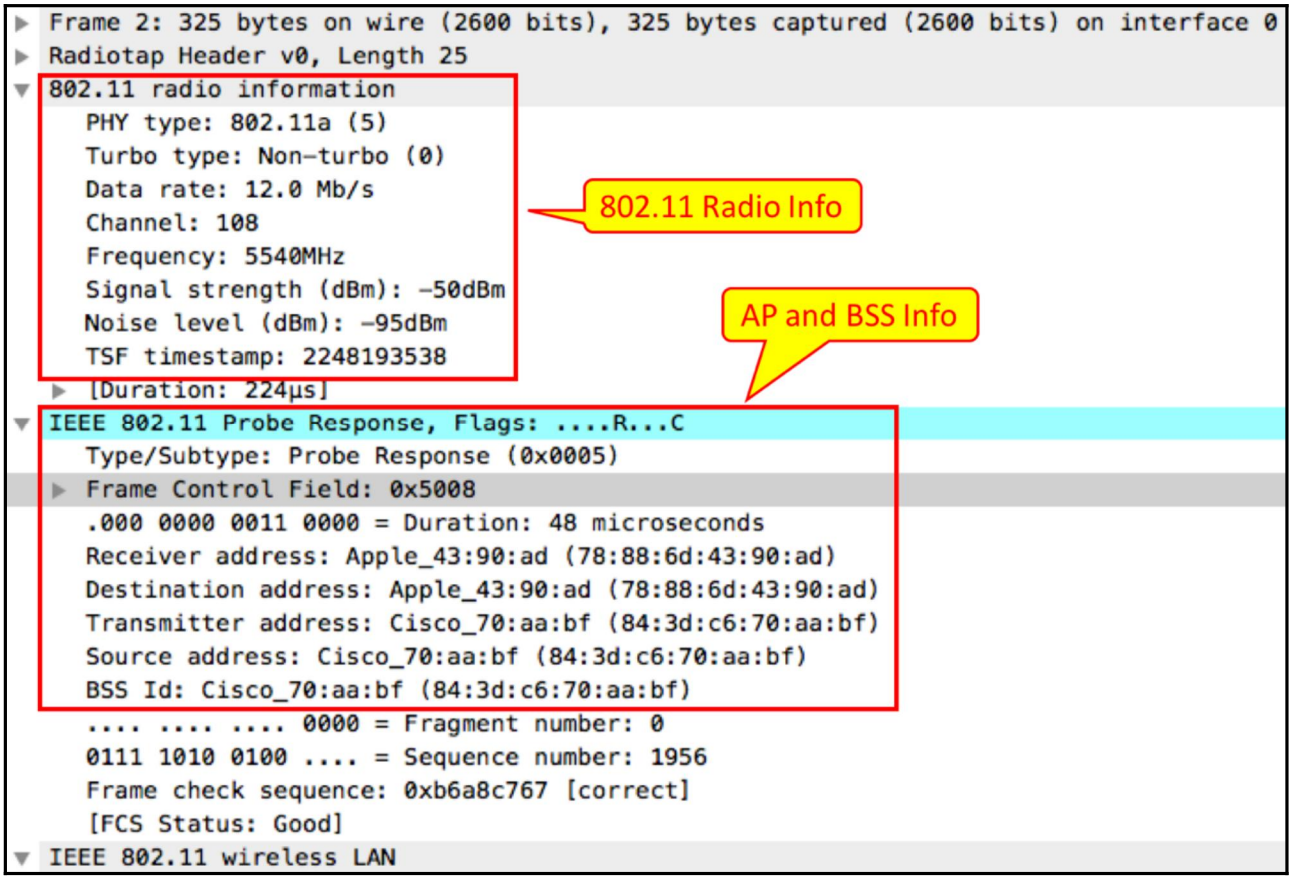

inSSIDer for Home
File View Help
LEARN
NETWORKS
metageek
Networks Table keyboard shortcuts: j=down, k=up, s=star, c=clear all
inSSIDer has starred the network you are connected to. To optimize a different one, star it in the Networks list below
FILTERS
SSID or Vendor
Channel
Signal
Security
802.11
SSID
SIGNAL
CHANNEL
SECURITY
MAC ADDRESS
802.11
Bezeq-NGN_160978 -66 6+10 Open 34:08:04:16:09:79 n
Bezeq Free 160978 -67 6+10 Open 34:08:04:16:09:7C n
bondy -72 6 WPA2-Personal C8:BE:19:10:23:FE n
DimA_2 -73 6+10 WEP FC:75:16:53:00:88 n
bondy
6 Channel
41 Link Score
MAC C8:BE:19:10:23:FE
Security WPA2-Personal
802.11 n
Max Rate 144
Co-Channel 3 Networks
Overlapping 0 Networks
Signal -72 dBm
Available networks
Networks RSSI over time
2.4 GHz NETWORKS
Network on channel 6
bondy

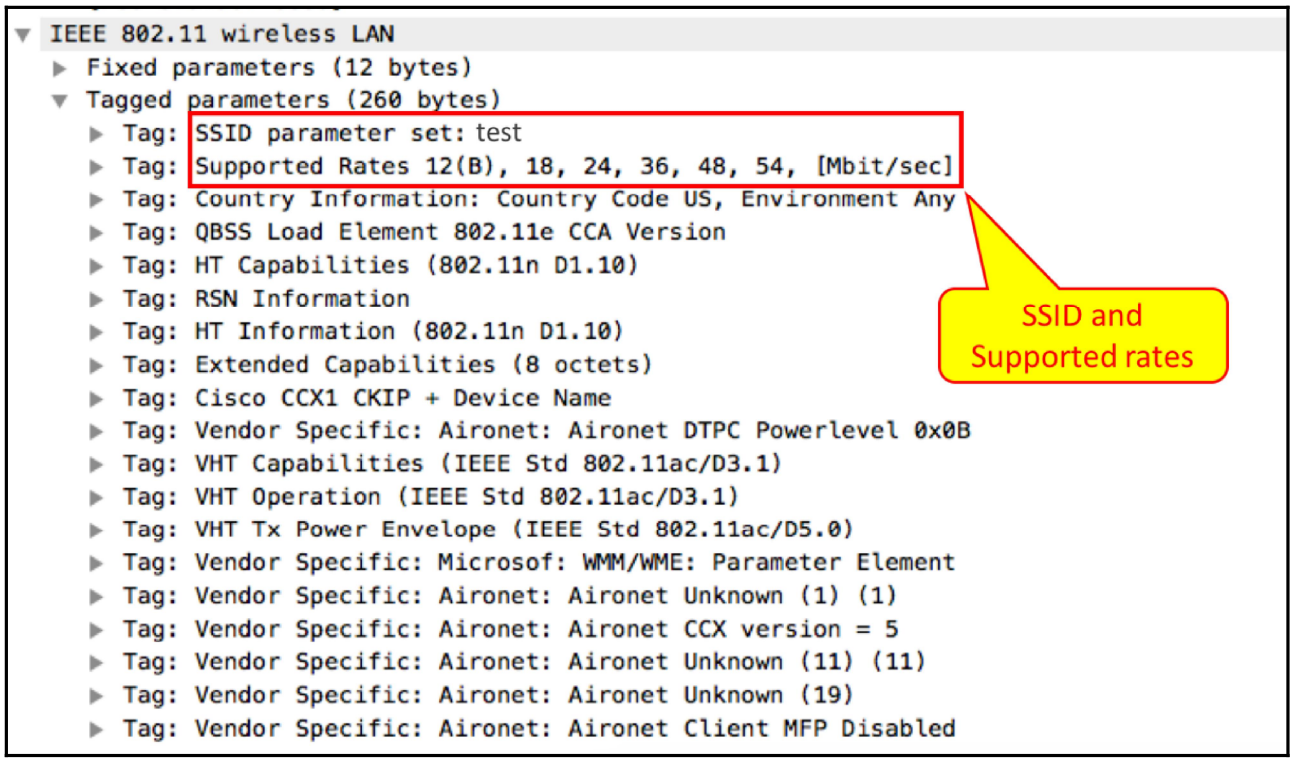

Microwave Ovens
Wireless Video Cameras
Flourescent Lights
Motion Detectors
Wireless Headphones
Wireless Game Controllers


Filter:
Expression... Clear Apply Save STP
No. Time Source Destination Protocol Info
39 3.174400 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=562, FN=0, Flags=.
40 3.276800 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=563, FN=0, Flags=.
41 3.370200 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=564, FN=0, Flags=.
42 3.478602 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=565, FN=0, Flags=.
43 3.584060 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=566, FN=0, Flags=.
44 3.666400 Cisco-Li_03:30:53 Broadcast 802.11 Beacon frame, SN=567, FN=0, Flags=.
Frame 39: 78 bytes on wire (624 bits), 78 bytes captu
IEEE 802.11 Beacon frame, Flags: ....
Type/Subtype: Beacon frame (0x08)
Frame Control: 0x0080 (Normal)
Duration: 0
Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
Source address: Cisco-Li_03:30:53 (00:14:bf:03:30:53)
BSS Id: Cisco-Li_03:30:53 (00:14:bf:03:30:53)
Fragment number: 0
Sequence number: 562
IEEE 802.11 wireless LAN management frame
Fixed parameters (12 bytes)
Tagged parameters (42 bytes)
Beacon frames transmitted by APs
BSS – the Base Station

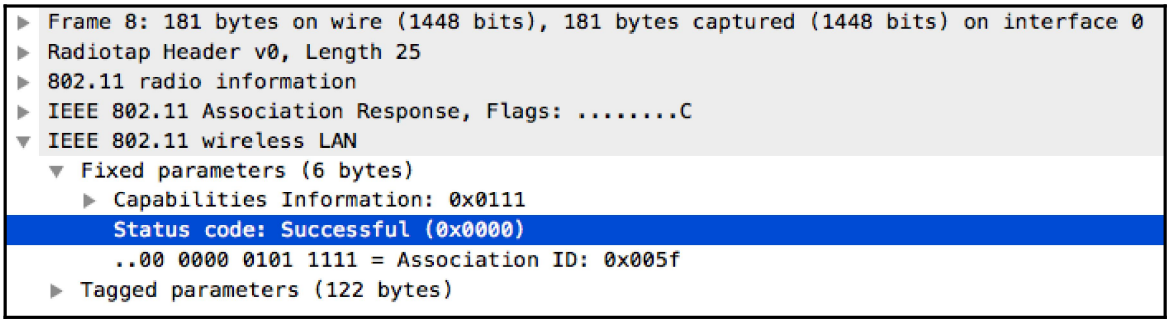

Interface
Traffic
Link-layer Header
Promiscuous
Snaplen (B)
Buffer (MB)
Monitor
Wi-Fi: en0 Ethernet default 2
p2p0 Raw IP default 2
awdl0 Ethernet
Thunderbolt Bridge: bridge0 Ethernet
utun0 BSD loopback default 2
Thunderbolt 1: en1 Ethernet default 2
Display FireWire: fw1 Apple IP-over-IEEE 1394 default 2
Thunderbolt 2: en2 Ethernet default 2
Display Ethernet: en5 Ethernet default 2
Loopback: lo0 BSD loopback default 2
Addresses: 127.0.0.1, ::1, fe80::1
gif0 BSD loopback default 2
stf0 BSD loopback default 2
Cisco remote capture: cisco Remote capture dependent DLT
Random packet generator: randpkt Generator dependent DLT
SSH remote capture: ssh Remote capture dependent DLT
UDP Listener remote capture: udpdump Exported PDUs
Loopback 0
Capture modes

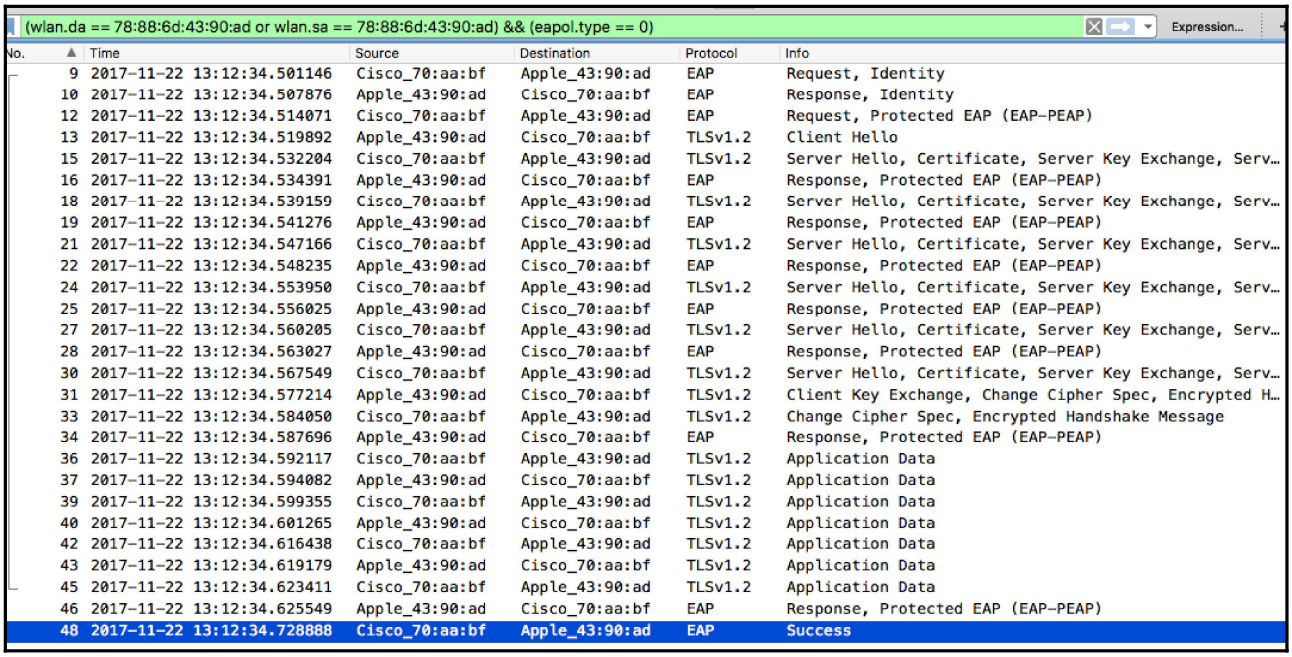

test-wireless5.pcapng
(wlan.fc == 0x4000) or (wlan.fc == 0x5008)
Expression...
No. Time Source Destination Protocol Info
1 2017-11-22 13:12:34.450638 Apple_43:90:ad Broadcast 802.11 Probe Request, SN=2674, FN=0, Fla
2 2017-11-22 13:12:34.450724 Cisco_70:aa:bf Apple_43:90:ad 802.11 Probe Response, SN=1956, FN=0, F
Probe Req & Resp
Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface 0
Radiotap Header v0, Length 25
802.11 radio information
IEEE 802.11 Probe Request, Flags: C
IEEE 802.11 wireless LAN


Frame 2: 325 bytes on wire (2600 bits), 325 bytes captured (2600 bits) on interface 0
Radiotap Header v0, Length 25
802.11 radio information
PHY type: 802.11a (5)
Turbo type: Non-turbo (0)
Data rate: 12.0 Mb/s
Channel: 108
Frequency: 5540MHz
Signal strength (dBm): -50dBm
Noise level (dBm): -95dBm
TSF timestamp: 2248193538
802.11 Radio Info
[Duration: 224µs]
AP and BSS Info
IEEE 802.11 Probe Response, Flags: ....R...C
Type/Subtype: Probe Response (0x0005)
Frame Control Field: 0x5008
.000 0000 0011 0000 = Duration: 48 microseconds
Receiver address: Apple_43:90:ad (78:88:6d:43:90:ad)
Destination address: Apple_43:90:ad (78:88:6d:43:90:ad)
Transmitter address: Cisco_70:aa:bf (84:3d:c6:70:aa:bf)
Source address: Cisco_70:aa:bf (84:3d:c6:70:aa:bf)
BSS Id: Cisco_70:aa:bf (84:3d:c6:70:aa:bf)
.... 0000 = Fragment number: 0
0111 1010 0100 .... = Sequence number: 1956
Frame check sequence: 0xb6a8c767 [correct]
[FCS Status: Good]
IEEE 802.11 wireless LAN



Source	Destination	Protocol	Info
Apple_43:90:ad	Broadcast	802.11	Probe Request, SN=2674, FN=0, Flags=........C, SSID=…
Cisco_70:aa:bf	Apple_43:90:ad	802.11	Probe Response, SN=1956, FN=0, Flags=....R...C, BI=1…
Apple_43:90:ad	Cisco_70:aa:bf	802.11	Authentication, SN=2675, FN=0, Flags=........C
	Apple_43:90:ad (78:8…	802.11	Acknowledgement, Flags=........C
Cisco_70:aa:bf	Apple_43:90:ad	802.11	Authentication, SN=2967, FN=0, Flags=........C
Apple_43:90:ad	Cisco_70:aa:bf	802.11	Association Request, SN=2676, FN=0, Flags=....R...C,…
	Apple_43:90:ad (78:8…	802.11	Acknowledgement, Flags=........C
Cisco_70:aa:bf	Apple_43:90:ad	802.11	Association Response, SN=2968, FN=0, Flags=........C

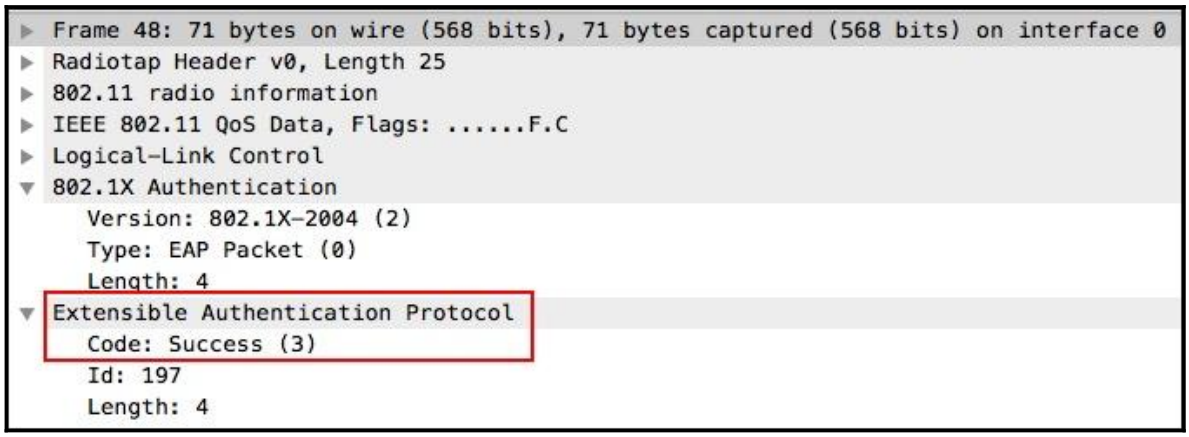




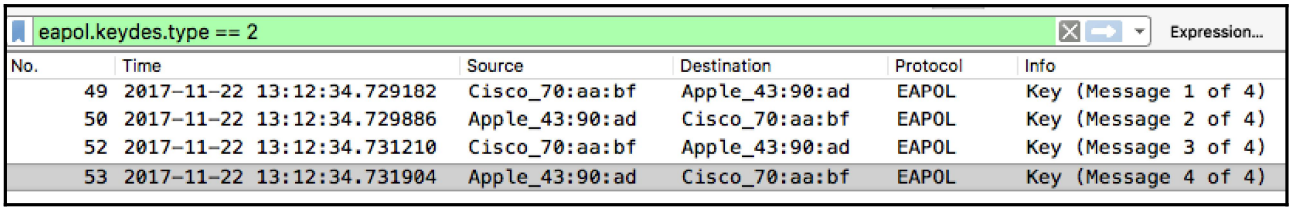
(wlan.da == 78:88:6d:43:90:ad or wlan.sa == 78:88:6d:43:90:ad) && (eapol.type == 0)

Expression...

No.	Time	Source	Destination	Protocol	Info
9	2017-11-22 13:12:34.501146	Cisco_70:aa:bf	Apple_43:90:ad	EAP	Request, Identity
10	2017-11-22 13:12:34.507876	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Identity
12	2017-11-22 13:12:34.514071	Cisco_70:aa:bf	Apple_43:90:ad	EAP	Request, Protected EAP (EAP-PEAP)
13	2017-11-22 13:12:34.519892	Apple_43:90:ad	Cisco_70:aa:bf	TLSv1.2	Client Hello
15	2017-11-22 13:12:34.532204	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
16	2017-11-22 13:12:34.534391	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
18	2017-11-22 13:12:34.539159	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
19	2017-11-22 13:12:34.541276	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
21	2017-11-22 13:12:34.547166	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
22	2017-11-22 13:12:34.548235	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
24	2017-11-22 13:12:34.553950	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
25	2017-11-22 13:12:34.556025	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
27	2017-11-22 13:12:34.560205	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
28	2017-11-22 13:12:34.563027	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
30	2017-11-22 13:12:34.567549	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Server Hello, Certificate, Server Key Exchange, Serv…
31	2017-11-22 13:12:34.577214	Apple_43:90:ad	Cisco_70:aa:bf	TLSv1.2	Client Key Exchange, Change Cipher Spec, Encrypted H…
33	2017-11-22 13:12:34.584050	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Change Cipher Spec, Encrypted Handshake Message
34	2017-11-22 13:12:34.587696	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
36	2017-11-22 13:12:34.592117	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Application Data
37	2017-11-22 13:12:34.594082	Apple_43:90:ad	Cisco_70:aa:bf	TLSv1.2	Application Data
39	2017-11-22 13:12:34.599355	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Application Data
40	2017-11-22 13:12:34.601265	Apple_43:90:ad	Cisco_70:aa:bf	TLSv1.2	Application Data
42	2017-11-22 13:12:34.616438	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Application Data
43	2017-11-22 13:12:34.619179	Apple_43:90:ad	Cisco_70:aa:bf	TLSv1.2	Application Data
45	2017-11-22 13:12:34.623411	Cisco_70:aa:bf	Apple_43:90:ad	TLSv1.2	Application Data
46	2017-11-22 13:12:34.625549	Apple_43:90:ad	Cisco_70:aa:bf	EAP	Response, Protected EAP (EAP-PEAP)
48	2017-11-22 13:12:34.728888	Cisco_70:aa:bf	Apple_43:90:ad	EAP	Success



```
▶ Frame 48: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
▶ Radiotap Header v0, Length 25
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: ......F.C
▶ Logical-Link Control
▼ 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: EAP Packet (0)
    Length: 4
▼ Extensible Authentication Protocol
    Code: Success (3)
    Id: 197
    Length: 4
```

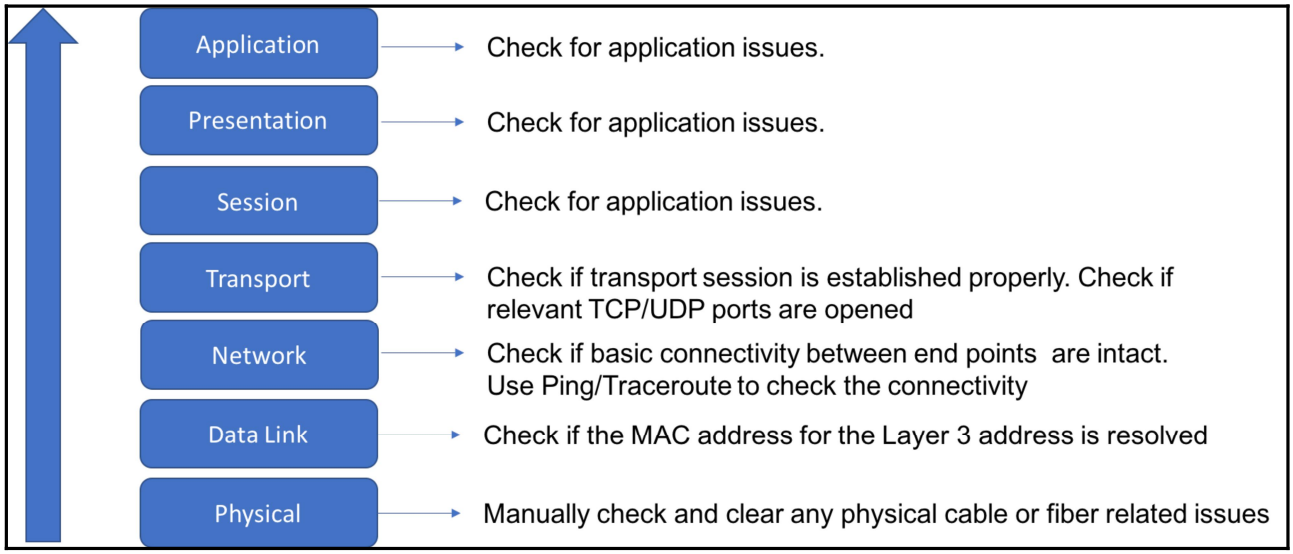


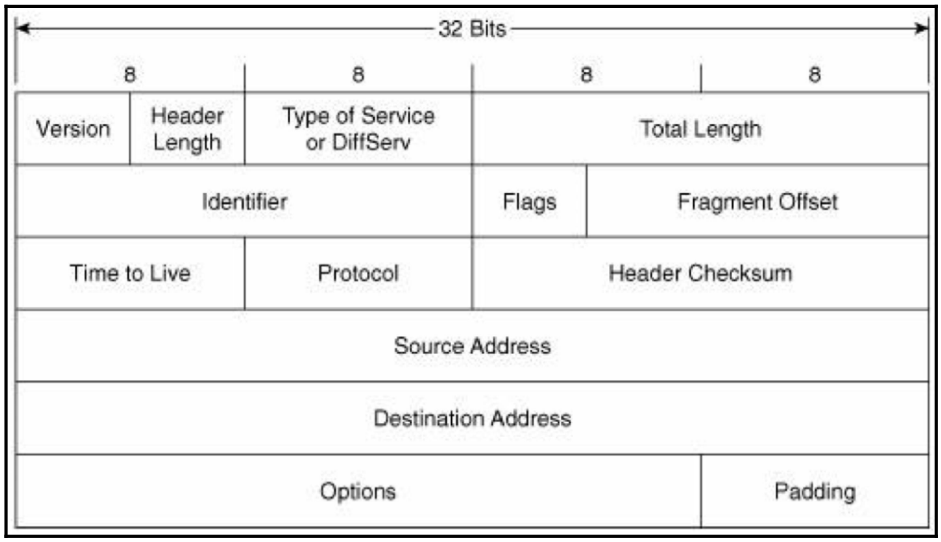
eapol.keydes.type == 2

Expression...

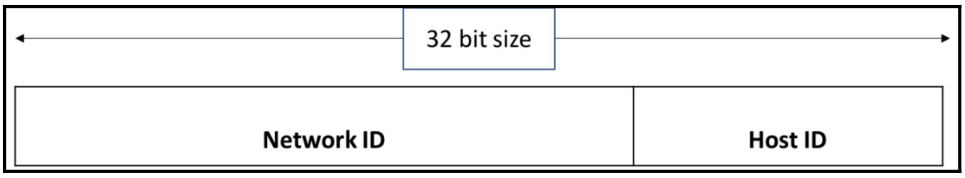
No.	Time	Source	Destination	Protocol	Info
49	2017-11-22 13:12:34.729182	Cisco_70:aa:bf	Apple_43:90:ad	EAPOL	Key (Message 1 of 4)
50	2017-11-22 13:12:34.729886	Apple_43:90:ad	Cisco_70:aa:bf	EAPOL	Key (Message 2 of 4)
52	2017-11-22 13:12:34.731210	Cisco_70:aa:bf	Apple_43:90:ad	EAPOL	Key (Message 3 of 4)
53	2017-11-22 13:12:34.731904	Apple_43:90:ad	Cisco_70:aa:bf	EAPOL	Key (Message 4 of 4)

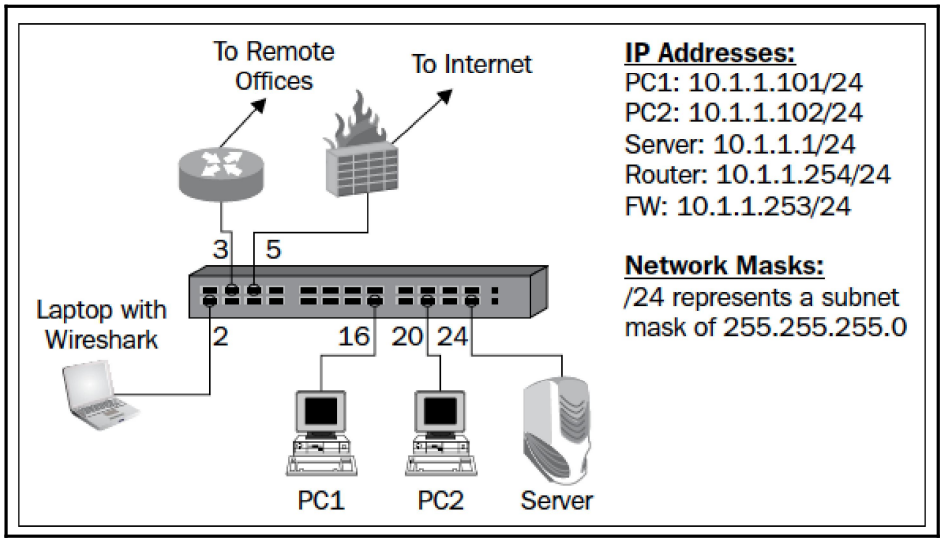
Chapter 10: Network Layer Protocols and Operations

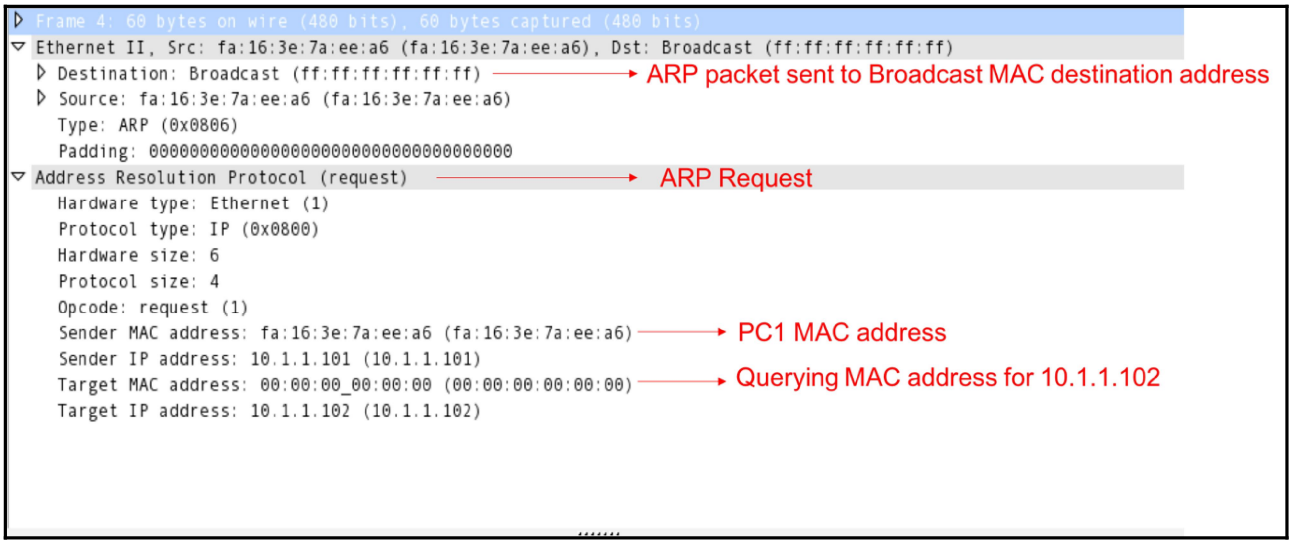


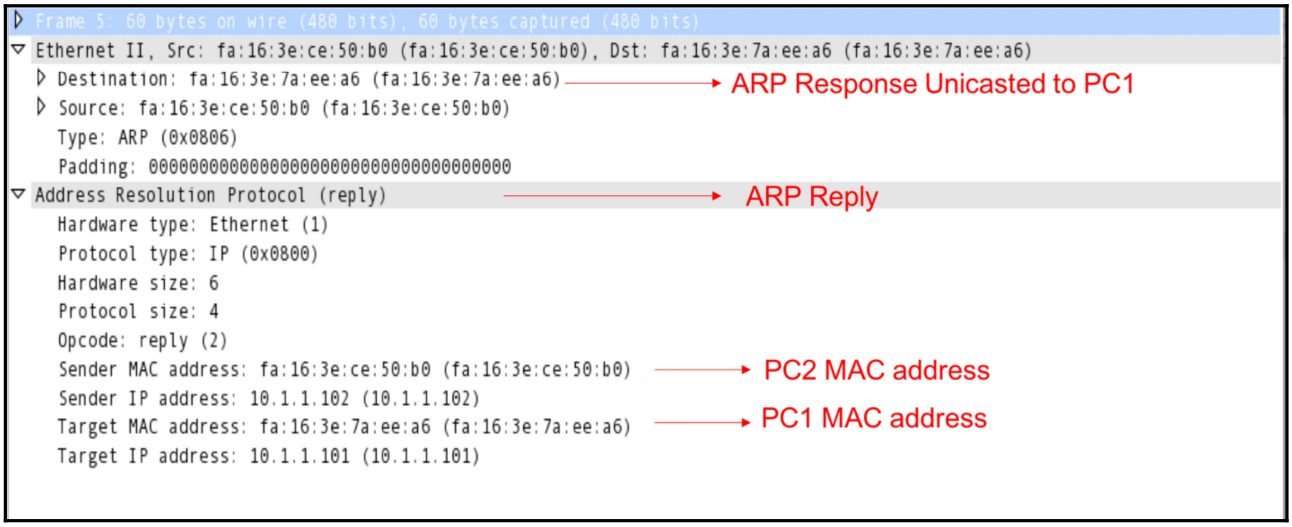


```
Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 10.0.0.101 (10.0.0.101)
    Version: 4
    Header Length: 20 bytes
  ▽ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
    Total Length: 100
    Identification: 0x002e (46)
  ▽ Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ▽ Header checksum: 0xa705 [validation disabled]
      [Good: False]
      [Bad: False]
    Source: 10.0.0.1 (10.0.0.1)
    Destination: 10.0.0.101 (10.0.0.101)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

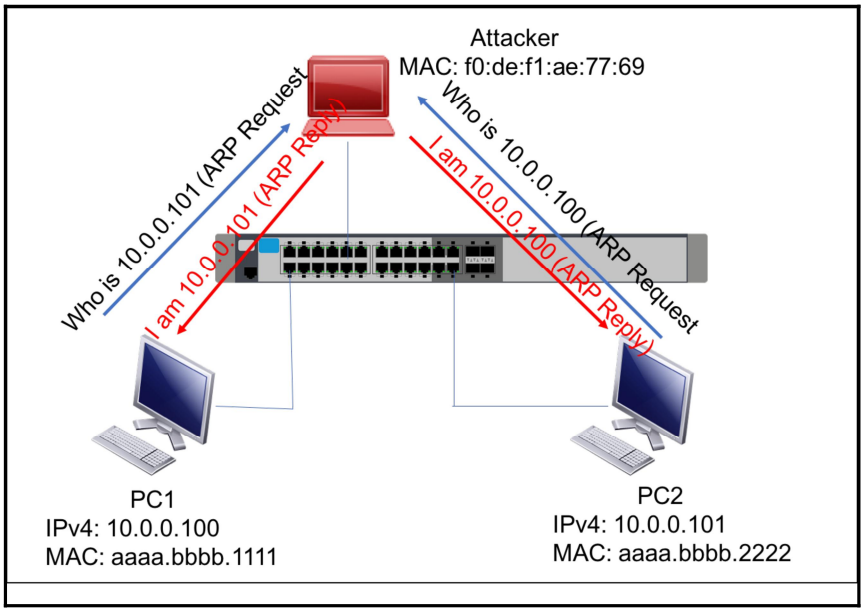


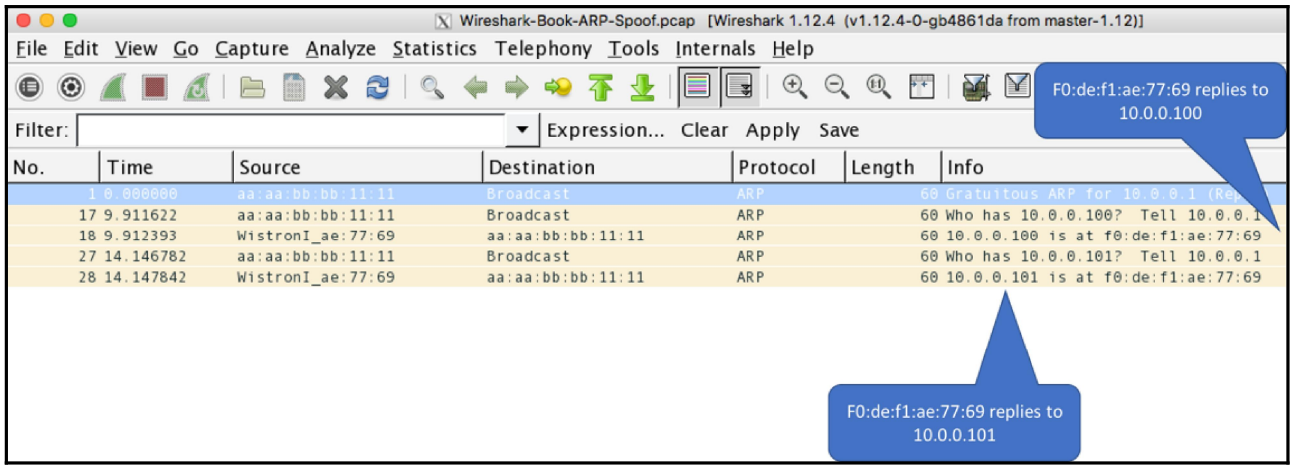






Filter	Description	Example
arp	Filters all ARP packets	arp
arp.opcode == <opcode>	ARP Operation code based filter. Opcode of 1 will filter all ARP Request packets and Opcode 2 will filter all ARP Reply packets	arp.opcode == 1 arp.opcode == 2
arp.src.hw_mac == <mac>	Filter the ARP packet that MAC address defined in ***Sender MAC address*** field	arp.src.hw_mac == fa:16:3e:ce:50:b0
arp.dst.hw_mac == <mac>	Filter the ARP packet that MAC address defined in ***Target MAC address*** field	arp.dst.hw_mac == fa:16:3e:ce:50:b0
arp.isgratuitous == <>	Filter all Gratuitous ARP packets	arp.isgratuitous == true


Attacker
MAC: f0:de:f1:ae:77:69
Who is 10.0.0.101 (ARP Request
I am 10.0.0.101 (ARP Reply)
Who is 10.0.0.100 (ARP Request
I am 10.0.0.100 (ARP Reply)
PC1
IPv4: 10.0.0.100
MAC: aaaa.bbbb.1111
PC2
IPv4: 10.0.0.101
MAC: aaaa.bbbb.2222


Wireshark-Book-ARP-Spoof.pcap [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 aa:aa:bb:bb:11:11 Broadcast ARP 60 Gratuitous ARP for 10.0.0.1 (Re
17 9.911622 aa:aa:bb:bb:11:11 Broadcast ARP 60 Who has 10.0.0.100? Tell 10.0.0.1
18 9.912393 WistronI_ae:77:69 aa:aa:bb:bb:11:11 ARP 60 10.0.0.100 is at f0:de:f1:ae:77:69
27 14.146782 aa:aa:bb:bb:11:11 Broadcast ARP 60 Who has 10.0.0.101? Tell 10.0.0.1
28 14.147842 WistronI_ae:77:69 aa:aa:bb:bb:11:11 ARP 60 10.0.0.101 is at f0:de:f1:ae:77:69
F0:de:f1:ae:77:69 replies to 10.0.0.100
F0:de:f1:ae:77:69 replies to 10.0.0.101

```
▷ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
▽ Ethernet II, Src: aa:aa:bb:bb:11:11 (aa:aa:bb:bb:11:11), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▷ Source: aa:aa:bb:bb:11:11 (aa:aa:bb:bb:11:11)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
▽ Address Resolution Protocol (reply/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    [Is gratuitous: True]
    Sender MAC address: aa:aa:bb:bb:11:11 (aa:aa:bb:bb:11:11)
    Sender IP address: 10.0.0.1 (10.0.0.1)
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 10.0.0.1 (10.0.0.1)
```

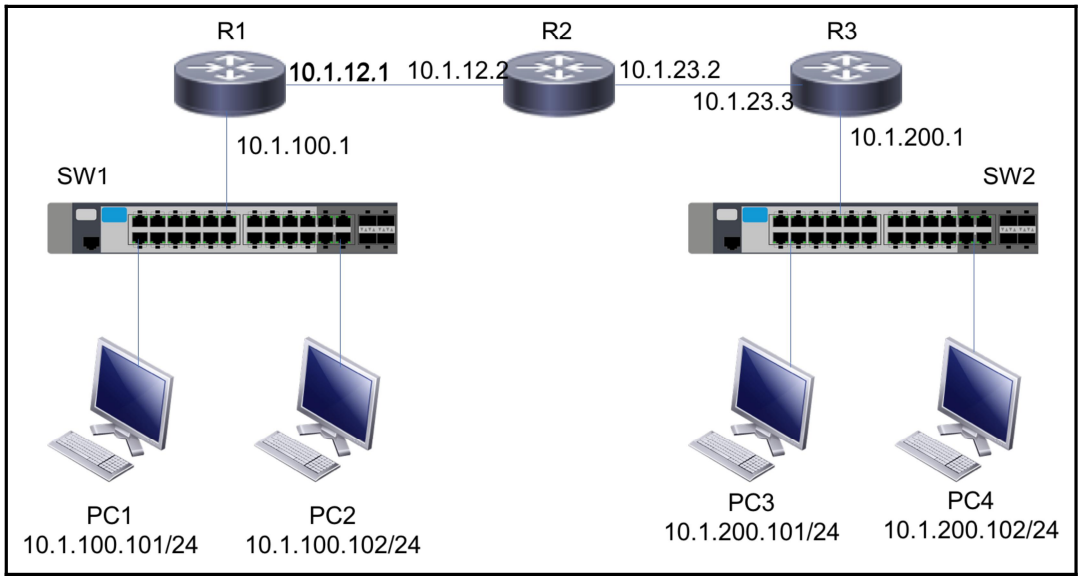
```
Filter: arp.isgratuitous   Expression... Clear Apply Save
No.  Time  Source  Destination  Protocol  Length  Info
```

Display filter: none

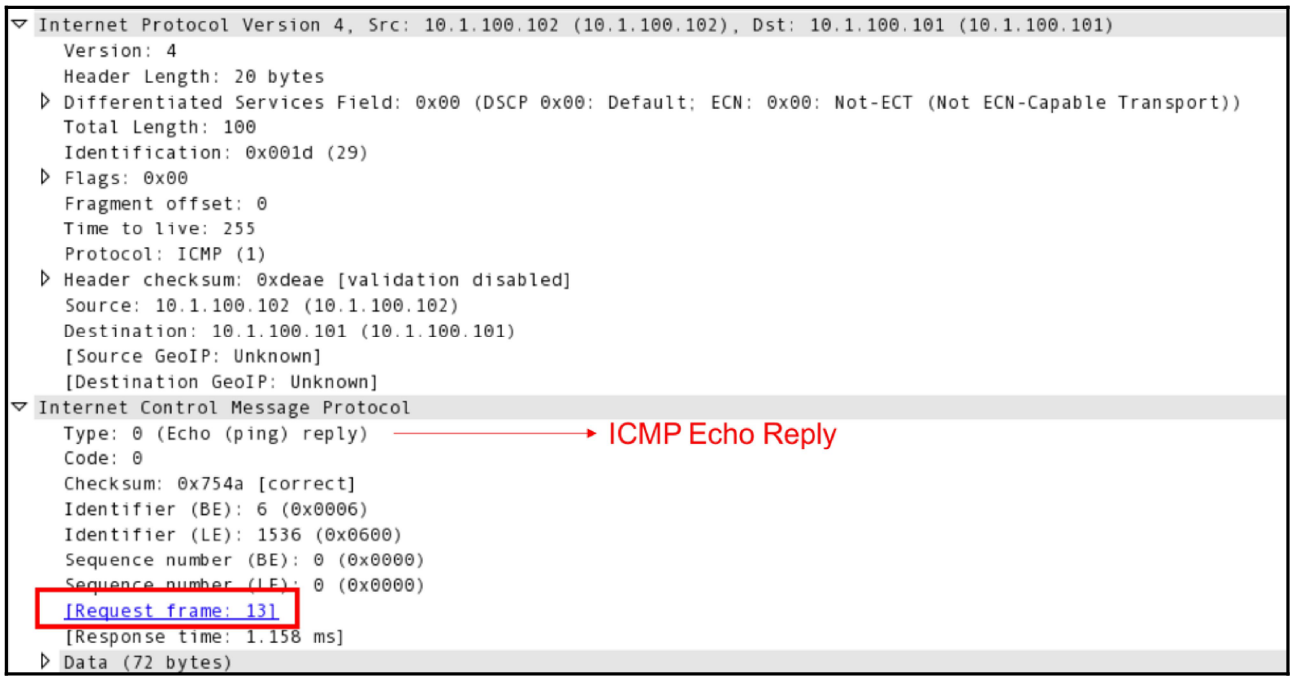
Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes
▽ Frame	100.00 %	37	100.00 %	3604	0.002	0	0
▽ Ethernet	100.00 %	37	100.00 %	3604	0.002	0	0
Address Resolution Protocol	13.51 %	5	8.32 %	300	0.000	5	300
▽ Internet Protocol Version 6	43.24 %	16	41.07 %	1480	0.001	0	0
Internet Control Message Protocol v6	43.24 %	16	41.07 %	1480	0.001	16	1480
▽ Internet Protocol Version 4	43.24 %	16	50.61 %	1824	0.001	0	0
Internet Control Message Protocol	43.24 %	16	50.61 %	1824	0.001	16	1824

Hardware Type		Protocol Type
Hardware Length	Protocol Length	OpCode (1 = Request, 2 = Reply)
Sender Hardware Address (0-3 Octets)		
Sender Hardware Address (4-5 Octets)		Sender Protocol Address (0 – 1 Octets)
Sender Protocol Address (2 – 3 Octets)		Target Hardware Address (0-1 Octets)
Target Hardware Address (2-5 Octets)		
Target Protocol Address		

Type	Code	Checksum
ICMP Message Dependant Variable		




```
▽ Internet Protocol Version 4, Src: 10.1.100.101 (10.1.100.101), Dst: 10.1.100.102 (10.1.100.102)
    Version: 4
    Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 100
    Identification: 0x001d (29)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)                    ──────► Protocol is ICMP
  ▷ Header checksum: 0xdeae [validation disabled]
    Source: 10.1.100.101 (10.1.100.101)
    Destination: 10.1.100.102 (10.1.100.102)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)        ──────► ICMP Echo Message
    Code: 0
    Checksum: 0x6d4a [correct]
    Identifier (BE): 6 (0x0006)
    Identifier (LE): 1536 (0x0600)
    Sequence number (BE): 0 (0x0000)
    Sequence number (LE): 0 (0x0000)
    [Response frame: 141]
  ▷ Data (72 bytes)
```

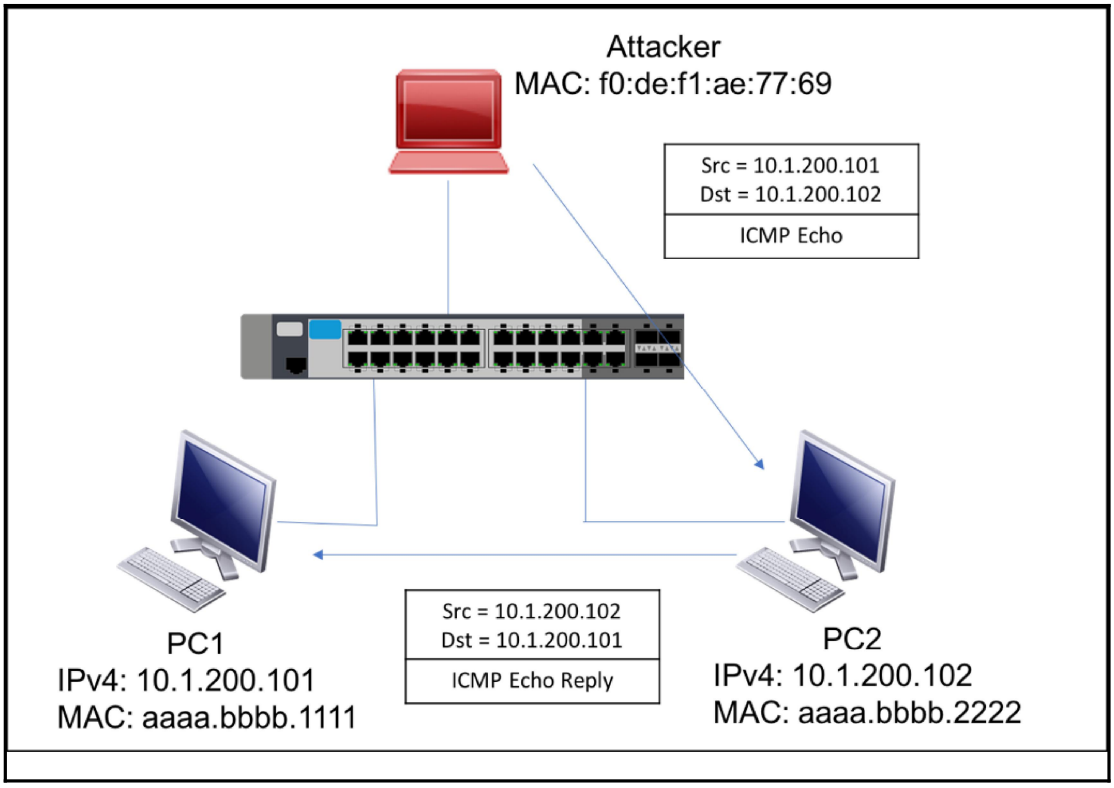


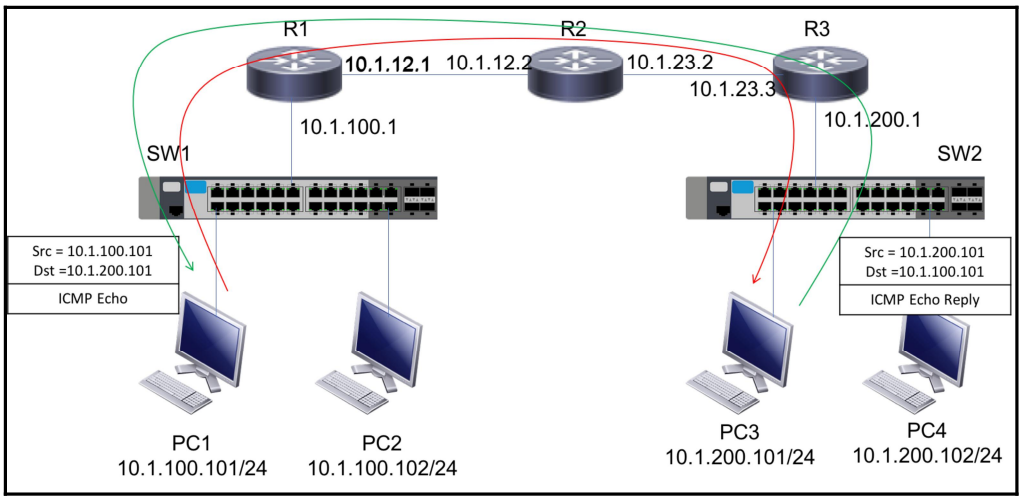
Filter	Description	Example
icmp	Filters all ICMP packets	icmp
icmp.type == <type>	ICMP type based filter. Type 8will filter all ICMP Echo messages and Type 0 will filter all ICMP Echo replies	icmp.type == 0 icmp.type == 8
icmp.code == <code>	ICMP Code based filter.	icmp.code == 0

60k ICMP received in few seconds

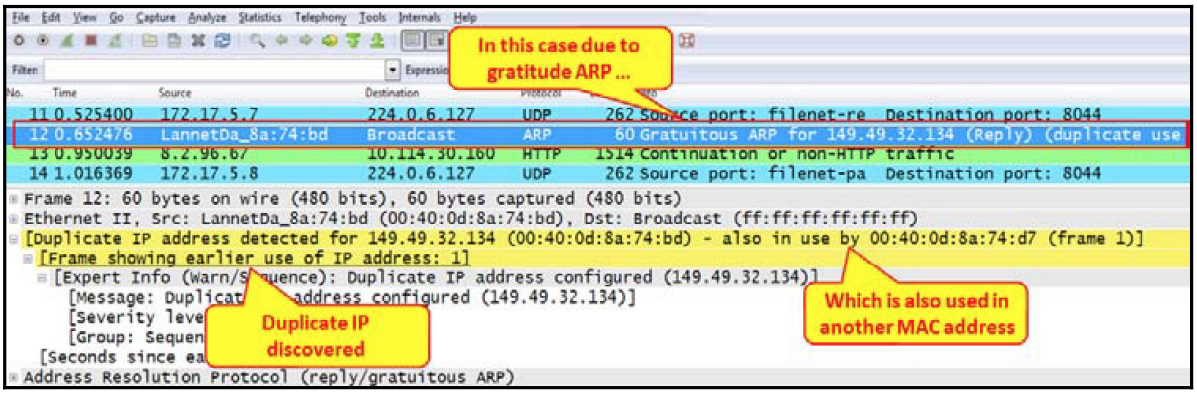
Display filter: none

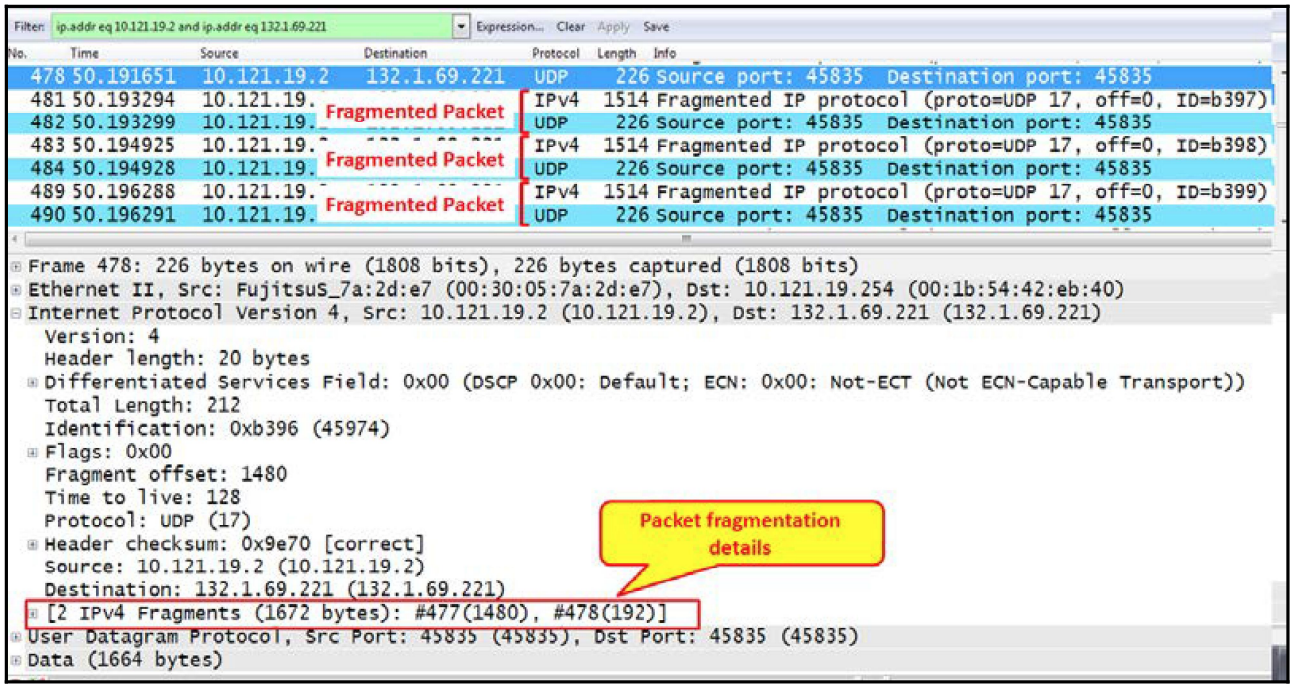
Protocol	% Packets	Packets	% Bytes	By	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	66132	100.00 %	54300	0.794	0	0	0.000
Ethernet	99.99 %	66127	99.99 %	7533850	0.794	0	0	0.000
Internet Protocol Version 4	99.85 %	66035	99.[illegible] %	7527606	0.793	0	0	0.000
Open Shortest Path First	0.02 %	16	0.02 %	1440	0.000	16	1440	0.000
Internet Control Message Protocol	99.83 %	66019	99.89 %	7526166	0.793	66019	7526166	0.793
Logical-Link Control	0.06 %	41	0.04 %	3116	0.000	0	0	0.000
Spanning Tree Protocol	0.06 %	37	0.03 %	2220	0.000	37	2220	0.000
Dynamic Trunk Protocol	0.00 %	2	0.00 %	120	0.000	2	120	0.000
Cisco Discovery Protocol	0.00 %	2	0.01 %	776	0.000	2	776	0.000
Data	0.01 %	4	0.00 %	308	0.000	4	308	0.000
Address Resolution Protocol	0.07 %	47	0.04 %	2820	0.000	47	2820	0.000
Cisco ISL	0.01 %	5	0.01 %	450	0.000	0	0	0.000
Ethernet	0.01 %	5	0.01 %	450	0.000	0	0	0.000
Logical-Link Control	0.01 %	5	0.01 %	450	0.000	0	0	0.000
Dynamic Trunk Protocol	0.01 %	5	0.01 %	450	0.000	5	450	0.000

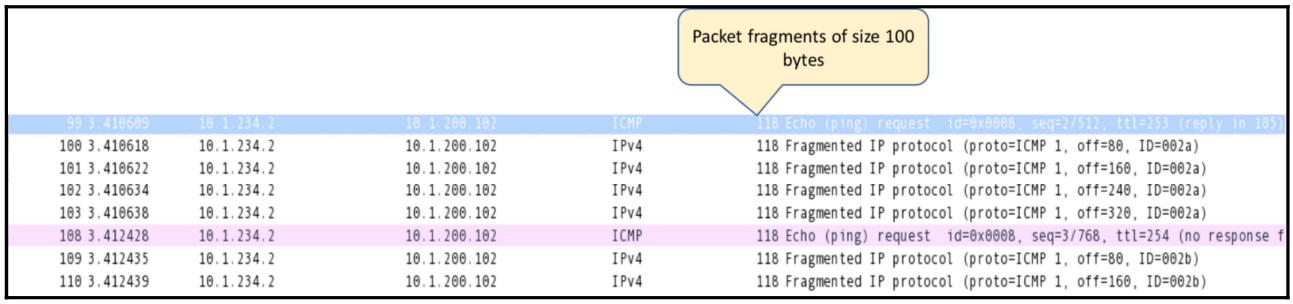


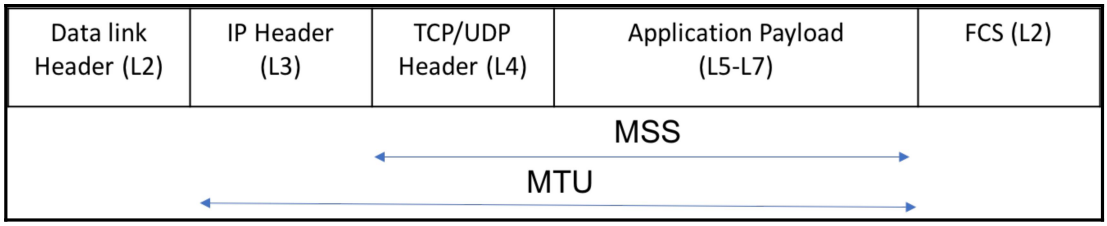


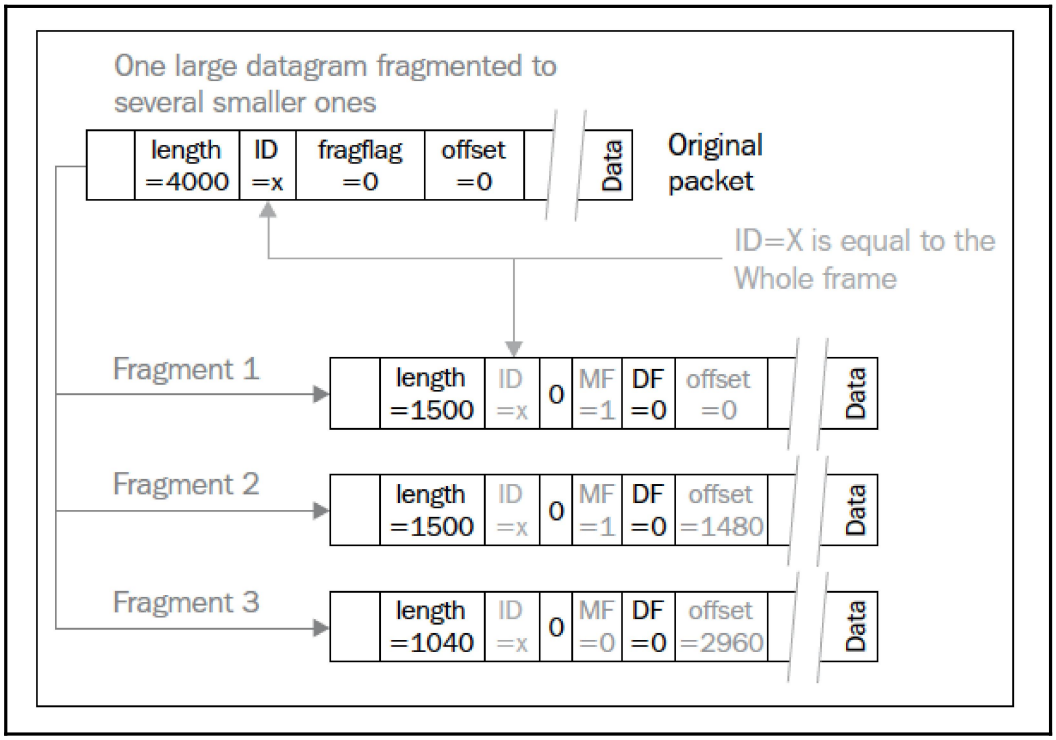
1145 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1145
1146 Note	Sequence	IPv4	"Time To Live" only 4
1146 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1146
1147 Note	Sequence	IPv4	"Time To Live" only 3
1147 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1147
1148 Note	Sequence	IPv4	"Time To Live" only 2
1148 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1148
1149 Note	Sequence	IPv4	"Time To Live" only 1
1149 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1149
1150 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1150
1151 Warn	Sequence	ICMP	No response seen to ICMP request in frame 1151

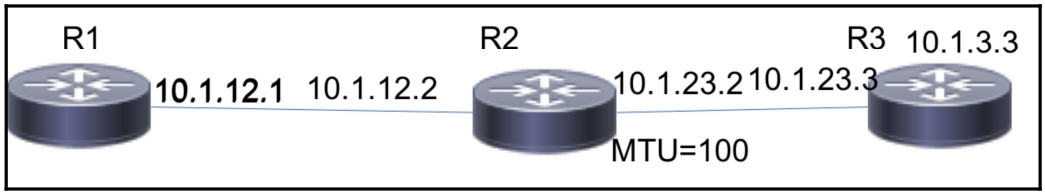


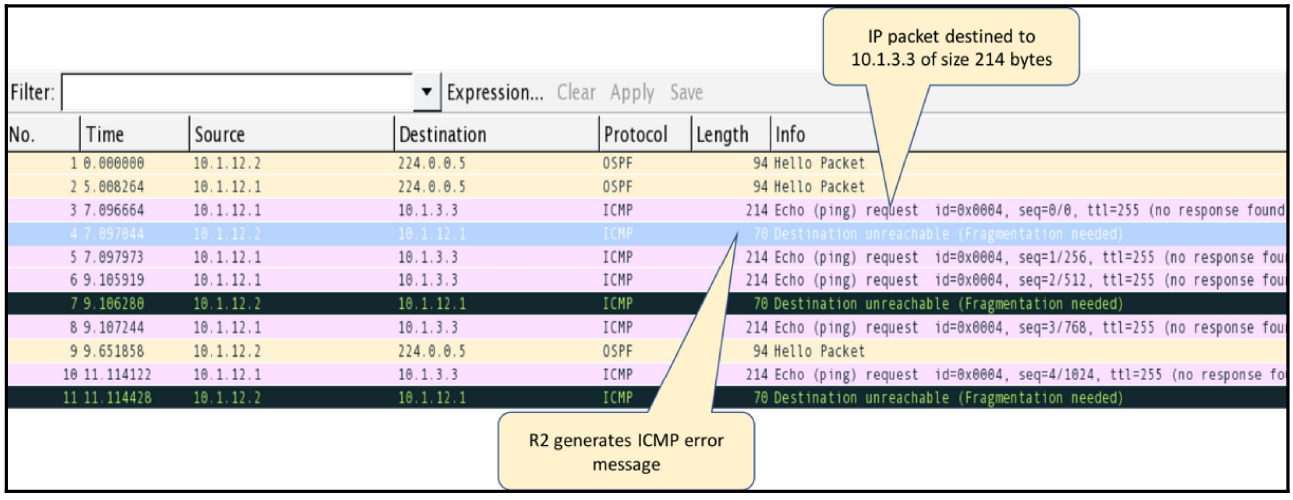

Filter: ip.addr eq 10.121.19.2 and ip.addr eq 132.1.69.221
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
478 50.191651 10.121.19.2 132.1.69.221 UDP 226 Source port: 45835 Destination port: 45835
481 50.193294 10.121.19. IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=b397)
482 50.193299 10.121.19. UDP 226 Source port: 45835 Destination port: 45835
483 50.194925 10.121.19. IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=b398)
484 50.194928 10.121.19. UDP 226 Source port: 45835 Destination port: 45835
489 50.196288 10.121.19. IPv4 1514 Fragmented IP protocol (proto=UDP 17, off=0, ID=b399)
490 50.196291 10.121.19. UDP 226 Source port: 45835 Destination port: 45835
Fragmented Packet
Fragmented Packet
Fragmented Packet
Frame 478: 226 bytes on wire (1808 bits), 226 bytes captured (1808 bits)
Ethernet II, Src: FujitsuS_7a:2d:e7 (00:30:05:7a:2d:e7), Dst: 10.121.19.254 (00:1b:54:42:eb:40)
Internet Protocol Version 4, Src: 10.121.19.2 (10.121.19.2), Dst: 132.1.69.221 (132.1.69.221)
Version: 4
Header length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 212
Identification: 0xb396 (45974)
Flags: 0x00
Fragment offset: 1480
Time to live: 128
Protocol: UDP (17)
Header checksum: 0x9e70 [correct]
Source: 10.121.19.2 (10.121.19.2)
Destination: 132.1.69.221 (132.1.69.221)
[2 IPv4 Fragments (1672 bytes): #477(1480), #478(192)]
User Datagram Protocol, Src Port: 45835 (45835), Dst Port: 45835 (45835)
Data (1664 bytes)
Packet fragmentation details


Packet fragments of size 100 bytes
99 3.410609 10.1.234.2 10.1.200.102 ICMP 118 Echo (ping) request id=0x0008, seq=2/512, ttl=253 (reply in 105)
100 3.410618 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=80, ID=002a)
101 3.410622 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=160, ID=002a)
102 3.410634 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=240, ID=002a)
103 3.410638 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=320, ID=002a)
108 3.412428 10.1.234.2 10.1.200.102 ICMP 118 Echo (ping) request id=0x0008, seq=3/768, ttl=254 (no response f
109 3.412435 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=80, ID=002b)
110 3.412439 10.1.234.2 10.1.200.102 IPv4 118 Fragmented IP protocol (proto=ICMP 1, off=160, ID=002b)


Data link Header (L2)
IP Header (L3)
TCP/UDP Header (L4)
Application Payload (L5-L7)
FCS (L2)
MSS
MTU


One large datagram fragmented to several smaller ones
length =4000
ID =x
fragflag =0
offset =0
Data
Original packet
ID=X is equal to the Whole frame
Fragment 1
length =1500
ID =x
0
MF =1
DF =0
offset =0
Data
Fragment 2
length =1500
ID =x
0
MF =1
DF =0
offset =1480
Data
Fragment 3
length =1040
ID =x
0
MF =0
DF =0
offset =2960
Data

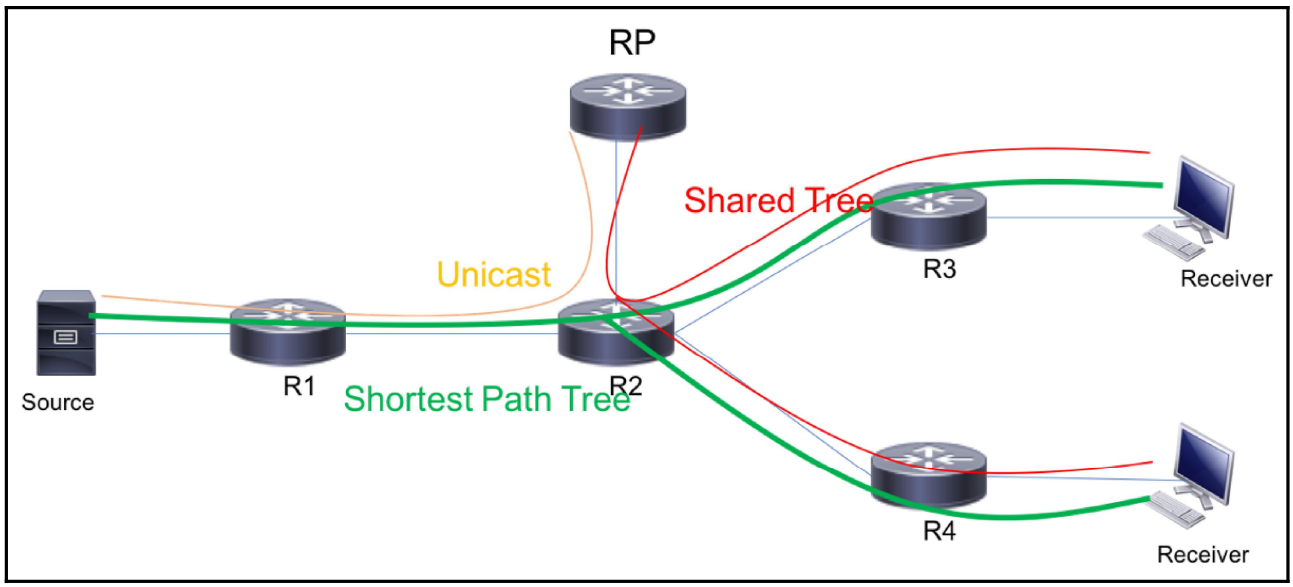

R1
10.1.12.1
10.1.12.2
R2
10.1.23.2
10.1.23.3
R3
10.1.3.3
MTU=100

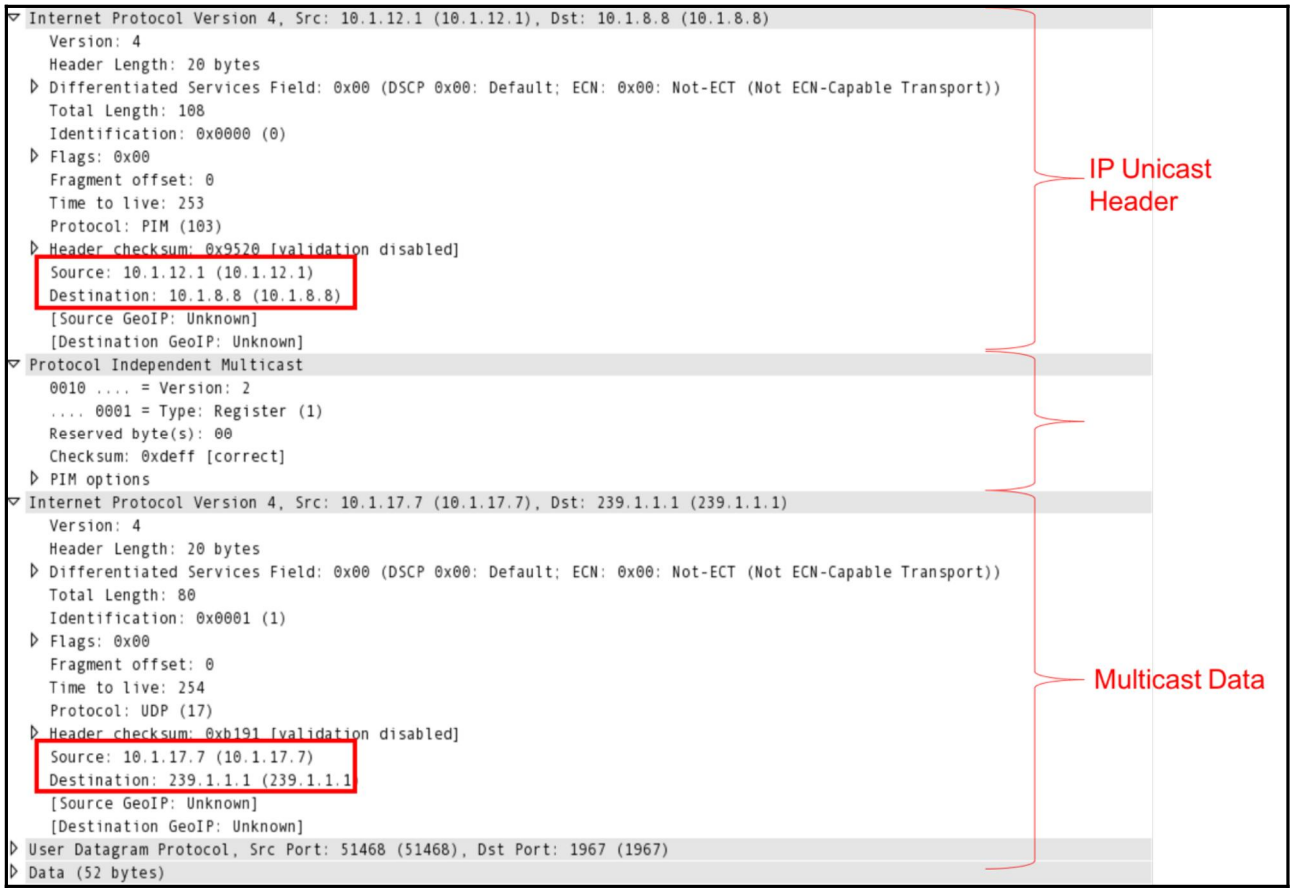

IP packet destined to 10.1.3.3 of size 214 bytes
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 10.1.12.2 224.0.0.5 OSPF 94 Hello Packet
2 5.008264 10.1.12.1 224.0.0.5 OSPF 94 Hello Packet
3 7.096664 10.1.12.1 10.1.3.3 ICMP 214 Echo (ping) request id=0x0004, seq=0/0, ttl=255 (no response found
4 7.097044 10.1.12.2 10.1.12.1 ICMP 70 Destination unreachable (Fragmentation needed)
5 7.097973 10.1.12.1 10.1.3.3 ICMP 214 Echo (ping) request id=0x0004, seq=1/256, ttl=255 (no response fou
6 9.105919 10.1.12.1 10.1.3.3 ICMP 214 Echo (ping) request id=0x0004, seq=2/512, ttl=255 (no response fou
7 9.106280 10.1.12.2 10.1.12.1 ICMP 70 Destination unreachable (Fragmentation needed)
8 9.107244 10.1.12.1 10.1.3.3 ICMP 214 Echo (ping) request id=0x0004, seq=3/768, ttl=255 (no response fou
9 9.651858 10.1.12.2 224.0.0.5 OSPF 94 Hello Packet
10 11.114122 10.1.12.1 10.1.3.3 ICMP 214 Echo (ping) request id=0x0004, seq=4/1024, ttl=255 (no response fo
11 11.114428 10.1.12.2 10.1.12.1 ICMP 70 Destination unreachable (Fragmentation needed)
R2 generates ICMP error message

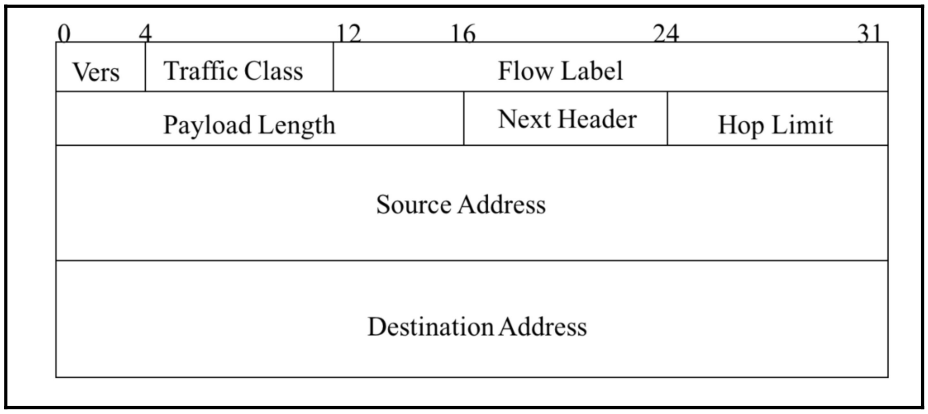
```
▽ Internet Protocol Version 4, Src: 10.1.12.2 (10.1.12.2), Dst: 10.1.12.1 (10.1.12.1)
    Version: 4
    Header Length: 20 bytes
  ▷ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 56
    Identification: 0x0000 (0)
  ▷ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: ICMP (1)
  ▷ Header checksum: 0x8fc0 [validation disabled]
    Source: 10.1.12.2 (10.1.12.2)
    Destination: 10.1.12.1 (10.1.12.1)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▽ Internet Control Message Protocol
    Type: 3 (Destination unreachable)
    Code: 4 (Fragmentation needed)
    Checksum: 0x63b4 [correct]
    MTU of next hop: 100
  ▷ Internet Protocol Version 4, Src: 10.1.12.1 (10.1.12.1), Dst: 10.1.3.3 (10.1.3.3)
  ▷ Internet Control Message Protocol
```

Destination unreachable error message generated with outgoing interface MTU as 100

Filter	Description	Example
ip.flags.mf == <flag>	Filters all fragmented packets with MF flag set to 1	ip.flags.mf == 1
ip.fragment	Filter all fragmented packets	ip.fragment
ip.flags.df == <flag>	Filters all packets with DF flag set	ip.flags.df == 1




Internet Protocol Version 4, Src: 10.1.12.1 (10.1.12.1), Dst: 10.1.8.8 (10.1.8.8)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 108
Identification: 0x0000 (0)
Flags: 0x00
Fragment offset: 0
Time to live: 253
Protocol: PIM (103)
Header checksum: 0x9520 [validation disabled]
Source: 10.1.12.1 (10.1.12.1)
Destination: 10.1.8.8 (10.1.8.8)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Protocol Independent Multicast
0010 .... = Version: 2
.... 0001 = Type: Register (1)
Reserved byte(s): 00
Checksum: 0xdeff [correct]
PIM options
Internet Protocol Version 4, Src: 10.1.17.7 (10.1.17.7), Dst: 239.1.1.1 (239.1.1.1)
Version: 4
Header Length: 20 bytes
Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
Total Length: 80
Identification: 0x0001 (1)
Flags: 0x00
Fragment offset: 0
Time to live: 254
Protocol: UDP (17)
Header checksum: 0xb191 [validation disabled]
Source: 10.1.17.7 (10.1.17.7)
Destination: 239.1.1.1 (239.1.1.1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 51468 (51468), Dst Port: 1967 (1967)
Data (52 bytes)
IP Unicast Header
Multicast Data


0
4
12
16
24
31
Vers
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source Address
Destination Address

```
Internet Protocol Version 6, Src: 2001:db8:12::1 (2001:db8:12::1), Dst: 2001:db8:12::2 (2001:db8:12::2)
  0110 .... = Version: 6
      [0110 .... = This field makes the filter "ip.version == 6" possible: 6]
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
      .... 0000 00.. .... .... .... .... .... = Differentiated Services Field: Default (0x00000000)
      .... .... ..0. .... .... .... .... .... = ECN-Capable Transport (ECT): Not set
      .... .... ...0 .... .... .... .... .... = ECN-CE: Not set
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 60
    Next header: ICMPv6 (58)
    Hop limit: 64
    Source: 2001:db8:12::1 (2001:db8:12::1)
    Destination: 2001:db8:12::2 (2001:db8:12::2)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

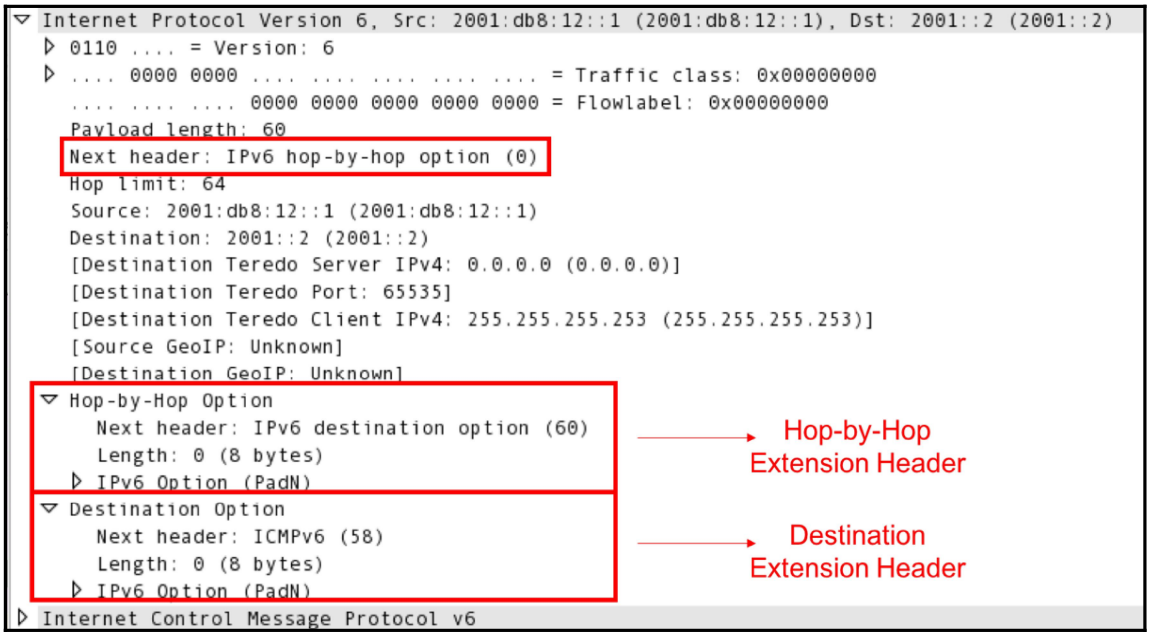
Network Prefix				Interface ID			
←16→	←16→	←16→	←16→	←16→	←16→	←16→	←16→

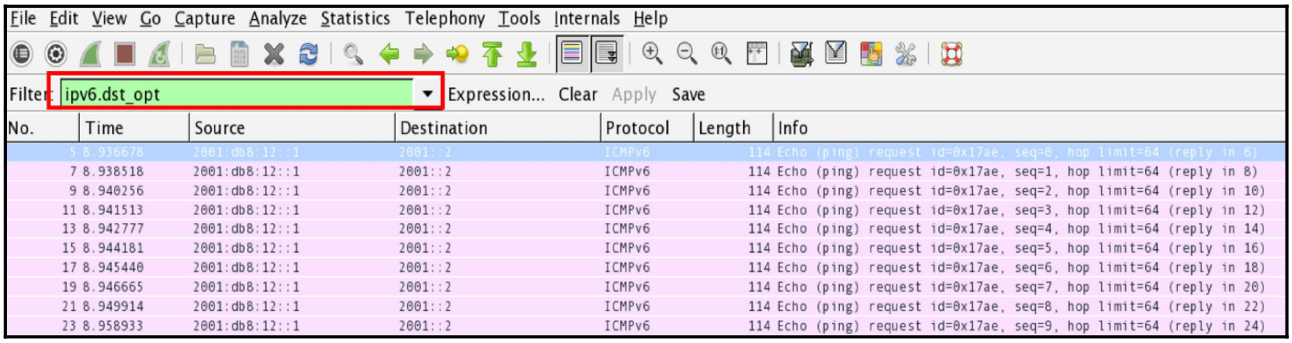
Address	Scope	Meaning
FF01::1	Node-Local	All Nodes
FF01::2	Node-Local	All Routers
FF02::1	Link-Local	All Nodes
FF02::2	Link-Local	All Routers
FF02::5	Link-Local	OSPFv3 Routers
FF02::6	Link-Local	OSPFv3 DR Routers
FF02::1:FFXX:XXXX	Link-Local	Solicited-Node

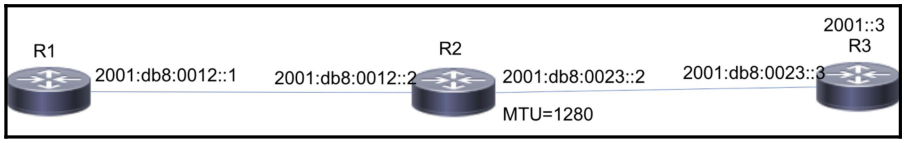
IPv6 Header Next Header = TCP	TCP Header + Data

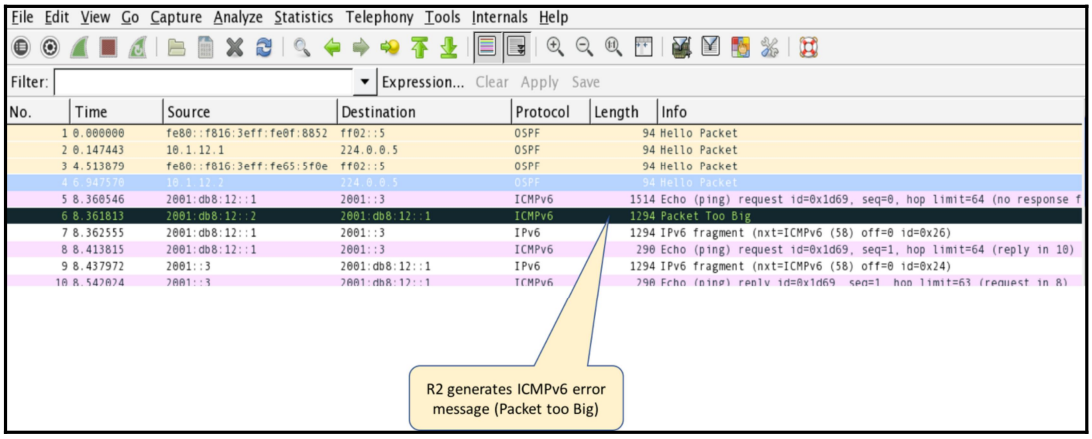
IPv6 Header Next Header = Fragment	Fragment Header Next Header = TCP	TCP Header + Data

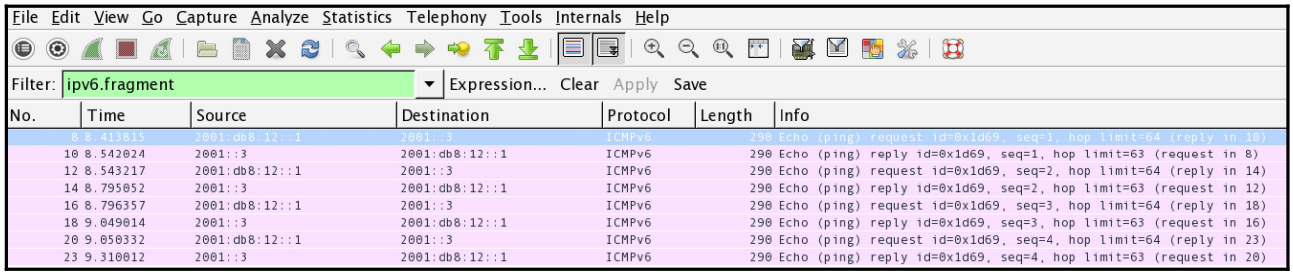
IPv6 Header Next Header = Hop-by-Hop	HbH Header Next Header = Fragment	Fragment Header Next Header = TCP	TCP Header + Data

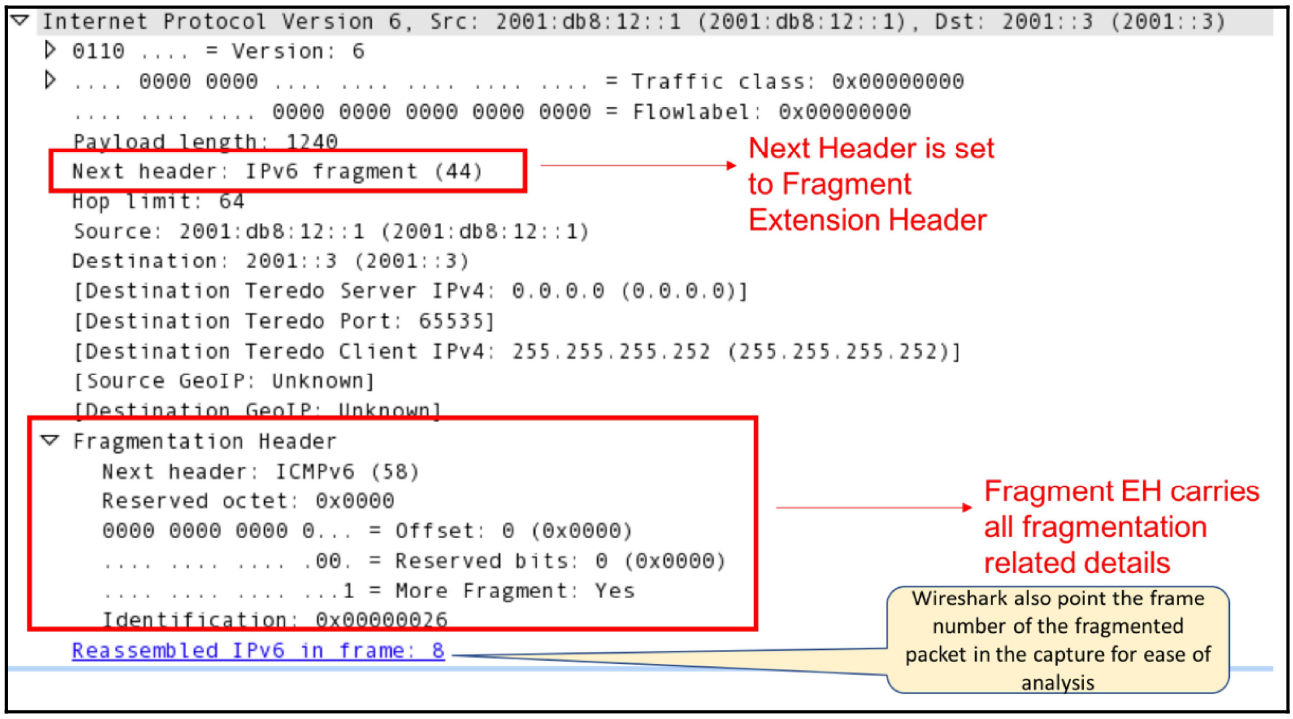

Internet Protocol Version 6, Src: 2001:db8:12::1 (2001:db8:12::1), Dst: 2001::2 (2001::2)
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 60
Next header: IPv6 hop-by-hop option (0)
Hop limit: 64
Source: 2001:db8:12::1 (2001:db8:12::1)
Destination: 2001::2 (2001::2)
[Destination Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]
[Destination Teredo Port: 65535]
[Destination Teredo Client IPv4: 255.255.255.253 (255.255.255.253)]
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Hop-by-Hop Option
Next header: IPv6 destination option (60)
Length: 0 (8 bytes)
IPv6 Option (PadN)
Destination Option
Next header: ICMPv6 (58)
Length: 0 (8 bytes)
IPv6 Option (PadN)
Internet Control Message Protocol v6
Hop-by-Hop Extension Header
Destination Extension Header


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ipv6.dst_opt
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
5 8.936678 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=0, hop limit=64 (reply in 6)
7 8.938518 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=1, hop limit=64 (reply in 8)
9 8.940256 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=2, hop limit=64 (reply in 10)
11 8.941513 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=3, hop limit=64 (reply in 12)
13 8.942777 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=4, hop limit=64 (reply in 14)
15 8.944181 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=5, hop limit=64 (reply in 16)
17 8.945440 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=6, hop limit=64 (reply in 18)
19 8.946665 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=7, hop limit=64 (reply in 20)
21 8.949914 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=8, hop limit=64 (reply in 22)
23 8.958933 2001:db8:12::1 2001::2 ICMPv6 114 Echo (ping) request id=0x17ae, seq=9, hop limit=64 (reply in 24)

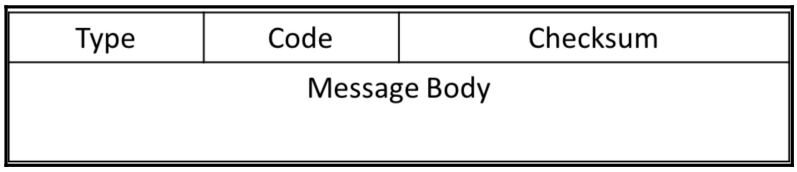

R1
2001:db8:0012::1
2001:db8:0012::2
R2
2001:db8:0023::2
2001:db8:0023::3
2001::3
R3
MTU=1280

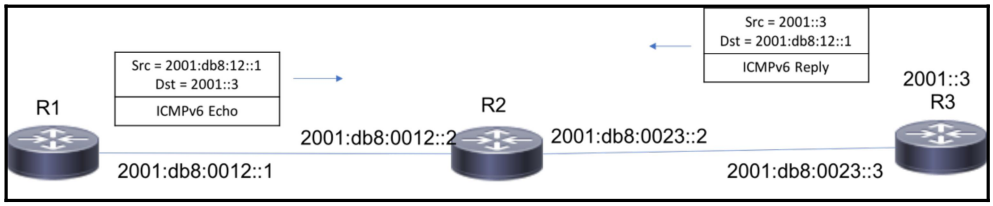

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1 0.000000 fe80::f816:3eff:fe0f:8852 ff02::5 OSPF 94 Hello Packet
2 0.147443 10.1.12.1 224.0.0.5 OSPF 94 Hello Packet
3 4.513879 fe80::f016:3eff:fe65:5f0e ff02::5 OSPF 94 Hello Packet
4 6.947570 10.1.12.2 224.0.0.5 OSPF 94 Hello Packet
5 8.360546 2001:db8:12::1 2001::3 ICMPv6 1514 Echo (ping) request id=0x1d69, seq=0, hop limit=64 (no response f
6 8.361813 2001:db8:12::2 2001:db8:12::1 ICMPv6 1294 Packet Too Big
7 8.362555 2001:db8:12::1 2001::3 IPv6 1294 IPv6 fragment (nxt=ICMPv6 (58) off=0 id=0x26)
8 8.413815 2001:db8:12::1 2001::3 ICMPv6 290 Echo (ping) request id=0x1d69, seq=1, hop limit=64 (reply in 10)
9 8.437972 2001::3 2001:db8:12::1 IPv6 1294 IPv6 fragment (nxt=ICMPv6 (58) off=0 id=0x24)
R2 generates ICMPv6 error message (Packet too Big)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: ipv6.fragment
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
8 8.413815 2001:db8:12::1 2001::3 ICMPv6 290 Echo (ping) request id=0x1d69, seq=1, hop limit=64 (reply in 10)
10 8.542024 2001::3 2001:db8:12::1 ICMPv6 290 Echo (ping) reply id=0x1d69, seq=1, hop limit=63 (request in 8)
12 8.543217 2001:db8:12::1 2001::3 ICMPv6 290 Echo (ping) request id=0x1d69, seq=2, hop limit=64 (reply in 14)
14 8.795052 2001::3 2001:db8:12::1 ICMPv6 290 Echo (ping) reply id=0x1d69, seq=2, hop limit=63 (request in 12)
16 8.796357 2001:db8:12::1 2001::3 ICMPv6 290 Echo (ping) request id=0x1d69, seq=3, hop limit=64 (reply in 18)
18 9.049014 2001::3 2001:db8:12::1 ICMPv6 290 Echo (ping) reply id=0x1d69, seq=3, hop limit=63 (request in 16)
20 9.050332 2001:db8:12::1 2001::3 ICMPv6 290 Echo (ping) request id=0x1d69, seq=4, hop limit=64 (reply in 23)
23 9.310012 2001::3 2001:db8:12::1 ICMPv6 290 Echo (ping) reply id=0x1d69, seq=4, hop limit=63 (request in 20)


Internet Protocol Version 6, Src: 2001:db8:12::1 (2001:db8:12::1), Dst: 2001::3 (2001::3)
0110 .... = Version: 6
.... 0000 0000 .... = Traffic class: 0x00000000
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 1240
Next header: IPv6 fragment (44)
Next Header is set to Fragment Extension Header
Hop limit: 64
Source: 2001:db8:12::1 (2001:db8:12::1)
Destination: 2001::3 (2001::3)
[Destination Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]
[Destination Teredo Port: 65535]
[Destination Teredo Client IPv4: 255.255.255.252 (255.255.255.252)]
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Fragmentation Header
Next header: ICMPv6 (58)
Reserved octet: 0x0000
0000 0000 0000 0... = Offset: 0 (0x0000)
.... .00. = Reserved bits: 0 (0x0000)
....1 = More Fragment: Yes
Identification: 0x00000026
Fragment EH carries all fragmentation related details
Reassembled IPv6 in frame: 8
Wireshark also point the frame number of the fragmented packet in the capture for ease of analysis

Filter	Description	Example
ipv6.hop_opt	Filters all IPv6 packets with HbH extension header	ipv6.hop_opt
ipv6.dst_opt	Filters all IPv6 packets with destination extension header	ipv6.dst_opt
ipv6.fragment	Filters all IPv6 packets with fragment extension header	ipv6.fragment





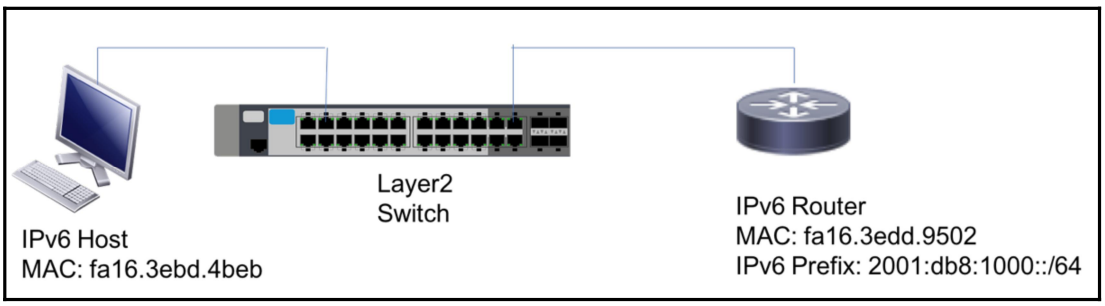

```
Internet Protocol Version 6, Src: 2001:db8:12::1 (2001:db8:12::1), Dst: 2001::3 (2001::3)
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 1240
  Next header: IPv6 fragment (44)
  Hop limit: 63
  Source: 2001:db8:12::1 (2001:db8:12::1)
  Destination: 2001::3 (2001::3)
  [Destination Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]
  [Destination Teredo Port: 65535]
  [Destination Teredo Client IPv4: 255.255.255.252 (255.255.255.252)]
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  Fragmentation Header
Internet Control Message Protocol v6
  Type: Echo (ping) request (128)
  Code: 0
  Checksum: 0xcf47
  Identifier: 0x1ce0
  Sequence: 1
  [Response In: 12]
  Data (1224 bytes)
```

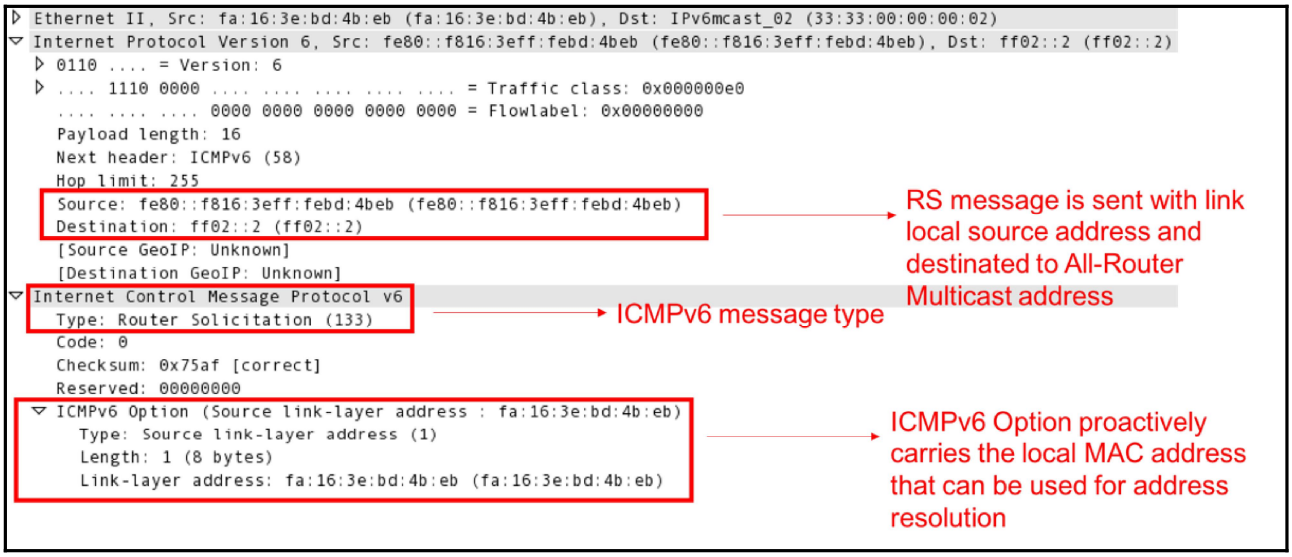
ICMPv6 Echo Request message

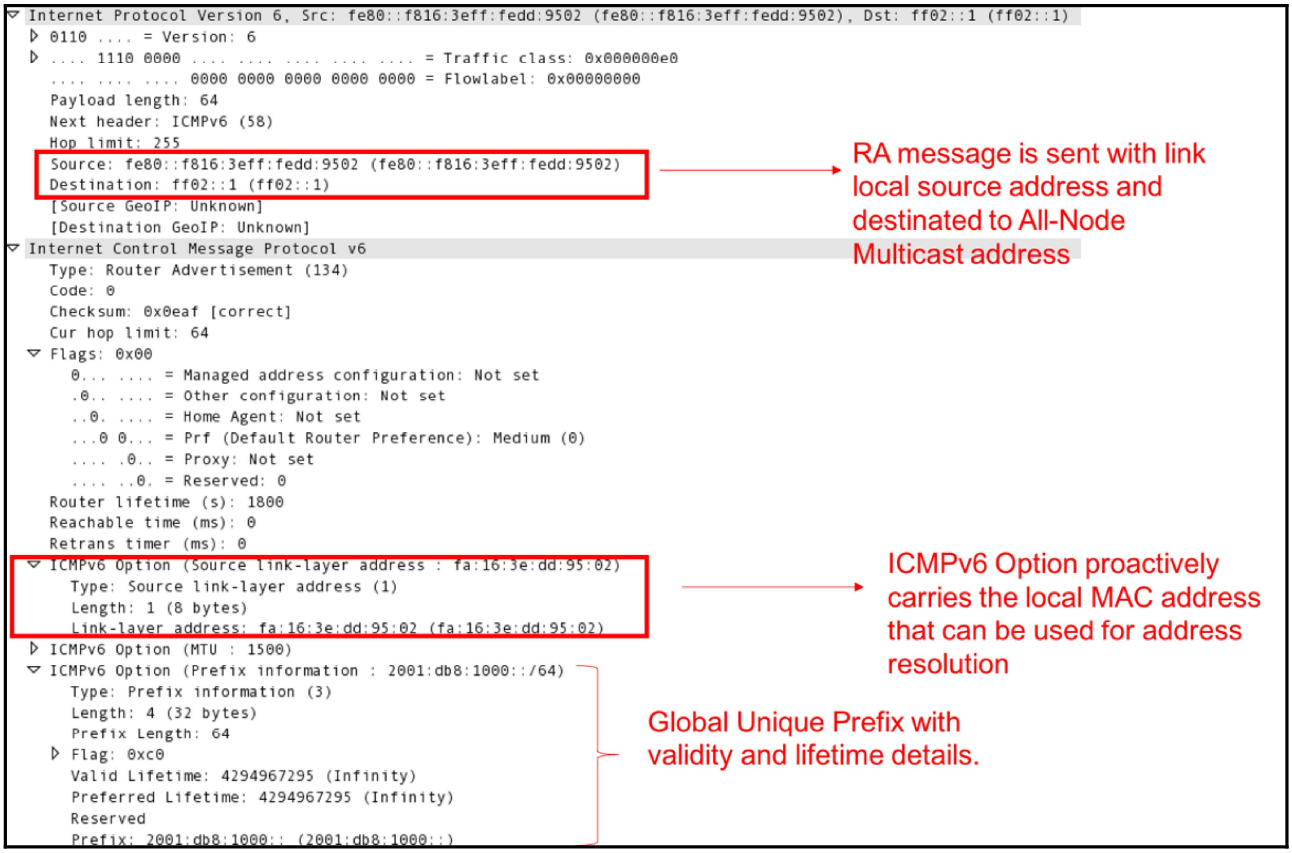
```
Internet Protocol Version 6, Src: 2001::3 (2001::3), Dst: 2001:db8:12::1 (2001:db8:12::1)
  0110 .... = Version: 6
  .... 0000 0000 .... .... .... .... .... = Traffic class: 0x00000000
  .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 1240
  Next header: IPv6 fragment (44)
  Hop limit: 64
  Source: 2001::3 (2001::3)
  [Source Teredo Server IPv4: 0.0.0.0 (0.0.0.0)]
  [Source Teredo Port: 65535]
  [Source Teredo Client IPv4: 255.255.255.252 (255.255.255.252)]
  Destination: 2001:db8:12::1 (2001:db8:12::1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
  Fragmentation Header
Internet Control Message Protocol v6
  Type: Echo (ping) reply (129)
  Code: 0
  Checksum: 0xce47
  Identifier: 0x1ce0
  Sequence: 1
  [Response To: 10]
  [Response Time: 103.977 ms]
```

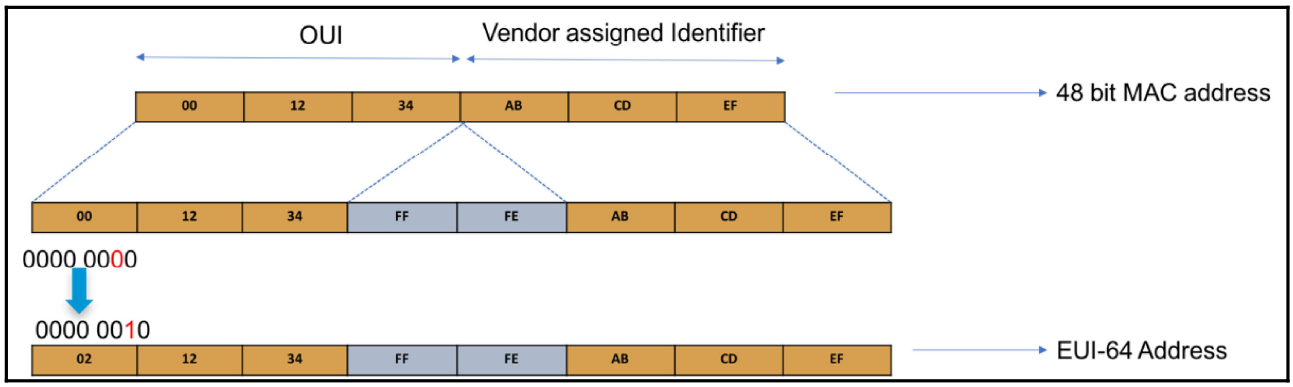
ICMPv6 Echo Reply message

Errors: 0 (0)	Warnings: 2 (2)	Notes: 0 (0)	Chats: 0 (0)	Details: 2	Packet Comments: 0
Group	Protocol	Summary			Count
Sequence	ICMPv6	No response seen to ICMPv6 request in frame 76			
Packet:	76				
Sequence	ICMPv6	No response seen to ICMPv6 request in frame 119			



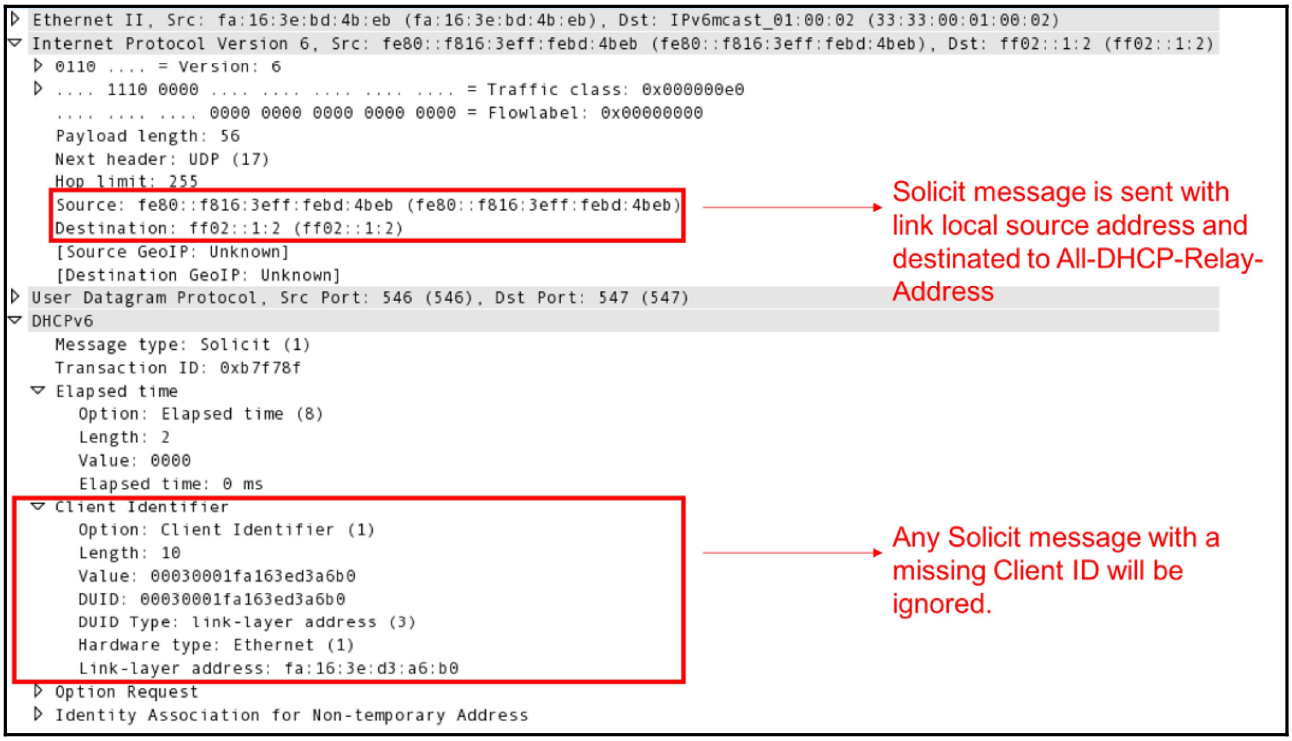

Ethernet II, Src: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb), Dst: ff02::2 (ff02::2)
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 16
Next header: ICMPv6 (58)
Hop limit: 255
Source: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb)
Destination: ff02::2 (ff02::2)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol v6
Type: Router Solicitation (133)
Code: 0
Checksum: 0x75af [correct]
Reserved: 00000000
ICMPv6 Option (Source link-layer address : fa:16:3e:bd:4b:eb)
Type: Source link-layer address (1)
Length: 1 (8 bytes)
Link-layer address: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb)
RS message is sent with link local source address and destinated to All-Router Multicast address
ICMPv6 message type
ICMPv6 Option proactively carries the local MAC address that can be used for address resolution

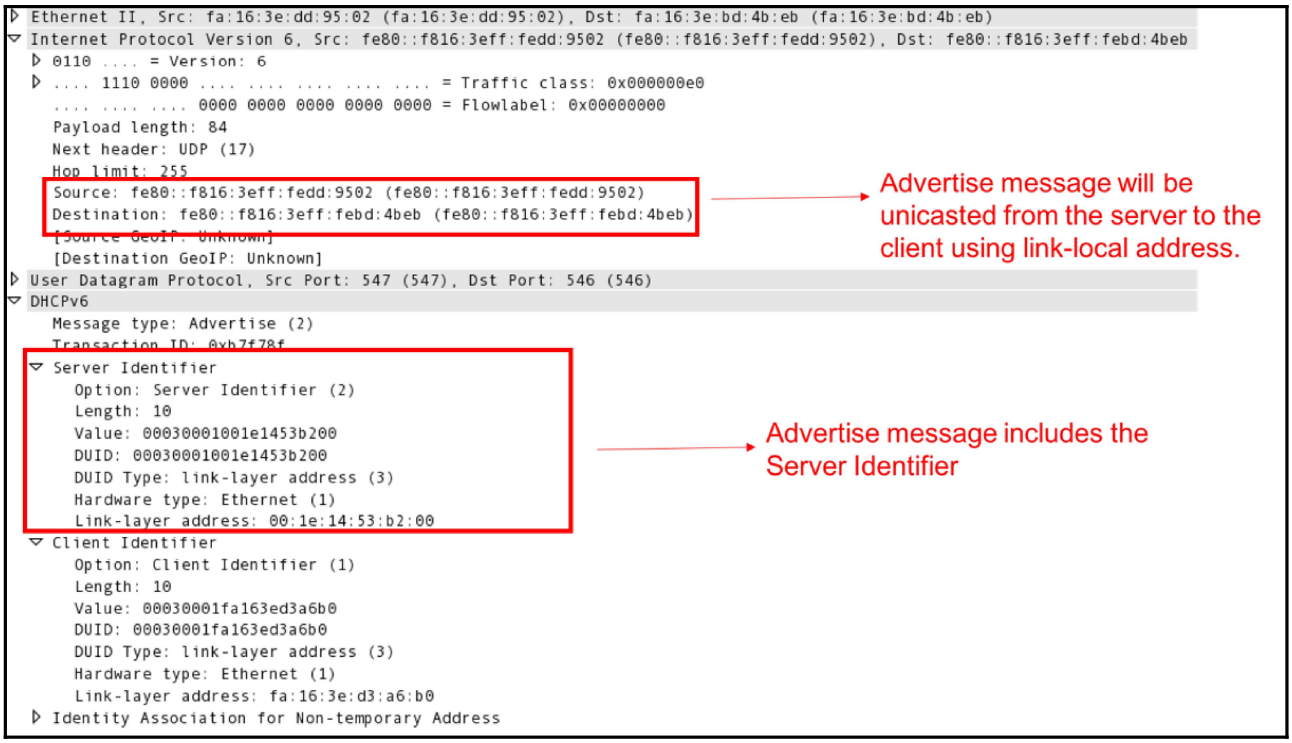

Internet Protocol Version 6, Src: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502), Dst: ff02::1 (ff02::1)
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 64
Next header: ICMPv6 (58)
Hop limit: 255
Source: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502)
Destination: ff02::1 (ff02::1)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol v6
Type: Router Advertisement (134)
Code: 0
Checksum: 0x0eaf [correct]
Cur hop limit: 64
Flags: 0x00
0... .... = Managed address configuration: Not set
.0.. .... = Other configuration: Not set
..0. .... = Home Agent: Not set
...0 0... = Prf (Default Router Preference): Medium (0)
.... .0.. = Proxy: Not set
.... ..0. = Reserved: 0
Router lifetime (s): 1800
Reachable time (ms): 0
Retrans timer (ms): 0
ICMPv6 Option (Source link-layer address : fa:16:3e:dd:95:02)
Type: Source link-layer address (1)
Length: 1 (8 bytes)
Link-layer address: fa:16:3e:dd:95:02 (fa:16:3e:dd:95:02)
ICMPv6 Option (MTU : 1500)
ICMPv6 Option (Prefix information : 2001:db8:1000::/64)
Type: Prefix information (3)
Length: 4 (32 bytes)
Prefix Length: 64
Flag: 0xc0
Valid Lifetime: 4294967295 (Infinity)
Preferred Lifetime: 4294967295 (Infinity)
Reserved
Prefix: 2001:db8:1000:: (2001:db8:1000::)
RA message is sent with link local source address and destinated to All-Node Multicast address
ICMPv6 Option proactively carries the local MAC address that can be used for address resolution
Global Unique Prefix with validity and lifetime details.

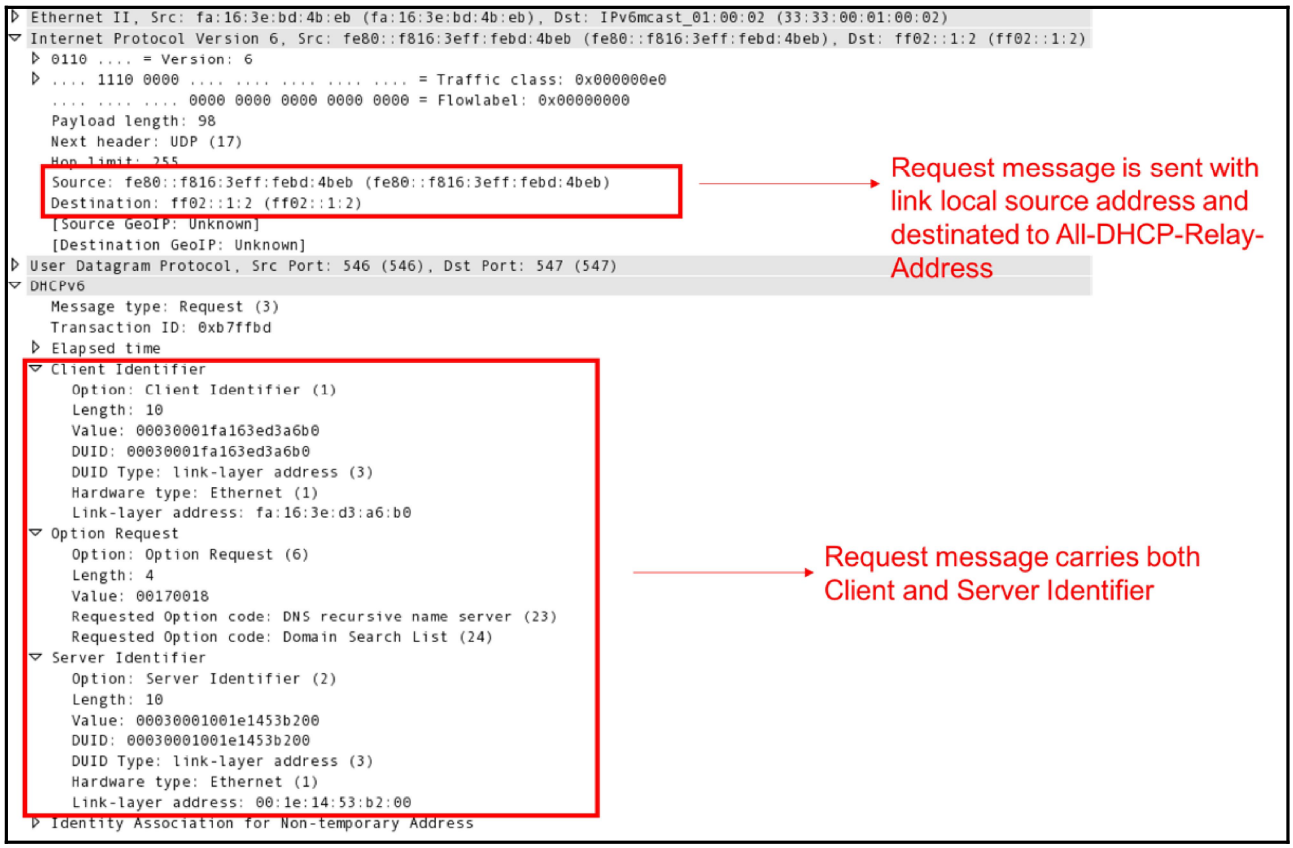


Type=133	Code=0	Checksum
Reserved		
Options		

Type=133	Code=0			Checksum
Hop Limit	M	O	Rsvd	Router Lifetime
Reachable Time				
Retransmission Timer				
Options				


Ethernet II, Src: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb), Dst: ff02::1:2 (ff02::1:2)
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 56
Next header: UDP (17)
Hop limit: 255
Source: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb)
Destination: ff02::1:2 (ff02::1:2)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
DHCPv6
Message type: Solicit (1)
Transaction ID: 0xb7f78f
Elapsed time
Option: Elapsed time (8)
Length: 2
Value: 0000
Elapsed time: 0 ms
Client Identifier
Option: Client Identifier (1)
Length: 10
Value: 00030001fa163ed3a6b0
DUID: 00030001fa163ed3a6b0
DUID Type: link-layer address (3)
Hardware type: Ethernet (1)
Link-layer address: fa:16:3e:d3:a6:b0
Option Request
Identity Association for Non-temporary Address
Solicit message is sent with link local source address and destinated to All-DHCP-Relay-Address
Any Solicit message with a missing Client ID will be ignored.

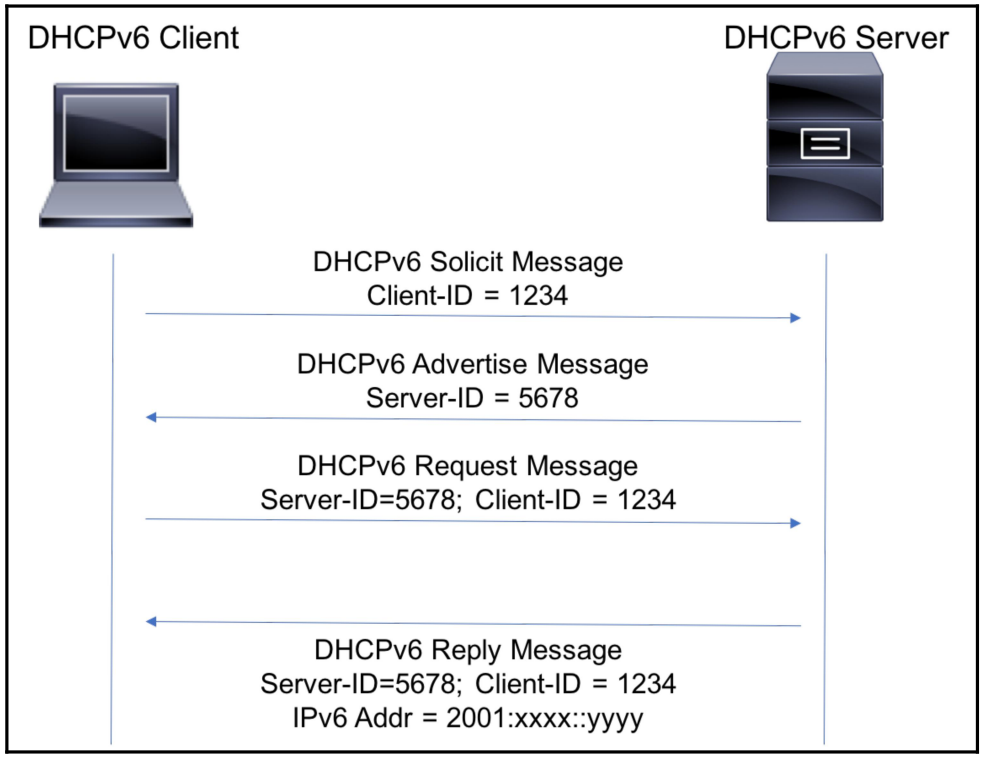

Ethernet II, Src: fa:16:3e:dd:95:02 (fa:16:3e:dd:95:02), Dst: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb)
Internet Protocol Version 6, Src: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502), Dst: fe80::f816:3eff:febd:4beb
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 84
Next header: UDP (17)
Hop limit: 255
Source: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502)
Destination: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 547 (547), Dst Port: 546 (546)
DHCPv6
Message type: Advertise (2)
Transaction ID: 0xb7f78f
Server Identifier
Option: Server Identifier (2)
Length: 10
Value: 00030001001e1453b200
DUID: 00030001001e1453b200
DUID Type: link-layer address (3)
Hardware type: Ethernet (1)
Link-layer address: 00:1e:14:53:b2:00
Client Identifier
Option: Client Identifier (1)
Length: 10
Value: 00030001fa163ed3a6b0
DUID: 00030001fa163ed3a6b0
DUID Type: link-layer address (3)
Hardware type: Ethernet (1)
Link-layer address: fa:16:3e:d3:a6:b0
Identity Association for Non-temporary Address
Advertise message will be unicasted from the server to the client using link-local address.
Advertise message includes the Server Identifier


Ethernet II, Src: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb), Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb), Dst: ff02::1:2 (ff02::1:2)
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 98
Next header: UDP (17)
Hop limit: 255
Source: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb)
Destination: ff02::1:2 (ff02::1:2)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 546 (546), Dst Port: 547 (547)
DHCPv6
Message type: Request (3)
Transaction ID: 0xb7ffbd
Elapsed time
Client Identifier
Option: Client Identifier (1)
Length: 10
Value: 00030001fa163ed3a6b0
DUID: 00030001fa163ed3a6b0
DUID Type: link-layer address (3)
Hardware type: Ethernet (1)
Link-layer address: fa:16:3e:d3:a6:b0
Option Request
Option: Option Request (6)
Length: 4
Value: 00170018
Requested Option code: DNS recursive name server (23)
Requested Option code: Domain Search List (24)
Server Identifier
Option: Server Identifier (2)
Length: 10
Value: 00030001001e1453b200
DUID: 00030001001e1453b200
DUID Type: link-layer address (3)
Hardware type: Ethernet (1)
Link-layer address: 00:1e:14:53:b2:00
Identity Association for Non-temporary Address
Request message is sent with link local source address and destinated to All-DHCP-Relay-Address
Request message carries both Client and Server Identifier

```
▷ Ethernet II, Src: fa:16:3e:dd:95:02 (fa:16:3e:dd:95:02), Dst: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb)
▽ Internet Protocol Version 6, Src: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502), Dst: fe80::f816:
  ▷ 0110 .... = Version: 6
  ▷ .... 1110 0000 .... .... .... .... .... = Traffic class: 0x000000e0
    .... .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
    Payload length: 84
    Next header: UDP (17)
    Hop limit: 255
    Source: fe80::f816:3eff:fedd:9502 (fe80::f816:3eff:fedd:9502)
    Destination: fe80::f816:3eff:febd:4beb (fe80::f816:3eff:febd:4beb)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▷ User Datagram Protocol, Src Port: 547 (547), Dst Port: 546 (546)
▽ DHCPv6
    Message type: Reply (7)
    Transaction ID: 0xb7ffbd
  ▷ Server Identifier
  ▷ Client Identifier
  ▽ Identity Association for Non-temporary Address
      Option: Identity Association for Non-temporary Address (3)
      Length: 40
      Value: 000300010000a8c000010e00000500182001 0db802000000...
      IAID: 00030001
      T1: 43200
      T2: 69120
    ▽ IA Address
        Option: IA Address (5)
        Length: 24
        Value: 20010db802000000adf8c97f60492ffaffffffffffffffff
        IPv6 address: 2001:db8:200:0:adf8:c97f:6049:2ffa (2001:db8:200:0:adf8:c97f:6049:2ffa)
        Preferred lifetime: infinity
        Preferred lifetime: infinity
```

Reply message will be unicasted from the server to the client using link-local address.

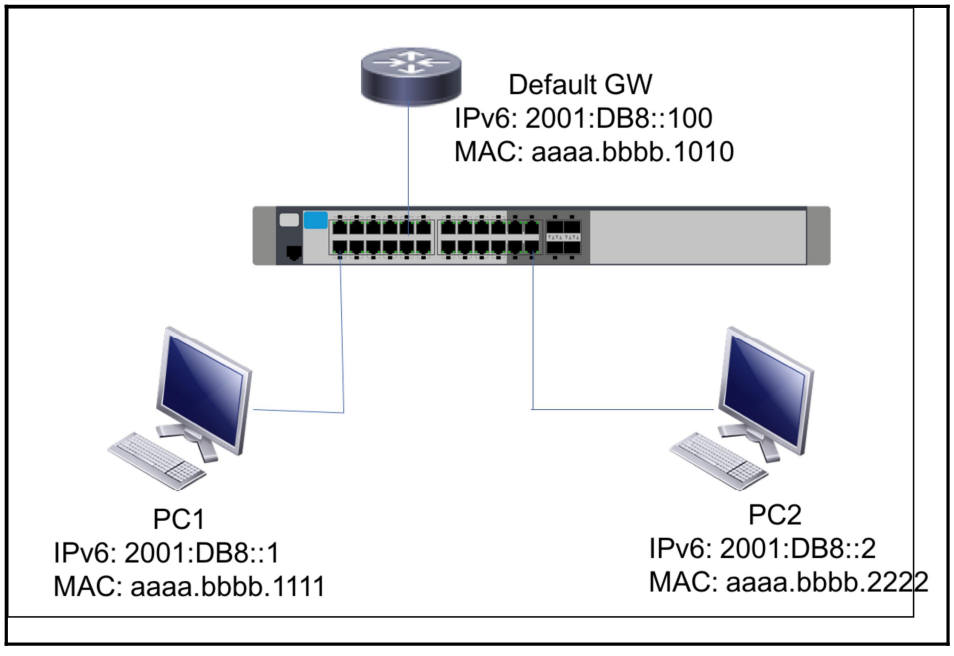
Assigned Address

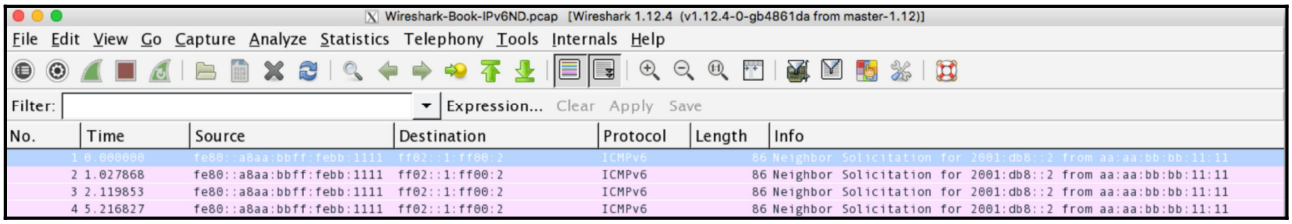


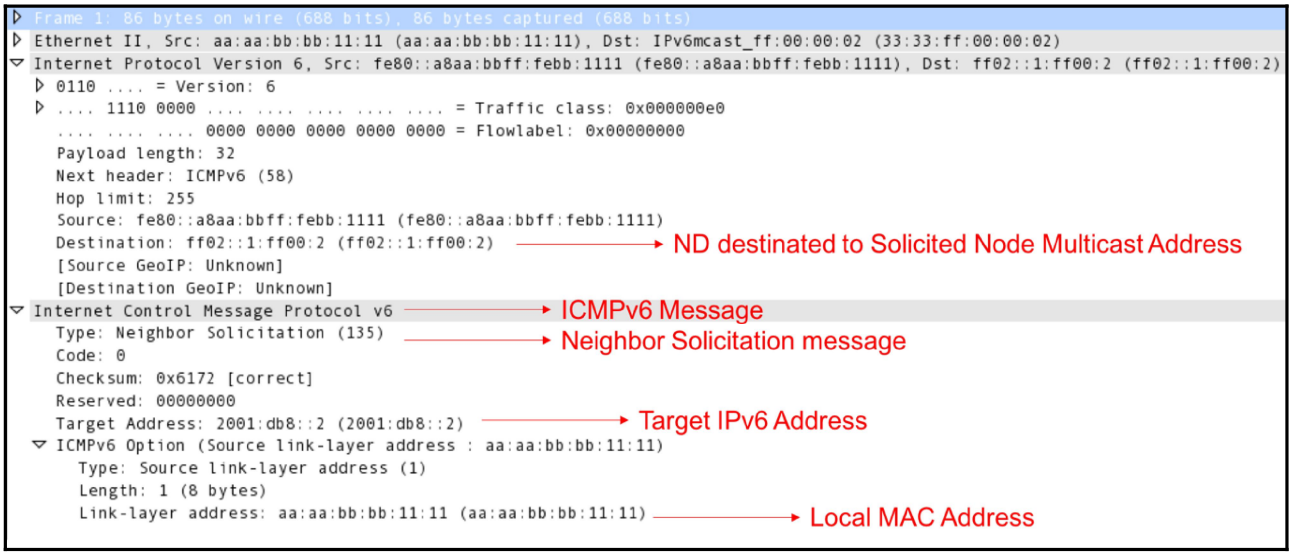
Filter	Description	Example
dhcpv6	Filters all DHCPv6 packets	dhcpv6
dhcpv6.msgtype ==<>	Filters all DHCPv6 packets based on the message type	dhcpv6.msgtype == solicit dhcpv6.msgtype == advertise
dhcpv6.iaaddr.ip == <>	Filters all DHCPv6 packets with the specific IA address	dhcpv6.iaaddr.ip == <addr>

Type = 135	Code = 0	Checksum
Reserved		
Target Address (8 Octets)		
Options (Variable)		

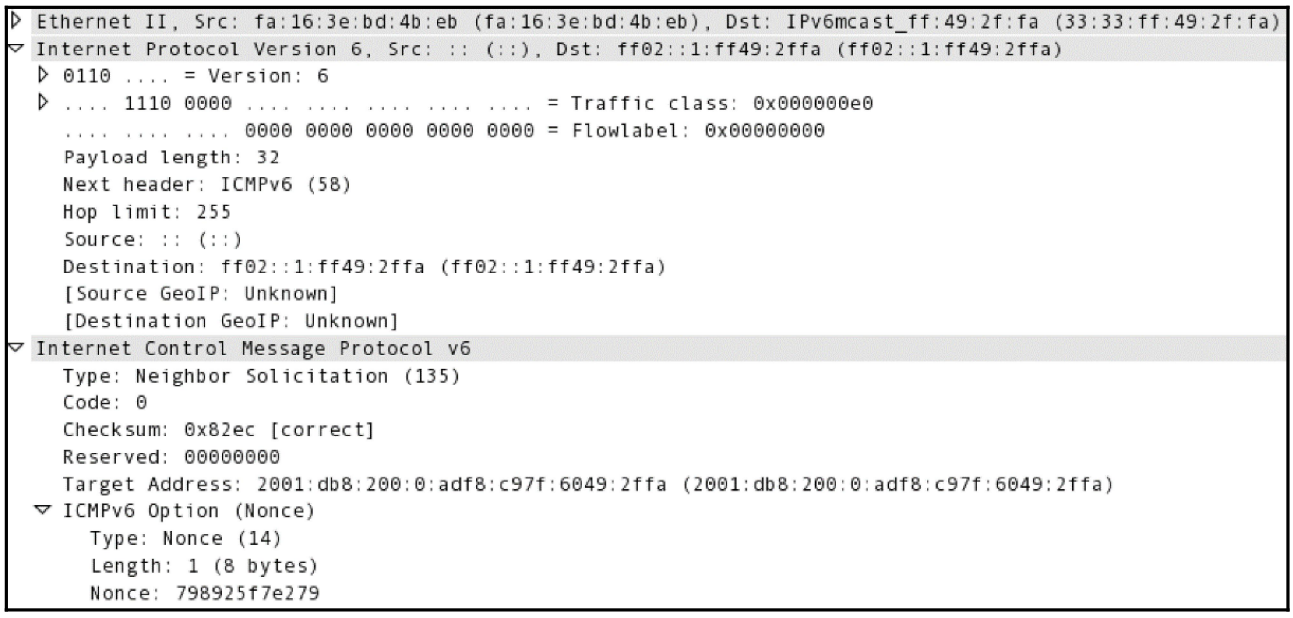
Type = 136	Code = 0	Checksum
R S O	Reserved	
Target Address (8 Octets)		
Options (Variable)		



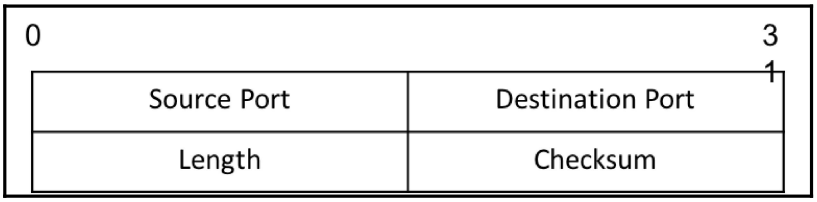




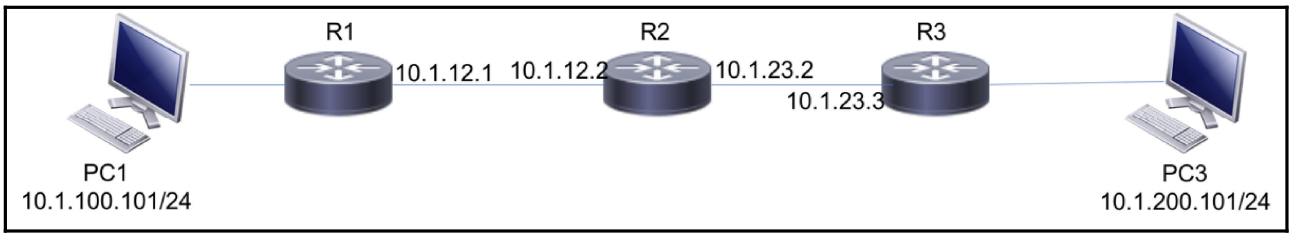
Filter	Description	Example
icmpv6.type == <type>	ICMPv6 type based filter. Type 135 will filter all IPv6 neighbor solicitation packets and type 136 will filter all IPv6 neighbor advertisement packets	icmpv6.type == 135 icmpv6.type == 136
icmpv6.nd.ns.target_address == <ipv6_addr>	Filter the NS packet with target IPv6 address	icmpv6.nd.ns.target_address == 2001:DB8::2
icmpv6.nd.ns.target_address == <ipv6_addr>	Filter the NA packet with target IPv6 address	icmpv6.nd.na.target_address == 2001:db8::1


Ethernet II, Src: fa:16:3e:bd:4b:eb (fa:16:3e:bd:4b:eb), Dst: IPv6mcast_ff:49:2f:fa (33:33:ff:49:2f:fa)
Internet Protocol Version 6, Src: :: (::), Dst: ff02::1:ff49:2ffa (ff02::1:ff49:2ffa)
0110 .... = Version: 6
.... 1110 0000 .... = Traffic class: 0x000000e0
.... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
Payload length: 32
Next header: ICMPv6 (58)
Hop limit: 255
Source: :: (::)
Destination: ff02::1:ff49:2ffa (ff02::1:ff49:2ffa)
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Internet Control Message Protocol v6
Type: Neighbor Solicitation (135)
Code: 0
Checksum: 0x82ec [correct]
Reserved: 00000000
Target Address: 2001:db8:200:0:adf8:c97f:6049:2ffa (2001:db8:200:0:adf8:c97f:6049:2ffa)
ICMPv6 Option (Nonce)
Type: Nonce (14)
Length: 1 (8 bytes)
Nonce: 798925f7e279

Chapter 11: Transport Layer Protocol Analysis




```
▶ Frame 14: 331 bytes on wire (2648 bits), 331 bytes captured (2648 bits)
▶ Ethernet II, Src: aa:bb:cc:03:f3:30 (aa:bb:cc:03:f3:30), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▼ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 317
    Identification: 0x1e26 (7718)
  ▶ Flags: 0x00
    Fragment offset: 0
    Time to live: 255
    Protocol: UDP (17)
    Header checksum: 0x9c8a [validation disabled]
    [Header checksum status: Unverified]
    Source: 0.0.0.0
    Destination: 255.255.255.255
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
▼ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 297
    Checksum: 0xf189 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
▶ Bootstrap Protocol (Discover)
```



```
▶ Frame 7: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)
▼ Ethernet II, Src: fa:16:3e:65:5f:0e (fa:16:3e:65:5f:0e), Dst: fa:16:3e:0f:88:52 (fa:16:3e:0f:88:52)
  ▼ Destination: fa:16:3e:0f:88:52 (fa:16:3e:0f:88:52)
      Address: fa:16:3e:0f:88:52 (fa:16:3e:0f:88:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: fa:16:3e:65:5f:0e (fa:16:3e:65:5f:0e)
      Address: fa:16:3e:65:5f:0e (fa:16:3e:65:5f:0e)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.1.12.1, Dst: 10.1.3.3
▼ User Datagram Protocol, Src Port: 50238, Dst Port: 1967
    Source Port: 50238
    Destination Port: 1967
    Length: 60
  ▶ Checksum: 0x0378 [correct]
    [Checksum Status: Good]
    [Stream index: 2]
▶ Data (52 bytes)
```

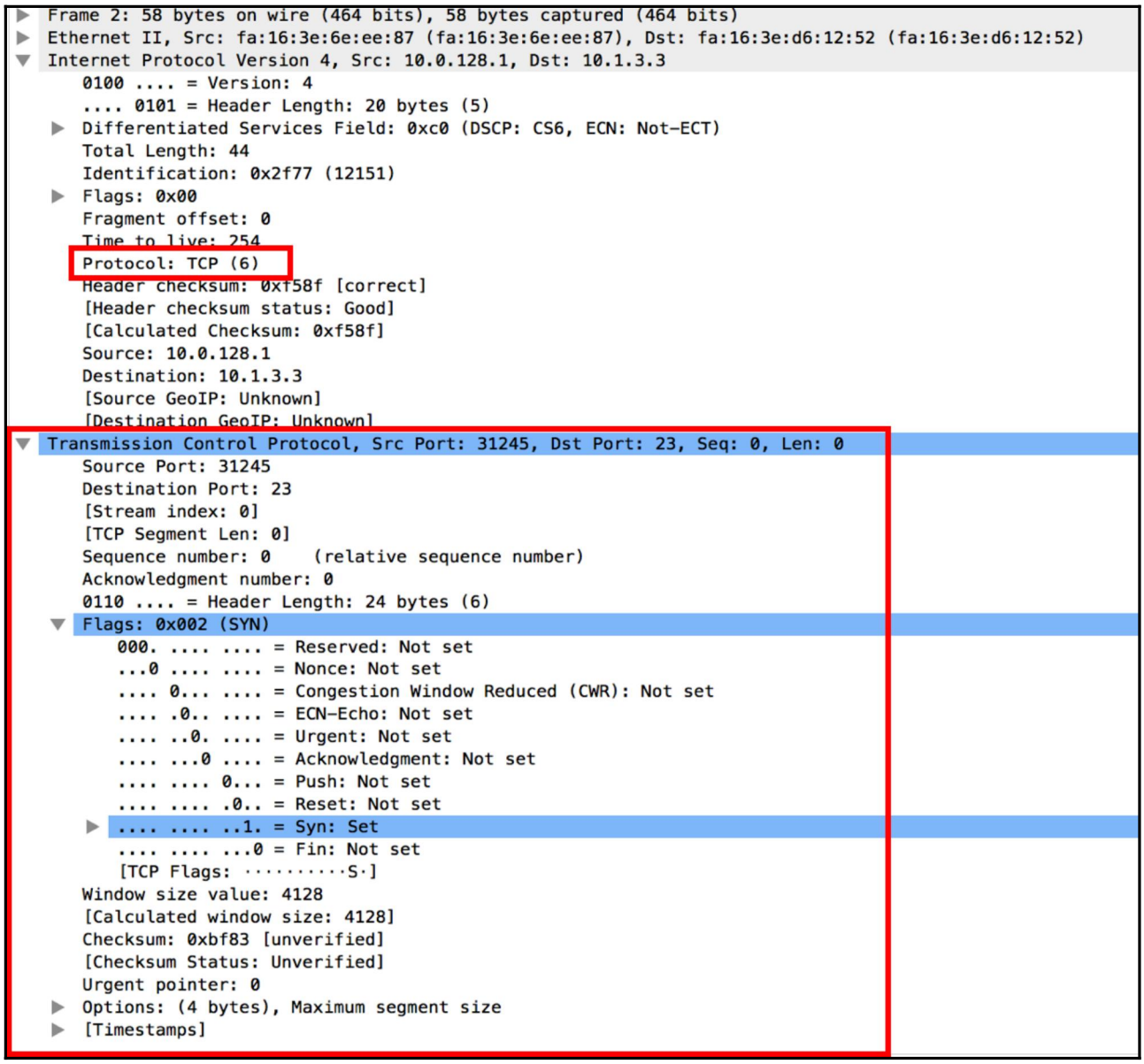
```
udp.stream eq 2                                                    Expression...  +
No.   Time        Source        Destination   Protocol  Length  Info
    7 0.999172    10.1.12.1     10.1.3.3      UDP           94  50238 → 1967 Len=…
    8 1.000405    10.1.3.3      10.1.12.1     UDP           66  1967 → 50238 Len=…
```

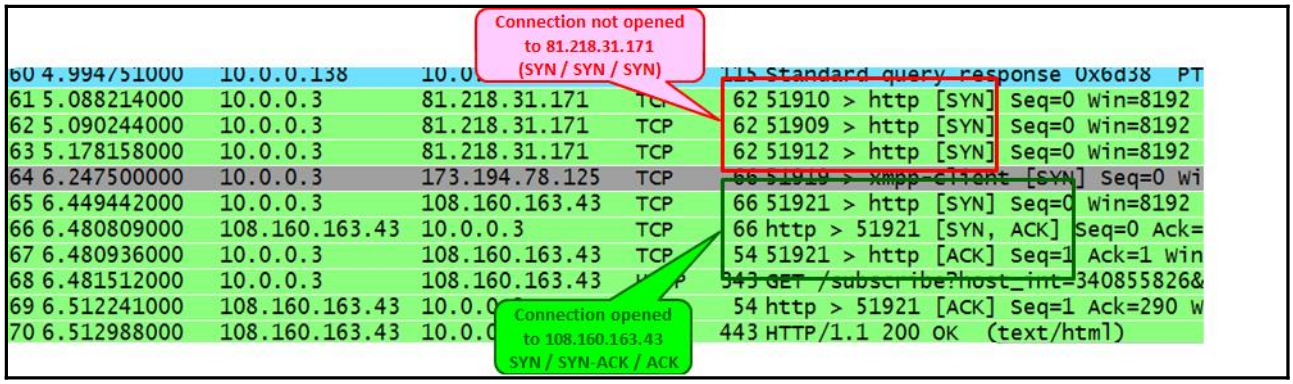
```
  ▼ Destination: fa:16:3e:0f:88:52 (fa:16:3e:0f:88:52)
      Address: fa:16:3e:0f:88:52 (fa:16:3e:0f:88:52)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: fa:16:3e:65:5f:0e (fa:16:3e:65:5f:0e)
      Address: fa:16:3e:65:5f:0e (fa:16:3e:65:5f:0e)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 10.1.12.1, Dst: 10.1.3.3
▼ User Datagram Protocol, Src Port: 50238, Dst Port: 1967
    Source Port: 50238
    Destination Port: 1967
    Length: 60
  ▶ Checksum: 0x0378 [correct]
    [Checksum Status: Good]
    [Stream index: 2]
```

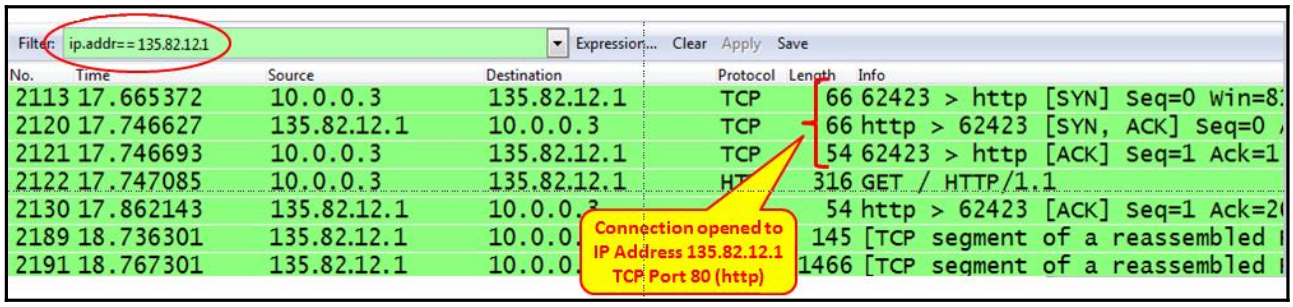
Filter	Description	Example
udp	Filters all UDP packets	udp
udp.stream eq <>	Filters all UDP packet matching the stram index	udp.stream eq 2
udp.port == <>	Filters all UDP port matching the value in source or destination port field	udp.port == 65000
udp.srcport == <>	Filters all UDP port matching the value in source port field	udp.srcport == 65000
udp.dstport == <>	Filters all UDP port matching the value in destination port field	udp.dstport == 65000

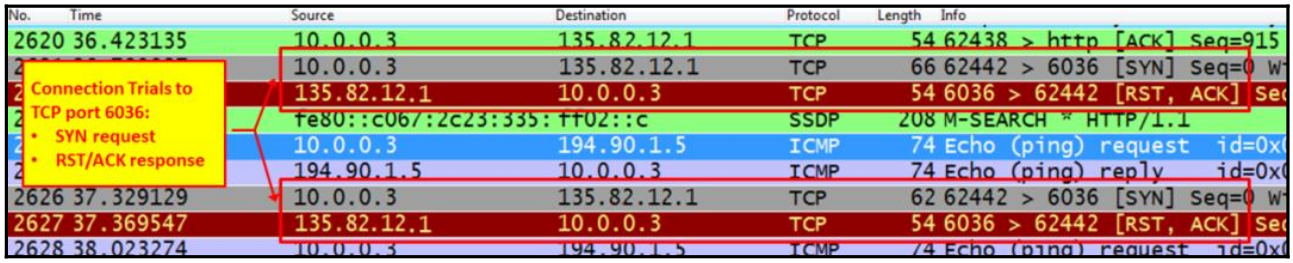
<table>
<tr><td colspan="5">Source Port</td><td colspan="5">Destination Port</td></tr>
<tr><td colspan="10">Sequence Number</td></tr>
<tr><td colspan="10">Acknowledgement Number</td></tr>
<tr><td>Offset</td><td>Resv</td><td>C</td><td>E</td><td>U</td><td>A</td><td>P</td><td>R</td><td>S</td><td>F</td><td>Window</td></tr>
<tr><td colspan="5">Checksum</td><td colspan="5">Urgent Pointer</td></tr>
<tr><td colspan="10">TCP Options (Optional)</td></tr>
</table>

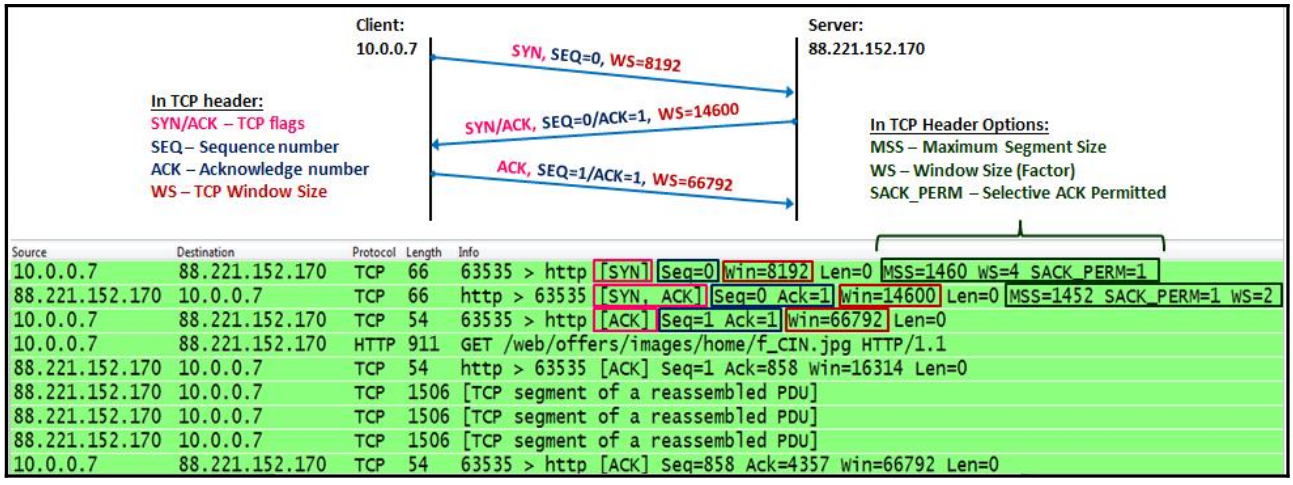
Application	TCP Port
WWW/HTTP	80
Simple Mail Transfer Protocol(SMTP)	25
Secure Shell (SSH)	22

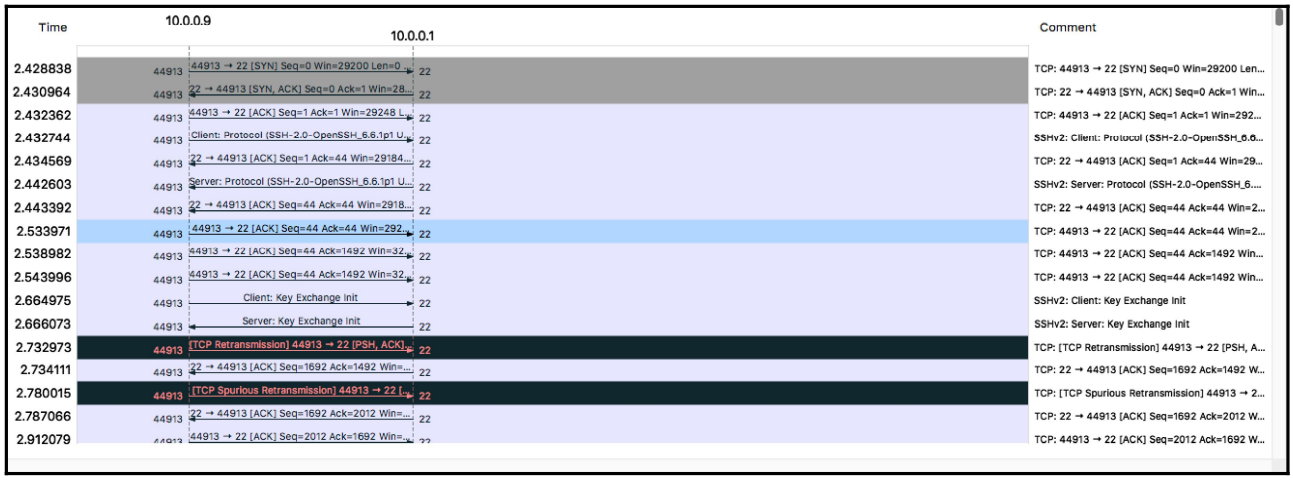

Frame 2: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
Ethernet II, Src: fa:16:3e:6e:ee:87 (fa:16:3e:6e:ee:87), Dst: fa:16:3e:d6:12:52 (fa:16:3e:d6:12:52)
Internet Protocol Version 4, Src: 10.0.128.1, Dst: 10.1.3.3
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
Total Length: 44
Identification: 0x2f77 (12151)
Flags: 0x00
Fragment offset: 0
Time to live: 254
Protocol: TCP (6)
Header checksum: 0xf58f [correct]
[Header checksum status: Good]
[Calculated Checksum: 0xf58f]
Source: 10.0.128.1
Destination: 10.1.3.3
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 31245, Dst Port: 23, Seq: 0, Len: 0
Source Port: 31245
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
0110 .... = Header Length: 24 bytes (6)
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
....0 = Fin: Not set
[TCP Flags: ·····S·]
Window size value: 4128
[Calculated window size: 4128]
Checksum: 0xbf83 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (4 bytes), Maximum segment size
[Timestamps]

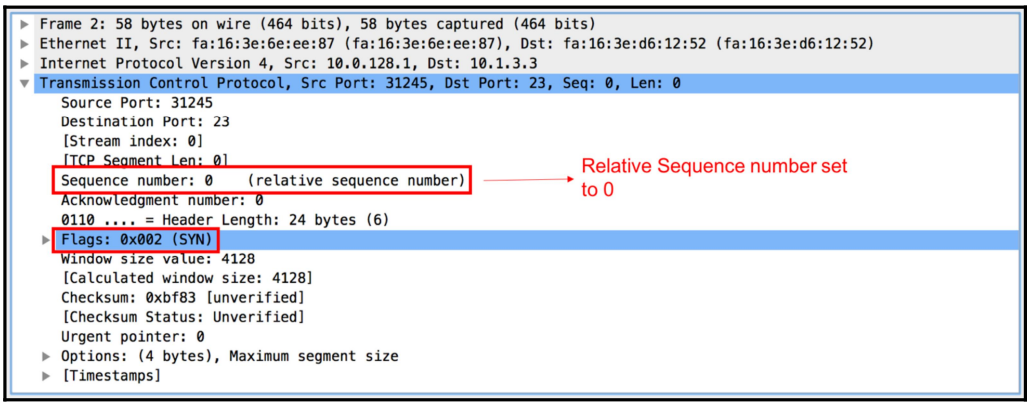

Connection not opened
to 81.218.31.171
(SYN / SYN / SYN)
Connection opened
to 108.160.163.43
SYN / SYN-ACK / ACK

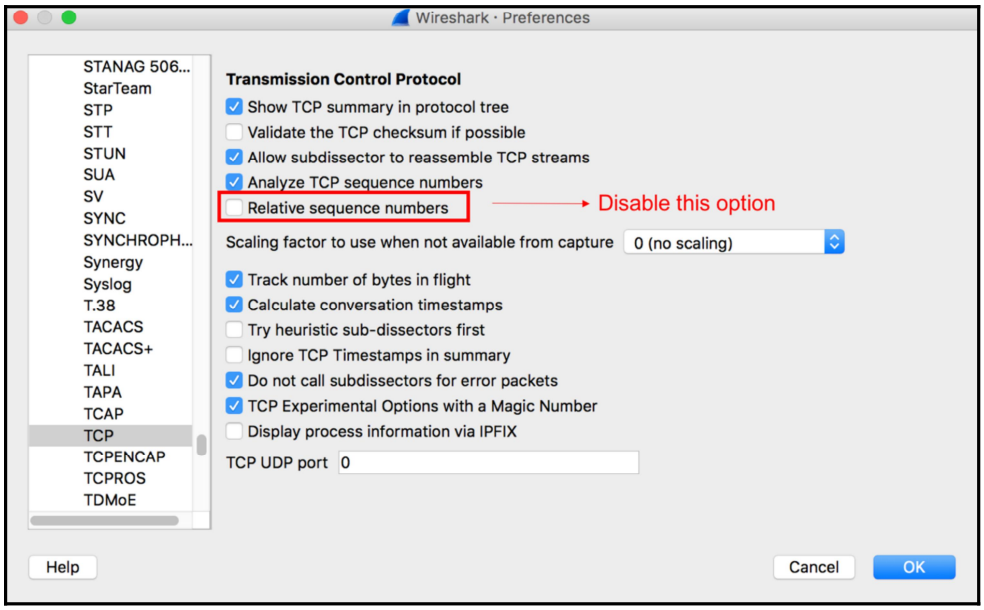

Filter: ip.addr==135.82.12.1
Expression... Clear Apply Save
Connection opened to
IP Address 135.82.12.1
TCP Port 80 (http)

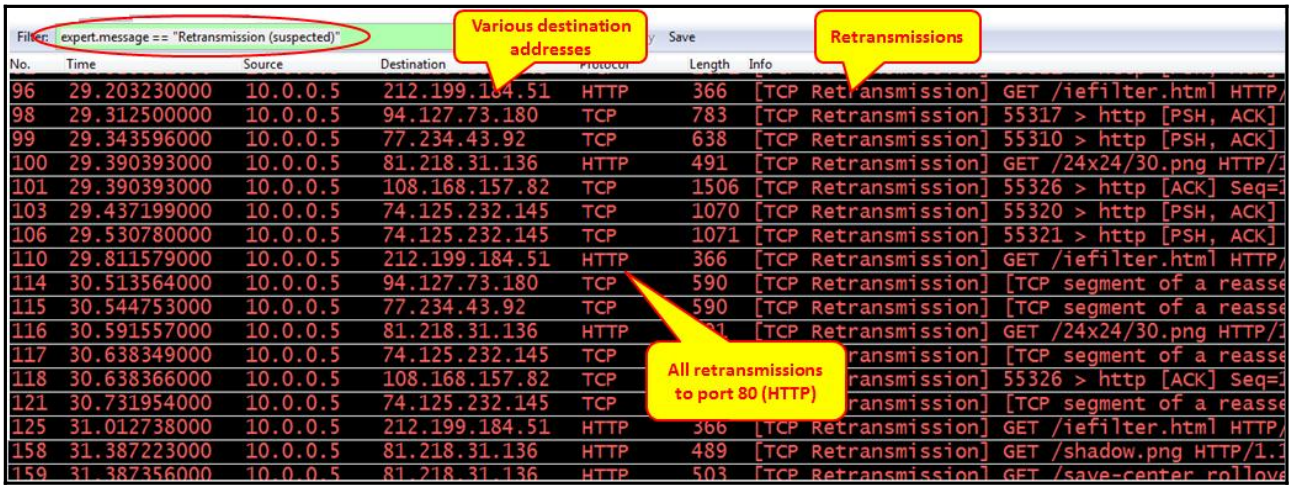

Connection Trials to
TCP port 6036:
• SYN request
• RST/ACK response

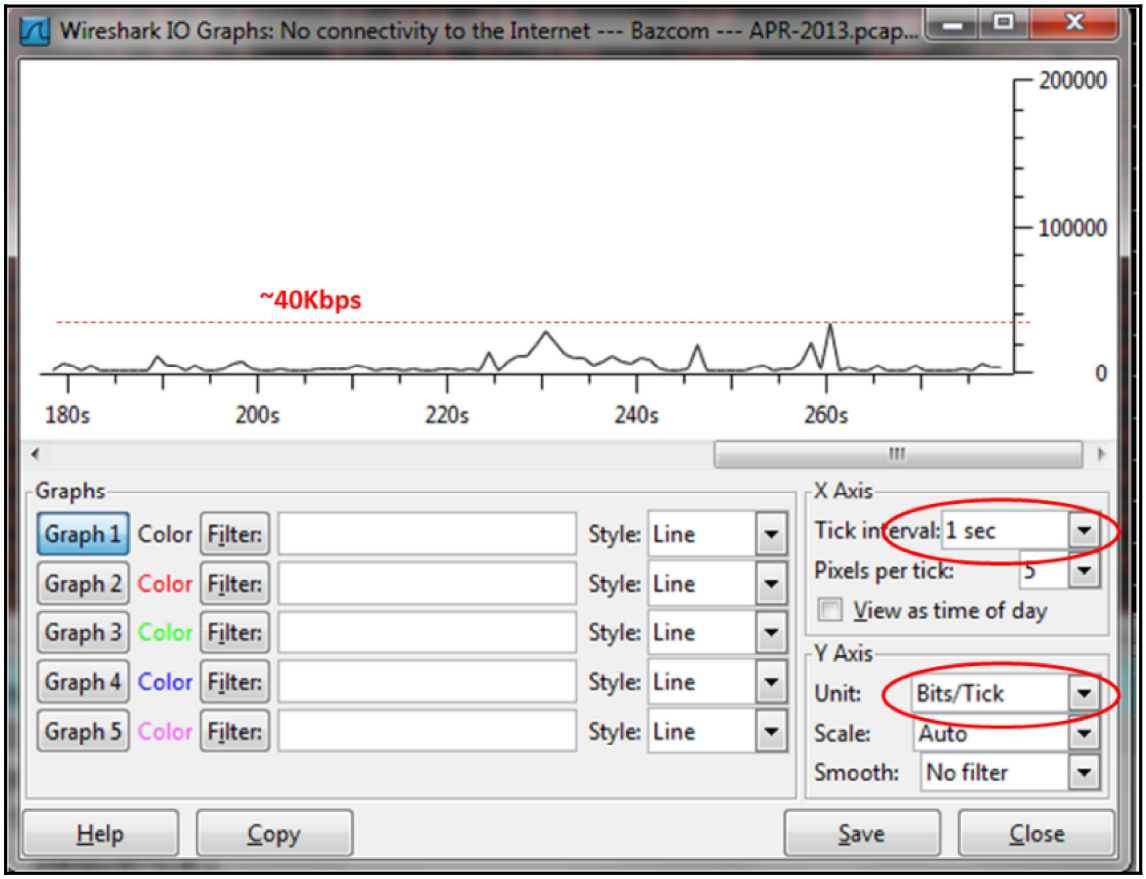

Client:
10.0.0.7
Server:
88.221.152.170
SYN, SEQ=0, WS=8192
SYN/ACK, SEQ=0/ACK=1, WS=14600
ACK, SEQ=1/ACK=1, WS=66792
In TCP header:
SYN/ACK – TCP flags
SEQ – Sequence number
ACK – Acknowledge number
WS – TCP Window Size
In TCP Header Options:
MSS – Maximum Segment Size
WS – Window Size (Factor)
SACK_PERM – Selective ACK Permitted

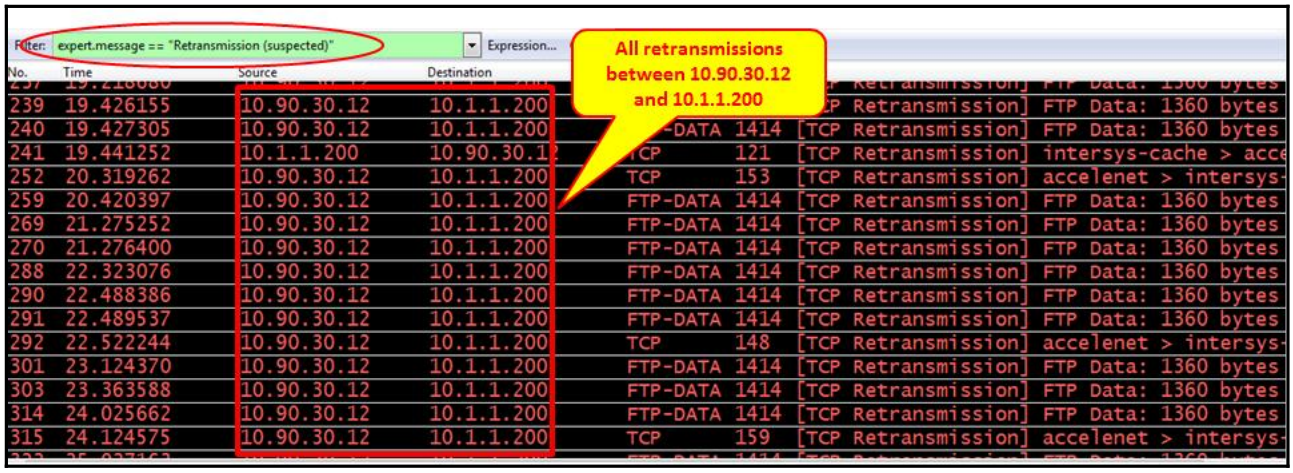

Time
10.0.0.9
10.0.0.1
Comment
2.428838 44913 → 22 [SYN] Seq=0 Win=29200 Len=0 22 TCP: 44913 → 22 [SYN] Seq=0 Win=29200 Len...
2.430964 44913 ← 22 [SYN, ACK] Seq=0 Ack=1 Win=28... 22 TCP: 22 → 44913 [SYN, ACK] Seq=0 Ack=1 Win...
2.432362 44913 → 22 [ACK] Seq=1 Ack=1 Win=29248 L... 22 TCP: 44913 → 22 [ACK] Seq=1 Ack=1 Win=292...
2.432744 44913 → Client: Protocol (SSH-2.0-OpenSSH_6.6.1p1 U... 22 SSHv2: Client: Protocol (SSH-2.0-OpenSSH_6.6...
2.434569 44913 ← 22 [ACK] Seq=1 Ack=44 Win=29184... 22 TCP: 22 → 44913 [ACK] Seq=1 Ack=44 Win=29...
2.442603 44913 ← Server: Protocol (SSH-2.0-OpenSSH_6.6.1p1 U... 22 SSHv2: Server: Protocol (SSH-2.0-OpenSSH_6....
2.443392 44913 ← 22 [ACK] Seq=44 Ack=44 Win=2918... 22 TCP: 22 → 44913 [ACK] Seq=44 Ack=44 Win=2...
2.533971 44913 → 44913 → 22 [ACK] Seq=44 Ack=44 Win=292... 22 TCP: 44913 → 22 [ACK] Seq=44 Ack=44 Win=2...
2.538982 44913 → 44913 → 22 [ACK] Seq=44 Ack=1492 Win=32... 22 TCP: 44913 → 22 [ACK] Seq=44 Ack=1492 Win...
2.543996 44913 → 44913 → 22 [ACK] Seq=44 Ack=1492 Win=32... 22 TCP: 44913 → 22 [ACK] Seq=44 Ack=1492 Win...
2.664975 44913 → Client: Key Exchange Init 22 SSHv2: Client: Key Exchange Init
2.666073 44913 ← Server: Key Exchange Init 22 SSHv2: Server: Key Exchange Init
2.732973 44913 → [TCP Retransmission] 44913 → 22 [PSH, ACK]... 22 TCP: [TCP Retransmission] 44913 → 22 [PSH, A...
2.734111 44913 ← 22 → 44913 [ACK] Seq=1692 Ack=1492 Win=... 22 TCP: 22 → 44913 [ACK] Seq=1692 Ack=1492 W...
2.780015 44913 → [TCP Spurious Retransmission] 44913 → 22 [... 22 TCP: [TCP Spurious Retransmission] 44913 → 2...
2.787066 44913 ← 22 → 44913 [ACK] Seq=1692 Ack=2012 Win=... 22 TCP: 22 → 44913 [ACK] Seq=1692 Ack=2012 W...
2.912079 44913 → 44913 → 22 [ACK] Seq=2012 Ack=1692 Win=... 22 TCP: 44913 → 22 [ACK] Seq=2012 Ack=1692 W...

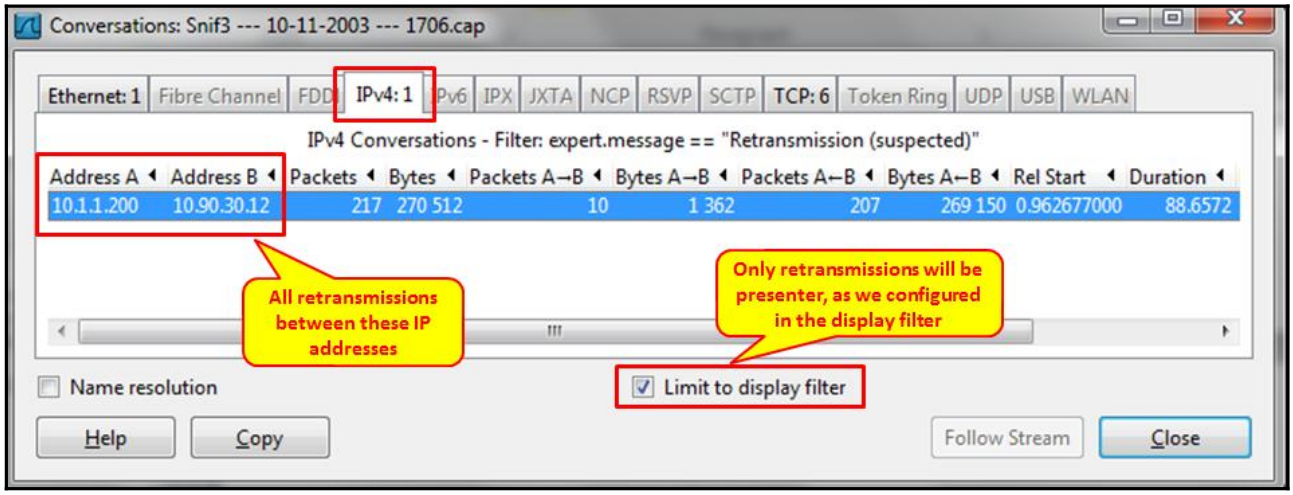

▶ Frame 2: 58 bytes on wire (464 bits), 58 bytes captured (464 bits)
▶ Ethernet II, Src: fa:16:3e:6e:ee:87 (fa:16:3e:6e:ee:87), Dst: fa:16:3e:d6:12:52 (fa:16:3e:d6:12:52)
▶ Internet Protocol Version 4, Src: 10.0.128.1, Dst: 10.1.3.3
▼ Transmission Control Protocol, Src Port: 31245, Dst Port: 23, Seq: 0, Len: 0
Source Port: 31245
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Relative Sequence number set to 0
Acknowledgment number: 0
0110 .... = Header Length: 24 bytes (6)
▶ Flags: 0x002 (SYN)
Window size value: 4128
[Calculated window size: 4128]
Checksum: 0xbf83 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
▶ Options: (4 bytes), Maximum segment size
▶ [Timestamps]

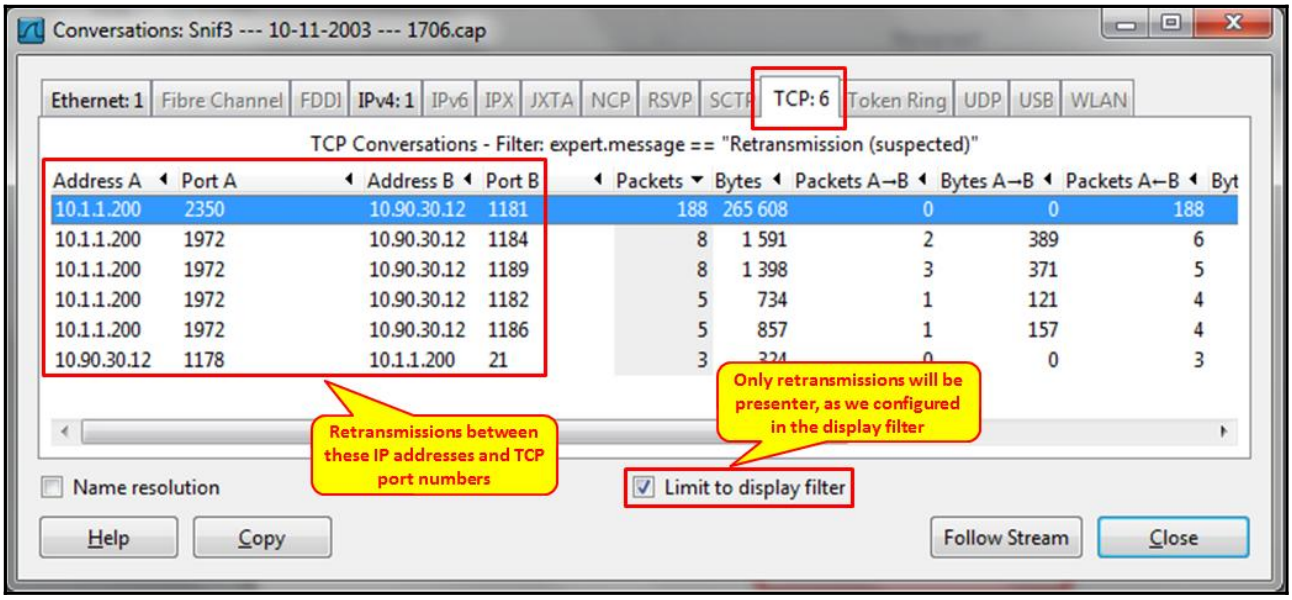

Wireshark · Preferences
STANAG 506...
StarTeam
STP
STT
STUN
SUA
SV
SYNC
SYNCHROPH...
Synergy
Syslog
T.38
TACACS
TACACS+
TALI
TAPA
TCAP
TCP
TCPENCAP
TCPROS
TDMoE
Transmission Control Protocol
Show TCP summary in protocol tree
Validate the TCP checksum if possible
Allow subdissector to reassemble TCP streams
Analyze TCP sequence numbers
Relative sequence numbers
Disable this option
Scaling factor to use when not available from capture
0 (no scaling)
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
Help
Cancel
OK

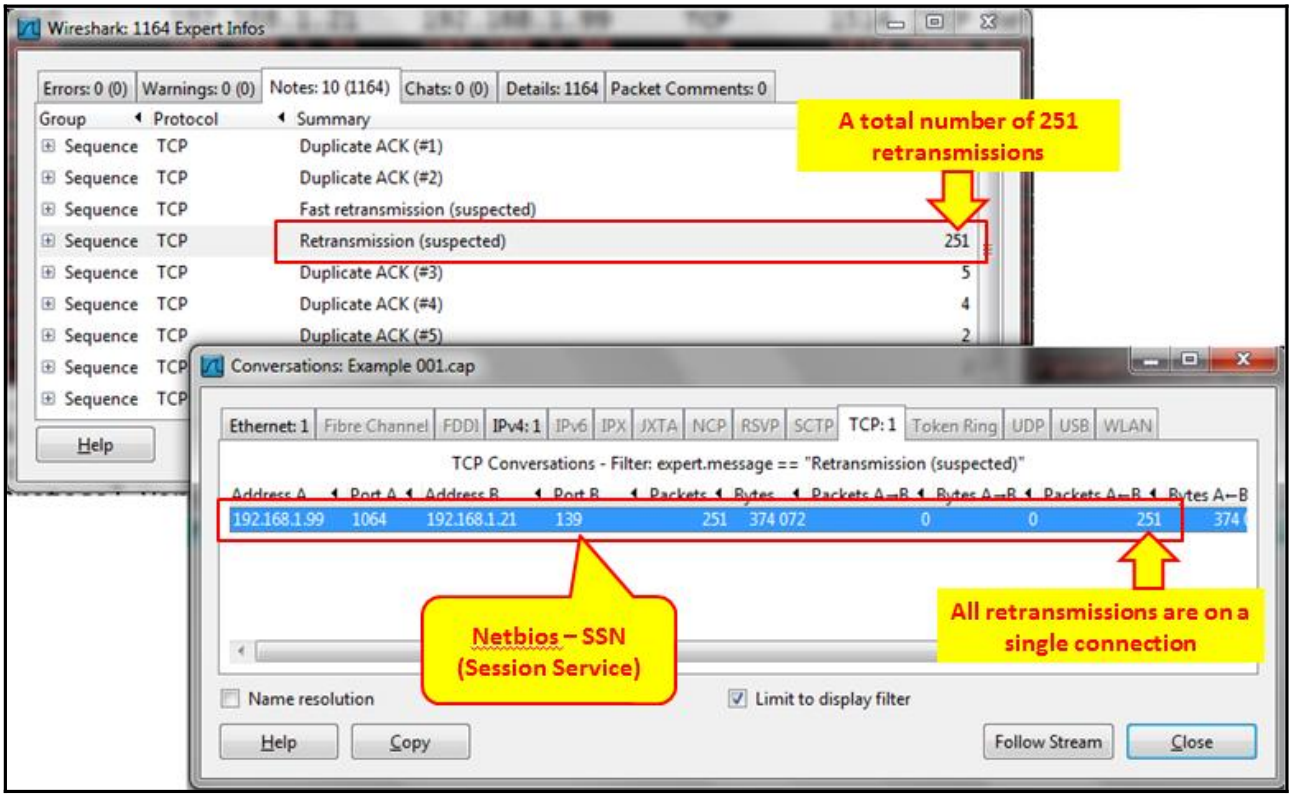

Filter: expert.message == "Retransmission (suspected)"
Save
Various destination addresses
Retransmissions
No. Time Source Destination Protocol Length Info
96 29.203230000 10.0.0.5 212.199.184.51 HTTP 366 [TCP Retransmission] GET /iefilter.html HTTP/
98 29.312500000 10.0.0.5 94.127.73.180 TCP 783 [TCP Retransmission] 55317 > http [PSH, ACK]
99 29.343596000 10.0.0.5 77.234.43.92 TCP 638 [TCP Retransmission] 55310 > http [PSH, ACK]
100 29.390393000 10.0.0.5 81.218.31.136 HTTP 491 [TCP Retransmission] GET /24x24/30.png HTTP/1
101 29.390393000 10.0.0.5 108.168.157.82 TCP 1506 [TCP Retransmission] 55326 > http [ACK] Seq=1
103 29.437199000 10.0.0.5 74.125.232.145 TCP 1070 [TCP Retransmission] 55320 > http [PSH, ACK]
106 29.530780000 10.0.0.5 74.125.232.145 TCP 1071 [TCP Retransmission] 55321 > http [PSH, ACK]
110 29.811579000 10.0.0.5 212.199.184.51 HTTP 366 [TCP Retransmission] GET /iefilter.html HTTP/
114 30.513564000 10.0.0.5 94.127.73.180 TCP 590 [TCP Retransmission] [TCP segment of a reasse
115 30.544753000 10.0.0.5 77.234.43.92 TCP 590 [TCP Retransmission] [TCP segment of a reasse
116 30.591557000 10.0.0.5 81.218.31.136 HTTP [TCP Retransmission] GET /24x24/30.png HTTP/1
117 30.638349000 10.0.0.5 74.125.232.145 TCP ransmission] [TCP segment of a reasse
118 30.638366000 10.0.0.5 108.168.157.82 TCP ransmission] 55326 > http [ACK] Seq=1
121 30.731954000 10.0.0.5 74.125.232.145 TCP ransmission] [TCP segment of a reasse
125 31.012738000 10.0.0.5 212.199.184.51 HTTP 366 [TCP Retransmission] GET /iefilter.html HTTP/
158 31.387223000 10.0.0.5 81.218.31.136 HTTP 489 [TCP Retransmission] GET /shadow.png HTTP/1.1
159 31.387356000 10.0.0.5 81.218.31.136 HTTP 503 [TCP Retransmission] GET /save-center rollove
All retransmissions to port 80 (HTTP)

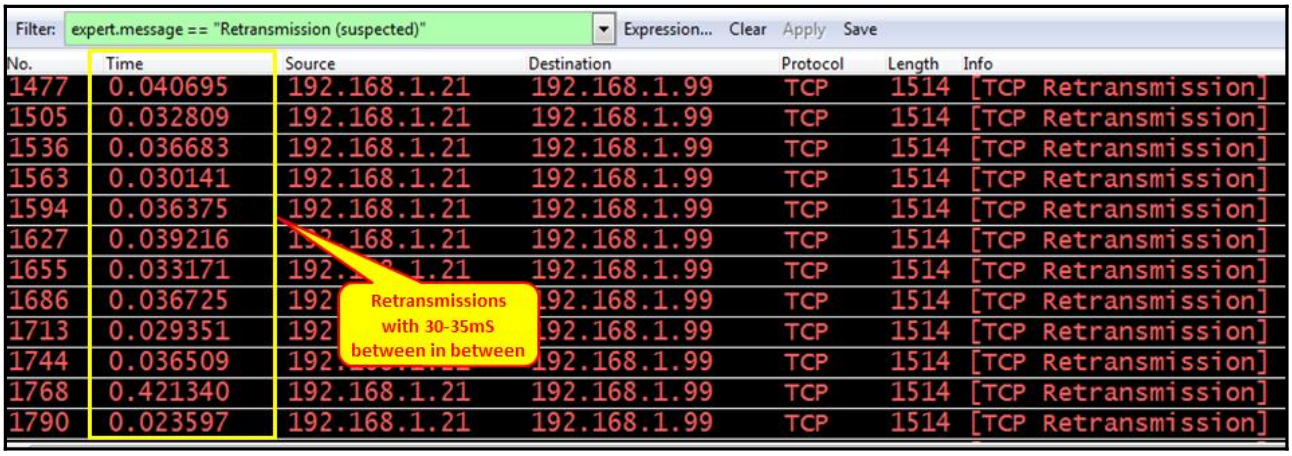

Wireshark IO Graphs: No connectivity to the Internet --- Bazcom --- APR-2013.pcap...
200000
100000
0
~40Kbps
180s
200s
220s
240s
260s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Bits/Tick
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close

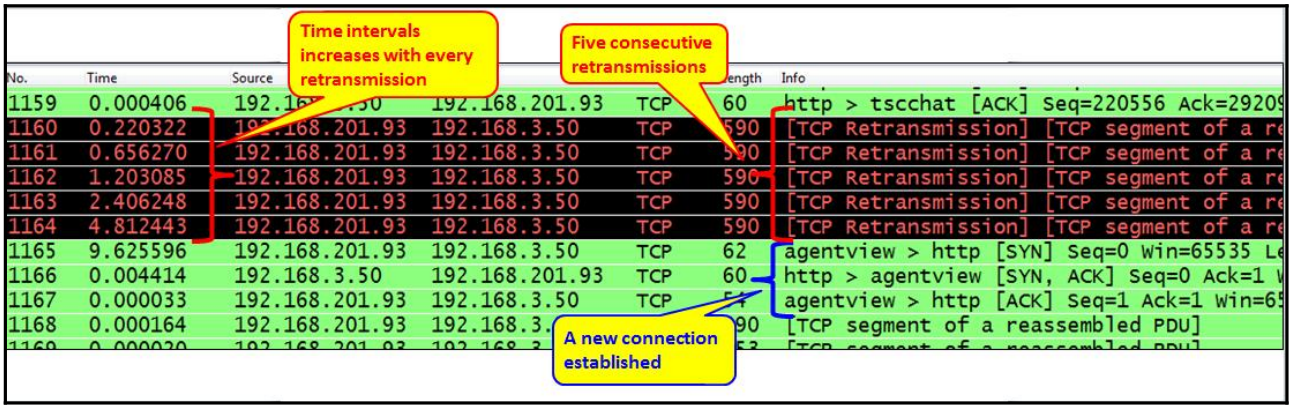

Filter: expert.message == "Retransmission (suspected)"
Expression...
All retransmissions between 10.90.30.12 and 10.1.1.200
No. Time Source Destination
239 19.426155 10.90.30.12 10.1.1.200 Retransmission] FTP Data: 1360 bytes
240 19.427305 10.90.30.12 10.1.1.200 -DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
241 19.441252 10.1.1.200 10.90.30.1 TCP 121 [TCP Retransmission] intersys-cache > acce
252 20.319262 10.90.30.12 10.1.1.200 TCP 153 [TCP Retransmission] accelenet > intersys-
259 20.420397 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
269 21.275252 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
270 21.276400 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
288 22.323076 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
290 22.488386 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
291 22.489537 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
292 22.522244 10.90.30.12 10.1.1.200 TCP 148 [TCP Retransmission] accelenet > intersys-
301 23.124370 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
303 23.363588 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
314 24.025662 10.90.30.12 10.1.1.200 FTP-DATA 1414 [TCP Retransmission] FTP Data: 1360 bytes
315 24.124575 10.90.30.12 10.1.1.200 TCP 159 [TCP Retransmission] accelenet > intersys-

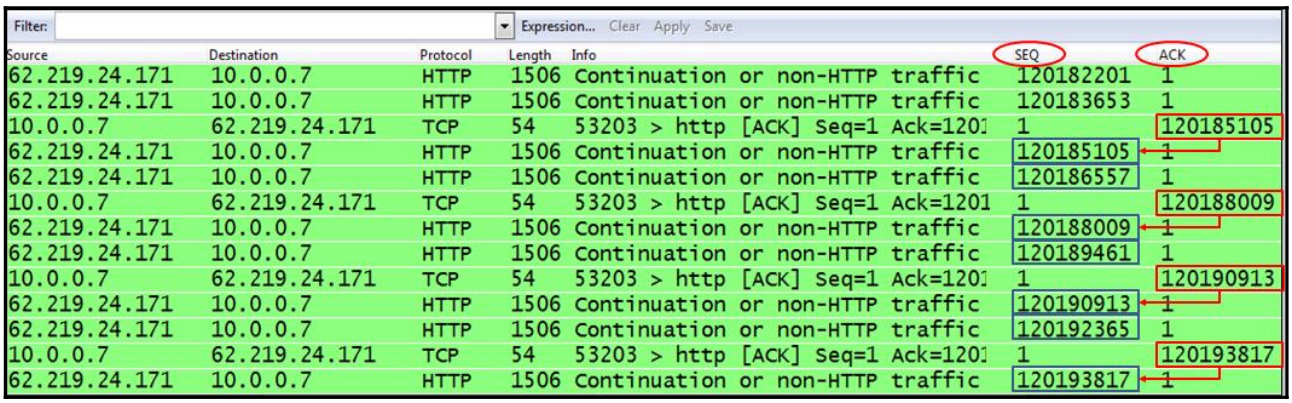

Conversations: Snif3 --- 10-11-2003 --- 1706.cap
Ethernet: 1 Fibre Channel FDDI IPv4: 1 IPv6 IPX JXTA NCP RSVP SCTP TCP: 6 Token Ring UDP USB WLAN
IPv4 Conversations - Filter: expert.message == "Retransmission (suspected)"
Address A Address B Packets Bytes Packets A→B Bytes A→B Packets A←B Bytes A←B Rel Start Duration
10.1.1.200 10.90.30.12 217 270 512 10 1 362 207 269 150 0.962677000 88.6572
All retransmissions between these IP addresses
Only retransmissions will be presenter, as we configured in the display filter
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

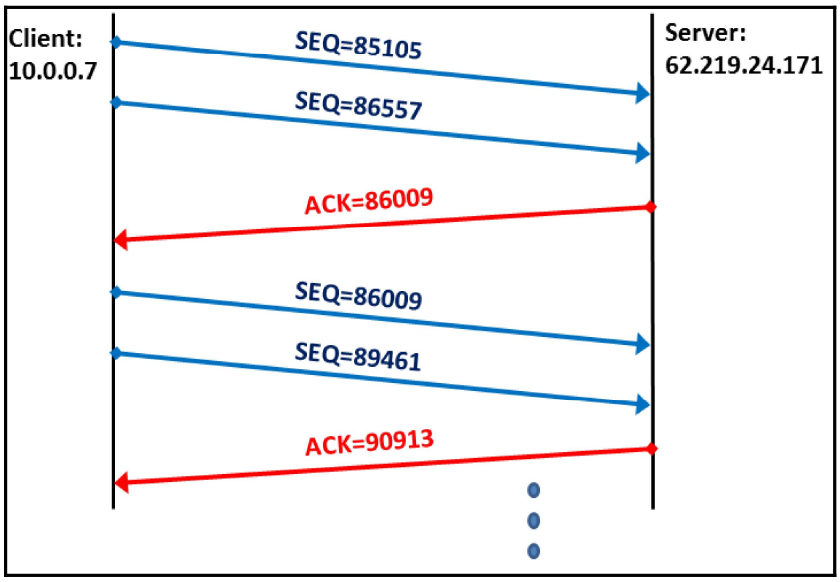

Conversations: Snif3 --- 10-11-2003 --- 1706.cap
Ethernet: 1
Fibre Channel
FDDI
IPv4: 1
IPv6
IPX
JXTA
NCP
RSVP
SCTP
TCP: 6
Token Ring
UDP
USB
WLAN
TCP Conversations - Filter: expert.message == "Retransmission (suspected)"
Address A
Port A
Address B
Port B
Packets
Bytes
Packets A→B
Bytes A→B
Packets A←B
Byt
10.1.1.200 2350 10.90.30.12 1181 188 265 608 0 0 188
10.1.1.200 1972 10.90.30.12 1184 8 1 591 2 389 6
10.1.1.200 1972 10.90.30.12 1189 8 1 398 3 371 5
10.1.1.200 1972 10.90.30.12 1182 5 734 1 121 4
10.1.1.200 1972 10.90.30.12 1186 5 857 1 157 4
10.90.30.12 1178 10.1.1.200 21 3 0 3
Retransmissions between these IP addresses and TCP port numbers
Only retransmissions will be presenter, as we configured in the display filter
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

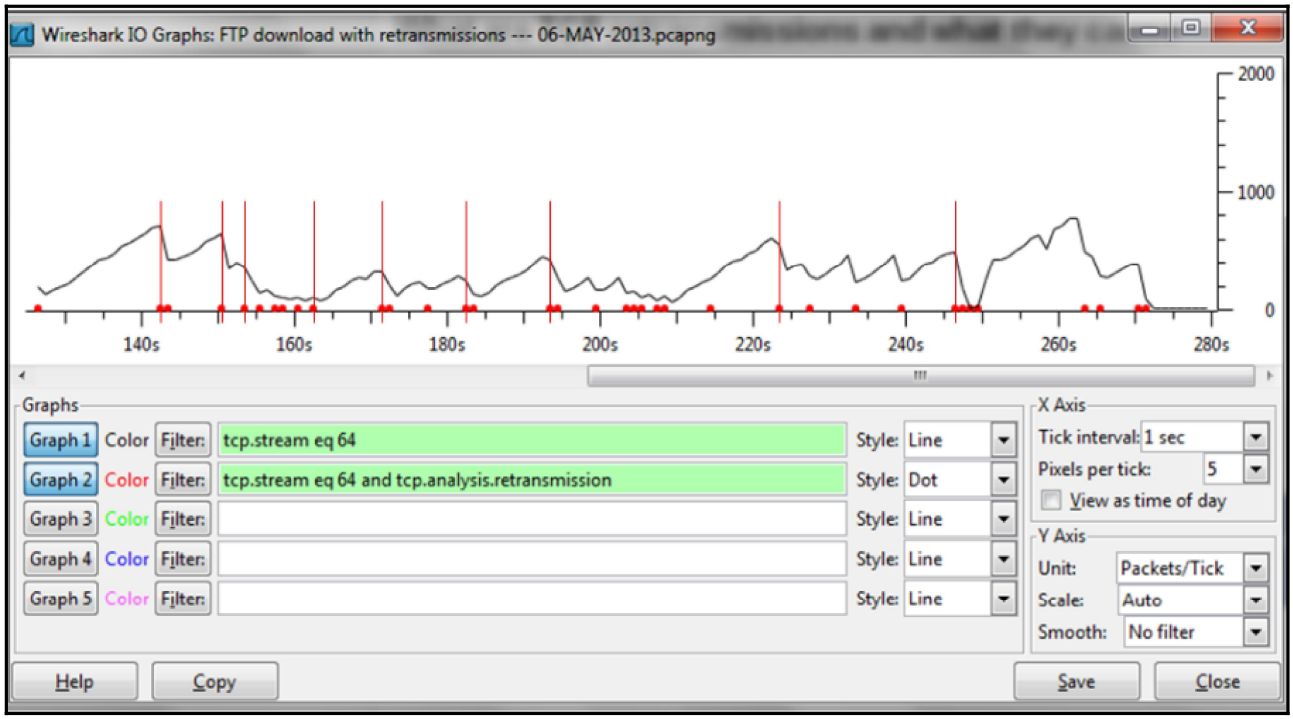

Wireshark: 1164 Expert Infos
Errors: 0 (0)
Warnings: 0 (0)
Notes: 10 (1164)
Chats: 0 (0)
Details: 1164
Packet Comments: 0
Group
Protocol
Summary
Sequence TCP Duplicate ACK (#1)
Sequence TCP Duplicate ACK (#2)
Sequence TCP Fast retransmission (suspected)
Sequence TCP Retransmission (suspected) 251
Sequence TCP Duplicate ACK (#3) 5
Sequence TCP Duplicate ACK (#4) 4
Sequence TCP Duplicate ACK (#5) 2
A total number of 251 retransmissions
Help
Conversations: Example 001.cap
Ethernet: 1
Fibre Channel
FDDI
IPv4: 1
IPv6
IPX
JXTA
NCP
RSVP
SCTP
TCP: 1
Token Ring
UDP
USB
WLAN
TCP Conversations - Filter: expert.message == "Retransmission (suspected)"
192.168.1.99 1064 192.168.1.21 139 251 374 072 0 0 251
Netbios – SSN (Session Service)
All retransmissions are on a single connection
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

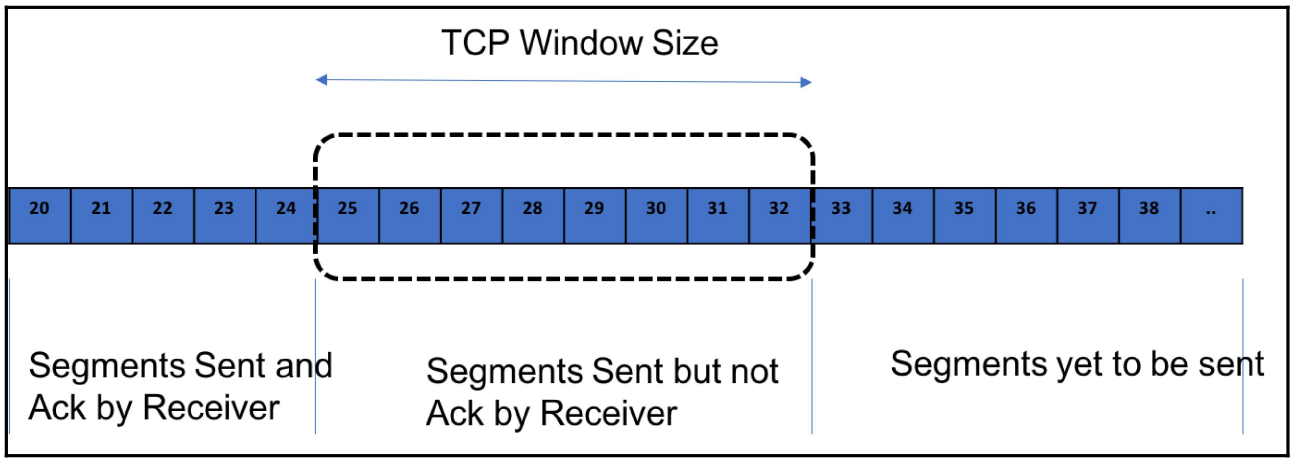

Filter: expert.message == "Retransmission (suspected)"
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
1477 0.040695 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1505 0.032809 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1536 0.036683 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1563 0.030141 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1594 0.036375 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1627 0.039216 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1655 0.033171 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1686 0.036725 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1713 0.029351 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1744 0.036509 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1768 0.421340 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
1790 0.023597 192.168.1.21 192.168.1.99 TCP 1514 [TCP Retransmission]
Retransmissions with 30-35mS between in between

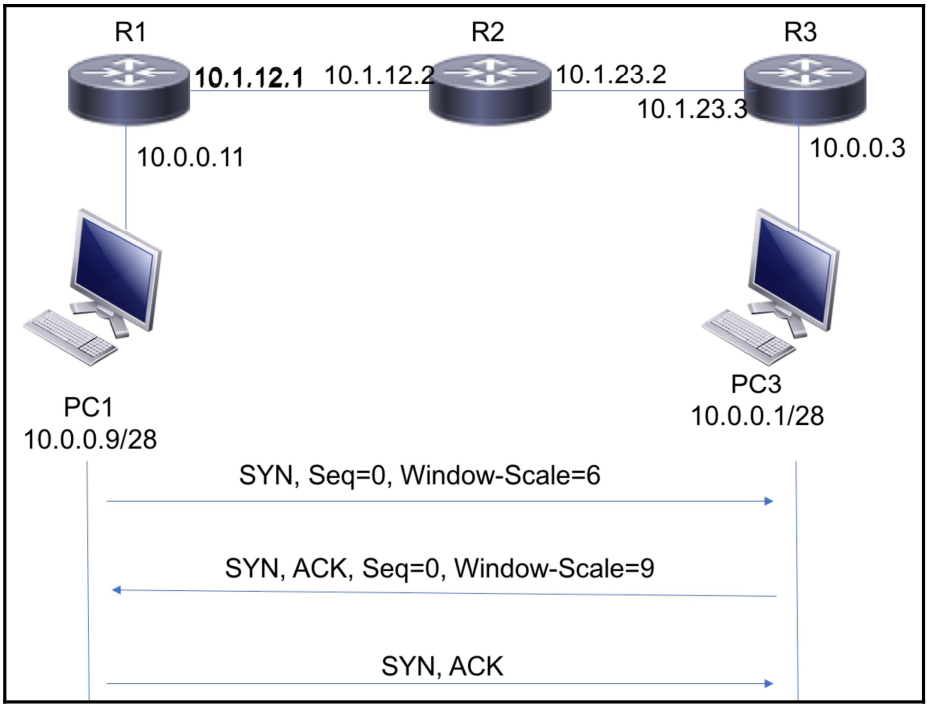

Time intervals increases with every retransmission
Five consecutive retransmissions
No. Time Source Destination Protocol Length Info
1159 0.000406 192.168.201.93 TCP 60 http > tscchat [ACK] Seq=220556 Ack=2920
1160 0.220322 192.168.201.93 192.168.3.50 TCP 590 [TCP Retransmission] [TCP segment of a re
1161 0.656270 192.168.201.93 192.168.3.50 TCP 590 [TCP Retransmission] [TCP segment of a re
1162 1.203085 192.168.201.93 192.168.3.50 TCP 590 [TCP Retransmission] [TCP segment of a re
1163 2.406248 192.168.201.93 192.168.3.50 TCP 590 [TCP Retransmission] [TCP segment of a re
1164 4.812443 192.168.201.93 192.168.3.50 TCP 590 [TCP Retransmission] [TCP segment of a re
1165 9.625596 192.168.201.93 192.168.3.50 TCP 62 agentview > http [SYN] Seq=0 Win=65535 Le
1166 0.004414 192.168.3.50 192.168.201.93 TCP 60 http > agentview [SYN, ACK] Seq=0 Ack=1 W
1167 0.000033 192.168.201.93 192.168.3.50 TCP agentview > http [ACK] Seq=1 Ack=1 Win=65
1168 0.000164 192.168.201.93 192.168.3. 90 [TCP segment of a reassembled PDU]
A new connection established


Filter:
Expression... Clear Apply Save
Source Destination Protocol Length Info SEQ ACK
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120182201 1
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120183653 1
10.0.0.7 62.219.24.171 TCP 54 53203 > http [ACK] Seq=1 Ack=120 1 120185105
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120185105 1
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120186557 1
10.0.0.7 62.219.24.171 TCP 54 53203 > http [ACK] Seq=1 Ack=120 1 120188009
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120188009 1
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120189461 1
10.0.0.7 62.219.24.171 TCP 54 53203 > http [ACK] Seq=1 Ack=120 1 120190913
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120190913 1
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120192365 1
10.0.0.7 62.219.24.171 TCP 54 53203 > http [ACK] Seq=1 Ack=120 1 120193817
62.219.24.171 10.0.0.7 HTTP 1506 Continuation or non-HTTP traffic 120193817 1


Client:
10.0.0.7
Server:
62.219.24.171
SEQ=85105
SEQ=86557
ACK=86009
SEQ=86009
SEQ=89461
ACK=90913

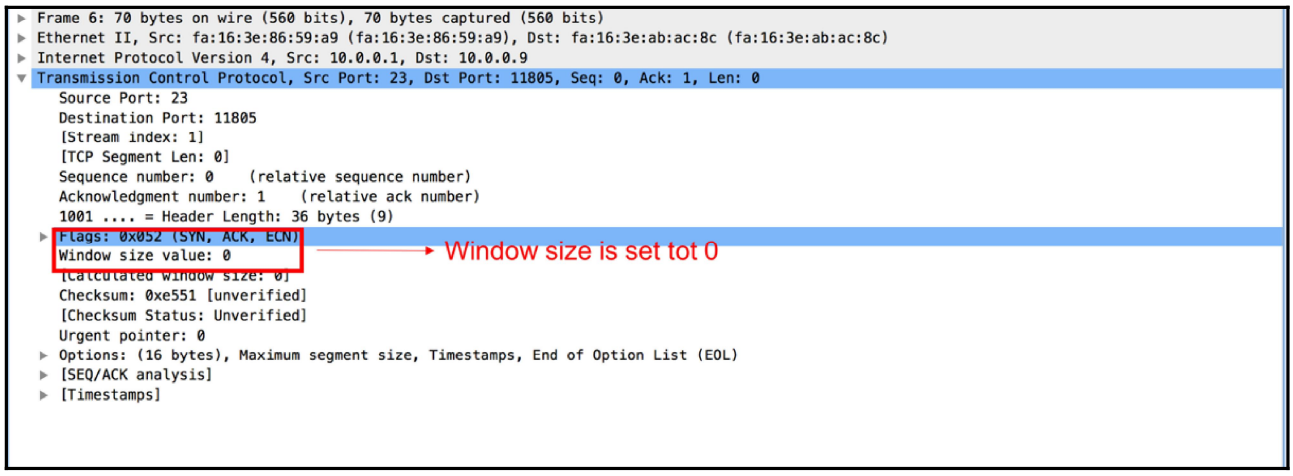

Wireshark IO Graphs: FTP download with retransmissions --- 06-MAY-2013.pcapng
2000
1000
0
140s
160s
180s
200s
220s
240s
260s
280s
Graphs
Graph 1 Color Filter: tcp.stream eq 64 Style: Line
Graph 2 Color Filter: tcp.stream eq 64 and tcp.analysis.retransmission Style: Dot
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close

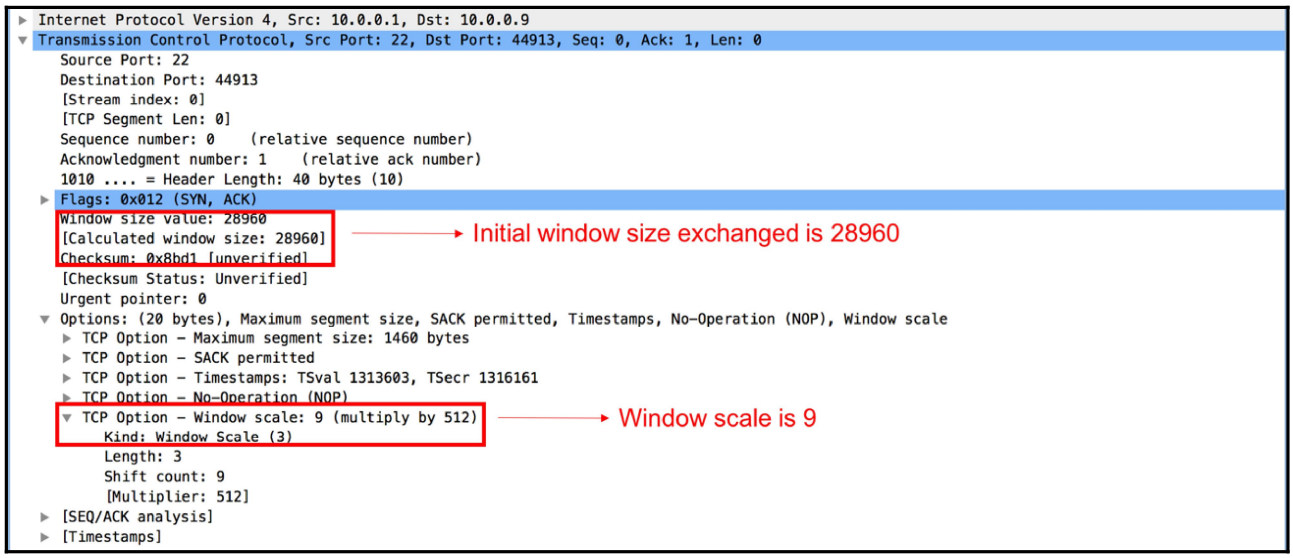




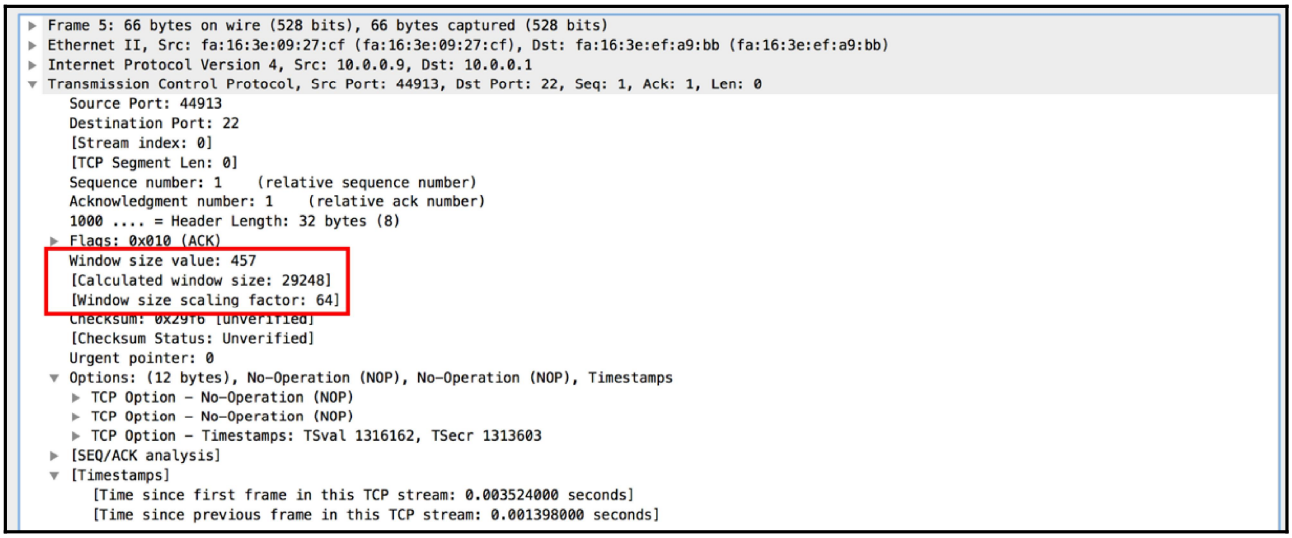
tcp.stream eq 1

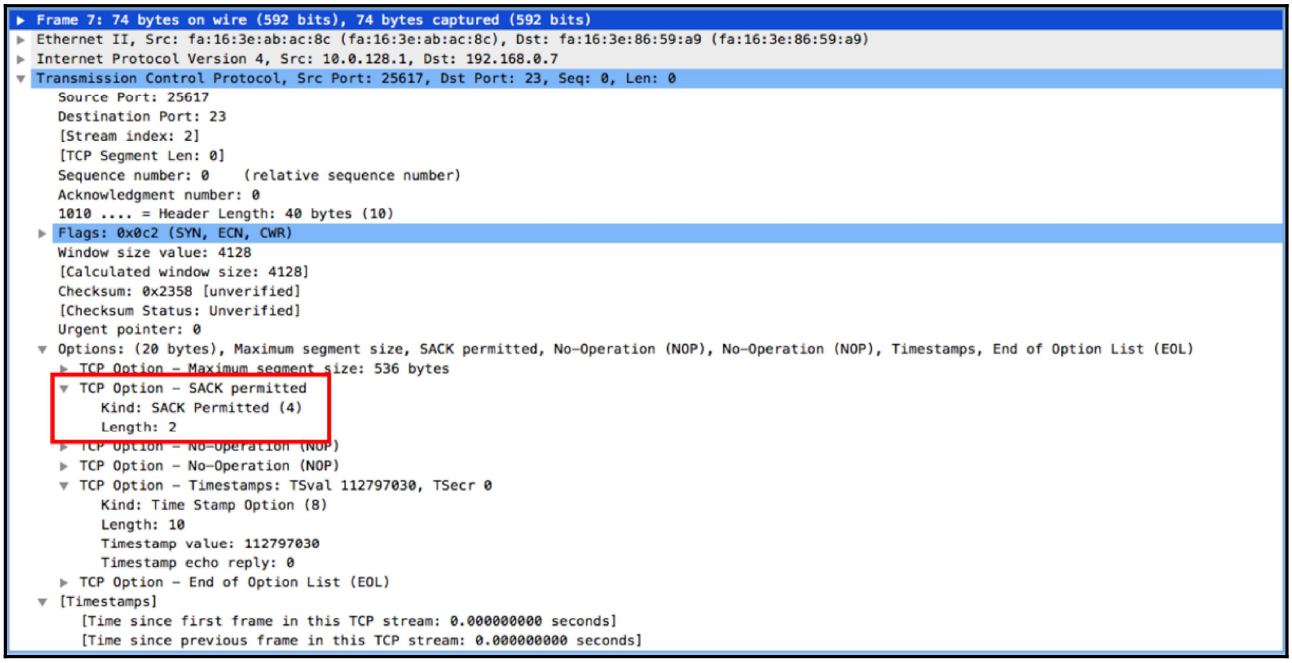
No.	Time	Source	Destination	Protocol	Length	Info
5	7.872718	10.0.0.9	10.0.0.1	TCP	70	11805 → 23 [SYN, ECN, CWR] Seq=0 Win=4128 Len=0 MSS=536 TSval=9468…
6	7.873586	10.0.0.1	10.0.0.9	TCP	70	23 → 11805 [SYN, ACK, ECN] Seq=0 Ack=1 Win=0 Len=0 MSS=536 TSval=9…
7	7.874366	10.0.0.9	10.0.0.1	TCP	66	11805 → 23 [ACK] Seq=1 Ack=1 Win=66048 Len=0 TSval=94685668 TSecr=…
8	7.875161	10.0.0.1	10.0.0.9	TELNET	78	[TCP ZeroWindow] Telnet Data ...
9	7.875467	10.0.0.1	10.0.0.9	TELNET	108	[TCP ZeroWindow] Telnet Data ...
10	7.876077	10.0.0.9	10.0.0.1	TCP	66	11805 → 23 [ACK] Seq=1 Ack=55 Win=65184 Len=0 TSval=94685669 TSecr…
13	10.500097	10.0.0.9	10.0.0.1	TELNET	67	[TCP ZeroWindowProbe] Telnet Data ...[Malformed Packet]
14	10.500778	10.0.0.1	10.0.0.9	TCP	66	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 23 → 11805 [ACK] Seq=55 …
15	15.750401	10.0.0.9	10.0.0.1	TELNET	67	[TCP ZeroWindowProbe] Telnet Data ...[Malformed Packet]
16	15.751430	10.0.0.1	10.0.0.9	TCP	66	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 23 → 11805 [ACK] Seq=55 …
21	26.250795	10.0.0.9	10.0.0.1	TELNET	67	[TCP ZeroWindowProbe] Telnet Data ...[Malformed Packet]
22	26.251537	10.0.0.1	10.0.0.9	TCP	66	[TCP ZeroWindowProbeAck] [TCP ZeroWindow] 23 → 11805 [ACK] Seq=55 …
29	38.235254	10.0.0.1	10.0.0.9	TELNET	109	[TCP ZeroWindow] Telnet Data ...
30	38.436371	10.0.0.9	10.0.0.1	TCP	66	11805 → 23 [ACK, CWR] Seq=1 Ack=98 Win=64496 Len=0 TSval=94716228 …
67	47.251752	10.0.0.9	10.0.0.1	TELNET	67	[TCP ZeroWindowProbe] Telnet Data ...[Malformed Packet]

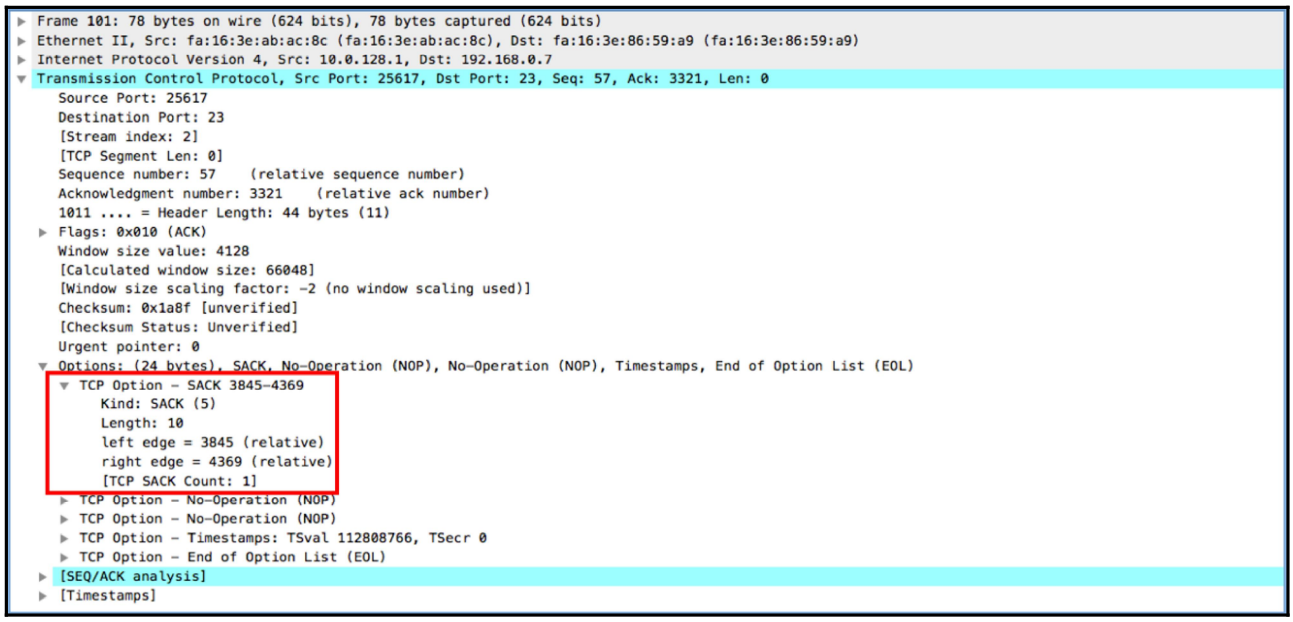


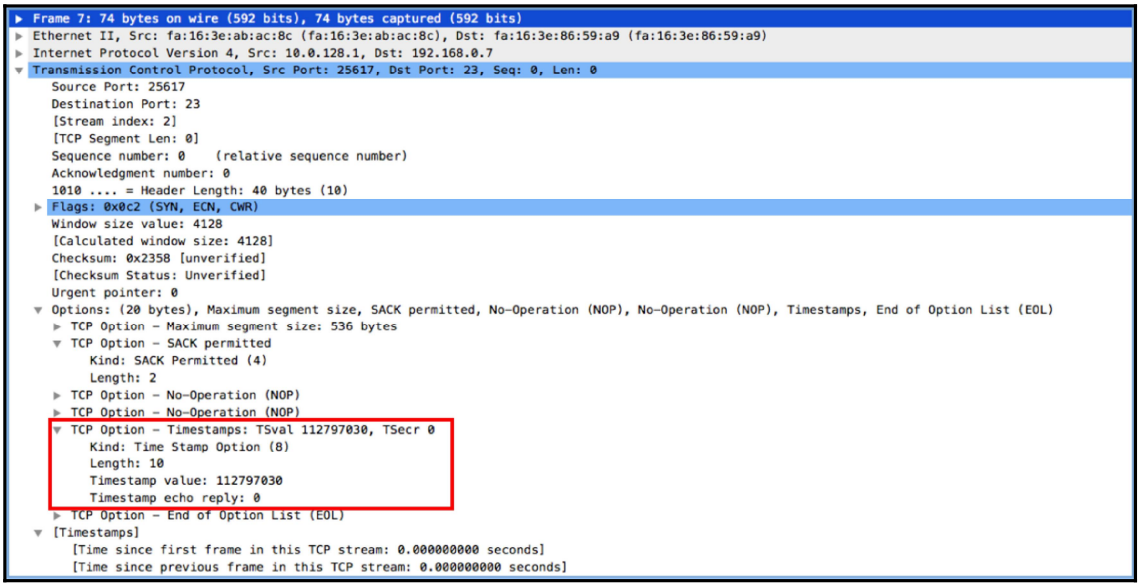


Sliding Window [Bytes] = Window * (2**Scale)

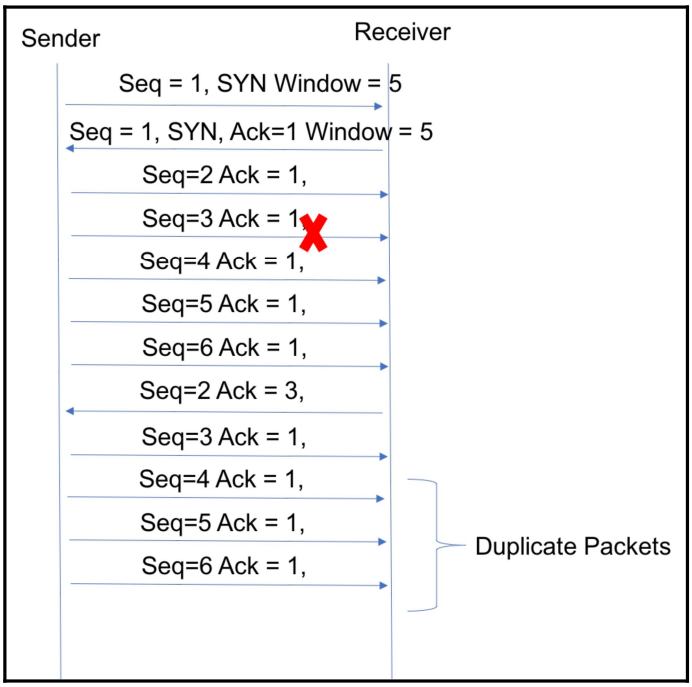

Frame 5: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
Ethernet II, Src: fa:16:3e:09:27:cf (fa:16:3e:09:27:cf), Dst: fa:16:3e:ef:a9:bb (fa:16:3e:ef:a9:bb)
Internet Protocol Version 4, Src: 10.0.0.9, Dst: 10.0.0.1
Transmission Control Protocol, Src Port: 44913, Dst Port: 22, Seq: 1, Ack: 1, Len: 0
Source Port: 44913
Destination Port: 22
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
1000 .... = Header Length: 32 bytes (8)
Flags: 0x010 (ACK)
Window size value: 457
[Calculated window size: 29248]
[Window size scaling factor: 64]
Checksum: 0x2916 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - Timestamps: TSval 1316162, TSecr 1313603
[SEQ/ACK analysis]
[Timestamps]
[Time since first frame in this TCP stream: 0.003524000 seconds]
[Time since previous frame in this TCP stream: 0.001398000 seconds]

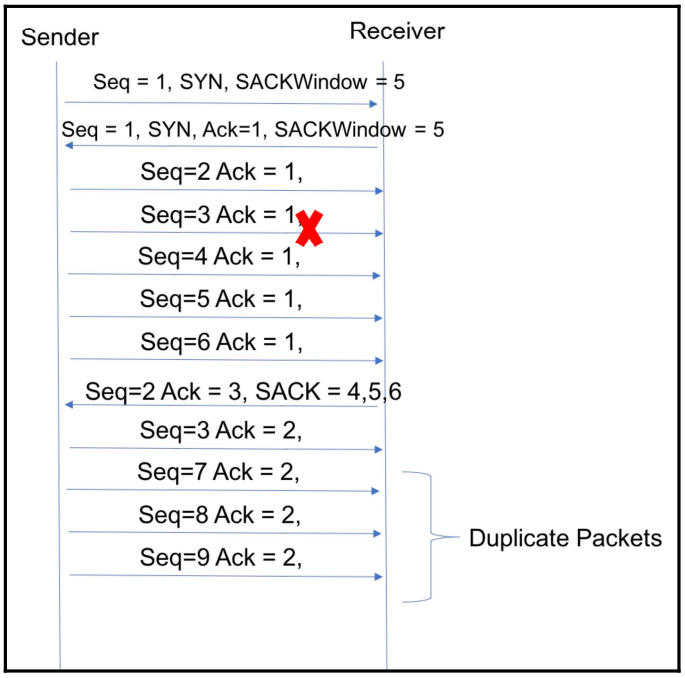

Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: fa:16:3e:ab:ac:8c (fa:16:3e:ab:ac:8c), Dst: fa:16:3e:86:59:a9 (fa:16:3e:86:59:a9)
Internet Protocol Version 4, Src: 10.0.128.1, Dst: 192.168.0.7
Transmission Control Protocol, Src Port: 25617, Dst Port: 23, Seq: 0, Len: 0
Source Port: 25617
Destination Port: 23
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x0c2 (SYN, ECN, CWR)
Window size value: 4128
[Calculated window size: 4128]
Checksum: 0x2358 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, No-Operation (NOP), No-Operation (NOP), Timestamps, End of Option List (EOL)
TCP Option - Maximum segment size: 536 bytes
TCP Option - SACK permitted
Kind: SACK Permitted (4)
Length: 2
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - Timestamps: TSval 112797030, TSecr 0
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 112797030
Timestamp echo reply: 0
TCP Option - End of Option List (EOL)
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

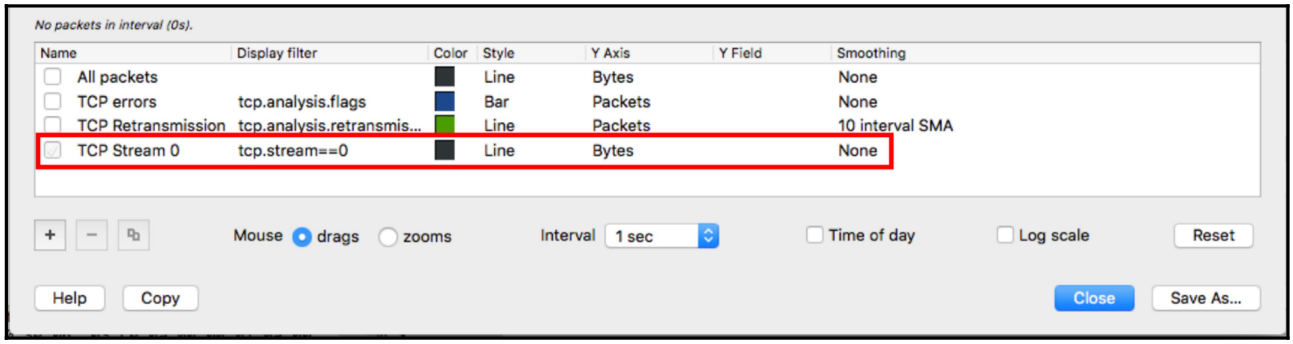

Frame 101: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: fa:16:3e:ab:ac:8c (fa:16:3e:ab:ac:8c), Dst: fa:16:3e:86:59:a9 (fa:16:3e:86:59:a9)
Internet Protocol Version 4, Src: 10.0.128.1, Dst: 192.168.0.7
Transmission Control Protocol, Src Port: 25617, Dst Port: 23, Seq: 57, Ack: 3321, Len: 0
Source Port: 25617
Destination Port: 23
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 57 (relative sequence number)
Acknowledgment number: 3321 (relative ack number)
1011 .... = Header Length: 44 bytes (11)
Flags: 0x010 (ACK)
Window size value: 4128
[Calculated window size: 66048]
[Window size scaling factor: -2 (no window scaling used)]
Checksum: 0x1a8f [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (24 bytes), SACK, No-Operation (NOP), No-Operation (NOP), Timestamps, End of Option List (EOL)
TCP Option - SACK 3845-4369
Kind: SACK (5)
Length: 10
left edge = 3845 (relative)
right edge = 4369 (relative)
[TCP SACK Count: 1]
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - Timestamps: TSval 112808766, TSecr 0
TCP Option - End of Option List (EOL)
[SEQ/ACK analysis]
[Timestamps]


Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: fa:16:3e:ab:ac:8c (fa:16:3e:ab:ac:8c), Dst: fa:16:3e:86:59:a9 (fa:16:3e:86:59:a9)
Internet Protocol Version 4, Src: 10.0.128.1, Dst: 192.168.0.7
Transmission Control Protocol, Src Port: 25617, Dst Port: 23, Seq: 0, Len: 0
Source Port: 25617
Destination Port: 23
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x0c2 (SYN, ECN, CWR)
Window size value: 4128
[Calculated window size: 4128]
Checksum: 0x2358 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (20 bytes), Maximum segment size, SACK permitted, No-Operation (NOP), No-Operation (NOP), Timestamps, End of Option List (EOL)
TCP Option - Maximum segment size: 536 bytes
TCP Option - SACK permitted
Kind: SACK Permitted (4)
Length: 2
TCP Option - No-Operation (NOP)
TCP Option - No-Operation (NOP)
TCP Option - Timestamps: TSval 112797030, TSecr 0
Kind: Time Stamp Option (8)
Length: 10
Timestamp value: 112797030
Timestamp echo reply: 0
TCP Option - End of Option List (EOL)
[Timestamps]
[Time since first frame in this TCP stream: 0.000000000 seconds]
[Time since previous frame in this TCP stream: 0.000000000 seconds]

```
▶ Frame 144: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
▶ Ethernet II, Src: fa:16:3e:ab:ac:8c (fa:16:3e:ab:ac:8c), Dst: fa:16:3e:86:59:a9 (fa:16:3e:86:59:a9)
▶ Internet Protocol Version 4, Src: 10.0.128.1, Dst: 192.168.0.7
▼ Transmission Control Protocol, Src Port: 25617, Dst Port: 23, Seq: 57, Ack: 7498, Len: 0
    Source Port: 25617
    Destination Port: 23
    [Stream index: 2]
    [TCP Segment Len: 0]
    Sequence number: 57    (relative sequence number)
    Acknowledgment number: 7498    (relative ack number)
    1011 .... = Header Length: 44 bytes (11)
  ▶ Flags: 0x010 (ACK)
    Window size value: 3966
    [Calculated window size: 63456]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0x8880 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ▼ Options: (24 bytes), SACK, No-Operation (NOP), No-Operation (NOP), Timestamps, End of Option List (EOL)
    ▶ TCP Option - SACK 7528-7536
    ▶ TCP Option - No-Operation (NOP)
    ▶ TCP Option - No-Operation (NOP)
    ▼ TCP Option - Timestamps: TSval 112816072, TSecr 112804954
        Kind: Time Stamp Option (8)
        Length: 10
        Timestamp value: 112816072
        Timestamp echo reply: 112804954
    ▶ TCP Option - End of Option List (EOL)
  ▶ [SEQ/ACK analysis]
  ▶ [Timestamps]
```



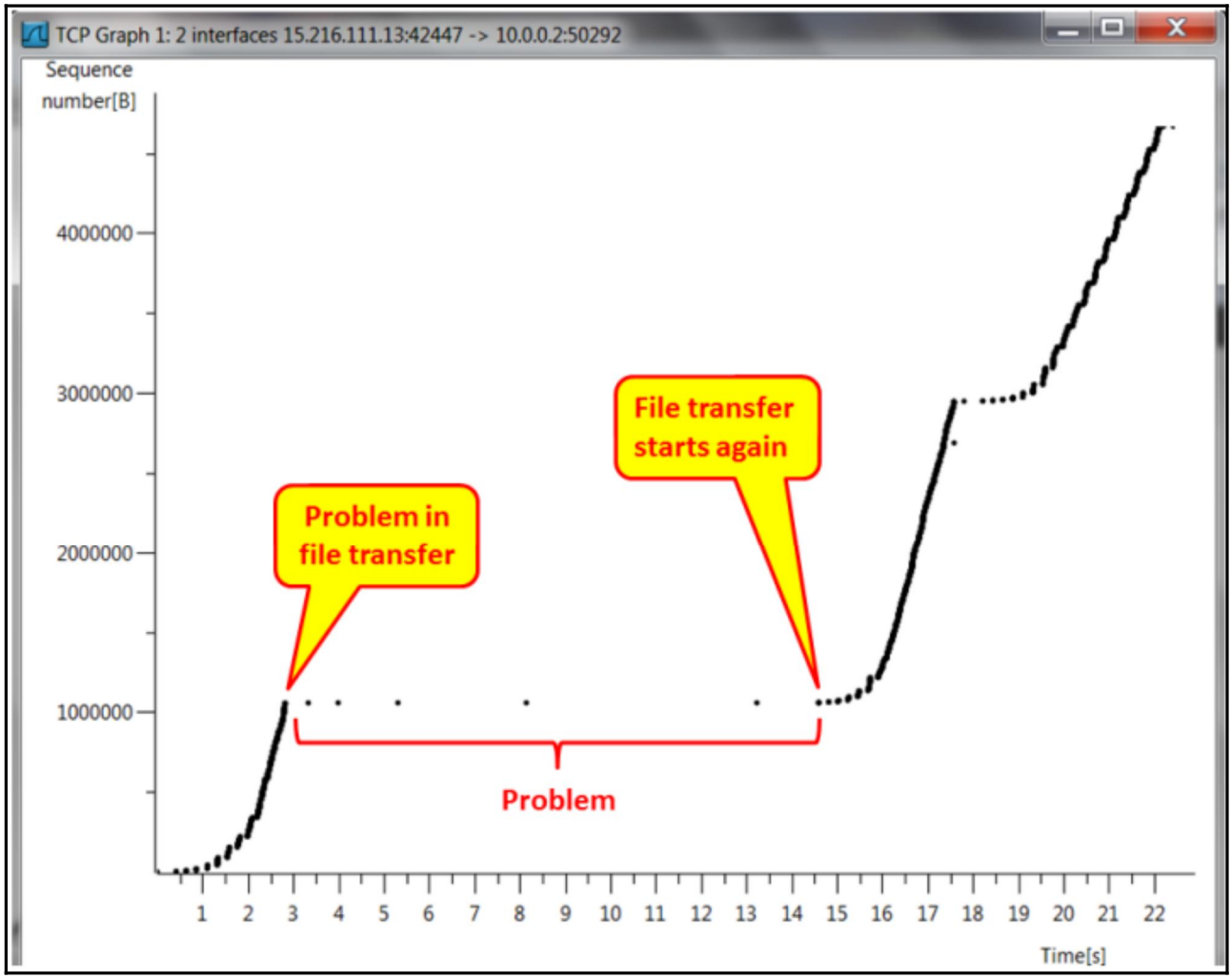

Sender
Receiver
Seq = 1, SYN, SACKWindow = 5
Seq = 1, SYN, Ack=1, SACKWindow = 5
Seq=2 Ack = 1,
Seq=3 Ack = 1,
Seq=4 Ack = 1,
Seq=5 Ack = 1,
Seq=6 Ack = 1,
Seq=2 Ack = 3, SACK = 4,5,6
Seq=3 Ack = 2,
Seq=7 Ack = 2,
Seq=8 Ack = 2,
Seq=9 Ack = 2,
Duplicate Packets

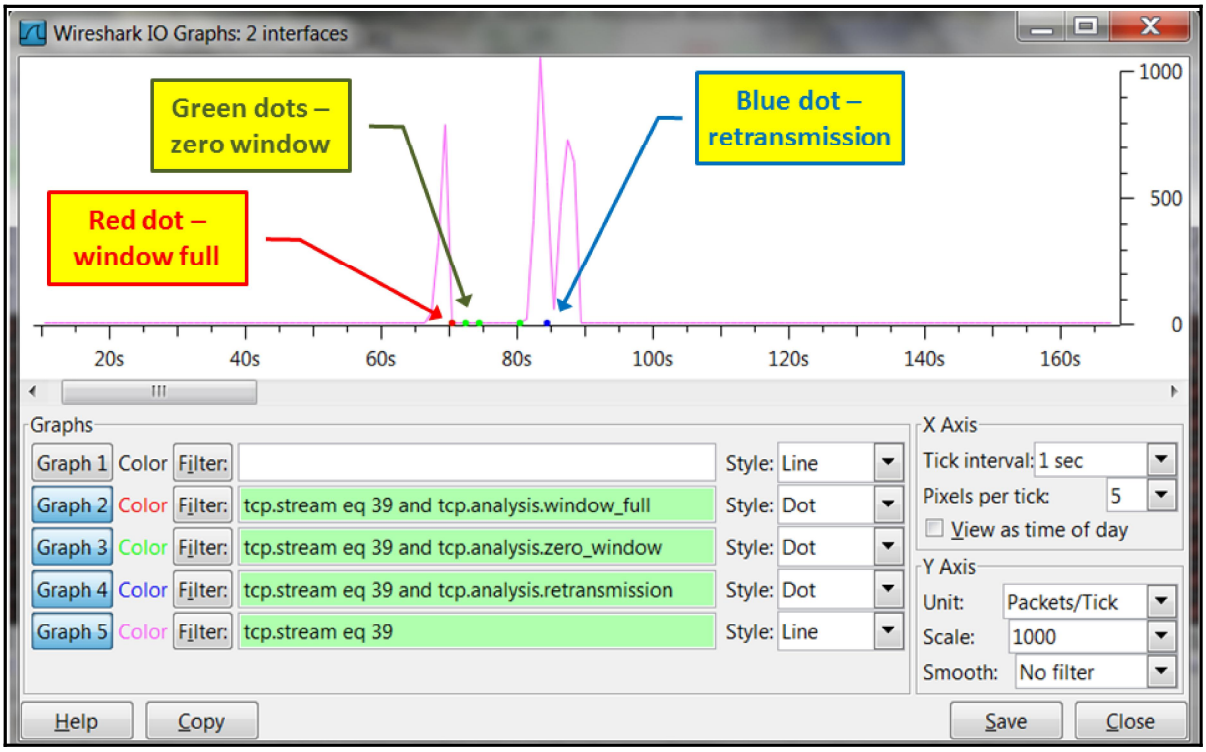

No packets in interval (0s).
Name
Display filter
Color
Style
Y Axis
Y Field
Smoothing
All packets
Line
Bytes
None
TCP errors
tcp.analysis.flags
Bar
Packets
None
TCP Retransmission
tcp.analysis.retransmis...
Line
Packets
10 interval SMA
TCP Stream 0
tcp.stream==0
Line
Bytes
None
Mouse
drags
zooms
Interval
1 sec
Time of day
Log scale
Reset
Help
Copy
Close
Save As...

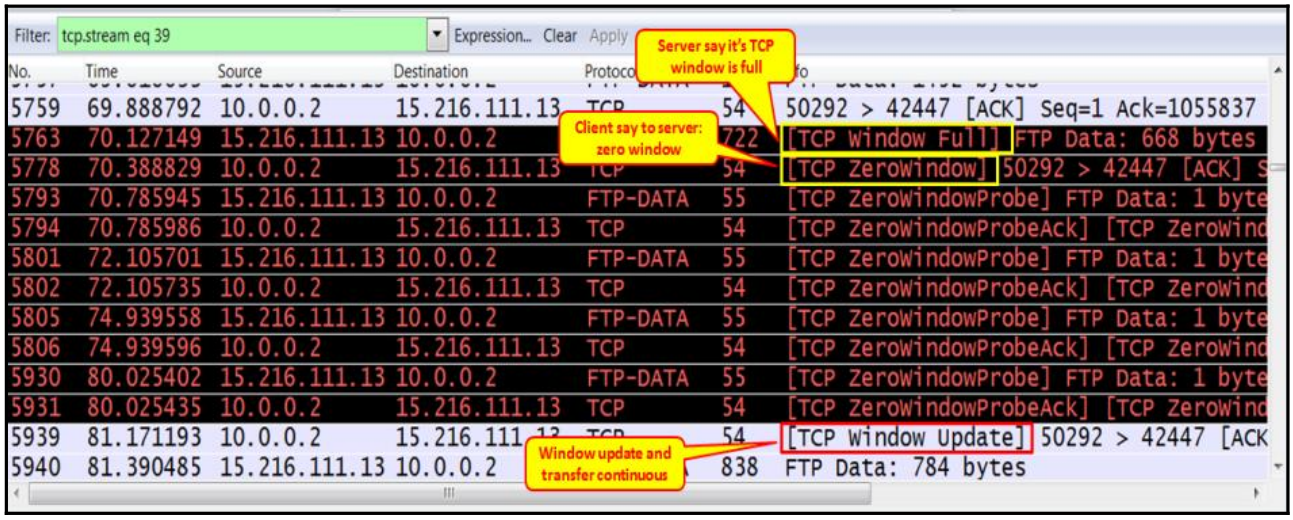
Severity	Summary	Group	Protocol	Cour
Error	Malformed Packet (Exception occurred)	Malformed	SSH	4
Warning	Previous segment(s) not captured (common at capture start)	Sequence	TCP	173
Note	This frame is a (suspected) retransmission	Sequence	TCP	209
Note	This frame is a (suspected) spurious retransmission	Sequence	TCP	1
Note	Duplicate ACK (#1)	Sequence	TCP	143
Note	Duplicate ACK (#2)	Sequence	TCP	101
Note	Duplicate ACK (#3)	Sequence	TCP	66
Note	Duplicate ACK (#4)	Sequence	TCP	32
Note	Duplicate ACK (#5)	Sequence	TCP	24
Note	Duplicate ACK (#6)	Sequence	TCP	20
Note	Duplicate ACK (#7)	Sequence	TCP	19
Note	Duplicate ACK (#8)	Sequence	TCP	16
Note	Duplicate ACK (#9)	Sequence	TCP	13
Note	Duplicate ACK (#10)	Sequence	TCP	12
Note	Duplicate ACK (#11)	Sequence	TCP	12
Note	Duplicate ACK (#12)	Sequence	TCP	12
Note	Duplicate ACK (#13)	Sequence	TCP	12
Note	Duplicate ACK (#14)	Sequence	TCP	12
Note	Duplicate ACK (#15)	Sequence	TCP	12
Note	Duplicate ACK (#16)	Sequence	TCP	12
Note	Duplicate ACK (#17)	Sequence	TCP	12
Note	Duplicate ACK (#18)	Sequence	TCP	12
Note	Duplicate ACK (#19)	Sequence	TCP	12
Note	Duplicate ACK (#20)	Sequence	TCP	12
Note	Duplicate ACK (#21)	Sequence	TCP	12
Note	Duplicate ACK (#22)	Sequence	TCP	12
Note	Duplicate ACK (#23)	Sequence	TCP	12
Note	Duplicate ACK (#24)	Sequence	TCP	12
Note	Duplicate ACK (#25)	Sequence	TCP	12
Note	Duplicate ACK (#26)	Sequence	TCP	12
Note	Duplicate ACK (#27)	Sequence	TCP	12
425	[TCP Dup ACK 363#27] 44913 → 22 [ACK] Seq=2724 Ack=22...			
871	[TCP Dup ACK 772#27] 44913 → 22 [ACK] Seq=2832 Ack=50...			
1204	[TCP Dup ACK 1146#27] 44913 → 22 [ACK] Seq=2904 Ack=7...			

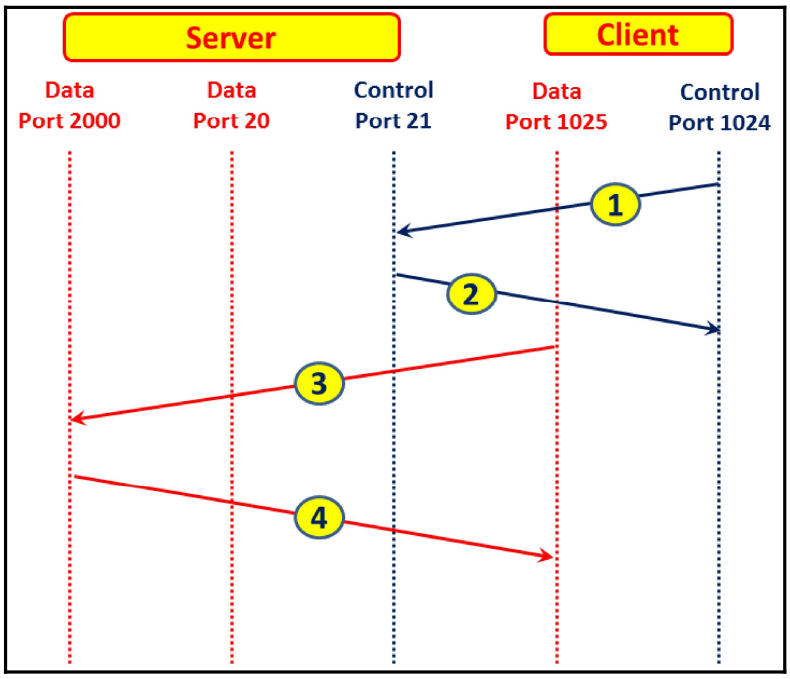
99	12.475560	192.168.0.5	192.168.0.7	TCP	590	[TCP Out-Of-Order] 23 → 24090 [ACK] Seq=3289 Ack=57 Win=999936 Len=524
100	12.476192	192.168.0.7	192.168.0.5	TCP	66	[TCP Dup ACK 97#1] 24090 → 23 [ACK] Seq=57 Ack=3289 Win=999472 Len=0
102	14.807786	192.168.0.5	192.168.0.7	TCP	590	[TCP Retransmission] 23 → 24090 [ACK] Seq=3289 Ack=57 Win=999936 Len=524
103	14.809273	192.168.0.7	192.168.0.5	TCP	66	24090 → 23 [ACK] Seq=57 Ack=4337 Win=999472 Len=0

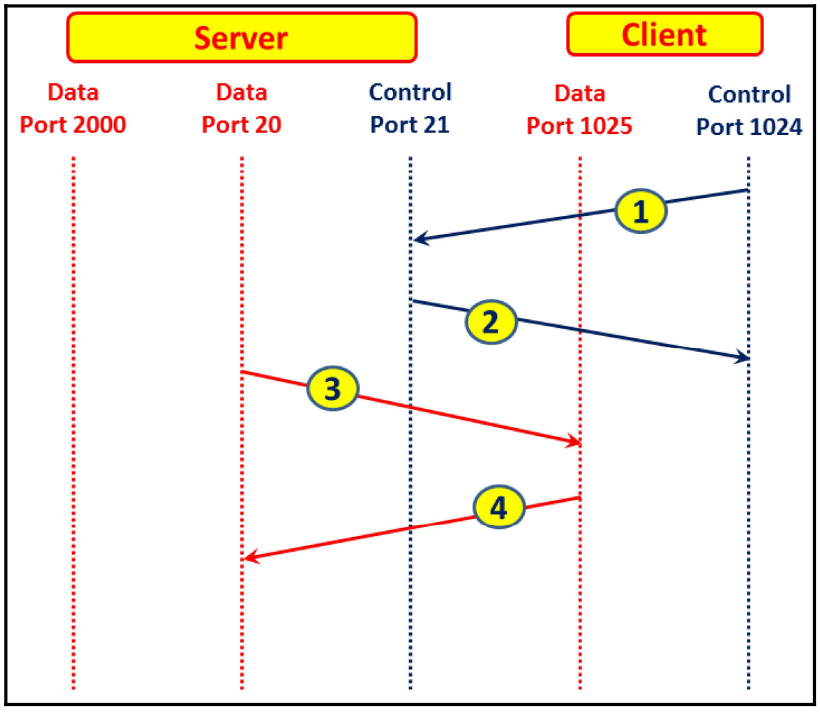
Chapter 12: FTP, HTTP/1, and HTTP/2

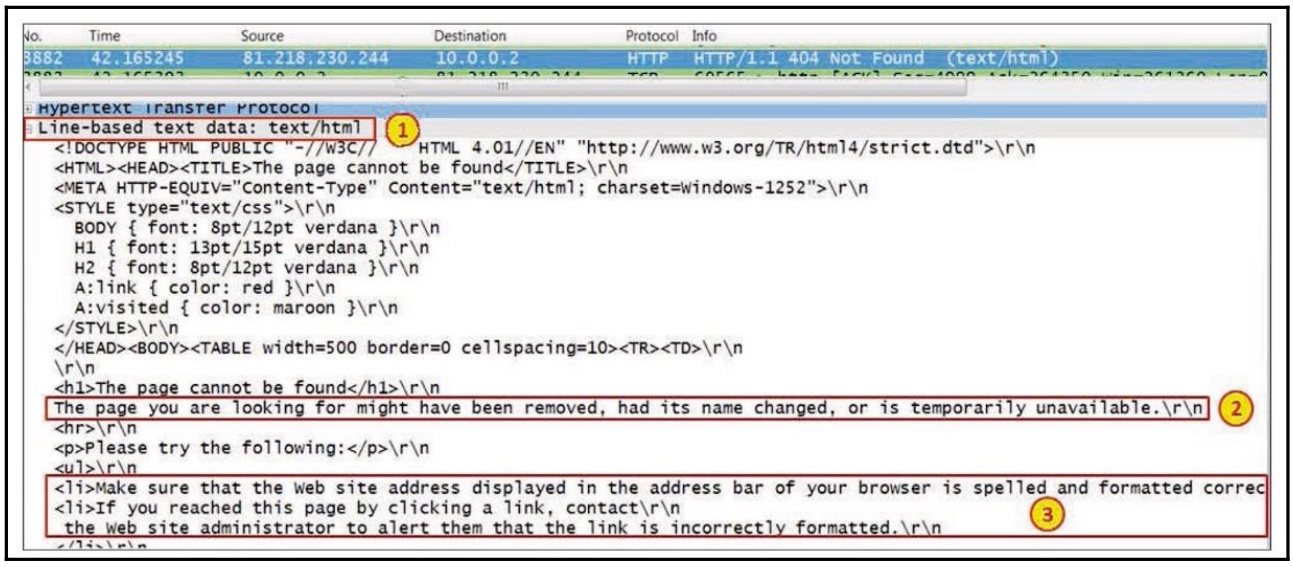


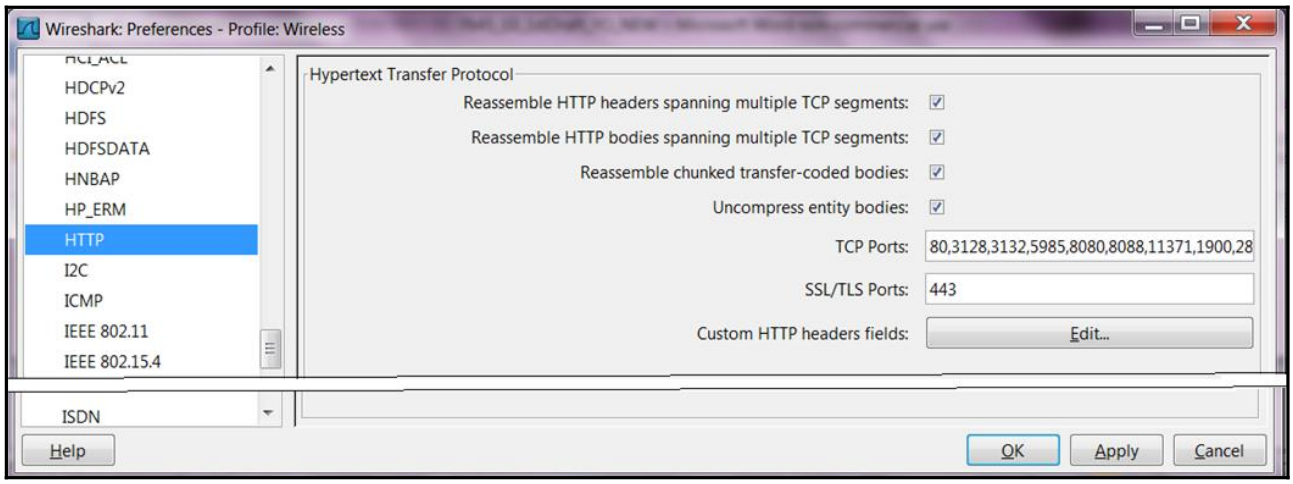

Wireshark IO Graphs: 2 interfaces
Green dots – zero window
Blue dot – retransmission
Red dot – window full
1000
500
0
20s
40s
60s
80s
100s
120s
140s
160s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: tcp.stream eq 39 and tcp.analysis.window_full Style: Dot
Graph 3 Color Filter: tcp.stream eq 39 and tcp.analysis.zero_window Style: Dot
Graph 4 Color Filter: tcp.stream eq 39 and tcp.analysis.retransmission Style: Dot
Graph 5 Color Filter: tcp.stream eq 39 Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: 1000
Smooth: No filter
Help
Copy
Save
Close

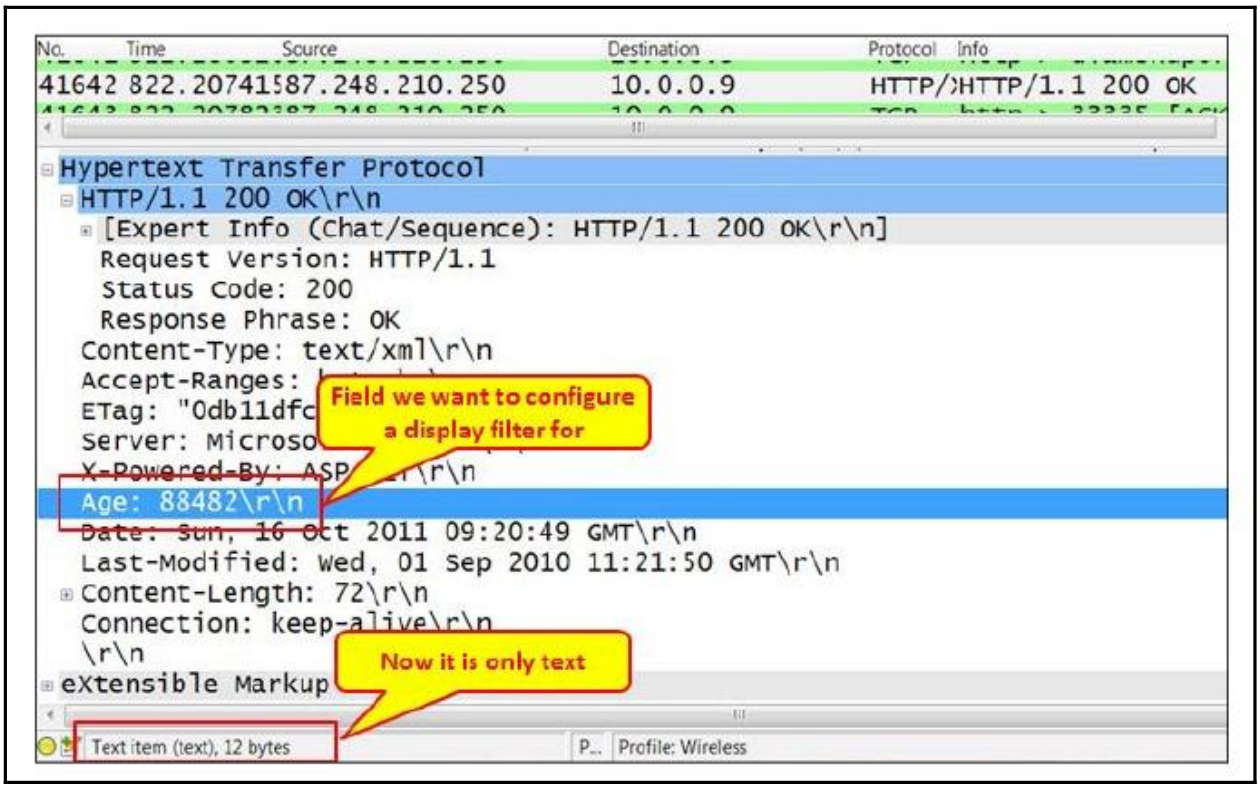

Filter: tcp.stream eq 39
Expression... Clear Apply
Server say it's TCP window is full
Client say to server: zero window
Window update and transfer continuous
No. Time Source Destination Protocol Info
5759 69.888792 10.0.0.2 15.216.111.13 TCP 54 50292 > 42447 [ACK] Seq=1 Ack=1055837
5763 70.127149 15.216.111.13 10.0.0.2 722 [TCP Window Full] FTP Data: 668 bytes
5778 70.388829 10.0.0.2 15.216.111.13 TCP 54 [TCP ZeroWindow] 50292 > 42447 [ACK]
5793 70.785945 15.216.111.13 10.0.0.2 FTP-DATA 55 [TCP ZeroWindowProbe] FTP Data: 1 byte
5794 70.785986 10.0.0.2 15.216.111.13 TCP 54 [TCP ZeroWindowProbeAck] [TCP ZeroWind
5801 72.105701 15.216.111.13 10.0.0.2 FTP-DATA 55 [TCP ZeroWindowProbe] FTP Data: 1 byte
5802 72.105735 10.0.0.2 15.216.111.13 TCP 54 [TCP ZeroWindowProbeAck] [TCP ZeroWind
5805 74.939558 15.216.111.13 10.0.0.2 FTP-DATA 55 [TCP ZeroWindowProbe] FTP Data: 1 byte
5806 74.939596 10.0.0.2 15.216.111.13 TCP 54 [TCP ZeroWindowProbeAck] [TCP ZeroWind
5930 80.025402 15.216.111.13 10.0.0.2 FTP-DATA 55 [TCP ZeroWindowProbe] FTP Data: 1 byte
5931 80.025435 10.0.0.2 15.216.111.13 TCP 54 [TCP ZeroWindowProbeAck] [TCP ZeroWind
5939 81.171193 10.0.0.2 15.216.111.13 TCP 54 [TCP Window Update] 50292 > 42447 [ACK
5940 81.390485 15.216.111.13 10.0.0.2 838 FTP Data: 784 bytes

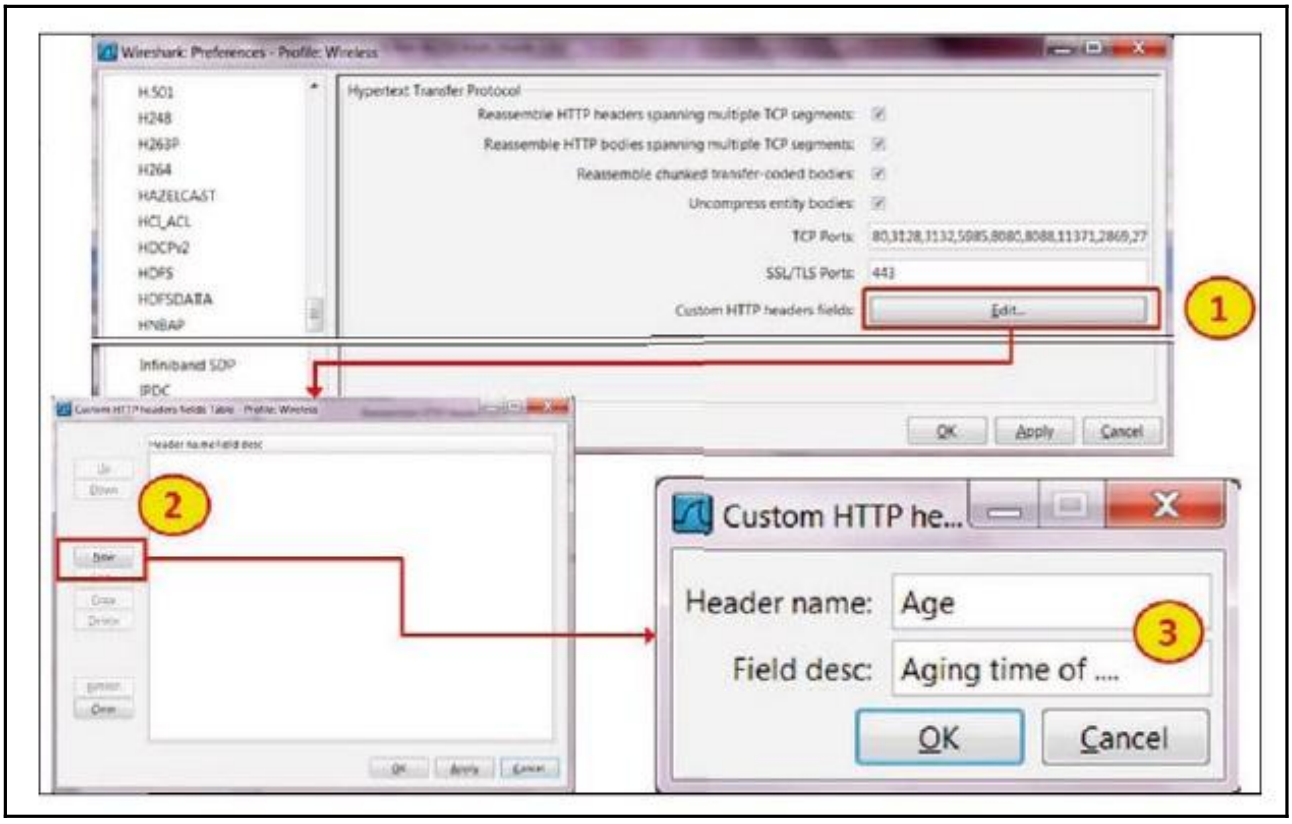

Server
Client
Data
Port 2000
Data
Port 20
Control
Port 21
Data
Port 1025
Control
Port 1024
1
2
3
4


Server
Client
Data
Port 2000
Data
Port 20
Control
Port 21
Data
Port 1025
Control
Port 1024
1
2
3
4

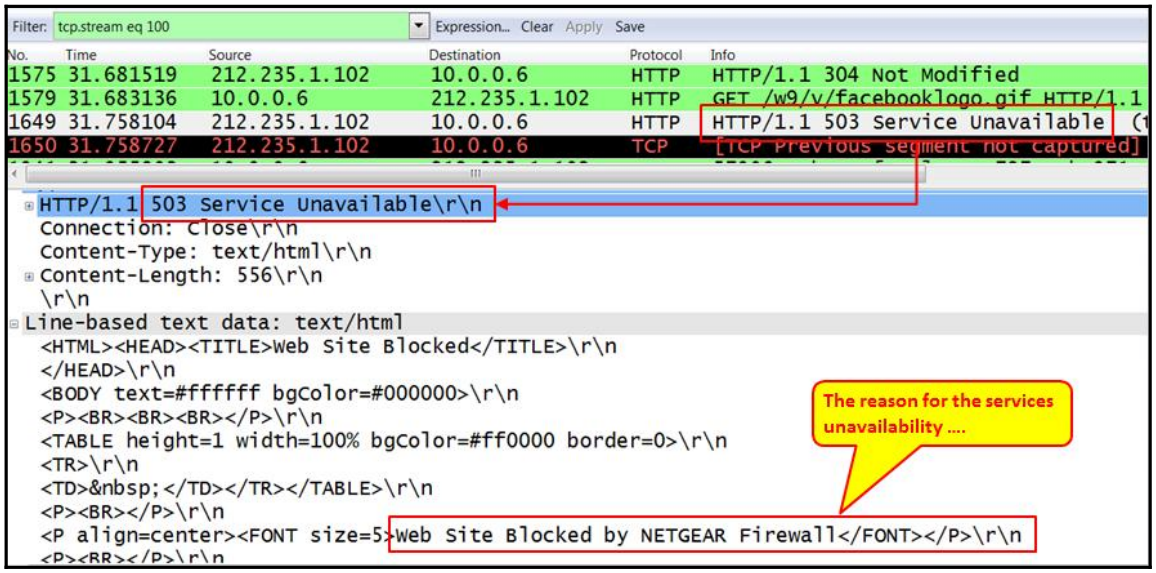

No. Time Source Destination Protocol Info
3882 42.165245 81.218.230.244 10.0.0.2 HTTP HTTP/1.1 404 Not Found (text/html)
Hypertext Transfer Protocol
Line-based text data: text/html
1
<!DOCTYPE HTML PUBLIC "-//W3C// HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">\r\n
<HTML><HEAD><TITLE>The page cannot be found</TITLE>\r\n
<META HTTP-EQUIV="Content-Type" Content="text/html; charset=Windows-1252">\r\n
<STYLE type="text/css">\r\n
BODY { font: 8pt/12pt verdana }\r\n
H1 { font: 13pt/15pt verdana }\r\n
H2 { font: 8pt/12pt verdana }\r\n
A:link { color: red }\r\n
A:visited { color: maroon }\r\n
</STYLE>\r\n
</HEAD><BODY><TABLE width=500 border=0 cellspacing=10><TR><TD>\r\n
\r\n
<h1>The page cannot be found</h1>\r\n
The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.\r\n
2
<hr>\r\n
Please try the following: \r\n
\r\n
Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correc
If you reached this page by clicking a link, contact\r\n
the Web site administrator to alert them that the link is incorrectly formatted.\r\n
3


Wireshark: Preferences - Profile: Wireless
HDCPv2
HDFS
HDFSDATA
HNBAP
HP_ERM
HTTP
I2C
ICMP
IEEE 802.11
IEEE 802.15.4
ISDN
Hypertext Transfer Protocol
Reassemble HTTP headers spanning multiple TCP segments:
Reassemble HTTP bodies spanning multiple TCP segments:
Reassemble chunked transfer-coded bodies:
Uncompress entity bodies:
TCP Ports: 80,3128,3132,5985,8080,8088,11371,1900,28
SSL/TLS Ports: 443
Custom HTTP headers fields: Edit...
Help
OK
Apply
Cancel

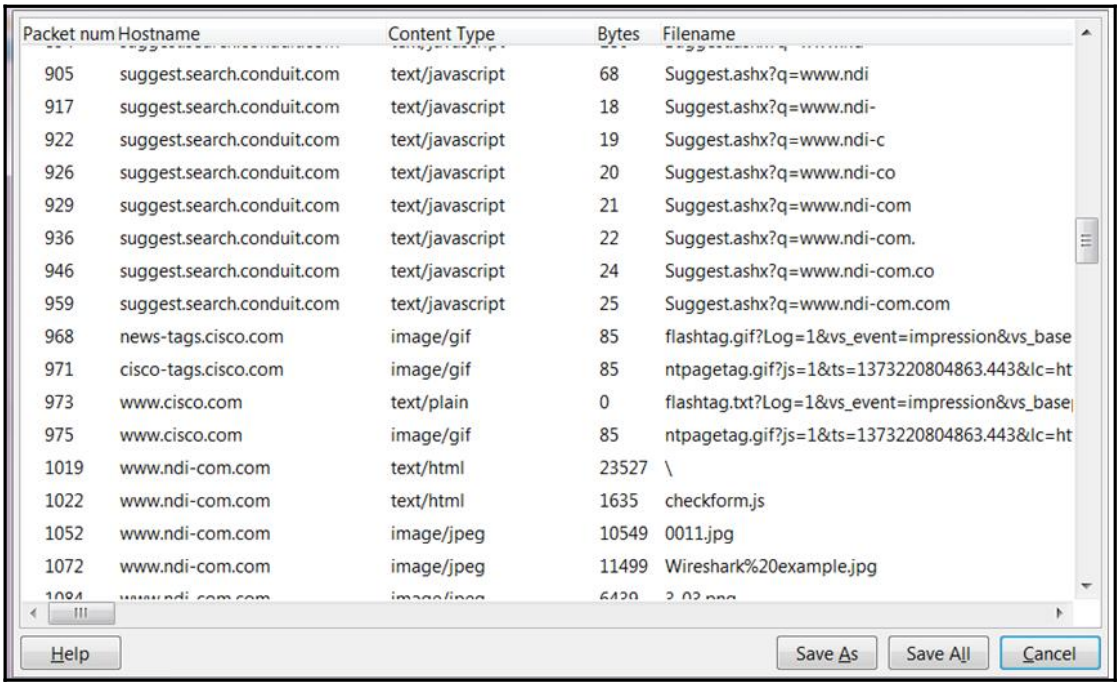

No. Time Source Destination Protocol Info
41642 822.20741587.248.210.250 10.0.0.9 HTTP/XHTTP/1.1 200 OK
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
Request Version: HTTP/1.1
Status Code: 200
Response Phrase: OK
Content-Type: text/xml\r\n
Accept-Ranges:
ETag: "0db11dfc
Server: Microso
X-Powered-By: ASP
Age: 88482\r\n
Date: Sun, 16 Oct 2011 09:20:49 GMT\r\n
Last-Modified: Wed, 01 Sep 2010 11:21:50 GMT\r\n
Content-Length: 72\r\n
Connection: keep-alive\r\n
\r\n
eXtensible Markup
Field we want to configure a display filter for
Now it is only text
Text item (text), 12 bytes
P... Profile: Wireless

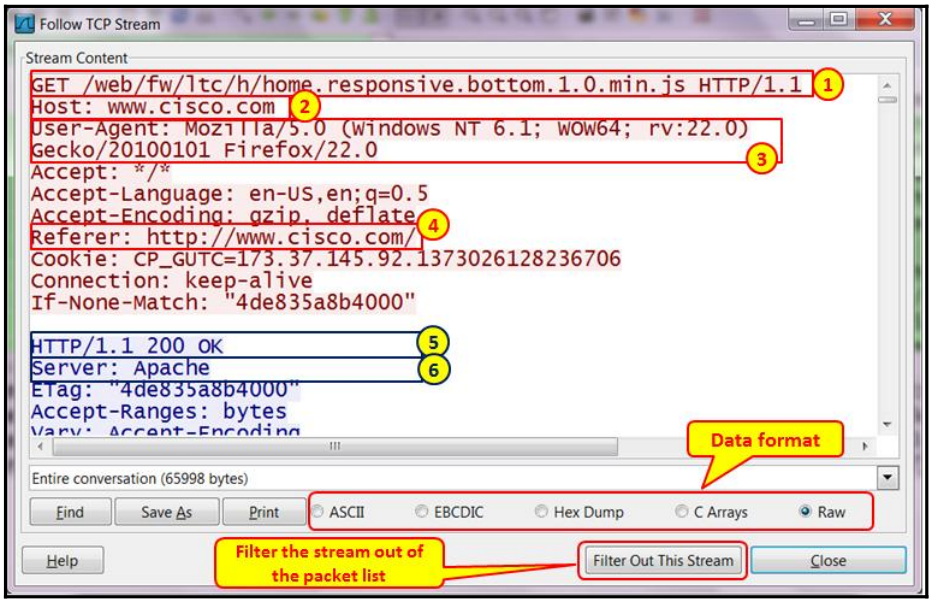


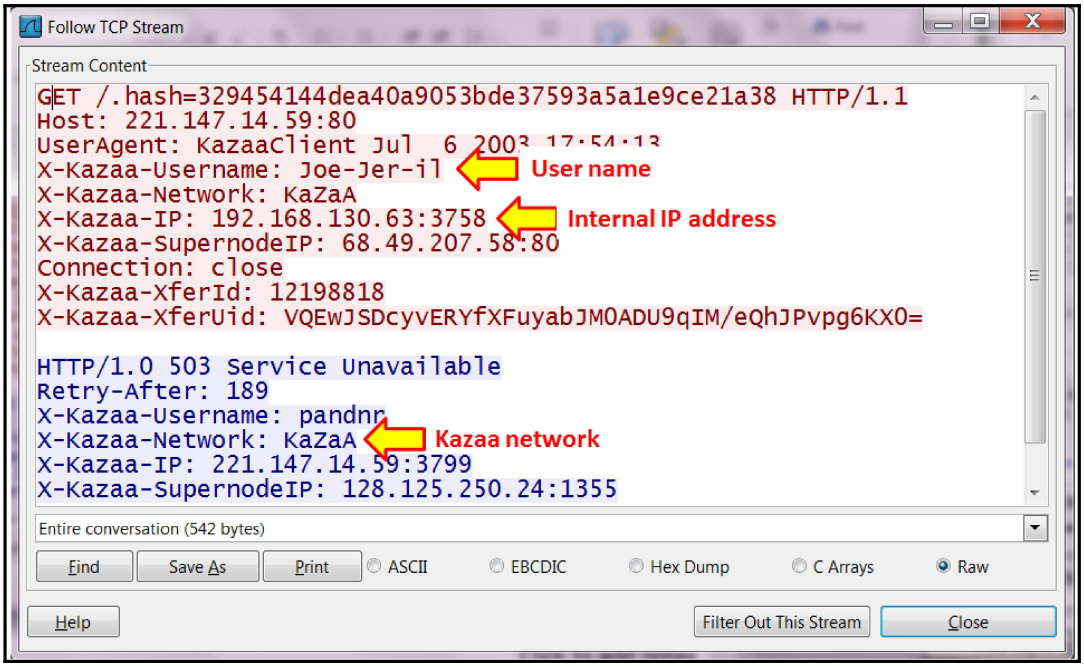

```
}
GET /poker-client/broadcast.htm HTTP/1.1 (1)
Accept: image/gif, image/jpeg, image/pjpeg, image/pjpeg, application/x-shockwave-flash, application/
x-ms-application, application/x-ms-xbap, application/vnd.ms-xpsdocument, application/xaml+xml,
application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer: http://www.888poker.com/poker-client/promotions.htm (2)
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; GTB7.1; Mozilla/4.0
(compatible; MSIE 6.0; Windows NT 5.1; SV1) ; .NET CLR 1.1.4322; .NET CLR 2.0.50727;
OfficeLiveConnector.1.3; OfficeLivePatch.0.0; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729;
InfoPath.1)
Host: www.888poker.com (3)

HTTP/1.1 404 Not Found (4)
Date: Sun, 16 Oct 2011 09:11:58 GMT
Server: Microsoft-IIS/6.0
srv: 2344432
```

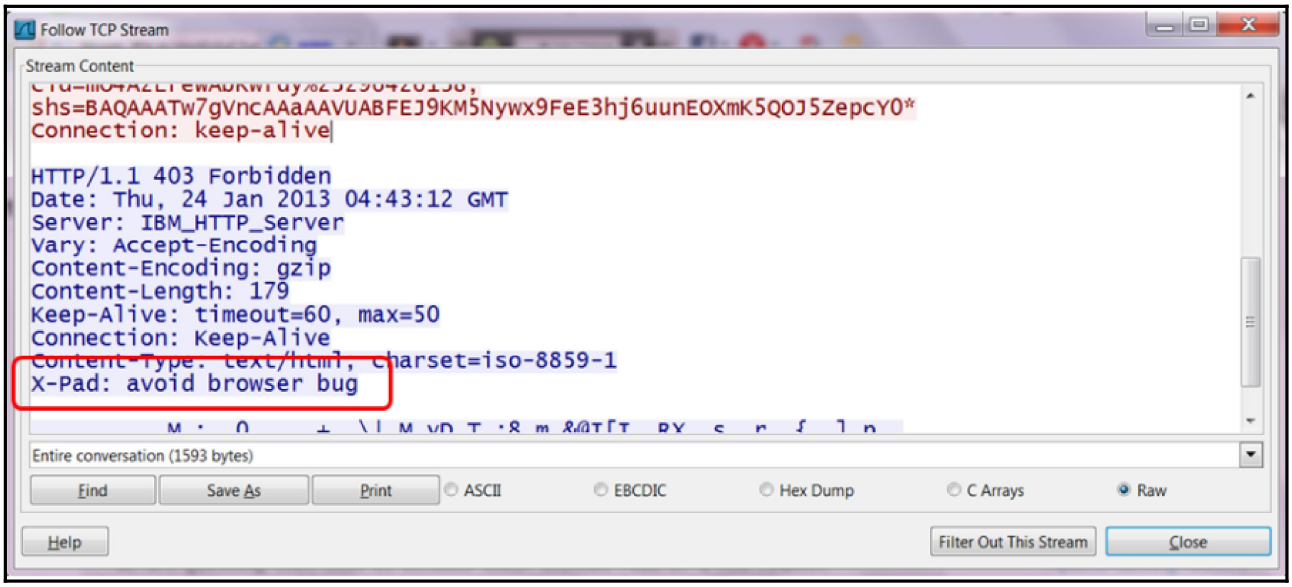

Filter: tcp.stream eq 100
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
1575 31.681519 212.235.1.102 10.0.0.6 HTTP HTTP/1.1 304 Not Modified
1579 31.683136 10.0.0.6 212.235.1.102 HTTP GET /w9/v/facebooklogo.gif HTTP/1.1
1649 31.758104 212.235.1.102 10.0.0.6 HTTP HTTP/1.1 503 Service Unavailable
1650 31.758727 212.235.1.102 10.0.0.6 TCP [TCP Previous segment not captured]
HTTP/1.1 503 Service Unavailable\r\n
Connection: Close\r\n
Content-Type: text/html\r\n
Content-Length: 556\r\n
\r\n
Line-based text data: text/html
<HTML><HEAD><TITLE>Web Site Blocked</TITLE>\r\n
</HEAD>\r\n
<BODY text=#ffffff bgColor=#000000>\r\n
<P>

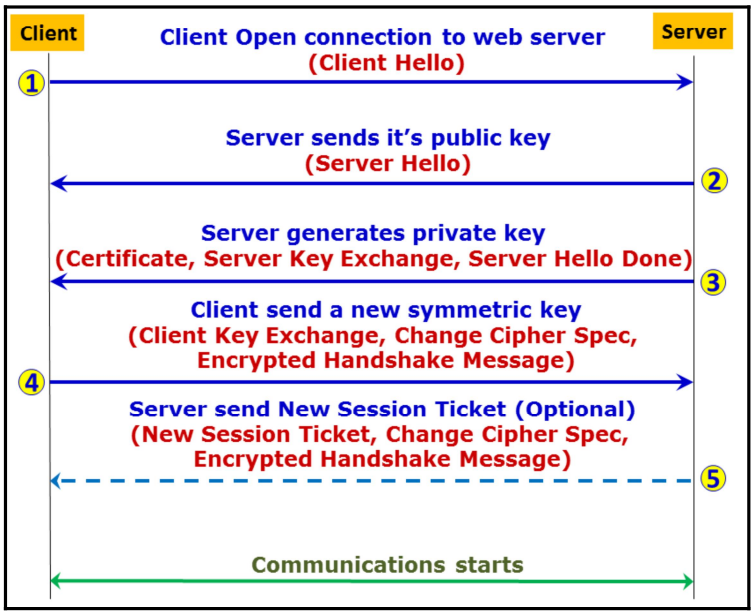
</P>\r\n
<TABLE height=1 width=100% bgColor=#ff0000 border=0>\r\n
<TR>\r\n
<TD> </TD></TR></TABLE>\r\n
<P>
</P>\r\n
<P align=center><FONT size=5>Web Site Blocked by NETGEAR Firewall</FONT></P>\r\n
The reason for the services unavailability ....

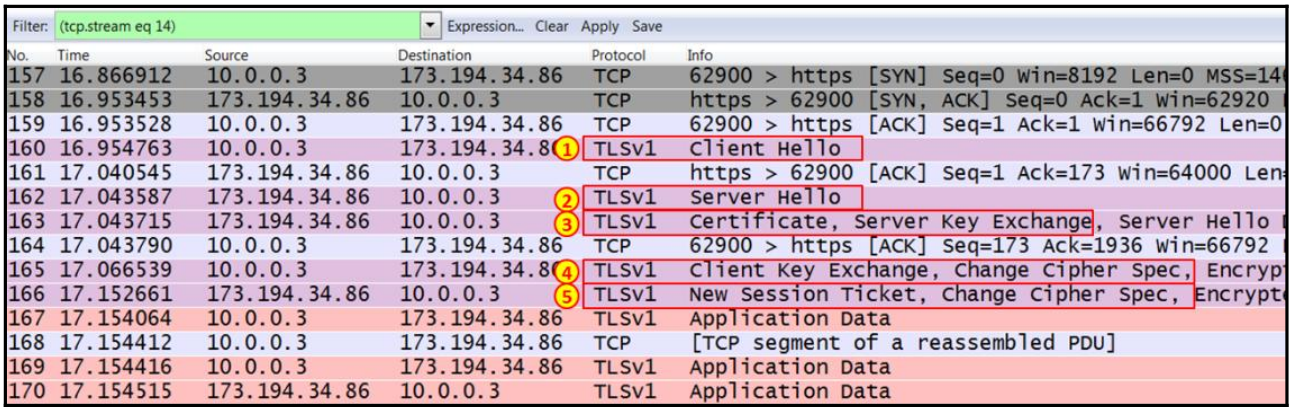

Packet num Hostname Content Type Bytes Filename
905 suggest.search.conduit.com text/javascript 68 Suggest.ashx?q=www.ndi
917 suggest.search.conduit.com text/javascript 18 Suggest.ashx?q=www.ndi-
922 suggest.search.conduit.com text/javascript 19 Suggest.ashx?q=www.ndi-c
926 suggest.search.conduit.com text/javascript 20 Suggest.ashx?q=www.ndi-co
929 suggest.search.conduit.com text/javascript 21 Suggest.ashx?q=www.ndi-com
936 suggest.search.conduit.com text/javascript 22 Suggest.ashx?q=www.ndi-com.
946 suggest.search.conduit.com text/javascript 24 Suggest.ashx?q=www.ndi-com.co
959 suggest.search.conduit.com text/javascript 25 Suggest.ashx?q=www.ndi-com.com
968 news-tags.cisco.com image/gif 85 flashtag.gif?Log=1&vs_event=impression&vs_base
971 cisco-tags.cisco.com image/gif 85 ntpagetag.gif?js=1&ts=1373220804863.443&lc=ht
973 www.cisco.com text/plain 0 flashtag.txt?Log=1&vs_event=impression&vs_base
975 www.cisco.com image/gif 85 ntpagetag.gif?js=1&ts=1373220804863.443&lc=ht
1019 www.ndi-com.com text/html 23527 \
1022 www.ndi-com.com text/html 1635 checkform.js
1052 www.ndi-com.com image/jpeg 10549 0011.jpg
1072 www.ndi-com.com image/jpeg 11499 Wireshark%20example.jpg
Help
Save As
Save All
Cancel

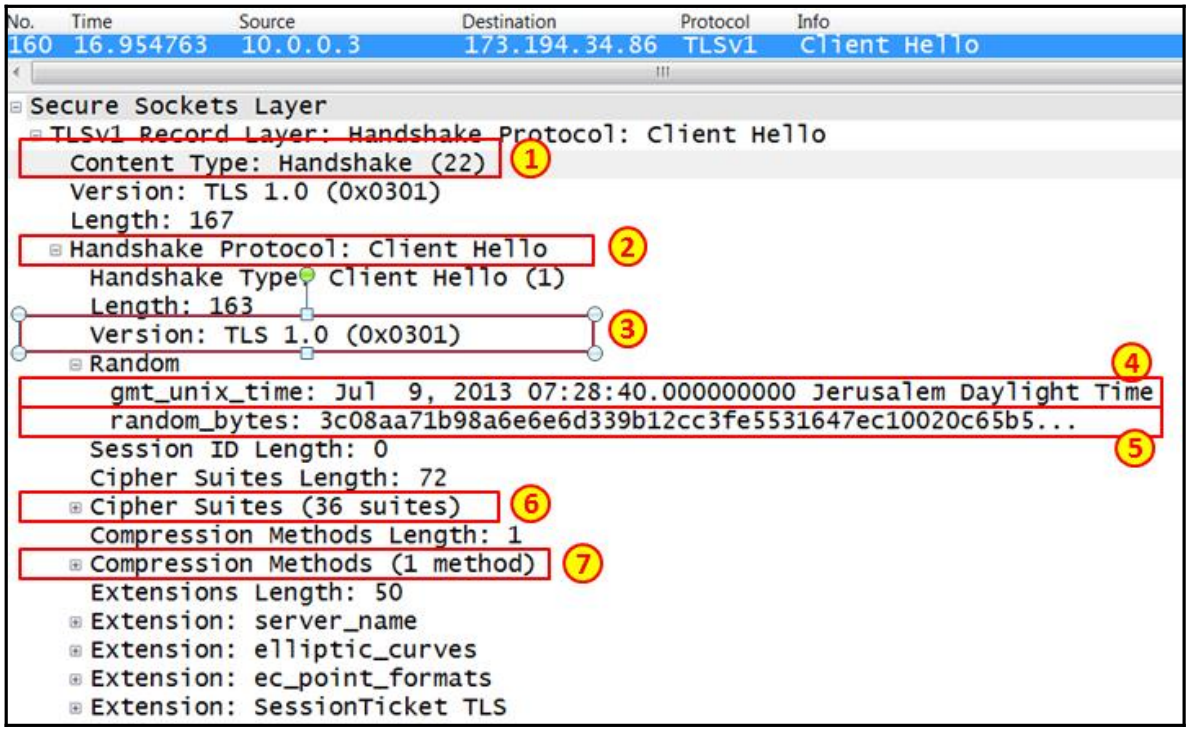

Follow TCP Stream
Stream Content
GET /web/fw/ltc/h/home.responsive.bottom.1.0.min.js HTTP/1.1
Host: www.cisco.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:22.0)
Gecko/20100101 Firefox/22.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.cisco.com/
Cookie: CP_GUTC=173.37.145.92.1373026128236706
Connection: keep-alive
If-None-Match: "4de835a8b4000"
HTTP/1.1 200 OK
Server: Apache
ETag: "4de835a8b4000"
Accept-Ranges: bytes
1
2
3
4
5
6
Data format
Entire conversation (65998 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter the stream out of the packet list
Filter Out This Stream
Close

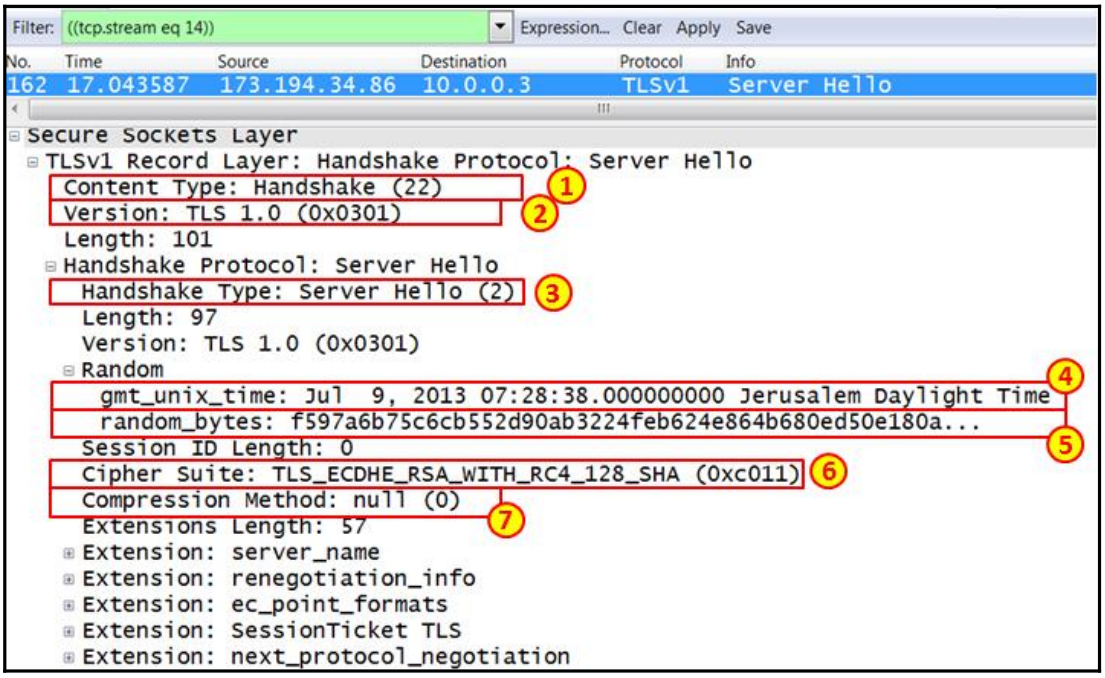

Follow TCP Stream
Stream Content
GET /.hash=329454144dea40a9053bde37593a5a1e9ce21a38 HTTP/1.1
Host: 221.147.14.59:80
X-Kazaa-Username: Joe-Jer-il
User name
X-Kazaa-Network: KaZaA
X-Kazaa-IP: 192.168.130.63:3758
Internal IP address
X-Kazaa-SupernodeIP: 68.49.207.58:80
Connection: close
X-Kazaa-XferId: 12198818
X-Kazaa-XferUid: VQEwJSDcyvERYfXFuyabJM0ADU9qIM/eQhJPvpg6KX0=
HTTP/1.0 503 Service Unavailable
Retry-After: 189
X-Kazaa-Username: pandnr
X-Kazaa-Network: KaZaA
Kazaa network
X-Kazaa-IP: 221.147.14.59:3799
X-Kazaa-SupernodeIP: 128.125.250.24:1355
Entire conversation (542 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

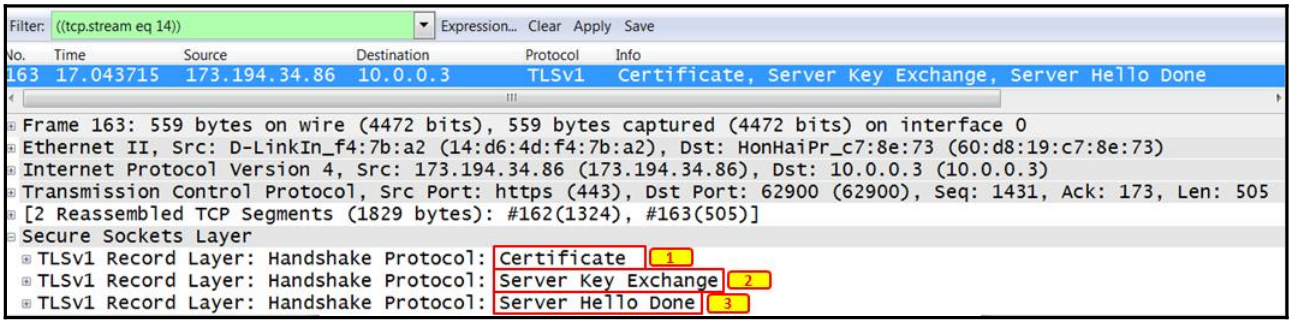

Follow TCP Stream
Stream Content
shs=BAQAAATw7gVncAAaAAVUABFEJ9KM5Nywx9FeE3hj6uunEOXmK5QOJ5ZepcY0*
Connection: keep-alive
HTTP/1.1 403 Forbidden
Date: Thu, 24 Jan 2013 04:43:12 GMT
Server: IBM_HTTP_Server
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 179
Keep-Alive: timeout=60, max=50
Connection: Keep-Alive
X-Pad: avoid browser bug
Entire conversation (1593 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

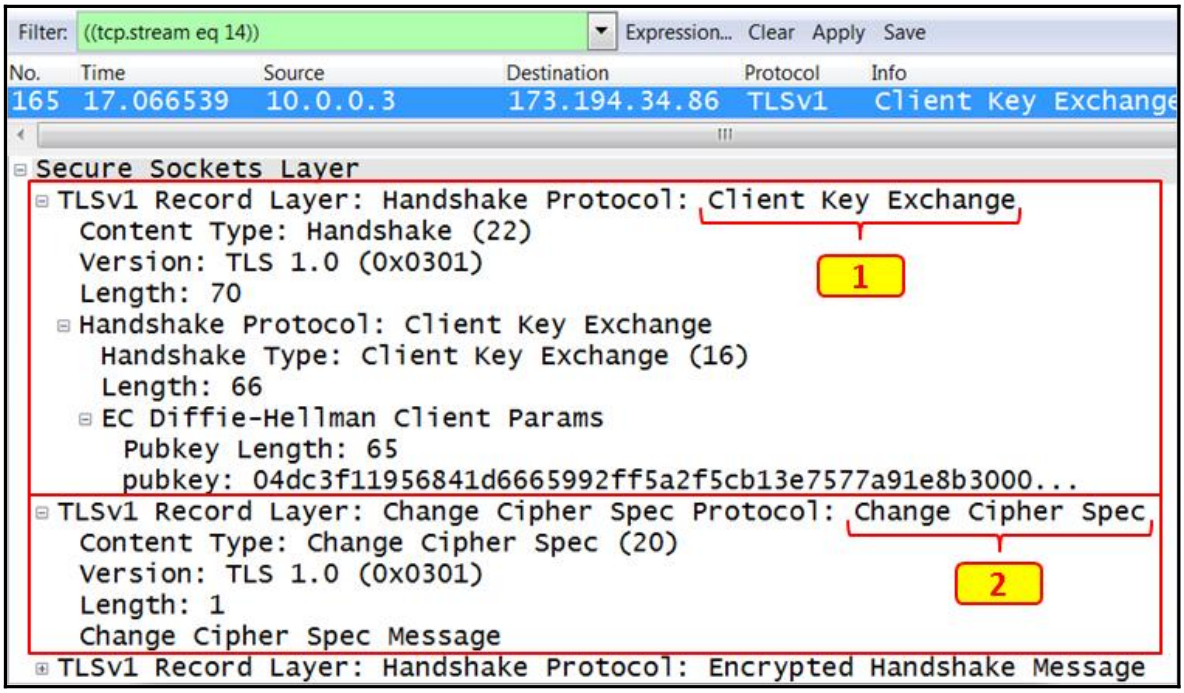

Client
Server
Client Open connection to web server
(Client Hello)
1
Server sends it's public key
(Server Hello)
2
Server generates private key
(Certificate, Server Key Exchange, Server Hello Done)
3
Client send a new symmetric key
(Client Key Exchange, Change Cipher Spec,
Encrypted Handshake Message)
4
Server send New Session Ticket (Optional)
(New Session Ticket, Change Cipher Spec,
Encrypted Handshake Message)
5
Communications starts

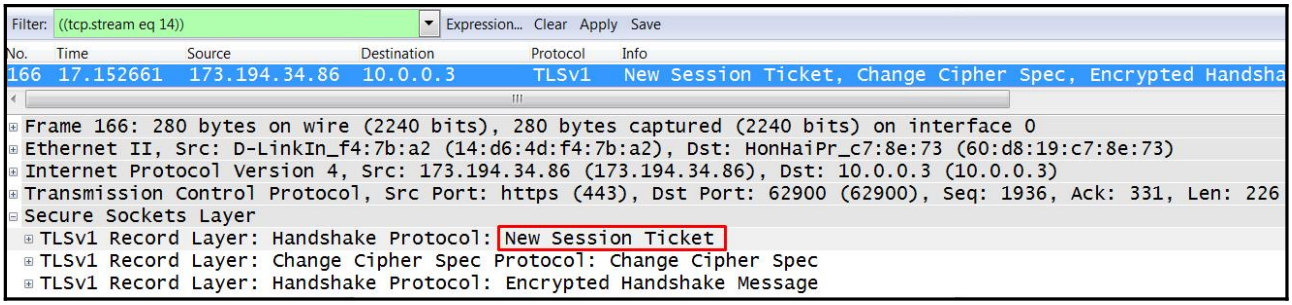

Filter: (tcp.stream eq 14)
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
157 16.866912 10.0.0.3 173.194.34.86 TCP 62900 > https [SYN] Seq=0 Win=8192 Len=0 MSS=14
158 16.953453 173.194.34.86 10.0.0.3 TCP https > 62900 [SYN, ACK] Seq=0 Ack=1 Win=62920
159 16.953528 10.0.0.3 173.194.34.86 TCP 62900 > https [ACK] Seq=1 Ack=1 Win=66792 Len=0
160 16.954763 10.0.0.3 173.194.34.8 1 TLSv1 Client Hello
161 17.040545 173.194.34.86 10.0.0.3 TCP https > 62900 [ACK] Seq=1 Ack=173 Win=64000 Len
162 17.043587 173.194.34.86 10.0.0.3 2 TLSv1 Server Hello
163 17.043715 173.194.34.86 10.0.0.3 3 TLSv1 Certificate, Server Key Exchange, Server Hello
164 17.043790 10.0.0.3 173.194.34.86 TCP 62900 > https [ACK] Seq=173 Ack=1936 Win=66792
165 17.066539 10.0.0.3 173.194.34.8 4 TLSv1 Client Key Exchange, Change Cipher Spec, Encryp
166 17.152661 173.194.34.86 10.0.0.3 5 TLSv1 New Session Ticket, Change Cipher Spec, Encrypt
167 17.154064 10.0.0.3 173.194.34.86 TLSv1 Application Data
168 17.154412 10.0.0.3 173.194.34.86 TCP [TCP segment of a reassembled PDU]
169 17.154416 10.0.0.3 173.194.34.86 TLSv1 Application Data
170 17.154515 173.194.34.86 10.0.0.3 TLSv1 Application Data


No. Time Source Destination Protocol Info
160 16.954763 10.0.0.3 173.194.34.86 TLSv1 Client Hello
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22) 1
Version: TLS 1.0 (0x0301)
Length: 167
Handshake Protocol: Client Hello 2
Handshake Type: Client Hello (1)
Length: 163
Version: TLS 1.0 (0x0301) 3
Random 4
gmt_unix_time: Jul 9, 2013 07:28:40.000000000 Jerusalem Daylight Time
random_bytes: 3c08aa71b98a6e6e6d339b12cc3fe5531647ec10020c65b5... 5
Session ID Length: 0
Cipher Suites Length: 72
Cipher Suites (36 suites) 6
Compression Methods Length: 1
Compression Methods (1 method) 7
Extensions Length: 50
Extension: server_name
Extension: elliptic_curves
Extension: ec_point_formats
Extension: SessionTicket TLS

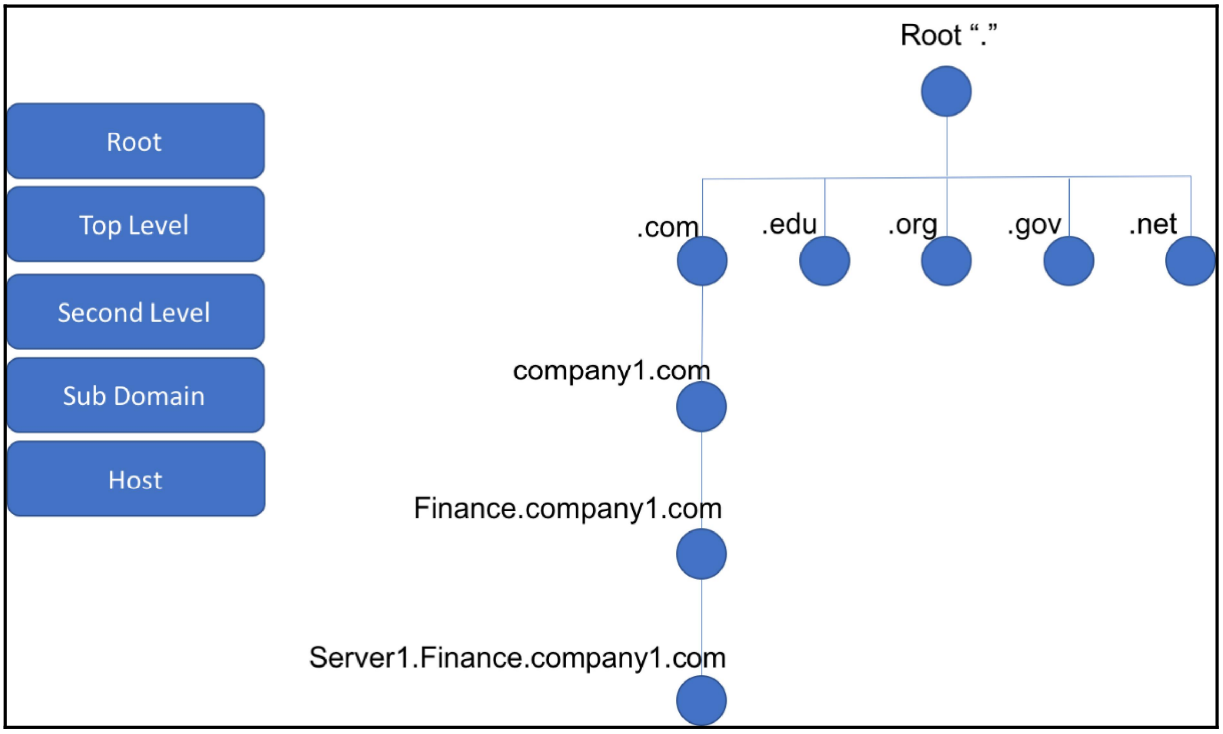

Filter: ((tcp.stream eq 14)) Expression... Clear Apply Save
No. Time Source Destination Protocol Info
162 17.043587 173.194.34.86 10.0.0.3 TLSv1 Server Hello
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Server Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 101
Handshake Protocol: Server Hello
Handshake Type: Server Hello (2)
Length: 97
Version: TLS 1.0 (0x0301)
Random
gmt_unix_time: Jul 9, 2013 07:28:38.000000000 Jerusalem Daylight Time
random_bytes: f597a6b75c6cb552d90ab3224feb624e864b680ed50e180a...
Session ID Length: 0
Cipher Suite: TLS_ECDHE_RSA_WITH_RC4_128_SHA (0xc011)
Compression Method: null (0)
Extensions Length: 57
Extension: server_name
Extension: renegotiation_info
Extension: ec_point_formats
Extension: SessionTicket TLS
Extension: next_protocol_negotiation
1
2
3
4
5
6
7

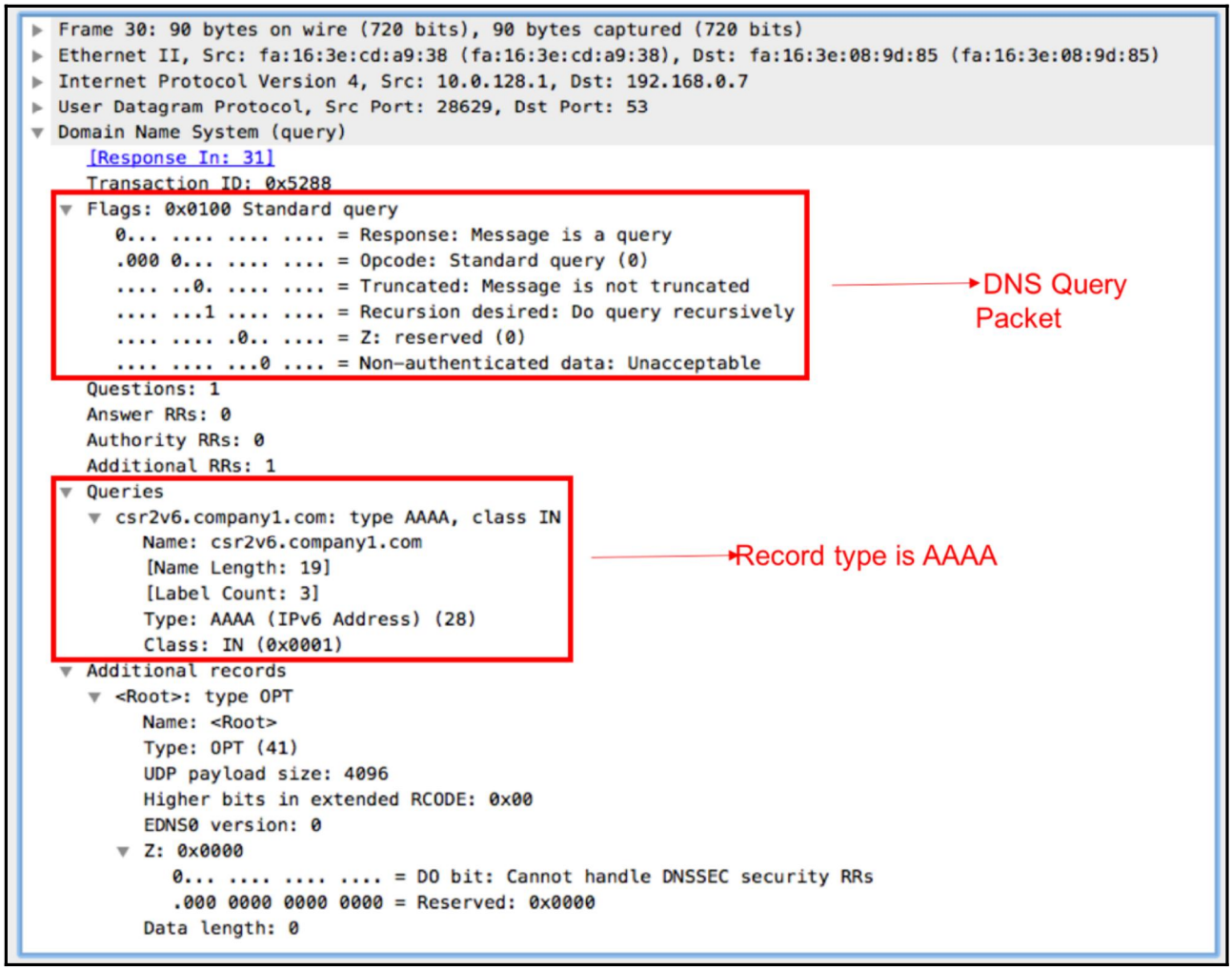

Filter: ((tcp.stream eq 14)) Expression... Clear Apply Save
No. Time Source Destination Protocol Info
163 17.043715 173.194.34.86 10.0.0.3 TLSv1 Certificate, Server Key Exchange, Server Hello Done
Frame 163: 559 bytes on wire (4472 bits), 559 bytes captured (4472 bits) on interface 0
Ethernet II, Src: D-LinkIn_f4:7b:a2 (14:d6:4d:f4:7b:a2), Dst: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73)
Internet Protocol Version 4, Src: 173.194.34.86 (173.194.34.86), Dst: 10.0.0.3 (10.0.0.3)
Transmission Control Protocol, Src Port: https (443), Dst Port: 62900 (62900), Seq: 1431, Ack: 173, Len: 505
[2 Reassembled TCP Segments (1829 bytes): #162(1324), #163(505)]
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Certificate
TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
TLSv1 Record Layer: Handshake Protocol: Server Hello Done
1
2
3

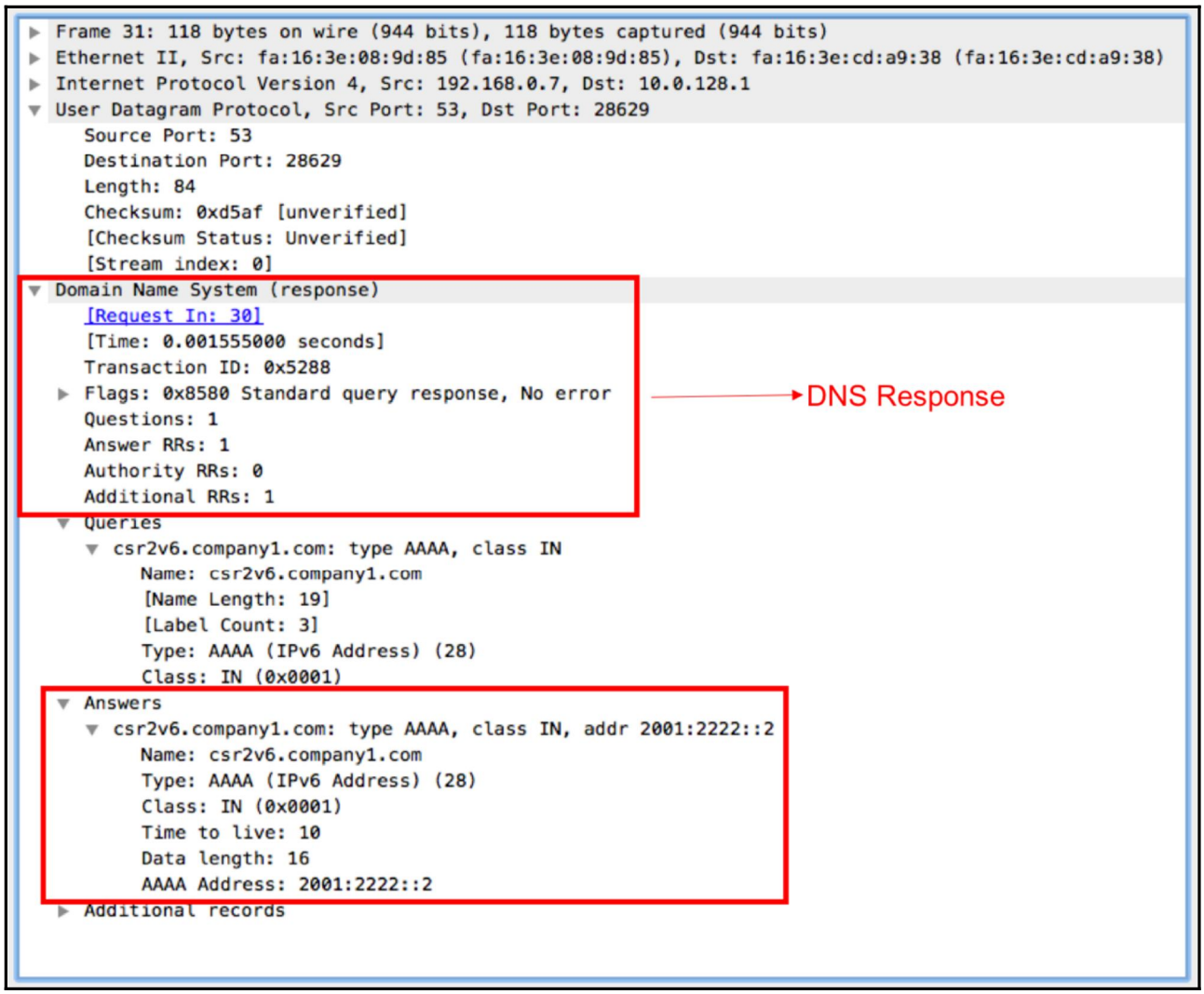

Filter: ((tcp.stream eq 14))
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
165 17.066539 10.0.0.3 173.194.34.86 TLSv1 Client Key Exchange
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: Client Key Exchange
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 70
Handshake Protocol: Client Key Exchange
Handshake Type: Client Key Exchange (16)
Length: 66
EC Diffie-Hellman Client Params
Pubkey Length: 65
pubkey: 04dc3f11956841d6665992ff5a2f5cb13e7577a91e8b3000...
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
Content Type: Change Cipher Spec (20)
Version: TLS 1.0 (0x0301)
Length: 1
Change Cipher Spec Message
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message
1
2

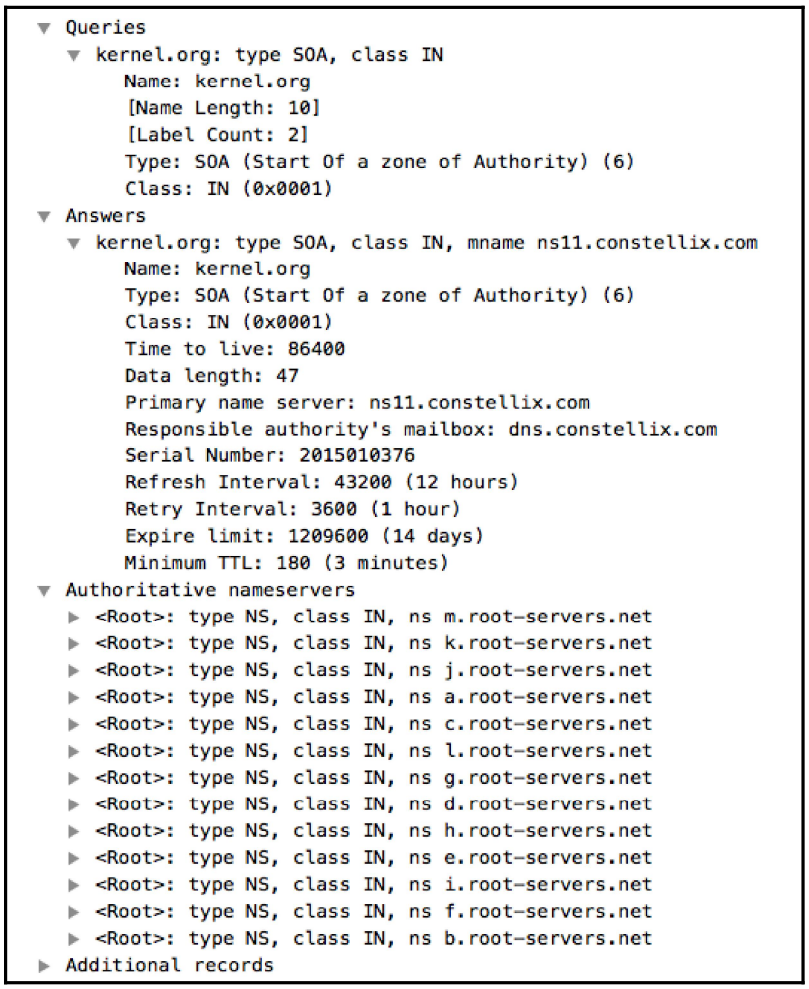

Filter: ((tcp.stream eq 14))
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
166 17.152661 173.194.34.86 10.0.0.3 TLSv1 New Session Ticket, Change Cipher Spec, Encrypted Handsha
Frame 166: 280 bytes on wire (2240 bits), 280 bytes captured (2240 bits) on interface 0
Ethernet II, Src: D-LinkIn_f4:7b:a2 (14:d6:4d:f4:7b:a2), Dst: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73)
Internet Protocol Version 4, Src: 173.194.34.86 (173.194.34.86), Dst: 10.0.0.3 (10.0.0.3)
Transmission Control Protocol, Src Port: https (443), Dst Port: 62900 (62900), Seq: 1936, Ack: 331, Len: 226
Secure Sockets Layer
TLSv1 Record Layer: Handshake Protocol: New Session Ticket
TLSv1 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
TLSv1 Record Layer: Handshake Protocol: Encrypted Handshake Message

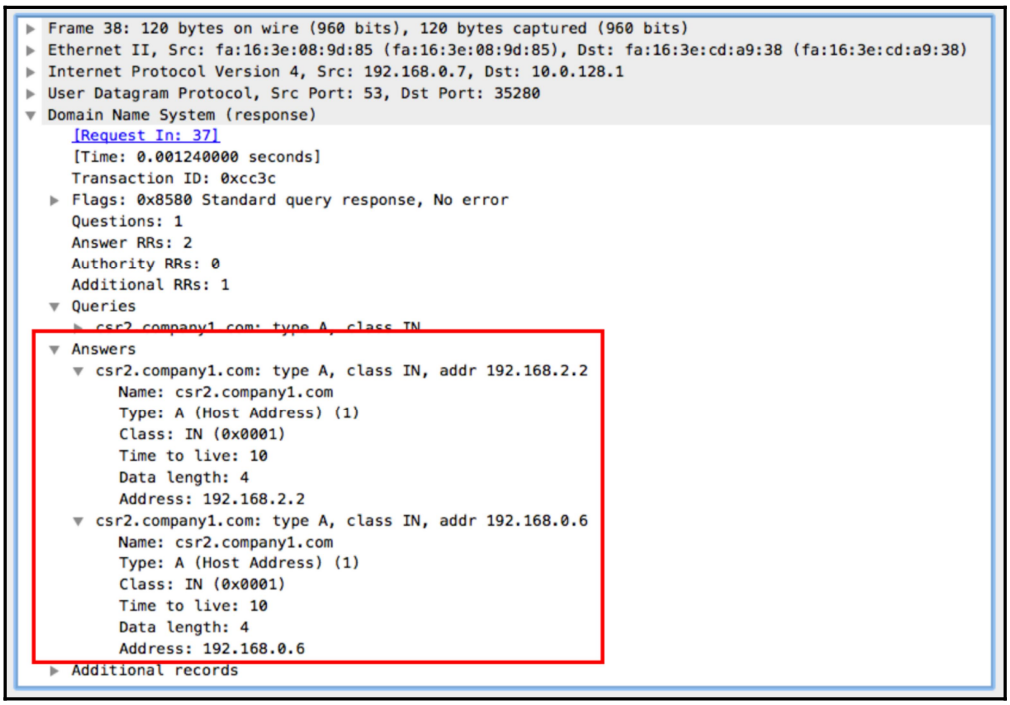
Chapter 13: DNS Protocol Analysis




Frame 30: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Ethernet II, Src: fa:16:3e:cd:a9:38 (fa:16:3e:cd:a9:38), Dst: fa:16:3e:08:9d:85 (fa:16:3e:08:9d:85)
Internet Protocol Version 4, Src: 10.0.128.1, Dst: 192.168.0.7
User Datagram Protocol, Src Port: 28629, Dst Port: 53
Domain Name System (query)
[Response In: 31]
Transaction ID: 0x5288
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
DNS Query Packet
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
csr2v6.company1.com: type AAAA, class IN
Name: csr2v6.company1.com
[Name Length: 19]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Record type is AAAA
Additional records
<Root>: type OPT
Name: <Root>
Type: OPT (41)
UDP payload size: 4096
Higher bits in extended RCODE: 0x00
EDNS0 version: 0
Z: 0x0000
0... .... = DO bit: Cannot handle DNSSEC security RRs
.000 0000 0000 0000 = Reserved: 0x0000
Data length: 0

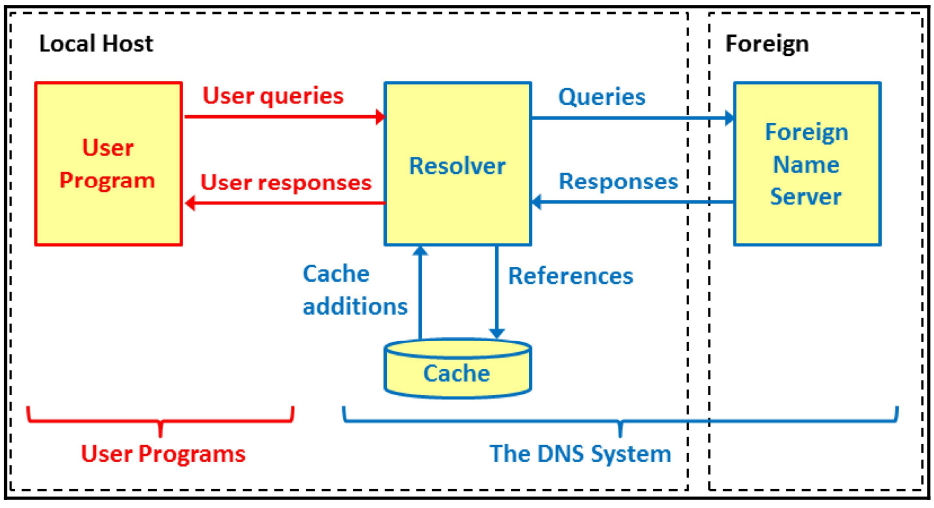

Frame 31: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
Ethernet II, Src: fa:16:3e:08:9d:85 (fa:16:3e:08:9d:85), Dst: fa:16:3e:cd:a9:38 (fa:16:3e:cd:a9:38)
Internet Protocol Version 4, Src: 192.168.0.7, Dst: 10.0.128.1
User Datagram Protocol, Src Port: 53, Dst Port: 28629
Source Port: 53
Destination Port: 28629
Length: 84
Checksum: 0xd5af [unverified]
[Checksum Status: Unverified]
[Stream index: 0]
Domain Name System (response)
[Request In: 30]
[Time: 0.001555000 seconds]
Transaction ID: 0x5288
Flags: 0x8580 Standard query response, No error
Questions: 1
Answer RRs: 1
Authority RRs: 0
Additional RRs: 1
Queries
csr2v6.company1.com: type AAAA, class IN
Name: csr2v6.company1.com
[Name Length: 19]
[Label Count: 3]
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Answers
csr2v6.company1.com: type AAAA, class IN, addr 2001:2222::2
Name: csr2v6.company1.com
Type: AAAA (IPv6 Address) (28)
Class: IN (0x0001)
Time to live: 10
Data length: 16
AAAA Address: 2001:2222::2
Additional records
DNS Response

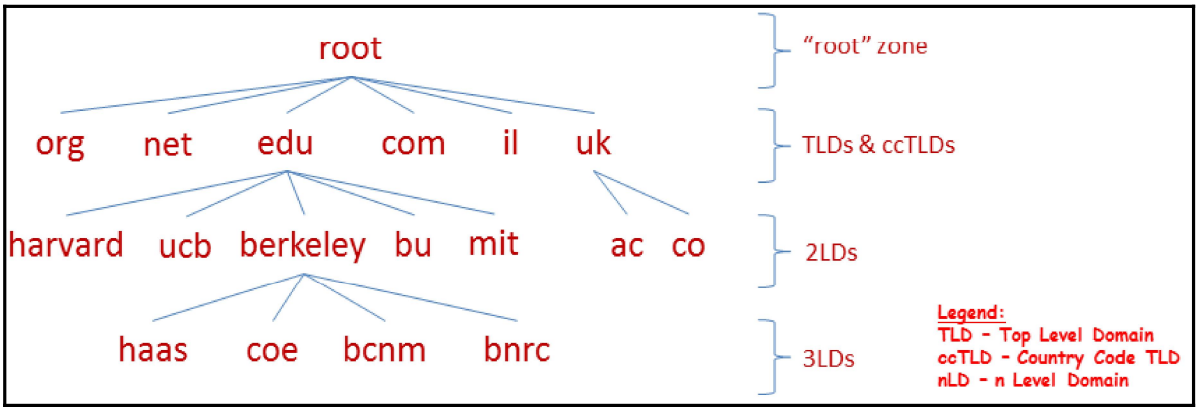

▼ Queries
▼ kernel.org: type SOA, class IN
Name: kernel.org
[Name Length: 10]
[Label Count: 2]
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
▼ Answers
▼ kernel.org: type SOA, class IN, mname ns11.constellix.com
Name: kernel.org
Type: SOA (Start Of a zone of Authority) (6)
Class: IN (0x0001)
Time to live: 86400
Data length: 47
Primary name server: ns11.constellix.com
Responsible authority's mailbox: dns.constellix.com
Serial Number: 2015010376
Refresh Interval: 43200 (12 hours)
Retry Interval: 3600 (1 hour)
Expire limit: 1209600 (14 days)
Minimum TTL: 180 (3 minutes)
▼ Authoritative nameservers
▶ <Root>: type NS, class IN, ns m.root-servers.net
▶ <Root>: type NS, class IN, ns k.root-servers.net
▶ <Root>: type NS, class IN, ns j.root-servers.net
▶ <Root>: type NS, class IN, ns a.root-servers.net
▶ <Root>: type NS, class IN, ns c.root-servers.net
▶ <Root>: type NS, class IN, ns l.root-servers.net
▶ <Root>: type NS, class IN, ns g.root-servers.net
▶ <Root>: type NS, class IN, ns d.root-servers.net
▶ <Root>: type NS, class IN, ns h.root-servers.net
▶ <Root>: type NS, class IN, ns e.root-servers.net
▶ <Root>: type NS, class IN, ns i.root-servers.net
▶ <Root>: type NS, class IN, ns f.root-servers.net
▶ <Root>: type NS, class IN, ns b.root-servers.net
▶ Additional records

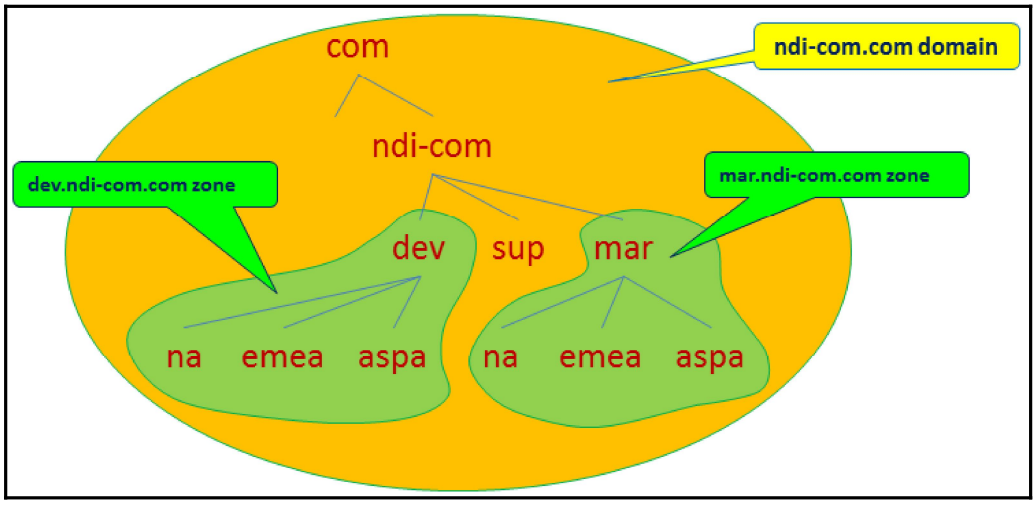


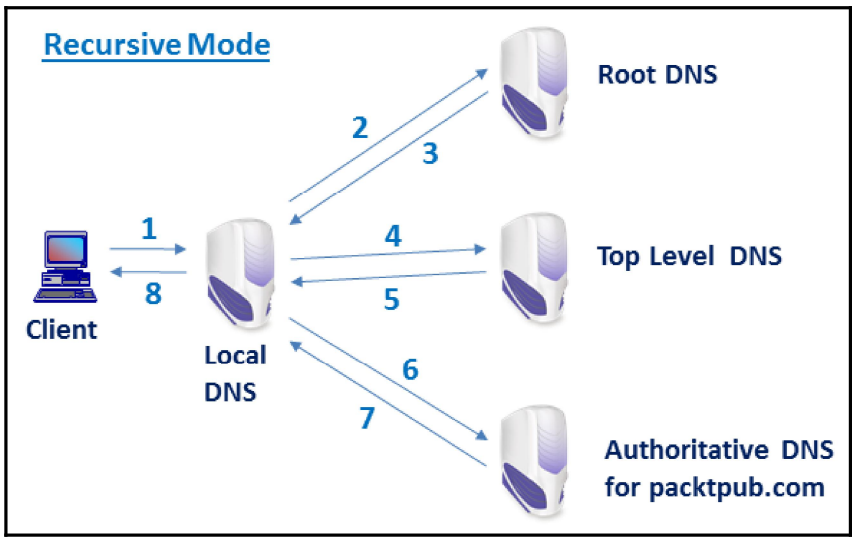
CNAME record		
Foo.example.com	Bar.example.com	CNAME
Bar.example.com	10.1.1.1	IP

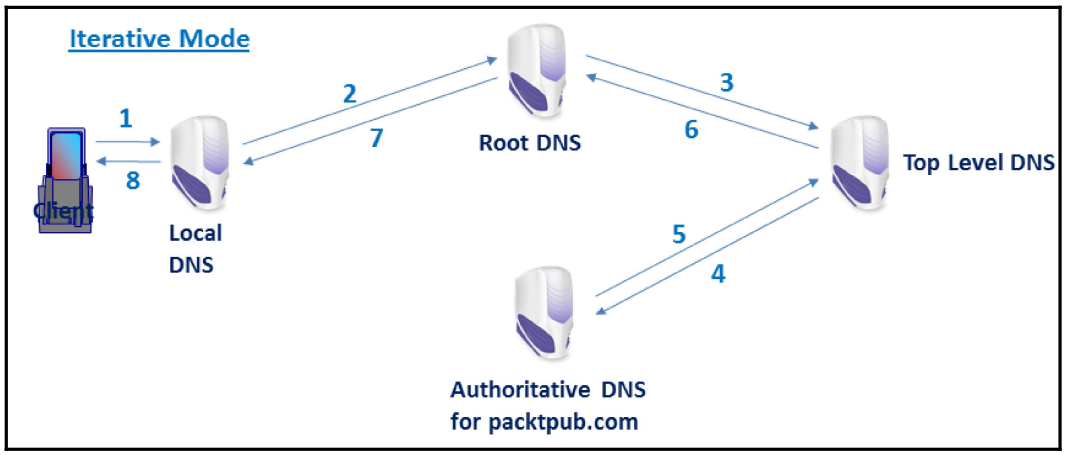
```
▶ User Datagram Protocol, Src Port: 67, Dst Port: 68
▼ Bootstrap Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x00000134
    Seconds elapsed: 0
  ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.2.0.3
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: fa:16:3e:08:9d:85 (fa:16:3e:08:9d:85)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Offer)
  ▶ Option: (61) Client identifier
  ▶ Option: (54) DHCP Server Identifier
  ▶ Option: (51) IP Address Lease Time
  ▶ Option: (58) Renewal Time Value
  ▶ Option: (59) Rebinding Time Value
  ▶ Option: (1) Subnet Mask
  ▶ Option: (3) Router
  ▼ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 192.168.0.7
  ▼ Option: (255) End
      Option End: 255
```



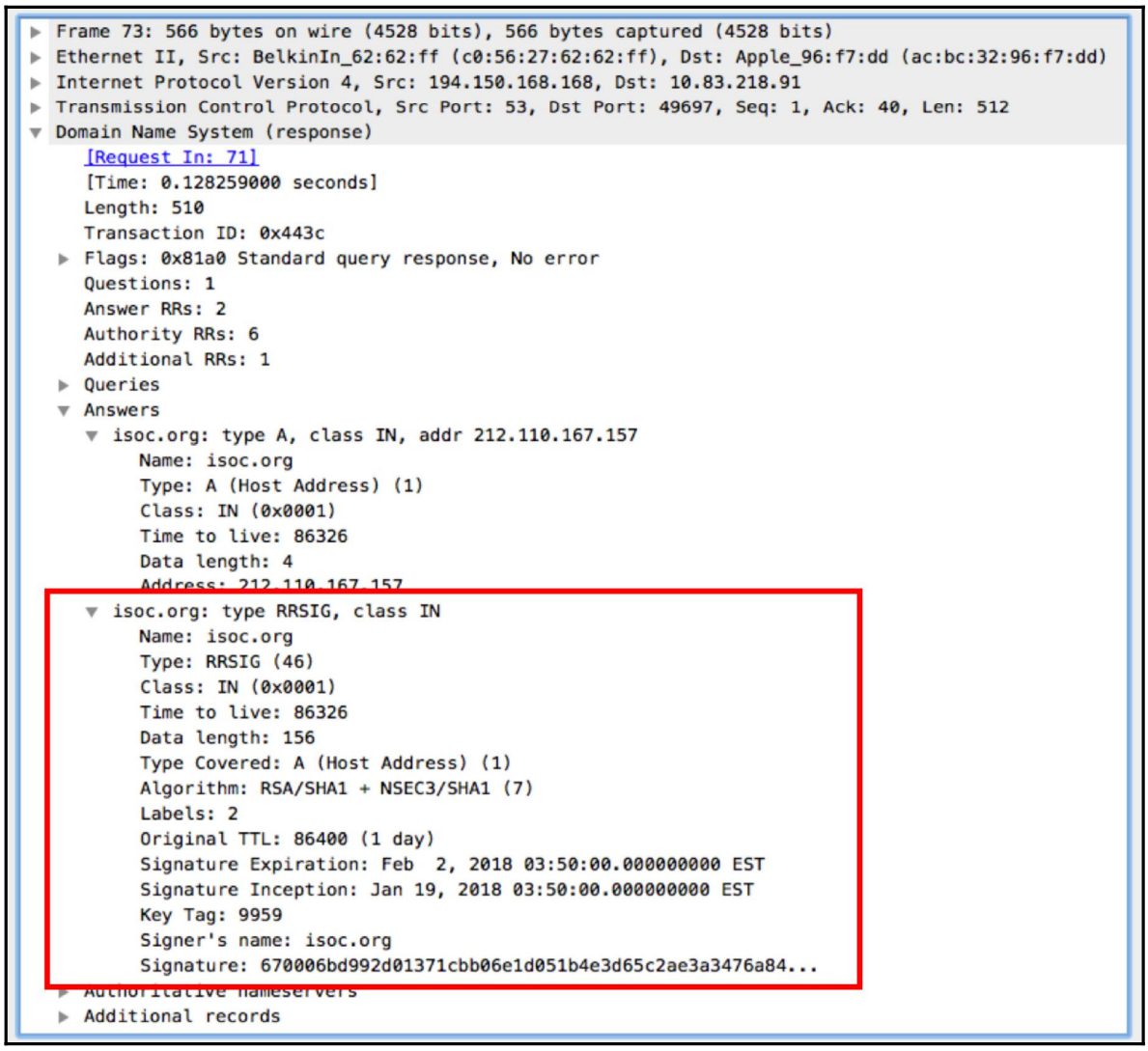

root
org
net
edu
com
il
uk
harvard
ucb
berkeley
bu
mit
ac
co
haas
coe
bcnm
bnrc
"root" zone
TLDs & ccTLDs
2LDs
3LDs
Legend:
TLD - Top Level Domain
ccTLD - Country Code TLD
nLD - n Level Domain


com
ndi-com.com domain
ndi-com
dev.ndi-com.com zone
mar.ndi-com.com zone
dev
sup
mar
na
emea
aspa
na
emea
aspa


Recursive Mode
Root DNS
Top Level DNS
Authoritative DNS
for packtpub.com
Client
Local
DNS
1
2
3
4
5
6
7
8

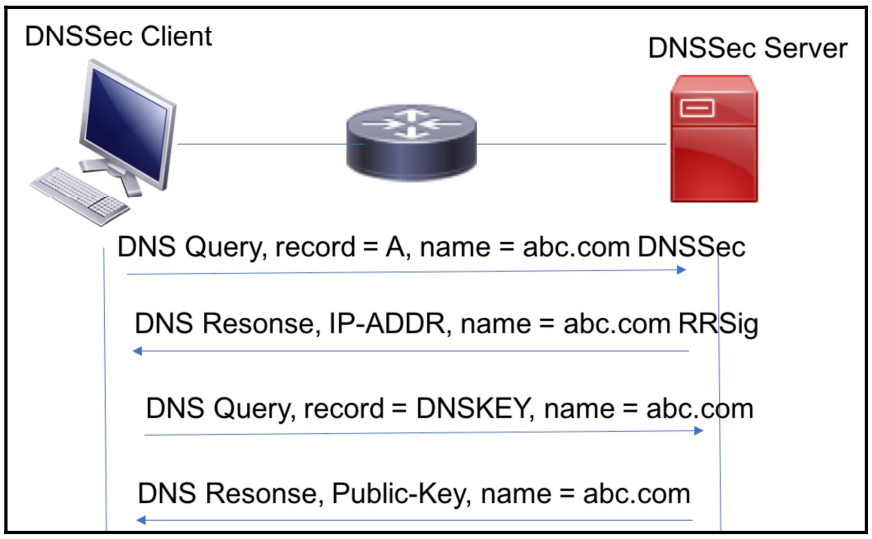


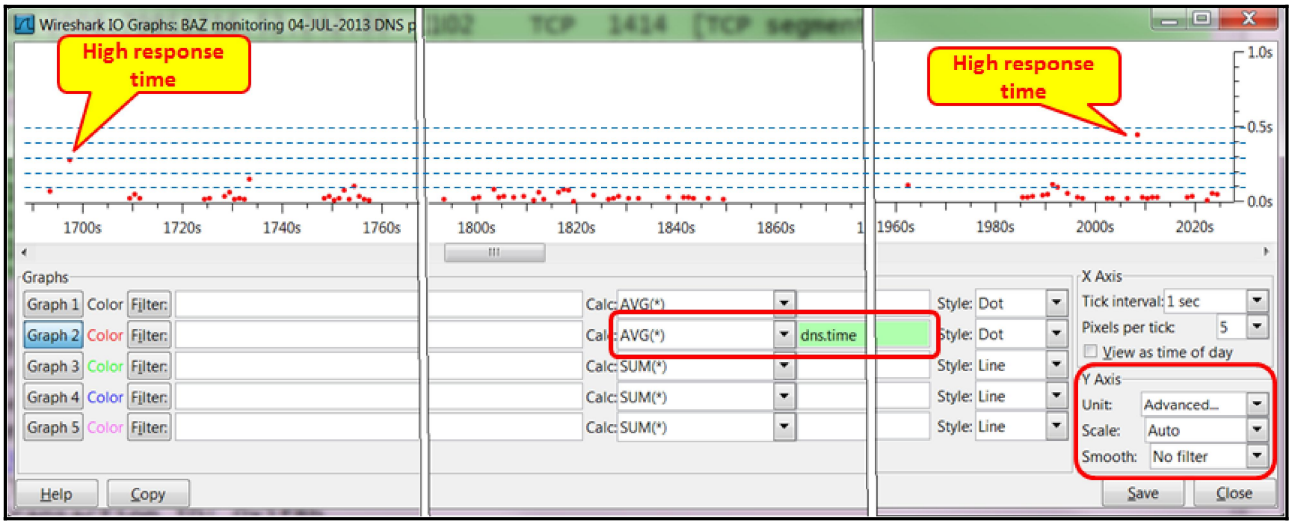

```
▶ Frame 71: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
▶ Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
▶ Internet Protocol Version 4, Src: 10.83.218.91, Dst: 194.150.168.168
▶ Transmission Control Protocol, Src Port: 49697, Dst Port: 53, Seq: 1, Ack: 1, Len: 39
▼ Domain Name System (query)
    [Response In: 73]
    Length: 37
    Transaction ID: 0x443c
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ isoc.org: type A, class IN
        Name: isoc.org
        [Name Length: 8]
        [Label Count: 2]
        Type: A (Host Address) (1)
        Class: IN (0x0001)
  ▼ Additional records
    ▼ <Root>: type OPT
        Name: <Root>
        Type: OPT (41)
        UDP payload size: 4096
        Higher bits in extended RCODE: 0x00
        EDNS0 version: 0
      ▼ Z: 0x8000
          1... .... .... .... = DO bit: Accepts DNSSEC security RRs
          .000 0000 0000 0000 = Reserved: 0x0000
        Data length: 0
```


Frame 73: 566 bytes on wire (4528 bits), 566 bytes captured (4528 bits)
Ethernet II, Src: BelkinIn_62:62:ff (c0:56:27:62:62:ff), Dst: Apple_96:f7:dd (ac:bc:32:96:f7:dd)
Internet Protocol Version 4, Src: 194.150.168.168, Dst: 10.83.218.91
Transmission Control Protocol, Src Port: 53, Dst Port: 49697, Seq: 1, Ack: 40, Len: 512
Domain Name System (response)
[Request In: 71]
[Time: 0.128259000 seconds]
Length: 510
Transaction ID: 0x443c
Flags: 0x81a0 Standard query response, No error
Questions: 1
Answer RRs: 2
Authority RRs: 6
Additional RRs: 1
Queries
Answers
isoc.org: type A, class IN, addr 212.110.167.157
Name: isoc.org
Type: A (Host Address) (1)
Class: IN (0x0001)
Time to live: 86326
Data length: 4
Address: 212.110.167.157
isoc.org: type RRSIG, class IN
Name: isoc.org
Type: RRSIG (46)
Class: IN (0x0001)
Time to live: 86326
Data length: 156
Type Covered: A (Host Address) (1)
Algorithm: RSA/SHA1 + NSEC3/SHA1 (7)
Labels: 2
Original TTL: 86400 (1 day)
Signature Expiration: Feb 2, 2018 03:50:00.000000000 EST
Signature Inception: Jan 19, 2018 03:50:00.000000000 EST
Key Tag: 9959
Signer's name: isoc.org
Signature: 670006bd992d01371cbb06e1d051b4e3d65c2ae3a3476a84...
Additional records

```
▶ Frame 84: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)
▶ Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
▶ Internet Protocol Version 4, Src: 10.83.218.91, Dst: 194.150.168.168
▶ Transmission Control Protocol, Src Port: 49698, Dst Port: 53, Seq: 1, Ack: 1, Len: 39
▼ Domain Name System (query)
    [Response In: 86]
    Length: 37
    Transaction ID: 0xdd86
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▼ isoc.org: type DNSKEY, class IN
        Name: isoc.org
        [Name Length: 8]
        [Label Count: 2]
        Type: DNSKEY (48)
        Class: IN (0x0001)
  ▶ Additional records
```

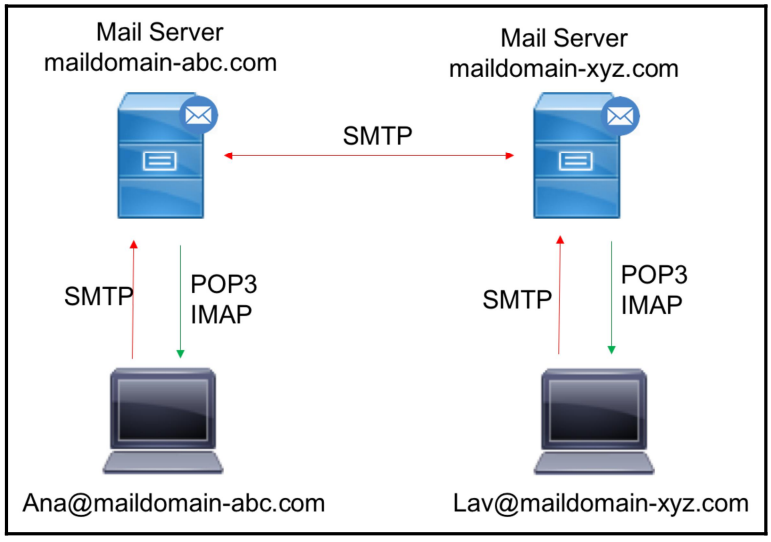
```
▶ Frame 86: 813 bytes on wire (6504 bits), 813 bytes captured (6504 bits)
▶ Ethernet II, Src: BelkinIn_62:62:ff (c0:56:27:62:62:ff), Dst: Apple_96:f7:dd (ac:bc:32:96:f7:dd)
▶ Internet Protocol Version 4, Src: 194.150.168.168, Dst: 10.83.218.91
▶ Transmission Control Protocol, Src Port: 53, Dst Port: 49698, Seq: 1, Ack: 40, Len: 759
▼ Domain Name System (response)
    [Request In: 84]
    [Time: 0.127825000 seconds]
    Length: 757
    Transaction ID: 0xdd86
  ▶ Flags: 0x81a0 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 1
  ▶ Queries
  ▼ Answers
    ▶ isoc.org: type DNSKEY, class IN
    ▼ isoc.org: type DNSKEY, class IN
        Name: isoc.org
        Type: DNSKEY (48)
        Class: IN (0x0001)
        Time to live: 13831
        Data length: 136
      ▶ Flags: 0x0100
        Protocol: 3
        Algorithm: RSA/SHA1 + NSEC3/SHA1 (7)
        [Key id: 9959]
        Public Key: 03010001aeeeb166fe5dda4762de2d5e551ebd9fe132639d...
    ▶ isoc.org: type RRSIG, class IN
  ▶ Additional records
```

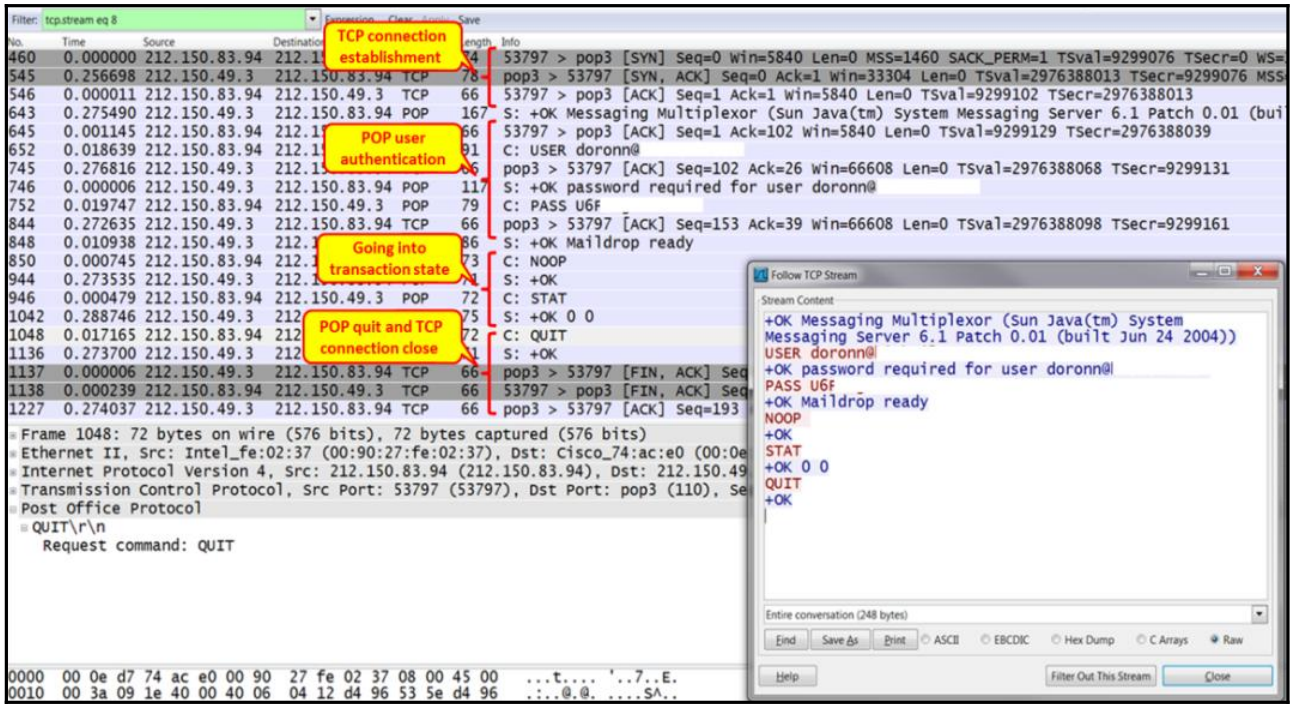

DNSSec Client
DNSSec Server
DNS Query, record = A, name = abc.com DNSSec
DNS Resonse, IP-ADDR, name = abc.com RRSig
DNS Query, record = DNSKEY, name = abc.com
DNS Resonse, Public-Key, name = abc.com

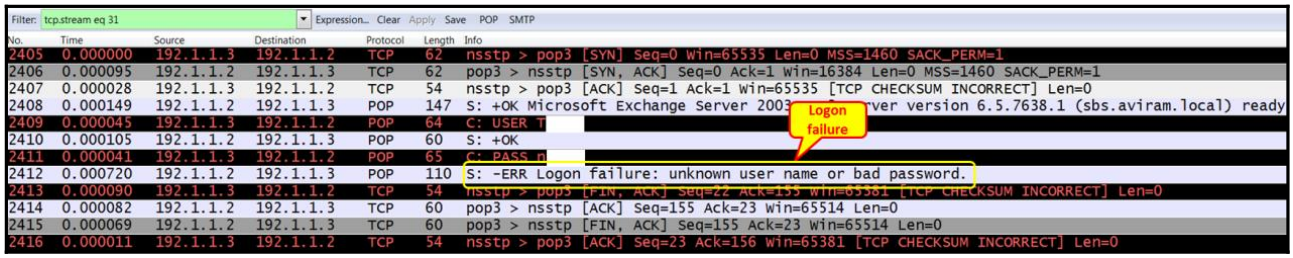

Wireshark IO Graphs: BAZ monitoring 04-JUL-2013 DNS p
High response time
High response time
1.0s
0.5s
0.0s
1700s
1720s
1740s
1760s
1800s
1820s
1840s
1860s
1960s
1980s
2000s
2020s
Graphs
Graph 1 Color Filter:
Graph 2 Color Filter:
Graph 3 Color Filter:
Graph 4 Color Filter:
Graph 5 Color Filter:
Calc: AVG(*)
Calc: AVG(*) dns.time
Calc: SUM(*)
Calc: SUM(*)
Calc: SUM(*)
Style: Dot
Style: Dot
Style: Line
Style: Line
Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Advanced...
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close

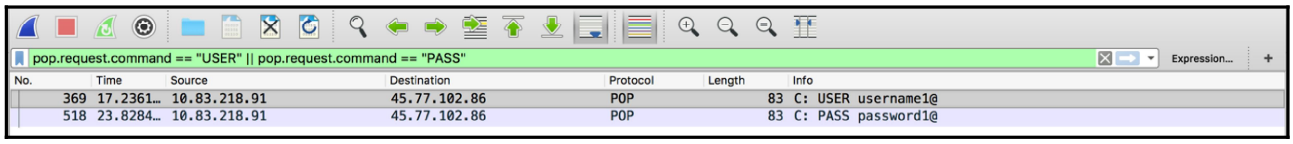
```
Ubuntu:~ naikumar$ dig www.packtpub.com

; <<>> DiG 9.8.3-P1 <<>> www.packtpub.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4108
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 13, ADDITIONAL: 0

;; QUESTION SECTION:
;www.packtpub.com.      IN  A

;; ANSWER SECTION:
www.packtpub.com.   5   IN  CNAME   varnish.packtpub.com.
varnish.packtpub.com.   5   IN  A   83.166.169.231

;; AUTHORITY SECTION:
com.            172739  IN  NS  j.gtld-servers.net.

;; Query time: 60 msec
;; SERVER: 64.102.6.247#53(64.102.6.247)
;; WHEN: Fri Jan 19 16:48:54 2018
;; MSG SIZE  rcvd: 296

Ubuntu:~ naikumar$
```

Chapter 14: Analyzing Mail Protocols

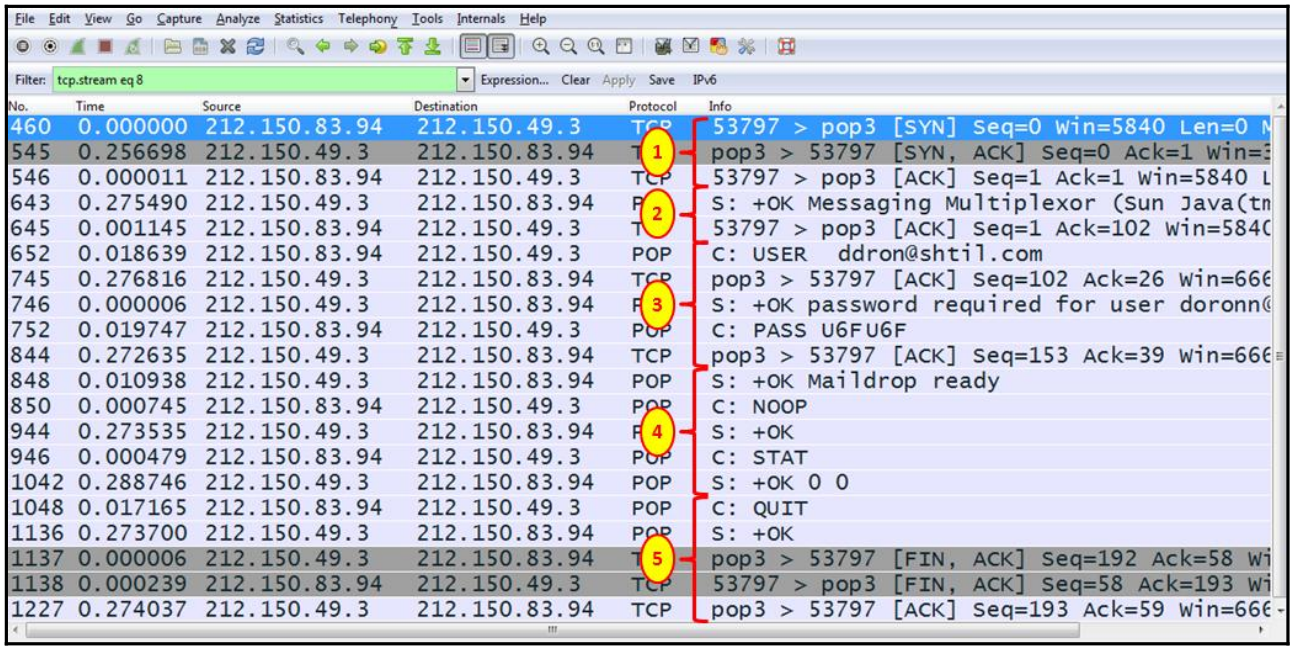


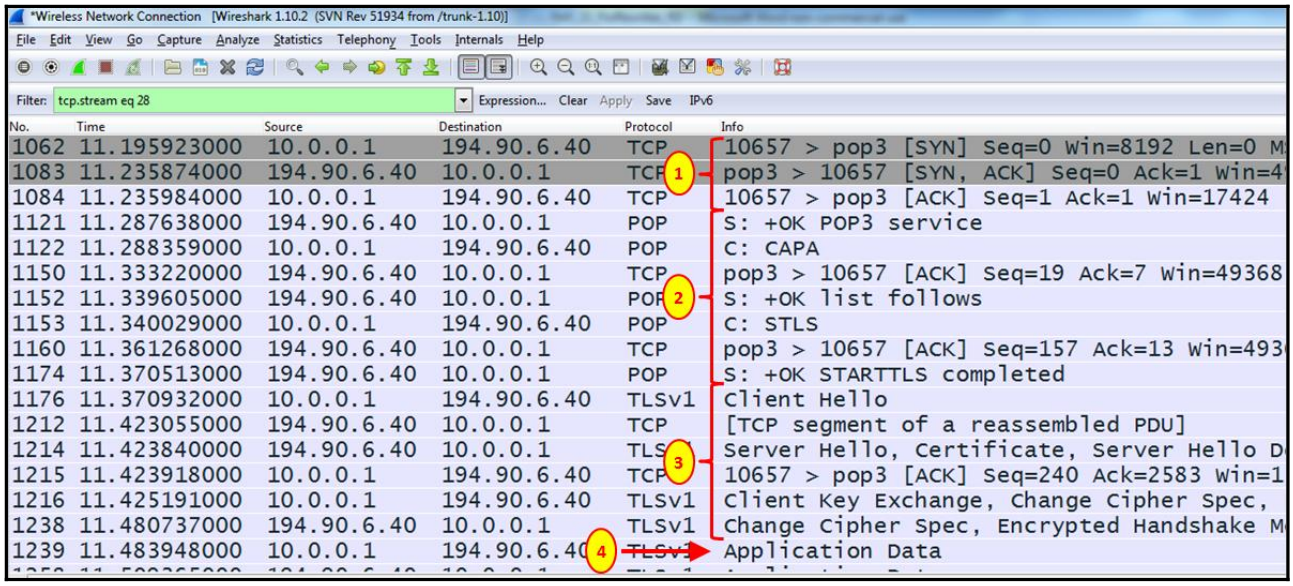


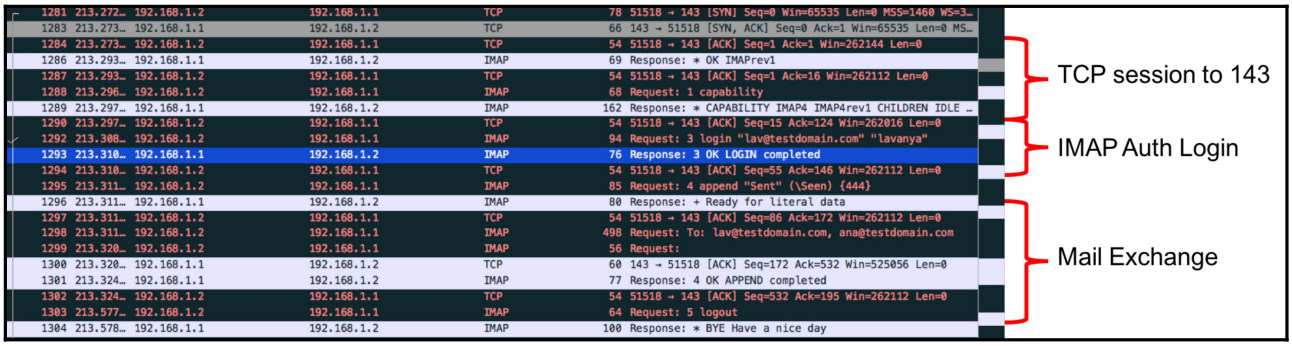


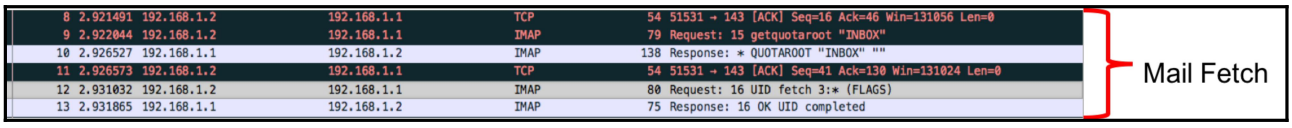


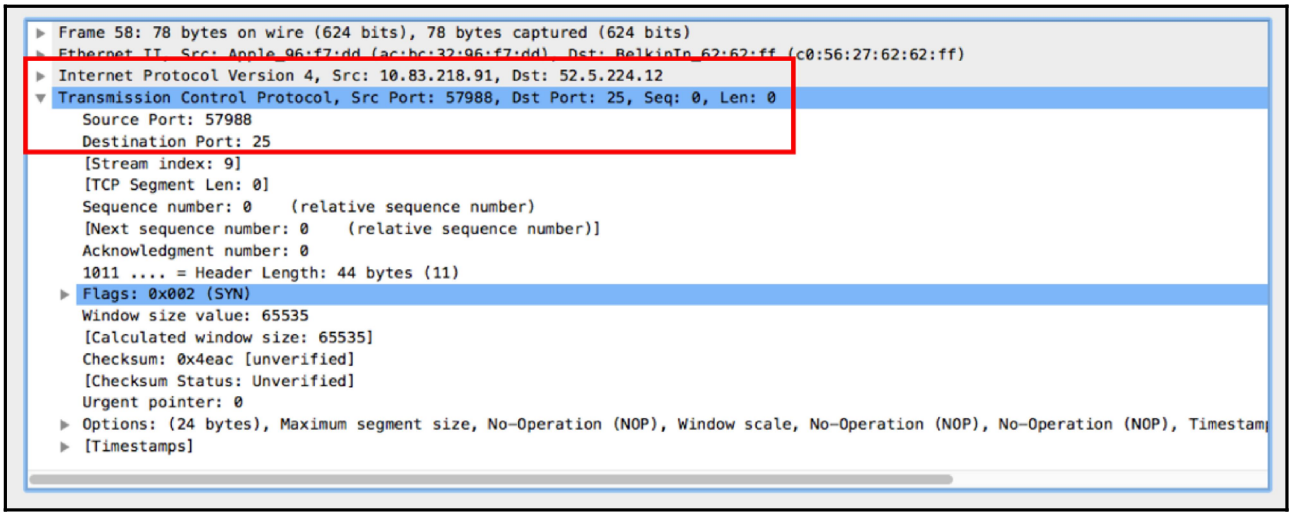

```
Trying 10.1.1.1...
Connected to smtp-server.
Escape character is '^]'.
220 smtp-server ESMTP ready
AUTH LOGIN
334 VXNlcm5hbWU6
<enter username>
334 UGFzc3dvcmQ6
<enter password>
235 2.0.0 OK
MAIL FROM:ana@domain-abc.com
250 2.1.0 Ok
RCPT TO:lav@domain-xyz.com
 250 2.1.0 Ok
DATA
354 Go ahead
test123.
250 2.0.0 Ok: queued
```

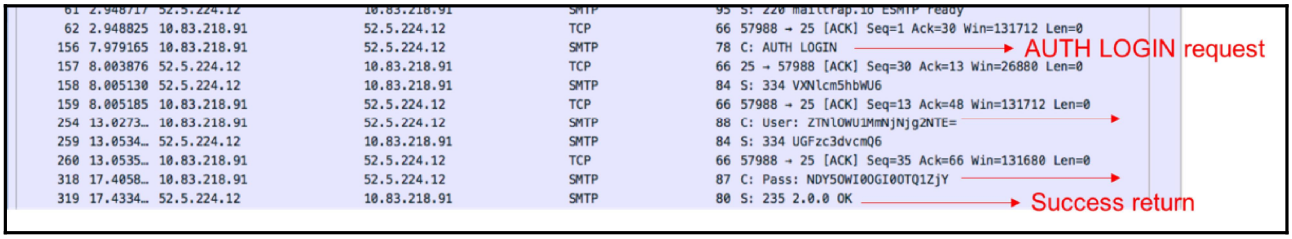

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 8
Expression... Clear Apply Save IPv6
No. Time Source Destination Protocol Info
460 0.000000 212.150.83.94 212.150.49.3 TCP 53797 > pop3 [SYN] Seq=0 Win=5840 Len=0
545 0.256698 212.150.49.3 212.150.83.94 TCP pop3 > 53797 [SYN, ACK] Seq=0 Ack=1 Win=
546 0.000011 212.150.83.94 212.150.49.3 TCP 53797 > pop3 [ACK] Seq=1 Ack=1 Win=5840
643 0.275490 212.150.49.3 212.150.83.94 POP S: +OK Messaging Multiplexor (Sun Java(tm
645 0.001145 212.150.83.94 212.150.49.3 TCP 53797 > pop3 [ACK] Seq=1 Ack=102 Win=584
652 0.018639 212.150.83.94 212.150.49.3 POP C: USER ddron@shtil.com
745 0.276816 212.150.49.3 212.150.83.94 TCP pop3 > 53797 [ACK] Seq=102 Ack=26 Win=66
746 0.000006 212.150.49.3 212.150.83.94 POP S: +OK password required for user doronn
752 0.019747 212.150.83.94 212.150.49.3 POP C: PASS U6FU6F
844 0.272635 212.150.49.3 212.150.83.94 TCP pop3 > 53797 [ACK] Seq=153 Ack=39 Win=66
848 0.010938 212.150.49.3 212.150.83.94 POP S: +OK Maildrop ready
850 0.000745 212.150.83.94 212.150.49.3 POP C: NOOP
944 0.273535 212.150.49.3 212.150.83.94 POP S: +OK
946 0.000479 212.150.83.94 212.150.49.3 POP C: STAT
1042 0.288746 212.150.49.3 212.150.83.94 POP S: +OK 0 0
1048 0.017165 212.150.83.94 212.150.49.3 POP C: QUIT
1136 0.273700 212.150.49.3 212.150.83.94 POP S: +OK
1137 0.000006 212.150.49.3 212.150.83.94 TCP pop3 > 53797 [FIN, ACK] Seq=192 Ack=58 W
1138 0.000239 212.150.83.94 212.150.49.3 TCP 53797 > pop3 [FIN, ACK] Seq=58 Ack=193 W
1227 0.274037 212.150.49.3 212.150.83.94 TCP pop3 > 53797 [ACK] Seq=193 Ack=59 Win=66
1
2
3
4
5

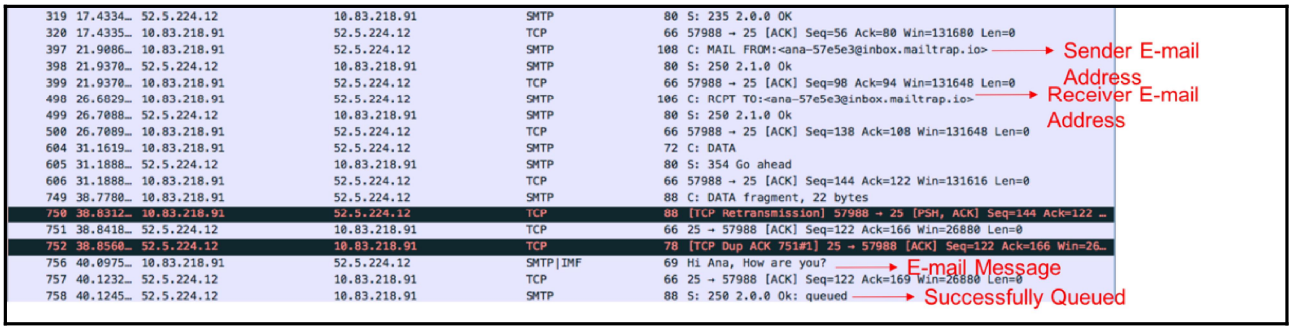

*Wireless Network Connection [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 28
Expression... Clear Apply Save IPv6
No. Time Source Destination Protocol Info
1062 11.195923000 10.0.0.1 194.90.6.40 TCP 10657 > pop3 [SYN] Seq=0 Win=8192 Len=0
1083 11.235874000 194.90.6.40 10.0.0.1 TCP pop3 > 10657 [SYN, ACK] Seq=0 Ack=1 Win=
1084 11.235984000 10.0.0.1 194.90.6.40 TCP 10657 > pop3 [ACK] Seq=1 Ack=1 Win=17424
1121 11.287638000 194.90.6.40 10.0.0.1 POP S: +OK POP3 service
1122 11.288359000 10.0.0.1 194.90.6.40 POP C: CAPA
1150 11.333220000 194.90.6.40 10.0.0.1 TCP pop3 > 10657 [ACK] Seq=19 Ack=7 Win=49368
1152 11.339605000 194.90.6.40 10.0.0.1 POP S: +OK list follows
1153 11.340029000 10.0.0.1 194.90.6.40 POP C: STLS
1160 11.361268000 194.90.6.40 10.0.0.1 TCP pop3 > 10657 [ACK] Seq=157 Ack=13 Win=493
1174 11.370513000 194.90.6.40 10.0.0.1 POP S: +OK STARTTLS completed
1176 11.370932000 10.0.0.1 194.90.6.40 TLSv1 Client Hello
1212 11.423055000 194.90.6.40 10.0.0.1 TCP [TCP segment of a reassembled PDU]
1214 11.423840000 194.90.6.40 10.0.0.1 TLS Server Hello, Certificate, Server Hello D
1215 11.423918000 10.0.0.1 194.90.6.40 TCP 10657 > pop3 [ACK] Seq=240 Ack=2583 Win=1
1216 11.425191000 10.0.0.1 194.90.6.40 TLSv1 Client Key Exchange, Change Cipher Spec,
1238 11.480737000 194.90.6.40 10.0.0.1 TLSv1 Change Cipher Spec, Encrypted Handshake M
1239 11.483948000 10.0.0.1 194.90.6.40 TLSv1 Application Data
1
2
3
4

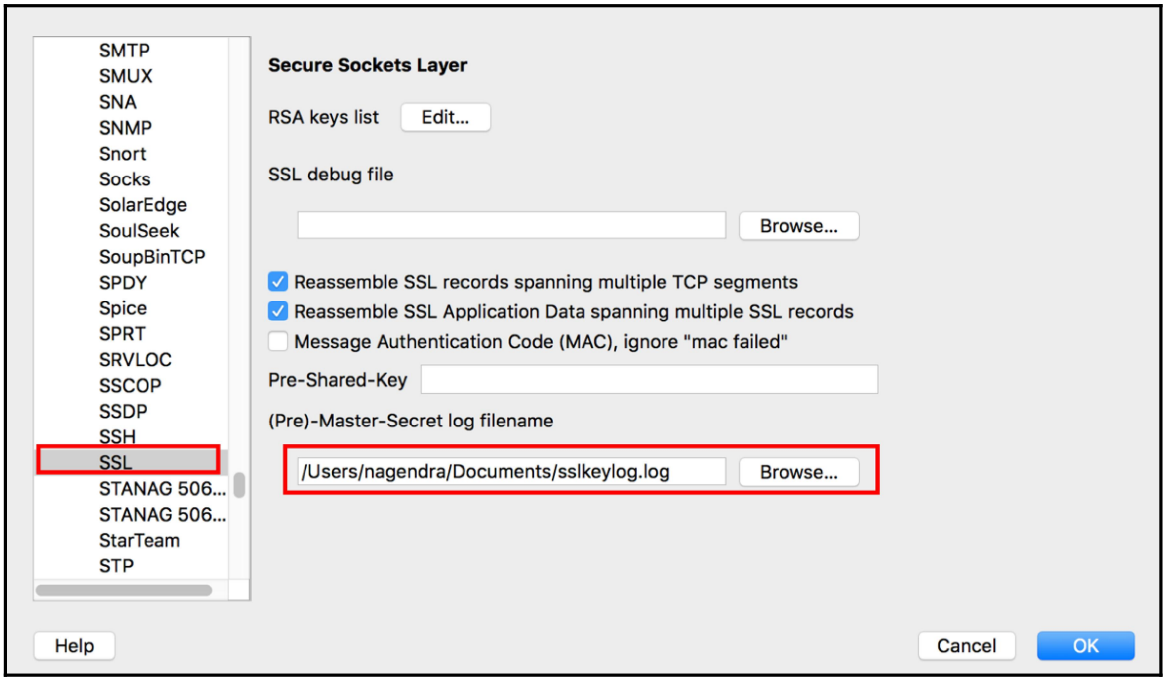

1281 213.272… 192.168.1.2 192.168.1.1 TCP 78 51518 → 143 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3…
1283 213.273… 192.168.1.1 192.168.1.2 TCP 66 143 → 51518 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MS…
1284 213.273… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=1 Ack=1 Win=262144 Len=0
1286 213.293… 192.168.1.1 192.168.1.2 IMAP 69 Response: * OK IMAPrev1
1287 213.293… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=1 Ack=16 Win=262112 Len=0
1288 213.296… 192.168.1.2 192.168.1.1 IMAP 68 Request: 1 capability
1289 213.297… 192.168.1.1 192.168.1.2 IMAP 162 Response: * CAPABILITY IMAP4 IMAP4rev1 CHILDREN IDLE …
1290 213.297… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=15 Ack=124 Win=262016 Len=0
1292 213.308… 192.168.1.2 192.168.1.1 IMAP 94 Request: 3 login "lav@testdomain.com" "lavanya"
1293 213.310… 192.168.1.1 192.168.1.2 IMAP 76 Response: 3 OK LOGIN completed
1294 213.310… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=55 Ack=146 Win=262112 Len=0
1295 213.311… 192.168.1.2 192.168.1.1 IMAP 85 Request: 4 append "Sent" (\Seen) {444}
1296 213.311… 192.168.1.1 192.168.1.2 IMAP 80 Response: + Ready for literal data
1297 213.311… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=86 Ack=172 Win=262112 Len=0
1298 213.311… 192.168.1.2 192.168.1.1 IMAP 498 Request: To: lav@testdomain.com, ana@testdomain.com
1299 213.320… 192.168.1.2 192.168.1.1 IMAP 56 Request:
1300 213.320… 192.168.1.1 192.168.1.2 TCP 60 143 → 51518 [ACK] Seq=172 Ack=532 Win=525056 Len=0
1301 213.324… 192.168.1.1 192.168.1.2 IMAP 77 Response: 4 OK APPEND completed
1302 213.324… 192.168.1.2 192.168.1.1 TCP 54 51518 → 143 [ACK] Seq=532 Ack=195 Win=262112 Len=0
1303 213.577… 192.168.1.2 192.168.1.1 IMAP 64 Request: 5 logout
1304 213.578… 192.168.1.1 192.168.1.2 IMAP 100 Response: * BYE Have a nice day
TCP session to 143
IMAP Auth Login
Mail Exchange

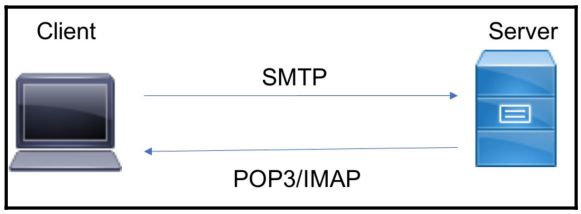

8 2.921491 192.168.1.2 192.168.1.1 TCP 54 51531 → 143 [ACK] Seq=16 Ack=46 Win=131056 Len=0
9 2.922044 192.168.1.2 192.168.1.1 IMAP 79 Request: 15 getquotaroot "INBOX"
10 2.926527 192.168.1.1 192.168.1.2 IMAP 138 Response: * QUOTAROOT "INBOX" ""
11 2.926573 192.168.1.2 192.168.1.1 TCP 54 51531 → 143 [ACK] Seq=41 Ack=130 Win=131024 Len=0
12 2.931032 192.168.1.2 192.168.1.1 IMAP 80 Request: 16 UID fetch 3:* (FLAGS)
13 2.931865 192.168.1.1 192.168.1.2 IMAP 75 Response: 16 OK UID completed
Mail Fetch

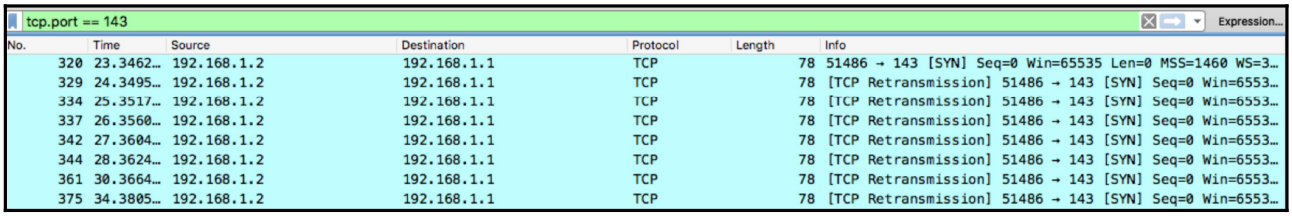

Frame 58: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
Internet Protocol Version 4, Src: 10.83.218.91, Dst: 52.5.224.12
Transmission Control Protocol, Src Port: 57988, Dst Port: 25, Seq: 0, Len: 0
Source Port: 57988
Destination Port: 25
[Stream index: 9]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0
1011 .... = Header Length: 44 bytes (11)
Flags: 0x002 (SYN)
Window size value: 65535
[Calculated window size: 65535]
Checksum: 0x4eac [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
Options: (24 bytes), Maximum segment size, No-Operation (NOP), Window scale, No-Operation (NOP), No-Operation (NOP), Timestamp
[Timestamps]


62 2.948825 10.83.218.91 52.5.224.12 TCP 66 57988 → 25 [ACK] Seq=1 Ack=30 Win=131712 Len=0
156 7.979165 10.83.218.91 52.5.224.12 SMTP 78 C: AUTH LOGIN
AUTH LOGIN request
157 8.003876 52.5.224.12 10.83.218.91 TCP 66 25 → 57988 [ACK] Seq=30 Ack=13 Win=26880 Len=0
158 8.005130 52.5.224.12 10.83.218.91 SMTP 84 S: 334 VXNlcm5hbWU6
159 8.005185 10.83.218.91 52.5.224.12 TCP 66 57988 → 25 [ACK] Seq=13 Ack=48 Win=131712 Len=0
254 13.0273… 10.83.218.91 52.5.224.12 SMTP 88 C: User: ZTNlOWU1MmNjNjg2NTE=
259 13.0534… 52.5.224.12 10.83.218.91 SMTP 84 S: 334 UGFzc3dvcmQ6
260 13.0535… 10.83.218.91 52.5.224.12 TCP 66 57988 → 25 [ACK] Seq=35 Ack=66 Win=131680 Len=0
318 17.4058… 10.83.218.91 52.5.224.12 SMTP 87 C: Pass: NDY5OWI0OGI0OTQ1ZjY
319 17.4334… 52.5.224.12 10.83.218.91 SMTP 80 S: 235 2.0.0 OK
Success return


Sender E-mail Address
Receiver E-mail Address
E-mail Message
Successfully Queued


SMTP
SMUX
SNA
SNMP
Snort
Socks
SolarEdge
SoulSeek
SoupBinTCP
SPDY
Spice
SPRT
SRVLOC
SSCOP
SSDP
SSH
SSL
STANAG 506...
STANAG 506...
StarTeam
STP
Secure Sockets Layer
RSA keys list
Edit...
SSL debug file
Browse...
Reassemble SSL records spanning multiple TCP segments
Reassemble SSL Application Data spanning multiple SSL records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared-Key
(Pre)-Master-Secret log filename
/Users/nagendra/Documents/sslkeylog.log
Browse...
Help
Cancel
OK


Client
Server
SMTP
POP3/IMAP


tcp.port == 143
Expression...
No. Time Source Destination Protocol Length Info
320 23.3462… 192.168.1.2 192.168.1.1 TCP 78 51486 → 143 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3…
329 24.3495… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
334 25.3517… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
337 26.3560… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
342 27.3604… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
344 28.3624… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
361 30.3664… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…
375 34.3805… 192.168.1.2 192.168.1.1 TCP 78 [TCP Retransmission] 51486 → 143 [SYN] Seq=0 Win=6553…

```
▶ Frame 76: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits)
▼ Ethernet II, Src: QuantaCo_d2:be:29 (c4:54:44:d2:be:29), Dst: Apple_3b:34:fc (a8:20:66:3b:34:fc)
  ▼ Destination: Apple_3b:34:fc (a8:20:66:3b:34:fc)
      Address: Apple_3b:34:fc (a8:20:66:3b:34:fc)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  ▼ Source: QuantaCo_d2:be:29 (c4:54:44:d2:be:29)
      Address: QuantaCo_d2:be:29 (c4:54:44:d2:be:29)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2
▶ Transmission Control Protocol, Src Port: 143, Dst Port: 52605, Seq: 124, Ack: 36, Len: 81
▼ Internet Message Access Protocol
  ▼ Line: 3 NO Invalid user name or password. Please use full email address as user name.\r\n
      Response Tag: 3
      Response Status: NO
      Response: NO Invalid user name or password. Please use full email address as user name.
```

Filter: tcp.analysis.retransmission — Expression... Clear Apply Save POP SMTP

No.	Time	Source	Destination	Protocol	Length	Info
4125	0.001469	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4127	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4129	0.000754	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4131	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4143	0.001762	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4145	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4147	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4152	0.000738	192.5.11.98	172.16.30.243	SMB	130	[TCP Retransmission] Trans2 Request, QUERY_FILE_INFO,
4154	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4156	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4158	0.000001	172.16.30.113	192.5.11.73	SMTP	566	[TCP Retransmission] C: DATA fragment, 500 bytes
4160	0.000001	172.16.30.243	192.5.11.98	SMB	142	[TCP Retransmission] Trans2 Response<unknown>

Conversations: cap 18-JUN-2013 - 001 SMTP problem.pcapng

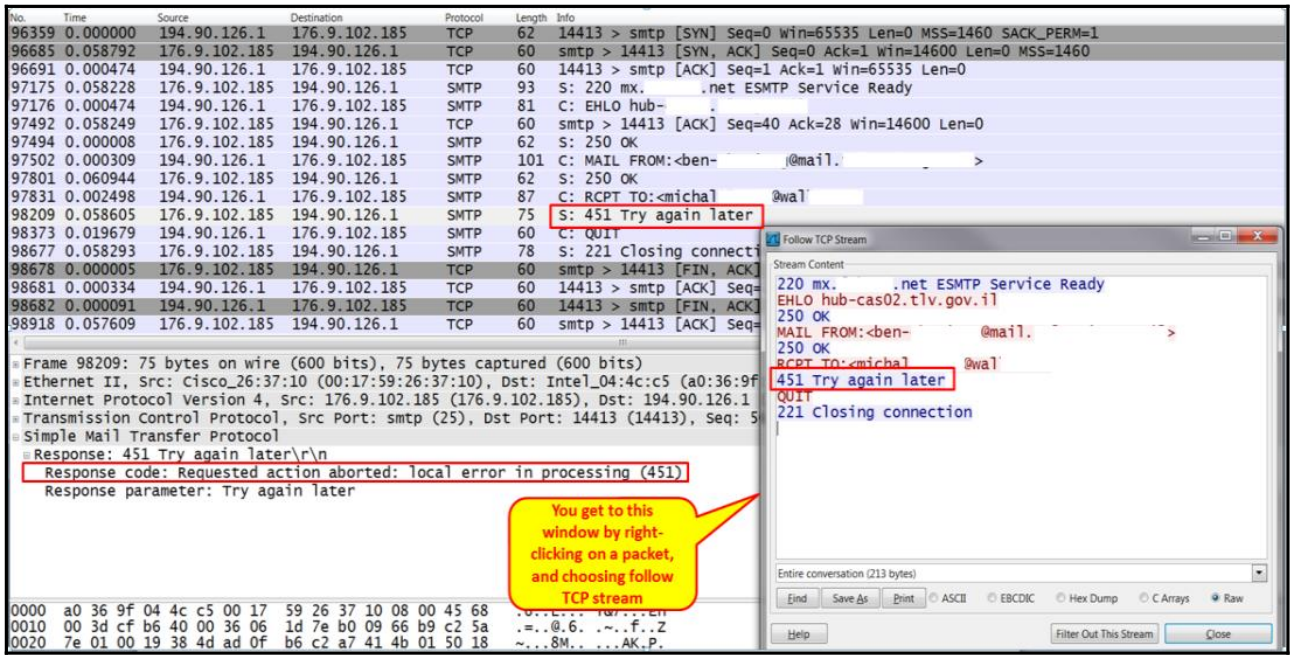
Ethernet: 150 | Fibre Channel | FDDI | IPv4: 351 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 787 | Token Ring | UDP | USB | WLAN

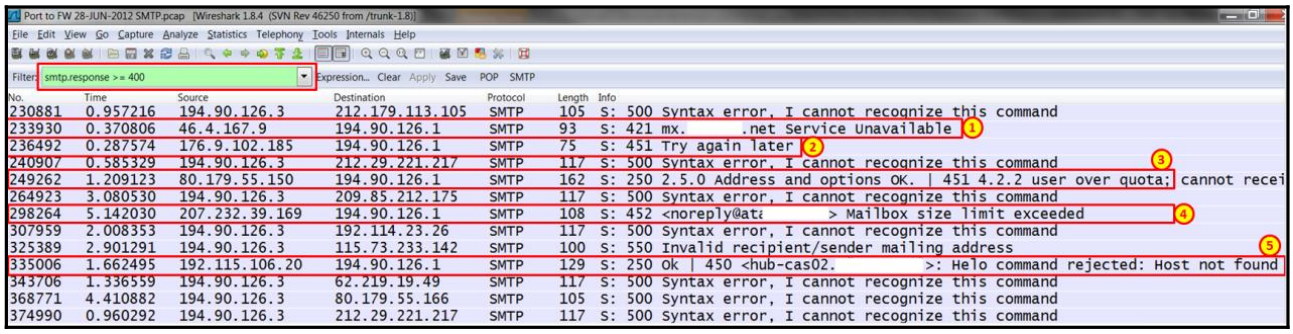
TCP Conversations - Filter: tcp.analysis.retransmission

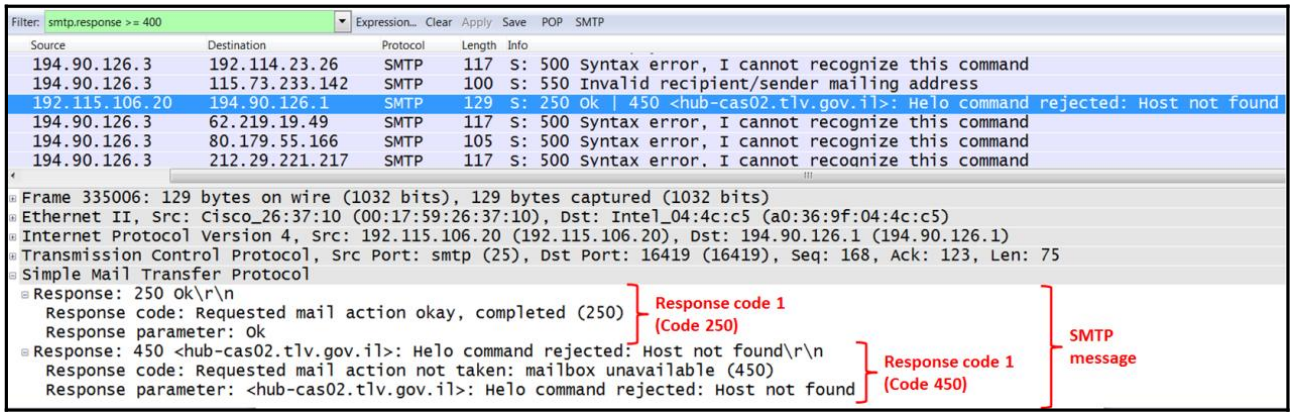
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A→B	Bytes A→B
172.16.30.247	3223	172.16.30.2	445	9 014	1 317 662	4 480	896 000
172.16.30.180	2329	192.5.11.198	80	2 319	3 499 838	3	2 015
172.16.30.176	1506	172.16.30.1	445	2 219	568 221	1 088	253 635
172.16.30.190	57820	192.5.11.73	30428	2 141	3 017 378	2 025	2 991 498
84.95.199.235	25168	172.16.30.176	3506	2 060	400 553	1 041	238 073
192.5.11.73	38508	172.16.30.226	4317	1 820	2 541 120	112	26 160
192.5.11.73	38508	172.16.30.233	1133	802	1 175 548	784	1 171 344
172.16.30.113	1109	192.5.11.73	25	793	442 147	787	441 401
172.16.30.180	2023	192.5.11.198	80	637	954 323	6	4 055
172.16.30.109	58857	192.5.11.73	38508	618	810 444	296	380 788

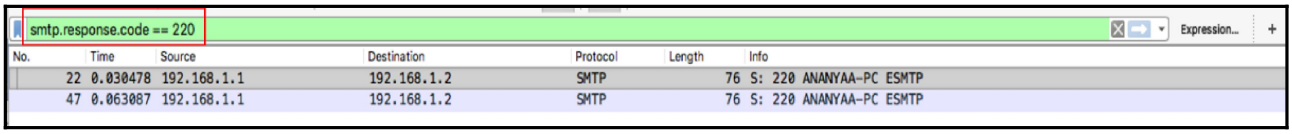
Name resolution | Limit to display filter

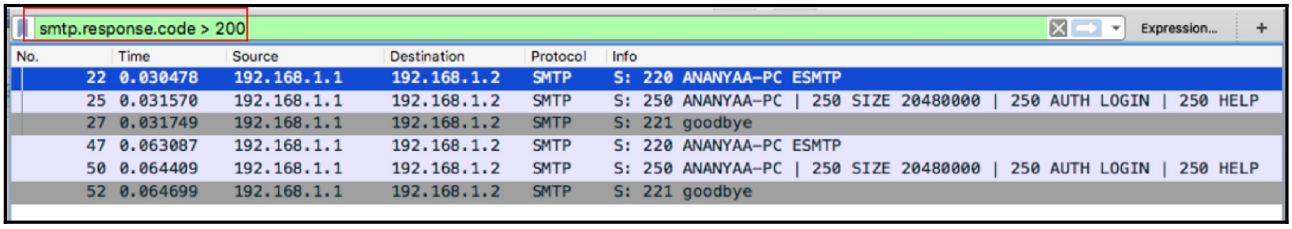
Help | Copy | Follow Stream | Close

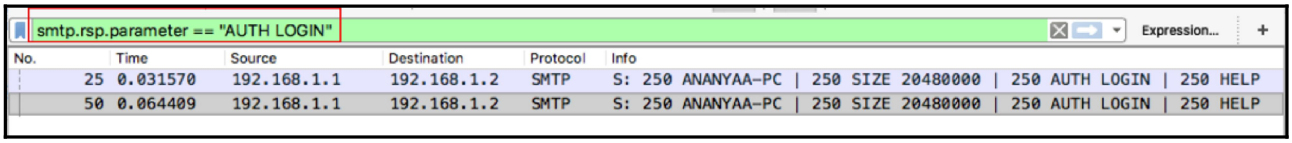

No. Time Source Destination Protocol Length Info
96359 0.000000 194.90.126.1 176.9.102.185 TCP 62 14413 > smtp [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
96685 0.058792 176.9.102.185 194.90.126.1 TCP 60 smtp > 14413 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
96691 0.000474 194.90.126.1 176.9.102.185 TCP 60 14413 > smtp [ACK] Seq=1 Ack=1 Win=65535 Len=0
97175 0.058228 176.9.102.185 194.90.126.1 SMTP 93 S: 220 mx. .net ESMTP Service Ready
97176 0.000474 194.90.126.1 176.9.102.185 SMTP 81 C: EHLO hub-
97492 0.058249 176.9.102.185 194.90.126.1 TCP 60 smtp > 14413 [ACK] Seq=40 Ack=28 Win=14600 Len=0
97494 0.000008 176.9.102.185 194.90.126.1 SMTP 62 S: 250 OK
97502 0.000309 194.90.126.1 176.9.102.185 SMTP 101 C: MAIL FROM:<ben- @mail. >
97801 0.060944 176.9.102.185 194.90.126.1 SMTP 62 S: 250 OK
97831 0.002498 194.90.126.1 176.9.102.185 SMTP 87 C: RCPT TO:<michal @wal
98209 0.058605 176.9.102.185 194.90.126.1 SMTP 75 S: 451 Try again later
98373 0.019679 194.90.126.1 176.9.102.185 SMTP 60 C: QUIT
98677 0.058293 176.9.102.185 194.90.126.1 SMTP 78 S: 221 Closing connecti
98678 0.000005 176.9.102.185 194.90.126.1 TCP 60 smtp > 14413 [FIN, ACK]
98681 0.000334 194.90.126.1 176.9.102.185 TCP 60 14413 > smtp [ACK] Seq=
98682 0.000091 194.90.126.1 176.9.102.185 TCP 60 14413 > smtp [FIN, ACK]
98918 0.057609 176.9.102.185 194.90.126.1 TCP 60 smtp > 14413 [ACK] Seq=
Frame 98209: 75 bytes on wire (600 bits), 75 bytes captured (600 bits)
Ethernet II, Src: Cisco_26:37:10 (00:17:59:26:37:10), Dst: Intel_04:4c:c5 (a0:36:9f
Internet Protocol Version 4, Src: 176.9.102.185 (176.9.102.185), Dst: 194.90.126.1
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 14413 (14413), Seq: 5
Simple Mail Transfer Protocol
Response: 451 Try again later\r\n
Response code: Requested action aborted: local error in processing (451)
Response parameter: Try again later
0000 a0 36 9f 04 4c c5 00 17 59 26 37 10 08 00 45 68
0010 00 3d cf b6 40 00 36 06 1d 7e b0 09 66 b9 c2 5a
0020 7e 01 00 19 38 4d ad 0f b6 c2 a7 41 4b 01 50 18
You get to this window by right-clicking on a packet, and choosing follow TCP stream
Follow TCP Stream
Stream Content
220 mx. .net ESMTP Service Ready
EHLO hub-cas02.tlv.gov.il
250 OK
MAIL FROM:<ben- @mail. >
250 OK
RCPT TO:<michal @wal
451 Try again later
QUIT
221 Closing connection
Entire conversation (213 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close

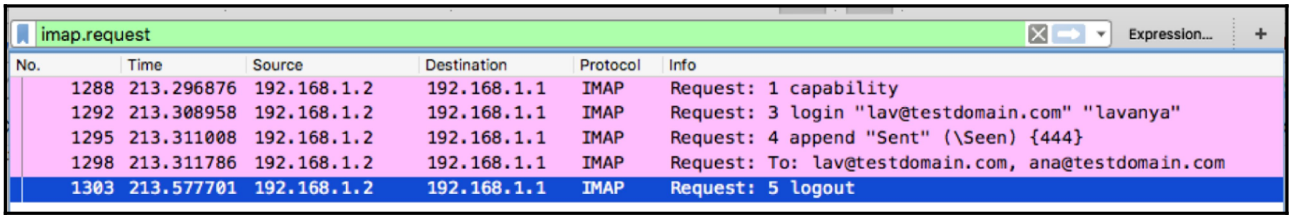

Port to FW 28-JUN-2012 SMTP.pcap [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: smtp.response >= 400 Expression... Clear Apply Save POP SMTP
No. Time Source Destination Protocol Length Info
230881 0.957216 194.90.126.3 212.179.113.105 SMTP 105 S: 500 Syntax error, I cannot recognize this command
233930 0.370806 46.4.167.9 194.90.126.1 SMTP 93 S: 421 mx. .net Service Unavailable 1
236492 0.287574 176.9.102.185 194.90.126.1 SMTP 75 S: 451 Try again later 2
240907 0.585329 194.90.126.3 212.29.221.217 SMTP 117 S: 500 Syntax error, I cannot recognize this command 3
249262 1.209123 80.179.55.150 194.90.126.1 SMTP 162 S: 250 2.5.0 Address and options OK. | 451 4.2.2 user over quota; cannot recei
264923 3.080530 194.90.126.3 209.85.212.175 SMTP 117 S: 500 Syntax error, I cannot recognize this command
298264 5.142030 207.232.39.169 194.90.126.1 SMTP 108 S: 452 <noreply@at > Mailbox size limit exceeded 4
307959 2.008353 194.90.126.3 192.114.23.26 SMTP 117 S: 500 Syntax error, I cannot recognize this command
325389 2.901291 194.90.126.3 115.73.233.142 SMTP 100 S: 550 Invalid recipient/sender mailing address 5
335006 1.662495 192.115.106.20 194.90.126.1 SMTP 129 S: 250 Ok | 450 <hub-cas02. >: Helo command rejected: Host not found
343706 1.336559 194.90.126.3 62.219.19.49 SMTP 117 S: 500 Syntax error, I cannot recognize this command
368771 4.410882 194.90.126.3 80.179.55.166 SMTP 105 S: 500 Syntax error, I cannot recognize this command
374990 0.960292 194.90.126.3 212.29.221.217 SMTP 117 S: 500 Syntax error, I cannot recognize this command

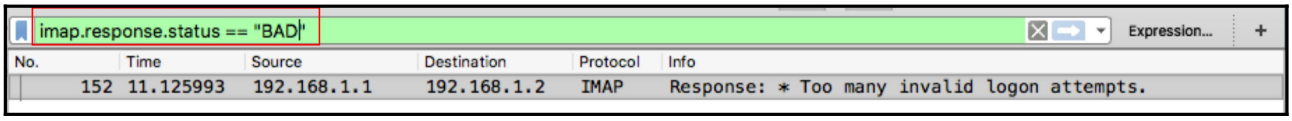

Filter: smtp.response >= 400 Expression... Clear Apply Save POP SMTP
Source Destination Protocol Length Info
194.90.126.3 192.114.23.26 SMTP 117 S: 500 Syntax error, I cannot recognize this command
194.90.126.3 115.73.233.142 SMTP 100 S: 550 Invalid recipient/sender mailing address
192.115.106.20 194.90.126.1 SMTP 129 S: 250 Ok | 450 <hub-cas02.tlv.gov.il>: Helo command rejected: Host not found
194.90.126.3 62.219.19.49 SMTP 117 S: 500 Syntax error, I cannot recognize this command
194.90.126.3 80.179.55.166 SMTP 105 S: 500 Syntax error, I cannot recognize this command
194.90.126.3 212.29.221.217 SMTP 117 S: 500 Syntax error, I cannot recognize this command
Frame 335006: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits)
Ethernet II, Src: Cisco_26:37:10 (00:17:59:26:37:10), Dst: Intel_04:4c:c5 (a0:36:9f:04:4c:c5)
Internet Protocol Version 4, Src: 192.115.106.20 (192.115.106.20), Dst: 194.90.126.1 (194.90.126.1)
Transmission Control Protocol, Src Port: smtp (25), Dst Port: 16419 (16419), Seq: 168, Ack: 123, Len: 75
Simple Mail Transfer Protocol
Response: 250 Ok\r\n
Response code: Requested mail action okay, completed (250)
Response parameter: Ok
Response: 450 <hub-cas02.tlv.gov.il>: Helo command rejected: Host not found\r\n
Response code: Requested mail action not taken: mailbox unavailable (450)
Response parameter: <hub-cas02.tlv.gov.il>: Helo command rejected: Host not found
Response code 1 (Code 250)
Response code 1 (Code 450)
SMTP message

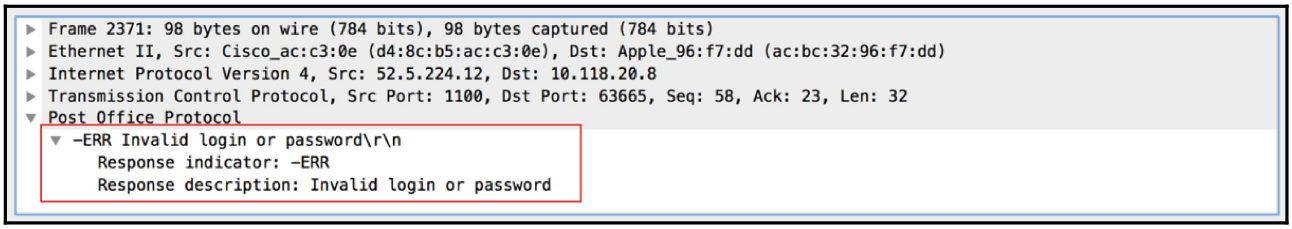

smtp.response.code == 220
Expression...
No. Time Source Destination Protocol Length Info
22 0.030478 192.168.1.1 192.168.1.2 SMTP 76 S: 220 ANANYAA-PC ESMTP
47 0.063087 192.168.1.1 192.168.1.2 SMTP 76 S: 220 ANANYAA-PC ESMTP

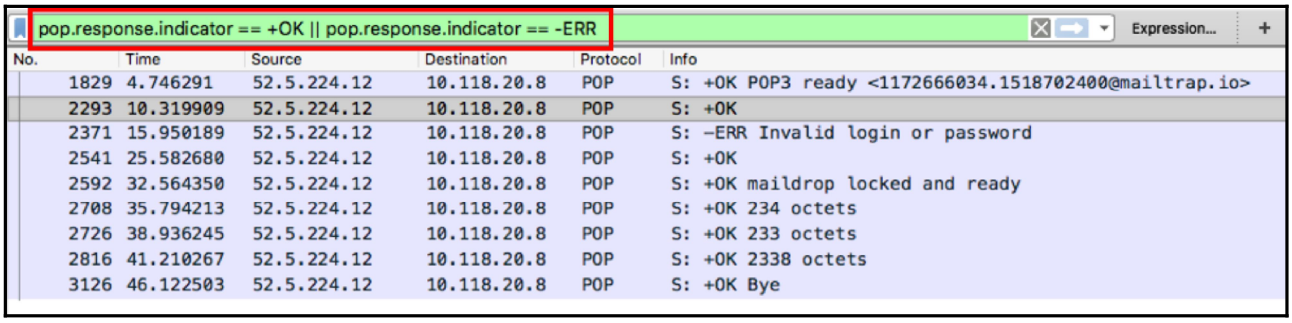

smtp.response.code > 200
Expression...
No. Time Source Destination Protocol Info
22 0.030478 192.168.1.1 192.168.1.2 SMTP S: 220 ANANYAA-PC ESMTP
25 0.031570 192.168.1.1 192.168.1.2 SMTP S: 250 ANANYAA-PC | 250 SIZE 20480000 | 250 AUTH LOGIN | 250 HELP
27 0.031749 192.168.1.1 192.168.1.2 SMTP S: 221 goodbye
47 0.063087 192.168.1.1 192.168.1.2 SMTP S: 220 ANANYAA-PC ESMTP
50 0.064409 192.168.1.1 192.168.1.2 SMTP S: 250 ANANYAA-PC | 250 SIZE 20480000 | 250 AUTH LOGIN | 250 HELP
52 0.064699 192.168.1.1 192.168.1.2 SMTP S: 221 goodbye

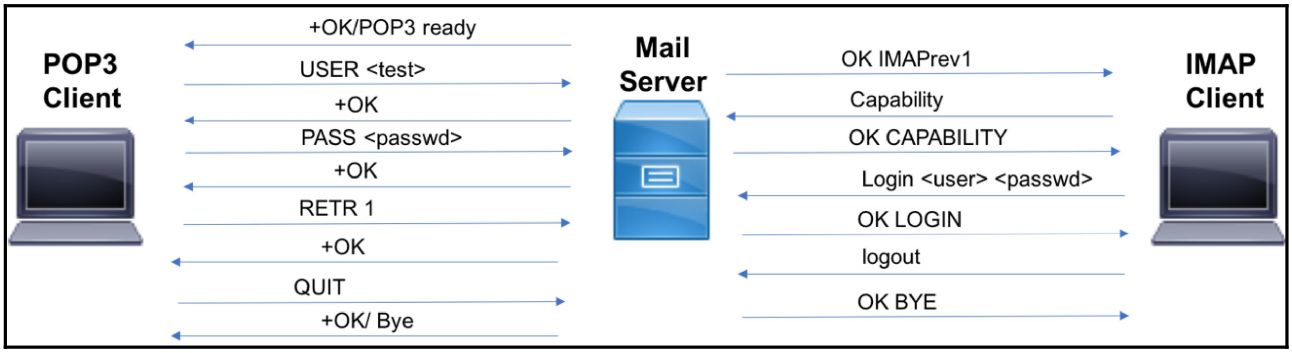

smtp.rsp.parameter == "AUTH LOGIN"
Expression...
No. Time Source Destination Protocol Info
25 0.031570 192.168.1.1 192.168.1.2 SMTP S: 250 ANANYAA-PC | 250 SIZE 20480000 | 250 AUTH LOGIN | 250 HELP
50 0.064409 192.168.1.1 192.168.1.2 SMTP S: 250 ANANYAA-PC | 250 SIZE 20480000 | 250 AUTH LOGIN | 250 HELP

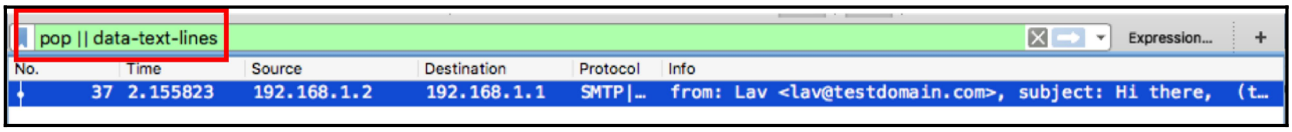

imap.request
Expression...
No. Time Source Destination Protocol Info
1288 213.296876 192.168.1.2 192.168.1.1 IMAP Request: 1 capability
1292 213.308958 192.168.1.2 192.168.1.1 IMAP Request: 3 login "lav@testdomain.com" "lavanya"
1295 213.311008 192.168.1.2 192.168.1.1 IMAP Request: 4 append "Sent" (\Seen) {444}
1298 213.311786 192.168.1.2 192.168.1.1 IMAP Request: To: lav@testdomain.com, ana@testdomain.com
1303 213.577701 192.168.1.2 192.168.1.1 IMAP Request: 5 logout

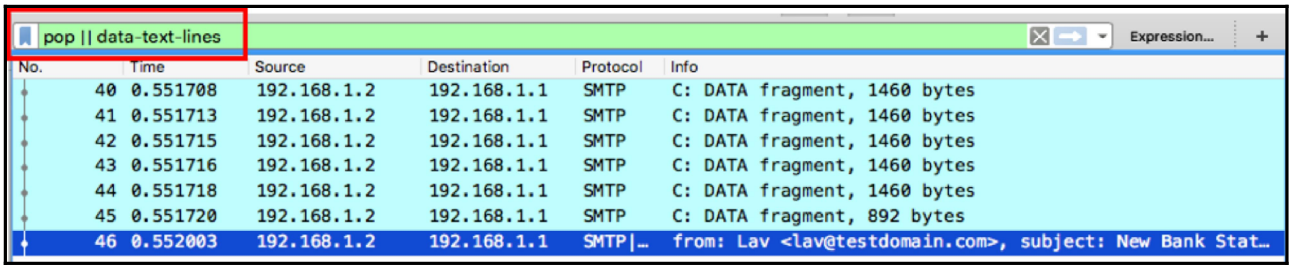

imap.response.status == "BAD"
Expression...
No. Time Source Destination Protocol Info
152 11.125993 192.168.1.1 192.168.1.2 IMAP Response: * Too many invalid logon attempts.

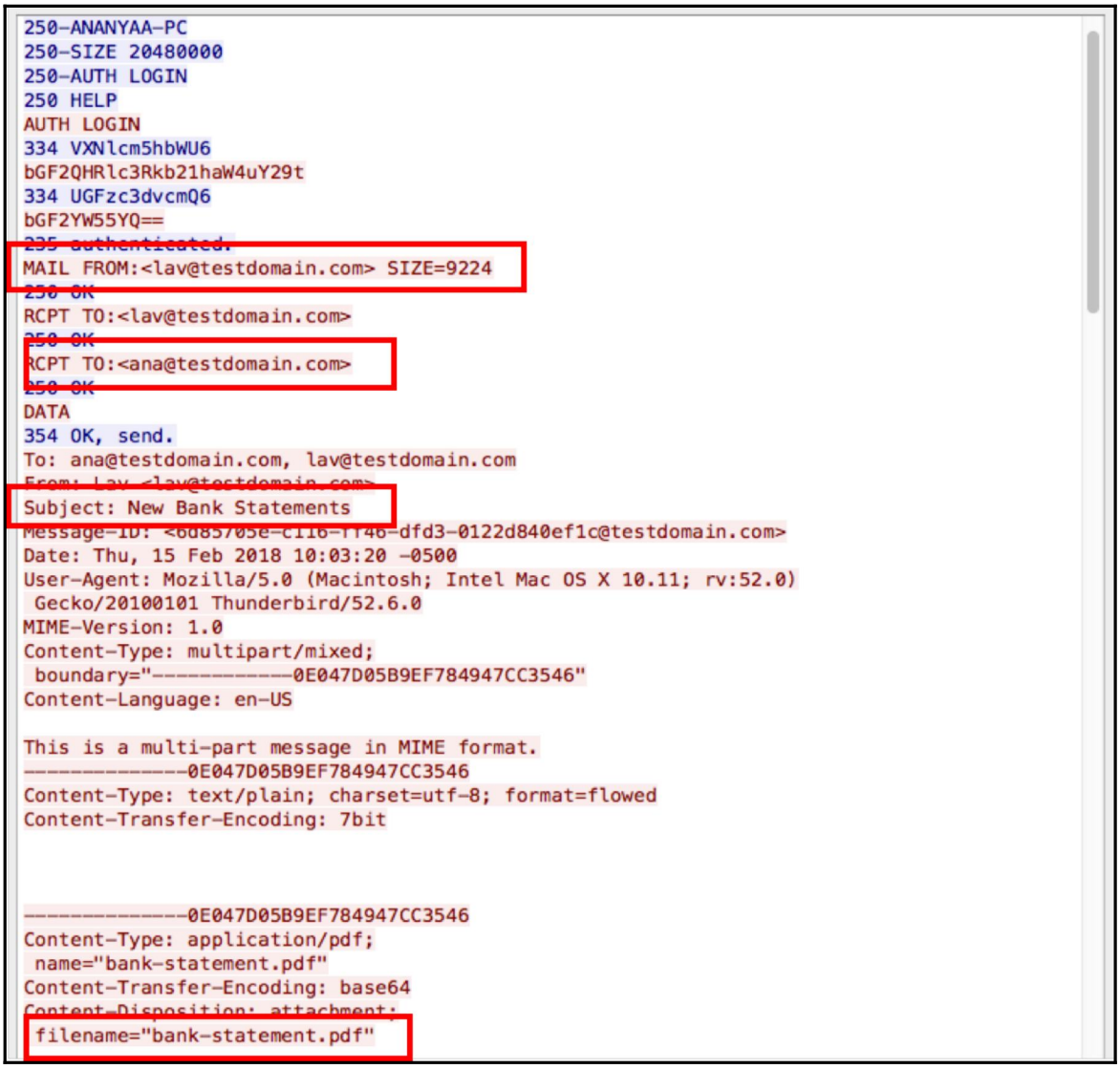

Frame 2371: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
Ethernet II, Src: Cisco_ac:c3:0e (d4:8c:b5:ac:c3:0e), Dst: Apple_96:f7:dd (ac:bc:32:96:f7:dd)
Internet Protocol Version 4, Src: 52.5.224.12, Dst: 10.118.20.8
Transmission Control Protocol, Src Port: 1100, Dst Port: 63665, Seq: 58, Ack: 23, Len: 32
Post Office Protocol
-ERR Invalid login or password\r\n
Response indicator: -ERR
Response description: Invalid login or password


pop.response.indicator == +OK || pop.response.indicator == -ERR
Expression...
No. Time Source Destination Protocol Info
1829 4.746291 52.5.224.12 10.118.20.8 POP S: +OK POP3 ready <1172666034.1518702400@mailtrap.io>
2293 10.319909 52.5.224.12 10.118.20.8 POP S: +OK
2371 15.950189 52.5.224.12 10.118.20.8 POP S: -ERR Invalid login or password
2541 25.582680 52.5.224.12 10.118.20.8 POP S: +OK
2592 32.564350 52.5.224.12 10.118.20.8 POP S: +OK maildrop locked and ready
2708 35.794213 52.5.224.12 10.118.20.8 POP S: +OK 234 octets
2726 38.936245 52.5.224.12 10.118.20.8 POP S: +OK 233 octets
2816 41.210267 52.5.224.12 10.118.20.8 POP S: +OK 2338 octets
3126 46.122503 52.5.224.12 10.118.20.8 POP S: +OK Bye


POP3 Client
+OK/POP3 ready
USER <test>
+OK
PASS <passwd>
+OK
RETR 1
+OK
QUIT
+OK/ Bye
Mail Server
OK IMAPrev1
Capability
OK CAPABILITY
Login <user> <passwd>
OK LOGIN
logout
OK BYE
IMAP Client

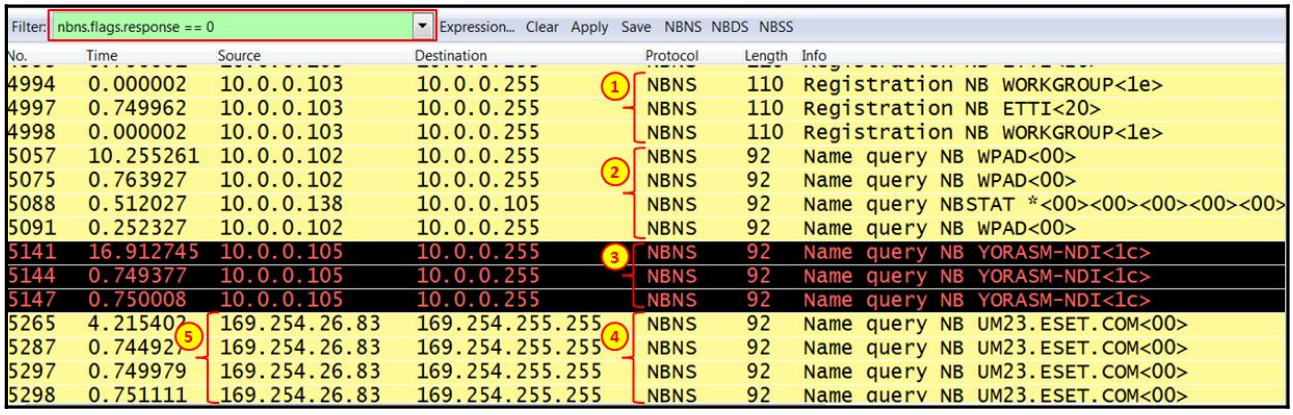

pop || data-text-lines
Expression...
No. Time Source Destination Protocol Info
37 2.155823 192.168.1.2 192.168.1.1 SMTP|… from: Lav <lav@testdomain.com>, subject: Hi there, (t…

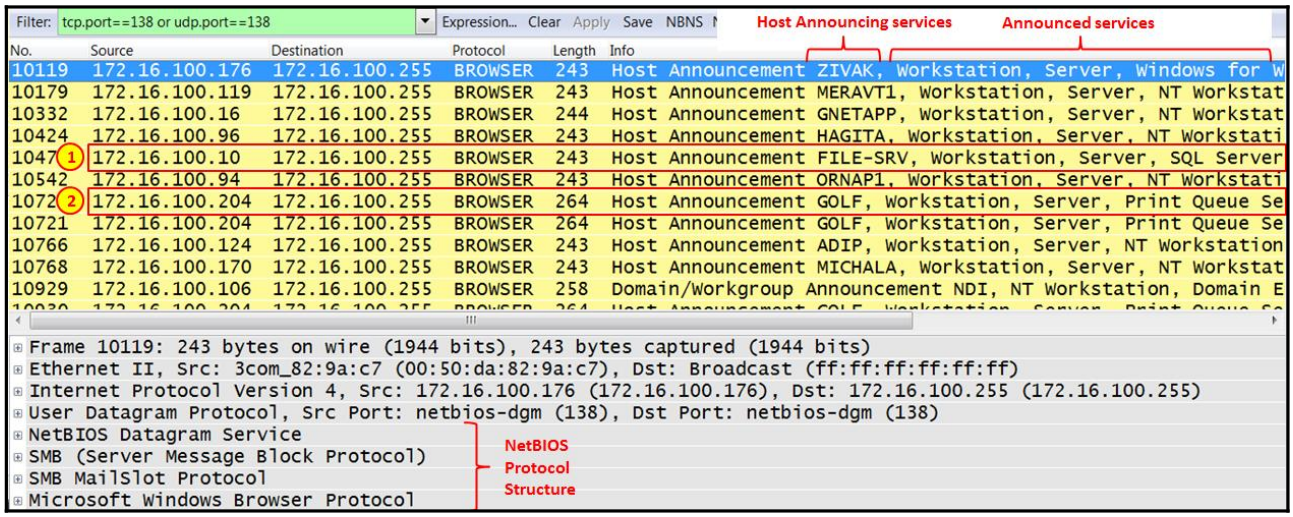

pop || data-text-lines
Expression...
No. Time Source Destination Protocol Info
40 0.551708 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 1460 bytes
41 0.551713 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 1460 bytes
42 0.551715 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 1460 bytes
43 0.551716 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 1460 bytes
44 0.551718 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 1460 bytes
45 0.551720 192.168.1.2 192.168.1.1 SMTP C: DATA fragment, 892 bytes
46 0.552003 192.168.1.2 192.168.1.1 SMTP|… from: Lav <lav@testdomain.com>, subject: New Bank Stat…

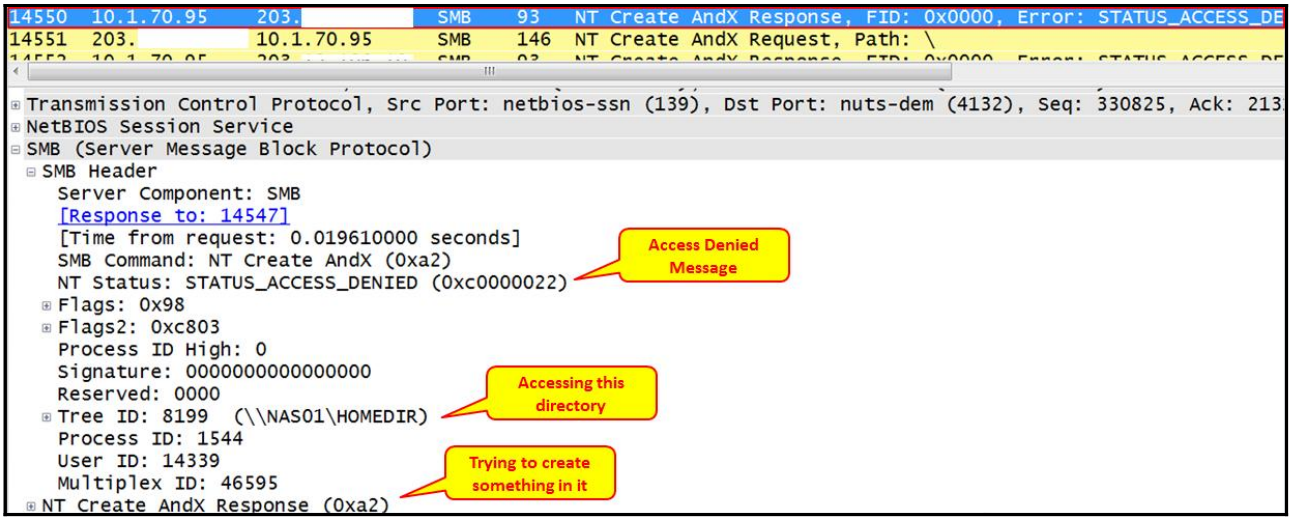


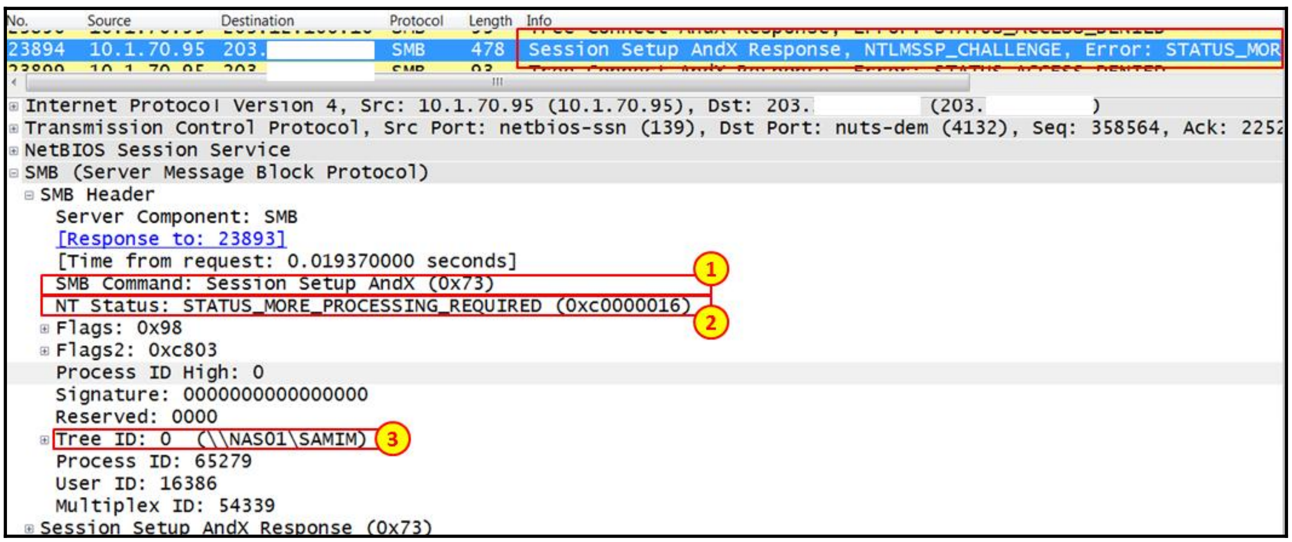
```
250-ANANYAA-PC
250-SIZE 20480000
250-AUTH LOGIN
250 HELP
AUTH LOGIN
334 VXNlcm5hbWU6
bGF2QHRlc3Rkb21haW4uY29t
334 UGFzc3dvcmQ6
bGF2YW55YQ==
235 authenticated.
MAIL FROM:<lav@testdomain.com> SIZE=9224
250 OK
RCPT TO:<lav@testdomain.com>
250 OK
RCPT TO:<ana@testdomain.com>
250 OK
DATA
354 OK, send.
To: ana@testdomain.com, lav@testdomain.com
From: Lav <lav@testdomain.com>
Subject: New Bank Statements
Message-ID: <6d85705e-c116-1146-dfd3-0122d840ef1c@testdomain.com>
Date: Thu, 15 Feb 2018 10:03:20 -0500
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:52.0)
 Gecko/20100101 Thunderbird/52.6.0
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="------------0E047D05B9EF784947CC3546"
Content-Language: en-US

This is a multi-part message in MIME format.
--------------0E047D05B9EF784947CC3546
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Transfer-Encoding: 7bit



--------------0E047D05B9EF784947CC3546
Content-Type: application/pdf;
 name="bank-statement.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="bank-statement.pdf"
```

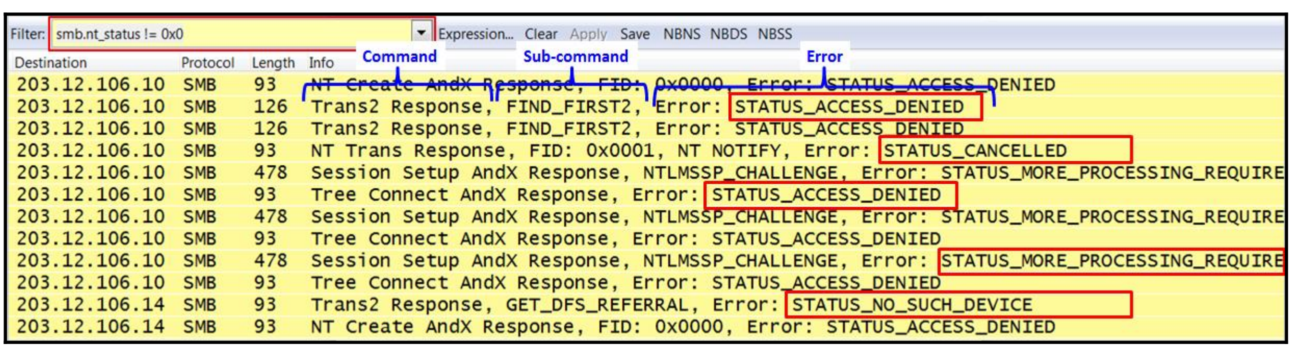
Chapter 15: NetBIOS and SMB Protocol Analysis

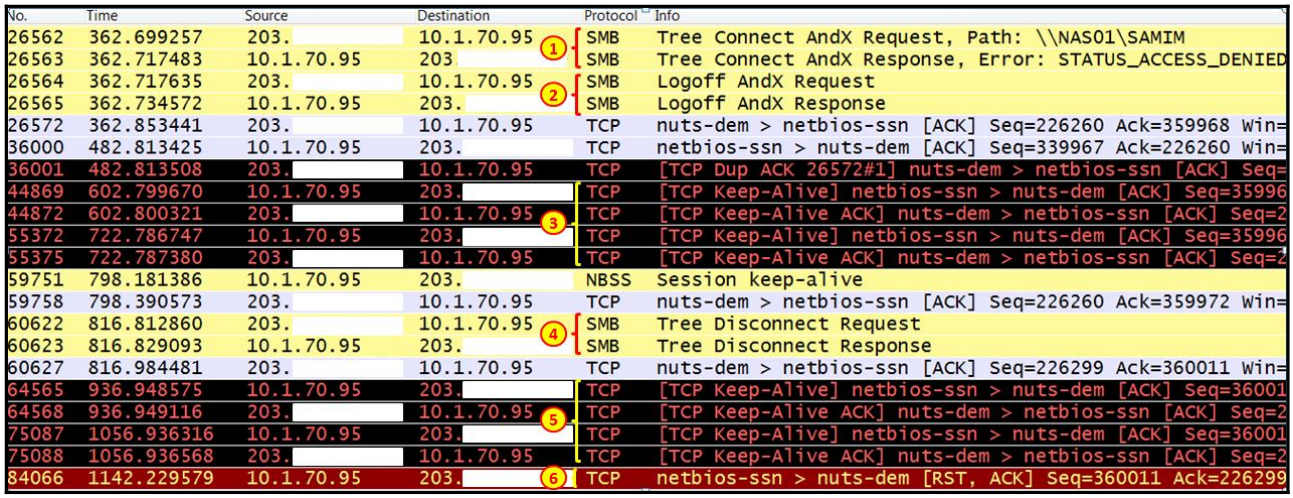




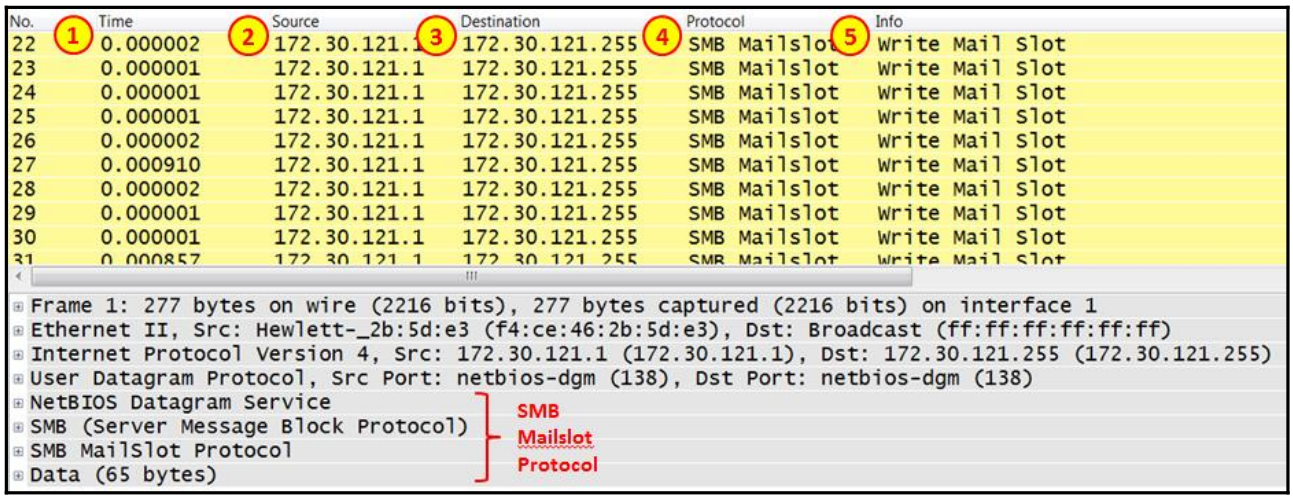

14550 10.1.70.95 203. SMB 93 NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DE
14551 203. 10.1.70.95 SMB 146 NT Create AndX Request, Path: \
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: nuts-dem (4132), Seq: 330825, Ack: 213
NetBIOS Session Service
SMB (Server Message Block Protocol)
SMB Header
Server Component: SMB
[Response to: 14547]
[Time from request: 0.019610000 seconds]
SMB Command: NT Create AndX (0xa2)
NT Status: STATUS_ACCESS_DENIED (0xc0000022)
Flags: 0x98
Flags2: 0xc803
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
Tree ID: 8199 (\\NAS01\HOMEDIR)
Process ID: 1544
User ID: 14339
Multiplex ID: 46595
NT Create AndX Response (0xa2)
Access Denied Message
Accessing this directory
Trying to create something in it


No. Source Destination Protocol Length Info
23894 10.1.70.95 203. SMB 478 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MOR
Internet Protocol Version 4, Src: 10.1.70.95 (10.1.70.95), Dst: 203. (203.)
Transmission Control Protocol, Src Port: netbios-ssn (139), Dst Port: nuts-dem (4132), Seq: 358564, Ack: 2252
NetBIOS Session Service
SMB (Server Message Block Protocol)
SMB Header
Server Component: SMB
[Response to: 23893]
[Time from request: 0.019370000 seconds]
SMB Command: Session Setup AndX (0x73)
NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
Flags: 0x98
Flags2: 0xc803
Process ID High: 0
Signature: 0000000000000000
Reserved: 0000
Tree ID: 0 (\\NAS01\SAMIM)
Process ID: 65279
User ID: 16386
Multiplex ID: 54339
Session Setup AndX Response (0x73)
1
2
3


Filter: smb.nt_status != 0x0
Expression... Clear Apply Save NBNS NBDS NBSS
Destination Protocol Length Info
Command
Sub-command
Error
203.12.106.10 SMB 93 NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED
203.12.106.10 SMB 126 Trans2 Response, FIND_FIRST2, Error: STATUS_ACCESS_DENIED
203.12.106.10 SMB 126 Trans2 Response, FIND_FIRST2, Error: STATUS_ACCESS_DENIED
203.12.106.10 SMB 93 NT Trans Response, FID: 0x0001, NT NOTIFY, Error: STATUS_CANCELLED
203.12.106.10 SMB 478 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRE
203.12.106.10 SMB 93 Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.10 SMB 478 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRE
203.12.106.10 SMB 93 Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.10 SMB 478 Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRE
203.12.106.10 SMB 93 Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
203.12.106.14 SMB 93 Trans2 Response, GET_DFS_REFERRAL, Error: STATUS_NO_SUCH_DEVICE
203.12.106.14 SMB 93 NT Create AndX Response, FID: 0x0000, Error: STATUS_ACCESS_DENIED



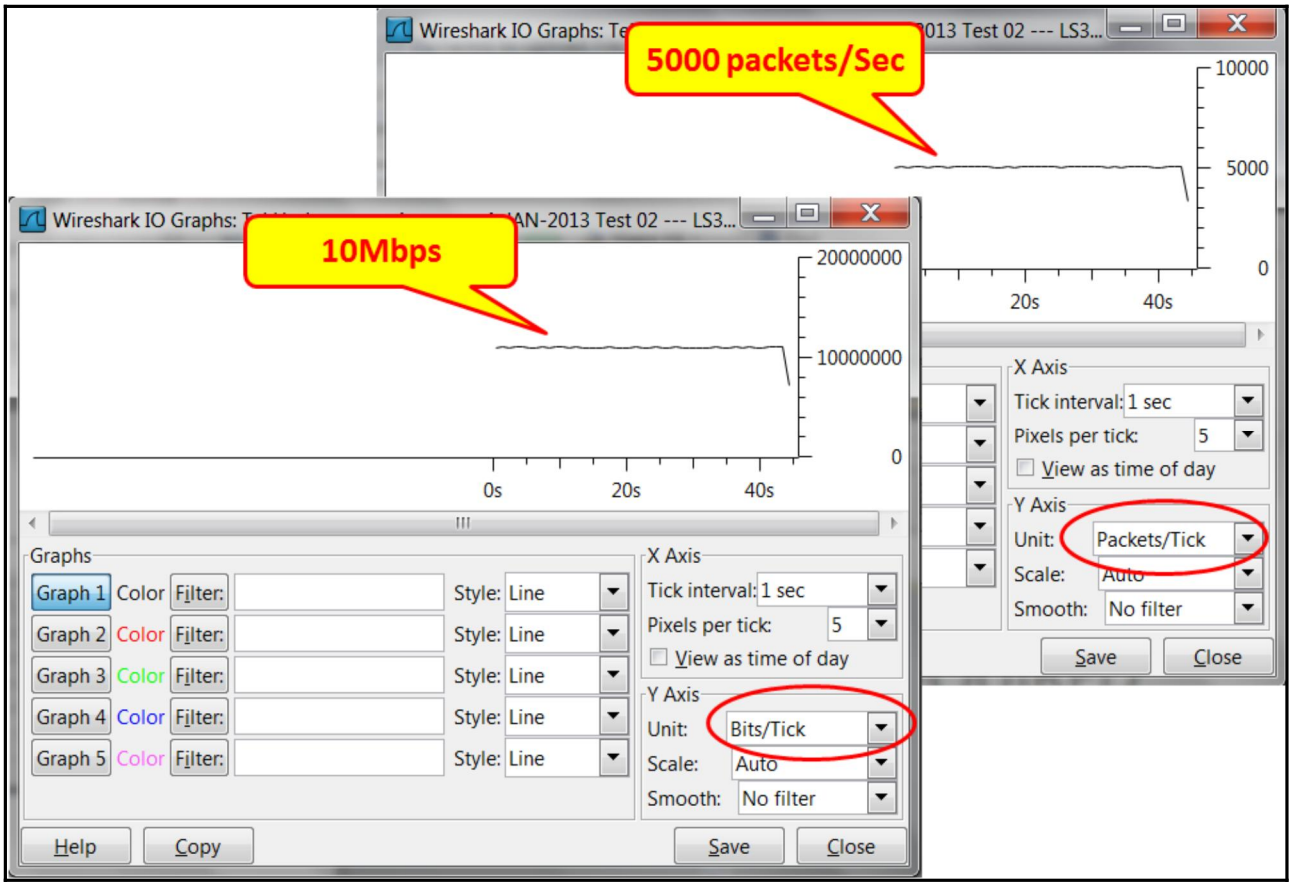
No.	Time	Source	Destination	Protocol	Info
26562	362.699257	203.	10.1.70.95	SMB	Tree Connect AndX Request, Path: \\NAS01\SAMIM
26563	362.717483	10.1.70.95	203	SMB	Tree Connect AndX Response, Error: STATUS_ACCESS_DENIED
26564	362.717635	203.	10.1.70.95	SMB	Logoff AndX Request
26565	362.734572	10.1.70.95	203.	SMB	Logoff AndX Response
26572	362.853441	203.	10.1.70.95	TCP	nuts-dem > netbios-ssn [ACK] Seq=226260 Ack=359968 Win=
36000	482.813425	10.1.70.95	203.	TCP	netbios-ssn > nuts-dem [ACK] Seq=339967 Ack=226260 Win=
36001	482.813508	203.	10.1.70.95	TCP	[TCP Dup ACK 26572#1] nuts-dem > netbios-ssn [ACK] Seq=
44869	602.799670	10.1.70.95	203.	TCP	[TCP Keep-Alive] netbios-ssn > nuts-dem [ACK] Seq=35996
44872	602.800321	203.	10.1.70.95	TCP	[TCP Keep-Alive ACK] nuts-dem > netbios-ssn [ACK] Seq=2
55372	722.786747	10.1.70.95	203.	TCP	[TCP Keep-Alive] netbios-ssn > nuts-dem [ACK] Seq=35996
55375	722.787380	203.	10.1.70.95	TCP	[TCP Keep-Alive ACK] nuts-dem > netbios-ssn [ACK] Seq=2
59751	798.181386	10.1.70.95	203.	NBSS	Session keep-alive
59758	798.390573	203.	10.1.70.95	TCP	nuts-dem > netbios-ssn [ACK] Seq=226260 Ack=359972 Win=
60622	816.812860	203.	10.1.70.95	SMB	Tree Disconnect Request
60623	816.829093	10.1.70.95	203.	SMB	Tree Disconnect Response
60627	816.984481	203.	10.1.70.95	TCP	nuts-dem > netbios-ssn [ACK] Seq=226299 Ack=360011 Win=
64565	936.948575	10.1.70.95	203.	TCP	[TCP Keep-Alive] netbios-ssn > nuts-dem [ACK] Seq=36001
64568	936.949116	203.	10.1.70.95	TCP	[TCP Keep-Alive ACK] nuts-dem > netbios-ssn [ACK] Seq=2
75087	1056.936316	10.1.70.95	203.	TCP	[TCP Keep-Alive] netbios-ssn > nuts-dem [ACK] Seq=36001
75088	1056.936568	203.	10.1.70.95	TCP	[TCP Keep-Alive ACK] nuts-dem > netbios-ssn [ACK] Seq=2
84066	1142.229579	10.1.70.95	203.	TCP	netbios-ssn > nuts-dem [RST, ACK] Seq=360011 Ack=226299

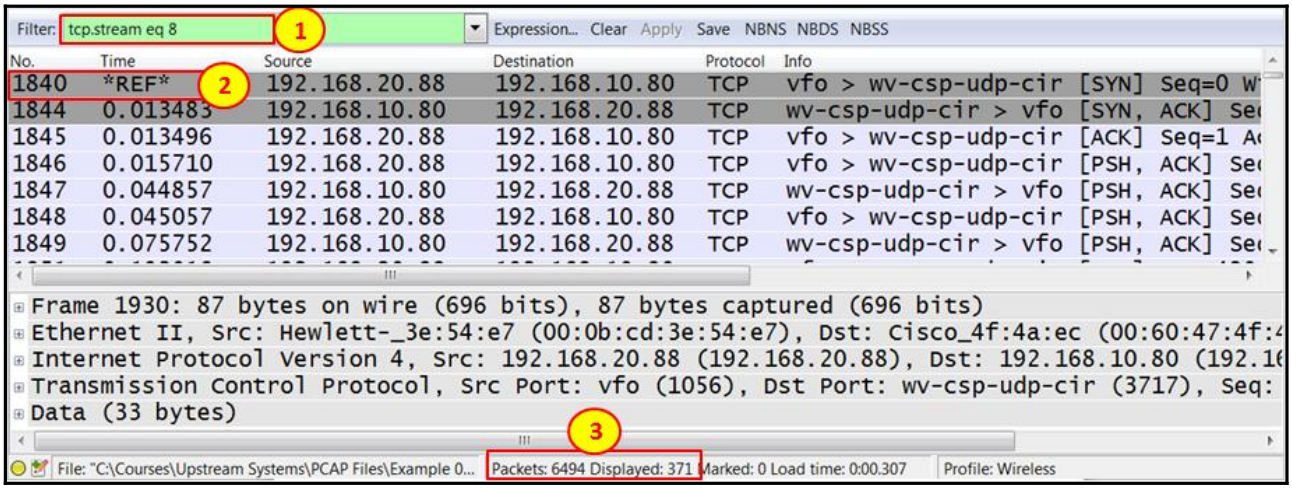


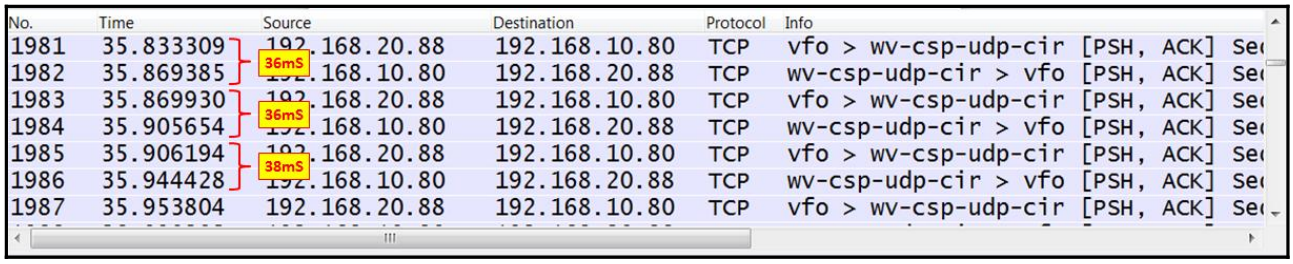
No.	Time	Source	Destination	Protocol	Info
22	0.000002	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
23	0.000001	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
24	0.000001	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
25	0.000001	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
26	0.000002	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
27	0.000910	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
28	0.000002	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
29	0.000001	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
30	0.000001	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot
31	0.000857	172.30.121.1	172.30.121.255	SMB Mailslot	Write Mail Slot

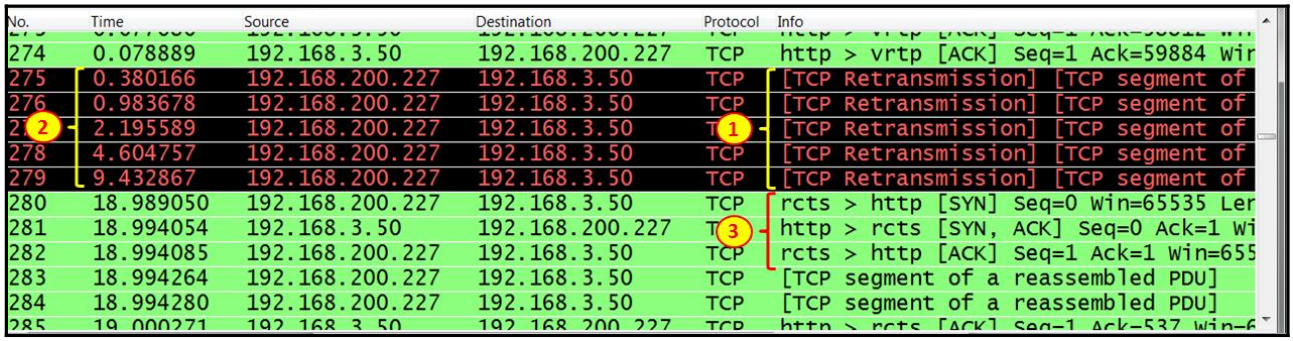
```
⊞ Frame 1: 277 bytes on wire (2216 bits), 277 bytes captured (2216 bits) on interface 1
⊞ Ethernet II, Src: Hewlett-_2b:5d:e3 (f4:ce:46:2b:5d:e3), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 172.30.121.1 (172.30.121.1), Dst: 172.30.121.255 (172.30.121.255)
⊞ User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
⊞ NetBIOS Datagram Service
⊞ SMB (Server Message Block Protocol)
⊞ SMB MailSlot Protocol
⊞ Data (65 bytes)
```

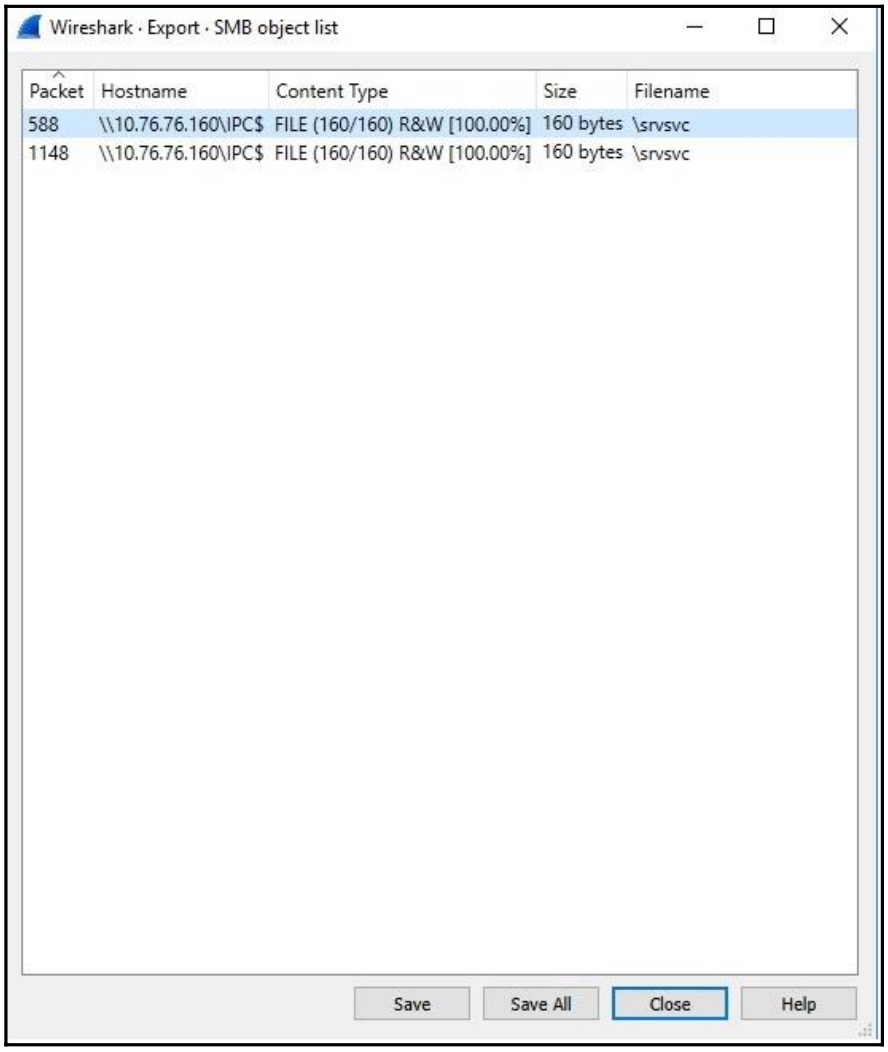
SMB Mailslot Protocol


Wireshark IO Graphs:
5000 packets/Sec
10000
5000
0
20s
40s
Wireshark IO Graphs:
10Mbps
20000000
10000000
0
0s
20s
40s
Graphs
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: Style: Line
Graph 5 Color Filter: Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Bits/Tick
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter
Save
Close

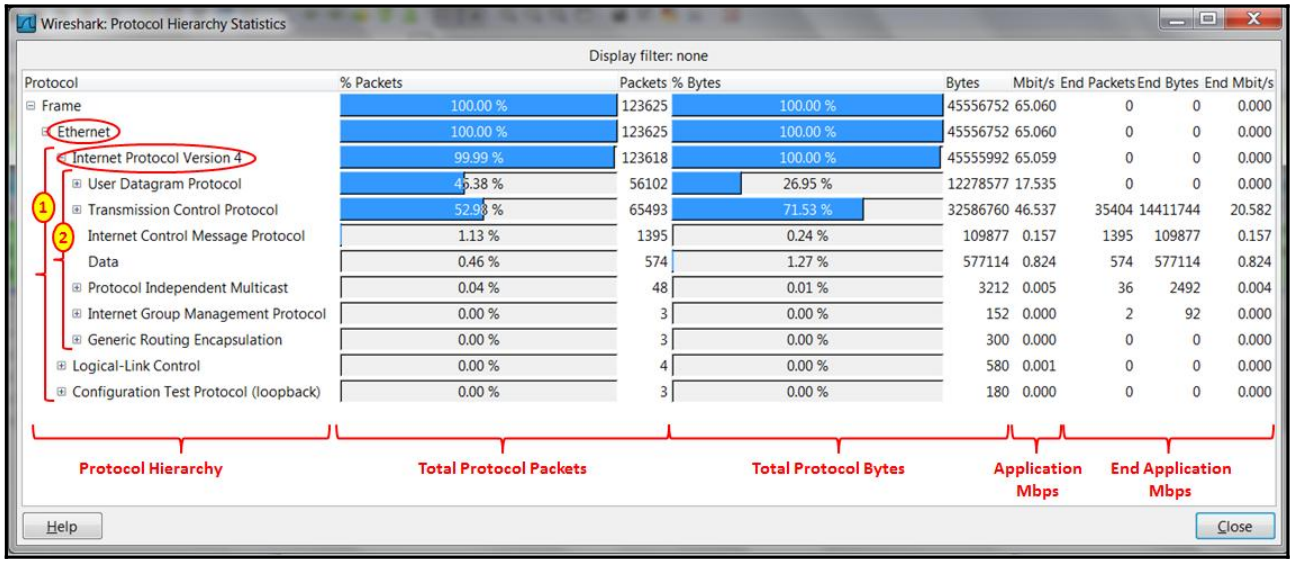

Filter: tcp.stream eq 8
1
Expression... Clear Apply Save NBNS NBDS NBSS
No. Time Source Destination Protocol Info
1840 *REF* 2 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [SYN] Seq=0 W
1844 0.013483 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [SYN, ACK] Se
1845 0.013496 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [ACK] Seq=1 A
1846 0.015710 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1847 0.044857 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1848 0.045057 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1849 0.075752 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
Frame 1930: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Hewlett-_3e:54:e7 (00:0b:cd:3e:54:e7), Dst: Cisco_4f:4a:ec (00:60:47:4f:
Internet Protocol Version 4, Src: 192.168.20.88 (192.168.20.88), Dst: 192.168.10.80 (192.1
Transmission Control Protocol, Src Port: vfo (1056), Dst Port: wv-csp-udp-cir (3717), Seq:
Data (33 bytes)
3
File: "C:\Courses\Upstream Systems\PCAP Files\Example 0...
Packets: 6494 Displayed: 371 Marked: 0 Load time: 0:00.307
Profile: Wireless

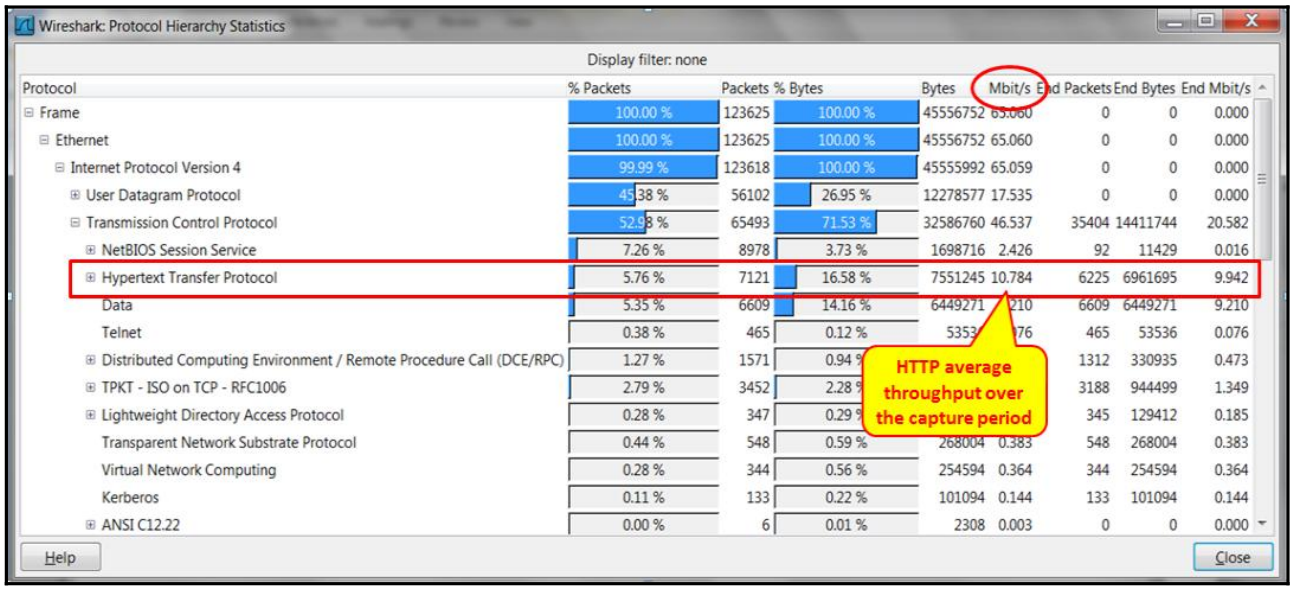

No. Time Source Destination Protocol Info
1981 35.833309 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1982 35.869385 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1983 35.869930 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1984 35.905654 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1985 35.906194 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1986 35.944428 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1987 35.953804 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
36mS
36mS
38mS

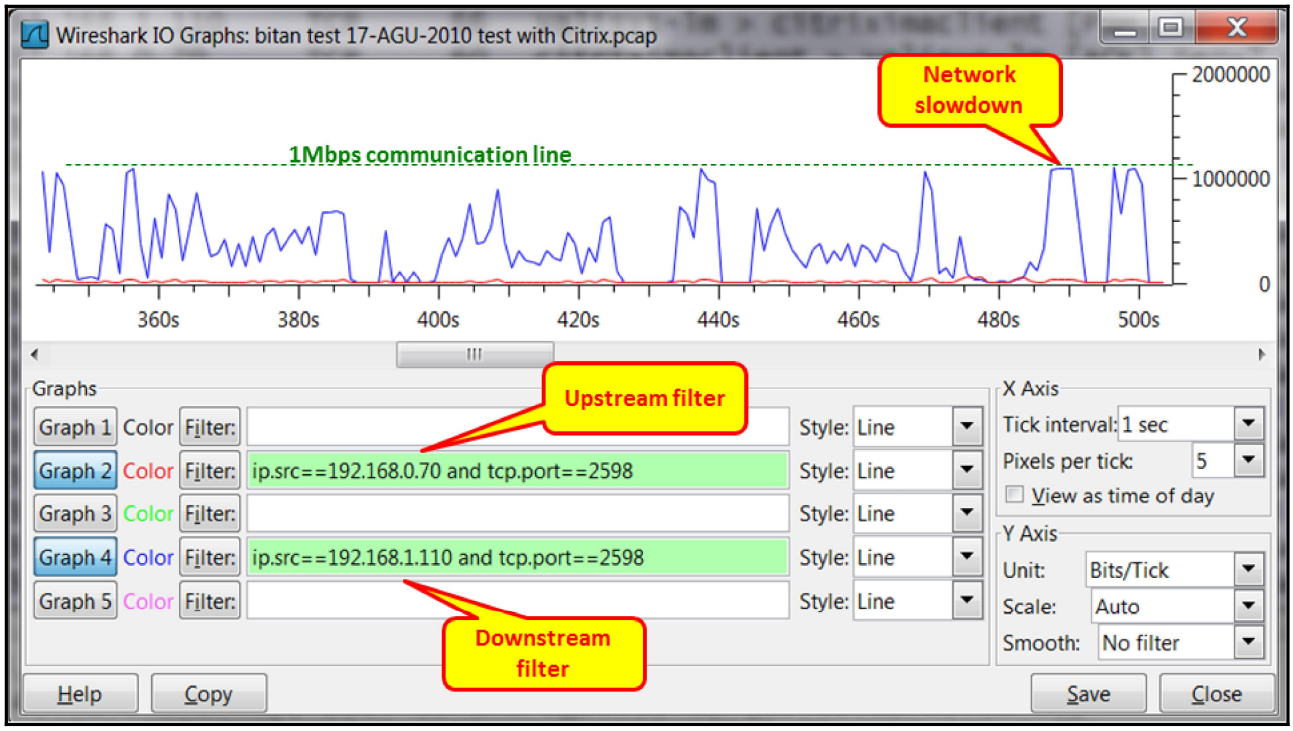

No. Time Source Destination Protocol Info
274 0.078889 192.168.3.50 192.168.200.227 TCP http > vrtp [ACK] Seq=1 Ack=59884 Wir
275 0.380166 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
276 0.983678 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
2 2.195589 192.168.200.227 192.168.3.50 T 1 [TCP Retransmission] [TCP segment of
278 4.604757 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
279 9.432867 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
280 18.989050 192.168.200.227 192.168.3.50 TCP rcts > http [SYN] Seq=0 Win=65535 Ler
281 18.994054 192.168.3.50 192.168.200.227 T 3 http > rcts [SYN, ACK] Seq=0 Ack=1 Wi
282 18.994085 192.168.200.227 192.168.3.50 TCP rcts > http [ACK] Seq=1 Ack=1 Win=655
283 18.994264 192.168.200.227 192.168.3.50 TCP [TCP segment of a reassembled PDU]
284 18.994280 192.168.200.227 192.168.3.50 TCP [TCP segment of a reassembled PDU]

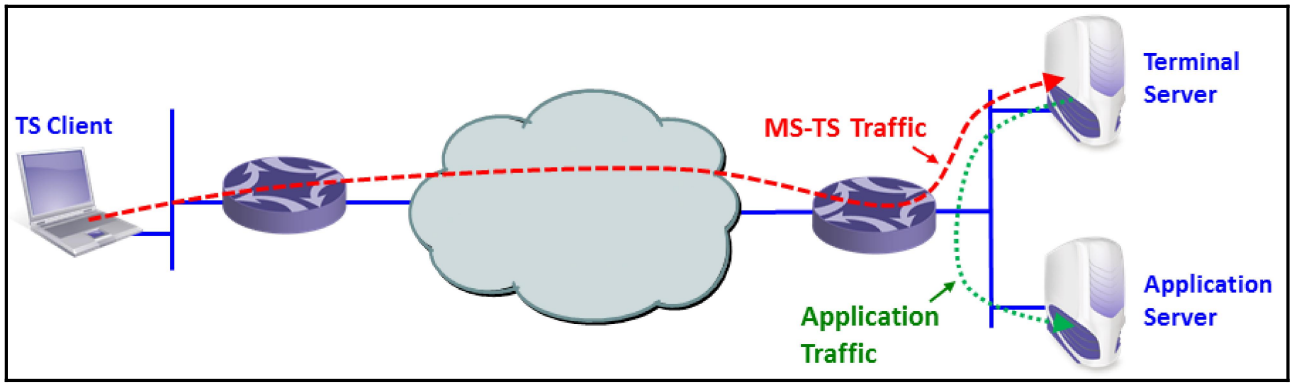

Wireshark · Export · SMB object list
Packet
Hostname
Content Type
Size
Filename
588
\\10.76.76.160\IPC$
FILE (160/160) R&W [100.00%]
160 bytes
\srvsvc
1148
\\10.76.76.160\IPC$
FILE (160/160) R&W [100.00%]
160 bytes
\srvsvc
Save
Save All
Close
Help

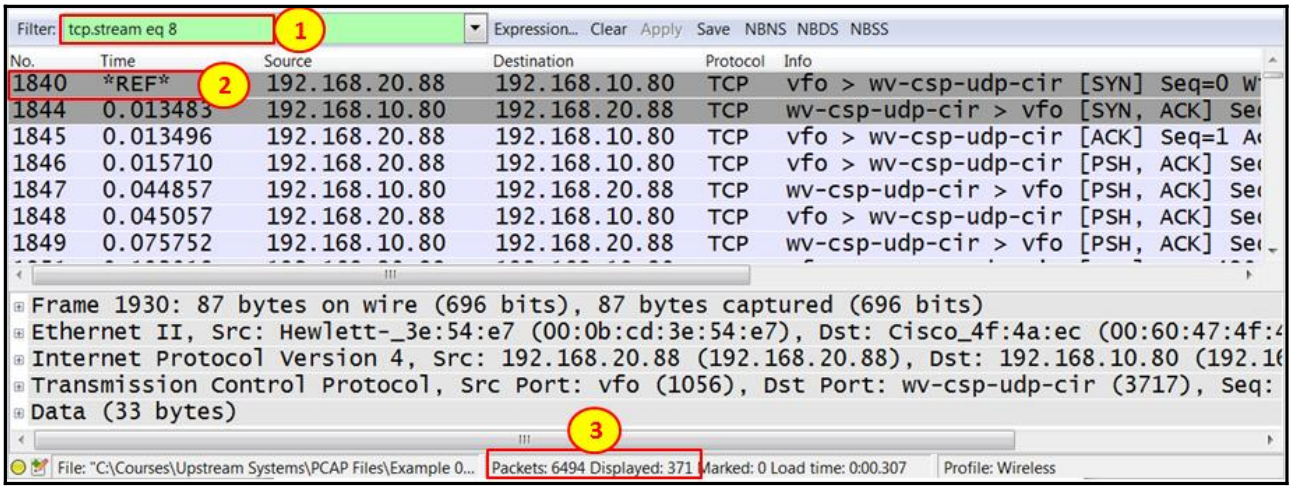
Chapter 16: Analyzing Enterprise Applications' Behavior

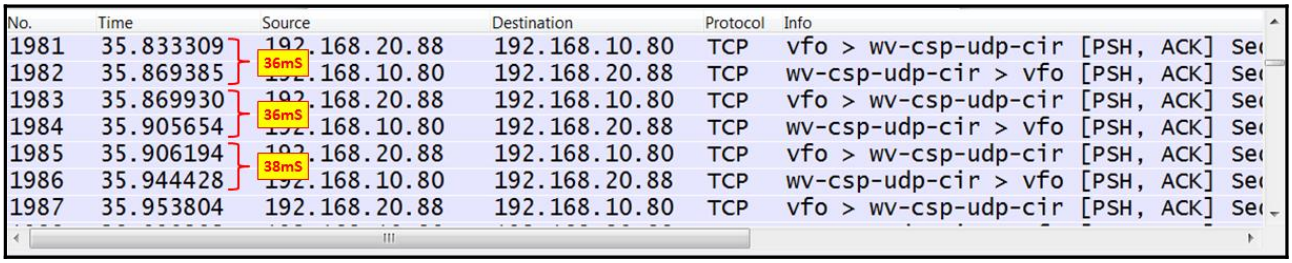


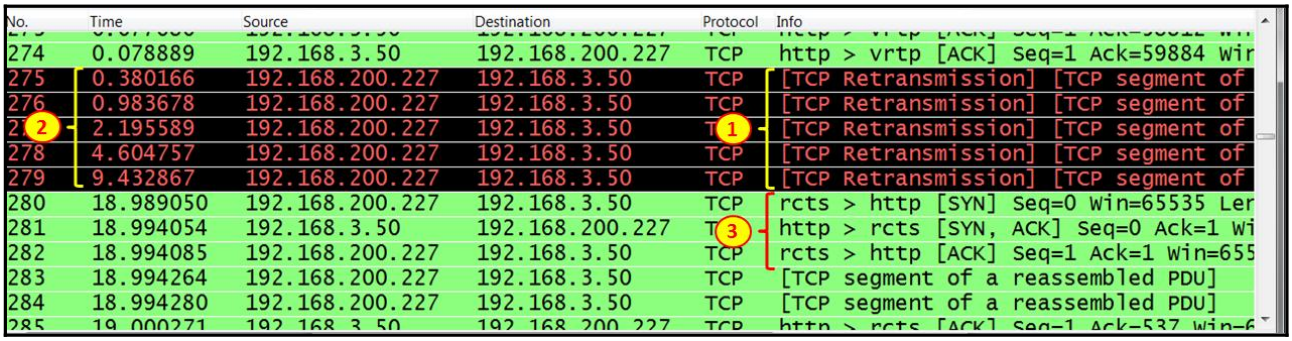



Wireshark IO Graphs: bitan test 17-AGU-2010 test with Citrix.pcap
Network slowdown
1Mbps communication line
2000000
1000000
0
360s
380s
400s
420s
440s
460s
480s
500s
Graphs
Upstream filter
Graph 1 Color Filter: Style: Line
Graph 2 Color Filter: ip.src==192.168.0.70 and tcp.port==2598 Style: Line
Graph 3 Color Filter: Style: Line
Graph 4 Color Filter: ip.src==192.168.1.110 and tcp.port==2598 Style: Line
Graph 5 Color Filter: Style: Line
Downstream filter
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Bits/Tick
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close

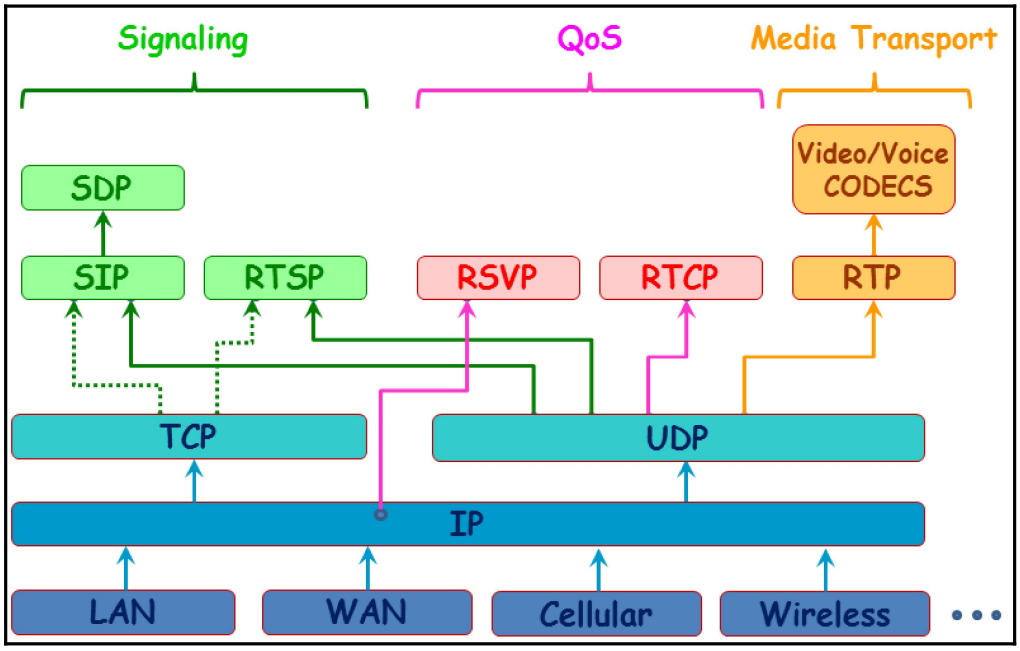

TS Client
MS-TS Traffic
Terminal Server
Application Server
Application Traffic

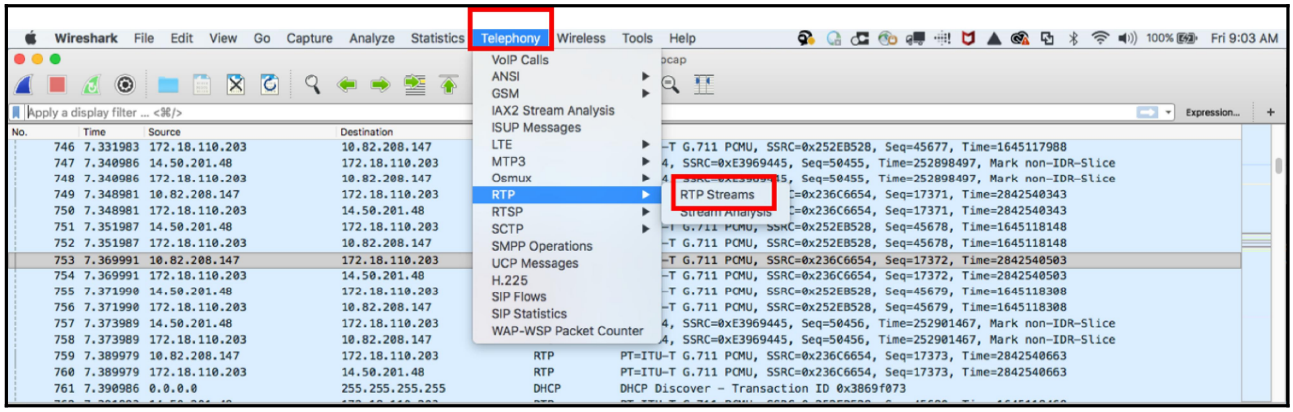

Filter: tcp.stream eq 8
1
Expression... Clear Apply Save NBNS NBDS NBSS
No. Time Source Destination Protocol Info
1840 *REF* 2 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [SYN] Seq=0 W
1844 0.013483 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [SYN, ACK] Se
1845 0.013496 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [ACK] Seq=1 A
1846 0.015710 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1847 0.044857 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1848 0.045057 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1849 0.075752 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
Frame 1930: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Hewlett-_3e:54:e7 (00:0b:cd:3e:54:e7), Dst: Cisco_4f:4a:ec (00:60:47:4f:4
Internet Protocol Version 4, Src: 192.168.20.88 (192.168.20.88), Dst: 192.168.10.80 (192.16
Transmission Control Protocol, Src Port: vfo (1056), Dst Port: wv-csp-udp-cir (3717), Seq:
Data (33 bytes)
3
File: "C:\Courses\Upstream Systems\PCAP Files\Example 0... Packets: 6494 Displayed: 371 Marked: 0 Load time: 0:00.307 Profile: Wireless

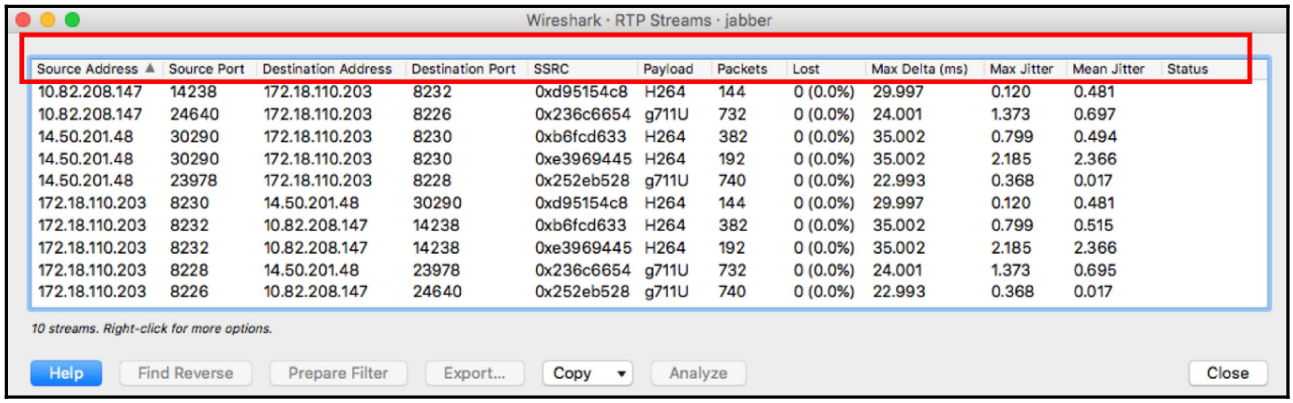

No. Time Source Destination Protocol Info
1981 35.833309 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1982 35.869385 36mS 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1983 35.869930 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1984 35.905654 36mS 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1985 35.906194 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se
1986 35.944428 38mS 192.168.10.80 192.168.20.88 TCP wv-csp-udp-cir > vfo [PSH, ACK] Se
1987 35.953804 192.168.20.88 192.168.10.80 TCP vfo > wv-csp-udp-cir [PSH, ACK] Se

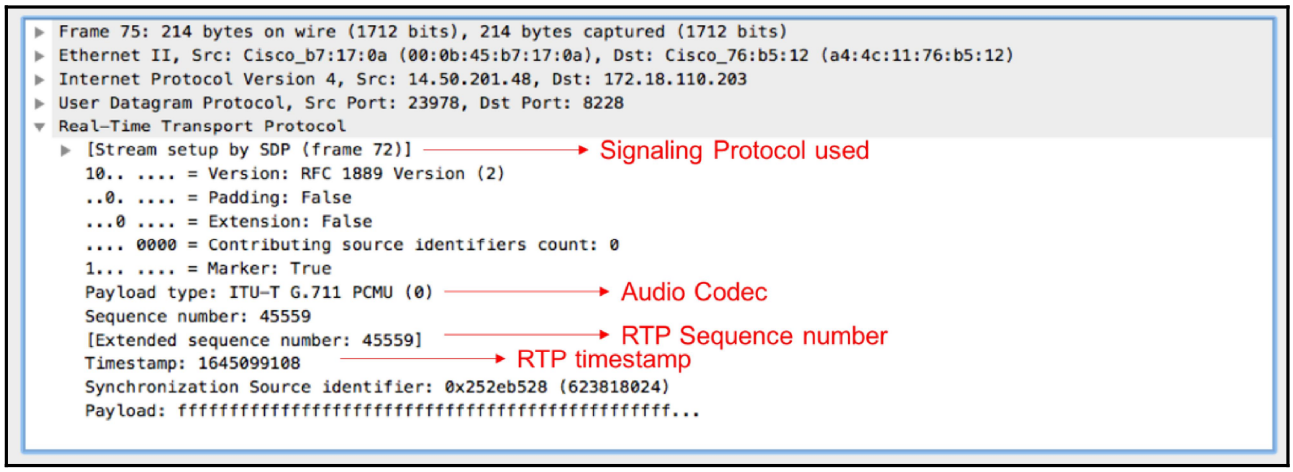

No. Time Source Destination Protocol Info
274 0.078889 192.168.3.50 192.168.200.227 TCP http > vrtp [ACK] Seq=1 Ack=59884 Wir
275 0.380166 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
276 0.983678 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
2 2.195589 192.168.200.227 192.168.3.50 TCP 1 [TCP Retransmission] [TCP segment of
278 4.604757 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
279 9.432867 192.168.200.227 192.168.3.50 TCP [TCP Retransmission] [TCP segment of
280 18.989050 192.168.200.227 192.168.3.50 TCP rcts > http [SYN] Seq=0 Win=65535 Len
281 18.994054 192.168.3.50 192.168.200.227 TCP 3 http > rcts [SYN, ACK] Seq=0 Ack=1 Wi
282 18.994085 192.168.200.227 192.168.3.50 TCP rcts > http [ACK] Seq=1 Ack=1 Win=655
283 18.994264 192.168.200.227 192.168.3.50 TCP [TCP segment of a reassembled PDU]
284 18.994280 192.168.200.227 192.168.3.50 TCP [TCP segment of a reassembled PDU]

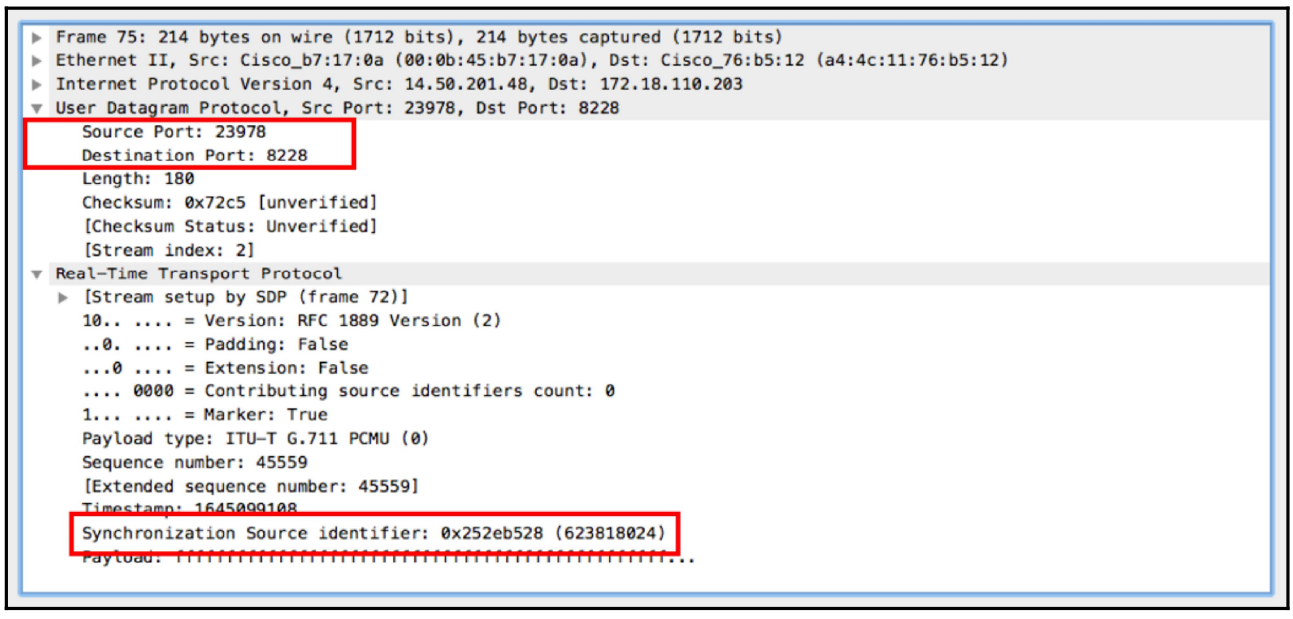
Chapter 17: Troubleshooting SIP, Multimedia, and IP Telephony



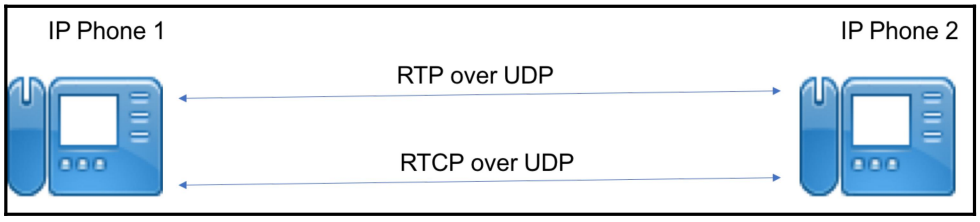



Wireshark · RTP Streams · jabber
Source Address | Source Port | Destination Address | Destination Port | SSRC | Payload | Packets | Lost | Max Delta (ms) | Max Jitter | Mean Jitter | Status
10.82.208.147 | 14238 | 172.18.110.203 | 8232 | 0xd95154c8 | H264 | 144 | 0 (0.0%) | 29.997 | 0.120 | 0.481
10.82.208.147 | 24640 | 172.18.110.203 | 8226 | 0x236c6654 | g711U | 732 | 0 (0.0%) | 24.001 | 1.373 | 0.697
14.50.201.48 | 30290 | 172.18.110.203 | 8230 | 0xb6fcd633 | H264 | 382 | 0 (0.0%) | 35.002 | 0.799 | 0.494
14.50.201.48 | 30290 | 172.18.110.203 | 8230 | 0xe3969445 | H264 | 192 | 0 (0.0%) | 35.002 | 2.185 | 2.366
14.50.201.48 | 23978 | 172.18.110.203 | 8228 | 0x252eb528 | g711U | 740 | 0 (0.0%) | 22.993 | 0.368 | 0.017
172.18.110.203 | 8230 | 14.50.201.48 | 30290 | 0xd95154c8 | H264 | 144 | 0 (0.0%) | 29.997 | 0.120 | 0.481
172.18.110.203 | 8232 | 10.82.208.147 | 14238 | 0xb6fcd633 | H264 | 382 | 0 (0.0%) | 35.002 | 0.799 | 0.515
172.18.110.203 | 8232 | 10.82.208.147 | 14238 | 0xe3969445 | H264 | 192 | 0 (0.0%) | 35.002 | 2.185 | 2.366
172.18.110.203 | 8228 | 14.50.201.48 | 23978 | 0x236c6654 | g711U | 732 | 0 (0.0%) | 24.001 | 1.373 | 0.695
172.18.110.203 | 8226 | 10.82.208.147 | 24640 | 0x252eb528 | g711U | 740 | 0 (0.0%) | 22.993 | 0.368 | 0.017
10 streams. Right-click for more options.
Help
Find Reverse
Prepare Filter
Export...
Copy
Analyze
Close

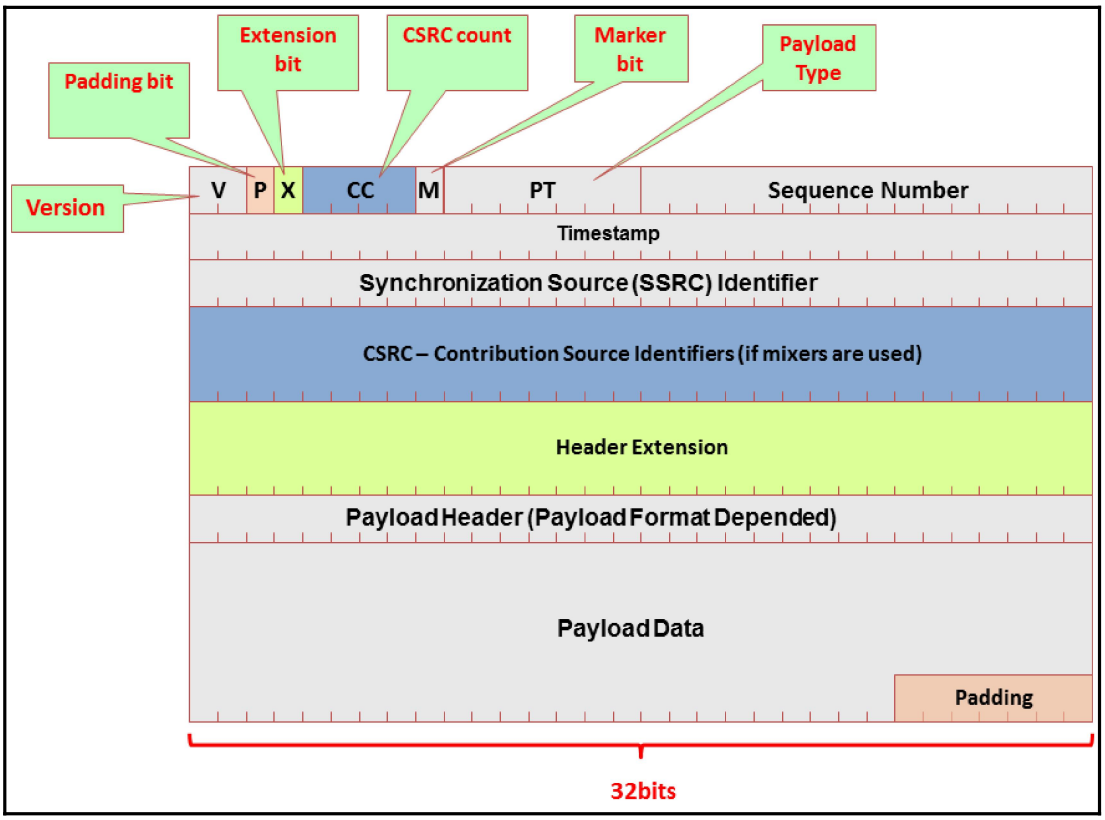

Frame 75: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
Ethernet II, Src: Cisco_b7:17:0a (00:0b:45:b7:17:0a), Dst: Cisco_76:b5:12 (a4:4c:11:76:b5:12)
Internet Protocol Version 4, Src: 14.50.201.48, Dst: 172.18.110.203
User Datagram Protocol, Src Port: 23978, Dst Port: 8228
Real-Time Transport Protocol
[Stream setup by SDP (frame 72)]
Signaling Protocol used
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)
Audio Codec
Sequence number: 45559
[Extended sequence number: 45559]
RTP Sequence number
Timestamp: 1645099108
RTP timestamp
Synchronization Source identifier: 0x252eb528 (623818024)
Payload: ffffffffffffffffffffffffffffffffffffffffffffffffffffffff...

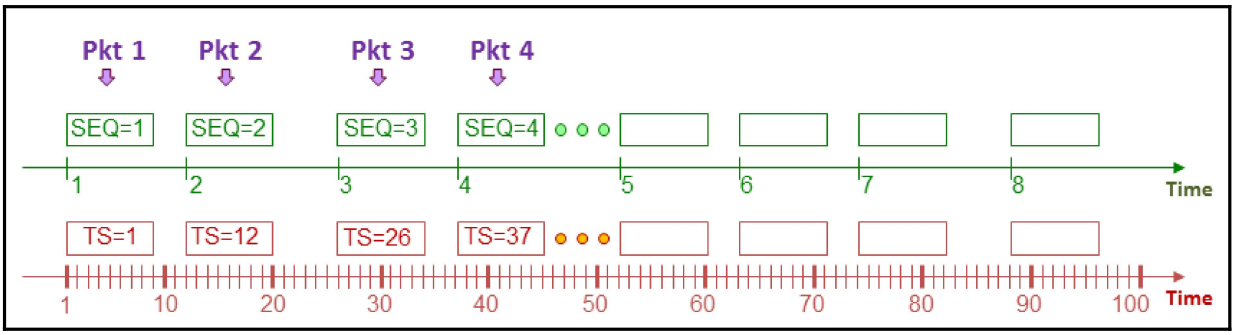

Frame 75: 214 bytes on wire (1712 bits), 214 bytes captured (1712 bits)
Ethernet II, Src: Cisco_b7:17:0a (00:0b:45:b7:17:0a), Dst: Cisco_76:b5:12 (a4:4c:11:76:b5:12)
Internet Protocol Version 4, Src: 14.50.201.48, Dst: 172.18.110.203
User Datagram Protocol, Src Port: 23978, Dst Port: 8228
Source Port: 23978
Destination Port: 8228
Length: 180
Checksum: 0x72c5 [unverified]
[Checksum Status: Unverified]
[Stream index: 2]
Real-Time Transport Protocol
[Stream setup by SDP (frame 72)]
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: 45559
[Extended sequence number: 45559]
Timestamp: 1645099108
Synchronization Source identifier: 0x252eb528 (623818024)
Payload: ffffffffffffffffffffffffffffffffffffffffffffffffffffffff...

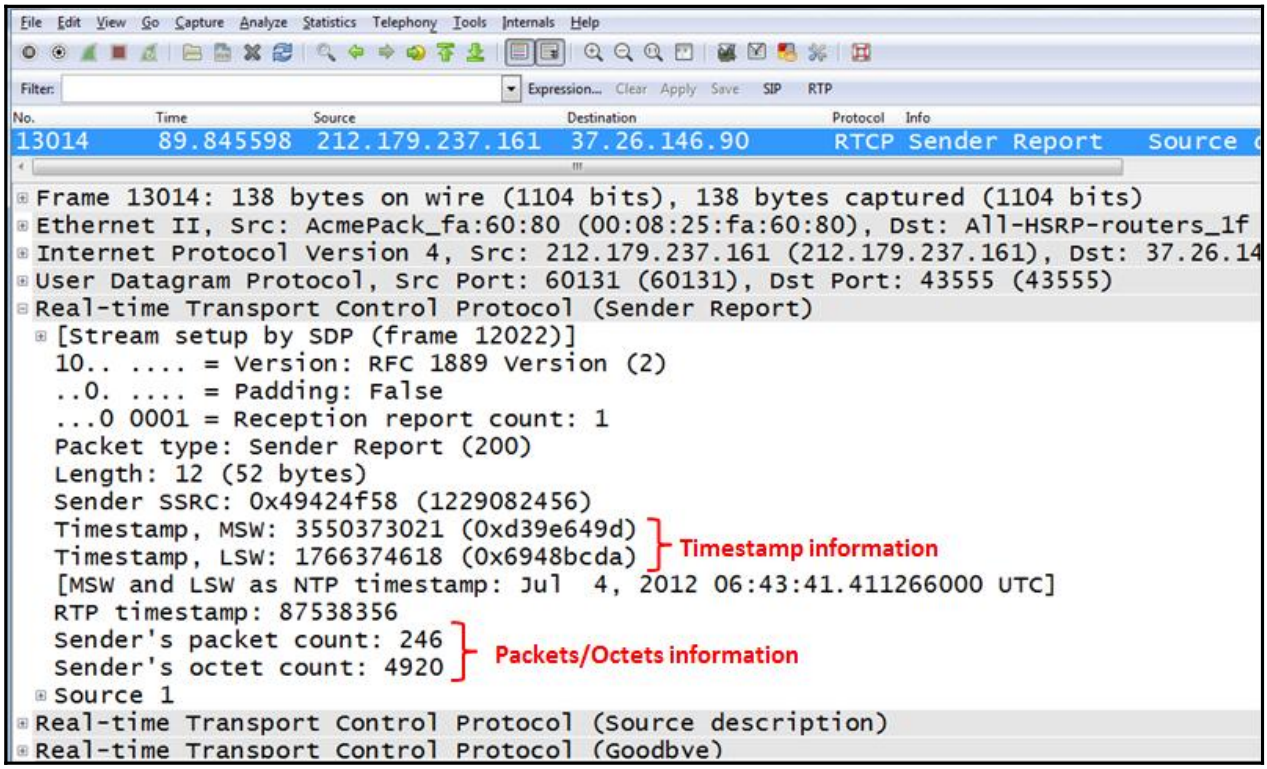
```
▶ Frame 2069: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
▶ Ethernet II, Src: Cisco_b7:17:0a (00:0b:45:b7:17:0a), Dst: Cisco_76:b5:12 (a4:4c:11:76:b5:12)
▶ Internet Protocol Version 4, Src: 14.50.201.48, Dst: 172.18.110.203
▶ User Datagram Protocol, Src Port: 23979, Dst Port: 8229
▼ Real-time Transport Control Protocol (Sender Report)
  ▼ [Stream setup by SDP (frame 72)]
      [Setup frame: 72]
      [Setup Method: SDP]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 0001 = Reception report count: 1
    Packet type: Sender Report (200)
    Length: 12 (52 bytes)
    Sender SSRC: 0x252eb528 (623818024)
    Timestamp, MSW: 3728372393 (0xde3a72a9)
    Timestamp, LSW: 3179194385 (0xbd7ea811)
    [MSW and LSW as NTP timestamp: Feb 23, 2018 10:59:53.740213874 UTC]
    RTP timestamp: 1645146724
    Sender's packet count: 298
    Sender's octet count: 47680
  ▼ Source 1
      Identifier: 0x236c6654 (594306644)
    ▼ SSRC contents
        Fraction lost: 0 / 256
        Cumulative number of packets lost: 0
    ▼ Extended highest sequence number received: 17549
        Sequence number cycles count: 0
        Highest sequence number received: 17549
      Interarrival jitter: 2
      Last SR timestamp: 1923794062 (0x72aac48e)
      Delay since last SR timestamp: 33685 (513 milliseconds)
▶ Real-time Transport Control Protocol (Source description)
```

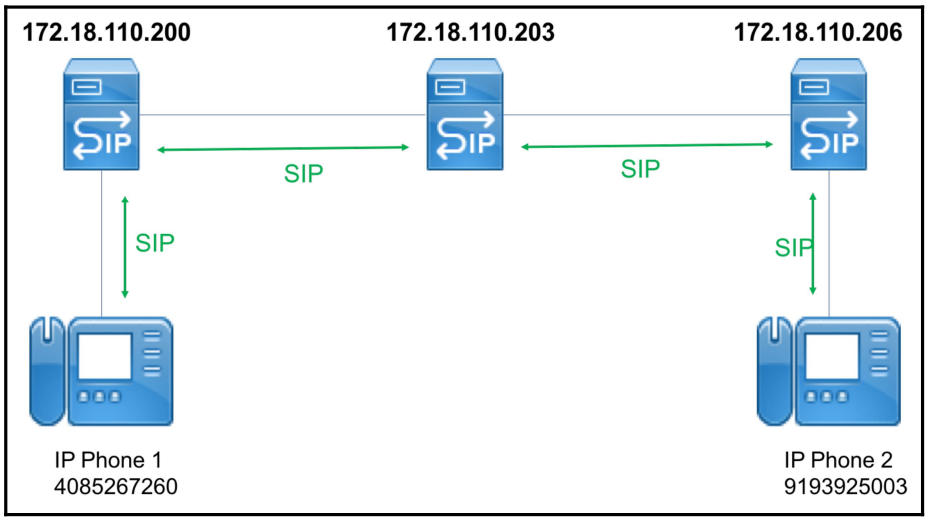


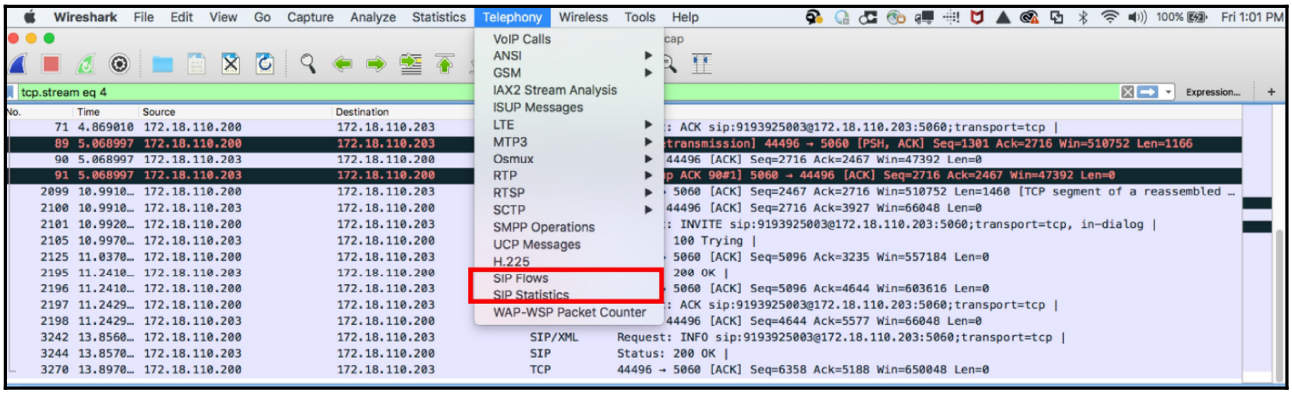
L2 Header	IP Header	UDP Header	RTP Header	Voice Payload

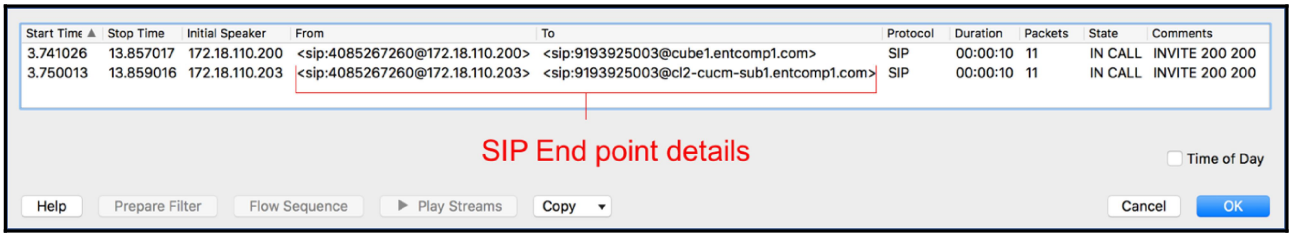

Padding bit
Extension bit
CSRC count
Marker bit
Payload Type
Version
V
P
X
CC
M
PT
Sequence Number
Timestamp
Synchronization Source (SSRC) Identifier
CSRC – Contribution Source Identifiers (if mixers are used)
Header Extension
Payload Header (Payload Format Depended)
Payload Data
Padding
32bits

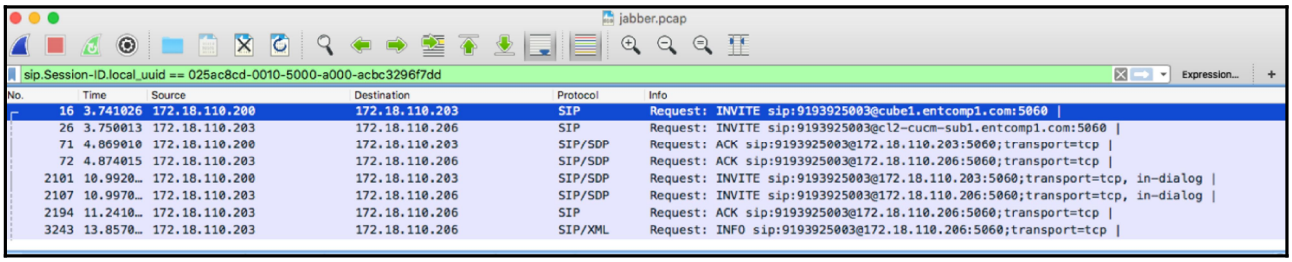

Pkt 1
Pkt 2
Pkt 3
Pkt 4
SEQ=1
SEQ=2
SEQ=3
SEQ=4
1
2
3
4
5
6
7
8
Time
TS=1
TS=12
TS=26
TS=37
1
10
20
30
40
50
60
70
80
90
100
Time

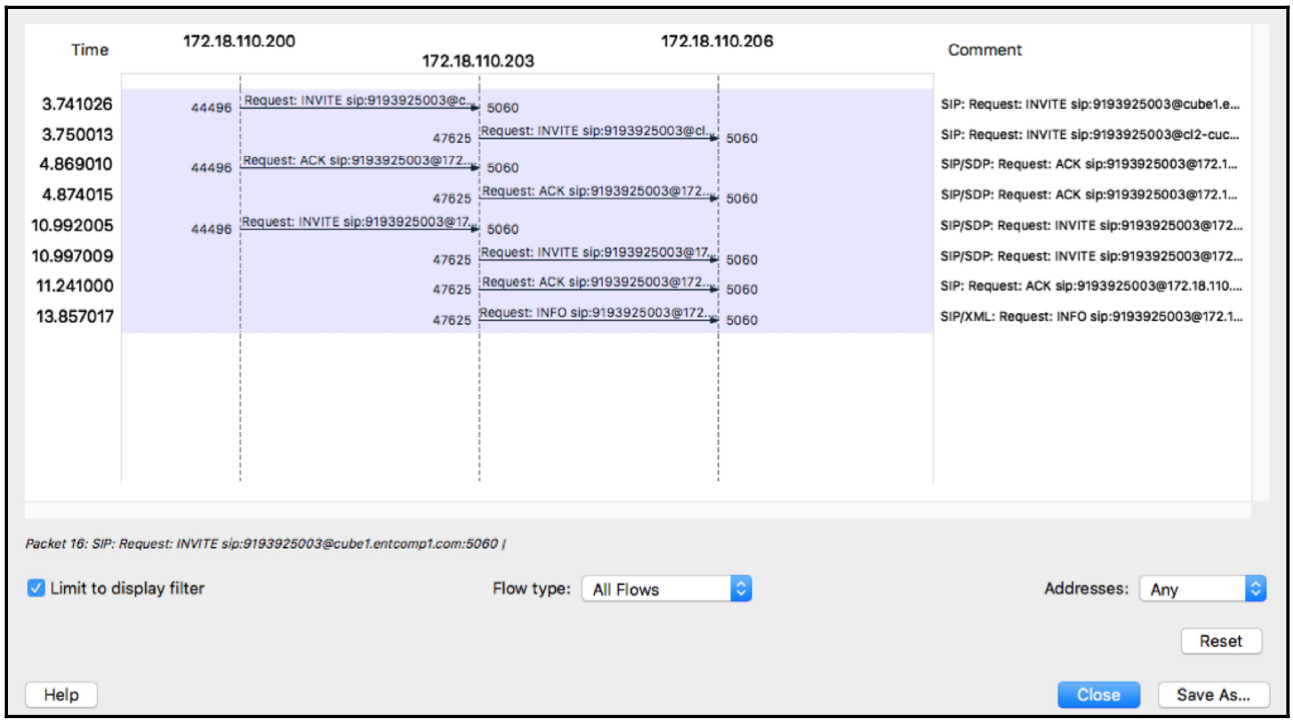

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save SIP RTP
No. Time Source Destination Protocol Info
13014 89.845598 212.179.237.161 37.26.146.90 RTCP Sender Report Source
Frame 13014: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits)
Ethernet II, Src: AcmePack_fa:60:80 (00:08:25:fa:60:80), Dst: All-HSRP-routers_1f
Internet Protocol Version 4, Src: 212.179.237.161 (212.179.237.161), Dst: 37.26.14
User Datagram Protocol, Src Port: 60131 (60131), Dst Port: 43555 (43555)
Real-time Transport Control Protocol (Sender Report)
[Stream setup by SDP (frame 12022)]
10.. .... = Version: RFC 1889 Version (2)
..0. .... = Padding: False
...0 0001 = Reception report count: 1
Packet type: Sender Report (200)
Length: 12 (52 bytes)
Sender SSRC: 0x49424f58 (1229082456)
Timestamp, MSW: 3550373021 (0xd39e649d)
Timestamp, LSW: 1766374618 (0x6948bcda)
Timestamp information
[MSW and LSW as NTP timestamp: Jul 4, 2012 06:43:41.411266000 UTC]
RTP timestamp: 87538356
Sender's packet count: 246
Sender's octet count: 4920
Packets/Octets information
Source 1
Real-time Transport Control Protocol (Source description)
Real-time Transport Control Protocol (Goodbye)

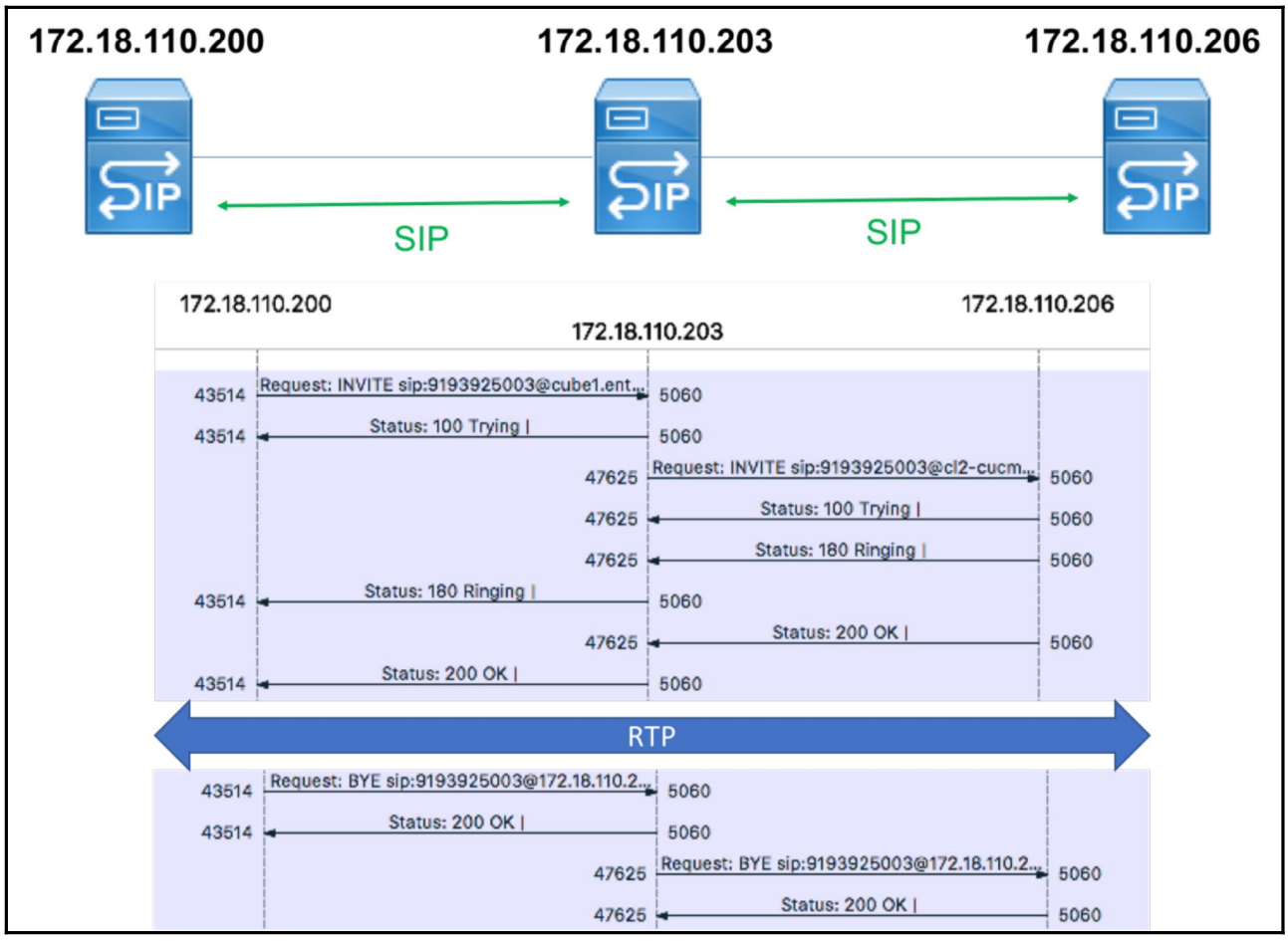

172.18.110.200
172.18.110.203
172.18.110.206
SIP
SIP
SIP
SIP
SIP
IP Phone 1
4085267260
IP Phone 2
9193925003

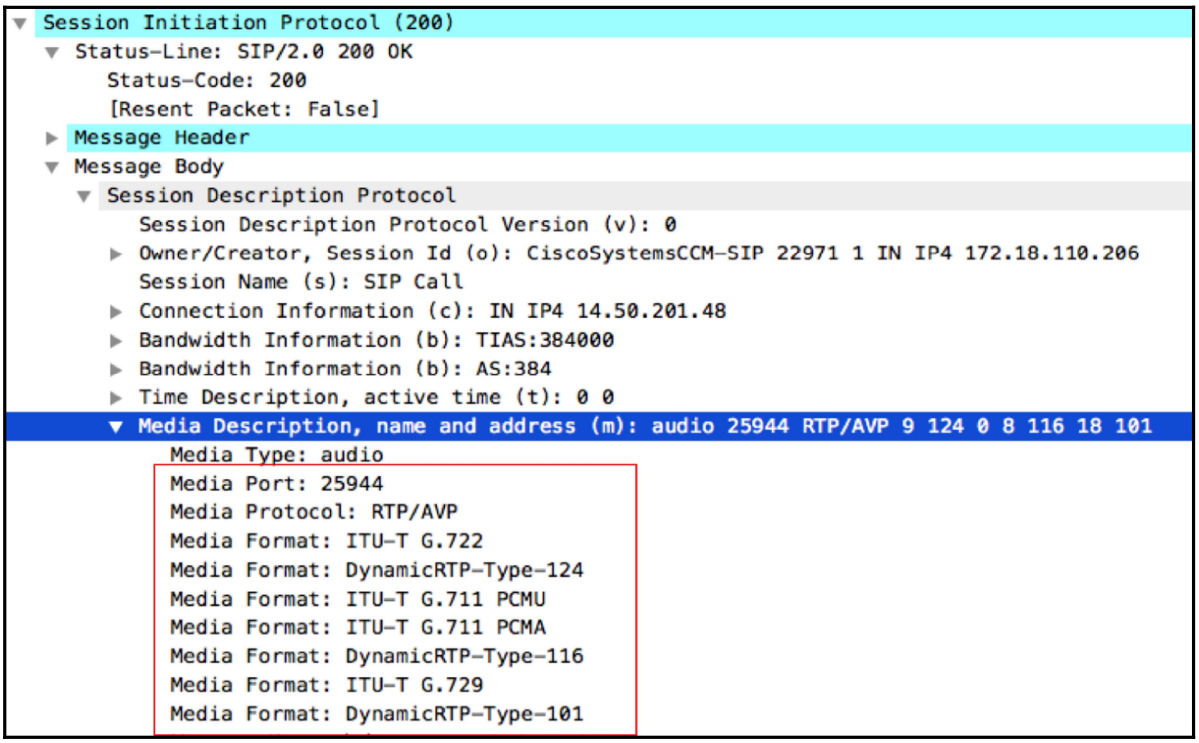

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
VoIP Calls
ANSI
GSM
IAX2 Stream Analysis
ISUP Messages
LTE
MTP3
Osmux
RTP
RTSP
SCTP
SMPP Operations
UCP Messages
H.225
SIP Flows
SIP Statistics
WAP-WSP Packet Counter
tcp.stream eq 4

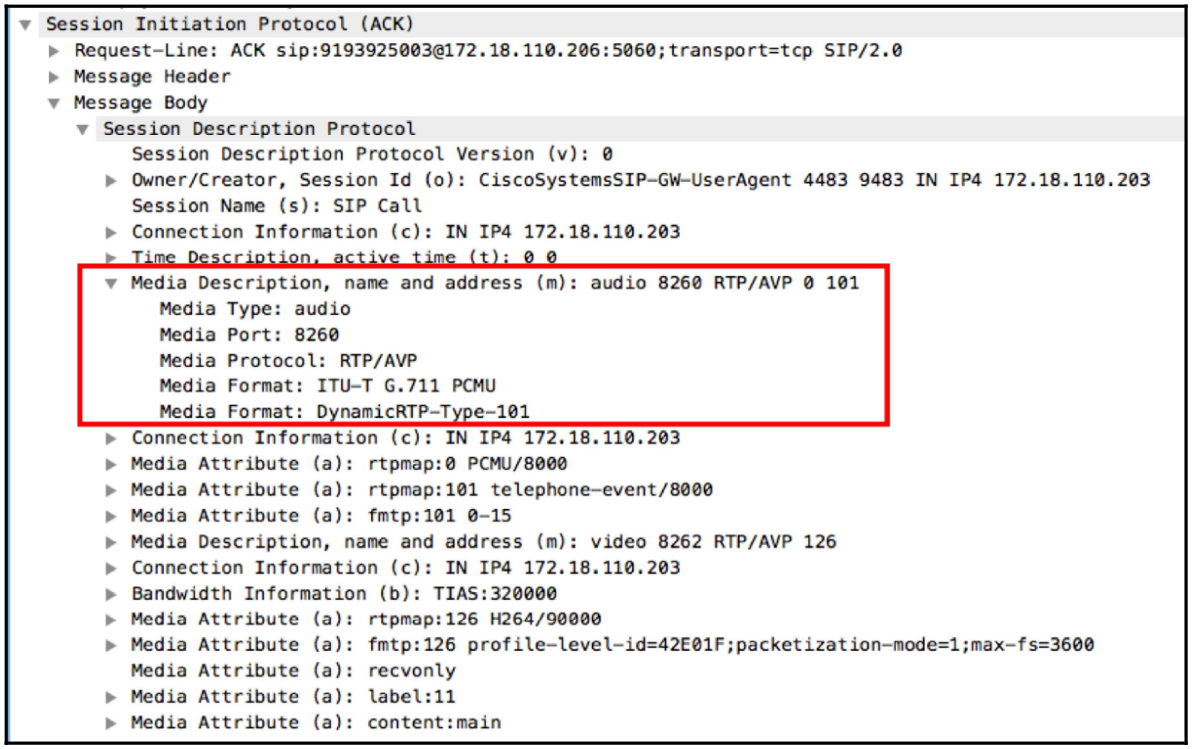

Start Time
Stop Time
Initial Speaker
From
To
Protocol
Duration
Packets
State
Comments
3.741026 13.857017 172.18.110.200 <sip:4085267260@172.18.110.200> <sip:9193925003@cube1.entcomp1.com> SIP 00:00:10 11 IN CALL INVITE 200 200
3.750013 13.859016 172.18.110.203 <sip:4085267260@172.18.110.203> <sip:9193925003@cl2-cucm-sub1.entcomp1.com> SIP 00:00:10 11 IN CALL INVITE 200 200
SIP End point details
Time of Day
Help
Prepare Filter
Flow Sequence
Play Streams
Copy
Cancel
OK

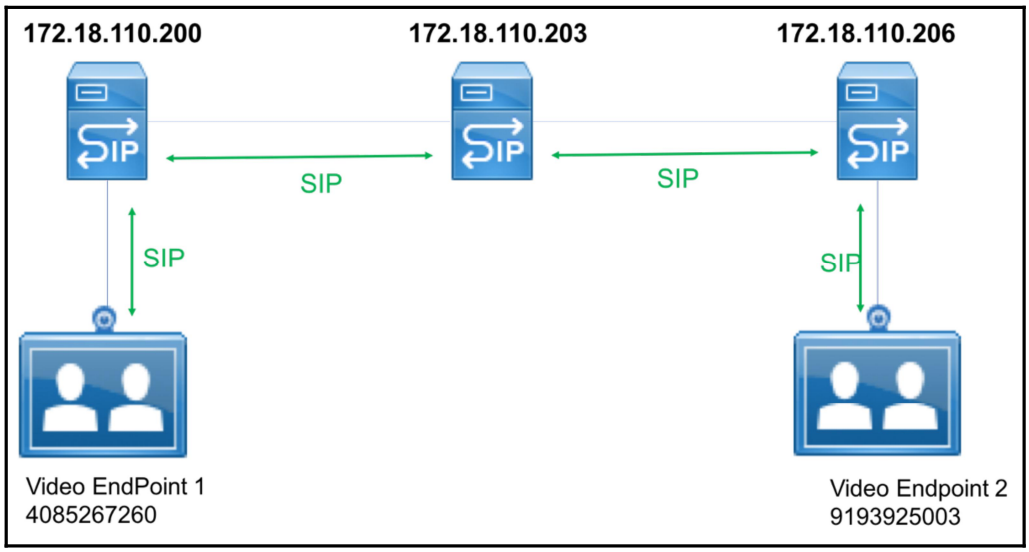

jabber.pcap
sip.Session-ID.local_uuid == 025ac8cd-0010-5000-a000-acbc3296f7dd
No. Time Source Destination Protocol Info
16 3.741026 172.18.110.200 172.18.110.203 SIP Request: INVITE sip:9193925003@cube1.entcomp1.com:5060 |
26 3.750013 172.18.110.203 172.18.110.206 SIP Request: INVITE sip:9193925003@cl2-cucm-sub1.entcomp1.com:5060 |
71 4.869010 172.18.110.200 172.18.110.203 SIP/SDP Request: ACK sip:9193925003@172.18.110.203:5060;transport=tcp |
72 4.874015 172.18.110.203 172.18.110.206 SIP/SDP Request: ACK sip:9193925003@172.18.110.206:5060;transport=tcp |
2101 10.9920… 172.18.110.200 172.18.110.203 SIP/SDP Request: INVITE sip:9193925003@172.18.110.203:5060;transport=tcp, in-dialog |
2107 10.9970… 172.18.110.203 172.18.110.206 SIP/SDP Request: INVITE sip:9193925003@172.18.110.206:5060;transport=tcp, in-dialog |
2194 11.2410… 172.18.110.203 172.18.110.206 SIP Request: ACK sip:9193925003@172.18.110.206:5060;transport=tcp |
3243 13.8570… 172.18.110.203 172.18.110.206 SIP/XML Request: INFO sip:9193925003@172.18.110.206:5060;transport=tcp |

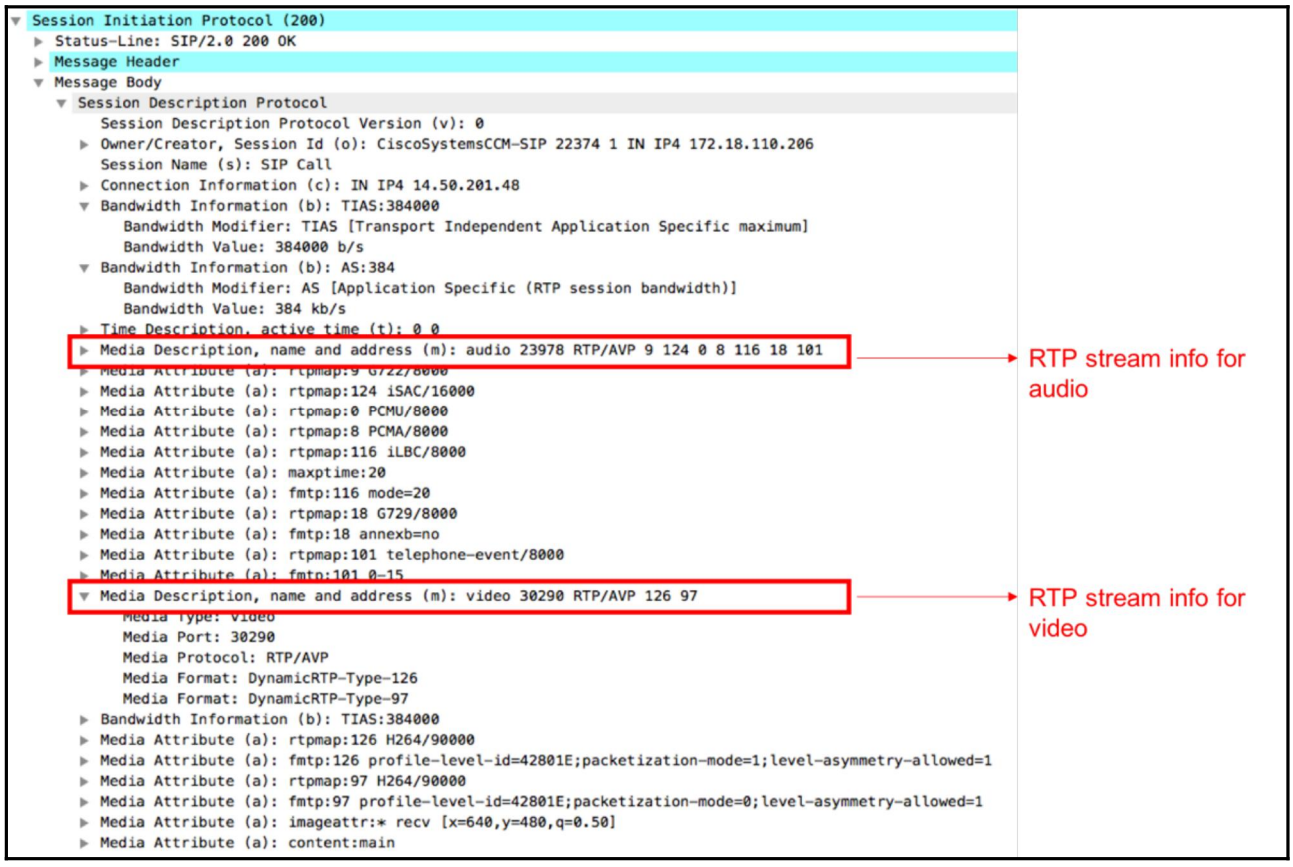

Time
172.18.110.200
172.18.110.203
172.18.110.206
Comment
3.741026
44496
Request: INVITE sip:9193925003@c...
5060
SIP: Request: INVITE sip:9193925003@cube1.e...
3.750013
47625
Request: INVITE sip:9193925003@cl...
5060
SIP: Request: INVITE sip:9193925003@cl2-cuc...
4.869010
44496
Request: ACK sip:9193925003@172...
5060
SIP/SDP: Request: ACK sip:9193925003@172.1...
4.874015
47625
Request: ACK sip:9193925003@172...
5060
SIP/SDP: Request: ACK sip:9193925003@172.1...
10.992005
44496
Request: INVITE sip:9193925003@17...
5060
SIP/SDP: Request: INVITE sip:9193925003@172...
10.997009
47625
Request: INVITE sip:9193925003@17...
5060
SIP/SDP: Request: INVITE sip:9193925003@172...
11.241000
47625
Request: ACK sip:9193925003@172...
5060
SIP: Request: ACK sip:9193925003@172.18.110....
13.857017
47625
Request: INFO sip:9193925003@172...
5060
SIP/XML: Request: INFO sip:9193925003@172.1...
Packet 16: SIP: Request: INVITE sip:9193925003@cube1.entcomp1.com:5060 |
Limit to display filter
Flow type:
All Flows
Addresses:
Any
Reset
Help
Close
Save As...


172.18.110.200
172.18.110.203
172.18.110.206
SIP
SIP
172.18.110.200
172.18.110.203
172.18.110.206
43514 Request: INVITE sip:9193925003@cube1.ent... 5060
43514 Status: 100 Trying | 5060
47625 Request: INVITE sip:9193925003@cl2-cucm... 5060
47625 Status: 100 Trying | 5060
47625 Status: 180 Ringing | 5060
43514 Status: 180 Ringing | 5060
47625 Status: 200 OK | 5060
43514 Status: 200 OK | 5060
RTP
43514 Request: BYE sip:9193925003@172.18.110.2... 5060
43514 Status: 200 OK | 5060
47625 Request: BYE sip:9193925003@172.18.110.2... 5060
47625 Status: 200 OK | 5060

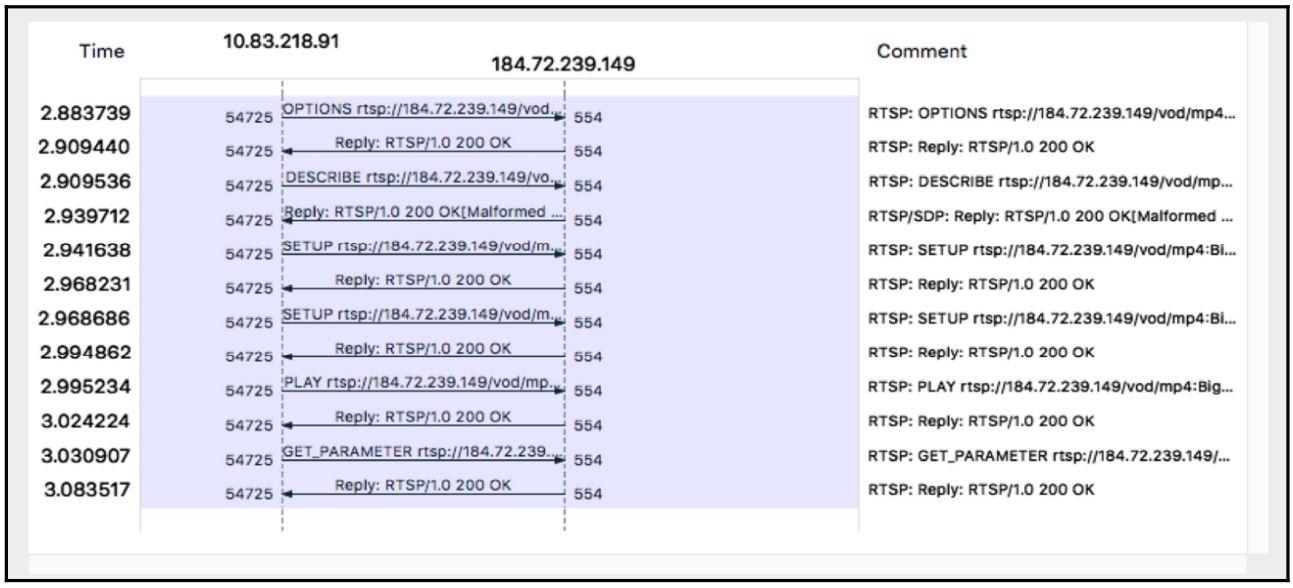

Session Initiation Protocol (200)
Status-Line: SIP/2.0 200 OK
Status-Code: 200
[Resent Packet: False]
Message Header
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): CiscoSystemsCCM-SIP 22971 1 IN IP4 172.18.110.206
Session Name (s): SIP Call
Connection Information (c): IN IP4 14.50.201.48
Bandwidth Information (b): TIAS:384000
Bandwidth Information (b): AS:384
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 25944 RTP/AVP 9 124 0 8 116 18 101
Media Type: audio
Media Port: 25944
Media Protocol: RTP/AVP
Media Format: ITU-T G.722
Media Format: DynamicRTP-Type-124
Media Format: ITU-T G.711 PCMU
Media Format: ITU-T G.711 PCMA
Media Format: DynamicRTP-Type-116
Media Format: ITU-T G.729
Media Format: DynamicRTP-Type-101

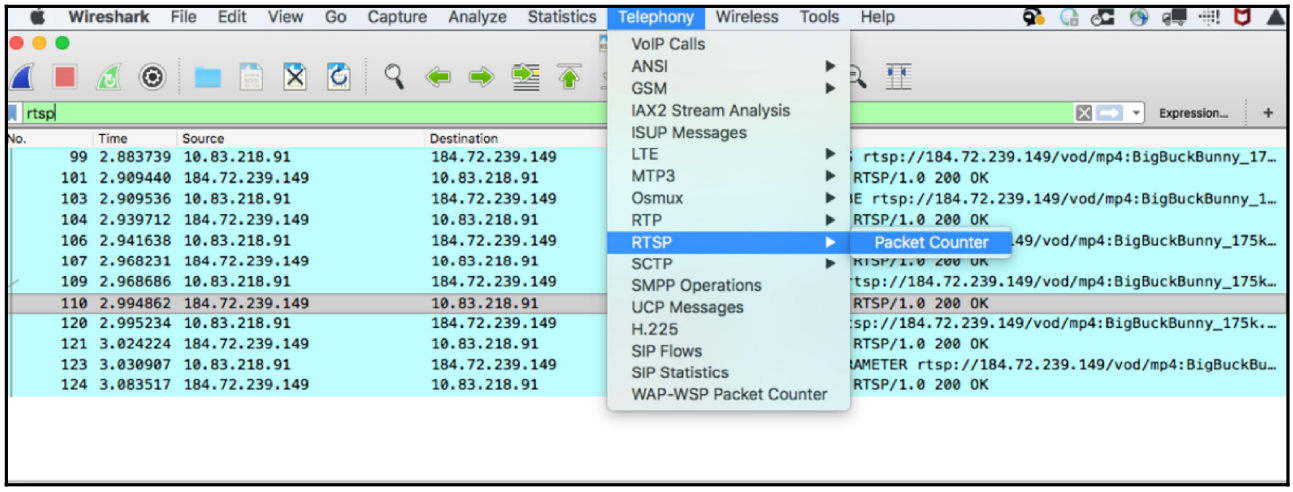

Session Initiation Protocol (ACK)
Request-Line: ACK sip:9193925003@172.18.110.206:5060;transport=tcp SIP/2.0
Message Header
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): CiscoSystemsSIP-GW-UserAgent 4483 9483 IN IP4 172.18.110.203
Session Name (s): SIP Call
Connection Information (c): IN IP4 172.18.110.203
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 8260 RTP/AVP 0 101
Media Type: audio
Media Port: 8260
Media Protocol: RTP/AVP
Media Format: ITU-T G.711 PCMU
Media Format: DynamicRTP-Type-101
Connection Information (c): IN IP4 172.18.110.203
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): fmtp:101 0-15
Media Description, name and address (m): video 8262 RTP/AVP 126
Connection Information (c): IN IP4 172.18.110.203
Bandwidth Information (b): TIAS:320000
Media Attribute (a): rtpmap:126 H264/90000
Media Attribute (a): fmtp:126 profile-level-id=42E01F;packetization-mode=1;max-fs=3600
Media Attribute (a): recvonly
Media Attribute (a): label:11
Media Attribute (a): content:main

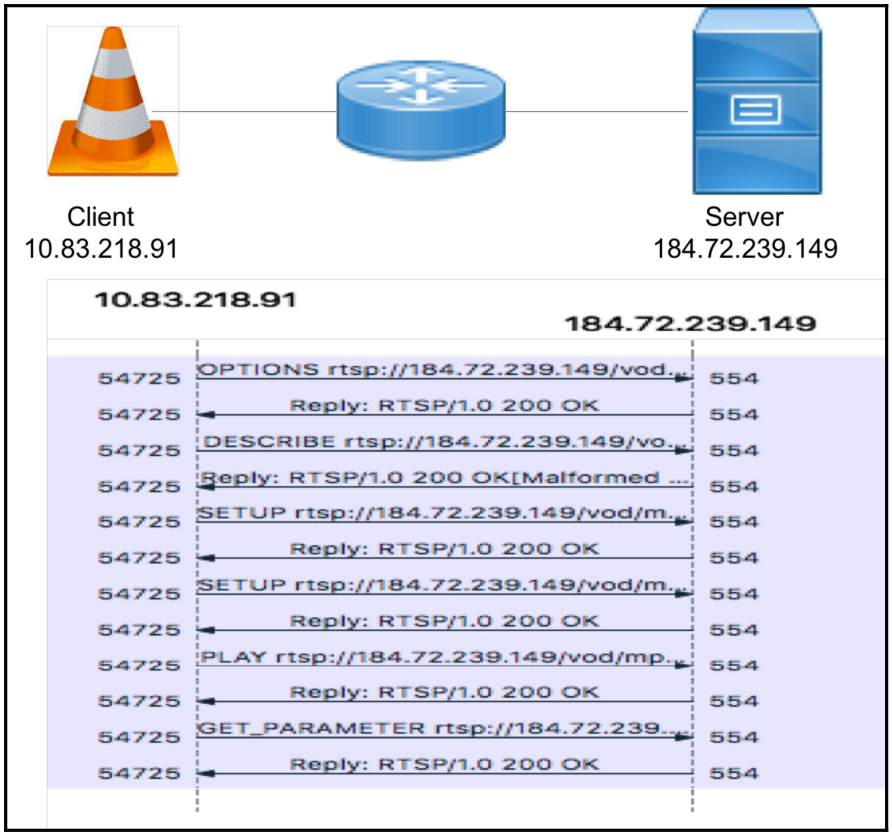

172.18.110.200
172.18.110.203
172.18.110.206
SIP
SIP
SIP
SIP
SIP
Video EndPoint 1
4085267260
Video Endpoint 2
9193925003


Session Initiation Protocol (200)
Status-Line: SIP/2.0 200 OK
Message Header
Message Body
Session Description Protocol
Session Description Protocol Version (v): 0
Owner/Creator, Session Id (o): CiscoSystemsCCM-SIP 22374 1 IN IP4 172.18.110.206
Session Name (s): SIP Call
Connection Information (c): IN IP4 14.50.201.48
Bandwidth Information (b): TIAS:384000
Bandwidth Modifier: TIAS [Transport Independent Application Specific maximum]
Bandwidth Value: 384000 b/s
Bandwidth Information (b): AS:384
Bandwidth Modifier: AS [Application Specific (RTP session bandwidth)]
Bandwidth Value: 384 kb/s
Time Description, active time (t): 0 0
Media Description, name and address (m): audio 23978 RTP/AVP 9 124 0 8 116 18 101
Media Attribute (a): rtpmap:124 iSAC/16000
Media Attribute (a): rtpmap:0 PCMU/8000
Media Attribute (a): rtpmap:8 PCMA/8000
Media Attribute (a): rtpmap:116 iLBC/8000
Media Attribute (a): maxptime:20
Media Attribute (a): fmtp:116 mode=20
Media Attribute (a): rtpmap:18 G729/8000
Media Attribute (a): fmtp:18 annexb=no
Media Attribute (a): rtpmap:101 telephone-event/8000
Media Attribute (a): fmtp:101 0-15
Media Description, name and address (m): video 30290 RTP/AVP 126 97
Media Port: 30290
Media Protocol: RTP/AVP
Media Format: DynamicRTP-Type-126
Media Format: DynamicRTP-Type-97
Bandwidth Information (b): TIAS:384000
Media Attribute (a): rtpmap:126 H264/90000
Media Attribute (a): fmtp:126 profile-level-id=42801E;packetization-mode=1;level-asymmetry-allowed=1
Media Attribute (a): rtpmap:97 H264/90000
Media Attribute (a): fmtp:97 profile-level-id=42801E;packetization-mode=0;level-asymmetry-allowed=1
Media Attribute (a): imageattr:* recv [x=640,y=480,q=0.50]
Media Attribute (a): content:main
RTP stream info for audio
RTP stream info for video

```
▶ Frame 116: 63 bytes on wire (504 bits), 63 bytes captured (504 bits)
▶ Ethernet II, Src: Cisco_b7:17:0a (00:0b:45:b7:17:0a), Dst: Cisco_76:b5:12 (a4:4c:11:76:b5:12)
▶ Internet Protocol Version 4, Src: 14.50.201.48, Dst: 172.18.110.203
▶ User Datagram Protocol, Src Port: 30290, Dst Port: 8230
▼ Real-Time Transport Protocol
  ▶ [Stream setup by SDP (frame 72)]
    10.. .... = Version: RFC 1889 Version (2)
    ..0. .... = Padding: False
    ...0 .... = Extension: False
    .... 0000 = Contributing source identifiers count: 0
    0... .... = Marker: False
    Payload type: H264 (126)
    Sequence number: 50377
    [Extended sequence number: 50377]
    Timestamp: 252700497
    Synchronization Source identifier: 0xe3969445 (3818296389)
▶ H.264
```



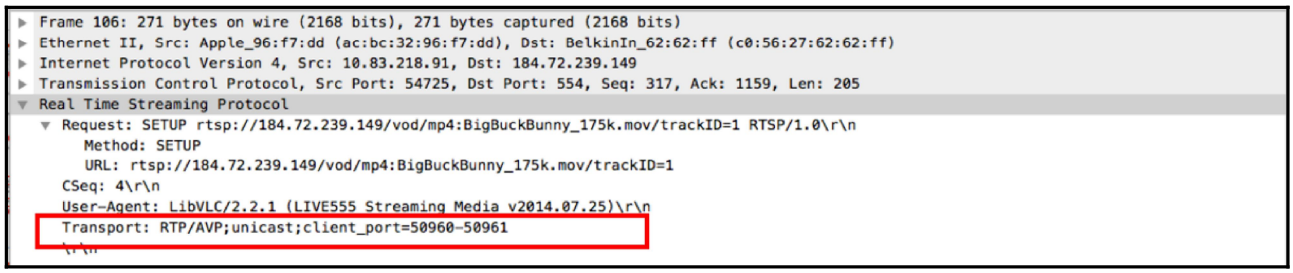

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
rtsp
No. Time Source Destination
99 2.883739 10.83.218.91 184.72.239.149
101 2.909440 184.72.239.149 10.83.218.91
103 2.909536 10.83.218.91 184.72.239.149
104 2.939712 184.72.239.149 10.83.218.91
106 2.941638 10.83.218.91 184.72.239.149
107 2.968231 184.72.239.149 10.83.218.91
109 2.968686 10.83.218.91 184.72.239.149
110 2.994862 184.72.239.149 10.83.218.91
120 2.995234 10.83.218.91 184.72.239.149
121 3.024224 184.72.239.149 10.83.218.91
123 3.030907 10.83.218.91 184.72.239.149
124 3.083517 184.72.239.149 10.83.218.91
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
Packet Counter

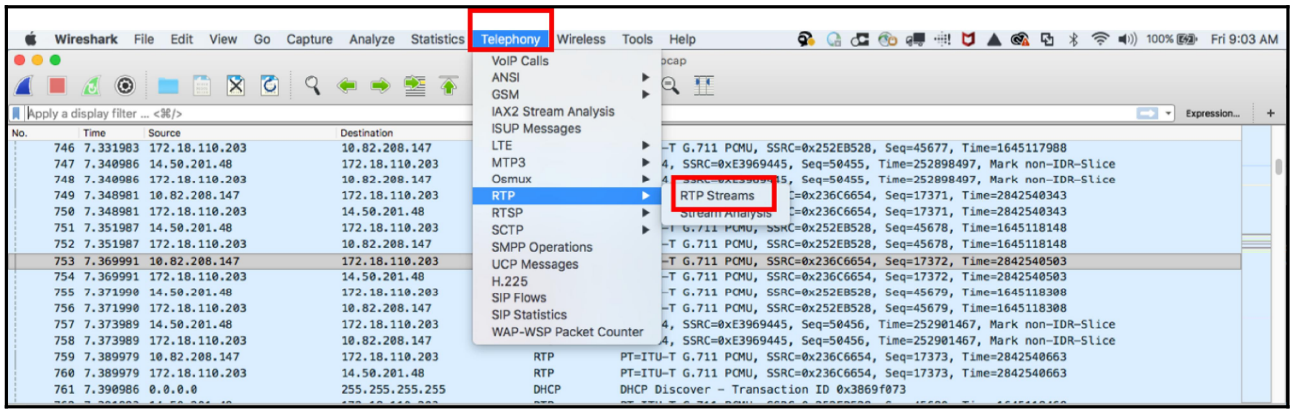

Client
10.83.218.91
Server
184.72.239.149
10.83.218.91
184.72.239.149
54725 OPTIONS rtsp://184.72.239.149/vod... 554
54725 Reply: RTSP/1.0 200 OK 554
54725 DESCRIBE rtsp://184.72.239.149/vo... 554
54725 Reply: RTSP/1.0 200 OK[Malformed ... 554
54725 SETUP rtsp://184.72.239.149/vod/m... 554
54725 Reply: RTSP/1.0 200 OK 554
54725 SETUP rtsp://184.72.239.149/vod/m... 554
54725 Reply: RTSP/1.0 200 OK 554
54725 PLAY rtsp://184.72.239.149/vod/mp... 554
54725 Reply: RTSP/1.0 200 OK 554
54725 GET_PARAMETER rtsp://184.72.239... 554
54725 Reply: RTSP/1.0 200 OK 554

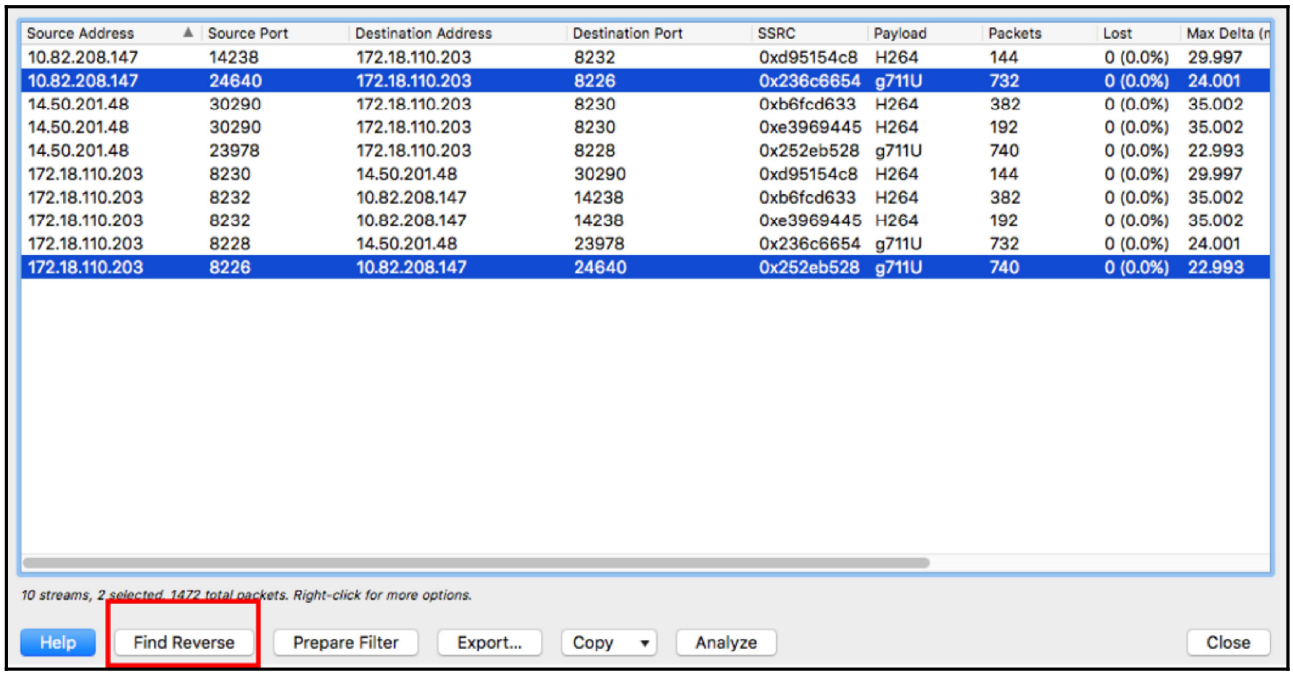
```
▶ Frame 99: 211 bytes on wire (1688 bits), 211 bytes captured (1688 bits)
▶ Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
▶ Internet Protocol Version 4, Src: 10.83.218.91, Dst: 184.72.239.149
▶ Transmission Control Protocol, Src Port: 54725, Dst Port: 554, Seq: 1, Ack: 1, Len: 145
▼ Real Time Streaming Protocol
  ▼ Request: OPTIONS rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov RTSP/1.0\r\n
      Method: OPTIONS
      URL: rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov
    CSeq: 2\r\n
    User-Agent: LibVLC/2.2.1 (LIVE555 Streaming Media v2014.07.25)\r\n
    \r\n
```

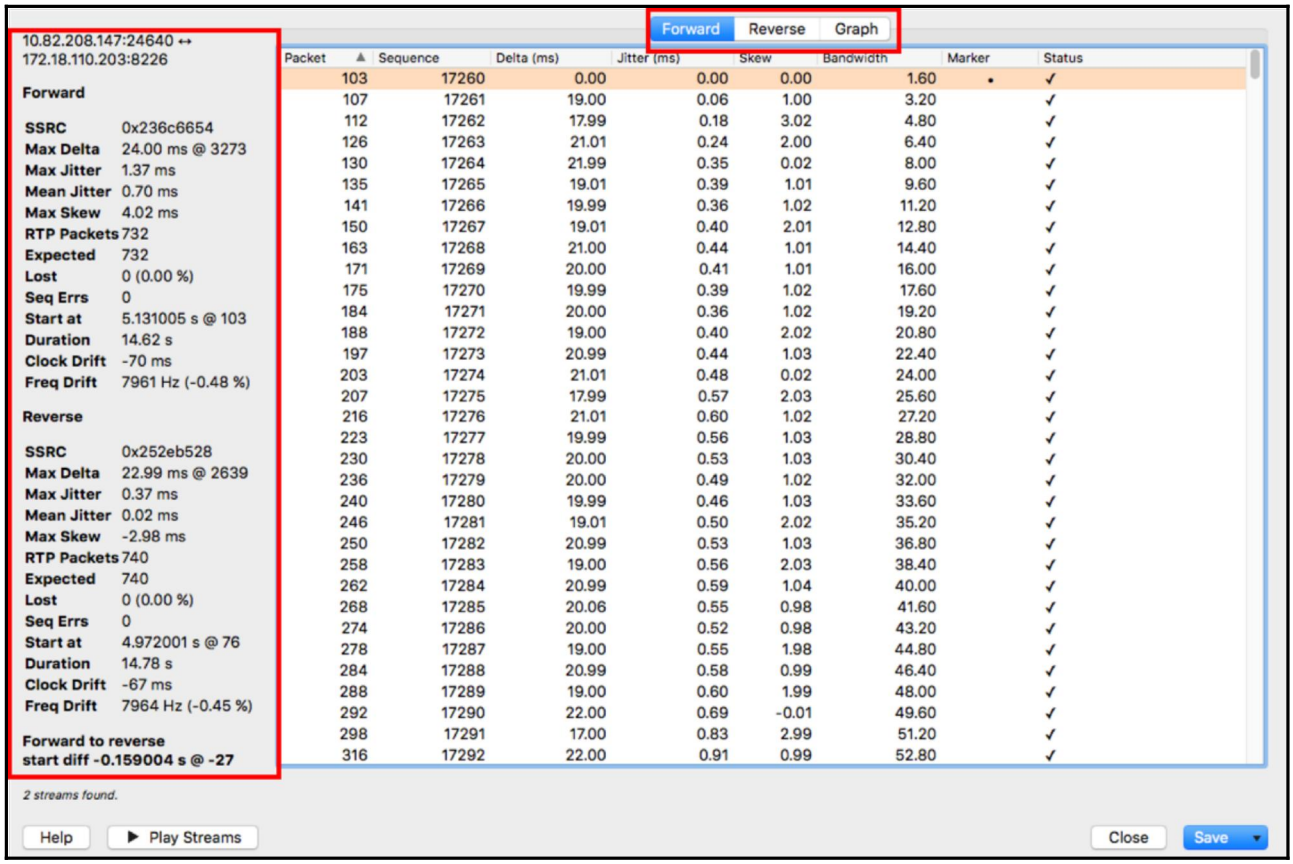
```
▶ Frame 103: 237 bytes on wire (1896 bits), 237 bytes captured (1896 bits)
▶ Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
▶ Internet Protocol Version 4, Src: 10.83.218.91, Dst: 184.72.239.149
▶ Transmission Control Protocol, Src Port: 54725, Dst Port: 554, Seq: 146, Ack: 235, Len: 171
▼ Real Time Streaming Protocol
  ▼ Request: DESCRIBE rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov RTSP/1.0\r\n
      Method: DESCRIBE
      URL: rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov
    CSeq: 3\r\n
    User-Agent: LibVLC/2.2.1 (LIVE555 Streaming Media v2014.07.25)\r\n
    Accept: application/sdp\r\n
    \r\n
```

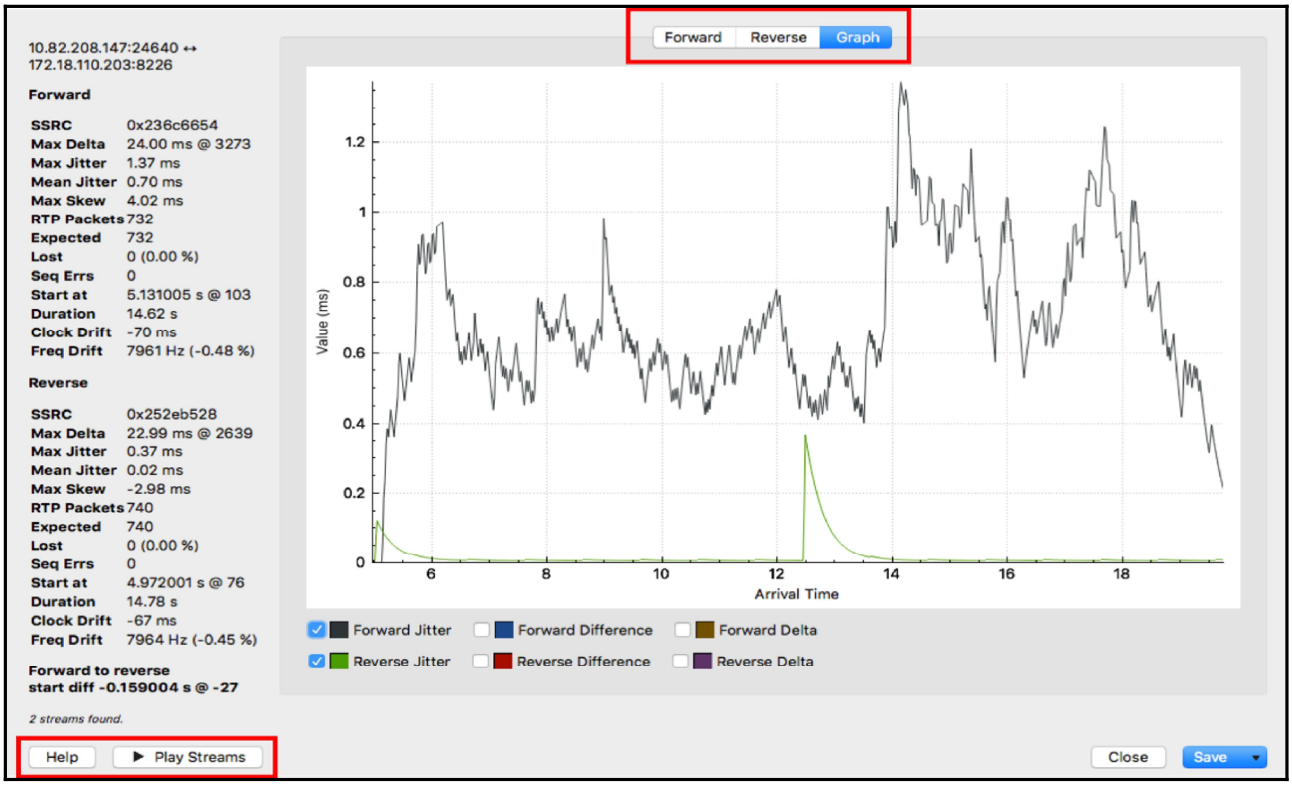
```
▶ Frame 104: 990 bytes on wire (7920 bits), 990 bytes captured (7920 bits)
▶ Ethernet II, Src: BelkinIn_62:62:ff (c0:56:27:62:62:ff), Dst: Apple_96:f7:dd (ac:bc:32:96:f7:dd)
▶ Internet Protocol Version 4, Src: 184.72.239.149, Dst: 10.83.218.91
▶ Transmission Control Protocol, Src Port: 554, Dst Port: 54725, Seq: 235, Ack: 317, Len: 924
▼ Real Time Streaming Protocol
  ▼ Response: RTSP/1.0 200 OK\r\n
      Status: 200
    CSeq: 3\r\n
    Server: Wowza Streaming Engine 4.7.3.02 build21313\r\n
    Cache-Control: no-cache\r\n
    Expires: Thu, 22 Feb 2018 01:08:08 UTC\r\n
    Content-length: 590
    Content-Base: rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov/\r\n
    Date: Thu, 22 Feb 2018 01:08:08 UTC\r\n
    Content-type: application/sdp
    Session: 1785054106;timeout=60
    \r\n
  ▼ Session Description Protocol
      Session Description Protocol Version (v): 0
    ▶ Owner/Creator, Session Id (o): - 1785054106 1785054106 IN IP4 184.72.239.149
      Session Name (s): BigBuckBunny_175k.mov
    ▶ Connection Information (c): IN IP4 184.72.239.149
    ▶ Time Description, active time (t): 0 0
    ▶ Session Attribute (a): sdplang:en
    ▶ Session Attribute (a): range:npt=0- 596.458
    ▶ Session Attribute (a): control:*
    ▶ Media Description, name and address (m): audio 0 RTP/AVP 96
    ▶ Media Attribute (a): rtpmap:96 mpeg4-generic/48000/2
    ▶ Media Attribute (a): fmtp:96 profile-level-id=1;mode=AAC-hbr;sizelength=13;indexlength=3;indexdeltalength=3;config=1190
    ▶ Media Attribute (a): control:trackID=1
    ▶ Media Description, name and address (m): video 0 RTP/AVP 97
    ▶ Media Attribute (a): rtpmap:97 H264/90000
    ▶ Media Attribute (a): fmtp:97 packetization-mode=1;profile-level-id=42C01E;sprop-parameter-sets=Z0LAHtkDxWhAAAADAEAAAAwDxYuS,aMuMsg==
    ▶ Media Attribute (a): cliprect:0,0,160,240
    ▶ Media Attribute (a): framesize:97 240-160
    ▶ Media Attribute (a): framerate:24.0
    ▶ Media Attribute (a): control:trackID=2
```

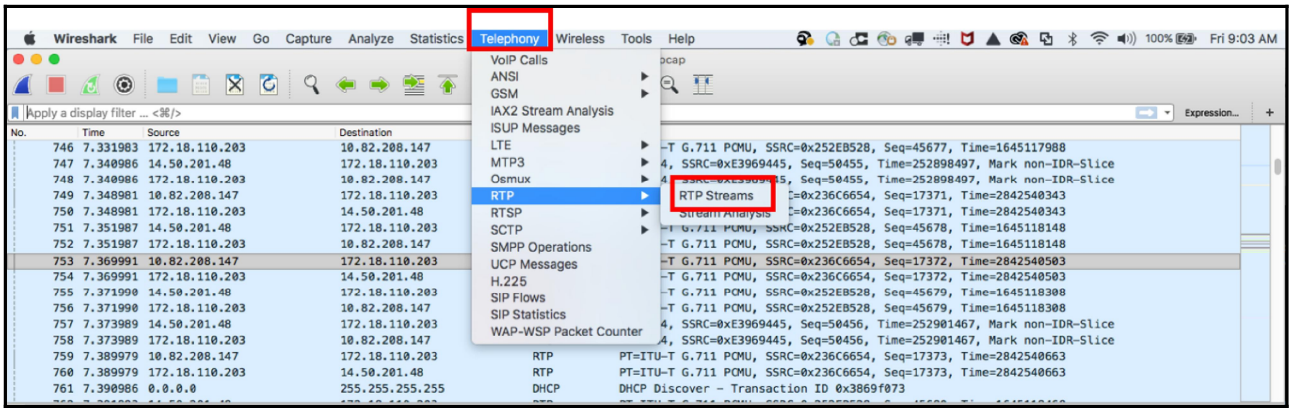

Frame 106: 271 bytes on wire (2168 bits), 271 bytes captured (2168 bits)
Ethernet II, Src: Apple_96:f7:dd (ac:bc:32:96:f7:dd), Dst: BelkinIn_62:62:ff (c0:56:27:62:62:ff)
Internet Protocol Version 4, Src: 10.83.218.91, Dst: 184.72.239.149
Transmission Control Protocol, Src Port: 54725, Dst Port: 554, Seq: 317, Ack: 1159, Len: 205
Real Time Streaming Protocol
Request: SETUP rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov/trackID=1 RTSP/1.0\r\n
Method: SETUP
URL: rtsp://184.72.239.149/vod/mp4:BigBuckBunny_175k.mov/trackID=1
CSeq: 4\r\n
User-Agent: LibVLC/2.2.1 (LIVE555 Streaming Media v2014.07.25)\r\n
Transport: RTP/AVP;unicast;client_port=50960-50961

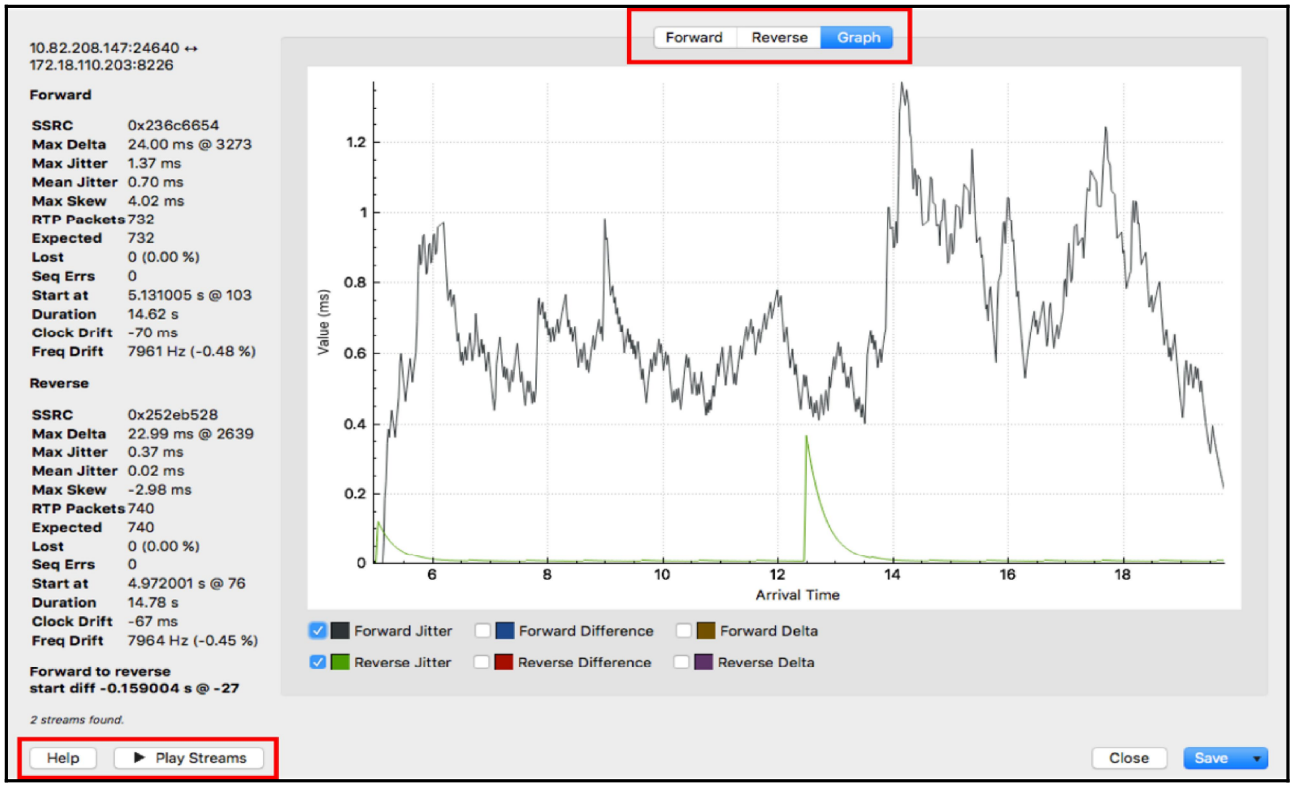

Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
VoIP Calls
ANSI
GSM
IAX2 Stream Analysis
ISUP Messages
LTE
MTP3
Osmux
RTP
RTSP
SCTP
SMPP Operations
UCP Messages
H.225
SIP Flows
SIP Statistics
WAP-WSP Packet Counter
RTP Streams


Source Address
Source Port
Destination Address
Destination Port
SSRC
Payload
Packets
Lost
Max Delta
10.82.208.147 14238 172.18.110.203 8232 0xd95154c8 H264 144 0 (0.0%) 29.997
10.82.208.147 24640 172.18.110.203 8226 0x236c6654 g711U 732 0 (0.0%) 24.001
14.50.201.48 30290 172.18.110.203 8230 0xb6fcd633 H264 382 0 (0.0%) 35.002
14.50.201.48 30290 172.18.110.203 8230 0xe3969445 H264 192 0 (0.0%) 35.002
14.50.201.48 23978 172.18.110.203 8228 0x252eb528 g711U 740 0 (0.0%) 22.993
172.18.110.203 8230 14.50.201.48 30290 0xd95154c8 H264 144 0 (0.0%) 29.997
172.18.110.203 8232 10.82.208.147 14238 0xb6fcd633 H264 382 0 (0.0%) 35.002
172.18.110.203 8232 10.82.208.147 14238 0xe3969445 H264 192 0 (0.0%) 35.002
172.18.110.203 8228 14.50.201.48 23978 0x236c6654 g711U 732 0 (0.0%) 24.001
172.18.110.203 8226 10.82.208.147 24640 0x252eb528 g711U 740 0 (0.0%) 22.993
10 streams, 2 selected, 1472 total packets. Right-click for more options.
Help
Find Reverse
Prepare Filter
Export...
Copy
Analyze
Close

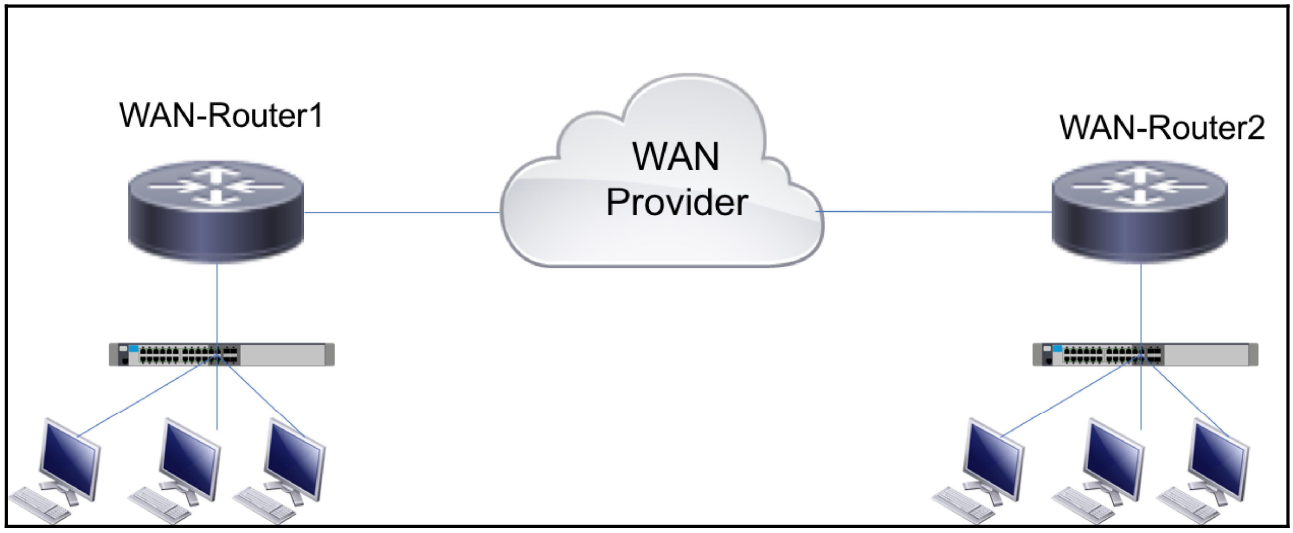

Forward
Reverse
Graph
10.82.208.147:24640 ↔
172.18.110.203:8226
Forward
SSRC 0x236c6654
Max Delta 24.00 ms @ 3273
Max Jitter 1.37 ms
Mean Jitter 0.70 ms
Max Skew 4.02 ms
RTP Packets 732
Expected 732
Lost 0 (0.00 %)
Seq Errs 0
Start at 5.131005 s @ 103
Duration 14.62 s
Clock Drift -70 ms
Freq Drift 7961 Hz (-0.48 %)
Reverse
SSRC 0x252eb528
Max Delta 22.99 ms @ 2639
Max Jitter 0.37 ms
Mean Jitter 0.02 ms
Max Skew -2.98 ms
RTP Packets 740
Expected 740
Lost 0 (0.00 %)
Seq Errs 0
Start at 4.972001 s @ 76
Duration 14.78 s
Clock Drift -67 ms
Freq Drift 7964 Hz (-0.45 %)
Forward to reverse
start diff -0.159004 s @ -27
Packet Sequence Delta (ms) Jitter (ms) Skew Bandwidth Marker Status
103 17260 0.00 0.00 0.00 1.60 ✓
107 17261 19.00 0.06 1.00 3.20 ✓
112 17262 17.99 0.18 3.02 4.80 ✓
126 17263 21.01 0.24 2.00 6.40 ✓
130 17264 21.99 0.35 0.02 8.00 ✓
135 17265 19.01 0.39 1.01 9.60 ✓
141 17266 19.99 0.36 1.02 11.20 ✓
150 17267 19.01 0.40 2.01 12.80 ✓
163 17268 21.00 0.44 1.01 14.40 ✓
171 17269 20.00 0.41 1.01 16.00 ✓
175 17270 19.99 0.39 1.02 17.60 ✓
184 17271 20.00 0.36 1.02 19.20 ✓
188 17272 19.00 0.40 2.02 20.80 ✓
197 17273 20.99 0.44 1.03 22.40 ✓
203 17274 21.01 0.48 0.02 24.00 ✓
207 17275 17.99 0.57 2.03 25.60 ✓
216 17276 21.01 0.60 1.02 27.20 ✓
223 17277 19.99 0.56 1.03 28.80 ✓
230 17278 20.00 0.53 1.03 30.40 ✓
236 17279 20.00 0.49 1.02 32.00 ✓
240 17280 19.99 0.46 1.03 33.60 ✓
246 17281 19.01 0.50 2.02 35.20 ✓
250 17282 20.99 0.53 1.03 36.80 ✓
258 17283 19.00 0.56 2.03 38.40 ✓
262 17284 20.99 0.59 1.04 40.00 ✓
268 17285 20.06 0.55 0.98 41.60 ✓
274 17286 20.00 0.52 0.98 43.20 ✓
278 17287 19.00 0.55 1.98 44.80 ✓
284 17288 20.99 0.58 0.99 46.40 ✓
288 17289 19.00 0.60 1.99 48.00 ✓
292 17290 22.00 0.69 -0.01 49.60 ✓
298 17291 17.00 0.83 2.99 51.20 ✓
316 17292 22.00 0.91 0.99 52.80 ✓
2 streams found.
Help
Play Streams
Close
Save


10.82.208.147:24640 ↔
172.18.110.203:8226
Forward
SSRC 0x236c6654
Max Delta 24.00 ms @ 3273
Max Jitter 1.37 ms
Mean Jitter 0.70 ms
Max Skew 4.02 ms
RTP Packets 732
Expected 732
Lost 0 (0.00 %)
Seq Errs 0
Start at 5.131005 s @ 103
Duration 14.62 s
Clock Drift -70 ms
Freq Drift 7961 Hz (-0.48 %)
Reverse
SSRC 0x252eb528
Max Delta 22.99 ms @ 2639
Max Jitter 0.37 ms
Mean Jitter 0.02 ms
Max Skew -2.98 ms
RTP Packets 740
Expected 740
Lost 0 (0.00 %)
Seq Errs 0
Start at 4.972001 s @ 76
Duration 14.78 s
Clock Drift -67 ms
Freq Drift 7964 Hz (-0.45 %)
Forward to reverse
start diff -0.159004 s @ -27
2 streams found.
Help
Play Streams
Forward
Reverse
Graph
Value (ms)
Arrival Time
Forward Jitter
Forward Difference
Forward Delta
Reverse Jitter
Reverse Difference
Reverse Delta
Close
Save


Wireshark File Edit View Go Capture Analyze Statistics 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
RTP Streams
Apply a display filter ... <⌘/>
No. Time Source Destination
746 7.331983 172.18.110.203 10.82.208.147
747 7.340986 14.50.201.48 172.18.110.203
748 7.340986 172.18.110.203 10.82.208.147
749 7.348981 10.82.208.147 172.18.110.203
750 7.348981 172.18.110.203 14.50.201.48
751 7.351987 14.50.201.48 172.18.110.203
752 7.351987 172.18.110.203 10.82.208.147
753 7.369991 10.82.208.147 172.18.110.203
754 7.369991 172.18.110.203 14.50.201.48
755 7.371990 14.50.201.48 172.18.110.203
756 7.371990 172.18.110.203 10.82.208.147
757 7.373989 14.50.201.48 172.18.110.203
758 7.373989 172.18.110.203 10.82.208.147
759 7.389979 10.82.208.147 172.18.110.203 RTP PT=ITU-T G.711 PCMU, SSRC=0x236C6654, Seq=17373, Time=2842540663
760 7.389979 172.18.110.203 14.50.201.48 RTP PT=ITU-T G.711 PCMU, SSRC=0x236C6654, Seq=17373, Time=2842540663
761 7.390986 0.0.0.0 255.255.255.255 DHCP DHCP Discover - Transaction ID 0x3869f073


10.82.208.147:24640 ↔
172.18.110.203:8226
Forward
SSRC 0x236c6654
Max Delta 24.00 ms @ 3273
Max Jitter 1.37 ms
Mean Jitter 0.70 ms
Max Skew 4.02 ms
RTP Packets 732
Expected 732
Lost 0 (0.00 %)
Seq Errs 0
Start at 5.131005 s @ 103
Duration 14.62 s
Clock Drift -70 ms
Freq Drift 7961 Hz (-0.48 %)
Reverse
SSRC 0x252eb528
Max Delta 22.99 ms @ 2639
Max Jitter 0.37 ms
Mean Jitter 0.02 ms
Max Skew -2.98 ms
RTP Packets 740
Expected 740
Lost 0 (0.00 %)
Seq Errs 0
Start at 4.972001 s @ 76
Duration 14.78 s
Clock Drift -67 ms
Freq Drift 7964 Hz (-0.45 %)
Forward to reverse
start diff -0.159004 s @ -27
2 streams found.
Help
Play Streams
Forward
Reverse
Graph
Value (ms)
Arrival Time
Forward Jitter
Forward Difference
Forward Delta
Reverse Jitter
Reverse Difference
Reverse Delta
Close
Save

Chapter 18: Troubleshooting Bandwidth and Delay Issues



Display

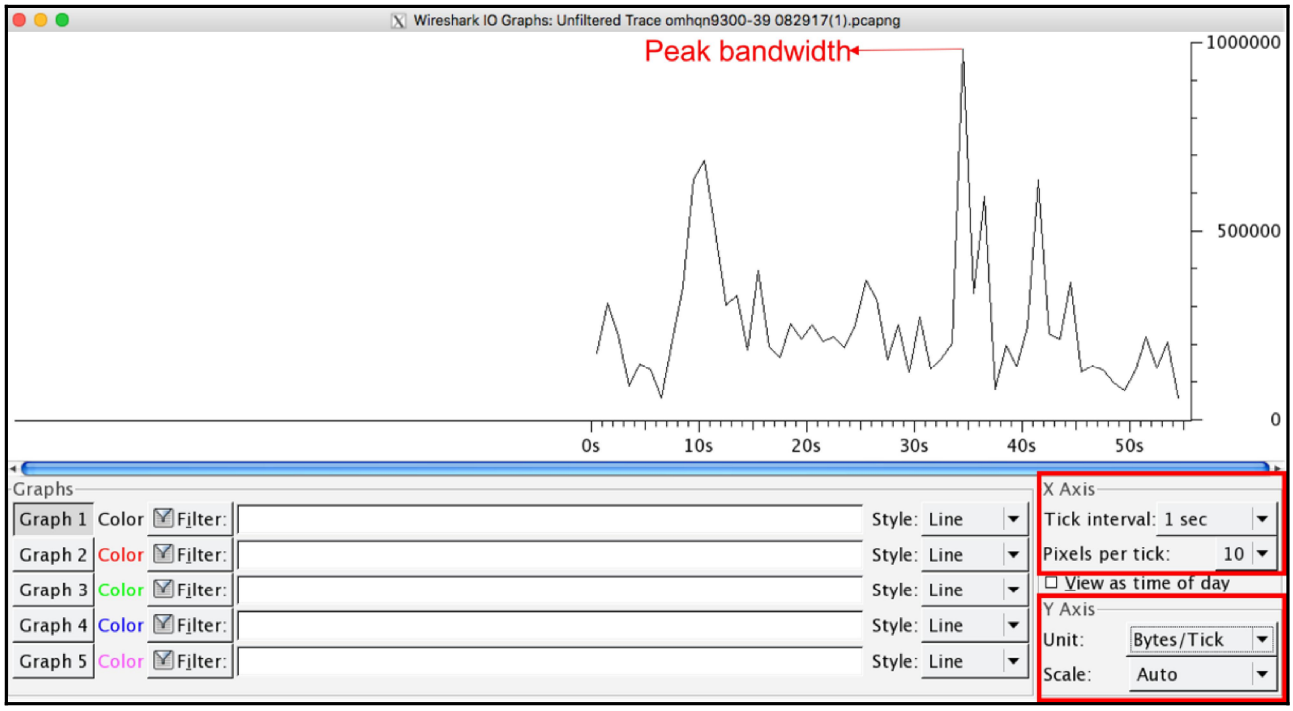
Display filter: none
Ignored packets: 0

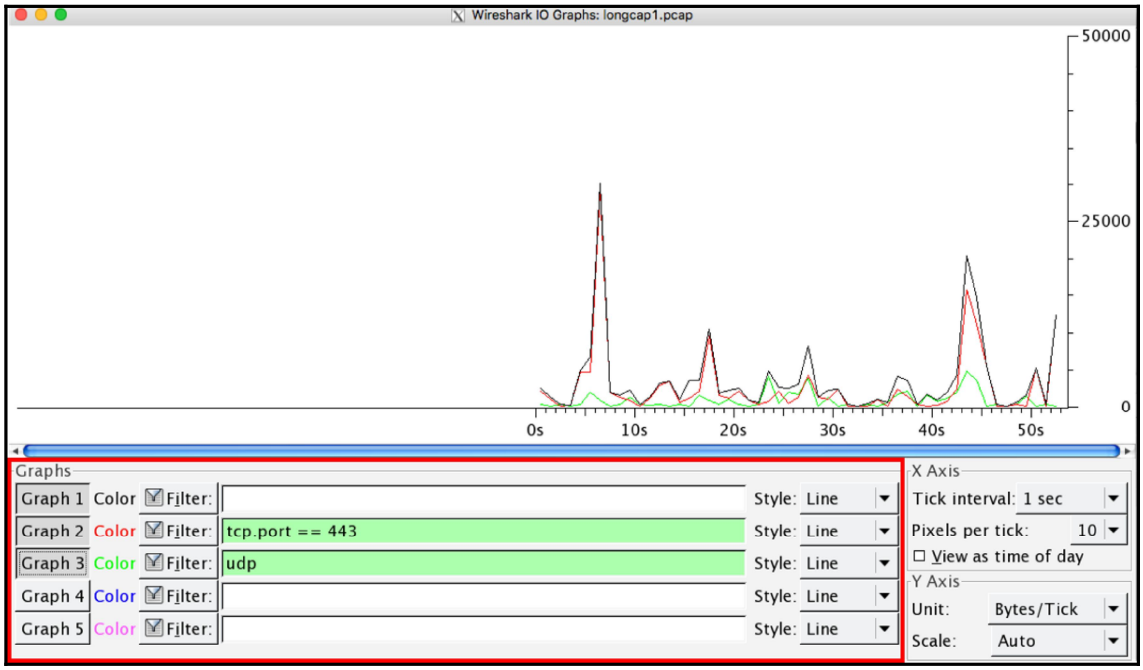
Traffic	Captured	Displayed	Marked
Packets	175391	175391	0
Between first and last packet	55.323 sec		
Avg. packets/sec	3170.284		
Avg. packet size	1289.011 bytes		
Bytes	226081014		
Avg. bytes/sec	4086531.946		
Avg. MBit/sec	32.692		

Display

Display filter:	tcp.stream eq 133
Ignored packets:	0

Traffic	Captured	Displayed	Marked
Packets	175391	110782	0
Between first and last packet	55.323 sec	10.537 sec	
Avg. packets/sec	3170.284	10513.801	
Avg. packet size	1289.011 bytes	1327.361 bytes	
Bytes	226081014	147047699	
Avg. bytes/sec	4086531.946	13955608.982	
Avg. MBit/sec	32.692	111.645	

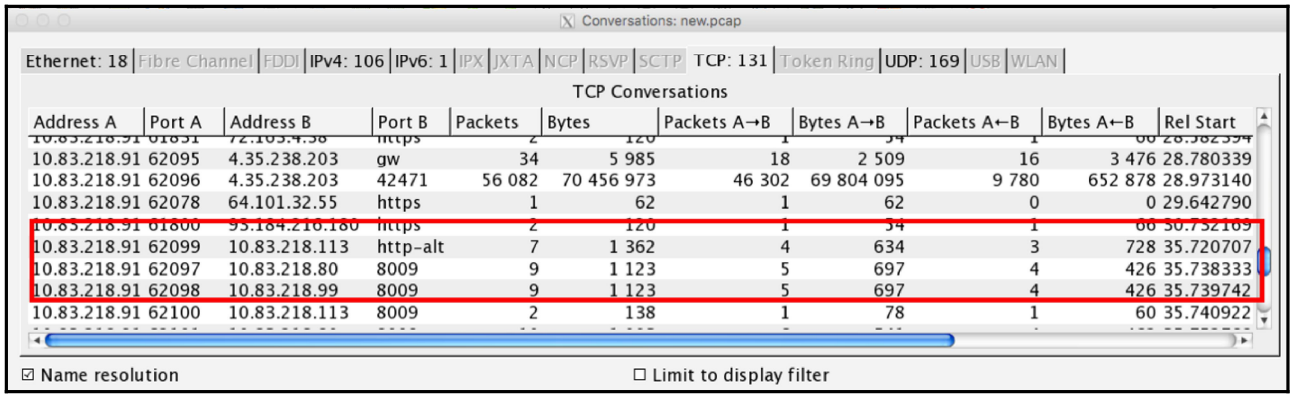


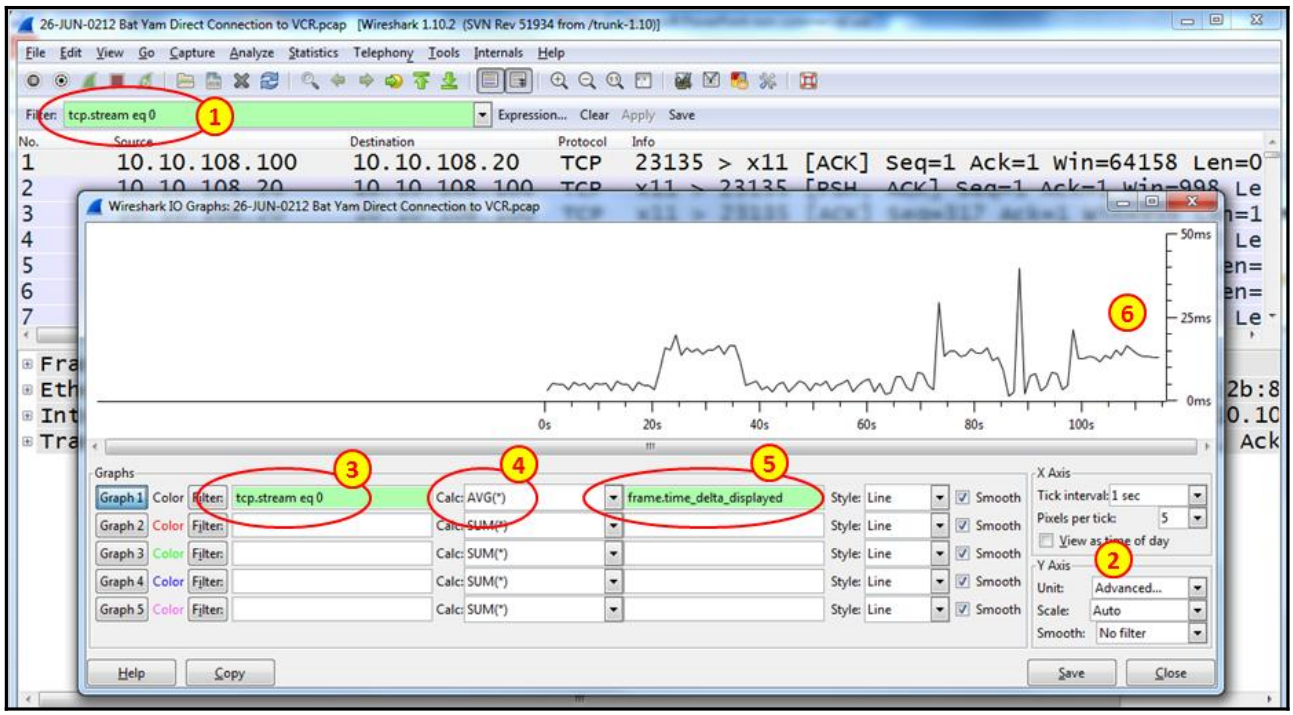


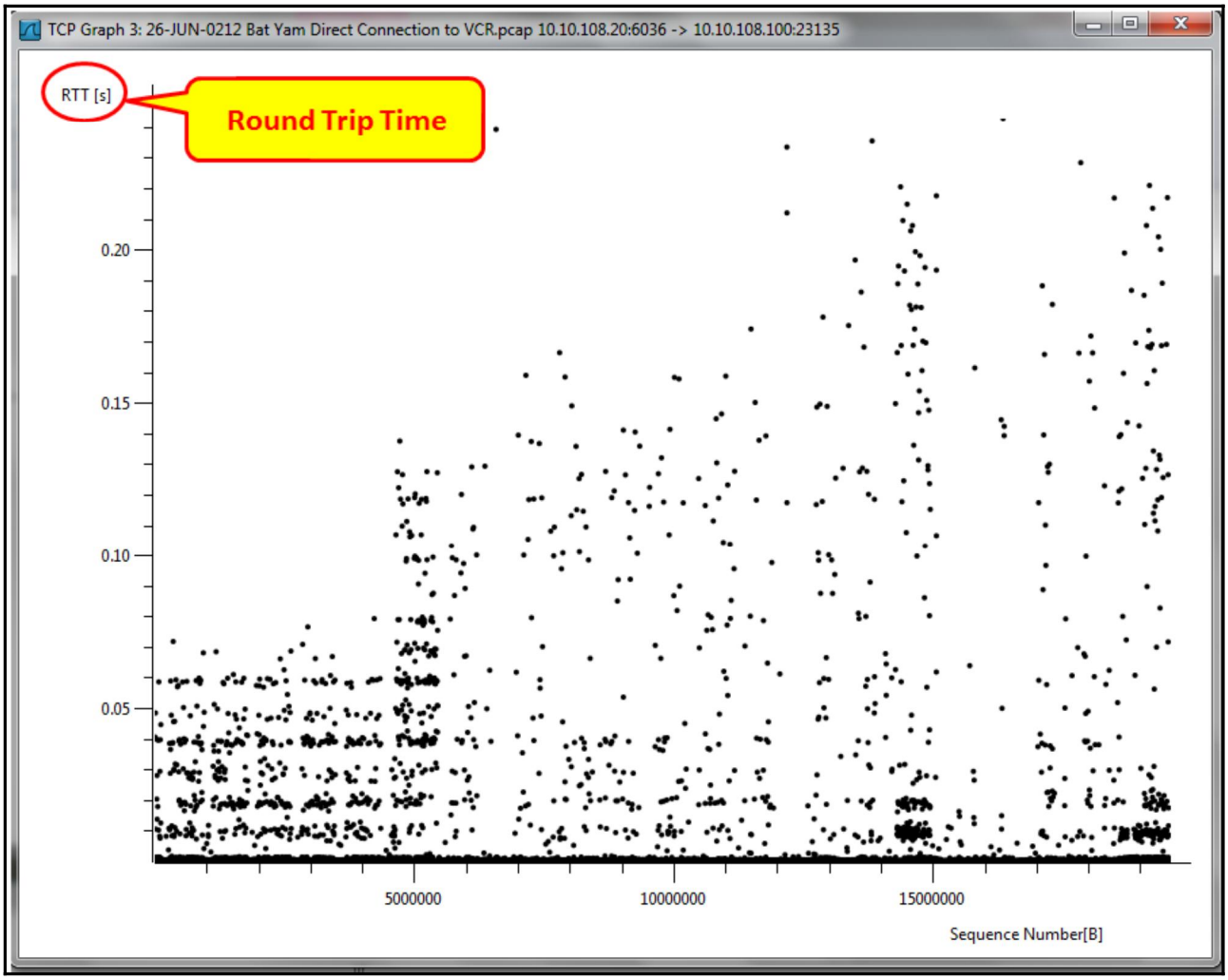
Ethernet: 3 | Fibre Channel | FDDI | IPv4: 12262 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 12260 | Token Ring | UDP | USB | WLAN

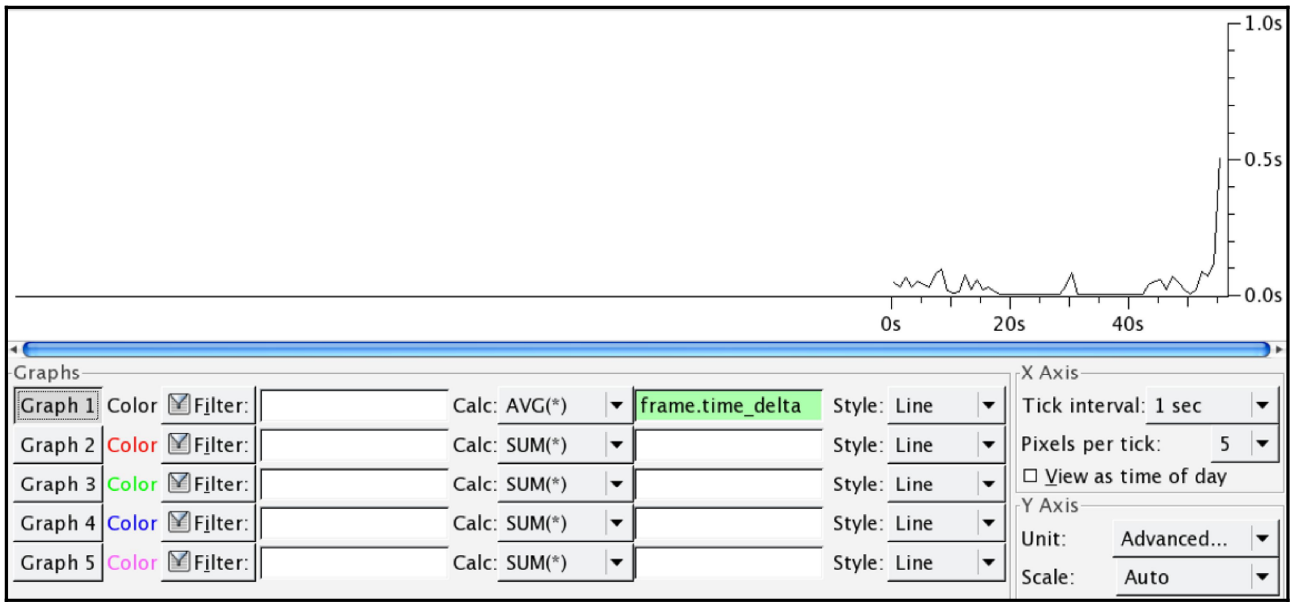
IPv4 Endpoints

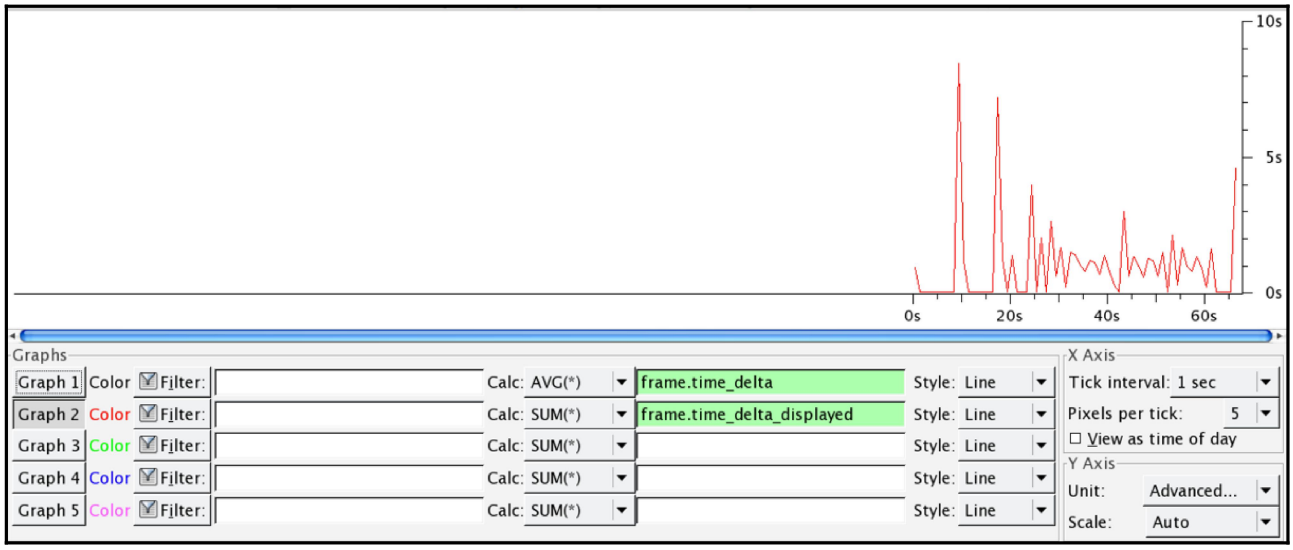
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
10.1.200.10	1 426	1 140 800	0	0	1 426	1 140 8(
10.1.200.9	1 408	1 126 400	0	0	1 408	1 126 4(
10.1.200.5	1 393	1 114 400	0	0	1 393	1 114 4(
10.1.200.6	1 362	1 089 600	0	0	1 362	1 089 6(
10.1.200.4	1 359	1 087 200	0	0	1 359	1 087 2(
10.1.200.3	1 355	1 084 000	0	0	1 355	1 084 0(
10.1.200.2	1 332	1 065 600	0	0	1 332	1 065 6(
10.1.200.7	1 311	1 048 800	0	0	1 311	1 048 8(
10.1.200.8	1 308	1 046 400	0	0	1 308	1 046 4(
10.7.209.185	2	1 600	2	1 600	0	
10.53.45.143	2	1 600	2	1 600	0	
10.8.63.166	2	1 600	2	1 600	0	
10.85.141.203	1	800	1	800	0	
10.160.26.239	1	800	1	800	0	

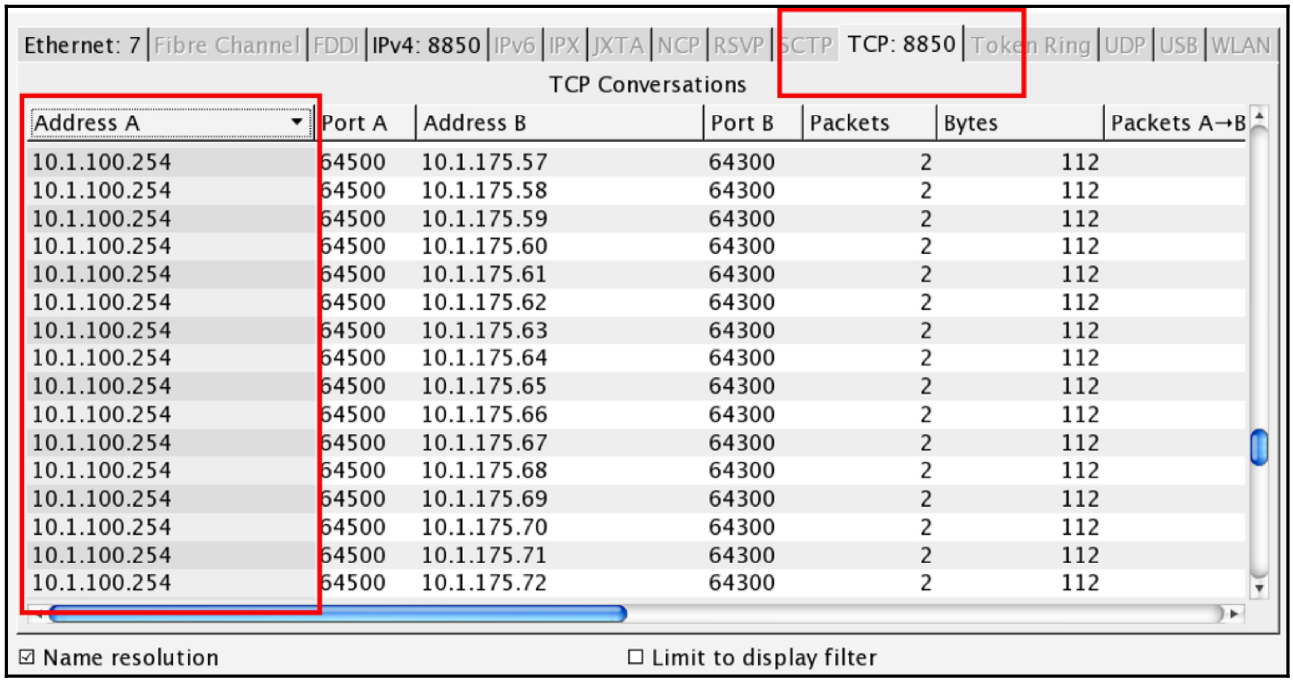

Conversations: new.pcap
Ethernet: 18 | Fibre Channel | FDDI | IPv4: 106 | IPv6: 1 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 131 | Token Ring | UDP: 169 | USB | WLAN
TCP Conversations
Address A | Port A | Address B | Port B | Packets | Bytes | Packets A→B | Bytes A→B | Packets A←B | Bytes A←B | Rel Start
10.83.218.91 62095 | 4.35.238.203 | gw | 34 | 5 985 | 18 | 2 509 | 16 | 3 476 | 28.780339
10.83.218.91 62096 | 4.35.238.203 | 42471 | 56 082 | 70 456 973 | 46 302 | 69 804 095 | 9 780 | 652 878 | 28.973140
10.83.218.91 62078 | 64.101.32.55 | https | 1 | 62 | 1 | 62 | 0 | 0 | 29.642790
10.83.218.91 61800 | 93.184.216.180 | https | 2 | 120 | 1 | 54 | 1 | 66 | 30.732169
10.83.218.91 62099 | 10.83.218.113 | http-alt | 7 | 1 362 | 4 | 634 | 3 | 728 | 35.720707
10.83.218.91 62097 | 10.83.218.80 | 8009 | 9 | 1 123 | 5 | 697 | 4 | 426 | 35.738333
10.83.218.91 62098 | 10.83.218.99 | 8009 | 9 | 1 123 | 5 | 697 | 4 | 426 | 35.739742
10.83.218.91 62100 | 10.83.218.113 | 8009 | 2 | 138 | 1 | 78 | 1 | 60 | 35.740922
Name resolution
Limit to display filter


26-JUN-0212 Bat Yam Direct Connection to VCR.pcap [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp.stream eq 0
Expression... Clear Apply Save
No. Source Destination Protocol Info
1 10.10.108.100 10.10.108.20 TCP 23135 > x11 [ACK] Seq=1 Ack=1 Win=64158 Len=0
Wireshark IO Graphs: 26-JUN-0212 Bat Yam Direct Connection to VCR.pcap
50ms
25ms
0ms
0s 20s 40s 60s 80s 100s
Graphs
Graph 1 Color Filter: tcp.stream eq 0 Calc: AVG(*) frame.time_delta_displayed Style: Line Smooth
Graph 2 Color Filter: Calc: SUM(*) Style: Line Smooth
Graph 3 Color Filter: Calc: SUM(*) Style: Line Smooth
Graph 4 Color Filter: Calc: SUM(*) Style: Line Smooth
Graph 5 Color Filter: Calc: SUM(*) Style: Line Smooth
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Advanced...
Scale: Auto
Smooth: No filter
Help Copy Save Close
1 2 3 4 5 6

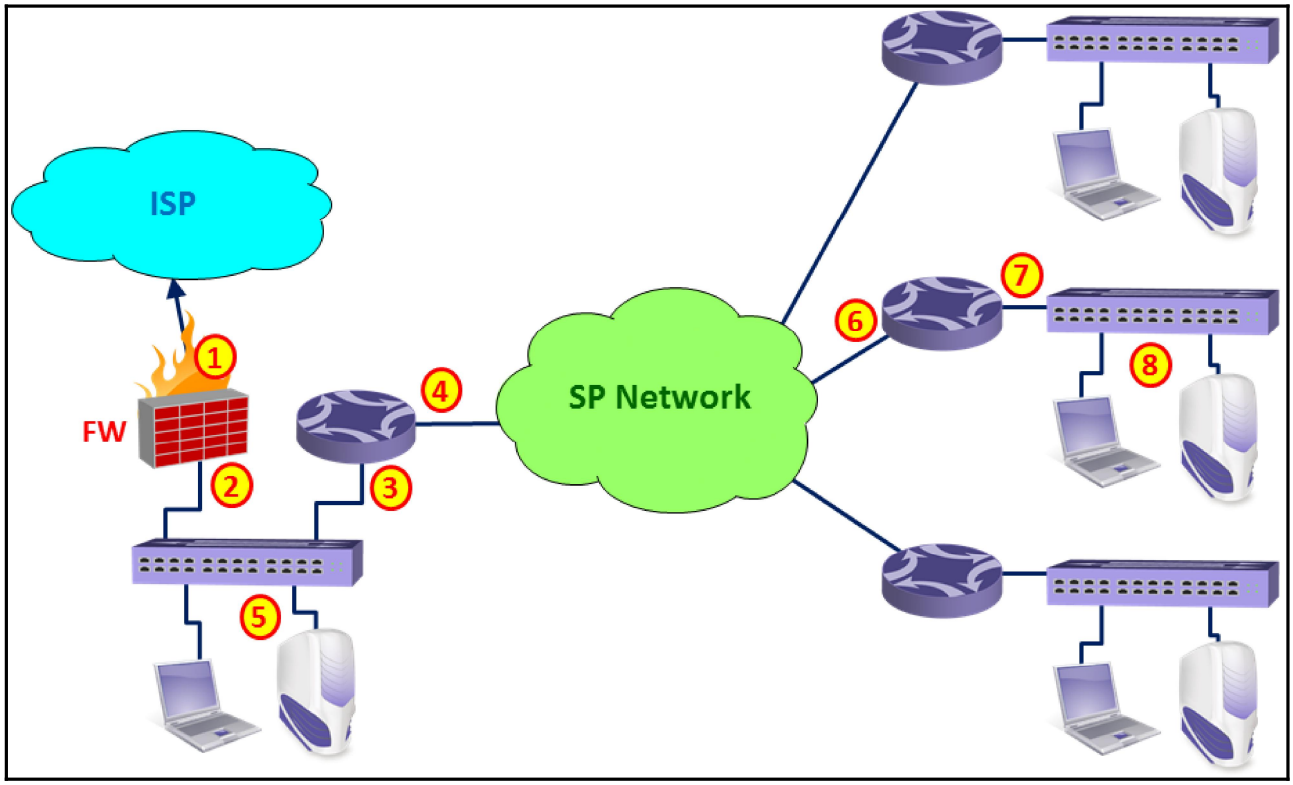

TCP Graph 3: 26-JUN-0212 Bat Yam Direct Connection to VCR.pcap 10.10.108.20:6036 -> 10.10.108.100:23135
RTT [s]
Round Trip Time
0.20
0.15
0.10
0.05
5000000
10000000
15000000
Sequence Number[B]

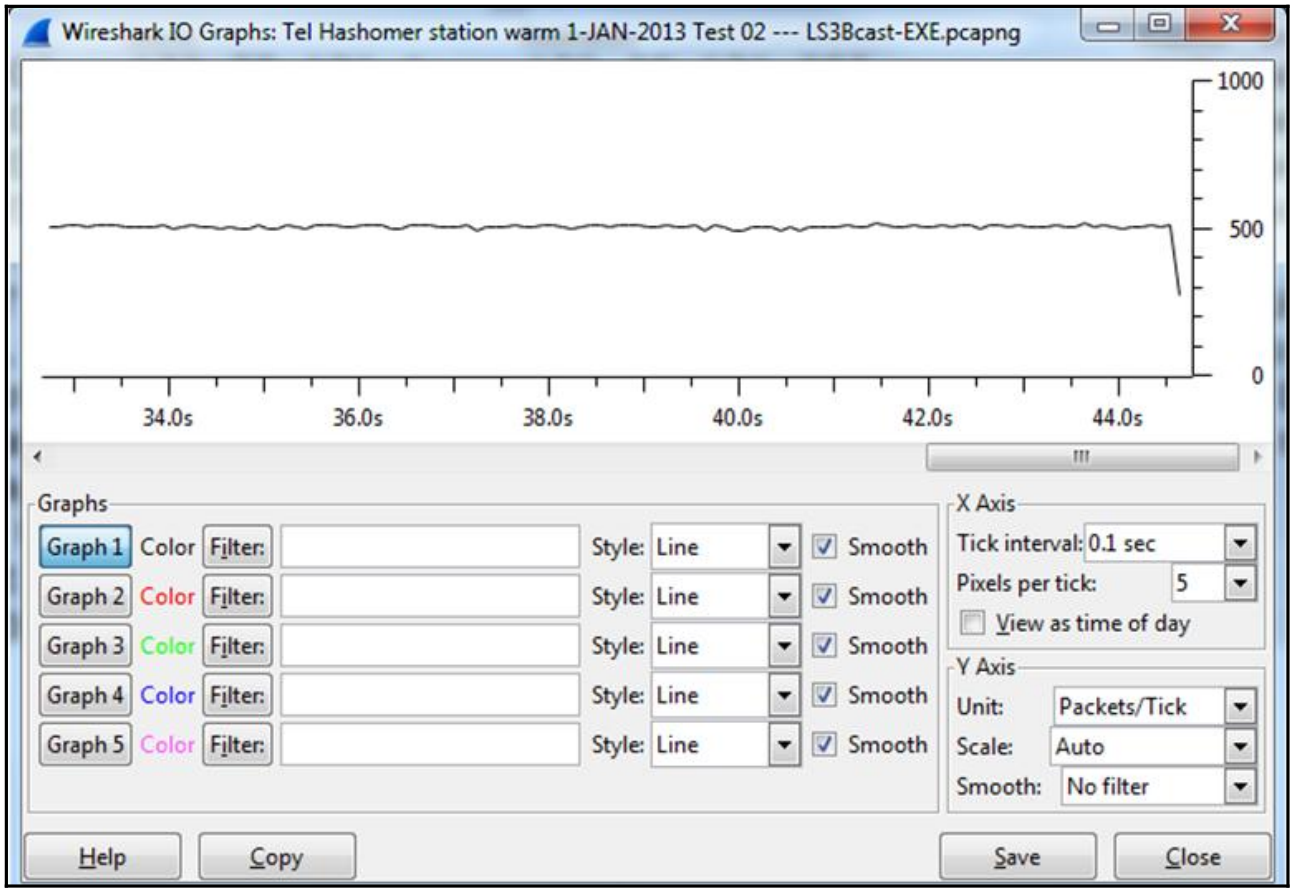

1.0s
0.5s
0.0s
0s
20s
40s
Graphs
Graph 1 Color Filter: Calc: AVG(*) frame.time_delta Style: Line
Graph 2 Color Filter: Calc: SUM(*) Style: Line
Graph 3 Color Filter: Calc: SUM(*) Style: Line
Graph 4 Color Filter: Calc: SUM(*) Style: Line
Graph 5 Color Filter: Calc: SUM(*) Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Advanced...
Scale: Auto

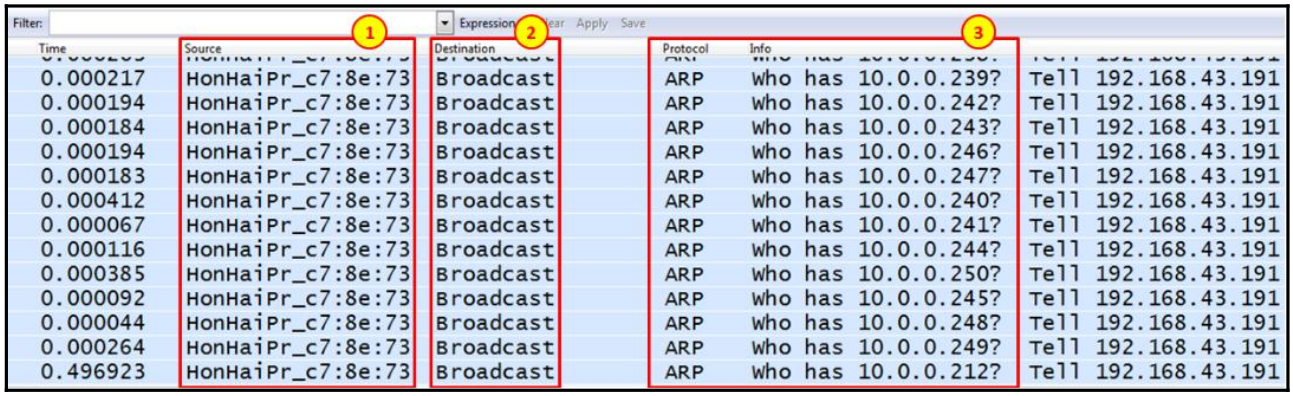

10s
5s
0s
0s
20s
40s
60s
Graphs
Graph 1 Color Filter: Calc: AVG(*) frame.time_delta Style: Line
Graph 2 Color Filter: Calc: SUM(*) frame.time_delta_displayed Style: Line
Graph 3 Color Filter: Calc: SUM(*) Style: Line
Graph 4 Color Filter: Calc: SUM(*) Style: Line
Graph 5 Color Filter: Calc: SUM(*) Style: Line
X Axis
Tick interval: 1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Advanced...
Scale: Auto

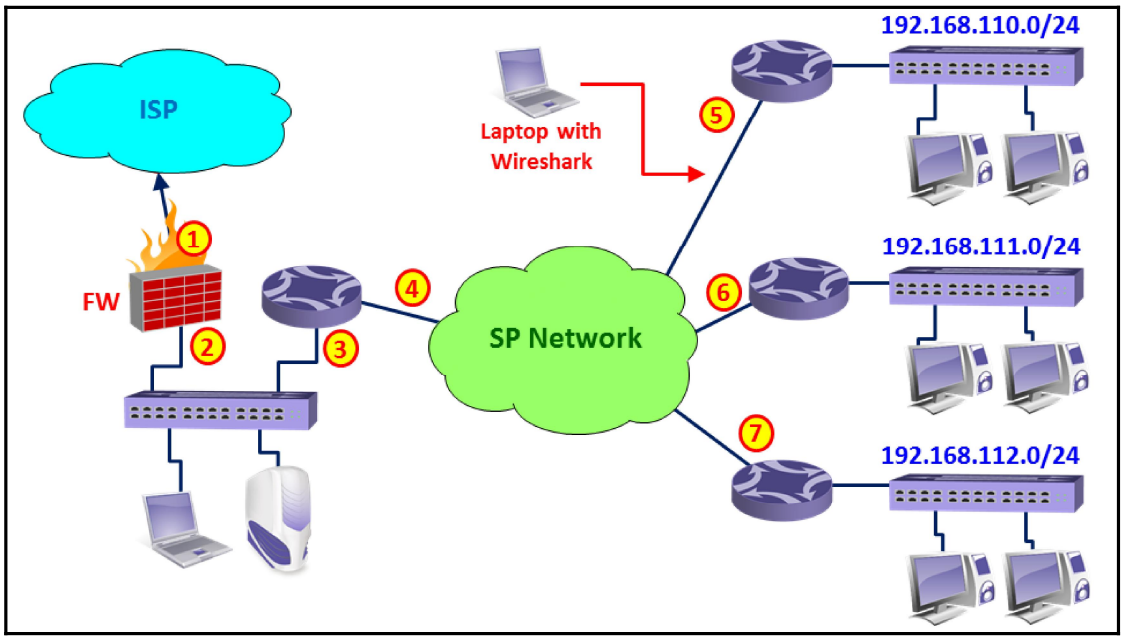

Ethernet: 7 | Fibre Channel | FDDI | IPv4: 8850 | IPv6 | IPX | JXTA | NCP | RSVP | SCTP | TCP: 8850 | Token Ring | UDP | USB | WLAN
TCP Conversations
Address A | Port A | Address B | Port B | Packets | Bytes | Packets A→B
10.1.100.254 64500 10.1.175.57 64300 2 112
10.1.100.254 64500 10.1.175.58 64300 2 112
10.1.100.254 64500 10.1.175.59 64300 2 112
10.1.100.254 64500 10.1.175.60 64300 2 112
10.1.100.254 64500 10.1.175.61 64300 2 112
10.1.100.254 64500 10.1.175.62 64300 2 112
10.1.100.254 64500 10.1.175.63 64300 2 112
10.1.100.254 64500 10.1.175.64 64300 2 112
10.1.100.254 64500 10.1.175.65 64300 2 112
10.1.100.254 64500 10.1.175.66 64300 2 112
10.1.100.254 64500 10.1.175.67 64300 2 112
10.1.100.254 64500 10.1.175.68 64300 2 112
10.1.100.254 64500 10.1.175.69 64300 2 112
10.1.100.254 64500 10.1.175.70 64300 2 112
10.1.100.254 64500 10.1.175.71 64300 2 112
10.1.100.254 64500 10.1.175.72 64300 2 112
Name resolution
Limit to display filter

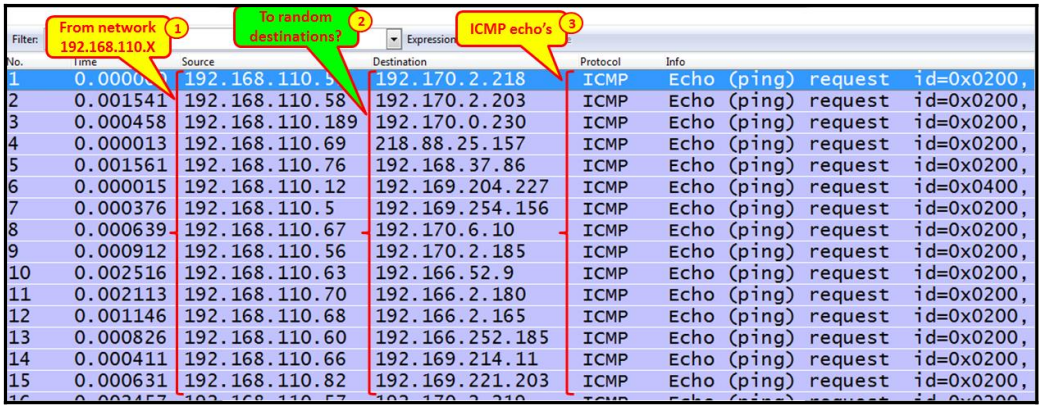
Chapter 19: Security and Network Forensics

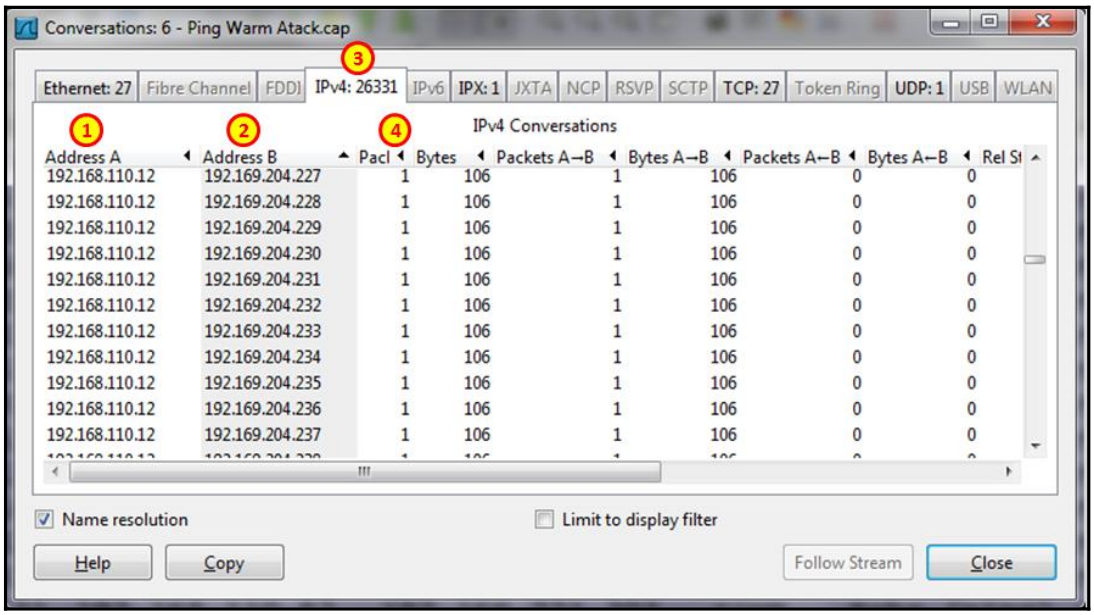


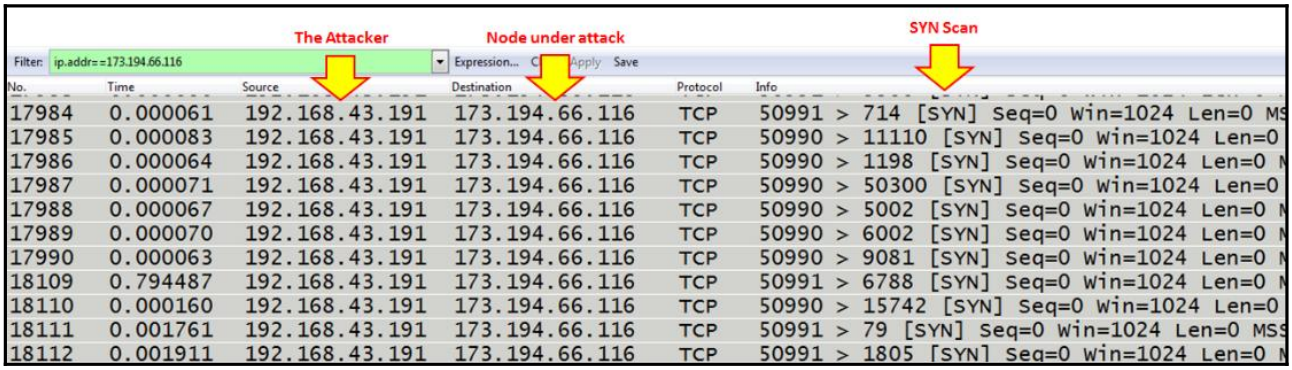

Wireshark IO Graphs: Tel Hashomer station warm 1-JAN-2013 Test 02 --- LS3Bcast-EXE.pcapng
1000
500
0
34.0s
36.0s
38.0s
40.0s
42.0s
44.0s
Graphs
Graph 1 Color Filter: Style: Line Smooth
Graph 2 Color Filter: Style: Line Smooth
Graph 3 Color Filter: Style: Line Smooth
Graph 4 Color Filter: Style: Line Smooth
Graph 5 Color Filter: Style: Line Smooth
X Axis
Tick interval: 0.1 sec
Pixels per tick: 5
View as time of day
Y Axis
Unit: Packets/Tick
Scale: Auto
Smooth: No filter
Help
Copy
Save
Close

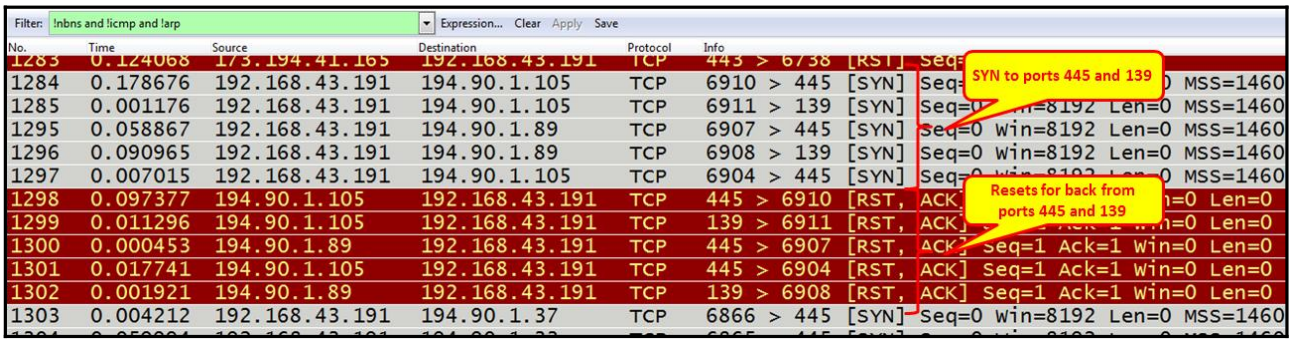

Filter:
Expression
Clear
Apply
Save
1
2
3
Time Source Destination Protocol Info
0.000217 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.239? Tell 192.168.43.191
0.000194 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.242? Tell 192.168.43.191
0.000184 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.243? Tell 192.168.43.191
0.000194 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.246? Tell 192.168.43.191
0.000183 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.247? Tell 192.168.43.191
0.000412 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.240? Tell 192.168.43.191
0.000067 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.241? Tell 192.168.43.191
0.000116 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.244? Tell 192.168.43.191
0.000385 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.250? Tell 192.168.43.191
0.000092 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.245? Tell 192.168.43.191
0.000044 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.248? Tell 192.168.43.191
0.000264 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.249? Tell 192.168.43.191
0.496923 HonHaiPr_c7:8e:73 Broadcast ARP Who has 10.0.0.212? Tell 192.168.43.191

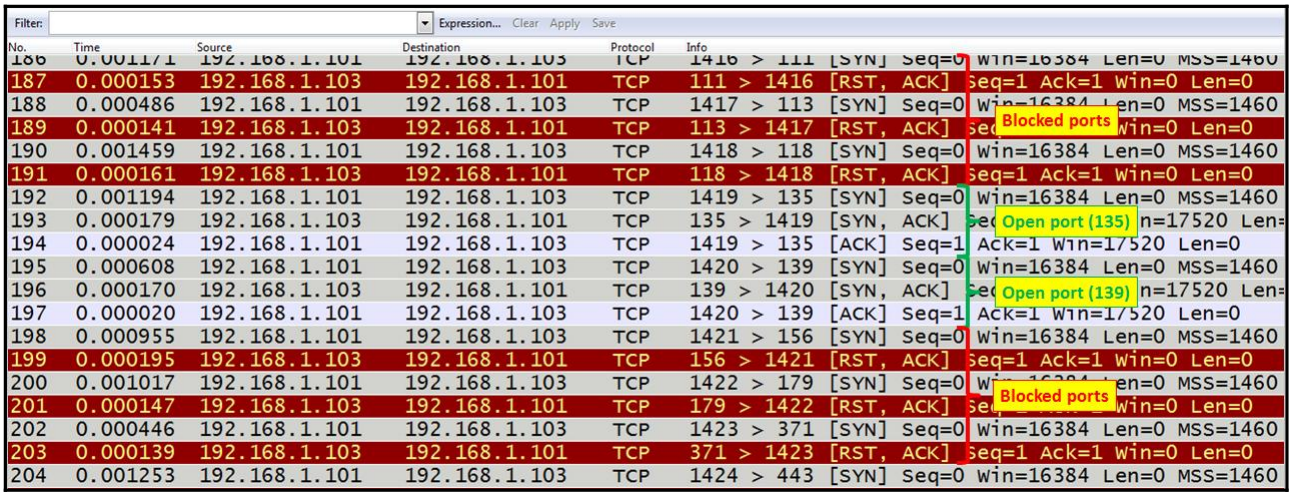

ISP
Laptop with Wireshark
192.168.110.0/24
192.168.111.0/24
192.168.112.0/24
FW
SP Network
1
2
3
4
5
6
7

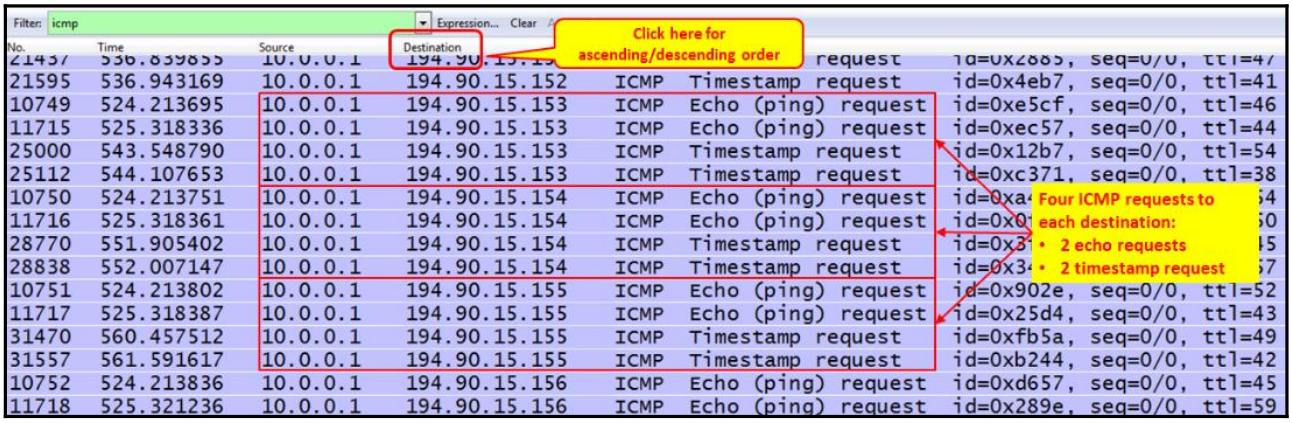

From network 192.168.110.X
1
To random destinations?
2
ICMP echo's
3
Filter:
Expression
No. Time Source Destination Protocol Info
1 0.0000 192.168.110.5 192.170.2.218 ICMP Echo (ping) request id=0x0200,
2 0.001541 192.168.110.58 192.170.2.203 ICMP Echo (ping) request id=0x0200,
3 0.000458 192.168.110.189 192.170.0.230 ICMP Echo (ping) request id=0x0200,
4 0.000013 192.168.110.69 218.88.25.157 ICMP Echo (ping) request id=0x0200,
5 0.001561 192.168.110.76 192.168.37.86 ICMP Echo (ping) request id=0x0200,
6 0.000015 192.168.110.12 192.169.204.227 ICMP Echo (ping) request id=0x0400,
7 0.000376 192.168.110.5 192.169.254.156 ICMP Echo (ping) request id=0x0200,
8 0.000639 192.168.110.67 192.170.6.10 ICMP Echo (ping) request id=0x0200,
9 0.000912 192.168.110.56 192.170.2.185 ICMP Echo (ping) request id=0x0200,
10 0.002516 192.168.110.63 192.166.52.9 ICMP Echo (ping) request id=0x0200,
11 0.002113 192.168.110.70 192.166.2.180 ICMP Echo (ping) request id=0x0200,
12 0.001146 192.168.110.68 192.166.2.165 ICMP Echo (ping) request id=0x0200,
13 0.000826 192.168.110.60 192.166.252.185 ICMP Echo (ping) request id=0x0200,
14 0.000411 192.168.110.66 192.169.214.11 ICMP Echo (ping) request id=0x0200,
15 0.000631 192.168.110.82 192.169.221.203 ICMP Echo (ping) request id=0x0200,

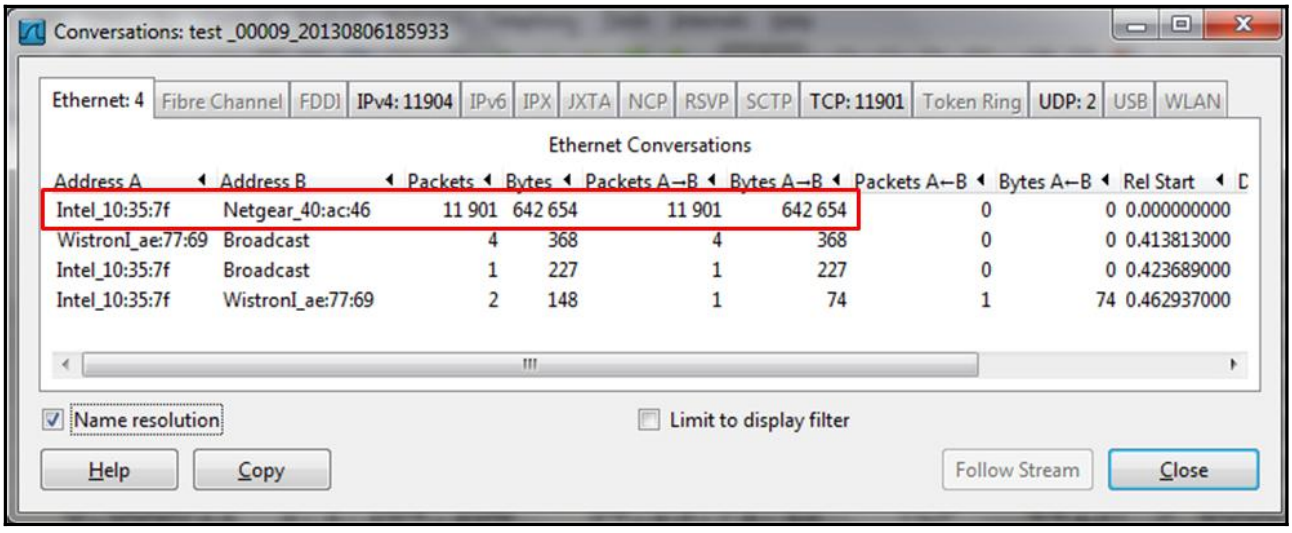

Conversations: 6 - Ping Warm Atack.cap
Ethernet: 27
Fibre Channel
FDDI
IPv4: 26331
IPv6
IPX: 1
JXTA
NCP
RSVP
SCTP
TCP: 27
Token Ring
UDP: 1
USB
WLAN
IPv4 Conversations
Address A
Address B
Pacl
Bytes
Packets A→B
Bytes A→B
Packets A←B
Bytes A←B
Rel St
192.168.110.12 192.169.204.227 1 106 1 106 0 0
192.168.110.12 192.169.204.228 1 106 1 106 0 0
192.168.110.12 192.169.204.229 1 106 1 106 0 0
192.168.110.12 192.169.204.230 1 106 1 106 0 0
192.168.110.12 192.169.204.231 1 106 1 106 0 0
192.168.110.12 192.169.204.232 1 106 1 106 0 0
192.168.110.12 192.169.204.233 1 106 1 106 0 0
192.168.110.12 192.169.204.234 1 106 1 106 0 0
192.168.110.12 192.169.204.235 1 106 1 106 0 0
192.168.110.12 192.169.204.236 1 106 1 106 0 0
192.168.110.12 192.169.204.237 1 106 1 106 0 0
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

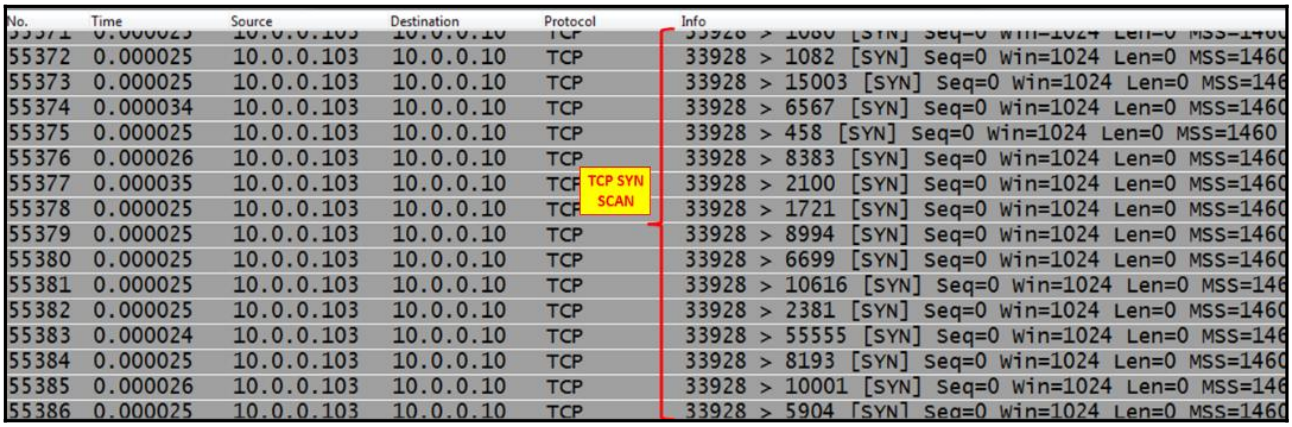

The Attacker
Node under attack
SYN Scan
Filter: ip.addr==173.194.66.116
Expression...
Apply
Save
No. Time Source Destination Protocol Info
17984 0.000061 192.168.43.191 173.194.66.116 TCP 50991 > 714 [SYN] Seq=0 Win=1024 Len=0
17985 0.000083 192.168.43.191 173.194.66.116 TCP 50990 > 11110 [SYN] Seq=0 Win=1024 Len=0
17986 0.000064 192.168.43.191 173.194.66.116 TCP 50990 > 1198 [SYN] Seq=0 Win=1024 Len=0
17987 0.000071 192.168.43.191 173.194.66.116 TCP 50990 > 50300 [SYN] Seq=0 Win=1024 Len=0
17988 0.000067 192.168.43.191 173.194.66.116 TCP 50990 > 5002 [SYN] Seq=0 Win=1024 Len=0
17989 0.000070 192.168.43.191 173.194.66.116 TCP 50990 > 6002 [SYN] Seq=0 Win=1024 Len=0
17990 0.000063 192.168.43.191 173.194.66.116 TCP 50990 > 9081 [SYN] Seq=0 Win=1024 Len=0
18109 0.794487 192.168.43.191 173.194.66.116 TCP 50991 > 6788 [SYN] Seq=0 Win=1024 Len=0
18110 0.000160 192.168.43.191 173.194.66.116 TCP 50990 > 15742 [SYN] Seq=0 Win=1024 Len=0
18111 0.001761 192.168.43.191 173.194.66.116 TCP 50991 > 79 [SYN] Seq=0 Win=1024 Len=0 MSS
18112 0.001911 192.168.43.191 173.194.66.116 TCP 50991 > 1805 [SYN] Seq=0 Win=1024 Len=0

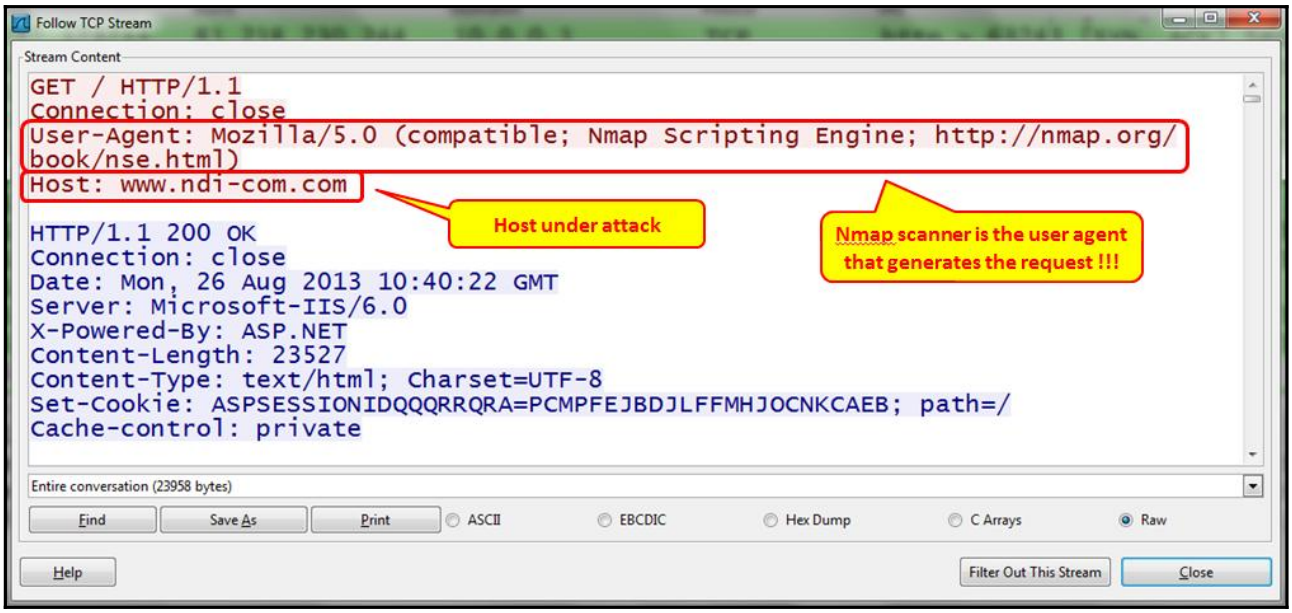

Filter: !nbns and !icmp and !arp
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
1284 0.178676 192.168.43.191 194.90.1.105 TCP 6910 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1285 0.001176 192.168.43.191 194.90.1.105 TCP 6911 > 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1295 0.058867 192.168.43.191 194.90.1.89 TCP 6907 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1296 0.090965 192.168.43.191 194.90.1.89 TCP 6908 > 139 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1297 0.007015 192.168.43.191 194.90.1.105 TCP 6904 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
1298 0.097377 194.90.1.105 192.168.43.191 TCP 445 > 6910 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1299 0.011296 194.90.1.105 192.168.43.191 TCP 139 > 6911 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1300 0.000453 194.90.1.89 192.168.43.191 TCP 445 > 6907 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1301 0.017741 194.90.1.105 192.168.43.191 TCP 445 > 6904 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1302 0.001921 194.90.1.89 192.168.43.191 TCP 139 > 6908 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
1303 0.004212 192.168.43.191 194.90.1.37 TCP 6866 > 445 [SYN] Seq=0 Win=8192 Len=0 MSS=1460
SYN to ports 445 and 139
Resets for back from ports 445 and 139

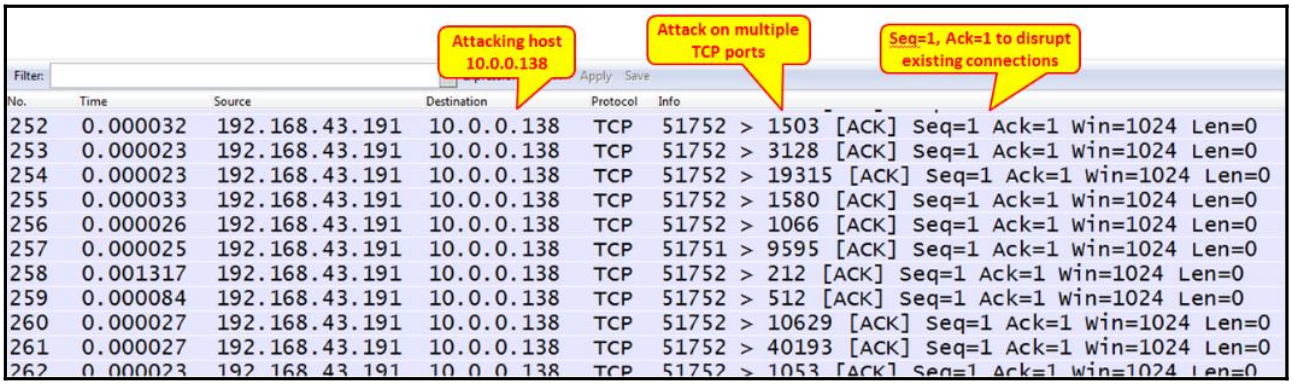

Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
187 0.000153 192.168.1.103 192.168.1.101 TCP 111 > 1416 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
188 0.000486 192.168.1.101 192.168.1.103 TCP 1417 > 113 [SYN] Seq=0
189 0.000141 192.168.1.103 192.168.1.101 TCP 113 > 1417 [RST, ACK]
Blocked ports
190 0.001459 192.168.1.101 192.168.1.103 TCP 1418 > 118 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
191 0.000161 192.168.1.103 192.168.1.101 TCP 118 > 1418 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192 0.001194 192.168.1.101 192.168.1.103 TCP 1419 > 135 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
193 0.000179 192.168.1.103 192.168.1.101 TCP 135 > 1419 [SYN, ACK]
Open port (135)
194 0.000024 192.168.1.101 192.168.1.103 TCP 1419 > 135 [ACK] Seq=1 Ack=1 Win=17520 Len=0
195 0.000608 192.168.1.101 192.168.1.103 TCP 1420 > 139 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
196 0.000170 192.168.1.103 192.168.1.101 TCP 139 > 1420 [SYN, ACK]
Open port (139)
197 0.000020 192.168.1.101 192.168.1.103 TCP 1420 > 139 [ACK] Seq=1 Ack=1 Win=17520 Len=0
198 0.000955 192.168.1.101 192.168.1.103 TCP 1421 > 156 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
199 0.000195 192.168.1.103 192.168.1.101 TCP 156 > 1421 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
200 0.001017 192.168.1.101 192.168.1.103 TCP 1422 > 179 [SYN] Seq=0
201 0.000147 192.168.1.103 192.168.1.101 TCP 179 > 1422 [RST, ACK]
Blocked ports
202 0.000446 192.168.1.101 192.168.1.103 TCP 1423 > 371 [SYN] Seq=0 Win=16384 Len=0 MSS=1460
203 0.000139 192.168.1.103 192.168.1.101 TCP 371 > 1423 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
204 0.001253 192.168.1.101 192.168.1.103 TCP 1424 > 443 [SYN] Seq=0 Win=16384 Len=0 MSS=1460

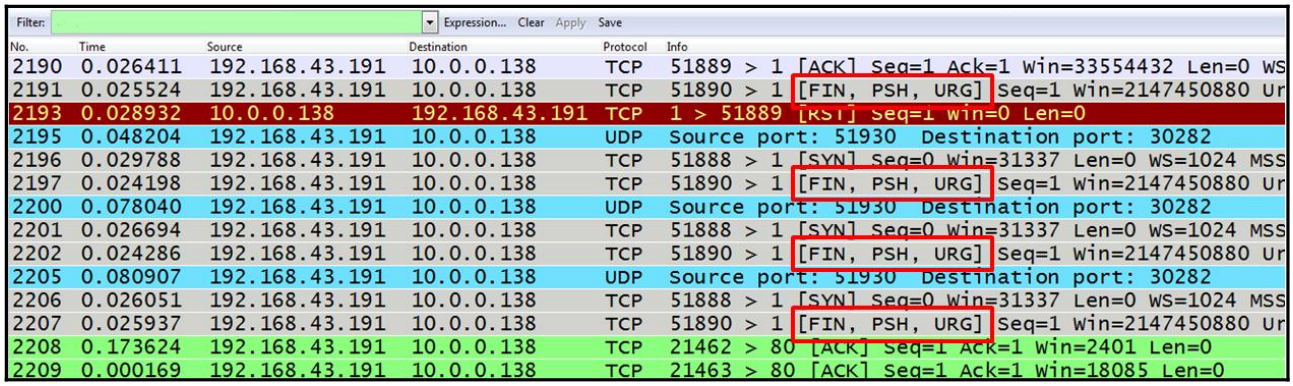

Filter: icmp
Expression... Clear
No. Time Source Destination
Click here for ascending/descending order
21595 536.943169 10.0.0.1 194.90.15.152 ICMP Timestamp request id=0x4eb7, seq=0/0, ttl=41
10749 524.213695 10.0.0.1 194.90.15.153 ICMP Echo (ping) request id=0xe5cf, seq=0/0, ttl=46
11715 525.318336 10.0.0.1 194.90.15.153 ICMP Echo (ping) request id=0xec57, seq=0/0, ttl=44
25000 543.548790 10.0.0.1 194.90.15.153 ICMP Timestamp request id=0x12b7, seq=0/0, ttl=54
25112 544.107653 10.0.0.1 194.90.15.153 ICMP Timestamp request id=0xc371, seq=0/0, ttl=38
10750 524.213751 10.0.0.1 194.90.15.154 ICMP Echo (ping) request
11716 525.318361 10.0.0.1 194.90.15.154 ICMP Echo (ping) request
28770 551.905402 10.0.0.1 194.90.15.154 ICMP Timestamp request
28838 552.007147 10.0.0.1 194.90.15.154 ICMP Timestamp request
Four ICMP requests to each destination:
• 2 echo requests
• 2 timestamp request
10751 524.213802 10.0.0.1 194.90.15.155 ICMP Echo (ping) request id=0x902e, seq=0/0, ttl=52
11717 525.318387 10.0.0.1 194.90.15.155 ICMP Echo (ping) request id=0x25d4, seq=0/0, ttl=43
31470 560.457512 10.0.0.1 194.90.15.155 ICMP Timestamp request id=0xfb5a, seq=0/0, ttl=49
31557 561.591617 10.0.0.1 194.90.15.155 ICMP Timestamp request id=0xb244, seq=0/0, ttl=42
10752 524.213836 10.0.0.1 194.90.15.156 ICMP Echo (ping) request id=0xd657, seq=0/0, ttl=45
11718 525.321236 10.0.0.1 194.90.15.156 ICMP Echo (ping) request id=0x289e, seq=0/0, ttl=59

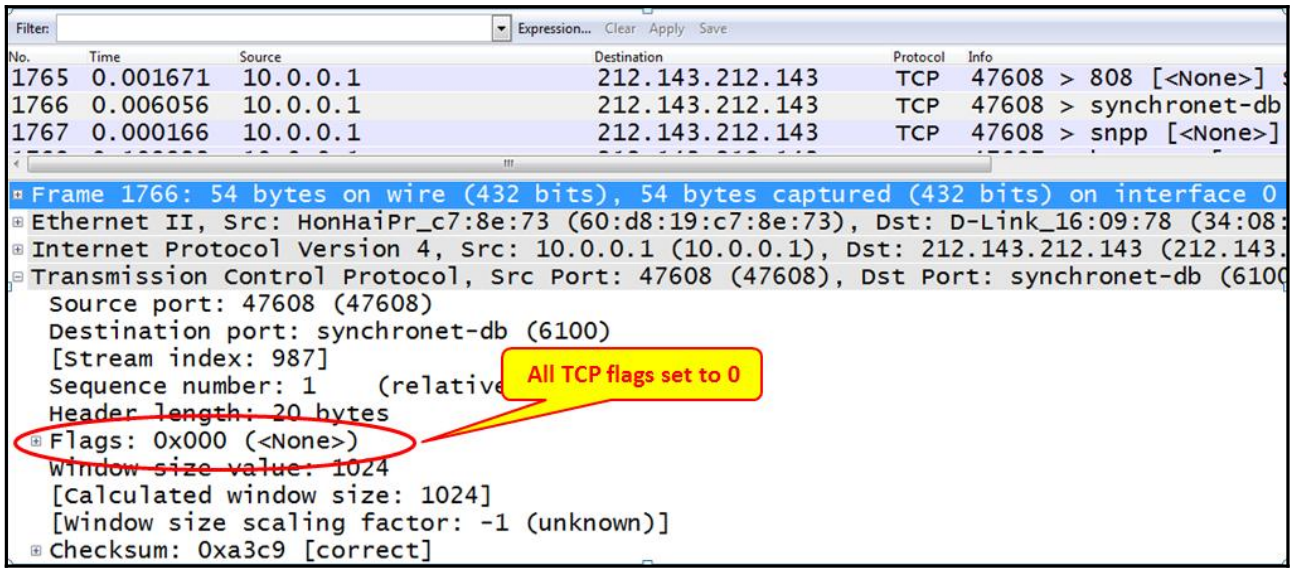

Conversations: test _00009_20130806185933
Ethernet: 4 Fibre Channel FDDI IPv4: 11904 IPv6 IPX JXTA NCP RSVP SCTP TCP: 11901 Token Ring UDP: 2 USB WLAN
Ethernet Conversations
Address A Address B Packets Bytes Packets A→B Bytes A→B Packets A←B Bytes A←B Rel Start
Intel_10:35:7f Netgear_40:ac:46 11 901 642 654 11 901 642 654 0 0 0.000000000
WistronI_ae:77:69 Broadcast 4 368 4 368 0 0 0.413813000
Intel_10:35:7f Broadcast 1 227 1 227 0 0 0.423689000
Intel_10:35:7f WistronI_ae:77:69 2 148 1 74 1 74 0.462937000
Name resolution
Limit to display filter
Help
Copy
Follow Stream
Close

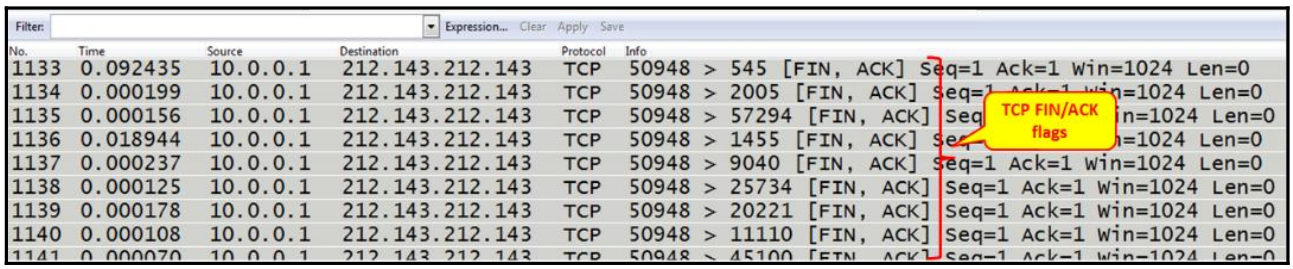

No. Time Source Destination Protocol Info
55372 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 1082 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55373 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 15003 [SYN] Seq=0 Win=1024 Len=0 MSS=146
55374 0.000034 10.0.0.103 10.0.0.10 TCP 33928 > 6567 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55375 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 458 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55376 0.000026 10.0.0.103 10.0.0.10 TCP 33928 > 8383 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55377 0.000035 10.0.0.103 10.0.0.10 TCP 33928 > 2100 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55378 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 1721 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55379 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 8994 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55380 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 6699 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55381 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 10616 [SYN] Seq=0 Win=1024 Len=0 MSS=146
55382 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 2381 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55383 0.000024 10.0.0.103 10.0.0.10 TCP 33928 > 55555 [SYN] Seq=0 Win=1024 Len=0 MSS=146
55384 0.000025 10.0.0.103 10.0.0.10 TCP 33928 > 8193 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
55385 0.000026 10.0.0.103 10.0.0.10 TCP 33928 > 10001 [SYN] Seq=0 Win=1024 Len=0 MSS=146
TCP SYN SCAN

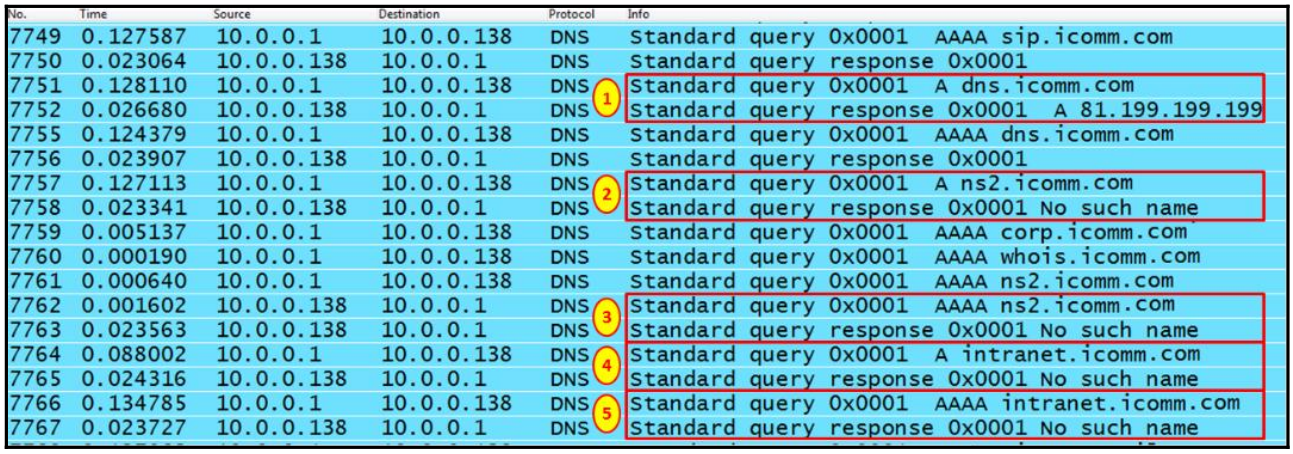

Follow TCP Stream
Stream Content
GET / HTTP/1.1
Connection: close
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)
Host: www.ndi-com.com
Host under attack
Nmap scanner is the user agent that generates the request !!!
HTTP/1.1 200 OK
Connection: close
Date: Mon, 26 Aug 2013 10:40:22 GMT
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Content-Length: 23527
Content-Type: text/html; Charset=UTF-8
Set-Cookie: ASPSESSIONIDQQQRRQRA=PCMPFEJBDJLFFMHJOCNKCAEB; path=/
Cache-control: private
Entire conversation (23958 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close


Attacking host 10.0.0.138
Attack on multiple TCP ports
Seq=1, Ack=1 to disrupt existing connections
Filter:
Apply
Save
No. Time Source Destination Protocol Info
252 0.000032 192.168.43.191 10.0.0.138 TCP 51752 > 1503 [ACK] Seq=1 Ack=1 Win=1024 Len=0
253 0.000023 192.168.43.191 10.0.0.138 TCP 51752 > 3128 [ACK] Seq=1 Ack=1 Win=1024 Len=0
254 0.000023 192.168.43.191 10.0.0.138 TCP 51752 > 19315 [ACK] Seq=1 Ack=1 Win=1024 Len=0
255 0.000033 192.168.43.191 10.0.0.138 TCP 51752 > 1580 [ACK] Seq=1 Ack=1 Win=1024 Len=0
256 0.000026 192.168.43.191 10.0.0.138 TCP 51752 > 1066 [ACK] Seq=1 Ack=1 Win=1024 Len=0
257 0.000025 192.168.43.191 10.0.0.138 TCP 51751 > 9595 [ACK] Seq=1 Ack=1 Win=1024 Len=0
258 0.001317 192.168.43.191 10.0.0.138 TCP 51752 > 212 [ACK] Seq=1 Ack=1 Win=1024 Len=0
259 0.000084 192.168.43.191 10.0.0.138 TCP 51752 > 512 [ACK] Seq=1 Ack=1 Win=1024 Len=0
260 0.000027 192.168.43.191 10.0.0.138 TCP 51752 > 10629 [ACK] Seq=1 Ack=1 Win=1024 Len=0
261 0.000027 192.168.43.191 10.0.0.138 TCP 51752 > 40193 [ACK] Seq=1 Ack=1 Win=1024 Len=0

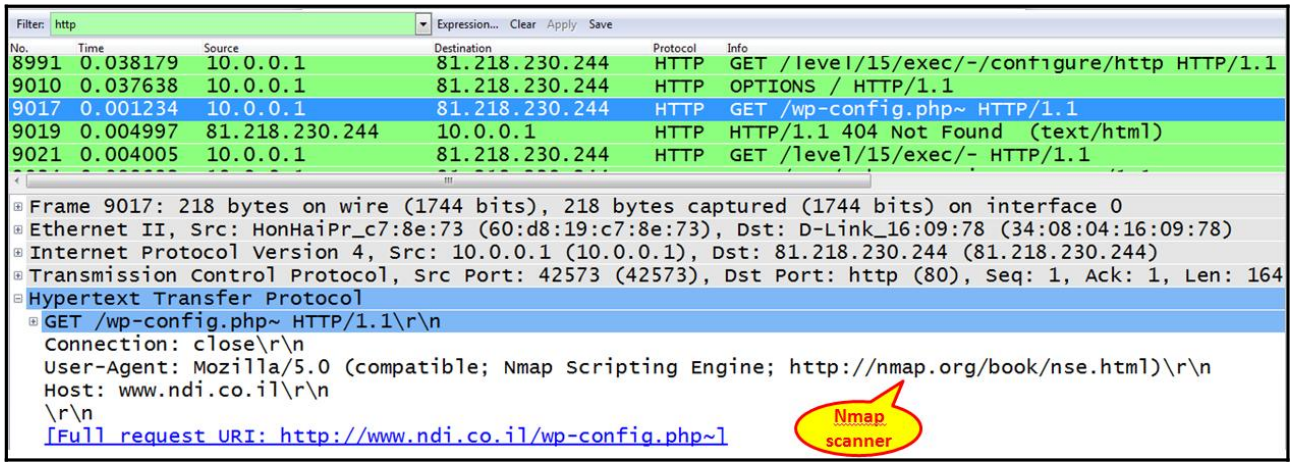

Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Info
2190 0.026411 192.168.43.191 10.0.0.138 TCP 51889 > 1 [ACK] Seq=1 Ack=1 Win=33554432 Len=0 WS
2191 0.025524 192.168.43.191 10.0.0.138 TCP 51890 > 1 [FIN, PSH, URG] Seq=1 Win=2147450880 Ur
2193 0.028932 10.0.0.138 192.168.43.191 TCP 1 > 51889 [RST] Seq=1 Win=0 Len=0
2195 0.048204 192.168.43.191 10.0.0.138 UDP Source port: 51930 Destination port: 30282
2196 0.029788 192.168.43.191 10.0.0.138 TCP 51888 > 1 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS
2197 0.024198 192.168.43.191 10.0.0.138 TCP 51890 > 1 [FIN, PSH, URG] Seq=1 Win=2147450880 Ur
2200 0.078040 192.168.43.191 10.0.0.138 UDP Source port: 51930 Destination port: 30282
2201 0.026694 192.168.43.191 10.0.0.138 TCP 51888 > 1 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS
2202 0.024286 192.168.43.191 10.0.0.138 TCP 51890 > 1 [FIN, PSH, URG] Seq=1 Win=2147450880 Ur
2205 0.080907 192.168.43.191 10.0.0.138 UDP Source port: 51930 Destination port: 30282
2206 0.026051 192.168.43.191 10.0.0.138 TCP 51888 > 1 [SYN] Seq=0 Win=31337 Len=0 WS=1024 MSS
2207 0.025937 192.168.43.191 10.0.0.138 TCP 51890 > 1 [FIN, PSH, URG] Seq=1 Win=2147450880 Ur
2208 0.173624 192.168.43.191 10.0.0.138 TCP 21462 > 80 [ACK] Seq=1 Ack=1 Win=2401 Len=0
2209 0.000169 192.168.43.191 10.0.0.138 TCP 21463 > 80 [ACK] Seq=1 Ack=1 Win=18085 Len=0


Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Info
1765 0.001671 10.0.0.1 212.143.212.143 TCP 47608 > 808 [<None>]
1766 0.006056 10.0.0.1 212.143.212.143 TCP 47608 > synchronet-db
1767 0.000166 10.0.0.1 212.143.212.143 TCP 47608 > snpp [<None>]
Frame 1766: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: D-Link_16:09:78 (34:08:
Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 212.143.212.143 (212.143.
Transmission Control Protocol, Src Port: 47608 (47608), Dst Port: synchronet-db (6100
Source port: 47608 (47608)
Destination port: synchronet-db (6100)
[Stream index: 987]
Sequence number: 1 (relative
Header length: 20 bytes
Flags: 0x000 (<None>)
Window size value: 1024
[Calculated window size: 1024]
[Window size scaling factor: -1 (unknown)]
Checksum: 0xa3c9 [correct]
All TCP flags set to 0


Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Info
1133 0.092435 10.0.0.1 212.143.212.143 TCP 50948 > 545 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1134 0.000199 10.0.0.1 212.143.212.143 TCP 50948 > 2005 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1135 0.000156 10.0.0.1 212.143.212.143 TCP 50948 > 57294 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1136 0.018944 10.0.0.1 212.143.212.143 TCP 50948 > 1455 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1137 0.000237 10.0.0.1 212.143.212.143 TCP 50948 > 9040 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1138 0.000125 10.0.0.1 212.143.212.143 TCP 50948 > 25734 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1139 0.000178 10.0.0.1 212.143.212.143 TCP 50948 > 20221 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
1140 0.000108 10.0.0.1 212.143.212.143 TCP 50948 > 11110 [FIN, ACK] Seq=1 Ack=1 Win=1024 Len=0
TCP FIN/ACK flags



No.	Time	Source	Destination	Protocol	Info
7749	0.127587	10.0.0.1	10.0.0.138	DNS	Standard query 0x0001 AAAA sip.icomm.com
7750	0.023064	10.0.0.138	10.0.0.1	DNS	Standard query response 0x0001
7751	0.128110	10.0.0.1	10.0.0.138	DNS	(1) Standard query 0x0001 A dns.icomm.com
7752	0.026680	10.0.0.138	10.0.0.1	DNS	(1) Standard query response 0x0001 A 81.199.199.199
7755	0.124379	10.0.0.1	10.0.0.138	DNS	Standard query 0x0001 AAAA dns.icomm.com
7756	0.023907	10.0.0.138	10.0.0.1	DNS	Standard query response 0x0001
7757	0.127113	10.0.0.1	10.0.0.138	DNS	(2) Standard query 0x0001 A ns2.icomm.com
7758	0.023341	10.0.0.138	10.0.0.1	DNS	(2) Standard query response 0x0001 No such name
7759	0.005137	10.0.0.1	10.0.0.138	DNS	Standard query 0x0001 AAAA corp.icomm.com
7760	0.000190	10.0.0.1	10.0.0.138	DNS	Standard query 0x0001 AAAA whois.icomm.com
7761	0.000640	10.0.0.1	10.0.0.138	DNS	Standard query 0x0001 AAAA ns2.icomm.com
7762	0.001602	10.0.0.138	10.0.0.1	DNS	(3) Standard query 0x0001 AAAA ns2.icomm.com
7763	0.023563	10.0.0.138	10.0.0.1	DNS	(3) Standard query response 0x0001 No such name
7764	0.088002	10.0.0.1	10.0.0.138	DNS	(4) Standard query 0x0001 A intranet.icomm.com
7765	0.024316	10.0.0.138	10.0.0.1	DNS	(4) Standard query response 0x0001 No such name
7766	0.134785	10.0.0.1	10.0.0.138	DNS	(5) Standard query 0x0001 AAAA intranet.icomm.com
7767	0.023727	10.0.0.138	10.0.0.1	DNS	(5) Standard query response 0x0001 No such name

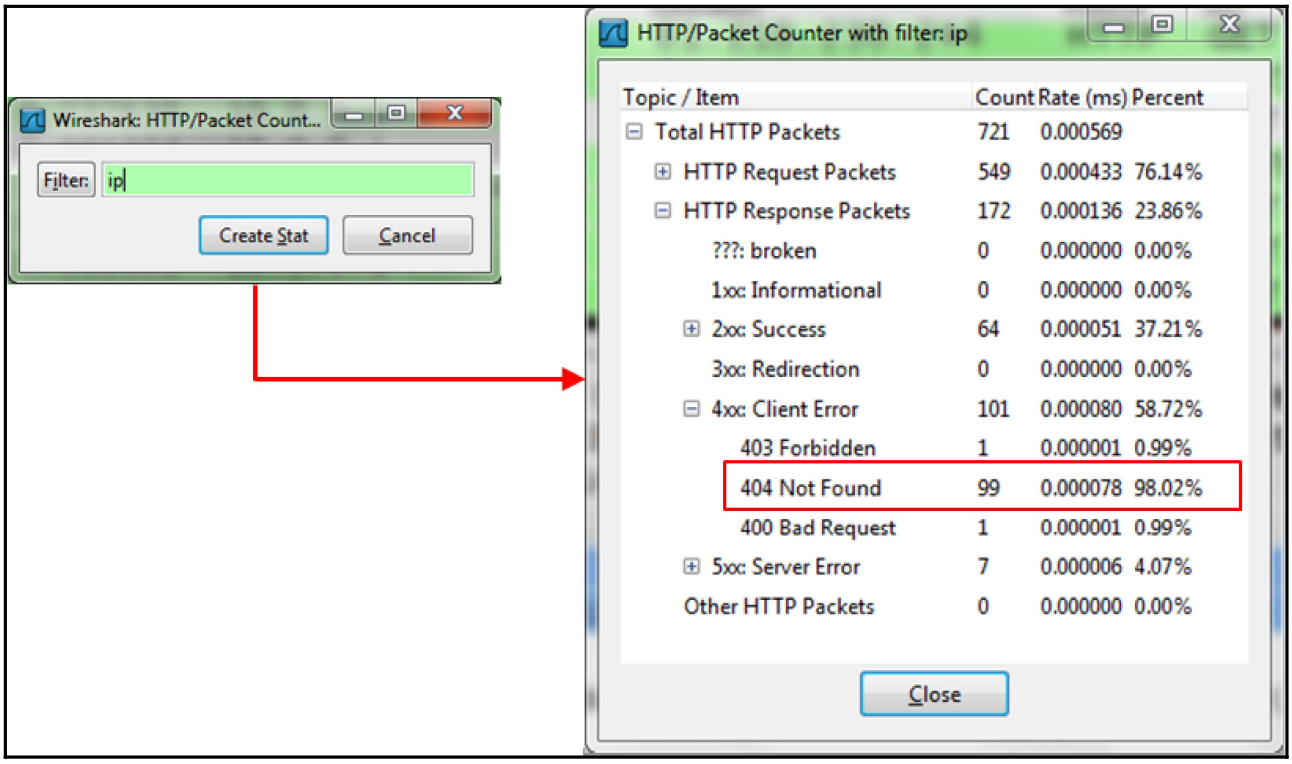


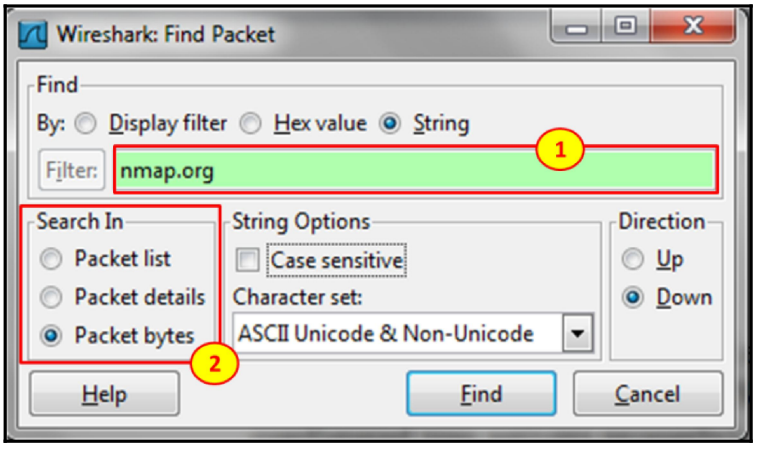
Filter: http Expression... Clear Apply Save

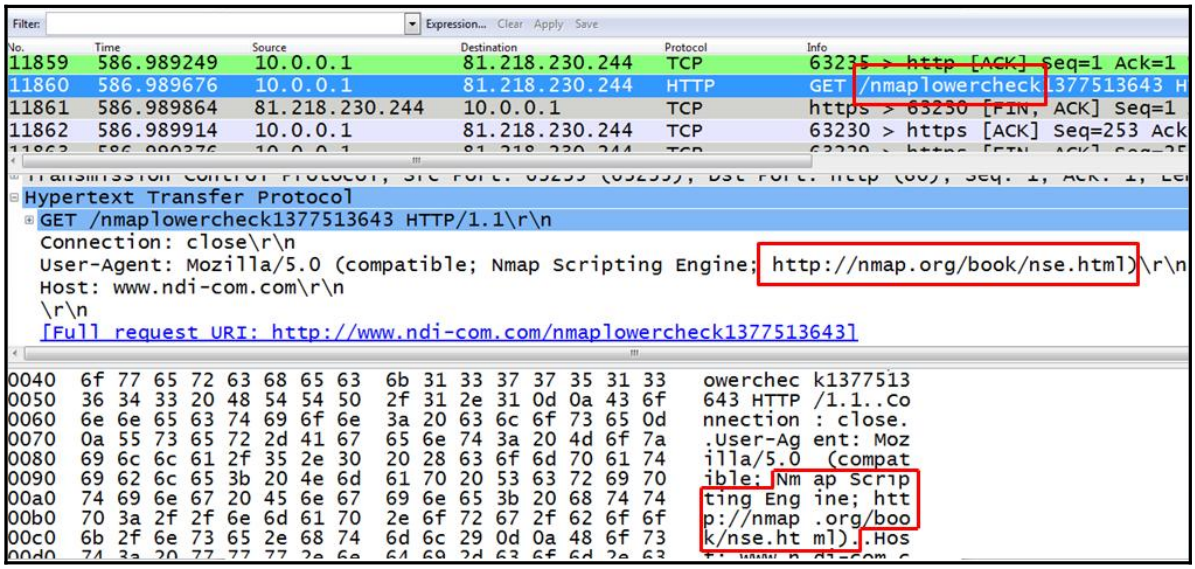
No.	Time	Source	Destination	Protocol	Info
8991	0.038179	10.0.0.1	81.218.230.244	HTTP	GET /level/15/exec/-/configure/http HTTP/1.1
9010	0.037638	10.0.0.1	81.218.230.244	HTTP	OPTIONS / HTTP/1.1
9017	0.001234	10.0.0.1	81.218.230.244	HTTP	GET /wp-config.php~ HTTP/1.1
9019	0.004997	81.218.230.244	10.0.0.1	HTTP	HTTP/1.1 404 Not Found (text/html)
9021	0.004005	10.0.0.1	81.218.230.244	HTTP	GET /level/15/exec/- HTTP/1.1

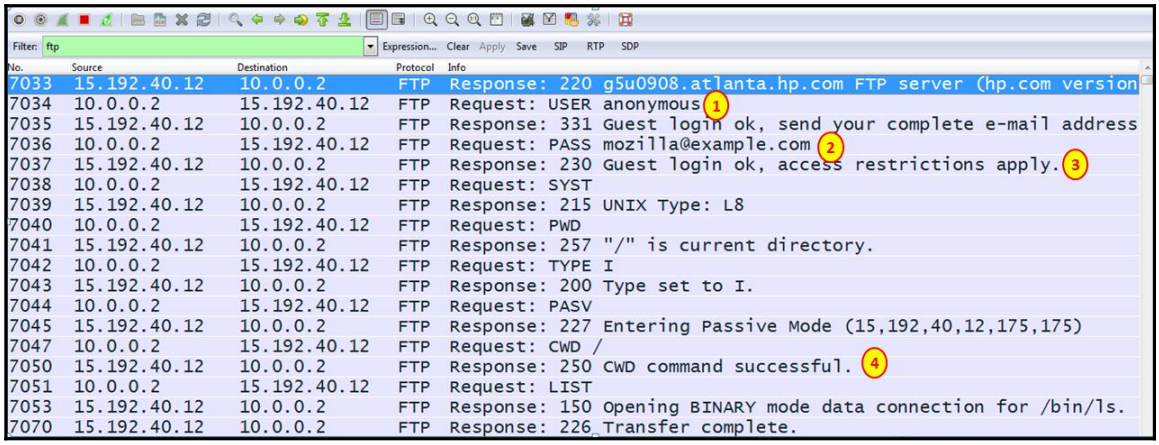
```
⊞ Frame 9017: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits) on interface 0
⊞ Ethernet II, Src: HonHaiPr_c7:8e:73 (60:d8:19:c7:8e:73), Dst: D-Link_16:09:78 (34:08:04:16:09:78)
⊞ Internet Protocol Version 4, Src: 10.0.0.1 (10.0.0.1), Dst: 81.218.230.244 (81.218.230.244)
⊞ Transmission Control Protocol, Src Port: 42573 (42573), Dst Port: http (80), Seq: 1, Ack: 1, Len: 164
⊟ Hypertext Transfer Protocol
  ⊞ GET /wp-config.php~ HTTP/1.1\r\n
    Connection: close\r\n
    User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)\r\n
    Host: www.ndi.co.il\r\n
    \r\n
    [Full request URI: http://www.ndi.co.il/wp-config.php~]
```

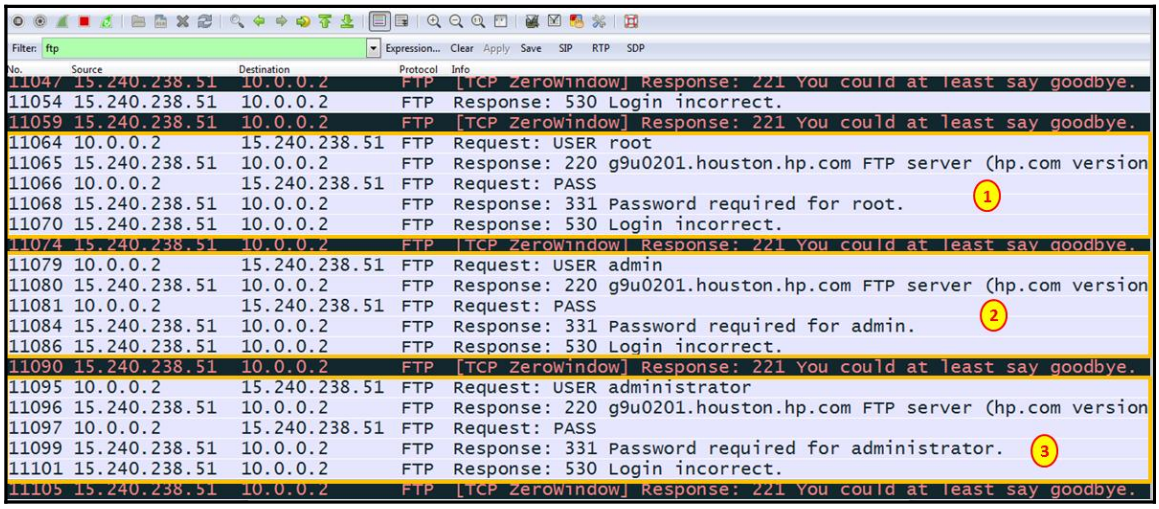
Nmap scanner


Wireshark: HTTP/Packet Count...
Filter:
ip
Create Stat
Cancel
HTTP/Packet Counter with filter: ip
Topic / Item
Count
Rate (ms)
Percent
Total HTTP Packets 721 0.000569
HTTP Request Packets 549 0.000433 76.14%
HTTP Response Packets 172 0.000136 23.86%
???: broken 0 0.000000 0.00%
1xx: Informational 0 0.000000 0.00%
2xx: Success 64 0.000051 37.21%
3xx: Redirection 0 0.000000 0.00%
4xx: Client Error 101 0.000080 58.72%
403 Forbidden 1 0.000001 0.99%
404 Not Found 99 0.000078 98.02%
400 Bad Request 1 0.000001 0.99%
5xx: Server Error 7 0.000006 4.07%
Other HTTP Packets 0 0.000000 0.00%
Close


Wireshark: Find Packet
Find
By:
Display filter
Hex value
String
Filter:
nmap.org
1
Search In
Packet list
Packet details
Packet bytes
2
String Options
Case sensitive
Character set:
ASCII Unicode & Non-Unicode
Direction
Up
Down
Help
Find
Cancel


Filter:
Expression... Clear Apply Save
No. Time Source Destination Protocol Info
11859 586.989249 10.0.0.1 81.218.230.244 TCP 63235 > http [ACK] Seq=1 Ack=1
11860 586.989676 10.0.0.1 81.218.230.244 HTTP GET /nmaplowercheck1377513643 H
11861 586.989864 81.218.230.244 10.0.0.1 TCP https > 63230 [FIN, ACK] Seq=1
11862 586.989914 10.0.0.1 81.218.230.244 TCP 63230 > https [ACK] Seq=253 Ack
Hypertext Transfer Protocol
GET /nmaplowercheck1377513643 HTTP/1.1\r\n
Connection: close\r\n
User-Agent: Mozilla/5.0 (compatible; Nmap Scripting Engine; http://nmap.org/book/nse.html)\r\n
Host: www.ndi-com.com\r\n
\r\n
[Full request URI: http://www.ndi-com.com/nmaplowercheck1377513643]
0040 6f 77 65 72 63 68 65 63 6b 31 33 37 37 35 31 33 owerchec k1377513
0050 36 34 33 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f 643 HTTP /1.1..Co
0060 6e 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d nnection : close.
0070 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Ag ent: Moz
0080 69 6c 6c 61 2f 35 2e 30 20 28 63 6f 6d 70 61 74 illa/5.0 (compat
0090 69 62 6c 65 3b 20 4e 6d 61 70 20 53 63 72 69 70 ible; Nm ap Scrip
00a0 74 69 6e 67 20 45 6e 67 69 6e 65 3b 20 68 74 74 ting Eng ine; htt
00b0 70 3a 2f 2f 6e 6d 61 70 2e 6f 72 67 2f 62 6f 6f p://nmap .org/boo
00c0 6b 2f 6e 73 65 2e 68 74 6d 6c 29 0d 0a 48 6f 73 k/nse.ht ml)..Hos


Filter: ftp
Expression... Clear Apply Save SIP RTP SDP
No. Source Destination Protocol Info
7033 15.192.40.12 10.0.0.2 FTP Response: 220 g5u0908.atlanta.hp.com FTP server (hp.com version
7034 10.0.0.2 15.192.40.12 FTP Request: USER anonymous 1
7035 15.192.40.12 10.0.0.2 FTP Response: 331 Guest login ok, send your complete e-mail address
7036 10.0.0.2 15.192.40.12 FTP Request: PASS mozilla@example.com 2
7037 15.192.40.12 10.0.0.2 FTP Response: 230 Guest login ok, access restrictions apply. 3
7038 10.0.0.2 15.192.40.12 FTP Request: SYST
7039 15.192.40.12 10.0.0.2 FTP Response: 215 UNIX Type: L8
7040 10.0.0.2 15.192.40.12 FTP Request: PWD
7041 15.192.40.12 10.0.0.2 FTP Response: 257 "/" is current directory.
7042 10.0.0.2 15.192.40.12 FTP Request: TYPE I
7043 15.192.40.12 10.0.0.2 FTP Response: 200 Type set to I.
7044 10.0.0.2 15.192.40.12 FTP Request: PASV
7045 15.192.40.12 10.0.0.2 FTP Response: 227 Entering Passive Mode (15,192,40,12,175,175)
7047 10.0.0.2 15.192.40.12 FTP Request: CWD /
7050 15.192.40.12 10.0.0.2 FTP Response: 250 CWD command successful. 4
7051 10.0.0.2 15.192.40.12 FTP Request: LIST
7053 15.192.40.12 10.0.0.2 FTP Response: 150 Opening BINARY mode data connection for /bin/ls.
7070 15.192.40.12 10.0.0.2 FTP Response: 226 Transfer complete.


Filter: ftp
Expression... Clear Apply Save SIP RTP SDP
No. Source Destination Protocol Info
11047 15.240.238.51 10.0.0.2 FTP [TCP ZeroWindow] Response: 221 You could at least say goodbye.
11054 15.240.238.51 10.0.0.2 FTP Response: 530 Login incorrect.
11059 15.240.238.51 10.0.0.2 FTP [TCP ZeroWindow] Response: 221 You could at least say goodbye.
11064 10.0.0.2 15.240.238.51 FTP Request: USER root
11065 15.240.238.51 10.0.0.2 FTP Response: 220 g9u0201.houston.hp.com FTP server (hp.com version
11066 10.0.0.2 15.240.238.51 FTP Request: PASS
11068 15.240.238.51 10.0.0.2 FTP Response: 331 Password required for root.
11070 15.240.238.51 10.0.0.2 FTP Response: 530 Login incorrect.
11074 15.240.238.51 10.0.0.2 FTP [TCP ZeroWindow] Response: 221 You could at least say goodbye.
11079 10.0.0.2 15.240.238.51 FTP Request: USER admin
11080 15.240.238.51 10.0.0.2 FTP Response: 220 g9u0201.houston.hp.com FTP server (hp.com version
11081 10.0.0.2 15.240.238.51 FTP Request: PASS
11084 15.240.238.51 10.0.0.2 FTP Response: 331 Password required for admin.
11086 15.240.238.51 10.0.0.2 FTP Response: 530 Login incorrect.
11090 15.240.238.51 10.0.0.2 FTP [TCP ZeroWindow] Response: 221 You could at least say goodbye.
11095 10.0.0.2 15.240.238.51 FTP Request: USER administrator
11096 15.240.238.51 10.0.0.2 FTP Response: 220 g9u0201.houston.hp.com FTP server (hp.com version
11097 10.0.0.2 15.240.238.51 FTP Request: PASS
11099 15.240.238.51 10.0.0.2 FTP Response: 331 Password required for administrator.
11101 15.240.238.51 10.0.0.2 FTP Response: 530 Login incorrect.
11105 15.240.238.51 10.0.0.2 FTP [TCP ZeroWindow] Response: 221 You could at least say goodbye.
1
2
3