Chapter 1: Getting Started with Wireshark - What, Why, and How?

<table>
<thead>
<tr>
<th>Sniffer Commands</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sniffer_dump</td>
<td>Retrieve captured packet data to PCAP file</td>
</tr>
<tr>
<td>sniffer_interfaces</td>
<td>Enumerate all sniffable network interfaces</td>
</tr>
<tr>
<td>sniffer_release</td>
<td>Free captured packets on a specific interface instead of downloading them</td>
</tr>
<tr>
<td>sniffer_start</td>
<td>Start packet capture on a specific interface</td>
</tr>
<tr>
<td>sniffer_stats</td>
<td>View statistics of an active capture</td>
</tr>
<tr>
<td>sniffer_stop</td>
<td>Stop packet capture on a specific interface</td>
</tr>
</tbody>
</table>

The Wireshark Network Analyzer - [Piyush Verma for PACKTPUB] - [Wireshark 1.12.6 (v1.12.6-0-gee1f1ce6 from master-1.12)]
About Wireshark

<table>
<thead>
<tr>
<th>Wireshark</th>
<th>Authors</th>
<th>Folders</th>
<th>Plugins</th>
<th>License</th>
</tr>
</thead>
</table>

Original Author
-------
Gerald Combs <gerald[AT]wireshark.org>

Contributors
-------
Gilbert Ramirez <gram[AT]alumni.rice.edu>
Thomas Bottom <tom.bottom[AT]labxtechnologies.com>
Chris Pane <chris-pane[AT]labxtechnologies.com>
Hannes R. Boehm <hannes[AT]boehm.org>
Mike Hall <mike[AT]hallzone.net>
Bobo Rajec <bobob[AT]bsp-consulting.sk>
Laurent Deniel <laurent.daniel[AT]free.fr>
Don Lafontaine <lafont02[AT]cn.ca>
Guy Harris <guy[AT]alum.mit.edu>
Simon Wilkinson <sxw[AT]dcs.ed.ac.uk>
Jorg Mayer <jmayer[AT]topof.de>
Martin Maciaszek <fastjack[AT]i-s-o.net>
Jun-ichiro itojun Hagino <itojun[AT]itojun.org>
Richard Sharpe <sharpe[AT]nsa.gov>
John McDermott <jim[AT]jinti.com>
Jeff Jahr <jeff[AT]shastarlets.com>
Brad Robel-Forrest <bradr[AT]watchguard.com>
Ashok Narayanan <ashok[AT]cisco.com>
Aaron Hillegass <aaron[AT]classmax.com>
Jason Lango <jil[AT]netapp.com>
Johan Feyaerts <Johan.Feyaerts[AT]siemens.com>
Olivier Abad <oabad[AT]roos.fr>
Thierry Andry <Thierry.Andry[AT]advvalses.be>
Jeff Foster <jfoste[AT]woodward.com>
Peter Torvalds <petertv[AT]xoommail.com>
Christophe Tronche <ch.tronche[AT]computer.org>

Filter:
ip.address == 192.168.1.1
ip.addr == 192.168.1.1

Save Filter as:
http.request.method == GET and ip.src == 192.168.20.130
GET Requests from 130
## Interface List
Live list of the capture interfaces (counts incoming packets)

### Start
Choose one or more interfaces to capture from, then **Start**

- VMware Network Adapter VMnet1
- Ethernet
- Wi-Fi
- VMware Network Adapter VMnet8

## Capture Options
Start a capture with detailed options

### Wireshark Capture Interfaces

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
<th>IP</th>
<th>Packets</th>
<th>Packets/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Network Adapter VMnet1</td>
<td>VMware Virtual Ethernet Adapter</td>
<td>fe80:81e5:1a9c:3ffe:506a</td>
<td>46</td>
<td>5</td>
</tr>
<tr>
<td>Ethernet</td>
<td>Realtek Ethernet Controller</td>
<td>fe80:8544:327:7378:4e3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Wi-Fi</td>
<td>Microsoft</td>
<td>fe80a:19b6:707a:7f1e:ds07</td>
<td>855</td>
<td>17</td>
</tr>
<tr>
<td>VMware Network Adapter VMnet8</td>
<td>VMware Virtual Ethernet Adapter</td>
<td>fe82:70:d72d:5d28:cf84</td>
<td>61</td>
<td>10</td>
</tr>
</tbody>
</table>

- [Help](#)  
- [Start](#)  
- [Stop](#)  
- [Options](#)  
- [Close](#)
Capture Help

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on:
Ethernet, WLAN, ...

Files

Open
Open a previously captured file

Open Recent:
X:\PackT\WNS\WNS\Chapter 1\TelnetCapture.pcap (11 kB)

Sample Captures
A rich assortment of example capture files on the wiki

Maximum recent files: 5

Wireshark: Capture Interfaces

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
<th>IP</th>
<th>Packets</th>
<th>Packets/s</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>Realtek Ethernet Controller</td>
<td>fe80::fca8:d134:33cf:8e07</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>WiFi</td>
<td>Microsoft</td>
<td>fe80::458d:264a:ee0f:8951</td>
<td>901</td>
<td>6</td>
</tr>
</tbody>
</table>

[Start] [Stop] [Options] [Close]
Chapter 2: Tweaking Wireshark

![Wireshark Capture Filter - Profile: Def...]

- **Edit**
  - **Capture Filter**
    - Ethernet address 00:08:15:00:08:15
    - Ethernet type 0x0806 (ARP)
    - No Broadcast and no Multicast
    - No ARP
    - IP only
    - IP address 192.168.0.1
    - IPX only
    - TCP only
    - UDP only
    - TCP or UDP port 80 (HTTP)
    - HTTP TCP port (80)
    - No ARP and no DNS
    - Non-HTTP and non-SMTP to/from www.wireshark.org

- **Delete**

- **Properties**
  - **Filter name:** Ethernet address 00:08:15:00:08:15
  - **Filter string:** ether host 00:08:15:00:08:15

- **Help**  
- **OK**  
- **Cancel**
### IPv4 Conversations

<table>
<thead>
<tr>
<th>Address A</th>
<th>Address B</th>
<th>Packets A-B</th>
<th>Bytes A-B</th>
<th>Packets A-&gt;B</th>
<th>Bytes A-&gt;B</th>
<th>Ref Start</th>
<th>Duration</th>
<th>bps A-B</th>
<th>bps A-&gt;B</th>
</tr>
</thead>
<tbody>
<tr>
<td>173.194.36.24</td>
<td>192.168.1.36</td>
<td>7</td>
<td>1,866</td>
<td>3</td>
<td>1,312</td>
<td>4</td>
<td>554</td>
<td>2,311967000</td>
<td>0.9999</td>
</tr>
<tr>
<td>104.130.120.128</td>
<td>192.168.1.36</td>
<td>16</td>
<td>1,229</td>
<td>7</td>
<td>432</td>
<td>9</td>
<td>797</td>
<td>5635600000</td>
<td>69,2034</td>
</tr>
<tr>
<td>102.1.175.1</td>
<td>192.168.1.36</td>
<td>728</td>
<td>439353</td>
<td>404</td>
<td>403065</td>
<td>324</td>
<td>36,288</td>
<td>49,811886000</td>
<td>48.7821</td>
</tr>
<tr>
<td>74.129.236.134</td>
<td>192.168.1.36</td>
<td>7</td>
<td>414</td>
<td>3</td>
<td>186</td>
<td>4</td>
<td>228</td>
<td>55,177722000</td>
<td>58.228</td>
</tr>
<tr>
<td>173.194.36.1</td>
<td>192.168.1.36</td>
<td>30</td>
<td>2,854</td>
<td>12</td>
<td>1,147</td>
<td>18</td>
<td>1,767</td>
<td>64,525138000</td>
<td>85.227</td>
</tr>
<tr>
<td>162.159.241.109</td>
<td>192.168.1.36</td>
<td>15</td>
<td>1,078</td>
<td>6</td>
<td>1,069</td>
<td>9</td>
<td>809</td>
<td>66,179240000</td>
<td>92.027</td>
</tr>
<tr>
<td>174.34.25.5</td>
<td>192.168.1.36</td>
<td>18</td>
<td>1,076</td>
<td>6</td>
<td>364</td>
<td>12</td>
<td>712</td>
<td>69,355460000</td>
<td>14,9738</td>
</tr>
<tr>
<td>67.215.252.139</td>
<td>192.168.1.36</td>
<td>10</td>
<td>1,700</td>
<td>5</td>
<td>780</td>
<td>5</td>
<td>920</td>
<td>69,523270000</td>
<td>1,416</td>
</tr>
<tr>
<td>173.154.36.15</td>
<td>192.168.1.36</td>
<td>35</td>
<td>30,757</td>
<td>22</td>
<td>29,623</td>
<td>13</td>
<td>1,134</td>
<td>69,701714000</td>
<td>3,0205</td>
</tr>
<tr>
<td>108.162.232.207</td>
<td>192.168.1.36</td>
<td>31</td>
<td>4,443</td>
<td>13</td>
<td>2,909</td>
<td>18</td>
<td>1,534</td>
<td>85,089728000</td>
<td>8,1839</td>
</tr>
</tbody>
</table>

### IPv4 Endpoints

<table>
<thead>
<tr>
<th>Address</th>
<th>Packets</th>
<th>Bytes</th>
<th>Tx Packets</th>
<th>Tx Bytes</th>
<th>Rx Packets</th>
<th>Rx Bytes</th>
<th>Country</th>
<th>City</th>
<th>Latitude</th>
<th>Longitude</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.36</td>
<td>15</td>
<td>1,702</td>
<td>6</td>
<td>896</td>
<td>9</td>
<td>806</td>
<td>United States</td>
<td>Mountain View, CA</td>
<td>37.419201</td>
<td>-122.057404</td>
</tr>
<tr>
<td>173.134.36.24</td>
<td>7</td>
<td>1,866</td>
<td>3</td>
<td>1,312</td>
<td>4</td>
<td>554</td>
<td>United States</td>
<td>Mountain View, CA</td>
<td>37.419201</td>
<td>-122.057404</td>
</tr>
<tr>
<td>104.130.120.128</td>
<td>16</td>
<td>1,229</td>
<td>7</td>
<td>432</td>
<td>9</td>
<td>797</td>
<td>United States</td>
<td>San Antonio, TX</td>
<td>29.488889</td>
<td>-98.395697</td>
</tr>
<tr>
<td>103.154.36.15</td>
<td>35</td>
<td>30,757</td>
<td>22</td>
<td>29,623</td>
<td>13</td>
<td>1,134</td>
<td>United States</td>
<td>Mountain View, CA</td>
<td>37.419201</td>
<td>-122.057404</td>
</tr>
<tr>
<td>174.34.25.5</td>
<td>18</td>
<td>1,076</td>
<td>6</td>
<td>364</td>
<td>12</td>
<td>712</td>
<td>United States</td>
<td>San Jose, CA</td>
<td>37.428999</td>
<td>-121.945999</td>
</tr>
<tr>
<td>67.215.252.139</td>
<td>10</td>
<td>1,700</td>
<td>5</td>
<td>780</td>
<td>5</td>
<td>920</td>
<td>United States</td>
<td>Santa Ana, CA</td>
<td>33,763302</td>
<td>-117.94197</td>
</tr>
<tr>
<td>173.154.36.15</td>
<td>35</td>
<td>30,757</td>
<td>22</td>
<td>29,623</td>
<td>13</td>
<td>1,134</td>
<td>United States</td>
<td>Mountain View, CA</td>
<td>37.419201</td>
<td>-122.057404</td>
</tr>
<tr>
<td>108.162.232.207</td>
<td>31</td>
<td>4,443</td>
<td>13</td>
<td>2,909</td>
<td>18</td>
<td>1,534</td>
<td>United States</td>
<td>San Francisco, CA</td>
<td>37.765699</td>
<td>-122.393203</td>
</tr>
</tbody>
</table>
Wireshark: 300 Expert Infos

Errors: 0 (0)  Warnings: 1 (5)  Notes: 2 (14)  Chats: 57 (231)  Details: 300  Packet Comments: 0

Expert - Expert info

.ws.expert.group - Group (Wireshark expert group)
.ws.expert.message - Message (Wireshark expert information)
.ws.expert.severity - Severity level (Wireshark expert severity level)

C:\\tshark -D
1. \Device\NPF_\{A0A69947-9A6A-4B5F-87EE-900B67D387A\}  (VMware Network Adapter VMnet1)
2. \Device\NPF_\{A0CC0E6D-5F3A-49EE-9AC7-98DBDF95FD0\}  (Ethernet)
3. \Device\NPF_\{A2BD2764-92CC-4DAE-8414-655ED62450C1\}  (Wi-Fi)
4. \Device\NPF_\{8D64F150-0BD8-46F0-8454-5B9527DE25C9\}  (Local Area Connection)
Chapter 3: Analyzing Threats to LAN Security

| 5  | 0.001510000 | 192.168.20.129 | 192.168.20.200 TCP 49944-21 [ACK] Seq=1 Ack=28 Win=29696 L  |
| 6  | 3.285827000 | 192.168.20.129 | 192.168.20.200 FTP Request: USER anonymous |
| 7  | 3.286395000 | 192.168.20.129 | 192.168.20.200 FTP Response: 331 Anonymous access allowed, |
| 9  | 5.610442000 | 192.168.20.129 | 192.168.20.100 FTP Request: PASS anonymous |
metasploitable login: mmssffaaddmmiinn
Password: msfadmin

TCP Ports: 80,3128,3132,5985,8080,8088,11371,1900,2869,2710
SSL/TLS Ports: 443

Entire conversation (77015 bytes)
192.168.20.200:20 → 192.168.20.129:57077 (0 bytes)

Stream Content
.... JPEG ............ Exif...II*
LCE-7

Errors: 1 (23597)  Warnings: 0 (0)  Notes: 0 (0)  Chats: 0 (0)  Details: 23597
Group  Protocol  Summary
Malformed TCP  Malformed Packet (Exception occurred)
### Interface: 192.168.20.132 --- 0xcb

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Physical Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.20.2</td>
<td>00-0c-27-9b-1a-7a</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.20.128</td>
<td>00-0c-27-9b-1a-7a</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.20.129</td>
<td>00-0c-27-9b-1a-7a</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.20.135</td>
<td>00-0c-27-9b-1a-7a</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

**Errors:** 0 (0)  **Warnings:** 6 (420)  **Notes:** 0 (0)  **Chats:** 0 (0)  **Details:** 420

**Group**  **Protocol**  **Summary**

1. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.135)**
2. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.254)**
3. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.132)**
4. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.128)**
5. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.2)**
6. **Sequence** ARP/RARP  **Duplicate IP address configured (192.168.20.1)**

### Table

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1650</td>
<td>0.964400</td>
<td>202.31.92.97</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1651</td>
<td>0.964445</td>
<td>24.128.209.15</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1652</td>
<td>0.964603</td>
<td>0.28.170.40</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1653</td>
<td>0.964651</td>
<td>81.103.181.82</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1655</td>
<td>0.970208</td>
<td>85.104.183.50</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1656</td>
<td>0.970305</td>
<td>85.104.183.50</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1657</td>
<td>0.970363</td>
<td>85.104.183.50</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1658</td>
<td>0.970412</td>
<td>152.8.91.49</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1659</td>
<td>0.970628</td>
<td>126.233.183.65</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1660</td>
<td>0.970681</td>
<td>126.233.183.65</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1661</td>
<td>0.970729</td>
<td>224.147.19.9</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
<tr>
<td>1662</td>
<td>0.970775</td>
<td>224.147.19.9</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>64</td>
<td>[Malformed Packet]</td>
</tr>
</tbody>
</table>

**Frame 1650:** 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Transmission Control Protocol, Src Port: 58221
Source Port: 58221 (58221)
Destination Port: 22 (22)
[Stream index: 16]

Header Length: 20 bytes

Flags: 0x000 (None)

Indicates a packet with NO TCP flags

<table>
<thead>
<tr>
<th>Time</th>
<th>192.168.20.129</th>
<th>192.168.20.134</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.013458</td>
<td>ACK</td>
<td>RST</td>
</tr>
<tr>
<td>13.014072</td>
<td>ACK</td>
<td>RST</td>
</tr>
<tr>
<td>13.014339</td>
<td>(923)</td>
<td>(923)</td>
</tr>
<tr>
<td>13.014442</td>
<td>(923)</td>
<td>(923)</td>
</tr>
</tbody>
</table>

Form item: "GALX" = "iLLGOCpBk_Q"
Form item: "continue" = "http://mail.google.com/mail/"
Form item: "service" = "mail"
Form item: "rm" = "false"
Form item: "tmpl" = "default"
Form item: "scc" = "1"
Form item: "ss" = "1"
Form item: "osld" = "1"
Form item: "_utf8" = "UTF-8"
Form item: "bgresponse" = "!FbdChXIXE5uStyNEA02AAdc6XX"
Form item: "pstMsg" = "1"
Form item: "dnConn" = ""
Form item: "checkConnection" = ""
Form item: "checkedDomains" = "youtube"
Form item: "Email" = "randomuser@gmail.com"
Form item: "Passwd" = "THE!R!SHC@FE"
Form item: "signIn" = "sign in"

Full request URL: http://login.yahoo.com/?src=ym&int
HTTP request 1/2
[Response in frame: 85221]
[Next request in frame: 85251]

HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "countrycode" = "1"
Form item: "username" = "randomuser@yahoo.com"
Form item: "passwd" = "SUPER$3CR3TP@$w0rd"
Write

Read the trace file and look for top processes
root@famstrang-vm:~# sysdig -cl

**Category: CPU Usage**

- **spectrogram**: Visualize OS latency in real time.
- **subsecoffset**: Visualize subsecond offset execution time.
- **topcontainers_cpu**: Top containers by CPU usage
- **topprocs_cpu**: Top processes by CPU usage

**Category: Errors**

- **topcontainers_error**: Top containers by number of errors
- **topfiles_errors**: Top files by number of errors
- **topprocs_errors**: Top processes by number of errors

```
C:\>Pcap2xml-1.0\64-bit\Pcap2XML.exe Wireless_Sample.pcap -s Wireless_Sample.db

PCAP2XML
ver 1.0 by Pentester Academy
Info: http://PentesterAcademy.com/pcap2xml
A tool to convert 802.11 trace files to XML and SQLite DB format
Ver. 1.0 only supports WLAN MAC Header

[+] Opening file: Wireless_Sample.pcap <175.1 kB>
[+] Processing packet 1093... <100.00 >>
[+] Parsing completed
[+] Dumping into XML and/or SQLite
[+] Processing done!
[+] Run statistics:

Filename: Wireless_Sample.pcap
Number of packets: 1093
Number of packets parsed: 1093
Data packets parsed: 286
Control packets parsed: 356
Management packets parsed: 451
SQLite output file: Wireless_Sample.db
Total time taken: 0.404 sec
[-] No update available. This is the latest version
```
```python
# ./sshflow.py SSH.pcap

loading analyzers
  general_stats
  nested_tunnels
  interactive_session
  jabber
  x11_tunneling
  scp

Generating statistics from pcap file, please wait...


processed 390 packets, analysis follows...


General statistics
  Detected ciphersuite: aes128-ctr hmac-md5 zlib@openssh.com
  Smallest possible packet for ciphersuite: 48
  Packets sent by client: 111
  Packets sent by server: 136
  Average client packet length: 890
  Average server packet length: 1165
  Total bytes (of SSH data) sent by client: 7120
  Total bytes (of SSH data) sent by server: 15416
  Most common client packet size: [(48, 101), (64, 3), (144, 2), (32, 1), (16, 1)]
  Most common server packet size: [(48, 57), (64, 49), (60, 15), (112, 3), (1446, 3)]
  Average time between client packets: 0.618071027236
  Average time between server packets: 0.507311671527

-> Likely an interactive shell session

--- End of analysis ---
```
```plaintext
# ./sshflow.py SSH2.pcap
loading analyzers
  general_stats
  nested_tunnels
  interactive_session
  jabber
  x11_tunneling
  scp

generating statistics from pcap file, please wait...

SSH handshake: 192.168.10.129:39961 -> 192.168.10.133:22

processed 148 packets, analysis follows...

General statistics
  Detected ciphersuite: aes128-ctr hmac-md5 zlilb@openssh.com
  Smallest possible packet for ciphersuite: 48
  Packets sent by client: 69
  Packets sent by server: 12
  Average client packet length: 7149
  Average server packet length: 275
  Total bytes (of SSH data) sent by client: 78640
  Total bytes (of SSH data) sent by server: 22000
  Most common client packet size: [(1448, 51), (64, 4), (504, 4), (32, 2), (144, 2)]
  Most common server packet size: [(48, 5), (32, 1), (64, 1), (50, 1), (128, 1)]
  Average time between client packets: 0.0535690151155
  Average time between server packets: 0.311237725345

--> likely a file copy from client to server

--- End of analysis ---

GET /sql-labs/LESS-1/?id=1 HTTP/1.1\r\nHost: 192.168.20.129\r\nAccept: */\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij\r\nConnection: Close\r\n
GET /sql-labs/LESS-1/?id=1 HTTP/1.1\r\nAccept-Language: en-us,en;q=0.5\r\nAccept-Encoding: gzip,deflate\r\nHost: 127.0.0.1\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\nUser-Agent: sqlmap/1.0-dev-nongit-20150228 (http://sqlmap.org)\r\n
Wireshark: Protocol Hierarchy Statistics

<table>
<thead>
<tr>
<th>Protocol</th>
<th>% Packets</th>
<th>Packets</th>
<th>%Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame</td>
<td>100.00 %</td>
<td>208428</td>
<td>100.00 %</td>
</tr>
<tr>
<td>IEEE 802.11 wireless LAN</td>
<td>100.00 %</td>
<td>208428</td>
<td>100.00 %</td>
</tr>
<tr>
<td>IEEE 802.11 wireless LAN management frame</td>
<td>0.10 %</td>
<td>213</td>
<td>0.14 %</td>
</tr>
<tr>
<td>Data</td>
<td>74.39 %</td>
<td>155051</td>
<td>95.07 %</td>
</tr>
</tbody>
</table>
```
Filter: wlan.wep.iv

802.11 Channel: Channel Offset: FCS Filter: All Frames

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Time</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>13.203262</td>
<td>Cisco-Li_4c:bb:74</td>
<td>8</td>
<td>13.342526</td>
</tr>
<tr>
<td>9</td>
<td>15.214526</td>
<td>Cisco-Li_4c:bb:74</td>
<td>14</td>
<td>23.34078</td>
</tr>
<tr>
<td>16</td>
<td>23.342522</td>
<td>Cisco-Li_4c:bb:74</td>
<td>18</td>
<td>23.354021</td>
</tr>
<tr>
<td>28</td>
<td>37.516094</td>
<td>Cisco-Li_4c:bb:74</td>
<td>37</td>
<td>521214</td>
</tr>
</tbody>
</table>

Packets: 208428 · Displayed: 155051 (74.4%)

Frame 5: 100 bytes on wire (800 bits), 100 bytes captured (8 bytes total)
- IEEE 802.11 Data, Flags: p....F.
  - Type/Subtype: Data (0x0020)
  - Frame Control Field: 0x0842
  - Duration: 48 microseconds
  - Receiver address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
  - Destination address: Apple_3e:91:68 (e4:ce:8f:3e:91:68)
  - Transmitter address: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
  - BSSID: Cisco-Li_4c:bb:76 (00:1a:70:4c:bb:76)
  - Source address: Cisco-Li_4c:bb:74 (00:1a:70:4c:bb:74)
  - Fragment number: 0
  - Sequence number: 2688

- WEP parameters
  - Initialization Vector: 0xa70468
  - Key Index: 0
  - WEP ICV: 0x0a624042 (not verified)

Aircrack-ng 1.2 rc2

[00:00:00] Tested 861 keys (got 50459 IVs)

<table>
<thead>
<tr>
<th>KB</th>
<th>depth</th>
<th>byte (vote)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0/13</td>
<td>28 (63744)</td>
</tr>
<tr>
<td>1</td>
<td>0/1</td>
<td>57 (75544)</td>
</tr>
<tr>
<td>2</td>
<td>1/2</td>
<td>1E (61952)</td>
</tr>
<tr>
<td>3</td>
<td>0/1</td>
<td>B4 (75264)</td>
</tr>
<tr>
<td>4</td>
<td>9/4</td>
<td>F9 (58368)</td>
</tr>
</tbody>
</table>


Decrypted correctly: 100%
Internet Message Format

Received: from [192.168.0.122] ([2.2.2.1]) by carolinacon8.com
Message-ID: <4F90B1BE.9060902@carolinacon8.com>
Date: Sun, 29 Apr 2012 17:25:18 -0400
From: metalman <metalman@carolinacon8.com>, 1 i
User-Agent: Mozilla/5.0 (Windows; U; Windows NT MIME-version: 1.0
To: crashman@carolinacon8.com, metalman@carolinacon8.com
Subject: yo...
Content-Type: text/plain; charset=ISO-8859-1; f
Content-Transfer-Encoding: 7bit
Return-Path: <metalman@carolinacon8.com>
Line-based text data: text/plain

cm,\n
is this right?\n
\n
`dGhlIHBhc3N3b3JkIgIzIGJvcmkkIHRvIg==`

Base-64 encoded string

```python
>>> python
Python 2.7.3 (default, Mar 14 2014, 11:57:14)
[GCC 4.7.2] on linux2
Type "help", "copyright", "credits" or "license"
>>> import base64
>>> base64.b64decode("dGhlIHBhc3N3b3JkIgIzIGJvcmkkIHRvIg==")
'the password is bostonMA1977\n'
```

BOSTON MARATHON

**Password:**

bostonmarathon2012
### Chapter 4: Probing E-mail Communications

#### Filters:
- **pop.request.command == PASS**
- **ftp.request.command**
- **ftp.response.code == 230**

#### Table 1: pop.request.command

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>30225</td>
<td>0.000422</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>3026</td>
<td>0.074131</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30322</td>
<td>0.199417</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30325</td>
<td>0.249480</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30326</td>
<td>0.262069</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30330</td>
<td>0.277704</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30331</td>
<td>0.277711</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30332</td>
<td>0.277711</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30345</td>
<td>0.327554</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
<tr>
<td>30346</td>
<td>0.327642</td>
<td>192.168.10.1</td>
<td>192.168.10.132</td>
<td>POP</td>
<td>C: PASS</td>
</tr>
</tbody>
</table>

#### Table 2: ftp.request.command

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>0.000557</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: USER admin</td>
</tr>
<tr>
<td>30</td>
<td>0.006026</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: USER admin</td>
</tr>
<tr>
<td>32</td>
<td>0.009513</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: PASS PACKT</td>
</tr>
<tr>
<td>34</td>
<td>0.021116</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: USER admin</td>
</tr>
<tr>
<td>36</td>
<td>0.031096</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: PASS packtpub</td>
</tr>
<tr>
<td>39</td>
<td>0.032572</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: USER admin</td>
</tr>
<tr>
<td>48</td>
<td>0.048233</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: USER admin</td>
</tr>
<tr>
<td>51</td>
<td>0.060492</td>
<td>192.168.10.129</td>
<td>192.168.10.133</td>
<td>FTP</td>
<td>Request: PASS ftppassword</td>
</tr>
</tbody>
</table>

#### Table 3: ftp.response.code == 230

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1576</td>
<td>10.316911</td>
<td>192.168.10.133</td>
<td>192.168.10.129</td>
<td>FTP</td>
<td>Response: 230 User msfadmin logged in</td>
</tr>
</tbody>
</table>

Note: The highlighted text in the tables indicates specific data points of interest.
content-Type: application/octet-stream; name="secret.rtf"
content-Transfer-Encoding: quoted-printable
content-disposition: attachment; filename="secret.rtf"

\{\rtf1\ansi\ansicpg1252\deff0\deflang2057{\fonttbl{\f0\fswiss\fcharset0 = Arial};}\}{\"\generator Mstedit 5.41.21.2509;\}\viewkind4\uc1\pard\f0\fs20 This is a secret proto type of the new car being launched by SecurityOverride.\par
\par
{\object\objemb{\#\objclass Package}\objw1200\objh810{\#\objdata=20
\parr
click and drag this photo on to your image.\par
\parr
Also I would be delivering the blue meet, \par
\parr
See you at \par
\parr
Location: Movie Park, Germany\par
date\tab : 29 February 2011\par

Beginning of the RTF file

End of RTF File
This is a secret prototype type of the new car being launched by SecurityOverride.

[Image]

concept.jpg

click and drag this photo onto your Desktop to see details of this image.

Also I would be delivering the blueprints of this car to you when I meet,

See you at

Location: Movie Park, Germany
Date: 29 February 2011

see you there..........................

```bash
Tamstrange@ol!: $ nc -v 192.168.20.160 25
itsecgames.com [192.168.20.160] 25 (smtp) open
220 bee-box ESMT Postfix (Ubuntu)
VRFY root
250 2.0.0 root
VRFY piyush
550 5.1.1 <piyush>: Recipient address rejected: User unknown in local recipient table
VRFY bee
250 2.0.0 bee

msf auxiliary(smtp_enum) > run
[*] 192.168.20.160:25 Users found: , avahi, avahi-autodip, backup, bin, daemon, ftp, games, gdm, gnats, haaldemo, hplip, irc, libuvuid, list, lp, mail, mar, meseagebus, news, nobody, postmaster, proxy, pulse, ssdh, sync, sys, syslog, uucp, www-data
```
Chapter 5: Inspecting Malware Traffic

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>SPort</th>
<th>Destination</th>
<th>DPort</th>
<th>Length</th>
<th>Protocol</th>
<th>HTTP Host</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>2346</td>
<td>17.03</td>
<td>172.16.165.2</td>
<td>53</td>
<td>172.16.165.132</td>
<td>57758</td>
<td>289</td>
<td>DNS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Coloring Rule Name: Unusual # of DNS Answers]
[Coloring Rule String: dns.count.answers > 5]
### How to detect the **ZeroAccess botnet** on your network and...

[scwa.com/how-to-detect-the-zeroaccess-botnet-on-your-network-and-st...](scwa.com/how-to-detect-the-zeroaccess-botnet-on-your-network-and-st...) Dec 11, 2013 - ZeroAccess (as of this writing) uses ports 16464, 16465, 16470, and / or 16471. The specific port depends on whether the version is 32-bit or...

### [PDF] The **ZeroAccess Botnet** – Mining and Fraud for Massive...


Sep 4, 2012 - Ports 16464 and 16465 are used by the 32-bit and 64-bit versions of one botnet; ports 16470 and 16471 are used by the 64-bit and 32-bit...
Malicious sample history communicated with this IP

<table>
<thead>
<tr>
<th>No.</th>
<th>SHA-256</th>
<th>Anti-virus</th>
<th>Scan Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>2144081a96ac5d690f72457e4a5e547f6ed727711f4ae175327e786d5948e1</td>
<td>35 / 47</td>
<td>2013-01-26 01:57:108</td>
</tr>
<tr>
<td>26</td>
<td>A8D1361664A8086D06266887CAB207F7DCD020B42611C1FA2A8D447B5C026C46F81</td>
<td>46 / 52</td>
<td>2014-03-27 01:21:29</td>
</tr>
<tr>
<td>25</td>
<td>C38E4C173F660275F512BD609FEB8C764765A529C6E935F0D44C1706F9492E4C61F3369</td>
<td>34 / 46</td>
<td>2013-08-17 03:45:19</td>
</tr>
<tr>
<td>24</td>
<td>8EF7360968571756223311BC86C1CFED3955F0D44C1706F9492E4C61F3369</td>
<td>8 / 46</td>
<td>2013-08-14 15:52:43</td>
</tr>
</tbody>
</table>

Host
tonerkozpont.com
raiwinnners.org
domicossos.com
domicossos.com
domicossos.com
domicossos.com
domicossos.com
domicossos.com

to
c

<html>
<head>
<meta http-equiv="Refresh" content="1;URL=http://raiwinnners.org/sword/in.cgi?2">
</head>
<body>

HTTP/1.1 202 Found
Date: Thu, 18 Jul 2013 20:45:33 GMT
Server: nginx/0.7.67
Location: http://domicossos.com/ngen/controlling/mydb.php
Connection: Keep-Alive

Graph Analysis

192.168.204.150  176.119.5.7

54618–80 [SYN] 91.186.20.51
54616–80 [SYN]  80–54616 [SYN] ...
54616–80 [ACK]  80–54616 [ACK] ...
GET /wp-content ...
TCP segment of ...
HTTP/1.1 200 OK
54618–80 [SYN]  54616–80 [ACK] ...
54616–80 [ACK]  54616–80 [ACK] ...

<table>
<thead>
<tr>
<th>Packet num</th>
<th>Hostname</th>
<th>Content Type</th>
<th>Size</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>tonerkopcnt.com</td>
<td>text/html</td>
<td>258 bytes</td>
<td>sftxte1.html</td>
</tr>
<tr>
<td>17</td>
<td>roiwinners.org</td>
<td>text/html</td>
<td>232 bytes</td>
<td>incgi12</td>
</tr>
<tr>
<td>93</td>
<td>domenicosso.com</td>
<td>text/html</td>
<td>46 kB</td>
<td>mydb.php</td>
</tr>
<tr>
<td>106</td>
<td>domenicosso.com</td>
<td>application/octet-stream</td>
<td>4170 bytes</td>
<td>shift.php</td>
</tr>
<tr>
<td>163</td>
<td>domenicosso.com</td>
<td>application/java-archive</td>
<td>31 kB</td>
<td>mydb.php!IMugUQWjIXMtBPsp=koYuyQ</td>
</tr>
<tr>
<td>665</td>
<td>domenicosso.com</td>
<td>application/x-mdsdownload</td>
<td>348 kB</td>
<td>mydb.php!F53322f312h&amp;be=2g522j3:</td>
</tr>
<tr>
<td>1017</td>
<td>domenicosso.com</td>
<td>application/x-mdsdownload</td>
<td>211 kB</td>
<td>mydb.php!HF=53322f312h&amp;ye=2g542d1:</td>
</tr>
<tr>
<td>1212</td>
<td>domenicosso.com</td>
<td>application/x-mdsdownload</td>
<td>102 kB</td>
<td>mydb.php!ff=53322f312h&amp;le=5552532f:</td>
</tr>
</tbody>
</table>

HTTP/1.1 200 OK  
Date: Thu, 18 Jul 2013 20:45:40 GMT  
ETag: "f472177c3d4f8d76cacb20c3a092a2cc"  
Server: nginx/0.7.67  
Connection: Keep-Alive  
Content-Type: application/java-archive  
X-Powered-By: PHP/5.3.23

HTTP/1.1 200 OK  
Date: Thu, 18 Jul 2013 20:45:42 GMT  
Pragma: public  
Server: nginx/0.7.67  
Expires: Thu, 18 Jul 2013 23:42:19 GMT  
Connection: Keep-Alive  
Content-Type: application/x-mdsdownload  
X-Powered-By: PHP/5.3.23  
Cache-Control: must-revalidate, post-check=0, pre-check=0  
Cache-Control: private  
Content-Length: 348160  
Content-Disposition: attachment; Filename="calc.exe"  
Content-Transfer-Encoding: binary

File-signature for EXE: MZ................@..!..!..This program cannot be run in DOS mode.

File-signature for EXE: MZ................@..!..!..This program cannot be run in DOS mode.

File-signature for EXE: MZ................@..!..!..This program cannot be run in DOS mode.
VirusTotal

SHA256: 43565420246215bef3f02615166e38eaec4cde9d77c59f322c99421d1693649c

File name: readme.exe

Detection ratio: 36 / 49

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Source Port</th>
<th>Destination</th>
<th>Destination Port</th>
<th>Length</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>19.02</td>
<td>147.32.84.165</td>
<td>1039</td>
<td>130.239.18.172</td>
<td>6667</td>
<td>101</td>
<td>IRC</td>
</tr>
<tr>
<td>47</td>
<td>19.06</td>
<td>130.239.18.172</td>
<td>6667</td>
<td>147.32.84.165</td>
<td>1039</td>
<td>118</td>
<td>IRC</td>
</tr>
<tr>
<td>58</td>
<td>19.22</td>
<td>130.239.18.172</td>
<td>6667</td>
<td>147.32.84.165</td>
<td>1039</td>
<td>159</td>
<td>IRC</td>
</tr>
</tbody>
</table>

Answers
- irc.freenode.net: type CNAME, class IN, cname chat.freenode.net
- chat.freenode.net: type A, class IN, addr 130.239.18.172
- chat.freenode.net: type A, class IN, addr 140.211.167.98
- chat.freenode.net: type A, class IN, addr 140.211.167.99
- chat.freenode.net: type A, class IN, addr 174.143.119.91
- chat.freenode.net: type A, class IN, addr 213.92.8.4
- chat.freenode.net: type A, class IN, addr 213.179.58.83
- chat.freenode.net: type A, class IN, addr 213.232.93.3
- chat.freenode.net: type A, class IN, addr 216.155.130.130
- chat.freenode.net: type A, class IN, addr 38.229.70.20
- chat.freenode.net: type A, class IN, addr 78.40.125.4
- chat.freenode.net: type A, class IN, addr 82.96.64.4
- chat.freenode.net: type A, class IN, addr 86.65.39.15
- chat.freenode.net: type A, class IN, addr 89.16.176.16
- chat.freenode.net: type A, class IN, addr 93.152.160.101
- chat.freenode.net: type A, class IN, addr 128.237.157.136

NICK Pepe889696
USER znuehjm 0 0 :Pepe889696
USERHOST Pepe889696
MODE Pepe889696 -x
JOIN #zarasa48
Chapter 6: Network Performance Analysis

- 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: ✓
### UDP Conversations

<table>
<thead>
<tr>
<th>Address A</th>
<th>Port A</th>
<th>Address B</th>
<th>Port B</th>
<th>Packets</th>
<th>Bytes</th>
<th>Packets A--B</th>
<th>Bytes A--B</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.10.132</td>
<td>46816</td>
<td>182.58.213.46</td>
<td>17940</td>
<td>471</td>
<td>372534</td>
<td>300</td>
<td>350583</td>
</tr>
<tr>
<td>192.168.10.132</td>
<td>46816</td>
<td>116.203.219.84</td>
<td>31098</td>
<td>283</td>
<td>231847</td>
<td>168</td>
<td>224215</td>
</tr>
<tr>
<td>192.168.10.132</td>
<td>46816</td>
<td>2.51.48.167</td>
<td>26372</td>
<td>109</td>
<td>41966</td>
<td>57</td>
<td>3534</td>
</tr>
</tbody>
</table>

- DNS Standard query Ox445  A version.vuze.com
- DNS Standard query Ox10c7  SOA piyush-40f60e5d.docomo.com
- DNS Standard query Ox0001  ANY tracker.istole.it
- DNS Standard query Ox0001  ANY 12.rarbg.me
- DNS Standard query Ox0002  ANY tracker.istole.it
- DNS Standard query Oxdc47  A ipv4.tracker.hurry.lu
- DNS Standard query Ox2746  A tracker.coppersurfer.tk
- DNS Standard query Ox5e40  A btracker.crunchbanglinux.org
- DNS Standard query Ox2943  A tracker1.wasabi1.com.tw
- DNS Standard query Oxae4d  A tracker.rwps.ws
- DNS Standard query Ox6b4c  A tracker.ccc.de

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>TCP Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>278630</td>
<td>191.901</td>
<td>19.8215870000</td>
</tr>
<tr>
<td>278309</td>
<td>191.754</td>
<td>19.6895910000</td>
</tr>
<tr>
<td>278143</td>
<td>191.678</td>
<td>19.5810390000</td>
</tr>
<tr>
<td>278151</td>
<td>191.682</td>
<td>19.5750950000</td>
</tr>
<tr>
<td>278151</td>
<td>191.666</td>
<td>19.5549240000</td>
</tr>
<tr>
<td>277988</td>
<td>191.625</td>
<td>19.5347620000</td>
</tr>
<tr>
<td>277805</td>
<td>191.525</td>
<td>19.3828420000</td>
</tr>
<tr>
<td>277185</td>
<td>191.244</td>
<td>19.1369070000</td>
</tr>
<tr>
<td>276868</td>
<td>191.103</td>
<td>19.0027150000</td>
</tr>
<tr>
<td>257247</td>
<td>166.221</td>
<td>18.8600830000</td>
</tr>
</tbody>
</table>
### Wireshark Graph: SluggishDownload.pcapng

#### Graphs
- **Graph 1**: Color bar, Filter: Calc:SUM(*)
- **Graph 2**: Color bar, Filter: Calc:MAX(*)
- **Graph 3**: Color bar, Filter: Calc:SUM(*)
- **Graph 4**: Color bar, Filter: Calc:SUM(*)
- **Graph 5**: Color bar, Filter: Calc:SUM(*)

#### X-Axis
- Tick interval: 1 sec
- Pixels per tick: 5
- View as time of day: unchecked

#### Y-Axis
- Units: Advanced...
- Scale: Auto
- Smooth: No filter

### Packet Filter Details
- **Filter**: tcp.flags.syn==1 & tcp.flags.ack==0

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Src Port</th>
<th>Dst Port</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1563</td>
<td>80</td>
<td>cadabra-lm [SYN] Seq=x0 Len=0</td>
</tr>
<tr>
<td>2</td>
<td>0.000873</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1564</td>
<td>80</td>
<td>pay-per-view [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
<tr>
<td>3</td>
<td>0.001093</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1565</td>
<td>80</td>
<td>windflb-http [SYN] Seq=x0 Len=0</td>
</tr>
<tr>
<td>4</td>
<td>0.001283</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1566</td>
<td>80</td>
<td>corevideo-http [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
<tr>
<td>5</td>
<td>0.001466</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1567</td>
<td>80</td>
<td>etscored-http [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
<tr>
<td>6</td>
<td>0.001645</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1568</td>
<td>80</td>
<td>ets-http [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
<tr>
<td>7</td>
<td>0.001822</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1569</td>
<td>80</td>
<td>orakld-http [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
<tr>
<td>8</td>
<td>0.002000</td>
<td>10.10.10.10</td>
<td>192.168.10.103</td>
<td>TCP</td>
<td>1570</td>
<td>80</td>
<td>orakld-http [SYN] Seq=x0 Win=512 Len=0</td>
</tr>
</tbody>
</table>