



Hands-on Network Traffic Analysis

2015 Cyber Defense Boot Camp



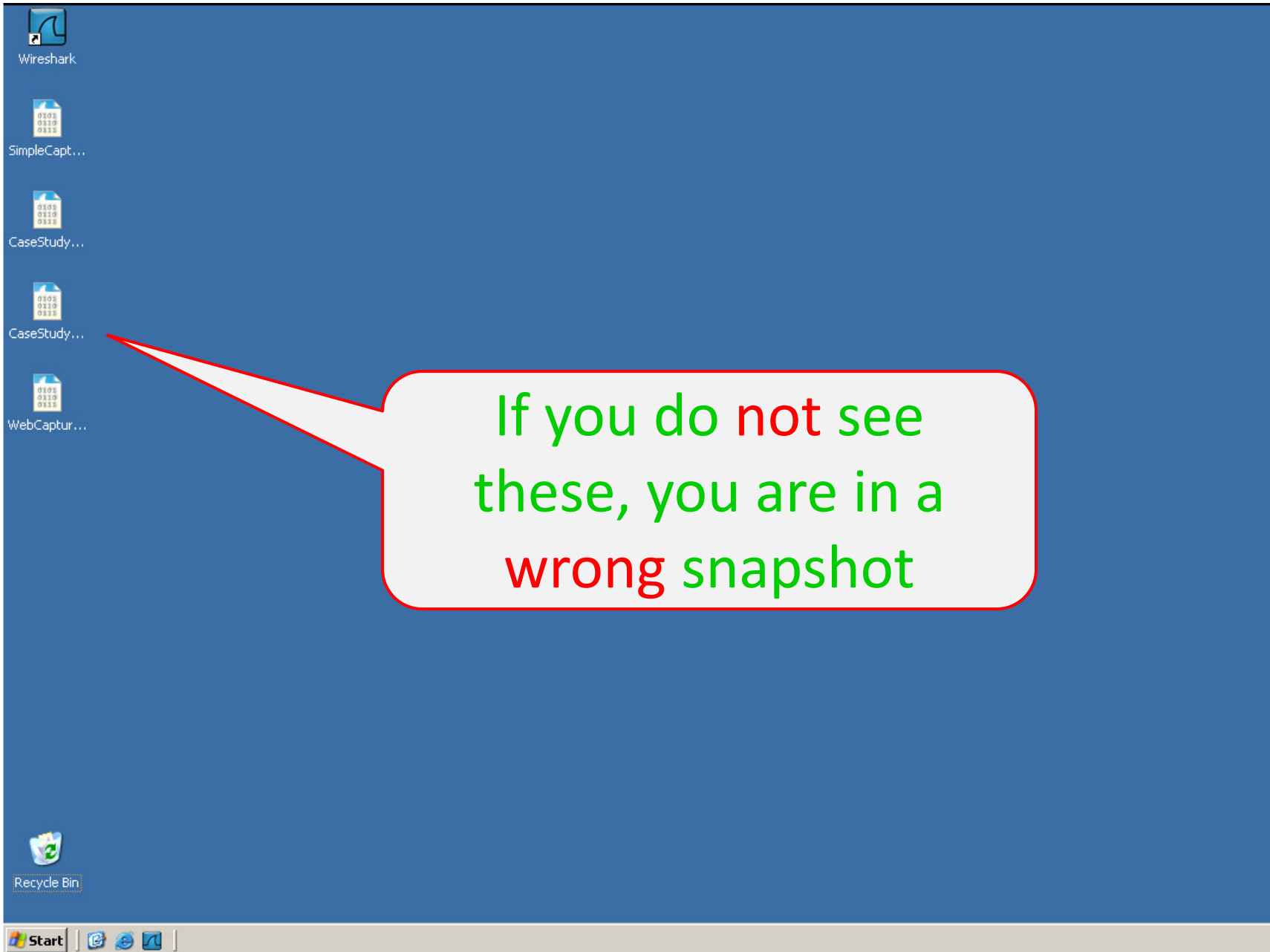
What is this about?

- Prerequisite: network packet & packet analyzer: (header, data)
 - Enveloped letters inside another envelope
- Exercises
 - ① Basic network traffic analysis
 - SimpleCapture.pcap, WebCapture.pcap
 - ② Gather information and statistics
 - CaseStudy1.pcap, CaseStudy2.pcap
 - Traffic searches: protocol hierarchy, HTTP requests, conversations, filters; attack analysis

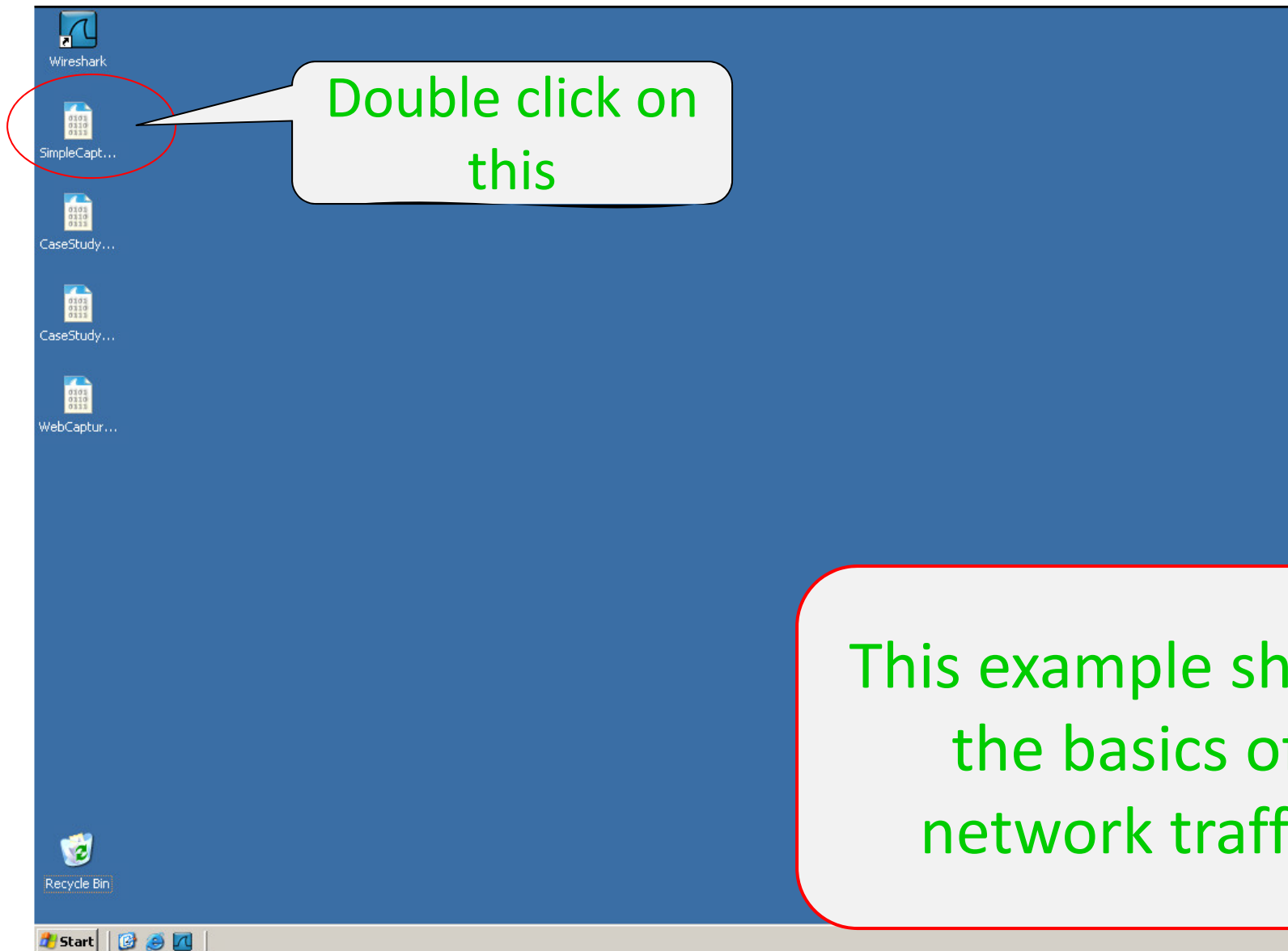


Step 0

- Go to your VM
- Select the “Network Sniffing Exercise” snapshot
- Log in as administrator
- Password: password



Exercise ①: Basic Network Analysis





One row,
one packet

SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | 0.00000000 | 192.168.78.254 | 192.168.78.253 | TPKT | 135 | Continuation |
| 2 | 0.12978800 | 192.168.78.253 | 192.168.78.254 | TPKT | 5298 | Continuation |
| 3 | 0.13128700 | 192.168.78.254 | 192.168.78.253 | TPKT | 142 | Continuation |
| 4 | 0.13137000 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112->3389 [ACK] Seq=146 Ack=4069 win=65427 Len=0 TSval=1138360336 TSecr=167390902 |
| 5 | 0.13141800 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112->3389 [ACK] Seq=146 Ack=5233 win=65281 Len=0 TSval=1138360336 TSecr=167390902 |
| 6 | 0.14187600 | 192.168.78.253 | 192.168.78.254 | TPKT | 3455 | Continuation |
| 7 | 0.14331700 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112->3389 [ACK] Seq=146 Ack=7945 win=65257 Len=0 TSval=1138360348 TSecr=167390903 |
| 8 | 0.14338600 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112->3389 [ACK] Seq=146 Ack=8622 win=65172 Len=0 TSval=1138360348 TSecr=167390903 |
| 9 | 0.23380300 | 192.168.78.254 | 192.168.78.253 | TPKT | 142 | Continuation |
| 10 | 0.24347600 | 192.168.78.253 | 192.168.78.254 | TPKT | 125 | Continuation |
| 11 | 0.24458000 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112->3389 [ACK] Seq=222 Ack=8681 win=65535 Len=0 TSval=1138360447 TSecr=167390913 |
| 12 | 0.38473600 | 192.168.78.254 | 192.168.78.253 | TPKT | 135 | Continuation |
| 13 | 0.57743900 | 192.168.78.253 | 192.168.78.254 | TCP | 66 | 3389->55112 [ACK] Seq=8681 Ack=291 win=258 Len=0 TSval=167390947 TSecr=1138360585 |
| 14 | 0.57847700 | 192.168.78.254 | 192.168.78.253 | TPKT | 142 | Continuation |
| 15 | 0.77842600 | 192.168.78.253 | 192.168.78.254 | TCP | 66 | 3389->55112 [ACK] Seq=8681 Ack=367 win=258 Len=0 TSval=167390967 TSecr=1138360777 |
| 16 | 0.77931300 | 192.168.78.254 | 192.168.78.253 | TPKT | 142 | Continuation |
| 17 | 0.90972900 | 192.168.78.253 | 192.168.78.254 | TPKT | 3578 | Continuation |
| 18 | 0.91111400 | 192.168.78.254 | 192.168.78.253 | TPKT | 128 | Continuation |

Frame 1: 135 bytes on wire (1080 bits), 135 bytes captured (1080 bits) on interface 0

Ethernet II, Src: DellInc_f5:27:7d (00:15:c5:f5:27:7d), Dst: Dell_3f:a6:37 (f0:4d:a2:3f:a6:37)

Internet Protocol Version 4, Src: 192.168.78.254 (192.168.78.254), Dst: 192.168.78.253 (192.168.78.253)

Transmission Control Protocol, Src Port: 55112 (55112), Dst Port: 3389 (3389), Seq: 1, Ack: 1, Len: 69

TPKT

0000 f0 4d a2 3f a6 37 00 15 c5 f5 27 7d 08 00 45 00 .M.?.. }..E.
0010 00 79 46 1a 40 00 3f 06 d6 18 c0 a8 4e fe c0 a8 .yF.@.?..N..
0020 4e fd d7 48 0d 3d 99 8d 22 0c 6e 19 89 f3 80 18 N..H.=..n....
0030 ff ff a5 e1 00 00 01 01 08 0a 43 d9 ff 8e 09 faC.....
0040 2e a0 17 03 01 00 40 46 16 80 2c 01 bf ae 4e 4b@F.....NK
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
File: "C:\tmp\Boot-capture\SimpleCapture...." Packets: 10730 · Displayed: 10730 (100.0%) · Load time: 0:00.131 Profile: Default

Inside the current
(i.e. **first**) packet

The data of the current (i.e. **first**) packet



SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|------------|----------------|----------------|----------|--------|--|
| 288 | 9.04231200 | 192.168.78.254 | 192.168.78.253 | IPK1 | 135 | Continuation |
| 289 | 9.84078700 | 192.168.78.253 | 192.168.78.254 | TCP | 66 | 3389→55112 [ACK] Seq=258702 Ack=2678 win=255 Len=0 TSval=16 |
| 290 | 9.84167600 | 192.168.78.254 | 192.168.78.253 | TPKT | 135 | Continuation |
| 291 | 9.84228500 | 192.168.78.253 | 192.168.78.254 | | | |
| 292 | 9.84324700 | 192.168.78.254 | 192.168.78.253 | | | |
| 293 | 9.86967100 | Cisco_b0:71:c1 | Spanning-tree | | | in=65535 Len=0 TSval=16 |
| 294 | 9.87551600 | 192.168.78.254 | 192.168.78.253 | | | Cost = 0 Port = 0x1 |
| 295 | 10.0707870 | 192.168.78.253 | 192.168.78.254 | | | in=254 Len=0 TSval=16 |
| 296 | 10.1020990 | 192.168.78.254 | 192.168.78.253 | TPKT | 107 | Continuation |
| 297 | 10.1118610 | 192.168.78.253 | 192.168.78.254 | | 125 | Continuation |
| 298 | 10.1128190 | 192.168.78.254 | 192.168.78.253 | | 66 | 55112→3389 [ACK] Seq=2864 Ack=258794 win=65535 Len=0 TSval=16 |
| 299 | 10.1218180 | 192.168.78.253 | 192.168.78.254 | | 119 | Continuation |
| 300 | 10.1228750 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2864 Ack=258847 win=65535 Len=0 TSval=16 |
| 301 | 10.2319140 | 192.168.78.253 | 192.168.78.254 | TPKT | 597 | Continuation |
| 302 | 10.2331550 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2864 Ack=259378 win=65530 Len=0 TSval=16 |
| 303 | 10.3018040 | 192.168.78.254 | 192.168.78.253 | TPKT | 100 | Continuation |
| 304 | 10.3086210 | 192.168.78.253 | 192.168.78.254 | DNS | 74 | Standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.168.78.253 | DNS | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.228.114 |

Click on packet 304

Right click

Frame 304: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on 0

Ethernet II, Src: Dell_3f:a6:37 (f0:4d:a2:3f:a6:37), Dst: Dellinc_f5:27:7d (f5:27:7d)

Internet Protocol Version 4, Src: 192.168.78.253 (192.168.78.253), Dst: 192.168.78.254 (192.168.78.254)

User Datagram Protocol, Src Port: 50187 (50187), Dst Port: 53 (53)

Domain Name System (query)

```
0000  00 15 c5 f5 27 7d f0 4d a2 3f a6 37 08 00 45 00  ....}.M.?.7..E.
0010  00 3c 1e 2e 00 00 80 11 00 00 c0 a8 4e fd c0 a8  .<.....N...
0020  4e fe c4 0b 00 35 00 28 1f 86 15 e6 01 00 00 01  N....5.( .....
0030  00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c  .....w ww.googl
0040  65 03 63 6f 6d 00 00 01 00 01  e.com... ..
```

File: "C:\tmp\Boot-capture\SimpleCapture...." Packets: 10730 · Displayed: 10730 (100.0%) · Load time: 0:00.385 Profile: Default



SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|------------|----------------|------------------------|----------|--------|---|
| 288 | 9.04231200 | 192.168.78.254 | 192.168.78.253 | TPKT | 135 | Continuation |
| 289 | 9.84078700 | 192.168.78.253 | 192.168.78.254 | TCP | 66 | 3389→55112 [ACK] Seq=258702 Ack=2678 win=255 Len=0 TSval=16 |
| 290 | 9.84167600 | 192.168.78.254 | 192.168.78.253 | TPKT | 135 | Continuation |
| 291 | 9.84228500 | 192.168.78.253 | 192.168.78.254 | TPKT | 99 | Continuation |
| 292 | 9.84324700 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2747 Ack=258735 win=65535 Len=0 TSval= |
| 293 | 9.86967100 | cisco_b0:71:c1 | Spanning-tree-(for-STP | | 60 | Conf. Root = 32768/0/00:23:eb:b0:71:bf Cost = 0 Port = 0x1 |
| 294 | 9.87551600 | 192.168.78.254 | 192.168.78.253 | TPKT | 142 | Continuation |
| 295 | 10.0707870 | 192.168.78.253 | 192.168.78.254 | TCP | 66 | 3389→55112 [ACK] Seq=258735 Ack=2823 win=254 Len=0 TSval=16 |
| 296 | 10.1020990 | 192.168.78.254 | 192.168.78.253 | TPKT | 107 | Continuation |
| 297 | 10.1118610 | 192.168.78.253 | 192.168.78.254 | TPKT | 125 | Continuation |
| 298 | 10.1128190 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2864 Ack=258794 win=65535 Len=0 TSval= |
| 299 | 10.1218180 | 192.168.78.253 | 192.168.78.254 | TPKT | 119 | Continuation |
| 300 | 10.1228750 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2864 Ack=258847 win=65535 Len=0 TSval= |
| 301 | 10.2319140 | 192.168.78.253 | 192.168.78.254 | TPKT | 597 | Continuation |
| 302 | 10.2331550 | 192.168.78.254 | 192.168.78.253 | TCP | 66 | 55112→3389 [ACK] Seq=2864 Ack=259378 win=65530 Len=0 TSval= |
| 303 | 10.3018040 | 192.168.78.254 | 192.168.78.253 | TPKT | 100 | Continuation |
| 304 | 10.3086210 | 192.168.78.253 | 192.16 | | 74 | Standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.16 | | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.2 |

Frame 304: 74 bytes on wire (592 bits), 7
Ethernet II, Src: Dell_3f:a6:37 (f0:4d:a2
Internet Protocol Version 4, Src: 192.168
User Datagram Protocol, Src Port: 50187
Domain Name System (query)

0000 00 15 c5 f5 27 7d f0 4d a2 3f a6 37
0010 00 3c 1e 2e 00 00 80 11 00 00 c0 a8
0020 4e fe c4 0b 00 35 00 28 1f 86 15 e6
0030 00 00 00 00 00 00 03 77 77 77 06 67
0040 65 03 63 6f 6d 00 00 01 00 01

File: "C:\tmp\Boot-capture\SimpleCapture...." Packets: 1

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream

74 Standard query 0x15e6 A www.google.com
290 Standard query response 0x15e6 A 74.125.228.114 A 74.125.2
on interface 0
27:7d (00:15:c5:f5:27:7d)
t: 192.168.78.254 (192.168.78.254)

② Choose this

me: 0:00.385 Profile: Default



SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 192.168.1.108 and ip.addr eq 74.125.228.114)

Follow UDP Stream

Stream Content

```
.....www.google.com.....www.google.com.....J}.  
r.....J}.s.....J}.t.....J}.p.....J}.q.....ns  
3.....ns2.....ns1.....ns4.....h...  
.....h..."  
.....h...$  
.....h...&
```

Entire conversation (280 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays **Raw**

Help Filter Out This Stream **Close**

File: "C:\tmp\Boot-capture\SimpleCapture.pcapng" Packets: 10750 • Displayed: 2 (0.0%) • Load time: 0:00:140 Profile: Default

SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port ... Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 304 | 10.3086210 | 192.168.78.253 | 192.168.78.254 | DNS | 74 | Standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.168.78.253 | DNS | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.228.115 A 74.125.228.116 A 74.125.228.117 |

Click on the first packet to make it the current packet

Frame 304: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

- Ethernet II, Src: Dell_3f:a6:37 (f0:4d:a2:3f:a6:37), Dst: DellInc_f5:27:7d (00:15:c5:f5:27:7d)
- Internet Protocol Version 4, Src: 192.168.78.253 (192.168.78.253), Dst: 192.168.78.254 (192.168.78.254)
- User Datagram Protocol, Src Port: 50187 (50187), Dst Port: 53 (53)
- Domain Name System (query)
 - [Response in: 305]
 - Transaction ID: 0x15e6
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.google.com: type A, class IN
 - Name: www.google.com
 - [Name Length: 14]
 - [Label Count: 3]
 - Type: A (Host Address) (1)
 - Class: IN (0x0001)

The details of the current packet:
This is a DNS query for the IP address of www.google.com

0000 00 15 c5 f5 27 7d f0 4d a2 3f a6 37 08 00 45 00 ...}.M.?..E.
 0010 00 3c 1e 2e 00 00 80 11 00 00 c0 a8 4e fd c0 a8 <.....N..
 0020 4e fe c4 0b 00 35 00 28 1f 86 15 e6 01 00 00 01 N...5.(.....
 0030 00 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6cw ww.goog
 0040 65 03 63 6f 6d 00 00 01 00 01 e.com.....

Data of the current packet

Frame (frame), 74 bytes Packets: 10730 · Displayed: 2 (0.0%) · Load time: 0:00.146



SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port ... Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 304 | 10.3086210 | 192.168.78.253 | 192.168.78.254 | DNS | 74 | Standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.168.78.253 | DNS | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.228.115 A 74.125.228.116 A 74.125.228.112 |

Click on the second packet

Frame 305: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface 0
Ethernet II, Src: DellInc_f5:27:7d (00:15:c5:f5:27:7d), Dst: Dell_3f:a6:37 (f0:4d:a2:3f:a6:37)
Internet Protocol Version 4, Src: 192.168.78.254 (192.168.78.254), Dst: 192.168.78.253 (192.168.78.253)
User Datagram Protocol, Src Port: 53 (53), Dst Port: 50187 (50187)
Domain Name System (response)
[Request In: 304]
[Time: 0.000375000 seconds]
Transaction ID: 0x15e6
Flags: 0x8180 Standard query response, No error
Questions: 1
Answer RRs: 5
Authority RRs: 4
Additional RRs: 4
Queries
www.google.com: type A, class IN
Name: www.google.com
[Name Length: 14]
[Label Count: 3]
Type: A (Host Address) (1)
Class: IN (0x0001)
Answers
www.google.com: type A, class IN, addr 74.125.228.114
www.google.com: type A, class IN, addr 74.125.228.115
www.google.com: type A, class IN, addr 74.125.228.116
www.google.com: type A, class IN, addr 74.125.228.112

The details of the current packet:
Response to the DNS query

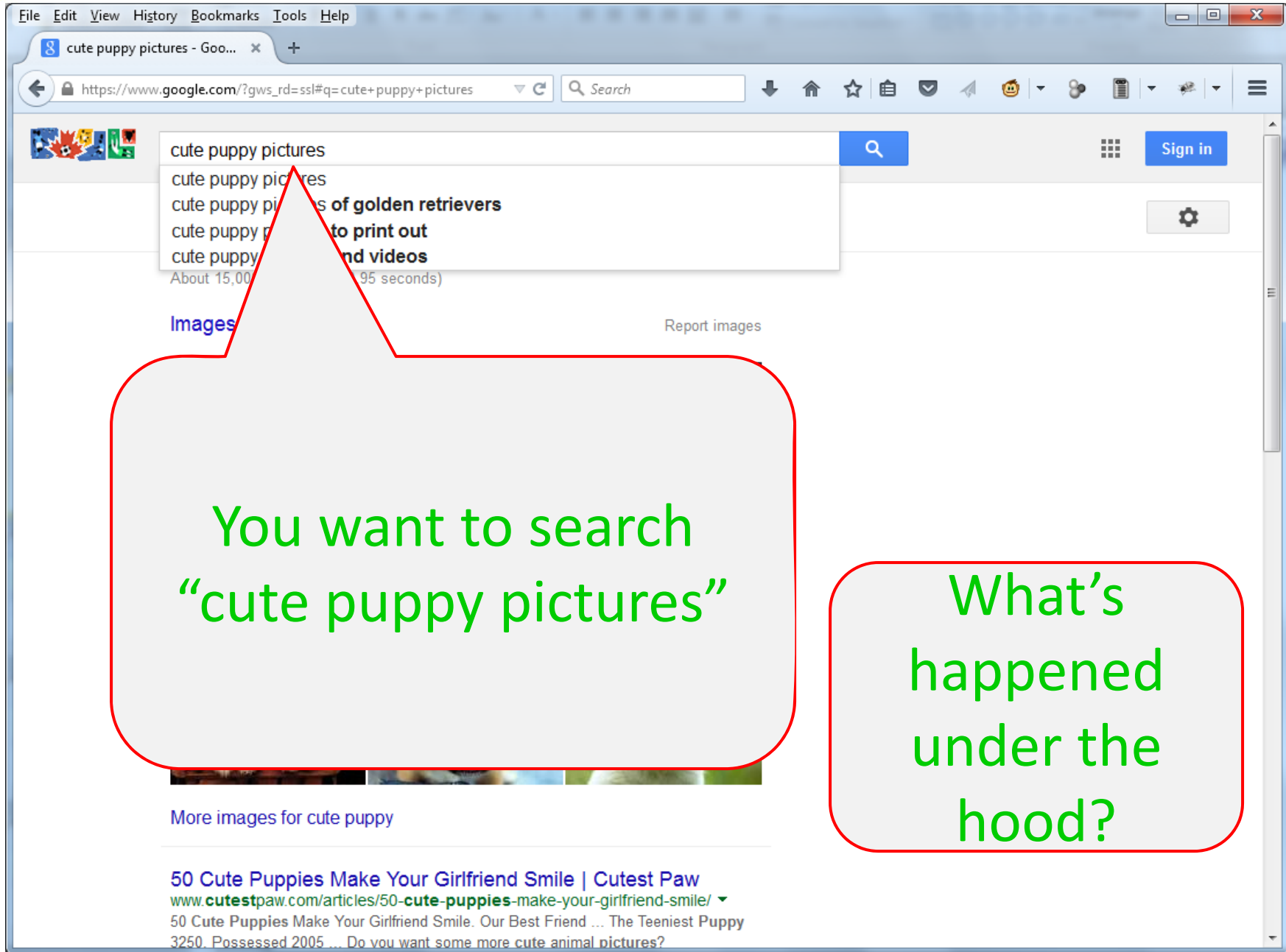
Data of the current packet

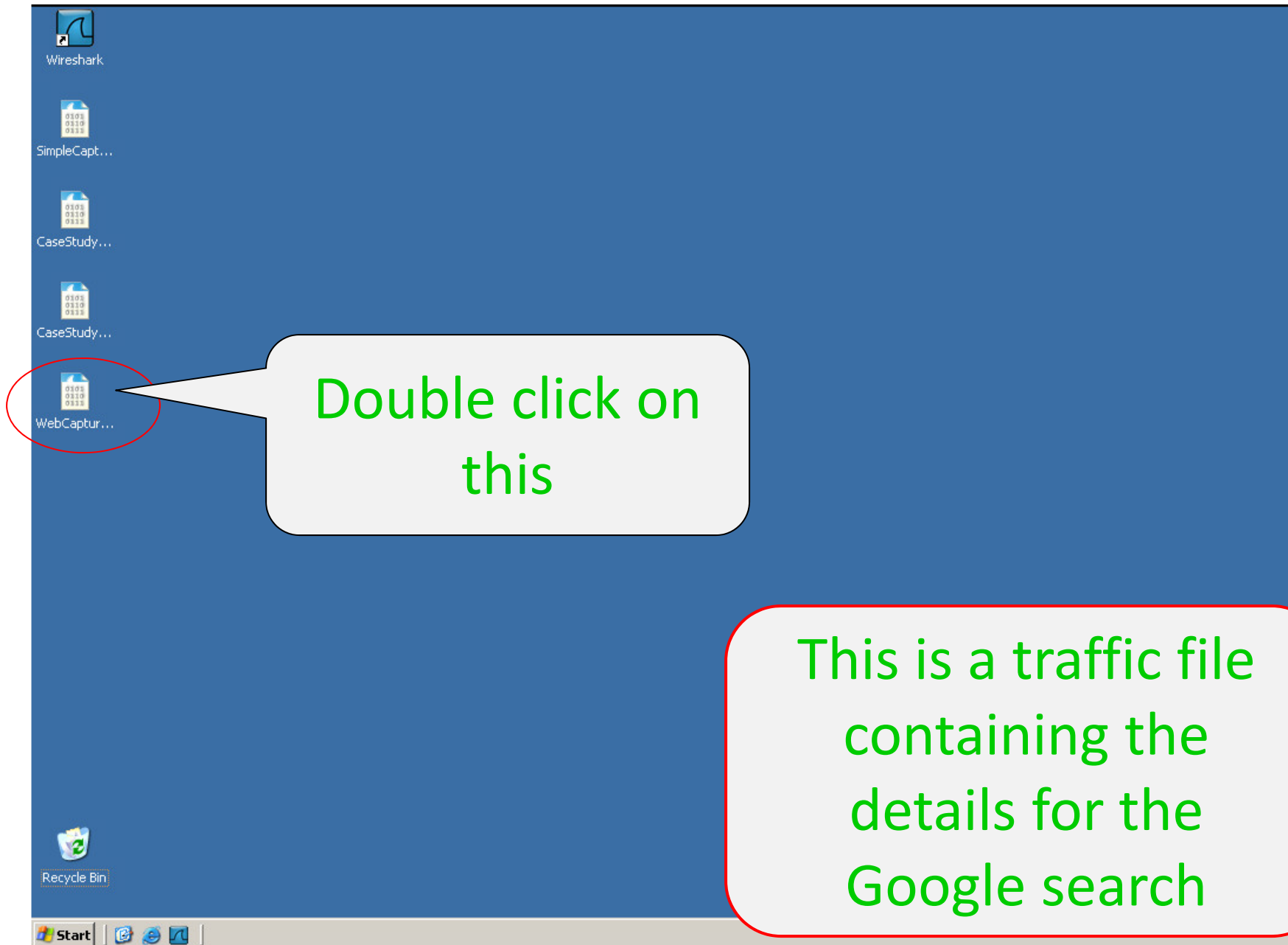
0000 f0 4d a2 3f a6 37 00 15 c5 f5 27 7d 08 00 45 00 .M.?..}..E.
0010 01 14 98 81 00 00 40 11 c2 0b c0 a8 4e fe c0 a8@...N..
0020 4e fd 00 35 c4 0b 01 00 d2 c7 15 e6 81 80 00 01 N..5.....
0030 00 05 00 04 00 04 03 77 77 77 06 67 6f 6f 67 6cw ww.goog
0040 65 03 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 e.com.....
0050 00 00 00 db 00 04 43 7d e4 72 c0 0f 00 01 00 01

Frame (frame), 290 bytes Packets: 10730 · Displayed: 2 (0.0%) · Load time: 0:00.146



So far, so good?







WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | 172.16.107.130 | 173.194.73.99 | TCP | 62 | 1190→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 0.038550 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 3 | 0.038564 | 172.16.107.130 | 173.194.73.99 | TCP | 54 | 1190→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 4 | 0.038844 | 172.16.107.130 | 173.194.73.99 | HTTP | 770 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHWQFjAT&url=http%3A%2F%2Fpinterest.co |
| 5 | 0.039059 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 6 | 0.079812 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK (text/html) |
| 7 | 0.109039 | 172.16.107.130 | 172.16.107.2 | DNS | 72 | Standard query 0 |
| 8 | 0.112534 | 172.16.107.130 | 173.194.73.99 | HTTP | 564 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHWQFjAT&url=http%3A%2F%2Fpinterest.co |
| 9 | 0.113491 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 10 | 0.152446 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK (text/html) |
| 11 | 0.152468 | 172.16.107.2 | 172.16.107.130 | DNS | 290 | Standard query response 0 |
| 12 | 0.155694 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1191→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 13 | 0.156416 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1192→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 14 | 0.167974 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1191 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 15 | 0.167983 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 16 | 0.168017 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1192 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 17 | 0.168022 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1192→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 18 | 0.168186 | 172.16.107.130 | 174.129.239.78 | HTTP | 621 | GET /racheloftherose/funny-puppy-pictures/ HTTP/1.1 |

Click on the first packet

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface 0
Ethernet II, Src: Vmware_4c:78:f3 (00:0c:29:4c:78:f3), Dst: Vmware_f9:f7:86 (00:50:56:f9:f7:86)
Internet Protocol Version 4, Src: 172.16.107.130 (172.16.107.130), Dst: 173.194.73.99 (173.194.73.99)
Transmission Control Protocol, Src Port: 1190 (1190), Dst Port: 80 (80), Seq: 0, Len: 0

Source Port: 1190 (1190)
Destination Port: 80 (80)
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 28 bytes

... 0000 0000 0010 = 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
.... 0... = Syn: Set

[Expert Info (Chat/Sequence): Connection establish request (SYN): server port 80]
[Connection establish request (SYN): server port 80]
[Severity level: Chat]

In the current packet: SYN is set

0000 00 50 56 f9 f7 86 00 0c 29 4c 78 f3 08 00 45 00 .PV....)Lx...E.
0010 00 30 57 c9 40 00 80 06 00 00 ac 10 6b 82 ad c2 .Ow.@... ..k...
0020 49 63 04 a6 00 50 dc ff 16 3e 00 00 00 70 02 Ic...P... >....p.
0030 fa f0 81 42 00 00 02 04 05 b4 01 01 04 02 ...B.....

Packets: 2038 · Displayed: 2038 (100.0%) · Load time: 0:00.028



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | 172.16.107.130 | 173.194.73.99 | TCP | 62 | 1190→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 0.038550 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 3 | 0.038564 | 172.16.107.130 | 173.194.73.99 | TCP | 54 | 1190→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 4 | 0.038844 | 172.16.107.130 | 173.194.73.99 | HTTP | 770 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.cc |
| 5 | 0.039059 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 6 | 0.079812 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK |
| 7 | 0.109039 | 172.16.107.130 | 172.16.107.2 | DNS | 73 | Standard query |
| 8 | 0.112534 | 172.16.107.130 | 173.194.73.99 | HTTP | 564 | GET / |
| 9 | 0.113491 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 10 | 0.152446 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK |
| 11 | 0.152468 | 172.16.107.2 | 172.16.107.130 | DNS | 290 | Standard query |
| 12 | 0.155694 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1191→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 13 | 0.156416 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1192→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 14 | 0.167974 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1191 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 15 | 0.167983 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 16 | 0.168017 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1192 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 17 | 0.168022 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1192→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 18 | 0.168186 | 172.16.107.130 | 174.129.239.78 | HTTP | 621 | GET /racheloftherose/funny-puppy-pictures/ HTTP/1.1 |

Click on the second packet

In the current packet: both ACK and SYN are set

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_f9:f7:86 (00:50:56:f9:f7:86), Dst: Vmware_4c:78:f3 (00:0c:29:4c:78:f3)

Internet Protocol Version 4, Src: 173.194.73.99 (173.194.73.99), Dst: 172.16.107.130 (172.16.107.130)

Transmission Control Protocol, Src Port: 80 (80), Dst Port: 1190 (1190), Seq: 0, Ack: 1, Len: 0

Source Port: 80 (80)

Destination Port: 1190 (1190)

[Stream index: 0]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 1 (relative ack number)

Header Length: 24 bytes

... 0000 0001 0010 = Flags: 0x012 (SYN, ACK)

000. = Reserved: Not set

...0 = Nonce: Not set

.... 0... = Congestion Window Reduced (CWR): Not set

.... .0.. = ECN-Echo: Not set

.... ..0. = Urgent: Not set

.... ...1 = Acknowledgment: Set

....0... = Push: Not set

....0. = Reset: Not set

....1. = Syn: Set

[Expert Info (Chat/Sequence): Connection establish acknowledge (SYN+ACK): server port 80]

[Connection establish acknowledge (SYN+ACK): server port 80]

[Severity level: chat]

0000 00 0c 29 4c 78 f3 00 50 56 f9 f7 86 08 00 45 00 ..)Lx..P V....E.

0010 00 2c a3 07 00 00 80 06 89 0c ad c2 49 63 ac 10IC..

0020 6b 82 00 50 04 a6 c7 e7 4c 84 dc ff 16 3f 60 12 k..P....L....?

0030 fa f0 81 cc 00 00 02 04 05 b4 00 00

Acknowledgment (tcp.flags.ack), 1 byte

Packets: 2038 · Displayed: 2038 (100.0%) · Load time: 0:00.028

Profile: Default



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | 172.16.107.130 | 173.194.73.99 | TCP | 62 | 1190→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 0.038550 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 3 | 0.038564 | 172.16.107.130 | 173.194.73.99 | TCP | 54 | 1190→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 4 | 0.038844 | 172.16.107.130 | 173.194.73.99 | HTTP | 770 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.co |
| 5 | 0.039059 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 6 | 0.079812 | 173.194.73.99 | 172.16.107.130 | HTTP | 645 | HTTP/1.1 200 OK (text/html) |
| 7 | 0.109039 | 172.16.107.130 | 172.16.107.2 | DNS | | Standard query |
| 8 | 0.112534 | 172.16.107.130 | 173.194.73.99 | HTTP | | Standard query |
| 9 | 0.113491 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 10 | 0.152446 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK (text/html) |
| 11 | 0.152468 | 172.16.107.2 | 172.16.107.130 | DNS | 290 | Standard query |
| 12 | 0.155694 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1191→80 [SYN] |
| 13 | 0.156416 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1192→80 [SYN] |
| 14 | 0.167974 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1191 [SYN] |
| 15 | 0.167983 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] |
| 16 | 0.168017 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1192 [SYN] |
| 17 | 0.168022 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1192→80 [ACK] |
| 18 | 0.168186 | 172.16.107.130 | 174.129.239.78 | HTTP | 621 | GET /racheloftherose/funny-puppy-pictures/ HTTP/1.1 |

Click on the third packet

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)

Ethernet II, Src: Vmware_4c:78:f3 (00:0c:29:4c:78:f3), Dst: Vmware_f9:f7:86 (00:50:56:f9:f7:86)

Internet Protocol Version 4, Src: 172.16.107.130 (172.16.107.130), Dst: 173.194.73.99 (173.194.73.99)

Transmission Control Protocol, Src Port: 1190 (1190), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 0

Source Port: 1190 (1190)
Destination Port: 80 (80)
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes

.... 0000 0001 0000 = Flags: 0x010 (ACK)
000. = Reserved: Not set
...0 = Nonce: Not set
.... 0... = Congestion window Reduced (CWR): Not set
.... .0.. = ECN-Echo: Not set
.... ..0. = Urgent: Not set
.... ...1 = Acknowledgment: Set

In the current packet: the ACK is set

What does this mean? Three wasted packets?
Your browser did a lot before your search keyword is sent to Google



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | 172.16.107.130 | 173.194.73.99 | TCP | 62 | 1190→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 2 | 0.038550 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 3 | 0.038564 | 172.16.107.130 | 173.194.73.99 | TCP | 54 | 1190→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 4 | 0.038844 | 172.16.107.130 | 173.194.73.99 | HTTP | 770 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.co |
| 5 | 0.039059 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 6 | 0.079812 | 173.194.73.99 | 172.16.107.130 | HTTP | 15 | HTTP/1.1 200 OK (text/html) |
| 7 | 0.109039 | 172.16.107.130 | 172.16.107.2 | DNS | 74 | Standard query |
| 8 | 0.112534 | 172.16.107.130 | 173.194.73.99 | HTTP | 564 | GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.co |
| 9 | 0.113491 | 173.194.73.99 | 172.16.107.130 | TCP | 60 | 80→1190 [ACK] Seq=1 Ack=717 win=64240 Len=0 |
| 10 | 0.152446 | 173.194.73.99 | 172.16.107.130 | HTTP | 1406 | HTTP/1.1 200 OK (text/html) |
| 11 | 0.152468 | 172.16.107.2 | 172.16.107.130 | DNS | 290 | Standard query response |
| 12 | 0.155694 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1191→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 13 | 0.156416 | 172.16.107.130 | 174.129.239.78 | TCP | 62 | 1192→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 14 | 0.167974 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1191 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 15 | 0.167983 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 16 | 0.168017 | 174.129.239.78 | 172.16.107.130 | TCP | 60 | 80→1192 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 17 | 0.168022 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1192→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 18 | 0.168186 | 172.16.107.130 | 174.129.239.78 | HTTP | 621 | GET /racheloftherose/funny-puppy-pictures/ HTTP/1.1 |

Click on the fourth packet

Header Length: 20 bytes
... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 64240
[calculated window size: 64240]
[window size scaling factor: -2 (no window scaling used)]
Checksum: 0x119f [validation disabled]
[Good Checksum: False]
[Bad Checksum: False]
Urgent pointer: 0
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.com
Host: www.google.com\r\n
User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:21.0) Gecko/20100101 Firefox/21.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Cookie: PREF=ID=3b7a6867adaf8522:TM=1370363771:LM=1370363771
Connection: keep-alive\r\n
Full request URI [truncated]: http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.com
[HTTP request 1/3]
[Response in frame: 61]
[Next request in frame: 81]

This is your Google search request!
It is **NOT** the first packet

0000 00 50 56 f9 f7 86 00 0c 29 4c 78 f3 08 00 45 00 .PV....)Lx...E.
0010 02 f4 57 cb 40 00 80 06 00 00 ac 10 6b 82 ad c2 ..W.@... ..k...
0020 49 63 04 a6 00 50 dc ff 16 3f c7 e7 4c 85 50 18 Ic...P... ?...L.P.
0030 fa f0 11 9f 00 00 47 45 54 20 2f 75 72 6c 3f 73GE T /url?s
0040 61 3d 74 26 72 63 74 3d 6a 26 71 3d 26 65 73 72 a=t&rct= j&q=&esr
0050 62 2d 72 26 72 65 75 72 62 65 2d 77 65 62 26 62 s=s&source=web&c

Frame (frame), 770 bytes Packets: 2038 · Displayed: 2038 (100.0%) · Load time: 0:00.028 Profile: Default



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|----------|----------------|----------------|----------|--------|--|
| 26 | 0.391928 | 174.129.239.78 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 27 | 0.391930 | 174.129.239.78 | 172.16.107.130 | TCP | 1478 | [TCP segment of a reassembled PDU] |
| 28 | 0.391937 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=568 Ack=5793 win=64240 Len=0 |
| 29 | 0.392163 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 30 | 0.392378 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 31 | 0.392387 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=568 Ack=5793 win=64240 Len=0 |
| 32 | 0.392520 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 33 | 0.392672 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 34 | 0.392699 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191→80 [ACK] Seq=568 Ack=5793 win=64240 Len=0 |
| 35 | 0.392730 | 174.129.239.78 | 172.16.107.130 | HTTP | 940 | HTTP/1.1 200 OK |
| 36 | 0.404601 | 172.16.107.130 | 172.16.107.2 | DNS | 84 | Standard query |
| 37 | 0.421443 | 172.16.107.130 | 172.16.107.2 | DNS | 84 | Standard query |
| 38 | 0.447314 | 172.16.107.2 | 172.16.107.130 | DNS | 228 | Standard query response |
| 39 | 0.447690 | 172.16.107.130 | 72.21.91.19 | TCP | 60 | 1193→80 [ACK] Seq=568 Ack=521 win=64240 Len=0 |
| 40 | 0.456766 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=521 win=64240 Len=0 |
| 41 | 0.456775 | 172.16.107.130 | 72.21.91.19 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=521 win=64240 Len=0 |
| 42 | 0.456908 | 172.16.107.130 | 72.21.91.19 | HTTP | 574 | GET /css/pinboard_63782886.css HTTP/1.1\r\nHost: passsets-ec.pinterest.com\r\n |
| 43 | 0.457044 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=521 win=64240 Len=0 |

Click on the 42th packet

① Right click on it

Frame 42: 574 bytes on wire (4592 bits), 574 bytes captured (4592 bits) on interface 0
Ethernet II, Src: Vmware_4c:78:f3 (00:0c:29:4c:78:f3), Dst: Vmware_f9:f7:86 (00:0c:29:4c:f9:f7:86)
Internet Protocol Version 4, Src: 172.16.107.130 (172.16.107.130), Dst: 72.21.91.19 (72.21.91.19)
Transmission Control Protocol, Src Port: 1193 (1193), Dst Port: 80 (80), Seq: 568 (568), Len: 520
Source Port: 1193 (1193)
Destination Port: 80 (80)
[Stream index: 3]
[TCP Segment Len: 520]
Sequence number: 1 (relative sequence number)
[Next sequence number: 521 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 20 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 64240
[Calculated window size: 64240]
[window size scaling factor: -2 (no window scaling used)]
Checksum: 0xbcd [validation disabled]
[Good checksum: False]
[Bad checksum: False]
Urgent pointer: 0
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /css/pinboard_63782886.css HTTP/1.1\r\nHost: passsets-ec.pinterest.com\r\n

0000 00 50 56 f9 f7 86 00 0c 29 4c 78 f3 08 00 45 00 .PV....)Lx...E.
0010 02 30 58 08 40 00 80 06 00 00 ac 10 6b 82 48 15 .0X.@... ..k.H.
0020 5b 13 04 a9 00 50 f5 16 72 86 6d 92 60 a7 50 18 [...P.. r.m..P.
0030 fa f0 bc dd 00 00 47 45 54 20 2f 63 73 73 2f 70GE T /css/p
0040 69 6e 62 6f 61 72 64 5f 36 33 37 38 32 38 38 36 inboard_ 63782886
0050 2a 62 72 72 20 48 54 54 50 2f 31 2a 21 0d 03 24 .css HTTP/1.1\r\n

File: "C:\tmp\Boot-capture\WebCapture.pcap" Packets: 2038 · Displayed: 2038 (100.0%) · Load time: 0:00.028 Profile: Default



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|----------|----------------|----------------|----------|--------|---|
| 26 | 0.391928 | 174.129.239.78 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 27 | 0.391930 | 174.129.239.78 | 172.16.107.130 | TCP | 1478 | [TCP segment of a reassembled PDU] |
| 28 | 0.391937 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191-80 [ACK] Seq=568 Ack=5793 win=64240 Len=0 |
| 29 | 0.392163 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 30 | 0.392378 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 31 | 0.392387 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191-80 [ACK] Seq=568 Ack=8689 win=64240 Len=0 |
| 32 | 0.392520 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 33 | 0.392672 | 174.129.239.78 | 172.16.107.130 | TCP | 1502 | [TCP segment of a reassembled PDU] |
| 34 | 0.392699 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191-80 [ACK] Seq=568 Ack=11585 win=64240 Len=0 |
| 35 | 0.392730 | 174.129.239.78 | 172.16.107.130 | HTTP | 940 | HTTP/1.1 200 OK (text/html) |
| 36 | 0.404601 | 172.16.107.130 | 172.16.107.2 | DNS | 84 | Standard query 0x95b3 A passsets-ec.pinterest.com |
| 37 | 0.421443 | 172.16.107.130 | 172.16.107.2 | DNS | 84 | Standard query 0x2a81 A passsets-ak.pinterest.com |
| 38 | 0.447314 | 172.16.107.2 | 172.16.107.130 | DNS | 228 | Standard query response 0x95b3 CNAME wac.7a97.edgecastcdn.net CNAME gs1.wac.edgecastcdn.net |
| 39 | 0.447690 | 172.16.107.130 | 72.21.91.19 | TCP | 62 | 1193-80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 40 | 0.456766 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80-1193 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 41 | 0.456775 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | 1193-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 42 | 0.456908 | 172.16.107.130 | 72.21.91.19 | HTTP | 574 | GET /css/pinboard_63782886.css HTTP/1.1 |
| 43 | 0.457044 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80-1193 [ACK] Seq=1 Ack=521 win=64240 Len=0 |

Frame 42: 574 bytes on wire (4592 bits)
Ethernet II, Src: Vmware_4c:78:f3 (00:0c:29:4c:78:f3), Dst: 72.21.91.19 (01:00:5e:f9:f7:86)
Internet Protocol Version 4, Src: 172.16.107.130, Dst: 72.21.91.19
Transmission Control Protocol, Src Port: 1193 (1193), Dst Port: 80 (80)
[Stream index: 3]
[TCP Segment Len: 520]
Sequence number: 1 (relative sequence number)
[Next sequence number: 521 (relative sequence number)]
Acknowledgment number: 1 (relative acknowledgment number)
Header Length: 20 bytes
... 0000 0001 1000 = Flags: 0x018 (PS)
window size value: 64240
[Calculated window size: 64240]
[window size scaling factor: -2 (no window scaling)]
Checksum: 0xbcd [validation disabled]
[Good Checksum: False]
[Bad Checksum: False]
Urgent pointer: 0
[SEQ/ACK analysis]
Hypertext Transfer Protocol
GET /css/pinboard_63782886.css HTTP/1.1
Host: passsets-ec.pinterest.com\r\n

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Protocol Preferences
Decode As...
Print...
Show Packet in New Window

② Choose this

0000 00 50 56 f9 f7 86 00 0c 29 4c 78 f3 08 00 45 00 .PV....)Lx...E.
0010 02 30 58 08 40 00 80 06 00 00 ac 10 6b 82 48 15 .Ox.@... ..k.H.
0020 5b 13 04 a9 00 50 f5 16 72 86 6d 92 60 a7 50 18 [....P.. r.m..P.
0030 fa f0 bc dd 00 00 47 45 54 20 2f 63 73 73 2f 70GE T /css/p
0040 69 6e 62 6f 61 72 64 5f 36 33 37 38 32 38 38 36 inboard_ 63782886
0050 2a 62 72 72 20 45 54 50 2f 31 2a 31 0d 03 48 ...css HTTP/1.1

File: "C:\tmp\Boot-capture\WebCapture.pcap" Packets: 2038 · Displayed: 2038 (100.0%) · Load time: 0:00.028 Profile: Default



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 3 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 39 | 0.447690 | 172.16.107.130 | 72.21.91.19 | TCP | 62 | 1193→80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 40 | 0.456766 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 41 | 0.456775 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | 1193→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 42 | 0.456908 | 172.16.107.130 | 72.21.91.19 | HTTP | 574 | GET /css/pinboard_63782886.css HTTP/1.1 |
| 43 | 0.457044 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 44 | 0.474208 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 45 | 0.474220 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 46 | 0.474222 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 47 | 0.474224 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 48 | 0.474226 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 49 | 0.474229 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 50 | 0.474231 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 51 | 0.474236 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 52 | 0.474238 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 53 | 0.474240 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | 80→1193 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 54 | 0.474247 | 172.16.107.130 | 72.21.91.19 | TCP | 60 | 1193→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 55 | 0.474323 | 172.16.107.130 | 72.21.91.19 | TCP | 60 | 1193→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 56 | 0.474361 | 172.16.107.130 | 72.21.91.19 | TCP | 60 | 1193→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |

Frame 42: 574 bytes on wire (4592 bits) captured on interface vmnic0 (0.474220 seconds) from 172.16.107.130 to 72.21.91.19

Ethernet II, Src: Vmware_4c:7e:48:3f, Dst: Vmware_00:0c:29:4c:78:f3

Internet Protocol Version 4, Src: 172.16.107.130, Destination: 72.21.91.19

Transmission Control Protocol, Src Port: 1193, Destination Port: 80

Source Port: 1193 (1193)

Destination Port: 80 (80)

[Stream index: 3]

[TCP Segment Len: 520]

Sequence number: 1 (related to 0.474220)

[Next sequence number: 521]

Acknowledgment number: 1

Header Length: 20 bytes

... 0000 0001 1000 = Flags

window size value: 64240

[calculated window size: 64240]

[window size scaling factor: 1]

Checksum: 0xbcd [validation: Good Checksum: False]

[Good Checksum: False]

[Bad Checksum: False]

urgent pointer: 0

[SEQ/ACK analysis]

Hypertext Transfer Protocol

GET /css/pinboard_63782886.css HTTP/1.1\r\n

Host: passsets-ec.pinterest.com\r\n

0000 00 50 56 f9 f7 86 00 0c 29 4c 78 f3 08 00 45 00 .PV....)Lx...E.

0010 02 30 58 08 40 00 80 06 00 00 ac 10 6b 82 48 15 .OX.@...k.H.

0020 5b 13 04 a9 00 50 f5 16 72 86 6d 92 60 a7 50 18 [...P...r.m..P.

0030 fa f0 bc dd 00 00 47 45 54 20 2f 63 73 73 2f 70GE T /css/p

0040 69 6e 62 6f 61 72 64 5f 36 33 37 38 32 38 38 36 inboard_ 63782886

0050 2f 63 73 73 2f 64 5f 36 33 37 38 32 38 38 36 /css/ HTTP/1.1

File: "C:\tmp\Boot-capture\WebCapture.pcap" Packets: 2038 · Displayed: 53 (2.6%) · Load time: 0:00:027 Profile: Default

Follow TCP Stream (tcp.stream eq 3)

Stream Content

GET /css/pinboard_63782886.css HTTP/1.1

Host: passsets-ec.pinterest.com

User-Agent: Mozilla/5.0 (Windows NT 5.2; rv:21.0) Gecko/20100101 Firefox/21.0

Accept: text/css,*/*;q=0.1

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Referer: http://pinterest.com/racheloftherose/funny-puppy-pictures/

Cookie: _pinterest_sess="eJZZk/AK86gIDTFNNSjTrypxLQ61zPETzYnISA21ty8vycxntfUN8TX2dfe18q1KN/JztLVVK04tLS5MsfXmisqIrPI19HfxLPCPTT1CwnkiQz3NPF1ca30dQmtBKO39XNXNI0KCTXTLE1BQCR/CMX"

Connection: keep-alive

HTTP/1.1 200 OK

Content-Encoding: gzip

Accept-Ranges: bytes

Cache-Control: max-age=31536000

Content-Type: text/css

Date: Tue, 04 Jun 2013 16:37:44 GMT

ETag: "f552890442cdc429e0ce01041b1ce4bd"

Expires: wed, 04 Jun 2014 16:37:44 GMT

Last-Modified: wed, 24 Apr 2013 18:01:32 GMT

Server: ECS (dca/2470)

Vary: Accept-Encoding

x-amz-id-2: oLATH3GeDDpIfHdwFRhi/3CrUeXOHBFVgyFNat+eLpCgWMZXXBSKhd4GJmxEQU

x-amz-request-id: 9233628493815D20

X-Cache: HIT

Content-Length: 28294

.....S+K..pinboard_63782886.css.....(...W.S..L{I.'...CUZ.1,+F...}.....Ip.R.....

+.*..[-v.=OK.&0.u ++.:l..F..l..o...h5l..<R..?....Mdf.....i..}w

Entire conversation (41435 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Filter Out This Stream Close



WebCapture.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: `!(tcp.stream eq 3)` Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|--|
| 38 | 0.447314 | 172.16.107.2 | 172.16.107.130 | DNS | 228 | Standard query response 0x95b3 CNAME wac.7a97.edgecastcdn.net CNAME gs1.wac.edgecastcdn.net |
| 70 | 0.488753 | 172.16.107.2 | 172.16.107.130 | DNS | 469 | Standard query response 0x2a81 CNAME passsets-ak.pinterest.com.edgesuite.net CNAME a1586.g |
| 71 | 0.492792 | 174.129.239.78 | 172.16.107.130 | TCP | 940 | [TCP Retransmission] 80-1191 [PSH, ACK] Seq=11585 Ack=568 win=64240 Len=886[reasassembly err |
| 72 | 0.492804 | 172.16.107.130 | 174.129.239.78 | TCP | 54 | 1191-80 [ACK] Seq=568 Ack=12471 win=63354 Len=0 |
| 73 | 0.493363 | 172.16.107.130 | 134.126.9.42 | TCP | 62 | 1194-80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 74 | 0.494121 | 172.16.107.130 | 134.126.9.42 | TCP | 62 | 1195-80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 75 | 0.494660 | 172.16.107.130 | 172.16.107.2 | DNS | 79 | Standard query 0xf84a A ajax.googleapis.com |
| 76 | 0.494919 | 172.16.107.130 | 134.126.9.42 | TCP | 62 | 1196-80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1 |
| 77 | 0.495311 | 134.126.9.42 | 172.16.107.130 | TCP | 60 | 80-1194 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 78 | 0.495318 | 172.16.107.130 | 134.126.9.42 | TCP | 54 | 1194-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 79 | 0.495873 | 134.126.9.42 | 172.16.107.130 | TCP | 60 | 80-1195 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 80 | 0.495880 | 172.16.107.130 | 134.126.9.42 | TCP | 54 | 1195-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 81 | 0.497596 | 134.126.9.42 | 172.16.107.130 | TCP | 60 | 80-1196 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460 |
| 82 | 0.497604 | 172.16.107.130 | 134.126.9.42 | TCP | 54 | 1196-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 83 | 0.498040 | 172.16.107.130 | 134.126.9.42 | HTTP | 559 | GET /js/bundle_pin_b779d4f2.js HTTP/1.1 |
| 84 | 0.500184 | 172.16.107.130 | 172.16.107.2 | DNS | 86 | Standard query 0xd73a A media-cache-ec0.pining.com |
| 85 | 0.500923 | 172.16.107.130 | 172.16.107.2 | DNS | 86 | Standard query 0xd96c A media-cache-ak0.pining.com |
| 86 | 0.502050 | 172.16.107.130 | 134.126.9.42 | HTTP | 543 | GET /images/favicon.png HTTP/1.1 |

Frame 38: 228 bytes on wire (1824 bits) (1824 bits captured) (1824 bits)

Ethernet II, Src: Vmware_f9:f7:86, Dst: Vmware_4c:78:f3 (00:0c:29:4c:78:f3)

Internet Protocol Version 4, Src: 172.16.107.2, Dst: 172.16.107.130 (172.16.107.130)

User Datagram Protocol, Src Port: 5452, Dst Port: 5452 (65452)

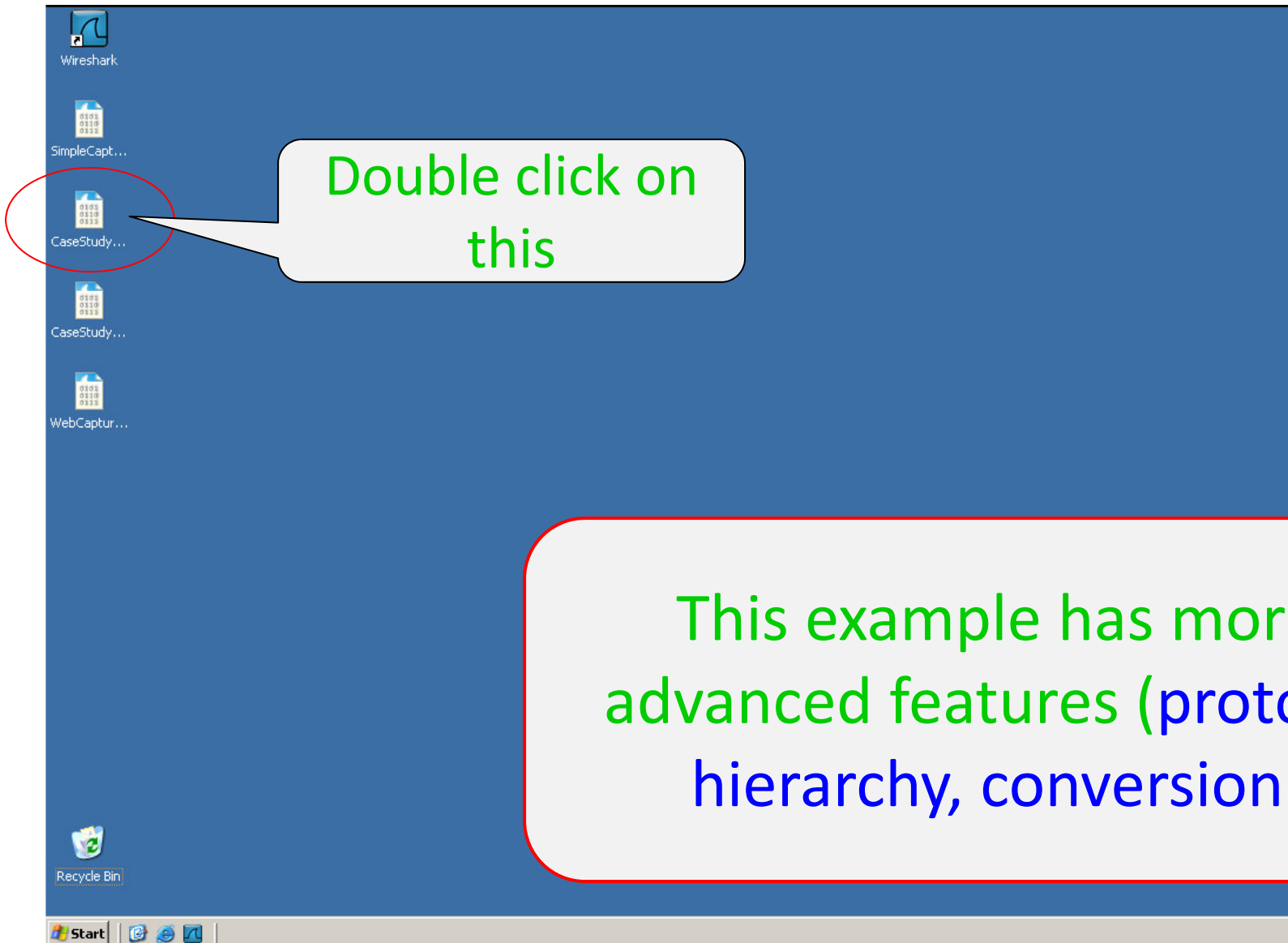
Domain Name System (response)

0000 00 0c 29 4c 78 f3 00 50 56 f9 f7 86 08 00 45 00 ..)Lx..P V....E.
0010 00 d6 a3 1a 00 00 80 11 68 57 ac 10 6b 02 ac 10hw..k...
0020 6b 82 00 35 ff ac 00 c2 6e 00 95 b3 81 80 00 01 k..5....n.....
0030 00 03 00 02 00 02 0a 70 61 73 73 65 74 73 2d 65p assets-e
0040 63 09 70 69 6e 74 65 72 65 73 74 03 63 6f 6d 00 c.pinter est.com.
0050 00 01 00 01 00 00 00 00 00 00 00 00 00 00 00 00

File: "C:\tmp\Boot-capture\WebCapture.pcap" Packets: 2038 · Displayed: 1985 (97.4%) · Load time: 0:00.024 Profile: Default

This pane has fewer packets now, all related to packet 42, making your life easier!

Exercise 2



This example has more advanced features (protocol hierarchy, conversion)



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | fe80::7cfa:9e3f:3124:ed69 | ff02::c | SSDP | 208 | M-SEARCH * HTTP/1.1 |
| 2 | 0.957053 | 192.168.1.7 | 192.168.1.1 | DNS | 71 | Standard query 0xbeb8 A www.msn.com |
| 3 | 0.983752 | 192.168.1.1 | 192.168.1.7 | DNS | 129 | Standard query response 0xbeb8 CNAME us.co1.cb3.glb dns.microsoft.com A 65.55.84.56 |
| 4 | 1.003867 | 192.168.1.7 | 65.55.84.56 | TCP | 66 | 49635->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 5 | 1.010498 | 169.254.1.213 | 255.255.255.255 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| 6 | 1.012715 | 169.254.1.213 | 255.255.255.255 | UDP | 181 | Source port: 21302 Destination port: 21302 |
| 7 | 1.013691 | 169.254.1.47 | 169.254.1.255 | UDP | 60 | Source port: 5056 Destination port: 5000 |
| 8 | 1.062768 | 65.55.84.56 | 192.168.1.7 | TCP | 62 | 80->49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 9 | 1.062847 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 10 | 1.063255 | 192.168.1.7 | 65.55.84.56 | HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| 11 | 1.182590 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 12 | 1.183190 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 13 | 1.183225 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=463 Ack=2921 win=64240 Len=0 |
| 14 | 1.235823 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 15 | 1.235830 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 16 | 1.235832 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 17 | 1.235919 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| 18 | 1.236712 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |

Frame 1: 208 bytes on wire (1664 bits) captured (1664 bits)

Ethernet II, Src: IntelCor_5e:df:7c:86:dd:60, Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::7cfa:9e3f:3124:ed69, Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 21302, Dst Port: 1900 (1900)

Hypertext Transfer Protocol

0000 33 33 00 00 00 0c 00 23 15 5e df 7c 86 dd 60 00 33.....# ^.^|..`
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 7c fa|
0020 9e 3f 31 24 ed 69 ff 02 00 00 00 00 00 00 00 00 .?1\$.i... ..
0030 00 00 00 00 00 0c f6 51 07 6c 00 9a 67 45 4d 2dQ .l.gEM-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 21 04 03 48 6f 72 74 23 5b 46 46 20 22 22 22 42 1 Host: ff02::c

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default

This example has many (too many?) packets



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze **Statistics** Telephony Tools Internals Help

Filter:

No. Time Source

| | | |
|----|----------|---------------------------|
| 1 | 0.000000 | fe80::7cfa:9e3f:3124:ed69 |
| 2 | 0.957053 | 192.168.1.7 |
| 3 | 0.983752 | 192.168.1.1 |
| 4 | 1.003867 | 192.168.1.7 |
| 5 | 1.010498 | 169.254.1.213 |
| 6 | 1.012715 | 169.254.1.213 |
| 7 | 1.013691 | 169.254.1.47 |
| 8 | 1.062768 | 65.55.84.56 |
| 9 | 1.062847 | 192.168.1.7 |
| 10 | 1.063255 | 192.168.1.7 |
| 11 | 1.182590 | 65.55.84.56 |
| 12 | 1.183190 | 65.55.84.56 |
| 13 | 1.183225 | 192.168.1.7 |
| 14 | 1.235823 | 65.55.84.56 |
| 15 | 1.235830 | 65.55.84.56 |
| 16 | 1.235832 | 65.55.84.56 |
| 17 | 1.235919 | 192.168.1.7 |
| 18 | 1.236712 | 65.55.84.56 |

Summary
Comments Summary
Show address resolution
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graph
Conversation List
Endpoint List
Service Response Time
29West
ANCP
BACnet
Collectd...
Compare...
Flow Graph...
HART-IP
HTTP
ONC-RPC Programs
Sametime
TCP StreamGraph
UDP Multicast Streams
WLAN Traffic
IP Statistics
BOOTP-DHCP...

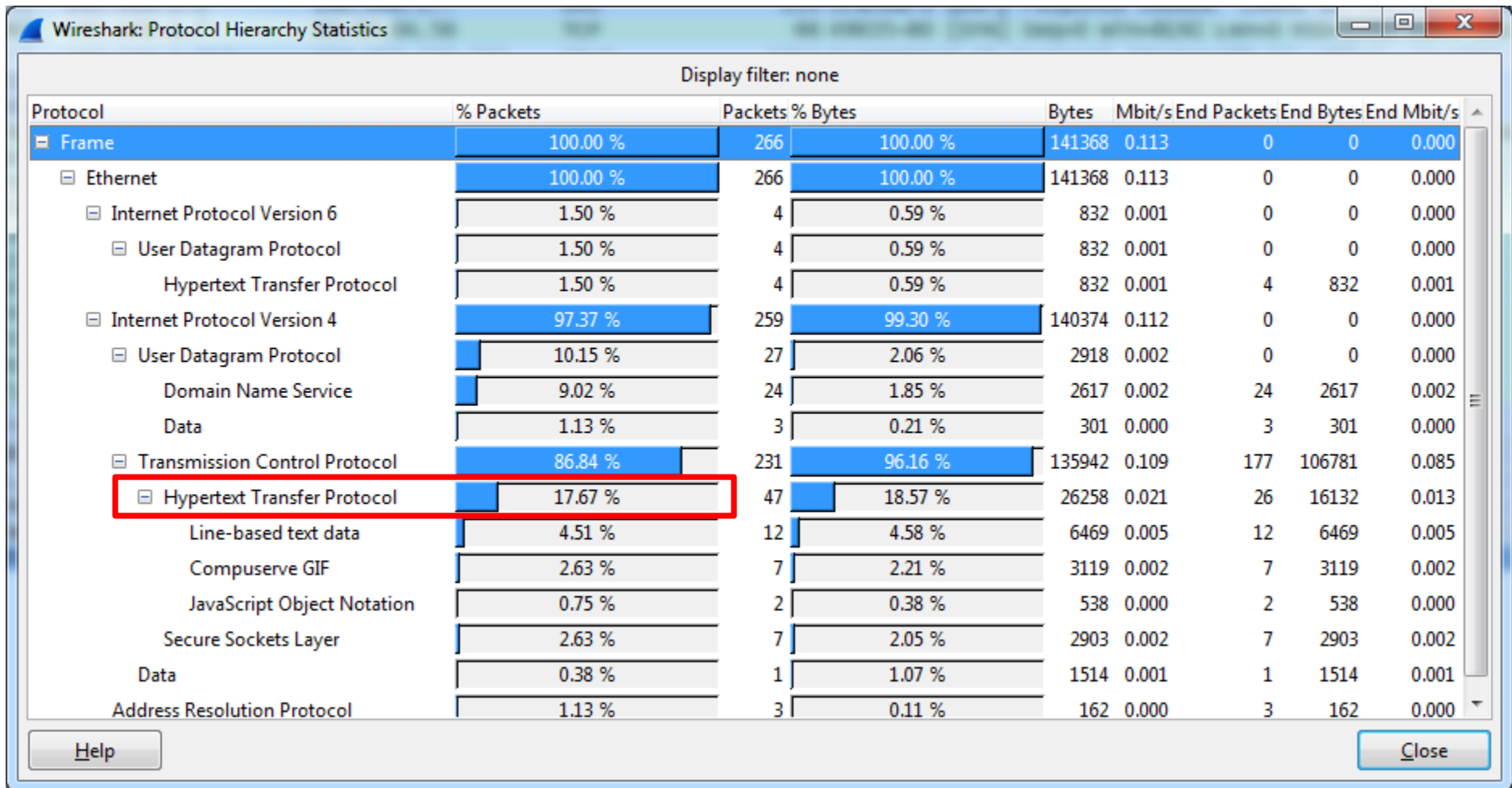
Protocol Length Info

| | | |
|------|------|---|
| SDP | 208 | M-SEARCH * HTTP/1.1 |
| NS | 71 | Standard query 0xbeb8 A www.msn.com |
| NS | 129 | Standard query response 0xbeb8 CNAME us.co1.cb3.glb dns.microsoft.com A 65.55.84.56 |
| CP | 66 | 49635-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| DP | 181 | Source port: 21302 Destination port: 21302 |
| DP | 60 | Source port: 5056 Destination port: 5000 |
| CP | 62 | 80-49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| CP | 54 | 49635-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=2921 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |

Frame 1: 208 bytes on wire (1664 bits)
Ethernet II, Src: IntelCor_5, Dst: fe80::7cfa:9e3f:3124:ed69
Internet Protocol Version 6, Src: fe80::7cfa:9e3f:3124:ed69, Dst: ff02::c
User Datagram Protocol, Src Port: 1900, Dst Port: 1900
Hypertext Transfer Protocol

0000 33 33 00 00 00 0c 00 23 15 5e df 7c 86 dd 60 00 33.....# .^.|...
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 7c fa|
0020 9e 3f 31 24 ed 69 ff 02 00 00 00 00 00 00 00 00 .?1\$.i.....
0030 00 00 00 00 00 0c f6 51 07 6c 00 9a 67 45 4d 2dQ .l..gEM-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 21 04 02 48 6f 72 24 23 5b 46 46 20 22 22 22 42 1 host: [ff02::c

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default





CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze **Statistics** Telephony Tools Internals Help

Filter:

| No. | Time | Source |
|-----|----------|---------------------------|
| 1 | 0.000000 | fe80::7cfa:9e3f:3124:ed69 |
| 2 | 0.957053 | 192.168.1.7 |
| 3 | 0.983752 | 192.168.1.1 |
| 4 | 1.003867 | 192.168.1.7 |
| 5 | 1.010498 | 169.254.1.213 |
| 6 | 1.012715 | 169.254.1.213 |
| 7 | 1.013691 | 169.254.1.47 |
| 8 | 1.062768 | 65.55.84.56 |
| 9 | 1.062847 | 192.168.1.7 |
| 10 | 1.063255 | 192.168.1.7 |
| 11 | 1.182590 | 65.55.84.56 |
| 12 | 1.183190 | 65.55.84.56 |
| 13 | 1.183225 | 192.168.1.7 |
| 14 | 1.235823 | 65.55.84.56 |
| 15 | 1.235830 | 65.55.84.56 |
| 16 | 1.235832 | 65.55.84.56 |
| 17 | 1.235919 | 192.168.1.7 |
| 18 | 1.236712 | 65.55.84.56 |

Summary
Comments Summary
Show address resolution
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graph
Conversation List
Endpoint List
Service Response Time
29West
ANCP
BACnet
Collectd...
Compare...
Flow Graph...
HART-IP
HTTP
ONC-RPC Programs
Sametime
TCP StreamGraph
UDP Multicast Streams
WLAN Traffic
IP Statistics
BOOTP-DHCP...

Protocol Length Info

| Protocol | Length | Info |
|----------|--------|---|
| SDP | 208 | M-SEARCH * HTTP/1.1 |
| NS | 71 | Standard query 0xbeb8 A www.msn.com |
| NS | 129 | Standard query response 0xbeb8 CNAME us.col.cb3.glb dns.microsoft.com A 65.55.84.56 |
| CP | 66 | 49635-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| DP | 181 | Source port: 21302 Destination port: 21302 |
| DP | 60 | Source port: 5056 Destination port: 5000 |
| CP | 62 | 80-49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| CP | 54 | 49635-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=2921 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |

Frame 1: 208 bytes on wire (1664 bits)
Ethernet II, Src: IntelCor_S
Internet Protocol Version 6,
User Datagram Protocol, Src
Hypertext Transfer Protocol

0000 33 33 00 00 00 0c 00 23 15 5e df 7c 86 dd 60 00 33.....# .^.|...
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 7c fa|
0020 9e 3f 31 24 ed 69 ff 02 00 00 00 00 00 00 00 00 .?1\$.i.....
0030 00 00 00 00 00 0c f6 51 07 6c 00 9a 67 45 4d 2dQ .l..gEM-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 21 04 03 48 6f 72 74 23 5b 46 46 20 22 22 22 42 1 host: [ff02::c

File: "C:\tmp\Boot-capture\CaseStudy1.pca..." Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

| No. | Time | Source |
|-----|----------|------------------|
| 1 | 0.000000 | fe80::7cfa:94... |
| 2 | 0.957053 | 192.168.1.7 |
| 3 | 0.983752 | 192.168.1.1 |
| 4 | 1.003867 | 192.168.1.7 |
| 5 | 1.010498 | 169.254.1.213 |
| 6 | 1.012715 | 169.254.1.213 |
| 7 | 1.013691 | 169.254.1.47 |
| 8 | 1.062768 | 65.55.84.56 |
| 9 | 1.062847 | 192.168.1.7 |
| 10 | 1.063255 | 192.168.1.7 |
| 11 | 1.182590 | 65.55.84.56 |
| 12 | 1.183190 | 65.55.84.56 |
| 13 | 1.183225 | 192.168.1.7 |
| 14 | 1.235823 | 65.55.84.56 |
| 15 | 1.235830 | 65.55.84.56 |
| 16 | 1.235832 | 65.55.84.56 |
| 17 | 1.235919 | 192.168.1.7 |
| 18 | 1.236712 | 65.55.84.56 |

Summary
Comments Summary
Show address resolution
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graph
Conversation List
Endpoint List
Service Response Time
29West
ANCP
BACnet
Collectd...
Compare...
Flow Graph...
HART-IP
HTTP
ONC-RPC Programs
Sametime
TCP StreamGraph
UDP Multicast Streams
WLAN Traffic
IP Statistics
BOOTP-DHCP...

Protocol Length Info

| Protocol | Length | Info |
|----------|--------|---|
| SDP | 208 | M-SEARCH * HTTP/1.1 |
| DNS | 71 | Standard query 0xbeb8 A www.msn.com |
| DNS | 129 | Standard query response 0xbeb8 CNAME us.col.cb3.glb dns.microsoft.com A 65.55.84.56 |
| TCP | 66 | 49635-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| UDP | 181 | Source port: 21302 Destination port: 21302 |
| UDP | 60 | Source port: 5056 Destination port: 5000 |
| TCP | 62 | 80-49635 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| TCP | 54 | 49635-80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |
| HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| TCP | 1514 | [TCP segment of a reassembled PDU] |
| TCP | 1514 | [TCP segment of a reassembled PDU] |
| TCP | 54 | 49635-80 [ACK] Seq=463 Ack=2921 Win=64240 Len=0 |
| TCP | 1514 | [TCP segment of a reassembled PDU] |
| TCP | 1514 | [TCP segment of a reassembled PDU] |
| TCP | 1514 | [TCP segment of a reassembled PDU] |
| TCP | 54 | 49635-80 [ACK] Seq=463 Ack=7301 Win=64240 Len=0 |
| TCP | 1514 | [TCP segment of a reassembled PDU] |

Frame 1: 208 bytes on wire (1664 bits) captured on interface eth0 (00:00:00:00:00:00) from 192.168.1.7 to 192.168.1.1
Ethernet II, Src: IntelCor_5 (08:00:00:00:00:00), Dst: ff02::c (01:00:5e:00:00:00)
Internet Protocol Version 6, Src: fe80::7cfa:94... (fe80::7cfa:94...), Dst: ff02::c (ff02::c)
User Datagram Protocol, Src Port: 21302, Dst Port: 1900 (1900)
Hypertext Transfer Protocol

33 33 00 00 00 0c 00 23 15 5e df 7c 86 dd 60 00 33.....# .^.|. .
0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 7c fa|.
0020 9e 3f 31 24 ed 69 ff 02 00 00 00 00 00 00 00 .?1\$.i.....
0030 00 00 00 00 00 0c f6 51 07 6c 00 9a 67 45 4d 2dQ .l..gEM-
0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
0050 21 0d 03 48 6f 72 74 23 5b 46 46 30 32 33 33 42 1 Host: [ff02::c]

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | fe80::7cfa:9e3f:3124:ed69 | ff02::c | SSDP | 208 | M-SEARCH * HTTP/1.1 |
| 2 | 0.957053 | 192.168.1.7 | 192.168.1.1 | DNS | 71 | Standard query 0xeb8 A www.msn.com |
| 3 | 0.983752 | 192.168.1.1 | 192.168.1.7 | DNS | 129 | Standard query response 0xeb8 CNAME us.co1.cb3.glb dns.microsoft.com A 65.55.84.56 |
| 4 | 1.003867 | 192.168.1.7 | 65.55.84.56 | TCP | 66 | 49635-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 5 | 1.010498 | 169.254.1.213 | 255.255.255.255 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| 6 | 1.012715 | 169.254.1.213 | 255.255.255.255 | UDP | 181 | Source port: 21302 Destination port: 21302 |
| 7 | 1.013691 | 169.254.1.47 | 169.254.1.47 | UDP | 54 | Source port: 5056 Destination port: 5000 |
| 8 | 1.062768 | 65.55.84.56 | 192.168.1.7 | TCP | 66 | 49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 9 | 1.062847 | 192.168.1.7 | 65.55.84.56 | TCP | 66 | 49635-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 10 | 1.063255 | 192.168.1.7 | 65.55.84.56 | HTTP | 1514 | GET /?ocid=iehp HTTP/1.1 |
| 11 | 1.182590 | 65.55.84.56 | 192.168.1.7 | TCP | 66 | 49635 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 12 | 1.183190 | 65.55.84.56 | 192.168.1.7 | TCP | 66 | 49635 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 13 | 1.183225 | 192.168.1.7 | 65.55.84.56 | TCP | 66 | 49635 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 14 | 1.235823 | 65.55.84.56 | 192.168.1.7 | TCP | 66 | 49635 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 15 | 1.235830 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 16 | 1.235832 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 17 | 1.235919 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635-80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| 18 | 1.236712 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |

Wireshark: Requests Stats Tree...

Filter:

Create Stat Cancel

Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits)

Ethernet II, Src: IntelCor_5e:df:7c (00:23:15:5e:df:7c), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::7cfa:9e3f:3124:ed69 (fe80::7cfa:9e3f:3124:ed69), Dst: ff02::c (ff02::c)

User Datagram Protocol, Src Port: 63057 (63057), Dst Port: 1900 (1900)

Hypertext Transfer Protocol

0000 33 33 00 00 00 0c 00 23 15 5e df 7c 86 dd 60 00 33.....# .^.|..`

0010 00 00 00 9a 11 01 fe 80 00 00 00 00 00 00 7c fa|..

0020 9e 3f 31 24 ed 69 ff 02 00 00 00 00 00 00 00 00 ..?1\$.i..

0030 00 00 00 00 00 0c f6 51 07 6c 00 9a 67 45 4d 2dQ..l..gEM-

0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.

0050 21 0d 03 48 6f 72 74 23 5b 46 46 20 22 22 22 42 1 Host: [ff02::c

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default



Requests with filter:

| Topic / Item | Count | Avera |
|---|-------|-------|
| [-] HTTP Requests by HTTP Host | 26 | |
| [+] rad.msn.com | 5 | |
| [+] [FF02::C]:1900 | 4 | |
| [-] www.msn.com | 3 | |
| /sck.aspx?cv=_SS%3dSID%3d7C73BA2D0DBD452E95CBDB3AFE1879B0%3b&h=fe92cd76-4cb3-03b6-8afc-cd7f85f73879 | 1 | |
| /ajax/conditionalbanners.aspx | 1 | |
| /?ocid=iehp | 1 | |
| [+] www.bing.com | 3 | |
| [+] www.google.com | 2 | |
| [+] udc.msn.com | 2 | |
| [+] media.match.com | 2 | |
| [+] view.atdmt.com | 1 | |
| [+] c.msn.com | 1 | |
| [+] b.scorecardresearch.com | 1 | |

Copy Save As Close



| Requests with filter: | | | |
|---|-------|---------|---|
| Topic / Item | Count | Average | M |
| [-] HTTP Requests by HTTP Host | 26 | | |
| [+] rad.msn.com | 5 | | |
| [+] [FF02::C]:1900 | 4 | | |
| [-] www.msn.com | 3 | | |
| /sck.aspx?cv=_SS%3dSID%3d7C73BA2D0DBD452E95CBDB3AFE1879B0%3b&h=fe92cd76-4cb3-03b6-8afc-cd7f85f73879 | 1 | | |
| /ajax/conditionalbanners.aspx | 1 | | |
| /?ocid=iehp | 1 | | |
| [+] www.bing.com | 3 | | |
| [+] www.google.com | 2 | | |
| [+] udc.msn.com | 2 | | |
| [+] media.match.com | 2 | | |
| [+] view.atdmt.com | 1 | | |
| [+] c.msn.com | 1 | | |
| [+] b.scorecardresearch.com | 1 | | |
| [+] api.bing.com | 1 | | |
| [+] amer.rel.msn.com | 1 | | |

Copy

Save As

Close



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze **Statistics** Telephony Tools Internals Help

Filter:

| No. | Time | Source |
|-----|----------|------------------|
| 1 | 0.000000 | fe80::7cfa:9e... |
| 2 | 0.957053 | 192.168.1.7 |
| 3 | 0.983752 | 192.168.1.1 |
| 4 | 1.003867 | 192.168.1.7 |
| 5 | 1.010498 | 169.254.1.213 |
| 6 | 1.012715 | 169.254.1.213 |
| 7 | 1.013691 | 169.254.1.47 |
| 8 | 1.062768 | 65.55.84.56 |
| 9 | 1.062847 | 192.168.1.7 |
| 10 | 1.063255 | 192.168.1.7 |
| 11 | 1.182590 | 65.55.84.56 |
| 12 | 1.183190 | 65.55.84.56 |
| 13 | 1.183225 | 192.168.1.7 |
| 14 | 1.235823 | 65.55.84.56 |
| 15 | 1.235830 | 65.55.84.56 |
| 16 | 1.235832 | 65.55.84.56 |
| 17 | 1.235919 | 192.168.1.7 |
| 18 | 1.236712 | 65.55.84.56 |

Statistics menu:

- Summary
- Comments Summary
- Show address resolution
- Protocol Hierarchy
- Conversations**
- Endpoints
- Packet Lengths...
- IO Graph
- Conversation List
- Endpoint List
- Service Response Time
- 29West
- ANCP
- BACnet
- Collectd...
- Compare...
- Flow Graph...
- HART-IP
- HTTP
- ONC-RPC Programs
- Sametime
- TCP StreamGraph
- UDP Multicast Streams
- WLAN Traffic
- IP Statistics
- BOOTP-DHCP...

Protocol Length Info

| Protocol | Length | Info |
|----------|--------|--|
| SDP | 208 | M-SEARCH * HTTP/1.1 |
| NS | 71 | Standard query 0xbeb8 A www.msn.com |
| NS | 129 | Standard query response 0xbeb8 CNAME us.co1.cb3.glbdns.microsoft.com A 65.55.84.56 |
| CP | 66 | 49635-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| Pv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| DP | 181 | Source port: 21302 Destination port: 21302 |
| DP | 60 | Source port: 5056 Destination port: 5000 |
| CP | 62 | 80-49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| CP | 54 | 49635-80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=2921 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 1514 | [TCP segment of a reassembled PDU] |
| CP | 54 | 49635-80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| CP | 1514 | [TCP segment of a reassembled PDU] |

Frame 2: 71 bytes on wire (568 bits)

Ethernet II, Src: Vmware_db:08:00:27:00:00:00, Dst: Actionte_b9:eb:02 (00:18:01:b9:eb:02)

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1 (192.168.1.1)

User Datagram Protocol, Src Port: 53, Dst Port: 53 (53)

Domain Name System (query) Response In: 31

Transaction ID: 0xbeb8

Flags: 0x0100 Standard query response

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.msn.com: type A, class IN

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00)..q..E.
0010 00 39 16 d2 00 00 80 11 00 00 c0 a8 01 07 c0 a89.....
0020 01 01 c2 ff 00 35 00 25 83 8f be b8 01 00 00 015.%.
0030 00 00 00 00 00 00 03 77 77 77 03 6d 73 6e 03 63w ww.msn.c
0040 6f 6d 00 00 01 00 01om.....

Frame (frame), 71 bytes

Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056

Profile: Default



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre Channel FDDI IPv4: 16 IPv6: 1 IPX JXTA NCP RSVP SCTP TCP: 15 Token Ring UDP: 16 USB WLAN

Ethernet Conversations

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets B→A | Bytes B→A | Rel Start | Duration | bps A→B | bps B→A |
|-------------------|-------------------|---------|---------|-------------|-----------|-------------|-----------|-------------|----------|------------|-----------|
| IntelCor_5e:df:7c | IPv6mcast_0c | 4 | 832 | 4 | 832 | 0 | 0 | 0.000000000 | 10.0024 | 665.44 | N/A |
| Vmware_db:f6:71 | Actionte_b9:eb:02 | 257 | 138 661 | 119 | 22 178 | 138 | 116 483 | 0.957053000 | 7.7711 | 22831.24 | 119913.93 |
| ArrisGro_54:07:b5 | Broadcast | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| ArrisGro_df:5f:ef | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| HtcCorpo_b7:d0:3a | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 2.236160000 | 0.0000 | N/A | N/A |
| ArrisGro_46:96:d2 | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph B→A Close

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00).q.E.
0010 00 39 16 d2 00 00 80 11 00 00 c0 a8 01 07 c0 a8 .9.....
0020 01 01 c2 ff 00 35 00 25 83 8f be b8 01 00 00 015.%
0030 00 00 00 00 00 00 03 77 77 77 03 6d 73 6e 03 63w ww.msn.c
0040 6f 6d 00 00 01 00 01om.....

Frame (frame), 71 bytes Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.056 Profile: Default



Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre Channel FDDI IPv4: 16 IPv6: 1 IPX JXTA NCP RSVP SCTP TCP: 15 Token Ring UDP: 16 USB WLAN

Ethernet Conversations

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets A←B | Bytes A←B | Rel Start | Duration | bps A→B | bps A←B |
|-------------------|-------------------|---------|---------|-------------|-----------|-------------|-----------|-------------|----------|------------|-----------|
| IntelCor_5e:df:7c | IPv6mcast_0c | 4 | 832 | 4 | 832 | 0 | 0 | 0.000000000 | 10.0024 | 665.44 | N/A |
| Vmware_db:f6:71 | Actionte_b9:eb:02 | 257 | 138 661 | 119 | 22 178 | 138 | 116 483 | 0.957053000 | 7.7711 | 22831.24 | 119913.93 |
| ArrisGro_54:07:b5 | Broadcast | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| ArrisGro_df:5f:ef | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| HtcCorpo_b7:d0:3a | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 2.236160000 | 0.0000 | N/A | N/A |
| ArrisGro_46:96:d2 | Broadcast | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close

Does not make much sense



One row, one
conversation

Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre Channel FDDI IPv4: 16 IPv6: 1 IPX: 1

IPv4 Conversations

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets B→A | Bytes B→A | Rel Start | Duration | bps A→B | bps B→A |
|----------------|-----------------|---------|--------|-------------|-----------|-------------|-----------|-------------|----------|------------|----------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 | 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 | 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 169.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
| 65.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 | 1.460531000 | 6.7915 | 1064.86 | 2438.34 |
| 192.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 | 1.463244000 | 0.1165 | 49226.76 | 31238.74 |
| 67.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 | 1.484162000 | 0.2664 | 25585.68 | 23033.12 |
| 64.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 | 1.500961000 | 0.4409 | 9725.76 | 15495.89 |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 | 1.509582000 | 1.1311 | 14838.76 | 12101.58 |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 | 1.963498000 | 0.8334 | 82192.08 | 36651.41 |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 | 1.974914000 | 0.2965 | 17913.87 | 19505.61 |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 | 2.130004000 | 0.3354 | 140969.79 | 48969.71 |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 | 2.566532000 | 0.4933 | 320986.75 | 37449.27 |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 | 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | fe80::7cfa:9e3f:312ff02::c | 208 M-SEARCH * HTTP/1.1 | SSDP | | |
| 2 | 0.957053 | 192.168.1.7 | 192.168.1.1 | DNS | 71 | Standard query 0xeb8 A www.msn.com |
| 3 | 0.983752 | 192.168.1.1 | 192.168.1.7 | DNS | 129 | Standard query response 0xeb8 CNAME us.co1.cb3.glb dns.microsoft.com A 65.55.84.56 |
| 4 | 1.003867 | 192.168.1.7 | 65.55.84.56 | TCP | 66 | 49635->80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 5 | 1.010498 | 169.254.1.213 | 255.255.255.255 | IPv4 | 1514 | Fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6] |
| 6 | 1.012715 | 169.254.1.213 | 255.255.255.255 | UDP | 181 | Source port: 21302 Destination port: 21302 |
| 7 | 1.013691 | 169.254.1.47 | 169.254.1.255 | UDP | 60 | Source port: 5056 Destination port: 5000 |
| 8 | 1.062768 | 65.55.84.56 | 192.168.1.7 | TCP | 62 | 80->49635 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 9 | 1.062847 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 10 | 1.063255 | 192.168.1.7 | 65.55.84.56 | HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| 11 | 1.182590 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 12 | 1.183190 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 13 | 1.183225 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=463 Ack=2921 win=64240 Len=0 |
| 14 | 1.235823 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 15 | 1.235830 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 16 | 1.235832 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 17 | 1.235919 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635->80 [ACK] Seq=463 Ack=7301 win=64240 Len=0 |
| 18 | 1.236712 | 65.55.84.56 | 192.168.1.7 | TCP | 1514 | [TCP segment of a reassembled PDU] |

Frame 2: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0

Ethernet II, Src: Vmware_db:f6:71 (00:0c:29:db:f6:71), Dst: 01:01:c2:ff:00:35 (01:01:c2:ff:00:35:00:25)

Internet Protocol Version 4, Src: 192.168.1.7, Dst: 65.55.84.56

User Datagram Protocol, Src Port: 49919, Dst Port: 80

Domain Name System (query)

[Response in: 3]

Transaction ID: 0xeb8

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.msn.com: type A, class IN

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 00 00 00 00

0010 00 39 16 d2 00 00 80 11 00 00 c0 a3 00 00 00 00

0020 01 01 c2 ff 00 35 00 25 83 8f be b9 00 00 00 00

0030 00 00 00 00 00 00 03 77 77 77 03 66 00 00 00 00

0040 6f 6d 00 00 01 00 01

Frame (frame), 71 bytes

Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre Channel: FDDI: IPv4: 16 IPv6: 1 IPX: JXTA: NCP: RSVP: SCTP: TCP: 15 Token Ring: UDP: 16 USB: WLAN:

IPv4 Conversations

| Address A | Address B | Packets | Bytes | Packets A-B | Bytes A-B | Packets B-A | Bytes B-A | Rel Start | Duration | bps A-B | bps B-A |
|----------------|-----------------|---------|--------|-------------|-----------|-------------|-----------|-------------|----------|------------|----------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 | 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 | 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 169.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
| 65.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 | 1.460531000 | 6.7915 | 1064.86 | 2438.34 |
| 192.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 | 1.463244000 | 0.1165 | 49226.76 | 31238.74 |
| 67.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 | 1.484162000 | 0.2664 | 25585.68 | 23033.12 |
| 64.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 | 1.500961000 | 0.4409 | 9725.76 | 15495.89 |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 | 1.509582000 | 1.1311 | 14838.76 | 12101.58 |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 | 1.963498000 | 0.8334 | 82192.08 | 36651.41 |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 | 1.974914000 | 0.2965 | 17913.87 | 19505.61 |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 | 2.130004000 | 0.3354 | 140969.79 | 48969.71 |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 | 2.566532000 | 0.4933 | 320986.75 | 37449.27 |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 | 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

Help Copy Follow Stream Graph A-B Graph B-A Close



Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre P: 15 Token Ring UDP: 16 USB WLAN

Right click on this

IPv4 Conversations

| Address A | Address B | Bytes | Packets A→B | Bytes A→B | Packets A→B | Bytes A←B | Rel Start | Duration | bps A→B | bps A←B |
|----------------|----------------|-------|-------------|-----------|-------------|-----------|-------------------|----------|------------|----------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 169.254.1.213 | 169.254.1.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 1.013691000 | 0.0000 | N/A | N/A |
| 192.168.1.7 | 207.46.140.4 | 13 | 3 809 | 1 | 664 | 5 | 1 000 0.3999 | 0.3999 | 19525.47 | 8242.31 |
| 65.55.253.27 | 192.168.1.7 | 28 | 12 380 | 1 | 664 | 5 | 1 000 6.7915 | 6.7915 | 1064.86 | 2438.34 |
| 192.168.1.7 | 207.46.193.3 | 9 | 1 387 | 4 | 664 | 5 | 1 000 0.1165 | 0.1165 | 49226.76 | 31238.74 |
| 67.148.147.113 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 000 0.2664 | 0.2664 | 25585.68 | 23033.12 |
| 64.4.21.39 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 1 000 0.4409 | 0.4409 | 9725.76 | 15495.89 |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 1 | 664 | 5 | 1 000 1.1311 | 1.1311 | 14838.76 | 12101.58 |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 1 | 664 | 5 | 2 000 0.8334 | 0.8334 | 82192.08 | 36651.41 |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 1 000 0.2965 | 0.2965 | 17913.87 | 19505.61 |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 1 000 0.3354 | 0.3354 | 140969.79 | 48969.71 |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 000 0.4933 | 0.4933 | 320986.75 | 37449.27 |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 4.990550000 | 0.0000 | N/A | N/A |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

Apply as Filter
Prepare a Filter
Find Packet
Colorize Conversation

Selected
Not Selected
... and Selected
... or Selected
... and not Selected
... or not Selected

A → B
A → B
A → B
A → Any
A → Any
A → Any
A → Any
Any → B
Any → B
Any → B

☒ Name resolution ☐ Limit to display filter

Help Copy Follow Stream Graph A→B Graph A←B Close



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr==192.168.1.7 && ip.addr==207.46.140.46

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 56 | 1.448913 | 192.168.1.7 | 207.46.140.46 | TCP | 66 | 49636-80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 82 | 1.537809 | 207.46.140.46 | 192.168.1.7 | TCP | 66 | 80-49636 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1 |
| 83 | 1.537891 | 192.168.1.7 | 207.46.140.46 | TCP | 54 | 49636-80 [ACK] Seq=1 Ack=1 win=65700 Len=0 |
| 84 | 1.538291 | 192.168.1.7 | 207.46.140.46 | HTTP | 802 | GET /default.aspx?parsergroup=hops&fk=w&gp=P&optkey=default&cp=default&rfr=di=340&pi=7317&ps |
| 95 | 1.630817 | 207.46.140.46 | 192.168.1.7 | HTTP | 346 | HTTP/1.1 204 No Content |
| 103 | 1.848801 | 192.168.1.7 | 207.46.140.46 | TCP | 54 | 49636-80 [ACK] Seq=749 Ack=293 win=65408 Len=0 |

Frame 56: 66 bytes on wire (528 bits),
Ethernet II, Src: Vmware_db:f6:71 (00:0c:29:db:f6:71), Dst: 08:00:27:2d:7a:8b (08:00:27:2d:7a:8b)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 207.46.140.46
Transmission Control Protocol, Src Port: 49636, Dst Port: 80

Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre Channel: FDDI: IPv4: 16 IPv6: 1 IPX: JXTA: NCP: RSVP: SCTP: TCP: 15 Token Ring: UDP: 16 USB: WLAN:

IPv4 Conversations

| Address A | Address B | Packets | Bytes | Packets A-B | Bytes A-B | Packets B-A | Bytes B-A | Rel Start | Duration | bps A-B | bps B-A |
|----------------|-----------------|---------|--------|-------------|-----------|-------------|-----------|-------------|----------|------------|----------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 | 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 | 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 169.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
| 65.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 | 1.460531000 | 6.7915 | 1064.86 | 2438.34 |
| 192.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 | 1.463244000 | 0.1165 | 49226.76 | 31238.74 |
| 67.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 | 1.484162000 | 0.2664 | 25585.68 | 23033.12 |
| 64.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 | 1.500961000 | 0.4409 | 9725.76 | 15495.89 |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 | 1.509582000 | 1.1311 | 14838.76 | 12101.58 |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 | 1.963498000 | 0.8334 | 82192.08 | 36651.41 |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 | 1.974914000 | 0.2965 | 17913.87 | 19505.61 |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 | 2.130004000 | 0.3354 | 140969.79 | 48969.71 |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 | 2.566532000 | 0.4933 | 320986.75 | 37449.27 |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 | 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71
0010 00 34 16 e5 40 00 80 06 00 00 c0 a1
0020 8c 2e c1 e4 00 50 9e 63 57 49 00 00
0030 20 00 1d 33 00 00 02 04 05 b4 01 00
0040 04 02

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packet

Name resolution Limit to display filter

Help Copy Follow Stream Graph A-B Graph B-A Close

This panel has fewer packets,
easier to study



Click here

CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|----------|----------------|----------------|----------|--------|--|
| 56 | 1.448913 | 192.168.1.7 | 207.46.140.46 | TCP | 66 | 49636→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 57 | 1.459771 | 192.168.1.1 | 192.168.1.7 | DNS | 127 | Standard query response 0x6c60 CNAME udc.udc0.glbdns.microsoft.com A 65.55.253.27 |
| 58 | 1.460531 | 192.168.1.7 | 65.55.253.27 | TCP | 66 | 49637→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 59 | 1.461213 | 192.168.1.7 | 192.168.1.1 | DNS | 69 | Standard query 0x5500 A c.msn.com |
| 60 | 1.462785 | 192.168.1.1 | 192.168.1.7 | DNS | 90 | Standard query response 0xce82 A 207.46.193.176 |
| 61 | 1.463244 | 192.168.1.7 | 207.46.193.176 | TCP | 66 | 49638→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 62 | 1.463791 | 192.168.1.7 | 192.168.1.1 | DNS | 72 | Standard query 0x236b A www.bing.com |
| 63 | 1.470807 | 65.55.253.27 | 192.168.1.7 | TCP | 66 | 80→49637 [SYN, ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1 |
| 64 | 1.470892 | 192.168.1.7 | 65.55.253.27 | TCP | 54 | 49637→80 [ACK] Seq=1 Ack=1 win=65700 Len=0 |
| 65 | 1.471377 | 192.168.1.7 | 65.55.253.27 | HTTP | 1049 | GET /c.gif?evt=impr&js=1&rid=45def397b817495bae983b0f282b2c51&exa=&pp=False&bd=&gnd=&cts=1 |
| 66 | 1.483302 | 192.168.1.1 | 192.168.1.7 | DNS | 197 | Standard query response 0x8281 CNAME b.scorecardresearch.com.edgesuite.net CNAME a1294.w2 |
| 67 | 1.484162 | 192.168.1.7 | 67.148.147.113 | TCP | 66 | 49639→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 68 | 1.489756 | 65.55.253.27 | 192.168.1.7 | HTTP | 419 | HTTP/1.1 200 OK (GIF89a) |
| 69 | 1.494163 | 192.168.1.1 | 192.168.1.7 | DNS | 118 | Standard query response 0x5500 CNAME c.msn.com.nsadc.net A 64.4.21.39 |
| 70 | 1.496408 | 207.46.193.176 | 192.168.1.7 | TCP | 62 | 80→49638 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 71 | 1.496475 | 192.168.1.7 | 207.46.193.176 | TCP | 54 | 49638→80 [ACK] Seq=1 Ack=1 win=64240 Len=0 |
| 72 | 1.499904 | 192.168.1.7 | 207.46.193.176 | HTTP | 489 | GET /action/MSN_Homepage_Remessaging_111808/nc?a=1 HTTP/1.1 |
| 73 | 1.500961 | 192.168.1.7 | 64.4.21.39 | TCP | 66 | 49640→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |

Frame 56: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)

Ethernet II, Src: Vmware_db:f6:71 (00:0c:29:db:f6:71), Dst: Actionte_b9:eb:02 (00:18:01:b9:eb:02)

Internet Protocol Version 4, Src: 192.168.1.7 (192.168.1.7), Dst: 207.46.140.46 (207.46.140.46)

Transmission Control Protocol, Src Port: 49636 (49636), Dst Port: 80 (80), Seq: 0, Len: 0

```
0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00  ....q..E.
0010 00 34 16 e5 40 00 80 06 00 00 c0 a8 01 07 cf 2e  .4..@.....
0020 8c 2e c1 e4 00 50 9e 63 57 49 00 00 00 80 02    ....P.C WI...
0030 20 00 1d 33 00 00 02 04 05 b4 01 03 03 02 01 01  ..3....
0040 04 02  ..
```

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 266 (100.0%) · Load time: 0:00.005 Profile: Default



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 |
|-----|----------|-------------|---------------|----------|--------|---|
| 56 | 1.448913 | 192.168.1.7 | 207.46.140.46 | TCP | 66 | 49636→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 57 | 1.459771 | 192.168.1.1 | 192.168.1.7 | DNS | 127 | Standard query response 0x6c60 CNAME udc.udc0.glbdns.microsoft.com A 65.55.253.27 |
| 58 | 1.460531 | 192.168.1.7 | 65.55.253.27 | TCP | 66 | 49637→80 [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 59 | 1.46121 | | | | | 0x5500 A c.msn.com |
| 60 | 1.46271 | | | | | response 0xce82 A 207.46.193.176 |
| 61 | 1.46321 | | | | | Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 62 | 1.46371 | | | | | 0x236b A www.bing.com |
| 63 | 1.47081 | | | | | ACK] Seq=0 Ack=1 win=4380 Len=0 MSS=1460 WS=1 SACK_PERM=1 |
| 64 | 1.47081 | | | | | Seq=1 Ack=1 win=65700 Len=0 |
| 65 | 1.47131 | | | | | =impr&js=1&rid=45def397b817495bae983b0f282b2c51&exa=&pp=False&bd=&gnd=&cts=1 |
| 66 | 1.48331 | | | | | response 0x8281 CNAME b.scorecardresearch.com.edgesuite.net CNAME a1294.w2 |
| 67 | 1.48411 | | | | | Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 68 | 1.48971 | | | | | (GIF89a) |
| 69 | 1.49411 | | | | | response 0x5500 CNAME c.msn.com.nsadc.net A 64.4.21.39 |
| 70 | 1.49641 | | | | | ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 SACK_PERM=1 |
| 71 | 1.49641 | | | | | Seq=1 Ack=1 win=64240 Len=0 |
| 72 | 1.49991 | | | | | _Homepage_Remessaging_111808/nc?a=1 HTTP/1.1 |
| 73 | 1.50091 | | | | | Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |

Wireshark: Filter Expression - Profile: Default

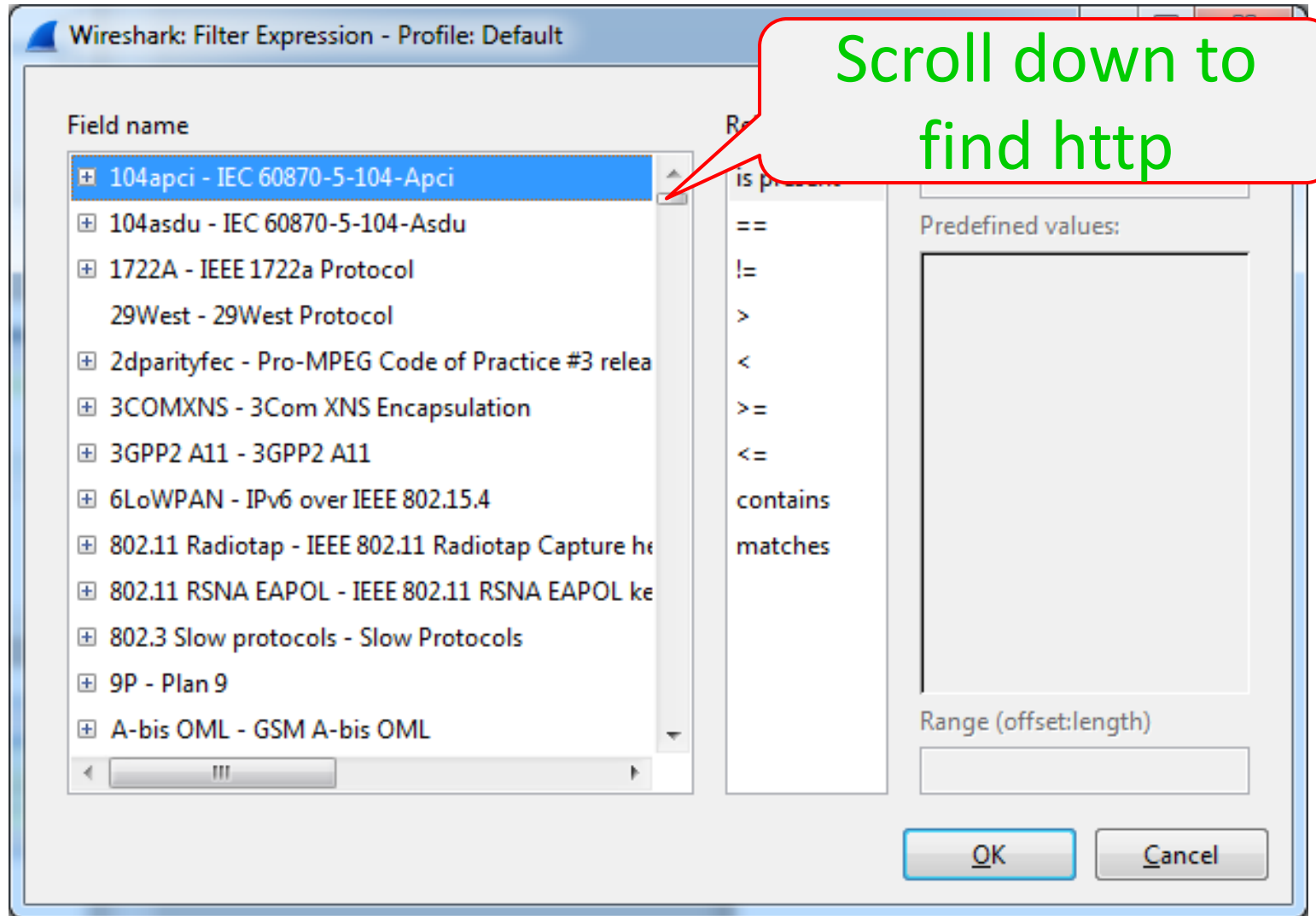
| Field name | Relation | Value (Protocol) |
|--|------------|------------------|
| 104apci - IEC 60870-5-104-Apci | is present | |
| 104asdu - IEC 60870-5-104-Asdu | == | |
| 1722A - IEEE 1722a Protocol | != | |
| 29West - 29West Protocol | > | |
| 2dparityfec - Pro-MPEG Code of Practice #3 relea | < | |
| 3COMXNS - 3Com XNS Encapsulation | >= | |
| 3GPP2 A11 - 3GPP2 A11 | <= | |
| 6LoWPAN - IPv6 over IEEE 802.15.4 | contains | |
| 802.11 Radiotap - IEEE 802.11 Radiotap Capture h | matches | |
| 802.11 RSNA EAPOL - IEEE 802.11 RSNA EAPOL ke | | |
| 802.3 Slow protocols - Slow Protocols | | |
| 9P - Plan 9 | | |
| A-bis OML - GSM A-bis OML | | |

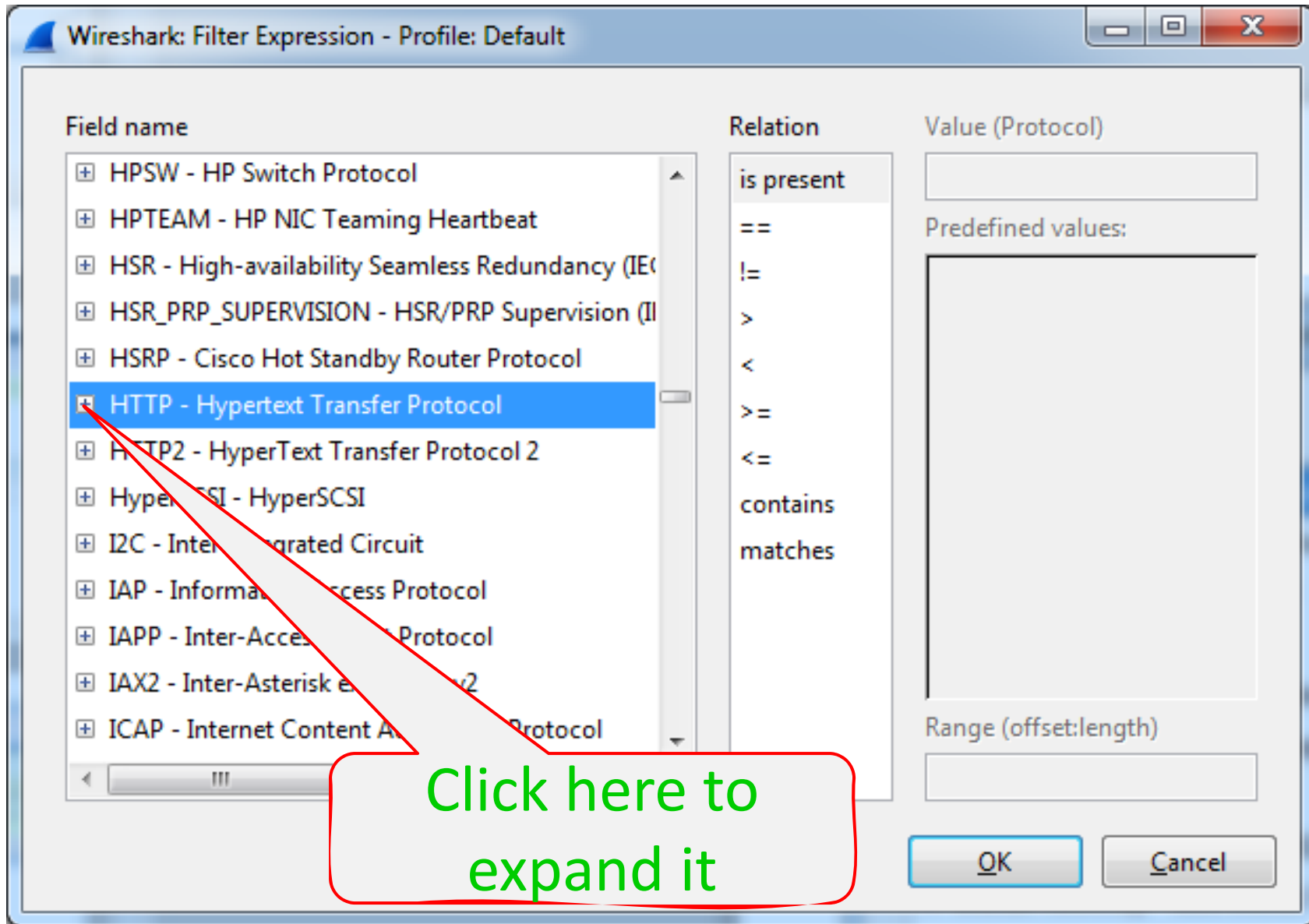
Range (offset:length)

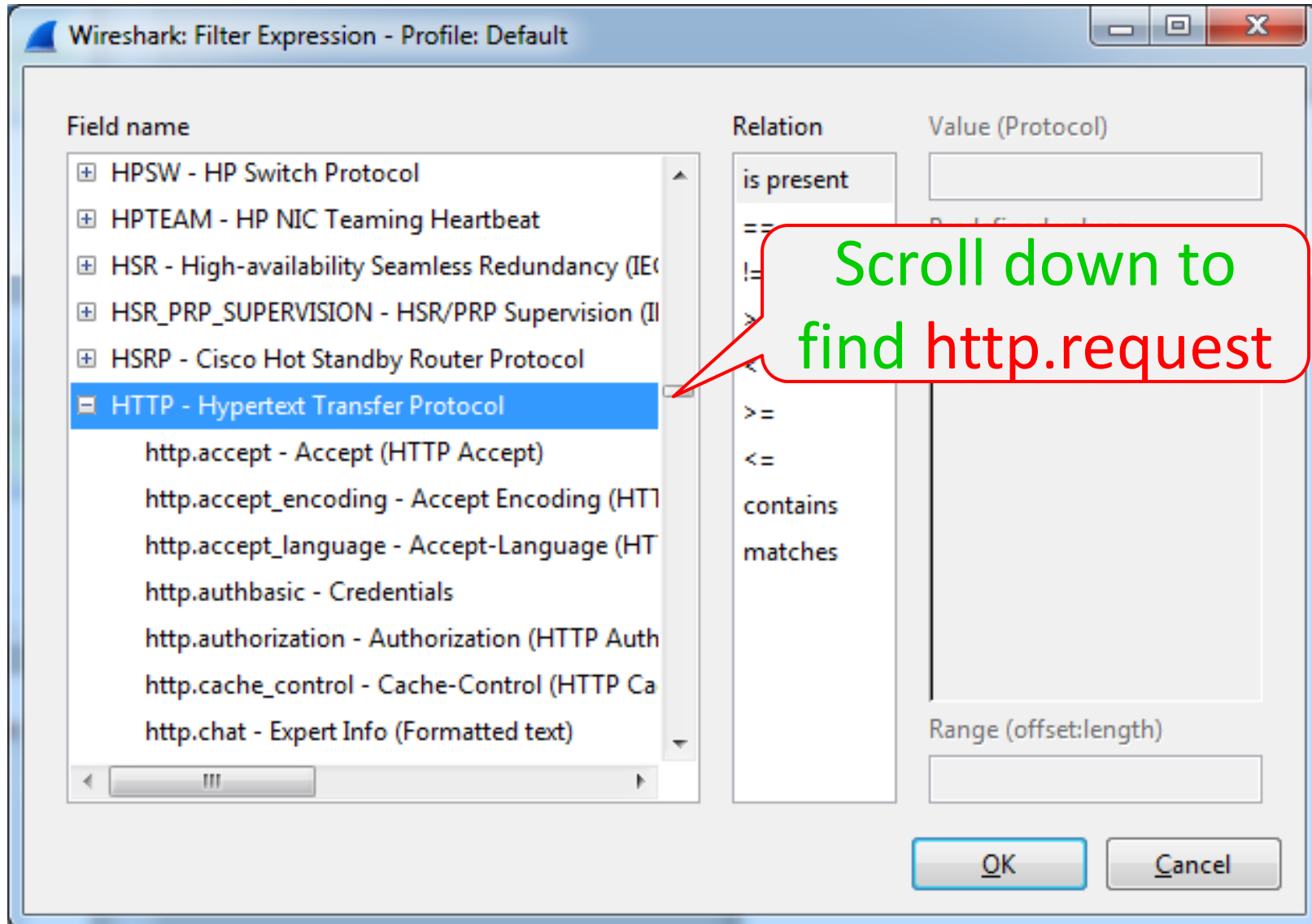
OK Cancel

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00).q..E.
0010 00 34 16 e5 40 00 80 06 00 00 c0 a8 01 07 cf 2e .4..@.....
0020 8c 2e c1 e4 00 50 9e 63 57 49 00 00 00 80 02P.C WI.....
0030 20 00 1d 33 00 00 02 04 05 b4 01 03 03 02 01 01 ..3.....
0040 04 02 ..

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 - Displayed: 266 (100.0%) - Load time: 0:00.005 Profile: Default







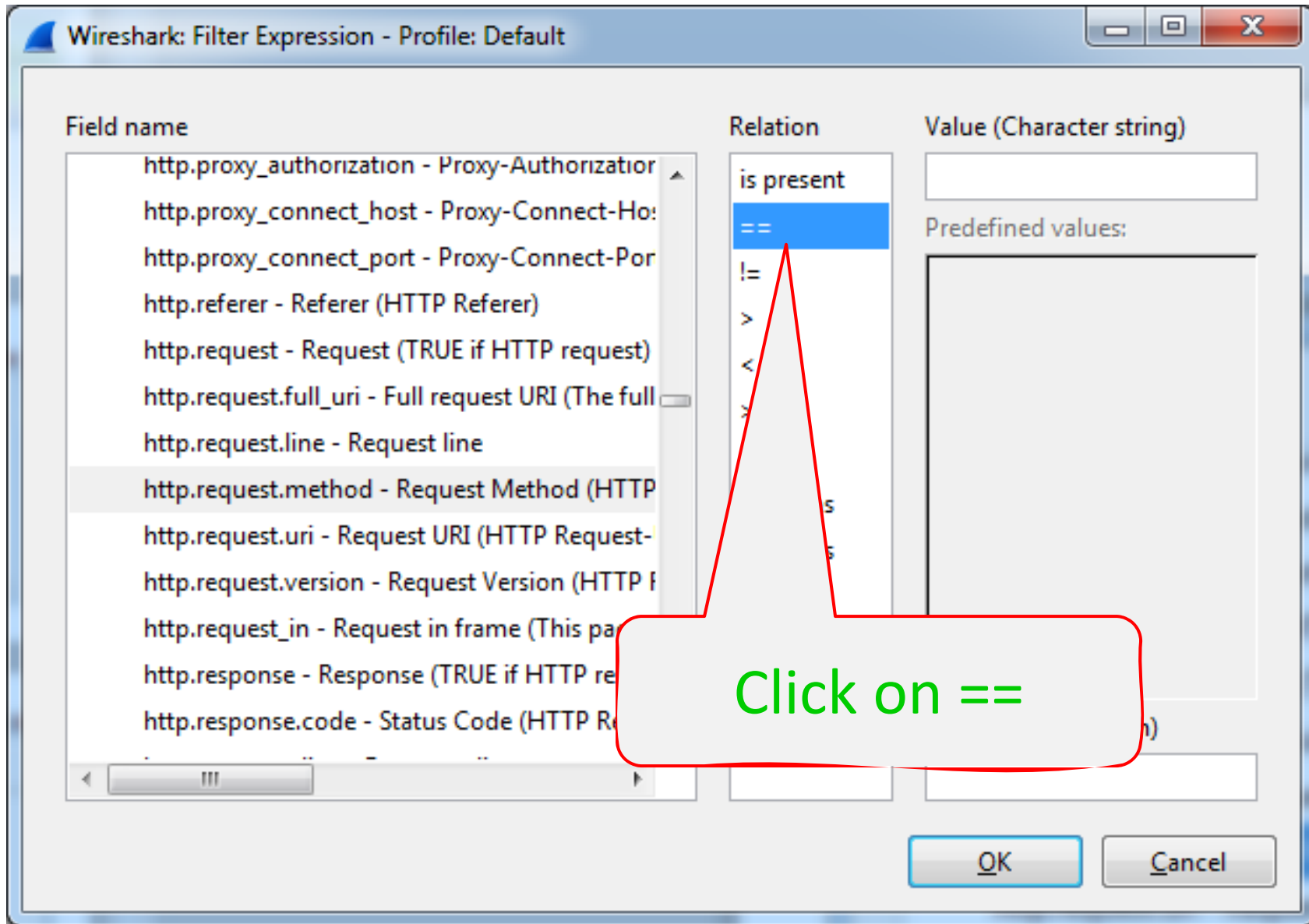


Wireshark: Filter Expression - Profile: Default

| Field name | Relation | Value (Character string) |
|--|------------|--------------------------|
| http.proxy_authorization - Proxy-Authorization | is present | <input type="text"/> |
| http.proxy_connect_host - Proxy-Connect-Ho: | == | Predefined values: |
| http.proxy_connect_port - Proxy-Connect-Por | != | <div></div> |
| http.referer - Referer (HTTP Referer) | > | |
| http.request - Request (TRUE if HTTP request) | < | |
| http.request.full_uri - Full request URI (The full | >= | |
| http.request.line - Request line | <= | |
| http.request.method - Request Method (HTTP | contains | |
| http.request.uri - Request URI (HTTP Request- | matches | |
| http.request.version - Request Version (HTTP | | |
| http.request_in - Request in frame (This packe | | |
| http.response - Response (TRUE if HTTP respo | | |
| http.response.code - Status Code (HTTP Respo | | |

Range (offset:length)

OK Cancel



Wireshark: Filter Expression - Profile: Default

| Field name | Relation | Value (Character string) |
|--|------------|--------------------------|
| http.proxy_authorization - Proxy-Authorization | is present | GET |
| http.proxy_connect_host - Proxy-Connect-Ho: | == | Predefined values: |
| http.proxy_connect_port - Proxy-Connect-Por | != | |
| http.referer - Referer (HTTP Referer) | > | |
| http.request - Request (TRUE if HTTP request) | < | |
| http.request.full_uri - Full request URI (The full | >= | |
| http.request.line - Request line | <= | |
| http.request.method - Request Method (HTTP | contains | |
| http.request.uri - Request URI (HTTP Request- | matches | |
| http.request.version - Request Version (HTTP | | |
| http.request_in - Request in frame (This packe | | |
| http.response - Response (TRUE if HTTP respo | | |
| http.response.code - Status Code (HTTP Respo | | |

Range (offset:length)

OK Cancel

Type in GET



CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: `http.request.method == "GET"` Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|-------------|----------------|----------|--------|---|
| 10 | 1.063255 | 192.168.1.7 | 65.55.84.56 | HTTP | 516 | GET /?ocid=iehp HTTP/1.1 |
| 65 | 1.471377 | 192.168.1.7 | 65.55.253.27 | HTTP | 1049 | GET /c.gif?evt=impr&js=1&rid=45def397b817495bae983b0f282b2c51&exa=&pp=False&bd=&gnd=&cts=1 |
| 72 | 1.499904 | 192.168.1.7 | 207.46.193.176 | HTTP | 489 | GET /action/MSN_Homepage_Remessaging_111808/nc?a=1 HTTP/1.1 |
| 77 | 1.508578 | 192.168.1.7 | 67.148.147.113 | HTTP | 527 | GET /b?c1=2&c2=3000001&c7=http%3A%2F%2Fwww.msn.com%2F%3Focid%3Ddiehp&c9=&rn=1332688523104 |
| 84 | 1.538291 | 192.168.1.7 | 207.46.140.46 | HTTP | 802 | GET /default.aspx?parsergroup=hops&fk=w&gp=P&optkey=default&cp=default&r=f&di=340&pi=73178 |
| 91 | 1.593353 | 192.168.1.7 | 64.4.21.39 | HTTP | 680 | GET /c.gif?udc=true&di=340&pi=7317&ps=95101&lng=en-us&tp=http%3A%2F%2Fwww.msn.com%2Fdefaul |
| 94 | 1.598267 | 192.168.1.7 | 204.245.34.139 | HTTP | 578 | GET /partner/primedns.gif HTTP/1.1 |
| 104 | 1.854517 | 192.168.1.7 | 204.245.34.139 | HTTP | 710 | GET /sck?cn=_55&r=http://www.msn.com/sck.aspx&form=MSN005&h=fe92cd76-4cb3-03b6-8afc-cd7f85 |
| 115 | 1.986251 | 192.168.1.7 | 63.235.36.105 | HTTP | 483 | GET /qsonhs.aspx?form=MSN005&q= HTTP/1.1 |
| 119 | 2.043988 | 192.168.1.7 | 65.55.84.56 | HTTP | 837 | GET /sck.aspx?cv=_55&3dSID%3d7C73BA2D0DBD452E95C8DB3AFE1879B0%3b&h=fe92cd76-4cb3-03b6-8afc |
| 122 | 2.056281 | 192.168.1.7 | 65.55.5.232 | HTTP | 636 | GET /ADSAdClient31.d11?GetSAd=&DPJS=4&PN=MSFT&ID=15A78A4A61DA691C0F38896465DA6922&MUID=15A |
| 129 | 2.188858 | 192.168.1.7 | 204.245.34.139 | HTTP | 636 | GET /msnhompagehistory.aspx?sid=7C73BA2D0DBD452E95C8DB3AFE1879B0&_id=1332688523926 HTTP/1.1 |
| 149 | 2.414240 | 192.168.1.7 | 65.55.5.232 | HTTP | 638 | GET /ADSAdClient31.d11?GetSAd=&DPJS=4&PN=MSFT&ID=15A78A4A61DA691C0F38896465DA6922&MUID=15A |
| 164 | 2.502977 | 192.168.1.7 | 65.55.5.232 | HTTP | 638 | GET /ADSAdClient31.d11?GetSAd=&DPJS=4&PN=MSFT&ID=15A78A4A61DA691C0F38896465DA6922&MUID=15A |
| 165 | 2.503215 | 192.168.1.7 | 65.55.5.232 | HTTP | 638 | GET /ADSAdClient31.d11?GetSAd=&DPJS=4&PN=MSFT&ID=15A78A4A61DA691C0F38896465DA6922&MUID=15A |
| 169 | 2.533468 | 192.168.1.7 | 65.55.5.232 | HTTP | 638 | GET /ADSAdClient31.d11?GetSAd=&DPJS=4&PN=MSFT&ID=15A78A4A61DA691C0F38896465DA6922&MUID=15A |
| 183 | 2.651686 | 192.168.1.7 | 75.98.29.8 | HTTP | 678 | GET /cookie/geoip/iframe?spacedesc=2186184_1116771_300x120_2186181_2186184&target=_blank&@C |
| 199 | 2.875084 | 192.168.1.7 | 75.98.29.8 | HTTP | 851 | GET /x1/PROD/19706/creatives/mat_boygr1_fbsingle_RePopScrollImgDssIveFadeForm_vsgeo_Mgendc |

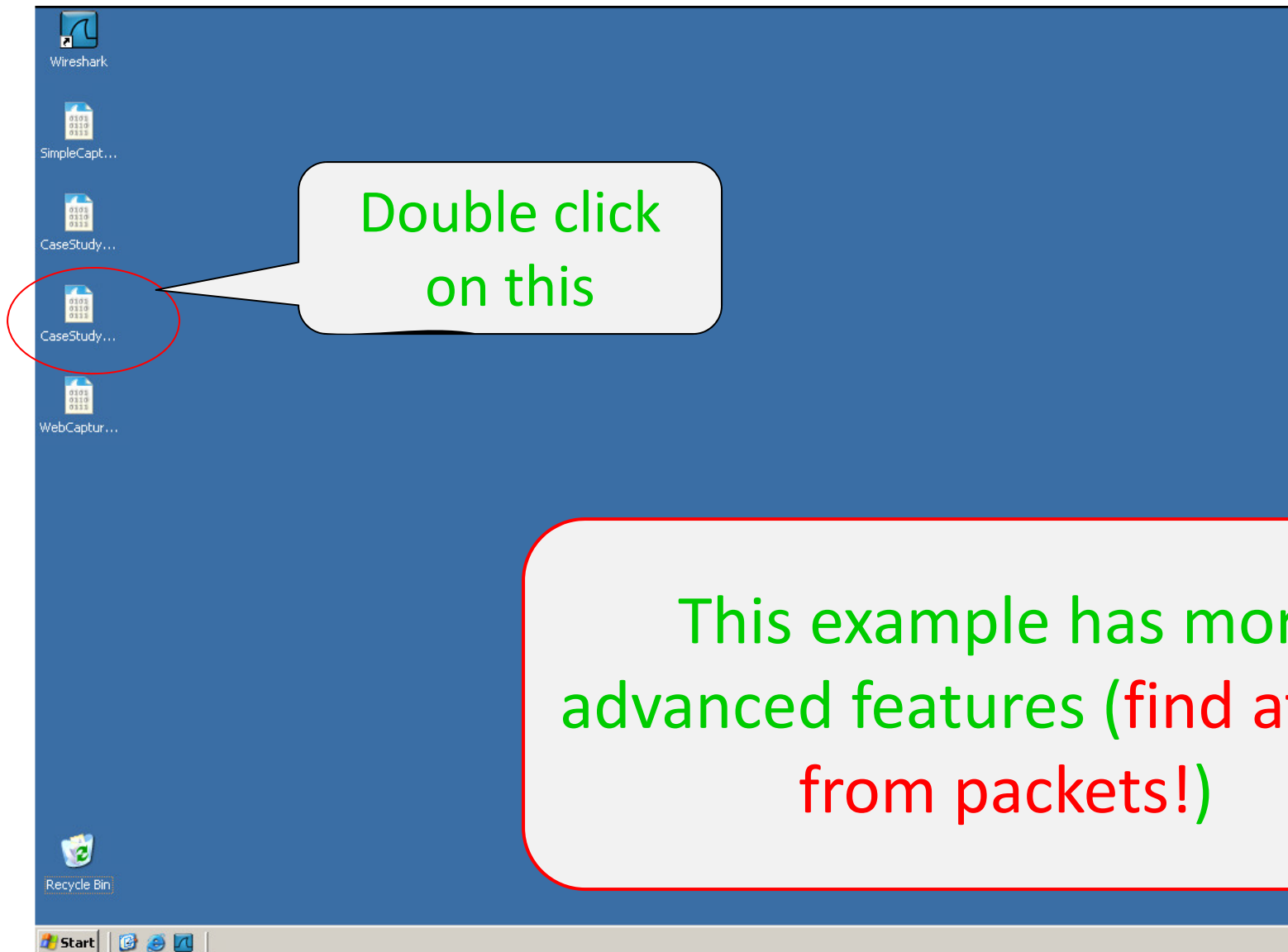
Frame 10: 516 bytes on wire (4128 bits), 516 bytes captured (4128 bits) on interface 0
Ethernet II, Src: Vmware_db:f6:71 (00:0c:29:db:f6:71), Dst: 65.55.84.56 (65.55.84.56)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 65.55.84.56
Transmission Control Protocol, Src Port: 5555, Dst Port: 80, Seq: 1, Ack: 1, Len: 462
Hypertext Transfer Protocol

This panel has fewer packets, easier to study

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00)..q..E.
0010 01 f6 16 d5 40 00 80 06 00 00 c0 a8 01 07 41 37@... ..A7
0020 54 38 c1 e3 00 50 f8 9c 14 b8 aa 49 97 cd 50 18 T8...P...I..P.
0030 fa f0 59 07 00 00 47 45 54 20 2f 3f 6f 63 69 64 ..Y...GE T /?ocid
0040 3d 69 65 68 70 20 48 54 54 50 2f 31 2e 31 0d 0a =iehp HT TP/1.1..
0050 41 62 62 65 70 74 22 20 22 2f 22 0d 02 41 62 62 .../.../.../...

File: "C:\tmp\Boot-capture\CaseStudy1.pca... Packets: 266 · Displayed: 22 (8.3%) · Load time: 0:00.005 Profile: Default

Exercise 2





CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 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 | fe80::9ce2:41a0:6715:cf12 | ff02::1:2 | DHCPv6 | 157 | Solicit XID: 0x267e0f CID: 000100011701d2b4000c29ff71d1 |
| 2 | 12.957913 | Vmware_ff:71:d1 | Broadcast | ARP | 42 | who has 192.168.1.1? Tell 192.168.1.105 |
| 3 | 12.959857 | Cisco-Li_bb:6b:fe | Vmware_ff:71:d1 | ARP | 60 | 192.168.1.1 is at 00:0f:66:bb:6b:fe |
| 4 | 12.959881 | 192.168.1.105 | 68.105.28.11 | DNS | 76 | Standard query 0x3f60 A go.microsoft.com |
| 5 | 12.975699 | 68.105.28.11 | 192.168.1.105 | DNS | 545 | Standard query response 0x3f60 CNAME www.go.microsoft.akadns.net A 65.55.57.251 |
| 6 | 16.086567 | Vmware_5a:49:c4 | Broadcast | ARP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| 7 | 16.086608 | Vmware_ff:71:d1 | Vmware_5a:49:c4 | ARP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| 8 | 16.104430 | Vmware_5a:49:c4 | Broadcast | ARP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| 9 | 16.104470 | Vmware_ff:71:d1 | Vmware_5a:49:c4 | ARP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-1720 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 13 | 16.114045 | Vmware_ff:71:d1 | Broadcast | ARP | 42 | who has 192.168.1.104? Tell 192.168.1.105 |
| 14 | 16.114648 | Vmware_5a:49:c4 | Vmware_ff:71:d1 | ARP | 60 | 192.168.1.104 is at 00:0c:29:5a:49:c4 |
| 15 | 16.114665 | 192.168.1.105 | 192.168.1.104 | TCP | 54 | 111-58368 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3389 [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-139 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 18 | 16.124550 | 192.168.1.105 | 192.168.1.104 | TCP | 58 | 3389-58368 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 |

Frame 1: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits) on interface 0
Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: ff02::1:2 (01:00:5e:00:00:02)
Internet Protocol Version 6, Src: fe80::9ce2:41a0:6715:cf12, Dst: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: 546 (546), Dst Port: 546 (546)
DHCPv6

This example has many (too many?) packets

0000 33 33 00 01 00 02 00 0c 29 ff 71 d1 86 dd 60 00 33.....).q...
0010 00 00 00 67 11 01 fe 80 00 00 00 00 00 9c e2 ...g.....
0020 41 a0 67 15 cf 12 ff 02 00 00 00 00 00 00 00 A.g.....
0030 00 00 00 01 00 02 02 22 02 23 00 67 5e f5 01 26".#.g^..&
0040 7e 0f 00 08 00 02 18 9c 00 01 00 0e 00 01 00 01 ~.....
0050 17 01 d3 b4 00 0c 20 ff 71 d1 00 02 00 0c 00 00
File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 204914 (100.0%) · Load time: 0:02.379 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze **Statistics** Telephony Tools Internals Help

Summary
Comments Summary
Show address resolution
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graph
Conversation List
Endpoint List
Service Response Time
29West
ANCP
BACnet
Collectd...
Compare...
Flow Graph...
HART-IP
HTTP
ONC-RPC Programs
Sametime
TCP StreamGraph
UDP Multicast Streams
WLAN Traffic
IP Statistics
BOOTP-DHCP...

Filter:

| No. | Time | Source |
|-----|-----------|---------------------------|
| 1 | 0.000000 | fe80::9ce2:41a0:6715:cf12 |
| 2 | 12.957913 | Vmware_ff:71 |
| 3 | 12.959857 | Cisco-Li_bb:6 |
| 4 | 12.959881 | 192.168.1.105 |
| 5 | 12.975699 | 68.105.28.11 |
| 6 | 16.086567 | Vmware_5a:49 |
| 7 | 16.086608 | Vmware_ff:71 |
| 8 | 16.104430 | Vmware_5a:49 |
| 9 | 16.104470 | Vmware_ff:71 |
| 10 | 16.113894 | 192.168.1.104 |
| 11 | 16.113896 | 192.168.1.104 |
| 12 | 16.113897 | 192.168.1.104 |
| 13 | 16.114045 | Vmware_ff:71 |
| 14 | 16.114648 | Vmware_5a:49 |
| 15 | 16.114665 | 192.168.1.105 |
| 16 | 16.124352 | 192.168.1.104 |
| 17 | 16.124355 | 192.168.1.104 |
| 18 | 16.124550 | 192.168.1.105 |

Protocol Length Info

| Protocol | Length | Info |
|----------|--------|---|
| DHCPv6 | 157 | Solicit XID: 0x267e0f CID: 000100011701d2b4000c29ff71d1 |
| IRP | 42 | who has 192.168.1.1? Tell 192.168.1.105 |
| IRP | 60 | 192.168.1.1 is at 00:0f:66:bb:6b:fe |
| NS | 76 | Standard query 0x3f60 A go.microsoft.com |
| NS | 545 | Standard query response 0x3f60 CNAME www.go.microsoft.akadns.net A 65.55.57.251 |
| IRP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| IRP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| IRP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| IRP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| CP | 60 | 58368-1720 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| CP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| CP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| IRP | 42 | who has 192.168.1.104? Tell 192.168.1.105 |
| IRP | 60 | 192.168.1.104 is at 00:0c:29:5a:49:c4 |
| CP | 54 | 111-58368 [RST, ACK] Seq=1 Ack=1 win=0 Len=0 |
| CP | 60 | 58368-3389 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| CP | 60 | 58368-139 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| CP | 58 | 3389-58368 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 |

Frame 1: 157 bytes on wire (1256 bits)
Ethernet II, Src: Vmware_ff:71:d1:86:dd:60, Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)
Internet Protocol Version 6, Src: fe80::9ce2:41a0:6715:cf12, Dst: ff02::1:2 (ff02::1:2)
User Datagram Protocol, Src Port: 547, Dst Port: 547
DHCPv6

0000 33 33 00 01 00 02 00 0c 29 ff 71 d1 86 dd 60 00 33.....).q...
0010 00 00 00 67 11 01 fe 80 00 00 00 00 00 00 9c e2 ...g...
0020 41 a0 67 15 cf 12 ff 02 00 00 00 00 00 00 00 00 A.g...
0030 00 00 00 01 00 02 02 22 02 23 00 67 5e f5 01 26".g^..&
0040 7e 0f 00 08 00 02 18 9c 00 01 00 0e 00 01 00 01 ~.....
0050 17 01 d2 b4 00 0c 29 ff 71 d1 00 02 00 0c 00 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 204914 (100.0%) · Load time: 0:02.379 Profile: Default



Wireshark: Protocol Hierarchy Statistics

Display filter: none

| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Packets | End Bytes | End Mbit/s |
|--|-----------|---------|----------|----------|--------|-------------|-----------|------------|
| Frame | 100.00 % | 204914 | 100.00 % | 21959465 | 0.788 | 0 | 0 | 0.000 |
| Ethernet | 100.00 % | 204914 | 100.00 % | 21959465 | 0.788 | 0 | 0 | 0.000 |
| Internet Protocol Version 6 | 0.00 % | 3 | 0.00 % | 327 | 0.000 | 0 | 0 | 0.000 |
| User Datagram Protocol | 0.00 % | 3 | 0.00 % | 327 | 0.000 | 0 | 0 | 0.000 |
| DHCPv6 | 0.00 % | 1 | 0.00 % | 157 | 0.000 | 1 | 157 | 0.000 |
| Domain Name Service | 0.00 % | 2 | 0.00 % | 170 | 0.000 | 2 | 170 | 0.000 |
| Address Resolution Protocol | 0.01 % | 19 | 0.00 % | 1014 | 0.000 | 19 | 1014 | 0.000 |
| Internet Protocol Version 4 | 99.99 % | 204892 | 99.99 % | 21958124 | 0.788 | 0 | 0 | 0.000 |
| User Datagram Protocol | 0.17 % | 342 | 0.33 % | 72921 | 0.003 | 0 | 0 | 0.000 |
| Domain Name Service | 0.15 % | 315 | 0.30 % | 66585 | 0.002 | 315 | 66585 | 0.002 |
| NetBIOS Datagram Service | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 | 0.000 |
| SMB (Server Message Block Protocol) | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 | 0.000 |
| SMB MailSlot Protocol | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 | 0.000 |
| Microsoft Windows Browser Protocol | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 9 | 2076 | 0.000 |
| Data | 0.00 % | 4 | 0.01 % | 1964 | 0.000 | 4 | 1964 | 0.000 |
| Hypertext Transfer Protocol | 0.01 % | 12 | 0.01 % | 2100 | 0.000 | 12 | 2100 | 0.000 |
| NetBIOS Name Service | 0.00 % | 2 | 0.00 % | 196 | 0.000 | 2 | 196 | 0.000 |
| Transmission Control Protocol | 99.82 % | 204550 | 99.66 % | 21885203 | 0.785 | 9555 | 4092824 | 0.147 |
| Hypertext Transfer Protocol | 0.71 % | 1449 | 4.54 % | 996229 | 0.036 | 786 | 510981 | 0.018 |
| Line-based text data | 0.12 % | 241 | 0.86 % | 189259 | 0.007 | 241 | 189259 | 0.007 |
| CompuServe GIF | 0.09 % | 177 | 0.51 % | 112399 | 0.004 | 177 | 112399 | 0.004 |
| Media Type | 0.02 % | 38 | 0.13 % | 27454 | 0.001 | 38 | 27454 | 0.001 |
| JPEG File Interchange Format | 0.05 % | 108 | 0.39 % | 86042 | 0.003 | 108 | 86042 | 0.003 |
| Portable Network Graphics | 0.02 % | 46 | 0.16 % | 36023 | 0.001 | 46 | 36023 | 0.001 |
| JavaScript Object Notation | 0.02 % | 36 | 0.09 % | 20632 | 0.001 | 3 | 598 | 0.000 |
| Line-based text data | 0.02 % | 33 | 0.09 % | 20034 | 0.001 | 33 | 20034 | 0.001 |
| Text item | 0.00 % | 1 | 0.01 % | 1304 | 0.000 | 1 | 1304 | 0.000 |
| Online Certificate Status Protocol | 0.01 % | 11 | 0.04 % | 9402 | 0.000 | 11 | 9402 | 0.000 |
| eXtensible Markup Language | 0.00 % | 1 | 0.00 % | 996 | 0.000 | 1 | 996 | 0.000 |
| Malformed Packet | 0.00 % | 3 | 0.00 % | 710 | 0.000 | 3 | 710 | 0.000 |
| HTML Form URL Encoded | 0.00 % | 1 | 0.00 % | 1027 | 0.000 | 1 | 1027 | 0.000 |
| Secure Sockets Layer | 0.03 % | 61 | 0.12 % | 26352 | 0.001 | 50 | 25240 | 0.001 |
| Secure Sockets Layer | 0.00 % | 2 | 0.01 % | 1103 | 0.000 | 2 | 1103 | 0.000 |
| File Transfer Protocol (FTP) | 94.40 % | 193445 | 76.30 % | 16755478 | 0.601 | 1 | 1 | 0.000 |
| Malformed Packet | 0.01 % | 18 | 0.05 % | 10257 | 0.000 | 18 | 10257 | 0.000 |
| NetBIOS Session Service | 0.01 % | 18 | 0.01 % | 2822 | 0.000 | 2 | 100 | 0.000 |
| SMB (Server Message Block Protocol) | 0.01 % | 16 | 0.01 % | 2626 | 0.000 | 12 | 1886 | 0.000 |
| SMB Pipe Protocol | 0.00 % | 1 | 0.00 % | 1027 | 0.000 | 1 | 1027 | 0.000 |
| Microsoft Windows Lanman Remote API Protocol | 0.00 % | 1 | 0.00 % | 1027 | 0.000 | 1 | 1027 | 0.000 |
| FTP Data | 0.00 % | 1 | 0.00 % | 1027 | 0.000 | 1 | 1027 | 0.000 |

Help

This is suspicious

How to further investigate?



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: **ftp** Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|------------------------------|-----------------|----------|--------|---|
| 1 | 0.00000 | fe80::9ce2:41a0:671ff02::1:2 | ff02::1:2 | DHCPv6 | 157 | Solicit XID: 0x267e0f CID: 000100011701d2b4000c29ff71d1 |
| 2 | 12.95791 | vmware_ff:71:d1 | Broadcast | ARP | 42 | who has 192.168.1.1? Tell 192.168.1.105 |
| 3 | 12.959857 | vmware_Li_bb:6b:fe | vmware_ff:71:d1 | ARP | 60 | 192.168.1.1 is at 00:0f:66:bb:6b:fe |
| 4 | 12.959881 | 192.168.1.105 | 68.105.28.11 | DNS | 76 | Standard query 0x3f60 A go.microsoft.com |
| 5 | 12.975699 | 68.105.28.11 | 192.168.1.105 | DNS | 545 | Standard query response 0x3f60 CNAME www.go.microsoft.akadns.net A 65.55.57.251 |
| 6 | 16.086567 | vmware_5a:49:c4 | Broadcast | ARP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| 7 | 16.086608 | vmware_5a:49:c4 | vmware_5a:49:c4 | ARP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| 8 | 16.104430 | vmware_5a:49:c4 | Broadcast | ARP | 60 | who has 192.168.1.105? Tell 192.168.1.104 |
| 9 | 16.104470 | vmware_5a:49:c4 | vmware_5a:49:c4 | ARP | 42 | 192.168.1.105 is at 00:0c:29:ff:71:d1 |
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-1720 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.105 | 192.168.1.104 | TCP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 13 | 16.114045 | vmware_ff:71:d1 | 192.168.1.104 | ARP | 42 | who has 192.168.1.104? Tell 192.168.1.105 |
| 14 | 16.114648 | vmware_5a:49:c4 | 192.168.1.104 | ARP | 60 | 192.168.1.104 is at 00:0c:29:5a:49:c4 |
| 15 | 16.114665 | 192.168.1.105 | 192.168.1.104 | TCP | 54 | 111-58368 [RST, ACK] Seq=1 Ack=1 win=0 Len=0 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3389 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.105 | 192.168.1.104 | TCP | 60 | 58368-120 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 18 | 16.124550 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-120 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |

Frame 1: 157 bytes on wire (Ethernet II, Src: Vmware_5a:49:c4, Dst: ff:ff:ff:ff:ff:ff, Type: DHCPv6 Solicit) Internet Protocol Version 6, Src: fe80::9ce2:41a0:671ff02::1:2, Dst: ff02::1:2 User Datagram Protocol, Src Port: 58368, Dst Port: 1720 DHCPv6

0000 33 33 00 01 00 02 00 0c 29 ff 71 d1 86 dd 60 00 33.....).q...
0010 00 00 00 67 11 01 fe 80 00 00 00 00 00 00 9c e2 ...g....
0020 41 a0 67 15 cf 12 ff 02 00 00 00 00 00 00 00 00 A.g....
0030 00 00 00 01 00 02 02 22 02 23 00 67 5e f5 01 26".#.g^..&
0040 7e 0f 00 08 00 02 18 9c 00 01 00 0e 00 01 00 01 ~.....
0050 17 01 d2 b4 00 0c 29 ff 71 d1 00 02 00 0c 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 204914 (100.0%) · Load time: 0:02.379 Profile: Default

We need to reduce the # of packets. Type this



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|-------------------------------------|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3444 | 52.738843 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3445 | 52.739045 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3446 | 52.739220 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3447 | 52.739428 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3448 | 52.739601 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3449 | 52.739819 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3450 | 52.739977 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3474 | 52.750934 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3475 | 52.751130 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3476 | 52.751302 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3477 | 52.751472 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3478 | 52.751644 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3479 | 52.751864 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3480 | 52.752035 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3481 | 52.752206 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3482 | 52.752400 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3483 | 52.752602 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |

Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 b...
Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware... (00:0c:29:5a:49:c4)
Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), D... (192.168.1.104)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (... Ack: 1, Len: 27
File Transfer Protocol (FTP)

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ...ZI...).q...E.
0010 00 4f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8 ...o. @... ..i..
0020 01 68 00 15 bd b2 e0 9e eb ed 3b ac 23 cb 80 18 ...h..... ;.#...
0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b ...C.....
0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20 o[220 Mi crosoft
0050 46 54 50 20 63 65 72 76 60 62 65 0d 02 ...FTP serv ice

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 193445 (94.4%) · Load time: 0:02.500 Profile: Default

This panel has fewer packets
but how to proceed?



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: ftp

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|-------------------------------------|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3444 | 52.738843 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3445 | 52.739045 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3446 | 52.739220 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3447 | 52.739428 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3448 | 52.739601 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3449 | 52.739819 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3450 | 52.739977 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3474 | 52.750934 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3475 | 52.751130 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3476 | 52.751302 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3477 | 52.751472 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3478 | 52.751644 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3479 | 52.751864 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3480 | 52.752035 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3481 | 52.752206 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3482 | 52.752400 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3483 | 52.752602 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |

Click on the first packet

Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

- Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)
- Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)
- Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (48562), Seq: 1, Ack: 1, Len: 27
 - Source Port: 21 (21)
 - Destination Port: 48562 (48562)
 - [Stream index: 1137]
 - [TCP Segment Len: 27]
 - Sequence number: 1 (relative sequence number)
 - [Next sequence number: 28 (relative sequence number)]
 - Acknowledgment number: 1 (relative ack number)
 - Header Length: 32 bytes
 - 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
 - Window size value: 260
 - [Calculated window size: 66560]
 - [Window size scaling factor: 256]
 - Checksum: 0x8463 [validation disabled]
 - Urgent pointer: 0
 - Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 - [SEQ/ACK analysis]
- File Transfer Protocol (FTP)
 - 220 Microsoft FTP Service\r\n
 - Response code: Service ready for new user (220)
 - Response arg: Microsoft FTP Service

The details of the first packet

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ..)21...).q...E.
0010 00 4f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8 .o.@...i..
0020 01 68 00 15 bd b2 e0 9e eb ed 3b ac 23 cb 80 18 .h.....:;#...
0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b ...C.....
0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20 o[220 Mi crosoft
0050 46 54 50 00 53 65 72 76 60 62 65 0d 0a 00 00 00 FTP Serv ice

Frame (frame), 93 bytes Packets: 204914 · Displayed: 193445 (94.4%) · Load time: 0:02.500 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: ftp Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|-------------------------------------|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3444 | 52.738843 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3445 | 52.739045 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3446 | 52.739220 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3447 | 52.739428 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3448 | 52.739601 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3449 | 52.739819 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3450 | 52.739977 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3474 | 52.750934 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3475 | 52.751130 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3476 | 52.751302 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3477 | 52.751472 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3478 | 52.751644 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3479 | 52.751864 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3480 | 52.752035 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3481 | 52.752206 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3482 | 52.752400 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3483 | 52.752602 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |

Click on the second packet

Frame 3444: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)

Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48563 (48563), Seq: 1, Ack: 1, Len: 27

Source Port: 21 (21)

Destination Port: 48563 (48563)

[Stream index: 1138]

[TCP Segment Len: 27]

Sequence number: 1 (relative sequence number)

[Next sequence number: 28 (relative sequence number)]

Acknowledgment number: 1 (relative acknowledgment number)

Header Length: 32 bytes

... 0000 0001 1000 = Flags: 0x018

window size value: 260

[calculated window size: 66560]

[window size scaling factor: 256]

Checksum: 0x8463 [validation disabled]

Urgent pointer: 0

Options: (12 bytes), No-operation (NOP), No-operation

[SEQ/ACK analysis]

File Transfer Protocol (FTP)

220 Microsoft FTP Service\r\n

Response code: Service ready for new user

Response arg: Microsoft FTP Service

The details of the 2nd packet

Close but a different number from the first packet

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71
0010 00 4f 11 61 40 00 80 06 00 00 c0
0020 01 68 00 15 bd b3 5e a3 32 2d 3b
0030 01 04 84 63 00 00 01 01 08 0a 00
0040 6f 5b 32 32 30 20 4d 69 63 72 6f
0050 46 54 50 20 52 65 72 76 60 63 65

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 193445 (94.4%) · Load time: 0:02.500 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: `ftp && tcp.dstport == 48652 || tcp.srcport == 48652`

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|-------------------------------------|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3444 | 52.738843 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3445 | 52.739045 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3446 | 52.739220 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3447 | 52.739428 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3448 | 52.739601 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3449 | 52.739819 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3450 | 52.739977 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3474 | 52.750934 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3475 | 52.751130 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3476 | 52.751302 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3477 | 52.751472 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3478 | 52.751644 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3479 | 52.751864 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3480 | 52.752035 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3481 | 52.752206 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3482 | 52.752400 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3483 | 52.752602 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |

Frame 3444: 93 bytes on wire (744 bytes captured) on interface 0
Ethernet II, Src: Vmware_ff:71:d1:08, Dst: Vmware_08:00:45:00:00:00
Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.104
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48563 (48563)
[Stream index: 1138]
[TCP Segment Len: 27]
Sequence number: 1 (relative to stream start)
[Next sequence number: 28 (relative to stream start)]
Acknowledgment number: 1 (relative to stream start)
Header Length: 32 bytes
... 0000 0001 1000 = Flags: PSH, ACK
window size value: 260
[Calculated window size: 66560]
[window size scaling factor: 256]
Checksum: 0x8463 [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-operation (NOP), No-operation (NOP), Timestamps
[SEQ/ACK analysis]
File Transfer Protocol (FTP)
220 Microsoft FTP Service\r\n
Response code: Service ready for new user (220)
Response arg: Microsoft FTP Service

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ..)ZI...).q...E.
0010 00 4f 11 61 40 00 80 06 00 00 c0 a8 01 69 c0 a8 .O.a@...i..
0020 01 68 00 15 bd b3 5e a3 32 2d 3b 2a ac 95 80 18 .h...^.. 2-;*....
0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b ...C... ..
0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20 o[220 Mi crosoft
0050 46 54 50 20 52 65 72 76 60 63 65 6d 00 00 00 00 FTP serv ice

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 193445 (94.4%) · Load time: 0:02:500 Profile: Default

We want to further reduce the #
of packets; type this (typo: it
should be 48562)



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: ftp && tcp.dstport == 48562 || tcp.srcport == 48562

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|---|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3515 | 52.754697 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3525 | 52.755195 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3556 | 52.757133 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 10th |
| 3619 | 52.775231 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3640 | 52.779121 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3662 | 52.781680 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3682 | 52.791395 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 1ht9 |
| 3721 | 52.796573 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3727 | 52.797271 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3775 | 52.802426 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3779 | 52.802861 | 192.168.1.104 | 192.168.1.105 | FTP | 81 | Request: PASS abalone1 |
| 3831 | 52.810754 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3836 | 52.811379 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3890 | 52.817932 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3896 | 52.818698 | 192.168.1.104 | 192.168.1.105 | FTP | 78 | Request: PASS 1ebba |
| 3951 | 52.825836 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3961 | 52.826452 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |

Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0 (00:0c:29:5a:49:c4)

Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_00:0c:29:5a:49:c4 (00:0c:29:5a:49:c4)

Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (48562), Seq: 1, Ack: 1, Len: 27

Source Port: 21 (21)

Destination Port: 48562 (48562)

[Stream index: 1137]

[TCP Segment Len: 27]

Sequence number: 1 (relative sequence number)

[Next sequence number: 28 (relative sequence number)]

Acknowledgment number: 1 (relative ack number)

Header Length: 32 bytes

.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

Window size value: 260

[Calculated window size: 66560]

[Window size scaling factor: 256]

Checksum: 0x8463 [validation disabled]

Urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation

[SEQ/ACK analysis]

File Transfer Protocol (FTP)

220 Microsoft FTP Service\r\n

Response code: Service ready for new user (220)

Response arg: Microsoft FTP Service

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00

0010 00 4f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8

0020 01 68 00 15 bd b2 e0 9e eb ed 3b ac 23 cb 80 18

0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b

0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20

0050 46 54 50 20 53 65 72 76 60 63 65 0d 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 5387 (2.6%) · Load time: 0:02:591

Profile: Default

This panel has fewer packets and it is clearer. Why?



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: `ftp && ftp.response.arg == "User logged in."`

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|---|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3515 | 52.754697 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3525 | 52.755195 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3556 | 52.757133 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 10th |
| 3619 | 52.775231 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3640 | 52.779121 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3662 | 52.781680 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3682 | 52.791395 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 1ht9 |
| 3721 | 52.796573 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3727 | 52.797271 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3775 | 52.802426 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3779 | 52.802861 | 192.168.1.104 | 192.168.1.105 | FTP | 81 | Request: PASS abalone1 |
| 3831 | 52.810754 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3836 | 52.811379 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3890 | 52.817932 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3896 | 52.818698 | 192.168.1.104 | 192.168.1.105 | FTP | 78 | Request: PASS 1ebba |
| 3951 | 52.825836 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3961 | 52.826452 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |

Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 0
Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_08:00:27:5a:49:c4 (00:0c:29:5a:49:c4)
Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (48562), Seq: 1, Len: 27
Source Port: 21 (21)
Destination Port: 48562 (48562)
[Stream index: 1137]
[TCP Segment Len: 27]
Sequence number: 1 (relative sequence number)
[Next sequence number: 28 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes
... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 260
[Calculated window size: 66560]
[window size scaling factor: 256]
Checksum: 0x8463 [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-operation (NOP), No-operation
[SEQ/ACK analysis]
File Transfer Protocol (FTP)
220 Microsoft FTP Service\r\n
Response code: Service ready for new user (220)
Response arg: Microsoft FTP Service

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00
0010 00 4f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8
0020 01 68 00 15 bd b2 e0 9e eb ed 3b ac 23 cb 80 18
0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b
0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20
0050 46 54 50 20 52 65 72 76 60 63 65 6d 00 00 00 00
o[220 Mi crosoft
FTP serv ice

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 5387 (2.6%) · Load time: 0:02.591 Profile: Default

It is a password brute-forcing attack. Let's type in to check whether it succeeded



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: ftp && ftp.response.arg == "User logged in." Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|--------|------------|---------------|---------------|----------|--------|-------------------------------|
| 202103 | 114.041576 | 192.168.1.105 | 192.168.1.104 | FTP | 87 | Response: 230 user logged in. |
| 203754 | 154.825849 | 192.168.1.105 | 192.168.1.104 | FTP | 87 | Response: 230 user logged in. |

Frame 202103: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)

Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)

Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48588 (48588), Seq: 79637, Ack: 33657, Len: 21

Source Port: 21 (21)

Destination Port: 48588 (48588)

[Stream index: 1163]

[TCP Segment Len: 21]

Sequence number: 79637 (relative sequence number)

[Next sequence number: 79658 (relative sequence number)]

Acknowledgment number: 33657 (relative ack number)

Header Length: 32 bytes

... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)

window size value: 259

[calculated window size: 66304]

[window size scaling factor: 256]

checksum: 0x845d [validation disabled]

urgent pointer: 0

Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

[SEQ/ACK analysis]

File Transfer Protocol (FTP)

230 user logged in.\r\n

Response code: User logged in, proceed (230)

Response arg: User logged in.

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ..)ZI...).q...E.

0010 00 49 20 4f 40 00 80 06 00 00 c0 a8 01 69 c0 a8 .I O@...i..

0020 01 68 00 15 bd cc 75 fd cc c9 3b a9 2b 10 80 18 .h...u. .;.+...

0030 01 03 84 5d 00 01 01 08 0a 00 04 e3 98 00 0b ...]....

0040 ab 27 32 33 30 20 55 73 65 72 20 6c 6f 67 67 65 .230 us er logge

0050 64 20 60 60 20 0d 02 ..

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 2 (0.0%) · Load time: 0:02.695

Profile: Default

The attack indeed
succeeded!



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp && ftp.response.arg ==

| No. | Time | Source |
|--------|------------|---------------|
| 202103 | 114.041576 | 192.168.1.105 |
| 203754 | 154.825849 | 192.168.1.104 |

Display Filters...
Display Filter Macros...
Apply as Column
Apply as Filter
Prepare a Filter
Enabled Protocols... Shift+Ctrl+E
Decode As...
User Specified Decodes...
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Expert Info
Conversation Filter

Protocol Length Info
FTP 87 Response: 230 user logged in.
FTP 87 Response: 230 user logged in.

Frame 202103: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)
Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)
Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)
Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48588 (48588), Seq: 79637, Ack: 33657, Len: 21
Source Port: 21 (21)
Destination Port: 48588 (48588)
[Stream index: 1163]
[TCP Segment Len: 21]
Sequence number: 79637 (relative sequence number)
[Next sequence number: 79658 (relative sequence number)]
Acknowledgment number: 33657 (relative ack number)
Header Length: 32 bytes
.... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
window size value: 259
[Calculated window size: 66304]
[Window size scaling factor: 256]
Checksum: 0x845d [validation disabled]
Urgent pointer: 0
Options: (12 bytes), No-operation (NOP), No-operation (NOP), Timestamps
[SEQ/ACK analysis]
File Transfer Protocol (FTP)
230 User logged in.\r\n
Response code: User logged in, proceed (230)
Response arg: User logged in.

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ..)ZI...).q...E.
0010 00 49 20 4f 40 00 80 06 00 00 c0 a8 01 69 c0 a8 .I o@...i..
0020 01 68 00 15 bd cc 75 fd cc c9 3b a9 2b 10 80 18 .h....u. ...;+...
0030 01 03 84 5d 00 00 01 01 08 0a 00 04 e3 98 00 0b ...].....
0040 ab 27 32 33 30 20 55 73 65 72 20 6c 6f 67 67 65 . 230 us er logge
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 2 (0.0%) · Load time: 0:02.695 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 1163 Expression... Clear Apply Save

| No. | Time | Source |
|--------|------------|---------------|
| 201583 | 113.901293 | 192.168.1.100 |
| 201585 | 113.901682 | 192.168.1.100 |
| 201658 | 113.911692 | 192.168.1.100 |
| 201664 | 113.912233 | 192.168.1.100 |
| 201732 | 113.922566 | 192.168.1.100 |
| 201736 | 113.923271 | 192.168.1.100 |
| 201801 | 113.930794 | 192.168.1.100 |
| 201808 | 113.931136 | 192.168.1.100 |
| 201882 | 113.943009 | 192.168.1.100 |
| 201885 | 113.943676 | 192.168.1.100 |
| 201948 | 113.951440 | 192.168.1.100 |
| 201958 | 113.952001 | 192.168.1.100 |
| 202022 | 113.958982 | 192.168.1.100 |
| 202026 | 113.959670 | 192.168.1.100 |
| 202103 | 114.041576 | 192.168.1.100 |
| 202213 | 114.053820 | 192.168.1.100 |
| 202216 | 114.053865 | 192.168.1.100 |
| 202253 | 114.061920 | 192.168.1.100 |

Follow TCP Stream (tcp.stream eq 1163)

Stream Content

```
220 Microsoft FTP Service
USER John
331 Password required for John.
PASS ht7
530 User cannot log in.
USER John
331 Password required for John.
PASS ttobba
530 User cannot log in.
USER John
331 Password required for John.
PASS abel
530 User cannot log in.
USER John
331 Password required for John.
PASS ecnayeba
530 User cannot log in.
USER John
331 Password required for John.
PASS able
530 User cannot log in.
USER John
331 Password required for John.
PASS aborning
530 User cannot log in.
USER John
331 Password required for John.
PASS abramson
530 User cannot log in.
USER John
331 Password required for John.
```

Entire conversation (110467 bytes)

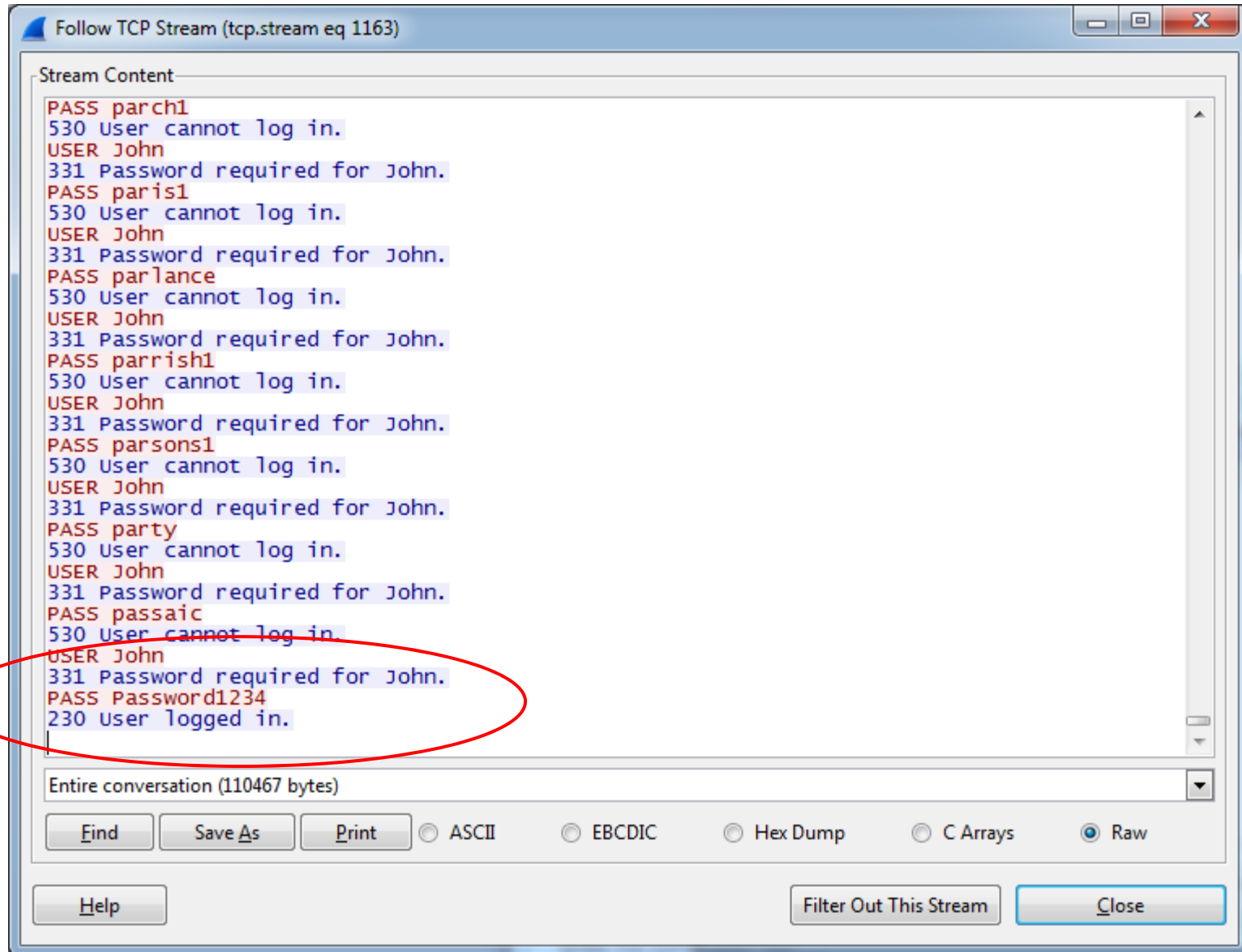
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw

Help Filter Out This Stream Close

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ..)ZI...).q...E.
0010 00 49 20 4f 40 00 80 06 00 00 c0 a8 01 69 c0 a8 .I O@...i..
0020 01 68 00 15 bd cc 75 fd cc c9 3b a9 2b 10 80 18 .h....u. .;.+...
0030 01 03 84 5d 00 00 01 01 08 0a 00 04 e3 98 00 0b ...].... ..
0040 ab 27 32 33 30 20 55 73 65 72 20 6c 6f 67 67 65 '230 us er logge
0050 64 20 6f 6e 6e 6e 6e 6e 6e 6e 6e 6e 6e 6e 6e d in

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 5394 (2.6%) · Load time: 0:02.679 Profile: Default

Scroll down to the
bottom





How did the attack start?
Let's type in this to find out



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.flags == 2 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-1720 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3389 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-139 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 22 | 16.128163 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-256 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 23 | 16.128166 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-199 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 24 | 16.128167 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-53 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 25 | 16.128168 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-113 [SYN] Seq=0 win=2048 Len=0 MSS=1460 |
| 30 | 16.138502 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-143 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 31 | 16.138503 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3306 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 32 | 16.138504 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-80 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-21 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 34 | 16.138506 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-445 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 35 | 16.138507 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-554 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 36 | 16.138508 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-135 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 37 | 16.138509 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-443 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 49 | 16.142004 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-22 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |

+

Frame 10: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_5a:49:c4 (00:0c:29:5a:49:c4), Dst: Vmware_ff:71:d1 (00:0c:29:ff:71:d1)

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.105 (192.168.1.105)

Transmission Control Protocol, Src Port: 58368 (58368), Dst Port: 1720 (1720), Seq: 0, Len: 0

0000

00 0c 29 ff 71 d1 00 0c 29 5a 49 c4 08 00 45 00 ..).q...)ZI...E.

0010

00 2c 3c c2 00 00 26 06 d3 e8 c0 a8 01 68 c0 a8 .;<...&.h..

0020

01 69 e4 00 06 b8 81 a0 8f e1 00 00 00 00 60 02 .i.....:.

0030

0c 00 0b ca 00 00 02 04 05 b4 00 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 1452 (0.7%) · Load time: 0:02.535 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

Filter: tcp.flags == 2

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-1720 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3389 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-139 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 22 | 16.128163 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-256 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 23 | 16.128166 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-199 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 24 | 16.128167 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-53 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 25 | 16.128168 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-113 [SYN] Seq=0 win=2048 Len=0 MSS=1460 |
| 30 | 16.138502 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-143 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 31 | 16.138503 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3306 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 32 | 16.138504 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-80 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-21 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 34 | 16.138506 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-445 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 35 | 16.138507 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-554 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 36 | 16.138508 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-135 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 37 | 16.138509 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-443 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 49 | 16.142004 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-22 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |

Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: Vmware_5a:49:c4 (00:0c:29:5a:49:c4), Dst: Vmware_ff:71:d1 (00:0c:29:ff:71:d1)

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.105 (192.168.1.105)

Transmission Control Protocol, Src Port: 58368 (58368), Dst Port: 80 (80), Seq: 0, Len: 0

Source Port: 58368 (58368)

Destination Port: 21 (21)

[Stream index: 12]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 0

Header Length: 24 bytes

... 0000 0000 0010 = Flags: 0x002 (SYN)

window size value: 1024

[Calculated window size: 1024]

Checksum: 0x1a6d [validation disabled]

Urgent pointer: 0

options: (4 bytes), Maximum segment size

0000 00 0c 29 ff 71 d1 00 0c 29 5a 49 c4 08 00 45 00
0010 00 2c 06 a6 00 00 28 06 08 05 c0 a8 01 68 c0 a8
0020 01 69 e4 00 00 15 81 a0 8f e1 00 00 00 00 60 02
0030 04 00 1a 6d 00 00 02 04 05 b4 00 00

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 1452 (0.7%) · Load time: 0:02.535 Profile: Default

Select packet 33;

RIGHT click on it



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.flags == 2 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-1720 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-587 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-111 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3389 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-139 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 22 | 16.128163 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-256 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 23 | 16.128166 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-199 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 24 | 16.128167 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-53 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 25 | 16.128168 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-113 [SYN] Seq=0 win=2048 Len=0 MSS=1460 |
| 30 | 16.138502 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-143 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 31 | 16.138503 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-3306 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 32 | 16.138504 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-80 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-21 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 34 | 16.138506 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-445 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 35 | 16.138507 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-554 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 36 | 16.138508 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-135 [SYN] Seq=0 win=3072 Len=0 MSS=1460 |
| 37 | 16.138509 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-443 [SYN] Seq=0 win=4096 Len=0 MSS=1460 |
| 49 | 16.142004 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368-22 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |

Mark Packet (toggle)
Ignore Packet (toggle)
Set Time Reference (toggle)
Time Shift...
Edit Packet
Packet Comment...
Manually Resolve Address
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize Conversation
SCTP
Follow TCP Stream
Follow UDP Stream
Follow SSL Stream
Copy
Protocol Preferences
Decode As...
Print...
Show Packet in New Window

bytes captured (480 bits)
9:5a:49:c4), Dst: vmware_ff:71:d1 (00:0c:29:ff:71:d1)
1.104 (192.168.1.104), Dst: 192.168.1.105 (192.168.1.105)
8368 (58368), Dst Port: 21 (21), Seq: 0, Len: 0

number)

```
0000 00 0c 29 ff 71 d1 00 0c 29 5a 49 c4 08 00 45 00  ..).q... )ZI...E.
0010 00 2c 06 a6 00 00 28 06 08 05 c0 a8 01 68 c0 a8  ....(. ....h..
0020 01 69 e4 00 00 15 81 a0 8f e1 00 00 00 00 60 02  .i..... .
0030 04 00 1a 6d 00 00 02 04 05 b4 00 00  ....m....
```

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 1452 (0.7%) · Load time: 0:02.535 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 12 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|---|
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368→21 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 41 | 16.138751 | 192.168.1.105 | 192.168.1.104 | TCP | 58 | 21→58368 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 |
| 46 | 16.139105 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368→21 [RST] Seq=1 win=0 Len=0 |

Follow TCP Stream (tcp.stream eq 12)

Stream Content

Entire conversation (0 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays **Raw**

Help Filter Out This Stream **Close**

Frame 33: 60 bytes on wire (480 bits) captured on interface eth0
Ethernet II, Src: Vmware, Dst: 08:00:00:00:00:00
Internet Protocol Version 4, Src: 192.168.1.104, Dst: 192.168.1.105
Transmission Control Protocol, Seq=0, Win=1024, Len=0

```
0000  00 0c 29 ff 71 d1 00 0c 29 5a 49 c4 08 00 45 00  ..).q... )ZI...E.
0010  00 2c 06 a6 00 00 28 06 08 05 c0 a8 01 68 c0 a8  .....(. ....h..
0020  01 69 e4 00 00 15 81 a0 8f e1 00 00 00 00 60 02  .i..... ..
0030  04 00 1a 6d 00 00 02 04 05 b4 00 00  .....m....
```

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 3 (0.0%) · Load time: 0:02.340 Profile: Default



CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 12 Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|---|
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368→21 [SYN] Seq=0 win=1024 Len=0 MSS=1460 |
| 41 | 16.138751 | 192.168.1.105 | 192.168.1.104 | TCP | 58 | 21→58368 [SYN, ACK] Seq=0 Ack=1 win=8192 Len=0 MSS=1460 |
| 46 | 16.139105 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368→21 [RST] Seq=1 win=0 Len=0 |

Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

Ethernet II, Src: Vmware_5a:49:c4 (00:0c:29:5a:49:c4), Dst: Vmware_ff:71:d1

Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: 58368 (58368), Dst Port: 21 (21)

Source Port: 58368 (58368)

Destination Port: 21 (21)

[Stream index: 12]

[TCP Segment Len: 0]

Sequence number: 0 (relative sequence number)

Acknowledgment number: 0

Header Length: 24 bytes

... 0000 0000 0010 = Flags: 0x002 (SYN)

window size value: 1024

[Calculated window size: 1024]

Checksum: 0xia6d [validation disabled]

Urgent pointer: 0

Options: (4 bytes), Maximum segment size

0000 00 0c 29 ff 71 d1 00 0c 29 5a 49 c4 08 00 45 00 ..).q...)ZI...E.

0010 00 2c 06 a6 00 00 28 06 08 05 c0 a8 01 68 c0 a8(.h..

0020 01 69 e4 00 00 15 81 a0 8f e1 00 00 00 00 60 02 ..i.....

0030 04 00 1a 6d 00 00 02 04 05 b4 00 00m.....

File: "C:\tmp\Boot-capture\CaseStudy2.pca... Packets: 204914 · Displayed: 3 (0.0%) · Load time: 0:02.438 Profile: Default

There are only three packets in this panel.

The attack started with port scanning



Summary

- Prerequisite: network packet & packet analyzer: (header, data)
 - Enveloped letters inside another envelope
- Exercises
 - ➊ Basic network traffic analysis
 - SimpleCapture.pcap, WebCapture.pcap
 - ➋ Gather information and statistics
 - CaseStudy1.pcap, CaseStudy2.pcap
 - Traffic searches: protocol hierarchy, HTTP requests, conversations, filters; attack analysis



Notes, with the same content,
are included

Network Sniffing and Packet Analysis Exercise

What is packet analysis and how to capture network traffic?

A **packet analyzer** is a piece of computer hardware or software that can intercept and log traffic passing over a digital network. When a network request is made (i.e. a web-page search, sent email message...) information is sent across the network from the source location to the destination via multiple data streams/packets. These streams contain header information that describes among other things the source of the request, the destination of the request, the type of data contained in the packet, various information describing the transaction and is then followed by the actual data. On simple web search can generate many data packets.

In this exercise we will analyze some previously captured traffic and explain the contents of the data in detail. We will discuss how to filter captured data streams to limit simplify and fine tune analysis. Through these demonstrations we will enlighten you on safety procedures and risks involved in running certain applications. Specifically we will analyze the following types of network traffic:

- Web Server – http
- File transfer Protocol – FTP
- Port scan
- Password cracking attempt

For these exercises we will use the Wireshark software application that has been installed on your virtual machine. Wireshark, formerly known as Ethereal, is a very powerful tool for network analysis. Wireshark is especially popular because it runs on Windows, Mac OS and Linux. It is a network packet analyzer that can peer inside the network and examine the details of traffic at varying levels. The information it can show you range from application-level information to the actual bits in a single packet.

We will analyze network traffic that was previously captured and has also been installed on your machine. You will need to connect to the vSphere Web Client. Start up and log in to the Snapshot entitled Packet Sniffing Exercise.

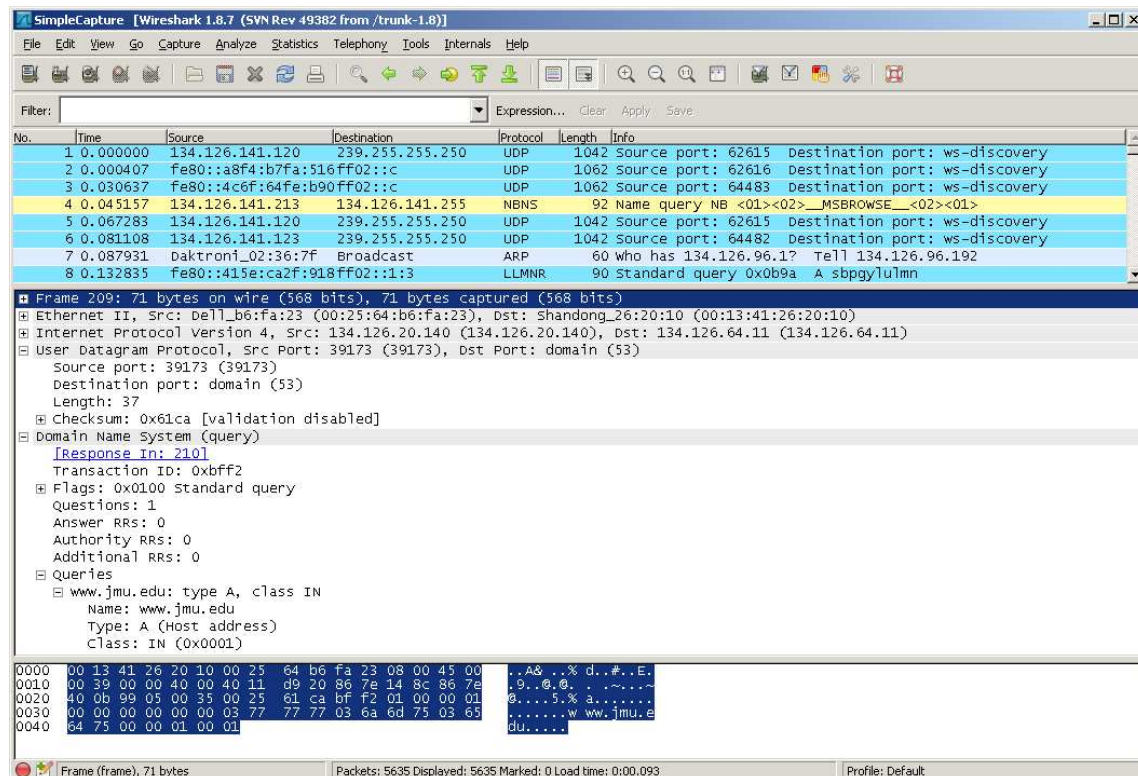
Exercise 1 –Using Wireshark to analyze basic network traffic

We will begin by analyzing a simple network traffic capture. *Double-click* on the **Wireshark** desktop icon. When Wireshark is used to capture and save network traffic it is saved in format known as a **.pcap** (packet capture) file.

Click on **File** → **Open** and select the **SimpleCapture.pcap** file located on your desktop.

Wireshark General Layout

Each line in the capture corresponds to a single packet seen on the network. This is shown in the top pane. The default display shows the time of the packet (relative to the start of the capture) as well as the source and destination IP addresses, the protocol used and some information about the packet. You can click on a row to obtain more information. This allows the other windows to be used. The middle pane contains more internal details on the packet selected in the top frame. These can be expanded out into varying levels of detail. The bottom screen displays the actual data. On the left-hand side you see the hexadecimal representation of the data. On the right-hand side the character representation is displayed. Note the headings displayed in the first section. The first column denotes the packet number. The second column is the time relative to the start of the capture. The remaining columns are the Source IP address, the Destination IP address, the Network Protocol, the Packet Length and Information about the packet.



The screenshot shows the Wireshark 1.8.7 interface with the 'SimpleCapture.pcap' file loaded. The top pane displays a list of captured packets. The middle pane shows the details of the selected packet (Frame 209), which is a DNS response. The bottom pane shows the raw packet data in hexadecimal and ASCII format.

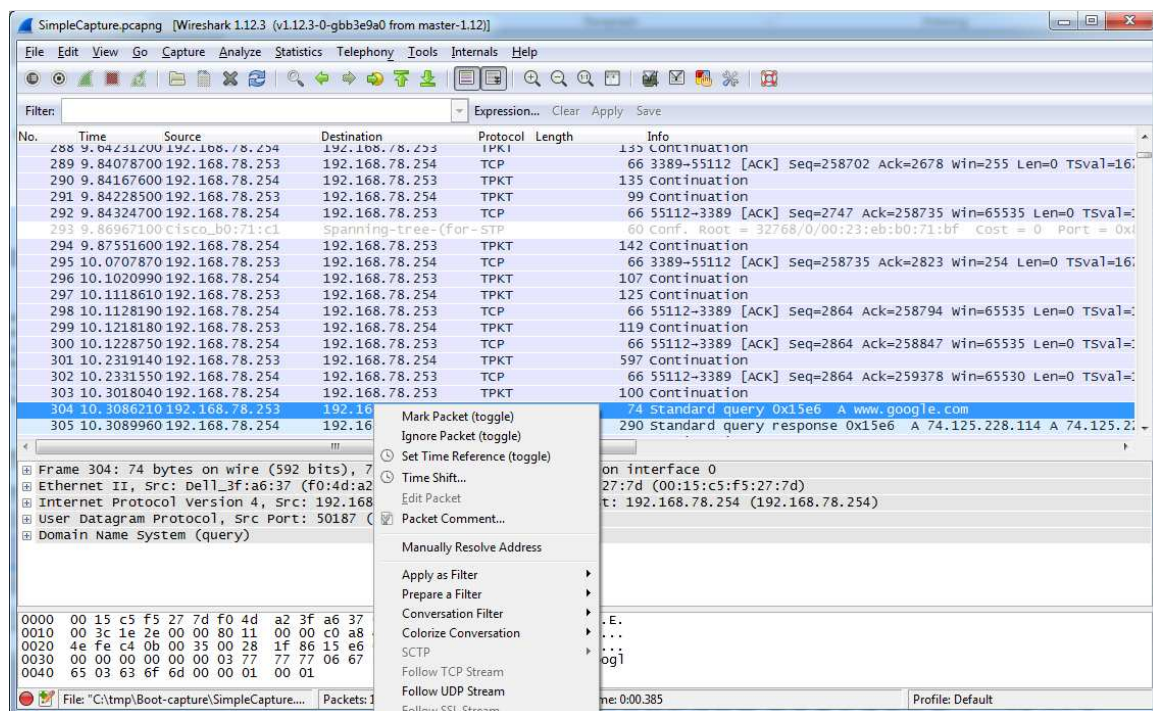
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|------------------------------|-----------------|----------|--------|---|
| 1 | 0.000000 | 134.126.141.120 | 239.255.255.250 | UDP | 1042 | Source port: 62615 Destination port: ws-discovery |
| 2 | 0.000407 | fe80::a8f4:b7fa:516ff02::c | | UDP | 1062 | Source port: 62616 Destination port: ws-discovery |
| 3 | 0.030637 | fe80::4c6f:64fe:b90ff02::c | | UDP | 1062 | Source port: 64483 Destination port: ws-discovery |
| 4 | 0.045157 | 134.126.141.213 | 134.126.141.255 | NBNS | 92 | Name query NB <01><02>_MSBROWSE_<02><01> |
| 5 | 0.067283 | 134.126.141.120 | 239.255.255.250 | UDP | 1042 | Source port: 62615 Destination port: ws-discovery |
| 6 | 0.081108 | 134.126.141.123 | 239.255.255.250 | UDP | 1042 | Source port: 64482 Destination port: ws-discovery |
| 7 | 0.087931 | baktroni_02:36:7f | Broadcast | ARP | 60 | who has 134.126.96.1? Tell 134.126.96.192 |
| 8 | 0.132835 | fe80::415e:ca2f:918ff02::1:3 | | LLMNR | 90 | Standard query 0x0b9a A sbpgylulmn |

Frame 209: 71 bytes on wire (568 bits), 71 bytes captured (568 bits)

- Ethernet II, Src: Dell_b6:fa:23 (00:25:64:b6:fa:23), Dst: Shandong_26:20:10 (00:13:41:26:20:10)
- Internet Protocol Version 4, Src: 134.126.20.140 (134.126.20.140), Dst: 134.126.64.11 (134.126.64.11)
- User Datagram Protocol, Src Port: 39173 (39173), Dst Port: domain (53)
 - Source port: 39173 (39173)
 - Destination port: domain (53)
 - Length: 37
 - Checksum: 0x61ca [validation disabled]
 - Domain Name System (query)
 - Transaction ID: 0xbff2
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
 - Queries
 - www.jmu.edu: type A, class IN
 - Name: www.jmu.edu
 - Type: A (Host address)
 - Class: IN (0x0001)

0000 00 13 41 26 20 10 00 25 64 b6 fa 23 08 00 45 00 ..A&.%d..#.E.
 0010 00 39 00 00 40 00 40 11 d9 20 86 7e 14 8c 86 7e .9..@.
 0020 40 0b 99 05 00 35 00 25 61 ca bf f2 01 00 00 01 @....5.%a.....
 0030 00 00 00 00 00 00 03 77 77 77 03 6a 6d 75 03 65w ww.jmu.e
 0040 64 75 00 00 01 00 01 du.....

We will begin by examining the sequence of events that take place when a user performs a DNS query. DNS stands for *Domain Name Services*. DNS takes a common fully qualified domain name and translates it to a corresponding Internet address. The sequences of events that take place are first a request is made from a source machine to a DNS server. If the server recognizes the name requested it sends a response with the IP address associated with the name. Two possible situations can occur if the server does not know the name requested. These situations depend upon how the request is configured. If the request is a recursive request then the source machine will depend on the server to forward on the request to find the answer. If the request is setup to be iterative then the server will respond that it does not know the name and the source machine will need to make a request to another server. Let's take a look at a simple request that was made in our network capture. In our example a user has made a request via the *nslookup* command to get the ip address for **www.google.com**. To view this traffic in Wireshark, scroll down and select packet # **304**. *Right-click* on the packet and select *Follow UDP Stream*



A Follow UDP Stream will appear. You will notice that the Stream Content contains **www.google.com** and other nonsensical characters. Close this window and return to the main Wireshark window. Notice now that only two packets appear. Click on the first packet and look in the second pane. If you look in the flags section you will notice that this is a recursive query. This tells us that the server will send on the request if it does not have an answer.

SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port) Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 304 | 10.3086210 | 192.168.78.253 | 192.168.78.254 | DNS | 74 | standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.168.78.253 | DNS | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.228.115 A 74.125.228.116 A 74.125.228.117 |

Frame 304: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

Ethernet II, Src: dell_3f:a6:37 (f0:4d:a2:3f:a6:37), Dst: dell_3f:a6:37 (f0:4d:a2:3f:a6:37)

Internet Protocol Version 4, Src: 192.168.78.253 (192.168.78.253), Dst: 192.168.78.254 (192.168.78.254)

User Datagram Protocol, Src Port: 50187 (50187), Dst Port: 53 (53)

Domain Name System (Query)

Response in: 305

Transaction ID: 0x15e6

Flags: 0x0100 Standard query

Questions: 1

Answer RRs: 0

Authority RRs: 0

Additional RRs: 0

Queries

www.google.com: type A, class IN

Name: www.google.com

[Name Length: 14]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

0000 00 15 c5 f5 27 7d f0 4d a2 3f a6 37 08 00 45 00 .M..?..E..

0010 00 3c 1e 2e 00 00 80 11 00 00 c0 a8 4e fd c0 a8 .<....N...

0020 4e fe c4 0b 00 35 00 28 1f 86 15 e6 01 00 00 01 N...5.(.....

0030 00 00 00 00 00 03 77 77 77 06 67 6f 6f 6f 6ew ww.goog

0040 65 03 83 8f 6d 00 00 01 00 01 c0 0c 00 01 00 01 e.com.....

Frame (frame), 74 bytes

Packets: 10730 - Displayed: 2 (0.0%) - Load time: 0:00:146

Profile: Default

SimpleCapture.pcapng [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port) Expression... Clear Apply Save

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 304 | 10.3086210 | 192.168.78.253 | 192.168.78.254 | DNS | 74 | standard query 0x15e6 A www.google.com |
| 305 | 10.3089960 | 192.168.78.254 | 192.168.78.253 | DNS | 290 | Standard query response 0x15e6 A 74.125.228.114 A 74.125.228.115 A 74.125.228.116 A 74.125.228.117 |

Frame 305: 290 bytes on wire (2320 bits), 290 bytes captured (2320 bits) on interface 0

Ethernet II, Src: dell_3f:a6:37 (f0:4d:a2:3f:a6:37), Dst: dell_3f:a6:37 (f0:4d:a2:3f:a6:37)

Internet Protocol Version 4, Src: 192.168.78.254 (192.168.78.254), Dst: 192.168.78.253 (192.168.78.253)

User Datagram Protocol, Src Port: 53 (53), Dst Port: 50187 (50187)

Domain Name System (response)

Request in: 304

[Time: 0.000375000 seconds]

Transaction ID: 0x15e6

Flags: 0x8180 standard query response, No error

Questions: 1

Answer RRs: 5

Authority RRs: 4

Additional RRs: 4

Queries

www.google.com: type A, class IN

Name: www.google.com

[Name Length: 14]

[Label Count: 3]

Type: A (Host Address) (1)

Class: IN (0x0001)

Answers

www.google.com: type A, class IN, addr 74.125.228.114

www.google.com: type A, class IN, addr 74.125.228.115

www.google.com: type A, class IN, addr 74.125.228.116

www.google.com: type A, class IN, addr 74.125.228.117

0000 f0 4d a2 3f a6 37 00 15 c5 f5 27 7d 08 00 45 00 .M..?..E..

0010 01 14 98 81 00 00 40 11 c2 0b c0 a8 4e fe c0 a8 .<....N...

0020 4e fe c4 0b 00 35 00 28 1f 86 15 e6 01 00 00 01 N...5.(.....

0030 00 05 00 04 00 04 03 77 77 77 06 67 6f 6f 6f 6ew ww.goog

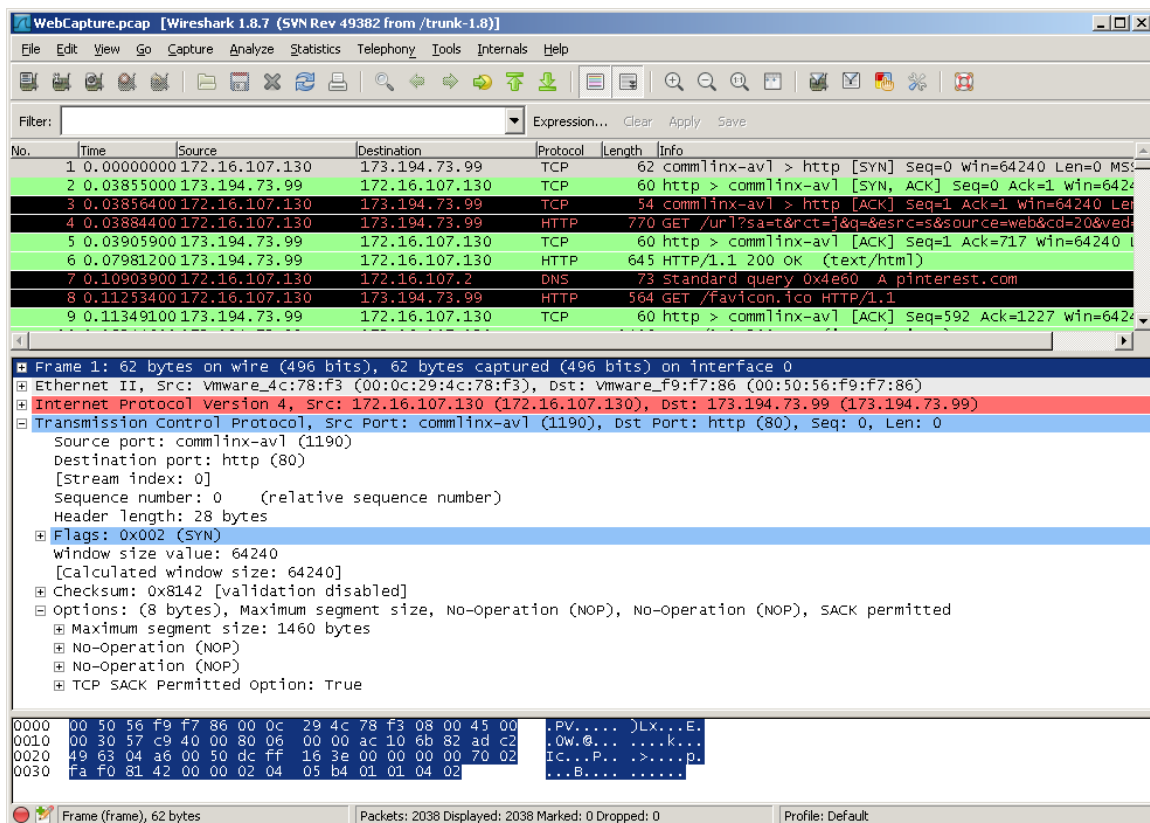
0040 65 03 83 8f 6d 00 00 01 00 01 c0 0c 00 01 00 01 e.com.....

Frame (frame), 290 bytes

Packets: 10730 - Displayed: 2 (0.0%) - Load time: 0:00:146

Profile: Default

A *three-way handshake* is used to initiate communication between two machines. When a source machine wants to communicate with a destination machine it will start by sending a SYN request. This tells the destination machine that a conversation is being requested. If the destination machine accepts the request it will respond with a SYN, ACK. When the initial machine receives this response it in turn responds with an ACK response and the conversation begins. Lets close our current packet capture and open another to observe this traffic. Go to *File* → *Close* to close the current capture. Then choose *File* → *Open* and select the file named **WebCapture.pcap**.



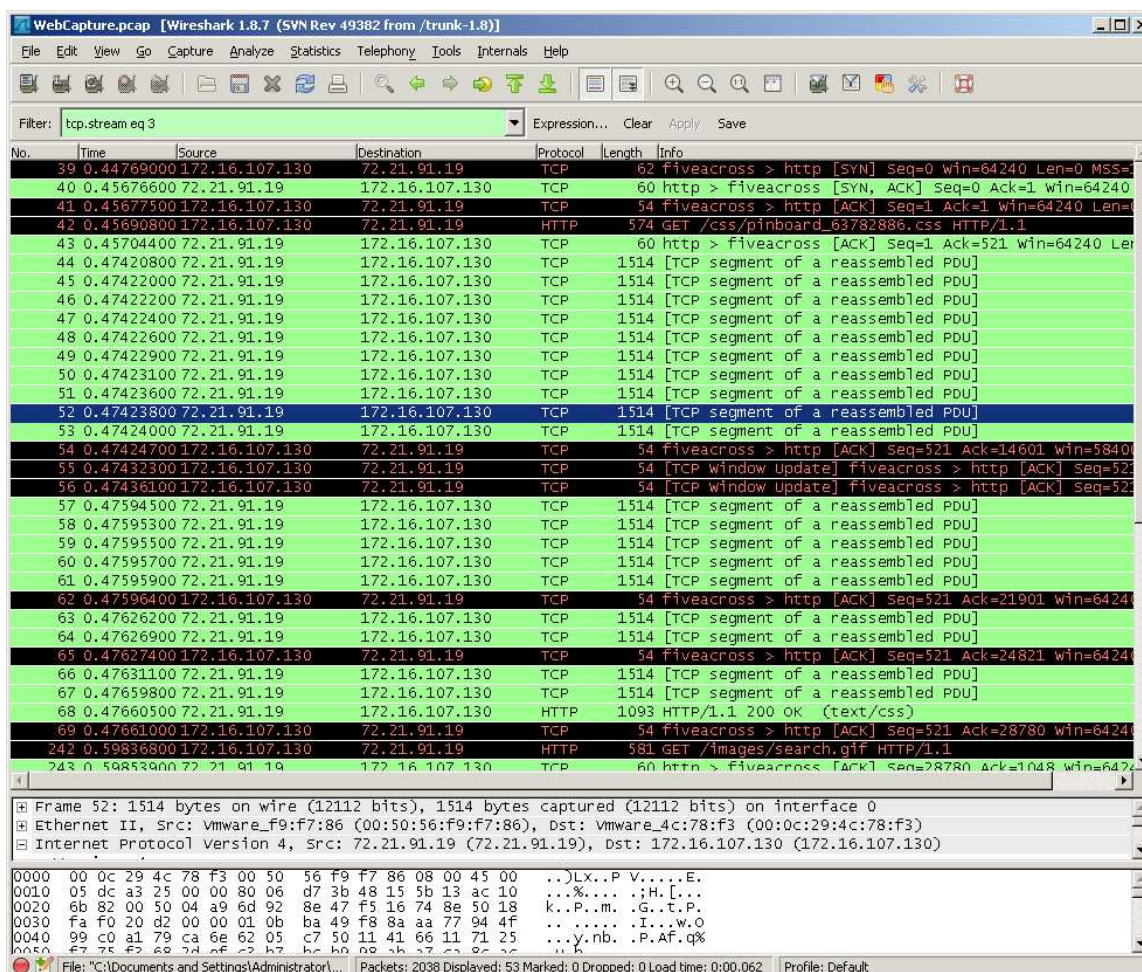
This is a capture of a simple web search. The user has opened up the Google search engine and ran a search for “cute puppy pictures”. The user then chose the Pinterest webpage, selected and downloaded a picture.

Lets take a look at the packet capture in detail. In the first packet we see that the source computer (172.16.107.130) sends a SYN request to the destination computer (173.194.73.99). If you expand the Transmission Control Protocol section of the second pane you can see that the source port is 1190 and the destination port is 80 (indicating an http request is coming). The Flags section shows that this is an initial SYN request. The next packet displays the SYN,ACK response coming back from 173.194.73.99 port 80 to

172.16.107.130 port 1190. Packet 3 shows the final ACK response completing the three-way handshake.

Packet 4 marks the beginning of the “cute puppy pictures” search. Packet 7 shows the DNS lookup (query) for pinterest.com (the site where the puppy picture resides). The DNS response is seen in packet 11. Packets 12-17 indicate two different three-way handshakes for requests from pinterest.

Scroll down and click on packet 42. Right click and choose Follow TCP Stream. Notice the two sets of headers followed by a bunch of confusing information. This confusing information is the binary picture being downloaded. If you close the Follow TCP Stream window you will notice a filter has been entered in the filter section (we will talk more about filters later). What is important to know at this point is that this request has filtered out all other packets and now we can follow just this network conversation.



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 39 | 0.44769000 | 172.16.107.130 | 72.21.91.19 | TCP | 62 | fiveacross > http [SYN] Seq=0 win=64240 Len=0 MSS= |
| 40 | 0.45676600 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | http > fiveacross [SYN, ACK] Seq=0 Ack=1 win=64240 |
| 41 | 0.45677500 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | fiveacross > http [ACK] Seq=1 Ack=1 win=64240 Len= |
| 42 | 0.45690800 | 172.16.107.130 | 72.21.91.19 | HTTP | 574 | GET /css/pinboard_63782886.css HTTP/1.1 |
| 43 | 0.45704400 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | http > fiveacross [ACK] Seq=1 Ack=521 win=64240 Len |
| 44 | 0.47420800 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 45 | 0.47422000 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 46 | 0.47422200 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 47 | 0.47422400 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 48 | 0.47422600 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 49 | 0.47422900 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 50 | 0.47423100 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 51 | 0.47423600 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 52 | 0.47423800 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 53 | 0.47424000 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 54 | 0.47424700 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | fiveacross > http [ACK] Seq=521 Ack=14601 win=5840 |
| 55 | 0.47432300 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | [TCP window update] fiveacross > http [ACK] Seq=521 |
| 56 | 0.47436100 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | [TCP window update] fiveacross > http [ACK] Seq=521 |
| 57 | 0.47594500 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 58 | 0.47595300 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 59 | 0.47595500 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 60 | 0.47595700 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 61 | 0.47595900 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 62 | 0.47596400 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | fiveacross > http [ACK] Seq=521 Ack=21901 win=64240 |
| 63 | 0.47626200 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 64 | 0.47626900 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 65 | 0.47627400 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | fiveacross > http [ACK] Seq=521 Ack=24821 win=64240 |
| 66 | 0.47631100 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 67 | 0.47659800 | 72.21.91.19 | 172.16.107.130 | TCP | 1514 | [TCP segment of a reassembled PDU] |
| 68 | 0.47660500 | 72.21.91.19 | 172.16.107.130 | HTTP | 1093 | HTTP/1.1 200 OK (text/css) |
| 69 | 0.47661000 | 172.16.107.130 | 72.21.91.19 | TCP | 54 | fiveacross > http [ACK] Seq=521 Ack=28780 win=64240 |
| 242 | 0.59836800 | 172.16.107.130 | 72.21.91.19 | HTTP | 581 | GET /images/search.gif HTTP/1.1 |
| 243 | 0.59853900 | 72.21.91.19 | 172.16.107.130 | TCP | 60 | http > fiveacross [ACK] Seq=28780 Ack=1048 win=64240 |

Frame 52: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0

Ethernet II, Src: vmware_f9:f7:86 (00:50:56:f9:f7:86), Dst: vmware_4c:78:f3 (00:0c:29:4c:78:f3)

Internet Protocol Version 4, Src: 72.21.91.19 (72.21.91.19), Dst: 172.16.107.130 (172.16.107.130)

0000 00 0c 29 4c 78 f3 00 50 56 f9 f7 86 08 00 45 00 ..)LX..P V.....E.

0010 05 dc a3 25 00 00 80 06 d7 3b 48 15 5b 13 ac 10 ...%....;H.[...

0020 6b 82 00 50 04 a9 6d 92 8e 47 f5 16 74 8e 50 18 k..P.m..G..t.P.

0030 fa f0 20 d2 00 00 01 0b ba 49 f8 8a aa 77 94 4fI...w.O

0040 99 c0 a1 79 ca 6e 62 05 c7 50 11 41 66 11 71 25 ...y.nb..P.Af.q%

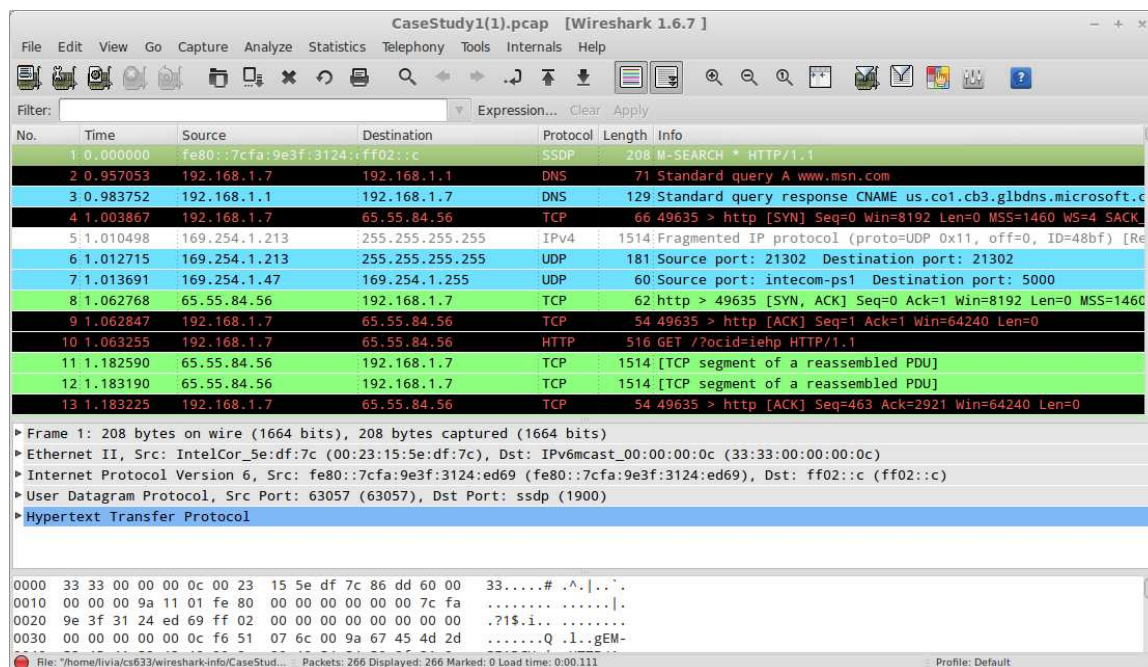
File: "C:\Documents and Settings\Administrator\..." Packets: 2038 Displayed: 53 Marked: 0 Dropped: 0 Load time: 0:00.062 Profile: Default

This section basically shows the downloading of the image. Notice all the lines which contain “1514 [TCP segment of a reassembled PDU]”. This is portions of the image being downloaded.

This concludes this exercise close the Capture file and procede to Exercise 2.

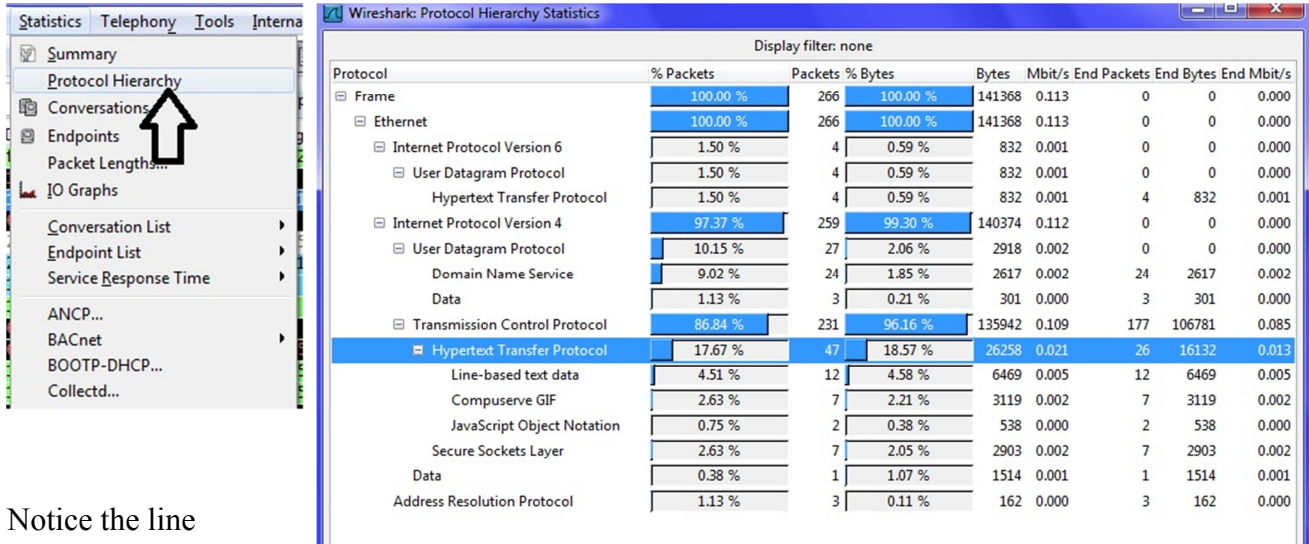
Exercise 2 - Gathering General Information and Statistics and More Wireshark Analysis

Click on *File* → *Open* and select the **CaseStudy1.pcap** file located on your desktop. You should now have a window displaying that is similar to below:



To determine what type of data has been captured in this file we can to go the *Statistics* section and select

Protocol Hierarchy

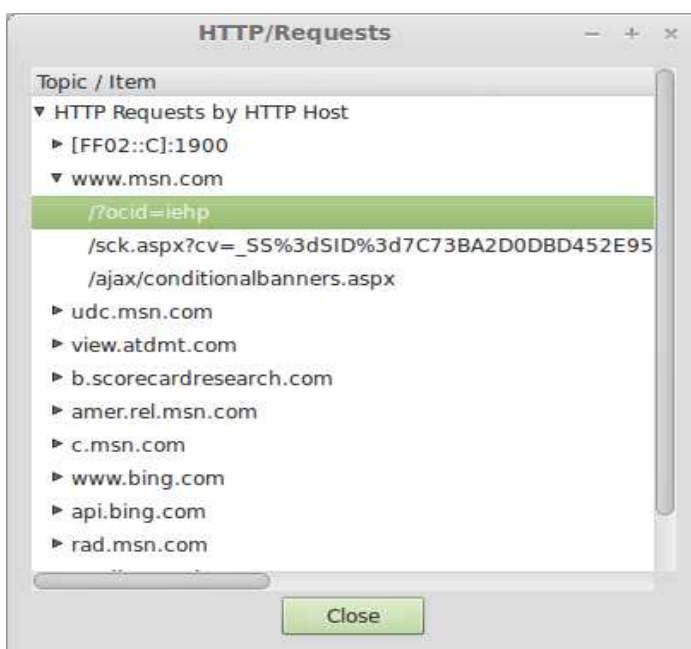
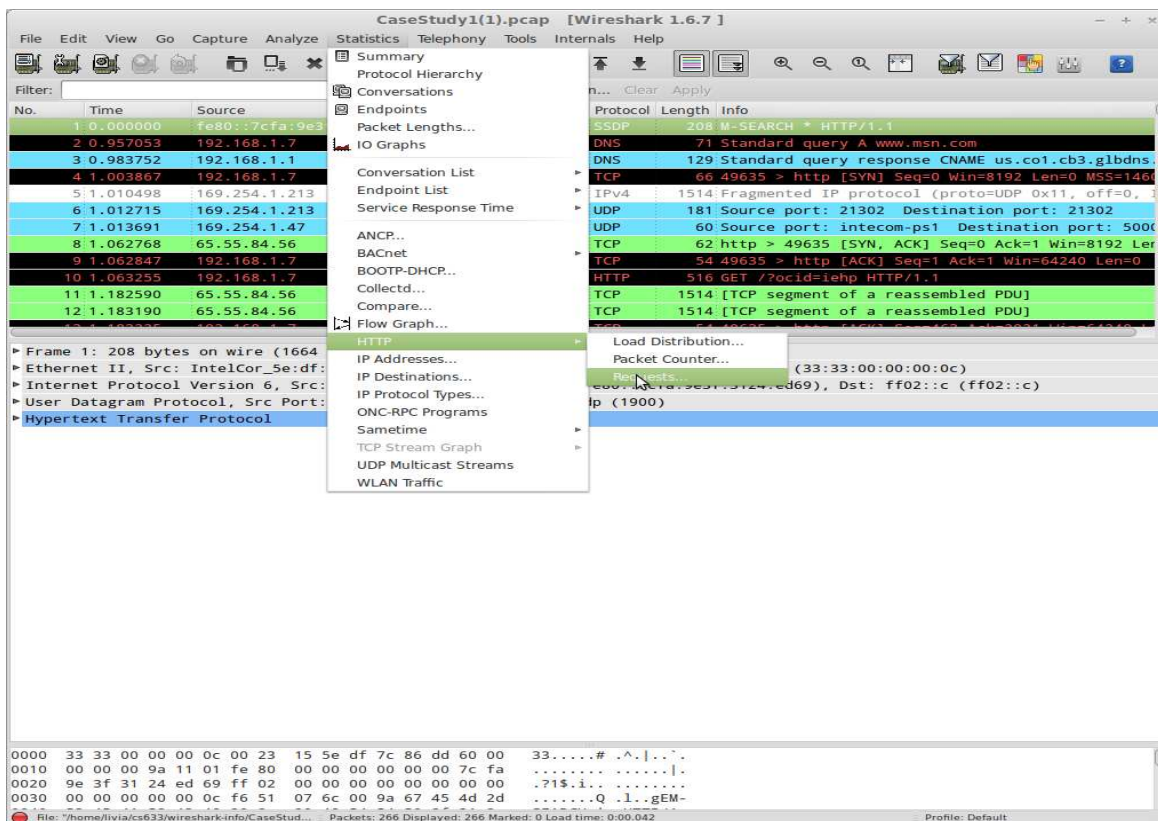


Notice the line highlighted above.

This shows that 17.67% of the traffic contained in this capture is Hypertext Transfer protocol (http – web traffic). This may not seem like a lot but you must remember that one web request will generate several packets of data.

Other interesting statistics can be gathered easily through selections made under the *Statistics* section. We will examine a few briefly.

Close your current window and select the *Statistics* section again. This time choose *HTTP → Requests...* Leave the filter blank and click on *Create Stat*



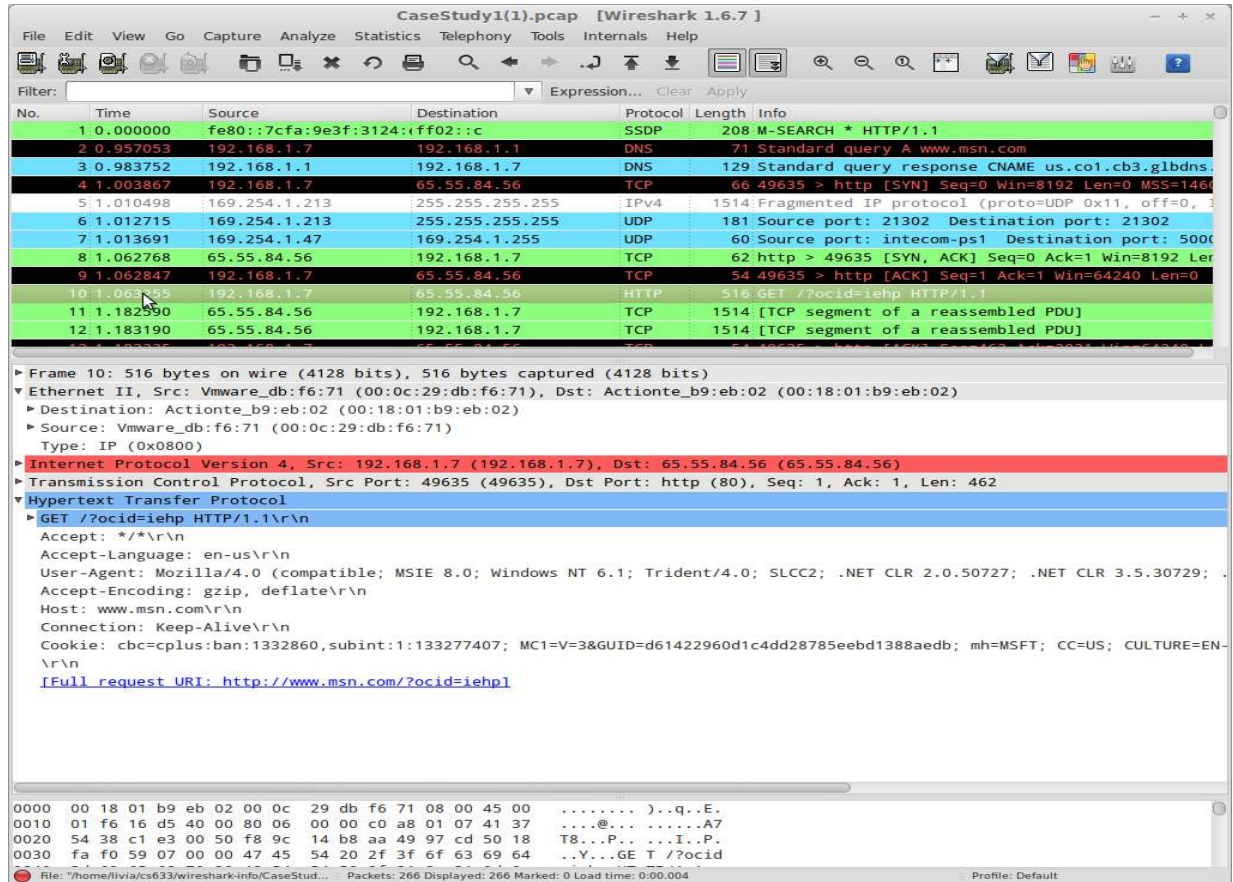
(The above figure might be obsolete and what you see might be a little bit different)

This list now contains all the http requests made.

Wireshark includes a complex color-coding scheme. The default settings are as follows:

| Name | String |
|-------------------------------|--|
| Bad TCP | tcp.analysis.flags |
| 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) (ip.dst == 224.0.0.0/24 && ip.ttl != 1) |
| Checksum Errors | cdp.checksum_bad==1 edp.checksum_bad==1 ip.checksum_bad==1 tcp.checksum_bad==1 udp.checksum_bad==1 |
| SMB | smb nbss nbns nbpx ipxsap netbios |
| HTTP | http tcp.port == 80 |
| IPX | ipx spx |
| DCERPC | dcerpc |
| Routing | hsrp eigrp ospf bgp cdp vrrp gvrp igmp ismp |
| TCP SYN/FIN | tcp.flags & 0x02 tcp.flags.fin == 1 |
| TCP | tcp |
| UDP | udp |
| Broadcast | eth[0] & 1 |

Close this window and lets analyze the first http packet – click on line 10.



Examine the information displayed in the middle pane of the windows. Wireshark does a great job of showing all the details of the packet (including the lower levels and not just the application layer). In this case, we get the most information from the application layer. Here we can tell that the HTTP packet is a GET request for the /?ocid=iehp page of [www.msn.com](http://www.msn.com/?ocid=iehp). Wireshark even summarizes the full request below to be <http://www.msn.com/?ocid=iehp>.

Conversations

A network conversation is the traffic between two specific endpoints. Along with the addresses, packet counters, and byte counters, this window also has the time in seconds between the start of the capture and the start of the conversation (“Rel Start”), the duration of the conversation in seconds, and the average bits (not bytes) per second in each direction. Lets take a look. Click on the Statistics section and go to Conversation

IPv4 Conversations: CaseStudy1(1).pcap

IPv4 Conversations: 16

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets B→A | Bytes B→A | Rel Start | Duration | bps A→B | bps B→A |
|----------------|-----------------|---------|--------|-------------|-----------|-------------|-------------------|-----------|------------|----------|---------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 0.957053000 | 6.8083 | 2035.16 | 1039.90 | |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 1.003867000 | 6.1139 | 62668.59 | 3837.79 | |
| 169.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 1.010498000 | 0.0022 | 6116373.48 | N/A | |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 1.013691000 | 0.0000 | N/A | N/A | |
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 1.448913000 | 0.3999 | 19525.47 | 8242.31 | |
| 65.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 1.460531000 | 6.7915 | 1064.86 | 2438.34 | |
| 192.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 1.463244000 | 0.1165 | 49226.76 | 31238.74 | |
| 67.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 1.484162000 | 0.2664 | 25585.68 | 23033.12 | |
| 64.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 1.500961000 | 0.4409 | 9725.76 | 15495.89 | |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 1.509582000 | 1.1311 | 14838.76 | 12101.58 | |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 1.963498000 | 0.8334 | 82192.08 | 36651.41 | |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 1.974914000 | 0.2965 | 17913.87 | 19505.61 | |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 2.130004000 | 0.3354 | 140969.79 | 48969.71 | |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 2.566532000 | 0.4933 | 320986.75 | 37449.27 | |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 4.990550000 | 0.0000 | N/A | N/A | |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 7.804066000 | 0.9241 | 233742.45 | 16734.23 | |

Help Copy Close

list → IPv4. A window similar to that below should appear.

Each row in the list shows the statistical values for exactly one conversation. Conversations can be further shown at each of the different levels. From the conversation window, filters can also be applied. To demonstrate this situate this window so that it is so that you can see both it and the top pane of the main Wireshark window as is demonstrated below:

CaseStudy1(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|----------------|----------------|----------|--------|---|
| 78 | 1.509582 | 192.168.1.7 | 204.245.34.139 | TCP | 66 | 49641 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 |
| 79 | 1.522328 | 67.148.147.113 | 192.168.1.7 | TCP | 60 | http > 49639 [ACK] Seq=1 Ack=474 Win=15672 Len=0 |
| 80 | 1.525734 | 67.148.147.113 | 192.168.1.7 | HTTP | 363 | HTTP/1.1 200 OK (GIF89a) |
| 81 | 1.529974 | 192.168.1.7 | 65.55.84.56 | TCP | 54 | 49635 > http [ACK] Seq=463 Ack=41208 Win=64240 Len=0 |
| 82 | 1.537809 | 207.46.140.46 | 192.168.1.7 | TCP | 66 | http > 49636 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 |
| 83 | 1.537891 | 192.168.1.7 | 207.46.140.46 | TCP | 54 | 49636 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 84 | 1.538291 | 192.168.1.7 | 207.46.140.46 | HTTP | 802 | GET /default.aspx?parsergroup=hops&fk=W&gp=P&opt=... |
| 85 | 1.548112 | 207.46.193.176 | 192.168.1.7 | HTTP | 333 | HTTP/1.1 200 OK (GIF89a) |
| 86 | 1.548194 | 192.168.1.7 | 207.46.193.176 | TCP | 54 | 49638 > http [ACK] Seq=436 Ack=281 Win=63961 Len=0 |
| 87 | 1.549298 | 192.168.1.7 | 207.46.193.176 | TCP | 54 | 49638 > http [FIN, ACK] Seq=436 Ack=281 Win=63961 Len=0 |
| 88 | 1.579766 | 207.46.193.176 | 192.168.1.7 | TCP | 60 | http > 49638 [ACK] Seq=281 Ack=437 Win=64240 Len=0 |
| 89 | 1.592868 | 64.4.21.39 | 192.168.1.7 | TCP | 60 | http > 49640 [SYN, ACK] Seq=0 Ack=1 Win=8190 Len=0 |

IPv4 Conversations: CaseStudy1(1).pcap

IPv4 Conversations: 16

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets B→A | Bytes B→A | Rel Start | Duration | bps A→B | bps B→A |
|----------------|-----------------|---------|--------|-------------|-----------|-------------|-----------|-------------|----------|------------|----------|
| 192.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 | 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 65.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 | 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 169.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 169.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
| 65.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 | 1.460531000 | 6.7915 | 1064.86 | 2438.34 |
| 192.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 | 1.463244000 | 0.1165 | 49226.76 | 31238.74 |
| 67.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 | 1.484162000 | 0.2664 | 25585.68 | 23033.12 |
| 64.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 | 1.500961000 | 0.4409 | 9725.76 | 15495.89 |
| 192.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 | 1.509582000 | 1.1311 | 14838.76 | 12101.58 |
| 65.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 | 1.963498000 | 0.8334 | 82192.08 | 36651.41 |
| 63.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 | 1.974914000 | 0.2965 | 17913.87 | 19505.61 |
| 157.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 | 2.130004000 | 0.3354 | 140969.79 | 48969.71 |
| 75.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 | 2.566532000 | 0.4933 | 320986.75 | 37449.27 |
| 169.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |
| 173.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 | 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

Help Copy Close

Since we have created no filters all the network traffic appears. Choose the fifth line down in the conversation window

| | | | | | | | | | | | |
|-------------|---------------|---|-------|---|-----|---|-----|-------------|--------|----------|---------|
| 192.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
|-------------|---------------|---|-------|---|-----|---|-----|-------------|--------|----------|---------|

Right-click on the line and choose Apply Filter then Selected then A ↔ B. Notice how the contents of the first pane of the main Wireshark Window has changed. Now you are viewing only the traffic which transpired between the source IP address of 192.168.1.7 and the destination address of 207.46.140.46

CaseStudy1(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ip.addr==192.168.1.7 && ip.addr==207.46.140.46` Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|----------|---------------|---------------|----------|--------|--|
| 56 | 1.448913 | 192.168.1.7 | 207.46.140.46 | TCP | 66 | 49636 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 W |
| 82 | 1.537809 | 207.46.140.46 | 192.168.1.7 | TCP | 66 | http > 49636 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 |
| 83 | 1.537891 | 192.168.1.7 | 207.46.140.46 | TCP | 54 | 49636 > http [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 84 | 1.538291 | 192.168.1.7 | 207.46.140.46 | HTTP | 802 | GET /default.aspx?parsergroup=hops&fk=W&gp=P&optke |
| 95 | 1.630817 | 207.46.140.46 | 192.168.1.7 | HTTP | 346 | HTTP/1.1 204 No Content |
| 103 | 1.848801 | 192.168.1.7 | 207.46.140.46 | TCP | 54 | 49636 > http [ACK] Seq=749 Ack=293 Win=65408 Len=0 |

IPv4 Conversations: CaseStudy1(1).pcap

IPv4 Conversations: 16

| Address A | Address B | Packets | Bytes | Packets A→B | Bytes A→B | Packets B→A | Bytes B→A | Rel Start | Duration | bps A→B | bps B→A |
|---------------|-----------------|---------|--------|-------------|-----------|-------------|-----------|-------------|----------|------------|----------|
| 92.168.1.1 | 192.168.1.7 | 24 | 2 617 | 12 | 1 732 | 12 | 885 | 0.957053000 | 6.8083 | 2035.16 | 1039.90 |
| 5.55.84.56 | 192.168.1.7 | 55 | 50 827 | 35 | 47 894 | 20 | 2 933 | 1.003867000 | 6.1139 | 62668.59 | 3837.79 |
| 69.254.1.213 | 255.255.255.255 | 2 | 1 695 | 2 | 1 695 | 0 | 0 | 1.010498000 | 0.0022 | 6116373.48 | N/A |
| 69.254.1.47 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 1.013691000 | 0.0000 | N/A | N/A |
| 92.168.1.7 | 207.46.140.46 | 6 | 1 388 | 4 | 976 | 2 | 412 | 1.448913000 | 0.3999 | 19525.47 | 8242.31 |
| 5.55.253.27 | 192.168.1.7 | 9 | 2 974 | 3 | 904 | 6 | 2 070 | 1.460531000 | 6.7915 | 1064.86 | 2438.34 |
| 92.168.1.7 | 207.46.193.176 | 8 | 1 172 | 5 | 717 | 3 | 455 | 1.463244000 | 0.1165 | 49226.76 | 31238.74 |
| 7.148.147.113 | 192.168.1.7 | 9 | 1 619 | 4 | 852 | 5 | 767 | 1.484162000 | 0.2664 | 25585.68 | 23033.12 |
| 4.4.21.39 | 192.168.1.7 | 6 | 1 390 | 2 | 536 | 4 | 854 | 1.500961000 | 0.4409 | 9725.76 | 15495.89 |
| 92.168.1.7 | 204.245.34.139 | 13 | 3 809 | 6 | 2 098 | 7 | 1 711 | 1.509582000 | 1.1311 | 14838.76 | 12101.58 |
| 5.55.5.232 | 192.168.1.7 | 28 | 12 380 | 12 | 8 562 | 16 | 3 818 | 1.963498000 | 0.8334 | 82192.08 | 36651.41 |
| 3.235.36.105 | 192.168.1.7 | 9 | 1 387 | 4 | 664 | 5 | 723 | 1.974914000 | 0.2965 | 17913.87 | 19505.61 |
| 57.56.51.123 | 192.168.1.7 | 19 | 7 963 | 9 | 5 910 | 10 | 2 053 | 2.130004000 | 0.3354 | 140969.79 | 48969.71 |
| 5.98.29.8 | 192.168.1.7 | 37 | 22 100 | 21 | 19 791 | 16 | 2 309 | 2.566532000 | 0.4933 | 320986.75 | 37449.27 |
| 69.254.1.69 | 169.254.1.255 | 1 | 60 | 1 | 60 | 0 | 0 | 4.990550000 | 0.0000 | N/A | N/A |
| 73.194.73.99 | 192.168.1.7 | 32 | 28 933 | 23 | 27 000 | 9 | 1 933 | 7.804066000 | 0.9241 | 233742.45 | 16734.23 |

Help Copy Close

Notice that the Filter section above the first pane has been filled in. Close the Conversation window and let's examine this further. The Filter that we applied was:

Filter: `ip.addr==192.168.1.7 && ip.addr==207.46.140.46`

This was one easy way to filter out all traffic except that between IP address 192.168.1.7 and IP address 207.46.140.46.

Filters are a good way to decipher through all the packets and zone in on specific information. Let's examine a few simple filters that we can make through the use of the *Expression...* builder. Press the *Clear* button located to the Filter and then press the *Expression...* key.

Filter:

▼ Expression...

It may take a few seconds but a Filter Expression window should appear

Wireshark: Filter Expression - Profile: Default

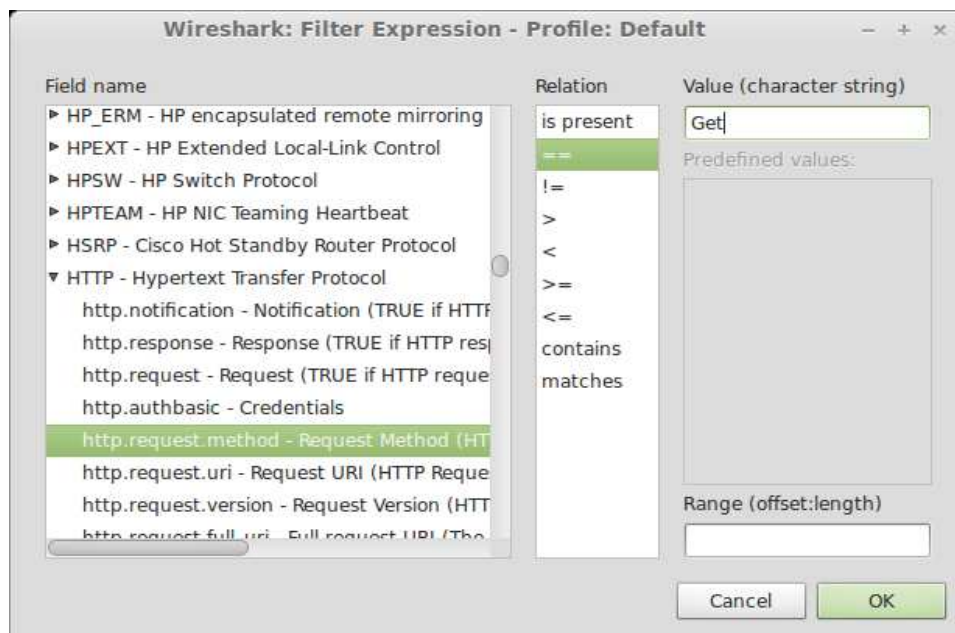
| Field name | Relation | Value (protocol) |
|--|------------|------------------|
| ▶ Expert - Expert Info | is present | |
| ▶ 104apci - IEC 60870-5-104-Apci | == | |
| ▶ 104asdu - IEC 60870-5-104-Asdu | != | |
| ▶ 2dparityfec - Pro-MPEG Code of Practice #3 n | > | |
| ▶ 3COMXNS - 3Com XNS Encapsulation | < | |
| ▶ 3GPP2 A11 - 3GPP2 A11 | >= | |
| ▶ 6LoWPAN - IPv6 over IEEE 802.15.4 | <= | |
| ▶ 802.11 MGT - IEEE 802.11 wireless LAN man | contains | |
| ▶ 802.11 Radiotap - IEEE 802.11 Radiotap Cap | matches | |
| ▶ 802.3 Slow protocols - Slow Protocols | | |
| ▶ 9P - Plan 9 9P | | |
| AAL1 - ATM AAL1 | | |
| AAL3/4 - ATM AAL3/4 | | |

Predefined values:

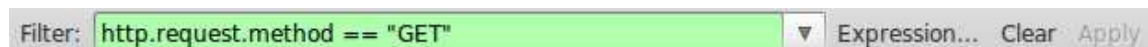
Range (offset:length)

Cancel OK

Here you can build your own filters. Scroll down to **Http** in the *Field Name* section and expand the options. Notice that there are many different sub-filters that you can use to fine tune your search. Lets narrow our search to all the Get requests. Click on the sub-filter labeled *http.request.method*. In the Relation section choose the == “equal” sign. Notice that the Value section becomes active. Type in **GET** (be sure to use all CAPITAL Letters) and click **OK**



Notice that the filter has been filled in:



Click on *Apply* and notice the packets that have been selected. This is a list of all the Get requests that have been made in the captured session.

This ends the first exercise. Click *Clear* on the Filter line to exist the filter. Then go to the *File* tab and select *Close* to close the **CaseStudy1.pcap** file.

Exercise 2 – More Traffic searches and Filters

Go to the *File* → *Open* tab and open the file located on your desktop named **CaseStudy2.pcap**

In this packet capture you will immediately notice that there is a lot more traffic. Lets start by looking at the *Protocol Hierarchy* statistics to see if we can gather some

information about what events have taken place. If you remember from the previous exercise this can be done by selecting *Statistics* → *Protocol Hierarchy*

If you enlarge the window you will notice that **94.4%** of the Packet traffic took involves the **File Transfer Protocol (FTP)**

Wireshark: Protocol Hierarchy Statistics

Display filter: none

| Protocol | % Packets | Packets | % Bytes | Bytes | Mbit/s | End Packets | End Bytes |
|---------------------------------------|-----------|---------|---------|----------|--------|-------------|-----------|
| Address Resolution Protocol | 0.01 % | 19 | 0.00 % | 1014 | 0.000 | 19 | 1014 |
| ▼ Internet Protocol Version 4 | 99.99 % | 204892 | 99.99 % | 21958124 | 0.788 | 0 | 0 |
| ▼ User Datagram Protocol | 0.17 % | 342 | 0.33 % | 72921 | 0.003 | 0 | 0 |
| Domain Name Service | 0.15 % | 315 | 0.30 % | 66585 | 0.002 | 315 | 66585 |
| ▼ NetBIOS Datagram Service | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 |
| ▼ SMB (Server Message Block Protocol) | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 |
| ▼ SMB MailSlot Protocol | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 0 | 0 |
| Microsoft Windows Browser Protocol | 0.00 % | 9 | 0.01 % | 2076 | 0.000 | 9 | 2076 |
| Data | 0.00 % | 4 | 0.01 % | 1964 | 0.000 | 4 | 1964 |
| Hypertext Transfer Protocol | 0.01 % | 12 | 0.01 % | 2100 | 0.000 | 12 | 2100 |
| NetBIOS Name Service | 0.00 % | 2 | 0.00 % | 196 | 0.000 | 2 | 196 |
| ▼ Transmission Control Protocol | 99.82 % | 204550 | 99.66 % | 21885203 | 0.785 | 9479 | 3965158 |
| ▼ Hypertext Transfer Protocol | 0.75 % | 1543 | 5.16 % | 1134152 | 0.041 | 882 | 648406 |
| Line-based text data | 0.12 % | 243 | 0.87 % | 191494 | 0.007 | 243 | 191494 |
| CompuServe GIF | 0.09 % | 177 | 0.51 % | 112399 | 0.004 | 177 | 112399 |
| JPEG File Interchange Format | 0.06 % | 132 | 0.46 % | 101710 | 0.004 | 132 | 101710 |
| Portable Network Graphics | 0.02 % | 46 | 0.16 % | 36023 | 0.001 | 46 | 36023 |
| Media Type | 0.01 % | 14 | 0.05 % | 11786 | 0.000 | 14 | 11786 |
| ▼ JavaScript Object Notation | 0.02 % | 36 | 0.09 % | 20632 | 0.001 | 3 | 598 |
| Line-based text data | 0.02 % | 33 | 0.09 % | 20034 | 0.001 | 33 | 20034 |
| Text item | 0.00 % | 1 | 0.01 % | 1304 | 0.000 | 1 | 1304 |
| Online Certificate Status Protocol | 0.01 % | 11 | 0.04 % | 9402 | 0.000 | 11 | 9402 |
| eXtensible Markup Language | 0.00 % | 1 | 0.00 % | 996 | 0.000 | 1 | 996 |
| Secure Sockets Layer | 0.03 % | 61 | 0.12 % | 26352 | 0.001 | 61 | 26352 |
| File Transfer Protocol (FTP) | 94.40 % | 193445 | 76.30 % | 16755478 | 0.601 | 193445 | 16755478 |
| ▼ NetBIOS Session Service | 0.01 % | 18 | 0.01 % | 2822 | 0.000 | 2 | 186 |
| ▼ SMB (Server Message Block Protocol) | 0.01 % | 16 | 0.01 % | 2636 | 0.000 | 12 | 1886 |

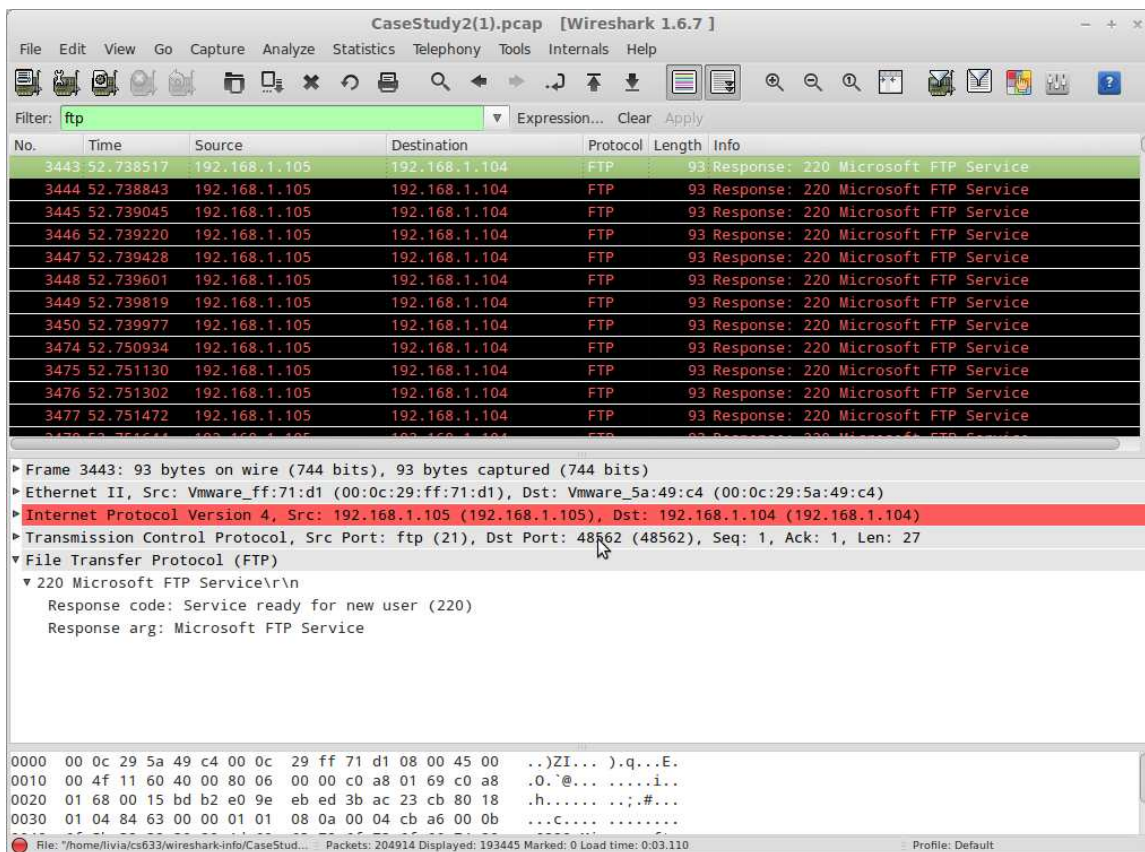
Help Close

This amount of FTP traffic in one network traffic seems very suspicious and warrants closer examination. To do this we need to apply a filter. This can be simply done by typing the word ftp in the Filter Section of the main Window and clicking apply

Filter: Expression... Clear Apply

This traffic appears even more suspicious since at first glance it appears that there are multiple repeated packets. This does not resemble the expected traffic of a legitimate FTP request. Lets examine some of the packets in more detail. Click on one of the first

packets in the Window and fully expand the File Transfer Protocol (FTP) section in the second pane



From this we gather that it appears that FTP is ready for a new user. This seems to suggest multiple sessions attempting to be opened and that they are all being attempted on same IP address. Click on the next several packets and take note of the Destination Port. This is pointed to by the the pointer in the above display and appears in the following line

► Transmission Control Protocol, Src Port: ftp (21), Dst Port: 48562 (48562),

Click on the next Packet in the first frame and notice that the Destination port has increased from 48562 to 48563. Click on the next several packets and again take note of the destination port's incremental changes. This raises another red flag and warrants further investigation. Let's fine tune our filter and see what we can find out. We will filter out all the traffic attempted at one of the destination ports listed. To display a

specific destination port we need to use the tcp.dstport filter. Type in the following in the Filter section and select Apply

Filter: `ftp && tcp.dstport == 48562` Expression... Clear Apply

CaseStudy2(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ftp && tcp.dstport == 48562` Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|---|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3525 | 52.755195 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3619 | 52.775231 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3662 | 52.781680 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3721 | 52.796573 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3775 | 52.802426 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3831 | 52.810754 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3890 | 52.817932 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3951 | 52.825836 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 4019 | 52.853054 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 4085 | 52.874921 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 4155 | 52.882632 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |

▶ Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

▶ Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)

▶ Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

▶ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 48562 (48562), Seq: 1, Ack: 1, Len: 27

▼ File Transfer Protocol (FTP)

▼ 220 Microsoft FTP Service\r\n

Response code: Service ready for new user (220)

Response arg: Microsoft FTP Service

With this filter it seems that someone is trying to login a multitude of time. We are, however, only getting one side of the conversation. This is because with the tcp.dstport setting we are only seeing the return response and not the original request. We can modify our filter to include both sides of the conversation by adding a filter for the source port as follows:

Filter: `ftp && tcp.dstport == 48562 || tcp.srcport == 48562` Expression... Clear Apply

Note the added output:

CaseStudy2(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ftp && tcp.dstport == 48562 || tcp.srcport == 48562` Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|---------------|---------------|----------|--------|---|
| 3443 | 52.738517 | 192.168.1.105 | 192.168.1.104 | FTP | 93 | Response: 220 Microsoft FTP Service |
| 3515 | 52.754697 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3525 | 52.755195 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3556 | 52.757133 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 10th |
| 3619 | 52.775231 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3640 | 52.779121 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3662 | 52.781680 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3682 | 52.791395 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: PASS 1ht9 |
| 3721 | 52.796573 | 192.168.1.105 | 192.168.1.104 | FTP | 91 | Response: 530 User cannot log in. |
| 3727 | 52.797271 | 192.168.1.104 | 192.168.1.105 | FTP | 77 | Request: USER John |
| 3775 | 52.802426 | 192.168.1.105 | 192.168.1.104 | FTP | 99 | Response: 331 Password required for John. |
| 3779 | 52.802861 | 192.168.1.104 | 192.168.1.105 | FTP | 81 | Request: PASS abalone1 |

Frame 3443: 93 bytes on wire (744 bits), 93 bytes captured (744 bits)

Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)

Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

Transmission Control Protocol, Src Port: ftp (21), Dst Port: 48562 (48562), Seq: 1, Ack: 1, Len: 27

File Transfer Protocol (FTP)

220 Microsoft FTP Service\r\n

Response code: Service ready for new user (220)

Response arg: Microsoft FTP Service

With this information we can finally see what is happening. It appears that this is a password attack against an ftp server. The only thing we do not know at this point is whether the password cracking attack was successful. We can determine this by adding one more filter. When a user successfully logs in the response “User Logged In” is sent. Now we will filter for this response by typing in the filter displayed below (Be sure to type the filter **exactly as it appears** below – including the **period** after the word **in**)

Filter: `ftp && ftp.response.arg=="User logged in."` Expression... Clear Apply

This filter returns two packets

CaseStudy2(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp && ftp.response.arg=="User logged in." Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|--------|------------|---------------|---------------|----------|--------|-------------------------------|
| 202103 | 114.041576 | 192.168.1.105 | 192.168.1.104 | FTP | 87 | Response: 230 User logged in. |
| 203754 | 154.825849 | 192.168.1.105 | 192.168.1.104 | FTP | 87 | Response: 230 User logged in. |

▶ Frame 202103: 87 bytes on wire (696 bits), 87 bytes captured (696 bits)

▶ Ethernet II, Src: Vmware_ff:71:d1 (00:0c:29:ff:71:d1), Dst: Vmware_5a:49:c4 (00:0c:29:5a:49:c4)

▶ Internet Protocol Version 4, Src: 192.168.1.105 (192.168.1.105), Dst: 192.168.1.104 (192.168.1.104)

▼ Transmission Control Protocol, Src Port: ftp (21), Dst Port: 48588 (48588), Seq: 79637, Ack: 33657, Len: 21

Source port: ftp (21)

Destination port: 48588 (48588)

[Stream index: 1188]

Sequence number: 79637 (relative sequence number)

[Next sequence number: 79658 (relative sequence number)]

Acknowledgement number: 33657 (relative ack number)

Header length: 32 bytes

▶ Flags: 0x018 (PSH, ACK)

Window size value: 259

[Calculated window size: 66304]

[Window size scaling factor: 256]

▶ Checksum: 0x845d [validation disabled]

▶ Options: (12 bytes)

▶ [SEQ/ACK analysis]

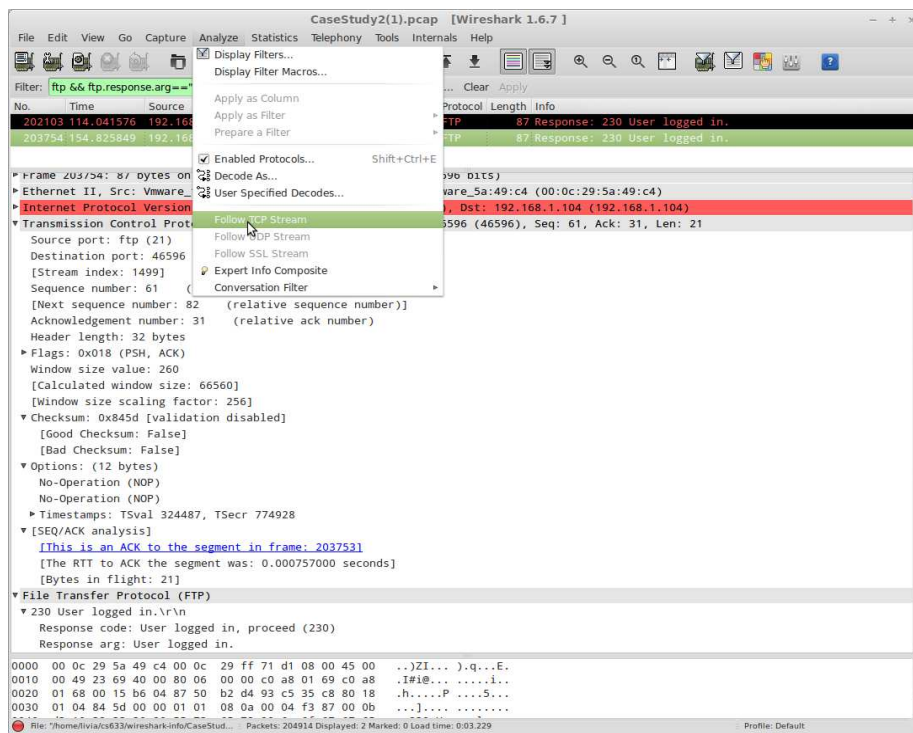
▼ File Transfer Protocol (FTP)

▼ 230 User logged in.\r\n

Response code: User logged in, proceed (230)

Response arg: User logged in.

Examining the detail found in the second pane shows that a successful login was made from IP address 192.168.1.105 to 192.168.1.104 via FTP on Dst Port 48588 and again on Dst Port 46596. To determine what login and password were used we can follow the TCP stream. This can be done by selecting one of the packets. Then go up to the *Analyze* label and click on *Follow TCP Stream*



A Follow TCP Stream window will appear. Scroll down to the last entries and you will see that after multiple unsuccessful attempts the User **John** logged in successfully using the password **Password1234**. John had a very weak password and his account was compromised via the use of a dictionary attack. Beyond this, we could look into the commands issued once the connection was established to determine what the attacker did once he obtained access to FTP.

One question might also be brought up. How did the attacker know FTP was enabled? This might suggest a port scan was performed. To check this, we need to perform a filter on some TCP flags. TCP packets have eight flags. They are FIN, SYN, RST, PSH, ACK, URG, ECE and CWR. These flags have decimal numbers assigned to them as follows:

FIN = 1

SYN = 2

RST = 4

PSH = 8

ACK = 16

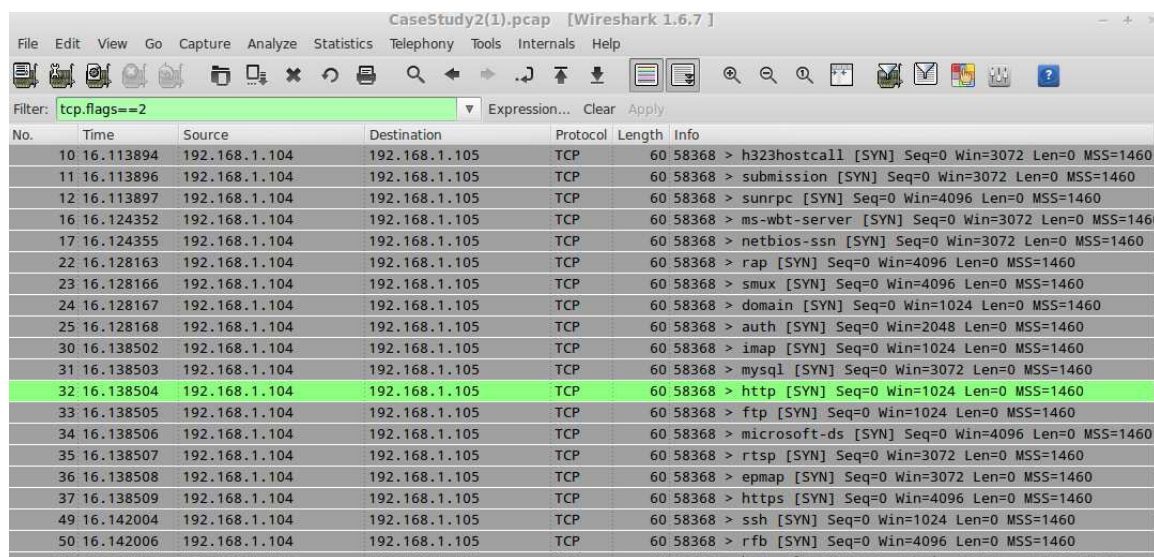
URG = 32

ECE = 64

CWR = 129

To check if a SYN/ACK flag is set we add 2 (the SYN value) to 16 (the ACK value) and the result would be 18. A common port scan is a SYN scan, We will first check for that using the following filter:

The resulting output indicates that a SYN scan was indeed executed:



| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|---|
| 10 | 16.113894 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > h323hostcall [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 11 | 16.113896 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > submission [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 12 | 16.113897 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > sunrpc [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 16 | 16.124352 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > ms-wbt-server [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 17 | 16.124355 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > netbios-ssn [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 22 | 16.128163 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > rap [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 23 | 16.128166 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > smux [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 24 | 16.128167 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > domain [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 25 | 16.128168 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > auth [SYN] Seq=0 Win=2048 Len=0 MSS=1460 |
| 30 | 16.138502 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > imap [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 31 | 16.138503 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > mysql [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 32 | 16.138504 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > http [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 34 | 16.138506 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > microsoft-ds [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 35 | 16.138507 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > rtsp [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 36 | 16.138508 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > epmap [SYN] Seq=0 Win=3072 Len=0 MSS=1460 |
| 37 | 16.138509 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > https [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |
| 49 | 16.142004 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 50 | 16.142006 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 > rfb [SYN] Seq=0 Win=4096 Len=0 MSS=1460 |

This tells us that the attacker knows the ports that were open and that an FTP server was running. Let's examine a few of these lines to see what ports are open. Since we are already aware that the FTP port is open let's scroll down and select line No 33 (see first column in the first pane). Now go to the *Analyze* tab as select *Follow TCP Stream*. Although nothing appears in the TCP Stream window if we close it we see three packets are displayed.

CaseStudy2(1).pcap [Wireshark 1.6.7]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `tcp.stream eq 13` Expression... Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|-----------|---------------|---------------|----------|--------|--|
| 33 | 16.138505 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 → ftp [SYN] Seq=0 Win=1024 Len=0 MSS=1460 |
| 41 | 16.138751 | 192.168.1.105 | 192.168.1.104 | TCP | 58 | ftp → 58368 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 |
| 46 | 16.139105 | 192.168.1.104 | 192.168.1.105 | TCP | 60 | 58368 → ftp [RST] Seq=1 Win=0 Len=0 |

▶ Frame 33: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

▶ Ethernet II, Src: Vmware_5a:49:c4 (00:0c:29:5a:49:c4), Dst: Vmware_ff:71:d1 (00:0c:29:ff:71:d1)

▶ Internet Protocol Version 4, Src: 192.168.1.104 (192.168.1.104), Dst: 192.168.1.105 (192.168.1.105)

▼ Transmission Control Protocol, Src Port: 58368 (58368), Dst Port: ftp (21), Seq: 0, Len: 0

Source port: 58368 (58368)

Destination port: ftp (21)

[Stream index: 13]

Sequence number: 0 (relative sequence number)

Header length: 24 bytes

▶ Flags: 0x002 (SYN)

Window size value: 1024

[Calculated window size: 1024]

▼ Checksum: 0x1a6d [validation disabled]

[Good Checksum: False]

[Bad Checksum: False]

▼ Options: (4 bytes)

Maximum segment size: 1460 bytes

The first line is Packet Number 33 and is the original SYN request. The second line (Packet 41) is the SYN, ACK response. This tells the requester that the port is in fact open. Looking in the second pane we see the Transmission Control Protocol line which confirms that the Dst Port is port 21 (FTP).

▼ Transmission Control Protocol, Src Port: 58368 (58368), Dst Port: ftp (21), Seq: 0, Len: 0

Clear the filter and let's try another protocol. Start again by typing `tcp.flags == 2` in the filter to filter out all SYN requests. This time select packet number 32 for http, and go to *Analyze* → *Follow TCP Stream*. Here we see that only two packets appear. The original SYN request and then a RST, ACK response. No SYN, ACK is displayed so can determine that this port is not open and no http server is running (or at least not on port 80).

This concludes the Network Analysis exercise. Please close out of the Wireshark application and shutdown your Network Analysis Virtual Machine.

References:

Wireshark Case Study[1,2].pdf presented by Florian Buchholz and Brett Tjaden

Wireshark User Guide

http://www.wireshark.org/docs/wsug_html_chunked/index.html

Advanced Wireshark tutorial: Packet and network security analysis

<http://searchsecurity.techtarget.in/tip/Advanced-Wireshark-tutorial-Packet-and-netowrk-security-analysis>

Quick and Dirty Wireshark Tutorial

<http://searchsecurity.techtarget.in/tutorial/Quick-and-dirty-Wireshark-tutorial>