



Hands-on Network Traffic Analysis

2016 Cyber Defense Boot Camp



What is this module about?



?



What is this module about?

- How to read network traffic?
 - 1) What does it look like?
 - 2) How to make sense out of it?
- Prerequisite: network **packet** & **packet analyzer**: (header, data)
 - Enveloped letters inside another envelope

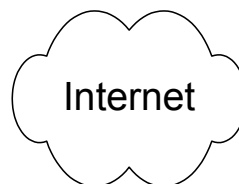


Prerequisite: TCP/IP Model (1/9)

- How does Internet work?



Alice

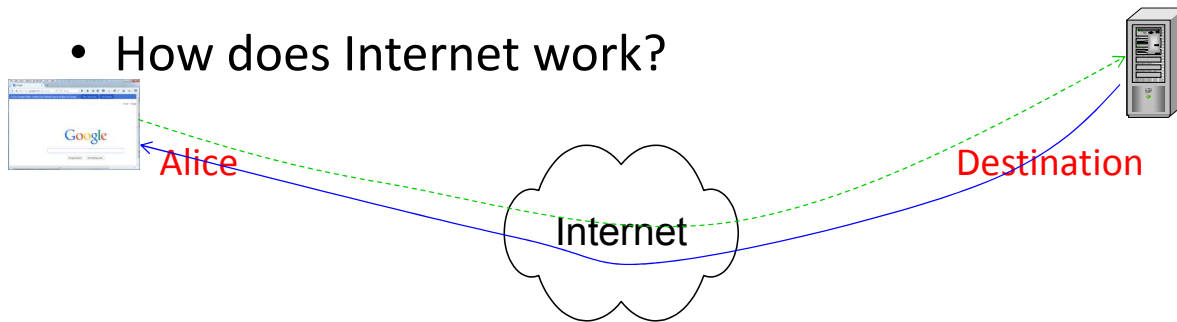


Destination



Prerequisite: TCP/IP Model (2/9)

- How does Internet work?

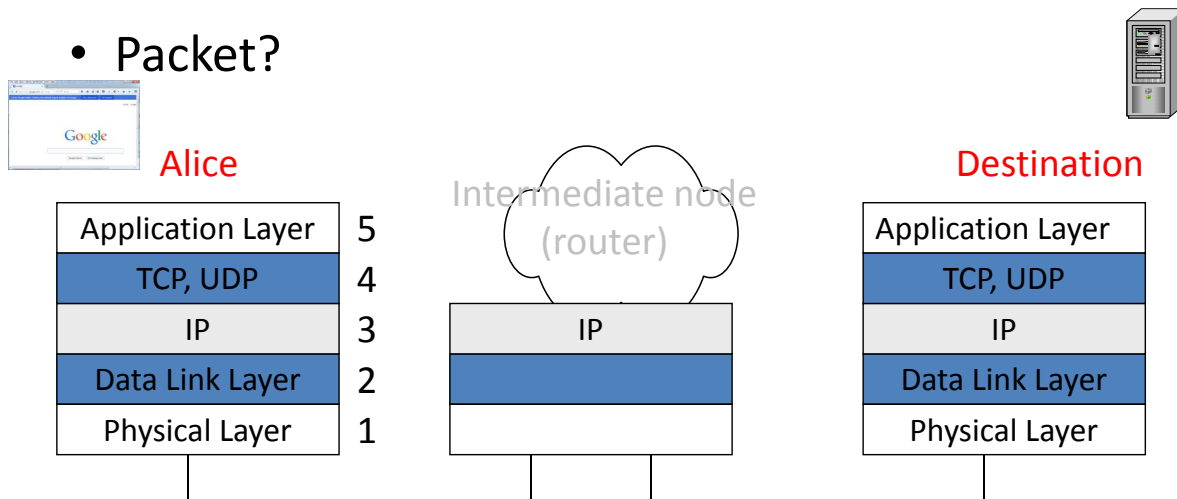


5



Prerequisite: TCP/IP Model (3/9)

- Packet?



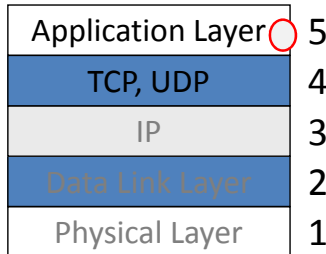
6

Prerequisite: TCP/IP Model (4/9)

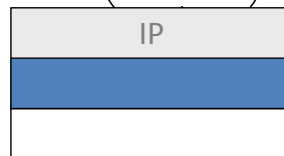
- Alice's browser wants to send data to the server



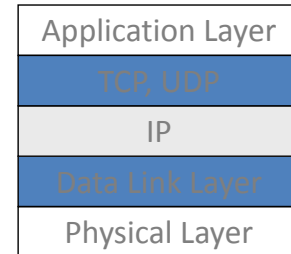
Alice



Intermediate node
(router)



Destination



Application data

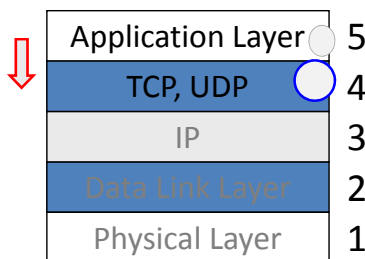
7

Prerequisite: TCP/IP Model (5/9)

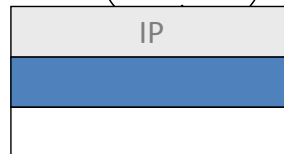
- Packet: header + "data"



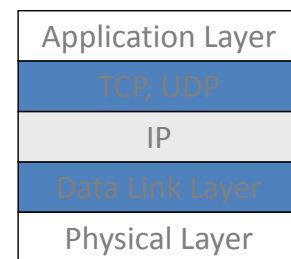
Alice



router



Destination



What is inside it?

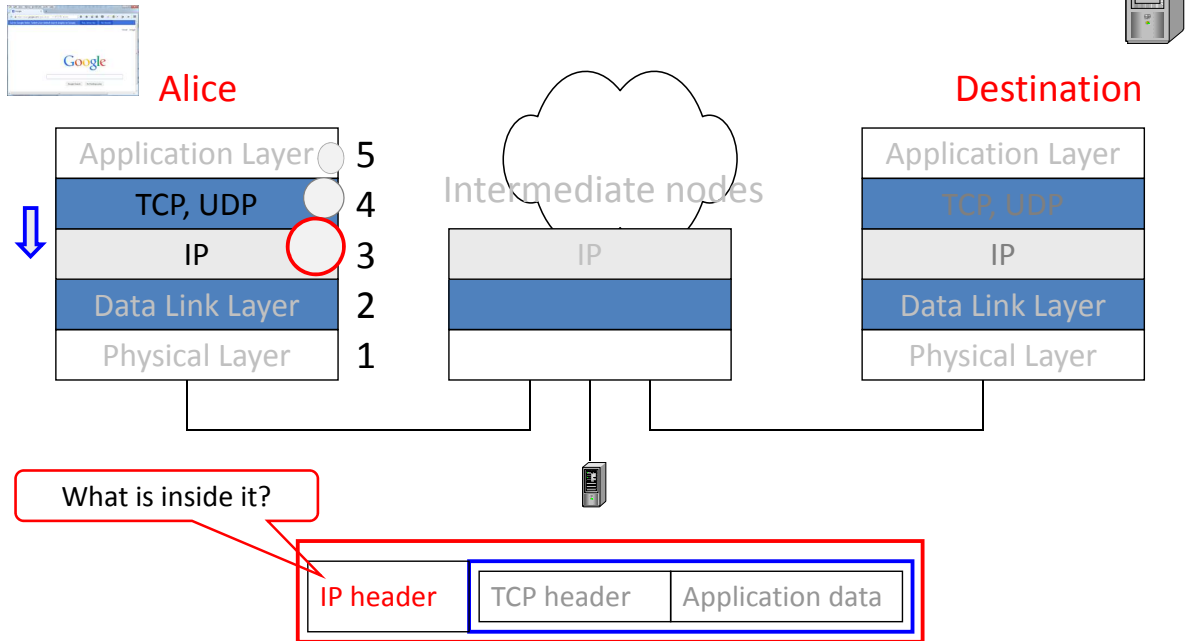
TCP header

Application data

8

Prerequisite: TCP/IP Model (6/9)

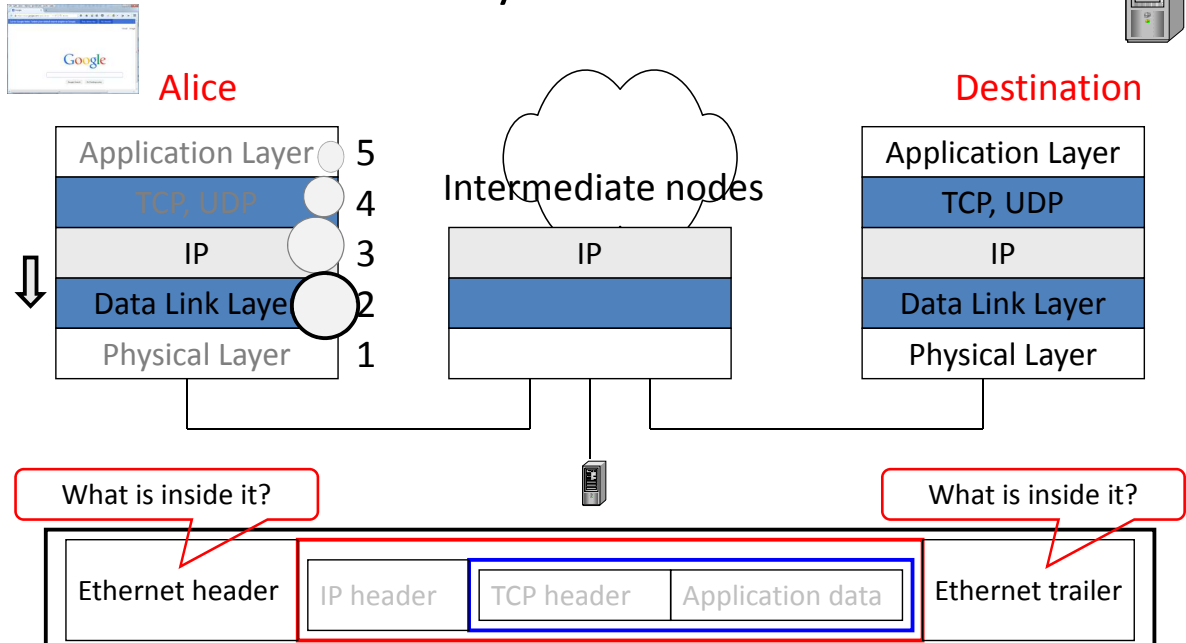
- TCP → IP



9

Prerequisite: TCP/IP Model (7/9)

- IP → Data Link Layer



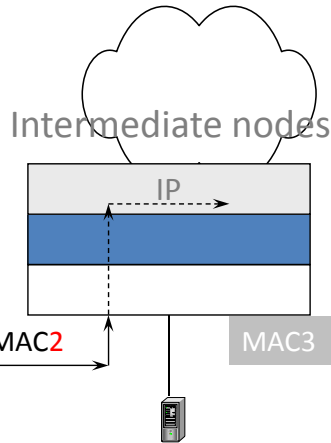
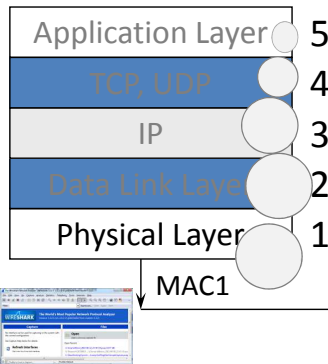
10

Prerequisite: TCP/IP Model (8/9)

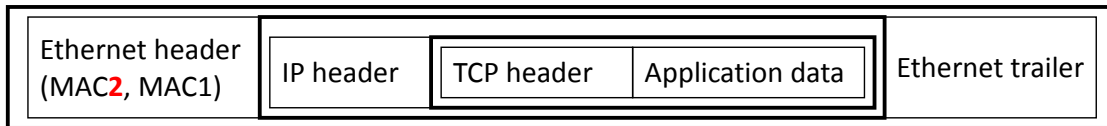
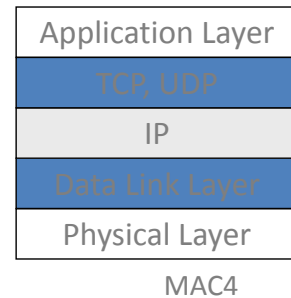
- Data Link Layer → physical layer



Alice



Destination



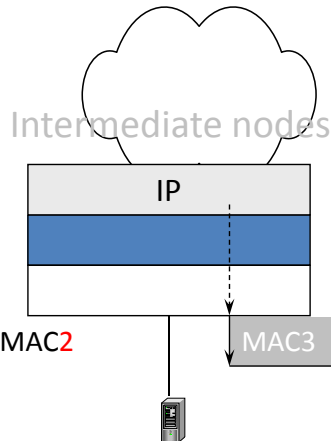
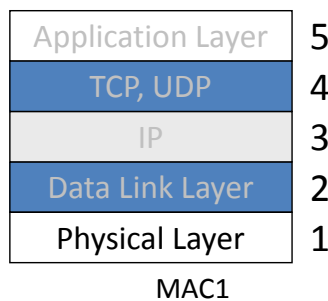
11

Prerequisite: TCP/IP Model (9/9)

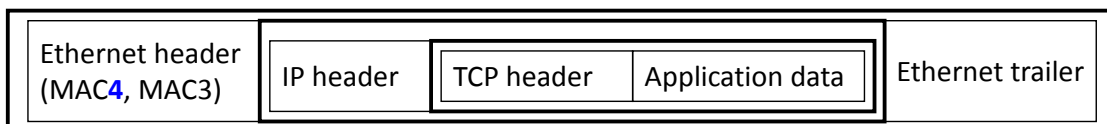
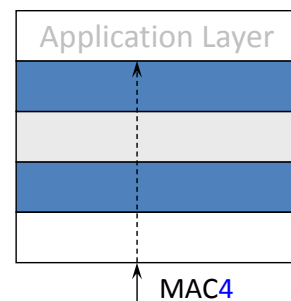
- IP routing



Alice



Destination



12

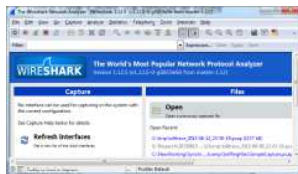
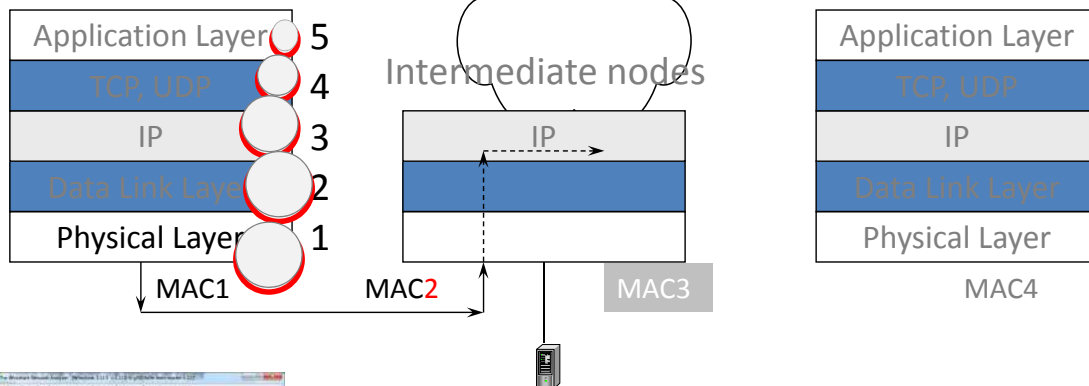
Goals of this module (1/2)

1) Examine single TCP/IP/Ethernet packets



Alice

Destination



13

Goals of this module (2/2)

2) Find all packets related to one specific packet

3) Learn how to reduce packets for **easy packet analysis**

- Statistics
 - Protocol hierarchy
 - HTTP requests
- Conversations
- Expressions

Two exercises

Exercise ①: goals 1) ~ 2)

SimpleCapture.pcap, WebCapture.pcap

Exercise ②: goals 3) ~ 4)

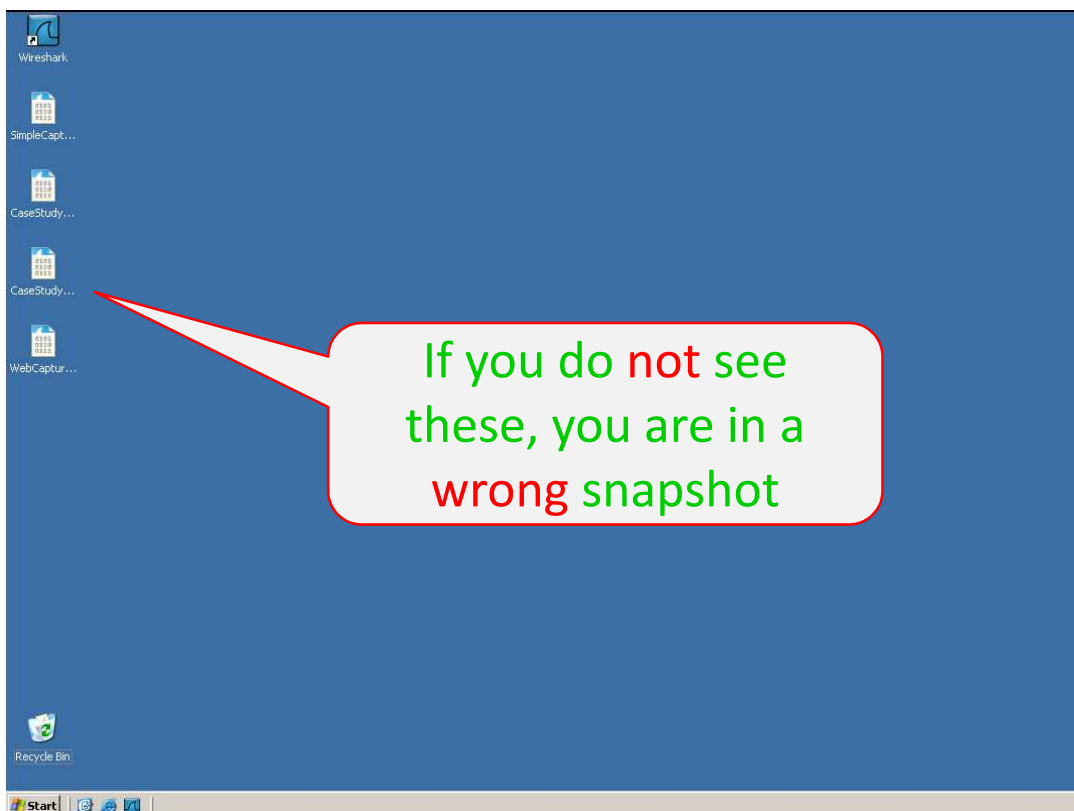
CaseStudy1.pcap, CaseStudy2.pcap

4) Learn how to find out attack packets (needle from a hay stack)

With what tool? Wireshark!

Step 0

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



Exercise ①: Basic Network Analysis

Double click on this

This example shows the basics of network traffic

What does a packet look like?

① One row, one packet (in chronological order)

② Inside the current (i.e. first) packet

③ The data of the current (i.e. first) packet

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	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=1138360348 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=1138360348 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	0.91114100	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:c3: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.P.7...E..

0010 00 79 46 1a 40 00 3f 06 d6 18 c0 a8 4e fe c0 a8 .yF.8.?....N...

0020 4e fd d7 48 0d 3d 99 80 22 0c 66 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 4b0F.....NK

0050



This is packet 304
How can we find all related packets?

① Click on packet 304

② Right click

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
289	9.84078700	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	9.843967100	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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 74.125.2...

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: 192.168.78.254, Dst: 192.168.78.253
User Datagram Protocol, Src Port: 50187, Dst Port: 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 6cw ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01e.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
289	9.84078700	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	9.843967100	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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	192.168.78.254	192.168.78.253	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 74.125.2...

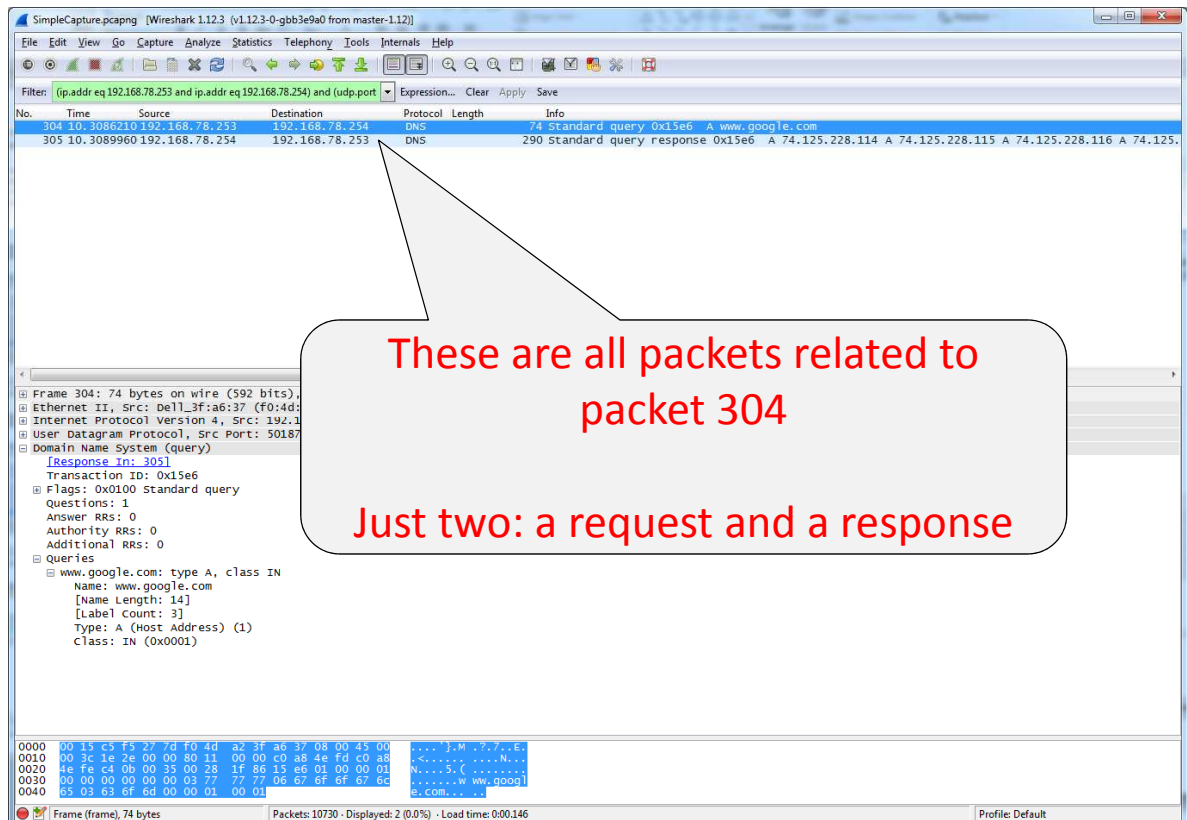
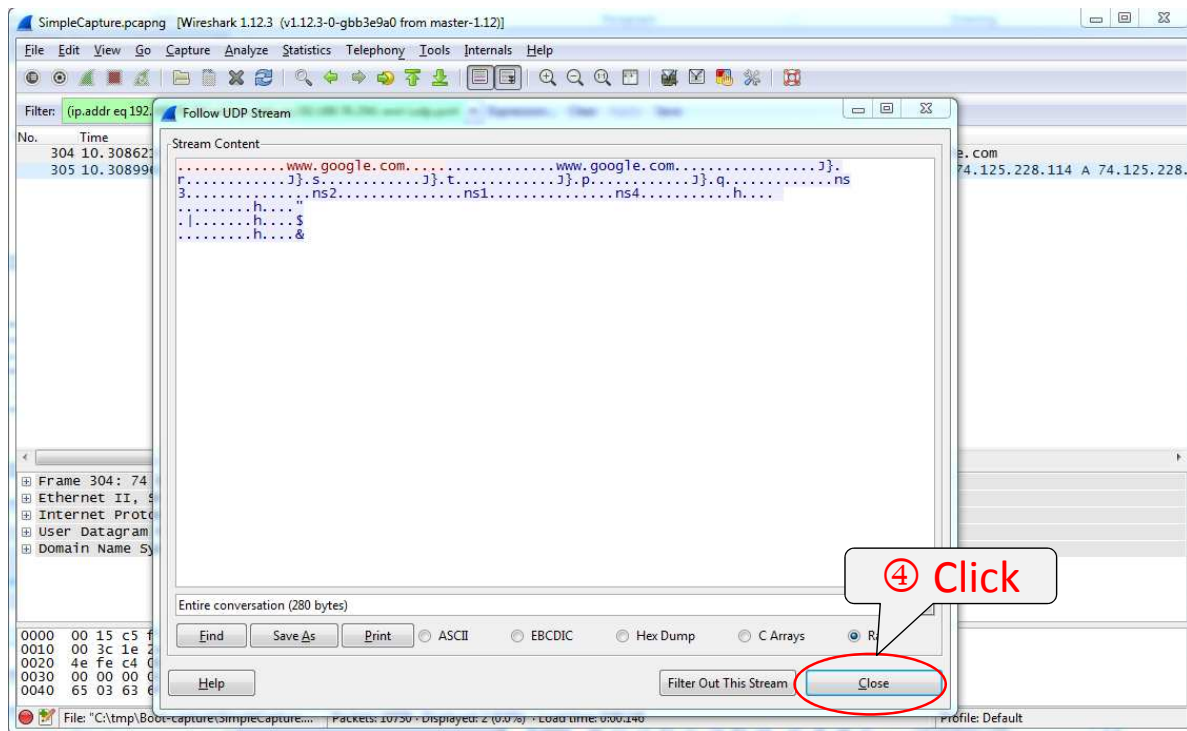
Frame 304: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Dell_3f:a6:37 (f0:4d:a2:3f:a6:37), Dst: Dellinc_f5:27:7d (00:15:c5:f5:27:7d)
Internet Protocol Version 4, Src: 192.168.78.254, Dst: 192.168.78.253
User Datagram Protocol, Src Port: 50187, Dst Port: 53
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 6cw ww.googl
0040 65 03 63 6f 6d 00 00 01 00 01e.com....

File: C:\tmp\Boot-capture\SimpleCapture... Packets: 10730 · Displayed: 10730 (100.0%) · Load time: 0:00:385 Profile: Default

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

③ Choose this





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

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port ...)

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

⑤ Click on the first packet to make it the current packet

⑥ The details of the current packet:
This is a DNS query for the IP address of www.google.com

⑦ Data of 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)
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 00M .? .? .? .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 13 e6 01 00 00 01 ... NS . (.
0030 00 00 00 00 03 77 77 06 67 6f 6f 67 6f 67 6cw ww.goog
0040 65 03 63 6f 6d 00 01 00 01 00 00 00 01 00 01 ... e,com

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)]

Filter: (ip.addr eq 192.168.78.253 and ip.addr eq 192.168.78.254) and (udp.port ...)

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

⑧ Click on the second packet

⑨ The details of the current packet:
Response to the DNS query

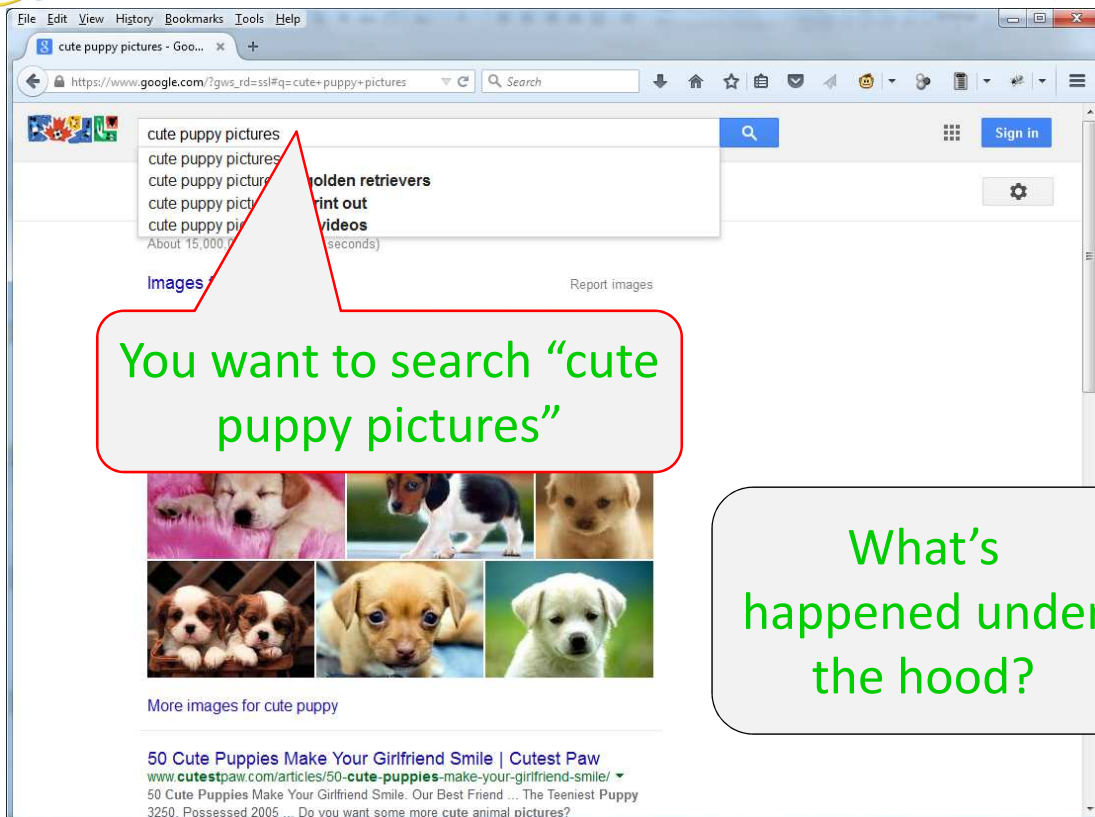
⑩ Data of the current packet

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)
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 00M .? .? .? .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 13 e6 01 00 00 01 ... NS . (.
0030 00 00 00 00 03 77 77 06 67 6f 6f 67 6f 67 6cw ww.goog
0040 65 03 63 6f 6d 00 01 00 01 00 00 00 01 00 01 ... e,com

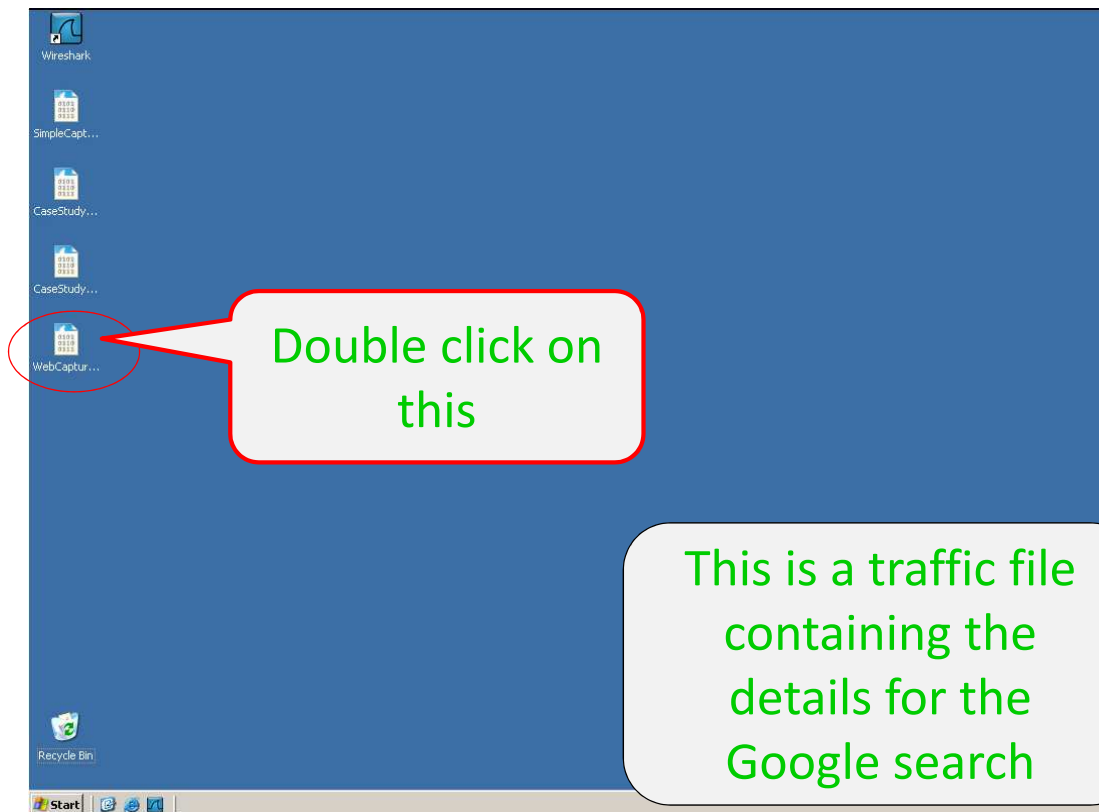
Frame (Frame), 290 bytes Packets: 10730 - Displayed: 2 (0.0%) - Load time: 0:00:146

So far, so good?



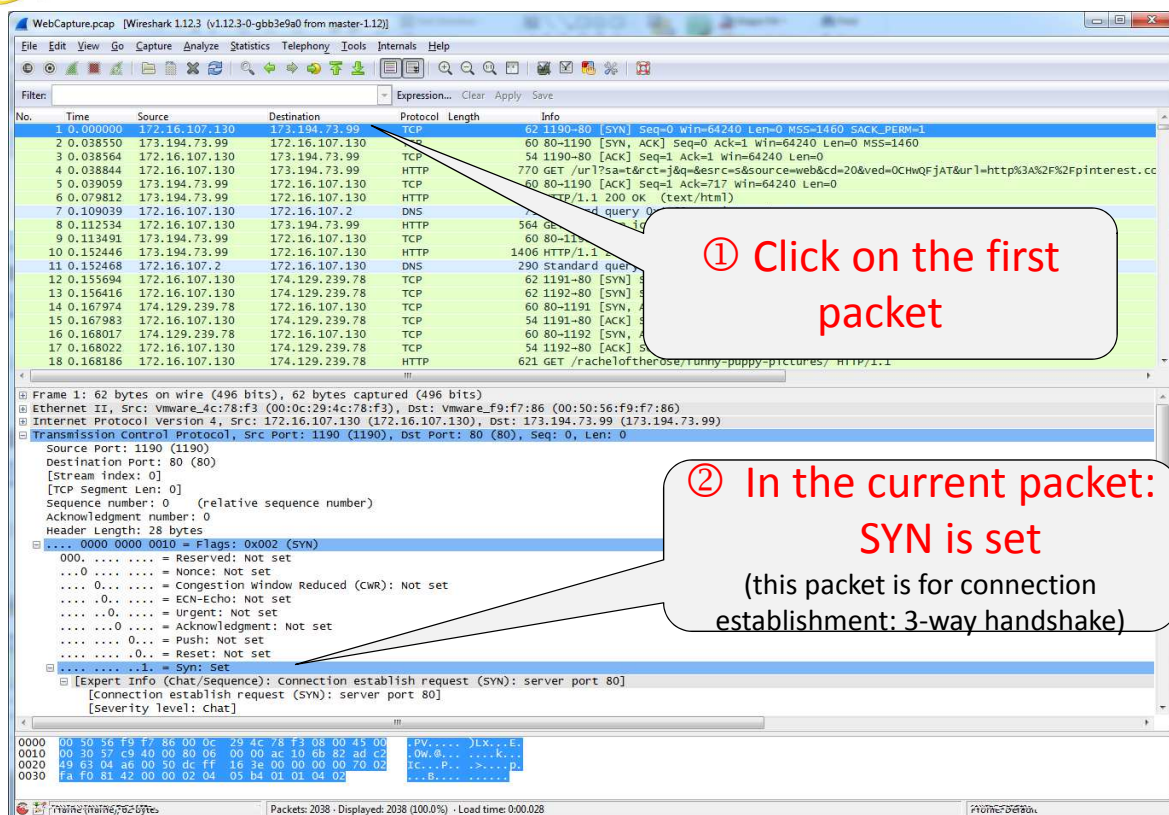
You want to search "cute puppy pictures"

What's happened under the hood?



Double click on this

This is a traffic file containing the details for the Google search



Click on the first packet

In the current packet:
SYN is set
(this packet is for connection establishment: 3-way handshake)



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

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	0.038564	172.16.107.130	173.194.73.99	TCP	60	80->1190 [ACK] Seq=1 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 MSS=1460
4	0.038844	172.16.107.130	173.194.73.99	HTTP	770	GET /url?sa=t&ct=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	645	HTTP/1.1 200 OK (text/html)
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 /racheloftherose/funny-puppy-pictures/ HTTP/1.1
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 (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] 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=1 Ack=1 win=64240 Len=0
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=1 Ack=1 win=64240 Len=0
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

Frame 2: 60 bytes on wire (480 bits), 60 bytes captured (480 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: 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)
... 0000 0000 = Reserved: Not set
... 0000 0000 = Nonce: Not set
... 0000 0000 = Congestion window Reduced (cwr): Not set
... 0000 0000 = ECN-Echo: Not set
... 0000 0000 = Urgent: Not set
... 0000 0000 = Acknowledgment: Set
... 0000 0000 = Push: Not set
... 0000 0000 = Reset: Not set
... 0000 0001 = 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 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

③ Click on the second packet

④ In the current packet: both ACK and SYN are set (this packet is for connection establishment: 2nd packet of the 3-way handshake)



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

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	0.038564	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 MSS=1460
4	0.038844	172.16.107.130	173.194.73.99	HTTP	770	GET /url?sa=t&ct=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	645	HTTP/1.1 200 OK (text/html)
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 /racheloftherose/funny-puppy-pictures/ HTTP/1.1
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 (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] 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=1 Ack=1 win=64240 Len=0
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=1 Ack=1 win=64240 Len=0
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

Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 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: 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)
... 0000 0000 = Reserved: Not set
... 0000 0000 = Nonce: Not set
... 0000 0000 = Congestion window Reduced (cwr): Not set
... 0000 0000 = ECN-Echo: Not set
... 0000 0000 = Urgent: Not set
... 0000 0000 = Acknowledgment: Set

⑤ Click on the third packet

⑥ In the current packet: the ACK is set (this packet is for connection establishment: 3rd packet of the 3-way handshake)

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)]

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	0.039059	173.194.73.99	172.16.107.130	TCP	60	80->1190 [ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.079812	173.194.73.99	172.16.107.130	HTTP	1406	HTTP/1.1 200 OK
6	0.079812	173.194.73.99	172.16.107.130	HTTP	290	Standard query
7	0.109039	172.16.107.130	172.16.107.2	DNS	564	GET /url?sa=t&rc=j&q=&src=ss&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.com/
8	0.112534	172.16.107.130	173.194.73.99	HTTP	60	80->1190
9	0.113491	173.194.73.99	172.16.107.130	TCP	60	80->1190
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]
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

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&rc=j&q=&src=ss&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: PRF=f-3b7a5867adaf85227m=1370363771;LW=1370363771
 connection: keep-alive/r/n
 [Full] request URI [truncated]: http://www.google.com/url?sa=t&rc=j&q=&src=ss&source=web&cd=20&ved=0CHwQFjAT&url=http%3A%2F%2Fpinterest.com/

[HTTP request 1/3]
 [Response in frame: 6]
 [Next request in frame: 8]

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)]

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
27	0.391930	174.129.239.78	172.16.107.130	TCP	1478	TCP segment of
28	0.391937	172.16.107.130	174.129.239.78	TCP	54	1191->80 [ACK]
29	0.392163	174.129.239.78	172.16.107.130	TCP	1502	TCP segment of
30	0.392378	174.129.239.78	172.16.107.130	TCP	1502	TCP segment of
31	0.392387	172.16.107.130	174.129.239.78	TCP	54	1191->80 [ACK]
32	0.392520	174.129.239.78	172.16.107.130	TCP	1502	TCP segment of
33	0.392672	174.129.239.78	172.16.107.130	TCP	1502	TCP segment of
34	0.392699	172.16.107.130	174.129.239.78	TCP	54	1191->80 [ACK]
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
39	0.447690	172.16.107.130	72.21.91.19	TCP	62	1191->80 [ACK]
40	0.456766	72.21.91.19	172.16.107.130	TCP	60	80->1191 [SYN]
41	0.456775	172.16.107.130	72.21.91.19	TCP	60	80->1191 [SYN]
42	0.457003	172.16.107.130	72.21.91.19	HTTP	60	80->1193 [ACK]
43	0.457044	72.21.91.19	172.16.107.130	TCP	60	80->1193 [ACK]

Frame 42: 574 bytes on wire (4592 bits), 574 bytes captured (4592 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: 72.21.91.19 (72.21.91.19)
 Transmission Control Protocol, Src Port: 1193 (1193), Dst Port: 80 (80), Seq: 1, Ack: 1, 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: 0xbcd0 [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/n
 Host: passsets-ec.pinterest.com/r/n

Frame (frame), 574 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)]

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
37	0.421443	172.16.107.130	172.16.107.2	DNS	84	Standard query response
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	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	0.456808	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), 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 (00:50:56: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: 521, Win: 64240, 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\n

Host: passets-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 .X.0....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 36 36 inboard_63782886

0050 7a e3 73 73 70 48 64 64 60 7e 31 7a 31 6d 0c 48 ccc utf-8 /1.1

File: C:\tmp\Boot-capture\WebCapture.pcap Packets: 2038 - Displayed: 2038 (100.0%) - Load time: 0:00:028 Profile: Default

① Click on the 42th packet

② Right click on it



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

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
37	0.421443	172.16.107.130	172.16.107.2	DNS	84	Standard query response
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	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	0.456808	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), 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 (00:50:56: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: 521, Win: 64240, 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\n

Host: passets-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 .X.0....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 36 36 inboard_63782886

0050 7a e3 73 73 70 48 64 64 60 7e 31 7a 31 6d 0c 48 ccc utf-8 /1.1

File: C:\tmp\Boot-capture\WebCapture.pcap Packets: 2038 - Displayed: 2038 (100.0%) - Load time: 0:00:028 Profile: Default

③ Choose this



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

Filter: tcp.stream eq 3

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	HTTP	60	200 OK
44	0.474208	72.21.91.19	172.16.107.130	TCP	62	1193->80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
45	0.474220	72.21.91.19	172.16.107.130	TCP	60	80->1193 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
46	0.474222	72.21.91.19	172.16.107.130	TCP	54	1193->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
47	0.474224	72.21.91.19	172.16.107.130	HTTP	574	GET /css/pinboard_63782886.css HTTP/1.1
48	0.474226	72.21.91.19	172.16.107.130	HTTP	60	200 OK
49	0.474229	72.21.91.19	172.16.107.130	TCP	62	1193->80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
50	0.474231	72.21.91.19	172.16.107.130	TCP	60	80->1193 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
51	0.474236	72.21.91.19	172.16.107.130	TCP	54	1193->80 [ACK] Seq=1 Ack=1 win=64240 Len=0
52	0.474238	72.21.91.19	172.16.107.130	HTTP	574	GET /css/pinboard_63782886.css HTTP/1.1
53	0.474240	72.21.91.19	172.16.107.130	HTTP	60	200 OK
54	0.474247	172.16.107.130	72.21.91.19	HTTP	574	GET /css/pinboard_63782886.css HTTP/1.1
55	0.474323	172.16.107.130	72.21.91.19	HTTP	60	200 OK
56	0.474361	172.16.107.130	72.21.91.19	HTTP	60	200 OK

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="e32zk/Ak86gDTfWnsITrypL0G1ZP2tZvYsA21tY8vyckNFUN8T2dfe18q1KN/
J2tLVV04tL5M5fXm1sq1rPI19HfXLPcPCTT1CwnK1Q23NPf1ca30dQmtBko39XNnKI0KCT2Tle1BQCR/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: "f5589042cdc429e0ce01041b1ce4bd"
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: oLATH3geDpIfHdwFRh1/3CrUeXOH1BFvGvFNaT+eLpcgwM2XXBShd4G3mxEQU
X-amz-request-id: 9233628493815020
X-cache: HIT
Content-Length: 28294

.....S+K..pinboard_63782886.css.....[...W.S...L[...CuZ.1,+F...}.....Ip.R.....
+...f-v=K..K0..u+...:1..F...0...h51...<R..?...MoF...1..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

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 gsl.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	54	1191->80 [ACK] Seq=568 Ack=12471 Win=63354 Len=0
72	0.492804	172.16.107.130	174.129.239.78	TCP	62	1191->80 [SYN] Seq=0 win=64240 Len=0 MSS=1460 SACK_PERM=1
73	0.493363	172.16.107.130	134.126.9.42	TCP	62	1195->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) captured (1824 bits)

Ethernet II, Src: Vmware_f9:78:f6, 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

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

Domain Name System (response)

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

0010 00 06 a3 1a 00 00 80 11 68 57 ac 10 6b 02 ac 10hw.k...

0020 6b 82 3f ff 00 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 65assets-e

0040 63 09 70 69 6e 74 65 72 65 73 74 03 6f 6d 00 c.pinter est.com.

File: C:\tmp\Boot-capture\WebCapture.p... Packets: 2038 - Displayed: 1985 (97.4%) - Load time: 0:00:024

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



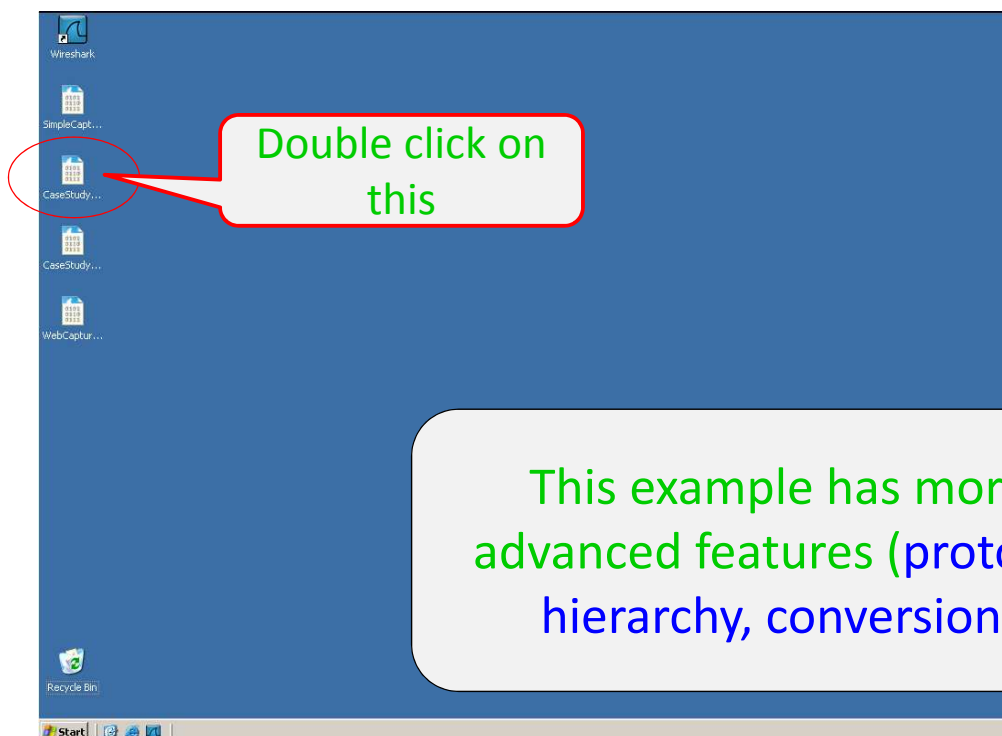
Quiz

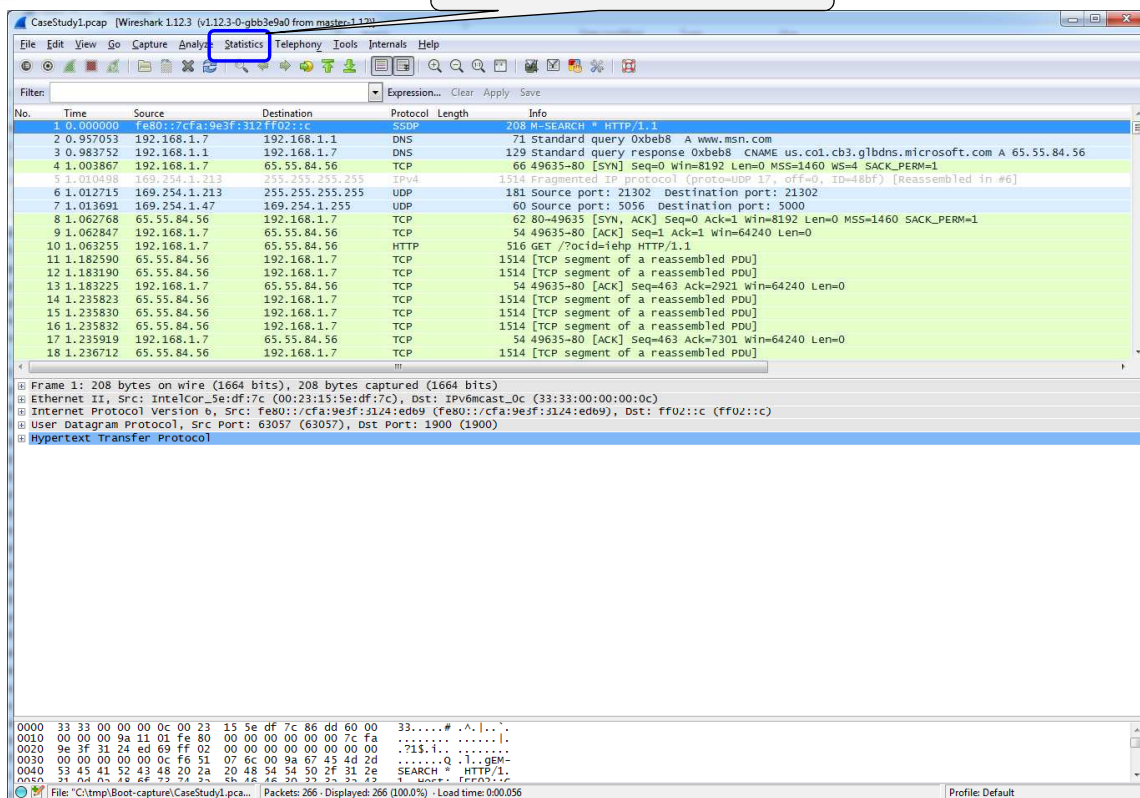
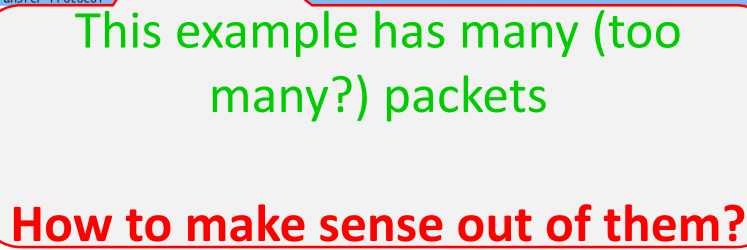
Everybody likes a quiz!

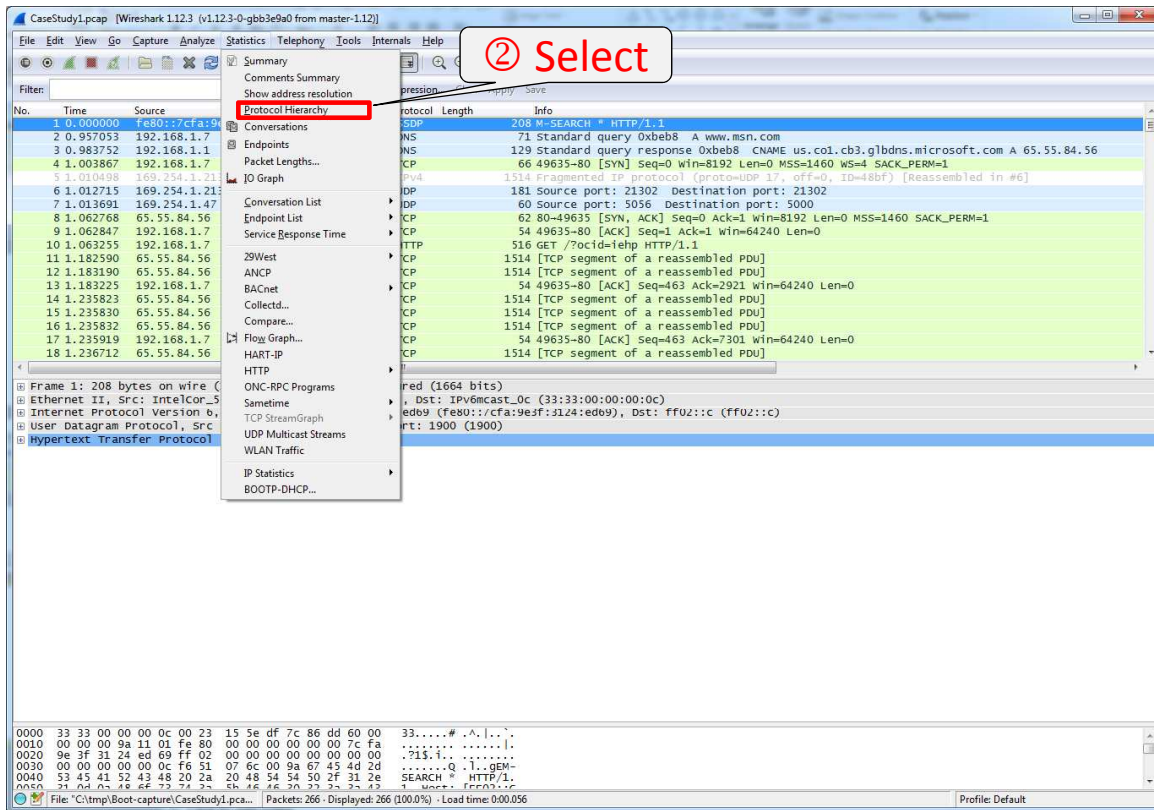
- Wireshark is a popular tool for:
 - a) Testing web applications for vulnerabilities
 - b) Cracking WEP encryption used in older wireless networks
 - c) Analyzing the contents of network traffic
 - d) Crafting phishing e-mails
 - e) None of the above



Exercise 2

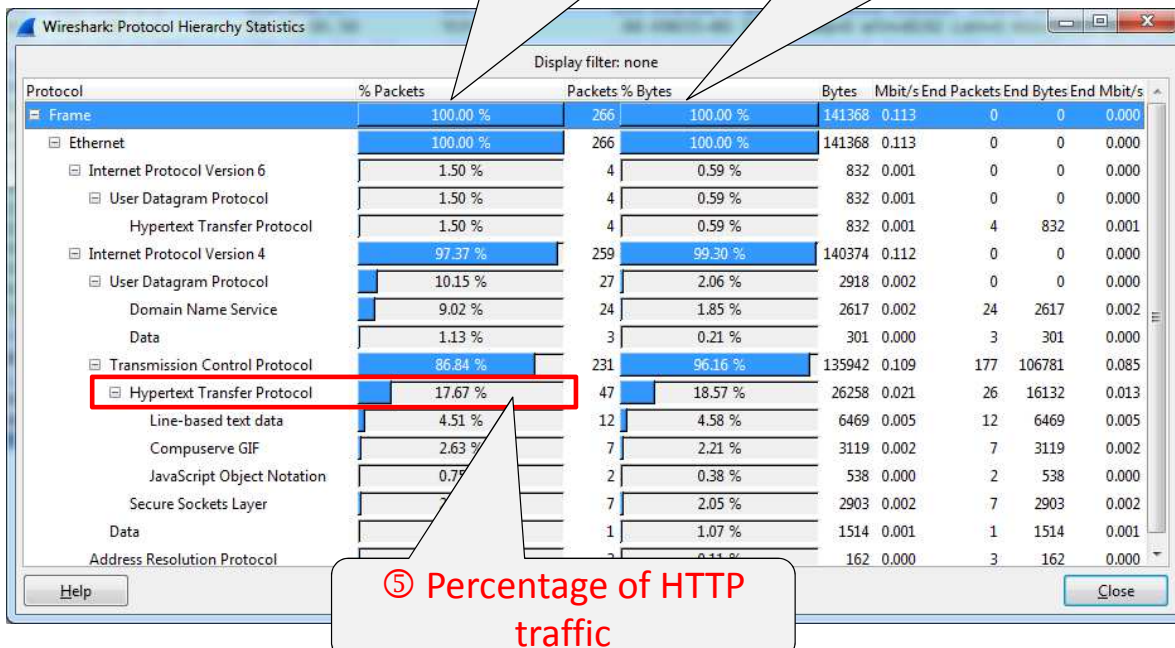






③ This column shows the packet # percentage

④ This column shows the byte # percentage





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

No.	Time	Source
1	0.000000	fe80::17cfa:9a...
2	0.957053	192.168.1.7
3	0.983752	192.168.1.1
4	1.003867	192.168.1.7
5	1.010498	169.254.1.21
6	1.012715	169.254.1.21
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 Summary

- Comments Summary
- Show address resolution
- Protocol Hierarchy
 - Conversations
 - Endpoints
 - Packet Lengths...
 - JO 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	SEARCH * HTTP/1.1
NS	71	Standard query 0xeb8 A www.msn.com
NS	129	Standard query response 0xeb8 CNAME us.col.cb3.glbldns.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=lehp 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	54	49635-80 [ACK] Seq=463 Ack=2921 Win=64240 Len=0
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...
Internet Protocol Version 6, Src: fe80::17cfa:9a...
User Datagram Protocol, Src Port: 21302, Dst Port: 5056
Hypertext Transfer Protocol

File: "C:\tmp\Boot-capture\CaseStudy1.pcap..." 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

No.	Time	Source
1	0.000000	fe80::17cfa:9a...
2	0.957053	192.168.1.7
3	0.983752	192.168.1.1
4	1.003867	192.168.1.7
5	1.010498	169.254.1.21
6	1.012715	169.254.1.21
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 Summary

- Comments Summary
- Show address resolution
- Protocol Hierarchy
 - Conversations
 - Endpoints
 - Packet Lengths...
 - JO 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	SEARCH * HTTP/1.1
NS	71	Standard query 0xeb8 A www.msn.com
NS	129	Standard query response 0xeb8 CNAME us.col.cb3.glbldns.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=lehp 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	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...
Internet Protocol Version 6, Src: fe80::17cfa:9a...
User Datagram Protocol, Src Port: 21302, Dst Port: 5056
Hypertext Transfer Protocol

File: "C:\tmp\Boot-capture\CaseStudy1.pcap..." 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:312:f02::c	192.168.1.1	SSDP	208	M-SEARCH * HTTP/1.1
2	0.957053	192.168.1.7	192.168.1.1	DNS	71	Standard query 0xb8b8 A www.msn.com
3	0.983752	192.168.1.1	192.168.1.7	DNS	129	Standard query response 0xb8b8 CNAME us.col.cb3.glbdns.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	ICMP	80	Source port: 5056 Destination port: 5000
8	1.062768	65.55.84.56	192.168.1.7	TCP	60	8035 [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	60	80 [ACK] Seq=1 Ack=1 win=64240 Len=0
10	1.063255	192.168.1.7	65.55.84.56	TCP	60	?ocid=iehp HTTP/1.1
11	1.182590	65.55.84.56	192.168.1.7	TCP	60	segment of a reassembled PDU
12	1.183190	65.55.84.56	192.168.1.7	TCP	60	segment of a reassembled PDU
13	1.183225	192.168.1.7	65.55.84.56	TCP	60	80 [ACK] Seq=463 Ack=2921 win=64240 Len=0
14	1.235823	65.55.84.56	192.168.1.7	TCP	60	segment of a reassembled PDU
15	1.235830	65.55.84.56	192.168.1.7	TCP	60	1514 [TCP segment of a reassembled PDU]
16	1.235832	65.55.84.56	192.168.1.7	TCP	60	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

⑧ Click

Frame 1: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface 0
 Ethernet II, Src: IntelCor_Se:df:7c (00:23:15:5e:df:7c), Dst: IPv6mcast:02:00:00:00:00:00 (02:00:00:00:00:00)
 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.....#.A...
 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 00715.1...
 0030 00 00 00 00 00 0c fe 51 07 6c 00 9a 67 45 4d 2dQ...gB-
 0040 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f 31 2e SEARCH * HTTP/1.
 0050 51 a4 0c 48 64 73 74 35 6b 46 46 20 35 35 35 35 1 User-Agent: fe80::7cfa:9e3f:3124:ed69

File: "C:\tmp\boot-capture\CaseStudy1.pcap" Packets: 266 - Displayed: 266 (100.0%) - Load time: 0:00:056 Profile: Default

Requests with filter:

Topic / Item

- HTTP Requests by HTTP Host
 - rad.msn.com
 - [FF02::C]:1900
 - www.msn.com
 - /sck.aspx?cv=_SS%3dSID%3d7C73BA2D0D8D452E95C8DB3AFE187980%3b&h=fe92cd76-4cb3-03b6-8afc-cd7f85f73879
 - /ajax/conditionalbanners.aspx
 - ?ocid=iehp
 - www.bing.com
 - www.google.com
 - udc.msn.com
 - media.match.com
 - view.atdmt.com
 - c.msn.com
 - b.scorecardresearch.com

Copy Save As Close

⑨ This shows the distribution of HTTP requests to each server



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%3d7C73BA2D0D8D452E95C8DB3AFE187980%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



① Select Statistics

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

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

Filter:

Conversations

Summary

Comments Summary

Show address resolution

Protocol Hierarchy

Conversations

Endpoints

Packet Lengths...

IO Graph

Conversation List

Endpoint List

Service Response Time

25West

ANCP

BACnet

Collectd...

Compare...

Flow Graph...

HART-IP

HTTP

ONC-RPC Programs

Sametime

TCP StreamGraph

UDP Multicast Streams

WLAN Traffic

IP Statistics

BOOTP-DHCP...

208 M-SEARCH * HTTP/1.1

71 standard query 0xb8b8 A www.msn.com

129 standard query response 0xb8b8 cNAME us.col.cb3.glbns.microsoft.com A 65.55.84.56

66 49635-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

1514 fragmented IP protocol (proto=UDP 17, off=0, ID=48bf) [Reassembled in #6]

181 Source port: 21302 Destination port: 21302

60 Source port: 5056 Destination port: 5000

62 80-49635 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 SACK_PERM=1

54 49635-80 [ACK] Seq=1 Ack=1 Win=64240 Len=0

1514 [TCP segment of a reassembled PDU]

1514 [TCP segment of a reassembled PDU]

54 49635-80 [ACK] Seq=463 Ack=2921 Win=64240 Len=0

1514 [TCP segment of a reassembled PDU]

1514 [TCP segment of a reassembled PDU]

54 49635-80 [ACK] Seq=463 Ack=7301 Win=64240 Len=0

1514 [TCP segment of a reassembled PDU]

(568 bits)

Dst: Actionte_b9:eb:02 (00:18:01:b9:eb:02)

1./, Dst: 192.168.1.1 (192.168.1.1)

rt: 53 (53)

Frame 2: 71 bytes on wire (568 bits)

Ethernet II, Src: Vmware_db:16:53:00, Dst: 08:00:00:08:00:08

Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.1

User Datagram Protocol, Src Port: 5056, Dst Port: 5000

Domain Name System (query)

Response in: 31

Transaction ID: 0xb8b8

Flags: 0x0100 Standard query 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 08 00 45 00

0010 00 39 16 d2 00 00 80 11 00 00 c0 a8 01 07 c0 a8

0020 01 01 c2 ff 00 35 00 25 83 8f be b8 01 00 00 01

0030 00 00 00 00 00 03 77 77 03 6d 73 6e 03 63

0040 ff 6d 00 00 01 00 01

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 A-B	Bytes A-B	Rel Start	Duration	bps A-B	bps A-B
IntelCor_5eddf7c	IPv6mcast_0c	4	832	4	832	0	0	0.000000000	10.0024	665.44	N/A
Vmware_dbf671	Actionte_b9eb02	257	138 661	119	22 178	138	116 483	0.957053000	7.7711	22831.24	119913.93
ArrisGro_54d07b5	Broadcast	2	1 695	2	1 695	0	0	1.010498000	0.0022	6116373.48	N/A
ArrisGro_dff5fef	Broadcast	1	60	1	60	0	0	1.013691000	0.0000	N/A	N/A
HtcCorpo_b7d03a	Broadcast	1	60	1	60	0	0	2.236160000	0.0000	N/A	N/A
ArrisGro_4696d2	Broadcast	1	60	1	60	0	0	4.990550000	0.0000	N/A	N/A

☒ Name resolution ☐ Limit to display filter

Help Copy Graph A-B Close

0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00J..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 03 6d 73 6e 03 63www.msn.com.....
0040 8f 6d 00 00 01 00 01om.....

Frame (frame), 71 bytes Packets: 266 - Displayed: 266 (100.0%) - Load time: 0.00.056 Profile: Default

This view does not make much sense



③ Click here

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_5eddf7c	IPv6mcast_0c	4	832	4	832	0	0	0.000000000	10.0024	665.44	N/A
Vmware_dbf671	Actionte_b9eb02	257	138 661	119	22 178	138	116 483	0.957053000	7.7711	22831.24	119913.93
ArrisGro_54d07b5	Broadcast	2	1 695	2	1 695	0	0	1.010498000	0.0022	6116373.48	N/A
ArrisGro_dff5fef	Broadcast	1	60	1	60	0	0	1.013691000	0.0000	N/A	N/A
HtcCorpo_b7d03a	Broadcast	1	60	1	60	0	0	2.236160000	0.0000	N/A	N/A
ArrisGro_4696d2	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



④ This window shows all conversations

Conversations: CaseStudy1.pcap

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

☒ Name resolution ☐ Limit to display filter

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

One row, one conversation



How can we find out details for this conversation?

CaseStudy1.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9d) from master-1.12.3]

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	SSDP	208	M-SEARCH * HTTP/1.1	
2	0.957053	192.168.1.7	192.168.1.1	DNS	71	Standard query 0xb8b8 A www.msn.com
3	0.983752	192.168.1.1	192.168.1.7	DNS	129	Standard query response 0xb8b8 CNAME us.co1.cb3.glbnds.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	UDP	154	Fragmented IP protocol (protocol 1, offset 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	
8	1.062768	65.55.84.56	192.168.1.7	TCP	62	
9	1.062847	192.168.1.7	65.55.84.56	TCP	54	
10	1.063255	192.168.1.7	65.55.84.56	HTTP	516	
11	1.182590	65.55.84.56	192.168.1.7	TCP	1514	
12	1.183190	65.55.84.56	192.168.1.7	TCP	1514	
13	1.183225	192.168.1.7	65.55.84.56	TCP	54	
14	1.235823	65.55.84.56	192.168.1.7	TCP	1514	
15	1.235830	65.55.84.56	192.168.1.7	TCP	1514	
16	1.235832	65.55.84.56	192.168.1.7	TCP	1514	
17	1.235919	192.168.1.7	65.55.84.56	TCP	54	
18	1.236712	65.55.84.56	192.168.1.7	TCP	1514	

Frame 2: 71 bytes on wire (568 bits), 71 captured (568 bytes) on interface 0
Ethernet II, Src: VMware_d8:f6:71 (00:0c:29:16:00:00), Dst: 02:00:0c:29:16:00:00
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.1
User Datagram Protocol, Src Port: 49919, Dst Port: 80
Domain Name System (Query)
[Response in: 3]
Transaction ID: 0xb8b8
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.msn.com: type A, class IN

Conversations: CaseStudy1.pcap

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

☒ Name resolution ☐ Limit to display filter

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

Conversations: CaseStudy1.pcap

Ethernet: 6 Fibre

① Right click on this

② Select this

③ Select this

④ Select this

Apply as Filter
Prepare Filter
Find Packet
Color Conversation

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

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

Address A	Address B	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	885.0957053000	6.8083	2035.16
65.55.84.56	192.168.1.7	55	50 827	35	47 894	20	2 933.1003867000	6.1139	62668.59
169.254.1.213	192.168.1.7	2	1 695	2	1 695	0	0.1010498000	0.0022	6116373.48
169.254.1.47	192.168.1.7	1	60	1	60	0	0.1013691000	0.0000	N/A
192.168.1.7	207.46.140.46	3	3 809	1	1 388	2	412.1448913000	0.3999	19525.47
65.55.253.27	192.168.1.7	9	2 974	3	904	6	2 070.1460531000	6.7915	1064.86
192.168.1.7	207.46.193.176	6	1 172	5	717	3	455.1463244000	0.1165	49226.76
67.148.147.113	192.168.1.7	9	1 619	4	652	5	767.1484163000	0.2664	25585.68
64.4.21.39	192.168.1.7	6	1 390	2	536	4	854.1500961000	0.4409	9725.76
192.168.1.7	204.245.34.139	13	3 809	6	2 098	7	1 711.1509582000	1.1311	14838.76
65.55.232	192.168.1.7	28	12 380	12	8 562	16	3 818.1963498000	0.8334	82192.08
63.235.36.105	192.168.1.7	9	1 387	4	664	5	723.1574914000	0.2965	17913.87
157.56.51.123	192.168.1.7	19	7 963	9	5 910	10	2 053.2130004000	0.3354	140969.79
75.98.29.8	192.168.1.7	37	22 100	21	19 791	16	2 309.2566532000	0.4933	320986.75
169.254.1.69	169.254.1.255	1	60	1	60	0	0.4990550000	0.0000	N/A
173.194.73.99	192.168.1.7	32	28 933	23	27 000	9	1 933.7804066000	0.9241	16734.23

☒ Name resolution
 ☐ Limit to display filter

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

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

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

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&g=P&optkey=default&cp=default&rf=8d1=340&pi=7317&ps=346 HTTP/1.1 204 No Content

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

This pane has fewer packets, easier to study this conversation

Frame 56: 66 bytes on wire (528 bits)
 Ethernet II, Src: vmware_db:f6:71 (00:0c:29:00:00:00), Dst: 192.168.1.7
 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: 1 IPv6: 1 IPX: 1 AX.25: 1 NCP: 1 RSP: 1 SCTP: 1 Token Ring: 1 UDP: 16 USB: 1 WLAN: 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	885.0957053000	6.8083	2035.16	1039.90	
65.55.84.56	192.168.1.7	55	50 827	35	47 894	20	2 933.1003867000	6.1139	62668.59	3837.79	
169.254.1.213	192.168.1.7	2	1 695	2	1 695	0	0.1010498000	0.0022	6116373.48	N/A	
169.254.1.47	169.254.1.255	1	60	1	60	0	0.1013691000	0.0000	N/A	N/A	
192.168.1.7	207.46.140.46	6	1 388	4	976	2	412.1448913000	0.3999	19525.47	8242.31	
65.55.253.27	192.168.1.7	9	2 974	3	904	6	2 070.1460531000	6.7915	1064.86	2438.34	
192.168.1.7	207.46.193.176	6	1 172	5	717	3	455.1463244000	0.1165	49226.76	31238.74	
67.148.147.113	192.168.1.7	9	1 619	4	652	5	767.1484163000	0.2664	25585.68	23033.12	
64.4.21.39	192.168.1.7	6	1 390	2	536	4	854.1500961000	0.4409	9725.76	15495.89	
192.168.1.7	204.245.34.139	13	3 809	6	2 098	7	1 711.1509582000	1.1311	14838.76	12101.58	
65.55.232	192.168.1.7	28	12 380	12	8 562	16	3 818.1963498000	0.8334	82192.08	36651.41	
63.235.36.105	192.168.1.7	9	1 387	4	664	5	723.1574914000	0.2965	17913.87	19505.61	
157.56.51.123	192.168.1.7	19	7 963	9	5 910	10	2 053.2130004000	0.3354	140969.79	48969.71	
75.98.29.8	192.168.1.7	37	22 100	21	19 791	16	2 309.2566532000	0.4933	320986.75	37449.27	
169.254.1.69	169.254.1.255	1	60	1	60	0	0.4990550000	0.0000	N/A	N/A	
173.194.73.99	192.168.1.7	32	28 933	23	27 000	9	1 933.7804066000	0.9241	23742.45	16734.23	

☒ Name resolution
 ☐ Limit to display filter

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



We can use expressions
to filter out 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: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
57	1.459771	192.168.1.1	192.168.1.7	DNS	127	Standard query response 0x6c60 CNAME udc.udc0.glb dns.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 0xc82 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->49638 [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&xa=&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 al294.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.nsatc.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>...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 00 80 02P.c WI.....
0030 20 00 1d 33 00 00 02 04 05 b4 01 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



① 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
57	1.459771	192.168.1.1	192.168.1.7	DNS	127	Standard query response 0x6c60 CNAME udc.udc0.glb dns.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 0xc82 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&xa=&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 al294.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.nsatc.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)

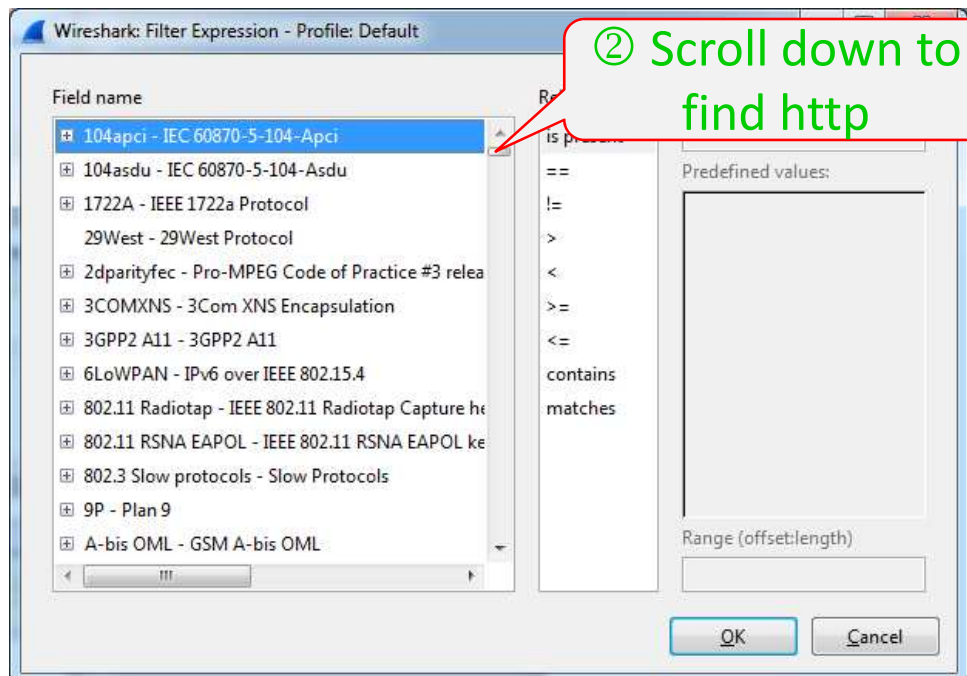
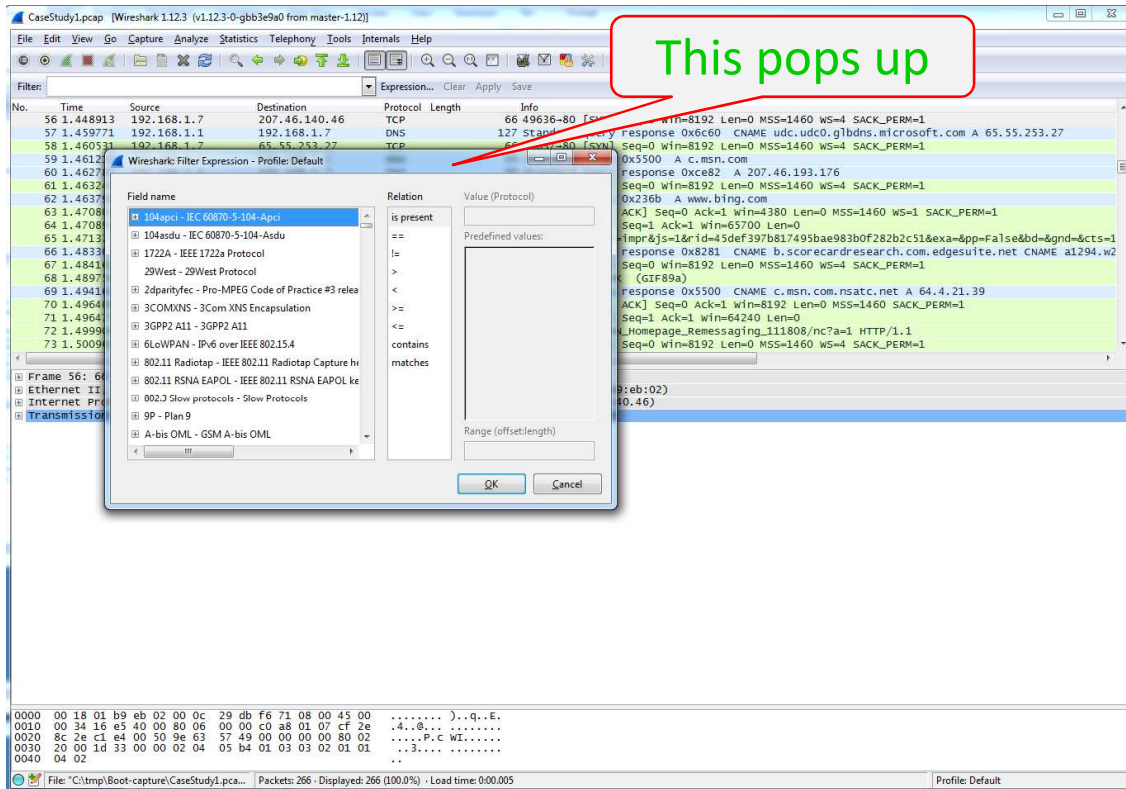
Ethernet II, Src: Vmware_db:f6:71 (00:0c:29:db:f6:71), Dst: Actionte_b9:eb:02 (00:18:01:b9:eb:02)

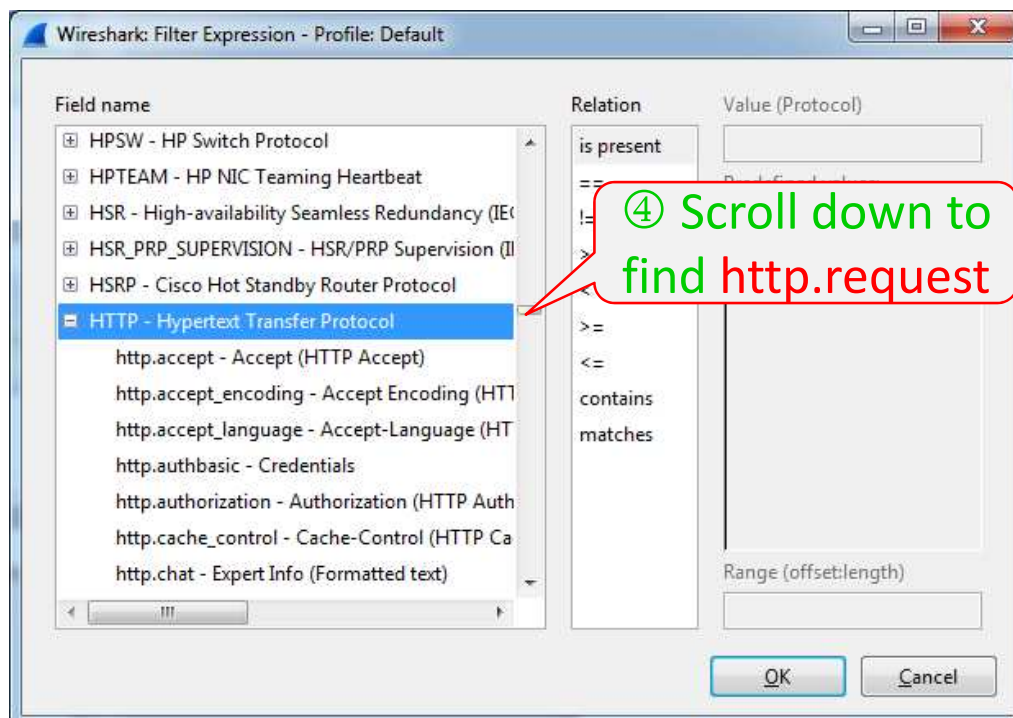
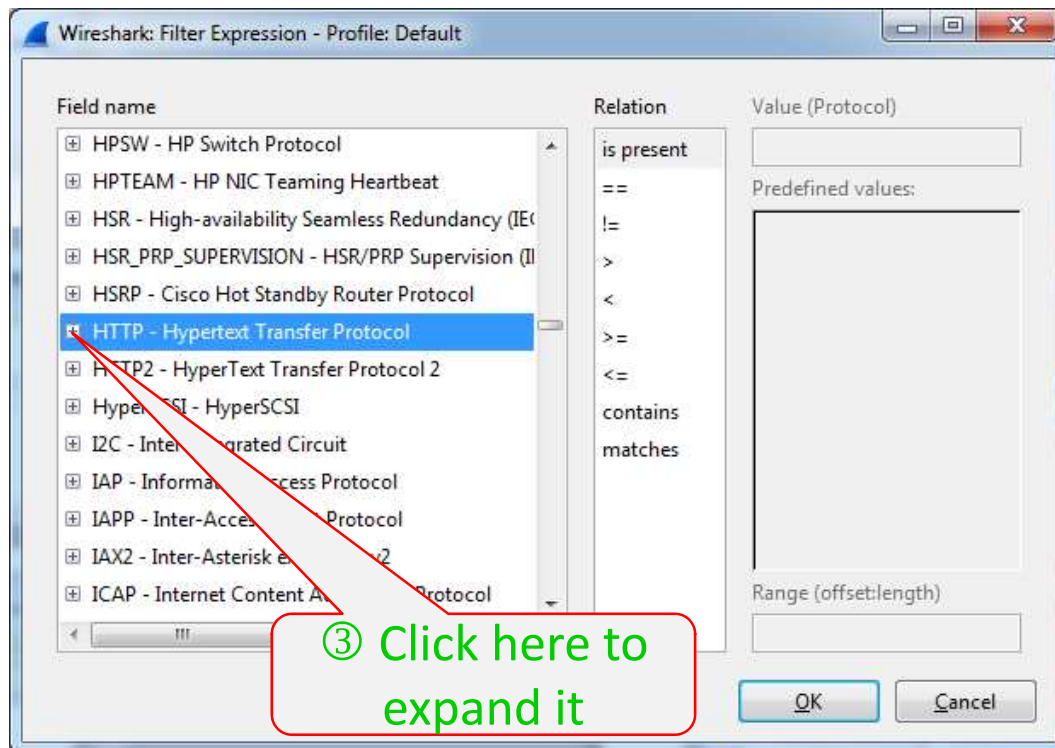
Internet Protocol Version 4, Src: 192.168.1.7 (192.168.1.7), Dst: 207.46.140.46 (207.46.140.46)

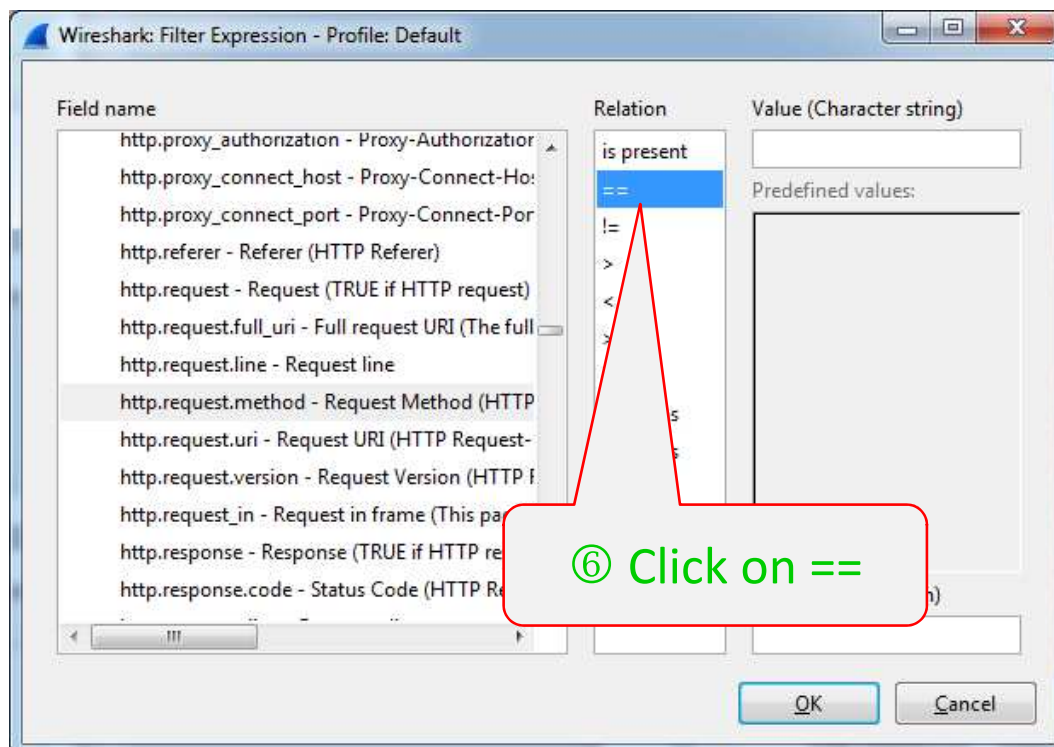
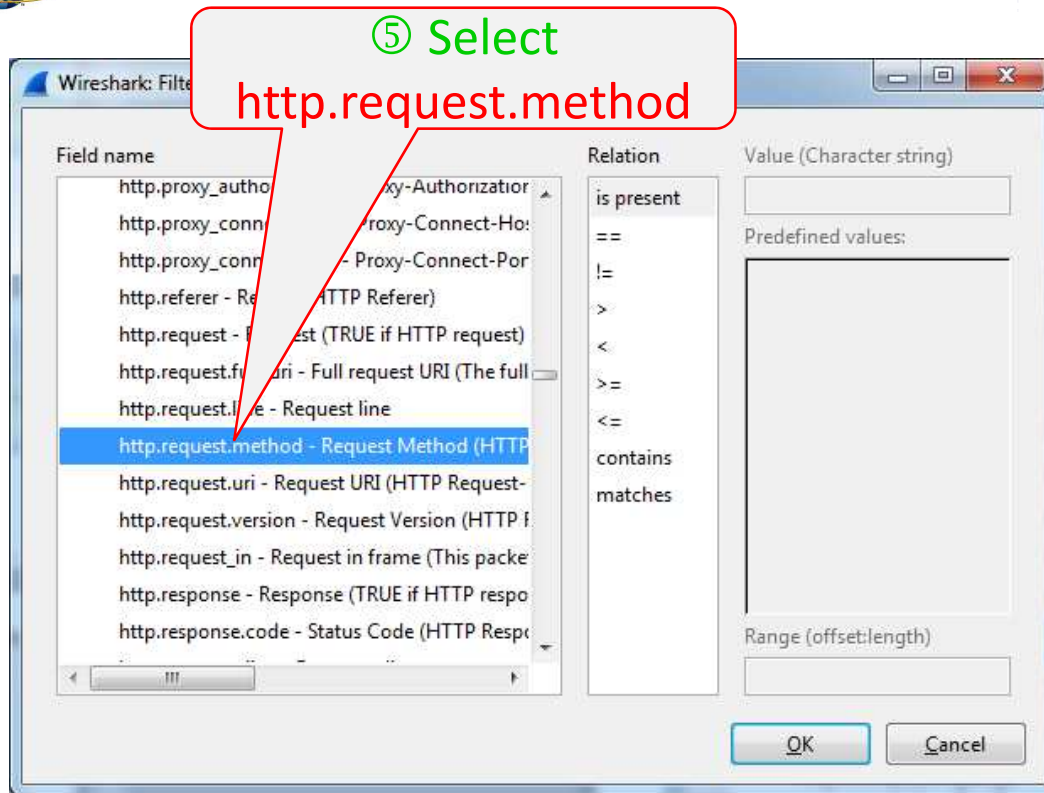
Transmission Control Protocol, Src Port: 49636 (49636), Dst Port: 80 (80), Seq: 0, Len: 0

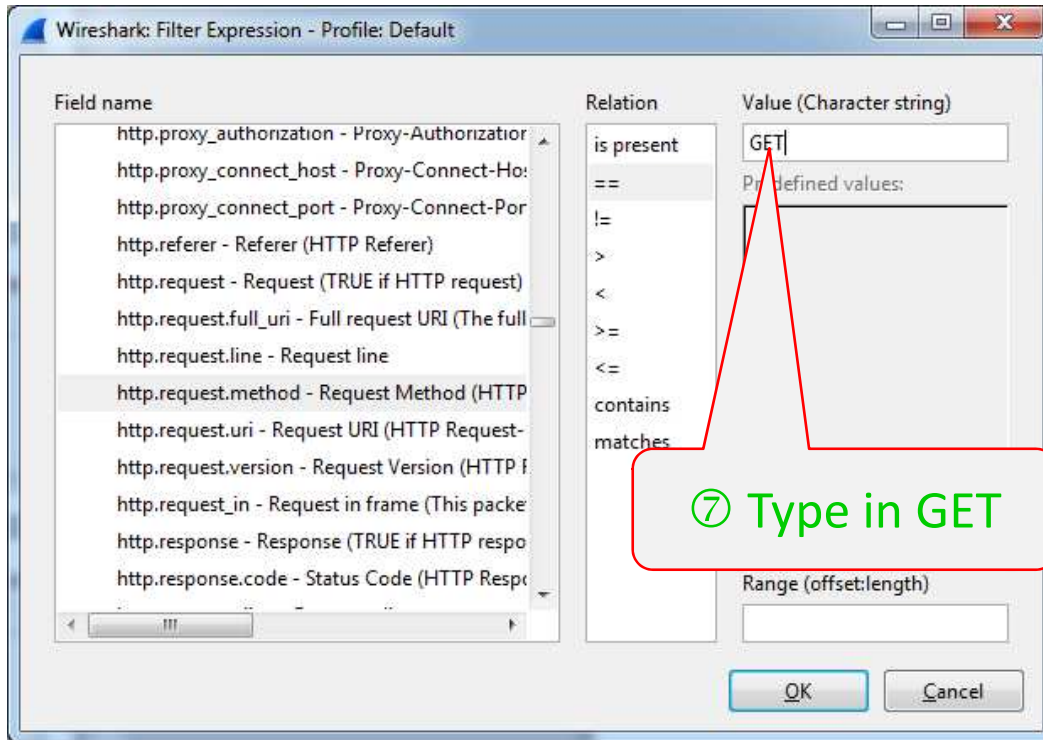
0000 00 18 01 b9 eb 02 00 0c 29 db f6 71 08 00 45 00>...E.
0010 00 34 16 e5 40 00 80 06 00 00 c0 a8 01 07 cf 2e .4..@.....
0020 8c 2e c1 e4 00 50 9e 63 57 49 00 00 00 00 80 02P.c WI.....
0030 20 00 1d 33 00 00 02 04 05 b4 01 03 02 01 01 ..3.....
0040 04 02 ..

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

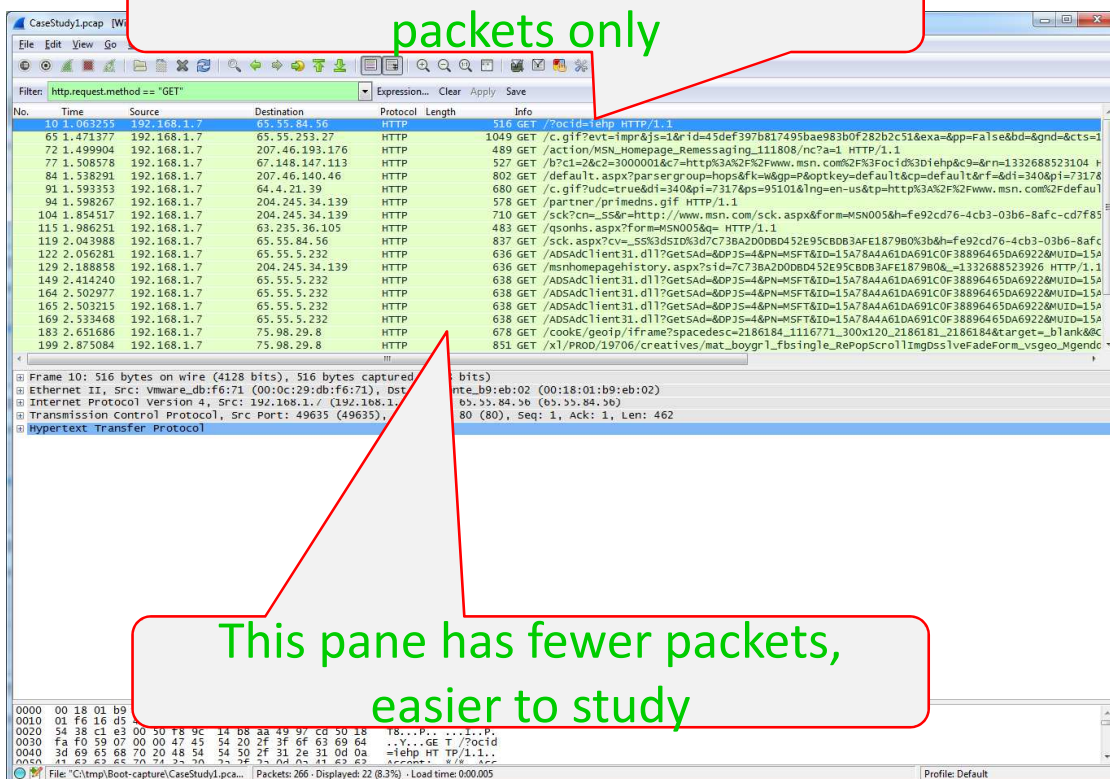




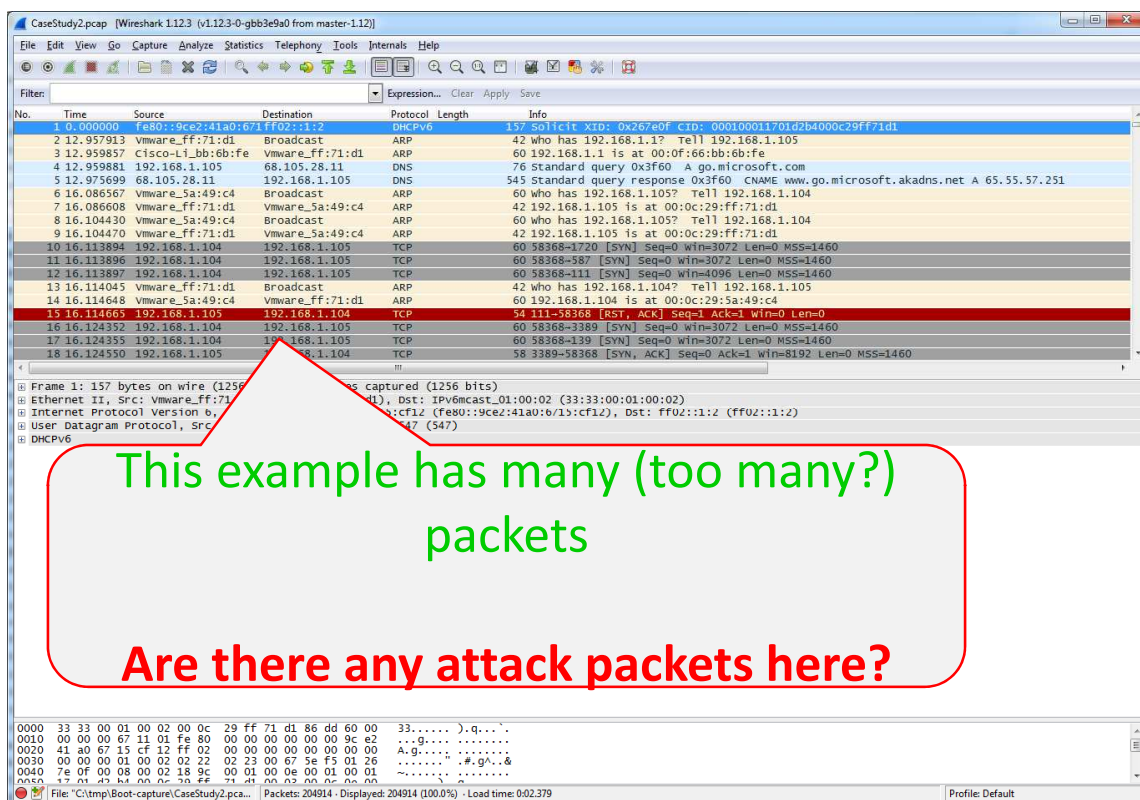
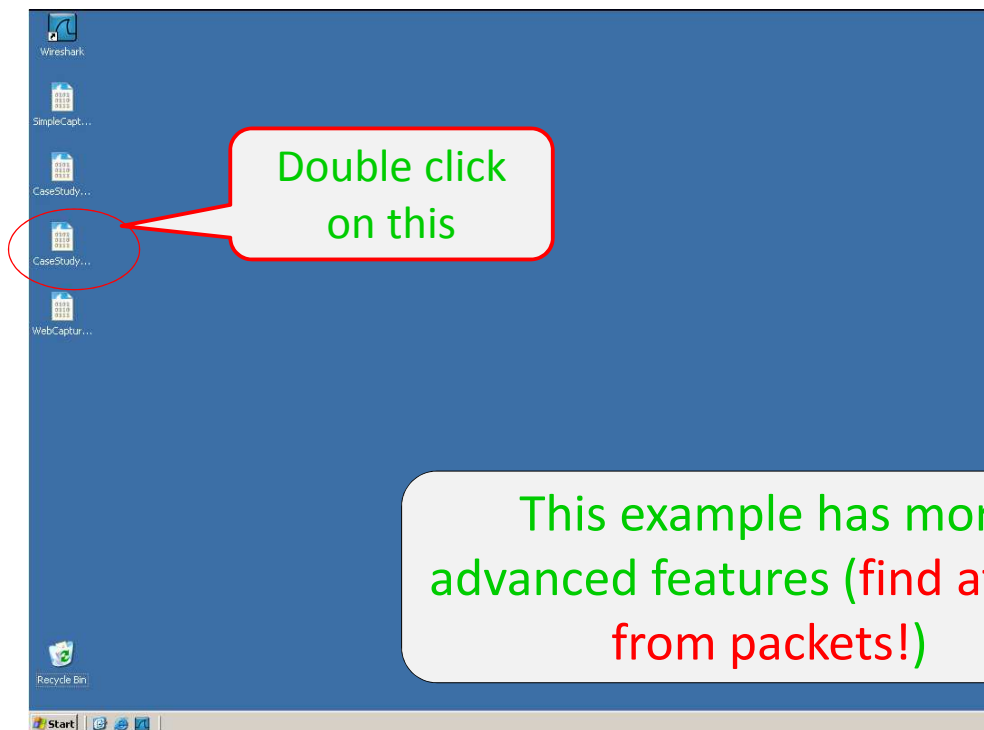




⑧ This window lists HTTP GET packets only



Exercise 2





① Select Statistics

Wireshark 1.12.3 (v1.12.3-0-gbb3e9d0 from master-1.12.1)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter:

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...

Flozz Graph...

HART-IP

HTTP

ONC-RPC Programs

Sametime

TCP StreamGraph

UDP Multicast Streams

WLAN Traffic

IP Statistics

BOOTP-DHCP...

Protocol Length Info

PKT IPv6 157 Solicit XID: 0x267e0f CID: 000100011701d2b4000c29ff771d1

RP 42 who has 192.168.1.1? Tell 192.168.1.105

RP 60 192.168.1.1 is at 00:0f:66:bb:6b:fe

NS 76 Standard query 0x3f60 A go.microsoft.com

NS 543 Standard query response 0x3f60 CNAME www.go.microsoft.akadns.net A 65.55.57.251

RP 60 who has 192.168.1.105? Tell 192.168.1.104

RP 42 192.168.1.105 is at 00:0c:29:ff:71:d1

RP 60 who has 192.168.1.105? Tell 192.168.1.104

RP 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 58368-387 [SYN] Seq=0 win=3072 Len=0 MSS=1460

CP 60 58368-111 [SYN] Seq=0 win=3072 Len=0 MSS=1460

RP 42 who has 192.168.1.104? Tell 192.168.1.105

RP 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

red (1256 bits)

Dst: IPv6mcast_01:00:02 (33:33:00:01:00:02)

cf12 (f80:9ce2:41a0:b13:cf12), Dst: ff02::1:2 (ff02::1:2)

S47 (547)

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 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~.....

0050 17 01 43 b4 00 20 20 ff 71 d1 86 dd 60 00 00~.....

File: C:\tmp\boot-capture\CaseStudy2.pcap... Packets: 204914 - Displayed: 204914 (100.0%) - Load time: 0:02:379 Profile: Default

② Select

③ This pops up

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 %	204914	0.788	0	0	0.000
Ethernet	100.00 %	204914	100.00 %	204914	0.788	0	0	0.000
Internet Protocol Version 6	0.00 %	3	0.00 %	32	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	0	0	0.000
Domain Name Service	0.00 %	2	0.00 %	17	0.000	0	0	0.000
Address Resolution Protocol	0.01 %	19	0.00 %	10	0.000	0	0	0.000
Internet Protocol Version 4	99.99 %	204892	99.99 %	219581	0.785	0	0	0.000
User Datagram Protocol	0.17 %	342	0.33 %	729	0.000	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	61	26352	0.001
File Transfer Protocol (FTP)	94.40 %	193445	76.30 %	18753478	0.661	18	10257	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	186	0.000
SMB (Server Message Block Protocol)	0.01 %	16	0.01 %	2636	0.000	12	1886	0.000
SMB Pipe Protocol	0.00 %	0	0.00 %	0	0.000	0	0	0.000
Microsoft Windows Lanman Remote API Protocol	0.00 %	0	0.00 %	0	0.000	0	0	0.000
FTP Data	0.00 %	0	0.00 %	0	0.000	0	0	0.000

Help

94%?

This is suspicious

How to further investigate?



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
1	0.000000	00:00:00:00:00:00	00:00:00:00:00:00	DHCPv6	157	Solicit XID: 0x267e0f CID: 00010001701d2b4000c29ff71d1
2	12.957913	00:00:00:00:00:00	ff:ff:71:d1	ARP	42	who has 192.168.1.1? Tell 192.168.1.105
3	12.959881	00:00:00:00:00:00	bb:6b:fe	VMware FF	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 FF	192.168.1.105	ARP	60	who has 192.168.1.105? Tell 192.168.1.104
7	16.086608	VMware FF	192.168.1.105	ARP	42	192.168.1.105 is at 00:0c:29:ff:71:d1
8	16.104430	VMware FF	192.168.1.105	ARP	60	who has 192.168.1.105? Tell 192.168.1.104
9	16.104470	VMware FF	192.168.1.105	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	192.168.1.105	ARP	42	who has 192.168.1.104? Tell 192.168.1.105
14	16.114648	VMware FF	192.168.1.105	ARP	60	192.168.1.104 is at 00:0c:29:5a:49:c4
15	16.114655	192.168.1.105	192.168.1.104	TCP	60	58368-3389 [SYN] Seq=0 win=3072 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	58368-130 [SYN] Seq=0 win=3072 Len=0 MSS=1460
18	16.124350	192.168.1.104	192.168.1.105	TCP	60	58368-130 [SYN] Seq=0 win=3072 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: VMware FF:71:d1 (00:0c:29:ff:71:d1)
Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.104
User Datagram Protocol, Src Port: 58368, Dst Port: 58368
DHCPv6

File: C:\tmp\Boot-capture\CaseStudy2.pcap... Packets: 204914 - Displayed: 42 (0.0%) - Load time: 0.02379 Profile: Default

④ We need to reduce the # of packets. Type this



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

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 FF:71:d1 (00:0c:29:ff:71:d1)
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)
File Transfer Protocol (FTP)

File: C:\tmp\Boot-capture\CaseStudy2.pcap... Packets: 204914 - Displayed: 19345 (9.4%) - Load time: 0.02500 Profile: Default

⑤ This pane has fewer packets but how to proceed?

CaseStudy2.pcap (v1.23.0-gbb3e9a9 from master-112.3)

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 bits) on interface 0

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

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ...J21... .q...e.

0010 00 4f 11 00 40 00 80 06 00 00 c0 a8 01 09 c0 a8 ...O.8...

0020 00 68 00 15 00 02 00 94 c0 e0 3b ac 73 c0 81 88 ...h...

0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 08 ...c...

0040 0f 50 32 32 30 20 40 69 63 72 6f 73 6f 66 74 20 ...[220 M]icrosoft

0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Frame (frame), 93 bytes

Packets: 240914 - Displayed: 193445 (94.4%) - Load time 0:02:500

Profile: Default

CaseStudy2.pcap [v12.123-0-gbb3e9a0 from master-112]

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 3444: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on 0
 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: 65560]
 [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 n
 Response arg: Microsoft FTP Service

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71
 0010 00 4f 11 61 40 00 80 06 00 c0 c0
 0020 01 68 00 01 1d b3 5a 32 32 3b 3b
 0030 01 04 84 63 00 00 01 01 08 0a 0a
 0040 6f 5b 32 32 30 20 4d 69 63 72 6f
 0050 46 54 50 20 53 73 72 69 63 65 04 03

File: C:\temp\Boot-capture\CaseStudy2.pcap... Packets: 204914 (94.4%) - Load time: 0:02:500 Profile: Default

Wireshark 2.12.3 (v1.123.0-gbb3e9a0 from master-1.123)

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: `ftp && tcp.dstport == 48562` 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

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

Frame 3444: 93 bytes on wire (744 bits) captured (11760 bits) on 0
 Ethernet II, Src: VMware FF:71:D1:00:00:00, Dst: 08:00:00:00:00:00
 Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.104
 Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (48562)
 [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: 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

0000 00 0c 29 5a 49 c4 00 0c 29 ff 71 d1 08 00 45 00 ...Z... .Q...E.
 0010 00 4f 11 61 40 00 80 01 00 00 c0 a8 01 69 c0 a8 ...0.a8... ..
 0020 01 68 00 15 bd b3 5e a3 32 2d 3b 2a ac 93 80 18 ...h...A...Z...
 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 7a 20 o[220 Microsoft
 0050 6f 64 0c 70 12 65 7f 74 69 63 65 0d 00 00 00 00 ...f... ..

File: C:\tmp\Boot-capture-CaseStudy2.pcap... Packets: 204914 - Displayed: 193445 (94.4%) - Load time: 0:02:500

Profile: Default

CaseStudy2.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e90 from master-112)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ftp && tcp.dstport == 48562 | tcp.srcport == 48562 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
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.
3539	52.757139	192.168.1.104	192.168.1.105	FTP	77	Request: PASS john
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	52.798573	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.
3832	52.81379	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	77	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:d1:00:00:29, Dst: VMware, 08:00:00:08:00:20, Len: 74
 Internet Protocol Version 4, Src: 192.168.1.105, Dst: 192.168.1.104
 Transmission Control Protocol, Src Port: 21 (21), Dst Port: 48562 (48562)
 Source Port: 21 (21)
 Destination Port: 48562 (48562)
 [Stream index: 1127]
 [TCP segment Len: 27]
 Sequence number: 1 (relative sequence number)
 [Next sequence number: 28 (relative sequence number)]
 Acknowledgment number: 1 (relative ack number)
 Window 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
 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 01 6f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8
 0020 01 68 00 13 bd 60 e0 eb ed 3b ac 23 cb 80 18
 0030 01 04 84 63 00 00 01 01 08 04 00 3b ac a6 00 00
 0040 6f 5b 32 32 30 20 4d 69 63 72 6f 73 6f 66 74 20
 0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

File: C:\temp\Boot-capture\CaseStudy2.pcap... Packets: 240914 · Displayed: 5387 (2.6%) · Load time: 0:02:591

Profile: Default



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

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

ftp && ftp.response.arg ==
"User logged in."

10 Let's type in to check whether it succeeded

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_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: 1137, 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)
[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 ...J2I...).q...E.
0010 00 4f 11 60 40 00 80 06 00 00 c0 a8 01 69 c0 a8 ...I 08... ..I..
0020 01 68 00 15 bd b2 e0 9e eb ed 3b ac 23 cb 80 18 ...h...u...+...
0030 01 04 84 63 00 00 01 01 08 0a 00 04 cb a6 00 0b ...;... ..+...
0040 6f 5b 32 30 20 4d 69 63 72 6f 73 6f 66 74 20 ...[220 MI crosoft ...
0050 46 54 60 70 52 65 72 76 60 62 65 0d 02 ...FTP Serv ice ..
Packets: 204914 - Displayed: 5387 (2.6%) - Load time: 0:02:591



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

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

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) on interface 0
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.

The attack indeed succeeded!

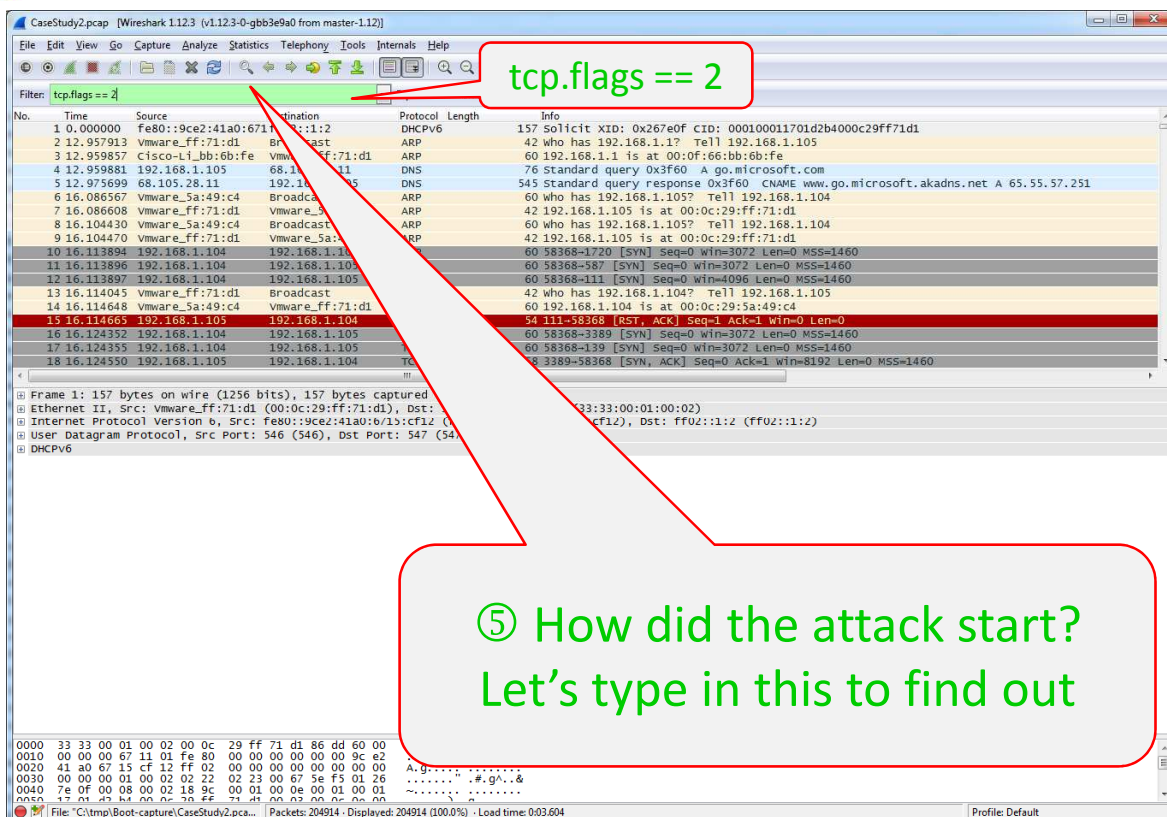
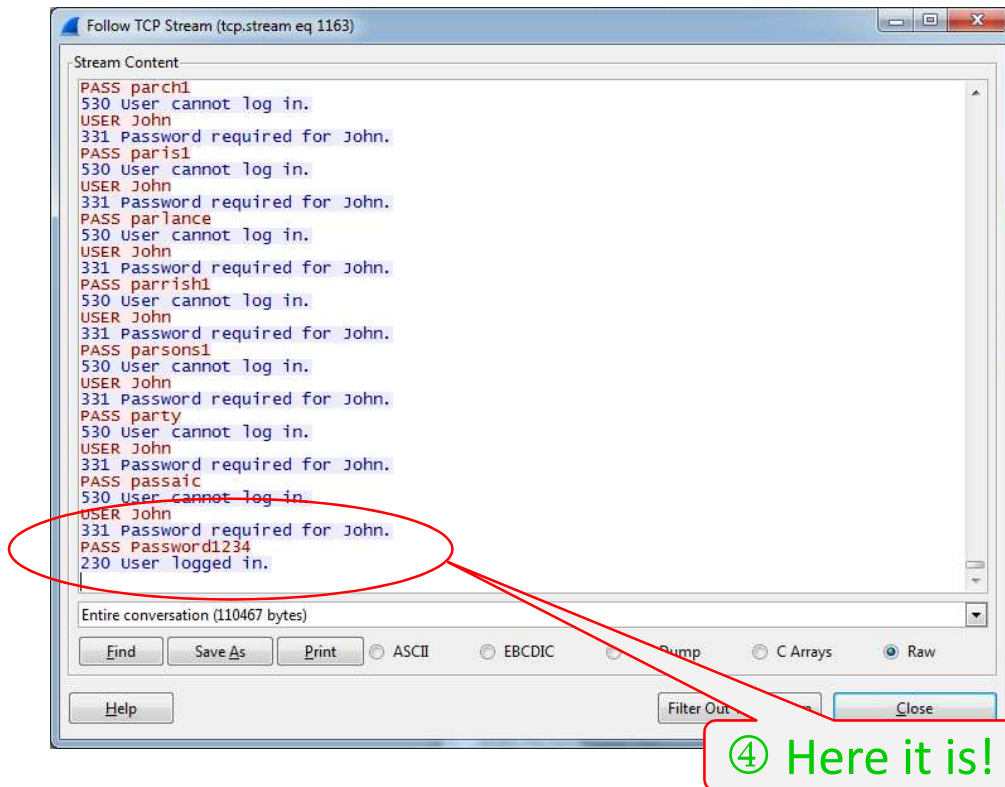


① Select Statistics

The screenshot shows the Wireshark interface with the 'Statistics' menu open. The 'Follow TCP Stream' option is highlighted. A red arrow points to this option with the label '② Select'. The main packet list shows a packet from 192.168.1.105 to 192.168.1.104, and the packet details pane shows the corresponding TCP and FTP data.



The screenshot shows the 'Follow TCP Stream' window in Wireshark. The 'Entire conversation (110467 bytes)' is selected. The 'Raw' button is highlighted. A red arrow points to this button with the label '③ Scroll down to the bottom'. The main packet list shows a packet from 192.168.1.105 to 192.168.1.104, and the packet details pane shows the corresponding TCP and FTP data.





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 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 ...!.....
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)
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: 21 (21), 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 ...).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 ...!.....
0030 04 00 1a 6d 00 00 15 81 a0 8f e1 00 00 00 00 60 02 ...!.....
...

File: "C:\tmp\Boot-capture\CaseStudy2.pca..." Packets: 204914 - Displayed: 1452 (0.7%) - Load time: 0:02:535 Profile: Default

⑥ Select packet 33;

RIGHT click on it



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	58368-258 [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	58368-3206 [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	58368-143 [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)
58368 (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 02f.....
0030 04 00 1a 6d 00 00 02 04 05 b4 00 00 00 00 00m.....

File: "C:\tmp\boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 1452 (0.7%) · Load time: 0:02:535 Profile: Default

⑦ Select



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

Filter: tcp.stream eq 12

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

Filter Out This Stream Close

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

File: "C:\tmp\boot-capture\CaseStudy2.pca..." Packets: 204914 · Displayed: 3 (0.0%) · Load time: 0:02:340 Profile: Default

⑧ Click

⑨ There are only three packets in this pane.
The attack started with port scanning

Summary

- 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



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.

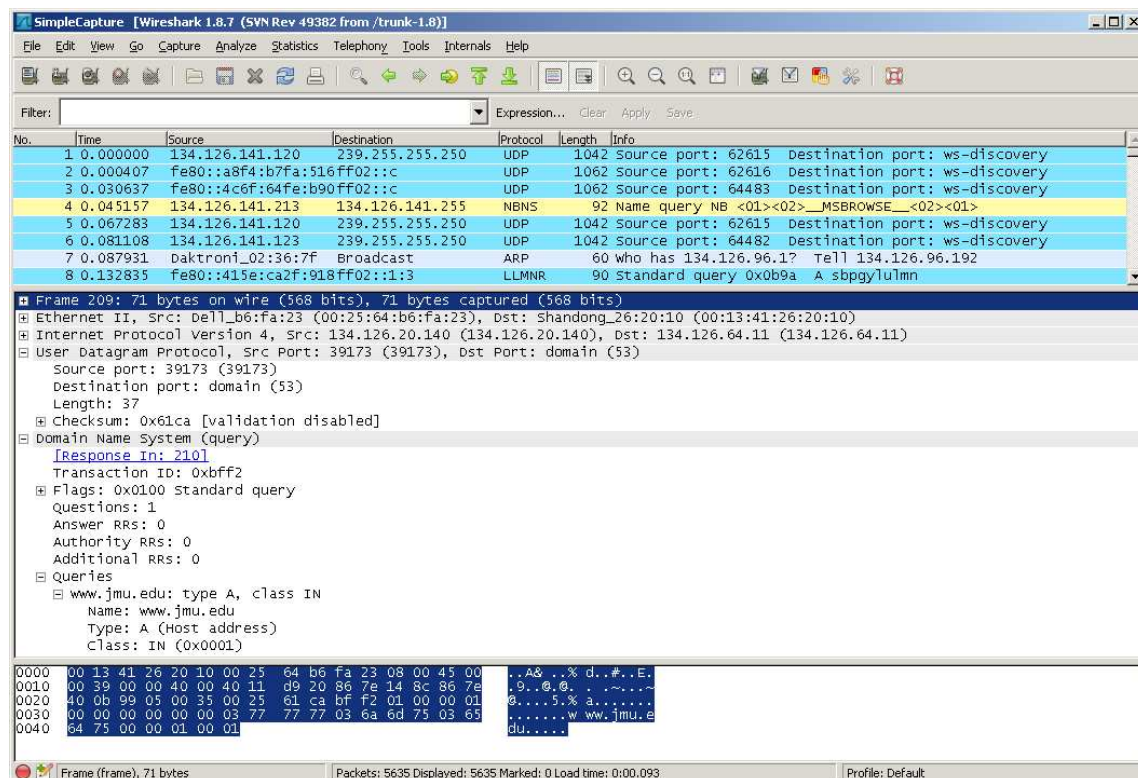
Exercise 1 –Using Wireshark to analyze basic network traffic

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.

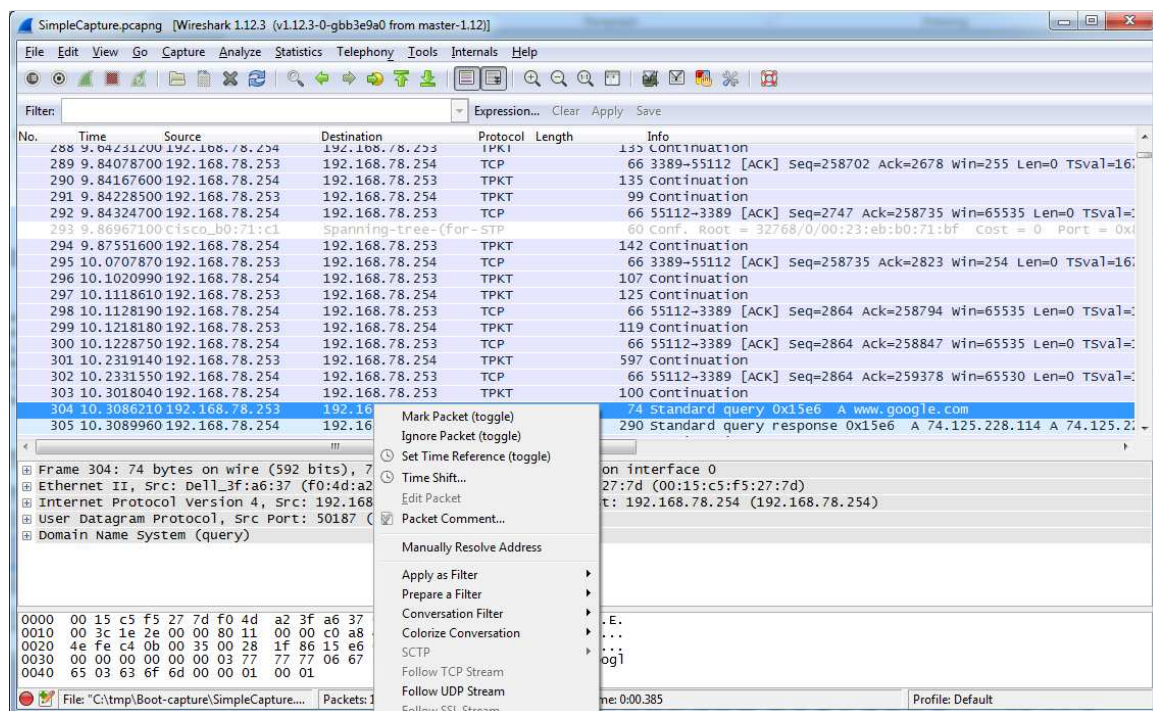
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	134.126.141.120	239.255.255.250	UDP	1042	Source port: 62615 Destination port: ws-discovery
2	0.000407	fe80::a8f4:b7fa:516ff02::c		UDP	1062	Source port: 62616 Destination port: ws-discovery
3	0.030637	fe80::4c6f:64fe:b90ff02::c		UDP	1062	Source 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)

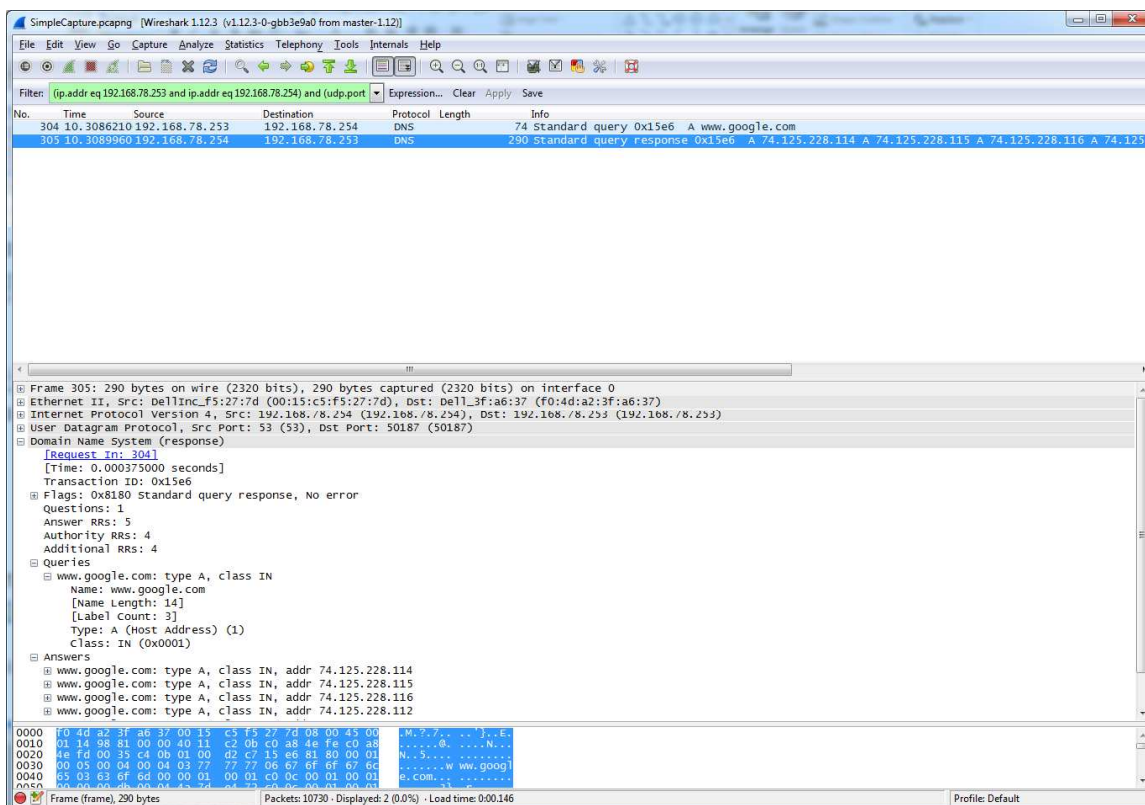
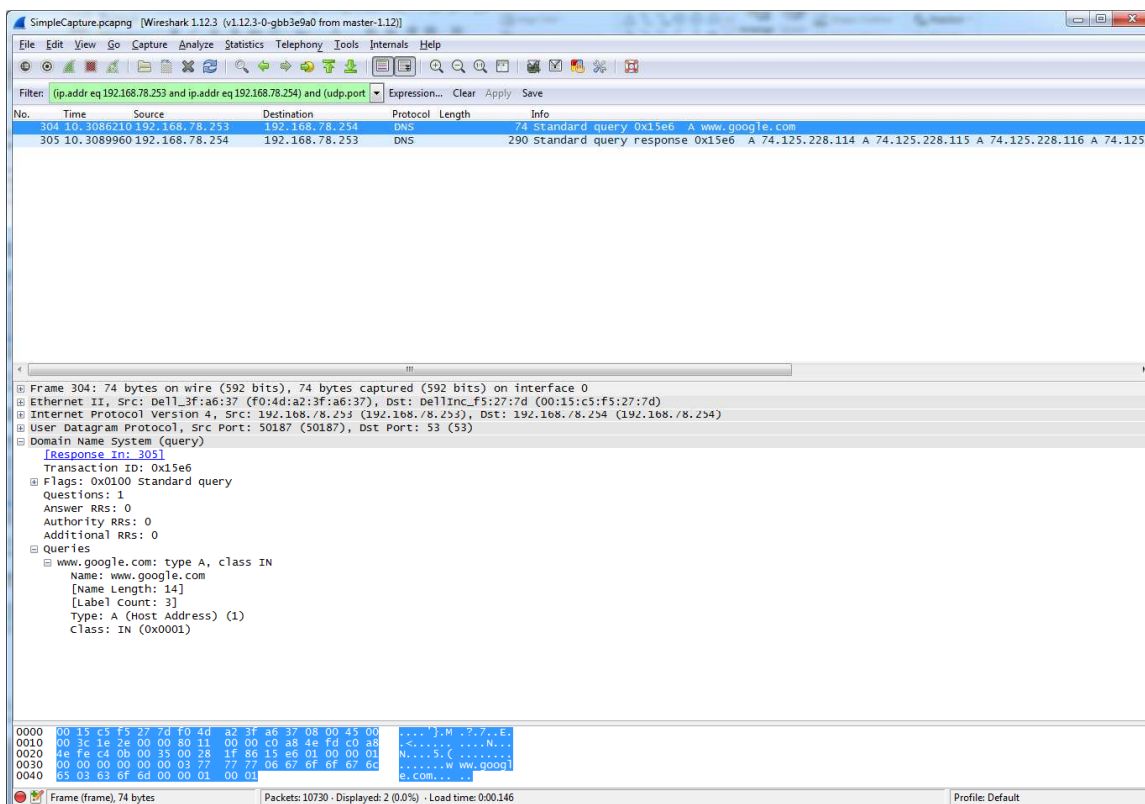
- Ethernet II, Src: Dell_b6:fa:23 (00:25:64:b6:fa:23), Dst: Shandong_26:20:10 (00:13:41:26:20:10)
- Internet Protocol Version 4, Src: 134.126.20.140 (134.126.20.140), Dst: 134.126.64.11 (134.126.64.11)
- User Datagram Protocol, Src Port: 39173 (39173), Dst Port: domain (53)
 - Source port: 39173 (39173)
 - 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.....

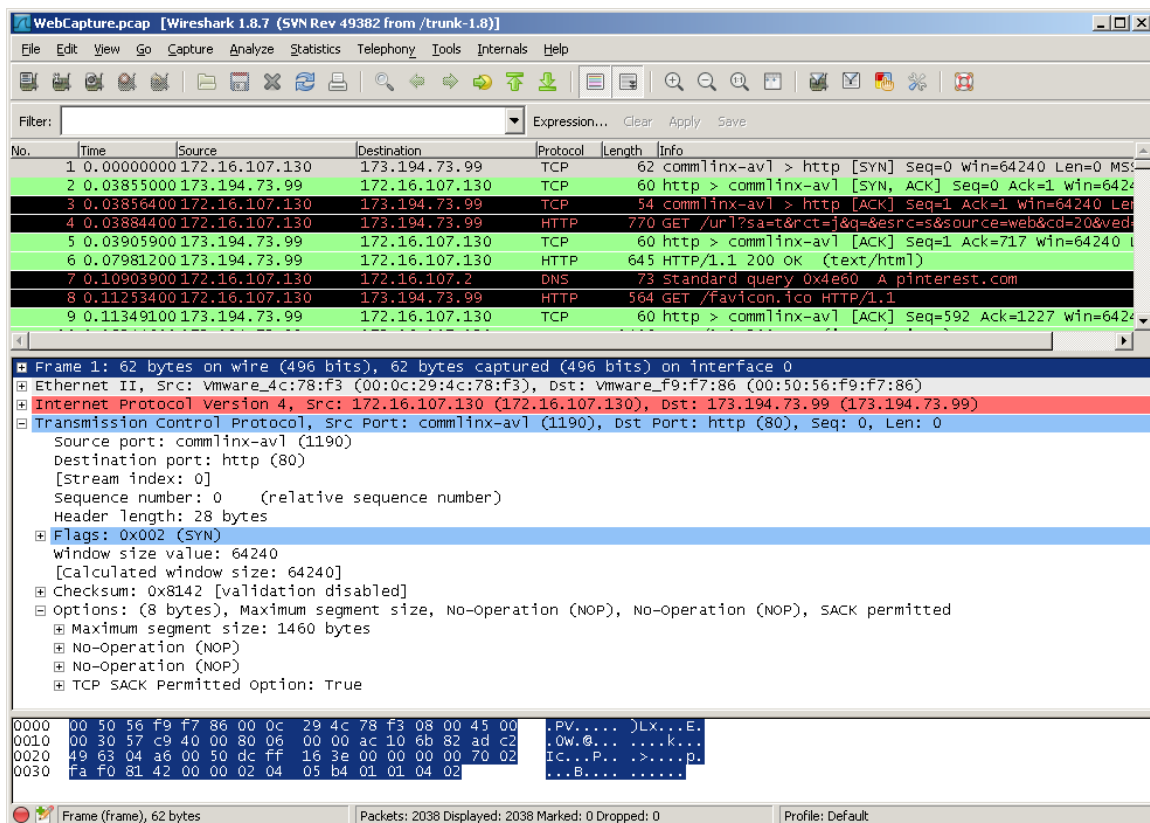
We will begin by examining the sequence of events that take place when a user performs a DNS query. DNS stands for *Domain Name Services*. DNS takes a common fully qualified domain name and translates it to a corresponding Internet address. The sequences of events that take place are first a request 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.



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**.



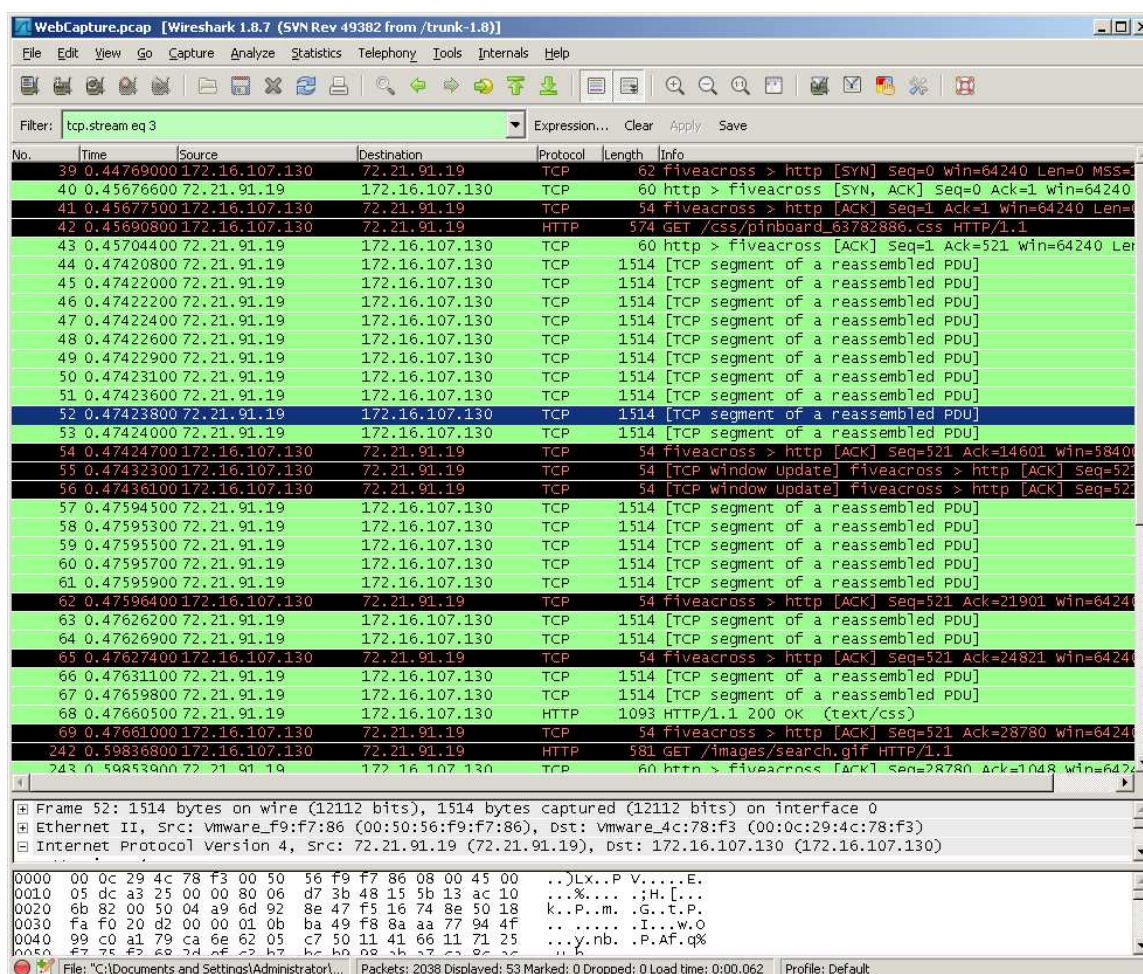
This is a capture of a simple web search. The user has opened up the Google search engine and ran a search for “cute puppy pictures”. The user then chose the Pinterest webpage, selected and downloaded a picture.

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.



WebCapture.pcap [Wireshark 1.8.7 (SVN Rev 49382 from /trunk-1.8)]

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

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%

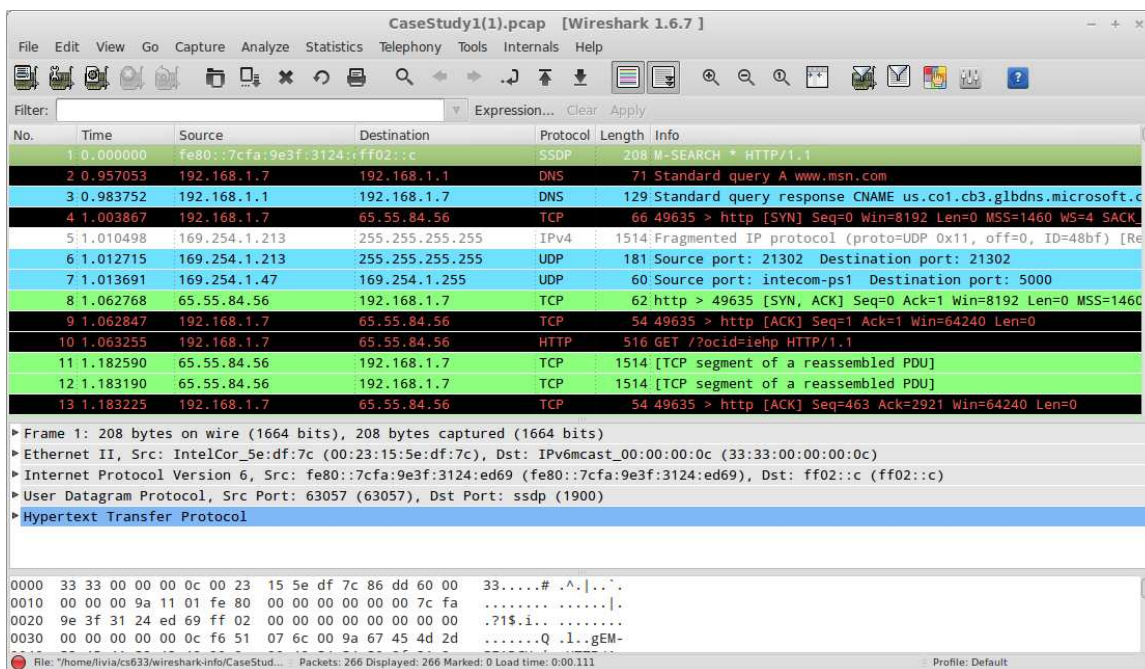
File: "C:\Documents and Settings\Administrator\..." Packets: 2038 Displayed: 53 Marked: 0 Dropped: 0 Load time: 0:00.062 Profile: Default

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.

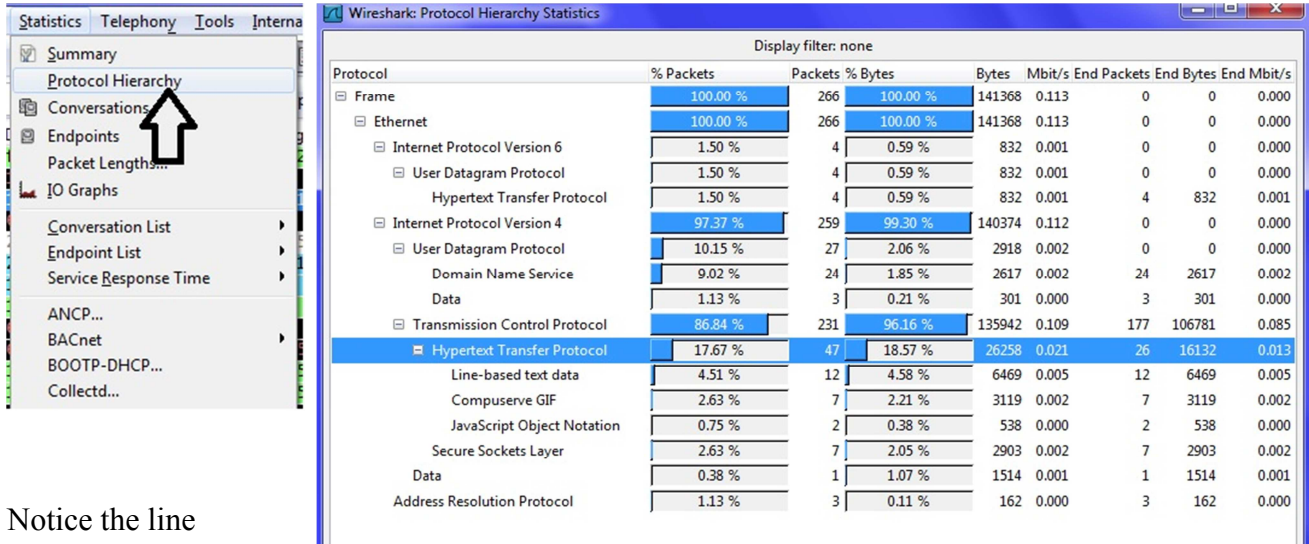
Exercise 2 - Gathering General Information and Statistics and More Wireshark Analysis

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

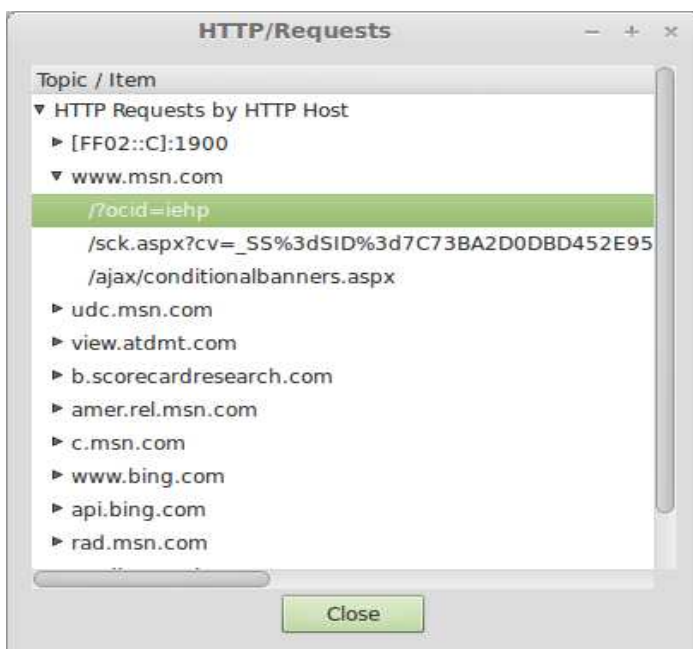
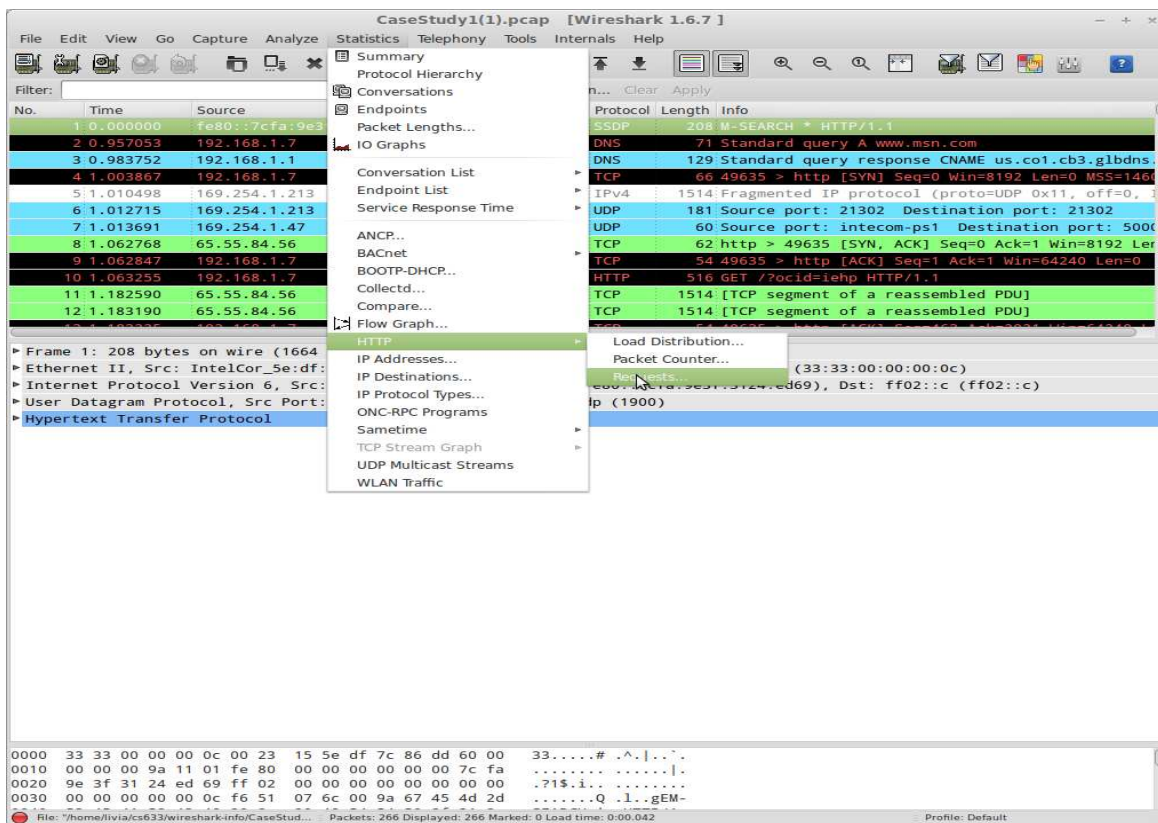


Notice the line highlighted above.

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*



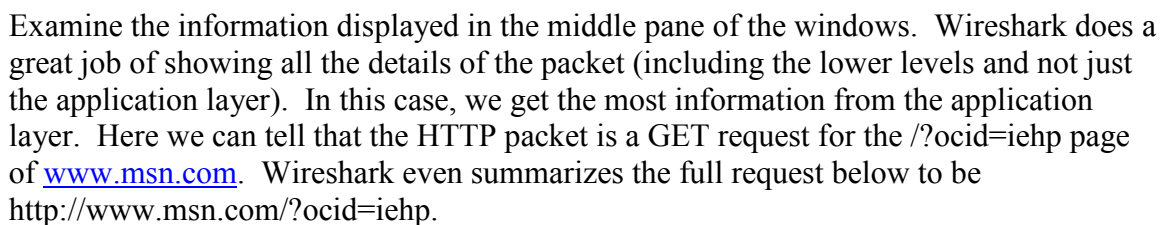
(The above figure might be obsolete and what you see might be a little bit different)

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.



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

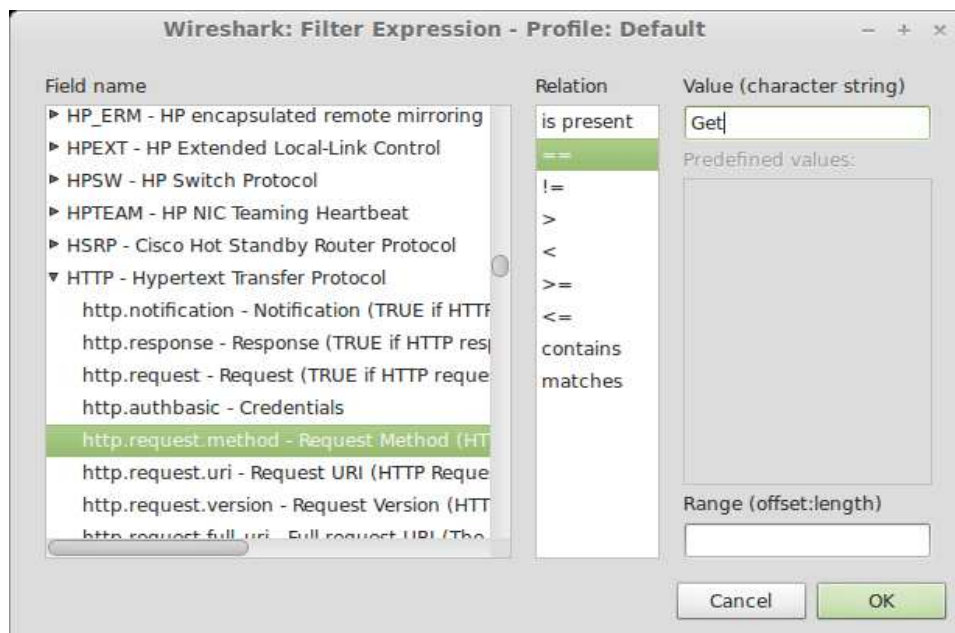
Field name	Relation	Value (protocol)
▶ Expert - Expert Info	is present	
▶ 104apci - IEC 60870-5-104-Apci	==	
▶ 104asdu - IEC 60870-5-104-Asdu	!=	
▶ 2dparityfec - Pro-MPEG Code of Practice #3 n	>	
▶ 3COMXNS - 3Com XNS Encapsulation	<	
▶ 3GPP2 A11 - 3GPP2 A11	>=	
▶ 6LoWPAN - IPv6 over IEEE 802.15.4	<=	
▶ 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:

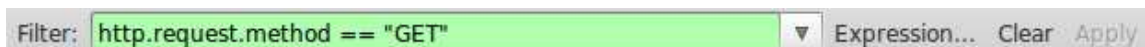
Range (offset:length)

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

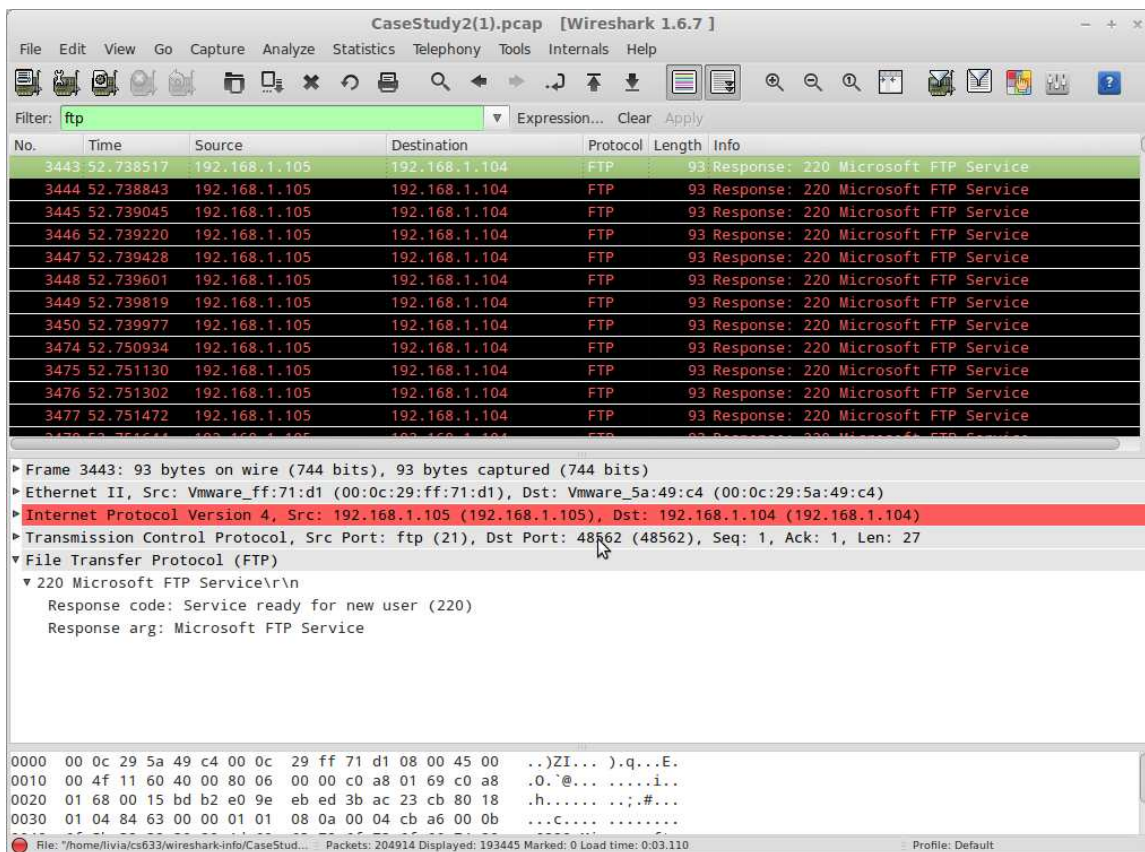
Help Close

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]

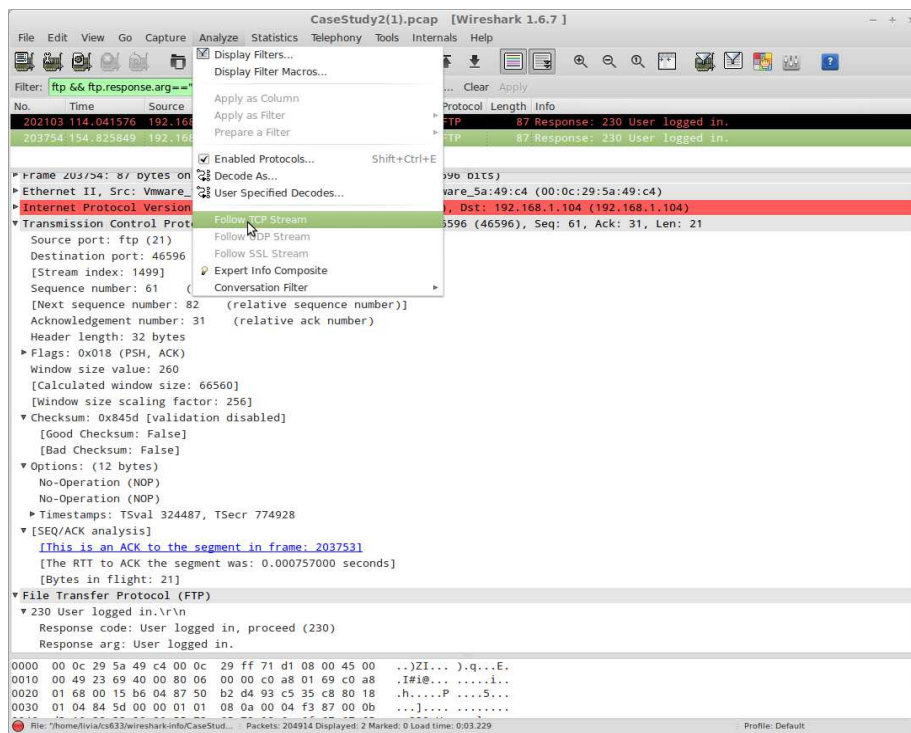
▼ File Transfer Protocol (FTP)

▼ 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

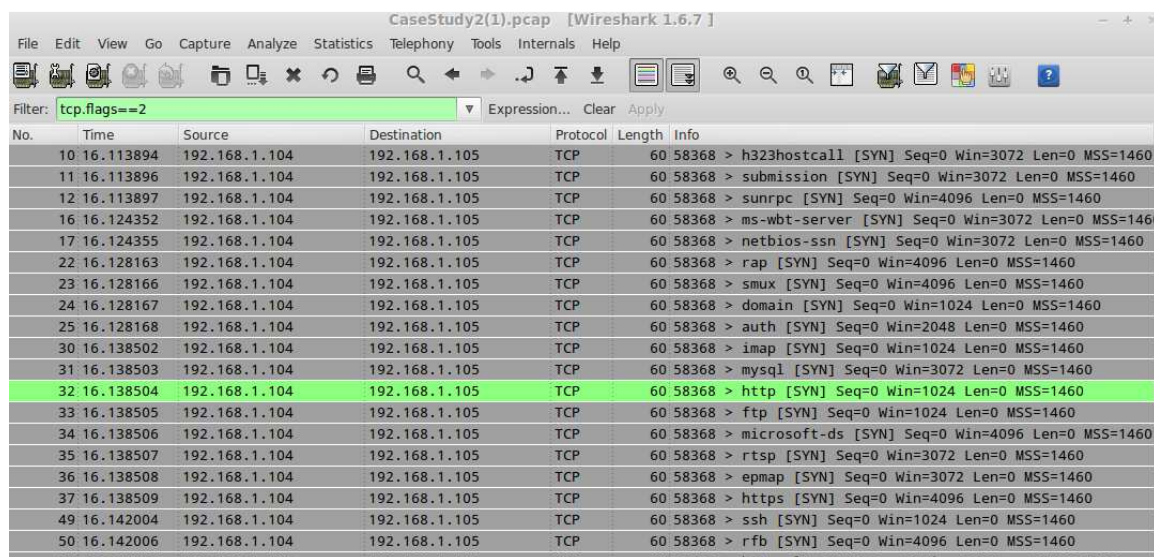
URG = 32

ECE = 64

CWR = 129

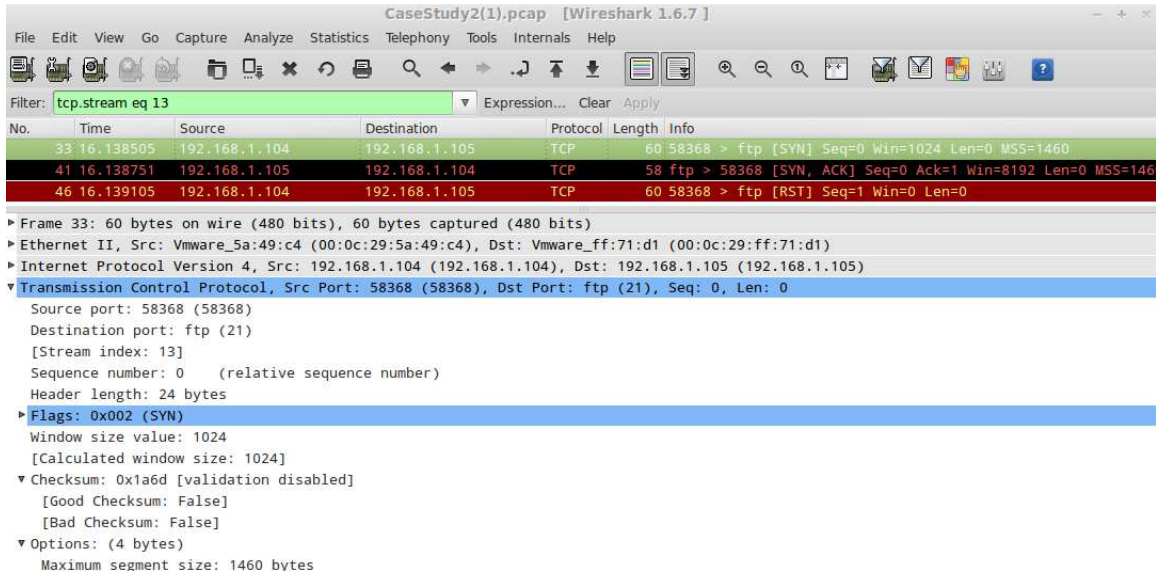
To check if a SYN/ACK flag is set we add 2 (the SYN value) to 16 (the ACK value) and the result would be 18. A common port scan is a SYN scan, We will first check for that using the following filter:

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.



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>