

Part one

Question #1. Capture and count the number of tcp packets that are NOT to or from host helios. 60

The screenshot shows the Wireshark interface with the file 'dump2_new.pcap' open. The packet list on the left shows a range of packets from 238 to 297. The details pane on the right shows the 'File' and 'Time' sections. The 'File' section indicates the file is 'C:\Users\Neil\Downloads\dump2_new.pcap' with a length of 60 KB. The 'Time' section shows the first packet at 2007-11-07 12:22:48 and the last packet at 2007-11-07 12:22:50. The 'Statistics' section shows a table with columns for Measurement, Captured, Displayed, and Marked. The table shows 300 packets captured, 60 displayed (20.0%), and 2.306 seconds time span.

Measurement	Captured	Displayed	Marked
Packets	300	60 (20.0%)	—
Time span, s	2.306	2.265	—
Average pps	130.1	26.5	—
Average packet size, B	186	448	—
Bytes	55902	26908 (48.1%)	0
Average bytes/s	24 k	11 k	—

Question #2. Capture and count the number of packets destined for telnet port 23 on any host.

The screenshot shows the Wireshark interface with the file 'dump2_new.pcap' open. The packet list on the left shows a range of packets from 8 to 22. The details pane on the right shows the 'File' and 'Time' sections. The 'File' section indicates the file is 'C:\Users\Neil\Downloads\dump2_new.pcap' with a length of 60 KB. The 'Time' section shows the first packet at 2007-11-07 12:22:48 and the last packet at 2007-11-07 12:22:50. The 'Statistics' section shows a table with columns for Measurement, Captured, Displayed, and Marked. The table shows 300 packets captured, 3 displayed (1.0%), and 2.306 seconds time span.

Measurement	Captured	Displayed	Marked
Packets	300	3 (1.0%)	—
Time span, s	2.306	2.265	—
Average pps	130.1	26.5	—
Average packet size, B	186	448	—
Bytes	55902	26908 (48.1%)	0
Average bytes/s	24 k	11 k	—

Question #3. Capture and count the HTTP packets (tcp port 80) destined for 136.168.246.23. 8 packets using

dump2.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 136.168.246.23

No.	Time	Source	Destination	RSS	Rate	Protocol	Length	Info
176	2007-11-07 12:22:50.084626	64-74-142-151.compu...	136.168.246.23			TCP	1230	80 → 3316 [ACK] Seq=1 Ack=1 Win=49640 Len=1176
178	2007-11-07 12:22:50.085024	64-74-142-151.compu...	136.168.246.23			TCP	1514	80 → 3316 [ACK] Seq=1177 Ack=1 Win=49640 Len=1460
179	2007-11-07 12:22:50.085145	64-74-142-151.compu...	136.168.246.23			TCP	1514	80 → 3316 [ACK] Seq=2637 Ack=1 Win=49640 Len=1460
180	2007-11-07 12:22:50.085246	64-74-142-151.compu...	136.168.246.23			TCP	1230	80 → 3316 [ACK] Seq=4097 Ack=1 Win=49640 Len=1176
181	2007-11-07 12:22:50.085368	64-74-142-151.compu...	136.168.246.23			TCP	1514	80 → 3316 [ACK] Seq=5273 Ack=1 Win=49640 Len=1460
183	2007-11-07 12:22:50.085492	64-74-142-151.compu...	136.168.246.23			TCP	1514	80 → 3316 [ACK] Seq=6733 Ack=1 Win=49640 Len=1460
183	2007-11-07 12:22:50.085593	64-74-142-151.compu...	136.168.246.23			TCP	1230	80 → 3316 [ACK] Seq=8193 Ack=1 Win=49640 Len=1176
184	2007-11-07 12:22:50.085716	64-74-142-151.compu...	136.168.246.23			TCP	1514	80 → 3316 [ACK] Seq=9369 Ack=1 Win=49640 Len=1460

Wireshark: Capture File Properties - dump2.pcap

Details

File

Name: C:\Users\Neil\Downloads\dump2.pcap

Length: 60 kB

Hash (SHA256): dc99623d04ccd8165ee2572d395cc881234946fad3e9d68ac4b977fc934eaea

Hash (SHA1): 47314a29e7394dfe91f8d509571e55ea4847738

Format: Wireshark/tcpdump/... - pcap

Encapsulation: Ethernet

Snapshot length: 65535

Time

First packet: 2007-11-07 12:22:48

Last packet: 2007-11-07 12:22:50

Elapsed: 00:00:02

Capture

Capture file comments

Refresh Save Comments Close Copy To Clipboard

Frame 176: 1230 bytes on wire (9840 bits), 1230 bytes captured (9840 bits) on interface 0
 Ethernet II, Src: Intel_ab:3d:15 (00:04:23:ab:3d:15), Dst: Intel_82:55:08 (00:0c:29:55:08:00), Protocol: TCP (6), Length: 1176, Capture length: 1176
 Internet Protocol Version 4, Src: 64-74-142-151.compute-1.amazonaws.com (64.74.142.151), Dst: 136.168.246.23 (136.168.246.23), Length: 60, Capture length: 60
 Transmission Control Protocol, Src Port: 80, Dst Port: 3316, Seq: 1, Win: 49640, Len: 1176
 Source Port: 80
 Destination Port: 3316
 [Stream index: 13]
 [Conversation completeness: Incomplete (8)]
 [TCP Segment Len: 1176]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1455397899
 [Next Sequence Number: 1177 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 3395620101

Question #4. Capture and count all packets involved to and from LaserPrinters.

dump2_new.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

cups

No.	Time	Source	Destination	RSS	Rate	Protocol	Length	Info
170	2007-11-07 12:22:48.652560	136.168.241.81	136.168.255.255			CUPS	170	ipp://136.168.241.81/printers/HP_LaserJet_4000_Series1 (idle)
143	2007-11-07 12:22:49.652954	136.168.240.113	136.168.255.255			CUPS	143	ipp://host-0-17-f2-d-ed-b6.dhcp.csu.edu:631/printers/CRE07000 (idle)
121	2007-11-07 12:22:49.652992	136.168.241.81	136.168.255.255			CUPS	170	ipp://136.168.241.81/printers/HP_LaserJet_4000_Series2 (idle)
260	2007-11-07 12:22:50.653376	136.168.240.113	136.168.255.255			CUPS	140	ipp://host-0-17-f2-d-ed-b6.dhcp.csu.edu:631/printers/PS4 (idle)
261	2007-11-07 12:22:50.653493	136.168.241.81	136.168.255.255			CUPS	171	ipp://136.168.241.81/printers/HP_LaserJet_4250 [C16F82] (idle)
263	2007-11-07 12:22:50.658396	136.168.247.44	136.168.255.255			CUPS	133	ipp://136.168.247.44:631/printers/AdobePDF8 (idle)
264	2007-11-07 12:22:50.658558	136.168.247.44	136.168.255.255			CUPS	154	ipp://host-0-16-cb-9d-9c-ed.dhcp.csu.edu:631/printers/AdobePDF8 (idle)
265	2007-11-07 12:22:50.658647	136.168.247.44	136.168.255.255			CUPS	156	ipp://136.168.247.44:631/printers/FineArt5 (idle)
266	2007-11-07 12:22:50.658743	136.168.247.44	136.168.255.255			CUPS	177	ipp://host-0-16-cb-9d-9c-ed.dhcp.csu.edu:631/printers/FineArt5 (idle)

Frame 3: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface 0
 Ethernet II, Src: Apple_b8:00:02 (00:0a:95:bc:b0:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff), Protocol: UDP (17), Length: 170, Capture length: 170
 Internet Protocol Version 4, Src: 136.168.241.81 (136.168.241.81), Dst: 136.168.255.255 (136.168.255.255), Length: 60, Capture length: 60
 User Datagram Protocol, Src Port: 4000, Dst Port: 631
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 156
 Identification: 0xd8e4 (55524)
 0000 = Flags: 0x0
 ...0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: UDP (17)
 Header Checksum: 0x9eca [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 136.168.241.81 (136.168.241.81)

Common Unix Printing System (CUPS) Browsing Protocol: Protocol

Packets: 300 - Displayed: 9 (3.0%)

Profile: Default

we'll get packets involved to and from Laser printers which is "9" packets in total

Part 2

Question #1. Capture and count the number of tcp packets that are NOT to or from host helios.

```
(neil@kali)-[/media/sf_shared]
$ tcpdump -r dump2_new.pcap tcp and not host 136.168.201.112
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:48.649525 IP 216.178.38.164.http > 136.168.101.1.55261: Flags [F.], seq 733809938, ack 1409471374, win 8190, length 0
12:22:48.658818 IP 209.85.171.127.http > 136.168.249.173.49424: Flags [S.], seq 2182939035, ack 2547905676, win 5672, options [mss 1430,sackOK,TS val 2096277582 ecr 2126099086,nop,wscale 6], length 0
12:22:48.693977 IP 209.85.171.127.http > 136.168.249.173.49424: Flags [.] , ack 824, win 115, options [nop,nop,TS val 2096277618 ecr 2126099086], length 0
12:22:48.695083 IP 209.85.171.127.http > 136.168.249.173.49424: Flags [P.], seq 1:214, ack 824, win 115, options [nop,nop,TS val 2096277619 ecr 2126099086], length 213: HTTP: HTTP/1.1 200 OK
12:22:48.736141 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [S.], seq 2017317393, ack 3185100515, win 5792, options [mss 1460,nop,nop,TS val 411284397 ecr 1244405387,nop,wscale 0], length 0
12:22:48.805021 IP unknown.yahoo.com.http > vm21.csub.edu.3537: Flags [P.], seq 4186677869:4186678248, ack 679072254, win 65535, length 379: HTTP: HTTP/1.0 200 OK
12:22:48.805043 IP unknown.yahoo.com.http > vm21.csub.edu.3537: Flags [F.], seq 379, ack 1, win 65535, length 0
12:22:48.836387 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [.] , ack 2897, win 11584, options [nop,nop,TS val 411284497 ecr 1244405388], length 0
12:22:48.836416 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [.] , ack 3389, win 14480, options [nop,nop,TS val 411284497 ecr 1244405388], length 0
12:22:48.837224 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [P.], seq 1:363, ack 3389, win 14480, options [nop,nop,TS val 411284498 ecr 1244405388], length 362: HTTP: HTTP/1.1 304 Not Modified
12:22:48.879472 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [F.], seq 363, ack 3390, win 14480, options [nop,nop,TS val 411284536 ecr 1244405388], length 0
12:22:48.969206 IP unknown.yahoo.com.http > vm21.csub.edu.3537: Flags [.] , ack 2, win 65535, length 0
12:22:49.305237 IP ssis-dev.csub.edu.2507 > 136.168.108.49.microsoft-ds: Flags [P.], seq 2141782858:2141783026, ack 1052684477, win 65075, length 168
12:22:49.368171 IP masovlani.csub.edu.nfs > 136.168.1.127.domain-s: Flags [P.], seq 2088280774:2088280890, ack 3224050586, win 31088, length 116: NFS reply xid 681317983 reply ok 112
12:22:49.436862 IP 216.34.240.137.http > stg-edu-136-168-55-4.dyn.csub.edu.49495: Flags [.] , ack 1046655000, win 2172, options [nop,nop,TS val 2877368534 ecr 1276297095], length 0
12:22:49.436894 IP 216.34.240.137.http > stg-edu-136-168-55-4.dyn.csub.edu.49494: Flags [.] , ack 1355677179, win 113, options [nop,nop,TS val 1359709390 ecr 1276297095], length 0
12:22:49.440643 IP 74.125.19.147.http > stg-edu-136-168-55-4.dyn.csub.edu.49496: Flags [R], seq 2347562500, win 0, length 0
12:22:49.523580 IP ssis-dev.csub.edu.2507 > 136.168.108.49.microsoft-ds: Flags [S.], ack 93, win 64983, length 0
12:22:49.546390 IP 63.236.1.146.http > 136.168.101.1.55265: Flags [F.], seq 363, ack 3390, win 14480, options [nop,nop,TS val 411285207 ecr 1244405388], l
```

Question #2. Capture and display the number of packets destined for telnet port 23 on any host.

3

```
(neil@kali)-[/media/sf_shared]
$ tcpdump -r dump2_new.pcap tcp port 23
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:48.693949 IP guru.cs.csubak.edu.39102 > calculon.cs.csubak.edu.telnet: Flags [.] , ack 1290819934, win 24820, length 0
12:22:48.694092 IP calculon.cs.csubak.edu.telnet > guru.cs.csubak.edu.39102: Flags [P.], seq 1:84, ack 0, win 8760, length 83
12:22:48.793857 IP guru.cs.csubak.edu.39102 > calculon.cs.csubak.edu.telnet: Flags [.] , ack 84, win 24820, length 0
```

Question #3. Capture and display the HTTP packets (tcp port 80) destined for 136.168.246.23. The Total number of HTTP packets at port 80 with destination 136.168.246.23 is “8” which can be read by using filter

```
(root@kali)-[/media/sf_shared]
# tcpdump -r dump2_new.pcap tcp port 80 and dst host 136.168.246.23
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:50.084626 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 1455397899:1455399075, ack 3395620101, win 49640, length 1176: HTTP
12:22:50.085024 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 1176:2636, ack 1, win 49640, length 1460: HTTP
12:22:50.085145 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 2636:4096, ack 1, win 49640, length 1460: HTTP
12:22:50.085246 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 4096:5272, ack 1, win 49640, length 1176: HTTP
12:22:50.085368 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 5272:6732, ack 1, win 49640, length 1460: HTTP
12:22:50.085492 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 6732:8192, ack 1, win 49640, length 1460: HTTP
12:22:50.085593 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 8192:9368, ack 1, win 49640, length 1176: HTTP
12:22:50.085716 IP 64-74-142-151.compute.santa-clara.internapcloud.net.http > 136.168.246.23.3316: Flags [.] , seq 9368:10828, ack 1, win 49640, length 1460: HTTP
```

Question #4. Capture and display all packets involved to and from LaserPrinters. Hint: use the -A switch for tcpdump and the -i switch for grep
we get total of "9" packet which involves Laser Printers

```
(root@kali)-[/media/sf_shared]
# tcpdump -r dump2_new.pcap port 631
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:48.652560 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 128
12:22:49.652954 IP 136.168.240.113.631 > 136.168.255.255.631: UDP, length 101
12:22:49.652992 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 128
12:22:50.653376 IP 136.168.240.113.631 > 136.168.255.255.631: UDP, length 98
12:22:50.653493 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 129
12:22:50.658396 IP 136.168.247.44.631 > 136.168.255.255.631: UDP, length 91
12:22:50.658558 IP 136.168.247.44.631 > 136.168.255.255.631: UDP, length 112
12:22:50.658647 IP 136.168.247.44.631 > 136.168.255.255.631: UDP, length 114
12:22:50.658743 IP 136.168.247.44.631 > 136.168.255.255.631: UDP, length 135
```

. Question #5. Explain the output of this command (Hint: use IANA's well-known port list, dig, and /etc/services):

IPP (Internet Printing Protocol) via UDP is carried out on port 631; in the output, the IP address 136.168.241.81 uses port 631 to interact with the printer via UDP protocol.

```
(root@kali)-[/media/sf_shared]
# tcpdump -r dump2_new.pcap host 136.168.241.81
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:48.652560 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 128
12:22:49.652992 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 128
12:22:50.653493 IP 136.168.241.81.631 > 136.168.255.255.631: UDP, length 129

(root@kali)-[/media/sf_shared]
#
```

6 Question #6. Explain the output of this command (Hint: look in tcpdump man page)

```
(root@kali)-[/media/sf_shared]
# tcpdump -r dump2_new.pcap icmp[icmptype] = icmp-echo
reading from file dump2_new.pcap, link-type EN10MB (Ethernet), snapshot length 65535
12:22:49.088774 IP statseeker.csub.edu > 136.168.211.39: ICMP echo request, id 256, seq 256, length 24
12:22:50.104633 IP statseeker.csub.edu > 136.168.1.145: ICMP echo request, id 256, seq 256, length 24

(root@kali)-[/media/sf_shared]
#
```

This command reads just echo packets, which can be either request or response packets from the icmp protocol.

Part 3

Question #1. What type of network traffic are you seeing in your capture file?

time	source	destination	protocol	length	info
1 2007-11-07 12:22:48.649525	216.178.38.164	136.168.101.1	TCP	60	http(80) → 55261 [FIN, ACK] Seq=1
2 2007-11-07 12:22:48.650607	CompalInform_12:94::	Broadcast	ARP	60	Who has 136.168.249.115? Tell 136
3 2007-11-07 12:22:48.652560	136.168.241.81	136.168.255.255	CUPS	170	ipp://136.168.241.81/printers/f
4 2007-11-07 12:22:48.654486	CompalCommun_a4:74::	Broadcast	ARP	60	Who has 136.168.245.103? Tell 136
5 2007-11-07 12:22:48.658818	209.85.171.127	136.168.249.173	TCP	74	http(80) → 49424 [SYN, ACK] Seq=1
6 2007-11-07 12:22:48.659394	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.139.137? Tell 136
7 2007-11-07 12:22:48.687499	Dell_b9:02:16	Broadcast	ARP	60	Who has 136.168.191.21? Tell 136
8 2007-11-07 12:22:48.693949	guru.cs.csusbak.edu	calculon.cs.csusbak.edu	TCP	60	39102 → telnet(23) [ACK] Seq=1
9 2007-11-07 12:22:48.693977	209.85.171.127	136.168.249.173	TCP	66	http(80) → 49424 [ACK] Seq=1
10 2007-11-07 12:22:48.694092	calculon.cs.csusbak.edu	guru.cs.csusbak.edu	TELNET	137	Telnet Data ...
11 2007-11-07 12:22:48.695083	209.85.171.127	136.168.249.173	HTTP	279	HTTP/1.1 200 OK (text/html)
12 2007-11-07 12:22:48.697957	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.44.28? Tell 136
13 2007-11-07 12:22:48.699911	136.168.243.208	136.168.255.255	NBNS	92	Name query NB PERARTS<1b>
14 2007-11-07 12:22:48.704947	stg-edu-136-168-62::	Broadcast	ARP	60	Who has 136.168.245.79? Tell 136
15 2007-11-07 12:22:48.708231	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.254.62? Tell 136
16 2007-11-07 12:22:48.714109	cb144444.00010335be...	00000000.ffffffffffff...	NBIPX	98	Find name UNIVADV<1d>
17 2007-11-07 12:22:48.721600	Dell_49:c2:6e	Broadcast	ARP	60	Who has 136.168.39.20? Tell 136
18 2007-11-07 12:22:48.731376	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.7.113? Tell 136
19 2007-11-07 12:22:48.736141	63.236.1.146	136.168.101.1	TCP	74	http(80) → 55265 [SYN, ACK] Seq=1
20 2007-11-07 12:22:48.755462	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.151.101? Tell 136
21 2007-11-07 12:22:48.778025	Intel_ab:3d:15	Broadcast	ARP	60	Who has 136.168.75.15? Tell 136

We can see TCP,ARP,CUPS and HTTP

Question #2. Find the ssh login attempt. Can you see your fake username and/or password in the packets?

Cant find ssh protocol in the pcap

Question #3. Find the ftp login attempt. Can you see your fake username and/or password in the packets?

Cant find any ftp in the pcap

Question #4. On TCPDump output connection capture the following bits for ACK, SYN, FIN, URG, PSH, RST using masking. The command below are some examples. Submit the command and results for individual bits and the following combinations? A) Only ACK, SYN, FIN, URG, PSH, RST B) ACK and SYN C) SYN and FIN D) PSH and URG and ACK and FIN E) ACK or SYN or FIN either of the three.

```
(root@kali):~/media/sf_shared
# sudo tcpdump 'tcp[13] & 10 !=0'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, Link-type EN10MB (Ethernet), snapshot length 262144 bytes
20:09:21.604613 IP 239.237.117.34.bc.googleusercontent.com.https > 10.0.2.15.53572: Flags [S.], seq 64001, ack 3061069778, win 65535, options [mss 1460], length 0
20:09:21.604678 IP 10.0.2.15.53572 > 239.237.117.34.bc.googleusercontent.com.https: Flags [P.], ack 1, win 64240, length 517
20:09:21.614012 IP 10.0.2.15.53572 > 239.237.117.34.bc.googleusercontent.com.https: Flags [P.], seq 1:518, ack 1, win 64240, length 517
20:09:21.614581 IP 239.237.117.34.bc.googleusercontent.com.https > 10.0.2.15.53572: Flags [P.], ack 518, win 65535, length 0
20:09:21.632831 IP 239.237.117.34.bc.googleusercontent.com.https > 10.0.2.15.53572: Flags [P.], seq 1:2921, ack 518, win 65535, length 2920
20:09:21.632875 IP 10.0.2.15.53572 > 239.237.117.34.bc.googleusercontent.com.https: Flags [P.], seq 2921:4517, ack 518, win 65535, length 1596
20:09:21.633411 IP 239.237.117.34.bc.googleusercontent.com.https > 10.0.2.15.53572: Flags [P.], seq 2921:4517, ack 518, win 65535, length 1596
20:09:21.633435 IP 10.0.2.15.53572 > 239.237.117.34.bc.googleusercontent.com.https: Flags [P.], seq 4517, win 61320, length 0
20:09:21.876132 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [S.], seq 128001, ack 3812527114, win 65535, options [mss 1460], length 0
20:09:21.876184 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], ack 1, win 64240, length 0
20:09:21.885489 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], seq 1:518, ack 1, win 64240, length 517
20:09:21.885977 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [P.], ack 518, win 65535, length 0
20:09:21.962845 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [P.], seq 1:2921, ack 518, win 65535, length 2920
20:09:21.962877 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], seq 2921, win 62780, length 0
20:09:21.965141 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [P.], seq 2921:5420, ack 518, win 65535, length 2499
20:09:21.965168 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], seq 5420, win 62780, length 0
20:09:22.001203 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], seq 518:644, ack 5420, win 62780, length 126
20:09:22.079136 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [P.], seq 5420:5660, ack 644, win 65535, length 240
20:09:22.120873 IP 10.0.2.15.46182 > ec2-34-196-199-111.compute-1.amazonaws.com.https: Flags [P.], seq 5660, win 62780, length 0
20:09:22.221600 IP a96-7-129-60.deploy.static.akamaitechnologies.com.http > 10.0.2.15.60258: Flags [S.], seq 256001, ack 3911788436, win 65535, options [mss 1460], length 0
20:09:22.221640 IP 10.0.2.15.60258 > a96-7-129-60.deploy.static.akamaitechnologies.com.http: Flags [P.], ack 1, win 64240, length 0
20:09:22.222041 IP 10.0.2.15.60258 > a96-7-129-60.deploy.static.akamaitechnologies.com.http: Flags [P.], seq 1:416, ack 1, win 64240, length 415: HTTP: POST / HTTP/1.1
20:09:22.222444 IP a96-7-129-60.deploy.static.akamaitechnologies.com.http > 10.0.2.15.60258: Flags [P.], ack 416, win 65535, length 0
20:09:22.239509 IP server-13-226-223-188.lax50.r.cloudfront.net.http > 10.0.2.15.40562: Flags [S.], seq 320001, ack 2323225341, win 65535, options [mss 1460], length 0
20:09:22.239559 IP 10.0.2.15.40562 > server-13-226-223-188.lax50.r.cloudfront.net.http: Flags [P.], ack 1, win 64240, length 0
20:09:22.239915 IP 10.0.2.15.40562 > server-13-226-223-188.lax50.r.cloudfront.net.http: Flags [P.], seq 1:426, ack 1, win 64240, length 425: HTTP: POST / HTTP/1.1
```

```
(root@kali)-[/media/sf_shared]  
# sudo tcpdump 'tcp[13] & 1 != 0'
```

```
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
```

```
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

```
20:16:00.850019 IP 10.0.2.15.51794 > a96-7-129-55.deploy.static.akamaitechnologies.com.http: Flags [F.], seq 2439738617, ack 89644444, win 64008, length 0
```