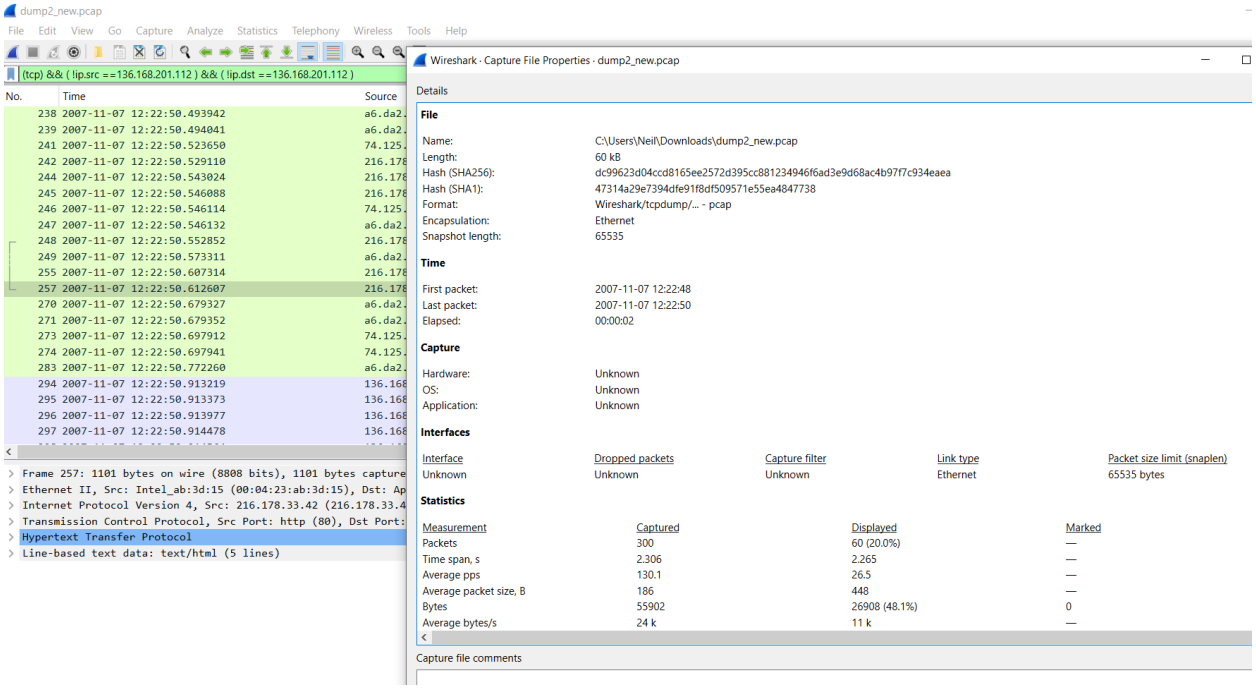
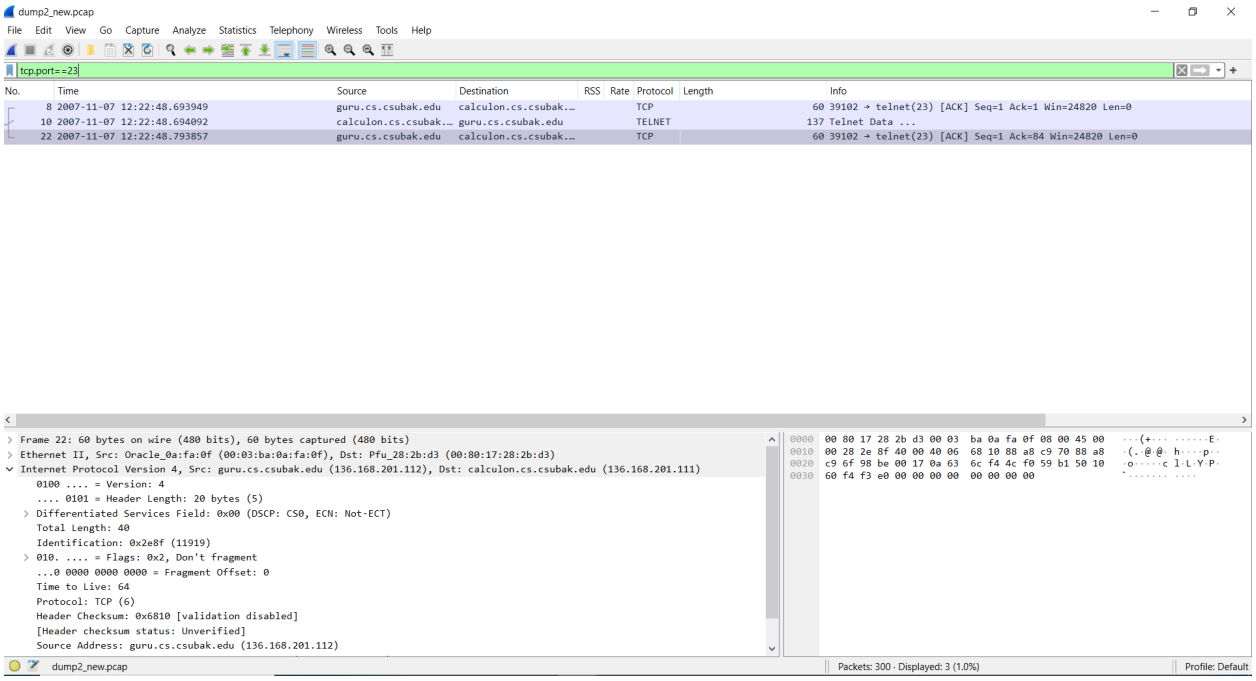
Part one

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

60

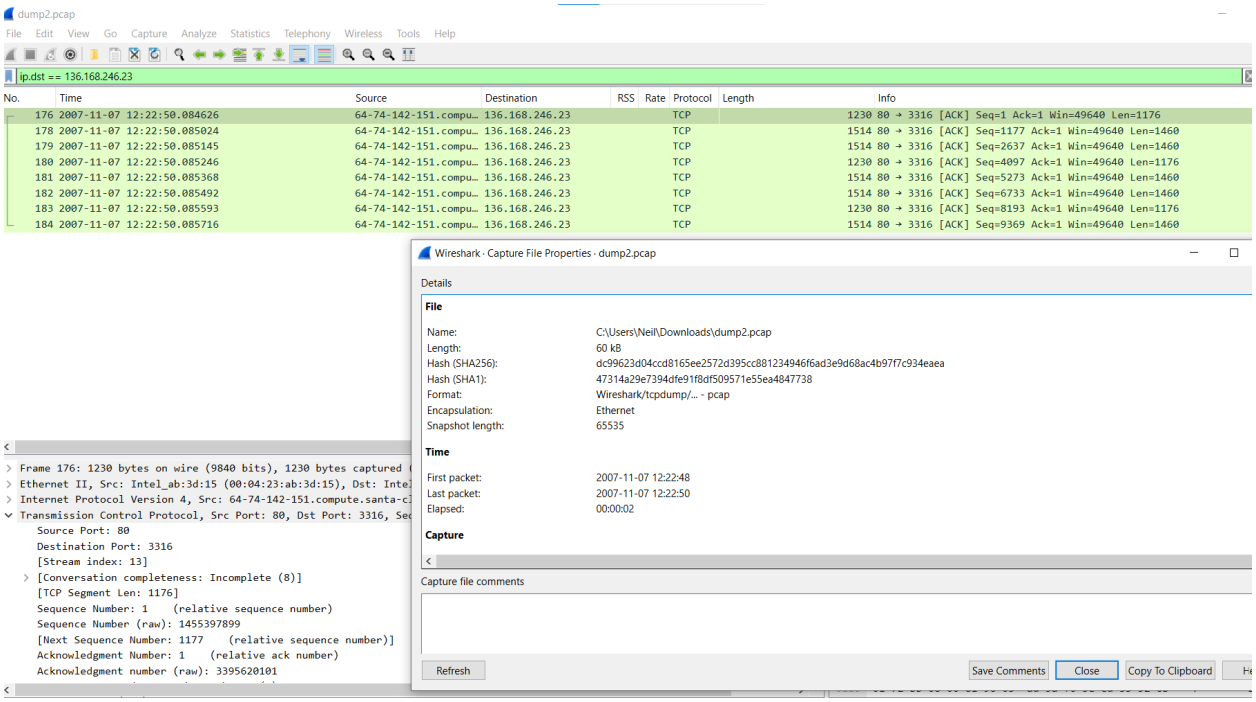


Question #2. Capture and count the number of packets destined for telnet port 23 on any host.

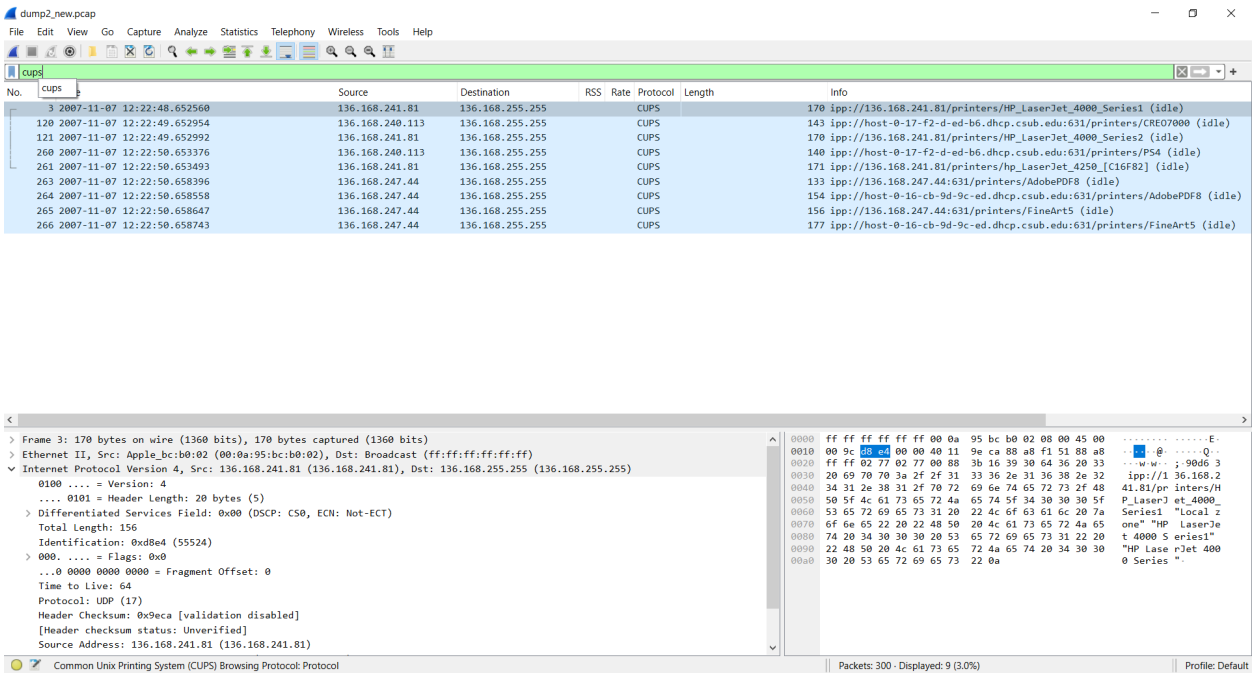


Question #3. Capture and count the HTTP packets (tcp port 80) destined for 136.168.246.23.

8 packets using



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

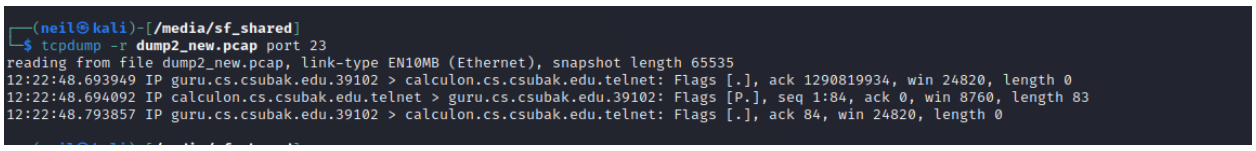


we'll get packets involved to and from Laser printers which is "9" packets in total

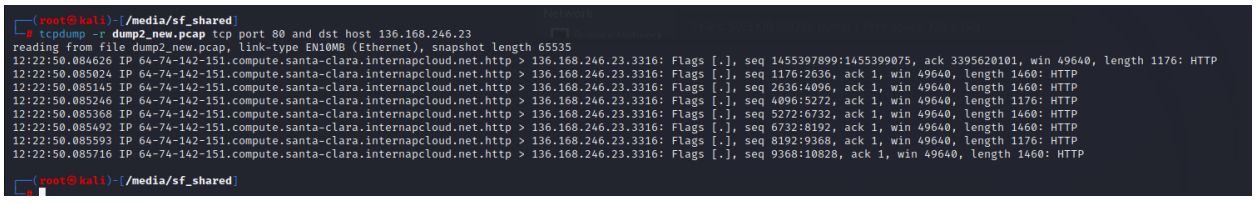
Part 2

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

Question #2. Capture and display the number of packets destined for telnet port 23 on any host.
3



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



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	RSS	Rate	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
2	2007-11-07 12:22:48.650607	CompalInform_12:94:…	Broadcast			ARP	60	Who has 136.168.249.115? Tell 1
3	2007-11-07 12:22:48.652560	136.168.241.81	136.168.255.255			CUPS	170	ipp://136.168.241.81/printers/h
4	2007-11-07 12:22:48.654486	CompalCommun_a4:74:…	Broadcast			ARP	60	Who has 136.168.245.103? Tell 1
5	2007-11-07 12:22:48.658818	209.85.171.127	136.168.249.173			TCP	74	http(80) → 49424 [SYN, ACK] Seq
6	2007-11-07 12:22:48.659394	Intel_ab:3d:15	Broadcast			ARP	60	Who has 136.168.139.137? Tell 1
7	2007-11-07 12:22:48.687499	Dell_b9:02:16	Broadcast			ARP	60	Who has 136.168.191.21? Tell 13
8	2007-11-07 12:22:48.693949	guru.cs.csubak.edu	calculon.cs.csubak.…			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 Ac
10	2007-11-07 12:22:48.694092	calculon.cs.csubak.…	guru.cs.csubak.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 13
15	2007-11-07 12:22:48.708231	Intel_ab:3d:15	Broadcast			ARP	60	Who has 136.168.254.62? Tell 13
16	2007-11-07 12:22:48.714109	cb144444.00010335be…	00000000.ffffffffff…			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
20	2007-11-07 12:22:48.755462	Intel_ab:3d:15	Broadcast			ARP	60	Who has 136.168.151.101? Tell 1
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] & 16 !=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 [.], ack 1, win 64240, length 0
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 [.], 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 [.], 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 [.], ack 2921, win 62780, length 0
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 [.], ack 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 [.], 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 [.], 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 [.], 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 [.], ack 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 [.], ack 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
20:09:22.001630 IP ec2-34-196-199-111.compute-1.amazonaws.com.https > 10.0.2.15.46182: Flags [.], ack 644, win 65535, length 0
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 [.], ack 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 [.], 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 [.], 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 [.], 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 8964444, win 64008, length 0
```