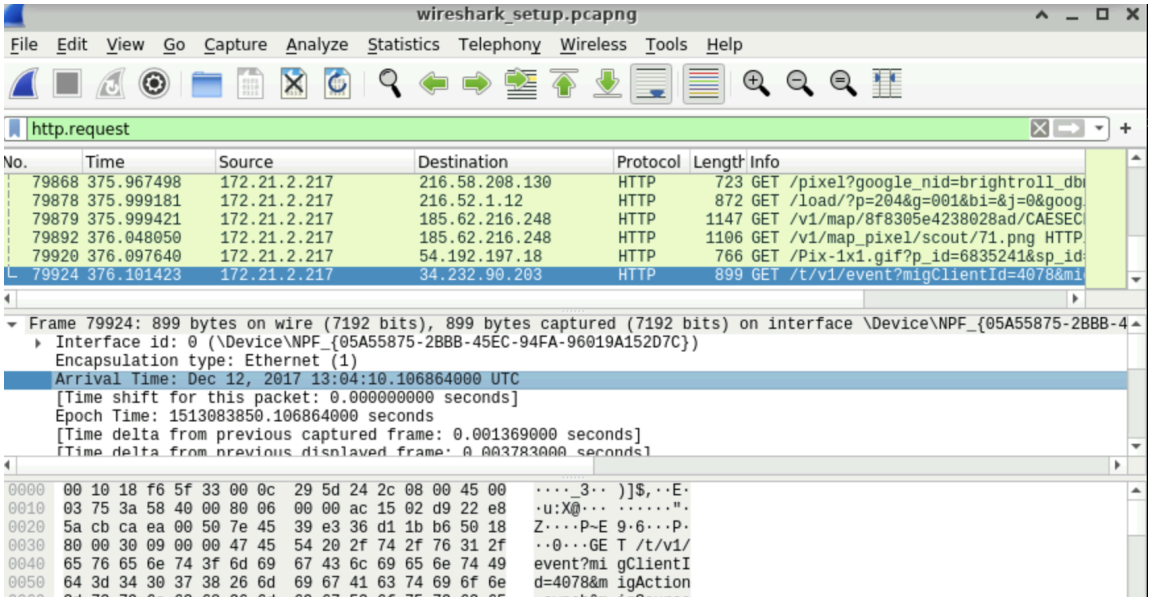
Network Capture, Analysis, and Scanning - Lab 2 - Arghya Sarkar - abs9425

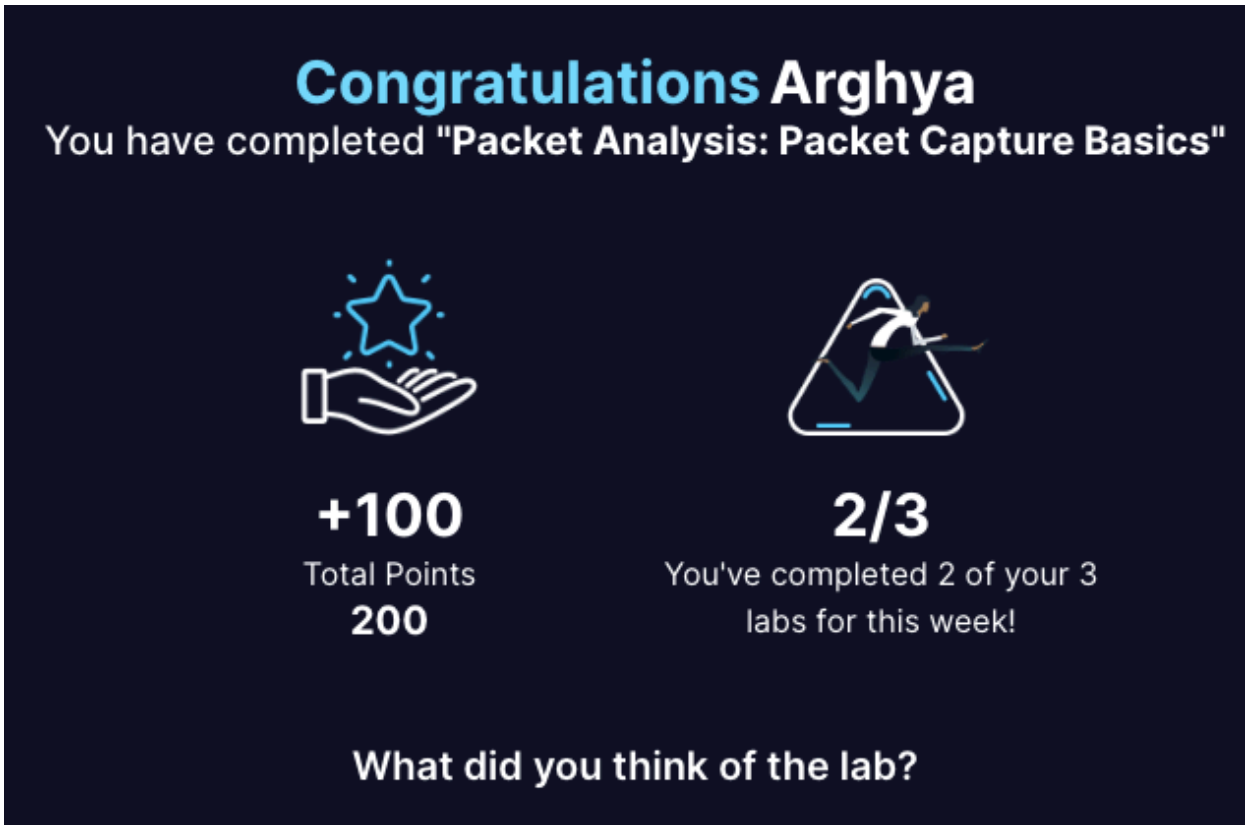
Explanation:

1. Raw data is too much info to display. With port numbers we can identify common protocols and services associated with them.
2. tcp.port eq 25 filters for SMTP traffic, which typically uses port 25
3. Filter for http.request (open pcapng file)

4. Double click on request and look at info

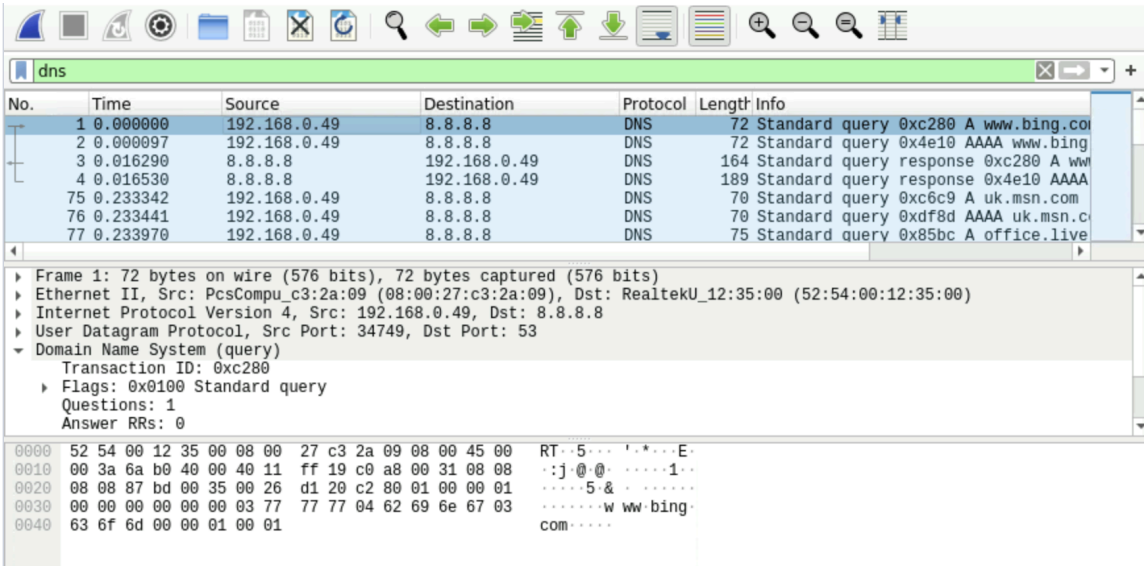


5. Look at the destination of request

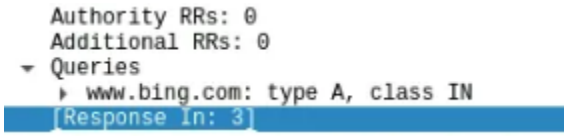


Explanation:

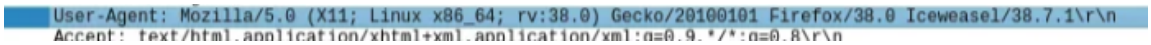
1. Filter for "dns", select the first DNS packet, expand "Domain Name System (query)" in the packet details, and check under "Queries"



2. Open the response packet, expand the "Domain Name System (query)" section, and locate the IP address in the query results



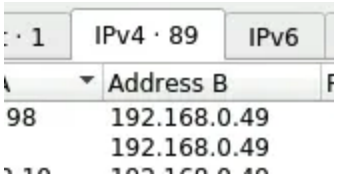
3. To get user agents analyze GET requests. Filter for GET requests (http.request.method == "GET"), select the first HTTP packet, expand Hypertext Transfer Protocol in the packet details pane, and locate the user-agent field



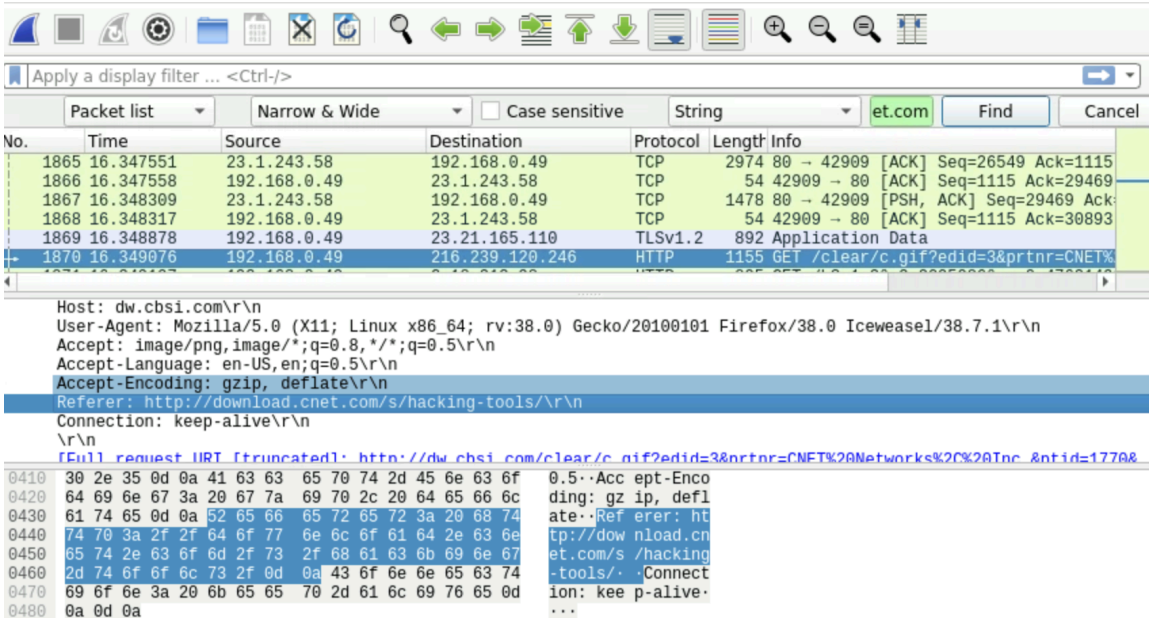
4. Filter for "http.server", select a packet, expand "Hypertext Transfer Protocol" in the details pane, and locate the "Server" heading

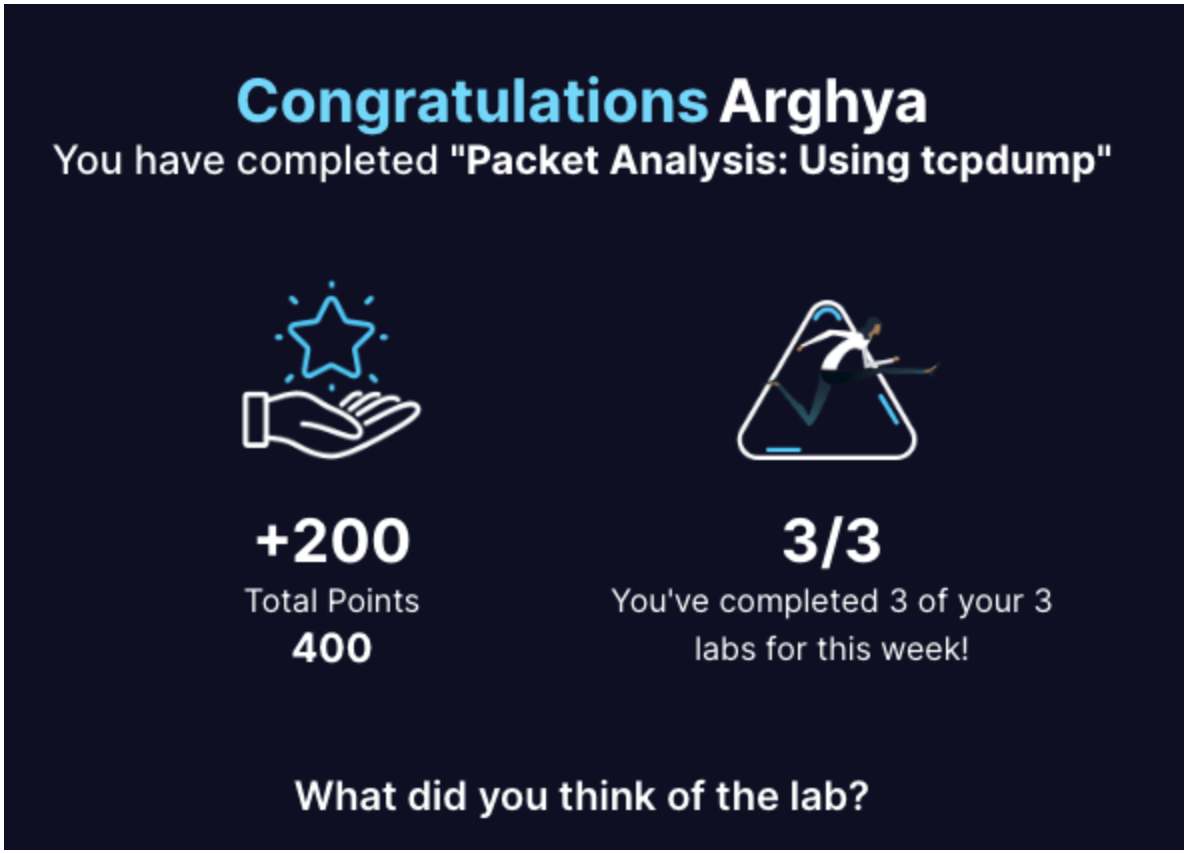
5. Use "Find Packet" (in Edit menu) with the PNG filename, locate the GET request, and note the response packet number. Export HTTP objects, filter for PNG, save the specific response packet, and open the downloaded image to view the required text

6. To find the number of conversations, use Wireshark's Statistics > Conversations feature and check the total count in the IPv4 tab or overall display



7. To find the searched term, locate the packet containing "download.cnet.com" and check the referrer heading in its Hypertext Transfer Protocol tab





Explanation:

1. Based on the briefing: “tcpdump allows you to output your results into a specified file type such as csv or txt. To do this you can specify the -w option”
2. Run ` tcpdump -D `

```
linux@tcpdump:~$ tcpdump -D
1.eth0 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
```

3. -X form cheatsheet

4. Run ` tcpdump -r tcpdump.pcap 'host 88.221.88.59' `

```
linux@tcpdump:~$ tcpdump -r tcpdump.pcap 'host 88.221.88.59'
reading from file tcpdump.pcap, link-type EN10MB (Ethernet)
07:31:56.197987 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 2054538429, win 30016, length 0
07:31:56.198136 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:06.438054 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:06.438365 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:16.677955 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:16.678082 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:26.921868 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:26.921990 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:37.158275 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:37.158725 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:47.397977 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:47.398547 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
33.eu-west-1.compute.internal.40646: Flags [.], ack 1, win 64240, length 0
07:32:57.638112 IP ip-192-168-21-133.eu-west-1.compute.internal.40646 > a88-221-88-59.depl
oy.static.akamaitechnologies.com.80: Flags [.], ack 1, win 30016, length 0
07:32:57.638538 IP a88-221-88-59.deploy.static.akamaitechnologies.com.80 > ip-192-168-21-1
```

5. Run
   tcpdump -r tcpdump.pcap -w filtered_packets.pcap 'host 184.107.41.72 and port 80'
   md5sum filtered_packets.pcap

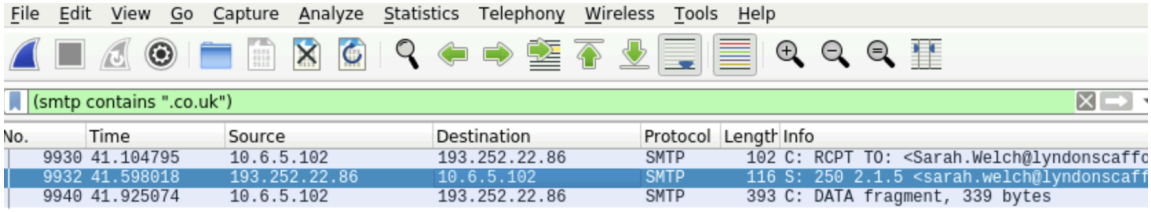
```
linux@tcpdump:~$ tcpdump -r tcpdump.pcap -w filtered_packets.pcap 'host 184.107.41.72 and
port 80'
reading from file tcpdump.pcap, link-type EN10MB (Ethernet)
linux@tcpdump:~$ md5sum filtered_packets.pcap
8e4b92724d9034a49cf10f6b147ac482  filtered_packets.pcap
```

Explanation:

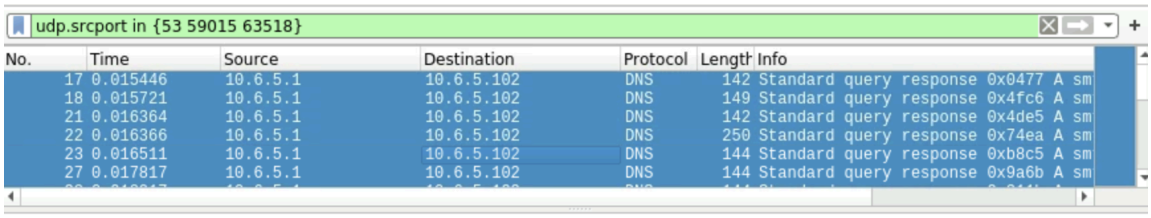
1. Apply the filter "(smtp contains "Subject: ")", open the first packet, and find the recipient's name under the "To" heading in the "Simple Mail Transfer Protocol" field

```
▸ Transmission Control Protocol, Src Port: 49269, Dst Port: 587,
▾ Simple Mail Transfer Protocol
  ▾ Line-based text data (23 lines)
      From: Bob Barton <ericrene.malherbe@wanadoo.fr>\r\n
      To: Sarah.Wells2@stockport.nhs.uk\r\n
      Message-ID: <2375801327.20186518318@stockport.nhs.uk>\r\n
      Subject: New Invoice / LN59175 / UR# 5010\r\n
      MIME-Version: 1.0\r\n
      Content-Type: multipart/mixed; boundary="----= NextPart_00
```

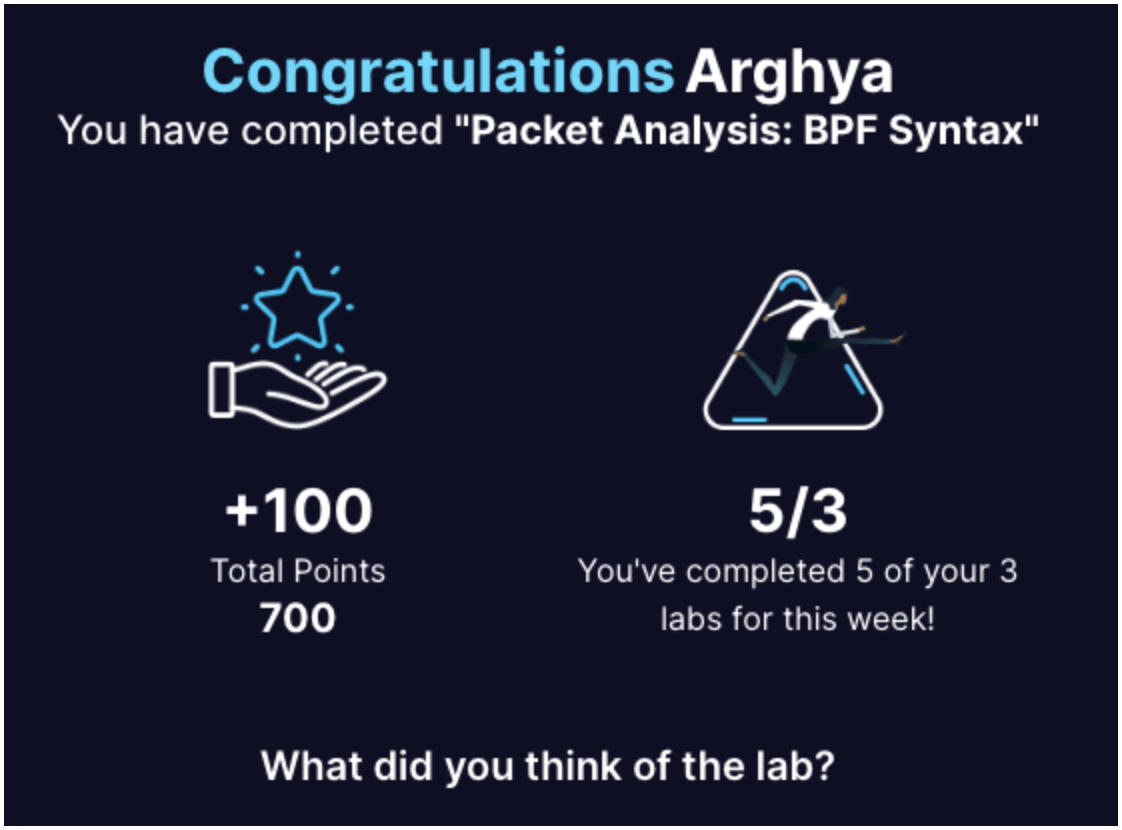
2. Filter by "(smtp contains ".co.uk")", add response packet number, and check STMP field for packet count



3. Use `udp.srcport in {53 59015 63518}` to filter UDP source ports; both yield identical results visible in the packet count. Then use cmd + A



4. Look at the frame index
5. Look at the frame index. Default is 0



Explanation:

1. Abbr.
2. The two primitives in this expression are: `wlan.addr == c5:52:7e:95:6:8d` AND `wlan.fc.type_subtype == 0x02`
3. Run ` tcpdump -r bpf-pcap.pcapng 'host 10.0.50.227 and tcp port 80' `

```
west-1.compute.amazonaws.com.80: Flags [P.], seq 1:386, ack 1, win 259, length 385: HTTP:
GET /5/c=10025/camp_int=Advertiser-153172%5ECampaign-814780%5Eimpressions HTTP/1.1
```

4. Run ` tcpdump -r bpf-pcap.pcapng udp port 57190 ` and check last packet

```
11:54:43.808109 IP ip-10-0-50-227.eu-west-1.compute.internal.57190 > lhr35s07-in-f3.1e100
net.443: UDP, length 41
```

5. Run (Note DNS = 53)
   tcpdump -r bpf-pcap.pcapng -w filtered_packets.pcap not port 53 and not tcp
   md5sum filtered_packets.pcap

```
linux@bpf-syntax:~$ tcpdump -r bpf-pcap.pcapng -w filtered_packets.pcap not port 53 and no
t tcp
reading from file bpf-pcap.pcapng, link-type EN10MB (Ethernet)
linux@bpf-syntax:~$ md5sum filtered_packets.pcap
b942d25b012745422c1719ac26419da6  filtered_packets.pcap
```

–

I have explained everything thoroughly and you can easily run my commands to verify results.