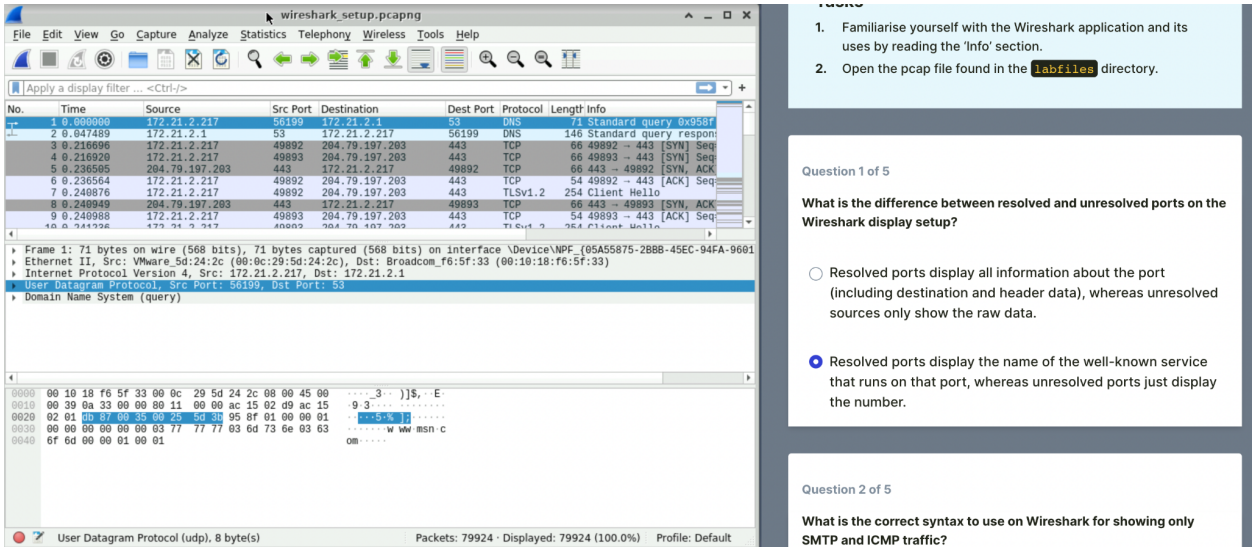
Amanda Gonzalez

# Lab 1

## Intro to Wireshark

*Question 1:* Resolved ports should display names of well-known service, but this version of Wireshark did not, the list from internet assigned numbers authority provided the service name for resolved ports, such as dest port 53 from packet no. 1

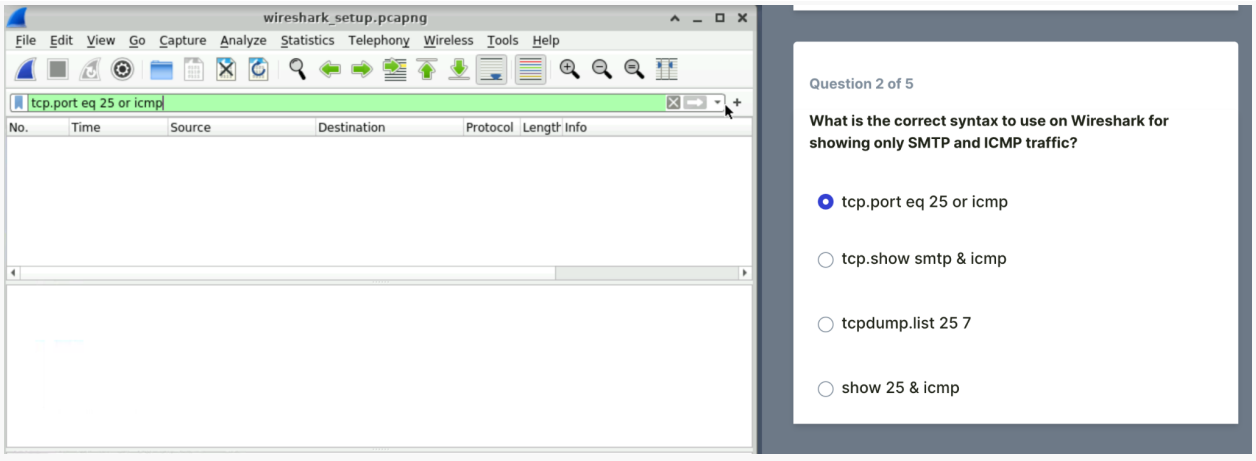



53 Search

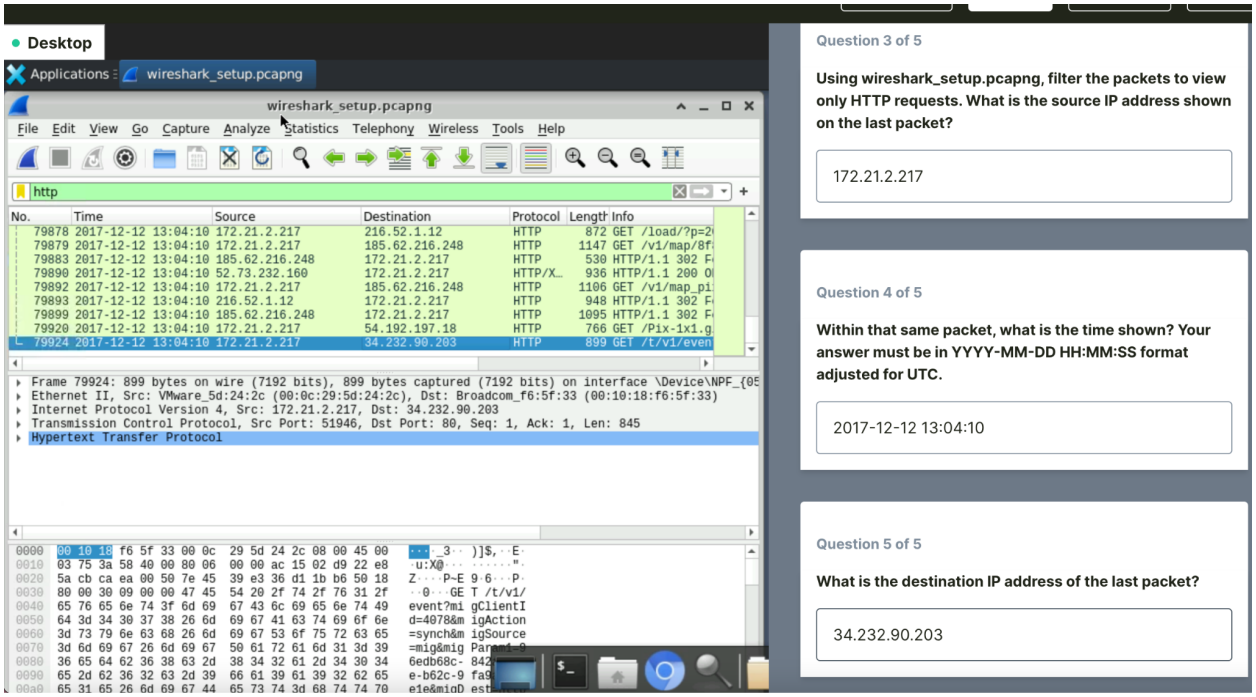
1 2 3 4

| Service Name | Port Number | Transport Protocol | Description | Assignee | Contact | Registration Date | Modification Date | Reference | Service Code | Unauthorized Use Reported | Assignment Notes |
|---|---|---|---|---|---|---|---|---|---|---|---|
| smtp | 25 | tcp | Simple Mail Transfer | [IESG] | [IETF Chair] | | 2017-06-05 | [RFC5321] | | | |
| smtp | 25 | udp | Simple Mail Transfer | [IESG] | [IETF Chair] | | 2017-06-05 | [RFC5321] | | | |
| domain | 53 | tcp | Domain Name Server | [Paul Mockapetris] | [Paul Mockapetris] | | | | | | |
| domain | 53 | udp | Domain Name Server | [Paul Mockapetris] | [Paul Mockapetris] | | | | | | |
| sgmp | 153 | tcp | SGMP | [Marty Schoffstahl] | [Marty Schoffstahl] | | | | | | |
| sgmp | 153 | udp | SGMP | [Marty Schoffstahl] | [Marty Schoffstahl] | | | | | | |
| ndsauth | 353 | tcp | NDSAUTH | [Jayakumar Ramalingam] | [Jayakumar Ramalingam] | | | | | | |
| ndsauth | 353 | udp | NDSAUTH | [Jayakumar Ramalingam] | [Jayakumar Ramalingam] | | | | | | |
| creativeserver | 453 | tcp | CreativeServer | | | | | | | | |
| creativeserver | 453 | udp | CreativeServer | | | | | | | | |
| courier | 530 | tcp | rpc | | | | | | | | |
| courier | 530 | udp | rpc | | | | | | | | |
| conference | 531 | tcp | chat | | | | | | | | |
| conference | 531 | udp | chat | | | | | | | | |
| netnews | 532 | tcp | readnews | | | | | | | | |
| netnews | 532 | udp | readnews | | | | | | | | |
| netwall | 533 | tcp | for emergency broadcasts | [Andreas Heidemann] | [Andreas Heidemann] | | | | | | |
| netwall | 533 | udp | for emergency broadcasts | [Andreas Heidemann] | [Andreas Heidemann] | | | | | | |
| windream | 534 | tcp | windream Admin | [Uwe Honermann] | [Uwe Honermann] | | | | | | |
| windream | 534 | udp | windream Admin | [Uwe Honermann] | [Uwe Honermann] | | | | | | |
| iiop | 535 | tcp | iiop | [Jeff M Michaud] | [Jeff M Michaud] | | | | | | |
| iiop | 535 | udp | iiop | [Jeff M Michaud] | [Jeff M Michaud] | | | | | | |
| opalis-rdv | 536 | tcp | opalis-rdv | [Laurent Domenech] | [Laurent Domenech] | | | | | | |
| opalis-rdv | 536 | udp | opalis-rdv | [Laurent Domenech] | [Laurent Domenech] | | | | | | |
| nmsp | 537 | tcp | Networked Media Streaming Protocol | [Paul Santinelli Jr] | [Paul Santinelli Jr] | | | | | | |

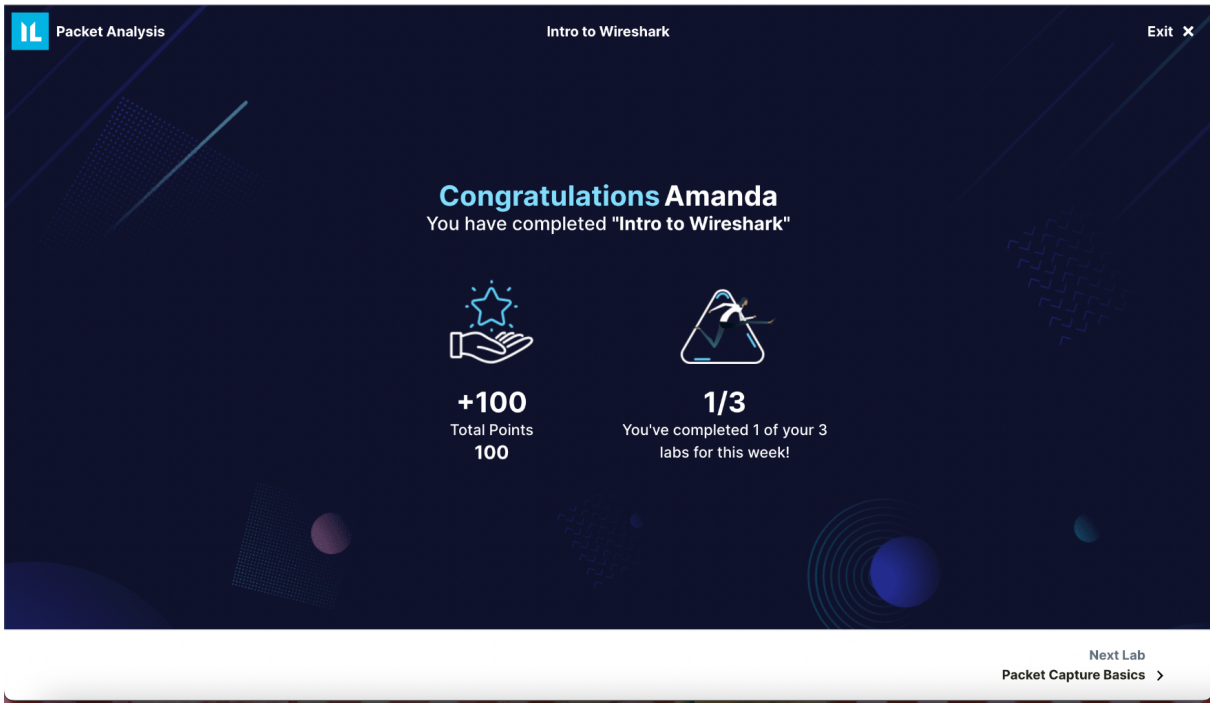
*Question 2:* There is no SMTP or ICMP traffic




*Question 3, 4, 5:* The source, time, and destination are listed under their respective column titles for the last packet.

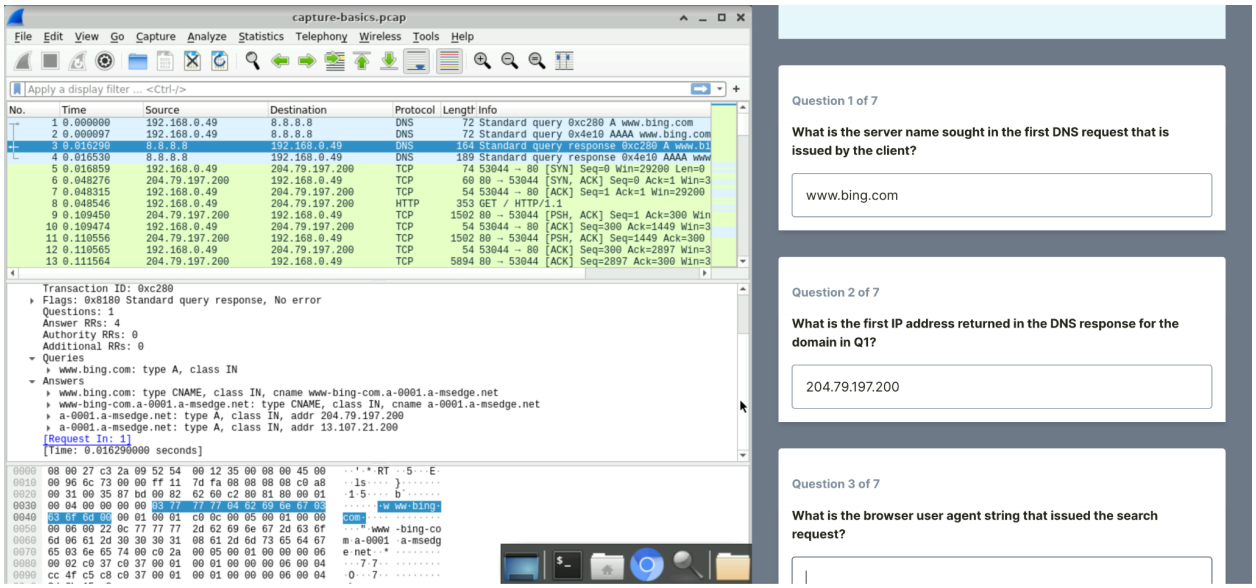


*Results:*

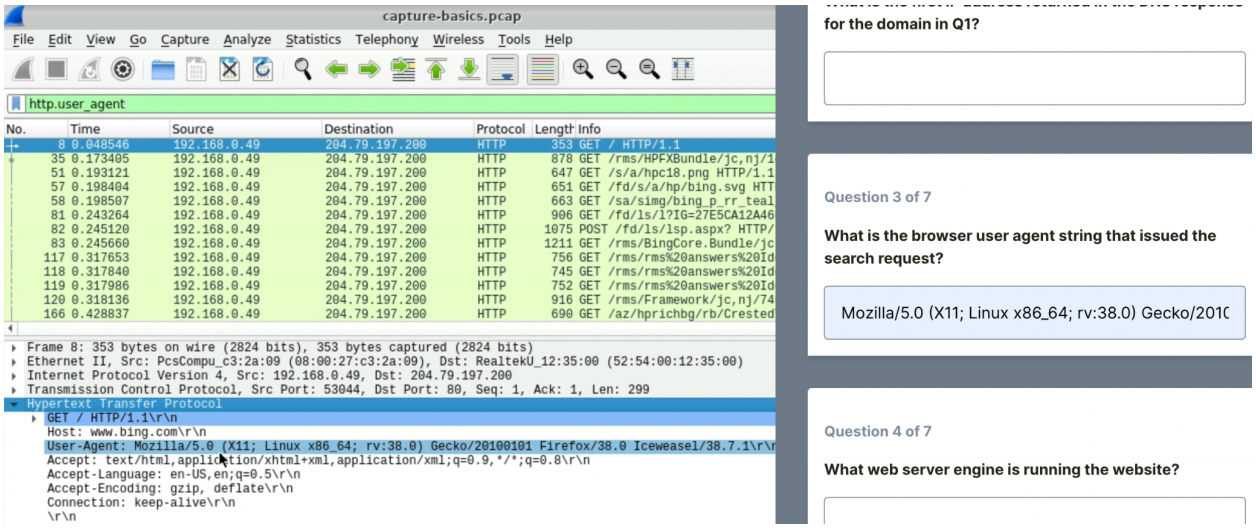

Packet Analysis
Intro to Wireshark
Exit
Congratulations Amanda
You have completed "Intro to Wireshark"
+100
Total Points
100
1/3
You've completed 1 of your 3 labs for this week!
Next Lab
Packet Capture Basics

## Packet Capture Basics

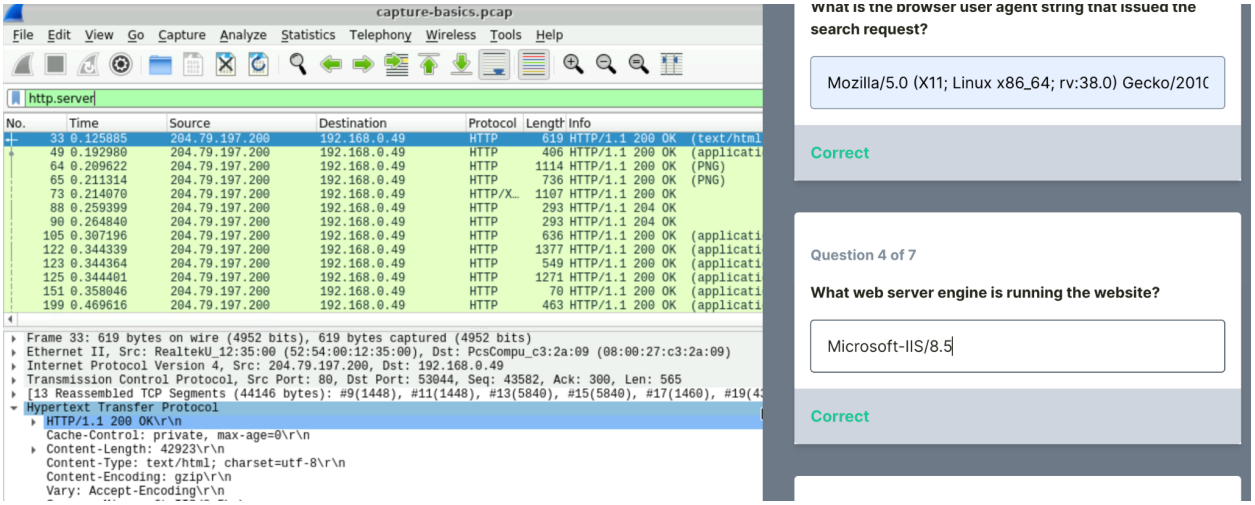
*Question 1 & 2:* The packet info (No. 1) displays the server name www.bing.com. The IP address returned is shown in the response packet in answers, which is 204.79.197.200.



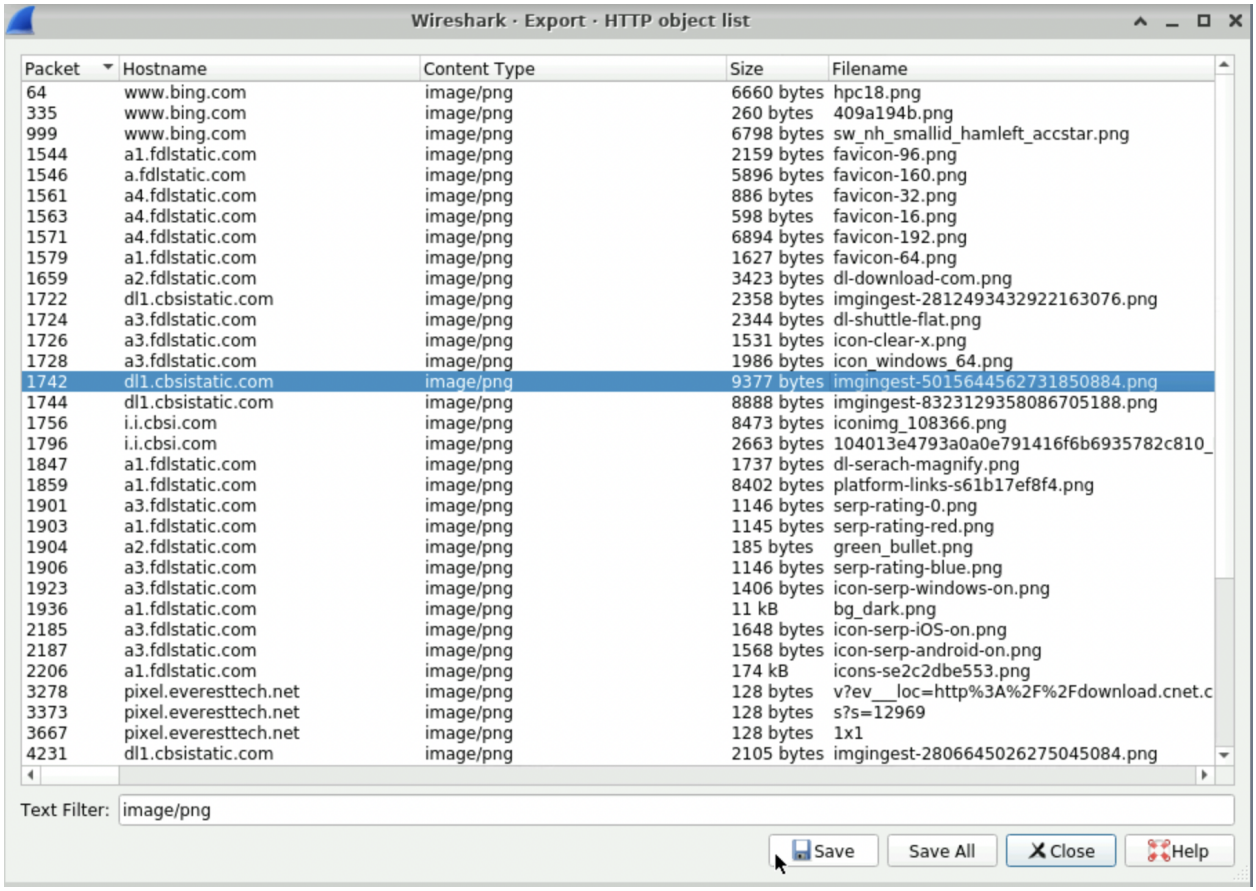

*Question 3:* The browser user agent string was Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1, found by filtering with http.user_agent.

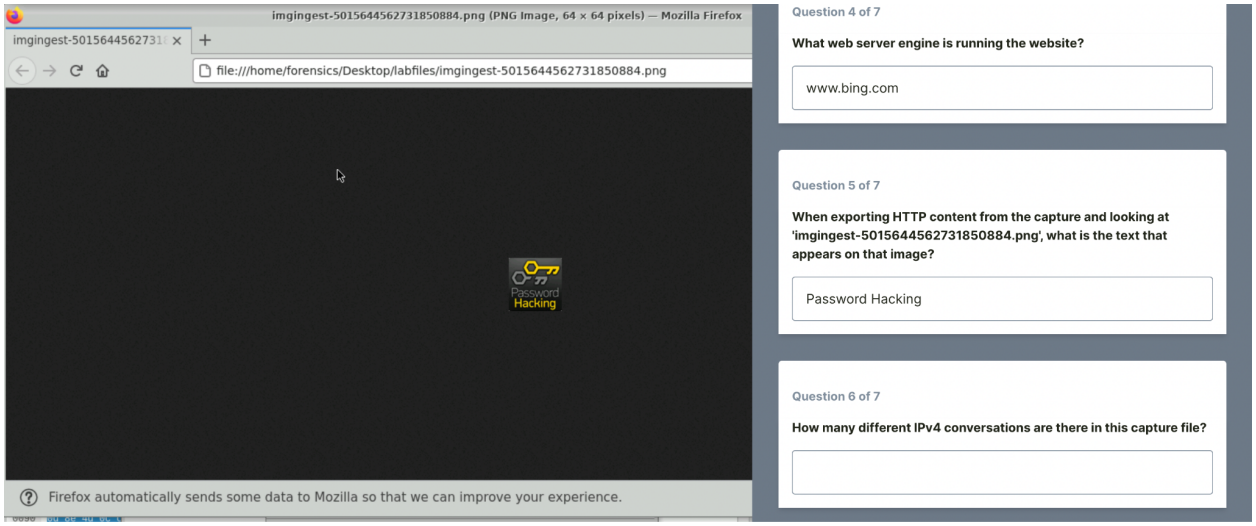


*Question 4:* The web server engine was Microsoft-IIS/8.5 found by filtering with http.server.

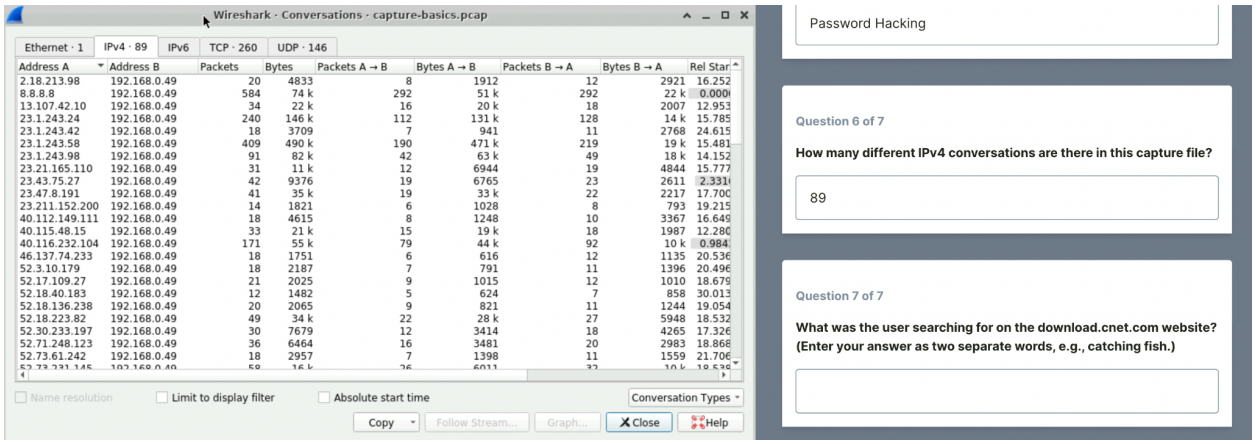



*Question 5:* The image was found by going to the HTTP object list and finding the filename we were looking for. To view the image, the file had to be downloaded and opened. The text states “Password Hacking”.

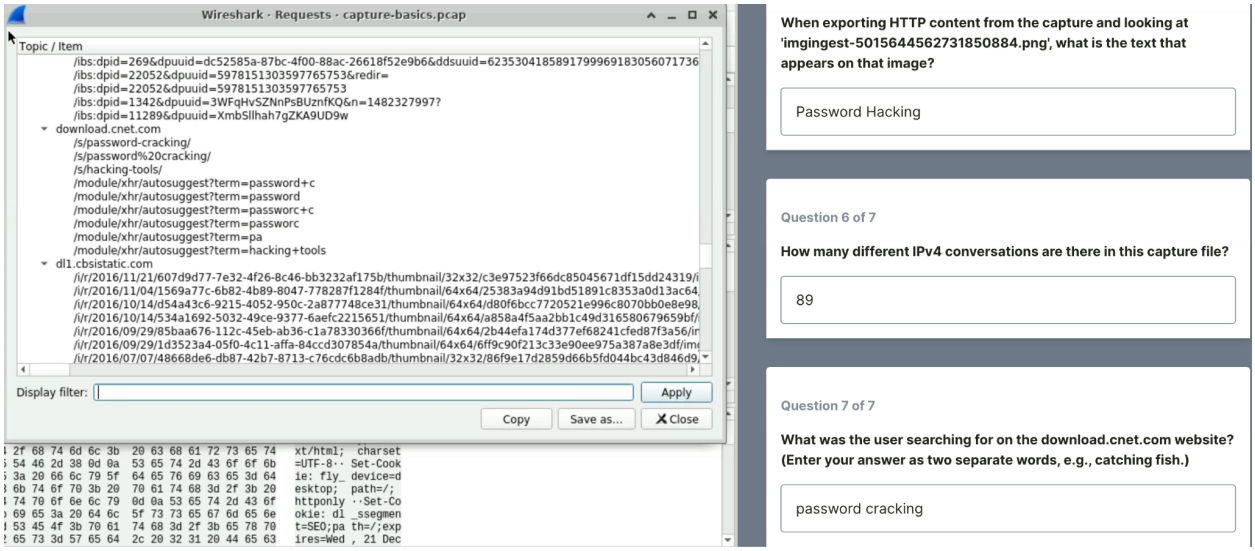




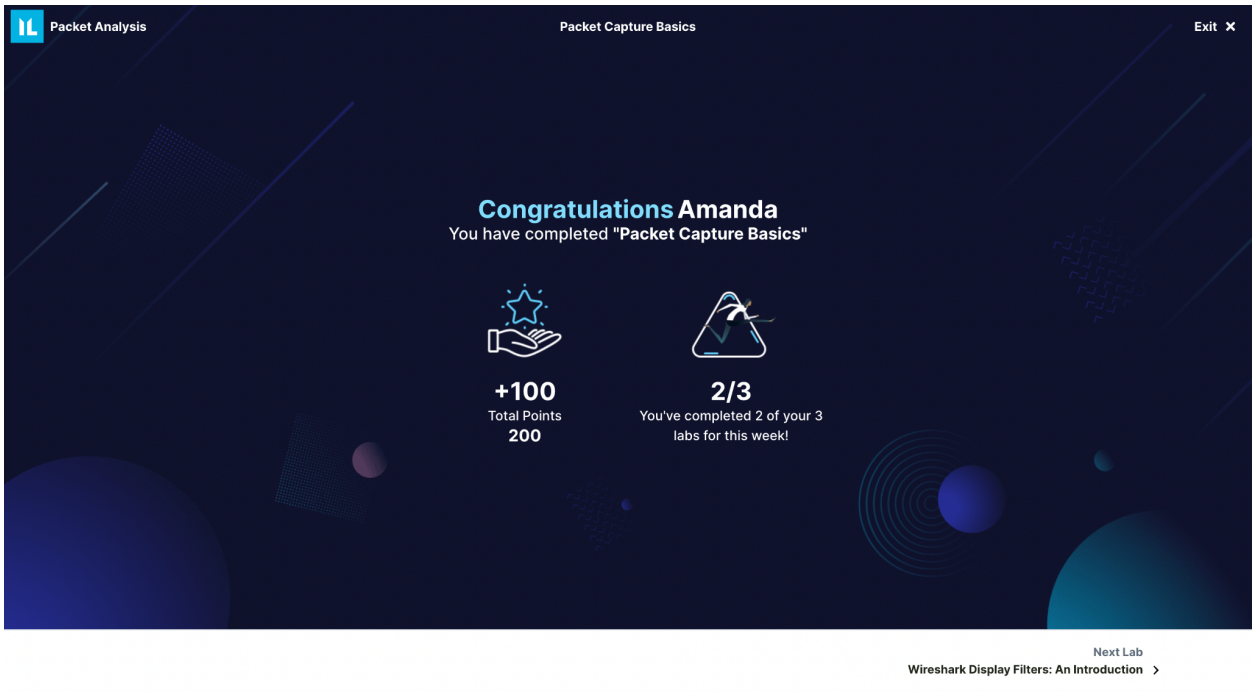

*Question 6:* There are 89 IPv4 Conversations, as found by going to Statistics > Conversations > IPv4.



*Question 7:* Found by going to Statistics > HTTP > Requests, under the host download.cnet.com, we can see the query for “password cracking”.

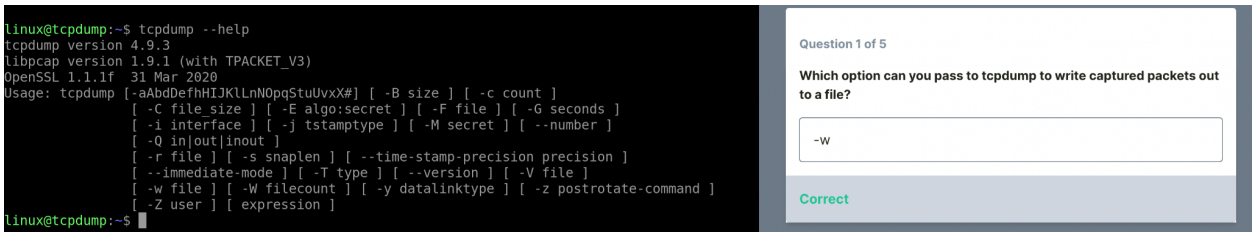



*Result:*

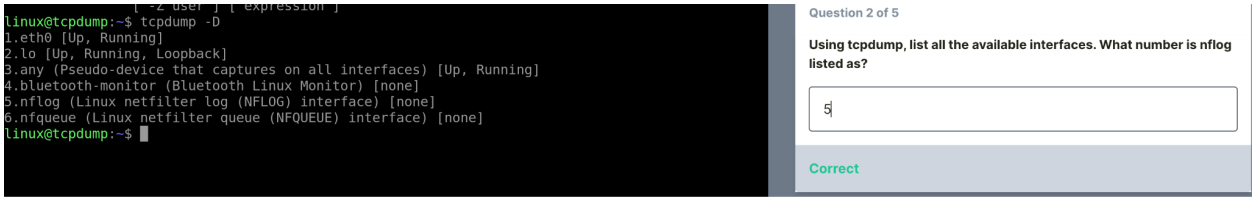


## TCP Dump

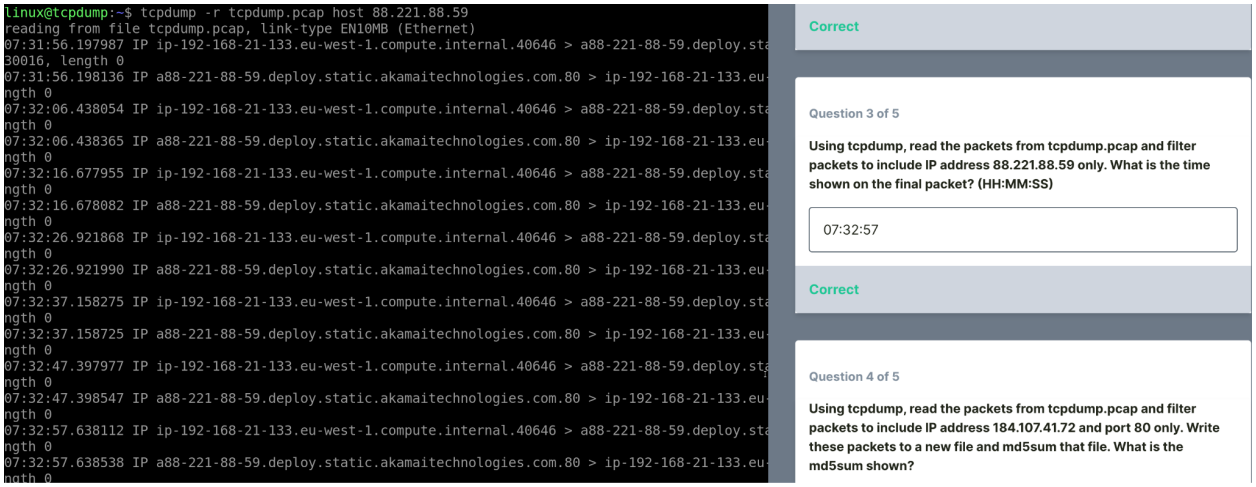
*Question 1:* The options show that -w will allow you to write to a file, you can do so with a command like tcpdump -r tcpdump.pcap -w output.txt



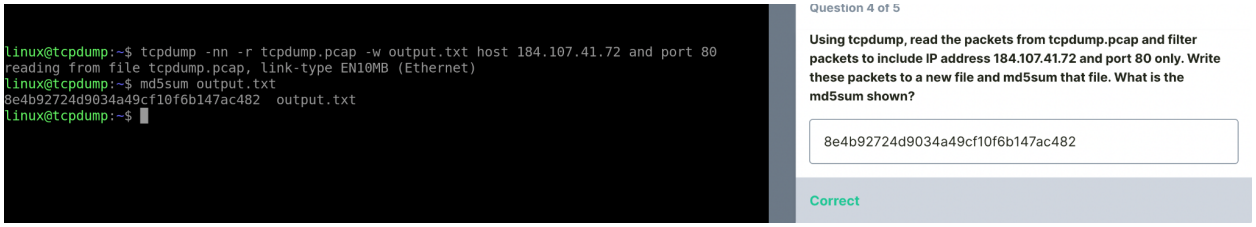

*Question 2:* Using the -D option, such as in the command tcpdump -D, we can see a list of all interfaces, and nflog is at number 5.



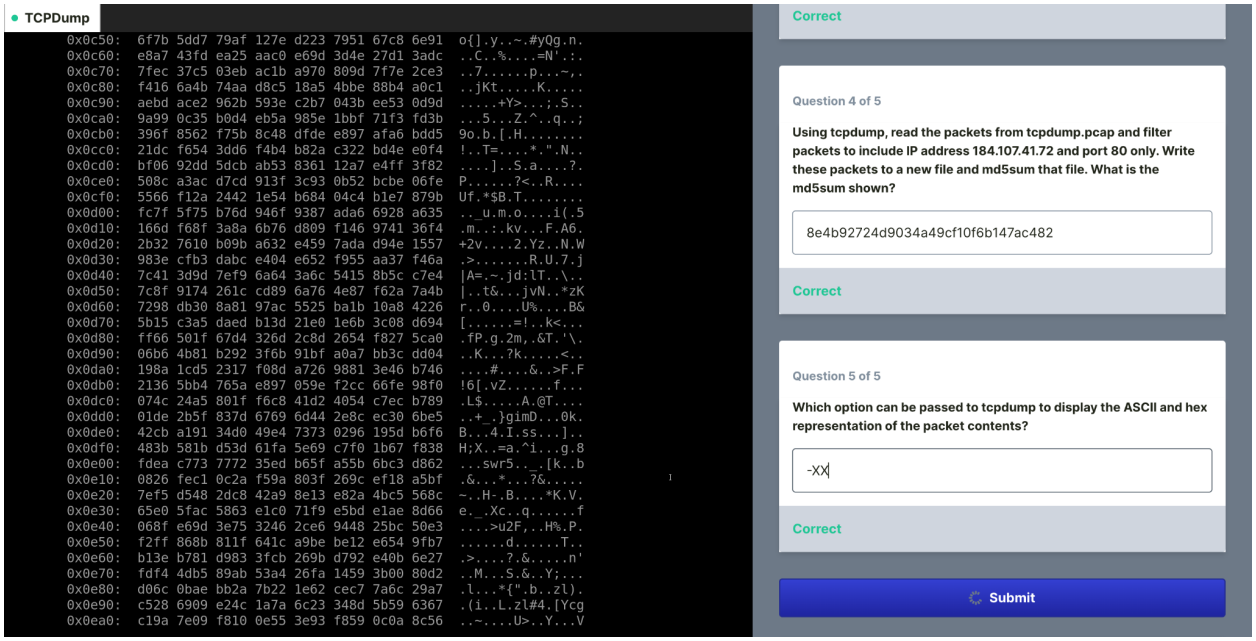

*Question 3:* By reading from tcpdump.pcap and filtering the IP address with the command, tcpdump -r tcpdump.pcap host 88.221.88.59, we can see the time on the last packet at the bottom to be 07:32:57.



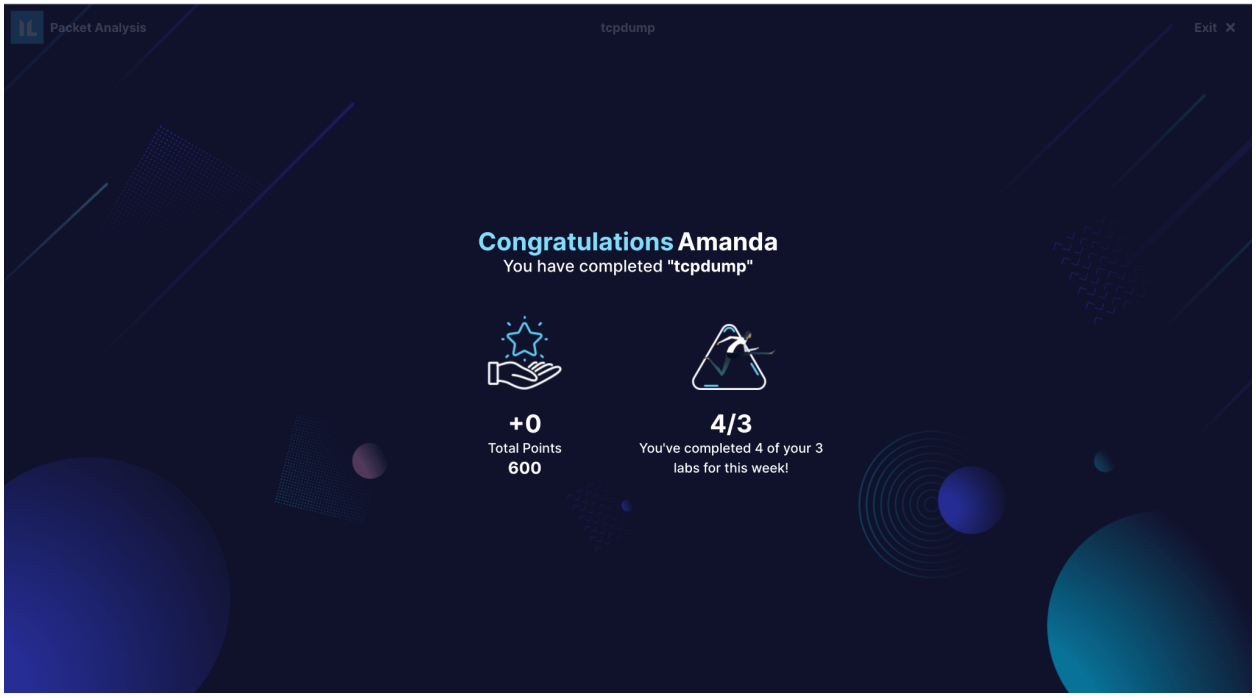
*Question 4:* To first read packets from the pcap file and filter for IP and port 80, I typed in ‘tcpdump -nn -r tcpdump.pcap -w output.txt host 184.107.41.71 and port 80’. Where the first part is reading from the pcap file, -w signifies writing to the file output.txt and host and port are filters. After writing to output.txt, I got the md5Sum of the file with ‘md5sum output.txt’, which is the hash of that file.




*Question 5:* To get ASCII and hex content from a packet, use the option -XX. I did this with tcpdump -r tcpdump.pcap -XX

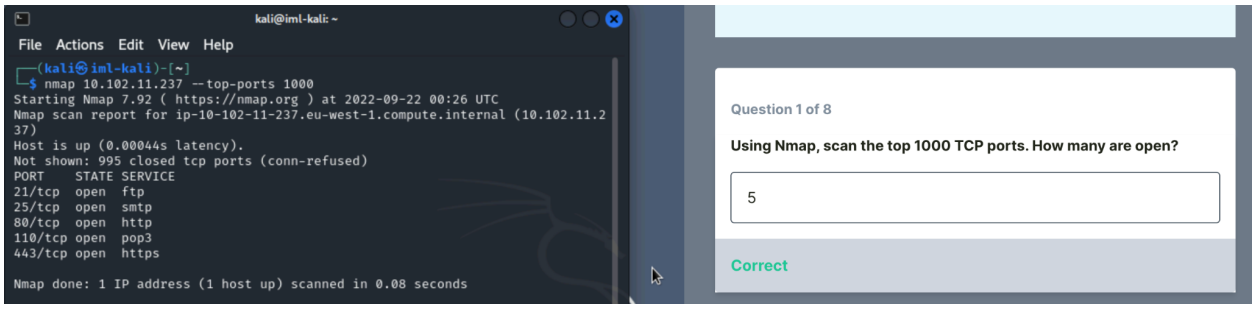


*Result:*

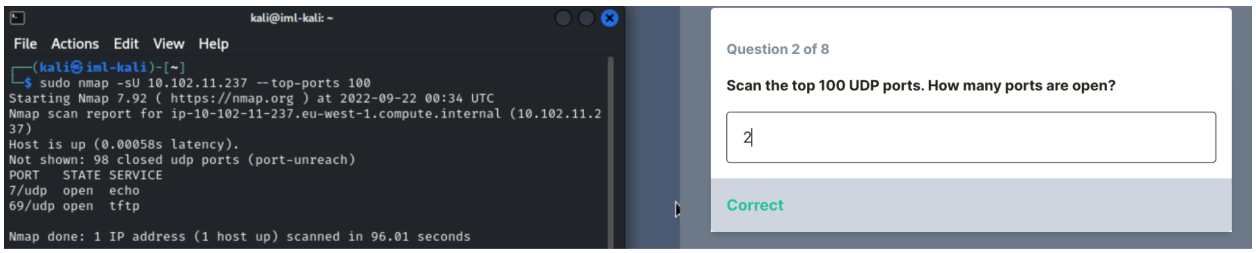

Packet Analysis
tcpdump
Exit
Congratulations Amanda
You have completed "tcpdump"
+0
Total Points
600
4/3
You've completed 4 of your 3 labs for this week!

**Nmap**

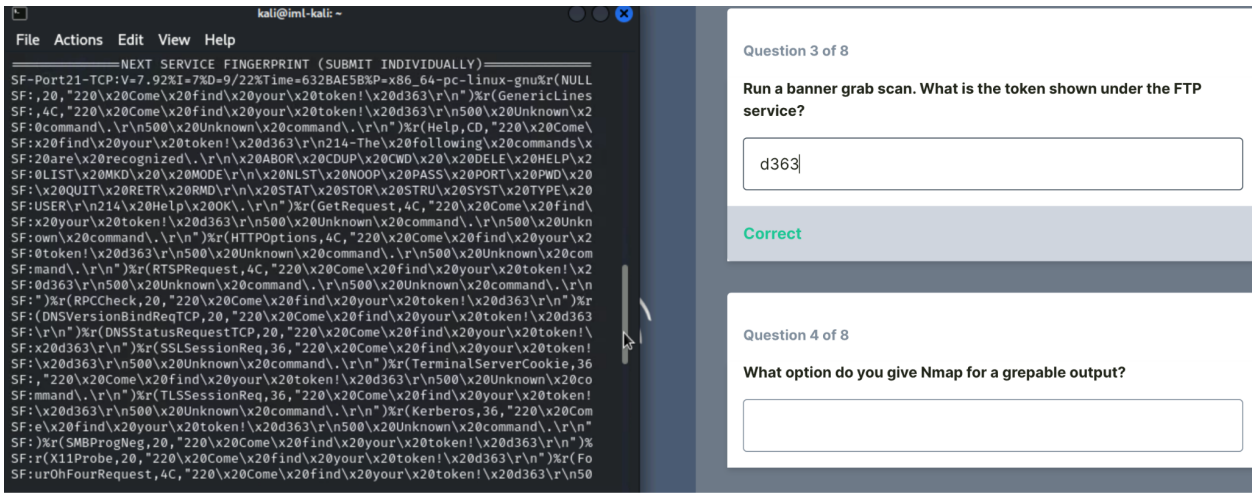
*Question 1:* Scanning the top 1000 ports with the option –top-ports 1000, we can see that 5 ports are open.



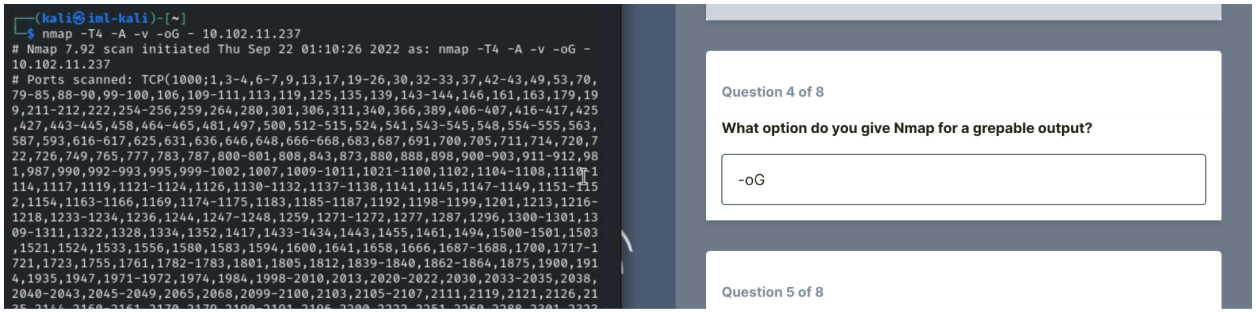

*Question 2:* To scan UDP ports only, I used the option -sU, and again –top-ports for the top 100 ports. This showed two open ports.



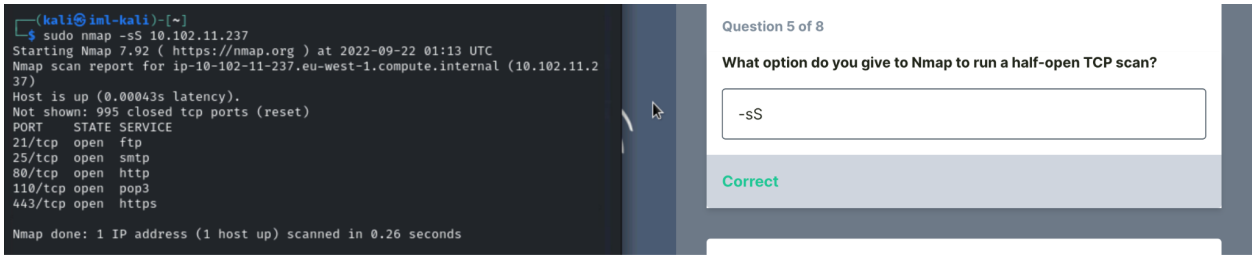

*Question 3:* I ran the banner scan with the command nmap -sV -v -p- 10.120.11.237. Reading through the text of the fingerprint, it states \x20Come\x20find\x20your\x20token!, followed by the token d363.



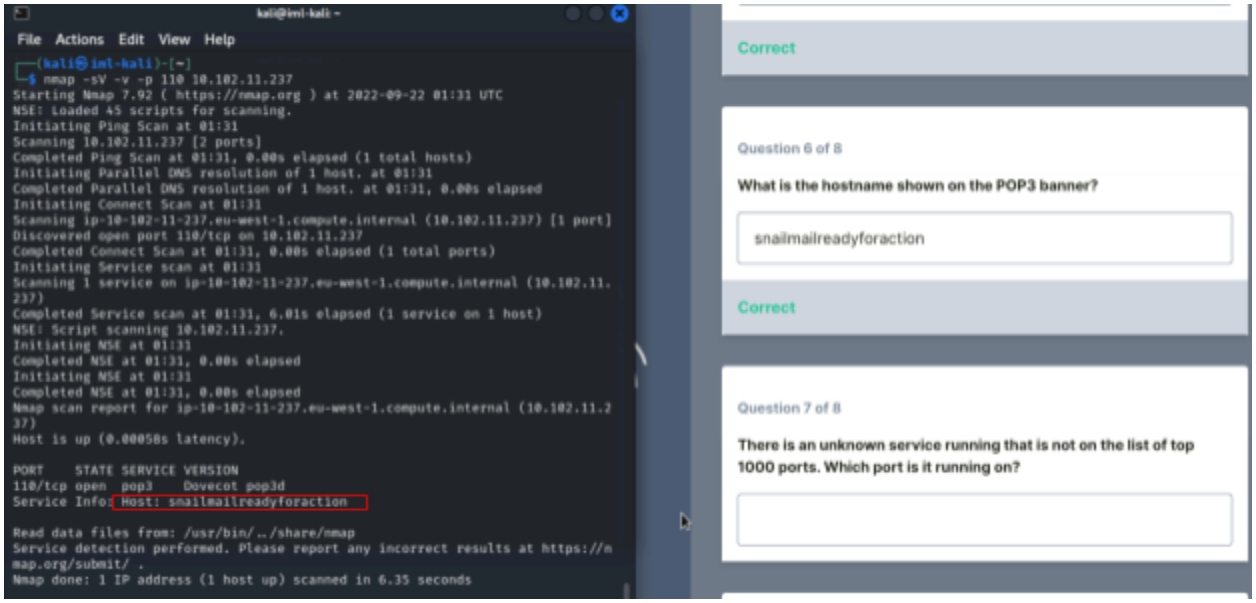
*Question 4:* The -oG option gives grepable output that lists the ports scanned.



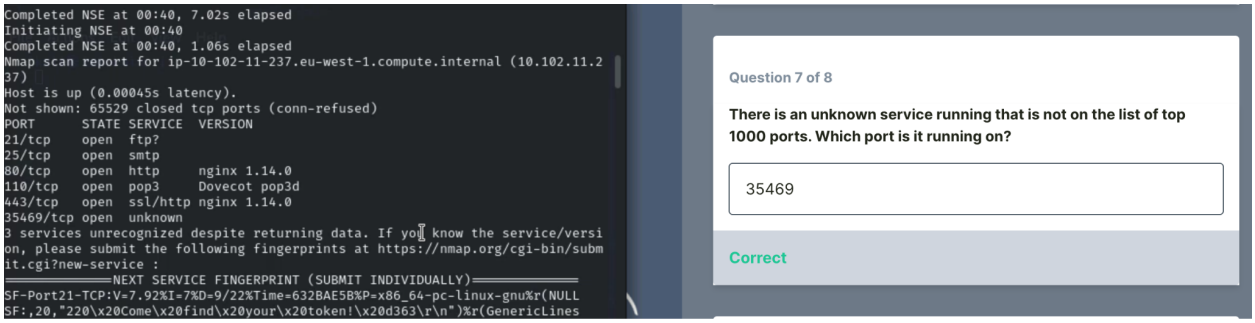

*Question 5:* The option -sS is called a half-open TCP scan because a full TCP connection is not opened.



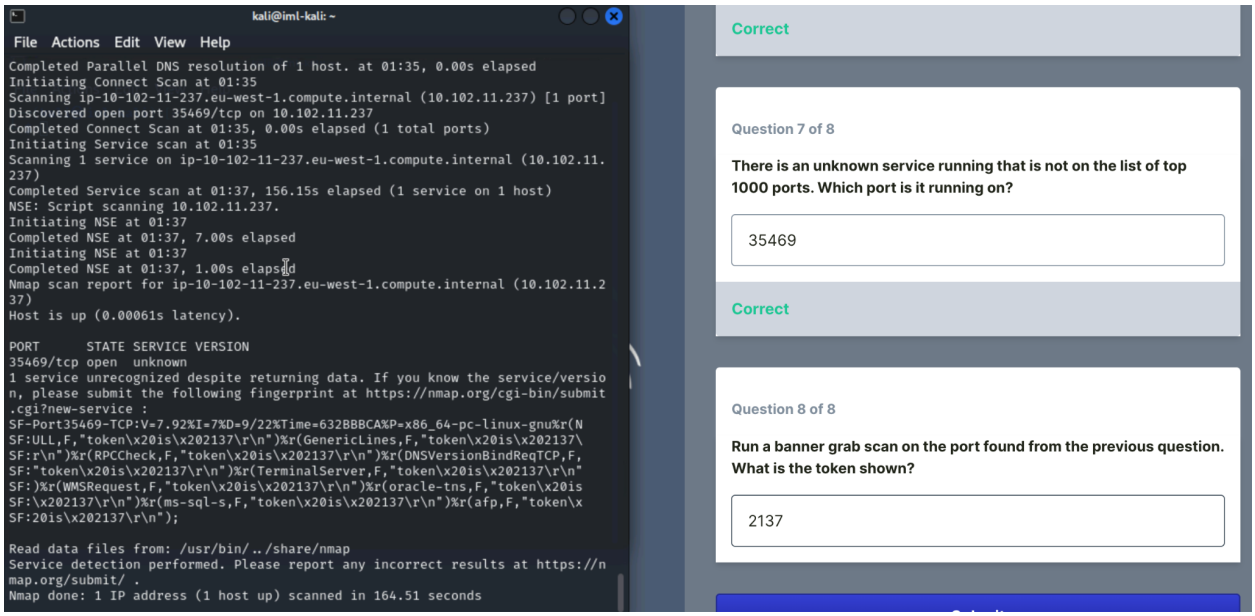

*Question 6:* Doing a banner grab on just port 110, for the pop3 service shows that the host is named snailmailreadyforaction.



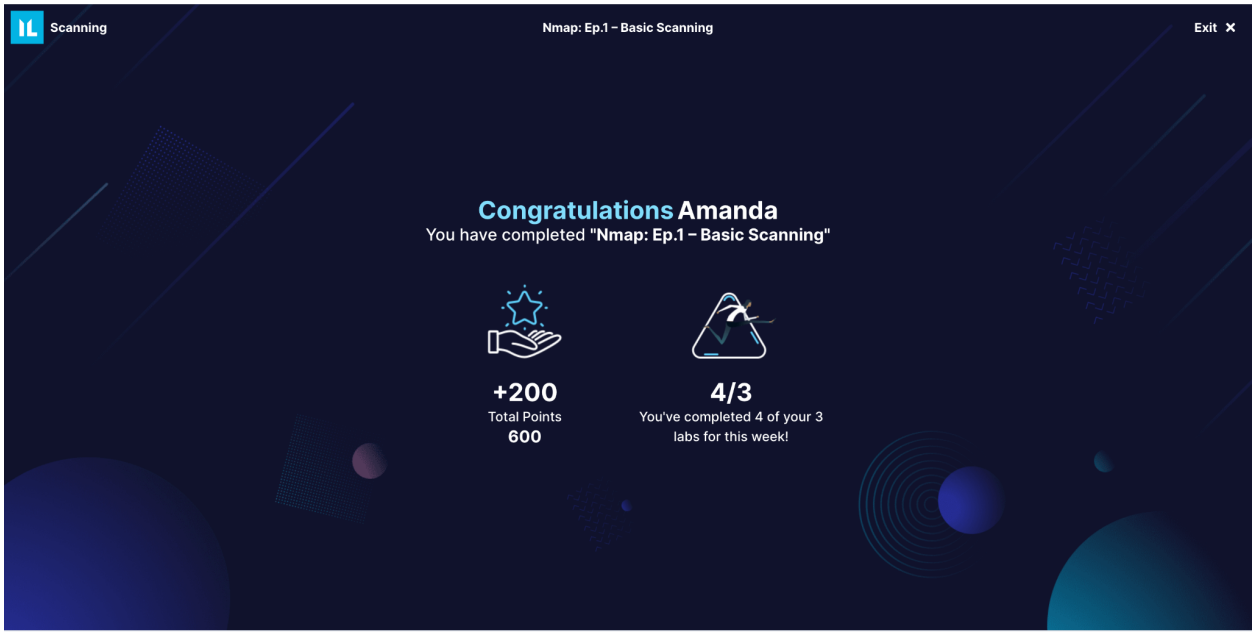
*Question 7:* From the prior banner grab, one of the open ports was on 35469, with a service called unknown.




*Question 8:* The banner grab ran on the aforementioned port, using the command, nmap -sV -v -p 35469 10.120.11.237 returned its fingerprint and the token as 2137.



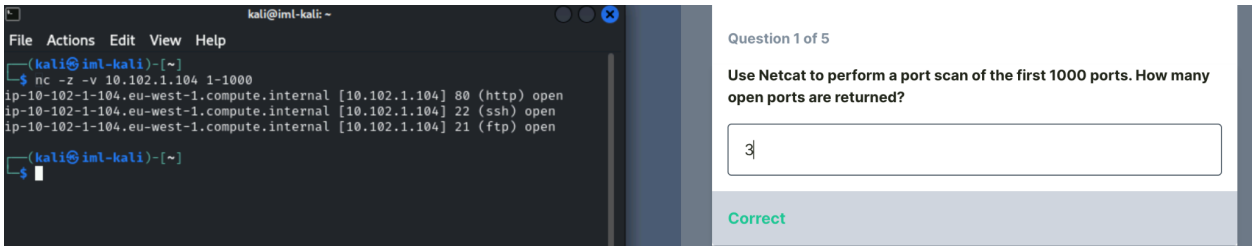
*Result:*




Next Lab
Banner Grabbing

**Network Scanning**

*Question 1:* I performed a port scan by specifying the option -z, and giving the target IP along with the range of 1-1000 ports in the command to find that 3 open ports were returned.

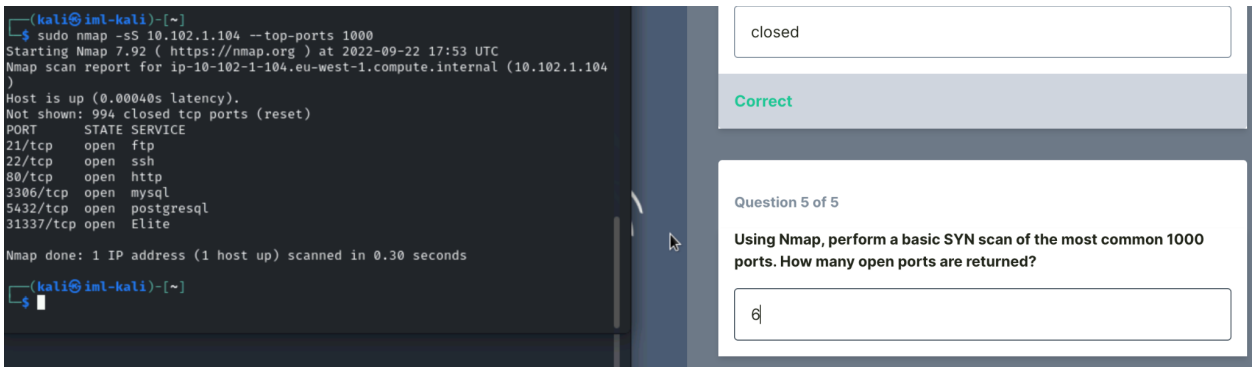



*Question 2:* To do a port scan on just one port, instead of providing a range I provided the specific port. The service running on the port was returned as postgresql.

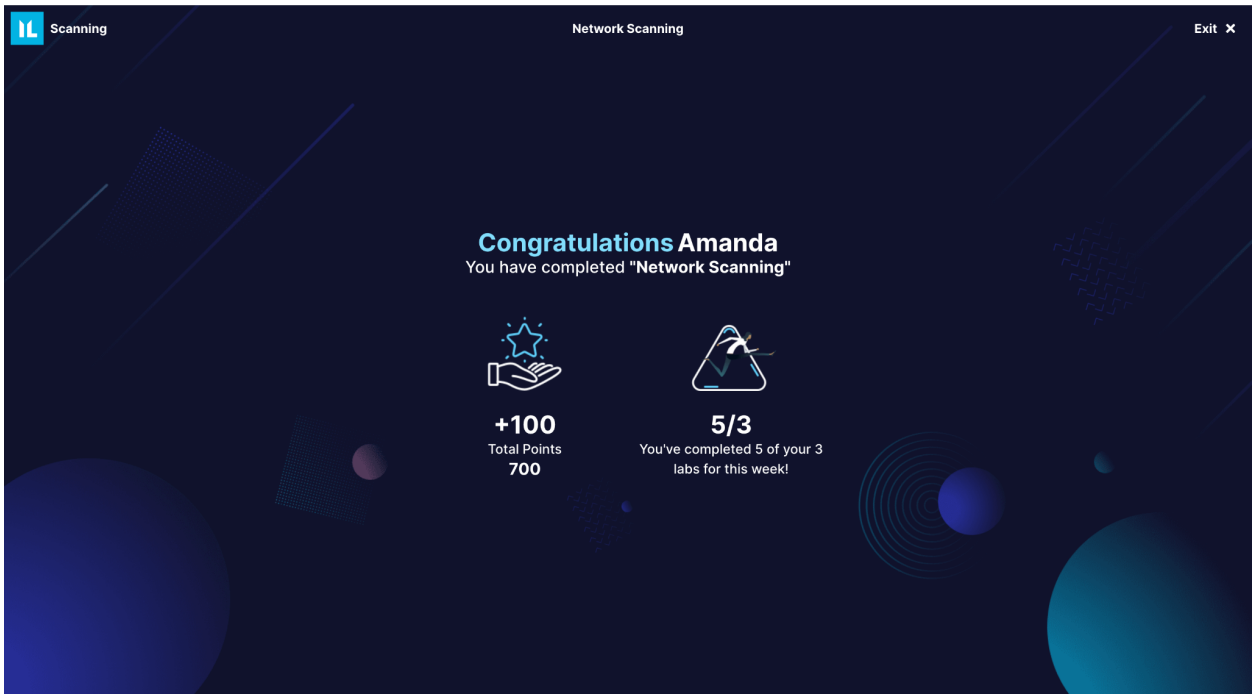

*Question 3:* Doing the same process as from question 2, instead of seeing a service, a connection refused message was returned.


*Question 4:* To do a port scan with Nmap, I used the option -sS which provides a half TCP SYN scan, and I specified the port 92. The state of the port was closed.

*Question 5:* The same SYN scan was done for question 5, but instead of specifying one specific port, I used the option –top-ports to scan the top 1000 ports.




*Result:*




**Writeup**

There are a multitude of tools that can be used to analyze the traffic on a network. To get details on packets, we used Wireshark which provided a user-friendly GUI and filter system to narrow down on exchanges between source and destination. Specifically, I learned how to export a packet as a png file to view its content, which could be used to exploit weaknesses. Similarly, we used tcpdump to analyze packets via the command line, because there was no GUI, I had to filter my scans more technically, following the options in the guide for tcpdump. Further, Nmap

was used to single in on ports and their state. I was able to determine which ports were open in UDP or TCP, and ran a banner scan where I learned about a service print for unrecognized services. Finally, NetCat was used to port scan to identify services and connection messages.