Name: Disha Sheshappa
Net ID: ds7615
N number: N18965487

Intro to wireshark :

a) What is the difference between resolved and unresolved ports on the Wireshark display setup?

Answer: Resolved ports display the name of the well-known service that runs on that port, whereas unresolved ports just display the number.
Explanation: Wireshark resolved ports reveal the service or application linked with a port. Wireshark resolves port 80 packets to "http," indicating HTTP communication. This simplifies network traffic analysis service identification. Only the port number appears in Unresolved Ports.

Wireshark displays unresolved ports as numeric port numbers without trying to convert them into service names. This is handy for seeing port numbers, particularly for non-standard services or network traffic analysis.

In conclusion, resolved ports make it easier to identify services connected with certain ports, whereas unresolved ports give a raw representation of port numbers for more deep study or less popular services.

b) What is the correct syntax to use on Wireshark for showing only SMTP and ICMP traffic?

Answer: tcp.port eq 25 or icmp

Explanation: The filter phrase tcp.port eq 25 instructs the system to record any communication when the TCP port is equal to 25. The Simple Mail Transfer Protocol (SMTP), which is used to transmit email, has a well-known port number of 25.

The logical operator "or" joins filter expressions together. In this instance, it indicates that the traffic should satisfy one of the given requirements.

The filter expression icmp records traffic for the Internet Control Message Protocol (ICMP). ICMP is used for a number of network-related tasks, such as reporting and diagnosing network errors.

c) sing wireshark_setup.pcapng, filter the packets to view only HTTP requests. What is the source IP address shown on the last packet?

Answer: 172.21.2.217

Explanation:
Applying display filter “http.request” in Wireshark will filter all the packets with http protocol.

In the packet details section of the last packet in the list will have its source IP address displayed. Here, it is "172.21.2.217."

d) Within that same packet, what is the time shown? Your answer must be in YYYY-MM-DD HH:MM:SS format adjusted for UTC.

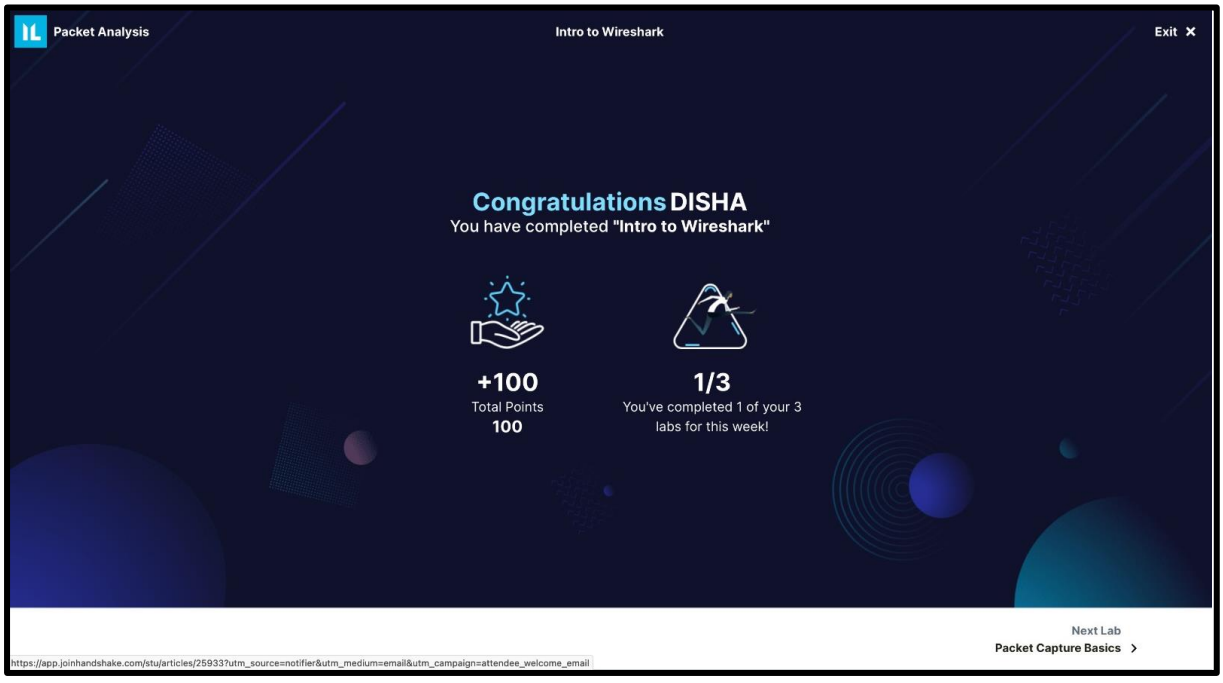
Answer: 2017-12-12 13:04:10
Explanation:
After getting in to the details of the last packet, the time stamp can be found in the Frame section under arrival time.

e) What is the destination IP address of the last packet?

Answer: 34.232.90.203
Explanation:
In the last packet we can find the destination IP displayed in the destination column.

Learnings:

- The detailed look into network traffic is made easier with the help of Wireshark, a network analysis tool. It differentiates resolved ports from unresolved ports by showing well-known service names to make the identification of network activity easier. Unresolved ports, on the other hand, do not display these names.
- Users may add filters to isolate certain kinds of traffic, such as HTTP requests, which enables more targeted analysis to be performed. In order to facilitate accurate temporal analysis of network activities, Wireshark logs exact timestamps in the UTC time format.
- In addition to this, it discloses the source and destination IP addresses, which gives information on the flow of data. Logical operators such as "or" increase the capabilities of filters, particularly in situations involving complicated networks.
- In general, the characteristics that Wireshark has make it an indispensable tool for network experts, since it enables efficient monitoring, troubleshooting, and security measures for networks.



Packet Capture Basics:

a) What is the server name sought in the first DNS request that is issued by the client?

Answer: www.bing.com
Explanation:
When we filter out all DNS requests using “dns.request” display filter. The server name can be seen in Domain name section under queries.

b) What is the first IP address returned in the DNS response for the domain in Q1?

Answer: 204.79.197.200
Explanation:
After getting into packets detail section we can find the destination IP displayed in the destination column.

c) What is the browser user agent string that issued the search request?

Answer: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.7.1
Explanation:
In the packet detail section user agent value can be found under Hypertext Transfer Protocol section.

d) What web server engine is running the website?

Answer: Microsoft ISS 18.5/
Explanation:
Apply display filter “http.response” go to detail section of the first packet, Under Hypertext Transfer protocol section server engine can be found.

e) When exporting HTTP content from the capture and looking at 'imgingest-5015644562731850884.png', what is the text that appears on that image?

Answer: Password Hacking
Explanation:
Click on File →Export Objects → HTTP → select 'imgingest-5015644562731850884.png’ and save it to local computer then we can view the image clearly

f) How many different IPv4 conversations are there in this capture file?

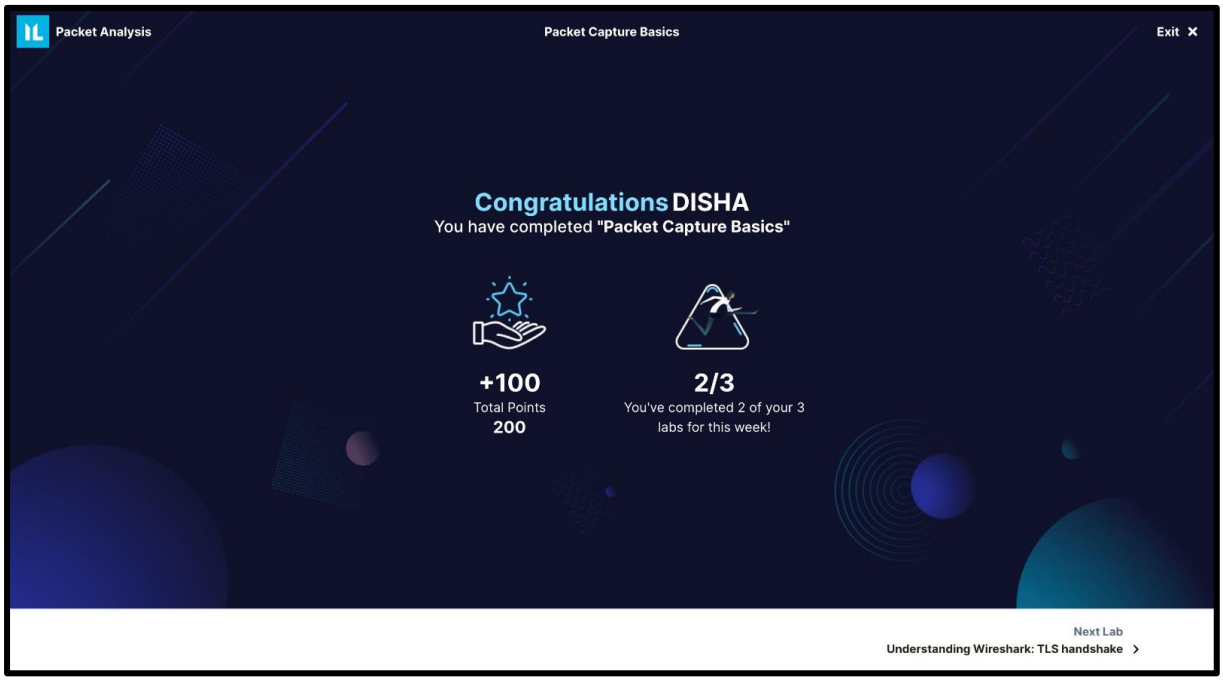
Answer: 89
Explanation:
Go to statistics in the top menu → Conversations → HTTP → go to IPV4 section

g) What was the user searching for on the download.cnet.com website? (Enter your answer as two separate words, e.g., catching fish.)

Answer: Hacking Tools
Explanation:
Apply filter “http.host == download.cnet.com” → open first packet → Answer can be found in the info section of the packet under GET.

Learnings:

- Network capture and analysis are crucial for network security and user behaviour analysis. This aids administrators, security specialists, and researchers. These insights empower you to maximise network performance and security with educated choices.
- We ask DNS for the names of the servers we wish to connect to. DNS responses provide us the IP addresses of those servers so we may talk with them. Websites use the User-Agent string in HTTP requests to improve content by giving browser and operating system information.
- HTTP response headers reveal the web server engine. Developers and security experts benefit from this knowledge. HTTP content, such photos, may provide significant details.
- The network analysis shows 89 IPv4 talks in this clip, demonstrating the complexity of network communication. The data demonstrates that gadgets interact in many ways, producing a diversified and dynamic ecosystem.



Tcpdump:

a) Which option can you pass to tcpdump to write captured packets out to a file?

Answer: -W
Explanation:
With the -W method, users can write the recorded or filtered packets to a file that they choose. "tcpdump <interface> -W name.pcap" is an example of this. All the packets that were recorded on the interface are saved to a file called "name.pcap."

b) Using tcpdump, list all the available interfaces. What number is `nflog` listed as?

Answer: 5
Explanation: We use the command "-D" (syntax: tcpdump -D) to show all the interfaces that are available. This will show a list of all the possible ports, each with a serial number before it. The 'nflog' interface is in the 5th row of the interfaces that are shown.

c) Which option can be passed to tcpdump to display the ASCII and hex representation of the packet contents?

Answer: -X
Explanation: We use the -X option to show the packet parts in both ASCII and hex format. "tcpdump <interface/file name> -X" is the syntax for this.
The <> can be changed to the name of the interface or the file that contains the recorded packets. This is where it shows the results in both ASCII and Hex.

d) Using tcpdump, read the packets from tcpdump.pcap and filter packets to include IP address 88.221.88.59 only. What is the time shown on the final packet? (HH:MM:SS)

Answer: 07:32:57
Explanation:
To begin, we need to filter the pcap file with the IP address 88.221.88.59. "tcpdump -r tcpdump.pcap -nn host 88.221.88.59" was used to do this. It shows all the packets with this IP address.
You can find the time in the time part of the last packet of the filtered list.

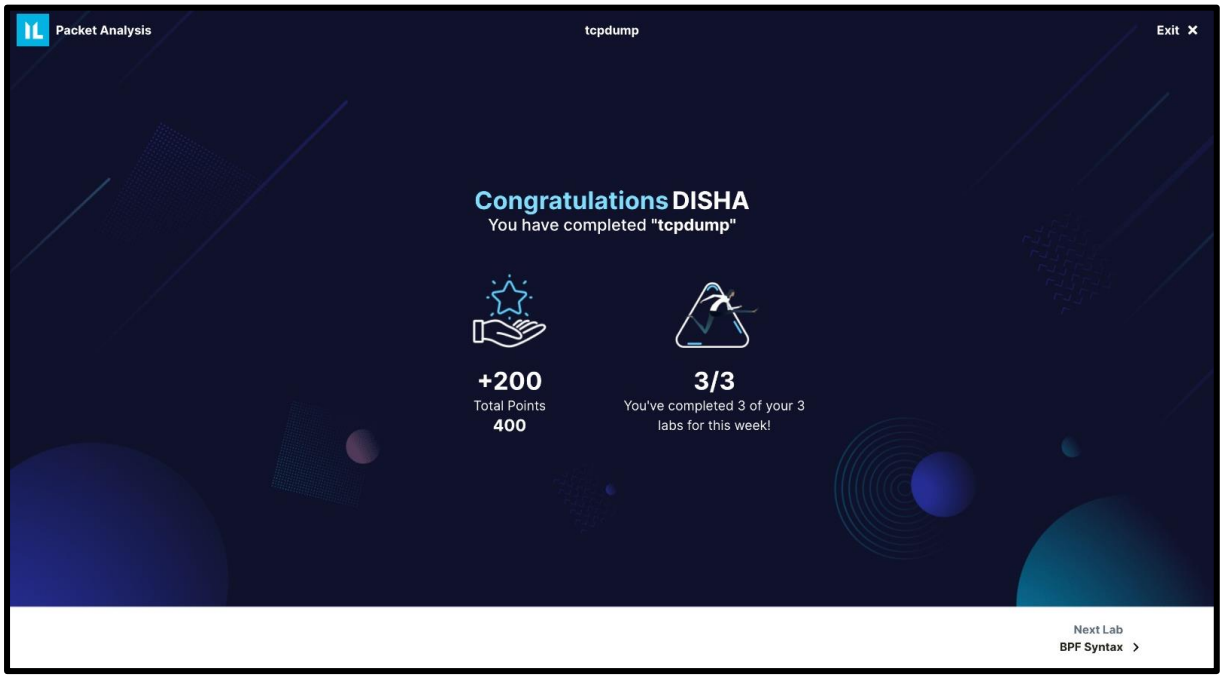
e) Using tcpdump, read the packets from tcpdump.pcap and filter packets to include IP address 184.107.41.72 and port 80 only. Write these packets to a new file and MD5sum that file. What is the MD5sum shown?

Answer: 8e4b92724d9034a49cf10f6b147ac482
Explanation:
To begin, we need to filter out the packets by using the command "tcpdump -r tcpdump.pcap -nn "host 184.107.41.72 and port 80" -w new.pcap." This command will filter the packets with a certain IP and port and write them to a new file named new.pcap.
Now, in order to get the md5 checksum of that file, we will use the command "md5sum new_packets.pcap."
The value is '8e4b92724d9034a49cf10f6b147ac482'.

Learnings:

- Tcpdump is a really useful tool for analysing network packets. It can help you gain a better understanding of how network traffic is collected and analysed.

- We are now able to display packet contents in both ASCII and hex forms, write recorded packets to files, list accessible interfaces, display packet contents in both formats, and efficiently filter traffic based on various parameters like IP addresses and ports.
- Also, we recognise the importance of MD5 checksums in preserving the integrity of the recorded packet files. Network administrators and security experts need these abilities in order to effectively diagnose and protect network infrastructure.
- Tcpdump, along with other similar programmes, plays a crucial role in maintaining the reliability and security of networks. Therefore, it is a crucial tool in the field of network administration and safeguarding data.



Wireshark display filters:

a) From the PCAP provided, apply a filter which displays all SMTP traffic containing the text "Subject: ". What is the first name of the recipient of that email?

Answer: Sarah
Explanation:
We can use the command <'smtp contains "Subject:" > to filter all SMTP data that has the string "Subject:" in it.
Inside the SMTP part of the first file, we can see that the recipient's email address is Sarah.Wendt@hapcor.com.

b) From the PCAP provided, apply a filter which displays all SMTP response traffic matching the text ".co.uk". What is the frame number of this packet?

Answer: 9932
Explanation:
The 'smtp.response contains ".co.uk"' filter will get all SMTP response packets that have the text '.co.uk' in them.
The frame number for this message is 9932.

c) From the PCAP provided, apply a filter which displays all packets from UDP source ports 53, 59015, and 63518. How many packets are then displayed?

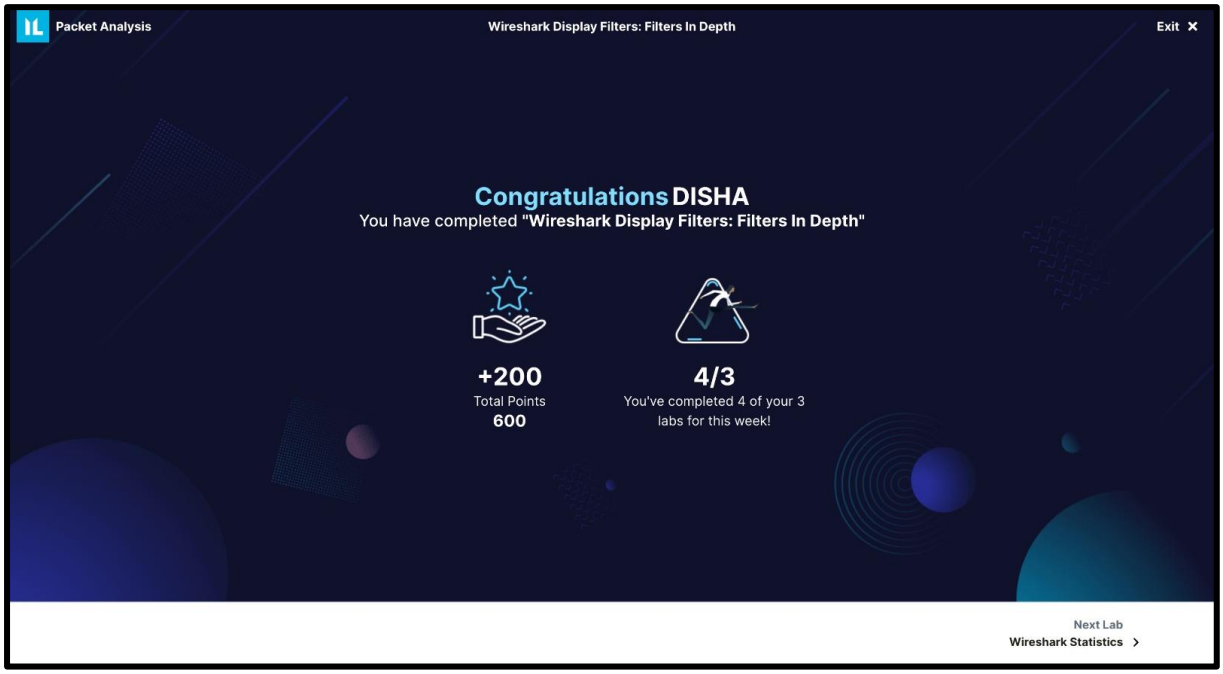
Answer: 60
Explanation:
with the help of filter "udp.srcport == {53 59015 63518}" which will get all UDP packets with port 53, 59015, or 63518.
The total number of packets are shown in the bottom right area. In this case, it is 60.

d) Take the following slice expression (frame[-4:4] == 0.1.2.3). At which offset does the slice begin?

Answer: -4
Explanation:
Frame[-4:4] == 0.1.2.3 is the given slice statement. The slice starts at the -4 on the left side of the colon (:).
It starts 4 bytes before the end of the "frame" and has the last 4 bytes of the frame.

e) Take the following slice expression (frame[:4] == 0.1.2.3). At which offset does the slice begin?

Answer: 0
Explanation:
When we write the slice statement frame[:4] == 0.1.2.3, the :4 that is located to the right of the colon (:) indicates where the slice comes to an end.
Due to the fact that there is no starting separation before the colon, the slice begins at the very beginning of the "frame."
In this instance, the beginning of the slice is located at offset 0.



Learnings:

- Recording and studying network data helps monitor, troubleshoot, and maintain computer networks. Getting network device data is part of the procedure. After sorting, data is examined.

- Filters locate and highlight interesting parts. Filters can be used to show SMTP data with certain content, UDP packets from specified source ports can be tallied, and SMTP answers matching certain patterns are detected.

- Frame splitting is a good way to examine certain packet portions. It's crucial for deep investigation. Additionally, network professionals must consider the larger picture. They must examine network issues, odd activity, and how individuals communicate. In general, PCAP files are valuable for investigating past events.

- They function well with various network research tools, therefore many professionals utilise them. To analyse a network, proper filtering and data analysis are essential. This simplifies network security and operation.

BPF Syntax:

a) What does BPF stand for?

Answer: Berkeley Packet Filter
Explanation: The full form for BPF is “Berkeley Packet Filter”.

b) wlan.addr == c5:52:7e:95:6:8d && wlan.fc.type_subtype == 0x02. How many primitives are in this expression?

Answer: 2
Explanation: The expression wlan.addr == c5:52:7e:95:6:8d && wlan.fc.type_subtype == 0x02 consists of two primitives.
The first is a wlan address with the following format: c5:52:7e:95:6:8d, which looks for packets that have the source or destination MAC address that was provided. wlan.fc.type_subtype == 0x02 is another condition that must be met, and it ensures that the wlan frame control header has the value 0x02.

c) Apply a filter to display all packets on port 80 with the source IP of 10.0.50.227. What is the length of the second GET request?

Answer: 385
Explanation: We use the command "tcpdump -r bpf-pcap.pcapng host 10.0.50.227 and port 80" to filter the packets, which displays all of the packets that have the IP address 10.0.50.227 and the port number 80.
Using this list, we were able to determine the length of the second GET request, which is 385 characters less than the column length.

d) Apply a filter to display all UDP packets on port 57190. What is the timestamp of the final packet?

Answer: 11:54:43

Explanation: To filter the file we use "tcpdump -r bpf-pcap.pcapng udp port 57190," which will display all of the udp packets that are passing via port 57190.
Due to the fact that it is the first field in the filtered list, we are able to locate the timestamp of the last packet in the starting position. This information is presented in the format of HH:MM:SS. In this particular instance, the time is 11:54:43.

e) Apply a filter which reads all traffic apart from DNS and TCP, and output this to a file. What is the md5sum of this file?

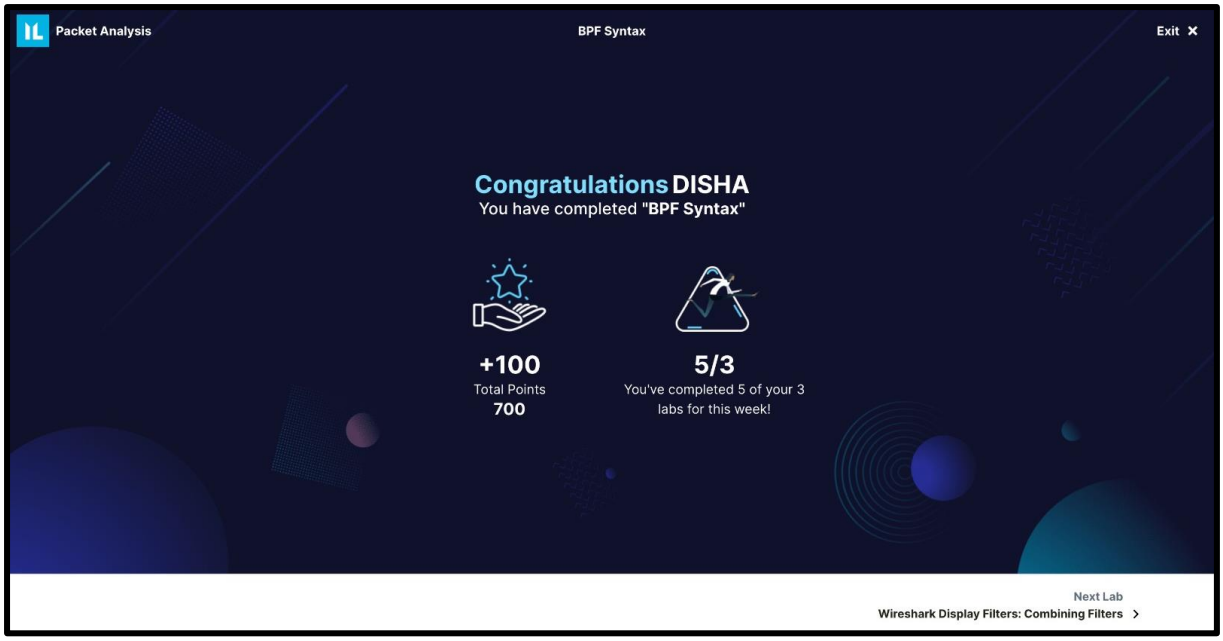
Answer: b942d25b012745422c1719ac26419da6
Explanation: To do this, run "tcpdump -r bpf-pcap.pcapng -w name.pcap 'not (port 53 or tcp)' " which will get all the messages except DNS and TCP. Port 53 is used here because that's the only way DNS packets can get through. They are saved in a file named "name.pcap" after they have been sorted.
With the command "md5sum name.pcap", we can now use md5 on this file. This will give us the file's MD5 hash, which in this case is "b942d25b012745422c1719ac26419da6".

Learnings:

- Monitoring and recording network traffic helps maintain computer networks secure and working properly. BPF (Berkeley Packet Filter) is crucial because it reliably selects and inspects packets. Different occupations show that BPF statements may have several basic. Each basic sets its own screening parameters. These primitives enable you analyse packets using source addresses, packet kinds, and other factors.

- Good network filtering abilities are essential. The example demonstrated how to filter packets by port and source IP. It helped us determine GET call length. Time stamps on packets let us track network events. We can also use them to monitor packet order.

- Filtering removes protocols and information kinds, producing particular files for analysis. Network researchers may detect issues, study how networks function, and make them safer using filters and BPF expressions. Obtaining and evaluating network data is essential to network management.


Packet Analysis
BPF Syntax
Exit
Congratulations DISHA
You have completed "BPF Syntax"
+100
Total Points
700
5/3
You've completed 5 of your 3 labs for this week!
Next Lab
Wireshark Display Filters: Combining Filters