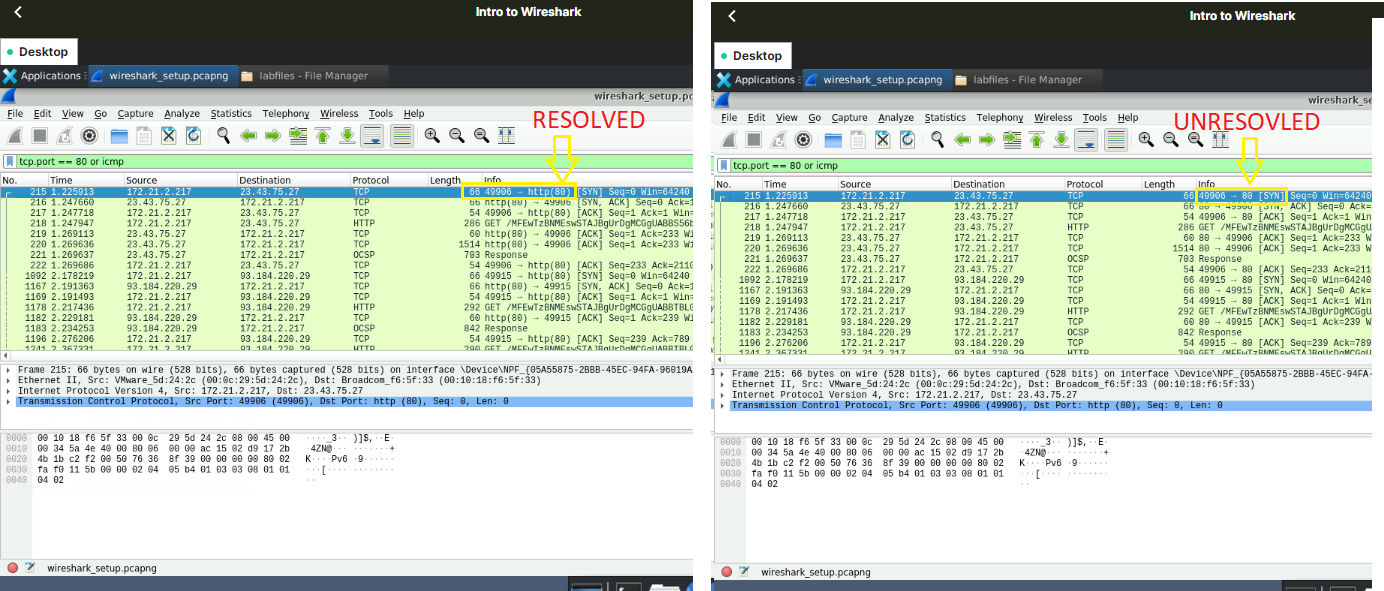
# **LAB 1 Network Capture, Analysis, and Scanning**

## TASK 1: INTRO TO WIRESHARK

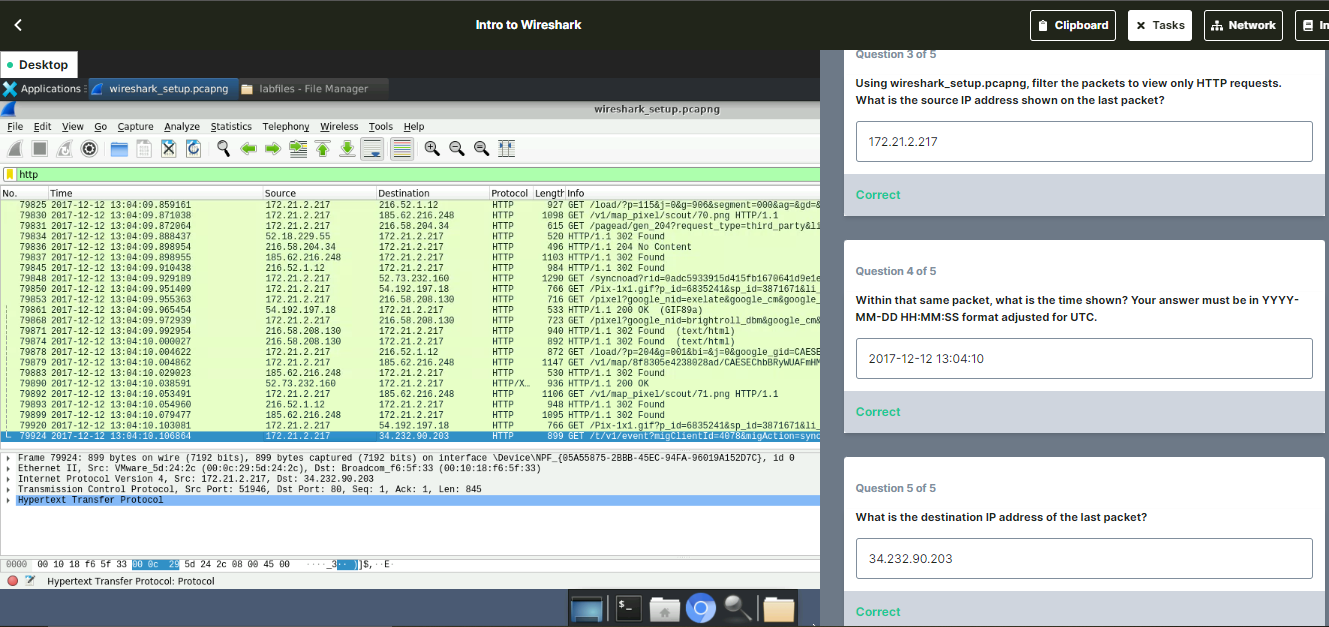
Q1.1) The unresolved port is the raw port number (with just number) whereas resolved port will show information of the port (whether http, sip, etc). There are multiple ways to maintain settings to view resolved and unresolved ports based on version of the wireshark. Here the column for source/destination port is not displayed, so chosing EDIT option -> Name Resolution -> unchecking Resolve Transport addresses option will display port in Info column in raw format, otherwise in resolved format.

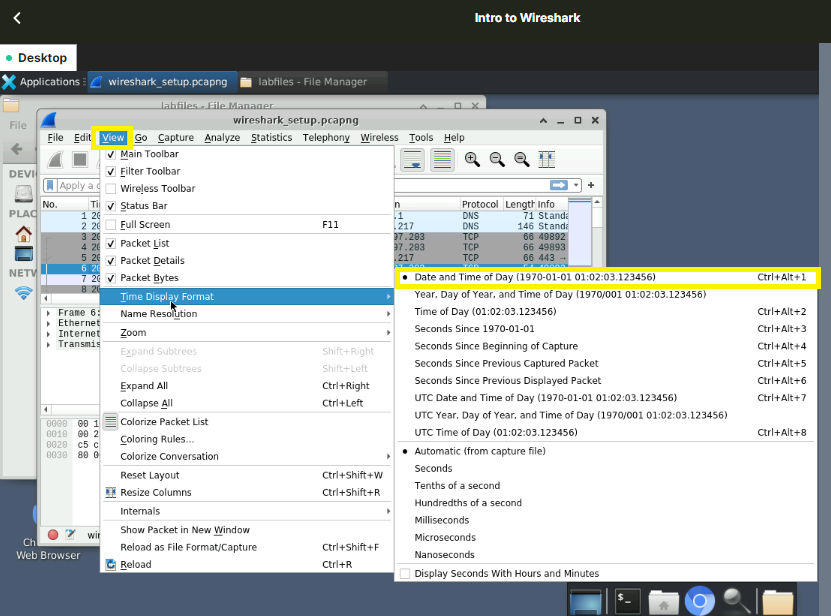


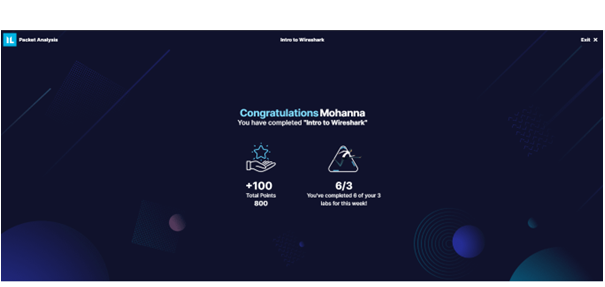
Q1.2)Wireshark is powerful tool for packet analyzer and supports boolean operations can be used to combine and compare the data. Port 25 is standard one used for SMTP communication. So, filtering tcp.port == 25 or icmp traffic will show all packets with source/destination port with port number 25 and ICMP protocol.



Q1.3, 1.4, 1.5) Similarly to get only HTTP communication, just typing ‘http’ in Filter display will display list of packets using HTTP protocol. Corresponding source and destination address can be found in the display columns. There are multiple formats available for time display which is very convenient for users to choose.

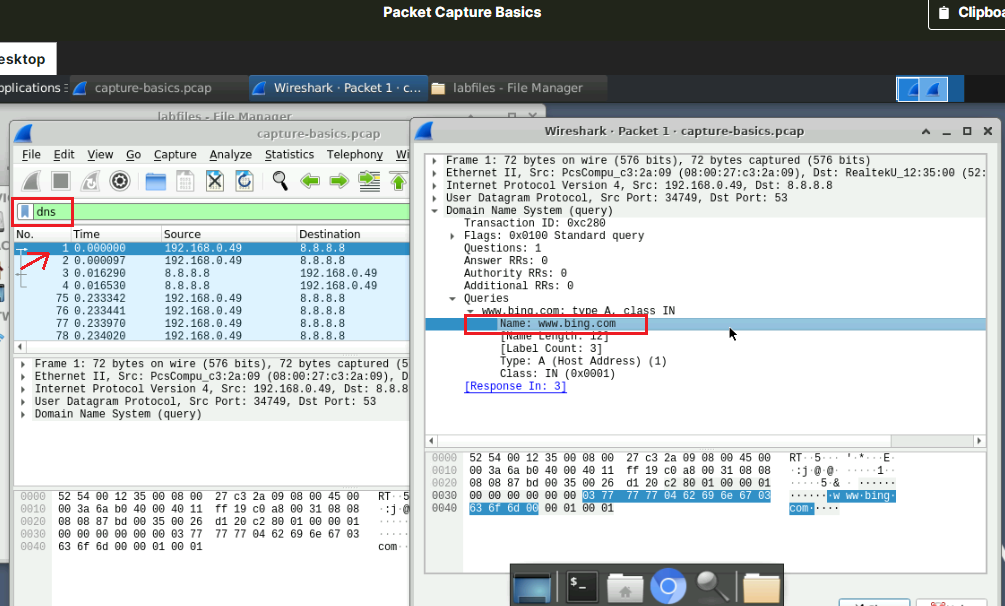






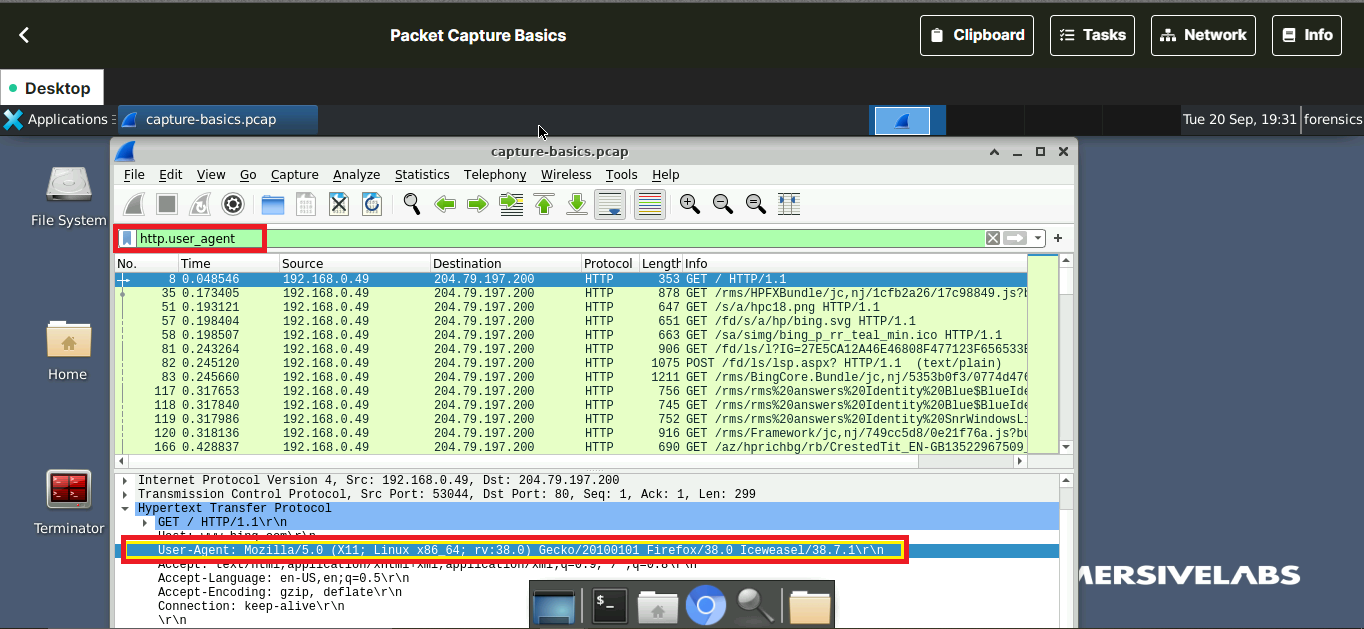
## TASK 2: PACKET CAPTURE BASICS

Q2.1) Double clicking on the first DNS request packet after filtering packets with ‘DNS’ protocol will show the detailed information where the DNS server name can be found under the Queries section

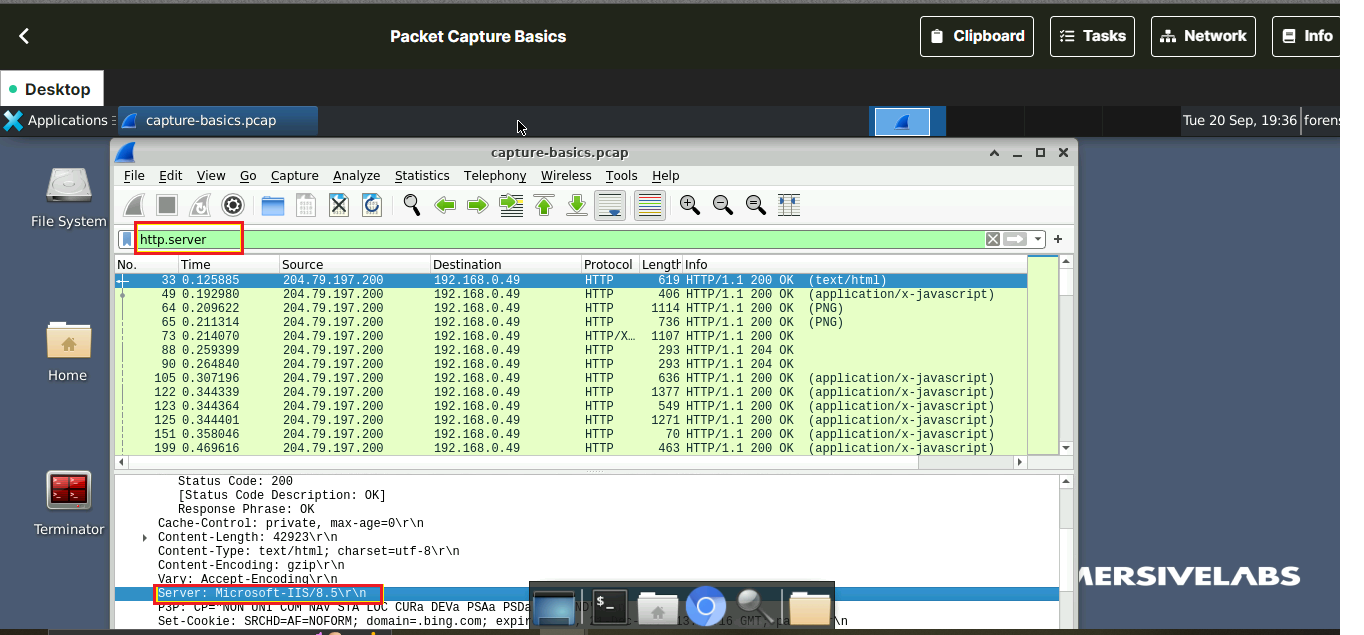


Q2.2) Similarly the detailed information of first DNS packet sent from host 8.8.8.8 to user IP (192.168.0.49) will have the answers including the IP address for the queries by the user

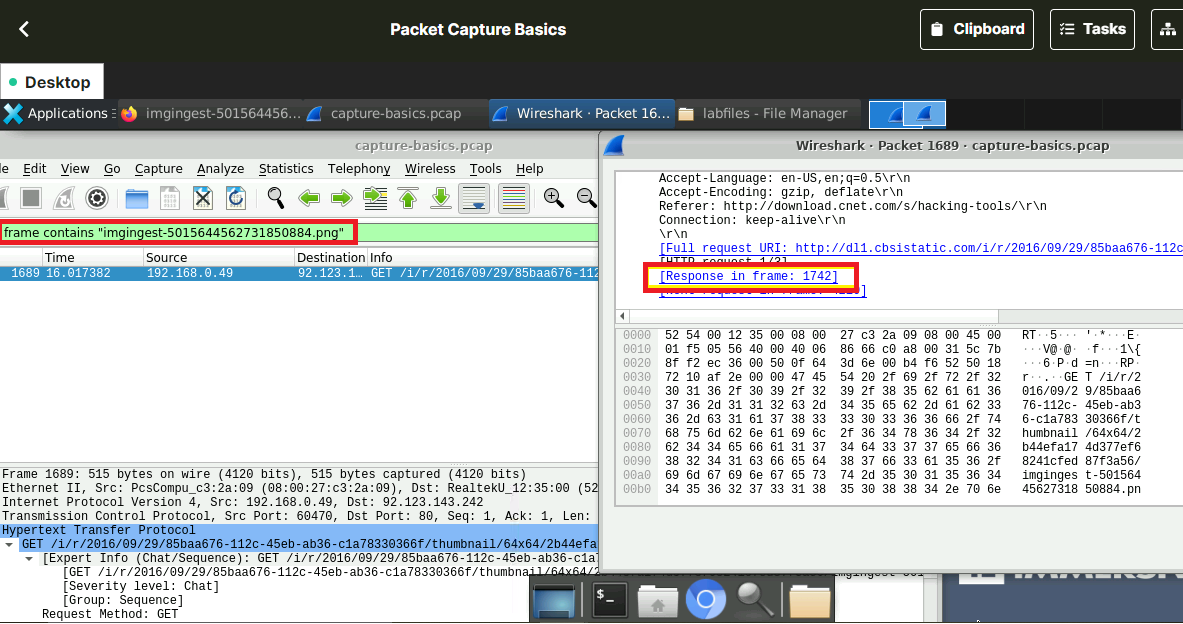


Q2.3) Browser User-Agent string (shortly known as UA) from headers in HTTP traffic specifies which browser, version and the operating system. This information helps in customizing content specific to each browser. Once ‘http.user\_agent ‘packets are filtered, UA can be found in Packet details pane. 

Q2.4) ‘http.server’ is an easy option to filter packets having Server field in HTTP packets.

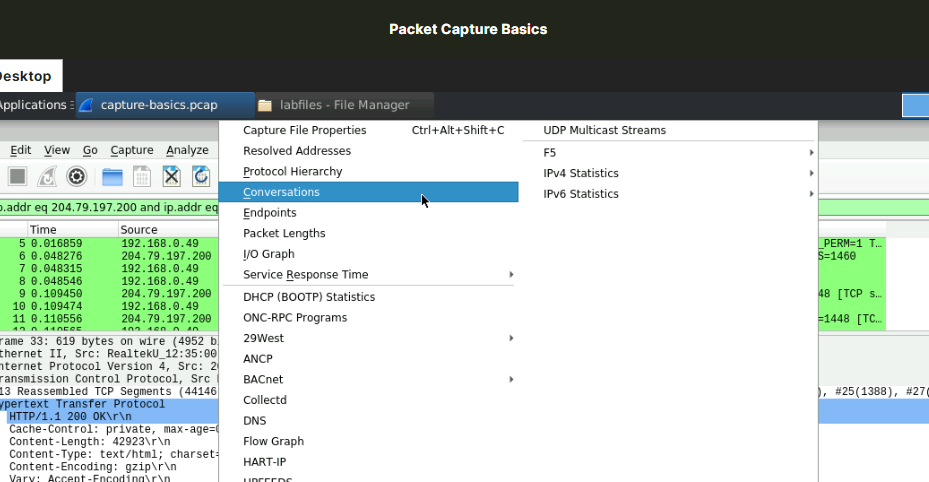


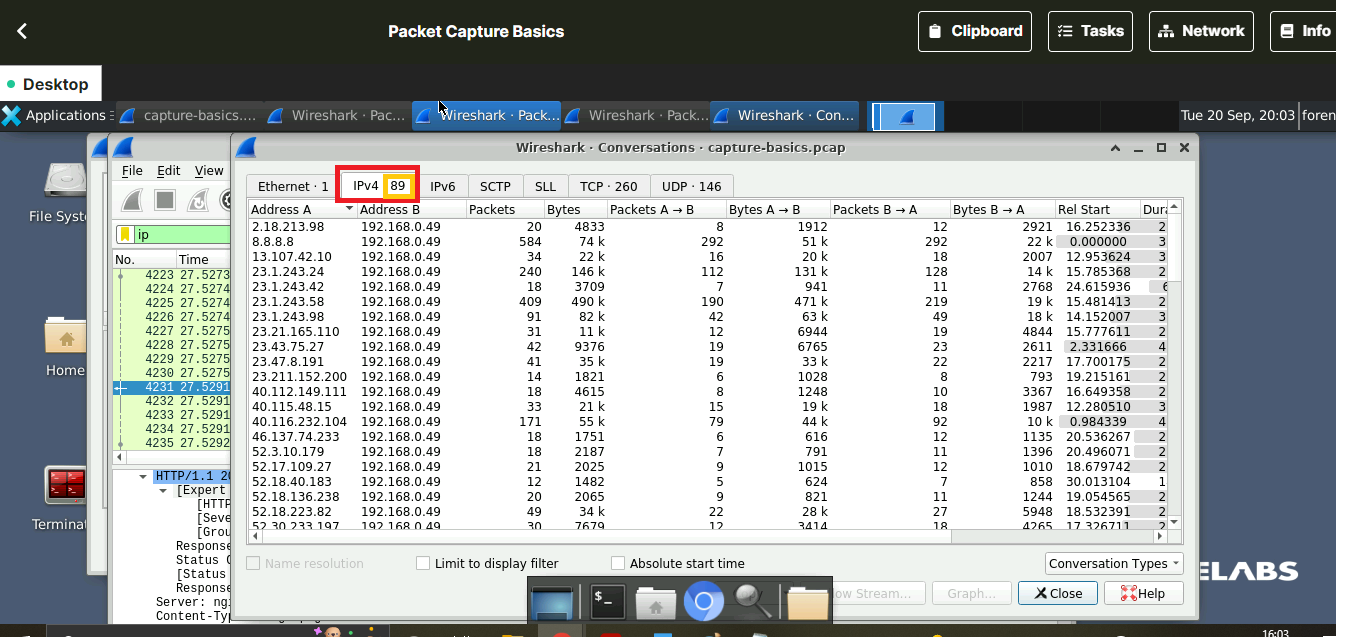
Q2.5) After filtering the request packet containing the file name, the packet details pane has a link to corresponding response frame number. Once this frame number is found, user can navigate to File->Export Objects to downlad the media present in the specific packet number.



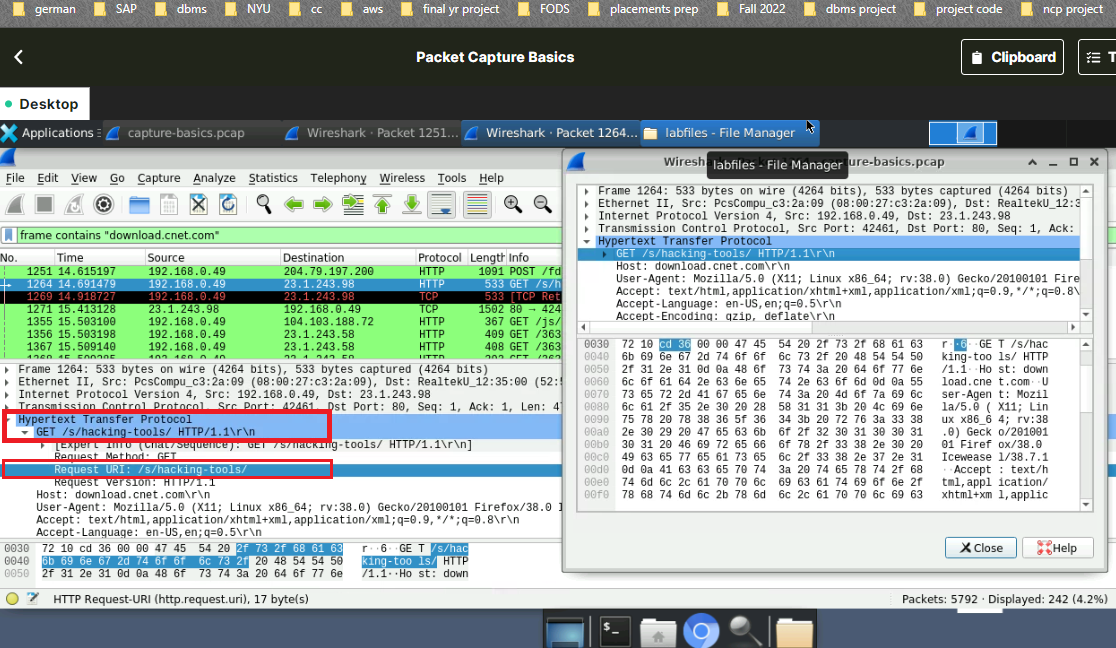


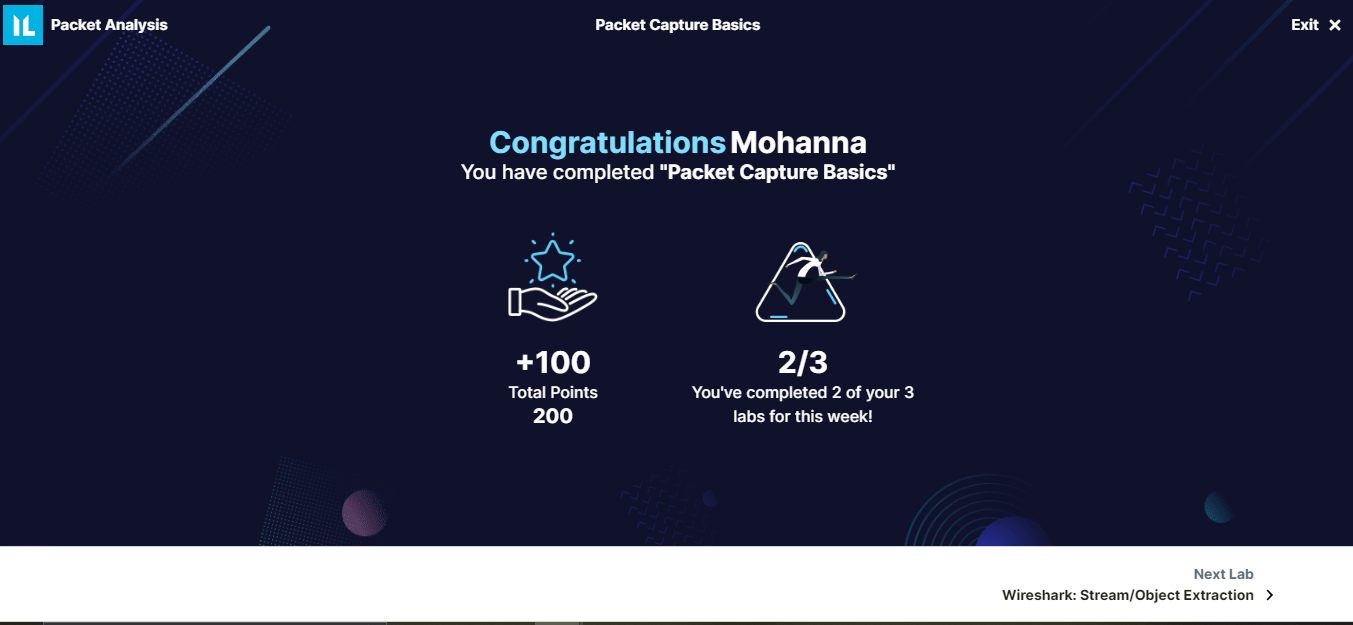
Q2.6) To get the statistics and details of any type of conversation Statistics ->Conversation option provides all the information.





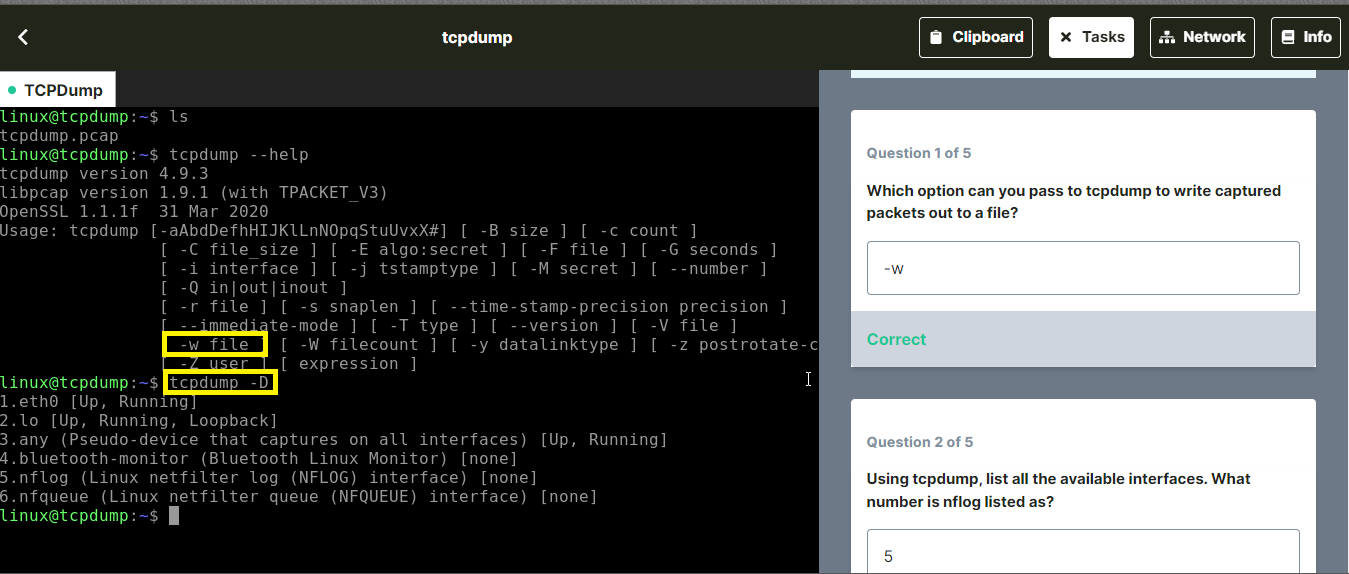
Q2.7) Request URIs of the packet are formatted user search strings that identifies a resource (using name, location, etc) upon which to apply the request. So, here the user searchstring request is ‘hacking-tools’ that can be seen under HTTP-GET parameter.



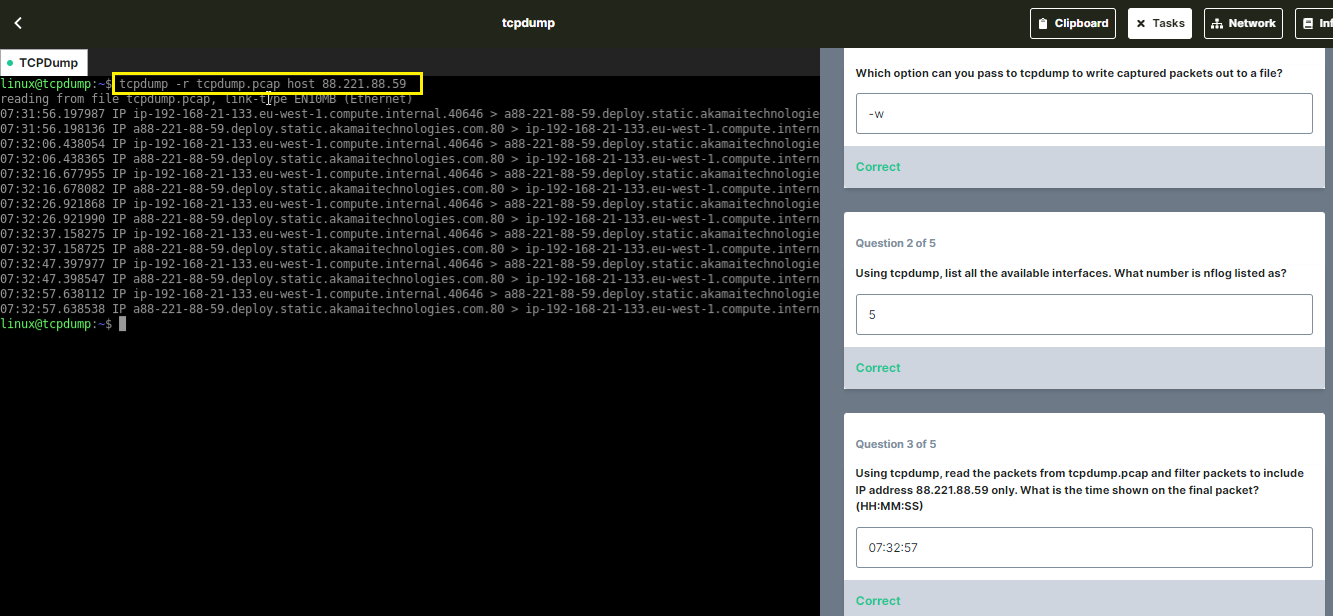


## TASK 3: TCPDUMP

Q3.1, 3.2) TCPDUMP is a command line alternative for wireshark. The command ‘tcpdump –help’ provides list of options that are present. ‘-w’ is option to write captured packets into preferred file and file format and ‘-D’ option identifies all the interfaces of packet capture.

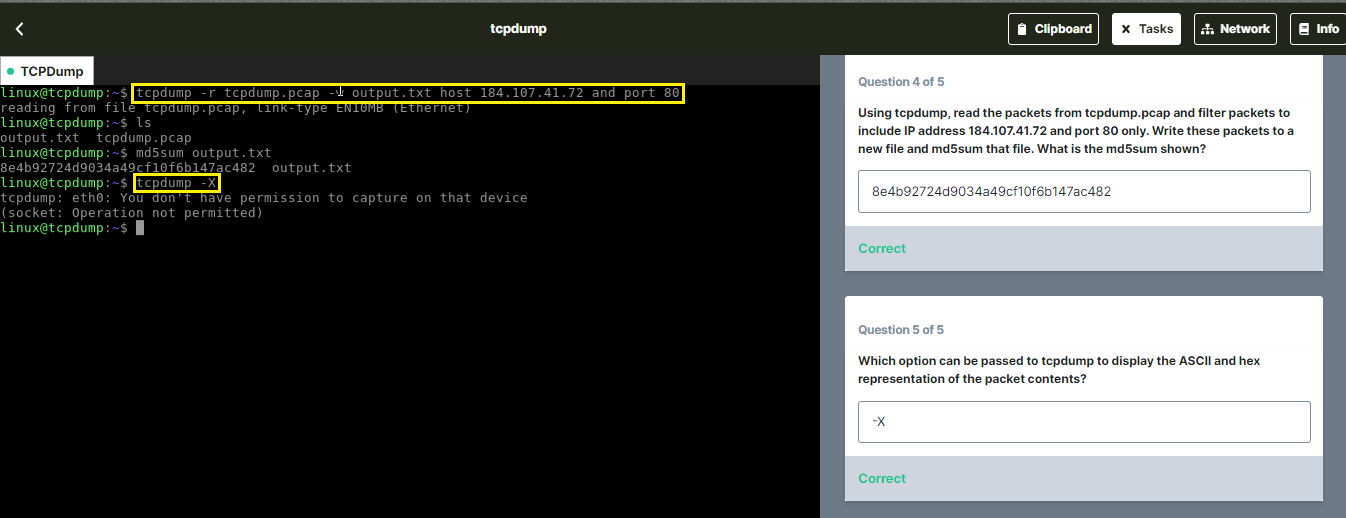


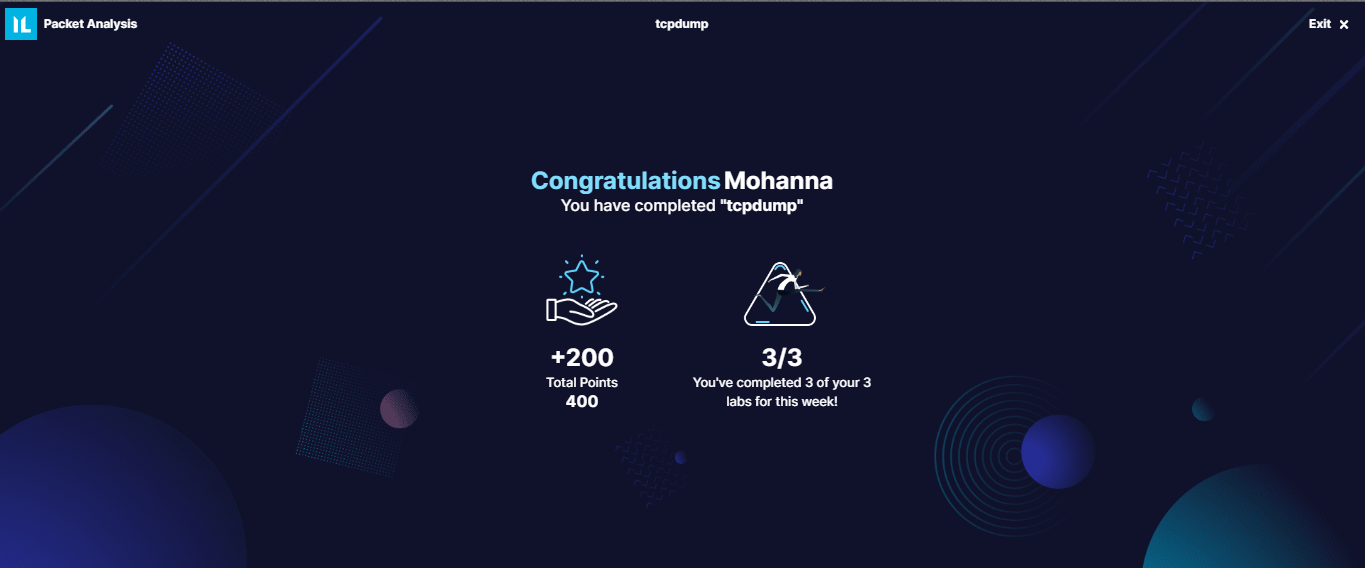
Q3.3) In order to read a \*.pcap file ‘-r’ option can be used. ‘host’ argument followed by the IP address will list out all the packets containing that address along with time stamp as seen below.



Q3.4)Once the .pcap file is read using ‘-r’, it can be written into any text file with filtered packet information. MD5 is 128-bit cryptographic hash and MD5SUM or MD5 checksum computes and verifies data integrity of the file.

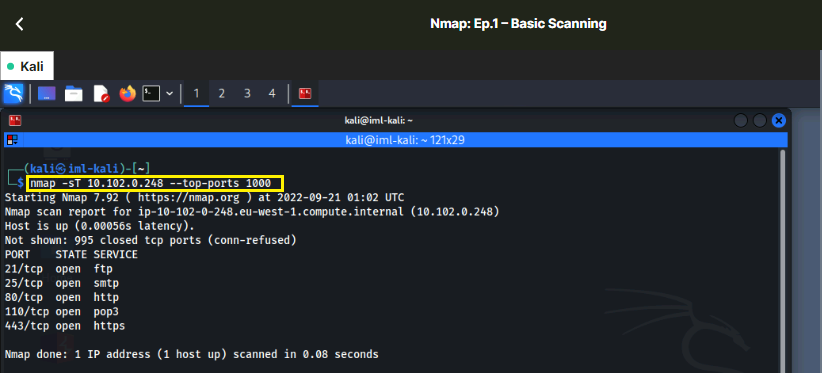
Q3.5) ‘-X’ is used to display ASCII and hex form of the packets. However, tcpdump requires permission to capture raw packets and network interface manipulation which needs to be changed at root-user level



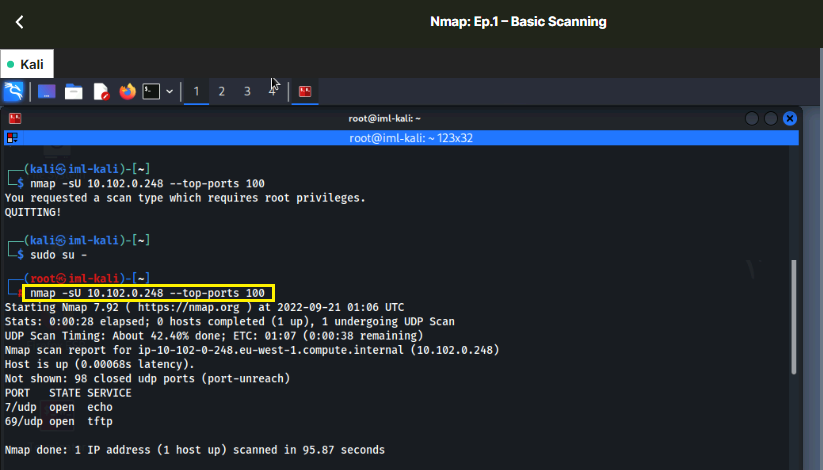


## TASK 4: NMAP: EP1 - BASIC SCANNING

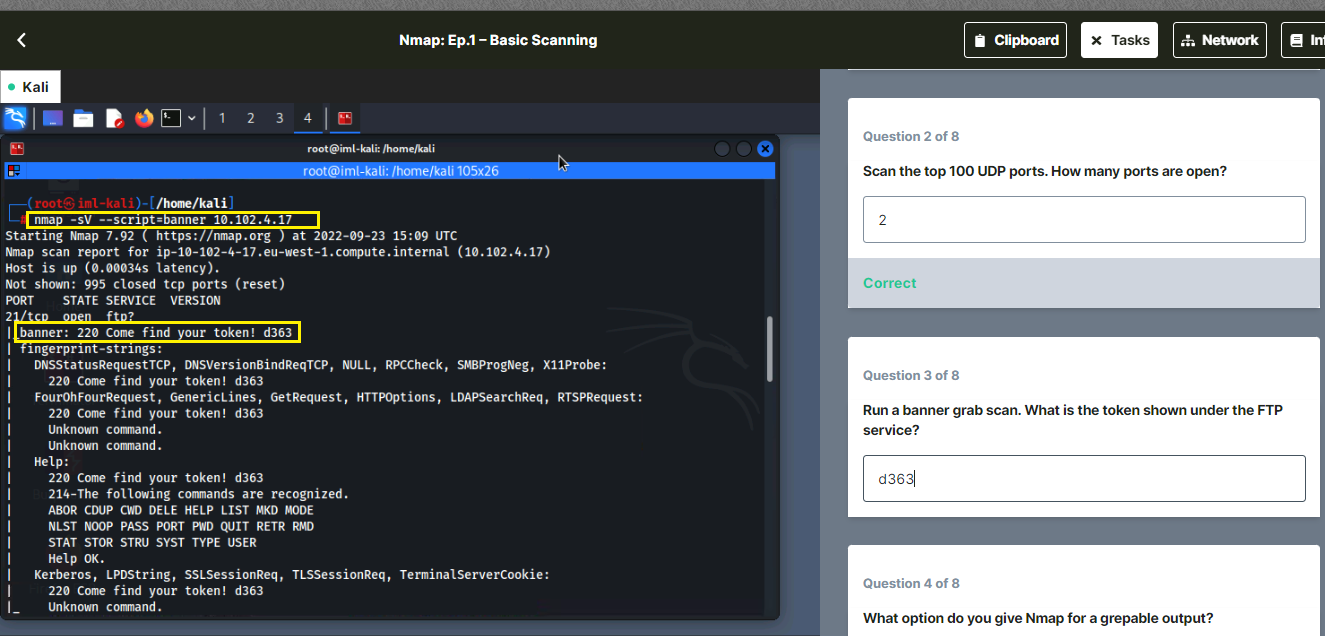
Q4.1) Nmap scan on top ports of specific protocols like TCP can be done using ‘-sT’ and ‘top-ports’



Q4.2) The same command as above doesn’t work for normal user to scan UDP protocols. This is because UDP doesn’t inform if the packet is dropped and applications need to implement error detection or determine dropped data. NMAP needs to access ICMP (which requires root access) to fetch result of packet transmission.

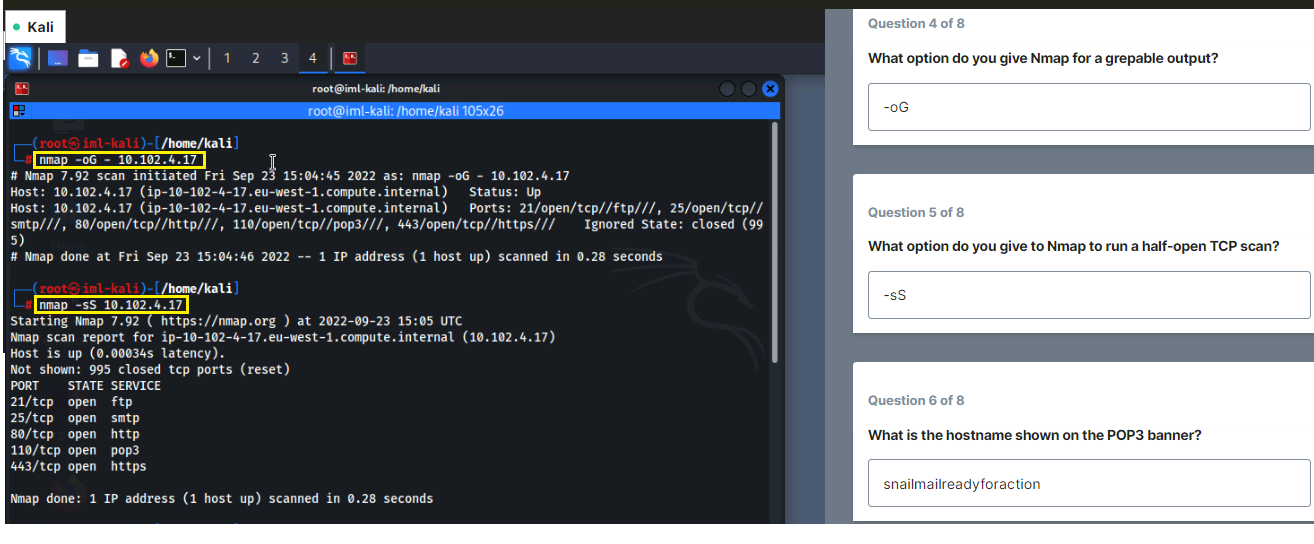


Q4.3) Grab scan is basically used to scan a port if there is any data printed by the service. And the the exact data/token will be printed in banner field for a recognized service. For unrecognized service, service fingerprint will be issued that has hex characters in between.



Q4.4) Nmap provides option to control scan verbosity and write to output files in different format and greppable output is one of them (deprecated) in XML format. ‘oG’ is the option used for this purpose.

Q4.5) Half-open TCP scan (or SYN scan) is fastest and popular scanning of ports that never completes a TCP connection making it unobtrusive. ‘-Ss’ option is used to perform this.

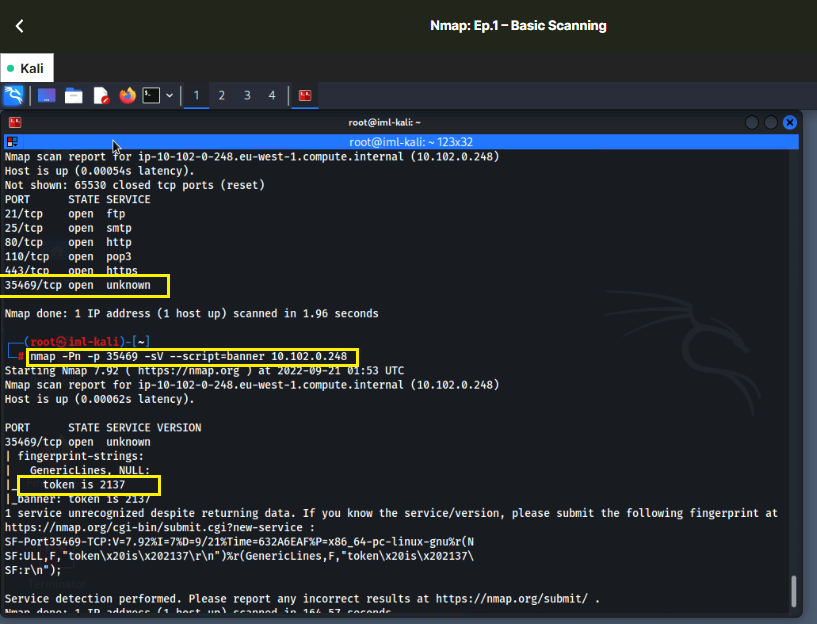


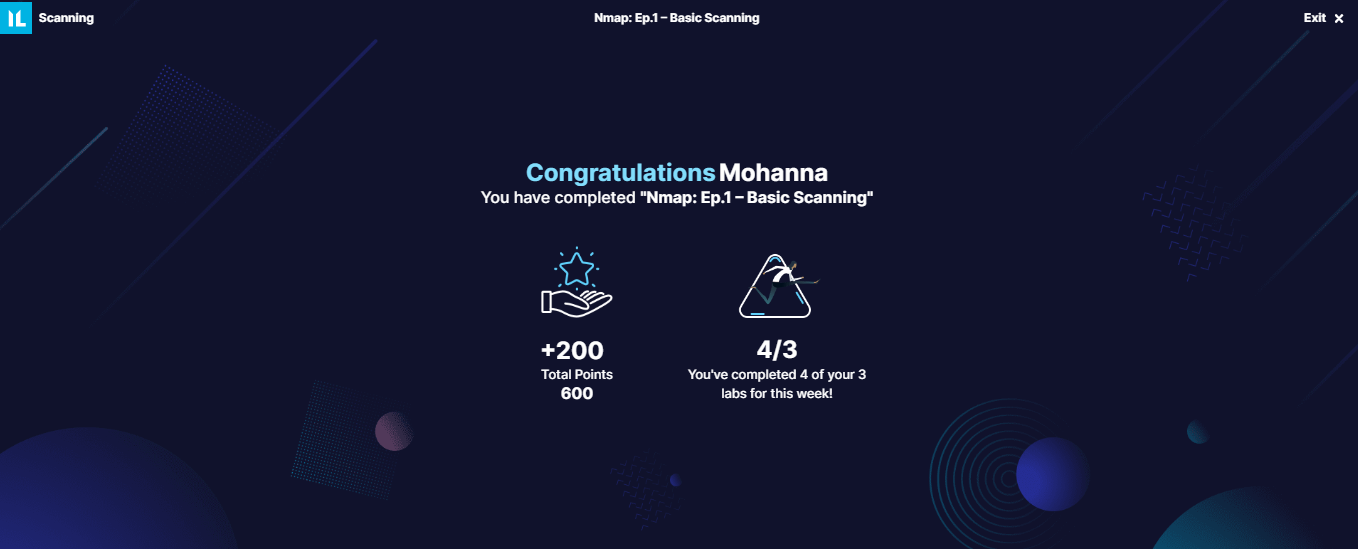
Q4.6) Scanning the POP3 port with ‘-p’ option in the IP address as below will provide the service hostname.



Q4.7) Upon scanning the top 1000 ports, there was no unknown service. Instead, scanning all the ports from 0-65535 displayed an unknown service in port 35469.

Q4.8) On performing banner grabbing on that port, we get the token.



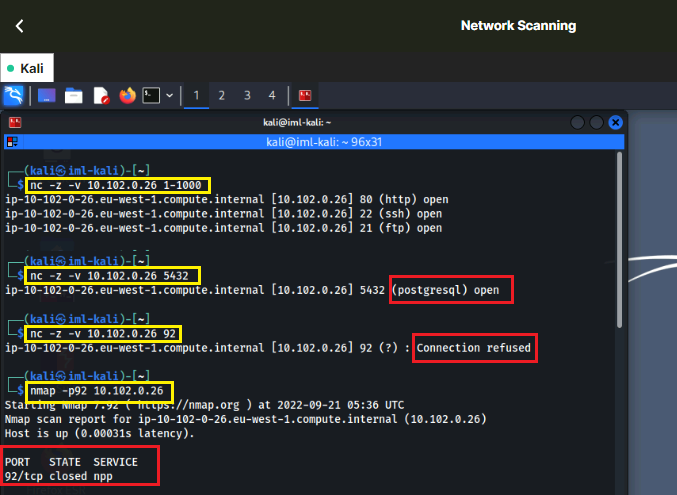


## TASK 5: NETWORK SCANNING

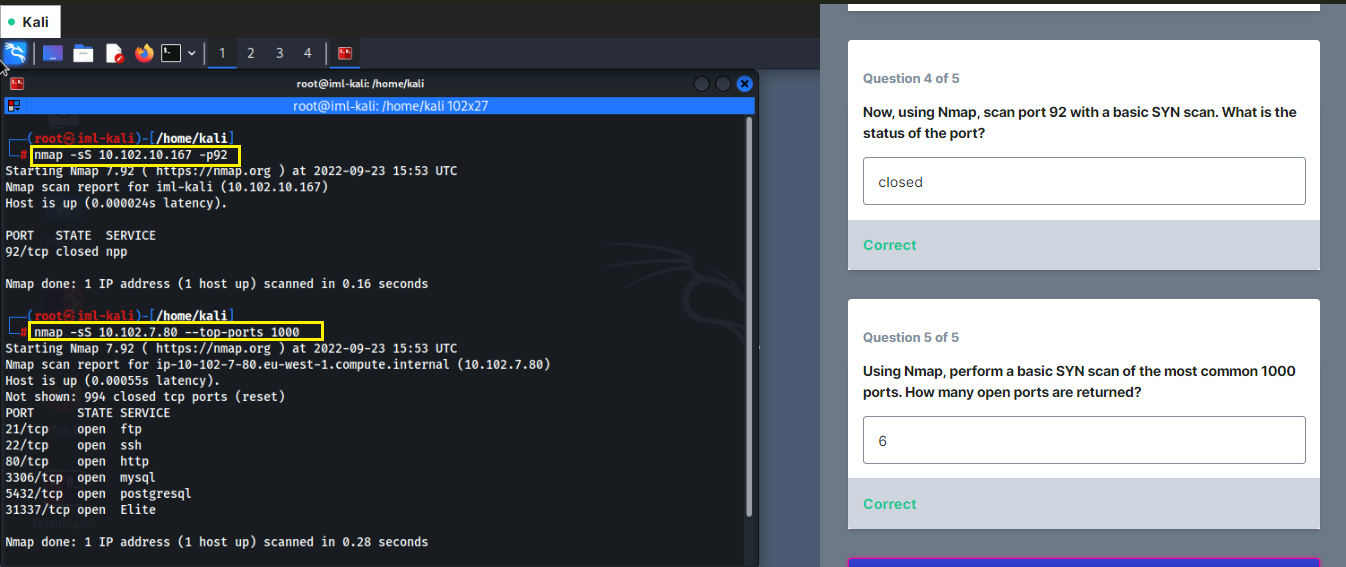
Q5.1) Netcat is a basic port scanner. ‘nc -z 10.102.0.26 1-1000’ will list first 1000 ports in the IP address 10.102.0.26 without attempting to make any connection (option -z)

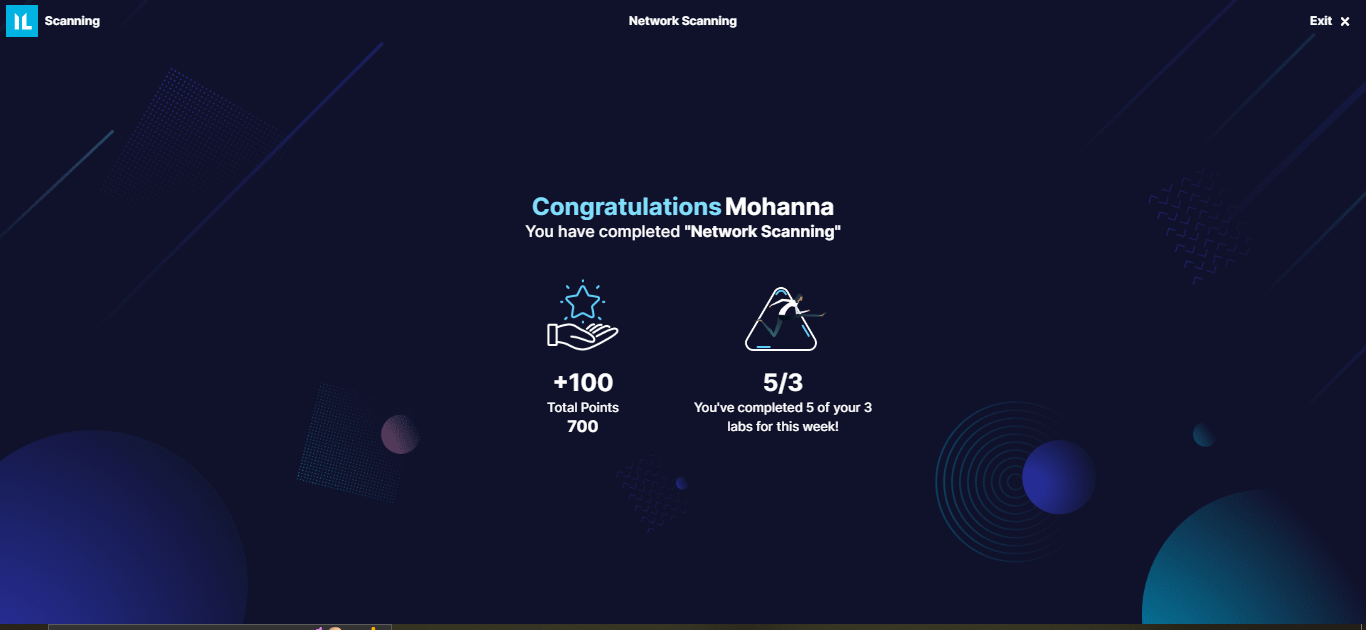
Q5.2, 5.3) There are 2 ways to scan a specific port number using nc command

1. with IP address followed by port number will provide the service running
2. with -p #port-number followed by IP address.



Q5.4, 5.5) As seen in previous task, ‘-sS’ is used to perform SYN scan on the ports. Same command is used here for port 92 and top 1000 ports





SUMMARY:

Network administration is necessary to safeguard a network from unauthorized and unusual access, network scan helps to manage, secure, and maintain the system in the network. This lab focuses on 2 main network administrators - Network scanners and network analyzers.

Network scanning involves identification of ports, service and live hosts. There are 3 different scanning techniques - network scanning, port scanning, vulnerability scanning and we have focused on first 2 scanning methods. Port scanning helps in diagnosing network and connectivity issues by checking network ports whether it is open, closed, or filtered state. Network scanning is one step ahead which allows decoding target system architecture and the operating system and helps in identifying vulnerabilities in a live host. Nmap and Netcat are popular scanning tool available which provides numerous techniques for different scenarios.

Network analyzing (also known as network sniffing or packet sniffing) involves evaluation and inspection of data packets transmitted across the network. Intercepting of data packet that is traversing a particular node in a network is known as packet capture (or network traffic capture). These captured packets contain raw data including network header details which helps to identify network congestion, data loss, forensic network analysis and troubleshoot unwanted threats. Wireshark (GUI version) and TCPDUMP (CLI version) are popular and powerful tools for packet analyzer.

Generally, these techniques can be employed by authorized administrators or unauthorized parties, providing good security as well as threats.