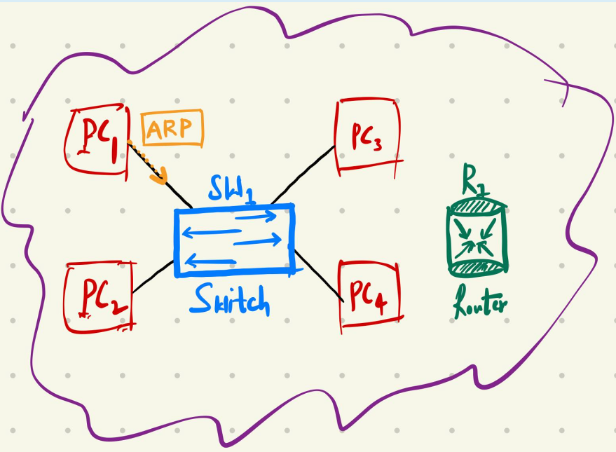
**[Q1]. Observe the topology below, where the PC1 is trying to send an ARP request.**



a). If you must perform a man-in-the-middle attack using ARP Spoofing in the topology. Where would you place yourself in the topology and which devices will you be connecting to?

To perform man in the middle attack, the threat actor should be in the same network. There are two choices for an attacker. The first one is to compromise any of the three computers(PC2, PC3, PC4) or he can connect to the network with another computer PC5(I am going with this option). As PC5 I am connected to Switch.

I want to be in the middle of PC1 and router. I can also spoof other PCs, but the router gives more information which can be interesting, (as PC1 can go to websites) like login credentials, sensitive info, PII.

b). The PC1 is sending the ARP request, explain where will that request go and what is your role as a "man-in-the-middle" attacker?

When the PC1 sends the ARP request, it goes to switch, which in turn sends the request to all devices connected to it(=broadcasts), namely PC2, PC3 and PC4 and router. And the one with the requested destination ip, replies with ARP reply.

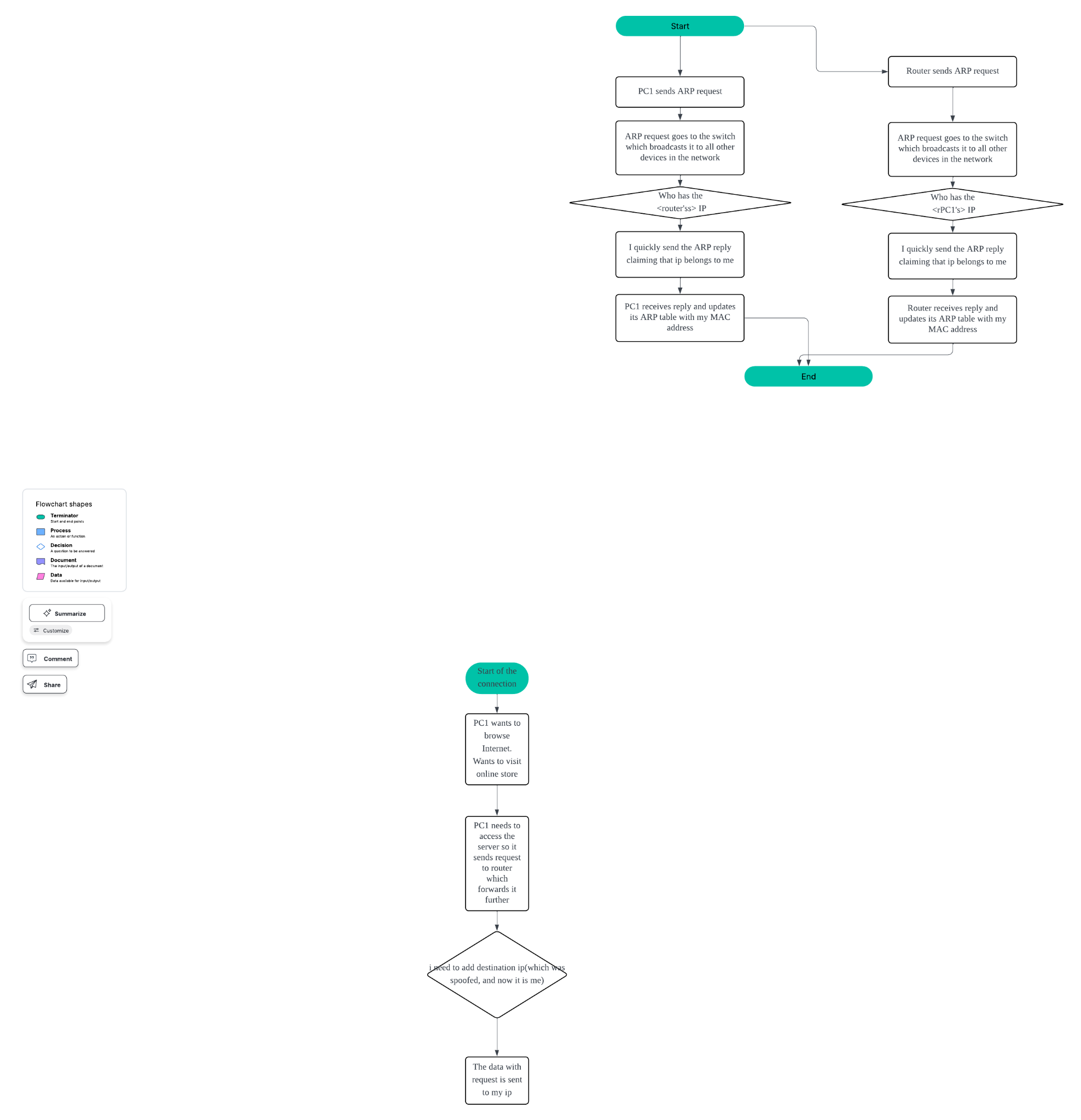
As a threat actor with PC5, I will send reply instead of a router, claiming that requested ip is mine. And I will send the reply with my MAC address(PC5’s MAC). PC1 will add my MAC address under router’s ip address to its ARP table.

c). Explain the COMPLETE activity in the topology if you as a "man-in-the-middle" attacker is initiating the ARP request. Draw the flowchart of the COMPLETE activity in the topology. Explain how will you get hold of the data?

Router starts to interact with PC1 but it doesn’t know its mac. Therefore it sends an ARP request. I will send ARP reply first to the router. But my source ip will be PC1’s ip. Then router adds my MAC to his ARP table. Now I can listen to communication between the PC1 and router.   
When PC1 sends the data, I can read and even modify the data using tools like packet sniffers (Wireshark). Then i send it to the router because PC1 shouldn’t suspect anything. The router sends reply. This reply goes to me. I read it and send it to PC1 (actual receiver). This way I get hold of the data.

Flowchart:

(Supposing that I want to intercept traffic between PC1 and router)



**Question 2:**  
What is significant about the contents of the destination address field?

The destination is written as broadcast. It is because the source doesn’t know yet the mac of the receiver, so it broadcasts the ARP request to every device on the network.

Why does the PC send out a broadcast ARP prior to sending the first ping request?

Because it doesn’t know who has the destination IP because there is no record in its ARP table. Then after adding it,PC can freely communicate with 192.168.1.1.

What is the MAC address of the source in the first frame?

f4:8c:50:62:62:6d

What is the Vendor ID (OUI) of the Source’s NIC?

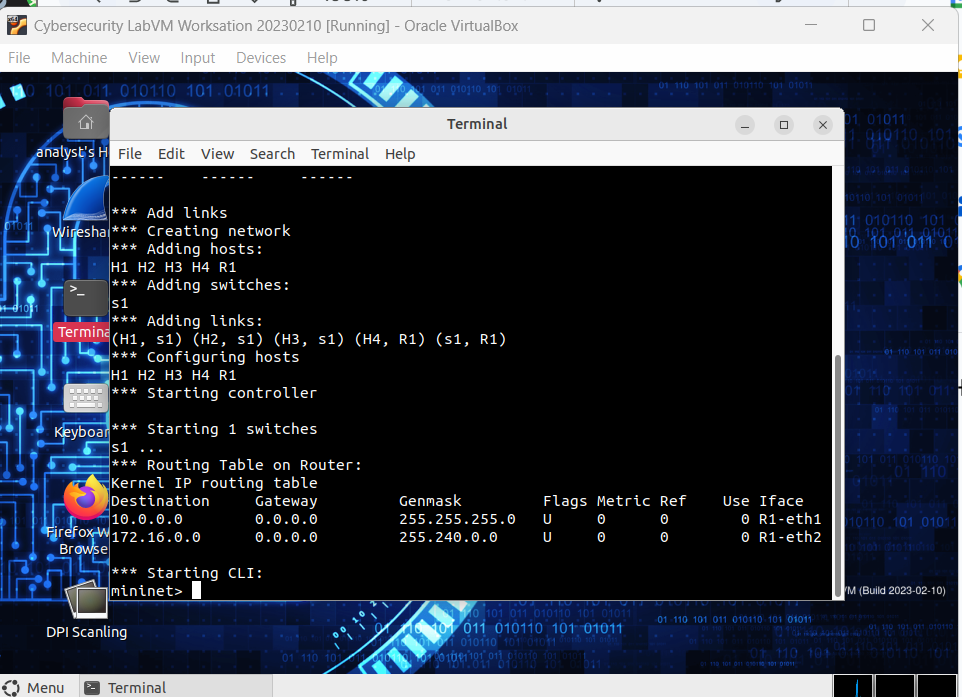
f4:8c:50

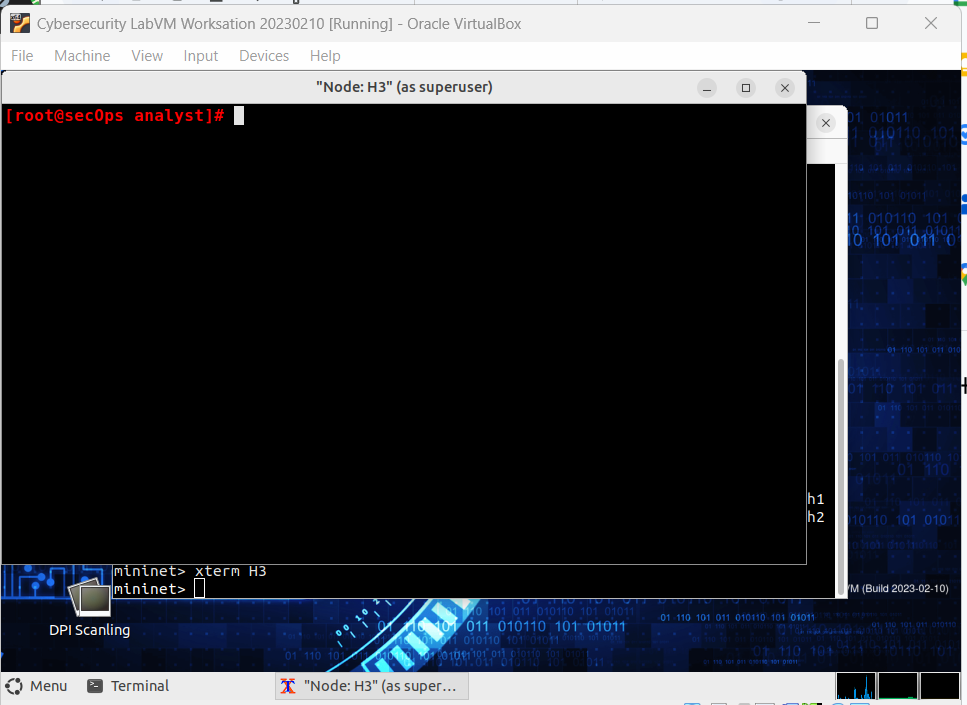
What portion of the MAC address is the OUI?

The first 3 bytes. The half of the MAc

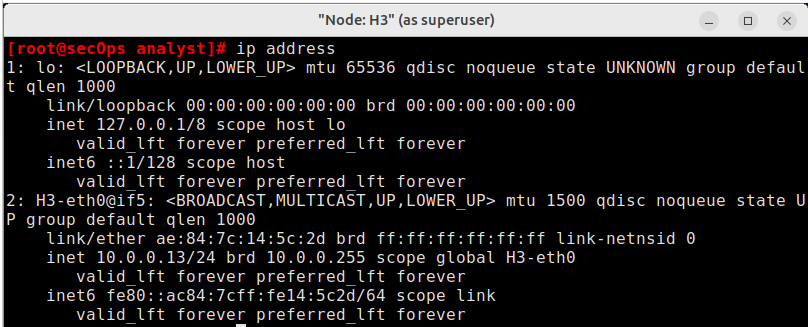
What is the Source’s NIC serial number?

The last six hex numbers are the serial number. It is 62:62:6d



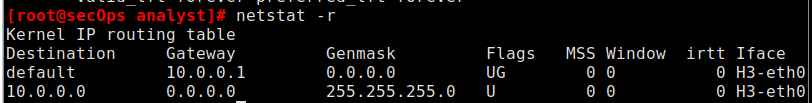


Node H3



IP ad: 10.0.0.13/24

MAC: ae:84:7c:14:5c:2d



IP of def gateway: 10.0.0.1

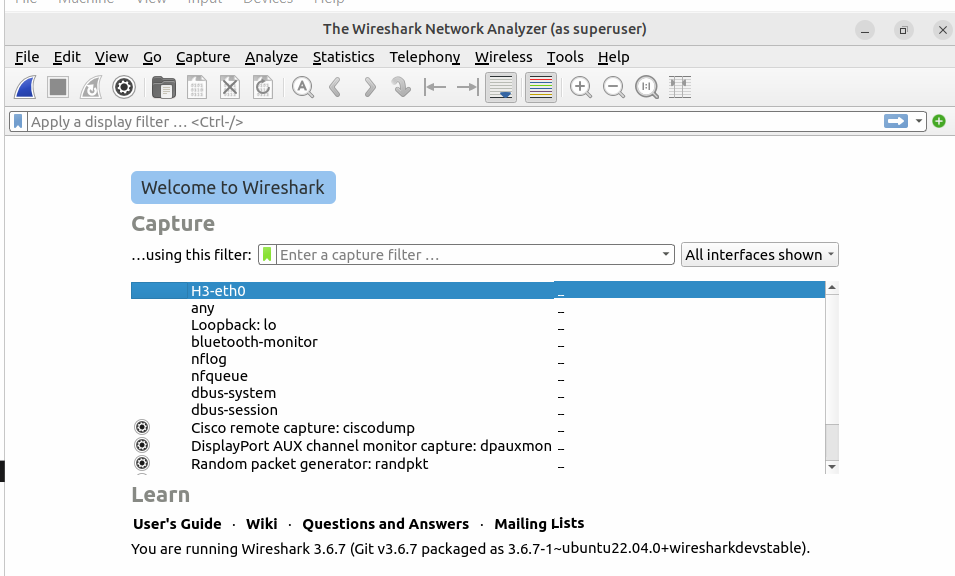


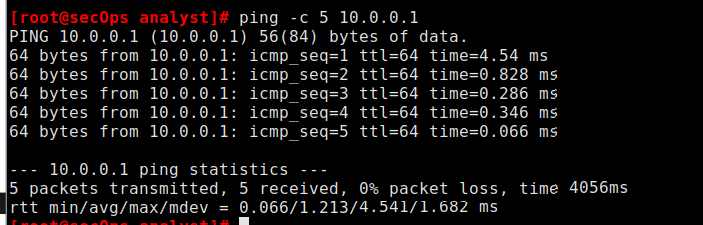
There are no mappings for now.

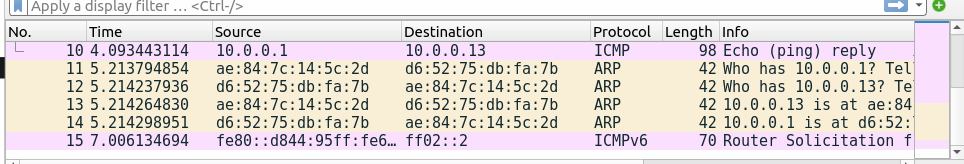


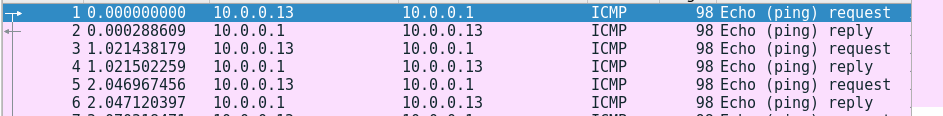
This command is for clearing any ARP entry in the ARP table.

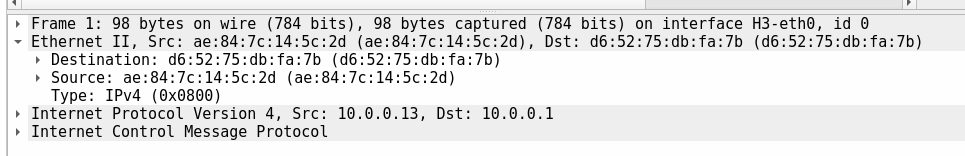
Since I have no mapping, i get this message “No ARP entry for X”











What is the MAC address of the PC’s NIC?

ae:84:7c:14:5c:2d

What is the default gateway’s MAC address?

d6:52:75:db:fa:7b

What type of frame is displayed?

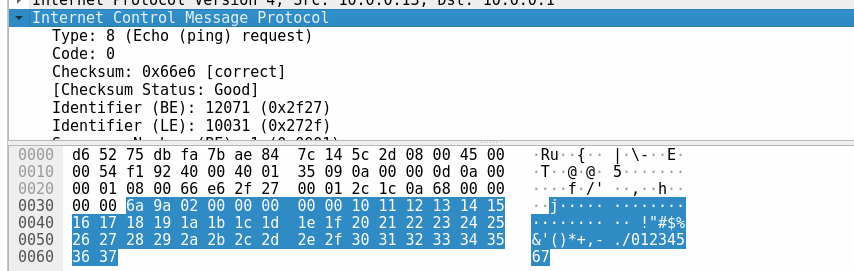
Type: IPv4 (0x0800)

What is the source IP address?

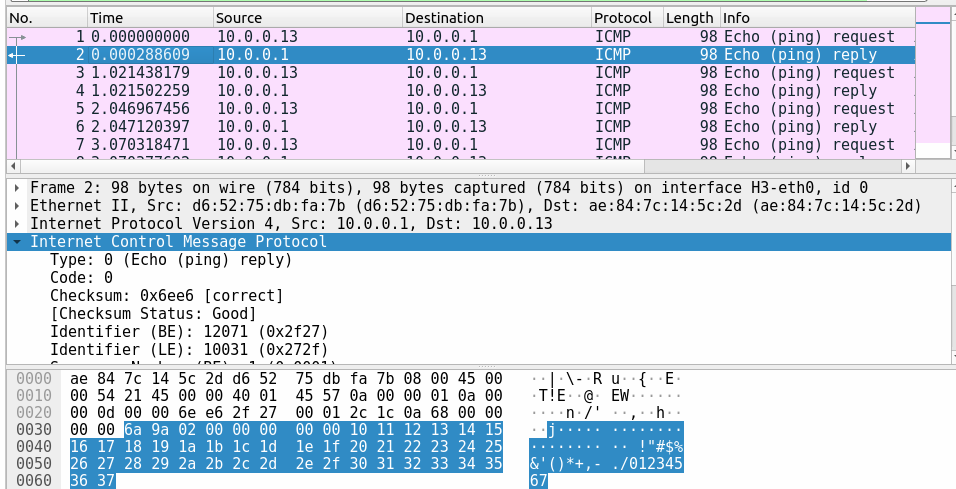
10.0.0.13

What is the destination IP address?

10.0.0.1



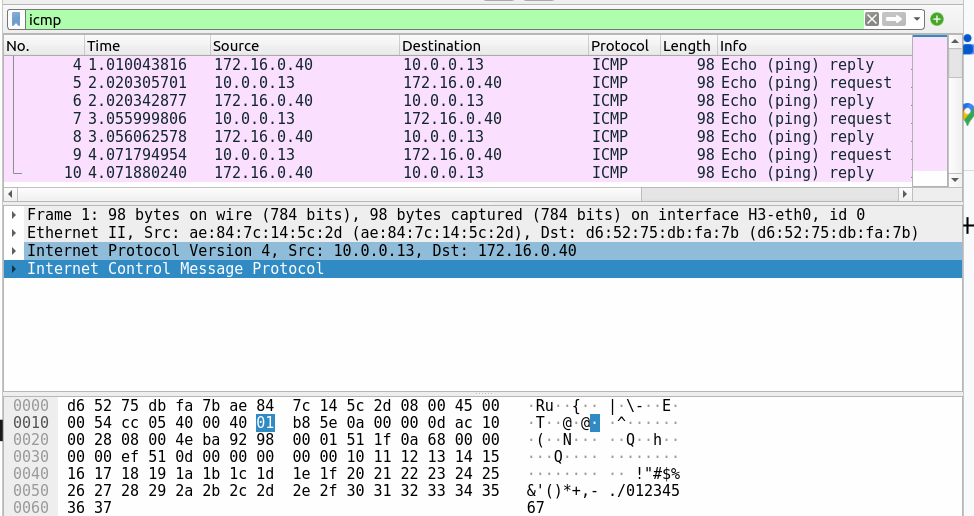
Filtered with only ICMP:



What device and MAC address is displayed as the destination address?

IP: 10.0.0.13

MAC: ae:84:7c:14:5c:2d



Source:

ae:84:7c:14:5c:2d

Destination:

d6:52:75:db:fa:7b

What are the source and destination IP addresses contained in the data field of the frame?

Source:

10.0.0.13

Destination:

172.16.0.40

Compare these addresses to the addresses you received in Step 5. The only address that changed is the

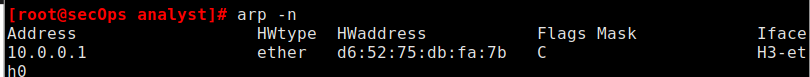
destination IP address.

Question:

Why has the destination IP address changed, while the destination MAC address remained the same?

The 172.16.0.40 is clearly from the outside network. So when the host3 sends ping, it goes to default getaway, which then forwards it to receiver. That’s why we have default gateway’s MAC address.

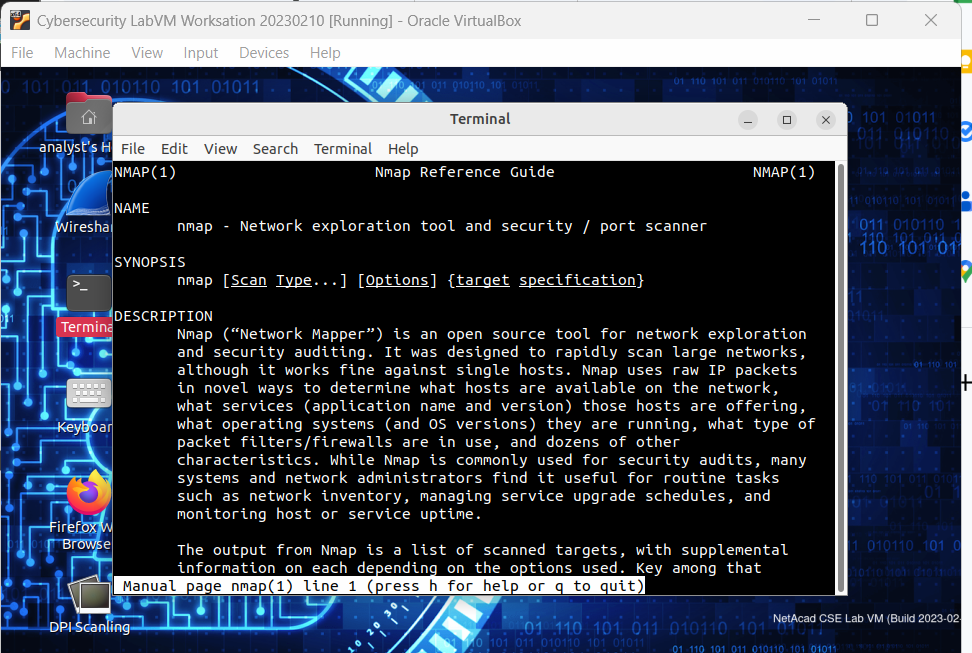
Ip doesn’t change. It remains the same because it is the receiver of the ping.



Wireshark does not display the preamble field of a frame header. What does the preamble contain?

This field contains synchronizing bits, processed by the NIC hardware. It indicates the start of the packet.

**[Q3]. Download the** [**Practical\_Activity#2**](https://drive.google.com/file/d/1mh20tkkXpY2N1wI0iu9cBIrrA14_Qx5d/view?usp=share_link) **and complete the lab on your VM. Paste the screenshots and responses in the Word file (YOURSTUDENTID\_CyberOps\_Midterm.docx)**

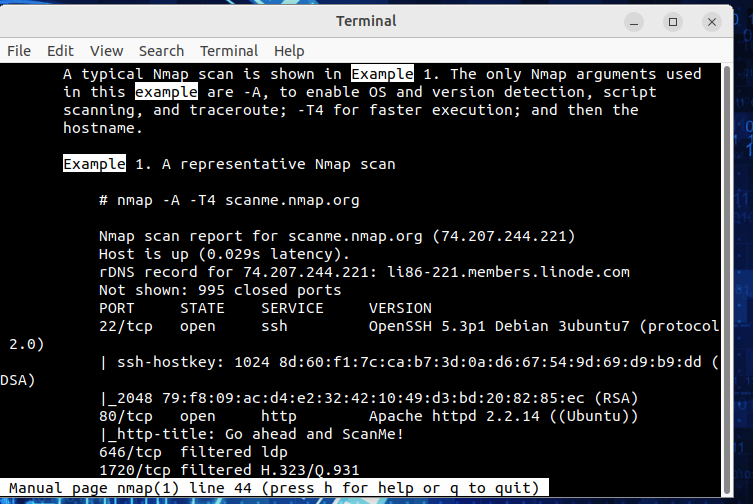


What is Nmap?

Nmap(Network Mapper) - open source tool for network exploration and security auditing.

What is nmap used for?

Used for scanning large networks as well as single hosts.



Question:

What is the nmap command used?

In Example 1 nmap command is used for scanning scanme.nmap.org site. It checks whether the site/server is working

Use the search function to answer the following questions.

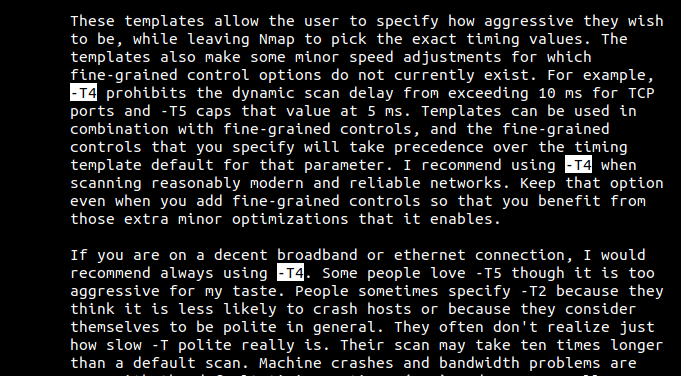
What does the switch -A do?

-A enables OS and version detection, script scanning and traceroute

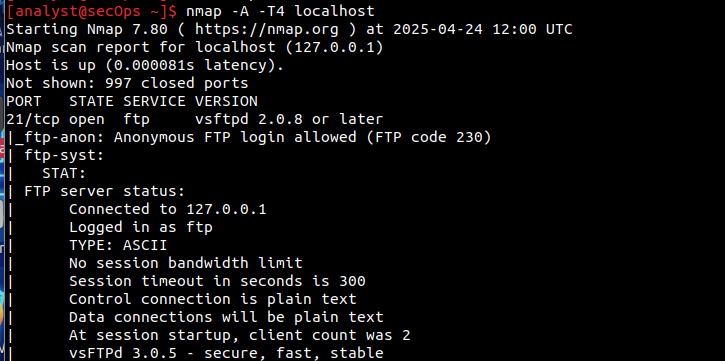


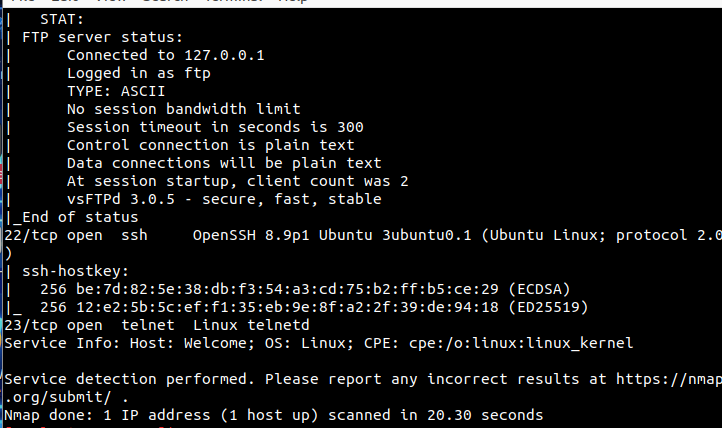
What does the switch -T4 do?

-T4 is for faster execution



a. If necessary, open a terminal on the VM. At the prompt, enter nmap -A -T4 localhost. Depending on your local network and devices, the scan will take anywhere from a few seconds to a few minutes.

****



Which ports and services are opened?

Port 21 is open for ftp

Port 22 for ssh

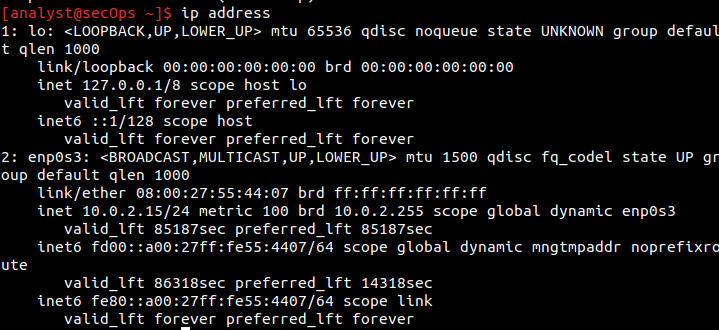
Port 23 for telnet

For each of the open ports, record the software that is providing the services.

Ftp: vsftpd 2.0.8.

Ssh: OpenSSH 8.9p1 Ubuntu

Telnet: Linux telnetd



Record the IP address and subnet mask for your VM.

10.0.2.15

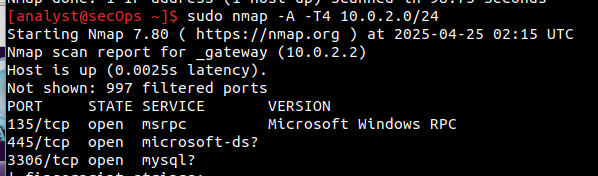
255.255.255.0

Which network does your VM belong to?

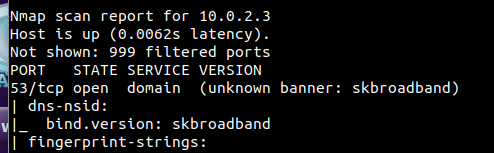
Private network 10.0.2.0/24

Enp0s3 - interface name

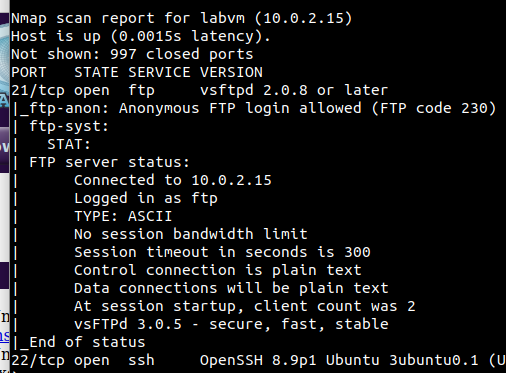
First host:

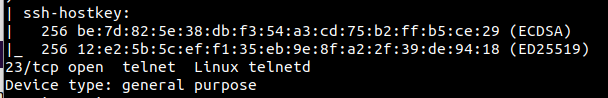


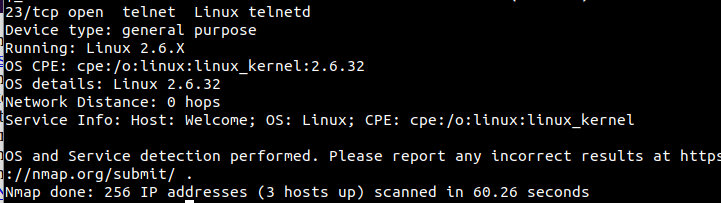
Second host:



Third host:







How many hosts are up?

Three hosts are up.

From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your VM.

List some of the services that are available on the detected hosts.

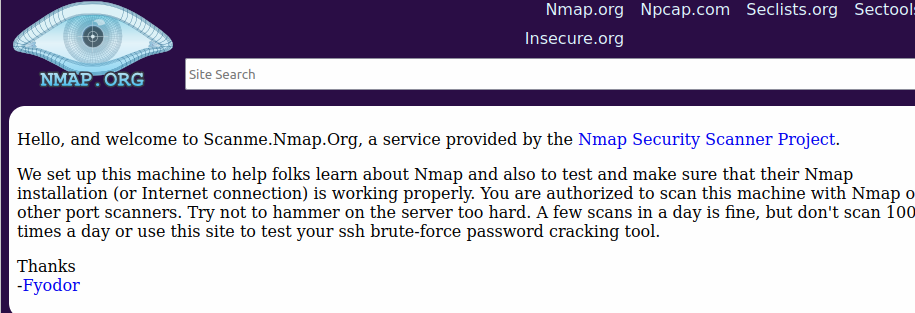
10.0.2.2 :

Msrpc. Microsoft-ds and mysql services are available on this host.

10.0.2.3:

domain service on port 53

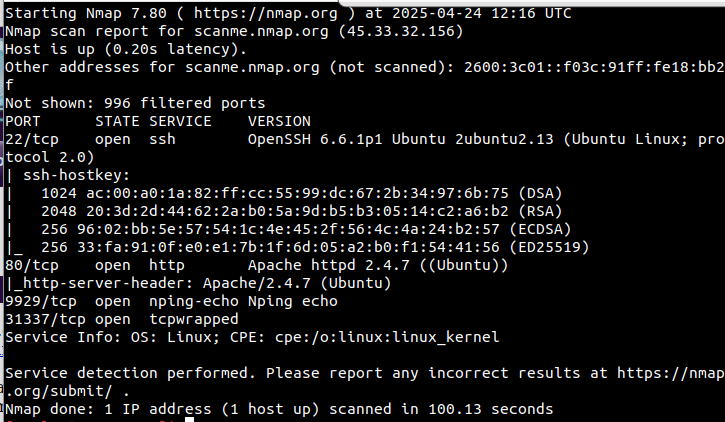
labvm(10.0.2.15):  
Ftp, ssh, telnet services are available on this host.



What is the purpose of this site?

To help learn nmap nad to test whether the namp is working properly. This site acts as a tester.

At the terminal prompt, enter nmap -A -T4 scanme.nmap.org.



c. Review the results and answer the following questions.

Questions:

Which ports and services are opened?

Port 22 - for ssh

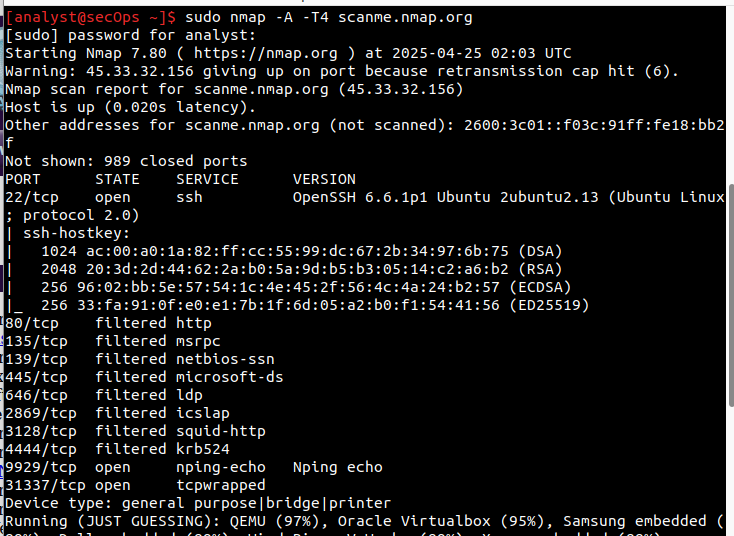
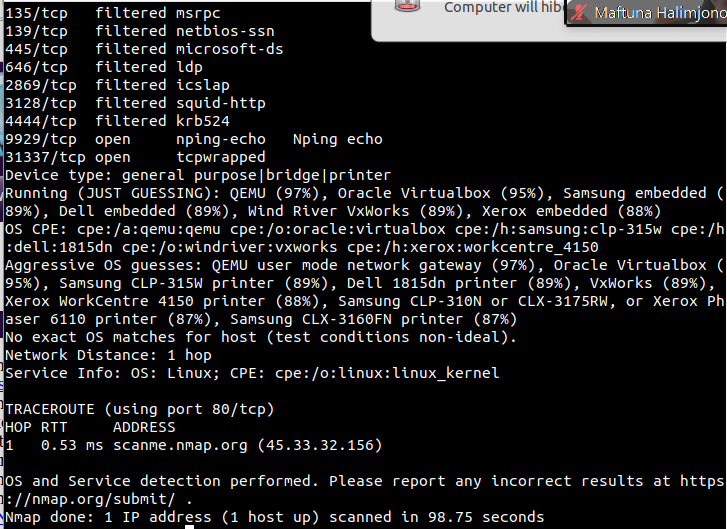
Port 80 for http

Port 9929 - nping-echo

Port 31337 - tcpwrapped

Which ports and services are filtered?

Filtered ports are not shown in the first case. But when I ran the command with sudo privileges, i can see now filtered ports:

There are 8 filtered ports:  
80 - http

135 - msrpc

139 - netbios-ssn

445 - microsoft-ds

646 - ldp

2869 - icslap

3128 - squid-http

4444 - krb524

What is the IP address of the server?

45.33.32.156



What is the operating system?

Linux

****

**Reflection Question**

**Nmap is a powerful tool for network exploration and management. How can Nmap help with network security?**

**How can Nmap be used by a threat actor as a nefarious tool?**

Security analysts can check whether the ports are open or closed and whether the hosts are up. It can help them to detect problems with websites easily if it is down. Also nmap provides info on services available by ports, OS that they are running on.

It can be tool for intelligence gathering. The threat actor can gather all the info about the network and tailor his/her plans and tools for that, for example for specific OS. THey can know which hosts are up to attack them later, their ips. So mainly nmap is for threat intelligence.