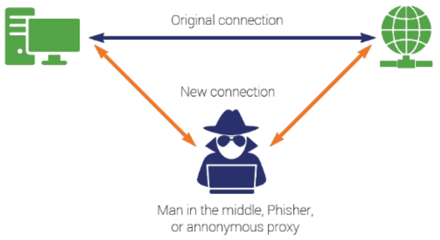
Activity 5
MITM Attack Simulation and Analysis

Using various virtual machines, be able to perform "Man-in-the-Middle Attack Simulation and Analysis" for possible targeted virtualized machines in the network. Also conduct a thorough analysis of a captured network traffic.



Activity Resources

Virtual Machines: Kali Linux, Ubuntu, Metasploitable
Network Traffic Capture: [Activity5]NetCapture_Scenario
Tools: Nmap or ZenMap, Wireshark, Ettercap, Driftnet

Disclaimer: Activity is for educational purposes only! Misuse or targeting other services outside the controlled or virtual environment is punishable by law and the University. The University and the Instructor have no liability for misuse of the tools used in this exercise.

Activity Procedure(s)

Task 1 MITM Attack Simulation

In your workstation, open/run Oracle VirtualBox Manager and configure virtual machines (Kali Linux, Ubuntu and Metasploitable) network adapter using the following configurations:

Adapter No. 1 Network Configurations

- Enable Network Adapter: YES (checked)
- Attached to: Host-Only Adapter
- Name: Virtual Host-Only Ethernet Adapter (note: choose network that is DHCP server enabled)
- Promiscuous Mode (Advanced): Deny
- Reset MAC Address (press the refresh button)

Run/Start virtual machine simultaneously (make sure all virtual machines are loaded and running). In your Kali Linux virtual machine, perform Network Scanning and Reconnaissance using Nmap or ZenMap tools to identify possible vulnerable target machines. Next, perform MITM attack on the target machines using Ettercap or Bettercap and Driftnet tool. While performing the attack, run Wireshark in Kali Linux to capture the network packet (observe and analyze the results). In your Ubuntu virtual machine, open a browser and access the website hosted by the targeted webserver (Metaploitable). Finally, observe and analyze the captured network traffic in Wireshark.

Note: Refer to your course manual on how to simulate an MITM Attack.

Task 2 Network Traffic Examination and Analysis

Open Wireshark and load the network capture file ([Activity5]NetCapture_Scenario). Perform the necessary network investigation of the captured network traffic using various examination techniques (filtering, statistics analysis, and expert information analysis).

Submission Note (Individual Activity)

Use file name convention (LASTNAME_CTAINASL_SECTION_TERM_AY_Activity5.pdf).
Submit/upload Softcopy (PDF file) in MS Teams
Submit a PRINTED activity rubric.

ACTIVITY DOCUMENTATION

Group Name M.O. Saturday, May 3, 2025

Members Surname, First Name MI. (Alphabetical)

Angeles, Johanes P.

Balbuena, Alezzandrei Ericka A.

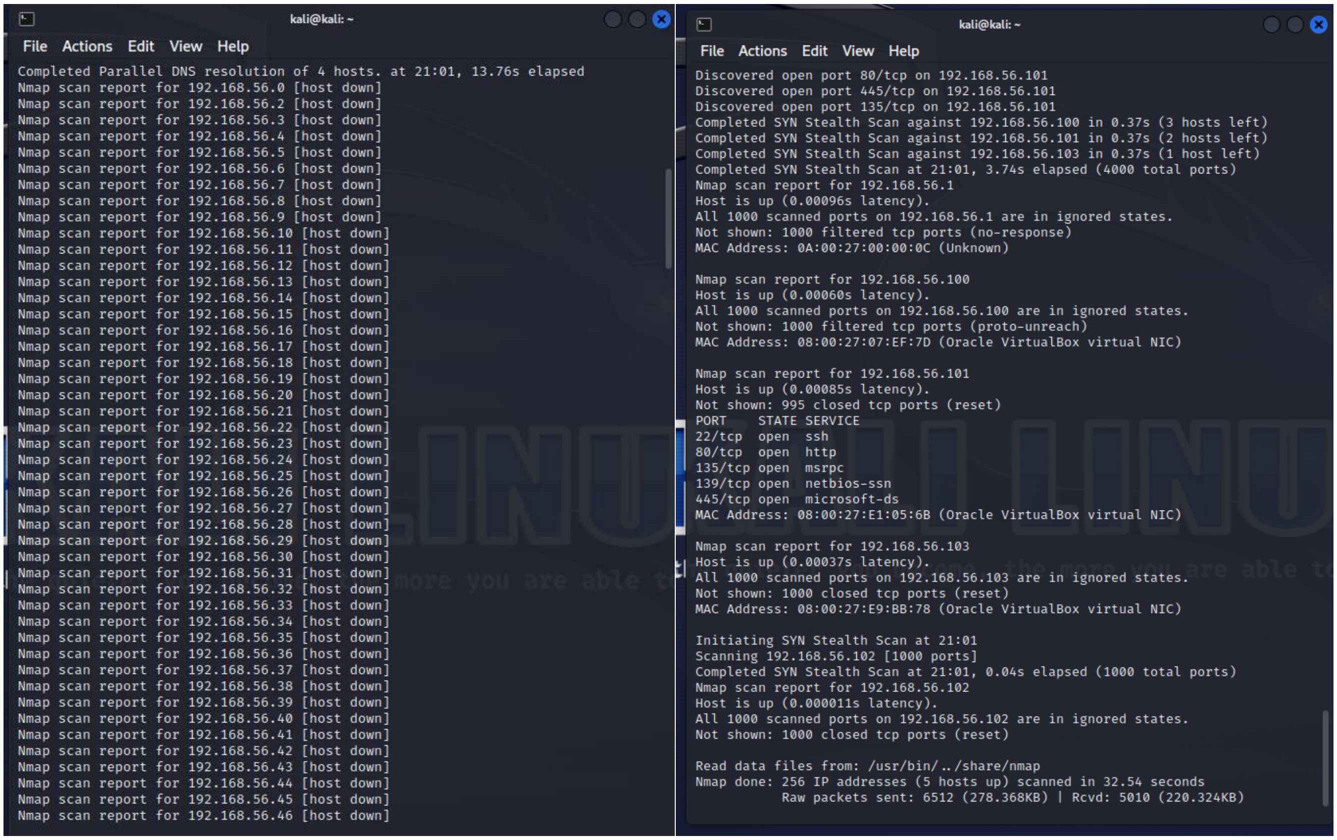
Canivel, Adrianne Bleu R.

Instruction(s): Provide the appropriate screenshot/screen capture of your workstation.

MITM Attack Simulation (ARP Poisoning)
Activity Task 1

Nmap/ZenMap Report

Display here the result of the Nmap/ZenMap report.

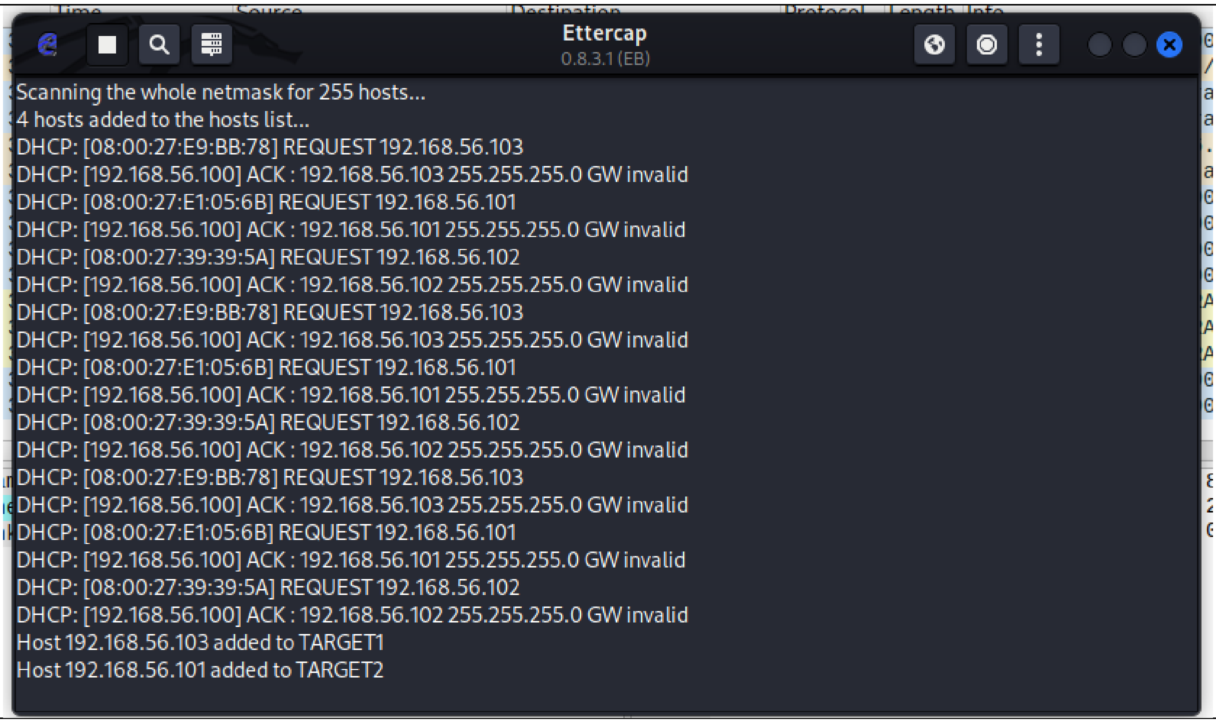


```
Completed Parallel DNS resolution of 4 hosts. at 21:01, 13.76s elapsed
Nmap scan report for 192.168.56.0 [host down]
Nmap scan report for 192.168.56.2 [host down]
Nmap scan report for 192.168.56.3 [host down]
Nmap scan report for 192.168.56.4 [host down]
Nmap scan report for 192.168.56.5 [host down]
Nmap scan report for 192.168.56.6 [host down]
Nmap scan report for 192.168.56.7 [host down]
Nmap scan report for 192.168.56.8 [host down]
Nmap scan report for 192.168.56.9 [host down]
Nmap scan report for 192.168.56.10 [host down]
Nmap scan report for 192.168.56.11 [host down]
Nmap scan report for 192.168.56.12 [host down]
Nmap scan report for 192.168.56.13 [host down]
Nmap scan report for 192.168.56.14 [host down]
Nmap scan report for 192.168.56.15 [host down]
Nmap scan report for 192.168.56.16 [host down]
Nmap scan report for 192.168.56.17 [host down]
Nmap scan report for 192.168.56.18 [host down]
Nmap scan report for 192.168.56.19 [host down]
Nmap scan report for 192.168.56.20 [host down]
Nmap scan report for 192.168.56.21 [host down]
Nmap scan report for 192.168.56.22 [host down]
Nmap scan report for 192.168.56.23 [host down]
Nmap scan report for 192.168.56.24 [host down]
Nmap scan report for 192.168.56.25 [host down]
Nmap scan report for 192.168.56.26 [host down]
Nmap scan report for 192.168.56.27 [host down]
Nmap scan report for 192.168.56.28 [host down]
Nmap scan report for 192.168.56.29 [host down]
Nmap scan report for 192.168.56.30 [host down]
Nmap scan report for 192.168.56.31 [host down]
Nmap scan report for 192.168.56.32 [host down]
Nmap scan report for 192.168.56.33 [host down]
Nmap scan report for 192.168.56.34 [host down]
Nmap scan report for 192.168.56.35 [host down]
Nmap scan report for 192.168.56.36 [host down]
Nmap scan report for 192.168.56.37 [host down]
Nmap scan report for 192.168.56.38 [host down]
Nmap scan report for 192.168.56.39 [host down]
Nmap scan report for 192.168.56.40 [host down]
Nmap scan report for 192.168.56.41 [host down]
Nmap scan report for 192.168.56.42 [host down]
Nmap scan report for 192.168.56.43 [host down]
Nmap scan report for 192.168.56.44 [host down]
Nmap scan report for 192.168.56.45 [host down]
Nmap scan report for 192.168.56.46 [host down]
```

```
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 135/tcp on 192.168.56.101
Completed SYN Stealth Scan against 192.168.56.100 in 0.37s (3 hosts left)
Completed SYN Stealth Scan against 192.168.56.101 in 0.37s (2 hosts left)
Completed SYN Stealth Scan against 192.168.56.103 in 0.37s (1 host left)
Completed SYN Stealth Scan at 21:01, 3.74s elapsed (4000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00096s latency).
All 1000 scanned ports on 192.168.56.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 0A:00:27:00:00:0C (Unknown)

Nmap scan report for 192.168.56.100
Host is up (0.00060s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:07:EF:7D (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.101
Host is up (0.00085s latency).
Not shown: 995 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http
135/tcp open  msrpc
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:E1:05:6B (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.103
Host is up (0.00037s latency).
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:E9:BB:78 (Oracle VirtualBox virtual NIC)

Initiating SYN Stealth Scan at 21:01
Scanning 192.168.56.102 [1000 ports]
Completed SYN Stealth Scan at 21:01, 0.04s elapsed (1000 total ports)
Nmap scan report for 192.168.56.102
Host is up (0.000011s latency).
All 1000 scanned ports on 192.168.56.102 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Read data files from: /usr/bin/../share/nmap
Nmap done: 256 IP addresses (5 hosts up) scanned in 32.54 seconds
           Raw packets sent: 6512 (278.368KB) | Rcvd: 5010 (220.324KB)
```

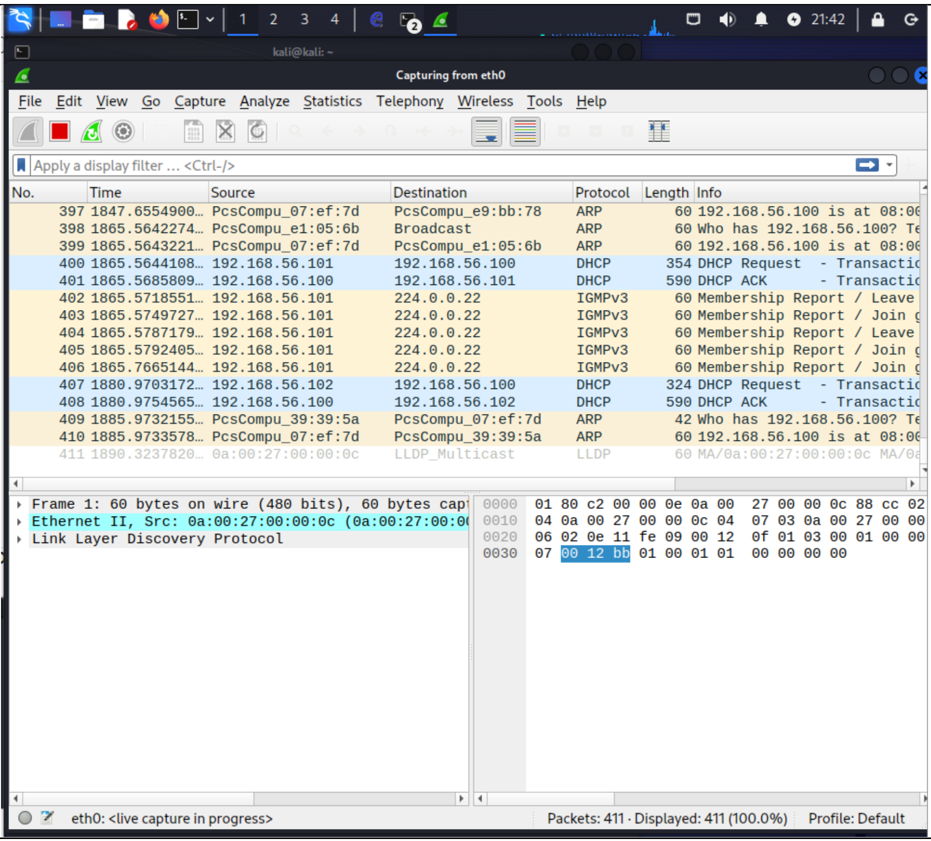
ARP Poisoning Attack Simulation

Display how ARP attack was performed using Ettercap GUI.



```
Scanning the whole netmask for 255 hosts...
4 hosts added to the hosts list...
DHCP: [08:00:27:E9:BB:78] REQUEST 192.168.56.103
DHCP: [192.168.56.100] ACK : 192.168.56.103 255.255.255.0 GW invalid
DHCP: [08:00:27:E1:05:6B] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK : 192.168.56.101 255.255.255.0 GW invalid
DHCP: [08:00:27:39:39:5A] REQUEST 192.168.56.102
DHCP: [192.168.56.100] ACK : 192.168.56.102 255.255.255.0 GW invalid
DHCP: [08:00:27:E9:BB:78] REQUEST 192.168.56.103
DHCP: [192.168.56.100] ACK : 192.168.56.103 255.255.255.0 GW invalid
DHCP: [08:00:27:E1:05:6B] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK : 192.168.56.101 255.255.255.0 GW invalid
DHCP: [08:00:27:39:39:5A] REQUEST 192.168.56.102
DHCP: [192.168.56.100] ACK : 192.168.56.102 255.255.255.0 GW invalid
DHCP: [08:00:27:E9:BB:78] REQUEST 192.168.56.103
DHCP: [192.168.56.100] ACK : 192.168.56.103 255.255.255.0 GW invalid
DHCP: [08:00:27:E1:05:6B] REQUEST 192.168.56.101
DHCP: [192.168.56.100] ACK : 192.168.56.101 255.255.255.0 GW invalid
DHCP: [08:00:27:39:39:5A] REQUEST 192.168.56.102
DHCP: [192.168.56.100] ACK : 192.168.56.102 255.255.255.0 GW invalid
Host 192.168.56.103 added to TARGET1
Host 192.168.56.101 added to TARGET2
```

Display here the Wireshark capture environment.



```
No.  Time            Source               Destination          Protocol Length Info
 397 1847.6554900… PcsCompu_07:ef:7d    PcsCompu_e9:bb:78    ARP        60 192.168.56.100 is at 08:0(
 398 1865.5642274… PcsCompu_e1:05:6b    Broadcast            ARP        60 Who has 192.168.56.100? Te
 399 1865.5643221… PcsCompu_07:ef:7d    PcsCompu_e1:05:6b    ARP        60 192.168.56.100 is at 08:0(
 400 1865.5644108… 192.168.56.101       192.168.56.100       DHCP      354 DHCP Request  - Transactic
 401 1865.5685809… 192.168.56.100       192.168.56.101       DHCP      590 DHCP ACK      - Transactic
 402 1865.5718551… 192.168.56.101       224.0.0.22           IGMPv3     60 Membership Report / Leave
 403 1865.5749727… 192.168.56.101       224.0.0.22           IGMPv3     60 Membership Report / Join g
 404 1865.5787179… 192.168.56.101       224.0.0.22           IGMPv3     60 Membership Report / Leave
 405 1865.5792405… 192.168.56.101       224.0.0.22           IGMPv3     60 Membership Report / Join g
 406 1865.7665144… 192.168.56.101       224.0.0.22           IGMPv3     60 Membership Report / Join g
 407 1880.9703172… 192.168.56.102       192.168.56.100       DHCP      324 DHCP Request  - Transactic
 408 1880.9754565… 192.168.56.100       192.168.56.102       DHCP      590 DHCP ACK      - Transactic
 409 1885.9732155… PcsCompu_39:39:5a    PcsCompu_07:ef:7d    ARP        42 Who has 192.168.56.100? Te
 410 1885.9733578… PcsCompu_07:ef:7d    PcsCompu_39:39:5a    ARP        60 192.168.56.100 is at 08:0(
 411 1890.3237820… 0a:00:27:00:00:0c    LLDP_Multicast       LLDP       60 MA/0a:00:27:00:00:0c MA/0a
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes capt
› Ethernet II, Src: 0a:00:27:00:00:0c (0a:00:27:00:0(
› Link Layer Discovery Protocol
```

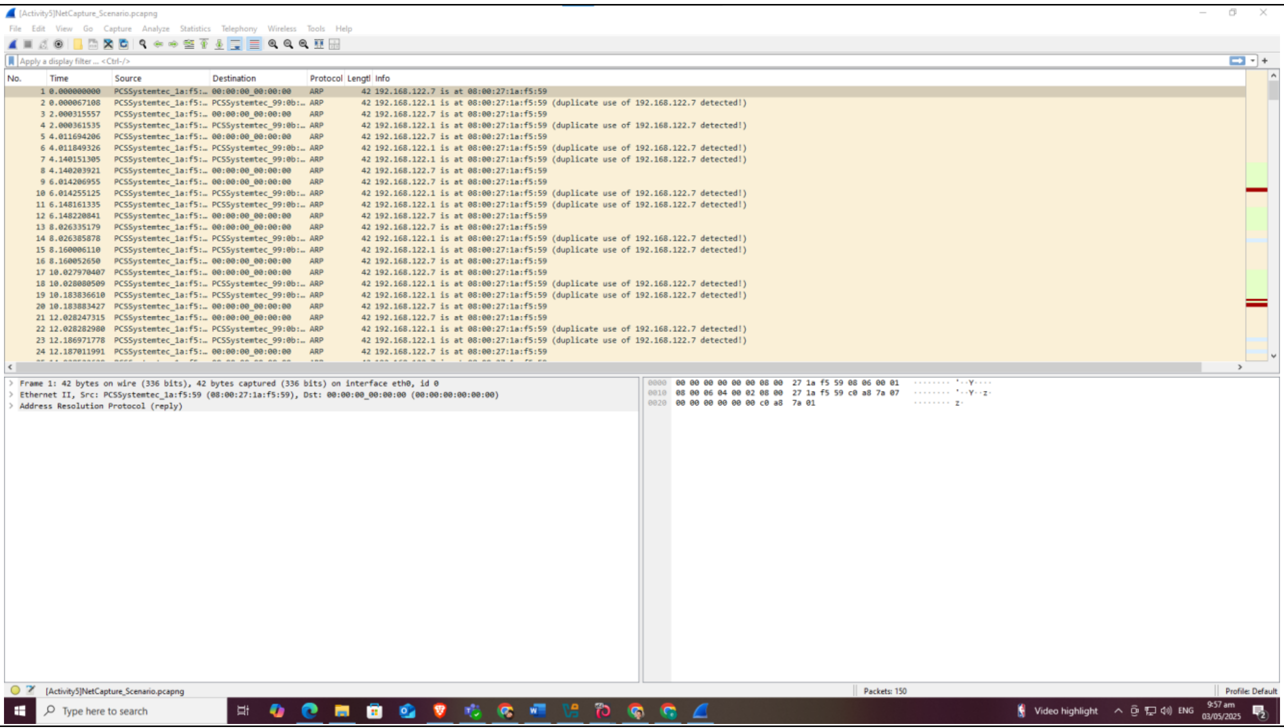
```
0000  01 80 c2 00 00 0e 0a 00  27 00 00 0c 88 cc 02
0010  04 0a 00 27 00 00 0c 04  07 03 0a 00 27 00 00
0020  06 02 0e 11 fe 09 00 12  0f 01 03 00 01 00 00
0030  07 00 12 bb 01 00 01 01  00 00 00 00
```

eth0: <live capture in progress>   Packets: 411 · Displayed: 411 (100.0%)   Profile: Default

Network Traffic Examination and Analysis
Activity Task 2

Wireshark Capture

Display here the loaded Wireshark capture file.

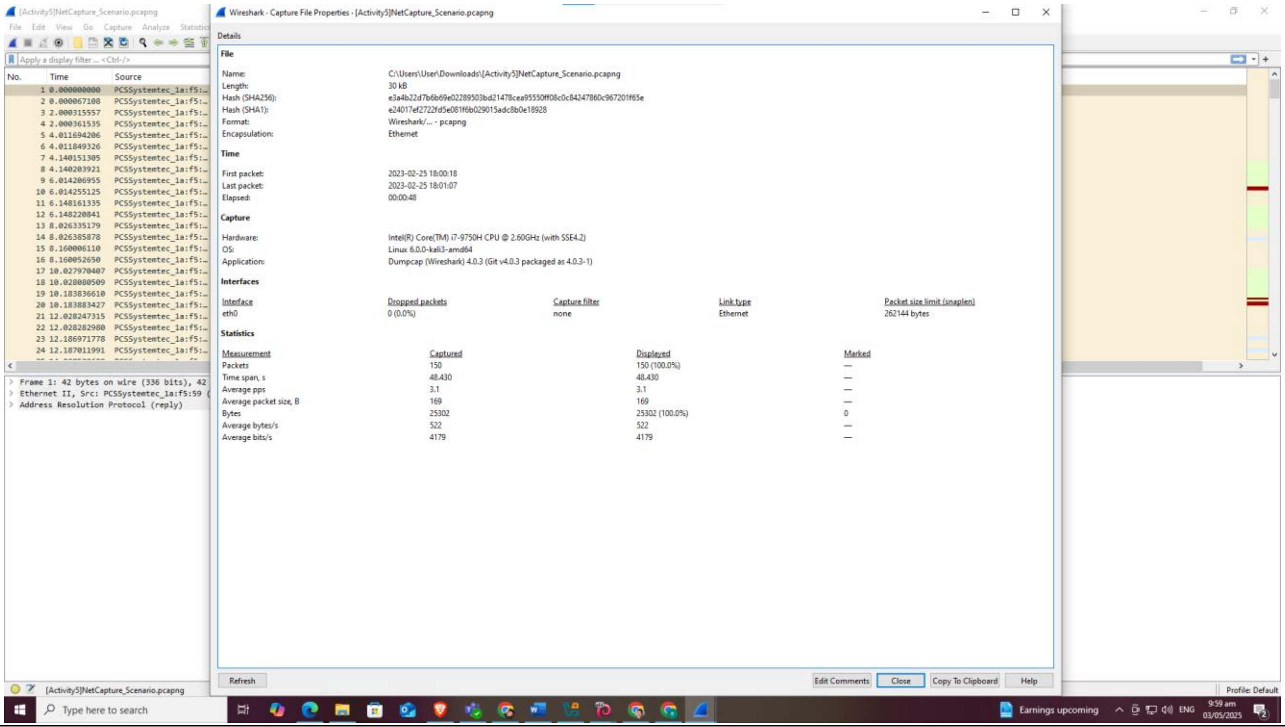


```
No.   Time          Source                 Destination            Protocol Lengtl Info
    1 0.000000000   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
    2 0.000067108   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    3 2.000315557   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
    4 2.000361535   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    5 4.011694206   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
    6 4.011849326   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    7 4.140151305   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    8 4.140203921   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
    9 6.014206955   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   10 6.014255125   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   11 6.148161335   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   12 6.148220841   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   13 8.026335179   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   14 8.026385878   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   15 8.160006110   PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   16 8.160052650   PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   17 10.027970407  PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   18 10.028080509  PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   19 10.183836610  PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   20 10.183883427  PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   21 12.028247315  PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
   22 12.028282980  PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   23 12.186971778  PCSSystemtec_1a:f5:…  PCSSystemtec_99:0b:…   ARP       42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   24 12.187011991  PCSSystemtec_1a:f5:…  00:00:00_00:00:00      ARP       42 192.168.122.7 is at 08:00:27:1a:f5:59
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_1a:f5:59 (08:00:27:1a:f5:59), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Address Resolution Protocol (reply)
```

```
0000  00 00 00 00 00 00 08 00  27 1a f5 59 08 06 00 01   ········ '··Y····
0010  08 00 06 04 00 02 08 00  27 1a f5 59 c0 a8 7a 07   ········ '··Y··z·
0020  00 00 00 00 00 00 c0 a8  7a 01                     ········ z·
```

Wireshark capture file properties information.



Details

File

Name:	C:\Users\User\Downloads\[Activity5]NetCapture_Scenario.pcapng
Length:	30 kB
Hash (SHA256):	e3a4b22d7b6b69e02289503bd21478cea95550ff08c0c84247860c967201f65e
Hash (SHA1):	e24017ef2722fd5e081f6b029015adc8b0e18928
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2023-02-25 18:00:18
Last packet:	2023-02-25 18:01:07
Elapsed:	00:00:48

Capture

Hardware:	Intel(R) Core(TM) i7-9750H CPU @ 2.60GHz (with SSE4.2)
OS:	Linux 6.0.0-kali3-amd64
Application:	Dumpcap (Wireshark) 4.0.3 (Git v4.0.3 packaged as 4.0.3-1)

Interfaces

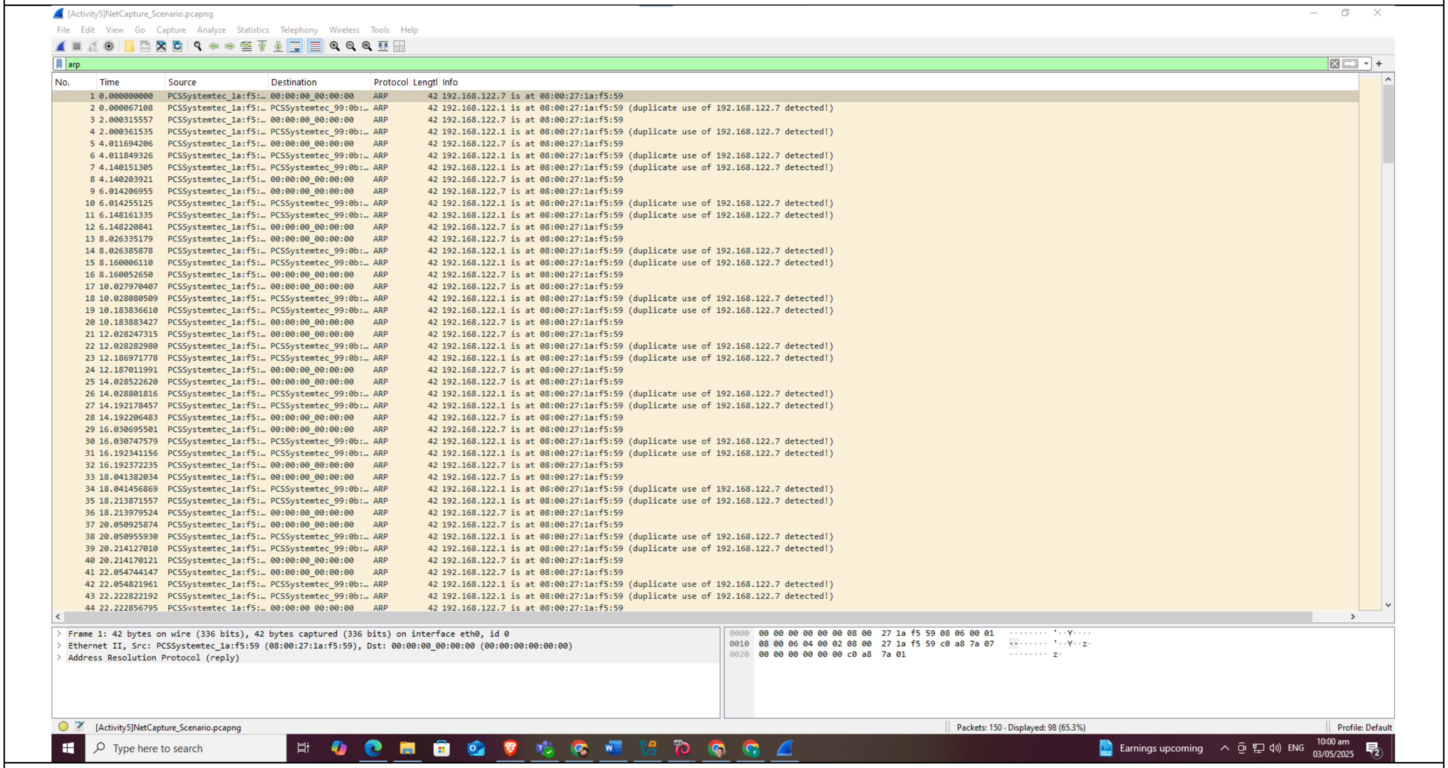
Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
eth0	0 (0.0%)	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	150	150 (100.0%)	—
Time span, s	48.430	48.430	—
Average pps	3.1	3.1	—
Average packet size, B	169	169	—
Bytes	25302	25302 (100.0%)	0
Average bytes/s	522	522	—
Average bits/s	4179	4179	—

Wireshark Filtering (ARP)

Display here the result of the Wireshark filter command.



```
arp
```

```
No.   Time         Source                 Destination            Protocol Lengtl Info
    1 0.000000000  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
    2 0.000067108  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    3 2.000315557  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
    4 2.000361535  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    5 4.011694206  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
    6 4.011849326  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    7 4.140151305  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
    8 4.140203921  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
    9 6.014206955  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   10 6.014255125  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   11 6.148161335  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   12 6.148220841  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   13 8.026335179  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   14 8.026385878  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   15 8.160006110  PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   16 8.160052650  PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   17 10.027970407 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   18 10.028080509 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   19 10.183836610 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   20 10.183883427 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   21 12.028247315 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   22 12.028282980 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   23 12.186971778 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   24 12.187011991 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   25 14.028522620 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   26 14.028801816 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   27 14.192178457 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   28 14.192206483 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   29 16.030695501 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   30 16.030747579 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   31 16.192341156 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   32 16.192372235 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   33 18.041382034 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   34 18.041456869 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   35 18.213871557 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   36 18.213979524 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   37 20.050925874 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   38 20.050955930 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   39 20.214127010 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   40 20.214170121 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   41 22.054744147 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
   42 22.054821961 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   43 22.222822192 PCSSystemtec_1a:f5:…   PCSSystemtec_99:0b:…   ARP      42 192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detected!)
   44 22.222856795 PCSSystemtec_1a:f5:…   00:00:00_00:00:00      ARP      42 192.168.122.7 is at 08:00:27:1a:f5:59
```

```
> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0
> Ethernet II, Src: PCSSystemtec_1a:f5:59 (08:00:27:1a:f5:59), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
> Address Resolution Protocol (reply)
```

```
0000  00 00 00 00 00 00 08 00  27 1a f5 59 08 06 00 01   ········ '··Y····
0010  08 00 06 04 00 02 08 00  27 1a f5 59 c0 a8 7a 07   ········ '··Y··z·
0020  00 00 00 00 00 00 c0 a8  7a 01                     ········ z·
```

```
[Activity5]NetCapture_Scenario.pcapng    Packets: 150 · Displayed: 98 (65.3%)    Profile: Default
```

Observation and Findings

What do the filter result suggest? Explain!

The filter results suggest that this is an ARP (Address Resolution Protocol) traffic capture. The pattern shows a series of ARP requests and replies between devices. There are numerous entries marked with "duplicate use of 192.168.122.7 detected!" which indicates that multiple packets are using the same IP address, potentially signaling an ARP-related issue such as an ARP storm or possible address conflicts.

The IP Address associated with the MAC Address 08:00:27:1a:f5:59 is 192.168.122.7.
This can be seen in the packet details section at the bottom of the screen where it shows: "Ethernet II, Src: PCSSystemtec_1a:f5:59 (08:00:27:1a:f5:59), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)"

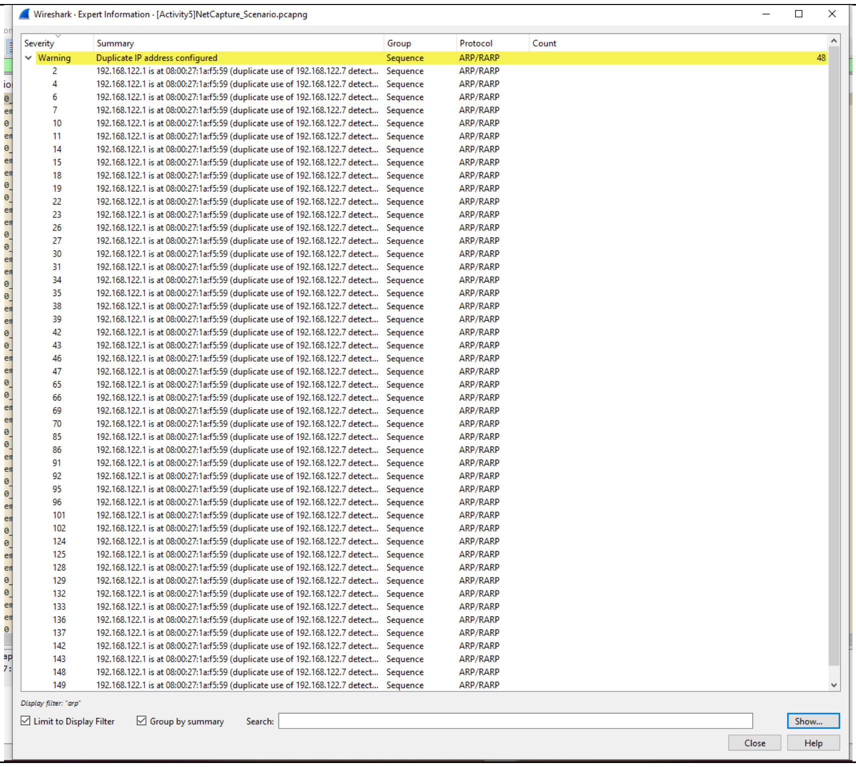
And throughout the capture, this MAC address is consistently associated with the IP 192.168.122.7 as shown in the "Info" column.

What is the IP Address associated with the MAC Address (08:00:27:1a:f5:59)?

IP Address : 192.168.122.7

Wireshark Expert Information

Display here the Expert Information summary report.



Wireshark · Expert Information · [Activity5]NetCapture_Scenario.pcapng

Severity	Summary	Group	Protocol	Count
Warning	Duplicate IP address configured	Sequence	ARP/RARP	48
2	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
4	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
6	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
7	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
10	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
11	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
14	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
15	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
18	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
19	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
22	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
23	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
26	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
27	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
30	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
31	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
34	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
35	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
38	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
39	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
42	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
43	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
46	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
47	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
65	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
66	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
69	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
70	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
85	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
86	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
91	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
92	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
95	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
96	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
101	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
102	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
124	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
125	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
128	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
129	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
132	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
133	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
136	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
137	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
142	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
143	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
148	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	
149	192.168.122.1 is at 08:00:27:1a:f5:59 (duplicate use of 192.168.122.7 detect...	Sequence	ARP/RARP	

Display filter: "arp"

☑ Limit to Display Filter ☑ Group by summary Search:

Observation and Findings

What do the expert information result suggest? Explain!

Based on the expert information display in Wireshark, the results suggest an IP address conflict on the network. The system has detected multiple instances of duplicate use of the IP address 192.168.122.7 associated with the MAC address 08:00:27:1a:f5:59.

The numerous warnings (indicated by the yellow triangle with exclamation mark in the "Severity" column) all show the same message: "Duplicate IP address configured" and "duplicate use of 192.168.122.7 detected." This is a clear indication of an IP address conflict where multiple devices are attempting to use the same IP address (192.168.122.7) on the network simultaneously.

This type of conflict can cause connectivity issues, intermittent network problems, and communication failures as packets may be routed to the wrong device. The expert information is specifically flagging this as a warning because IP address conflicts are a significant network issue that requires resolution to ensure proper network functionality.

Question and Answer

What is the IP and MAC Address of the victim machine in the captured network traffic?

Answer (Victim's IP Address)	:	192.168.122.7
Answer (Victim's MAC Address)	:	08:00:27:1a:f5:59

What is the IP and MAC Address of the DHCP Server in the captured network traffic?

Answer (DHCP IP Address)	:	192.168.56.101
Answer (DHCP MAC Address)	:	08:00:27:E1:05:6B

What is the sniffed password credential of the user "admin" in the captured network traffic?

Answer: admin123

Mitigation and Recommendations

What are the necessary countermeasures to avoid or prevent Denial-of-Service attacks.

1. Implement firewall rules to block unauthorized port scanning (like the nmap SYN stealth scans shown)
2. Configure IDS/IPS systems to detect and alert on scanning activities
3. Disable responses from unused ports and services to minimize attack surface
4. Use network segmentation to isolate critical systems
5. Implement rate limiting to prevent network flooding
6. Deploy anti-spoofing measures to prevent ARP and DHCP-based attacks
7. Use DHCP snooping on switches to validate DHCP traffic and prevent rogue DHCP servers
8. Configure dynamic ARP inspection to validate ARP packets
9. Implement secure DHCP configurations with proper lease time and reservation policies
10. Regularly monitor network traffic for unusual patterns or unauthorized scanning activities
11. Use load balancers and traffic distribution systems for critical services
12. Employ DDoS protection services for internet-facing resources

ACTIVITY RUBRICS

Group Name M.O. Saturday, May 3, 2025

Members Surname, First Name MI. (Alphabetical)

Angeles, Johanes P.
Balbuena, Alezzandrei Ericka A.
Canivel, Adrianne Bleu R.

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	**Beginning (1 point)**	**Developing (2 points)**	**Proficient (3 points)**	**Exemplary (4 points)**	
Use of Tools & Techniques	No attempt to use relevant tool(s).	Incorrect or unsuitable tool(s) selected.	Tool(s) used is/are somewhat suitable but not optimal.	Selected appropriate tool(s) with minor mismatches to the scenario.	Selected the most appropriate tool(s) for the task based on scenario.	
Execution of Simulation	No attempt to execute attack simulation.	Poorly executed; goals unmet; major safety/ethical concerns.	Execution had flaws; goals only partially met; some safety concerns.	Attack executed with minor issues; met most goals; adhered to safety.	MITM attack executed safely, ethically, and effectively within controlled environment; met all goals.	
Use of Wireshark Filters and Features	No attempt to perform filtering of network traffic data.	Filters not used or configured incorrectly, leading to large irrelevant data.	Basic filters applied; excessive or irrelevant data captured.	Capture filters set up correctly with minor inefficiencies.	Capture filters configured accurately; unnecessary data excluded effectively.	
	No attempt to use Wireshark features.	Wireshark features not used effectively; manual analysis dominates.	Limited use of Wireshark features; investigation hindered by inefficiency.	Basic features used effectively; advanced features used with some errors.	Advanced features used effectively (e.g., filters, color coding, statistics)	
Analysis, Interpretation and Mitigation	No attempt to conduct analysis and interpretation.	Minimal or incorrect analysis; important information overlooked.	Basic analysis performed, but some important findings are missed or misinterpreted.	Results analyzed accurately but with some minor gaps in interpretation.	Detailed and accurate analysis of results; clear identification of open ports, services, and potential vulnerabilities.	
	No attempt to provide recommendations for mitigation.	Incorrect recommendations for mitigation.	Generalized or incomplete recommendations; lacks actionable steps.	Mostly accurate and actionable recommendations with minor omissions.	Accurate and actionable recommendations tailored to the scenario.	
Documentation	No attempt to provide report documentation of findings.	Poor documentation of findings; lacks structure or critical details.	Basic report provided with significant omissions or unclear explanations.	Detailed report provided; minor gaps in methods or findings.	Comprehensive report including methods, findings, and recommendations.	

Total Score and Feedback				
☐ Exemplary	20	Exemplary work demonstrating mastery of Wireshark features, thorough investigation, analysis, and comprehensive reporting.	**TOTAL POINTS EARNED (20 max points)**	
☐ Proficient	16-19	Solid performance with minor gaps in technical skills or documentation.		
☐ Developing	12-15	Basic understanding of Wireshark and investigation concepts; several significant gaps in execution.		
☐ Beginning	8-11	Minimal effort or understanding; critical errors or omissions in the capture, analysis, or reporting.		
☐ Not Attempted	0-7	Indicates failure to perform network investigation and analysis.		

Evaluated by: **Mr. Edward Matthew Sanmocte** Name of Course Instructor	**Remarks/Comments**