

CYSE 301: Cybersecurity Technique and Operations

Assignment 2: Traffic Tracing and Sniffing

- **Task A – Get started with Wireshark**

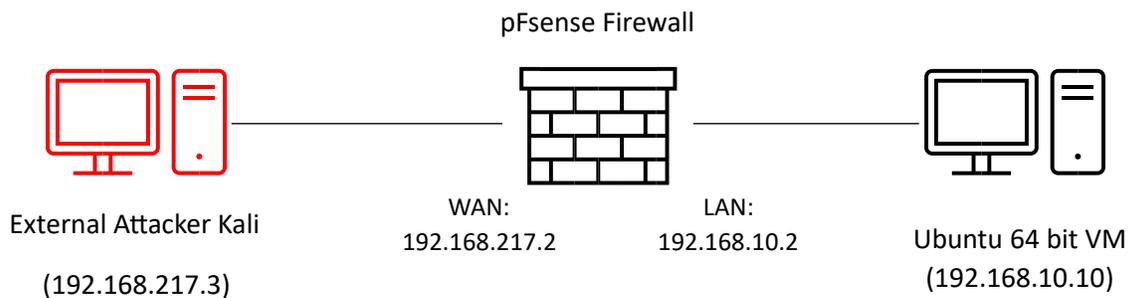
This document covers the first half of the assignment #2. The second half will be released after the complete discussion of Computer Network. Student needs to submit a report that covers both halves.

Each student needs to login into the **CCIA virtual environment** to complete this assignment.

Task A: Get started with Wireshark (5 point each x 6 questions = 30 points)

In this task, you will be using Wireshark on External Kali to monitor the traffic when External Kali and Ubuntu VM are talking to each other.

*Tip: Please power on the pfsense VM and **DO NOT** revert to a previous checkpoint.*



You should keep Wireshark running in the background while performing the following tasks.

1. Open Wireshark on External Kali and listen on interface "eth0".
2. Open a new terminal then ping Ubuntu VM for 5 – 10 secnds.
3. **Stop capturing (the red button on the tool bar).**

Now, answer the following questions. You need to provide a screenshot that contains the answers to each question.

Q1. How many packets are captured in total? How many packets are displayed? **171 packets**

The screenshot shows the Wireshark interface with the following details:

- Packet List:**

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	192.168.217.3	192.168.10.10	ICMP	98
2	0.003809800	192.168.10.10	192.168.217.3	ICMP	98
3	1.001505800	192.168.217.3	192.168.10.10	ICMP	98
4	1.014005500	192.168.10.10	192.168.217.3	ICMP	98
5	2.003286100	192.168.217.3	192.168.10.10	ICMP	98
6	2.027299300	192.168.10.10	192.168.217.3	ICMP	98
- Packet Details:**
 - Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 - Ethernet II, Src: Microsof_40:57:05 (00:15:5d:40:57:05), Dst: Microsof_40:57:1f (00:15:5d:40:57:1f)
 - Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
 - Internet Control Message Protocol
- Packet Bytes:**

```
0000  00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00  ..]@w... ]@w...E.
0010  00 54 5b 7e 40 00 40 01 7a cc c0 a8 d9 03 c0 a8  -T[~@ @ z.....
0020  0a 0a 08 00 7b 39 18 71 00 01 b9 68 0f 65 00 00  ....{9-q ...h.e..
0030  00 00 d7 b3 05 00 00 00 00 00 10 11 12 13 14 15  .....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,- ./012345
0060  36 37 67
```

The status bar at the bottom of the Wireshark window shows: **wireshark...IX.pcapng Packets: 171 - Displayed: 171 (100.0%) - Dropped: 0 (0.0%) Profile: Default**

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous question (Q1). **171 total packets total and 126 packets displayed after filtering.**

The screenshot shows the Wireshark network protocol analyzer interface. The display filter is set to 'icmp'. The packet list pane shows several ICMP packets. The packet details pane shows the structure of an ICMP Echo (ping) request. The packet bytes pane shows the raw hex and ASCII data of the packet. The status bar at the bottom indicates that 171 packets were captured, 126 were displayed (73.7%), and 0 were dropped.

No.	Time	Source	Destination	Protocol	Length
1	0.000000000	192.168.217.3	192.168.10.10	ICMP	98
2	0.003809800	192.168.10.10	192.168.217.3	ICMP	98
3	1.001505800	192.168.217.3	192.168.10.10	ICMP	98
4	1.0014005500	192.168.10.10	192.168.217.3	ICMP	98
5	2.003286100	192.168.217.3	192.168.10.10	ICMP	98
6	2.002799300	192.168.10.10	192.168.217.3	ICMP	98

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
Ethernet II, Src: Microsof_40:57:05 (00:15:5d:40:57:05), Dst: Microsof_40:57:1f (08:00:0c:27:1f:00)
Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.10.10
Internet Control Message Protocol

```
0000  00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00  ..]@w... ]@w...E.  
0010  00 54 5b 7e 40 00 40 01 7a cc c0 a8 d9 03 c0 a8  .T[-@.@.z.....  
0020  0a 0a 08 00 7b 39 18 71 00 01 b9 68 0f 65 00 00  ...{9.q...h.e..  
0030  00 00 d7 b3 05 00 00 00 00 00 10 11 12 13 14 15  .....  
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  ..... !"#$$%  
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &!()*+,-./012345  
0060  36 37 67
```

Internet Co...l: Protocol: Packets: 171 · Displayed: 126 (73.7%) · Dropped: 0 (0.0%) Profile: Default

Q3. Select an Echo (reply) message from the list. What are the source and destination IPs of this packet? What are the sequence number and the size of the data? What is the response time? **Source: 192.168.10.10, destination: 192.168.217.3. Sequence number: 2, size 48 bytes. Response time:12.5MS.**

The screenshot shows a Wireshark capture on interface *eth0. The packet list pane displays several ICMP Echo (ping) messages. The selected packet (Frame 4) is an Echo (ping) reply from 192.168.10.10 to 192.168.217.3, with sequence number 2 and a length of 98 bytes. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

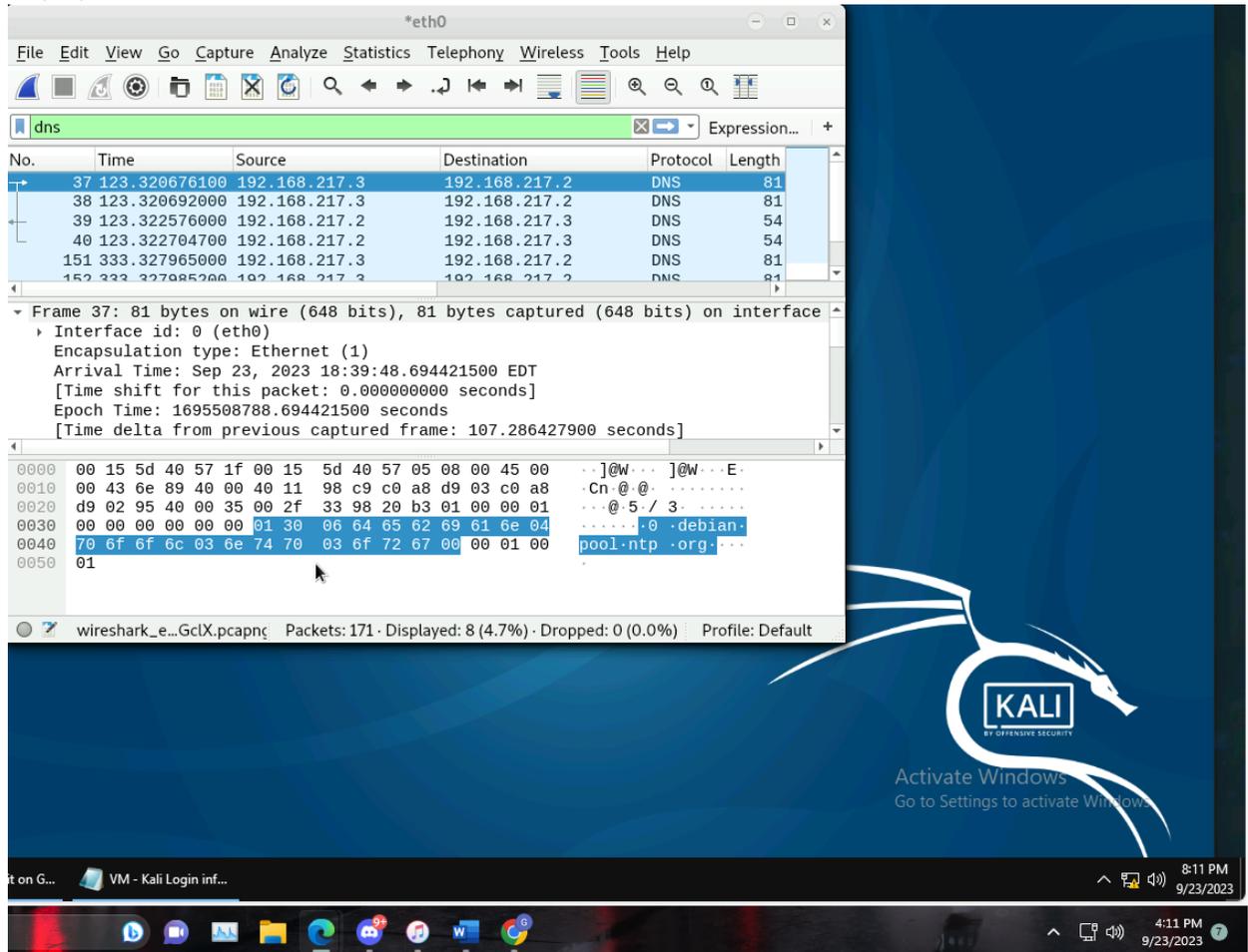
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) request id=0x1871, seq=1/256, ttl=64 (reply in 2)
2	0.000000	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) reply id=0x1871, seq=1/256, ttl=63 (request in...)
3	0.000000	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) request id=0x1871, seq=2/512, ttl=64 (reply in 4)
4	0.000000	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) reply id=0x1871, seq=2/512, ttl=63 (request in...)
5	0.000000	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) request id=0x1871, seq=3/768, ttl=64 (reply in 6)
6	0.000000	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) reply id=0x1871, seq=3/768, ttl=63 (request in...)
7	0.000000	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) request id=0x1871, seq=4/1024, ttl=64 (reply in ...)
8	0.000000	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) reply id=0x1871, seq=4/1024, ttl=63 (request i...)
9	0.000000	192.168.10.10	192.168.217.3	ICMP	98	Echo (ping) request id=0x1871, seq=5/1280, ttl=64 (reply in ...)
10	0.000000	192.168.217.3	192.168.10.10	ICMP	98	Echo (ping) reply id=0x1871, seq=5/1280, ttl=63 (request i...)

Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0
 Ethernet II, Src: Microsof_40:57:1f (00:15:5d:40:57:1f), Dst: Microsof_40:57:05 (00:15:5d:40:57:05)
 Internet Protocol Version 4, Src: 192.168.10.10, Dst: 192.168.217.3
 Internet Control Message Protocol

```

0000  00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00  ..]@W... ]@W...E.
0010  00 54 a7 38 00 00 3f 01 70 12 c0 a8 0a 0a c0 a8  .T8..?. p.....
0020  d9 03 00 00 b4 32 18 71 00 02 ba 68 0f 65 00 00  ....2.q...h.e..
0030  00 00 a5 b9 05 00 00 00 00 00 10 11 12 13 14 15  .....,.....
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25  .....,.....!#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35  &'()*+,-./012345
0060  36 37                                     67
  
```

Q4. Apply “DNS” as a display filter in Wireshark. How many packets are displayed? **4 Packets are displayed.**



Q5. Find a DNS query packet. What is the domain name this host is trying to resolve? What is the source IP and port number, destination IP and port number? Please express in the format: **IP:port.**

Microsoft. Source:192.168.217.3:38208. Destination:192.168.217.2:53.

Wireshark - Packet 37 - eth0

- Frame 37: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
- Ethernet II, Src: Microsof_40:57:05 (08:15:5d:40:57:05), Dst: Microsof_40:57:1f (08:15:5d:40:57:1f)
 - Destination: Microsof_40:57:1f (08:15:5d:40:57:1f)
 - Source: Microsof_40:57:05 (08:15:5d:40:57:05)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.217.3, Dst: 192.168.217.2
 - 0100 ... = Version: 4
 - ... 0101 = Header Length: 20 bytes (5)
 - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 67
 - Identification: 0x6e89 (28297)
 - Flags: 0x4000, Don't fragment
 - Time to live: 64
 - Protocol: UDP (17)
 - Header checksum: 0x98c9 [validation disabled]
 - [Header checksum status: Unverified]
 - Source: 192.168.217.3
 - Destination: 192.168.217.2
- User Datagram Protocol, Src Port: 38208, Dst Port: 53
- Domain Name System (query)

```
0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 00 00 45 00  ...]@W... ]@W...E
0010 00 43 6e 89 40 00 40 11 98 c9 c0 a8 d9 03 c0 a8  ...Cn @ @
0020 d9 02 95 40 00 35 00 2f 33 98 20 b3 01 00 00 01  ...@5 3
0030 00 00 00 00 00 01 30 06 64 65 62 69 61 6e 04  ...@ @ .debian
0040 70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 01 00  pool.ntp .org
0050 01
```

Windows taskbar and system tray area. Includes Start button, Search bar, taskbar icons (Edge, File Explorer, etc.), system tray icons (network, volume), and system clock showing 4:45 PM on 9/23/2023.

Activate Windows
Go to Settings to activate Windows.

Q6. Find the **corresponding** DNS response to the query you selected at the previous step, and what is the source IP and port number, destination IP and port number? What is the message replied from the DNS server? **Source:192.168.217.2:53. Destination:192.168.217.3:38208. Refused.**

Wireshark - Packet 39 - eth0

... 0101 = Header Length: 20 bytes (5)

- Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 40
- Identification: 0x2a2d (10797)
- Flags: 0x0000
- Time to live: 64
- Protocol: UDP (17)
- Header checksum: 0x1d41 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.217.2
- Destination: 192.168.217.3
- User Datagram Protocol, Src Port: 53, Dst Port: 38208
- Domain Name System (response)
- Transaction ID: 0x20b3
- Flags: 0x8105 Standard query response, Refused
- Questions: 0
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 0
- [Request In: 37]
- [Time: 0.001899900 seconds]

0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00 ...]@W...]@W...E-

0010 00 28 2a 2d 00 00 40 11 1d 41 c0 a8 d9 02 c0 a8 ...(*-.-@- A-.....

0020 d9 03 00 35 95 40 00 14 95 40 20 b3 81 05 00 00 ...-5@-.-@-.....

0030 00 00 00 00 00 00

No.: 39 - Time: 123.322576000 - Source: 192.168.217.2 - Destination: 192.168.217.3 - Protocol: DNS - Length: 54 - Info: Standard query response 0x20b3 Refused

Help Close

Activate Windows
Go to Settings to activate Windows.

4:54 PM
9/23/2023