

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

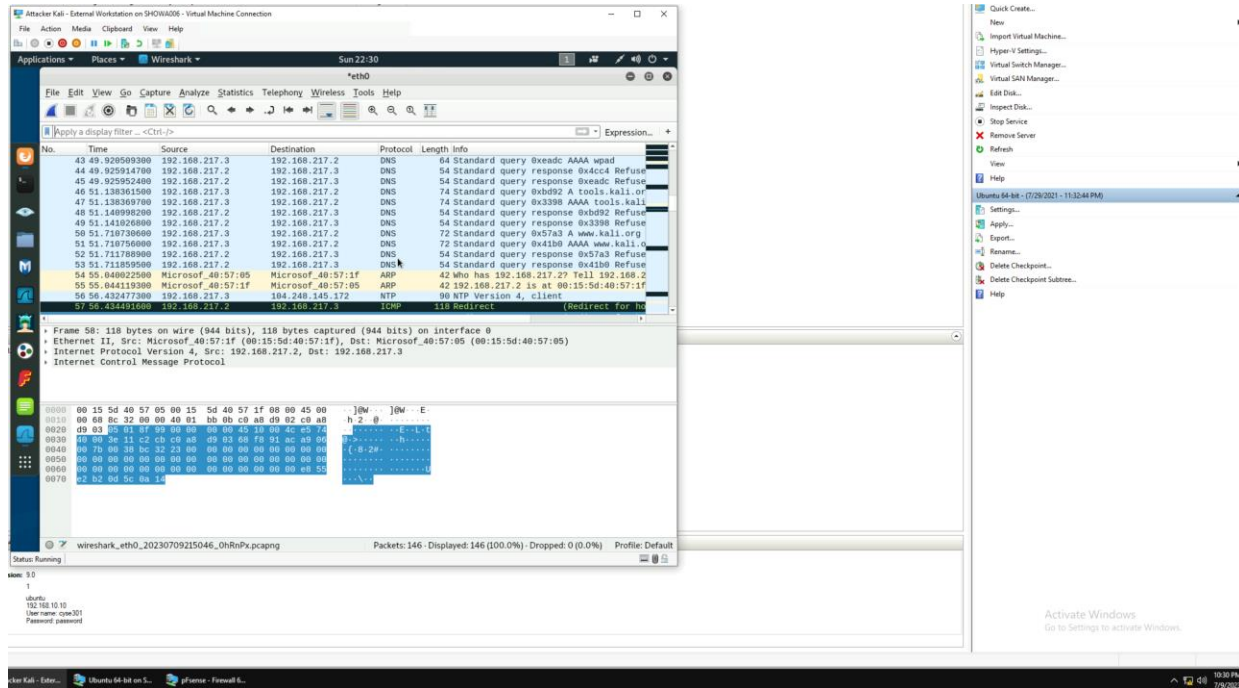
Assignment 2: Traffic Tracing and Sniffing pt A.

Stuart N. Howard

01241576

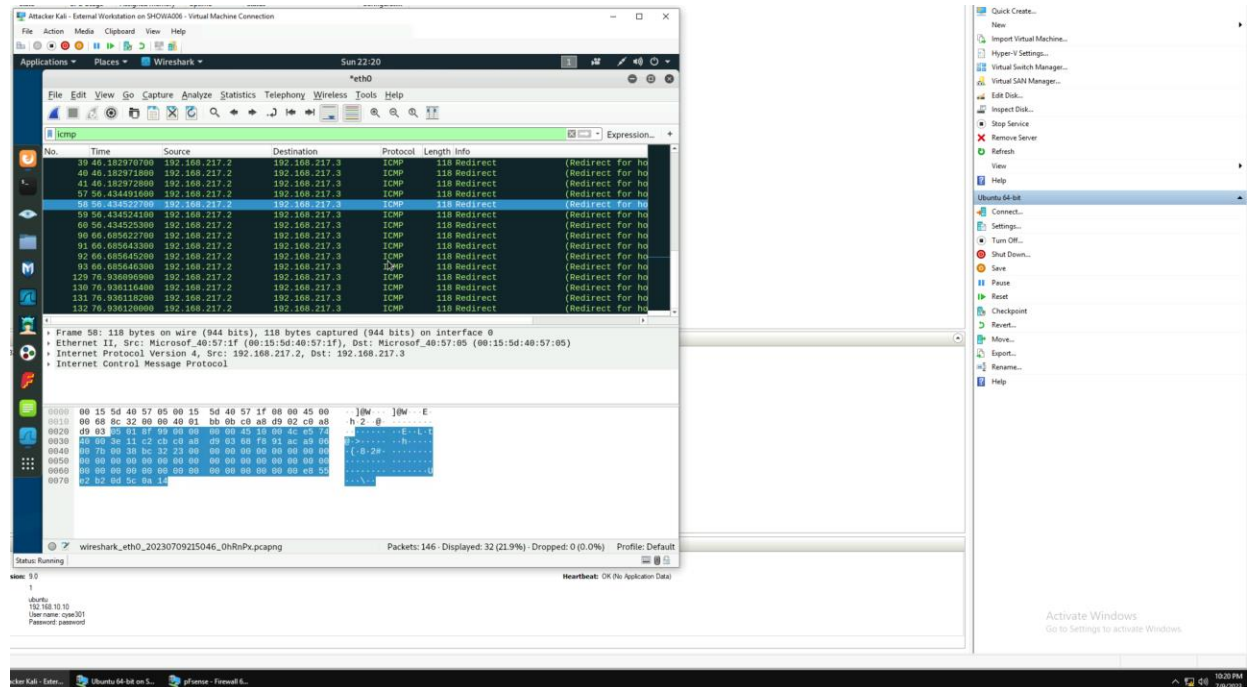
Q1. How many packets are captured in total? How many packets are displayed?

146 Total packages captured, 146 packages displayed.



Q2. Apply "ICMP" as a display filter in Wireshark. Then repeat the previous question (Q1).

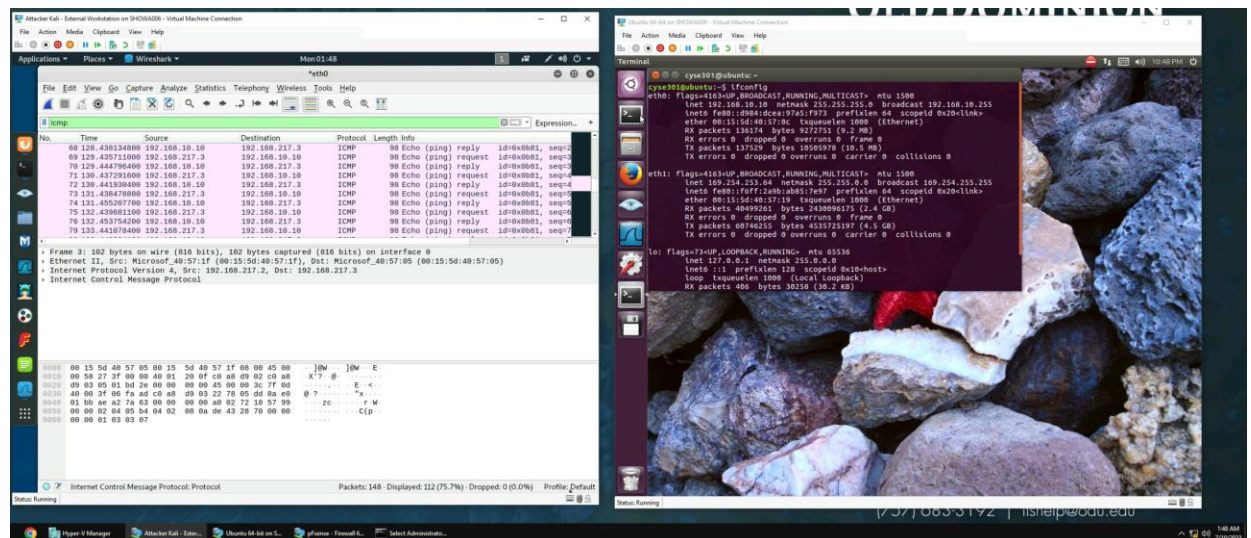
146 Total packages captured, 32 packages displayed.



Q3. Select an Echo (reply) message from the list.

What are the source and destination IPs of this packet?

Source IP is 192.168.10.10 and destination IP is 192.168.217.3



What are the sequence number and the size of the data?

Sequence number is (BE) 6 (LE) 1536 and data size is 48bytes

What is the response time?

Response time is 14.037 ms

Attacker Kali - External Workstation on SHOWA006 - Virtual Machine Connection

File Action Media Clipboard View Help

Applications Places Wireshark Mon 02:01

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|---------------|---------------|---------------|----------|--------|-------------------------------------|
| 68 | 128.438134800 | 192.168.10.10 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0xb81, seq=2 |
| 69 | 129.435711000 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0xb81, seq=3 |
| 70 | 129.444796400 | 192.168.10.10 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0xb81, seq=3 |
| 71 | 130.437291600 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0xb81, seq=4 |
| 72 | 130.441930400 | 192.168.10.10 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0xb81, seq=4 |
| 73 | 131.438478800 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0xb81, seq=5 |
| 74 | 131.455207700 | 192.168.10.10 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0xb81, seq=5 |
| 75 | 132.439681100 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0xb81, seq=6 |
| 76 | 132.453754200 | 192.168.10.10 | 192.168.217.3 | ICMP | 98 | Echo (ping) reply id=0xb81, seq=6 |
| 79 | 133.441078400 | 192.168.217.3 | 192.168.10.10 | ICMP | 98 | Echo (ping) request id=0xb81, seq=7 |

Code: 0
Checksum: 0x82a7 [correct]
[Checksum Status: Good]
Identifier (BE): 2945 (0xb81)
Identifier (LE): 33035 (0x810b)
Sequence number (BE): 6 (0x0006)
Sequence number (LE): 1536 (0x0600)
[Request frame: 75]
[Response time: 14.073 ms]
Timestamp from icmp data: Jul 10, 2023 01:45:38.000000000 EDT
[Timestamp from icmp data (relative): 0.341530700 seconds]
Data (48 bytes)

```
0000 00 15 5d 40 57 05 00 15 5d 40 57 1f 08 00 45 00  ..]@W... ]@W... E-
0010 00 54 8a 91 00 00 3f 01 8c b9 c0 a8 0a 0a c0 a8  .T....?.. ....
0020 d9 03 00 00 82 a7 0b 81 00 06 02 9b ab 64 00 00  .d....
0030 00 00 00 ff 04 00 00 00 00 00 10 11 12 13 14 15  .!""#$%&'()*+,-./012345
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  .
0060 36 37 67
```

Internet Control Message Protocol: Protocol Packets: 148 - Displayed: 112 (75.7%) - Dropped: 0 (0.0%) Profile: Default

Status: Running

Activate Windows
Go to Settings to activate Windows.

2:01 AM
7/10/2023

10:01 PM
7/9/2023

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

146 Total packages captured, 98 packages displayed.

The screenshot shows the Wireshark network protocol analyzer interface. The display filter at the top is set to 'dns'. The packet list on the left shows 146 packets captured, with 98 displayed. The packet details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Domain Name System (DNS) fields. The status bar at the bottom indicates 'Packets: 146 - Displayed: 98 (67.1%) - Dropped: 0 (0.0%)'.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|---------------------------------------|
| 112 | 74.166163000 | 192.168.217.3 | 192.168.217.2 | DNS | 79 | Standard query 0x49f9 A home.pearsonv |
| 113 | 74.166175300 | 192.168.217.3 | 192.168.217.2 | DNS | 79 | Standard query 0xb701 AAAA home.pear |
| 114 | 74.168083800 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x49f9 Refuse |
| 115 | 74.168101400 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xb701 Refuse |
| 116 | 74.173099500 | 192.168.217.3 | 192.168.217.2 | DNS | 64 | Standard query 0x17c3 A wpad |
| 117 | 74.173709300 | 192.168.217.3 | 192.168.217.2 | DNS | 64 | Standard query 0x03c9 AAAA wpad |
| 118 | 74.175569300 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x17c3 Refuse |
| 119 | 74.175620900 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x03c9 Refuse |
| 120 | 74.294501700 | 192.168.217.3 | 192.168.217.2 | DNS | 83 | Standard query 0xaa55 A www.backtrack |
| 121 | 74.294512600 | 192.168.217.3 | 192.168.217.2 | DNS | 83 | Standard query 0xbccc AAAA www.backtr |
| 122 | 74.295703500 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xaa55 Refuse |
| 123 | 74.295745000 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xbccc Refuse |
| 124 | 75.311485400 | 192.168.217.3 | 192.168.217.2 | DNS | 76 | Standard query 0xab33 A www.facebook |
| 125 | 75.311493300 | 192.168.217.3 | 192.168.217.2 | DNS | 76 | Standard query 0xb338 AAAA www.facebo |
| 126 | 75.311853600 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xab33 Refuse |

Q5. Find a DNS query packet.

What is the domain name this host is trying to resolve?

www.linkedin.com

The screenshot displays a Kali Linux virtual machine environment. The main window is Wireshark, which is capturing network traffic on the 'eth0' interface. A filter 'dns' is applied to the packet list. The list shows several DNS packets, with packet 46 selected. This packet is a standard query for 'www.linkedin.com'. The packet details pane shows the query structure, including the question section with 'Name: www.linkedin.com' and 'type AAAA, class IN'. The packet bytes pane shows the raw data in hexadecimal and ASCII. The status bar at the bottom indicates that 146 packets are displayed, with 98 (67.1%) shown and 0 dropped.

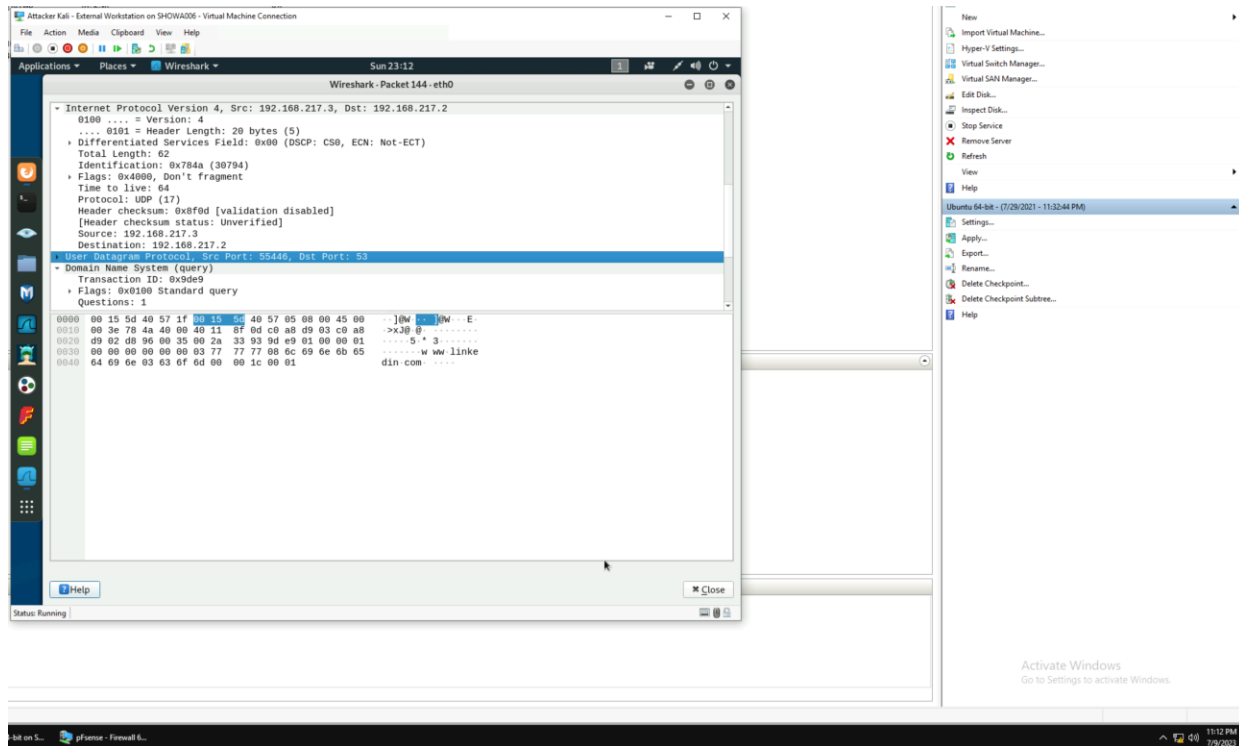
| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|---------------------------------------------|
| 25 | 75.311493380 | 192.168.217.3 | 192.168.217.2 | DNS | 76 | Standard query 0xb338 AAAA www.facebook.com |
| 26 | 75.311853600 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xab33 Refused |
| 27 | 75.311876300 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xb338 Refused |
| 33 | 79.246769900 | 192.168.217.3 | 192.168.217.2 | DNS | 71 | Standard query 0xb387 A twitter.com |
| 34 | 79.246773900 | 192.168.217.3 | 192.168.217.2 | DNS | 71 | Standard query 0xd19f AAAA twitter.com |
| 35 | 79.247483700 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xb387 Refused |
| 36 | 79.247510400 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xd19f Refused |
| 39 | 81.283172900 | 192.168.217.3 | 192.168.217.2 | DNS | 75 | Standard query 0xa8b3 A wpad.mshome.net |
| 40 | 81.283180200 | 192.168.217.3 | 192.168.217.2 | DNS | 75 | Standard query 0xb8b9 AAAA wpad.mshome.net |
| 41 | 81.284273200 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xa8b3 Refused |
| 42 | 81.284280900 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0xb8b9 Refused |
| 43 | 81.724055500 | 192.168.217.3 | 192.168.217.2 | DNS | 76 | Standard query 0x19e2 A www.linkedin.com |
| 44 | 81.724064000 | 192.168.217.3 | 192.168.217.2 | DNS | 76 | Standard query 0x05d0 AAAA www.linkedin.com |
| 45 | 81.728157600 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x19e2 Refused |
| 46 | 81.728157900 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x9de9 Refused |

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
- Queries
- www.linkedin.com: type AAAA, class IN
Name: www.linkedin.com
0000 00 15 5d 40 57 1f 00 15 5d 40 57 05 00 00 45 00 ...]0w ...]0w ... E:
0010 00 3e 78 4a 40 00 48 11 8f 0d c0 a8 d9 03 c0 a8 ... ->x30 0:
0020 09 02 d8 96 00 35 60 2a 33 93 0d e9 01 00 00 01 ... 5 * 3
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 04 09 68 83 63 6f 6d 00 00 1c 00 01 lin.com
Query Name (dns.qry.name), 18 bytes
Packets: 146 - Displayed: 98 (67.1%) - Dropped: 0 (0.0%) Profile: Default
Status: Running

What is the source IP and port number, destination IP and port number? Please express in the format: IP:port.

Source IP/port 192.168.217.3:55446

Dst IP/port 192.168.217.2:53



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

Source IP/port 192.168.217.2:53

Dst IP/port 192.168.217.3:55446?

What is the message replied from the DNS server?

Flags: 0x8105 Standard query response, Refused

