

OLD DOMINION UNIVERSITY

CYSE 301 CYBERSECURITY TECHNIQUES AND OPERATIONS

Assignment #2 Traffic Tracing and Sniffing

Ava Baratz
01192426

TASK A

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

The screenshot shows the Wireshark interface with the 'Capture File Properties' dialog box open for the eth0 interface. The 'Statistics' section is circled in red, showing the following data:

| Measurement | Captured | Displayed | Marked |
|------------------------|----------|---------------|--------|
| Packets | 36 | 36 (100.0%) | — |
| Time span, s | 20.018 | 20.018 | — |
| Average pps | 1.8 | 1.8 | — |
| Average packet size, B | 78 | 78 | — |
| Bytes | 2806 | 2806 (100.0%) | 0 |
| Average bytes/s | 140 | 140 | — |
| Average bits/s | 1,121 | 1,121 | — |

The background shows the main Wireshark window with a packet list containing 36 packets. The system tray at the bottom right indicates the time is 5:08 PM on 2/6/2023.

Here, I opened the WireShark Capture File Properties which shows there were 36 packets captured and 36 packets displayed in the eth0 interface.

TASK A (CONTINUED)

Q2. Apply “ICMP” as a display filter in Wireshark. Then repeat the previous step Q1.

The screenshot shows the Wireshark interface with the 'Capture File Properties' window open for the 'eth0' interface. The 'Statistics' tab is selected, and a red circle highlights the following data:

| Measurement | Captured | Displayed | Marked |
|------------------------|----------|--------------|--------|
| Packets | 36 | 14 (38.9%) | |
| Time span, s | 20.018 | 6.026 | — |
| Average pps | 1.8 | 2.3 | — |
| Average packet size, B | 78 | 98 | — |
| Bytes | 2806 | 1372 (48.9%) | 0 |
| Average bytes/s | 140 | 227 | — |
| Average bits/s | 1,121 | 1,821 | — |

The background shows the main Wireshark interface with the display filter 'icmp' applied in the search bar. The packet list on the left shows several ICMP packets, with packet 30 selected. The system tray at the bottom indicates the time is 5:09 PM on 2/6/2023.

Here, I applied the “icmp” display filter in the search bar. The capture file properties with the ICMP display filter show that there were 36 captured packets and 14 packets displayed in the eth0 interface.

TASK A (CONTINUED)

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?

The screenshot shows a Wireshark interface with a list of ICMP Echo (ping) messages. The 20th packet is selected, and its details are expanded. The source IP is 192.168.10.10 and the destination IP is 192.168.217.3. The sequence number is 3 and the length is 98 bytes. The details pane shows the following information:

- Time to live: 63
- Protocol: ICMP (1)
- Header checksum: 0xd582 [validation disabled]
- [Header checksum status: Unverified]
- Source: 192.168.10.10
- Destination: 192.168.217.3
- Internet Control Message Protocol
- Type: 0 (Echo (ping) reply)
- Code: 0
- Checksum: 0x8217 [correct]
- [Checksum Status: Good]
- Identifier (BE): 2392 (0x0958)

The packet bytes pane shows the raw data of the ICMP Echo (ping) reply, including the type, code, checksum, identifier, and sequence number.



I selected the 20th packet which is a reply message from the list. This packet has a source IP of 192.168.10.10 and a destination IP of 192.168.217.3.

), contact the ITS Help Desk:
92 | itshelp@odu.edu

TASK A (CONTINUED)

Q3. (Continued) Select an Echo (reply) message from the list. packet? What are the sequence number and the size of the data? What is the response time?

The screenshot shows a Wireshark interface with a list of ICMP Echo (ping) messages. The 20th packet is selected, and its details are expanded. The details pane shows the following information:

- [Checksum Status: Good]
- Identifier (BE): 2392 (0x0958)
- Identifier (LE): 22537 (0x5809)
- Sequence number (BE): 3 (0x0003)
- Sequence number (LE): 768 (0x0300)
- [Request frame: 19]
- [Response time: 12.878 ms]
- Timestamp from icmp data: Feb 6, 2023 16:59:17.000000000 EST
- [Timestamp from icmp data (relative): 0.856311600 seconds]
- Data (48 bytes)
- Data: 92de0c0000000000101112131415161718191a1b1c1d1e1f...
- [Length: 48]

The details pane also shows a hex dump of the data, which is a standard ICMP Echo reply structure.

Here, from the 20th packet which is a reply message, the Sequence Number (BE) is 3 (0x0003), and the sequence number (LE) is 768 (0x0300.) The data is 48 bytes. The response time is 12.878 ms.

TASK A (CONTINUED)

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

The screenshot shows the Wireshark interface with the 'Capture File Properties' window open for the interface 'eth0'. The display filter is set to 'dns'. The statistics table indicates that 36 packets were captured and 20 were displayed after applying the filter.

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

| Measurement | Captured | Displayed | Marked |
|------------------------|----------|--------------|--------|
| Packets | 36 | 20 (55.6%) | — |
| Time span, s | 20.018 | 20.018 | — |
| Average pps | 1.8 | 1.0 | — |
| Average packet size, B | 78 | 68 | — |
| Bytes | 2806 | 1350 (48.1%) | 0 |
| Average bytes/s | 140 | 67 | — |

Here, I applied “dns” in the search bar as a display filter in Wireshark. Using Wireshark capture file properties, it shows that 36 packets are captured and 20 packets are displayed with the DNS filter applied.

TASK A (CONTINUED)

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.

The screenshot displays the Wireshark interface on a Kali Linux virtual machine. The main window shows a list of captured packets on the interface eth0. The second packet is selected, and its details are expanded to show a Domain Name System (query) packet. The packet details include the source IP (192.168.217.3), destination IP (192.168.217.2), and the query for the domain 0x2b8a. The packet bytes pane shows the raw data of the query, including the domain name 0x2b8a. The system tray at the bottom right shows the date and time as 5:19 PM on 2/6/2023.

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|--------------|---------------|---------------|----------|--------|---------------------------------------|
| 1 | 0.000000000 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0x3d83 A 0.debian.pool |
| 2 | 0.000009500 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0x2b8a AAAA 0.debian.p |
| 3 | 0.003002500 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x3d83 Refuse |
| 4 | 0.003026500 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x2b8a Refuse |
| 5 | 5.003846200 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0x3d83 A 0.debian.pool |
| 6 | 5.003855800 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0x2b8a AAAA 0.debian.p |
| 7 | 5.005787700 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x3d83 Refuse |
| 8 | 5.005797600 | 192.168.217.2 | 192.168.217.3 | DNS | 54 | Standard query response 0x2b8a Refuse |
| 11 | 10.004405600 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0xe4b5 A 1.debian.pool |
| 12 | 10.004414700 | 192.168.217.3 | 192.168.217.2 | DNS | 81 | Standard query 0x96bb AAAA 1.debian.p |

Source: 192.168.217.3
Destination: 192.168.217.2
User Datagram Protocol, Src Port: 49868, Dst Port: 53
Domain Name System (query)
Transaction ID: 0x2b8a
Flags: 0x0100 Standard query
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
[Response In: 4]

```
0000  00 15 5d 40 57 1f 00 15 5d 40 57 05 08 00 45 00  ..]@W... ]@W...E.  
0010  00 43 cb 43 40 00 40 11 3c 0f c0 a8 d9 03 c0 a8  .C.C@.<.....  
0020  d9 02 c2 cc 00 35 00 2f 33 98 2b 8a 01 00 00 01  .....5/3+.....  
0030  00 00 00 00 00 00 01 30 06 64 65 62 69 61 6e 04  .....0 .debian.  
0040  70 6f 6f 6c 03 6e 74 70 03 6f 72 67 00 00 1c 00  pool.ntp.org...  
0050  01
```

Here, I selected the 2nd packet which is a standard query packet. The domain name that the host is trying to resolve is 0x2b8a. The source IP and source port is 192.168.217.3 : 49868. The destination IP and dst port is 168.192.217.2 : 53.