

# Part B – Wireshark Practical

## 1. HTTP Traffic (Application over TCP)

The image shows a Wireshark capture of HTTP traffic. The top pane displays a list of packets, with packet 404 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packets List:**

| No. | Time     | Source       | Destination  | Protocol | Length | Info                               |
|-----|----------|--------------|--------------|----------|--------|------------------------------------|
| 316 | 6.632735 | 172.20.8.138 | 23.215.0.136 | HTTP     | 489    | GET / HTTP/1.1                     |
| 404 | 7.281138 | 23.215.0.136 | 172.20.8.138 | HTTP     | 787    | HTTP/1.1 200 OK (text/html)        |
| 418 | 7.688329 | 172.20.8.138 | 23.215.0.136 | HTTP     | 429    | GET /favicon.ico HTTP/1.1          |
| 436 | 7.988996 | 23.215.0.136 | 172.20.8.138 | HTTP     | 997    | HTTP/1.1 404 Not Found (text/html) |

**Packet 404 Details:**

- Frame 404: Packet, 787 bytes on wire (6296 bits), 787 bytes captured (6296 bits) on interface \Device\NPF\_{ECEF2FF9-0D9D-4515-97B9-007541CEF741}
- Ethernet II, Src: Sophos\_d1:3f:f0 (7c:5a:1c:d1:3f:f0), Dst: Intel\_c5:89:56 (60:e3:2b:c5:89:56)
  - Destination: Intel\_c5:89:56 (60:e3:2b:c5:89:56)
  - Source: Sophos\_d1:3f:f0 (7c:5a:1c:d1:3f:f0)
  - Type: IPv4 (0x0800)
  - [Stream index: 27]
- Internet Protocol Version 4, Src: 23.215.0.136, Dst: 172.20.8.138
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 773
  - Identification: 0xa105 (41221)
  - 010. .... = Flags: 0x2, Don't fragment
  - ...0 0000 0000 0000 = Fragment Offset: 0
  - Time to Live: 64
  - Protocol: TCP (6)
  - Header Checksum: 0xc9f0 [validation disabled]
  - [Header checksum status: Unverified]
  - Source Address: 23.215.0.136
  - Destination Address: 172.20.8.138
  - [Stream index: 29]
- Transmission Control Protocol, Src Port: 80, Dst Port: 62070, Seq: 1, Ack: 436, Len: 733
  - Source Port: 80

**Raw Packet Data (Hex):**

```
0000 60 e3 2b c5 89 56 7c 0000 80 05 a1 05 40 00 40
0010 0020 00 8a 00 50 f2 76 e8 0030 00 ed 9a 0c 00 00 48
0040 30 30 20 4f 4b 0d 0a 0050 6e 67 65 73 3a 20 62
0060 74 65 6e 74 2d 54 79 0070 68 74 6d 6c 0d 0a 45
0080 34 37 33 61 31 38 65 0090 65 62 61 35 63 65 38
00a0 36 30 30 32 38 31 32 00b0 0d 0a 4c 61 73 74 2d
00c0 20 54 68 75 2c 20 30 00d0 35 20 31 36 3a 34 32
00e0 56 61 72 79 3a 20 41 00f0 6f 64 69 6e 67 0d 0a
0100 6e 63 6f 64 69 6e 67 0110 6f 6e 74 65 6e 74 2d
0120 36 33 0d 0a 43 61 63 0130 6c 3a 20 6d 61 78 2d
0140 0d 0a 44 61 74 65 3a 0150 44 65 63 20 32 30 32
0160 34 20 47 4d 54 0d 0a
```

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | Time     | Source       | Destination  | Protocol | Length | Info                               |
|-----|----------|--------------|--------------|----------|--------|------------------------------------|
| 316 | 6.632735 | 172.20.8.138 | 23.215.0.136 | HTTP     | 489    | GET / HTTP/1.1                     |
| 404 | 7.281138 | 23.215.0.136 | 172.20.8.138 | HTTP     | 787    | HTTP/1.1 200 OK (text/html)        |
| 418 | 7.680329 | 172.20.8.138 | 23.215.0.136 | HTTP     | 429    | GET /favicon.ico HTTP/1.1          |
| 436 | 7.988996 | 23.215.0.136 | 172.20.8.138 | HTTP     | 997    | HTTP/1.1 404 Not Found (text/html) |

Transmission Control Protocol, Src Port: 80, Dst Port: 62070, Seq: 1, Ack: 436, Len: 733

Source Port: 80  
Destination Port: 62070  
[Stream index: 5]  
[Stream Packet Number: 6]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 733]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 3899452645  
[Next Sequence Number: 734 (relative sequence number)]  
Acknowledgment Number: 436 (relative ack number)  
Acknowledgment number (raw): 4059609204  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x018 (PSH, ACK)  
Window: 237  
[Calculated window size: 30336]  
[Window size scaling factor: 128]  
Checksum: 0x9a0c [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
[Client Contiguous Streams: 1]

Internet Protocol Version 4 (ip), 20 bytes

Packets: 557 · Displayed: 4 (0.7%) · Dropped: 0 (0.0%)

Profile: Default

\*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

| No. | Time     | Source       | Destination  | Protocol | Length | Info                               |
|-----|----------|--------------|--------------|----------|--------|------------------------------------|
| 316 | 6.632735 | 172.20.8.138 | 23.215.0.136 | HTTP     | 489    | GET / HTTP/1.1                     |
| 404 | 7.281138 | 23.215.0.136 | 172.20.8.138 | HTTP     | 787    | HTTP/1.1 200 OK (text/html)        |
| 418 | 7.680329 | 172.20.8.138 | 23.215.0.136 | HTTP     | 429    | GET /favicon.ico HTTP/1.1          |
| 436 | 7.988996 | 23.215.0.136 | 172.20.8.138 | HTTP     | 997    | HTTP/1.1 404 Not Found (text/html) |

[Server Contiguous Streams: 1]  
TCP payload (733 bytes)

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n  
Accept-Ranges: bytes\r\n  
Content-Type: text/html\r\n  
ETag: "bc2473a18e003bdb249eba5ce893033f:1760028122.592274"\r\n  
Last-Modified: Thu, 09 Oct 2025 16:42:02 GMT\r\n  
Vary: Accept-Encoding\r\n  
Content-Encoding: gzip\r\n  
Content-Length: 363\r\n  
Cache-Control: max-age=86000\r\n  
Date: Mon, 01 Dec 2025 10:22:54 GMT\r\n  
Via: HTTP/1.1 forward-http.proxy:3128\r\n  
Connection: keep-alive\r\n  
\r\n  
[Request in frame: 316]  
[Time since request: 648.403000 milliseconds]  
[Request URI: /]  
[Full request URI: http://example.com/]  
Content-encoded entity body (gzip): 363 bytes -> 513 bytes  
File Data: 513 bytes

Line-based text data: text/html (1 lines)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 557 · Displayed: 4 (0.7%) · Dropped: 0 (0.0%)

Profile: Default

## 2. TCP Packets

Wireshark packet capture showing a TCP ACK packet (No. 409) from 172.20.8.138 to 23.220.75.245. The packet details show it is an ACK for sequence 436, with a window size of 253. The packet length is 80 bytes.

| No. | Time     | Source          | Destination     | Protocol | Length | Info   |
|-----|----------|-----------------|-----------------|----------|--------|--|
| 384 | 6.764534 | 172.20.8.138    | 142.250.194.227 | TLSv1.3  | 89     | Application Data   |
| 385 | 6.769073 | 142.250.194.227 | 172.20.8.138    | TCP      | 60     | 443 → 63773 [ACK] Seq=5752 Ack=3399 Win=38784 Len=0                  |
| 403 | 7.281138 | 23.220.75.245   | 172.20.8.138    | TLSv1.3  | 318    | Server Hello, Change Cipher Spec, Application Data, Application Data |
| 404 | 7.281138 | 23.215.0.136    | 172.20.8.138    | HTTP     | 787    | HTTP/1.1 200 OK (text/html)  |
| 405 | 7.281791 | 172.20.8.138    | 23.220.75.245   | TLSv1.3  | 134    | Change Cipher Spec, Application Data                                 |
| 406 | 7.283299 | 23.220.75.245   | 172.20.8.138    | TCP      | 60     | 443 → 52093 [ACK] Seq=265 Ack=2105 Win=35072 Len=0                   |
| 407 | 7.318824 | 172.20.8.138    | 172.217.24.142  | TCP      | 55     | 1548 → 443 [ACK] Seq=1 Ack=1 Win=250 Len=1                           |
| 408 | 7.312268 | 172.217.24.142  | 172.20.8.138    | TCP      | 66     | 443 → 1548 [ACK] Seq=1 Ack=2 Win=332 Len=0 SLE=1 SRE=2               |
| 409 | 7.332505 | 172.20.8.138    | 23.215.0.136    | TCP      | 54     | 62070 → 80 [ACK] Seq=436 Ack=734 Win=64768 Len=0                     |
| 413 | 7.577992 | 23.220.75.245   | 172.20.8.138    | TLSv1.3  | 341    | Application Data   |

Transmission Control Protocol, Src Port: 62070, Dst Port: 80, Seq: 436, Ack: 734, Len: 0

Source Port: 62070  
Destination Port: 80  
[Stream index: 5]  
[Stream Packet Number: 7]  
[Conversation completeness: Incomplete, DATA (15)]  
[TCP Segment Len: 6]  
Sequence Number: 436 (relative sequence number)  
Sequence Number (raw): 4059609204  
[Next Sequence Number: 436 (relative sequence number)]  
Acknowledgment Number: 734 (relative ack number)  
Acknowledgment number (raw): 3899453378  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window: 253  
[Calculated window size: 64768]  
[Window size scaling factor: 256]  
Checksum: 0xcd17 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]  
[Client Contiguous Streams: 1]

Source Port (tcp.srcport), 2 bytes

Packets: 557 - Displayed: 150 (26.9%) - Dropped: 0 (0.0%) Profile: Default

Wireshark packet capture showing a TCP ACK packet (No. 409) from 172.20.8.138 to 23.220.75.245. The packet details show it is an ACK for sequence 436, with a window size of 253. The packet length is 80 bytes.

| No. | Time     | Source          | Destination     | Protocol | Length | Info   |
|-----|----------|-----------------|-----------------|----------|--------|--|
| 384 | 6.764534 | 172.20.8.138    | 142.250.194.227 | TLSv1.3  | 89     | Application Data   |
| 385 | 6.769073 | 142.250.194.227 | 172.20.8.138    | TCP      | 60     | 443 → 63773 [ACK] Seq=5752 Ack=3399 Win=38784 Len=0                  |
| 403 | 7.281138 | 23.220.75.245   | 172.20.8.138    | TLSv1.3  | 318    | Server Hello, Change Cipher Spec, Application Data, Application Data |
| 404 | 7.281138 | 23.215.0.136    | 172.20.8.138    | HTTP     | 787    | HTTP/1.1 200 OK (text/html)  |
| 405 | 7.281791 | 172.20.8.138    | 23.220.75.245   | TLSv1.3  | 134    | Change Cipher Spec, Application Data                                 |
| 406 | 7.283299 | 23.220.75.245   | 172.20.8.138    | TCP      | 60     | 443 → 52093 [ACK] Seq=265 Ack=2105 Win=35072 Len=0                   |
| 407 | 7.318824 | 172.20.8.138    | 172.217.24.142  | TCP      | 55     | 1548 → 443 [ACK] Seq=1 Ack=1 Win=250 Len=1                           |
| 408 | 7.312268 | 172.217.24.142  | 172.20.8.138    | TCP      | 66     | 443 → 1548 [ACK] Seq=1 Ack=2 Win=332 Len=0 SLE=1 SRE=2               |
| 409 | 7.332505 | 172.20.8.138    | 23.215.0.136    | TCP      | 54     | 62070 → 80 [ACK] Seq=436 Ack=734 Win=64768 Len=0                     |
| 413 | 7.577992 | 23.220.75.245   | 172.20.8.138    | TLSv1.3  | 341    | Application Data   |

Acknowledgment Number: 734 (relative ack number)  
Acknowledgment number (raw): 3899453378  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
000. .... = Reserved: Not set  
...0 .... = Accurate ECN: Not set  
....0... .... = Congestion Window Reduced: Not set  
....0... .... = ECN-Echo: Not set  
....0... .... = Urgent: Not set  
....1... .... = Acknowledgment: Set  
....0... .... = Push: Not set  
....0... .... = Reset: Not set  
....0... .... = Syn: Not set  
....0... .... = Fin: Not set  
[TCP Flags: .....A....]  
Window: 253  
[Calculated window size: 64768]  
[Window size scaling factor: 256]  
Checksum: 0xcd17 [unverified]  
[Checksum Status: Unverified]  
Urgent Pointer: 0  
[Timestamps]  
[SEQ/ACK analysis]

Source Port (tcp.srcport), 2 bytes

Packets: 557 - Displayed: 150 (26.9%) - Dropped: 0 (0.0%) Profile: Default

### 3. UDP Packets

The screenshot shows a Wireshark capture of UDP traffic. The packet list pane displays several DNS-related packets. Packet 24 is highlighted, showing a Multicast Domain Name System (query) packet. The packet details pane shows the following information:

- Frame 24: Packet, 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface \Device\NPF\_{ECEF2FF9-0D9D-4515-97B9-007541CEF741}, id 0000
- Ethernet II, Src: 86:76:ef:97:da:09 (86:76:ef:97:da:09), Dst: IPv4mcast\_fb (01:00:5e:00:00:fb)
- Internet Protocol Version 4, Src: 172.20.6.220, Dst: 224.0.0.251
- User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  - Source Port: 5353
  - Destination Port: 5353
  - Length: 66
  - Checksum: 0x1422 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 2]
  - [Stream Packet Number: 1]
  - [Timestamps]
  - UDP payload (58 bytes)
    - Multicast Domain Name System (query)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IPv4 header, and UDP header.

### 4. ICMP Packets (Ping)

The screenshot shows a Wireshark capture of ICMP traffic. The packet list pane displays several ICMP Echo (ping) packets. Packet 224 is highlighted, showing an Echo (ping) request packet. The packet details pane shows the following information:

- Frame 224: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF\_{ECEF2FF9-0D9D-4515-97B9-007541CEF741}, id 0000
- Ethernet II, Src: Intel\_c5:89:56 (60:e3:2b:c5:89:56), Dst: Sophos\_d1:3f:f0 (7c:5a:1c:d1:3f:f0)
- Internet Protocol Version 4, Src: 172.20.8.138, Dst: 8.8.8.8
- Internet Control Message Protocol
  - Type: Echo (ping) request (8)
  - Code: 0
  - Checksum: 0x4d55 [correct]
  - [Checksum Status: Good]
  - Identifier (BE): 1 (0x0001)
  - Identifier (LE): 256 (0x0100)
  - Sequence Number (BE): 6 (0x0006)
  - Sequence Number (LE): 1536 (0x0600)
  - [Response frame: 225]
  - Data (32 bytes)

The packet bytes pane shows the raw data of the packet, including the Ethernet II header, IPv4 header, and ICMP header.

