Professional Documentation: Wireshark Packet Analysis Lab

Date: July 18, 2025
Analyst: Aarush Nepali
Lab Duration: 1 Hour
Lab Level: Beginner

Lab Overview

Objective

The objective of this lab was to gain hands-on experience with **Wireshark**, a network protocol analyzer, to inspect and filter packet capture (`.pcap`) data. Tasks included analyzing network traffic related to a user connecting to a website (`opensource.google.com`), applying filters to isolate specific traffic, and examining packet details across different protocol layers.

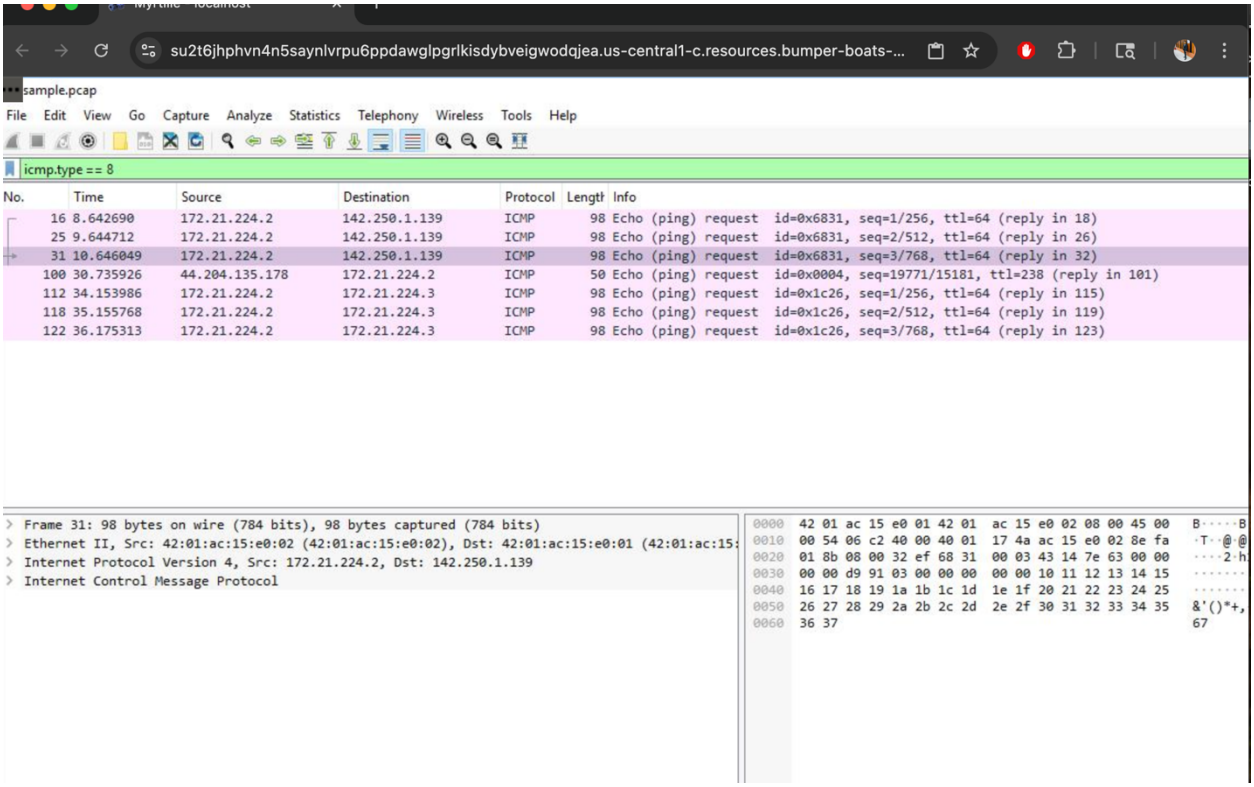
Key Skills Demonstrated

- Navigating Wireshark's interface
- Applying display filters to isolate traffic by IP address, MAC address, and protocol
- Inspecting packet details at the **Frame, Ethernet, IP, TCP, and DNS** layers
- Analyzing DNS queries and responses
- Examining TCP traffic, including HTTP payloads

Detailed Task Breakdown

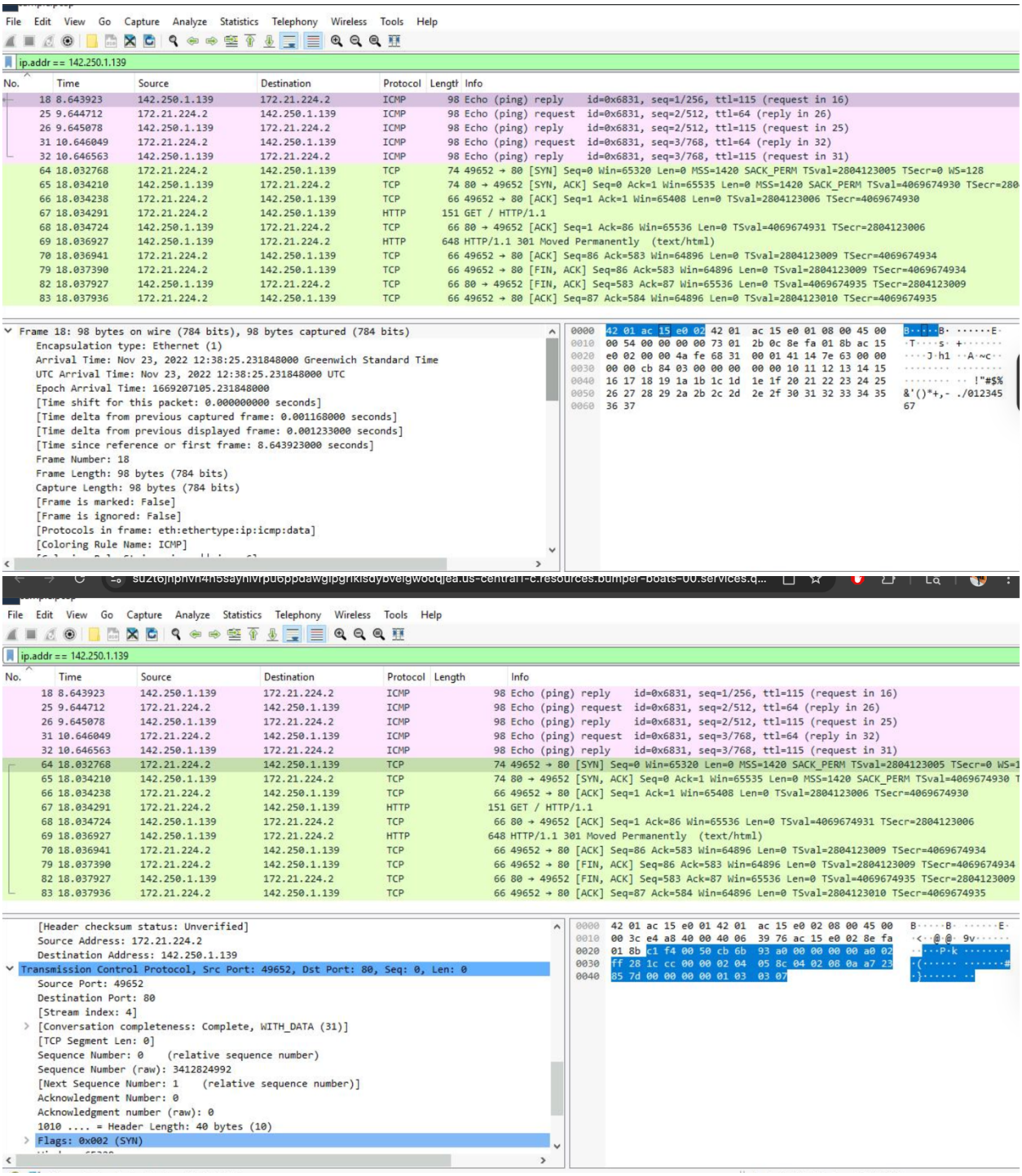
Task 1: Explore Data with Wireshark

- **Action:** Opened the provided `sample.pcap` file in Wireshark.
- **Observations:**
  - The packet list displayed various protocols (**DNS, TCP, HTTP, ICMP**).
  - **Coloring rules** helped visually distinguish traffic types (e.g., light blue for DNS, green for TCP/HTTP).
  - Located an **ICMP Echo (ping) request** packet.
- **Key Finding:**
  - The protocol for the first packet with an **"Echo (ping) request"** in the Info column was **ICMP**.



Task 2: Apply a Basic Wireshark Filter and Inspect a Packet

- **Action:** Applied the filter `ip.addr == 142.250.1.139` to isolate traffic involving this IP.
- **Packet Inspection:**
  - **Double-clicked a TCP packet** to examine its layers:
    1. **Frame:** Metadata (length, arrival time)
    2. **Ethernet II:** Source and destination MAC addresses
    3. **IPv4:** Source and destination IPs, protocol (TCP)
    4. **TCP:** Source and destination ports (notably **port 80** for HTTP), flags
- **Key Findings:**
  - **TCP destination port:** `80` (HTTP)
  - **TCP flags:** Examined SYN/ACK flags for connection establishment

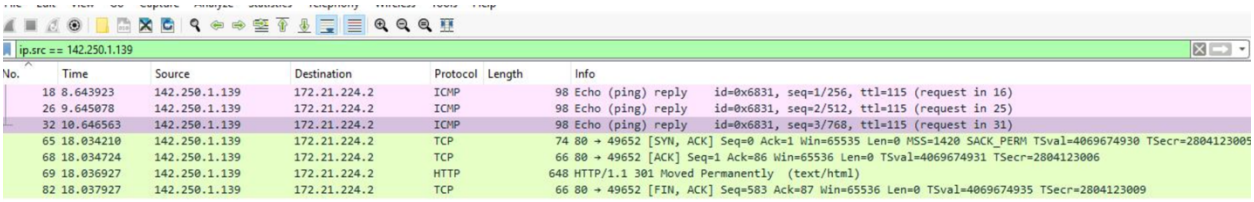


Task 3: Use Filters to Select Packets

- **Actions Performed:**
    1. Filtered by **source IP**: `ip.src == 142.250.1.139` (outgoing traffic)
    2. Filtered by **destination IP**: `ip.dst == 142.250.1.139` (incoming traffic)
    3. Filtered by **MAC address**: `eth.addr == 42:01:ac:15:e0:02`

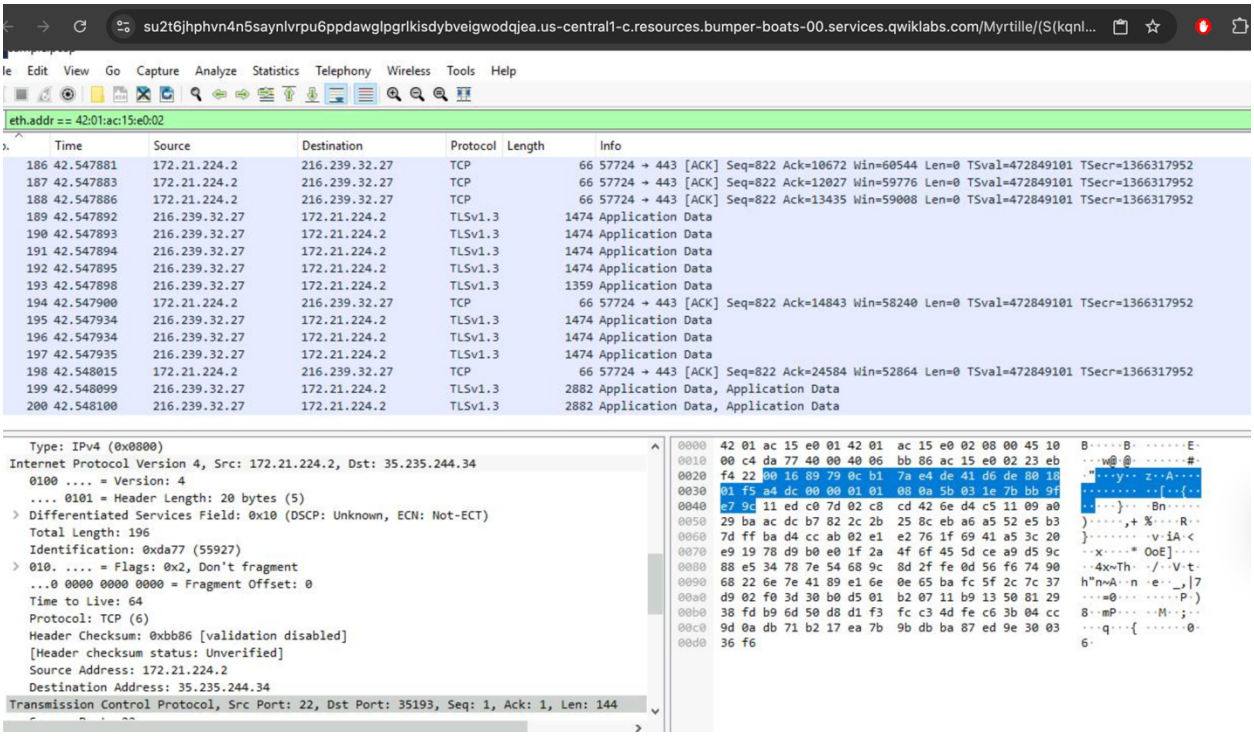
- **Key Finding:**
    - The first packet related to the MAC address contained **TCP** data in the IPv4 subtree

---



ip.src == 142.250.1.139

No.	Time	Source	Destination	Protocol	Length	Info
18	8.643923	142.250.1.139	172.21.224.2	ICMP	98	Echo (ping) reply id=0x6831, seq=1/256, ttl=115 (request in 16)
26	9.645078	142.250.1.139	172.21.224.2	ICMP	98	Echo (ping) reply id=0x6831, seq=2/512, ttl=115 (request in 25)
32	10.646563	142.250.1.139	172.21.224.2	ICMP	98	Echo (ping) reply id=0x6831, seq=3/768, ttl=115 (request in 31)
65	18.034210	142.250.1.139	172.21.224.2	TCP	74	80 → 49652 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1420 SACK_PERM TSval=4069674930 TSecr=2804123005
68	18.034724	142.250.1.139	172.21.224.2	TCP	66	80 → 49652 [ACK] Seq=1 Ack=86 Win=65536 Len=0 TSval=4069674931 TSecr=2804123006
69	18.036927	142.250.1.139	172.21.224.2	HTTP	648	HTTP/1.1 301 Moved Permanently (text/html)
82	18.037927	142.250.1.139	172.21.224.2	TCP	66	80 → 49652 [FIN, ACK] Seq=583 Ack=87 Win=65536 Len=0 TSval=4069674935 TSecr=2804123009



su2t6jhphvn4n5saynlvrpu6ppdawglpgrlkisdybveigwodqjea.us-central1-c.resources.bumper-boats-00.services.qwiklabs.com/Myrtille/(S(kqnl...

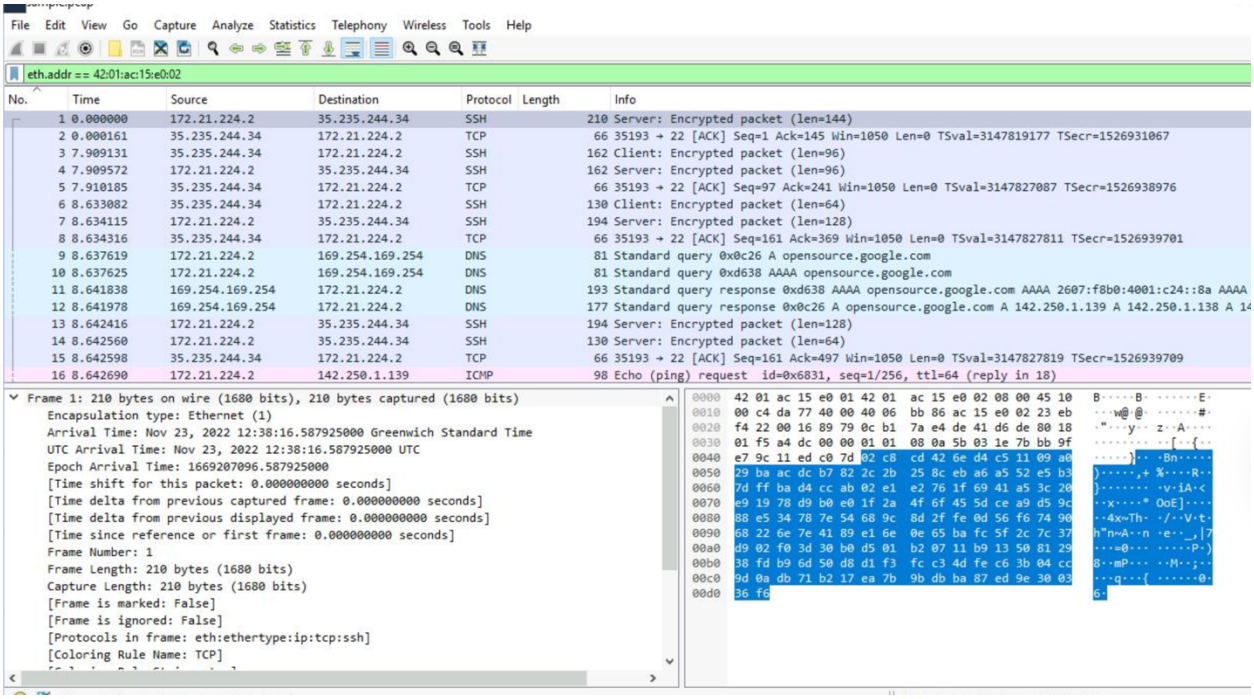
Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == 42:01:ac:15:e0:02

	Time	Source	Destination	Protocol	Length	Info
186	42.547881	172.21.224.2	216.239.32.27	TCP	66	57724 → 443 [ACK] Seq=822 Ack=10672 Win=60544 Len=0 TSval=472849101 TSecr=1366317952
187	42.547883	172.21.224.2	216.239.32.27	TCP	66	57724 → 443 [ACK] Seq=822 Ack=12027 Win=59776 Len=0 TSval=472849101 TSecr=1366317952
188	42.547886	172.21.224.2	216.239.32.27	TCP	66	57724 → 443 [ACK] Seq=822 Ack=13435 Win=59008 Len=0 TSval=472849101 TSecr=1366317952
189	42.547892	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
190	42.547893	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
191	42.547894	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
192	42.547895	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
193	42.547898	216.239.32.27	172.21.224.2	TLSv1.3	1359	Application Data
194	42.547900	172.21.224.2	216.239.32.27	TCP	66	57724 → 443 [ACK] Seq=822 Ack=14843 Win=58240 Len=0 TSval=472849101 TSecr=1366317952
195	42.547934	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
196	42.547934	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
197	42.547935	216.239.32.27	172.21.224.2	TLSv1.3	1474	Application Data
198	42.548015	172.21.224.2	216.239.32.27	TCP	66	57724 → 443 [ACK] Seq=822 Ack=24584 Win=52864 Len=0 TSval=472849101 TSecr=1366317952
199	42.548099	216.239.32.27	172.21.224.2	TLSv1.3	2882	Application Data, Application Data
200	42.548100	216.239.32.27	172.21.224.2	TLSv1.3	2882	Application Data, Application Data


```
   Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.21.224.2, Dst: 35.235.244.34
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
   Total Length: 196
   Identification: 0xda77 (55927)
 > 010. .... = Flags: 0x2, Don't fragment
   ...0 0000 0000 0000 = Fragment Offset: 0
   Time to Live: 64
   Protocol: TCP (6)
   Header Checksum: 0xbb86 [validation disabled]
   [Header checksum status: Unverified]
   Source Address: 172.21.224.2
   Destination Address: 35.235.244.34
Transmission Control Protocol, Src Port: 22, Dst Port: 35193, Seq: 1, Ack: 1, Len: 144
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 10   B·····B· ·····E·
0010  00 c4 da 77 40 00 40 06  bb 86 ac 15 e0 02 23 eb   ···w@·@· ·····#·
0020  f4 22 00 16 89 79 0c b1  7a e4 de 41 d6 de 80 18   ·"···y·· z··A····
0030  01 f5 a4 dc 00 00 01 01  08 0a 5b 03 1e 7b bb 9f   ········ ··[··{··
0040  e7 9c 11 ed c0 7d 02 c8  cd 42 6e d4 c5 11 09 a0   ·····}·· ·Bn·····
0050  29 ba ac dc b7 82 2c 2b  25 8c eb a6 a5 52 e5 b3   )·····,+ %····R··
0060  7d ff ba d4 cc ab 02 e1  e2 76 1f 69 41 a5 3c 20   }········ ·v·iA·<
0070  e9 19 78 d9 b0 e0 1f 2a  4f 6f 45 5d ce a9 d5 9c   ··x····* OoE]····
0080  88 e5 34 78 7e 54 68 9c  8d 2f fe 0d 56 f6 74 90   ··4x~Th· ·/··V·t·
0090  68 22 6e 7e 41 89 e1 6e  0e 65 ba fc 5f 2c 7c 37   h"n~A··n ·e··_,|7
00a0  d9 02 f0 3d 30 b0 d5 01  b2 07 11 b9 13 50 81 29   ···=0··· ·····P·)
00b0  38 fd b9 6d 50 d8 d1 f3  fc c3 4d fe c6 3b 04 cc   8··mP··· ··M··;··
00c0  9d 0a db 71 b2 17 ea 7b  9b db ba 87 ed 9e 30 03   ···q···{ ·····0·
00d0  36 f6                                              6·
```



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.addr == 42:01:ac:15:e0:02

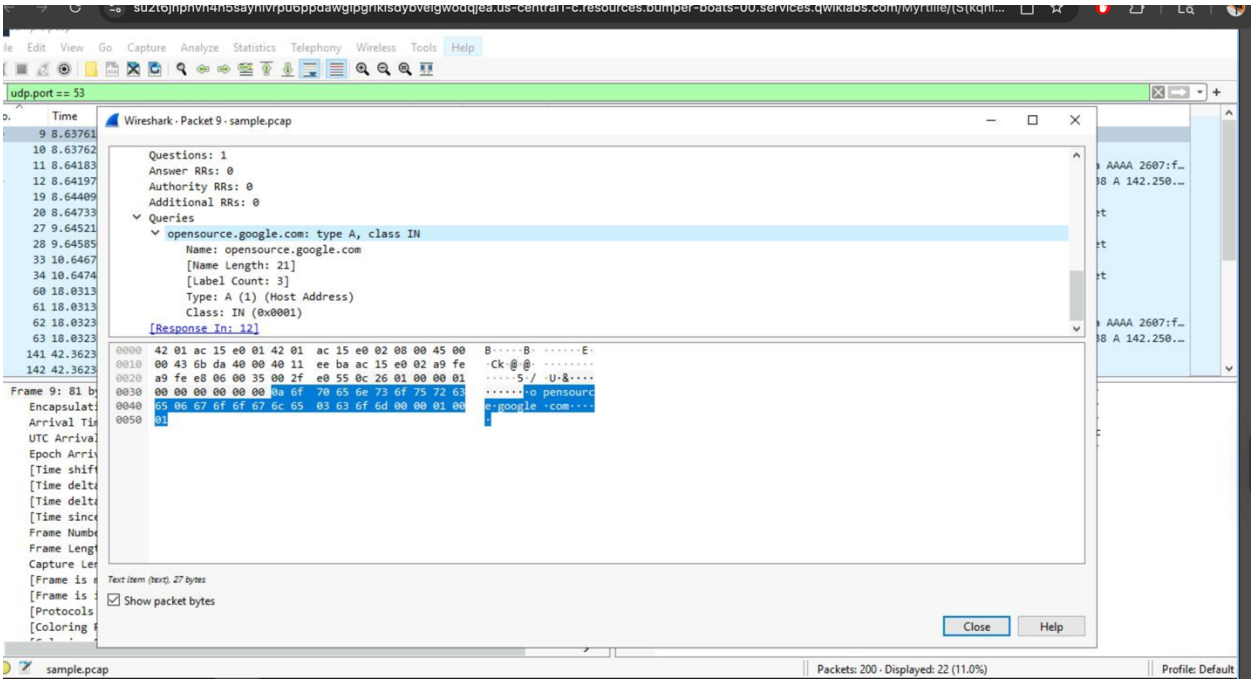
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.21.224.2	35.235.244.34	SSH	210	Server: Encrypted packet (len=144)
2	0.000161	35.235.244.34	172.21.224.2	TCP	66	35193 → 22 [ACK] Seq=1 Ack=145 Win=1050 Len=0 TSval=3147819177 TSecr=1526931067
3	7.909131	35.235.244.34	172.21.224.2	SSH	162	Client: Encrypted packet (len=96)
4	7.909572	172.21.224.2	35.235.244.34	SSH	162	Server: Encrypted packet (len=96)
5	7.910185	35.235.244.34	172.21.224.2	TCP	66	35193 → 22 [ACK] Seq=97 Ack=241 Win=1050 Len=0 TSval=3147827087 TSecr=1526938976
6	8.633082	35.235.244.34	172.21.224.2	SSH	130	Client: Encrypted packet (len=64)
7	8.634115	172.21.224.2	35.235.244.34	SSH	194	Server: Encrypted packet (len=128)
8	8.634316	35.235.244.34	172.21.224.2	TCP	66	35193 → 22 [ACK] Seq=161 Ack=369 Win=1050 Len=0 TSval=3147827811 TSecr=1526939701
9	8.637619	172.21.224.2	169.254.169.254	DNS	81	Standard query 0x0c26 A opensource.google.com
10	8.637625	172.21.224.2	169.254.169.254	DNS	81	Standard query 0xd638 AAAA opensource.google.com
11	8.641838	169.254.169.254	172.21.224.2	DNS	193	Standard query response 0xd638 AAAA opensource.google.com AAAA 2607:f8b0:4001:c24::8a AAAA
12	8.641978	169.254.169.254	172.21.224.2	DNS	177	Standard query response 0x0c26 A opensource.google.com A 142.250.1.139 A 142.250.1.138 A 14
13	8.642416	172.21.224.2	35.235.244.34	SSH	194	Server: Encrypted packet (len=128)
14	8.642560	172.21.224.2	35.235.244.34	SSH	130	Server: Encrypted packet (len=64)
15	8.642598	35.235.244.34	172.21.224.2	TCP	66	35193 → 22 [ACK] Seq=161 Ack=497 Win=1050 Len=0 TSval=3147827819 TSecr=1526939709
16	8.642690	172.21.224.2	142.250.1.139	ICMP	98	Echo (ping) request id=0x6831, seq=1/256, ttl=64 (reply in 18)

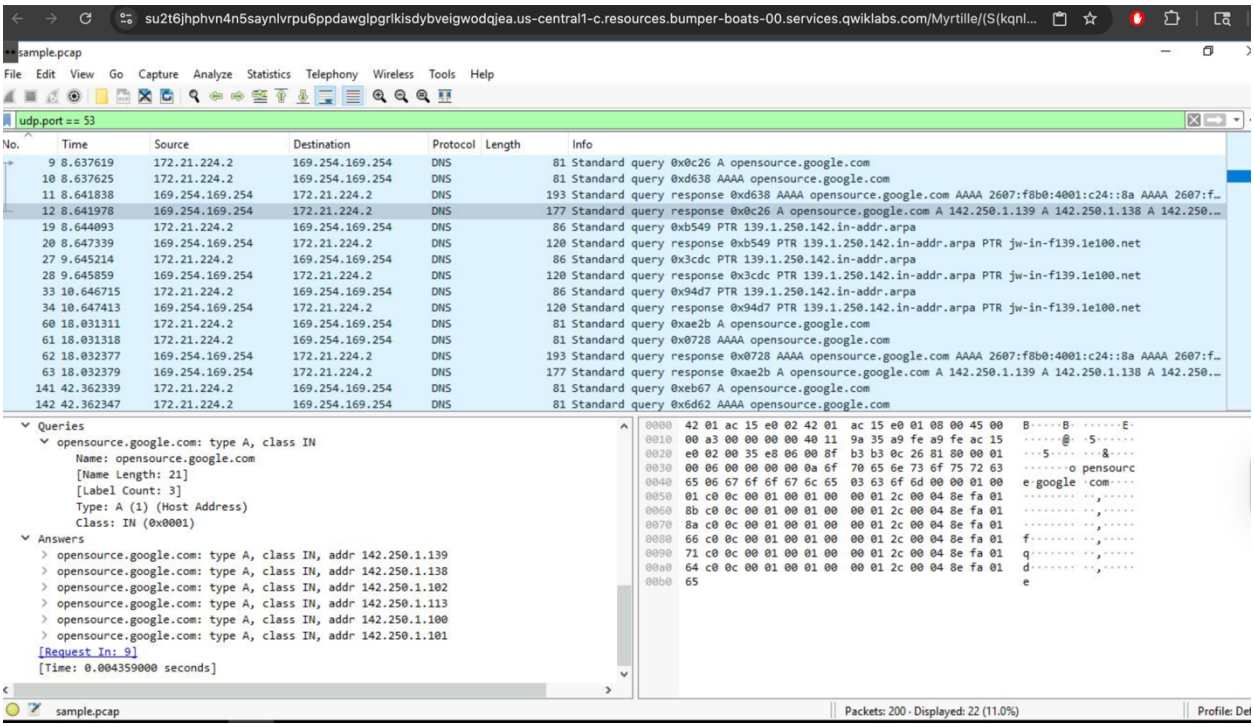
```
Frame 1: 210 bytes on wire (1680 bits), 210 bytes captured (1680 bits)
   Encapsulation type: Ethernet (1)
   Arrival Time: Nov 23, 2022 12:38:16.587925000 Greenwich Standard Time
   UTC Arrival Time: Nov 23, 2022 12:38:16.587925000 UTC
   Epoch Arrival Time: 1669207096.587925000
   [Time shift for this packet: 0.000000000 seconds]
   [Time delta from previous captured frame: 0.000000000 seconds]
   [Time delta from previous displayed frame: 0.000000000 seconds]
   [Time since reference or first frame: 0.000000000 seconds]
   Frame Number: 1
   Frame Length: 210 bytes (1680 bits)
   Capture Length: 210 bytes (1680 bits)
   [Frame is marked: False]
   [Frame is ignored: False]
   [Protocols in frame: eth:ethertype:ip:tcp:ssh]
   [Coloring Rule Name: TCP]
```

```
0000  42 01 ac 15 e0 01 42 01  ac 15 e0 02 08 00 45 10   B·····B· ·····E·
0010  00 c4 da 77 40 00 40 06  bb 86 ac 15 e0 02 23 eb   ···w@·@· ·····#·
0020  f4 22 00 16 89 79 0c b1  7a e4 de 41 d6 de 80 18   ·"···y·· z··A····
0030  01 f5 a4 dc 00 00 01 01  08 0a 5b 03 1e 7b bb 9f   ········ ··[··{··
0040  e7 9c 11 ed c0 7d 02 c8  cd 42 6e d4 c5 11 09 a0   ·····}·· ·Bn·····
0050  29 ba ac dc b7 82 2c 2b  25 8c eb a6 a5 52 e5 b3   )·····,+ %····R··
0060  7d ff ba d4 cc ab 02 e1  e2 76 1f 69 41 a5 3c 20   }········ ·v·iA·<
0070  e9 19 78 d9 b0 e0 1f 2a  4f 6f 45 5d ce a9 d5 9c   ··x····* OoE]····
0080  88 e5 34 78 7e 54 68 9c  8d 2f fe 0d 56 f6 74 90   ··4x~Th· ·/··V·t·
0090  68 22 6e 7e 41 89 e1 6e  0e 65 ba fc 5f 2c 7c 37   h"n~A··n ·e··_,|7
00a0  d9 02 f0 3d 30 b0 d5 01  b2 07 11 b9 13 50 81 29   ···=0··· ·····P·)
00b0  38 fd b9 6d 50 d8 d1 f3  fc c3 4d fe c6 3b 04 cc   8··mP··· ··M··;··
00c0  9d 0a db 71 b2 17 ea 7b  9b db ba 87 ed 9e 30 03   ···q···{ ·····0·
00d0  36 f6                                              6·
```

Task 4: Use Filters to Explore DNS Packets

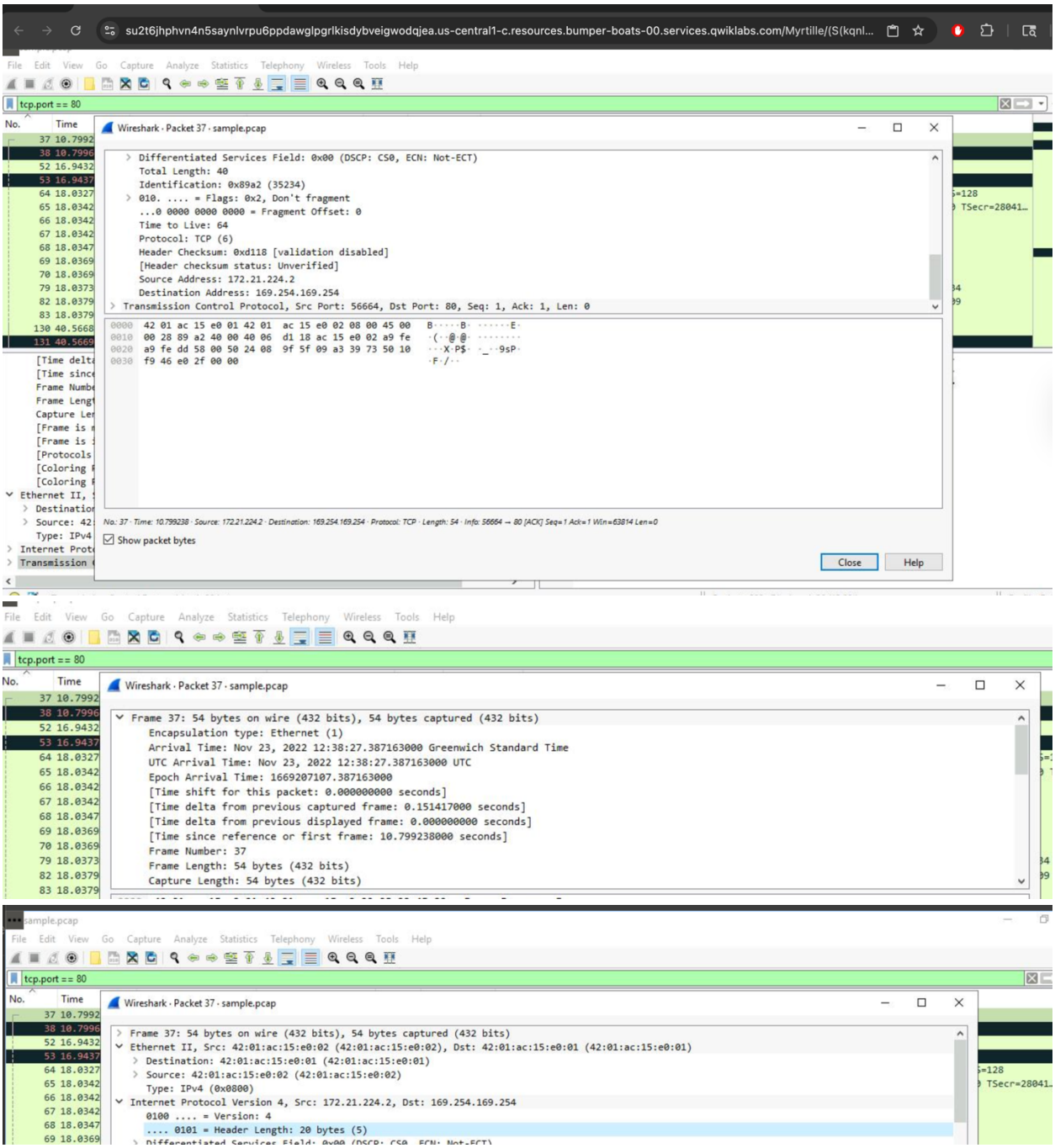
- **Action:** Applied the filter `udp.port == 53` to isolate DNS traffic
- **Packet Analysis:**
  - **First Packet (DNS Query):**
    - Queried domain: `opensource.google.com`
  - **Fourth Packet (DNS Response):**
    - Resolved IP: `142.250.1.139`
- **Key Finding:**
  - Confirmed DNS resolution for `opensource.google.com` mapped to `142.250.1.139`

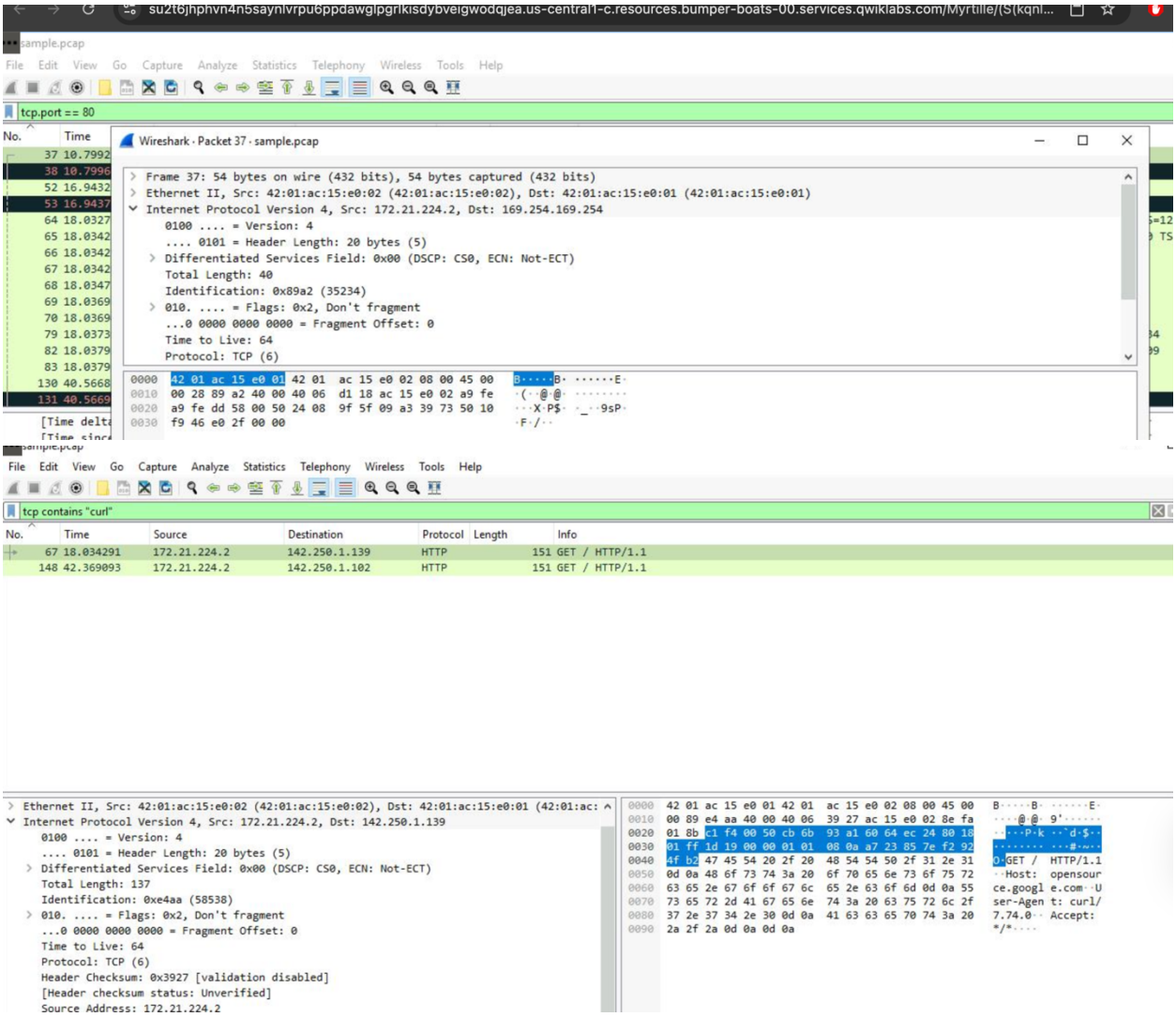




Task 5: Use Filters to Explore TCP Packets

- **Actions Performed:**
    1. Filtered **TCP port 80** (`tcp.port == 80`) to analyze HTTP traffic
    2. Inspected a packet destined for `169.254.169.254` (metadata service IP)
        - **Time to Live (TTL):** `64`
        - **Frame Length:** `54 bytes`
        - **IP Header Length:** `20 bytes`
    3. Applied `tcp contains "curl"` to detect HTTP requests made via `curl`
- **Key Findings:**
    - Confirmed HTTP traffic analysis, including header and payload inspection


su2t6jhphvn4n5saynlvrpu6ppdawglpgrlkisdybveigwodqjea.us-central1-c.resources.bumper-boats-00.services.qwiklabs.com/Myrtille/(S(kqnl...
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 80
No. Time
Wireshark · Packet 37 · sample.pcap
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 40
Identification: 0x89a2 (35234)
010. .... = Flags: 0x2, Don't fragment
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 64
Protocol: TCP (6)
Header Checksum: 0xd118 [validation disabled]
[Header checksum status: Unverified]
Source Address: 172.21.224.2
Destination Address: 169.254.169.254
Transmission Control Protocol, Src Port: 56664, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
0000 42 01 ac 15 e0 01 42 01 ac 15 e0 02 08 00 45 00
0010 00 28 89 a2 40 00 40 06 d1 18 ac 15 e0 02 a9 fe
0020 a9 fe dd 58 00 50 24 08 9f 5f 09 a3 39 73 50 10
0030 f9 46 e0 2f 00 00
No.: 37 · Time: 10.799238 · Source: 172.21.224.2 · Destination: 169.254.169.254 · Protocol: TCP · Length: 54 · Info: 56664 → 80 [ACK] Seq=1 Ack=1 Win=63814 Len=0
Show packet bytes
Close
Help
Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 23, 2022 12:38:27.387163000 Greenwich Standard Time
UTC Arrival Time: Nov 23, 2022 12:38:27.387163000 UTC
Epoch Arrival Time: 1669207107.387163000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.151417000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 10.799238000 seconds]
Frame Number: 37
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
sample.pcap
Frame 37: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
Ethernet II, Src: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02), Dst: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
Destination: 42:01:ac:15:e0:01 (42:01:ac:15:e0:01)
Source: 42:01:ac:15:e0:02 (42:01:ac:15:e0:02)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.21.224.2, Dst: 169.254.169.254
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)



Conclusion & Takeaways

- Successfully **filtered and analyzed** network traffic using Wireshark
- Identified **source/destination IPs**, **MAC addresses**, and **protocols** (TCP, UDP, ICMP)
- Verified **DNS resolution** and **TCP handshake** details
- Recognized the importance of **display filters** in isolating relevant traffic during security investigations

---

End of Report

Lab Artifacts

- **Filter Queries Used:**

```
plaintext
CopyEdit
ip.addr == 142.250.1.139
ip.src == 142.250.1.139
ip.dst == 142.250.1.139
eth.addr == 42:01:ac:15:e0:02
udp.port == 53
tcp.port == 80
tcp contains "curl"
```

- **Key Packet Details:**
  - DNS Response IP: `142.250.1.139`
  - TCP Destination Port: `80`
  - ICMP Echo Request: Protocol `ICMP`