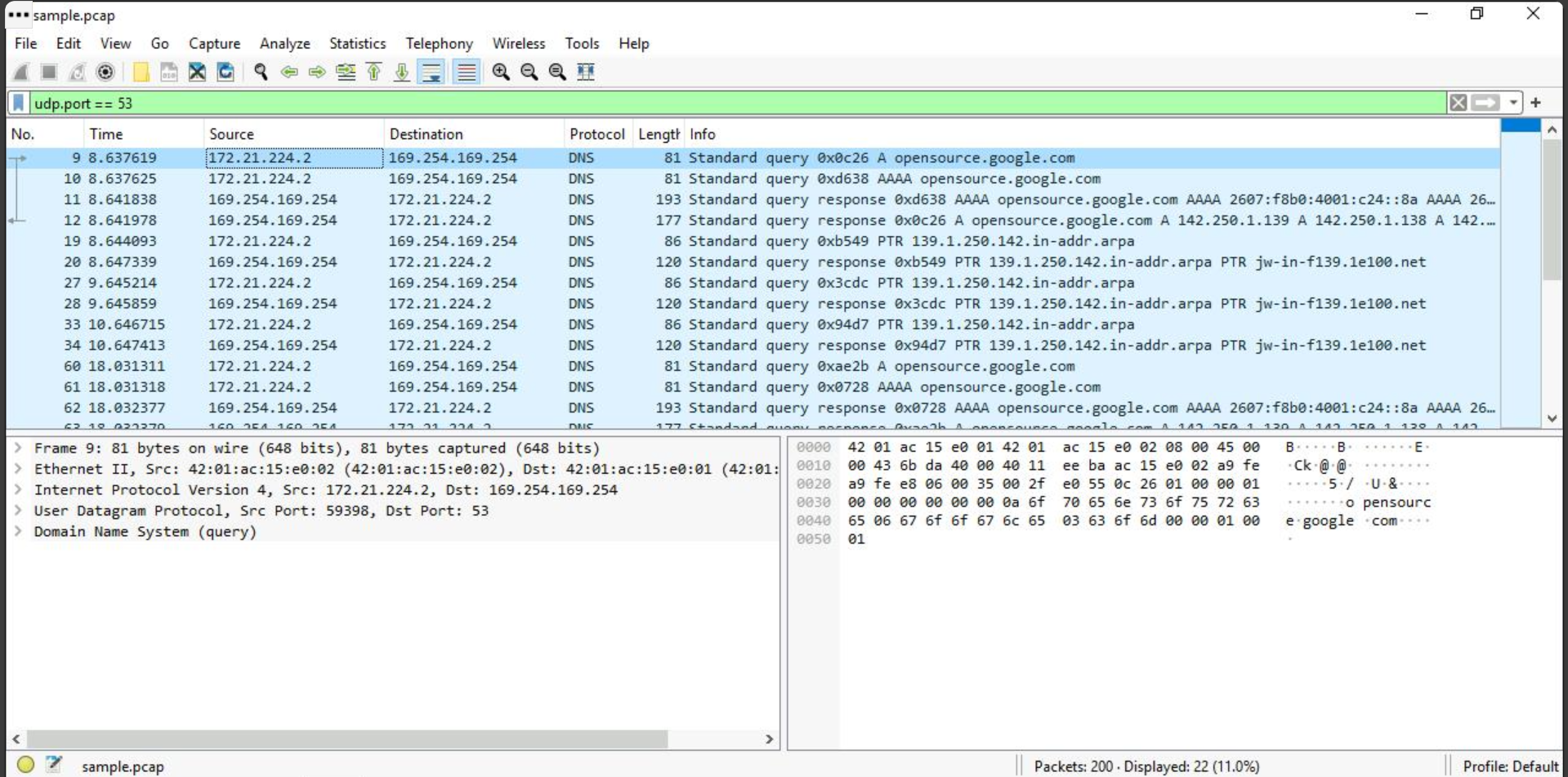
**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:** 01/17/26 | **Entry: 2** |
| Description | Analyzing a packet capture file |
| Tool(s) used | I used the network protocol analyzer which is Wireshark to analyze a network packet capture file. The display filter was utilized to get specific information needed. This tool is beneficial in detecting suspicious patterns in the network. |
| The 5 W's | * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A |
| Additional notes | The graphical user interface of Wireshark helps make its navigation easier. The color coding for the protocols is also helpful. |

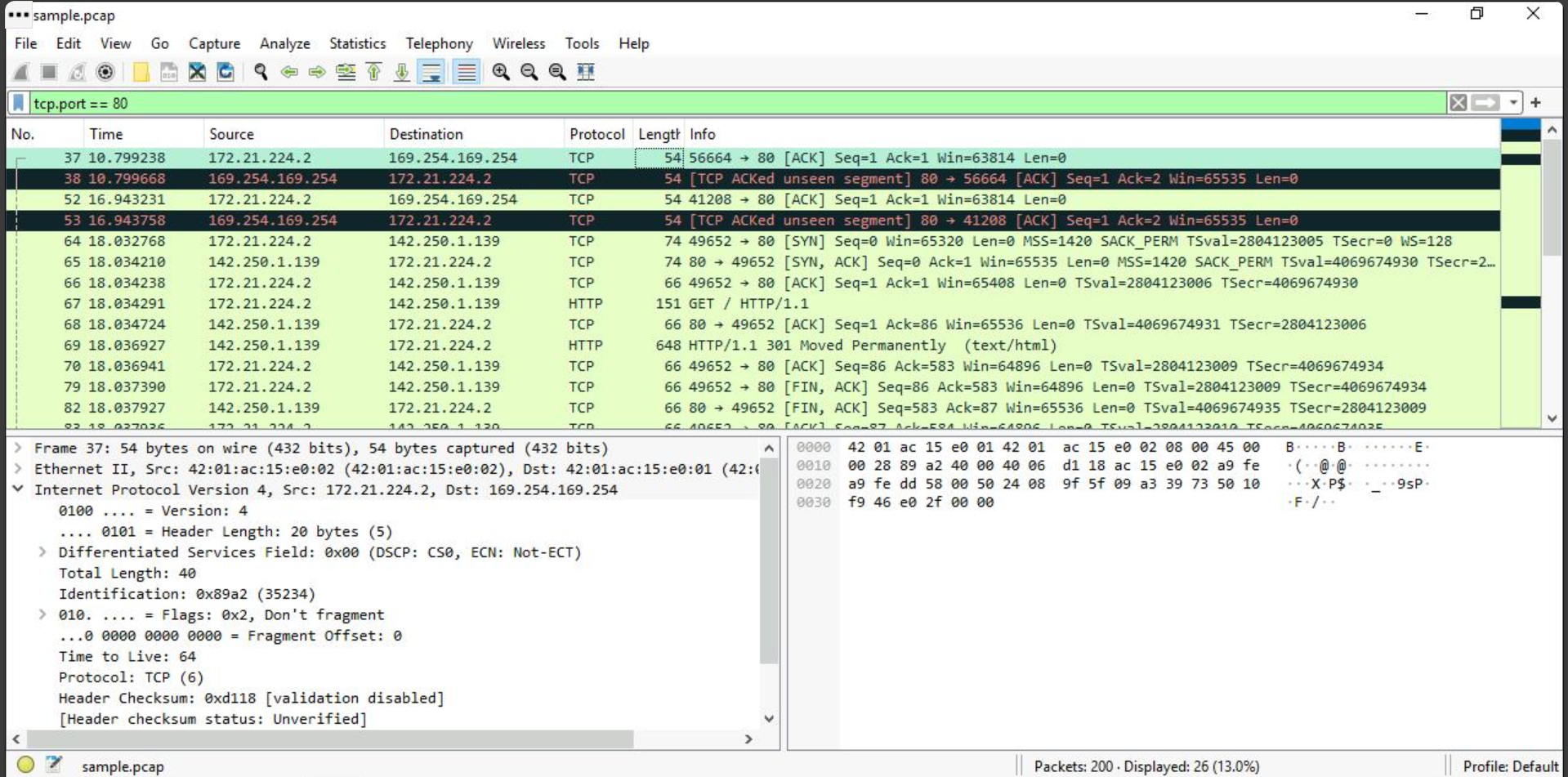


Using Wireshark, the network packet capture file was analyzed. I placed **udp.port == 53** in the display filter which is the port used by DNS packets to examine it.

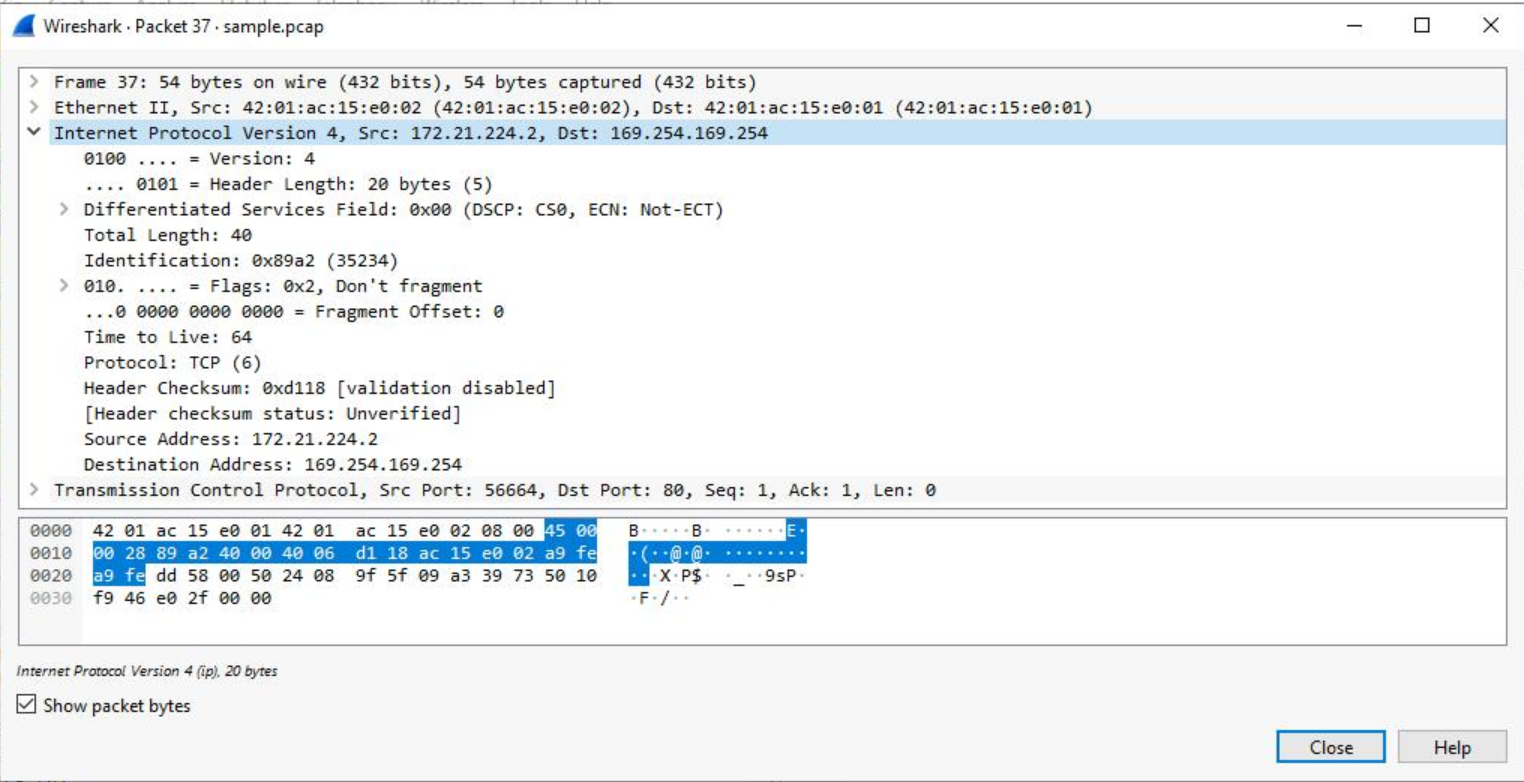
A screenshot of a computer

AI-generated content may be incorrect.

I opened the first packet to check for its details. Under the **Queries** portion of the **Domain Name System (query)** showed that the domain being queried was **opensource.google.com**.



I now placed **tcp.port == 80** in the display filter which is the port used by TCP packets to examine it. The protocols used when the user makes the connection to the website are also shown such as the TCP and HTTP.



I opened the first packet to check for its details. The source and destination IP addresses can be seen on the **Internet Protocol Version 4** section. The **Ack** flag can also be seen which ensures connection between the systems.