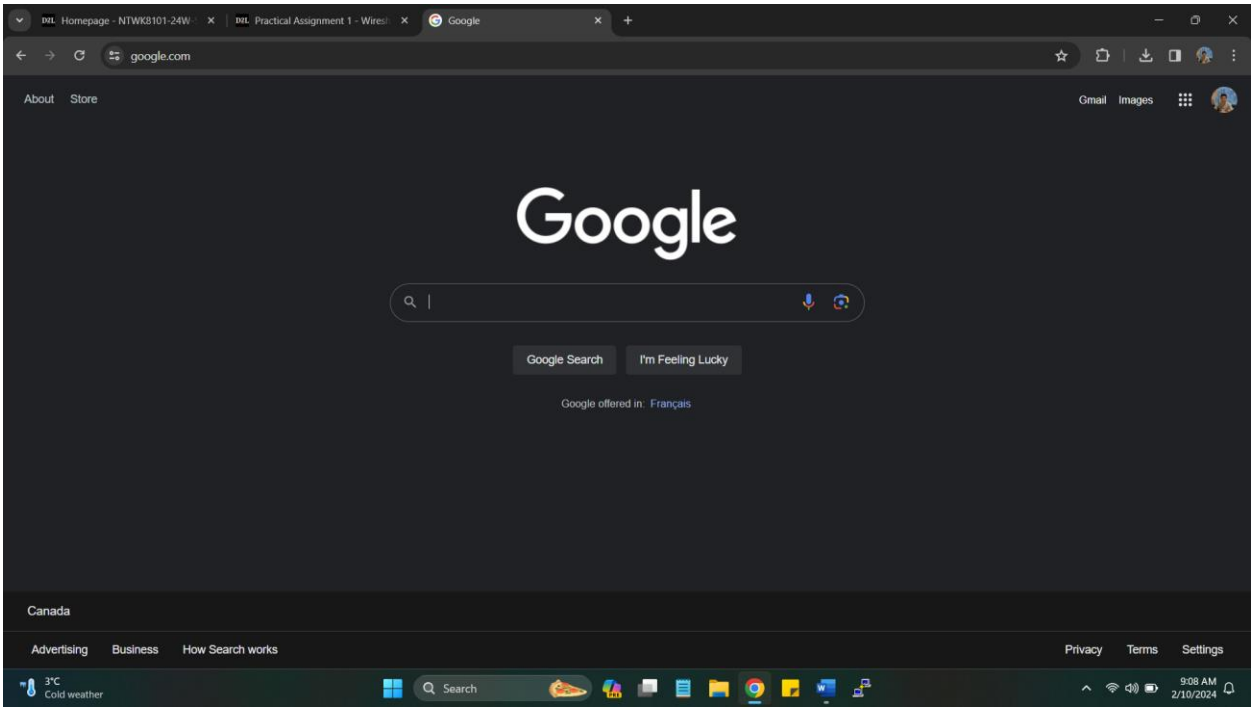
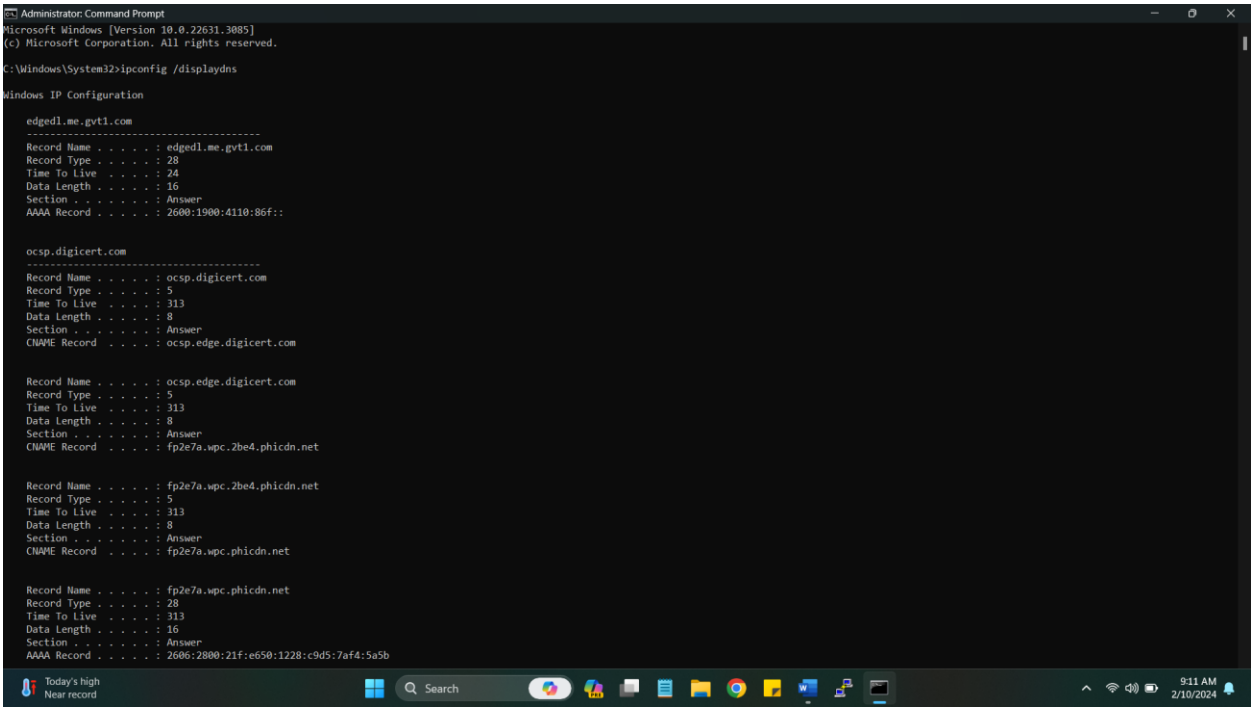
1. Open a browser and browse to www.google.com, then close browser



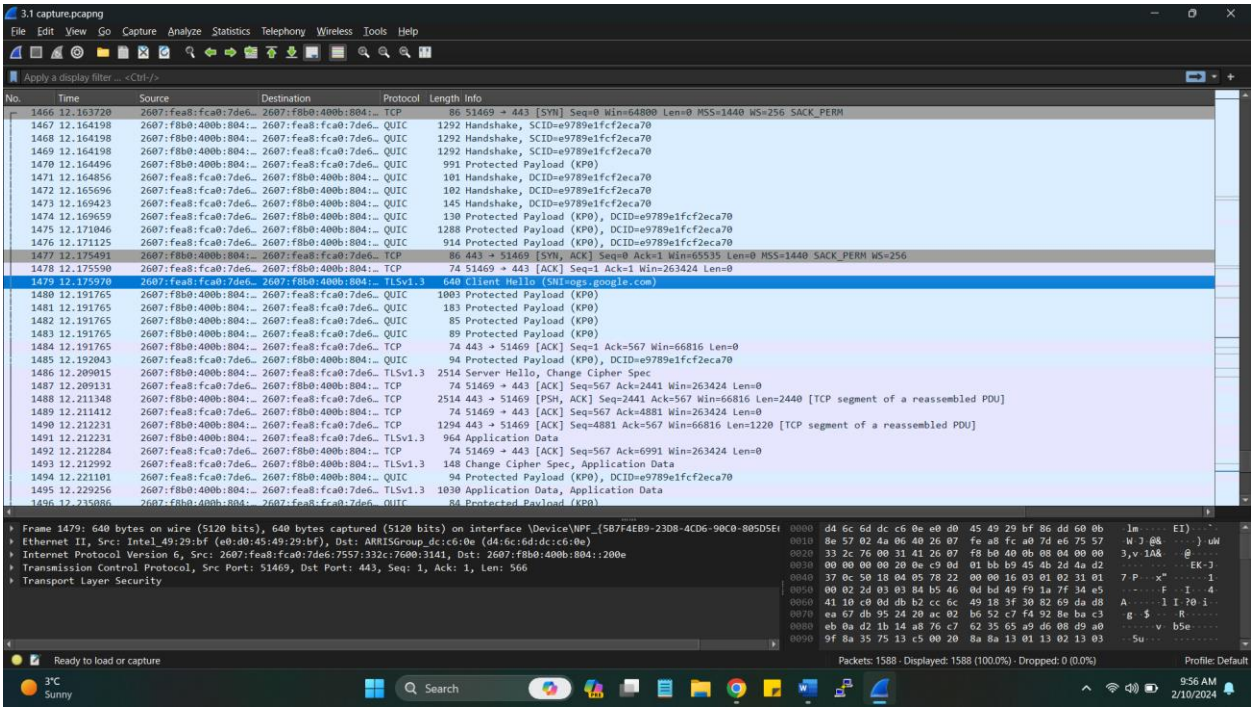
2. Open a command prompt and display the DNS resolver cache
   - Include screenshot of DNS resolver cache
   - Explain what is the importance of the DNS resolver cache?
   - ➔ "By default, most operating systems will cache IP addresses and other Domain Name System (DNS) records in order to fulfill future requests more quickly. This is DNS cache. The DNS cache prevents browsers from having to make a new request so that, instead, it can use stored information to load the website. This reduces server response times, making the site load more quickly." (Fitzgerald, 2023)

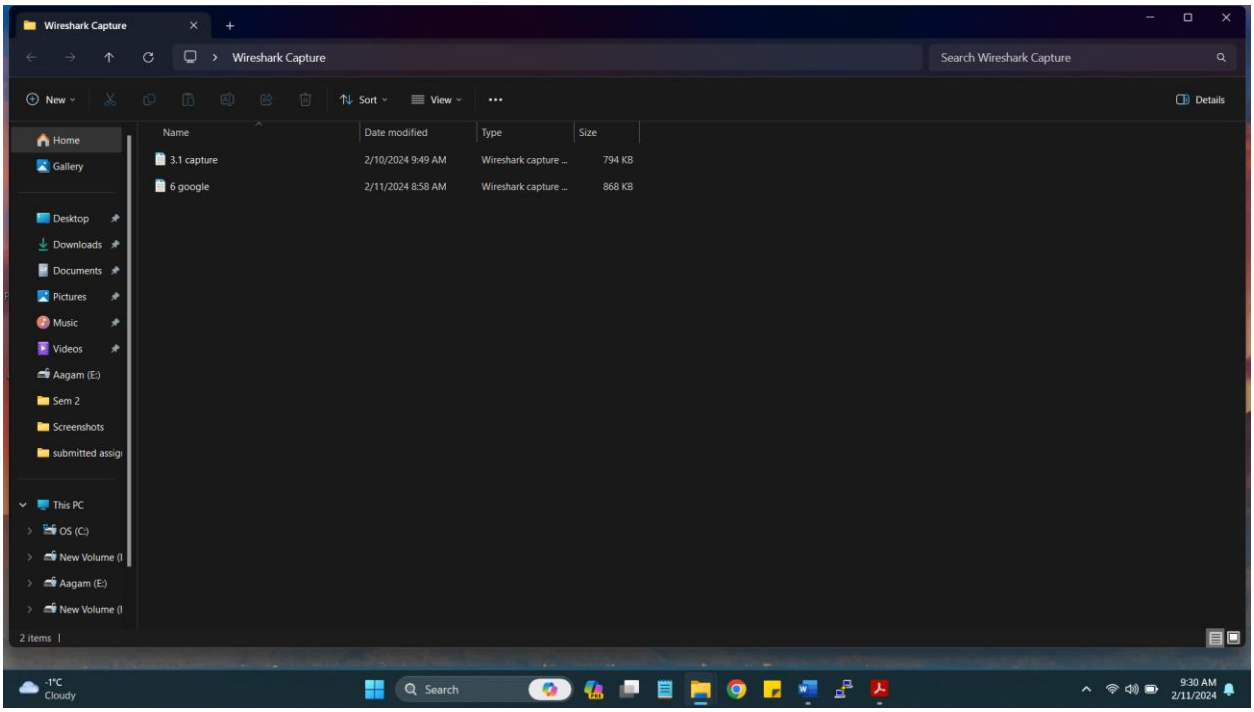
     Reference: Fitzgerald, A. (2023, October 23). Flush DNS: What It Is & How to Easily Clear DNS Cache. DNS. https://blog.hubspot.com/website/flush-dns#:~:text=By%20default%2C%20most%20operating%20systems,information%20to%20load%20the%20website.



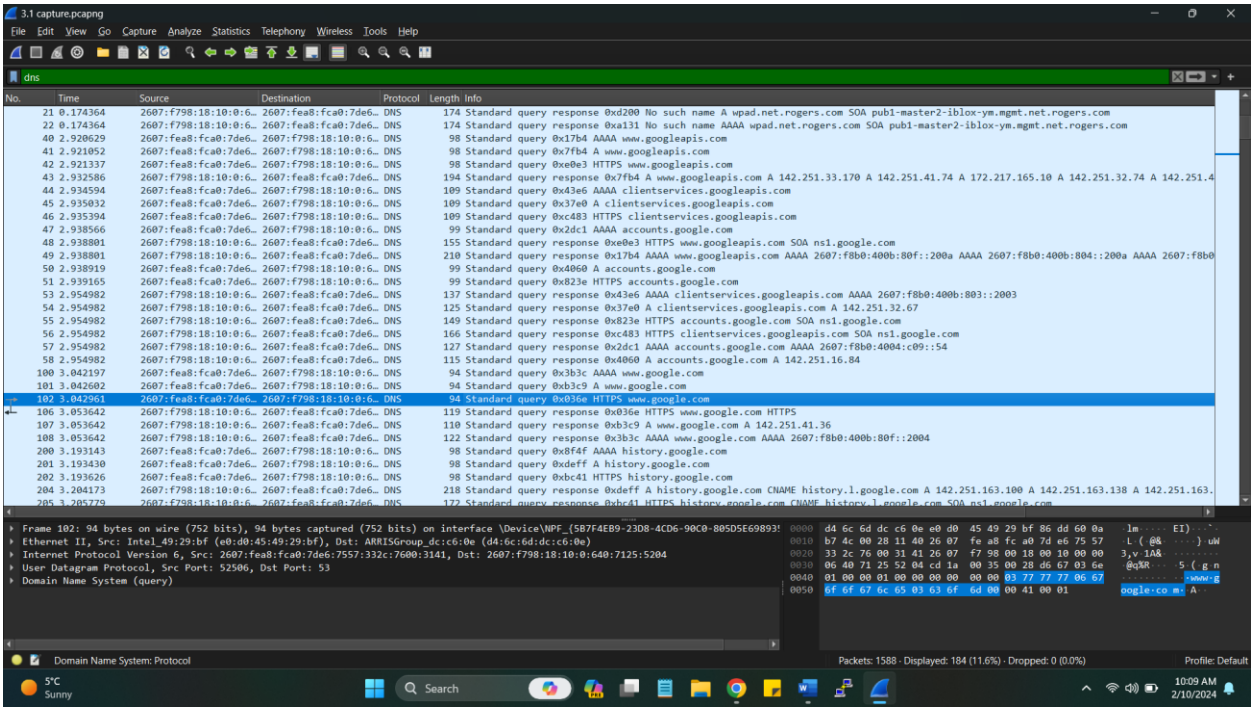
3. Start Wireshark and browse again to www.google.com, stop and save capture
    - Include screenshot of saving the network capture
    - Explain why it is important to save the network capture before analyzing it?

    ➔ As Wireshark application is used to capture packets, further it is important to save the packets captured as it will be helpful for future packets, ports, incoming out-going traffic/data on ports on which it is being monitored. It allows for investigations and helps in troubleshooting issue and monitoring the flow.

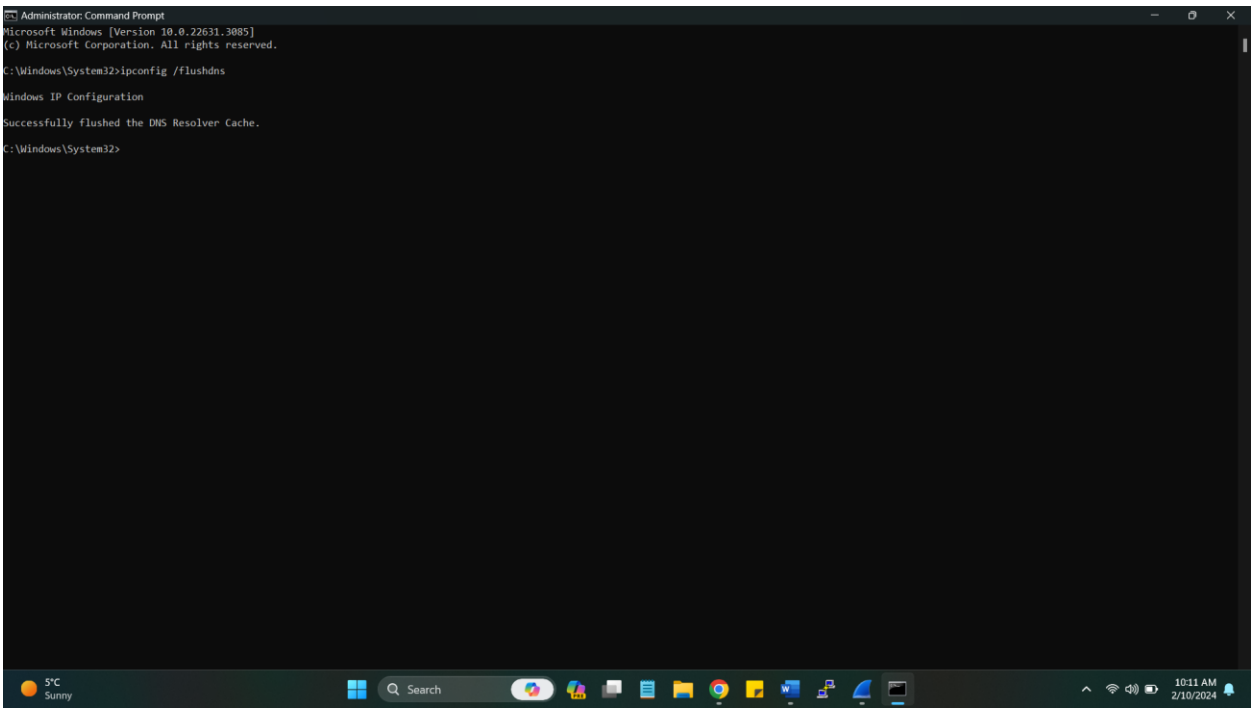




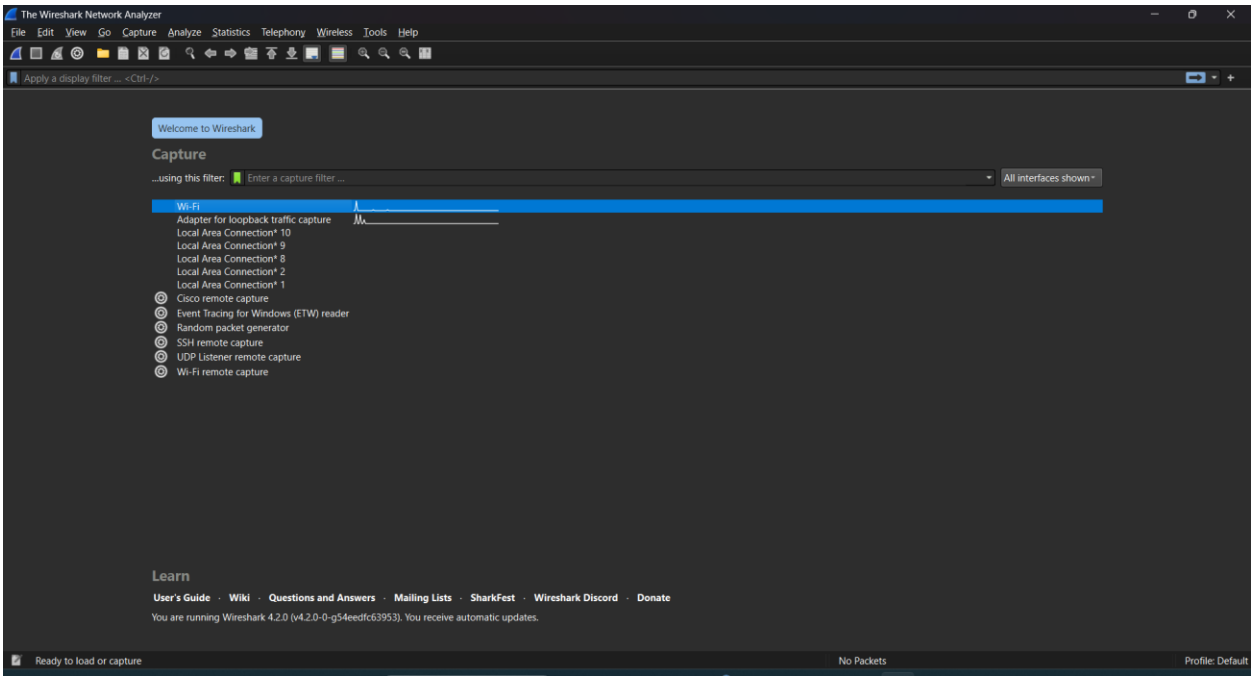
4. Enter dns as filter, do you see dns request for site?
    - Include screenshot showing dns filter has been entered
    - Why should you not see DNS traffic for www.google.com right now?
      →As DNS traffic for www.google.com response is cached on local machine, that's why we cannot see DNS Traffic.

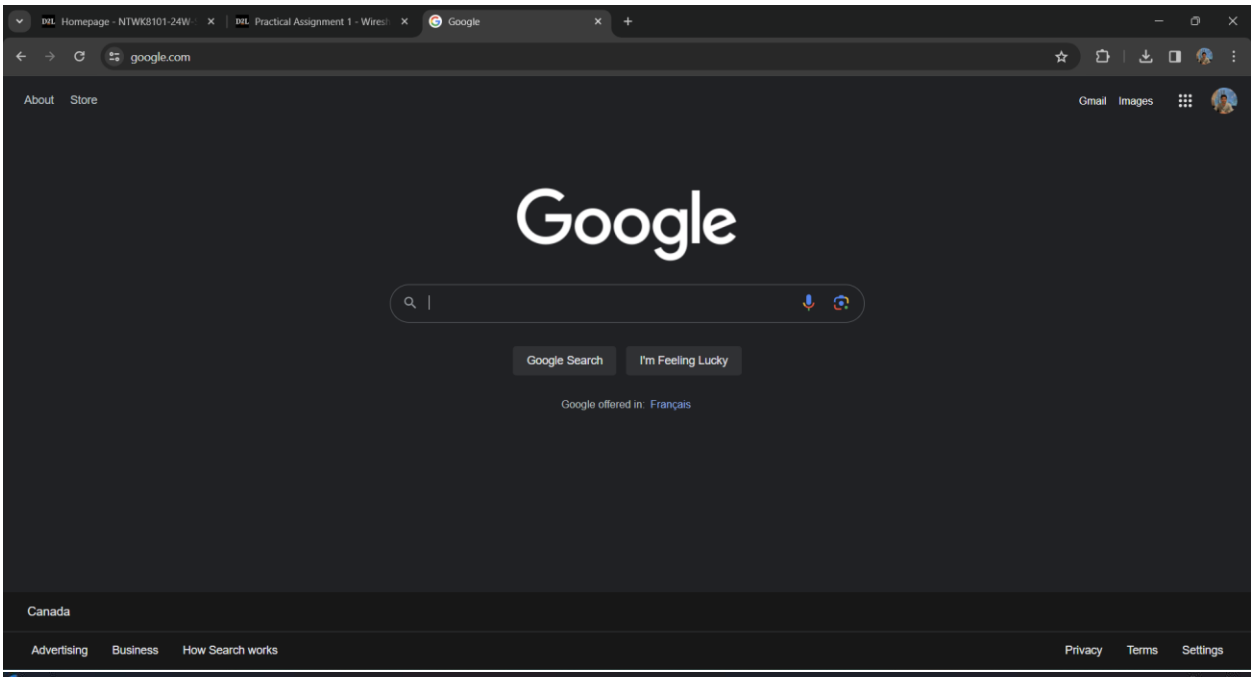


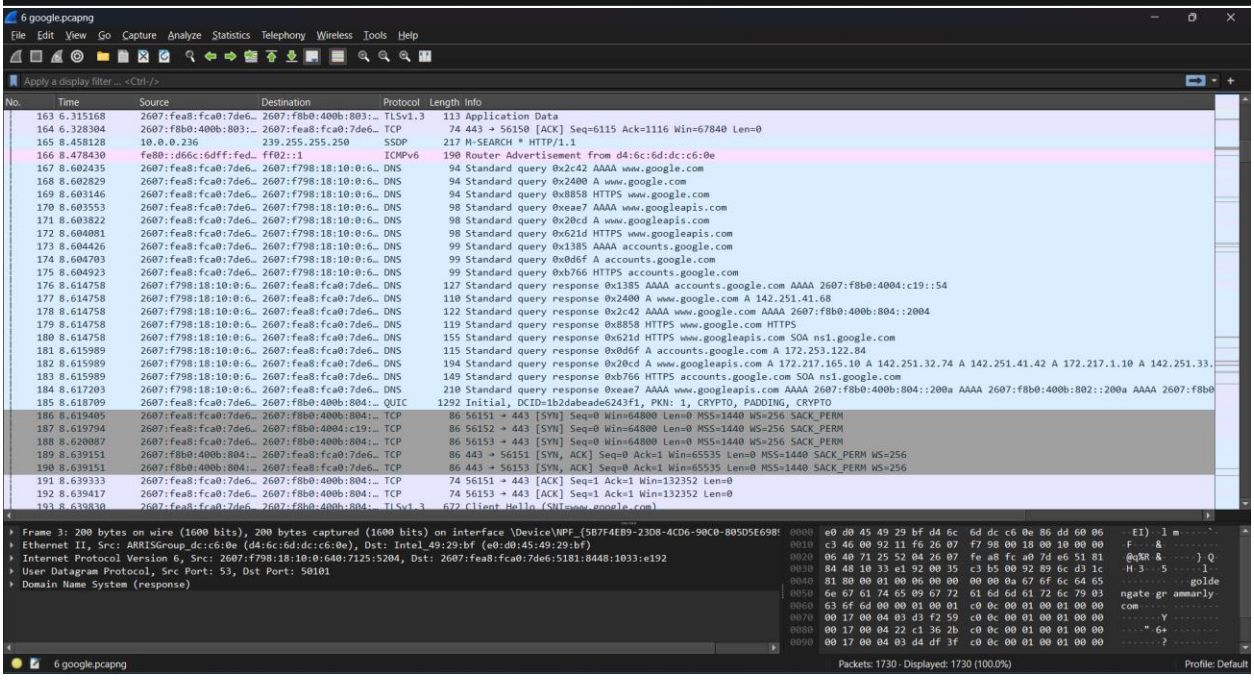
5. Back at the command prompt do ipconfig /flushdns
    - Include screenshot showing the DNS resolver cache successfully flushed

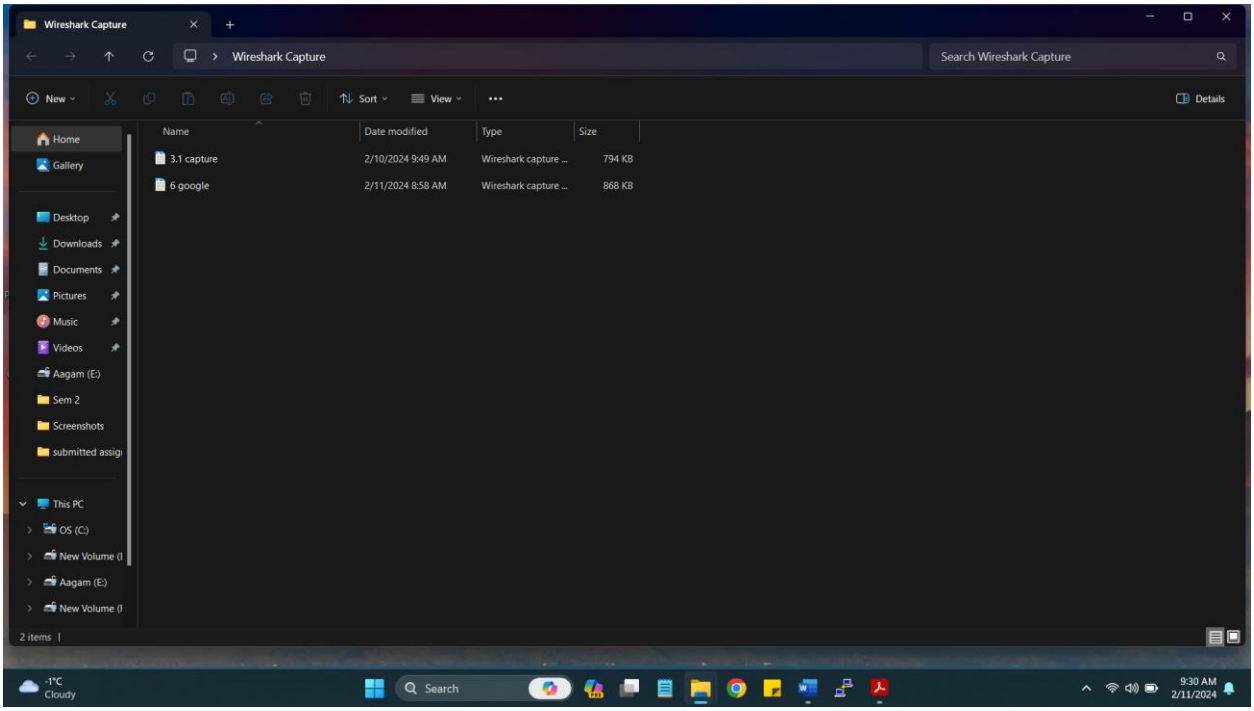


6. Start wireshark capture, browse to www.google.com, stop wireshark and save file


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
Wi-Fi
Adapter for loopback traffic capture
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Cisco remote capture
Event Tracing for Windows (ETW) reader
Random packet generator
SSH remote capture
UDP Listener remote capture
Wi-Fi remote capture
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.2.0 (v4.2.0-0-g54eedfc63953). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Default

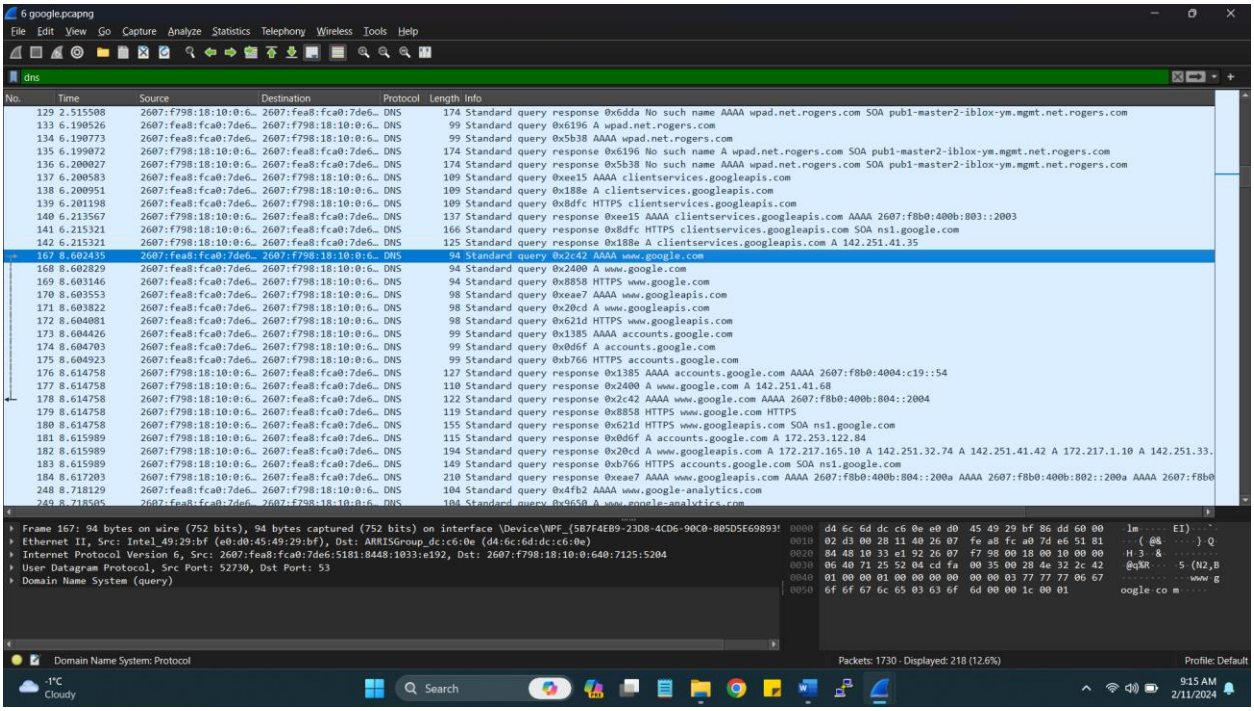

Homepage - NTWK8101-24W
Practical Assignment 1 - Wires
Google
google.com
About
Store
Gmail
Images
Google
Google Search
I'm Feeling Lucky
Google offered in: Français
Canada
Advertising
Business
How Search works
Privacy
Terms
Settings


6 google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
163 6.315168 2607:fea8:fca0:7de6... 2607:f8b0:400b:803:... TLSv1.3 113 Application Data
164 6.328304 2607:f8b0:400b:803:... 2607:fea8:fca0:7de6... TCP 74 443 → 56150 [ACK] Seq=6115 Ack=1116 Win=67840 Len=0
165 8.458128 10.0.0.236 239.255.255.250 SSDP 217 M-SEARCH * HTTP/1.1
166 8.478430 fe80::d66c:6dff:fed... ff02::1 ICMPv6 190 Router Advertisement from d4:6c:6d:dc:c6:0e
167 8.602435 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 94 Standard query 0x2c42 AAAA www.google.com
168 8.602829 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 94 Standard query 0x2400 A www.google.com
169 8.603146 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 94 Standard query 0x8858 HTTPS www.google.com
170 8.603553 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 98 Standard query 0xeae7 AAAA www.googleapis.com
171 8.603822 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 98 Standard query 0x20cd A www.googleapis.com
172 8.604081 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 98 Standard query 0x621d HTTPS www.googleapis.com
173 8.604426 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 99 Standard query 0x1385 AAAA accounts.google.com
174 8.604703 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 99 Standard query 0x0d6f A accounts.google.com
175 8.604923 2607:fea8:fca0:7de6... 2607:f798:18:10:0:6... DNS 99 Standard query 0xb766 HTTPS accounts.google.com
176 8.614758 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 127 Standard query response 0x1385 AAAA accounts.google.com AAAA 2607:f8b0:4004:c19::54
177 8.614758 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 110 Standard query response 0x2400 A www.google.com A 142.251.41.68
178 8.614758 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 122 Standard query response 0x2c42 AAAA www.google.com AAAA 2607:f8b0:400b:804::2004
179 8.614758 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 119 Standard query response 0x8858 HTTPS www.google.com HTTPS
180 8.614758 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 155 Standard query response 0x621d HTTPS www.googleapis.com SOA ns1.google.com
181 8.615989 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 115 Standard query response 0x0d6f A accounts.google.com A 172.253.122.84
182 8.615989 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 194 Standard query response 0x20cd A www.googleapis.com A 172.217.165.10 A 142.251.32.74 A 142.251.41.42 A 172.217.1.10 A 142.251.33.
183 8.615989 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 149 Standard query response 0xb766 HTTPS accounts.google.com SOA ns1.google.com
184 8.617203 2607:f798:18:10:0:6... 2607:fea8:fca0:7de6... DNS 210 Standard query response 0xeae7 AAAA www.googleapis.com AAAA 2607:f8b0:400b:804::200a AAAA 2607:f8b0:802::200a AAAA 2607:f8b0
185 8.618709 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... QUIC 1292 Initial, DCID=1b2dabeade6243f1, PKN: 1, CRYPTO, PADDING, CRYPTO
186 8.619405 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... TCP 86 56151 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
187 8.619794 2607:fea8:fca0:7de6... 2607:f8b0:4004:c19:... TCP 86 56152 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
188 8.620087 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... TCP 86 56153 → 443 [SYN] Seq=0 Win=64800 Len=0 MSS=1440 WS=256 SACK_PERM
189 8.639151 2607:f8b0:400b:804:... 2607:fea8:fca0:7de6... TCP 86 443 → 56151 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=256
190 8.639151 2607:f8b0:400b:804:... 2607:fea8:fca0:7de6... TCP 86 443 → 56153 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 SACK_PERM WS=256
191 8.639333 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... TCP 74 56151 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
192 8.639417 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... TCP 74 56153 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
193 8.639830 2607:fea8:fca0:7de6... 2607:f8b0:400b:804:... TLSv1.3 672 Client Hello (SNI=www.google.com)
Frame 3: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface \Device\NPF_{5B7F4EB9-23D8-4CD6-90C0-805D5E698
Ethernet II, Src: ARRISGroup_dc:c6:0e (d4:6c:6d:dc:c6:0e), Dst: Intel_49:29:bf (e0:d0:45:49:29:bf)
Internet Protocol Version 6, Src: 2607:f798:18:10:0:640:7125:5204, Dst: 2607:fea8:fca0:7de6:5181:8448:1033:e192
User Datagram Protocol, Src Port: 53, Dst Port: 50101
Domain Name System (response)
0000 e0 d0 45 49 29 bf d4 6c 6d dc c6 0e 86 dd 60 06
0010 c3 46 00 92 11 f6 26 07 f7 98 00 18 00 10 00 00
0020 06 40 71 25 52 04 26 07 fe a8 fc a0 7d e6 51 81
0030 84 48 10 33 e1 92 00 35 c3 b5 00 92 89 6c d3 1c
0040 81 80 00 01 00 06 00 00 00 00 0a 67 6f 6c 64 65
0050 6e 67 61 74 65 09 67 72 61 6d 6d 61 72 6c 79 03
0060 63 6f 6d 00 00 01 00 01 c0 0c 00 01 00 01 00 00
0070 00 17 00 04 03 d3 f2 59 c0 0c 00 01 00 01 00 00
0080 00 17 00 04 22 c1 36 2b c0 0c 00 01 00 01 00 00
0090 00 17 00 04 03 d4 df 3f c0 0c 00 01 00 01 00 00
6 google.pcapng
Packets: 1730 · Displayed: 1730 (100.0%)
Profile: Default



7. Enter dns filter
    - Include screenshot showing newly filtered network capture showing the DNS query for www.google.com
    - Explain why this is now visible in the network capture?

As DNS entry is cached on local system, for that reason now the DNS packets are captured for www.google.com and now it's visible. Since DNS cache database has all the records of recently visited sites.



8. Right click on one of the DNS frames and choose follow stream
    - Include screenshot of filtered network capture showing the filtered stream traffic
    - Does it show communication with the actual google endpoint? Explain why or why not.

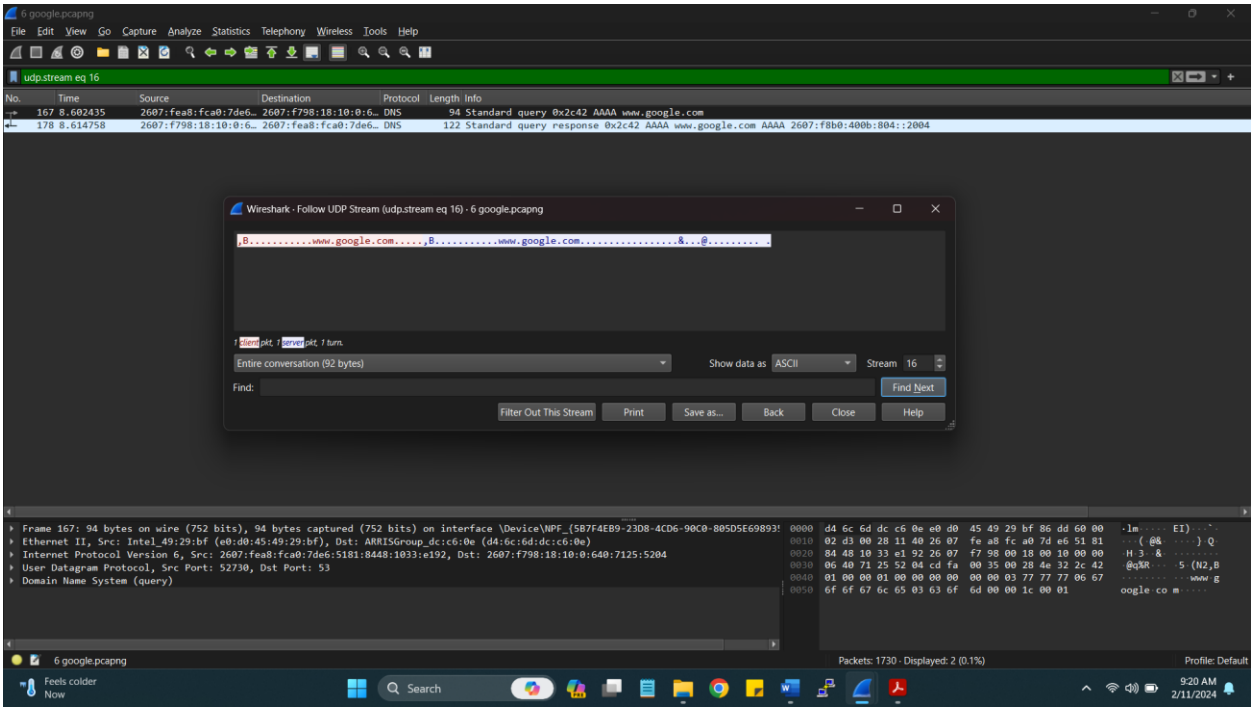
    →No, it doesn't show the actual google endpoint as packet captured is filtered with only DNS server entries.

    - What port and protocol does DNS use?

    → "The Domain Name System (DNS) uses UDP port 53 and TCP port 53. The storage system does not typically listen on these ports because it does not run a domain name server. However, if DNS is enabled on your storage system, it makes outgoing connections using UDP port 53 for host name and IP address lookups." (*DNS*, n.d.)

Reference: DNS. (n.d.). (C) Copyright 2013.

https://library.netapp.com/ecmdocs/ECMP1155586/html/GUID-D052D155-EF55-4D19-A70F-B9A8FA86A6D3.html#:~:text=The%20Domain%20Name%20System%20(DNS,name%20and%20IP%20address%20lookups.


6 google.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp.stream eq 16
No. Time Source Destination Protocol Length Info
167 8.602435 2607:fea8:fca0:7de6… 2607:f798:18:10:0:6… DNS 94 Standard query 0x2c42 AAAA www.google.com
178 8.614758 2607:f798:18:10:0:6… 2607:fea8:fca0:7de6… DNS 122 Standard query response 0x2c42 AAAA www.google.com AAAA 2607:f8b0:400b:804::2004
Wireshark · Follow UDP Stream (udp.stream eq 16) · 6 google.pcapng
,B.....www.google.com.....,B.....www.google.com.....&...@.....
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (92 bytes)
Show data as ASCII
Stream 16
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Frame 167: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface \Device\NPF_{5B7F4EB9-23D8-4CD6-90C0-805D5E69893
Ethernet II, Src: Intel_49:29:bf (e0:d0:45:49:29:bf), Dst: ARRISGroup_dc:c6:0e (d4:6c:6d:dc:c6:0e)
Internet Protocol Version 6, Src: 2607:fea8:fca0:7de6:5181:8448:1033:e192, Dst: 2607:f798:18:10:0:640:7125:5204
User Datagram Protocol, Src Port: 52730, Dst Port: 53
Domain Name System (query)
0000 d4 6c 6d dc c6 0e e0 d0 45 49 29 bf 86 dd 60 00
0010 02 d3 00 28 11 40 26 07 fe a8 fc a0 7d e6 51 81
0020 84 48 10 33 e1 92 26 07 f7 98 00 18 00 10 00 00
0030 06 40 71 25 52 04 cd fa 00 35 00 28 4e 32 2c 42
0040 01 00 00 01 00 00 00 00 00 00 03 77 77 77 06 67
0050 6f 6f 67 6c 65 03 63 6f 6d 00 00 1c 00 01
6 google.pcapng
Packets: 1730 · Displayed: 2 (0.1%)
Profile: Default
Feels colder Now
Search
9:20 AM 2/11/2024