

PROJECT MODULE TASK



WIRESHARK PACKET CAPTURE

CYBERSECURITY & ETHICAL HACKING PROJECT TASKS



PROJECT MODULE

WIRESHARK PACKET CAPTURE

Background

Wireshark is a free tool that captures the packets moving across a network and lets you read them one by one. Network engineers use it to find problems and security teams use it to spot suspicious traffic.

When you open a website, your laptop first asks a DNS server for the IP address of that website. It then connects to that IP address and starts a secure TLS connection. In this lab you will capture your own Wi-Fi traffic while you open a website, and read this information from the packets.

Task

Capture your own Wi-Fi traffic with Wireshark on your Windows laptop while you open networkwalks.com, then find the six answers below in the packets.

Website: <https://networkwalks.com>

Questions to answer:

1. What is the IP address of your own laptop?
2. What is the IP address of your DNS server?
3. What is the IP address of the website networkwalks.com?
4. Which website name (Server Name) is sent in the TLS Client Hello?
5. Which server port is used for the secure connection?
6. Which TLS version does the website use?

Submit one screenshot of Wireshark showing the DNS answer with the website IP, and your answers to the six questions.

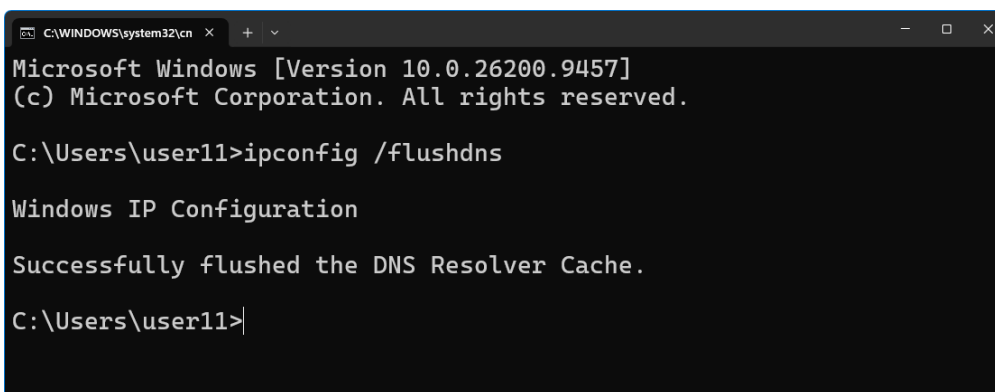
Solution

STEP 1

Close all browser windows. Open Command Prompt and run this command to clear the DNS cache:

```
ipconfig /flushdns
```

You should see Successfully flushed the DNS Resolver Cache. Without this step your laptop may remember the website and skip the DNS query.



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.26200.9457]
(c) Microsoft Corporation. All rights reserved.

C:\Users\user11>ipconfig /flushdns

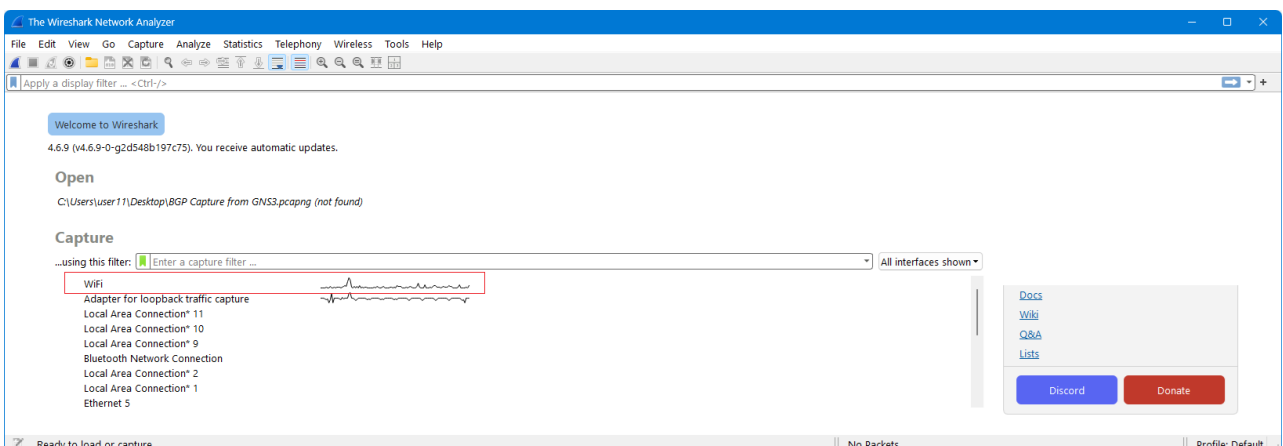
Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Users\user11>
```

STEP 2

Open Wireshark. On the start screen, double-click the adapter that shows a moving line (usually Wi-Fi). The capture starts at once.

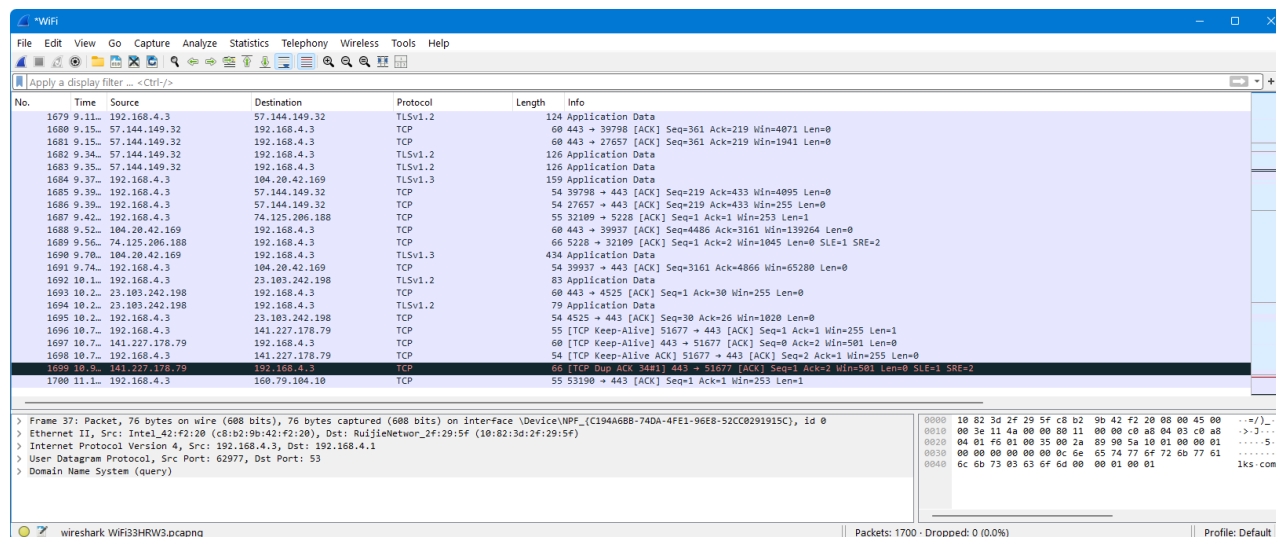


STEP 3

Open a new Incognito window in Chrome (Ctrl + Shift + N) and go to the website. Wait until the page loads fully.

<https://networkwalks.com>

Come back to Wireshark and stop the capture with the red square button.

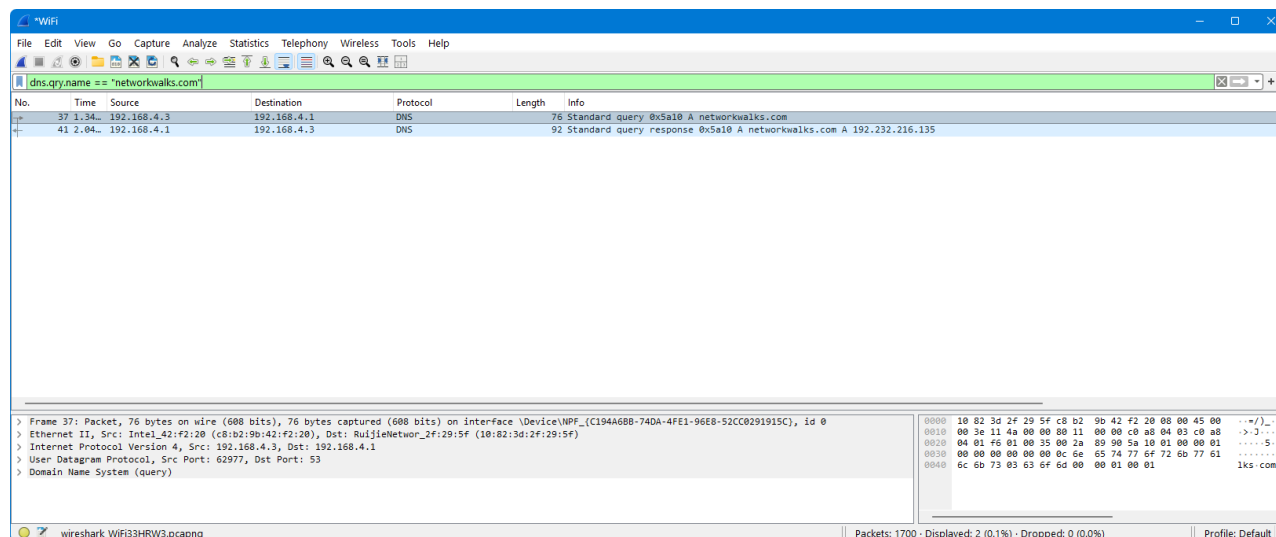


STEP 4

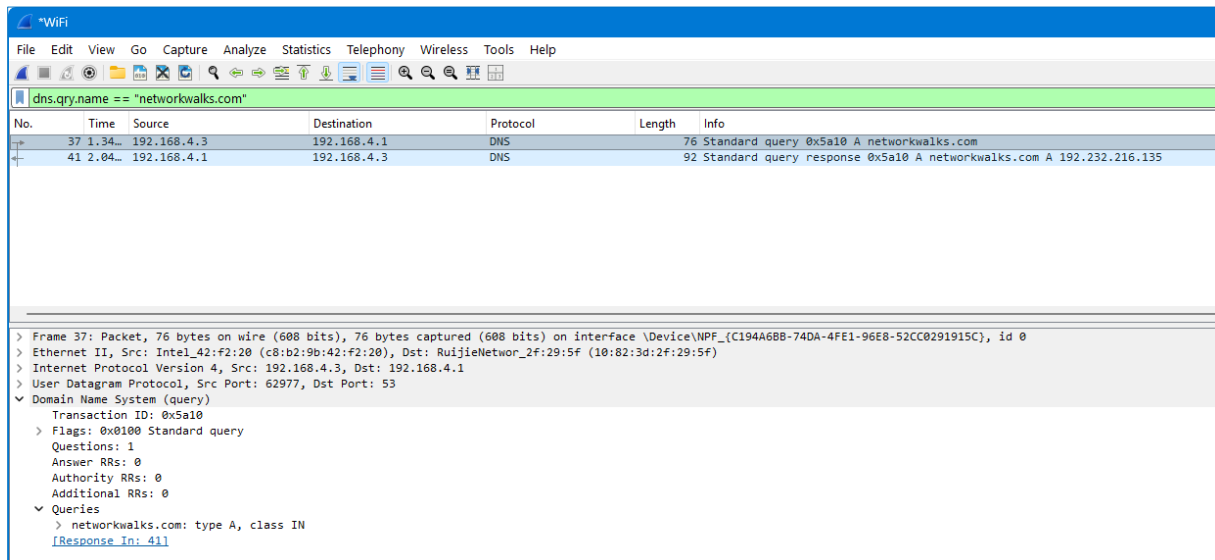
Type this in the display filter bar and press Enter:

`dns.qry.name == "networkwalks.com"`

You should see two packets, a query and a response.



Click the query. The Source is your laptop and the Destination is your DNS server.

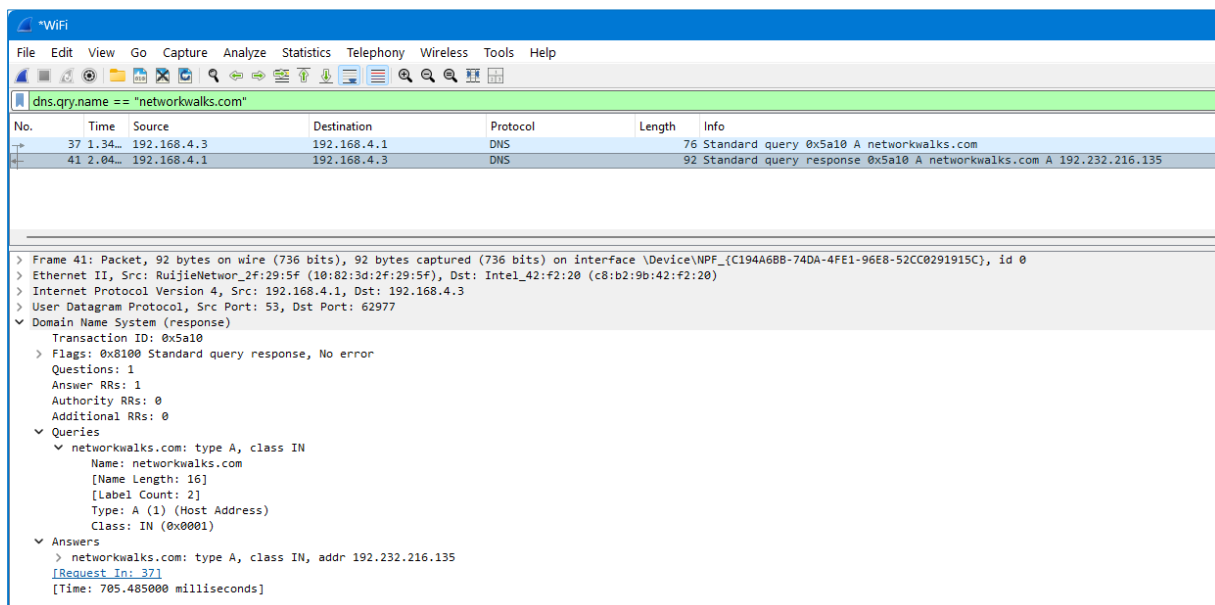


The screenshot shows a Wireshark capture of a DNS query. The packet list pane shows two packets: a standard query (No. 37) and a standard query response (No. 41). The packet details pane for packet 41 shows the Domain Name System (query) section expanded, displaying the transaction ID (0x5a10), flags (0x0100), and the query for networkwalks.com.

Answer1: Laptop IP is 192.168.4.3

Answer2: DNS Server IP is 192.168.4.1

Now click the response. In the middle pane expand Domain Name System (response), then Answers. The Address is the website IP.



The screenshot shows a Wireshark capture of a DNS response. The packet list pane shows two packets: a standard query (No. 37) and a standard query response (No. 41). The packet details pane for packet 41 shows the Domain Name System (response) section expanded, displaying the transaction ID (0x5a10), flags (0x0100), and the response for networkwalks.com. The Answers section is expanded, showing the IP address 192.232.216.135.

Answer3: Website IP is 192.232.216.135

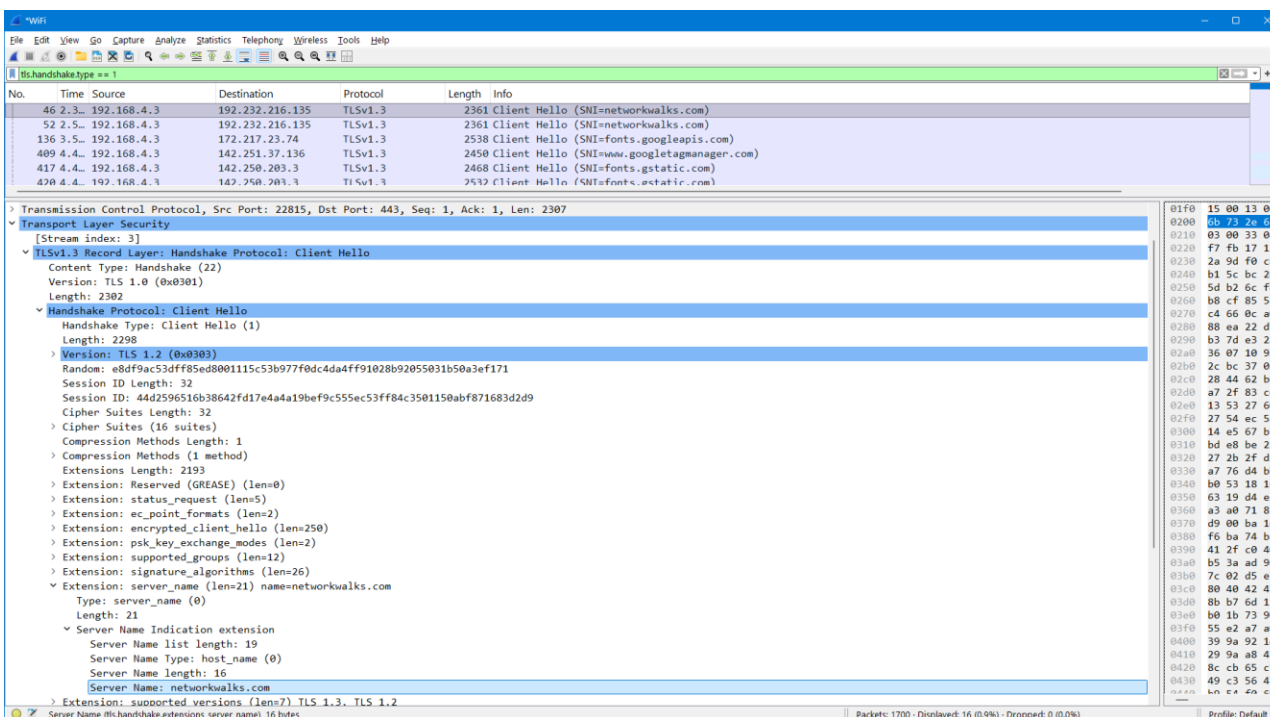
Tip: If no packet shows, close the browser fully, run `ipconfig /flushdns` again and capture again. Also check that Chrome Secure DNS is off (Settings > Privacy and security > Security), because it hides the DNS query.

STEP 5

Use this filter:

`tls.handshake.type == 1`

This shows the Client Hello, the first packet of the secure connection. Click the one that says SNI=networkwalks.com. Its Destination is the website IP. Expand Transport Layer Security > Handshake Protocol: Client Hello > Extension: server_name.



The screenshot shows the Wireshark network protocol analyzer. The packet list on the left shows several TLSv1.3 Client Hello packets. The selected packet (No. 46) is expanded to show the Handshake Protocol details. The 'Extension: server_name' field is highlighted, showing the value 'networkwalks.com'.

Answer4: Server Name: networkwalks.com

Then expand the Transmission Control Protocol line. The Destination Port is the Server port.

No.	Time	Source	Destination	Protocol	Length	Info
46	2.3...	192.168.4.3	192.232.216.135	TLSv1.3	2361	Client Hello (SNI=networkwalks.com)
52	2.5...	192.168.4.3	192.232.216.135	TLSv1.3	2361	Client Hello (SNI=networkwalks.com)
136	3.5...	192.168.4.3	172.217.23.74	TLSv1.3	2538	Client Hello (SNI=fonts.googleapis.com)
409	4.4...	192.168.4.3	142.251.37.136	TLSv1.3	2450	Client Hello (SNI=www.googletagmanager.com)
417	4.4...	192.168.4.3	142.250.203.3	TLSv1.3	2468	Client Hello (SNI=fonts.gstatic.com)
420	4.4...	192.168.4.3	142.250.203.3	TLSv1.3	2532	Client Hello (SNI=fonts.gstatic.com)

> Frame 46: Packet, 2361 bytes on wire (18888 bits), 2361 bytes captured (18888 bits) on interface \Device\NPF_{C194A6BB-74DA-4FE1-96E8-52CC0291915C}, id 0

> Ethernet II, Src: Intel_42:f2:20 (c8:b2:9b:42:f2:20), Dst: RuijieNetwork_2f:29:5f (10:82:3d:2f:29:5f)

> Internet Protocol Version 4, Src: 192.168.4.3, Dst: 192.232.216.135

> Transmission Control Protocol, Src Port: 22815, Dst Port: 443, Seq: 1, Ack: 1, Len: 2307

Source Port: 22815

Destination Port: 443

[Stream index: 4]

[Stream Packet Number: 4]

> [Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 2307]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 3318511513

Answer5: Server Port is 443

Tip: If the Protocol column says QUIC, this is normal. Chrome uses QUIC (HTTP/3) on port 443 for some sites. The filter still works. If you see no packet, try the same steps in another browser.

STEP 6

Apply this filter:

`tls.handshake.type == 2`

This shows the Server Hello, the reply from the website. Pick the one where the Source is the website IP from Step 4.

Look at the Protocol column. It shows the TLS version.

No.	Time	Source	Destination	Protocol	Length	Info
51	2...	192.232.216.135	192.168.4.3	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data, Application Data
63	2...	192.232.216.135	192.168.4.3	TLSv1.3	308	Server Hello, Change Cipher Spec, Application Data, Application Data
206	3...	172.217.23.74	192.168.4.3	TLSv1.3	1466	Server Hello, Change Cipher Spec
430	4...	142.251.37.136	192.168.4.3	TLSv1.3	1466	[TCP Out-of-Order], Server Hello, Change Cipher Spec
545	4...	104.20.42.169	192.168.4.3	TLSv1.3	1429	Server Hello, Change Cipher Spec, Application Data
604	4...	142.250.203.3	192.168.4.3	TLSv1.3	1466	Server Hello, Change Cipher Spec
610	4...	142.250.203.3	192.168.4.3	TLSv1.3	1466	[TCP Out-of-Order], Server Hello, Change Cipher Spec
1071	5...	172.217.112.4	192.168.4.3	TLSv1.3	1466	Server Hello, Change Cipher Spec
1097	5...	67.23.251.4	192.168.4.3	TLSv1.3	292	Server Hello, Change Cipher Spec, Application Data, Application Data
1111	5...	172.217.112.4	192.168.4.3	TLSv1.3	1466	Server Hello, Change Cipher Spec
1125	5...	67.23.251.4	192.168.4.3	TLSv1.3	292	Server Hello, Change Cipher Spec, Application Data, Application Data
1127	5...	142.251.151.119	192.168.4.3	QUIC	1292	Initial, SCID=f0b43dbbfccf034, PKN: 6, CRYPTO, PADDING
1140	5...	142.250.202.134	192.168.4.3	TLSv1.3	1466	Server Hello, Change Cipher Spec
1196	6...	104.20.42.169	192.168.4.3	QUIC	1242	Initial, SCID=01482a1b1069abcd0048991b09693acd00889125, PKN: 2, CRYPTO
1434	6...	172.66.161.212	192.168.4.3	QUIC	1242	Protected Payload (KP0)
1599	7...	104.20.42.169	192.168.4.3	TLSv1.3	1506	Server Hello, change cipher spec

> Frame 51: Packet, 308 bytes on wire (2464 bits), 308 bytes captured (2464 bits) on interface \Device\NPF_{C194A6BB-74DA-4FE1-96E8-52CC0291915C}, id 0

> Ethernet II, Src: RuijieNetwork_2f:29:5f (10:82:3d:2f:29:5f), Dst: Intel_42:f2:20 (c8:b2:9b:42:f2:20)

> Internet Protocol Version 4, Src: 192.232.216.135, Dst: 192.168.4.3

> Transmission Control Protocol, Src Port: 443, Dst Port: 22815, Seq: 1, Ack: 2308, Len: 254

> Transport Layer Security

0020 04 03 01
0030 01 62 5f
0040 03 5d 1e
0050 b2 fc 09
0060 b3 20 44
0070 ef 9c 55
0080 d2 d9 13

Destination Port (tcp.dstport), 2 bytes

Packets: 1700 - Displayed: 16 (0.9%) - Dropped: 0 (0.0%)

Profile: Default

Answer6: TLS version is TLSv1.3



© All Rights are reserved, Networkwalks

Contact us today for your Cybersecurity & Network consultancy or your next training course & certification on
Cisco CCNA, Cybersecurity, Ethical Hacking, Python programming, Linux & AI.

 **+27 766 222 218 | +27 788 220 600**

Leave your feedback at: info@networkwalks.com. Your technical questions, comments & suggestions are always Welcomed.
www.networkwalks.com