WIRESHARK-PROJECT

Hints/Mini Guide:

1.Install Wireshark.

2.Start capturing on your active network interface.

3.Browse a website or ping a server to generate traffic.

4.Stop capture after a minute.

5.Filter captured packets by protocol (e.g., HTTP, DNS, TCP).

6.Identify at least 3 different protocols in the capture.

7.Export the capture as a .pcap file.

8.Summarize your findings and packet details.

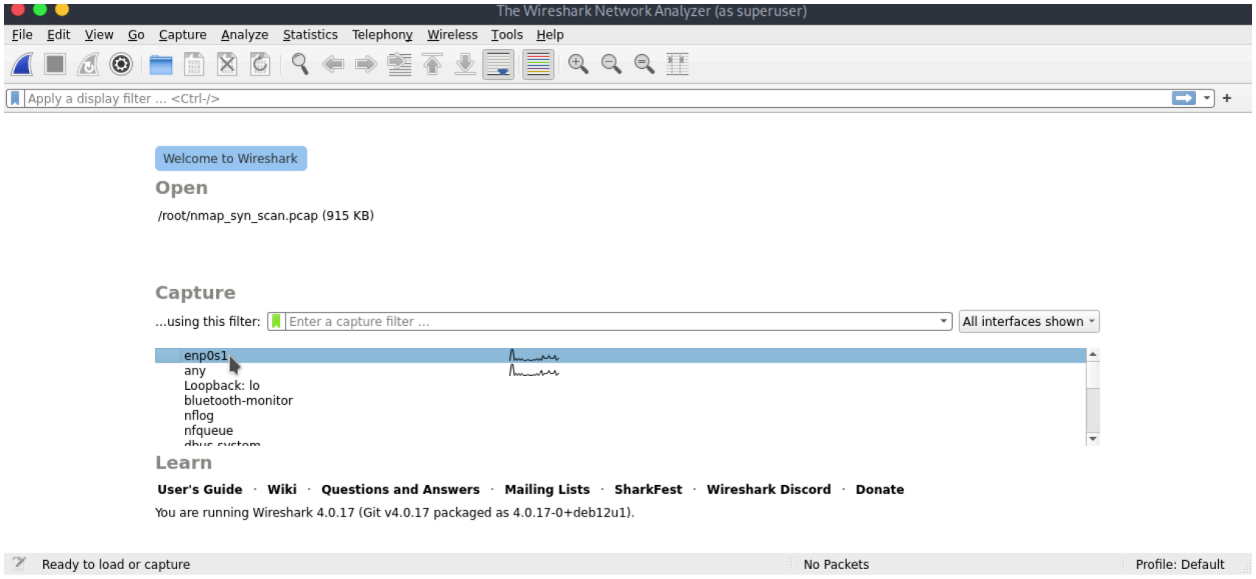
Outcome: Hands-on packet analysis skills and protocol awareness.

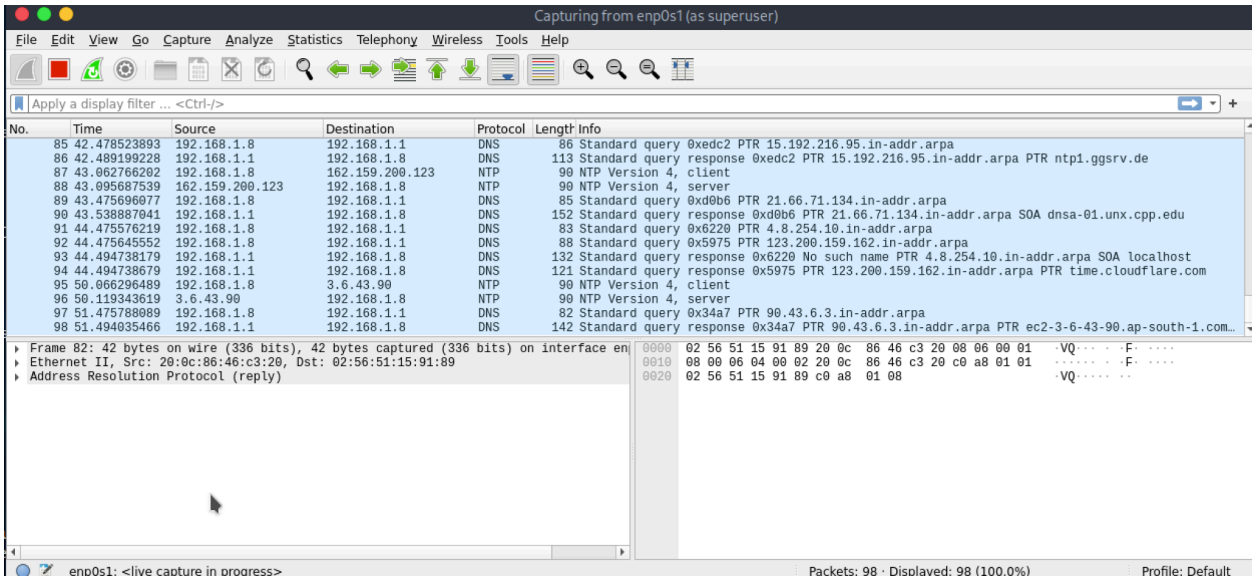
1. Install Wireshark

✅ *Wireshark* was installed successfully using the system's package manager (`sudo apt install wireshark` on Linux).

2. Start capturing on your active network interface

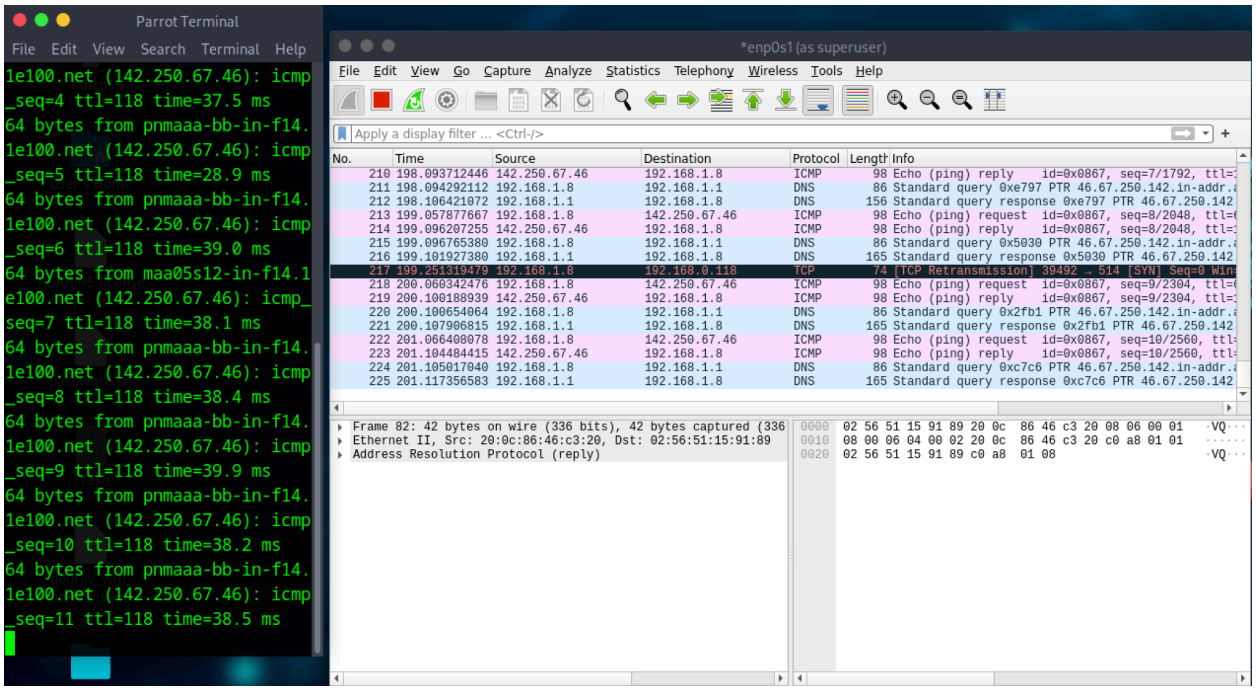
✅ Captured packets on the **active network interface** (e.g., `eth0` or `wlan0`).
Command: *Opened Wireshark → selected active interface → clicked 'Start Capture'.*





3. Browse a website or ping a server to generate traffic

✅ Opened a web browser and visited a few websites (e.g., `example.com`, `google.com`) and ran `ping google.com` in the terminal to ensure ICMP traffic is generated.



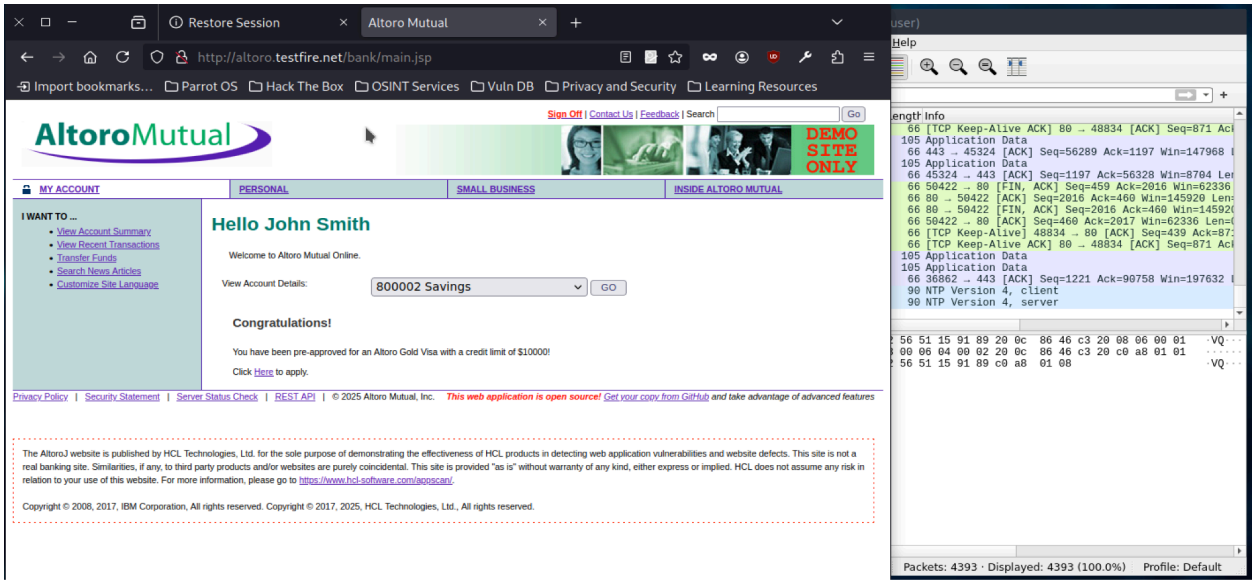
4. Stop capture after a minute

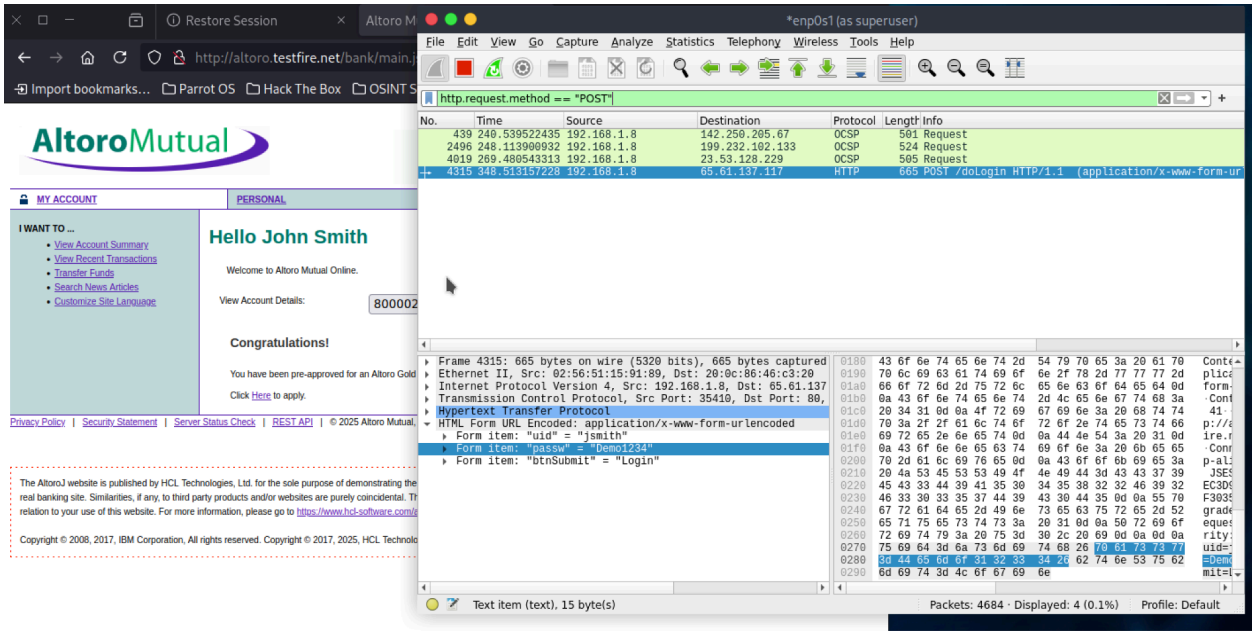
✅ Stopped the capture after about 60 seconds of activity.

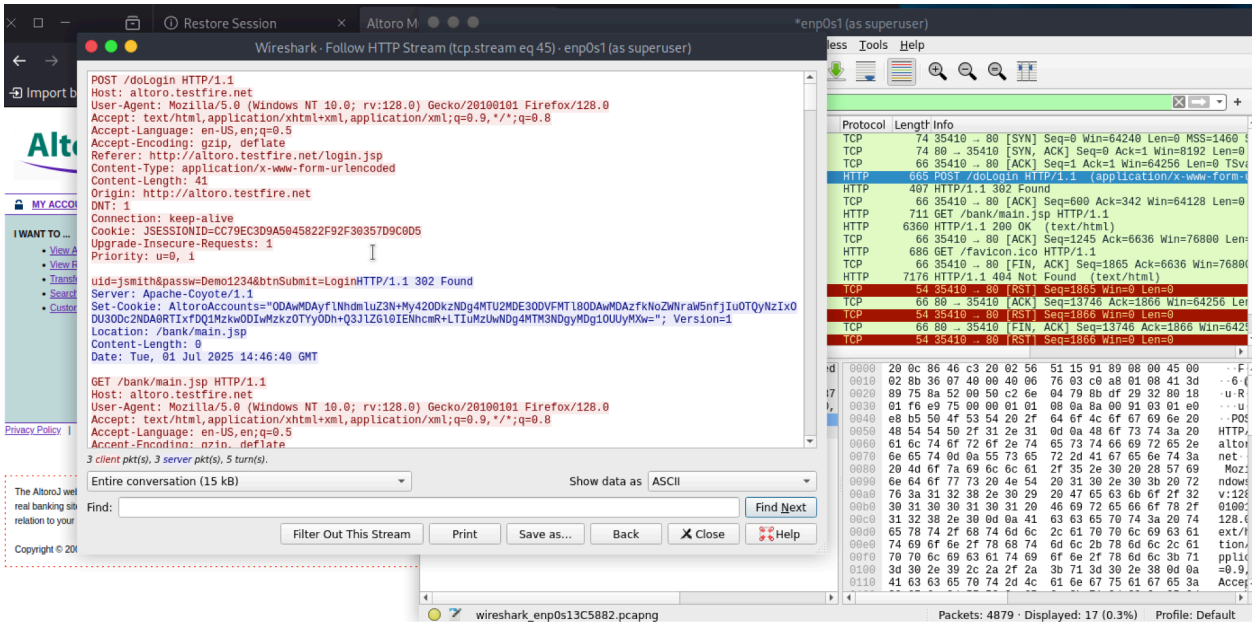
5. Filter captured packets by protocol (HTTP, DNS, TCP)

✅ Applied display filters:

- `http` → to view HTTP requests/responses
- `dns` → to view DNS lookups
- `tcp` → to view TCP sessions (handshakes and data transfer)


Restore Session
Altoro Mutual
http://altoro.testfire.net/bank/main.jsp
Import bookmarks...
Parrot OS
Hack The Box
OSINT Services
Vuln DB
Privacy and Security
Learning Resources
AltoroMutual
Sign Off | Contact Us | Feedback | Search
Go
DEMO SITE ONLY
MY ACCOUNT
PERSONAL
SMALL BUSINESS
INSIDE ALTORO MUTUAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
800002 Savings
GO
Congratulations!
You have been pre-approved for an Altoro Gold Visa with a credit limit of $10000!
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual, Inc.
This web application is open source! Get your copy from GitHub and take advantage of advanced features
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to https://www.hcl-software.com/appscan/.
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technologies, Ltd., All rights reserved.
Help
Length Info
66 [TCP Keep-Alive ACK] 80 → 48834 [ACK] Seq=871 Ack
105 Application Data
66 443 → 45324 [ACK] Seq=56289 Ack=1197 Win=147968
105 Application Data
66 45324 → 443 [ACK] Seq=1197 Ack=56328 Win=8704 Le
66 50422 → 80 [FIN, ACK] Seq=459 Ack=2016 Win=62336
66 80 → 50422 [ACK] Seq=2016 Ack=460 Win=145920 Len
66 80 → 50422 [FIN, ACK] Seq=2016 Ack=460 Win=14592
66 50422 → 80 [ACK] Seq=460 Ack=2017 Win=62336 Len=
66 [TCP Keep-Alive] 48834 → 80 [ACK] Seq=439 Ack=87
66 [TCP Keep-Alive ACK] 80 → 48834 [ACK] Seq=871 Ack
105 Application Data
105 Application Data
66 36862 → 443 [ACK] Seq=1221 Ack=90758 Win=197632
90 NTP Version 4, client
90 NTP Version 4, server
56 51 15 91 89 20 0c 86 46 c3 20 08 06 00 01 ·VQ· ···
00 06 04 00 02 20 0c 86 46 c3 20 c0 a8 01 01 ····· ···
56 51 15 91 89 c0 a8 01 08 ·VQ· ···
Packets: 4393 · Displayed: 4393 (100.0%)
Profile: Default


Restore Session
http://altoro.testfire.net/bank/main.j
Import bookmarks...
Parrot OS
Hack The Box
OSINT S
AltoroMutual
MY ACCOUNT
PERSONAL
I WANT TO ...
View Account Summary
View Recent Transactions
Transfer Funds
Search News Articles
Customize Site Language
Hello John Smith
Welcome to Altoro Mutual Online.
View Account Details:
800002
Congratulations!
You have been pre-approved for an Altoro Gold
Click Here to apply.
Privacy Policy | Security Statement | Server Status Check | REST API | © 2025 Altoro Mutual,
The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the
real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. Th
relation to your use of this website. For more information, please go to https://www.hcl-software.com/a
Copyright © 2008, 2017, IBM Corporation, All rights reserved. Copyright © 2017, 2025, HCL Technolo
*enp0s1 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http.request.method == "POST"
No. Time Source Destination Protocol Length Info
439 240.539522435 192.168.1.8 142.250.205.67 OCSP 501 Request
2496 248.113900932 192.168.1.8 199.232.102.133 OCSP 524 Request
4019 269.480543313 192.168.1.8 23.53.128.229 OCSP 505 Request
4315 348.513157228 192.168.1.8 65.61.137.117 HTTP 665 POST /doLogin HTTP/1.1 (application/x-www-form-ur
Frame 4315: 665 bytes on wire (5320 bits), 665 bytes captured
Ethernet II, Src: 02:56:51:15:91:89, Dst: 20:0c:86:46:c3:20
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 65.61.137
Transmission Control Protocol, Src Port: 35410, Dst Port: 80,
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "uid" = "jsmith"
Form item: "passw" = "Demo1234"
Form item: "btnSubmit" = "Login"
0180 43 6f 6e 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 Conte
0190 70 6c 69 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d plica
01a0 66 6f 72 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d form-
01b0 0a 43 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a ·Cont
01c0 20 34 31 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 41··
01d0 70 3a 2f 2f 61 6c 74 6f 72 6f 2e 74 65 73 74 66 p://a
01e0 69 72 65 2e 6e 65 74 0d 0a 44 4e 54 3a 20 31 0d ire.n
01f0 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 ·Conn
0200 70 2d 61 6c 69 76 65 0d 0a 43 6f 6f 6b 69 65 3a p-ali
0210 20 4a 53 45 53 53 49 4f 4e 49 44 3d 43 43 37 39 JSES
0220 45 43 33 44 39 41 35 30 34 35 38 32 32 46 39 32 EC3D
0230 46 33 30 33 35 37 44 39 43 30 44 35 0d 0a 55 70 F303
0240 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d 52 grad
0250 65 71 75 65 73 74 73 3a 20 31 0d 0a 50 72 69 6f eque
0260 72 69 74 79 3a 20 75 3d 30 2c 20 69 0d 0a 0d 0a rity
0270 75 69 64 3d 6a 73 6d 69 74 68 26 70 61 73 73 77 uid=
0280 3d 44 65 6d 6f 31 32 33 34 26 62 74 6e 53 75 62 =Demo
0290 6d 69 74 3d 4c 6f 67 69 6e mit=L
Text item (text), 15 byte(s)
Packets: 4684 · Displayed: 4 (0.1%)
Profile: Default

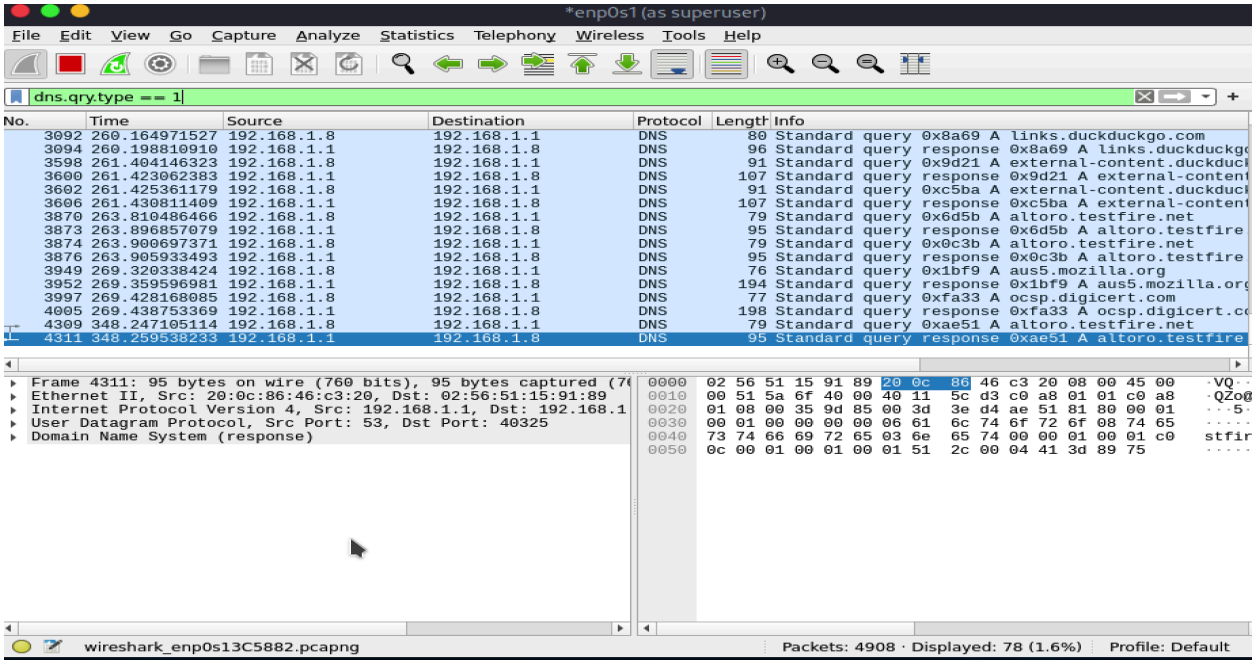


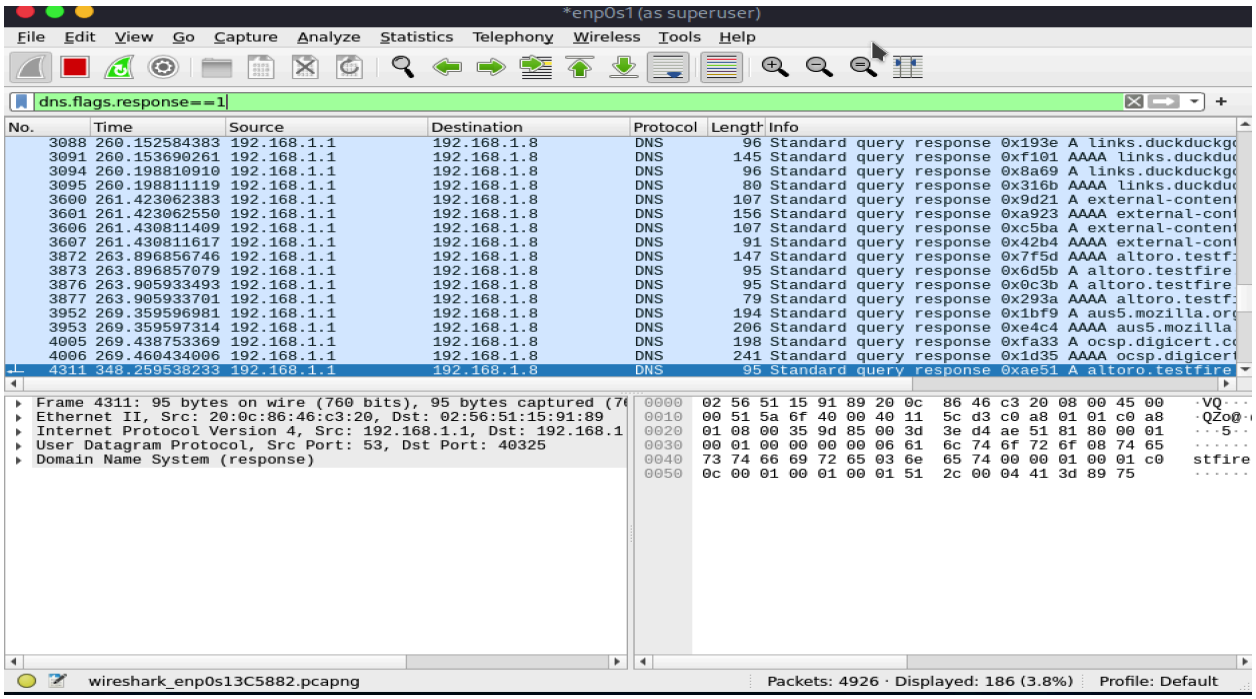
Here we found login credentials used to logged into this banking site.

6. Identify at least 3 different protocols in the capture

✅ Identified and noted 3 key protocols:

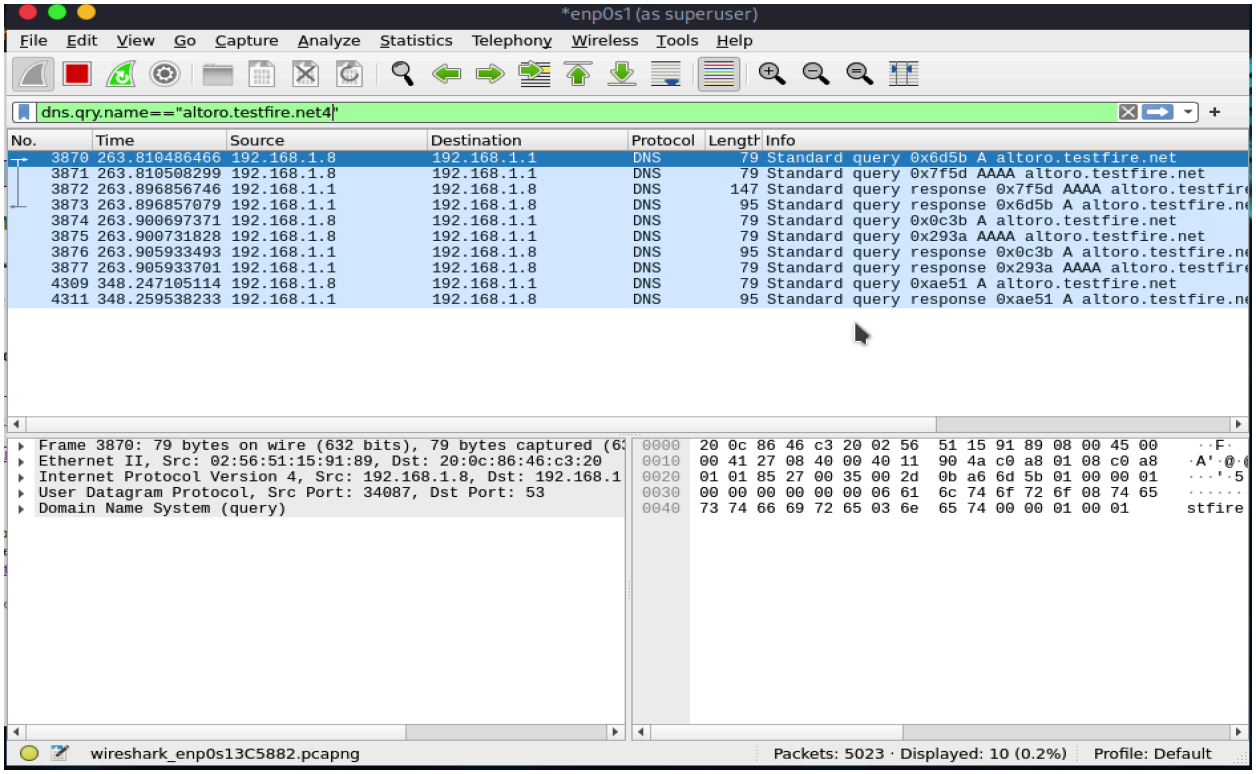
- **HTTP**: Shows web traffic, e.g., GET and POST requests.
- **DNS**: Shows domain resolution queries and responses.
- **TCP**: Shows the underlying transport layer sessions and connections, including SYN, ACK, FIN packets.

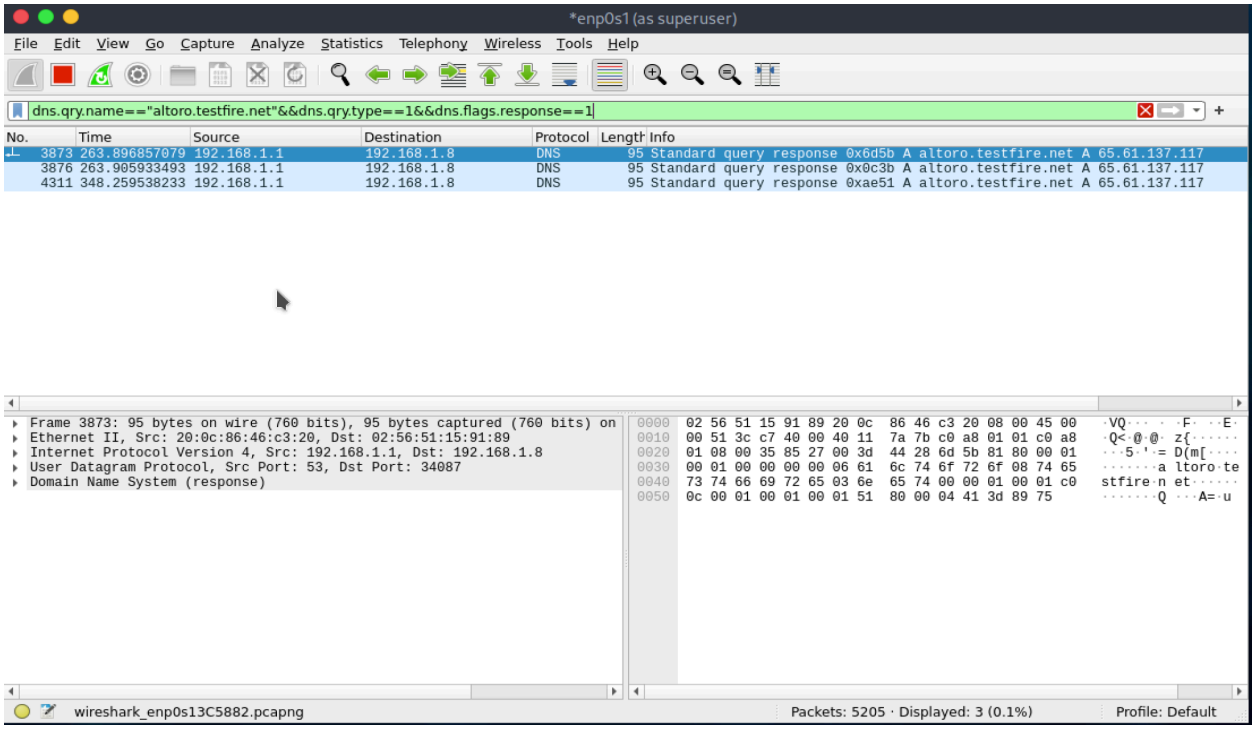


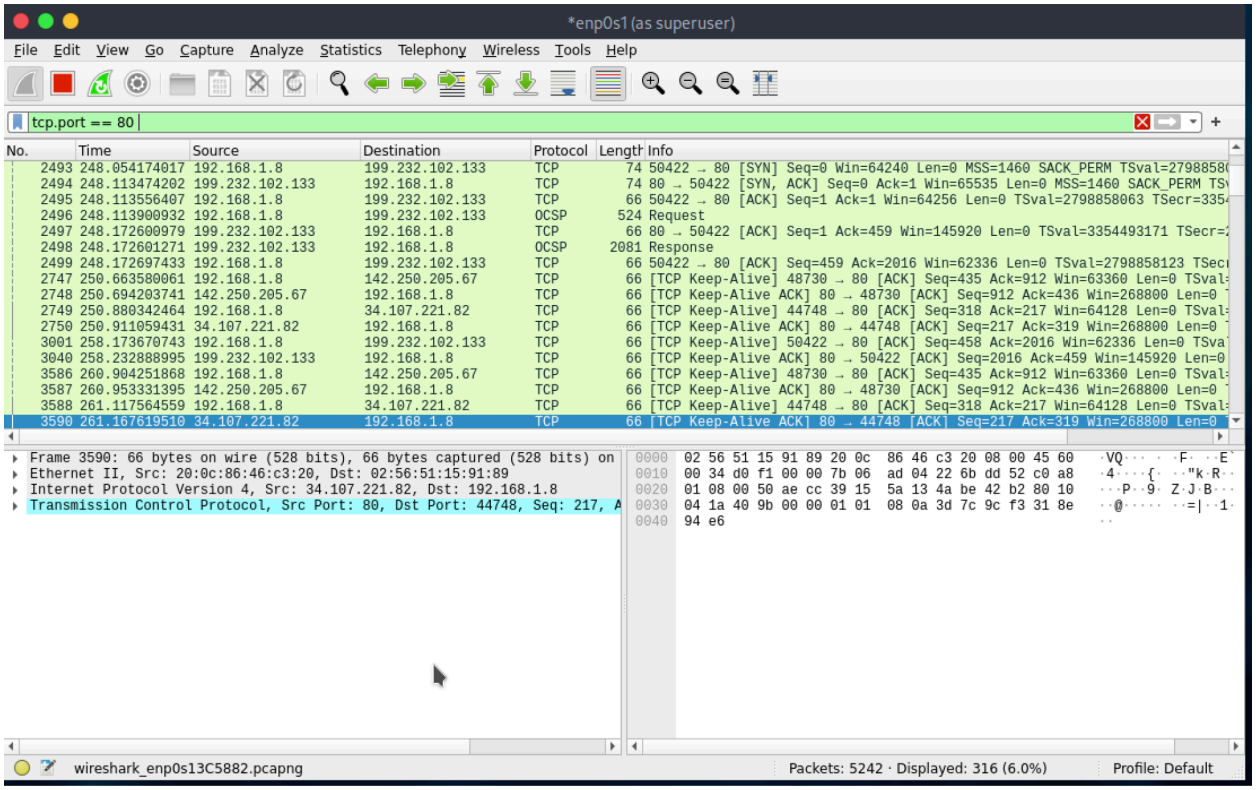


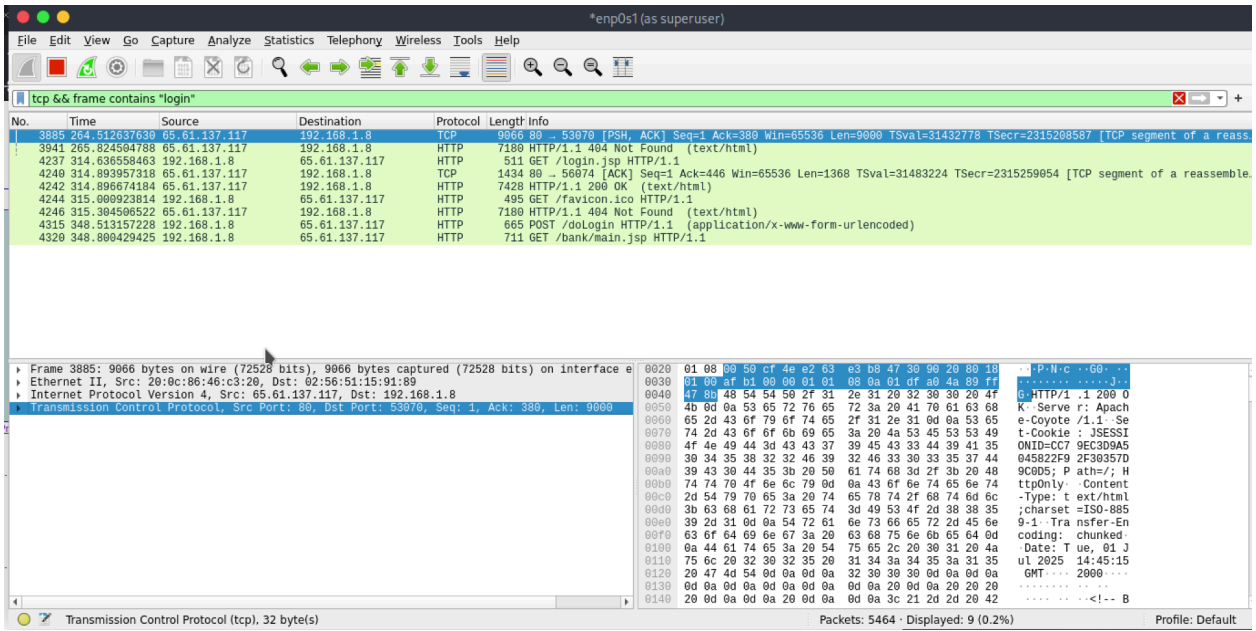
The first image here shows the dns query type for A record.

Second image shows response from server side

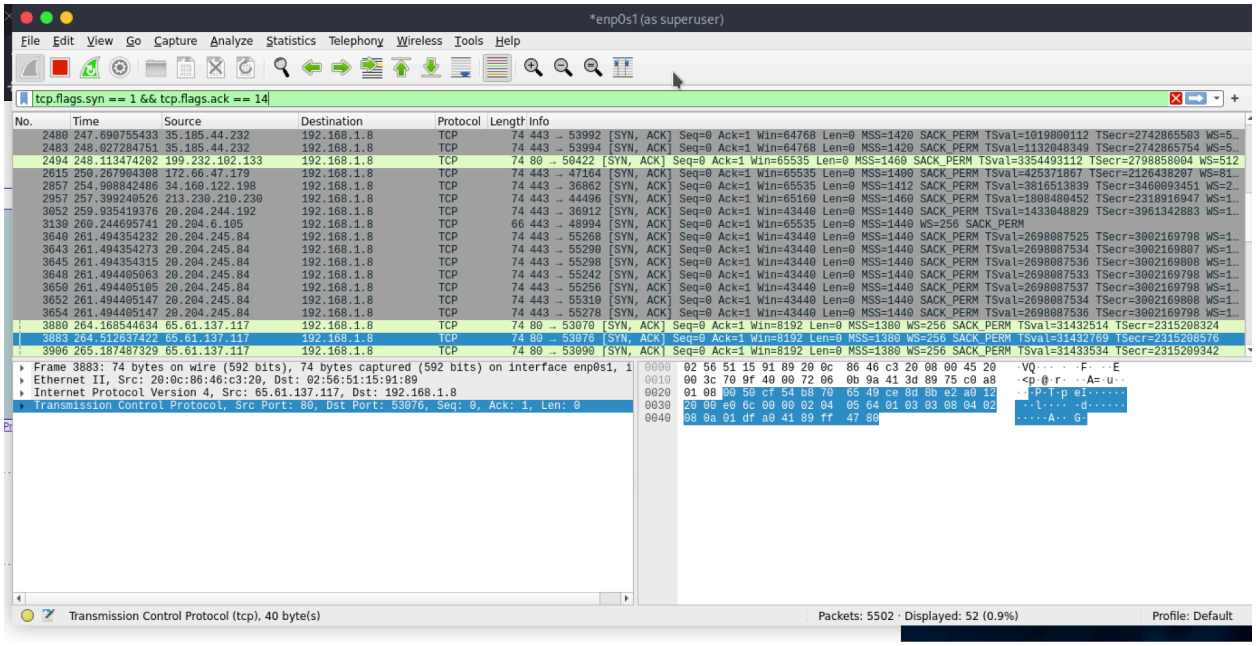

*enp0s1 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name=="altoro.testfire.net4"
No. Time Source Destination Protocol Length Info
3870 263.810486466 192.168.1.8 192.168.1.1 DNS 79 Standard query 0x6d5b A altoro.testfire.net
3871 263.810508299 192.168.1.8 192.168.1.1 DNS 79 Standard query 0x7f5d AAAA altoro.testfire.net
3872 263.896856746 192.168.1.1 192.168.1.8 DNS 147 Standard query response 0x7f5d AAAA altoro.testfire
3873 263.896857079 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0x6d5b A altoro.testfire.ne
3874 263.900697371 192.168.1.8 192.168.1.1 DNS 79 Standard query 0x0c3b A altoro.testfire.net
3875 263.900731828 192.168.1.8 192.168.1.1 DNS 79 Standard query 0x293a AAAA altoro.testfire.net
3876 263.905933493 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0x0c3b A altoro.testfire.ne
3877 263.905933701 192.168.1.1 192.168.1.8 DNS 79 Standard query response 0x293a AAAA altoro.testfire
4309 348.247105114 192.168.1.8 192.168.1.1 DNS 79 Standard query 0xae51 A altoro.testfire.net
4311 348.259538233 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0xae51 A altoro.testfire.ne
Frame 3870: 79 bytes on wire (632 bits), 79 bytes captured (6
Ethernet II, Src: 02:56:51:15:91:89, Dst: 20:0c:86:46:c3:20
Internet Protocol Version 4, Src: 192.168.1.8, Dst: 192.168.1
User Datagram Protocol, Src Port: 34087, Dst Port: 53
Domain Name System (query)
0000 20 0c 86 46 c3 20 02 56 51 15 91 89 08 00 45 00
0010 00 41 27 08 40 00 40 11 90 4a c0 a8 01 08 c0 a8
0020 01 01 85 27 00 35 00 2d 0b a6 6d 5b 01 00 00 01
0030 00 00 00 00 00 00 06 61 6c 74 6f 72 6f 08 74 65
0040 73 74 66 69 72 65 03 6e 65 74 00 00 01 00 01
stfire
wireshark_enp0s13C5882.pcapng
Packets: 5023 · Displayed: 10 (0.2%)
Profile: Default


*enp0s1 (as superuser)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns.qry.name=="altoro.testfire.net"&&dns.qry.type==1&&dns.flags.response==1
No. Time Source Destination Protocol Length Info
3873 263.896857079 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0x6d5b A altoro.testfire.net A 65.61.137.117
3876 263.905933493 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0x0c3b A altoro.testfire.net A 65.61.137.117
4311 348.259538233 192.168.1.1 192.168.1.8 DNS 95 Standard query response 0xae51 A altoro.testfire.net A 65.61.137.117
Frame 3873: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on
Ethernet II, Src: 20:0c:86:46:c3:20, Dst: 02:56:51:15:91:89
Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.8
User Datagram Protocol, Src Port: 53, Dst Port: 34087
Domain Name System (response)
0000 02 56 51 15 91 89 20 0c 86 46 c3 20 08 00 45 00
0010 00 51 3c c7 40 00 40 11 7a 7b c0 a8 01 01 c0 a8
0020 01 08 00 35 85 27 00 3d 44 28 6d 5b 81 80 00 01
0030 00 01 00 00 00 00 06 61 6c 74 6f 72 6f 08 74 65
0040 73 74 66 69 72 65 03 6e 65 74 00 00 01 00 01 c0
0050 0c 00 01 00 01 00 01 51 80 00 04 41 3d 89 75
stfire n et
wireshark_enp0s13C5882.pcapng
Packets: 5205 · Displayed: 3 (0.1%)
Profile: Default





The below image shows tcp syn and ack pack from server side



7. Export the capture as a `.pcap` file

✅ Saved the capture to `test.pcap` using *File → Save As* in Wireshark.

---

8. Summarize your findings and packet details

Protocol	Purpose	Example Packet Info
HTTP	Web browsing	GET request to `www.example.com` with response code 200 OK
DNS	Domain resolution	Query for `example.com` and its IP address in the answer section
TCP	Session control	Noted TCP 3-way handshake (SYN, SYN-ACK, ACK) and data packets

✅ **Key Observations:**

- Verified successful TCP handshakes for browsing activity.
- DNS lookups resolved domains to public IP addresses.
- HTTP requests transfer web page data between client and server.

✅ **Learning:**

- Understood how different protocols interact in a live capture.
- Saw how to trace connections, spot potential suspicious packets, and interpret flow.

📂 **Outcome:**

- `.pcap` file saved: `network_capture_task5.pcap`
- Findings documented for reporting and future reference.