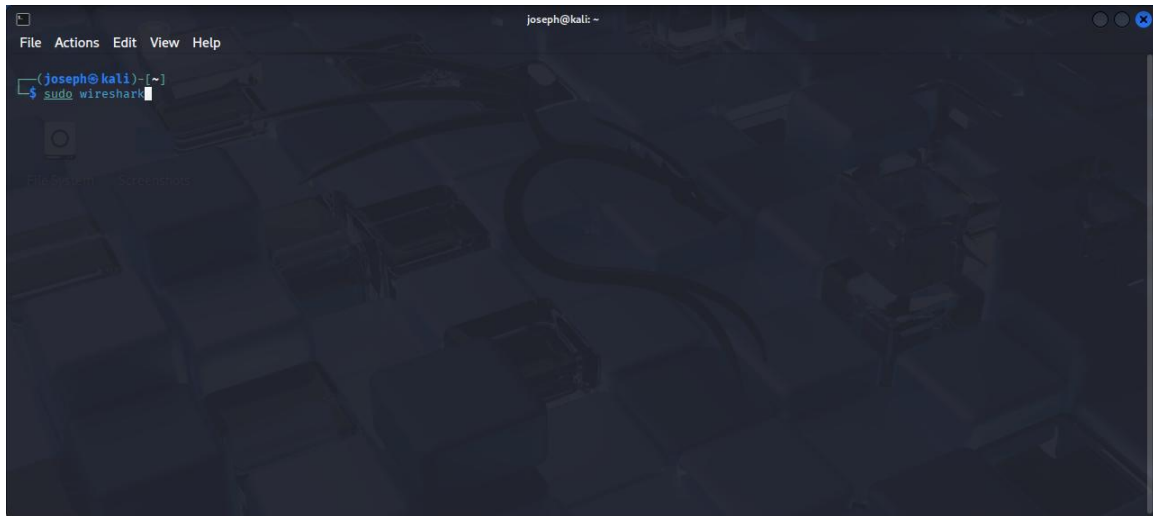


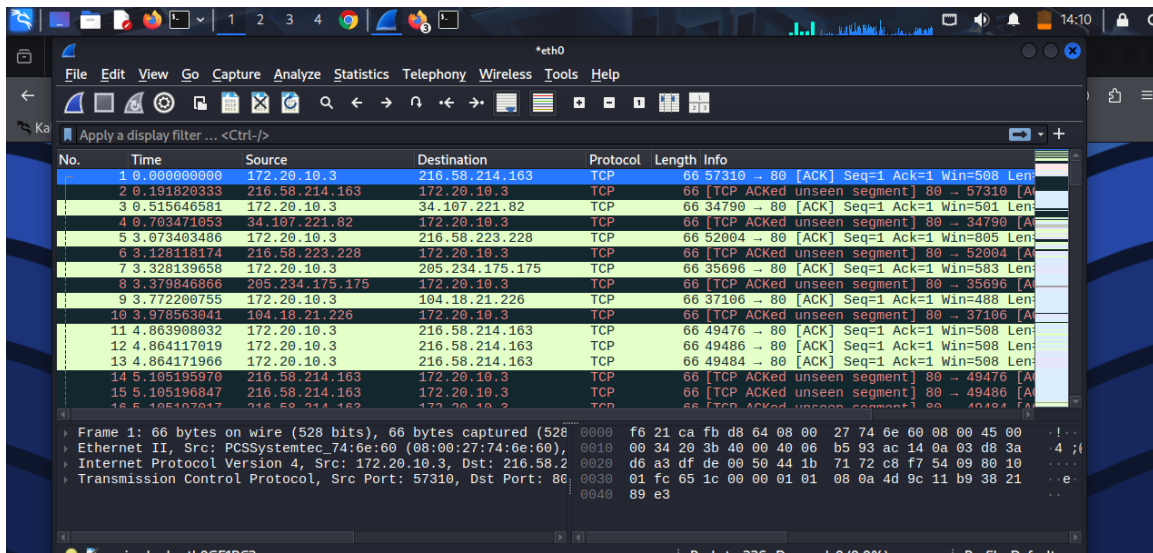
Packet Analysis with Wireshark

Step 1 login as Admin



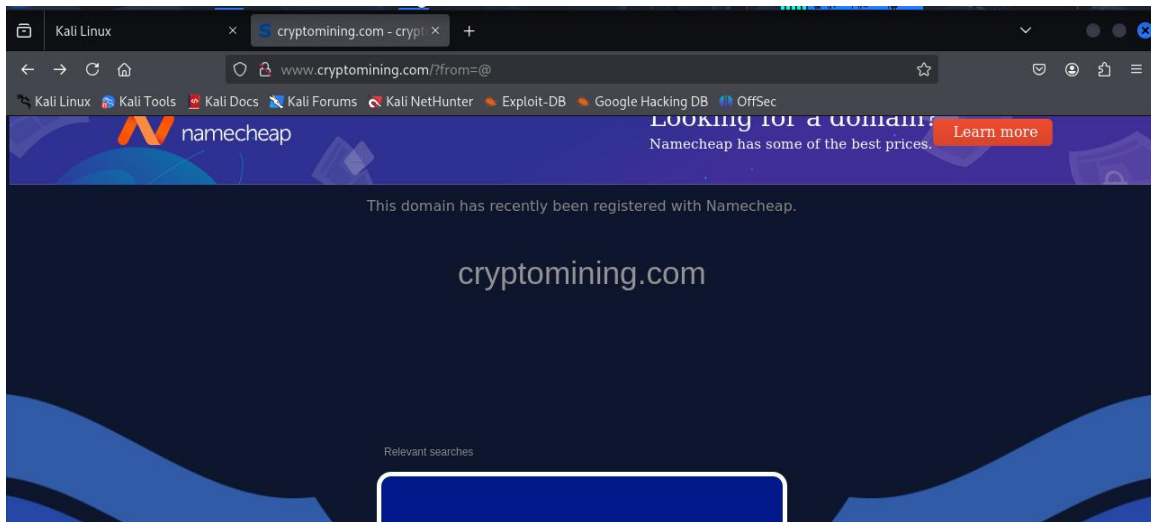
In other to login as root user to get direct access to the network I used Sudo wireshark.

Step 2 Start capturing Packets



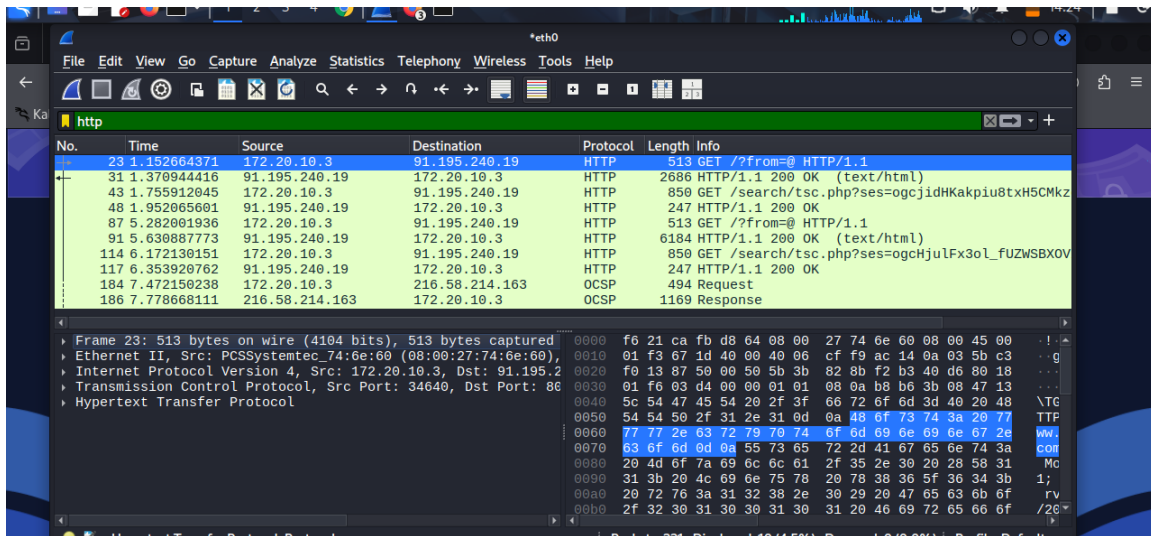
I started capturing packets from my network by clicking on the blue shark fin on the top left of the wireshark GUI interface

Step 3 Load up a website using HTTP unsecure port



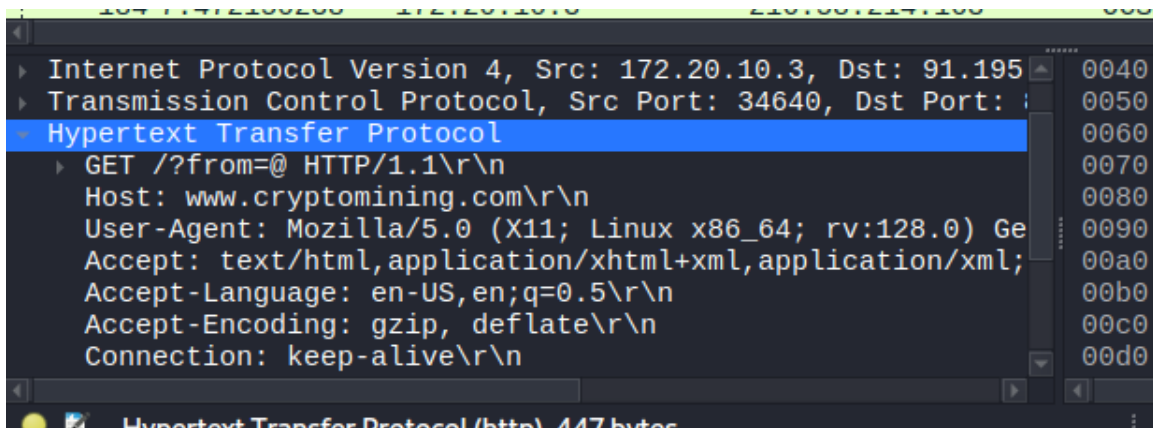
In other to get HTTP traffic from my network I load up a website using unsecure HTTP port 80

Step 4 Analyzing HTTP traffic



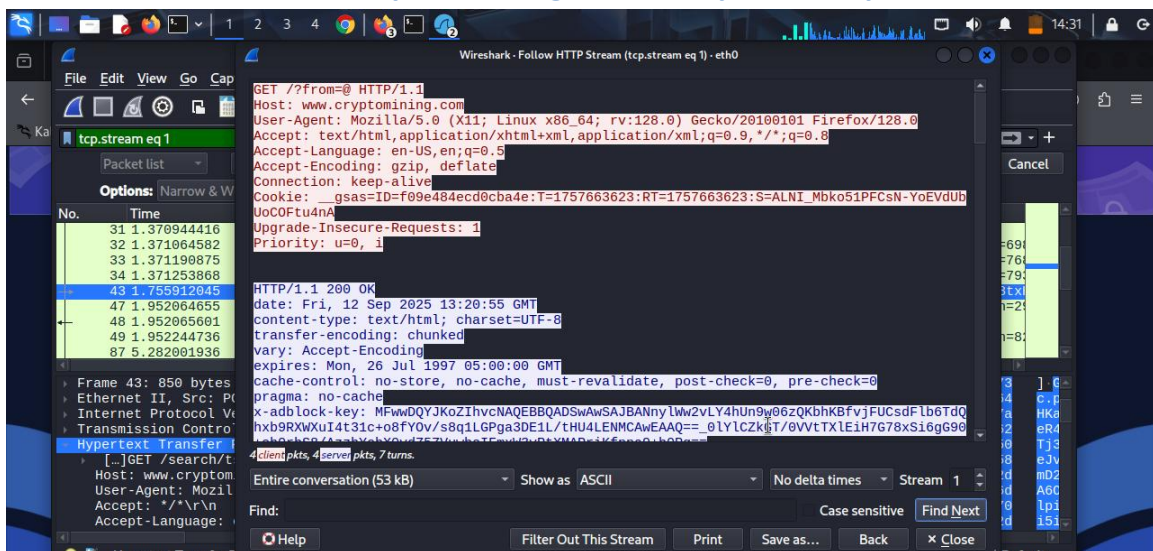
After getting a couple of traffic I streamline the filter by focusing on HTTP traffic alone, and I got a couple of details, seen the communication between my system and the http website I loaded previously.

Step 5 HTTP Request / Response

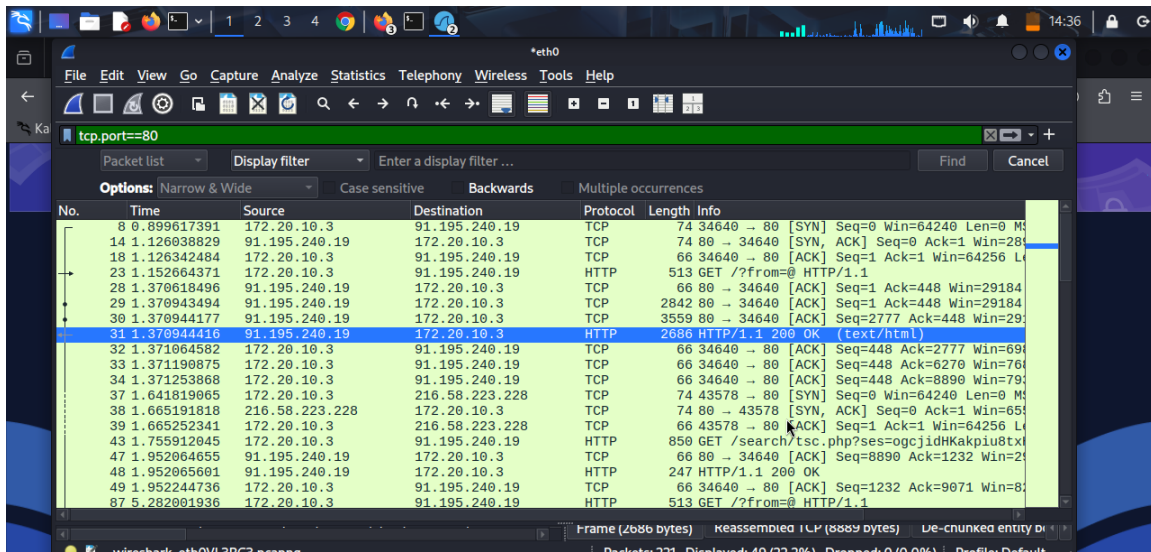


To see more details about the http packet captured I click on one of the packet and click on the hypertext transfer protocol to find some details about the http connection, there I found a couple of details include the host website, the user agent that was used in connecting the http website, the OS that was used in connecting, the language of the web page and other detail.

Step 6 Analyzing the packet to get more details about the website my system connected to via unsecure port 80 I dig down the packet http stream



Step 9 — Final Notes / Wrap-up



The image shows a Wireshark network traffic capture. The filter bar at the top displays 'tcp.port==80'. The packet list table below shows various network packets, with packet 31 selected. The details pane on the right shows the selected packet's structure, including Ethernet II, Internet Protocol Version 4, and Hypertext Transfer Protocol.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.899617391	172.20.10.3	91.195.240.19	TCP	74	34640 → 80 [SYN] Seq=0 Win=64240 Len=0 M
14	1.126038829	91.195.240.19	172.20.10.3	TCP	74	80 → 34640 [SYN, ACK] Seq=0 Ack=1 Win=28
18	1.126342484	172.20.10.3	91.195.240.19	TCP	66	34640 → 80 [ACK] Seq=1 Ack=1 Win=64256 L
23	1.152664371	172.20.10.3	91.195.240.19	HTTP	513	GET /?from=@ HTTP/1.1
28	1.370618496	91.195.240.19	172.20.10.3	TCP	66	80 → 34640 [ACK] Seq=1 Ack=448 Win=29184
29	1.370943494	91.195.240.19	172.20.10.3	TCP	2842	80 → 34640 [ACK] Seq=1 Ack=448 Win=29184
30	1.370944177	91.195.240.19	172.20.10.3	TCP	3559	80 → 34640 [ACK] Seq=2777 Ack=448 Win=29
31	1.370944416	91.195.240.19	172.20.10.3	HTTP	2686	HTTP/1.1 200 OK (text/html)
32	1.371064582	172.20.10.3	91.195.240.19	TCP	66	34640 → 80 [ACK] Seq=448 Ack=2777 Win=69
33	1.371190875	172.20.10.3	91.195.240.19	TCP	66	34640 → 80 [ACK] Seq=448 Ack=6270 Win=76
34	1.371253868	172.20.10.3	91.195.240.19	TCP	66	34640 → 80 [ACK] Seq=448 Ack=8890 Win=79
37	1.641819065	172.20.10.3	216.58.223.228	TCP	74	43578 → 80 [SYN] Seq=0 Win=64240 Len=0 M
38	1.665191818	216.58.223.228	172.20.10.3	TCP	74	80 → 43578 [SYN, ACK] Seq=0 Ack=1 Win=65
39	1.665252341	172.20.10.3	216.58.223.228	TCP	66	43578 → 80 [ACK] Seq=1 Ack=1 Win=64256 L
43	1.755912045	172.20.10.3	91.195.240.19	HTTP	850	GET /search/tsc.php?ses=ogcjidHKakpiu8txl
47	1.952064655	91.195.240.19	172.20.10.3	TCP	66	80 → 34640 [ACK] Seq=8890 Ack=1232 Win=2
48	1.952065601	91.195.240.19	172.20.10.3	HTTP	247	HTTP/1.1 200 OK
49	1.952244736	172.20.10.3	91.195.240.19	TCP	66	34640 → 80 [ACK] Seq=1232 Ack=9071 Win=8
87	5.282001936	172.20.10.3	91.195.240.19	HTTP	513	GET /?from=@ HTTP/1.1

Other details can be gotten from each and every packet that was scanned from your network it all depends on what you are looking to discover or troubleshoot.