

NAME: RESHMA AL

DATE:14.10.25

ROLL NO.:241901089

EXERCISE 16

TO CAPTURE, SAVE AND ANALYZE NETWORK TRAFFIC ON TCP/UDP/IP/HTTP/ARP/DHCP/ICMP/DNS USING WIRESHARK TOOL

AIM:

To capture, save, and analyse network traffic using Wireshark to understand protocol packet structures and develop competency in network analysis, troubleshooting, and security assessment.

ALGORITHM:

1. Launch Wireshark - Open the application and verify the network interfaces available
2. Select Network Interface - Choose active interface (Ethernet/Wi-Fi) and enable promiscuous mode
3. Start Packet Capture - Click the Start button to begin capturing packets
4. Generate Network Traffic - Open browser, ping hosts, browse websites to create TCP/UDP/ICMP/DNS traffic
5. Stop Capture - Click the Stop button after collecting sufficient packets (50-200 packets typical)
6. Apply Protocol Filters - Filter traffic using:
 - tcp for TCP packets
 - udp for UDP packets
 - icmp for ICMP ping traffic
 - dns for DNS queries
 - arp for ARP requests/replies
 - dhcp for DHCP messages
 - http for HTTP traffic
7. Analyze Individual Packets - Select packet, examine headers (Ethernet, IP, TCP/UDP), view payload data
8. Examine Protocol Layers - Review encapsulation from Layer 2 (Ethernet) → Layer 3 (IP) → Layer 4 (TCP/UDP) → Layer 7 (Application)
9. Save Capture File - File → Save As, choose format (pcapng or pcap), save with descriptive filename

10. Generate Statistics - Use Statistics menu to view protocol hierarchy, conversations, and endpoints

11. Document Findings - Record observations about protocol behavior, connections, and traffic patterns

12. Create Analysis Report - Compile results with conclusions about network communication

OUTPUT:

i. CAPTURE THE PACKET

Frame ID	Time	Source IP	Destination IP	Protocol	Details
1 0.000000	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=2 Win=8442 Len=0	
2 0.000015	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=3 Win=8442 Len=1	
3 0.000030	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=4 Win=8442 Len=1	
4 0.000037	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=5 Win=8442 Len=1	
5 0.000141	127.0.0.1	127.0.0.1	TCP	123 51615 + 51652 [PSH, ACK] Seq=1 Ack=1 Win=8374 Len=79	
6 0.000146	127.0.0.1	127.0.0.1	TCP	44 51652 + 51615 [ACK] Seq=1 Ack=99 Win=8356 Len=8	
7 0.035778	127.0.0.1	127.0.0.1	TCP	123 51615 + 51652 [PSH, ACK] Seq=89 Ack=1 Win=8376 Len=79	
8 0.035882	127.0.0.1	127.0.0.1	TCP	44 51692 + 51615 [ACK] Seq=91 Ack=199 Win=8394 Len=8	
9 0.035887	127.0.0.1	127.0.0.1	TCP	128 51615 + 51652 [PSH, ACK] Seq=159 Ack=1 Win=8374 Len=237	
10 0.035890	127.0.0.1	127.0.0.1	TCP	44 51692 + 51615 [ACK] Seq=160 Ack=1 Win=8374 Len=8	
11 0.119626	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1	
12 0.119655	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=4 Win=8442 Len=1	
13 0.158482	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=1	
14 0.158499	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=4 Win=8435 Len=0	
15 0.187275	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1	
16 0.187300	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=4 Ack=4 Win=8433 Len=0	
17 0.187305	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=79	
18 0.187306	127.0.0.1	127.0.0.1	TCP	44 51682 + 51615 [ACK] Seq=1 Ack=4 Win=8442 Len=1	
19 0.217736	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1	
20 0.217735	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=7 Win=8433 Len=0	
21 0.228416	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=7 Ack=2 Win=8442 Len=1	
22 0.228428	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=8 Win=8433 Len=0	
23 0.297823	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=9 Ack=1 Win=8442 Len=1	
24 0.297857	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=9 Win=8433 Len=0	
25 0.297965	127.0.0.1	127.0.0.1	TCP	123 51615 + 51652 [PSH, ACK] Seq=175 Ack=1 Win=8374 Len=79	

ii. CAPTURE THE TCP/UDP PACKETS

Frame ID	Time	Source IP	Destination IP	Protocol	Details
1 0.000000	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1	
2 0.000018	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0	
3 0.102600	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1	
4 0.102627	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0	
5 0.103105	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1	
6 0.103129	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0	
7 0.103679	127.0.0.1	127.0.0.1	TCP	123 51615 + 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Len=79	
8 0.103709	127.0.0.1	127.0.0.1	TCP	44 51652 + 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0	
9 0.145169	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=1	
10 0.145193	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0	
11 0.164356	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1	
12 0.164379	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0	
13 0.165479	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=1	
14 0.165502	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0	
15 0.172615	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1	
16 0.172634	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=8 Win=8351 Len=0	
17 0.176466	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=8 Ack=1 Win=8442 Len=1	
18 0.176479	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=9 Win=8351 Len=0	
19 0.196283	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=9 Ack=1 Win=8442 Len=1	
20 0.196296	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=1 Ack=10 Win=8351 Len=0	
21 0.206330	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=10 Ack=1 Win=8442 Len=1	
22 0.206341	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=11 Ack=1 Win=8351 Len=0	
23 0.206357	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=11 Ack=1 Win=8442 Len=1	
24 0.206362	127.0.0.1	127.0.0.1	TCP	44 51610 + 51611 [ACK] Seq=12 Ack=1 Win=8351 Len=0	
25 0.207050	127.0.0.1	127.0.0.1	TCP	45 51611 + 51610 [PSH, ACK] Seq=12 Ack=1 Win=8442 Len=1	

Time	127.0.0.1	172.16.
0.000000	51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=0	51610
0.000010	51611 ← 51610 [ACK] Seq=1 Ack=2 Win=8351 Len=0	51610
0.102600	51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=0	51610
0.102627	51611 ← 51610 [ACK] Seq=1 Ack=3 Win=8351 Len=0	51610
0.103105	51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=0	51610
0.103129	51611 ← 51610 [ACK] Seq=1 Ack=4 Win=8351 Len=0	51610
0.103679	51652 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Len=0	51615
0.103709	51652 ← 51652 [ACK] Seq=1 Ack=80 Win=8198 Len=0	51615
0.145169	51611 → 51610 [PSH, ACK] Seq=4 Ack=1 Win=8442 Len=0	51610
0.145193	51611 ← 51610 [ACK] Seq=1 Ack=5 Win=8351 Len=0	51610
0.164356	51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=0	51610
0.164379	51611 ← 51610 [ACK] Seq=1 Ack=6 Win=8351 Len=0	51610
0.165479	51611 → 51610 [PSH, ACK] Seq=6 Ack=1 Win=8442 Len=0	51610
0.165502	51611 ← 51610 [ACK] Seq=1 Ack=7 Win=8351 Len=0	51610

iii. CAPTURE ARP PACKET

Time	127.0.0.1	127.0.0.1	HTTP	806 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
http3 22363	127.0.0.1	127.0.0.1	HTTP	812 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
497 5.023044	127.0.0.1	127.0.0.1	HTTP	813 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
508 5.023124	127.0.0.1	127.0.0.1	HTTP	875 HTTP/1.1 200 OK (text/plain)
524 5.023487	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
534 5.023569	127.0.0.1	127.0.0.1	HTTP	115 HTTP/1.1 200 OK (text/plain)
1873 14.015350	127.0.0.1	127.0.0.1	HTTP	806 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
1885 14.015758	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
1902 14.077463	127.0.0.1	127.0.0.1	HTTP	812 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
1914 14.077958	127.0.0.1	127.0.0.1	HTTP	875 HTTP/1.1 200 OK (text/plain)
2127 15.020582	127.0.0.1	127.0.0.1	HTTP	806 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2129 15.020629	127.0.0.1	127.0.0.1	HTTP	812 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2131 15.020664	127.0.0.1	127.0.0.1	HTTP	813 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2149 15.020852	127.0.0.1	127.0.0.1	HTTP	115 HTTP/1.1 200 OK (text/plain)
2157 15.020870	127.0.0.1	127.0.0.1	HTTP	875 HTTP/1.1 200 OK (text/plain)
2175 15.021317	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
2424 17.010262	127.0.0.1	127.0.0.1	HTTP	806 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2429 17.010628	127.0.0.1	127.0.0.1	HTTP	812 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2441 17.010941	127.0.0.1	127.0.0.1	HTTP	875 HTTP/1.1 200 OK (text/plain)
2455 17.011123	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
2887 19.011958	127.0.0.1	127.0.0.1	HTTP	806 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2819 19.013327	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
2826 19.014433	127.0.0.1	127.0.0.1	HTTP	812 GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0a24cac
2840 19.014730	127.0.0.1	127.0.0.1	HTTP	875 HTTP/1.1 200 OK (text/plain)
Time	127.0.0.1	127.0.0.1	HTTP	10922 HTTP/1.1 200 OK (text/plain)
5.022363	63656	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
5.022623	63657	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
5.023044	63658	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
5.023124	63657	HTTP/1.1 200 OK (text/plain)		19575
5.023487	63656	HTTP/1.1 200 OK (text/plain)		19575
5.023569	63658	HTTP/1.1 200 OK (text/plain)		19575
14.015350	63715	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
14.015758	63715	HTTP/1.1 200 OK (text/plain)		19575
14.077463	63724	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
14.077958	63724	HTTP/1.1 200 OK (text/plain)		19575
15.020582	63759	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
15.020629	63761	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
15.020664	63762	GET /gui/?token=14df19bf3af3d353611ea5e616c5cca0		19575
15.020852	63762	HTTP/1.1 200 OK (text/plain)		19575
15.020870	63761	HTTP/1.1 200 OK (text/plain)		19575

iv. CAPTURE IP/ICMP PACKETS

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1
2	0.000010	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0
3	0.102600	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1
4	0.102627	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=3 Win=8351 Len=0
5	0.103105	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=3 Ack=1 Win=8442 Len=1
6	0.103129	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=4 Win=8351 Len=0
7	0.103679	127.0.0.1	127.0.0.1	TCP	123	51615 → 51652 [PSH, ACK] Seq=1 Ack=1 Win=8356 Len=79
8	0.103709	127.0.0.1	127.0.0.1	TCP	44	51652 → 51615 [ACK] Seq=1 Ack=80 Win=8198 Len=0
9	0.145169	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=0 Ack=1 Win=8442 Len=1
10	0.145193	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=5 Win=8351 Len=0
11	0.164356	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=5 Ack=1 Win=8442 Len=1
12	0.164379	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=6 Win=8351 Len=0
13	0.165479	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=0 Ack=1 Win=8442 Len=1
14	0.165502	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=7 Win=8351 Len=0
15	0.172615	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=7 Ack=1 Win=8442 Len=1
16	0.172634	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=8 Win=8351 Len=0
17	0.176466	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=0 Ack=1 Win=8442 Len=1
18	0.176479	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=9 Win=8351 Len=0
19	0.196283	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=9 Ack=1 Win=8442 Len=1
20	0.196296	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=10 Win=8351 Len=0
21	0.206330	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=10 Ack=1 Win=8442 Len=1
22	0.206341	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=11 Win=8351 Len=0
23	0.206357	127.0.0.1	127.0.0.1	TCP	45	51611 → 51610 [PSH, ACK] Seq=11 Ack=1 Win=8442 Len=1
24	0.206362	127.0.0.1	127.0.0.1	TCP	44	51610 → 51611 [ACK] Seq=1 Ack=12 Win=8351 Len=0

RESULT:

Wireshark captures and displays packets for all major protocols, enabling analysis of handshake sequences, address mappings, and network statistics across TCP, UDP, ICMP, ARP, DHCP, DNS, and HTTP.