NAME: SIVARANJANII.M

DATE:14.10.25 ROLL NO.:241901109

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.

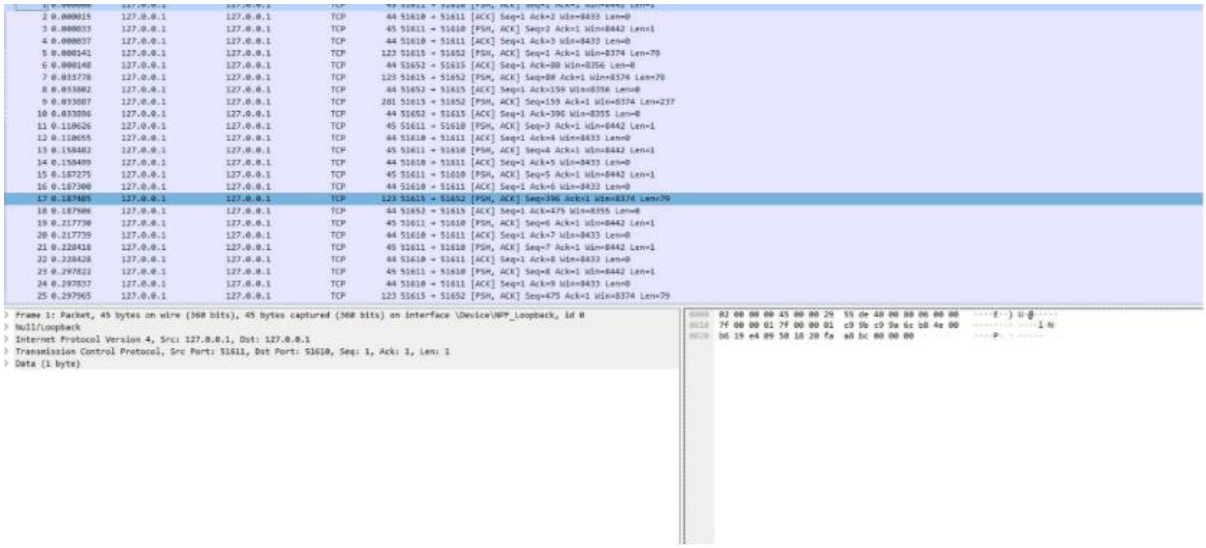
ALGORITHM:

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

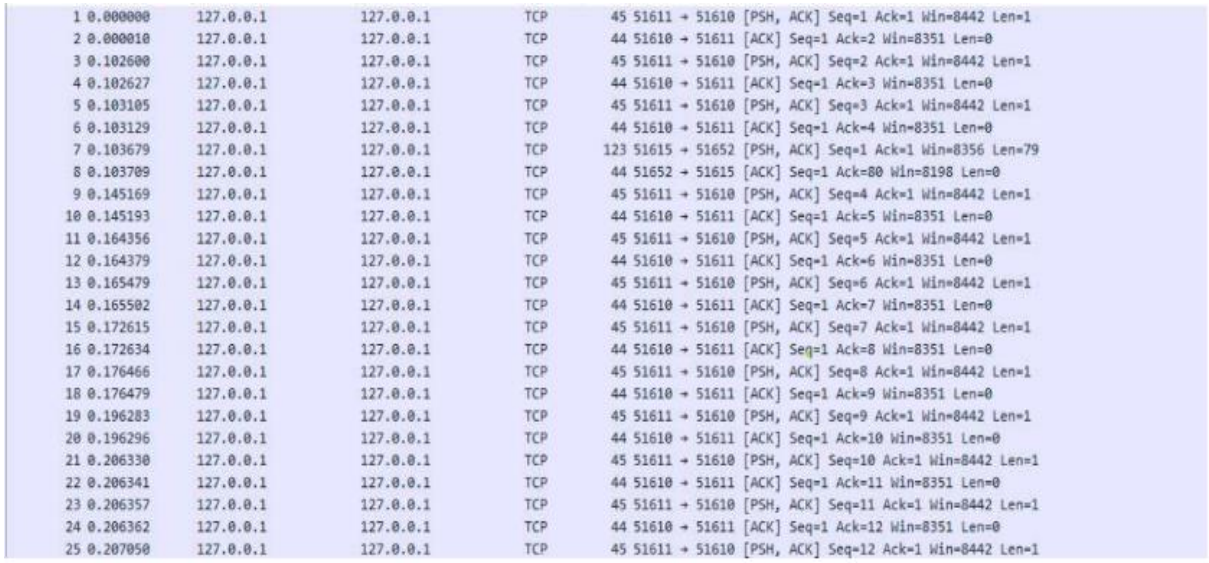
10. Generate Statistics - Use Statistics menu to view protocol hierarchy, conversations, and endpoints
11. Document Findings - Record observations about protocol behavior, connections, and traffic patterns
12. Create Analysis Report - Compile results with conclusions about network communication

OUTPUT:

i. CAPTURE THE PACKET

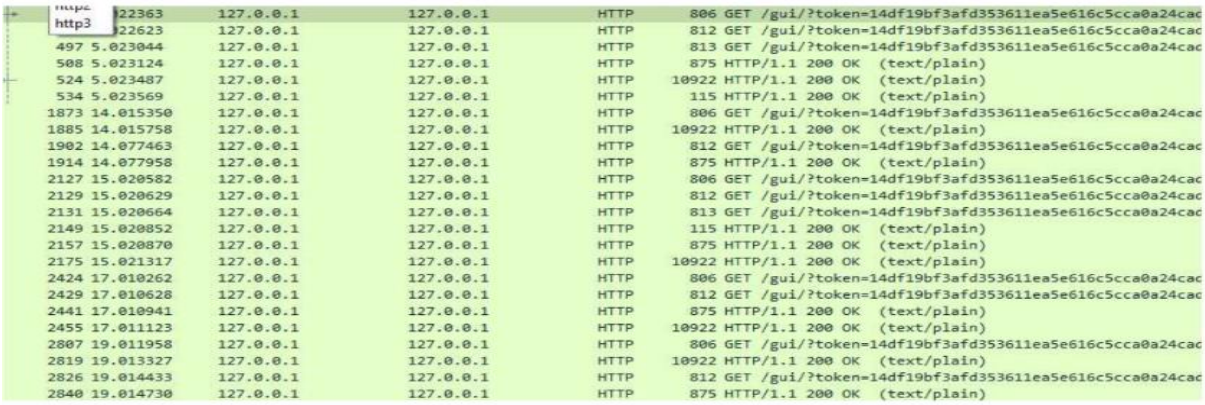


ii. CAPTURE THE TCP/UDP PACKETS

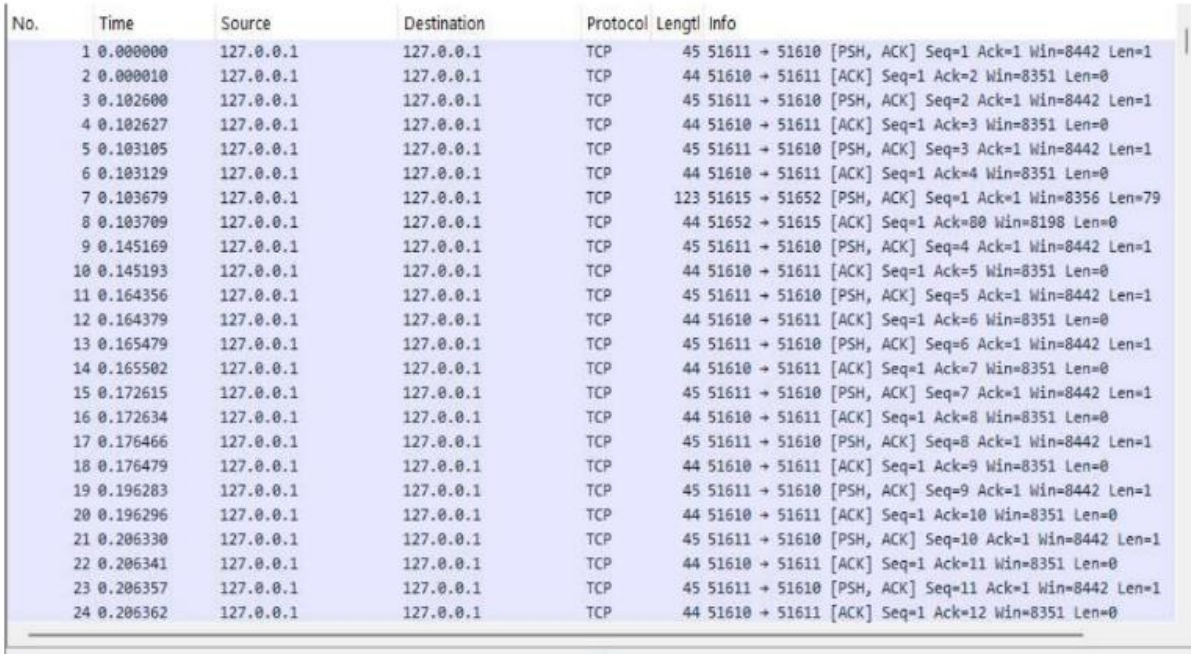


1	0.000000	127.0.0.1	127.0.0.1	TCP	45 51611 → 51610 [PSH, ACK] Seq=1 Ack=1 Win=8442 Len=1
2	0.000010	127.0.0.1	127.0.0.1	TCP	44 51610 → 51611 [ACK] Seq=1 Ack=2 Win=8351 Len=0
3	0.102600	127.0.0.1	127.0.0.1	TCP	45 51611 → 51610 [PSH, ACK] Seq=2 Ack=1 Win=8442 Len=1
4	0.102627	127.0.0.1	127.0.0.1	TCP	44 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=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=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
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

iii. CAPTURE ARP PACKET



iv. CAPTURE IP/ICMP PACKETS



No.	Time	Source	Destination	Protocol	Lengtl	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=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=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.