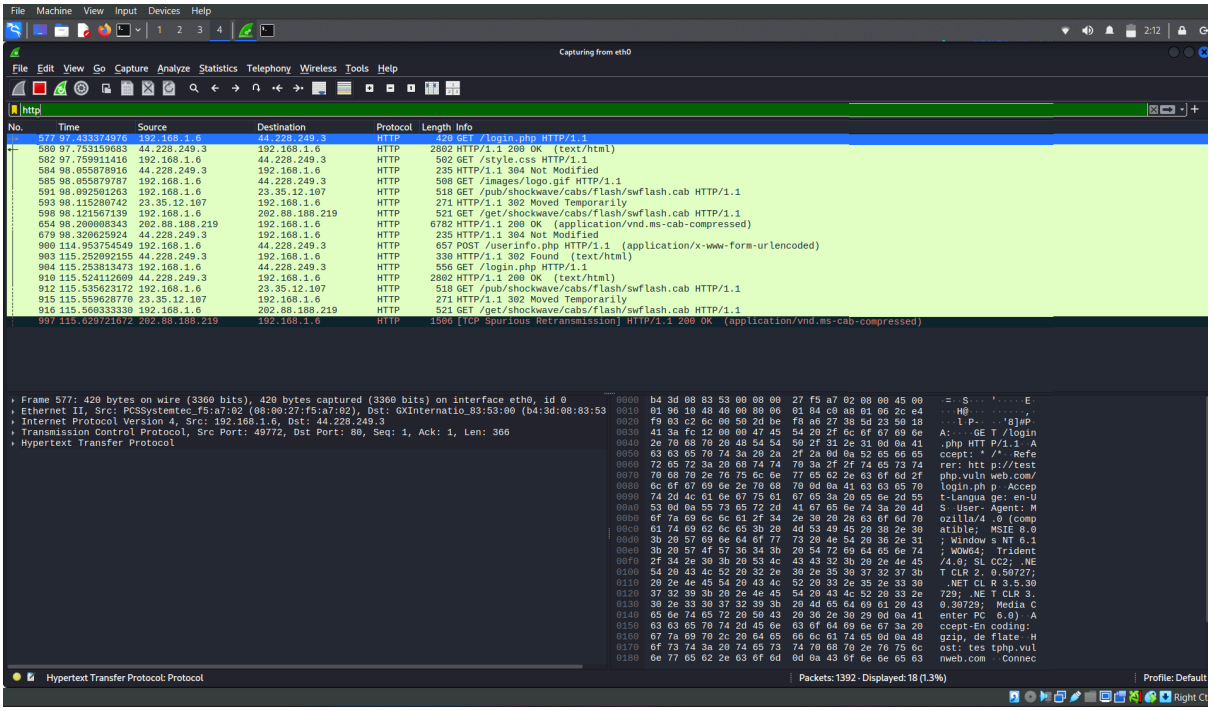
ELEVATES LABS

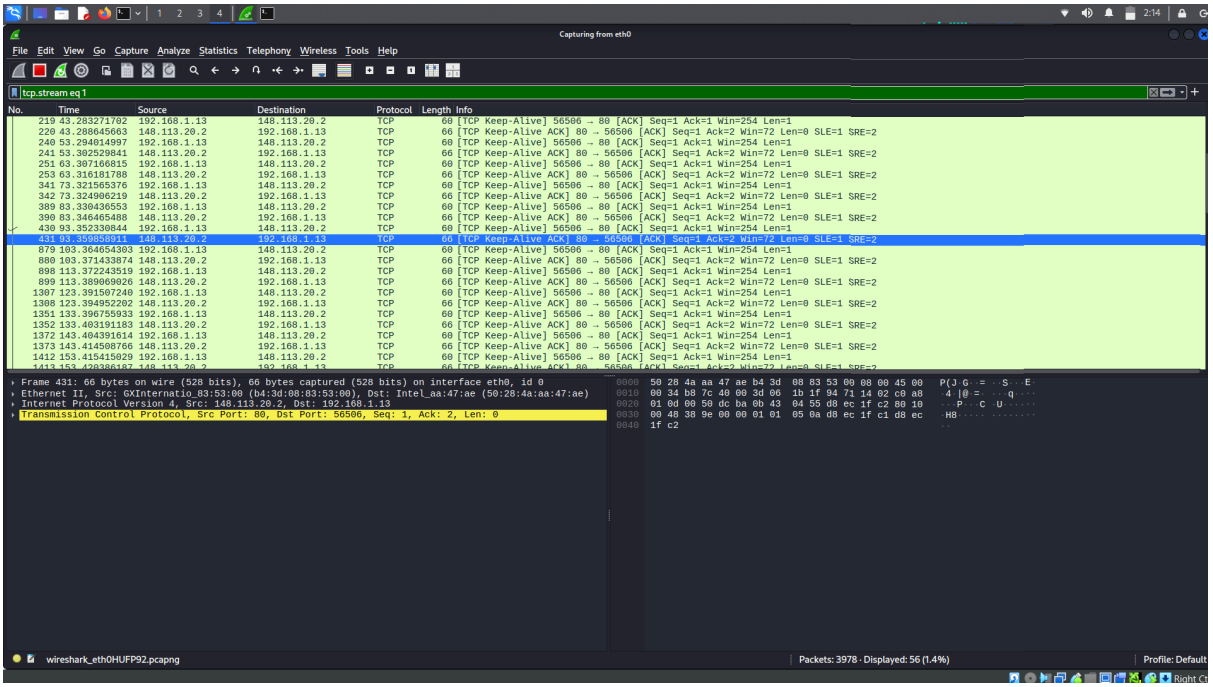
TASK-5

Capture and Analyze Network Traffic Using Wireshark.
Objective: Capture live network packets and identify basic protocols and traffic types.
Tools: Wireshark (free).
Deliverables: A packet capture (.pcap) file and a short report of protocols identified.

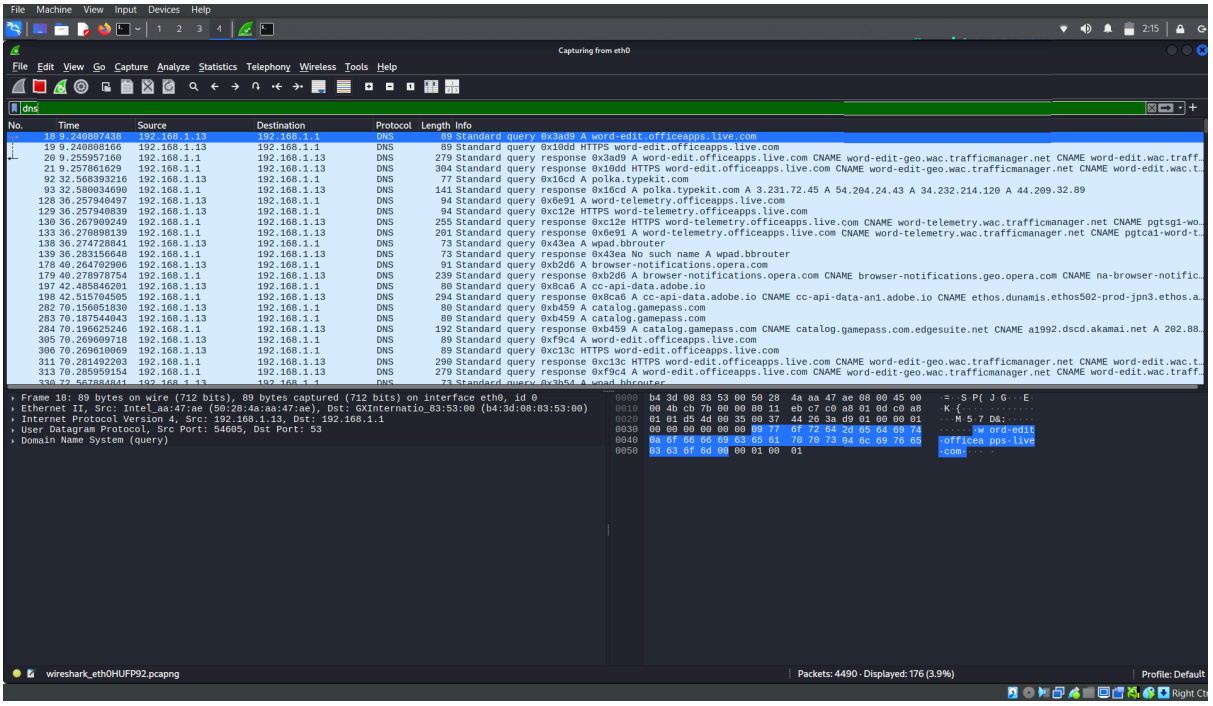
Http


Capturing from eth0
http
No. Time Source Destination Protocol Length Info
577 97.433374976 192.168.1.6 44.228.249.3 HTTP 420 GET /login.php HTTP/1.1
580 97.753159683 44.228.249.3 192.168.1.6 HTTP 2802 HTTP/1.1 200 OK (text/html)
582 97.759911416 192.168.1.6 44.228.249.3 HTTP 502 GET /style.css HTTP/1.1
584 98.055878916 44.228.249.3 192.168.1.6 HTTP 235 HTTP/1.1 304 Not Modified
585 98.055879787 192.168.1.6 44.228.249.3 HTTP 508 GET /images/logo.gif HTTP/1.1
591 98.092501263 192.168.1.6 23.35.12.107 HTTP 518 GET /pub/shockwave/cabs/flash/swflash.cab HTTP/1.1
593 98.115280742 23.35.12.107 192.168.1.6 HTTP 271 HTTP/1.1 302 Moved Temporarily
598 98.121567139 192.168.1.6 202.88.188.219 HTTP 521 GET /get/shockwave/cabs/flash/swflash.cab HTTP/1.1
654 98.200008343 202.88.188.219 192.168.1.6 HTTP 6782 HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
679 98.320625924 44.228.249.3 192.168.1.6 HTTP 235 HTTP/1.1 304 Not Modified
900 114.953754549 192.168.1.6 44.228.249.3 HTTP 657 POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
903 115.252092155 44.228.249.3 192.168.1.6 HTTP 330 HTTP/1.1 302 Found (text/html)
904 115.253813473 192.168.1.6 44.228.249.3 HTTP 556 GET /login.php HTTP/1.1
910 115.524112609 44.228.249.3 192.168.1.6 HTTP 2802 HTTP/1.1 200 OK (text/html)
912 115.535623172 192.168.1.6 23.35.12.107 HTTP 518 GET /pub/shockwave/cabs/flash/swflash.cab HTTP/1.1
915 115.559628770 23.35.12.107 192.168.1.6 HTTP 271 HTTP/1.1 302 Moved Temporarily
916 115.560333330 192.168.1.6 202.88.188.219 HTTP 521 GET /get/shockwave/cabs/flash/swflash.cab HTTP/1.1
997 115.629721672 202.88.188.219 192.168.1.6 HTTP 1506 [TCP Spurious Retransmission] HTTP/1.1 200 OK (application/vnd.ms-cab-compressed)
Frame 577: 420 bytes on wire (3360 bits), 420 bytes captured (3360 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_f5:a7:02 (08:00:27:f5:a7:02), Dst: GXInternatio_83:53:00 (b4:3d:08:83:53
Internet Protocol Version 4, Src: 192.168.1.6, Dst: 44.228.249.3
Transmission Control Protocol, Src Port: 49772, Dst Port: 80, Seq: 1, Ack: 1, Len: 366
Hypertext Transfer Protocol
Hypertext Transfer Protocol: Protocol
Packets: 1392 · Displayed: 18 (1.3%)
Profile: Default

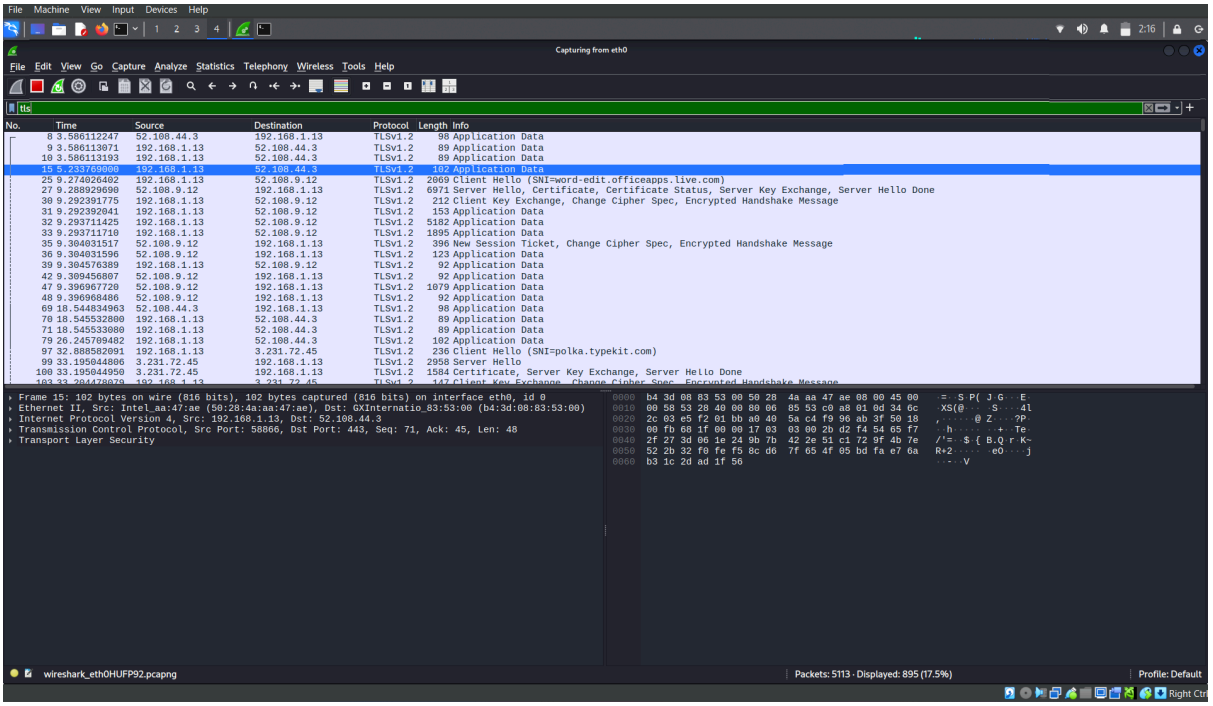
Tcp


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
No. Time Source Destination Protocol Length Info
219 43.283271702 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
220 43.288645663 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
240 53.294014997 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
241 53.302529841 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
251 63.307166815 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
253 63.316181788 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
341 73.321565376 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
342 73.324906219 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
389 83.330436553 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
390 83.346465488 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
430 93.352330844 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
431 93.360098811 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
879 103.364654303 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
880 103.371433874 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
898 113.372243519 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
899 113.389069026 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
1307 123.391507240 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
1308 123.394952202 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
1351 133.396755933 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
1352 133.403191183 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
1372 143.404391614 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
1373 143.414508766 148.113.20.2 192.168.1.13 TCP 66 [TCP Keep-Alive ACK] 80 → 56506 [ACK] Seq=1 Ack=2 Win=72 Len=0 SLE=1 SRE=2
1412 153.415415029 192.168.1.13 148.113.20.2 TCP 60 [TCP Keep-Alive] 56506 → 80 [ACK] Seq=1 Ack=1 Win=254 Len=1
Frame 431: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth0, id 0
Ethernet II, Src: GXInternatio_83:53:00 (b4:3d:08:83:53:00), Dst: Intel_aa:47:ae (50:28:4a:aa:47:ae)
Internet Protocol Version 4, Src: 148.113.20.2, Dst: 192.168.1.13
Transmission Control Protocol, Src Port: 80, Dst Port: 56506, Seq: 1, Ack: 2, Len: 0
0000 50 28 4a aa 47 ae b4 3d 08 83 53 00 08 00 45 00
0010 00 34 b8 7c 40 00 3d 06 1b 1f 94 71 14 02 c0 a8
0020 01 0d 00 50 dc ba 0b 43 04 55 d8 ec 1f c2 80 10
0030 00 48 38 9e 00 00 01 01 05 0a d8 ec 1f c1 d8 ec
0040 1f c2
wireshark_eth0HUFP92.pcapng
Packets: 3978 · Displayed: 56 (1.4%)
Profile: Default

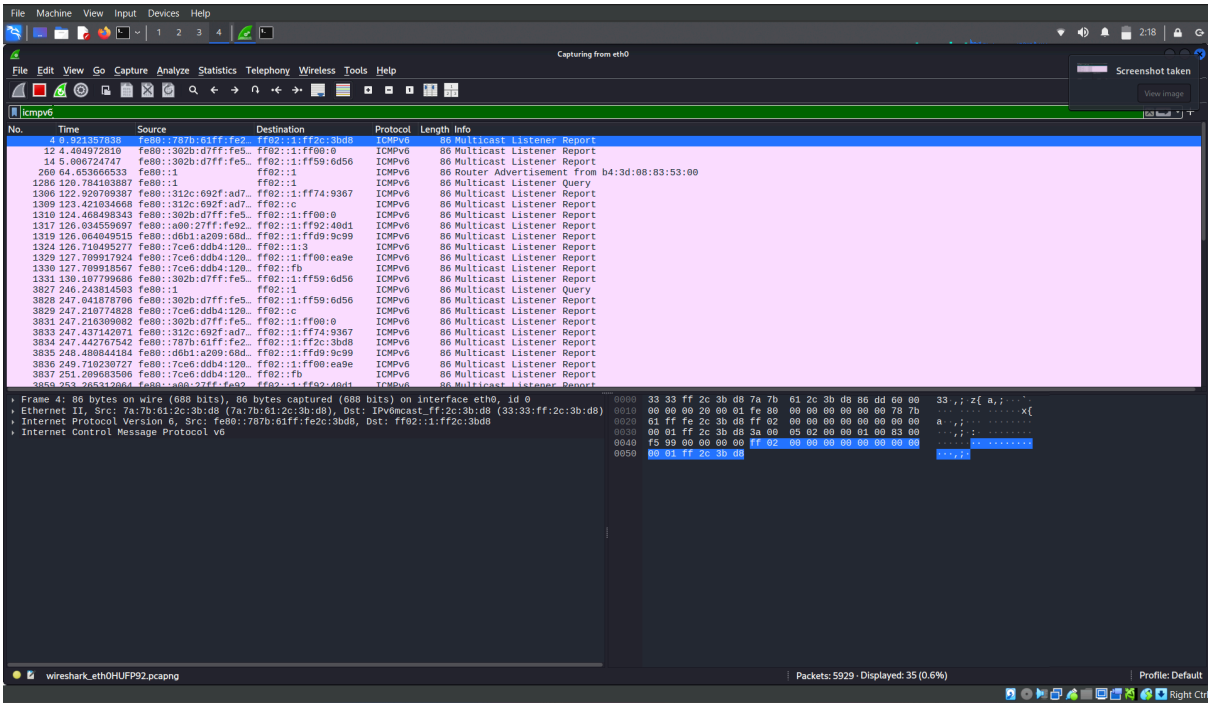
DNS


Capturing from eth0
dns
wireshark_eth0HUFP92.pcapng
Packets: 4490 · Displayed: 176 (3.9%)
Profile: Default

Tls


Capturing from eth0
tls
wireshark_eth0HUFP92.pcapng
Packets: 5113 · Displayed: 895 (17.5%)
Profile: Default

Icmp



Protocols Identified – Short Report

After analyzing the `.pcap` file in Wireshark, you might observe several common protocols:

- **ARP** is used to map IP addresses to MAC addresses within a local network.
- **DNS** handles domain name resolution, converting human-readable URLs into IP addresses.
- **HTTP** represents unencrypted web traffic, typically on port 80.
- **HTTPS** is the encrypted version of HTTP, using TLS for secure communication, usually on port 443.

- **TCP** is a connection-oriented protocol used for reliable data transfer, common in web and email traffic.
- **UDP** is a connectionless protocol used for lightweight communication, often seen in DNS and streaming.
- **ICMP** is used for diagnostic purposes, such as ping and traceroute.
- **TLS** provides encryption for secure sessions, often seen during HTTPS handshakes.

You might also notice patterns like frequent DNS queries, TLS handshakes indicating secure sessions, and ARP traffic typical of LAN environments