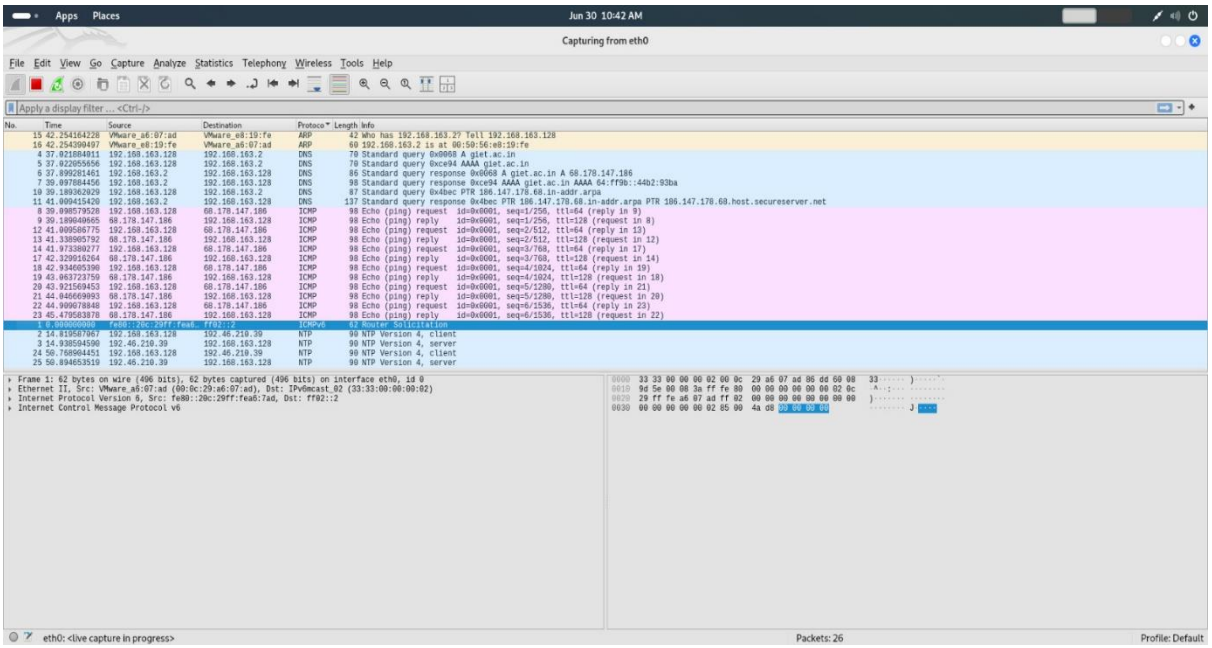
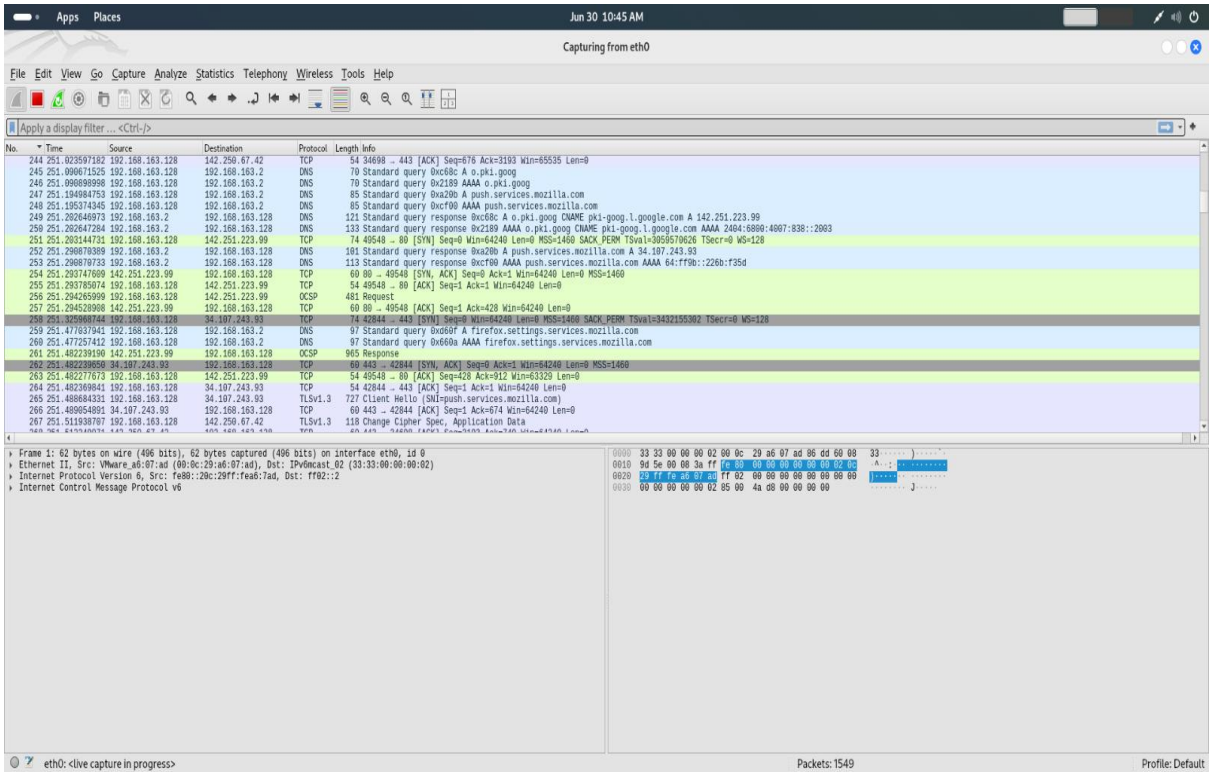
Task 5 : Capture and Analyze Network Traffic Using Wireshark.

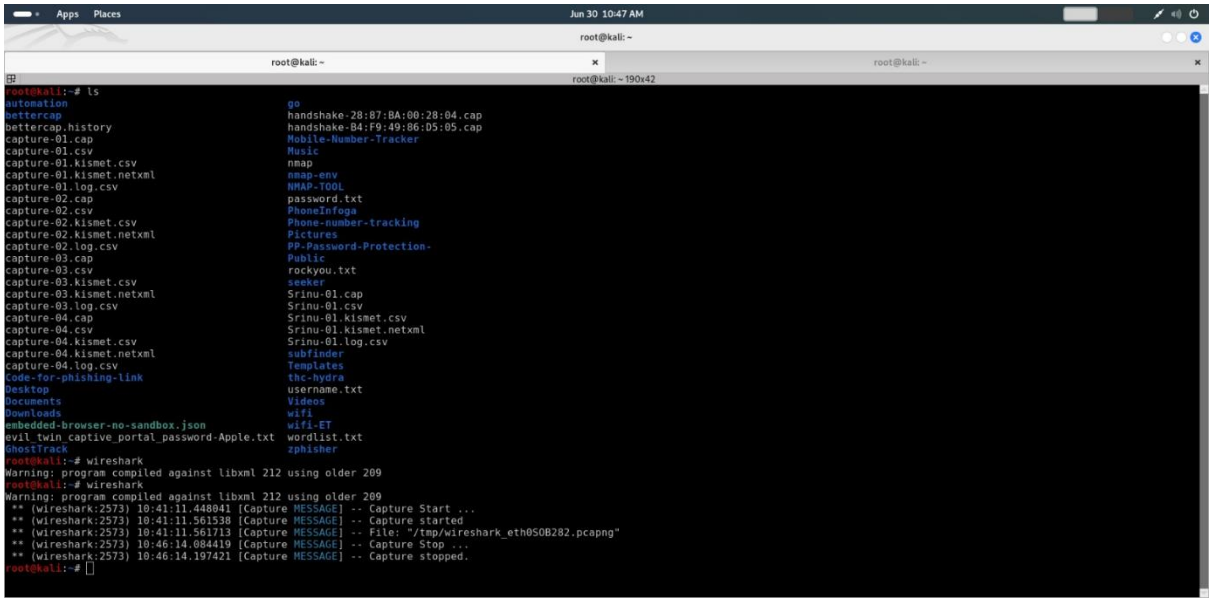
Objective: Capture live network packets and identify basic protocols and traffic types.

Steps Performed

1. **Wireshark Installation:**
    - Wireshark was downloaded from https://www.wireshark.org/ and installed on the system.
2. **Interface Selection:**
    - The active network interface (e.g., Wi-Fi) was selected for live packet capture.
3. **Traffic Generation:**
    - During the capture, several actions were taken to generate diverse traffic:
        - Visited a few websites via a browser.
        - Used the ping command to reach google.com.
        - Checked basic DNS resolution using nslookup.
4. **Capture Duration:**
    - Traffic was captured for approximately **1 minute** and then stopped to ensure a manageable number of packets.
5. **Protocol Filtering:**
    - Wireshark's filter bar was used to isolate specific protocol types:
        - http for web traffic
        - dns for domain name lookups
        - tcp for general transmission control traffic
6. **Exporting Capture:**
    - The entire packet capture was exported as a .pcap file for further review and submission.


Apps Places
Jun 30 10:42 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protoco Length Info
15 42.254164228 VMware_a6:07:ad VMware_e8:19:fe ARP 42 Who has 192.168.163.27 Tell 192.168.163.128
16 42.254399497 VMware_e8:19:fe VMware_a6:07:ad ARP 60 192.168.163.2 is at 00:50:56:e8:19:fe
4 37.921884911 192.168.163.128 192.168.163.2 DNS 70 Standard query 0x0068 A giet.ac.in
5 37.922055656 192.168.163.128 192.168.163.2 DNS 70 Standard query 0xce94 AAAA giet.ac.in
6 37.899281461 192.168.163.2 192.168.163.128 DNS 86 Standard query response 0x0068 A giet.ac.in A 68.178.147.186
7 39.097884456 192.168.163.2 192.168.163.128 DNS 98 Standard query response 0xce94 AAAA giet.ac.in AAAA 64:ff9b::44b2:93ba
10 39.189362029 192.168.163.128 192.168.163.2 DNS 87 Standard query 0x4bec PTR 186.147.178.68.in-addr.arpa
11 41.009415420 192.168.163.2 192.168.163.128 DNS 137 Standard query response 0x4bec PTR 186.147.178.68.in-addr.arpa PTR 186.147.178.68.host.secureserver.net
8 39.098579528 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=1/256, ttl=64 (reply in 9)
9 39.189040665 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 8)
12 41.009586775 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=2/512, ttl=64 (reply in 13)
13 41.338905792 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in 12)
14 41.973380277 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=3/768, ttl=64 (reply in 17)
17 42.329016264 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in 14)
18 42.934605390 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=4/1024, ttl=64 (reply in 19)
19 43.063723759 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request in 18)
20 43.921569453 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 21)
21 44.046609993 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=5/1280, ttl=128 (request in 20)
22 44.909078848 192.168.163.128 68.178.147.186 ICMP 98 Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 23)
23 45.479583878 68.178.147.186 192.168.163.128 ICMP 98 Echo (ping) reply id=0x0001, seq=6/1536, ttl=128 (request in 22)
1 0.000000000 fe80::20c:29ff:fea6.. ff02::2 ICMPv6 62 Router Solicitation
2 14.819507067 192.168.163.128 192.46.210.39 NTP 90 NTP Version 4, client
3 14.938594590 192.46.210.39 192.168.163.128 NTP 90 NTP Version 4, server
24 50.768904451 192.168.163.128 192.46.210.39 NTP 90 NTP Version 4, client
25 50.894653519 192.46.210.39 192.168.163.128 NTP 90 NTP Version 4, server
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
Ethernet II, Src: VMware_a6:07:ad (00:0c:29:a6:07:ad), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::20c:29ff:fea6:7ad, Dst: ff02::2
Internet Control Message Protocol v6
0000 33 33 00 00 00 02 00 0c 29 a6 07 ad 86 dd 60 08 33
0010 9d 5e 00 08 3a ff fe 80 00 00 00 00 00 00 02 0c
0020 29 ff fe a6 07 ad ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 02 85 00 4a d8 00 00 00 00
eth0: <live capture in progress>
Packets: 26
Profile: Default


Apps Places
Jun 30 10:45 AM
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
244 251.023597182 192.168.163.128 142.250.67.42 TCP 54 34698 → 443 [ACK] Seq=676 Ack=3193 Win=65535 Len=0
245 251.090671525 192.168.163.128 192.168.163.2 DNS 70 Standard query 0xc68c A o.pki.goog
246 251.090898998 192.168.163.128 192.168.163.2 DNS 70 Standard query 0x2189 AAAA o.pki.goog
247 251.194984753 192.168.163.128 192.168.163.2 DNS 85 Standard query 0xa20b A push.services.mozilla.com
248 251.195374345 192.168.163.128 192.168.163.2 DNS 85 Standard query 0xcf00 AAAA push.services.mozilla.com
249 251.202640973 192.168.163.2 192.168.163.128 DNS 121 Standard query response 0xc68c A o.pki.goog CNAME pki-goog.l.google.com A 142.251.223.99
250 251.202647284 192.168.163.2 192.168.163.128 DNS 133 Standard query response 0x2189 AAAA o.pki.goog CNAME pki-goog.l.google.com AAAA 2404:6800:4007:838::2003
251 251.203144731 192.168.163.128 142.251.223.99 TCP 74 49548 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3059570626 TSecr=0 WS=128
252 251.290870389 192.168.163.2 192.168.163.128 DNS 101 Standard query response 0xa20b A push.services.mozilla.com A 34.107.243.93
253 251.290870733 192.168.163.2 192.168.163.128 DNS 113 Standard query response 0xcf00 AAAA push.services.mozilla.com AAAA 64:ff9b::226b:f35d
254 251.293747609 142.251.223.99 192.168.163.128 TCP 60 80 → 49548 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
255 251.293785074 192.168.163.128 142.251.223.99 TCP 54 49548 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
256 251.294265999 192.168.163.128 142.251.223.99 OCSP 481 Request
257 251.294528908 142.251.223.99 192.168.163.128 TCP 60 80 → 49548 [ACK] Seq=1 Ack=428 Win=64240 Len=0
258 251.325968744 192.168.163.128 34.107.243.93 TCP 74 42844 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3432155302 TSecr=0 WS=128
259 251.477037941 192.168.163.128 192.168.163.2 DNS 97 Standard query 0x660f A firefox.settings.services.mozilla.com
260 251.477257412 192.168.163.2 192.168.163.128 DNS 97 Standard query 0x660a AAAA firefox.settings.services.mozilla.com
261 251.482239190 142.251.223.99 192.168.163.128 OCSP 965 Response
262 251.482239650 34.107.243.93 192.168.163.128 TCP 60 443 → 42844 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
263 251.482277673 192.168.163.128 142.251.223.99 TCP 54 49548 → 80 [ACK] Seq=428 Ack=912 Win=63329 Len=0
264 251.482369841 192.168.163.128 34.107.243.93 TCP 54 42844 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
265 251.488684331 192.168.163.128 34.107.243.93 TLSv1.3 727 Client Hello (SNI=push.services.mozilla.com)
266 251.489054891 34.107.243.93 192.168.163.128 TCP 60 443 → 42844 [ACK] Seq=1 Ack=674 Win=64240 Len=0
267 251.511938707 192.168.163.128 142.250.67.42 TLSv1.3 118 Change Cipher Spec, Application Data
Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface eth0, id 0
Ethernet II, Src: VMware_a6:07:ad (00:0c:29:a6:07:ad), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::20c:29ff:fea6:7ad, Dst: ff02::2
Internet Control Message Protocol v6
0000 33 33 00 00 00 02 00 0c 29 a6 07 ad 86 dd 60 08 33
0010 9d 5e 00 08 3a ff fe 80 00 00 00 00 00 00 02 0c
0020 29 ff fe a6 07 ad ff 02 00 00 00 00 00 00 00 00
0030 00 00 00 00 00 02 85 00 4a d8 00 00 00 00 J
eth0: <live capture in progress>
Packets: 1549
Profile: Default


Apps Places
Jun 30 10:47 AM
root@kali: ~
root@kali: ~
root@kali: ~
root@kali: ~ 190x42
root@kali:~# ls
automation
bettercap
bettercap.history
capture-01.cap
capture-01.csv
capture-01.kismet.csv
capture-01.kismet.netxml
capture-01.log.csv
capture-02.cap
capture-02.csv
capture-02.kismet.csv
capture-02.kismet.netxml
capture-02.log.csv
capture-03.cap
capture-03.csv
capture-03.kismet.csv
capture-03.kismet.netxml
capture-03.log.csv
capture-04.cap
capture-04.csv
capture-04.kismet.csv
capture-04.kismet.netxml
capture-04.log.csv
Code-for-phishing-link
Desktop
Documents
Downloads
embedded-browser-no-sandbox.json
evil_twin_captive_portal_password-Apple.txt
GhostTrack
go
handshake-28:87:BA:00:28:04.cap
handshake-B4:F9:49:86:D5:05.cap
Mobile-Number-Tracker
Music
nmap
nmap-env
NMAP-TOOL
password.txt
PhoneInfoga
Phone-number-tracking
Pictures
PP-Password-Protection-
Public
rockyou.txt
seeker
Srinu-01.cap
Srinu-01.csv
Srinu-01.kismet.csv
Srinu-01.kismet.netxml
Srinu-01.log.csv
subfinder
Templates
thc-hydra
username.txt
Videos
wifi
wifi-ET
wordlist.txt
zphisher
root@kali:~# wireshark
Warning: program compiled against libxml 212 using older 209
root@kali:~# wireshark
Warning: program compiled against libxml 212 using older 209
** (wireshark:2573) 10:41:11.448041 [Capture MESSAGE] -- Capture Start ...
** (wireshark:2573) 10:41:11.561538 [Capture MESSAGE] -- Capture started
** (wireshark:2573) 10:41:11.561713 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0SOB282.pcapng"
** (wireshark:2573) 10:46:14.084419 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:2573) 10:46:14.197421 [Capture MESSAGE] -- Capture stopped.
root@kali:~#