

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

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
15	42.254164296	Vhware.a8:07:ad	Vhware.a8:19:fe	ARP	42	Who has 192.168.163.2? Tell 192.168.163.128
16	42.254990497	Vhware.a8:19:fe	Vhware.a8:07:ad	ARP	60	192.168.163.2 is at 00:50:56:a8:19:fe
4	47.421084911	192.168.163.128	192.168.163.2	DNS	70	Standard query 0x0060 A giat.ac.in
5	47.422955656	192.168.163.128	192.168.163.2	DNS	70	Standard query 0x0e94 AAAA giat.ac.in
6	47.499281481	192.168.163.2	192.168.163.128	DNS	86	Standard query response 0x0060 A giat.ac.in A 68.178.147.186
7	50.497781450	192.168.163.2	192.168.163.128	DNS	98	Standard query response 0x0e94 AAAA giat.ac.in AAAA 64:ff9b:44b2:93ba
19	109.896262929	192.168.163.128	192.168.163.2	DNS	87	Standard query 0x4bec PTR 186.147.176.68.in-addr.arpa
11	41.000454540	192.168.163.2	192.168.163.128	DNS	117	Standard query response 0x4bec PTR 186.147.176.68.in-addr.arpa PTR 186.147.176.68.host.secureserver.net
8	39.898579528	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=1256, ttl=64 (reply in 8)
9	39.189849955	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=1256, ttl=128 (request in 8)
12	41.000668775	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=2512, ttl=64 (reply in 12)
13	41.339865792	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=2512, ttl=128 (request in 12)
14	41.973380077	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=3768, ttl=64 (reply in 14)
17	42.329916264	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=3768, ttl=128 (request in 14)
18	42.344065306	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=4104, ttl=64 (reply in 18)
19	42.493723759	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=4104, ttl=128 (request in 18)
20	42.921564553	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=51280, ttl=64 (reply in 21)
21	44.046660983	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=51280, ttl=128 (request in 20)
22	44.909678848	192.168.163.128	68.178.147.186	ICMP	98	Echo (ping) request id=0x0001, seq=61536, ttl=64 (reply in 23)
23	45.976563978	68.178.147.186	192.168.163.128	ICMP	98	Echo (ping) reply id=0x0001, seq=61536, ttl=128 (request in 22)
1	0.000000000	fe80::2::2::ff::fe::2	ff02::2	ICMPv6	64	Router Solicitation
2	14.813581087	192.168.163.128	192.46.210.39	NTP	60	NTP Version 4, client
3	14.938584598	192.46.210.39	192.168.163.128	NTP	60	NTP Version 4, server
24	50.769864451	192.168.163.128	192.46.210.39	NTP	60	NTP Version 4, client
25	50.894853512	192.46.210.39	192.168.163.128	NTP	60	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: Vhware.a8:07:ad (00:0c:29:a6:07:ad), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::2::2::ff::fe::2, Dst: ff02::2
Internet Control Message Protocol v6

eth0: <live capture in progress> Packets: 26 Profile: Default

Apps Places

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
244	251.023897352	192.168.163.128	142.250.87.42	TCP	54	34698 → 443 [ACK] Seq=6176 Ack=3193 Win=5535 Len=0
245	251.030671525	192.168.163.128	192.168.163.2	DNS	70	Standard query 61c6c A o.pki.goog
246	251.090889998	192.168.163.128	192.168.163.2	DNS	70	Standard query 0x2189 AAAA o.pki.goog
247	251.149847533	192.168.163.128	192.168.163.2	DNS	85	Standard query 0xa2b0 A push.services.mozilla.com
248	251.150214345	192.168.163.128	192.168.163.2	DNS	85	Standard query 0xc190 AAAA push.services.mozilla.com
249	251.202649873	192.168.163.2	192.168.163.128	DNS	121	Standard query response 0xc6bc 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 2404:6880:4007:838::2003
251	251.203244731	192.168.163.128	142.251.223.99	TCP	74	49548 → 80 [STN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=393570626 TSecr=0 WS=128
252	251.208070389	192.168.163.2	192.168.163.128	DNS	101	Standard query response 0xa2b0 A push.services.mozilla.com A 34-107.243.93
253	251.208079733	192.168.163.2	192.168.163.128	DNS	113	Standard query response 0xc1f0 AAAA push.services.mozilla.com AAAA 64:ff9b:226b:7f5d
254	251.207470899	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	251.207505714	192.168.163.128	142.251.223.99	TCP	54	49548 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
256	251.204265999	192.168.163.128	142.251.223.99	OCSP	481	Request
257	251.204269088	142.251.223.99	192.168.163.128	TCP	60	80 → 49548 [ACK] Seq=1 Ack=428 Win=64240 Len=0
258	251.205097944	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	251.477637941	192.168.163.128	192.168.163.2	DNS	97	Standard query 0xd59f A firefox.settings.services.mozilla.com
260	251.477257412	192.168.163.128	192.168.163.2	DNS	97	Standard query 0x60ba AAAA firefox.settings.services.mozilla.com
261	251.482239150	142.251.223.99	192.168.163.128	OCSP	965	Response
262	251.482239966	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	251.482271673	192.168.163.128	142.251.223.99	TCP	54	49548 → 80 [ACK] Seq=428 Ack=912 Win=63329 Len=0
264	251.482269841	192.168.163.128	34.107.243.93	TCP	54	42844 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
265	251.488848321	192.168.163.128	34.107.243.93	TLV3.3	727	Client Hello (SHA256, 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	251.511938787	192.168.163.128	142.250.87.42	TLV3.3	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: Vhware.a8:07:ad (00:0c:29:a6:07:ad), Dst: IPv6mcast_02 (33:33:00:00:00:02)
Internet Protocol Version 6, Src: fe80::2::2::ff::fe::2, Dst: ff02::2
Internet Control Message Protocol v6

eth0: <live capture in progress> Packets: 1549 Profile: Default

```
root@kali: ~  
root@kali:~# ls  
automation go  
bettercap handshake-28:87:BA:60:28:84.cap  
bettercap.history handshake-84:F9:49:06:05:05.cap  
capture-01.cap Mobile-Number-Tracker  
capture-01.csv Music  
capture-01.kismet.csv nmap  
capture-01.kismet.netxml nmap-env  
capture-01.log.csv NMAP-TOOL  
capture-02.cap password.txt  
capture-02.csv PhoneInfo  
capture-02.kismet.csv Phone-number-tracking  
capture-02.kismet.netxml Pictures  
capture-02.log.csv PP-Password-Protection-  
capture-03.cap Public  
capture-03.csv rockyou.txt  
capture-03.kismet.csv sseeker  
capture-03.kismet.netxml Srinu-01.cap  
capture-03.log.csv Srinu-01.csv  
capture-04.cap Srinu-01.kismet.csv  
capture-04.csv Srinu-01.kismet.netxml  
capture-04.kismet.csv Srinu-01.log.csv  
capture-04.kismet.netxml subfinder  
capture-04.log.csv Templates  
cde-for-phishing-link the-hydra  
desktop username.txt  
documents Videos  
downloads wifi  
unhedded-browser-no-sandbox.json wifi-ET  
evil_twin_captive_portal_password-Apple.txt wordlist.txt  
GhostTrack 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_ethn050B282.pcapng"  
** (Wireshark:2573) 10:46:14.084419 [Capture MESSAGE] -- Capture Stop ...  
** (Wireshark:2573) 10:46:14.197421 [Capture MESSAGE] -- Capture stopped.  
root@kali:~#
```