

# **Title: Network Traffic Analysis Using Wireshark**

## **Objective**

To capture live network packets and identify basic network protocols.

## **Tool Used**

Wireshark

## **Procedure**

(Briefly summarize the steps you followed.)

## **Protocols Identified**

### **1. DNS**

- Used for domain name resolution.
- Observed query to google.com.
- Uses UDP port 53.

### **2. TCP**

- Transport layer protocol.
- Provides reliable communication.
- Observed TCP handshake (SYN, SYN-ACK, ACK).

### **3. TLS**

- Used for secure communication (HTTPS).
- Encrypts website traffic.

### **4. ICMP**

- Used for ping.
- Observed echo request and reply.

### **5. Observations**

- Large number of TCP packets observed.
- DNS queries precede website loading.
- HTTPS traffic encrypted using TLS.

We get into the wireshark tools and use the wifi port

Wireshark Screenshot:

- Packets:** 24
- Profile:** Default

```

> Frame 1: Packet, 124 bytes on wire (992 bits), 12 bytes captured (992 bits) on interface Wi-Fi 2
> Ethernet II, Src: LiteonTechno_df:1c:6f (d0:39:57:48:08:08), Dst: 00:0c:29:9c:c5:0c (NetlinkIct_c9:9c:c5)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.1
> Transmission Control Protocol, Src Port: 50509, Dst Port: 443
> Transport Layer Security
> Transport Layer Security

```

No.	Time	Source	Destination	Protocol	Length	Info
16	1.945416	192.168.1.1	224.0.0.1	IGMPv3	50	Membership Query, general
17	2.254481	192.168.1.5	224.0.0.22	IGMPv3	70	Membership Report / Join Group
18	2.351274	NetlinkIct_c9:9c:c5	Broadcast	ARP	60	ARP Announcement for 192.168.1.5
19	2.375565	192.168.1.5	52.182.143.210	TCP	55	59881 → 443 [ACK] Seq=1
20	2.391510	192.168.1.5	20.190.174.43	TCP	55	52099 → 443 [ACK] Seq=1
21	2.456603	20.190.174.43	192.168.1.5	TCP	66	443 → 52099 [ACK] Seq=1
22	2.767219	52.182.143.210	192.168.1.5	TCP	66	443 → 59881 [ACK] Seq=1
23	5.484983	192.168.1.5	44.235.223.145	TCP	55	57619 → 443 [ACK] Seq=1
24	5.840464	44.235.223.145	192.168.1.5	TCP	66	443 → 57619 [ACK] Seq=1

### DNS Packet Captured :

Wireshark Screenshot:

```

> Frame 341: Packet, 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{...}
> Ethernet II, Src: LiteonTechno_df:1c:6f (d0:39:57:48:08:08), Dst: NetlinkIct_c9:9c:c5 (8c:c7:c3:c9:9c:c5)
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 192.168.1.5
> User Datagram Protocol, Src Port: 54820, Dst Port: 53
> Domain Name System (query)

```

No.	dns	dnsserver	Source	Destination	Protocol	Length	Info
1088		192.168.1.5	43.239.200.28	DNS	74	Standard query 0xd0ed A ecs.office.com	
342	17.350343	192.168.1.5	43.239.200.28	DNS	86	Standard query 0xbab4 A officeclient.microsoft.com	
343	17.360292	43.239.200.28	192.168.1.5	DNS	255	Standard query response 0xd0ed A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skygate.com CNAME ...	
346	17.463090	43.239.200.28	192.168.1.5	DNS	406	Standard query response 0xbab4 A officeclient.microsoft.com CNAME config.officeapps.live.com CNAME prod.configsvclive.com.akadns.net	
458	18.369040	192.168.1.5	43.239.200.28	DNS	93	Standard query 0x8944 A metadata.templates.cdn.office.net	
461	18.468416	43.239.200.28	192.168.1.5	DNS	245	Standard query response 0x944 A metadata.templates.cdn.office.net CNAME templatesmetadata.office.net CNAME templatesmetadata.office.net	
524	18.815080	192.168.1.5	43.239.200.28	DNS	87	Standard query 0x8343 A roaming.svc.cloud.microsoft	
548	18.859862	192.168.1.5	43.239.200.28	DNS	86	Standard query 0x3d79 A recent.svc.cloud.microsoft	
549	18.885910	43.239.200.28	192.168.1.5	DNS	372	Standard query response 0x343 A roaming.svc.cloud.microsoft CNAME prod.ocws1.live.com.akadns.net CNAME https://8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
556	18.927159	43.239.200.28	192.168.1.5	DNS	368	Standard query response 0x3d79 A recent.svc.cloud.microsoft CNAME prod.ocws1.live.com.akadns.net CNAME https://8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
836	19.696758	192.168.1.5	8.8.8.8	DNS	113	Standard query 0x2118 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
837	19.697287	192.168.1.5	8.8.8.8	DNS	113	Standard query 0x998d A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
852	19.883860	8.8.8.8	192.168.1.5	DNS	170	Standard query response 0xd218 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com SOA ns1.footprintdns.com	
854	19.883860	8.8.8.8	192.168.1.5	DNS	265	Standard query response 0x989d No such name A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com CNAME canary.trafficmanager.net...	
859	19.910410	192.168.1.5	43.239.200.28	DNS	113	Standard query 0x78f5 A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
860	19.956218	192.168.1.5	43.239.200.28	DNS	91	Standard query 0x02ae A messaging_engagement.office.com	
873	20.041027	43.239.200.28	192.168.1.5	DNS	265	Standard query response 0x78f5 No such name A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com CNAME canary.trafficmanager.net...	
874	20.041027	43.239.200.28	192.168.1.5	DNS	182	Standard query response 0x02ae A messaging_engagement.office.com CNAME prod_campaignaggregator.omexexternalfb.office.net.akadns.net	
917	20.157533	192.168.1.5	8.8.8.8	DNS	113	Standard query 0x0187 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com	
918	20.158266	192.168.1.5	8.8.8.8	DNS	113	Standard query 0x5e5c8 A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com	

## TCP Packet Captured :

No.	tcp	Destination	Protocol	Length	Info
1	tcp port == 8883				
2	tcp port == 80    udp.port == ...				
3	133.73	192.168.1.5	TCP	54	443 → 60782 [ACK] Seq=41 Ack=3 Win=19 Len=0
4	tcp	1.5	TLSv1.2	124	Application Data
5	tcp.options.acc_ecn	57.144.243.32	TLSv1.2	124	Application Data
6	tcp.options.ad	43.32	TCP	54	443 → 50509 [ACK] Seq=1163 Ack=852 Win=496 Len=0
7	tcp.options.ccc	43.32	TLSv1.2	126	Application Data
8	tcp.options.cecho	1.5	TCP	54	50509 → 443 [ACK] Seq=852 Ack=1235 Win=254 Len=0
9	tcp.options.cnew	1.5	TLSv1.2	144	Application Data
10	tcp.options.echo	104.18.39.21	TLSv1.2	133	Application Data
11	tcp.options.ecoreply	1.5	TCP	54	443 → 60400 [ACK] Seq=841 Ack=879 Win=17 Len=0
12	tcp.options.est	1.5	TCP	54	60400 → 443 [ACK] Seq=879 Ack=920 Win=255 Len=0
13	tcp.options.experimental	1.5	TCP	55	[TCP Keep-Alive] 60915 → 5228 [ACK] Seq=27 Ack=25 Win=253 Len=1
14	tcp.options.m05	142.250.4.188	TCP	66	[TCP Keep-Alive ACK] 5228 → 60915 [ACK] Seq=25 Ack=28 Win=1047 Len=0 SLE=27 SRE=28
15	tcp.options.mss	1.5	TLSv1.2	144	Application Data
16	tcp.options.nop	9.21	TCP	54	443 → 60400 [ACK] Seq=920 Ack=969 Win=17 Len=0
17	tcp.options.qs	9.21	TLSv1.2	133	Application Data
18	tcp.options.rbd_probe	1.5	TCP	54	60400 → 443 [ACK] Seq=969 Ack=999 Win=255 Len=0
19	tcp.options.rbd_trpy	9.21	TLSv1.2	78	Application Data
20	tcp.options.sack	1.5	TLSv1.2	82	Application Data
21	tcp.options.sack_perm	9.21	TCP	54	443 → 60400 [ACK] Seq=1023 Ack=997 Win=17 Len=0
22	tcp	172.188.155.25	TCP	55	[TCP Keep-Alive] 50406 → 443 [ACK] Seq=67 Ack=68 Win=250 Len=1
23	4500 183.511347	172.188.155.25	TCP	66	[TCP Keep-Alive ACK] 443 → 50406 [ACK] Seq=68 Ack=68 Win=290 Len=0 SLE=67 SRE=68
24	Frame 337: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{...}				
25	> Ethernet II, Src: NetlinkIct_{:9:9c:c5} (8c:c7:c3:c9:c5:c5), Dst: LiteonTechno_df:1c:6f (d0:39:57:f1:c6:6f)				
26	> Internet Protocol Version 4, Src: 23.202.229.135, Dst: 192.168.1.5				
27	> Transmission Control Protocol, Src Port: 443, Dst Port: 62431, Seq: 6449, Ack: 2762, Len: 0				

## TLS Packet Captured :

No.	tls	Time	Source	Destination	Protocol	Length	Info
1	1 0.000000	192.168.1.5	57.144.243.32		TLSv1.2	124	Application Data
2	5 0.306373	57.144.243.32	192.168.1.5		TLSv1.2	126	Application Data
3	9 0.819671	104.18.39.21	192.168.1.5		TLSv1.2	78	Application Data
4	10 0.820301	192.168.1.5	104.18.39.21		TLSv1.2	82	Application Data
5	92 14.542070	192.168.1.5	49.44.136.97		QUIC	1292	Initial, DCID=b5d44ef5c
6	93 14.542232	192.168.1.5	49.44.136.97		QUIC	1292	Initial, DCID=b5d44ef5c
7	96 14.644138	49.44.136.97	192.168.1.5		QUIC	1292	Initial, SCID=147ca412e
8	149 14.949694	192.168.1.5	8.8.4.4		QUIC	1292	Initial, DCID=dc971d4f8
9	154 15.052539	8.8.4.4	192.168.1.5		QUIC	1292	Initial, SCID=fc971d4f8
10	155 15.052539	8.8.4.4	192.168.1.5		QUIC	1292	Initial, SCID=fc971d4f8
11	> Frame 1: Packet, 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF_{...}						
12	> Ethernet II, Src: NetlinkIct_{:9:9c:c5} (8c:c7:c3:c9:c5:c5), Dst: LiteonTechno_df:1c:6f (d0:39:57:f1:c6:6f)						
13	> Internet Protocol Version 4, Src: 23.202.229.135, Dst: 192.168.1.5, Seq: 50509, Ack: 62431, Len: 124						
14	> Transmission Control Protocol, Src Port: 50509, Dst Port: 62431, Seq: 6449, Ack: 2762, Len: 124						
15	> Transport Layer Security						

## ICMP Packet Captured :

No.	icmp	Source	Destination	Protocol	Length	Info
1	1 53927	192.168.1.5	142.250.70.110	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 4014)
2	4014 107.715263	142.250.70.110	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=116 (request in 4011)
3	4015 108.678591	192.168.1.5	142.250.70.110	ICMP	74	Echo (ping) request id=0x0001, seq=29/7424, ttl=128 (reply in 4016)
4	4016 108.851606	142.250.70.110	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=29/7424, ttl=116 (request in 4015)
5	4026 109.694351	192.168.1.5	142.250.70.110	ICMP	74	Echo (ping) request id=0x0001, seq=30/7680, ttl=128 (reply in 4027)
6	4027 109.774088	142.250.70.110	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=30/7680, ttl=116 (request in 4026)
7	4030 110.703267	192.168.1.5	142.250.70.110	ICMP	74	Echo (ping) request id=0x0001, seq=31/7936, ttl=128 (reply in 4031)
8	4031 110.797171	142.250.70.110	192.168.1.5	ICMP	74	Echo (ping) reply id=0x0001, seq=31/7936, ttl=116 (request in 4030)