

# **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

The image shows the Wireshark interface with a list of captured packets. The packets are filtered by 'Apply a display filter ... <Ctrl-/>'. The list shows packets 16 through 24, all originating from 192.168.1.5. Packets 16-18 are IGMPv3 and ARP. Packets 19-24 are TCP ACKs. The detailed view on the right shows the selected packet (No. 19) as a TCP ACK from 192.168.1.5 to 52.182.143.210. The packet structure is shown as Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The packet bytes are displayed in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
16	1.945416	192.168.1.1	224.0.0.1	IGMPv3	50	Membership Query, gener
17	2.254481	192.168.1.5	224.0.0.22	IGMPv3	70	Membership Report / Joi
18	2.351274	NetlinkIct_c9:9c:c5	Broadcast	ARP	60	ARP Announcement for 15
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

Frame 19: Packet, 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF...  
Ethernet II, Src: LiteonTechno\_df:1c:6f (d0:39:57:df:1c:6f), Dst: NetlinkIct\_c9:9c:c5 (8c:c7:c3:c9:9c:c5)  
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 52.182.143.210  
Transmission Control Protocol, Src Port: 50509, Dst Port: 443  
Transport Layer Security

0000 8c c7 c3 c9 9c c5 d0 39 57 df 1c 6f 08 00 45  
0010 00 6e be 58 40 00 80 06 4d d3 c0 a8 01 05 35  
0020 f3 20 c5 4d 01 bb ea cf 22 b2 97 ee 50 a9 56  
0030 00 fd ce 28 00 00 17 03 03 00 41 d6 68 70 9a  
0040 e8 25 e7 e4 a5 09 7c eb 89 92 56 12 6d 4c b1  
0050 24 76 f5 8a 1d 8f 21 eb c0 c7 a5 c6 63 81 d6  
0060 82 24 19 2a 22 ca 0c 8c 8f 38 ce af 8d ee 16  
0070 f5 a1 96 45 ab 0f d4 e6 33 22 e5 4a

DNS Packet Captured :

The image shows the Wireshark interface with a list of captured DNS packets. The packets are filtered by 'dns'. The list shows packets 342 through 918, all originating from 192.168.1.5. The detailed view on the right shows the selected packet (No. 342) as a DNS Standard query from 192.168.1.5 to 43.239.200.28. The packet structure is shown as Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes are displayed in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
342	17.350343	192.168.1.5	43.239.200.28	DNS	74	Standard query 0xbdbd A ecs.office.com
343	17.360292	43.239.200.28	192.168.1.5	DNS	86	Standard query response 0xbdbd A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skype.com CNAME...
346	17.463090	43.239.200.28	192.168.1.5	DNS	255	Standard query response 0xbdbd A ecs.office.com CNAME ecs.office.trafficmanager.net CNAME dual-s-0005-office.config.skype.com CNAME...
458	18.369040	192.168.1.5	43.239.200.28	DNS	406	Standard query response 0xbdbd A officeclient.microsoft.com CNAME config.officeapps.live.com CNAME prod.configsvc1.live.com.akadns...
461	18.468416	43.239.200.28	192.168.1.5	DNS	93	Standard query 0x8944 A metadata.templates.cdn.office.net
524	18.815006	192.168.1.5	43.239.200.28	DNS	245	Standard query response 0x8944 A metadata.templates.cdn.office.net CNAME templatesmetadata.office.net CNAME templatesmetadata.offic...
548	18.859862	192.168.1.5	43.239.200.28	DNS	87	Standard query 0x3d79 A recent.svc.cloud.microsoft
549	18.885910	43.239.200.28	192.168.1.5	DNS	86	Standard query response 0x3d79 A recent.svc.cloud.microsoft CNAME prod.roaming1.live.com.akadns.net CNAME asia.roaming1.live.com.a...
556	18.927159	43.239.200.28	192.168.1.5	DNS	372	Standard query response 0x8343 A roaming.svc.cloud.microsoft CNAME prod.ocws1.live.com.akadns.net CNAME asia2.ocws1.live.com.akadns...
836	19.696758	192.168.1.5	8.8.8.8	DNS	368	Standard query response 0x3479 A recent.svc.cloud.microsoft CNAME prod.ocws1.live.com.akadns.net CNAME asia2.ocws1.live.com.akadns...
837	19.697287	192.168.1.5	8.8.8.8	DNS	113	Standard query 0xd218 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com
852	19.883866	8.8.8.8	192.168.1.5	DNS	113	Standard query response 0xd218 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com
854	19.883866	8.8.8.8	192.168.1.5	DNS	170	Standard query response 0xd218 HTTPS 8291426558b88018f27bcd459e553a33.clo.footprintdns.com SOA ns1.footprintdns.com
859	19.910410	192.168.1.5	43.239.200.28	DNS	265	Standard query response 0x098d A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com CNAME canary.trafficmanager.net...
860	19.956218	192.168.1.5	43.239.200.28	DNS	113	Standard query 0x78f5 A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com
873	20.041027	43.239.200.28	192.168.1.5	DNS	91	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	265	Standard query response 0x02ae A messaging.engagement.office.com CNAME prod-campaignaggregator.omexternal1fb.office.net.akadns.ne...
917	20.157533	192.168.1.5	8.8.8.8	DNS	182	Standard query response 0x02ae A messaging.engagement.office.com CNAME prod-campaignaggregator.omexternal1fb.office.net.akadns.ne...
918	20.158266	192.168.1.5	8.8.8.8	DNS	113	Standard query 0xe5c8 A 8291426558b88018f27bcd459e553a33.clo.footprintdns.com

Frame 342: 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:df:1c:6f), Dst: NetlinkIct\_c9:9c:c5 (8c:c7:c3:c9:9c:c5)  
Internet Protocol Version 4, Src: 192.168.1.5, Dst: 43.239.200.28  
User Datagram Protocol, Src Port: 54820, Dst Port: 53  
Domain Name System (query)

0000 8c c7 c3 c9 9c c5 d0 39 57 df 1c 6f 08 00 45 00  
0010 00 3c 8c e0 00 00 11 f0 0c c0 a8 01 05 2b af  
0020 c8 1c d6 24 00 35 00 28 2f 16 d0 ed 01 00 00 01  
0030 00 00 00 00 00 03 65 63 73 06 6f 66 66 69 63  
0040 65 03 63 6f 6d 00 00 01 00 01

## TCP Packet Captured :

tcp

No.

tcp.port == 8882  
tcp.port == 80 | udp.port == ...

Destination

133.73  
1.5  
43.32  
43.32  
1.5  
1.5  
9.21  
9.21  
1.5  
1.5  
4.188  
1.5  
9.21  
9.21  
1.5  
9.21  
1.5  
9.21  
1.5  
9.21  
1.5  
9.21  
1.5  
4500 183.511347

172.188.155.25

Protocol

TCP  
TLSv1.2  
TCP  
TLSv1.2  
TCP  
TLSv1.2  
TCP  
TLSv1.2  
TCP  
TCP  
TCP  
TLSv1.2  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP  
TCP

Length

54  
124  
54  
126  
54  
144  
133  
54  
54  
55  
66  
144  
54  
133  
54  
78  
82  
54  
55  
66

Info

Seq=41 Ack=3 Win=19 Len=0  
[ACK]  
Seq=1163 Ack=852 Win=496 Len=0  
[ACK]  
Seq=852 Ack=1235 Win=254 Len=0  
[ACK]  
Seq=841 Ack=879 Win=17 Len=0  
[ACK]  
Seq=879 Ack=920 Win=255 Len=0  
[TCP Keep-Alive] 60915 → 5228 [ACK] Seq=27 Ack=25 Win=253 Len=1  
[TCP Keep-Alive ACK] 5228 → 60915 [ACK] Seq=25 Ack=28 Win=1047 Len=0 SLE=27 SRE=28  
[ACK]  
Seq=920 Ack=969 Win=17 Len=0  
[ACK]  
Seq=969 Ack=999 Win=255 Len=0  
[ACK]  
Seq=1023 Ack=997 Win=17 Len=0  
[TCP Keep-Alive] 50406 → 443 [ACK] Seq=67 Ack=60 Win=250 Len=1  
[TCP Keep-Alive ACK] 443 → 50406 [ACK] Seq=60 Ack=68 Win=290 Len=0 SLE=67 SRE=68

> Frame 337: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{0000 d0 39 57 df 1c 6f 8c c7} c3 c9 9c c5 08 00 45 00  
> Ethernet II, Src: NetLinkIt\_c9:9c:c5 (8c:c7:c3:c9:9c:c5), Dst: LiteonTechno\_df:1c:6f (d0:39:57:df:1c:6f) 0010 00 28 03 88 40 00 37 06 81 49 17 ca e5 87 c0 a8  
> Internet Protocol Version 4, Src: 23.202.229.135, Dst: 192.168.1.5 0020 01 05 01 bb f3 df 8c 67 c2 6d cd 81 ac 70 50 10  
> Transmission Control Protocol, Src Port: 443, Dst Port: 62431, Seq: 6449, Ack: 2762, Len: 0 0030 01 e7 21 84 00 00  
-j...

## TLS Packet Captured :

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.5	57.144.243.32	TLSv1.2	124	Application Data
5	0.306373	57.144.243.32	192.168.1.5	TLSv1.2	126	Application Data
9	0.819671	104.18.39.21	192.168.1.5	TLSv1.2	78	Application Data
10	0.820301	192.168.1.5	104.18.39.21	TLSv1.2	82	Application Data
92	14.542070	192.168.1.5	49.44.136.97	QUIC	1292	Initial, DCID=b5d44ef5c
93	14.542232	192.168.1.5	49.44.136.97	QUIC	1292	Initial, DCID=b5d44ef5c
96	14.644138	49.44.136.97	192.168.1.5	QUIC	1292	Initial, SCID=147ca412e
149	14.949694	192.168.1.5	8.8.4.4	QUIC	1292	Initial, DCID=dc971d4f8
154	15.052539	8.8.4.4	192.168.1.5	QUIC	1292	Initial, SCID=fc971d4f8
155	15.052539	8.8.4.4	192.168.1.5	QUIC	1292	Initial, SCID=fc971d4f8

> Frame 1: Packet, 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface \Device\NPF...  
> Ethernet II, Src: LiteonTechno\_df:1c:6f (d0:39:57:df:1c:6f), Dst: 192.168.1.5  
> Internet Protocol Version 4, Src: 192.168.1.5, Dst: 57.144.243.32  
> Transmission Control Protocol, Src Port: 50509, Dst Port: 60782, Len: 0  
> Transport Layer Security

## ICMP Packet Captured :

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