

CS352 Project 2: Wireshark

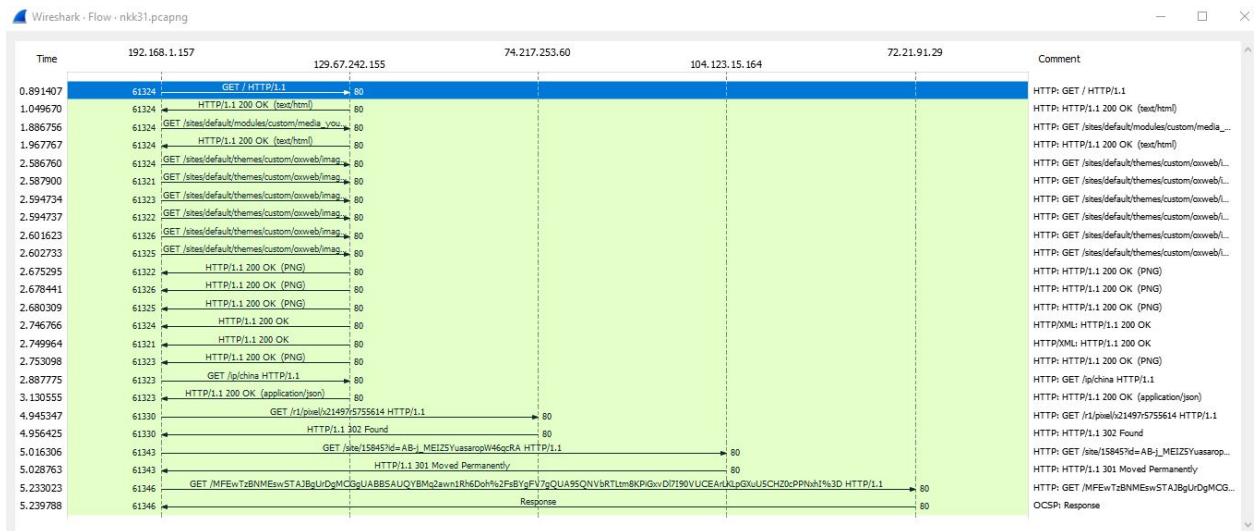
Nikita Kolotov, nkk31

1.)

Trace File located within folder

2.)

- A. The most common is TCP (Transmission Control Protocol)
- B. TCP sets up a connection and HTTP transfers data through that connection
- C.



3.)

- A. 16 0.819609 192.168.1.157 31.13.71.7 TCP 66 61328 → 443 [SYN]
Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1

8	0.813777	192.168.1.157	129.67.242.155	TCP	66	61321 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
9	0.813910	192.168.1.1	192.168.1.157	DNS	168	Standard query response 0x71cb A www.googletagmanager.com CNAME www.googletagmanager.l.google.com A 172.217...
10	0.814219	192.168.1.157	129.67.242.155	TCP	66	61322 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
11	0.814608	192.168.1.157	129.67.242.155	TCP	66	61323 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
12	0.815022	192.168.1.157	129.67.242.155	TCP	66	61324 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	0.815378	192.168.1.157	129.67.242.155	TCP	66	61325 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	0.815747	192.168.1.157	129.67.242.155	TCP	66	61326 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
15	0.819488	192.168.1.157	172.217.6.232	TCP	66	61327 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
16	0.819609	192.168.1.157	31.13.71.7	TCP	66	61328 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
17	0.820327	192.168.1.157	192.168.1.1	DNS	80	Standard query 0x6576 A fonts.googleapis.com

> Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd), Dst: Verizon_dd:23:fe (20:c0:47:dd:23:fe)
> Internet Protocol Version 4, Src: 192.168.1.157, Dst: 129.67.242.155
> Transmission Control Protocol, Src Port: 61321, Dst Port: 80, Seq: 0, Len: 0

a.

B.

<u>Layer</u>	<u>Protocol</u>
Network	IP
Transport	TCP
Application	HTTP

4.)

A.

```
Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix  . : fios-router.home
Description . . . . . : Ralink RT3290 802.11bgn Wi-Fi Adapter
Physical Address. . . . . : BC-85-56-A3-BB-CD
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::60b0:b4d9:d90a:bc51%8(Preferred)
IPv4 Address. . . . . : 192.168.1.157(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Saturday, July 13, 2019 6:54:28 PM
Lease Expires . . . . . : Monday, July 15, 2019 10:00:13 PM
Default Gateway . . . . . : 192.168.1.1
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 62686550
DHCPv6 Client DUID. . . . . : 00-01-00-01-22-2C-06-2B-6C-3B-E5-8D-A7-C1
DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
Connection-specific DNS Suffix Search List :
                                     fios-router.home
```

B. I can find the MAC address in the trace. The MAC address for my machine is BC:85:56:A3:BB:CD

```
> Frame 125: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▼ Ethernet II, Src: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd), Dst: Verizon_dd:23:fe (20:c0:47:dd:23:fe)
  > Destination: Verizon_dd:23:fe (20:c0:47:dd:23:fe)
  > Source: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.1.157, Dst: 31.13.71.36
  > Transmission Control Protocol, Src Port: 61339, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

a.

C. No, the destination is the Verizon router since that is the provider for my internet service. We are connecting to this device because we need to travel through a series of routers to get to that web service. Therefore, from my machine I must first connect to a device that will allow me to reach the router of the web server.

5.)

- A. I did get 4 replies. The time refers to how long it took for the ping and acknowledgements to get through.

```
C:\Users\nikit>ping www.ox.ac.uk

Pinging www.ox.ac.uk [129.67.242.155] with 32 bytes of data:
Reply from 129.67.242.155: bytes=32 time=128ms TTL=49
Reply from 129.67.242.155: bytes=32 time=96ms TTL=49
Reply from 129.67.242.155: bytes=32 time=97ms TTL=49
Reply from 129.67.242.155: bytes=32 time=85ms TTL=49

Ping statistics for 129.67.242.155:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 85ms, Maximum = 128ms, Average = 101ms
```

- a.
b.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help									
icmp									
No.	Time	Source	Destination	Protocol	Length	Info			
540	3.590213	192.168.1.157	129.67.242.155	ICMP	74	Echo (ping) request	id=0x0001, seq=1/256, ttl=128 (reply in 777)		
777	3.718135	129.67.242.155	192.168.1.157	ICMP	74	Echo (ping) reply	id=0x0001, seq=1/256, ttl=49 (request in 540)		
3955	4.607696	192.168.1.157	129.67.242.155	ICMP	74	Echo (ping) request	id=0x0001, seq=2/512, ttl=128 (reply in 4496)		
4496	4.703982	129.67.242.155	192.168.1.157	ICMP	74	Echo (ping) reply	id=0x0001, seq=2/512, ttl=49 (request in 3955)		
5403	5.625679	192.168.1.157	129.67.242.155	ICMP	74	Echo (ping) request	id=0x0001, seq=3/768, ttl=128 (reply in 5404)		
5404	5.722752	129.67.242.155	192.168.1.157	ICMP	74	Echo (ping) reply	id=0x0001, seq=3/768, ttl=49 (request in 5403)		
5405	6.643352	192.168.1.157	129.67.242.155	ICMP	74	Echo (ping) request	id=0x0001, seq=4/1024, ttl=128 (reply in 5406)		
5406	6.728707	129.67.242.155	192.168.1.157	ICMP	74	Echo (ping) reply	id=0x0001, seq=4/1024, ttl=49 (request in 5405)		

> Frame 540: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0									
▼ Ethernet II, Src: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd), Dst: Verizon_dd:23:fe (20:c0:47:dd:23:fe)									
▼ Destination: Verizon_dd:23:fe (20:c0:47:dd:23:fe)									
Address: Verizon_dd:23:fe (20:c0:47:dd:23:fe)									
.... 0. = LG bit: Globally unique address (factory default)									
.... 0. = IG bit: Individual address (unicast)									
▼ Source: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd)									
Address: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd)									
.... 0. = LG bit: Globally unique address (factory default)									
.... 0. = IG bit: Individual address (unicast)									
Type: IPv4 (0x0800)									
> Internet Protocol Version 4, Src: 192.168.1.157, Dst: 129.67.242.155									
> Internet Control Message Protocol									
0000	20 c0 47 dd 23 fe bc 85	56 a3 bb cd 08 00 45 00	..G#...V....E.						
0010	00 3c 25 c6 00 00 80 01	de d6 c0 a8 01 9d 81 43	.<%.....C						
0020	f2 9b 08 00 4d 5a 00 01	00 01 61 62 63 64 65 66MZ...abcdef						
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	ghijklmn opqrstuv						

- B. The time is greater than in part A. This is because New Zealand is where this server is located. Since NZ is further away than the UK, we can see that it takes longer to reach this website. $2(\text{Distance} / \text{Propagation Factor}) = \text{RTT}$.

a.

```
C:\Users\nikit>ping www.lincoln.ac.nz

Pinging www.lincoln.ac.nz [103.240.53.22] with 32 bytes of data:
Reply from 103.240.53.22: bytes=32 time=203ms TTL=118
Reply from 103.240.53.22: bytes=32 time=231ms TTL=118
Reply from 103.240.53.22: bytes=32 time=216ms TTL=118
Reply from 103.240.53.22: bytes=32 time=209ms TTL=118

Ping statistics for 103.240.53.22:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 203ms, Maximum = 231ms, Average = 214ms
```

b.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
44	10.050787	192.168.1.157	103.240.53.22	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=128 (reply in 45)
45	10.253910	103.240.53.22	192.168.1.157	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=118 (request in 44)
46	11.054909	192.168.1.157	103.240.53.22	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=128 (reply in 47)
47	11.285969	103.240.53.22	192.168.1.157	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=118 (request in 46)
50	12.072918	192.168.1.157	103.240.53.22	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=128 (reply in 51)
51	12.289286	103.240.53.22	192.168.1.157	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=118 (request in 50)
55	13.092711	192.168.1.157	103.240.53.22	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=128 (reply in 58)
58	13.302004	103.240.53.22	192.168.1.157	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=118 (request in 55)

> Frame 44: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: HonHaiPr_a3:bb:cd (bc:85:56:a3:bb:cd), Dst: Verizon_dd:23:fe (20:c0:47:dd:23:fe)

> Internet Protocol Version 4, Src: 192.168.1.157, Dst: 103.240.53.22

> Internet Control Message Protocol

Offset	Hex	ASCII
0000	20 c0 47 dd 23 fe bc 85 56 a3 bb cd 08 00 45 00	.G.#...V.....E.
0010	00 3c 73 d2 00 00 80 01 67 a3 c0 a8 01 9d 67 f0	..<s.....g.....g.
0020	35 16 08 00 4d 56 00 01 00 05 61 62 63 64 65 66	5...MV... ..abcdef
0030	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstuv