

# Wireshark lab 1

Name: Nirmith Victor D'Almeida

Student Number : 101160124

1. The 3 different protocols that appear in the protocol column are TCP, SSDP and DNS (unfiltered)

No.	Time	Source	Destination	Protocol	Length	Info
1	10:51:46.531055	192.168.2.42	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
2	10:51:46.531055	192.168.2.20	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
3	10:51:47.364890	192.168.2.42	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4	10:51:47.364890	192.168.2.20	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	10:51:47.555146	192.168.2.42	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
6	10:51:47.555146	192.168.2.20	239.255.255.250	SSDP	210	M-SEARCH * HTTP/1.1
7	10:51:48.374231	192.168.2.42	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
8	10:51:48.374231	192.168.2.20	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
9	10:51:48.511638	192.168.2.24	192.168.2.1	DNS	89	Standard query 0x7eec A v10.events.data.microsoft.com
10	10:51:48.551578	192.168.2.24	207.164.234.193	DNS	89	Standard query 0x7eec A v10.events.data.microsoft.com
11	10:51:48.552132	192.168.2.1	192.168.2.24	DNS	221	Standard query response 0x7eec A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedsc
12	10:51:48.553642	192.168.2.24	13.69.239.74	TCP	66	55486 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
13	10:51:48.564880	207.164.234.193	192.168.2.24	DNS	216	Standard query response 0x7eec A v10.events.data.microsoft.com CNAME global.asimov.events.data.trafficmanager.net CNAME onedsc
14	10:51:48.650550	13.69.239.74	192.168.2.24	TCP	66	443 → 55486 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1440 WS=256 SACK_PERM=1
15	10:51:48.650818	192.168.2.24	13.69.239.74	TCP	54	55486 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
16	10:51:48.651676	192.168.2.24	13.69.239.74	TLSv1.2	268	Client Hello
17	10:51:48.747751	13.69.239.74	192.168.2.24	TCP	1506	443 → 55486 [ACK] Seq=1 Ack=215 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
18	10:51:48.747751	13.69.239.74	192.168.2.24	TCP	1506	443 → 55486 [ACK] Seq=1453 Ack=215 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
19	10:51:48.747751	13.69.239.74	192.168.2.24	TCP	1506	443 → 55486 [ACK] Seq=2905 Ack=215 Win=525312 Len=1452 [TCP segment of a reassembled PDU]
20	10:51:48.747751	13.69.239.74	192.168.2.24	TLSv1.2	100	Server Hello, Certificate, Server Key Exchange, Server Hello Done
21	10:51:48.747909	192.168.2.24	13.69.239.74	TCP	54	55486 → 443 [ACK] Seq=215 Ack=4403 Win=132352 Len=0
22	10:51:48.760700	192.168.2.24	13.69.239.74	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message

2. → when we get the link

833	10:53:41.591506	192.168.2.24	128.119.245.12	HTTP	542	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
-----	-----------------	--------------	----------------	------	-----	---

→ arrival time for ^

- ✓ Frame 833: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124},
  - › Interface id: 0 (\Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124})
  - Encapsulation type: Ethernet (1)
  - Arrival Time: Jan 18, 2022 10:53:41.591506000 Eastern Standard Time

→Http Ok

835	10:53:41.634212	128.119.245.12	192.168.2.24	HTTP	492	HTTP/1.1 200 OK (text/html)
-----	-----------------	----------------	--------------	------	-----	-----------------------------

→ arrival time for ^

- ✓ Frame 835: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124},
  - › Interface id: 0 (\Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124})
  - Encapsulation type: Ethernet (1)
  - Arrival Time: Jan 18, 2022 10:53:41.634212000 Eastern Standard Time
  - [Time shift for this packet: 0.000000000 seconds]

Therefore it has taken nearly 00:00:00.0042706 seconds to get the Http Ok

No.	Time	Source	Destination	Protocol	Length	Info
→	833.10.53.41	192.168.2.24	128.119.245.12	HTTP	542	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Source: 192.168.2.24 -> my computer internet address

No.	Time	Source	Destination	Protocol	Length	Info
833	10:53:41.591506	192.168.2.24	128.119.245.12	HTTP	542	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
Frame 833: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF_{BA372CA9-5429-49F8-8456-6EA88AA88124}, id 0						
Ethernet II, Src: HonHaiPr_62:08:ad (d8:9c:67:62:08:ad), Dst: Sagemcom_dc:a5:00 (b8:66:85:dc:a5:00)						
Internet Protocol Version 4, Src: 192.168.2.24, Dst: 128.119.245.12						
Transmission Control Protocol, Src Port: 57221, Dst Port: 80, Seq: 1, Ack: 1, Len: 488						
Hypertext Transfer Protocol						

  

No.	Time	Source	Destination	Protocol	Length	Info
835	10:53:41.634212	128.119.245.12	192.168.2.24	HTTP	492	HTTP/1.1 200 OK (text/html)
Frame 835: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF_{BA372CA9-5429-49F8-8456-6EA88AA88124}, id 0						
Ethernet II, Src: Sagemcom_dc:a5:00 (b8:66:85:dc:a5:00), Dst: HonHaiPr_62:08:ad (d8:9c:67:62:08:ad)						
Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.24						
Transmission Control Protocol, Src Port: 80, Dst Port: 57221, Seq: 1, Ack: 489, Len: 438						
Hypertext Transfer Protocol						
Line-based text data: text/html (3 lines)						

No.	Time	Source	Destination	Protocol	Length	Info
833	10:53:41.591506	192.168.2.24	128.119.245.12	HTTP	542	GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1

Frame 833: 542 bytes on wire (4336 bits), 542 bytes captured (4336 bits) on interface \Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124}, id 0

Ethernet II, Src: HonHaiPr\_62:08:ad (d8:9c:67:62:08:ad), Dst: Sagemcom\_dc:a5:00 (b8:66:85:dc:a5:00)

Internet Protocol Version 4, Src: 192.168.2.24, Dst: 128.119.245.12

Transmission Control Protocol, Src Port: 57221, Dst Port: 80, Seq: 1, Ack: 1, Len: 488

Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
835	10:53:41.634212	128.119.245.12	192.168.2.24	HTTP	492	HTTP/1.1 200 OK (text/html)

Frame 835: 492 bytes on wire (3936 bits), 492 bytes captured (3936 bits) on interface \Device\NPF\_{BA372CA9-5429-49F8-8456-6EA88AA88124}, id 0

Ethernet II, Src: Sagemcom\_dc:a5:00 (b8:66:85:dc:a5:00), Dst: HonHaiPr\_62:08:ad (d8:9c:67:62:08:ad)

Internet Protocol Version 4, Src: 128.119.245.12, Dst: 192.168.2.24

Transmission Control Protocol, Src Port: 80, Dst Port: 57221, Seq: 1, Ack: 489, Len: 438

Hypertext Transfer Protocol

Line-based text data: text/html (3 lines)