

Lab Sheet I5- Analysing HTTP Traffic using Wireshark.

Academic year: 2020-2021

Branch/ Class: B.Tech/M.Tech

Semester: Winter

Date: 05/6/2021

Faculty Name: Dr.HUSSAIN SYED

School: SCOPE

Student name: Hariprasad K K

Reg. no.: I9BCE7079

Analysing HTTP Traffic using Wireshark.




INTRODUCTION TO WIRESHARK:

Home page:

Welcome to Wireshark

Capture

...using this filter:

	Local Area Connection* 11	—
	Local Area Connection* 10	—
	Local Area Connection* 9	—
	Wi-Fi	
	Local Area Connection* 12	—
	Local Area Connection* 3	—
	Adapter for loopback traffic capture	
	Ethernet	—

Packetlist and packet panel:

Lab Sheet I5- Analysing HTTP Traffic using Wireshark.

Academic year: 2020-2021

Branch/ Class: B.Tech/M.Tech

Semester: Winter

Date: 05/6/2021

Faculty Name: Dr.HUSSAIN SYED

School: SCOPE

Student name: Hariprasad K K

Reg. no.: I9BCE7079

No.	Time	Source	Destination	Protocol	Length	Info
9	1.194159	192.168.0.159	13.107.6.171	TLSv1.2	493	Application Data
10	1.194223	192.168.0.159	13.107.6.171	TLSv1.2	2197	Application Data
11	1.215176	13.107.6.171	192.168.0.159	TCP	54	443 → 62682 [ACK] Seq=614 Ack=4825 Min=2851 Len=0
12	1.226263	13.107.6.171	192.168.0.159	TCP	54	443 → 62682 [ACK] Seq=614 Ack=6168 Min=2850 Len=0
13	1.231196	13.107.6.171	192.168.0.159	TLSv1.2	486	Application Data
14	1.231196	13.107.6.171	192.168.0.159	TLSv1.2	92	Application Data
15	1.231276	192.168.0.159	13.107.6.171	TCP	54	62682 → 443 [ACK] Seq=6168 Ack=1084 Min=513 Len=0
16	1.348778	192.168.0.159	52.111.252.2	TLSv1.2	83	Application Data
17	1.393412	52.111.252.2	192.168.0.159	TLSv1.2	79	Application Data
18	1.443147	192.168.0.159	52.111.252.2	TCP	54	56993 → 443 [ACK] Seq=38 Ack=26 Min=517 Len=0
19	1.445280	192.168.0.159	239.255.255.250	SSDP	169	M-SEARCH * HTTP/1.1
20	2.297601	52.111.252.0	192.168.0.159	TLSv1.2	105	Application Data
21	2.352106	192.168.0.159	52.111.252.0	TCP	54	62498 → 443 [ACK] Seq=1 Ack=52 Min=516 Len=0
22	2.353932	192.168.0.159	13.107.6.171	TLSv1.2	186	Application Data
23	2.354014	192.168.0.159	13.107.6.171	TLSv1.2	100	Application Data
24	2.373442	13.107.6.171	192.168.0.159	TCP	54	443 → 57877 [ACK] Seq=1 Ack=133 Min=2852 Len=0
25	2.373442	13.107.6.171	192.168.0.159	TCP	54	443 → 57877 [ACK] Seq=1 Ack=179 Min=2852 Len=0
26	2.373442	13.107.6.171	192.168.0.159	TLSv1.2	180	Application Data

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{62574751-2A64-458D-899F-4A31648481A7}, id 0
> Ethernet II, Src: D-LinkIn_61:84:73 (f0:b4:d2:61:84:73), Dst: IntelCor_9a:5b:e6 (d8:f8:83:9a:5b:e6)
> Internet Protocol Version 4, Src: 13.107.6.171, Dst: 192.168.0.159
> Transmission Control Protocol, Src Port: 443, Dst Port: 62682, Seq: 1, Ack: 1, Len: 38
> Transport Layer Security

Packetbytes panel:

> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{62574751-2A64-458D-899F-4A31648481A7}, id 0		
> Ethernet II, Src: D-LinkIn_61:84:73 (f0:b4:d2:61:84:73), Dst: IntelCor_9a:5b:e6 (d8:f8:83:9a:5b:e6)		
> Internet Protocol Version 4, Src: 13.107.6.171, Dst: 192.168.0.159		
> Transmission Control Protocol, Src Port: 443, Dst Port: 62682, Seq: 1, Ack: 1, Len: 38		
> Transport Layer Security		

0000	d8 f8 83 9a 5b e6 f0 b4 d2 61 84 73 08 00 45 00a.s..E
0010	00 4e 81 74 40 08 75 06 2e d9 0b 0b 0b 0b c0 a8	..N.t@u...k..
0020	00 9f 81 bb f4 8a 40 1c d1 7b c2 f6 b7 0c 50 18@...[...P
0030	00 05 23 81 00 00 17 03 03 00 21 00 00 00 00 00	..#.....!.....
0040	00 06 19 1d d8 ad 7e 37 c5 08 d3 6a 03 8a a4 d57...j.....
0050	23 f6 aa f3 82 a6 cd c2 12 b9 96 f7#.....

ANALYSING OF HTTPUSING WIRESHARK:

1. Before starting http analysis run the Wireshark.
2. Go to options in capture menu and filter the capture to tcp port http, also enable the promiscuous mode.
3. Open any browser and search for anything.
4. This will send the http request.

Lab Sheet I5- Analysing HTTP Traffic using Wireshark.

Academic year: 2020-2021

Branch/ Class: B.Tech/M.Tech

Semester: Winter

Date: 05/6/2021

Faculty Name: Dr.HUSSAIN SYED

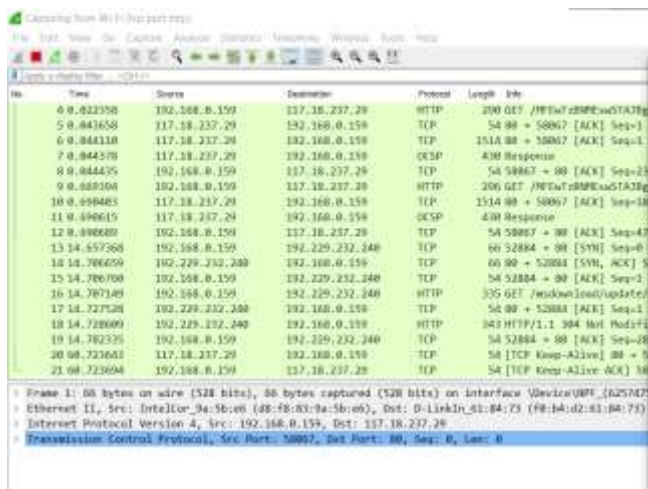
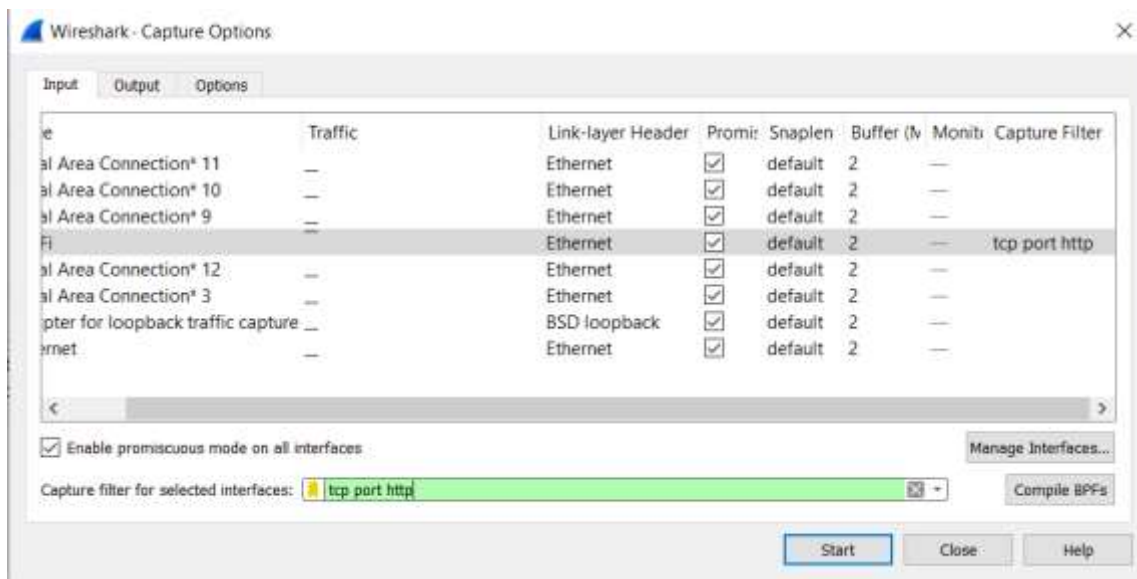
School: SCOPE

Student name: Hariprasad K K

Reg. no.: I9BCE7079

5. Wireshark tracks every request which is sent through the http.
6. Use display filter to show only http information.
7. We can keep track of particular ip also.

OBSERVATION:



Lab Sheet I5- Analysing HTTP Traffic using Wireshark.

Academic year: 2020-2021

Branch/ Class: B.Tech/M.Tech

Semester: Winter

Date: 05/6/2021

Faculty Name: Dr.HUSSAIN SYED

School: SCOPE

Student name: Hariprasad K K

Reg. no.: I9BCE7079

No.	Time	Source	Destination	Protocol	Length	Info
7	0.044370	117.18.237.29	192.168.0.159	OSCP	430	Response
8	0.044435	192.168.0.159	117.18.237.29	TCP	54	58067 → 80 [ACK] Seq=237 Ack=1837 Win=131328 Len=0
9	0.669394	192.168.0.159	117.18.237.29	HTTP	296	GET /PFEwTzBWEsw5TAJ8gvGpGgUABBTBL0V278VZ7L8duo02FcyB455PUEwQJ5Z12H1H4PyxX28ghUhcZ70v4E
10	0.690403	117.18.237.29	192.168.0.159	TCP	1514	80 → 58067 [ACK] Seq=1837 Ack=479 Win=68096 Len=1460 [TCP segment of a reassembled PDU]
11	0.690615	117.18.237.29	192.168.0.159	OSCP	430	Response
12	0.690689	192.168.0.159	117.18.237.29	TCP	54	58067 → 80 [ACK] Seq=479 Ack=3673 Win=131328 Len=0
13	14.657368	192.168.0.159	192.229.232.240	TCP	66	52884 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	14.706659	192.229.232.240	192.168.0.159	TCP	66	80 → 52884 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
15	14.706760	192.168.0.159	192.229.232.240	TCP	54	52884 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
16	14.707149	192.168.0.159	192.229.232.240	HTTP	335	GET /msdownload/update/v3/static/trusted/en/authrootst1.cab?8053ef223027692f HTTP/1.1
17	14.727529	192.229.232.240	192.168.0.159	TCP	54	80 → 52884 [ACK] Seq=1 Ack=282 Win=67072 Len=0
18	14.728609	192.229.232.240	192.168.0.159	HTTP	343	HTTP/1.1 304 Not Modified
19	14.782335	192.168.0.159	192.229.232.240	TCP	54	52884 → 80 [ACK] Seq=282 Ack=200 Win=131072 Len=0
20	60.723043	117.18.237.29	192.168.0.159	TCP	54	[TCP Keep-Alive] 80 → 58067 [ACK] Seq=3672 Ack=479 Win=68096 Len=0
21	60.723054	192.168.0.159	117.18.237.29	TCP	54	[TCP Keep-Alive ACK] 58067 → 80 [ACK] Seq=479 Ack=3673 Win=131328 Len=0
22	74.730410	192.168.0.159	192.229.232.240	TCP	54	52884 → 80 [FIN, ACK] Seq=282 Ack=290 Win=131072 Len=0
23	74.752311	192.229.232.240	192.168.0.159	TCP	54	80 → 52884 [FIN, ACK] Seq=290 Ack=283 Win=67072 Len=0
24	74.752381	192.168.0.159	192.229.232.240	TCP	54	52884 → 80 [ACK] Seq=283 Ack=291 Win=131072 Len=0

Frame 11: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 'Device\NPF_{62574751-2A64-45B0-899F-4A3164B481A7}', id 0
Ethernet II, Src: IntelCor_9a:5b:a6 (d8:f8:b3:9a:5b:a6), Dst: D-linkIn_01:84:73 (f0:b4:d2:61:84:73)
Internet Protocol Version 4, Src: 192.168.0.159, Dst: 117.18.237.29
Transmission Control Protocol, Src Port: 58067, Dst Port: 80, Seq: 0, Len: 0

No.	Time	Source	Destination	Protocol	Length	Info
http2	0.022358	192.168.0.159	117.18.237.29	HTTP	296	GET /PFEwTzBWEsw5TAJ8gvGpGgUABBTBL0V278VZ7L8duo02FcyB455PUEwQJ5Z12H1H4PyxX28ghUhcZ70v4E
http2	0.044370	117.18.237.29	192.168.0.159	OSCP	430	Response
http3	0.669394	192.168.0.159	117.18.237.29	HTTP	296	GET /PFEwTzBWEsw5TAJ8gvGpGgUABBTBL0V278VZ7L8duo02FcyB455PUEwQJ5Z12H1H4PyxX28ghUhcZ70v4E
	0.690615	117.18.237.29	192.168.0.159	OSCP	430	Response
	16.14.707149	192.168.0.159	192.229.232.240	HTTP	335	GET /msdownload/update/v3/static/trusted/en/authrootst1.cab?8053ef223027692f HTTP/1.1
	18.14.728609	192.229.232.240	192.168.0.159	HTTP	343	HTTP/1.1 304 Not Modified

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.159	117.18.237.29	TCP	66	58067 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.021820	117.18.237.29	192.168.0.159	TCP	66	80 → 58067 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
3	0.021923	192.168.0.159	117.18.237.29	TCP	54	58067 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
4	0.022358	192.168.0.159	117.18.237.29	HTTP	296	GET /PFEwTzBWEsw5TAJ8gvGpGgUABBTBL0V278VZ7L8duo02FcyB455PUEwQJ5Z12H1H4PyxX28ghUhcZ70v4E
5	0.043658	117.18.237.29	192.168.0.159	TCP	54	80 → 58067 [ACK] Seq=1 Ack=237 Win=67072 Len=0
6	0.044110	117.18.237.29	192.168.0.159	TCP	1514	80 → 58067 [ACK] Seq=1 Ack=237 Win=67072 Len=1460 [TCP segment of a reassembled PDU]
7	0.044370	117.18.237.29	192.168.0.159	OSCP	430	Response
8	0.044435	192.168.0.159	117.18.237.29	TCP	54	58067 → 80 [ACK] Seq=237 Ack=1837 Win=131328 Len=0
9	0.669394	192.168.0.159	117.18.237.29	HTTP	296	GET /PFEwTzBWEsw5TAJ8gvGpGgUABBTBL0V278VZ7L8duo02FcyB455PUEwQJ5Z12H1H4PyxX28ghUhcZ70v4E
10	0.690403	117.18.237.29	192.168.0.159	TCP	1514	80 → 58067 [ACK] Seq=1837 Ack=479 Win=68096 Len=1460 [TCP segment of a reassembled PDU]
11	0.690615	117.18.237.29	192.168.0.159	OSCP	430	Response
12	0.690689	192.168.0.159	117.18.237.29	TCP	54	58067 → 80 [ACK] Seq=479 Ack=3673 Win=131328 Len=0
13	14.657368	192.168.0.159	192.229.232.240	TCP	66	52884 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
14	14.706659	192.229.232.240	192.168.0.159	TCP	66	80 → 52884 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1 WS=512
15	14.706760	192.168.0.159	192.229.232.240	TCP	54	52884 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0
16	14.707149	192.168.0.159	192.229.232.240	HTTP	335	GET /msdownload/update/v3/static/trusted/en/authrootst1.cab?8053ef223027692f HTTP/1.1
17	14.727529	192.229.232.240	192.168.0.159	TCP	54	80 → 52884 [ACK] Seq=1 Ack=282 Win=67072 Len=0
18	14.728609	192.229.232.240	192.168.0.159	HTTP	343	HTTP/1.1 304 Not Modified