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.: 19BCE7079

Analysing HTTP Traffic using Wireshark.

INTRODUCTION TO WIRESHARK:

Home page:

Welcome to Wireshark	
Capture	
using this filter: 📕 Enter a capture filter	
Local Area Connection* 11	_
Local Area Connection* 10 Local Area Connection* 9	_
Wi-Fi	<u></u>
Local Area Connection* 12 Local Area Connection* 3	
Adapter for loopback traffic capture	, <u>~</u>
Ethernet	

Packetlist and packet panel:

Branch/ Class: B. Tech/M. Tech Academic year: 2020-2021

Date: 05/6/2021 Semester: Winter

Faculty Name: Dr.HUSSAIN SYED School: SCOPE

Student name: Hariprasad K K Reg. no.: 19BCE7079

Time.	Seurce	Destriation	Protocet	Langth 34%
9-1.194159	192.168.0.159	13.107.6.171	TL5V1.2	493 Application Data
10 1 194223	192,168,0,159	13.107.6.171	11.5v1.2	2197 Application Data
11 1.215176	13.107.6.171	192,168.0,159	TCP	54 443 + 62682 [ACK] 5eq:614 Ack:4025 Win=2851 Len:8
12 1, 226263	13,107,6,171	192,168.0,159	TCP	54 443 + 62682 [ACK] Seq-614 Ack-6168 Win-2858 Len-8
13 1.231196	13.107.6.171	192.168.0.159	TL5v1.2	486 Application Data
14 1.211196	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 62602 + 443 [ACK] Seq=6168 Ack=1884 Win=513 Len=8
16 1.348778	192,168,8,159	52.111.252.2	TLSv1.2	83 Application Data
17 1.393412	52,111,252,2	192,168,0,159	TL5v1.2	79 Application Data
18 1.443347	192,168,0,159	52.111.252.2	TCP	54 56993 + 443 [ACK] Seq=38 Ack=26 Win=517 Len=8
19 2 145280	197,168,0,196	239,255,255,258	SSDP	169 N-SEARCH * HTTP/1.1
20 2.297681	52,111,252.0	192.168.0.159	TL5v1.2	105 Application Data
21 2.352196	192,168,8,159	52,111,252.0	TCP	54 62498 + 443 [ACK] Seq=1 Ack=52 Win=516 Len=0
22 2.353932	192,168,0,159	13,107.6,171	TL5v1.2	186 Application Data
23 2-354014	192,168,0,159	13.107.6.171	TLSv1.2	100 Application Data
24 2.173442	13.107.6.171	192,168,0.159	TCP	54 443 + 57877 [ACK] Seg=1 Ack=133 Min=2852 Len=8
25 2.373442	13, 107, 6, 171	192.168.0.159	TCP	54 443 + 57877 [ACK] Seg=1 Ack=179 Min=2852 Len=0
26 2 373442	13.107.6.171	192,168,0,159	TLSv1.2	100 Application Data

- Ethernet II, Src: D-LinkIn_61:84:73 (f0:b4:d2:61:84:73), Det: IntelCor_9a:5b:e6 (d8:f8:83:9a:5b:e6)
- Internet Protocol Version 4, Src: 13.107.6.171, Ost: 192.168.0.159
 Transmission Control Protocol, Src Port: 443, Ost Port: 62682, Seq: 1, Ack: 1, Lem: 38
- Transport Layer Security

Packetbytes panel:

```
> Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\APF_(62574751-2A64-458D-899F-AA31648481A7), id 0 Ethernet II, Src: 0-LinkIn_61:84:73 (f6:b4:d2:61:84:73), Ost: 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

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.

Academic year: 2020-2021 Branch/ Class: B.Tech/M.Tech

Semester: Winter Date: 05/6/2021

Faculty Name: Dr. HUSSAIN SYED School: SCOPE

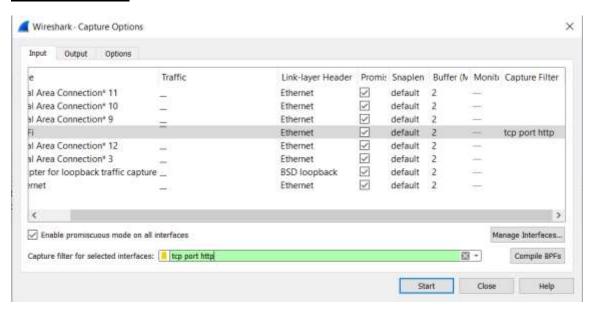
Student name: Hariprasad K K Reg. no.: 19BCE7079

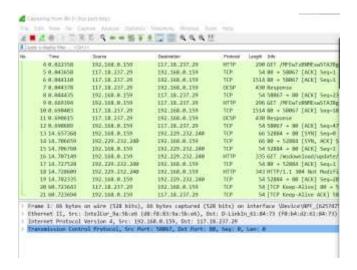
5. Wireshark tracks every request which is sent through the http.

6. Use display filter to show only http information.

7. We can keep track of particular ip also.

OBSERVATION:





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.: 19BCE7079

Titre	bouns	Destination	Protocol	Longth - Info
7 8.844378	117,18,237,29	192.268.8.159	0050	438 Response
8 8 844435	192,168,0,159	117, 18, 237, 29	TCP	54 58067 + 80 [AOK] Seq-227 Ack-1837 Win-171328 Lm-8
9 0.609394	192,100.0.150	117,18,237,29	HETP	200 GET /PET-MYSTATINGU-OGECGGUARITEG/92/WYZYLINA-SEZE-MMSSPULAGUSZTZEH HARY-\$22ghun-270
10.0.090403	117,18,237,29	192,168,8,159	TCP	1518 88 + 58067 [ACK] Seq-1837 Ack-479 Win-68096 Len-1400 [TCP segment of a reassembled FDN]
11.0.698615	11,7,18,237,25	192.168.6.159	0058	438 Response
12 0.690680	192,168.8.259	117,18,237.29	TCP.	54 58067 = 80 [ACK] 5eq=470 Ack>3671 Win=131328 Len=0
13 14.657368	192,168,0,159	192.229.212.240	TCP	06 12884 + 80 [579] Sequil Minu64240 Limin MS5-2000 MS5-250 SACK_PERFAIL
14.14,706659	192,229,232,248	192.168.8.159	TEP	86 88 + 52884 [SYN, ACK] Seq-8 Ack-1 W1n-65535 Len-8 PSS-1468 SACK_PSBM-1 WS-512
15 14,786768	192.168.0.159	192,229,232,240	TCP	54 52884 + 88 [ACK] Seg=1 Ack=1 Win=131328 Lm=8
16 14.797169	102,168,0.159	197, 229, 212, 200	HETP	IDS GET /mmbsecload/update/v3/static/trustedr/en/authroptstl.cab78053ef223027602F HTTP/L.I
17 14 727529	192.229.232.248	192.368.8.159	TEP	54 88 + 52884 [ACK] Seq=1 Ack=282 Win=67072 Len=0
18 14,728609	197, 229, 232, 248	192.168.8.159	HITTE	343 9TTP/1.1 364 Not Modified
19 14,782335	192,168,0,159	192, 229, 232, 340	TCP	54 52884 + 80 [ACK] 5eq=282 Ack=200 Min=131072 Lan=0
20 60.723943	117.18.237.29	192.168.8.159	TEP	54 (TCP Keep-Alive) 88 + 38907 (ACK) Sequings Acked79 Winnessen Lenne
25.69.723694	192.168.0.159	117,18,237,29	TCP	54 (TCP Keep-Alive ACE) 58867 + 80 (ACE) 5eq-479 Ack-3673 Win-131328 Len-0
22 74.738418	192,168,0,159	192.229.232.240	TCP	54 52884 + 80 [FIN, AIN] Seq-202 Ack-200 Win-131072 Len-0
23.74.752311	102,220,232,248	192,188,8,199	TEP	54 88 + 52854 [FIN, ACK] Seq:290 Acks263 Winni2072 Lenot
24.74.752301	392,368,8,359	192,229,232,268	TEP	54 52884 + 88 (ACK) Seq-283 Ack-291 Win-131872 LenuB

in.	MID		South	Destruction	Protecti	Langiti 3rlo
	http2	\$2235B	192,168,8,159	117,38,337,29	HTTP	298-EET / MEEUT 2898E out TAJBgot-tight right right 1912/99/17/16/10/09/19/15/99/99/12/90/17/12/90
	httpI	34370	117.18.237.29	192,168,0,159	OCSP	438 Response
	9.8	669394	192,168,8,159	117.18.237.29	HITP	296 GET /MFEWT28WEEwSTA38gorOgPCfigU88BT8L0V27RVZ7LBduox82FxY9455P0EvQU5Z12M2348Pys\$28g98MoZ
	11.0	690615	317, 18, 297, 29	192,168.8.159	0057	A10 Response
	16:1	4.707149	192,168.8,139	192,229,232,240	HITP	335 6E7 /msdownload/update/v3/static/trustedr/en/authroatst1.coh/8853ef223027692f HTTP/1.1
	18 1/	4.728609	192,229,232,248	192.168.0.159	HITP	343 HTTP/1.1 364 Not Modified

D pos	mm+100.000.015W	2000	200111-00		
No.	Time	Source	Destination	Phylocol	Lungth Sels
	1 0.000000	192,168,0,159	117.18.237,29	ECP	66 58867 = 88 [SYN] Seq=0 Win-64240 Len=0 PES=1460 WS=256 5ACK_PERM=1
	2 0.021828	117,18,237,28	192.168.0.139	ECH	66 80 + 18067 [SYN, ACK] Sego0 Acks1 Wins65515 Lemn8 MSS-1460 SACK_PIND-1 WS-512
	1 0.021921	192.108.0.150	117, 18, 277, 29	14h	34 58867 + 88 (AEK) Segul Ackul Minulliliza Lenu8
+	4.6.022358	192,168,0,159	117, 18, 217, 29	HTTP	290 GET //FEWT2DPESIGTA)Rgsv0g/K.6gsABETRUNV27RVZ7LBio.comTFFcW84SSPJExQUSZ12RT1HaPyST28gsURicZ7Dru
	5 8.843658	117_18.237,29	192,168,8,159	TCP	54 88 * 58867 [ACK] Seq=1 Ack=237 Win+67872 Len=8
	6.0.044110	117.18.237.29	102.168.0.150	TEP	1514 BB + 58067 [ACK] Seq:1 Ack:217 Winen7072 Lenc1468 [YEP segment of a reasonabled PDB]
+	7 0 201378	117.18.237.29	192.168.0.159	DESF	438 Response
	8 0.044435	192.168.0.150	117.18.237.29	TCP	54 58967 + 88 (ACK) Seq-237 Ack-1837 Win-131128 Len-8
+.	9.0.669394	192,168,0,159	117.18.237.29	HITP	296-GET /MEEuTzBRMEsviSTA3Bg0xGgMCGgURBETBLBV27RVZ7LBdvonB2FeV845SPUEvQUSZ12RL3HiBHyCK28gruRuZ7DvU
	10.0.600403	117,18,237,29	282.168.6.158	ECP	1514 88 + 58967 [ACK] Seq-1837 Ack+479 Min-68896 Lan-1468 [TCP segment of a reassembled PDU]
	11 9.000615	117.10.217.29	192.166.0.150	OCSP	A10 Response
	12 0 699689	192,169,9,159	117.18.237.29	TCP	54 58867 + 88 [ADK] Seg-479 Ack-3673 Min-131328 Len-8
	17 14:657368	192,168,0,150	192.229.237.249	TEP	66 52884 + 80 [SYN] Seq-0 Min-64240 Len-0 PSS-1460 MS-256 SACK PERM-1
	14 14,786659	192,229,232,240	192,168.0.159	TCP	66 60 + 52884 [SVN, ACK] Seq=0 Ach=1 Min=65535 Lam=0 MSS=1460 SACK_PERM=1 MS=512
	13 14,706768	102,168,0,158	102.229.212.288	TEP	54 52884 + BF (ACK) Sequi Acksi Winsillian Lense
	16 14 707149	292,108,0,150	192.229.232.248	WITH	335 SET /msdownload/update/v3/static/trustedr/en/authrootstl.cab/9053ef223027692f HTTP/1.1
	17 14,727528	192, 229, 232, 240	192.168.0.158	ECP	54 88 + 52884 [ACK] Seq-1 Ack-282 Win-67072 Len-0
	18 14,728669	192, 229, 232, 240	192,168,6,159	HTTP	343 HTTP/1.1 304 Mut Hodified