

Xuan(James) Zhai

CS3339 Lab

March 19<sup>th</sup>, 2021

## CS 3339 - Lab 5 - Lab Report

1: Carefully read the lab instructions and finish all tasks above. Attach screenshots to your report for steps 7, 8 and 10.

http.host==faculty.smu.edu						
No.	Time	Source	Destination	Protocol	Length	Info
18	4.101888	192.168.43.228	129.119.70.31	HTTP	1080	GET /csc/documentation/ HTTP/1.1
> Frame 18: 1080 bytes on wire (8640 bits), 1080 bytes captured (8640 bits) on interface \Device\NPF_{2FC289F9-F168-44E > Ethernet II, Src: Apple_ee:02:6c (48:bf:6b:ee:02:6c), Dst: Fn-LinkT_2c:8d:69 (58:63:56:2c:8d:69) > Internet Protocol Version 4, Src: 192.168.43.228, Dst: 129.119.70.31 > Transmission Control Protocol, Src Port: 12165, Dst Port: 80, Seq: 1, Ack: 1, Len: 1026 > Hypertext Transfer Protocol						
0000	58 63 56 2c 8d 69 48 bf	6b ee 02 6c 08 00 45 00	XcV, .iH. k..1..E.			
0010	04 2a 44 a4 40 00 80 06	fe 06 c0 a8 2b e4 81 77	.*D.@... ..+..w			
0020	46 1f 2f 85 00 50 2f 0c	fb ee d0 37 d0 00 50 18	F-/..P/. ...7..P.			
0030	01 fc fe 3d 00 00 47 45	54 20 2f 63 73 63 2f 64	....-GE T /csc/d			
0040	6f 63 75 6d 65 6e 74 61	74 69 6f 6e 2f 20 48 54	ocumenta tion/ HT			
0050	54 50 2f 31 2e 31 0d 0a	48 6f 73 74 3a 20 66 61	TP/1.1.. Host: fa			
0060	63 75 6c 74 79 2e 73 6d	75 2e 65 64 75 0d 0a 43	culty.sm u.edu..C			
0070	6f 6e 6e 65 63 74 69 6f	6e 3a 20 6b 65 65 70 2d	onnectio n: keep-			
0080	61 6c 69 76 65 0d 0a 43	61 63 68 65 2d 43 6f 6e	alive..C ache-Con			
0090	74 72 6f 6c 3a 20 6d 61	78 2d 61 67 65 3d 30 0d	trol: ma x-age=0.			
00a0	0a 55 70 67 72 61 64 65	2d 49 6e 73 65 63 75 72	.Upgrade -Insecur			
00b0	65 2d 52 65 71 75 65 73	74 73 3a 20 31 0d 0a 55	e-Request: 1..U			
00c0	73 65 72 2d 41 67 65 6e	74 3a 20 4d 6f 7a 69 6c	ser-Agen t: Mozil			

Fig 1: http.host==faculty.smu.edu

No.	Time	Source	Destination	Protocol	Length	Info
19	4.103347	192.168.43.228	192.168.43.1	DNS	80	Standard query 0xf82a A fonts.googleapis.com
30	4.160859	192.168.43.1	192.168.43.228	DNS	96	Standard query response 0xf82a A fonts.googleapis.com A 74.125.200.95
101	4.959848	192.168.43.228	192.168.43.1	DNS	71	Standard query 0x6a69 A idp.smu.edu
102	5.220307	192.168.43.228	192.168.43.1	DNS	71	Standard query 0x6a69 A idp.smu.edu
103	5.477399	192.168.43.1	192.168.43.228	DNS	246	Standard query response 0x6a69 A idp.smu.edu CNAME sdars197.systems.sm

  

```

> Frame 19: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface \Device\NPF_{2FC289F9-F168-44EC-8C64-650D101240FF}, id 0
> Ethernet II, Src: Apple_ee:02:6c (48:bf:6b:ee:02:6c), Dst: Fn-LinkT_2c:8d:69 (58:63:56:2c:8d:69)
> Internet Protocol Version 4, Src: 192.168.43.228, Dst: 192.168.43.1
> User Datagram Protocol, Src Port: 59058, Dst Port: 53
> Domain Name System (query)

```

  

```

0000  58 63 56 2c 8d 69 48 bf 6b ee 02 6c 08 00 45 00  XcV, iH- k--1..E-
0010  00 42 c2 53 00 00 80 11 a0 21 c0 a8 2b e4 c0 a8  :B.S....:!.+...
0020  2b 01 e6 b2 00 35 00 2e 63 7d f8 2a 01 00 00 01  +----5..c).*....
0030  00 00 00 00 00 05 66 6f 6e 74 73 0a 67 6f 6f  ....f onts goo
0040  67 6c 65 61 70 69 73 03 63 6f 6d 00 00 01 00 01  gleapis- com.....

```

Fig 2: DNS

```

Wireshark · Follow TCP Stream (tcp.stream eq 8) · WLAN

GET /csc/documentation/ HTTP/1.1
Host: faculty.smu.edu
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.82 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en-US;q=0.8,en;q=0.7,zh-TW;q=0.6
Cookie: __ga=GA1.2.2031369866.1516321303; __vwo_uuid=D290A8137CABE571B20B1CC78F797FA7A; __qca=P0-994421879-1583526253434; _hjid=dda06627-f9b6-4f55-abb9-bfb373ea43ea; _gcl_au=1.1.1938856854.1613220329; __rdt_uuid=1614767845812.2b3a7bb4-0a3f-47ce-bc98-744875b5509f; _fbp=fb.1.1614767846266.1499836726; _sctr=1|1614700800000; _gid=GA1.2.381871773.1615311867; mysmu-8000-PORTAL-PSJSESSIONID=XponZMRBCJ1Iuzexc1n-lvUGbXqtoqBxI-1821023107
If-None-Match: "28ff2f35e815d71:0"
If-Modified-Since: Wed, 10 Mar 2021 20:01:49 GMT

HTTP/1.1 304 Not Modified
Accept-Ranges: bytes
ETag: "28ff2f35e815d71:0"
Server: Microsoft-IIS/8.5
X-Powered-By: ASP.NET
Date: Fri, 12 Mar 2021 20:01:31 GMT

```

Fig 3: TCP Stream

2: If a packet is highlighted by black, what does it mean for the packet?

If a packet is highlighted by black, it means that the TCP packets may have some problem. For example, they could have been delivered out of order.

3: What is the filter command for listing all outgoing http traffic?

Only type “http”.

#### 4: Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?

Compared to TCP Stream, UDP Stream is much faster. Also, DNS requests are generally very small, and they fit well within UDP segments. For HTTP requests, it requires reliable delivery, so it needs TCP Stream which has a three-way handshake and the re-transmission of lost packets.

#### 5: Using Wireshark to capture the FTP password. Explain how you found the password and attach a screenshot of the password packet. How could we have prevented sending the FTP login credentials in plain text over the network?

125	13.636593	192.168.43.228	66.220.9.50	FTP	70 Request: USER smucs3339
126	13.821806	66.220.9.50	192.168.43.228	FTP	88 Response: 331 User name ok, need password.
127	13.821877	192.168.43.228	66.220.9.50	TCP	54 12868 → 21 [ACK] Seq=17 Ack=219 Win=261888 Len=0
128	13.821984	192.168.43.228	66.220.9.50	FTP	76 Request: PASS @raBm95z9QRH7X8
129	14.004484	66.220.9.50	192.168.43.228	FTP	130 Response: 230 User smucs3339 logged on. Free service has restrictions and is slower.
130	14.004632	192.168.43.228	66.220.9.50	TCP	54 12868 → 21 [ACK] Seq=39 Ack=295 Win=261632 Len=0
131	14.006423	192.168.43.228	66.220.9.50	FTP	68 Request: opts utf8 on
132	14.184592	66.220.9.50	192.168.43.228	FTP	77 Response: 200 Enable UTF8 mode.
133	14.184736	192.168.43.228	66.220.9.50	TCP	54 12868 → 21 [ACK] Seq=53 Ack=318 Win=261632 Len=0
134	14.184966	192.168.43.228	66.220.9.50	FTP	60 Request: CWD

  

Frame 128: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF\_{2FC289F9-F168-44EC-8C64-650D101240FF}, id 0  
 Ethernet II, Src: Apple\_ee:02:6c (48:bf:6b:ee:02:6c), Dst: Fn-LinkT\_2c:8d:69 (58:63:56:2c:8d:69)  
 Internet Protocol Version 4, Src: 192.168.43.228, Dst: 66.220.9.50  
 Transmission Control Protocol, Src Port: 12868, Dst Port: 21, Seq: 17, Ack: 219, Len: 22  
 File Transfer Protocol (FTP)  
 Current working directory: ]

  

0	58 63 56 2c 8d 69 48 bf	6b ee 02 6c 08 00 45 00	XcV, .iH: k...I..E.
0	00 3e 67 0b 40 00 80 06	5b 14 c0 a8 2b e4 42 dc	..>g:@... [....+B.
0	09 32 32 44 00 15 a8 24	5f b4 92 ac c2 d2 50 18	..22D...\$ ..-...P.
0	03 ff b8 8d 00 00 50 41	53 53 20 40 72 61 42 6d	.....PA SS @raBm
0	39 35 7a 39 51 52 48 37	58 38 0d 0a	95z9QRH7 X8..

Fig 4: FTP Password

From the graph about we can find out that Wireshark captured the FTP request and response with server name, username, and password. To prevent a potential password leak, we could hash the password with salt to make it be unable to interpret, we could even hash the username to make more confusion.