Computer Networks Lab 3 CS F303

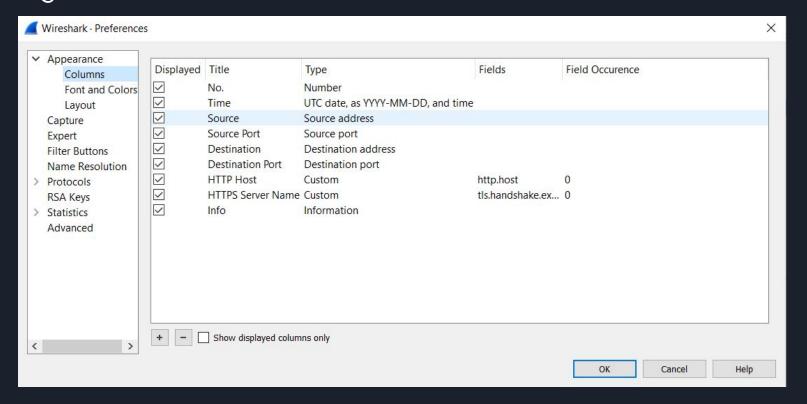
Question 1

Q1. Customize your Wireshark - (6 marks)

Generally, WireShark columns are arranged in the following order (which you can observe on your machine) - No., Time, Source, Destination, Protocol, Length. etc. Being a security expert you have to arrange the WireShark display in such a way that it must have only the following items (1 mark per correct display item with the correct filter/field value and a screenshot).

- a. Date & time in UTC
- b. Source IP and source port
- c. Destination IP and destination port
- d. HTTP host
- e. HTTPS server
- f. Info

Names and fields of columns used to answer O1



Question 2

Q2. Wireshark dump analysis - (24 marks)

Using the given Lab3-Q2.pcapng, file answer the following questions. You have to write down the filter you have used (2 marks) and attach a screenshot and explain your output (2 marks).

- a. Identify the http request packet
- b. Identify the http response packet
- c. Display the statistics of the TCP and UDP packets
- d. List out the TCP packets whose syn. and ack. Flags are on.
- e. List out the TCP and UDP packets where destination port=80.
- f. List out the ARP packets.

a. Identify the http request packet

Use the command: http.request

Some columns are omitted from the screenshot due to clarity issues.

This command lists all the packets which were requested from the server by the client using http

http	http.request											
No.	^	Time	Source	Source Port	Destination	Destination Port	HTTP Host	Н				
	12925	2021-02-04 13:28:04.992277	10.4.8.21	64886	239.255.255.250	1900	239.255.255.25					
	13363	2021-02-04 13:28:05.992728	10.4.8.21	64886	239.255.255.250	1900	239.255.255.25					
	14607	2021-02-04 13:28:10.605111	10.4.8.18	50698	172.217.166.46	80	redirector.gvt					
	14625	2021-02-04 13:28:10.749730	10.4.8.18	50699	49.44.83.143	80	r4sn-gwpa-c	• 0				
	14629	2021-02-04 13:28:10.814373	10.4.8.18	50698	172.217.166.46	80	redirector.gvt					
	14633	2021-02-04 13:28:10.916725	10.4.8.18	50699	49.44.83.143	80	r4sn-gwpa-c	. j				
	14637	2021-02-04 13:28:11.019258	10.4.8.18	50698	172.217.166.46	80	redirector.gvt					
	14657	2021-02-04 13:28:11.125763	10.4.8.18	50699	49.44.83.143	80	r4sn-gwpa-c					
	14665	2021-02-04 13:28:11.173746	10.4.8.18	50698	172.217.166.46	80	redirector.gvt					
<												

a. Identify the http response packet

Use the command: http.response

Some columns are omitted from the screenshot due to clarity issues.

This command lists all the packets which were sent to the server by the client using http

	http.respo	nse					http.response										
No).	Time	^	Source	Source Port	Destination	Destination Port										
4	14618	2021-02-04	13:28:10.747872	172.217.166.46	80	10.4.8.18	50698										
1	14628	2021-02-04	13:28:10.813041	49.44.83.143	80	10.4.8.18	50699										
+	14632	2021-02-04	13:28:10.915961	172.217.166.46	80	10.4.8.18	50698										
1	14636	2021-02-04	13:28:11.009340	49.44.83.143	80	10.4.8.18	50699										
	14656	2021-02-04	13:28:11.124053	172.217.166.46	80	10.4.8.18	50698										
1	14664	2021-02-04	13:28:11.172517	49.44.83.143	80	10.4.8.18	50699										
	14668	2021-02-04	13:28:11.275708	172.217.166.46	80	10.4.8.18	50698										
1	14672	2021-02-04	13:28:11.351582	49.44.83.143	80	10.4.8.18	50699										
	14676	2021-02-04	13:28:11.467130	172.217.166.46	80	10.4.8.18	50698										
1	14679	2021-02-04	13:28:11.500668	49.44.83.143	80	10.4.8.18	50699										
	14683	2021-02-04	13:28:11.603436	172.217.166.46	80	10.4.8.18	50698										
<																	

c. Display the statistics of the TCP and UDP packets

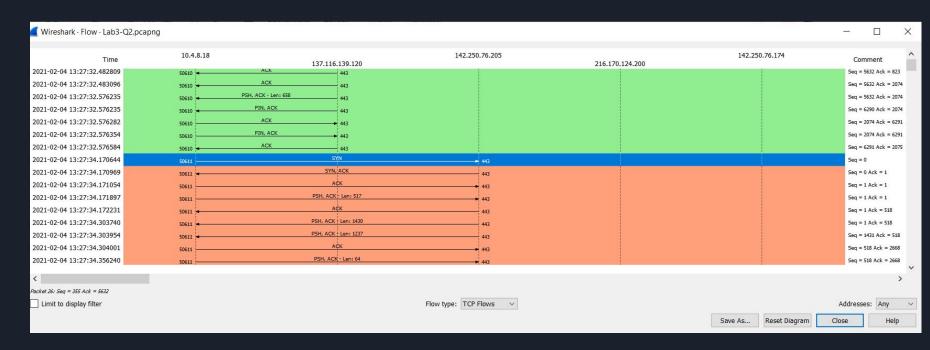
From the statistics tab, we can get the flow graph with the tcp filter which describes the tcp packets. We can also use the Protocol Hierarchy Statistics to see the statistics of tcp packets. This option too is under the statistics tab of the wireshark app.

From the statistics tab, we can also get the UDP multicast streams which shows the source and destination addresses and ports, average bandwidth, packets, packets/sec and other statistics

Images are on next two pages

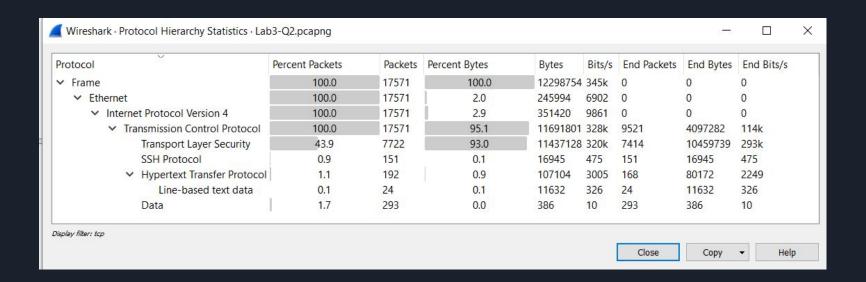
TCP statistics I:

This is the flow graph which describes all the flags as statistics in comment tab and gives source and destination addresses and port numbers.



TCP Statistics II:

This is the Protocol Hierarchy Statistics with the tcp filter. It shows stats like size, speed of transfer and number of packets



UDP statistics: UDP Multicast Streams

✓ Wireshark · UDP Multicast St	reams · Lab3-Q2.pcapng									-	□ ×
Source Address	Source Port Destination Address	Destination Port	Packets	Packets/s	Avg BW (bps)	Max BW (bps)	Max Burst	Burst Alarms	Max Buffers (B)	Buff	fer Alarms ^
fe80::754f:9028:b446:2673	5353 ff02::fb	5353	38	0.14	100	15k	2 / 100ms	0	90		0
fe80::754f:9028:b446:2673	54792 ff02::1:3	5355	2	4.96	3333	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	57120 ff02::1:3	5355	2	4.87	3272	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	58682 ff02::1:3	5355	2	4.87	3275	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	53631 ff02::1:3	5355	2	4.87	3545	0	1 / 100ms	0	91		0
fe80::754f:9028:b446:2673	58961 ff02::1:3	5355	2	4.87	3429	0	1 / 100ms	0	88		0
fe80::754f:9028:b446:2673	51961 ff02::1:3	5355	2	4.86	3541	0	1 / 100ms	0	91		0
fe80::754f:9028:b446:2673	53421 ff02::1:3	5355	2	4.79	3215	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	62355 ff02::1:3	5355	2	4.87	3274	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	64959 ff02::1:3	5355	2	4.88	3276	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	55672 ff02::1:3	5355	2	4.88	3279	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	54864 ff02::1:3	5355	2	4.79	3220	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	57926 ff02::1:3	5355	2	4.86	3266	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	65184 ff02::1:3	5355	2	4.87	3273	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	57544 ff02::1:3	5355	2	5.04	3386	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	65462 ff02::1:3	5355	2	4.88	3282	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	53383 ff02::1:3	5355	2	5.00	3361	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	53579 ff02::1:3	5355	2	4.89	3952	0	1 / 100ms	0	101		0
fe80::754f:9028:b446:2673	52060 ff02::1:3	5355	2	4.90	3962	0	1 / 100ms	0	101		0
fe80::754f:9028:b446:2673	51759 ff02::1:3	5355	2	4.80	3224	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	63520 ff02::1:3	5355	2	4.74	3184	0	1 / 100ms	0	84		0
fe80::754f:9028:b446:2673	54281 ff02::1:3	5355	2	4.99	3355	0	1 / 100ms	0	84		0
10.4.8.33	50129 239.255.255.250	1900	4	1.32	2282	0	1 / 100ms	0	216		0
10.4.8.33	56448 239.255.255.250	1900	4	1.32	2281	0	1 / 100ms	0	216		0
10.4.8.21	64886 230 255 255 250	1900	4	1 32	2288	0	1 / 100ms	0	216		0 ~
52 streams, avg bw: 559bps, max bw: 62kbps,	max burst: 11 / 100ms, max buffer: 70B				100						
Burst measurement interval (ms):	100		Burs	t alarm thres	nold (packets): 50	ij .			Buffer alar	rm threshold (B): 10000	
Stream empty speed (Kb/s):	5000			Total empty	speed (Kb/s): 10	0000					
Display filter:											Apply
									Сор	y Save as	Close

d. List out the TCP packets whose syn. and ack. Flags are on.

Use the command: tcp.flags.syn==1 && tcp.flags.ack==1

This command checks all the tcp packets which have ack and syn flags set to on. We use the AND operator here. SYN stands for synchronization and ack stands for acknowledgement.

tcp.	tcp.flags.syn==1 && tcp.flags.ack==1										
No.	Time	Source	Source Port	Destination	Destination Port	HTTP Host	HTTPS Server Name	Info			
	8 2021-02-04 13:27:32.194119	137.116.139.120	443	10.4.8.18	50610			443 → 50610 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	58 2021-02-04 13:27:34.170969	142.250.76.205	443	10.4.8.18	50611			443 → 50611 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	90 2021-02-04 13:27:34.486420	216.170.124.200	443	10.4.8.18	50612			443 → 50612 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
	104 2021-02-04 13:27:34.805466	142.250.76.174	443	10.4.8.18	50613			443 → 50613 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	167 2021-02-04 13:27:35.361519	142.250.76.170	443	10.4.8.18	50614			443 → 50614 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	176 2021-02-04 13:27:35.449303	142.250.77.40	443	10.4.8.18	50615			443 → 50615 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	209 2021-02-04 13:27:35.538416	103.205.143.18	443	10.4.8.18	50616			443 → 50616 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	215 2021-02-04 13:27:35.544556	82.196.1.114	443	10.4.8.18	50617			443 → 50617 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	636 2021-02-04 13:27:36.115514	172.217.166.163	443	10.4.8.18	50618			443 → 50618 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
	644 2021-02-04 13:27:36.127417	103.205.143.18	443	10.4.8.18	50619			443 → 50619 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
•	647 2021-02-04 13:27:36.128164	142.250.192.35	443	10.4.8.18	50620			443 → 50620 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			
	669 2021-02-04 13:27:36.182050	37.139.12.133	443	10.4.8.18	50621			443 → 50621 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=128			

e. List out the TCP and UDP packets where destination port=80.

Use the command: tcp.dstport==80 || udp.dstport==80

This command lists all TCP and UDP packets with destination port number 80. We use the OR operator here

t	tcp.dstport==80 udp.dstport==80											
No.		Time	^	Source	Source Port	Destination	Destination Por	HTTP Host	HTTPS Server Name	Info		
	14601	2021-02-04	13:28:10.596818	10.4.8.18	50608	172.217.166.46	80			50608 → 80	[FIN,	
-	14602	2021-02-04	13:28:10.597013	10.4.8.18	50698	172.217.166.46	80			50698 → 80	[SYN]	
	14604	2021-02-04	13:28:10.597119	10.4.8.18	50608	172.217.166.46	80			50608 → 80	[ACK]	
	14606	2021-02-04	13:28:10.597304	10.4.8.18	50698	172.217.166.46	80			50698 → 80	[ACK]	
	14607	2021-02-04	13:28:10.605111	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1		GET /edgedl	/relea:	
1	14619	2021-02-04	13:28:10.748667	10.4.8.18	50609	49.44.83.143	80			50609 → 80	[FIN,	
	14620	2021-02-04	13:28:10.748950	10.4.8.18	50699	49.44.83.143	80			50699 → 80	[SYN]	
	14622	2021-02-04	13:28:10.749023	10.4.8.18	50609	49.44.83.143	80			50609 → 80	[ACK]	
	14624	2021-02-04	13:28:10.749207	10.4.8.18	50699	49.44.83.143	80			50699 → 80	[ACK]	
	14625	2021-02-04	13:28:10.749730	10.4.8.18	50699	49.44.83.143	80	r4sn-gwpa-ccp		GET /edgedl	/relea:	
	14627	2021-02-04	13:28:10.788276	10.4.8.18	50698	172.217.166.46	80			50698 → 80	[ACK]	
	14629	2021-02-04	13:28:10.814373	10.4.8.18	50698	172.217.166.46	80	redirector.gvt1		HEAD /edged	1/rele	

f. List out the ARP packets.

Use the command: arp

This command is used to find the MAC address associated with an IPv4 address

ar	р								
No.		Time	^	Source	Source Port	Destination	Destination Pol HTTP Host	HTTPS Server Name	Info
	129	2021-02-04	13:27:35.064012	Augmenti_ce:87:01		Broadcast			Who has 10.20.0.1? Tell 10.4.8.21
1	136	2021-02-04	13:27:35.068952	Augmenti_ce:87:01		Broadcast			Who has 10.4.8.1? Tell 10.4.8.21
	137	2021-02-04	13:27:35.069133	Augmenti_ce:87:01		Broadcast			Who has 10.4.8.1? Tell 10.4.8.21
	992	2021-02-04	13:27:38.194242	Cisco_34:14:0e		Cisco_49:b0:99			10.4.8.47 is at 00:17:e0:34:14:0e
	2127	2021-02-04	13:27:44.070653	Cisco_49:b0:99		LANBitCo_1b:b			Who has 10.4.8.12? Tell 0.0.0.0
			13:27:51.615444			LCFCHeFe_41:a			Who has 10.4.8.18? Tell 0.0.0.0
	7542	2021-02-04	13:27:51.615456	LCFCHeFe_41:a3:c8		Cisco_49:b4:1b			10.4.8.18 is at 28:d2:44:41:a3:c8
	12937	2021-02-04	13:28:05.035518	Cisco_5a:ab:40		LCFCHeFe_41:a			Who has 10.4.8.18? Tell 10.4.8.1
3	12938	2021-02-04	13:28:05.035518	Cisco_5a:ab:40		HewlettP_e6:3			Who has 10.4.8.13? Tell 10.4.8.1
1	12939	2021-02-04	13:28:05.035534	LCFCHeFe_41:a3:c8		Cisco_5a:ab:40			10.4.8.18 is at 28:d2:44:41:a3:c8
> F	rame	129: 60 byt	es on wire (480	bits), 60 bytes cap	tured (480	bits) on inter	face \Device\NPF_{B807628E-62	22D-4299-8AD8-5[09AAB0D8657}, id 0
> E	thern	et II, Src:	Augmenti_ce:87:	:01 (00:0f:29:ce:87:	01), Dst:	Broadcast (ff:f	f:ff:ff:ff:ff)		
~ A	ddres	s Resolution	n Protocol (requ	uest)					
	Har	dware type:	Ethernet (1)						
	Pro	tocol type:	IPv4 (0x0800)						
	Har	dware size:	6						
	Pro	tocol size:	4						
	0pc	ode: request	(1)						
	Sen	der MAC addı	ess: Augmenti_c	e:87:01 (00:0f:29:c	2:87:01)				
	Sen	der IP addre	ess: 10.4.8.21						
	Tar	get MAC addr	ess: 00:00:00_0	0:00:00 (00:00:00:00	0:00:00)				
	Tar	get IP addre	ess: 10.20.0.1						