

This Lab is done by Mohammed Ammaruddin

Q1 129.120.231.230 is the ip address

http.host==www.unt.edu					
No.	Time	Source	Destination	Protocol	Length Info
+	2048.230	551598198 10.0.2.15	129.120.231.230	HTTP	643 GET / HTTP/1.1
Frame 2048: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface eth0, id 0					
Ethernet II, Src: PcsCompu_1c:60:34 (08:00:27:1c:60:34), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)					
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 129.120.231.230					
Transmission Control Protocol, Src Port: 50438, Dst Port: 80, Seq: 4041963166, Ack: 42752002, Len: 589					
Hypertext Transfer Protocol					
GET / HTTP/1.1\r\nHost: www.unt.edu\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n					
0000	52 54 00 12 35 02 08 00	27 1c 60 34 08 00 45 00	RT-5...	4: E	
0010	02 75 55 d2 40 00 40 06	6d 43 0a 00 02 0f 81 78	uU@0-mC...	x	
0020	e7 e6 c5 06 00 50 f0 eb	76 9e 02 8c 58 02 50 18	...P...v...X.P.		
0030	fa f0 77 d5 00 00 47 45	54 20 2f 20 48 54 54 50	...w...GE T / HTTP		
0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 77 77 77 2e	/1.1...to st: www.		
0050	75 6e 74 2a 05 64 75 0d	0a 55 73 65 72 2d 41 67	unt.edu- User-Ag		
0060	65 6e 74 3a 20 40 6f 7a	69 6c 6c 61 2f 35 2e 30	ent: Mozilla/5.0		
0070	20 28 58 31 31 3b 20 4c	69 6e 75 78 20 78 38 36	(X11; L inux x86		
0080	5f 36 34 3b 20 72 76 3a	31 30 32 2e 30 29 20 47	_64; rv: 102.0) G		
0090	65 63 6b 6f 2f 32 30 31	30 30 31 30 31 20 46 69	ecko/201 00101 F1		
00a0	72 65 66 6f 78 2f 31 30	32 2e 30 0d 0a 41 63 63	refox/10 2.0--Acc		

Q2 mozilla firefox is used

http.host==www.unt.edu					
No.	Time	Source	Destination	Protocol	Length Info
+	2048.230	551598198 10.0.2.15	129.120.231.230	HTTP	643 GET / HTTP/1.1
Frame 2048: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface eth0, id 0					
Ethernet II, Src: PcsCompu_1c:60:34 (08:00:27:1c:60:34), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)					
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 129.120.231.230					
Transmission Control Protocol, Src Port: 50438, Dst Port: 80, Seq: 4041963166, Ack: 42752002, Len: 589					
Hypertext Transfer Protocol					
GET / HTTP/1.1\r\nHost: www.unt.edu\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\nAccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nAccept-Encoding: gzip, deflate\r\nConnection: keep-alive\r\n					
0000	52 54 00 12 35 02 08 00	27 1c 60 34 08 00 45 00	RT-5...	4: E	
0010	02 75 55 d2 40 00 40 06	6d 43 0a 00 02 0f 81 78	uU@0-mC...	x	
0020	e7 e6 c5 06 00 50 f0 eb	76 9e 02 8c 58 02 50 18	...P...v...X.P.		
0030	fa f0 77 d5 00 00 47 45	54 20 2f 20 48 54 54 50	...w...GE T / HTTP		
0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 77 77 77 2e	/1.1...to st: www.		
0050	75 6e 74 2a 05 64 75 0d	0a 55 73 65 72 2d 41 67	unt.edu- User-Ag		
0060	65 6e 74 3a 20 40 6f 7a	69 6c 6c 61 2f 35 2e 30	ent: Mozilla/5.0		
0070	20 28 58 31 31 3b 20 4c	69 6e 75 78 20 78 38 36	(X11; L inux x86		
0080	5f 36 34 3b 20 72 76 3a	31 30 32 2e 30 29 20 47	_64; rv: 102.0) G		
0090	65 63 6b 6f 2f 32 30 31	30 30 31 30 31 20 46 69	ecko/201 00101 F1		
00a0	72 65 66 6f 78 2f 31 30	32 2e 30 0d 0a 41 63 63	refox/10 2.0--Acc		

### Q3 linux is the operating system

No.	Time	Source	Destination	Protocol	Length	Info
2048	238.551598198	10.0.2.15	129.129.231.230	HTTP	643	GET / HTTP/1.1

Frame 2048: 643 bytes on wire (5144 bits), 643 bytes captured (5144 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_1c:00:34 (08:00:27:1c:00:34), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 129.129.231.230
Transmission Control Protocol, Src Port: 50438, Dst Port: 80, Seq: 4041963166, Ack: 42752002, Len: 589
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
Host: www.unt.edu\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Connection: keep-alive\r\n

0000	52 54 00 12 35 02 08 00	27 1c 00 34 08 00 45 00	RTT: 5.000000000	4: E
0010	02 75 55 d2 40 00 40 06	6d 43 0a 00 02 0f 81 78	..U.0.0..mc..x	
0020	e7 e6 c5 06 00 50 f0 eb	76 9e 02 8c 58 02 50 18	...P...v...X.P	
0030	fa f0 77 d5 00 00 47 45	54 20 2f 20 48 54 54 50	..w...GE T / HTTP	
0040	2f 31 2e 31 0d 0a 48 6f	73 74 3a 20 77 77 77 2e	/1.1..Host: www.	
0050	75 6e 74 2a 65 64 75 6d	6a 55 73 65 72 2d 41 67	unt.edu: User-Ag	
0060	65 6e 74 3a 20 4d 6f 7a	69 6c 6c 61 2f 35 2e 30	ent: Mozilla/5.0	
0070	20 28 58 31 31 3b 20 4c	69 6e 75 78 20 78 38 36	(X11; Linux x86	
0080	5f 36 34 3b 20 72 76 3a	31 30 32 2e 30 29 20 47	_64; rv: 102.0) G	
0090	65 63 6b 6f 2f 32 30 31	30 30 31 30 31 20 46 69	ecko/20100101 Fi	
00a0	72 65 66 6f 78 2f 31 30	32 2e 30 0d 0a 41 63 63	refox/102.0-Acc	

Q4 ACK (Acknowledgment): This flag is used to acknowledge that data has been received. When a host receives a packet with the ACK flag set, it means that the previous packet was received successfully.

No.	Time	Source	Destination	Protocol	Length	Info
2048	238.551598198	10.0.2.15	129.129.231.230	HTTP	643	GET / HTTP/1.1

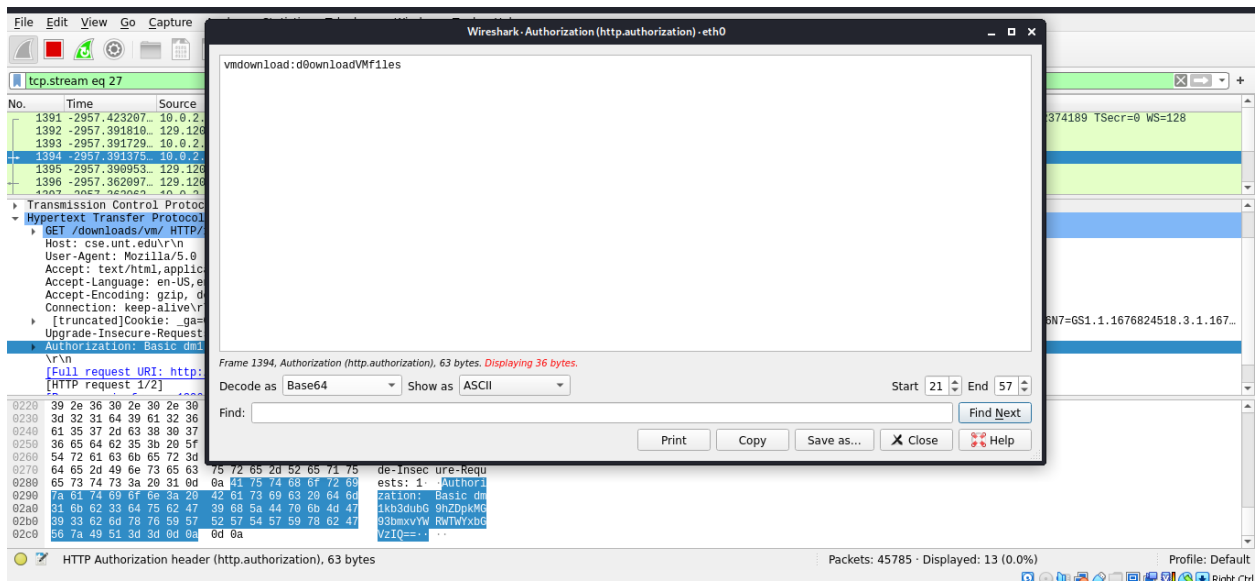
  

Flags: 0x018 (PSH, ACK)
000. .... = Reserved: Not set
...0. .... = Nonce: Not set
....0. .... = Congestion Window Reduced (CWR): Not set
....0. .... = ECN-Echo: Not set
....0. .... = Urgent: Not set
....1. .... = Acknowledgment: Set
....1. .... = Push: Set
....0. .... = Reset: Not set
....0. .... = Syn: Not set
....0. .... = Fin: Not set
[TCP Flags: .....AP...]
Window size value: 64240
[Calculated window size: 64240]

### Q5

GET /downloads/vm/ HTTP/1.1
Host: cse.unt.edu
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Cookie: _ga=GA1.2.450505599.1676793455; _gid=GA1.2.1848396348.1676793455; _tt_enable_cookie=1; _tpt=R8XDCJ2E05jSrIqaYsrF1lWlhqu; _ga_33TTT716N7=GS1.1.1676824518.3.1.1676825319.60.0.0; nmstat=21d9a261-5611-ea57-c807-39fb9506edb5; _gat_urcmTracker=1
Upgrade-Insecure-Requests: 1
Authorization: Basic dm1kb3dubG9hZDpkMG93bmxyYWRWTWYxbGVzIQ==

Q6



Q7 TCP protocol is being used, cant find credentials in this case. Filtered with ip.host==128.129.107.147 canvas.edu.unt's ip address