# **PACKET SNIFFING**

	Registration Number	Surname	Forename	% Contribution
Student 1	001131628	Chavush	Chisel	25%
Student 2	001174434	Turker	Selin	25%
Student 3	001141387	Hasan	Zahid	25%
Student 4	001141646	Ekrem Said	lz	25%

### TASK 1-

### a) We identified the DNS look up to request.

39 2.880178	10.100.10.92	10.0.0.2	DNS	83 Standard query 0x5903 A pod.comms.cms.gre.ac.uk
40 2.880776	10.0.0.2	10.100.10.92	DNS	140 Standard query response 0x5903 A pod.comms.cms.gre.ac.uk A 10.0.0.6 NS comms-dhcp.comms.cms.gre.ac.uk A 10.0.0.2

# b) DNS response returned with the IP address

	39 2.880178	10.100.10.92	10.0.0.2	DNS	83 Standard query 0x5903 A pod.comms.cms.gre.ac.uk
١	40 2.880776	10.0.0.2	10.100.10.92	DNS	140 Standard query response 0x5903 A pod.comms.cms.gre.ac.uk A 10.0.0.6 NS comms-dhcp.comms.cms.gre.ac.uk A 10.0.0.2

\*In our case, you can see the first three line as a 3-way handshake. First line is going to give you [SYN] Seq=0, Second line is [SYN, ACK] and the Seq=0 ACK=1 and finally in the Third line we are seeing [ACK] with the Seq=1.

### c)

42 2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM=1
45 2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46 2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
47 2.882801	10.100.10.92	10.0.0.6	HTTP	487 GET / HTTP/1.1
48 2.886095	10.0.0.6	10.100.10.92	HTTP	659 HTTP/1.1 200 OK (text/html)
49 2.936616	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=434 Ack=606 Win=262144 Len=0
50 2.950500	10.100.10.92	10.0.0.6	HTTP	419 GET /favicon.ico HTTP/1.1
51 2.951291	10.0.0.6	10.100.10.92	TCP	1514 80 → 50789 [ACK] Seq=606 Ack=799 Win=63442 Len=1460 [TCP segment of a reassembled PDL
52 2.951291	10.0.0.6	10.100.10.92	HTTP	389 HTTP/1.1 404 Not Found (text/html)
53 2.951335	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=799 Ack=2401 Win=262656 Len=0
54 3.148794	10.0.0.6	10.100.10.92	TCP	60 [TCP Dup ACK 51#1] 80 → 50789 [ACK] Seq=2401 Ack=799 Win=63442 Len=0
57 3.886389	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
143 5.887356	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PER
	10.0.0.6	10.100.10.92	TCP	66 80 + 50788 [SYN, ACK] Seg=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK PERM=1
144 6.101936	10.0.0.0			
145 6.102053	10.100.10.92	10.0.0.6	TCP	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
145 6.102053 Ethernet II, Src:	10.100.10.92 10.100.10.02 VMware_28:dd:2c (00	0:0c:29:28:dd:2c), Dst	t: Clevo_83:	54 50788 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
Ethernet II, Src: Internet Protocol	10.100.10.92 10.100.10.92 VMware_28:dd:2c (00 Version 4, Src: 10.	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol	10.100.10.92 10.100.10.92 VMware_28:dd:2c (00 Version 4, Src: 10.	0:0c:29:28:dd:2c), Dst	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Transmission Contr	10.100.10.92 VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  15:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Transmission Contr	10.100.10.92 VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Transmission Contr	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053  Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n</html>	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po- Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507	t: Clevo_83:	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n       <br< td=""><td>10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol sta: text/html (12 l</td><td>0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507</td><td>t: Clevo_83: 3.92 789, Seq: 1,</td><td>54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)</td></br<></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></html>	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:10 ort: 80, Dst Port: 507	t: Clevo_83: 3.92 789, Seq: 1,	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n             <br< td=""><td>10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po Protocol sta: text/html (12 l</td><td>0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10:100.10 rt: 80, Dst Port: 507</td><td>t: Clevo_83: 3.92 789, Seq: 1,</td><td>54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)</td></br<></br></br></br></br></html>	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10:100.10 rt: 80, Dst Port: 507	t: Clevo_83: 3.92 789, Seq: 1,	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053  ***ALA CRASSTAN  Ethernet II, Src:  Internet Protocol  Transmission Contr  Hypertext Transfer  Line-based text da <html>\r\n  <body>\r\n  <center><h2>\r\n  Welcome to the</h2></center></body></html>	10.100.10.92  Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10:100.10 rt: 80, Dst Port: 507	t: Clevo_83: 3.92 789, Seq: 1,	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  11f:af (80:fa:5b:83:1f:af)
145 6.102053 Ethernet II, Src: Internet Protocol Irransmission Contr Hypertext Transfer Line-based text (ATML)*\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n	10.100.10.92  VPWare_28idd:2c (00  Version 4, Src: 10.  Tol Protocol, Src Por  Protocol  ta: text/html (12 1  In  Ping of Death server	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10:100.10 rt: 80, Dst Port: 507	t: Clevo_83: 3.92 789, Seq: 1,	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  101:16:46 (80:6:5:5:83:1f:af)  Ack: 434, Len: 605
145 6.102053 Ethernet II, Src: Internet Protocol Iransmission Contr Hypertext Transfer Line-based text do (HTML)\n\n (body\n\n (center>\n2\n\n) Welcome to the \n2\n\n\n (br\n\n\n)	10.100.10.92  VPWare_28idd:2c (00  Version 4, Src: 10.  Tol Protocol, Src Por  Protocol  ta: text/html (12 1  In  Ping of Death server	8:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 ort: 80, Dst Port: 507 lines)	t: Clevo_83: 3.92 789, Seq: 1,	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  101:16:46 (80:6:5:5:83:1f:af)  Ack: 434, Len: 605
145 6.18283  Ethernet II, Src: Internet Protocol Internet Brotocol Iransmission Contr Hypertext Transfer Line-based text da (HTML)\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	10.100.10.92  Noware_28idd:2c (00 Version 4, Src: 10. Ol Protocol, Src Portocol sta: text/html (12 l  nn Ping of Death serve ur\n  mme money at the <a< td=""><td>0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)</td><td>t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n</td><td>54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  101:16:46 (80:6:5:5:83:1f:af)  Ack: 434, Len: 605</td></a<>	0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)	t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0  101:16:46 (80:6:5:5:83:1f:af)  Ack: 434, Len: 605
145 6.18283  Ethernet II, Src: Internet Protocol Internet Brotocol Iransmission Contr Hypertext Transfer Line-based text da (HTML)\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\	10.100.10.92  Noware_28idd:2c (00 Version 4, Src: 10. Ol Protocol, Src Portocol sta: text/html (12 l  nn Ping of Death serve ur\n  mme money at the <a< td=""><td>0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)</td><td>t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n</td><td>54 50788 + 38 [ACK] Seq=1 Ack=1 Min=262656 Len=0  11f:af (80:fa:5b:83:1f:af)  Ack: 434, Len: 605</td></a<>	0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)	t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n	54 50788 + 38 [ACK] Seq=1 Ack=1 Min=262656 Len=0  11f:af (80:fa:5b:83:1f:af)  Ack: 434, Len: 605
145 6.102053  Ethernet II, Src: Internet Protocol Irransmission Contr Hypertext Transfer Line-based text da (HTML)/r\n (chody>\r\n (center> <h2>\r\n Welcome to the (/center&gt;/h2/\r\n Why not wire so (chr&gt;\r\n ) r buy that spe</h2>	10.100.10.92  Noware_28idd:2c (00 Version 4, Src: 10. Ol Protocol, Src Portocol sta: text/html (12 l  nn Ping of Death serve ur\n  mme money at the <a< td=""><td>0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)</td><td>t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n</td><td>54 50788 + 30 [Ack] Seq-1 Ack-1 Win-262656 Len-0  11f:af (80:fa:5b:83:1f:af)  Ack: 434, Len: 605</td></a<>	0:0c:29:28:dd:2c), Dst 0:0.0.6, Dst: 10:100.10 ort: 80, Dst Port: 507 dines)	t: Clevo_83: 3.92 789, Seq: 1, etwork\r\n	54 50788 + 30 [Ack] Seq-1 Ack-1 Win-262656 Len-0  11f:af (80:fa:5b:83:1f:af)  Ack: 434, Len: 605

### d)

42 2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45 2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46 2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
47 2.882801	10.100.10.92	10.0.0.6	HTTP	487 GET / HTTP/1.1
48 2.886095	10.0.0.6	10.100.10.92	HTTP	659 HTTP/1.1 200 OK (text/html)
49 2.936616	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=434 Ack=606 Win=262144 Len=0
50 2.950500	10.100.10.92	10.0.0.6	HTTP	419 GET /favicon.ico HTTP/1.1
51 2.951291	10.0.0.6	10.100.10.92	TCP	1514 80 → 50789 [ACK] Seq=606 Ack=799 Win=63442 Len=1460 [TCP segment of a reassembled PDU]
52 2.951291	10.0.0.6	10.100.10.92	HTTP	389 HTTP/1.1 404 Not Found (text/html)
53 2.951335	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=799 Ack=2401 Win=262656 Len=0
54 3.148794	10.0.0.6	10.100.10.92		60 [TCP Dup ACK 51#1] 80 + 50789 [ACK] Seq=2401 Ack=799 Win=63442 Len=0
57 3.886389	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=
143 5.887356	10.100.10.92	10.0.0.6	TCP	66 [TCP Retransmission] 50788 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=:
144 6.101936	10.0.0.6	10.100.10.92	TCP	66 80 → 50788 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK PERM=1
145 6.102053	10.100.10.92	10.0.0.6	TCP	54 50788 + 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
140 C FOADED	10 100 10 02	10.0.0.0	LITTO	COO CCT. (6) a manhan (finder, ben) 17770/4 4
Ethernet II, Src:	VMware_28:dd:2c (00	10.00 c 0:0c:29:28:dd:2c), Dst	t: Clevo_83	
Ethernet II, Src: Internet Protocol	VMware_28:dd:2c (00 Version 4, Src: 10.	10.00.c 1:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	10.00 c 0:0c:29:28:dd:2c), Dst	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:16 prt: 80, Dst Port: 50	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:16 prt: 80, Dst Port: 50	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n</html>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:16 prt: 80, Dst Port: 50	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <body>\r\n</body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po r Protocol ata: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:16 prt: 80, Dst Port: 50	t: Clevo_83:	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <body>\r\n <center><h2>\r'\n</h2></center></body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. rool Protocol, Src Por Protocol ata: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10.100.10 rt: 80, Dst Port: 50 ines)	t: Clevo_83: 9.92 789, Seq: 1,	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <body>\r\n <center><h2>\r'\n</h2></center></body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. rool Protocol, Src Por Protocol ata: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0.6, Dst: 10:100:16 prt: 80, Dst Port: 50	t: Clevo_83: 9.92 789, Seq: 1,	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <body>\r\n <center><h2>\r'\n</h2></center></body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10.100.10 rt: 80, Dst Port: 50 ines)	t: Clevo_83: 9.92 789, Seq: 1,	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <body>\r\n <center>kl2&gt;\r' Welcome to the</center></body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10.100.10 rt: 80, Dst Port: 50 ines)	t: Clevo_83: 9.92 789, Seq: 1,	:1f:af (88:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d (HTML>\r\n <box>\r\n <center><h2>\r\n \left\( \text{ernet} \rightarrow \frac{1}{2} \rangle \rightarr</h2></center></box>	Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l Nn Ping of Death serve \r\n	0:0c:29:28:dd:2c), Dst 0:0c:09:28:dd:2c), Dst 0:0.6, Dst: 10.100.10 rt: 80, Dst Port: 50 ines)	t: Clevo_83: 8.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d (HTML>\r\n <box>\r\n <center><h2>\r\n \left\( \text{ernet} \rightarrow \frac{1}{2} \rangle \rightarr</h2></center></box>	Whware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l Nn Ping of Death serve \r\n	::0.29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 ines)	t: Clevo_83: 8.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d (HTML>\r\n (center> <h2>\r\n (center&gt;<h2>\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n</h2></h2>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l \n \prime ping of Death serve \n \n \n \n \n mome money at the <a< td=""><td>ines)  ", hosted on Comms ne href="HacmeBank_v2_bie</td><td>t: Clevo_83: 3.92 789, Seq: 1,</td><td>:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605</td></a<>	ines)  ", hosted on Comms ne href="HacmeBank_v2_bie	t: Clevo_83: 3.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d (HTML>\r\n (center> <h2>\r\n (center&gt;<h2>\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n (draw)\r\n</h2></h2>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l \n \prime ping of Death serve \n \n \n \n \n mome money at the <a< td=""><td>ines)  ", hosted on Comms ne href="HacmeBank_v2_bie</td><td>t: Clevo_83: 3.92 789, Seq: 1,</td><td>:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605</td></a<>	ines)  ", hosted on Comms ne href="HacmeBank_v2_bie	t: Clevo_83: 3.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Cont Hypertext Transfe Line-based text d <html>\r\n <center><h2>\r\n <center><h2>\r\n Welcome to the </h2></center></h2>\r\n Why not wire so    <pre>  <pre></pre> <pre> <pre></pre> <pre> <pre></pre> <pre></pre> <pre> </pre> <pre> <pre></pre> <pre> <pre></pre> <pre> <pre></pre> <pre></pre> <pre> <pre></pre> <pre> <pre></pre> <pre></pre> <pre> <pre><pre></pre> <pre><pre><pre></pre> <pre></pre> <pre> <pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></pre></center></html>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Por Protocol ata: text/html (12 l \n \prime ping of Death serve \n \n \n \n \n mome money at the <a< td=""><td>ines)  ", hosted on Comms ne href="HacmeBank_v2_bie</td><td>t: Clevo_83: 3.92 789, Seq: 1,</td><td>:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605</td></a<>	ines)  ", hosted on Comms ne href="HacmeBank_v2_bie	t: Clevo_83: 3.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605

42 2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45 2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46 2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
47 2.882801	10.100.10.92	10.0.0.6	HTTP	487 GET / HTTP/1.1
48 2.886095	10.0.0.6	10.100.10.92	HTTP	659 HTTP/1.1 200 OK (text/html)
49 2.936616	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=434 Ack=606 Win=262144 Len=0
50 2.950500	10.100.10.92	10.0.0.6	HTTP	419 GET /favicon.ico HTTP/1.1
51 2.951291	10.0.0.6	10.100.10.92	TCP	1514 80 → 50789 [ACK] Seq=606 Ack=799 Win=63442 Len=1460 [TCP segment of a reassembled P
52 2.951291	10.0.0.6	10.100.10.92	HTTP	389 HTTP/1.1 404 Not Found (text/html)
53 2.951335	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=799 Ack=2401 Win=262656 Len=0
54 3.148794	10.0.0.6	10.100.10.92		60 [TCP Dup ACK 51#1] 80 → 50789 [ACK] Seq=2401 Ack=799 Win=63442 Len=0
57 3.886389	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
143 5.887356	10.100.10.92	10.0.0.6	TCP	66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PE
144 6.101936	10.0.0.6	10.100.10.92	TCP	66 80 → 50788 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
145 6.102053	10.100.10.92	10.0.0.6	TCP	54 50788 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
Ethernet TT. Src.	VMware 28:dd:2c (9)	0.0c.29.28.dd.2c) Dst	t. Clevo 83	:1f:af (80:fa:5b:83:1f:af)
		.0.0.6, Dst: 10.100.10		
		ort: 80, Dst Port: 50		. Ack: 434, Len: 605
Hypertext Transfe		,	,,,	
	lata: text/html (12	lines)		
<html>\r\n</html>				
<body>\r\n</body>				
<center><h2>\r</h2></center>	\n			
Welcome to the	Ping of Death serve	er, hosted on Comms ne	etwork\r\n	
	\r\n			
\r\n				
Why not wire s	ome money at the <a< td=""><td>href="HacmeBank v2 We</td><td>bsite"&gt;Hacm</td><td>me Bank.\r\n</td></a<>	href="HacmeBank v2 We	bsite">Hacm	me Bank.\r\n
\r\n	Selficial accounts of the property of the prop			
Or buy that sp	ecial someone some	flowers at the <a href<="" td=""><td>f="flowersho</td><td>pp\index.html"&gt;Flower Shop</td></a> .\r\n	f="flowersho	pp\index.html">Flower Shop
\r\n				
\r\n				

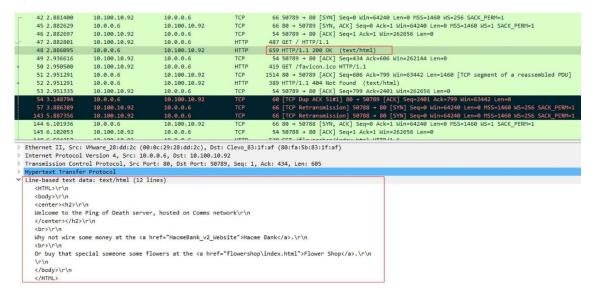
# f-)HTTP request home page from server.

42 2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45 2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46 2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
47 2.882801	10.100.10.92	10.0.0.6	HTTP	487 GET / HTTP/1.1
48 2.886095	10.0.0.6	10.100.10.92	HTTP	659 HTTP/1.1 200 OK (text/html)
49 2.936616	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=434 Ack=606 Win=262144 Len=0
50 2.950500	10.100.10.92	10.0.0.6	HTTP	419 GET /favicon.ico HTTP/1.1
51 2.951291	10.0.0.6	10.100.10.92	TCP	1514 80 → 50789 [ACK] Seq=606 Ack=799 Win=63442 Len=1460 [TCP segment of a reassembled PDU]
52 2.951291	10.0.0.6	10.100.10.92	HTTP	389 HTTP/1.1 404 Not Found (text/html)
53 2.951335	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=799 Ack=2401 Win=262656 Len=0
54 3.148794	10.0.0.6	10.100.10.92		60 [TCP Dup ACK 51#1] 80 → 50789 [ACK] Seq=2401 Ack=799 Win=63442 Len=0
57 3.886389	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
143 5.887356	10.100.10.92	10.0.0.6	TCP	66 [TCP Retransmission] 50788 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=
144 6.101936	10.0.0.6	10.100.10.92	TCP	66 80 + 50788 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
145 6.102053	10.100.10.92	10.0.0.6	TCP	54 50788 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
140 € 504357	10 100 10 00	10.0.0.0	UTTO	FOO CET (6) a marker (dadam bits) (ITTO // 4
Ethernet II, Src:	VMware_28:dd:2c (00	:0c:29:28:dd:2c), Dst	: Clevo_83	
Ethernet II, Src: Internet Protocol	VMware_28:dd:2c (00 Version 4, Src: 10.	::0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10	:: Clevo_83:	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	:0c:29:28:dd:2c), Dst	:: Clevo_83:	:1f:af (80:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer	VMware_28:dd:2c (00 Version 4, Src: 10. Tol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83:	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83:	:1f:af (80:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n</html>	VMware_28:dd:2c (00 Version 4, Src: 10. Tol Protocol, Src Po	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83:	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html \n<br=""><body>\r\n</body></html>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83:	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n <body>\r\n <center><h2>\r\</h2></center></body></html>	Whware_28:dd:2c (00 Version 4, Src: 10. vol Protocol, Src Po Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83: 0.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n <body>\r\n <center><h2>\r\</h2></center></body></html>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po- Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83: 0.92 789, Seq: 1,	:1f:af (80:fa:5b:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da <html>\r\n <body>\r\n <center><h2>\r\ Welcome to the</h2></center></body></html>	VMware_28:dd:2c (00 Version 4, Src: 10. rol Protocol, Src Po- Protocol sta: text/html (12 l	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83: 0.92 789, Seq: 1,	:1f:af (80:fa:Sb:83:1f:af)
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text de «HTML>\r\n   (center><\2>\r\n Welcome to the <\h2>\r\n	VMware_28:dd:2c (00 Version 4, Src: 10. ol Protocol, Src Po Protocol tta: text/html (12 1  n Ping of Death serve r\n	::0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.18 rt: 80, Dst Port: 507 ines)	:: Clevo_83: .92 /89, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text de «HTML>\r\n   (center><\2>\r\n Welcome to the <\h2>\r\n	VMware_28:dd:2c (00 Version 4, Src: 10. ol Protocol, Src Po Protocol tta: text/html (12 1  n Ping of Death serve r\n	0:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 rt: 80, Dst Port: 507	:: Clevo_83: .92 /89, Seq: 1,	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da (HTML\\r\n) <center\<h2\\r\n \(center\<h2\\r\n\)="" \(de<="" \(delta\)="" td=""><td>Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2</td><td>:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We</td><td>:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n</td><td>:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605</td></center\<h2\\r\n>	Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2	:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We	:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n	:1f:af (80:fa:5b:83:1f:af) , Ack: 434, Len: 605
Ethernet II, Src: Internet Protocol Transmission Contr Hypertext Transfer Line-based text da (HTML\\r\n) <center\<h2\\r\n \(center\<h2\\r\n\)="" \(de<="" \(delta\)="" td=""><td>Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2</td><td>:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We</td><td>:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n</td><td>### Bank.\r\n</td></center\<h2\\r\n>	Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2	:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We	:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n	### Bank.\r\n
Ethernet II, Src: Internet Protocol Transmission Control Transmission Control Mypertext Transfer Line-based text da <hr/> <hr <="" td=""/> <td>Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2</td> <td>:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We</td> <td>:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n</td> <td>### Bank.\r\n</td>	Whare_28:dd:2c (00 Vhare_28:dd:2c (00 Vhare_28:dd:2	:0c:29:28:dd:2c), Dst 0.0.6, Dst: 10.100.10 nt: 80, Dst Port: 507 ines)  r, hosted on Comms ne href="HacmeBank_v2_We	:: Clevo_83: 0.92 789, Seq: 1, etwork\r\n	### Bank.\r\n

#### g)HTTP Response from the server with text/html.

42 2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 + 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45 2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46 2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
47 2.882801	10.100.10.92	10.0.0.6	HTTP	487 GET / HTTP/1.1
48 2.886095	10.0.0.6	10.100.10.92	HTTP	659 HTTP/1.1 200 OK (text/html)
49 2.936616	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=434 Ack=606 Win=262144 Len=0
50 2.950500	10.100.10.92	10.0.0.6	HTTP	419 GET /favicon.ico HTTP/1.1
51 2.951291	10.0.0.6	10.100.10.92	TCP	1514 80 → 50789 [ACK] Seq=606 Ack=799 Win=63442 Len=1460 [TCP segment of a reassembled PDL
52 2.951291	10.0.0.6	10.100.10.92	HTTP	389 HTTP/1.1 404 Not Found (text/html)
53 2.951335	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=799 Ack=2401 Win=262656 Len=0
54 3.148794	10.0.0.6	10.100.10.92		60 [TCP Dup ACK 51#1] 80 → 50789 [ACK] Seq=2401 Ack=799 Win=63442 Len=0
57 3.886389	10.100.10.92	10.0.0.6		66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
143 5.887356	10.100.10.92	10.0.0.6	TCP	66 [TCP Retransmission] 50788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
144 6.101936	10.0.0.6	10.100.10.92	TCP	66 80 → 50788 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
145 6.102053	10.100.10.92	10.0.0.6	TCP	54 50788 → 80 [ACK] Seq=1 Ack=1 Win=262656 Len=0
		ort: 80, Dst Port: 50	789, Seq: 1	, Ack: 434, Len: 605
Hypertext Transf				
	data: text/html (12	lines)		
<html>\r\n</html>				
<body>\r\n</body>	12.0			
<center><h2></h2></center>				
		er, hosted on Comms n	etwork\r\n	
<td>2&gt;\r\n</td> <td></td> <td></td> <td></td>	2>\r\n			
\r\n				
Why not wire \r\n	some money at the <a< td=""><td>href="HacmeBank_v2_W</td><td>ebsite"&gt;Hacr</td><td>me Bank.\r\n</td></a<>	href="HacmeBank_v2_W	ebsite">Hacr	me Bank.\r\n
Or buy that s	special someone some	flowers at the <a hre<="" td=""><td>f="flowersho</td><td>op\index.html"&gt;Flower Shop</td></a> .\r\n	f="flowersho	op\index.html">Flower Shop
\r\n				
\r\n				

#### h) We can see here html codes in line-based section.

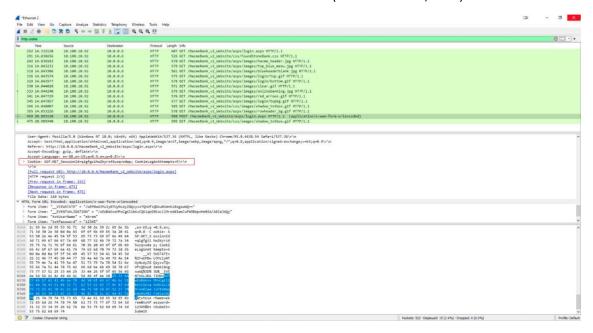


#### **TASK 2-**

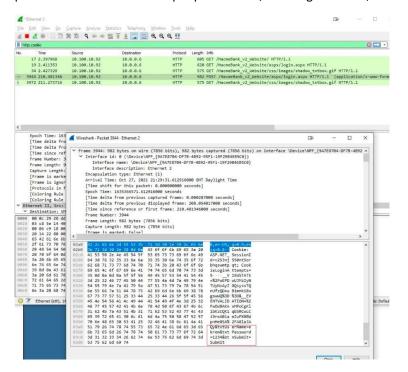
#### It has been cancelled

#### **TASK 3-**

**a)** In our case we are able to capture cookies from the website since <a href="http://pod/">http://pod/</a> is not https. Therefore, every cookie can be seen in normal text format and can be sniffed. Because http: websites cannot set the attribute "secure" to the cookie (MDN Web Docs, 2021).



**b)** Since adversary can sniff packets and capture cookies from http unsecured websites, they can see personal information of the people. Such as, their log in details, emails, addresses and so on.



#### **TASK 4-**

3 protocols can be given as: ARP (Address Resolution Protocol), TCP (Transmission Control Protocol) and IP (Internet Protocol)

ARP can be found in Network layer of the OSI Model and help us to convert IP addresses into MAC/Physical addresses.

TCP can be found in Transport layer of the OSI Model and help us to transfer data among hosts.

IP can be found in Network layer of the OSI Model and help us to define the location of the hosts.

```
658 41.190480 VMware_b3:21:12 Clevo_83:1f:af ARP 60 Who has 10.100.10.92? Tell 10.0.0.2 659 41.190490 Clevo_83:1f:af VMware_b3:21:12 ARP 42 10.100.10.92 is at 80:fa:5b:83:1f:af
```

Here it broadcasts our IPv4 Address to ask who has this as a host and our machine replies back with our mac address. This can be seen clearly in our ARP packets that we have captured.

#### **REFERENCES:**

MDN Web Docs. (2021). *Devoloper Mozilla*. Retrieved 01 28, 2021, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies