

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	Iz	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
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 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	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	TCP	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=1
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
146	6.504373	10.100.10.92	10.0.0.6	HTTP	530 GET / HTTP/1.1
> Ethernet II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
> Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
> Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
> Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

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	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	TCP	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=1
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
146	6.504373	10.100.10.92	10.0.0.6	HTTP	530 GET / HTTP/1.1
> Ethernet II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
> Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
> Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
> Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

e)

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	2.886895	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	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	TCP	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=1
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 II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

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	2.886895	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	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	TCP	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=1
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 II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

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 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	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	TCP	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=1
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 II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

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

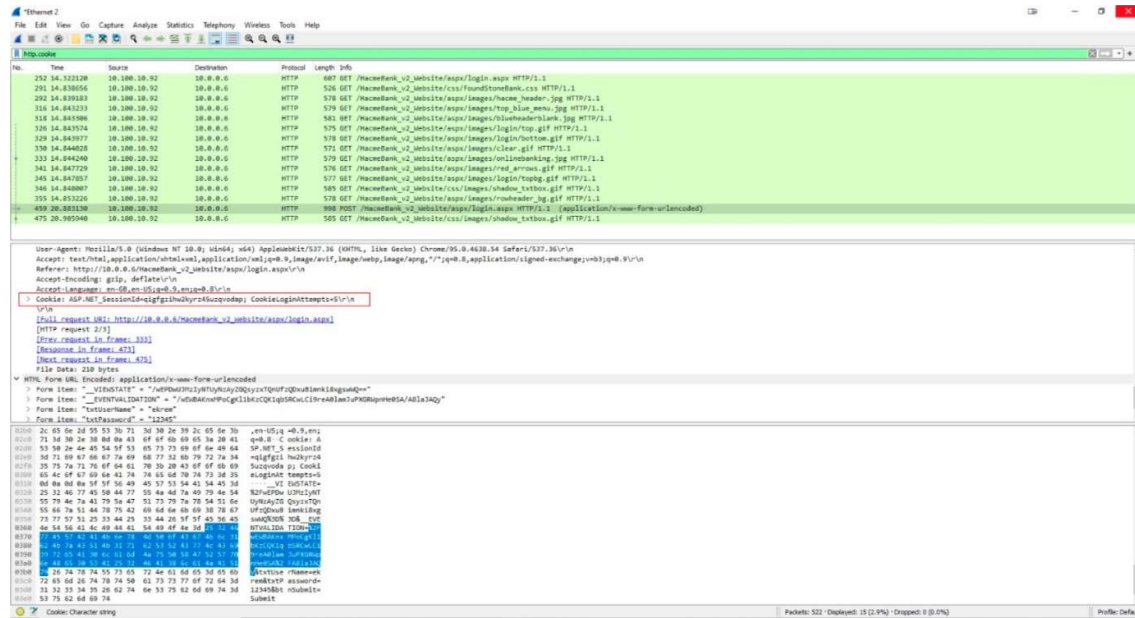
42	2.881400	10.100.10.92	10.0.0.6	TCP	66 50789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
45	2.882629	10.0.0.6	10.100.10.92	TCP	66 80 → 50789 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=1 SACK_PERM=1
46	2.882697	10.100.10.92	10.0.0.6	TCP	54 50789 → 80 [ACK] Seq=1 Ack=1 Win=262656 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	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	TCP	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=1
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 II, Src: VMware_28:dd:2c (00:0c:29:28:dd:2c), Dst: Clevo_83:1f:af (80:fa:5b:83:1f:af)					
Internet Protocol Version 4, Src: 10.0.0.6, Dst: 10.100.10.92					
Transmission Control Protocol, Src Port: 80, Dst Port: 50789, Seq: 1, Ack: 434, Len: 605					
Hypertext Transfer Protocol					
Line-based text data: text/html (12 lines)					
<HTML>\r\n					
<body>\r\n					
<center><h2>\r\n					
Welcome to the Ping of Death server, hosted on Comms network\r\n					
</center></h2>\r\n					
 \r\n					
Why not wire some money at the Hacme Bank.\r\n					
 \r\n					
Or buy that special someone some flowers at the Flower Shop.\r\n					
\r\n					
</body>\r\n					
</HTML>					

TASK 2-

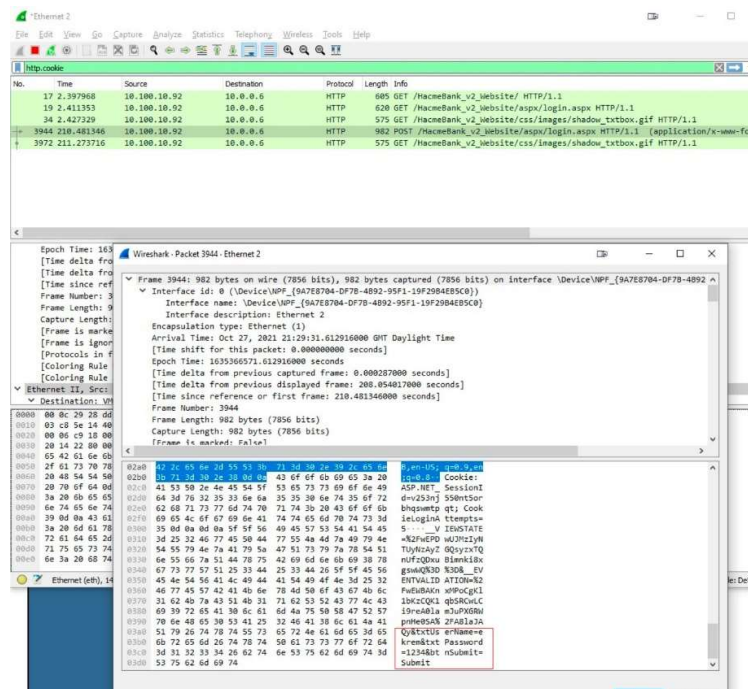
It has been cancelled

TASK 3-

a) In our case we are able to capture cookies from the website since <http://pod/> 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). *Developer Mozilla*. Retrieved 01 28, 2021, from <https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies>