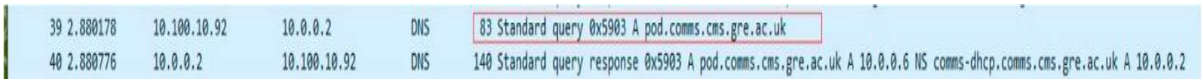
PACKET SNIFFING

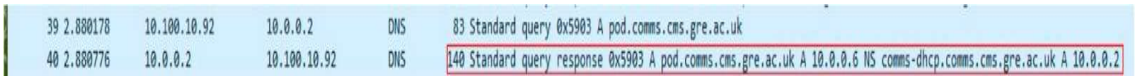
	Registration Number	Surname	Forename	% Contribution
Student 1	001131628	Chavush	Chisel	25%
Student 2	001174434	Turker	Selin	25%
Student 3	001141387	Hasan	Zahid	25%
Student 4	001141646	Ekrem Said	Iz	25%

TASK 1-

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

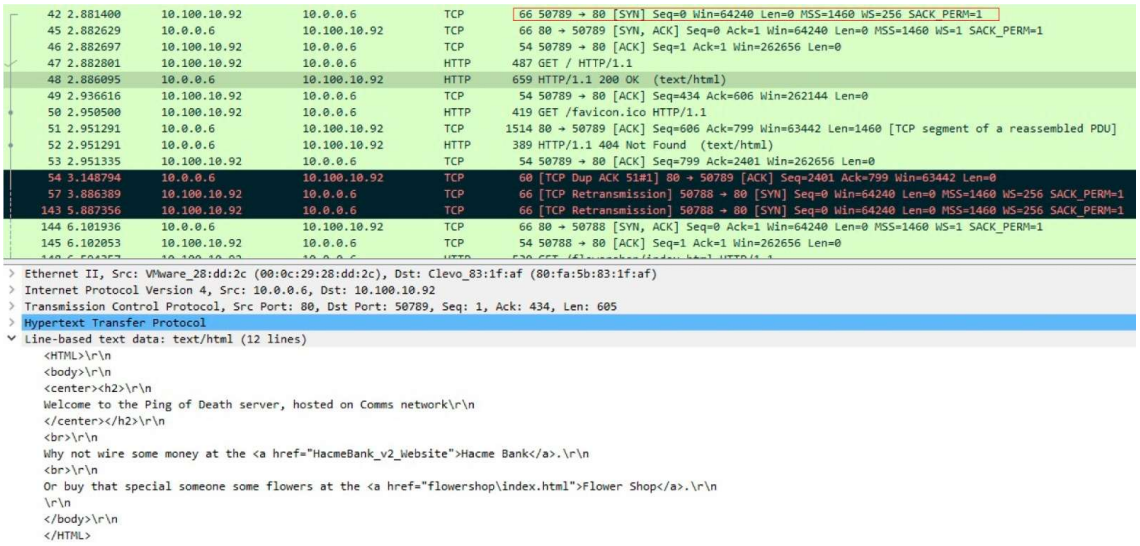


b) **DNS response returned with the IP address**

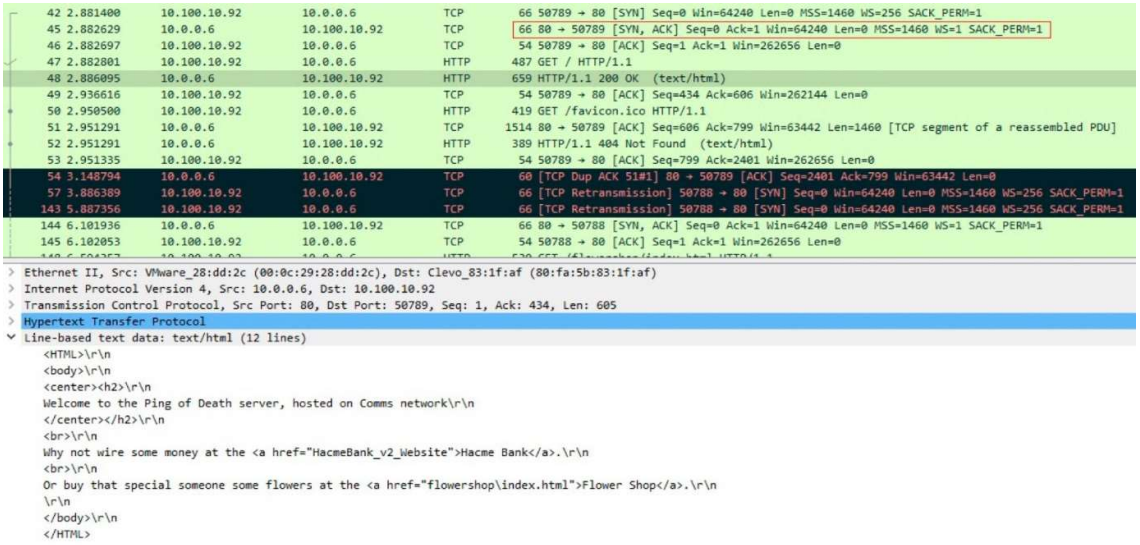


***In our case, you can see the first three line as a 3-way handshake. First line is going to give you [SYN] Seq=0, Second line is [SYN, ACK] and the Seq=0 ACK=1 and finally in the Third line we are seeing [ACK] with the Seq=1.**

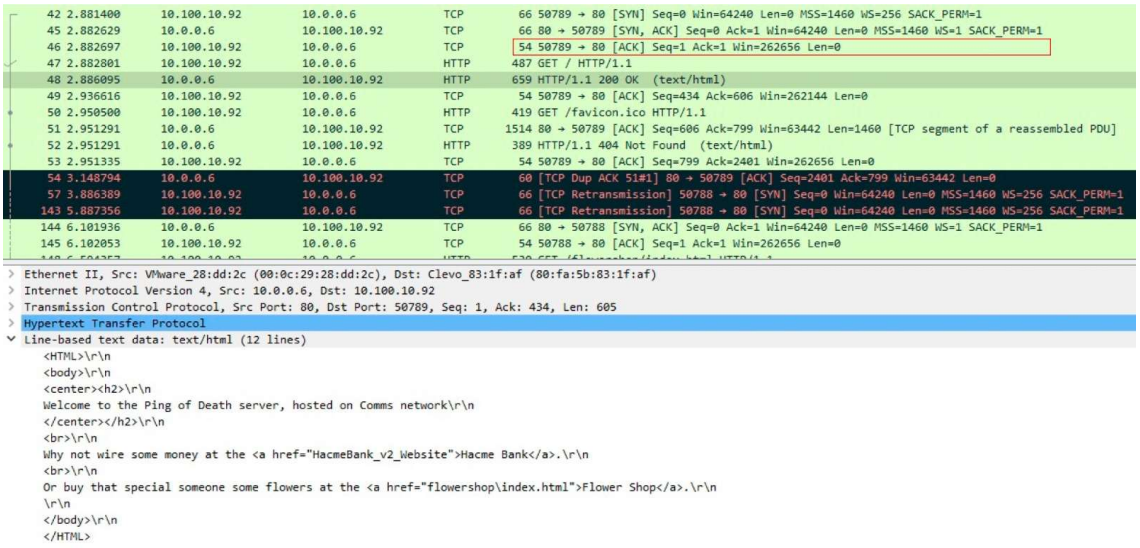
c)



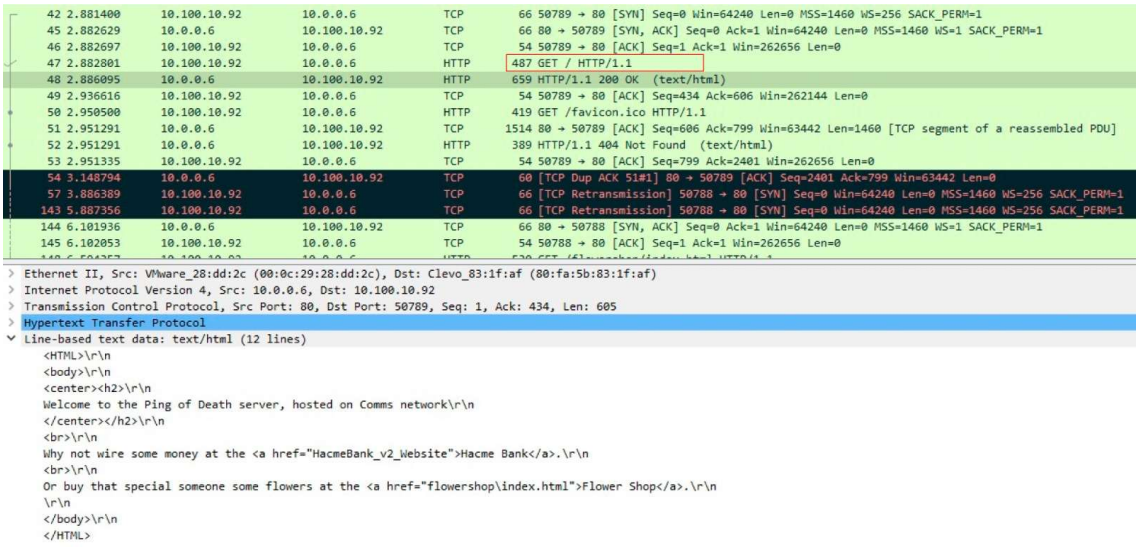
d)



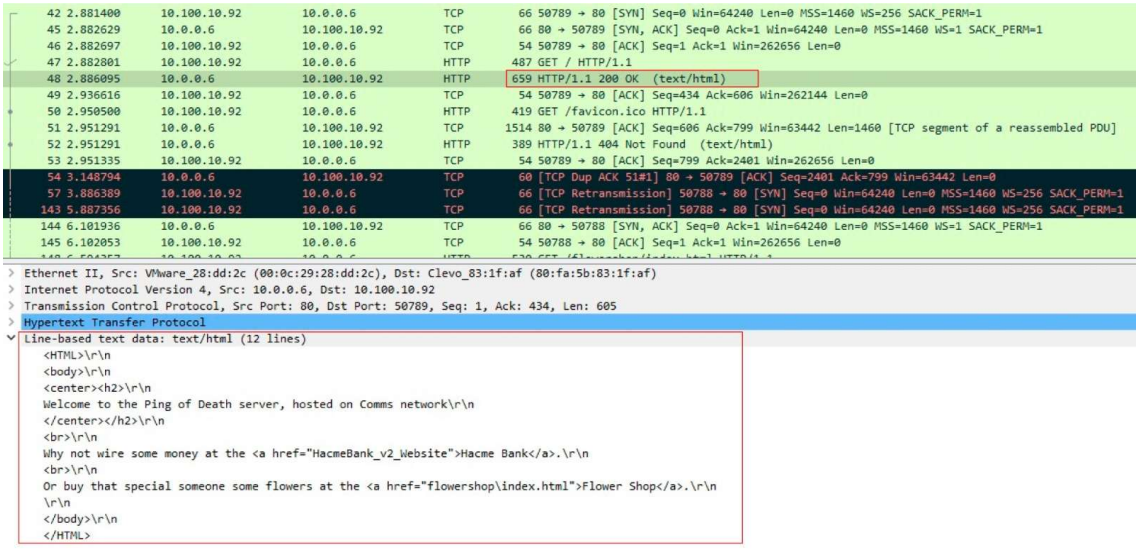
e)



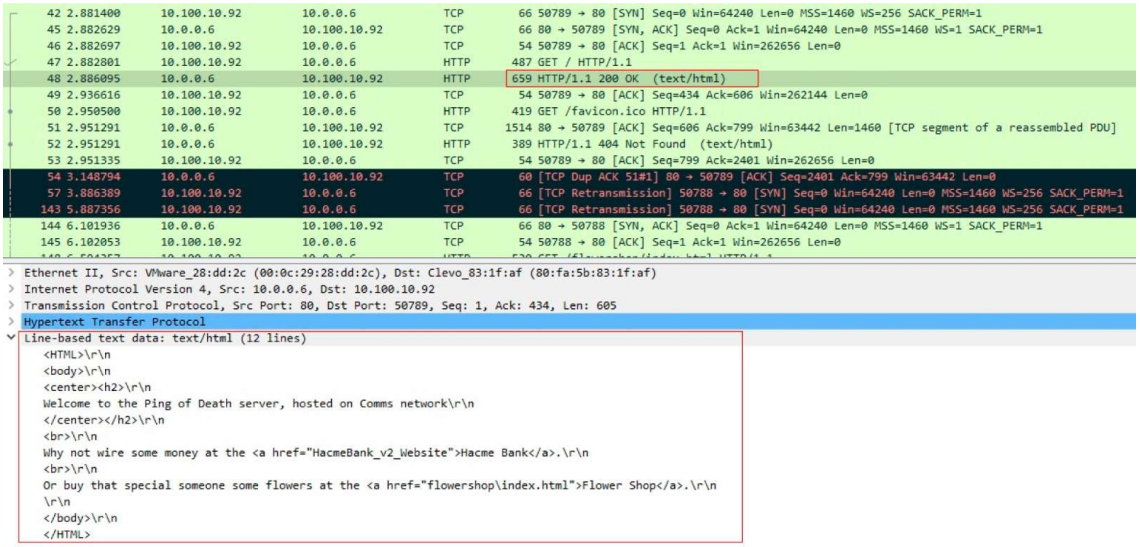
f-)HTTP request home page from server.



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



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

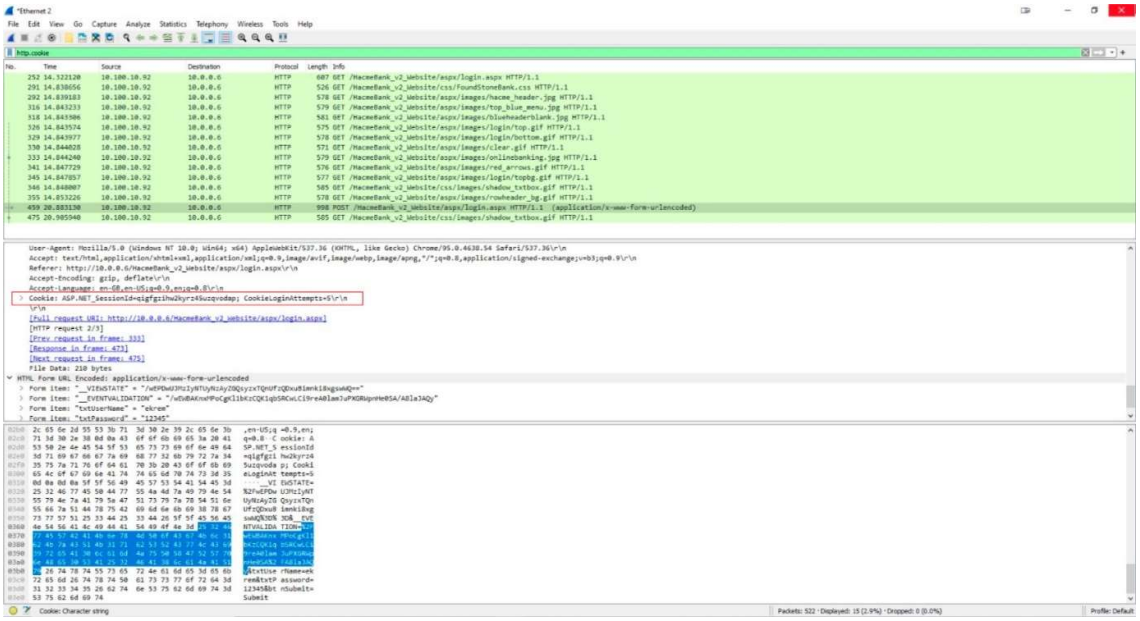


TASK 2-

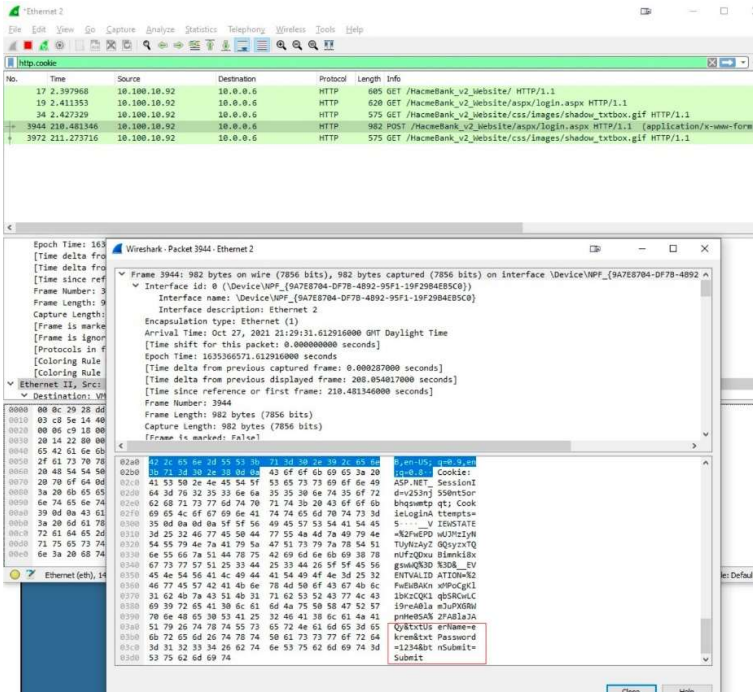
It has been cancelled

TASK 3-

a) In our case we are able to capture cookies from the website since 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.



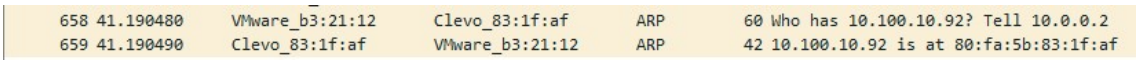
TASK 4-

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.



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