AKASH PINNAKA

180905030

CSE-D

ROLL NO 10

CN LAB 3

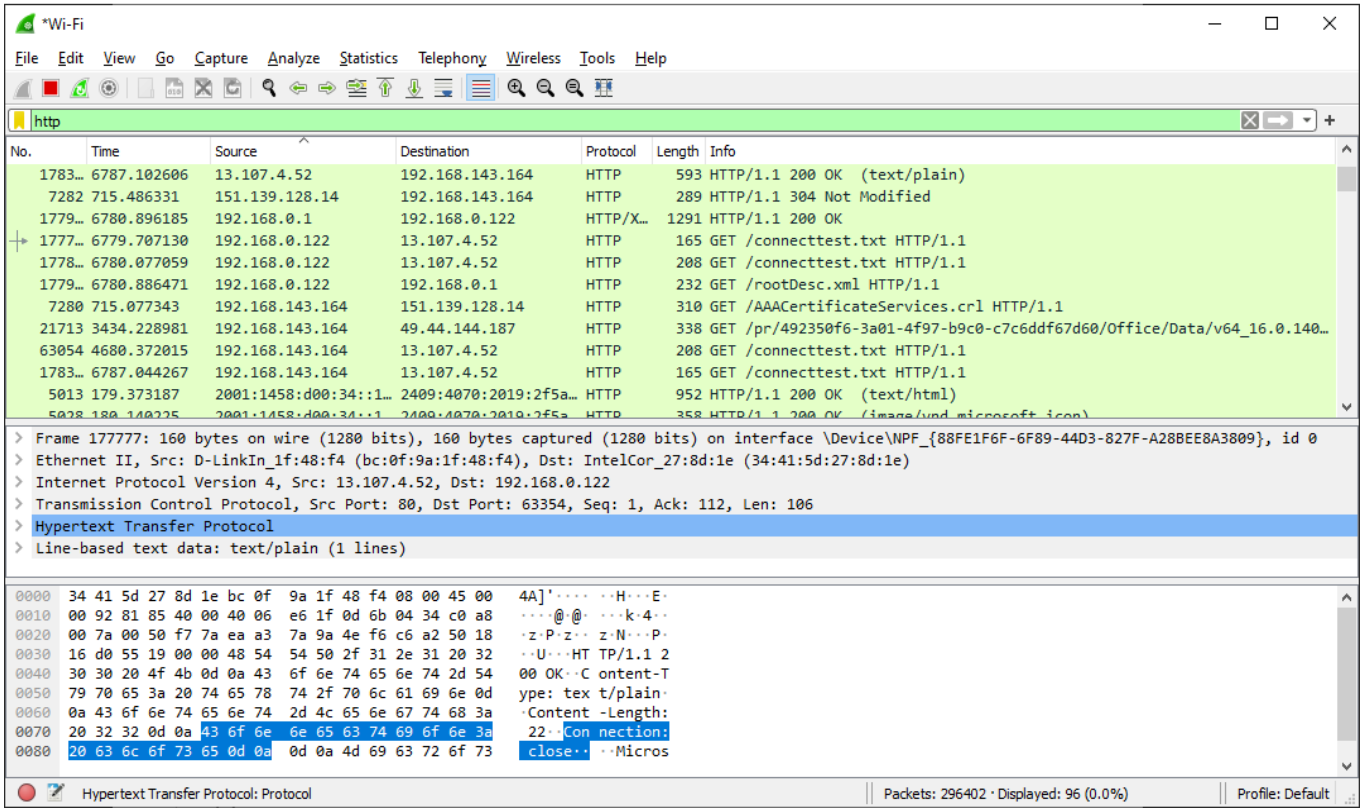
Q1) Retrieve web pages using HTTP. Use Wireshark to capture packets for analysis. Learn about mostcommon HTTP messages . Also capture response messages and analyze them.During the labsession, also examine and analyze some HTTP headers.

DETAILS:

HTTP is an application layer protocol invented by CERN in the late 1990s. It sends data over the secure TCP channel and uses an RDT mechanism. In HTTP, the data is shared in plain text format and hence can't be relied on to transfer confidential information such as passwords and credit card numbers.

Although the HTTP is stateless, it can't maintain a state, and you can no way ensure that two similar requests are delivered through the same connection. Hence it is unfit for e-commerce websites. But the HTTP protocol has sessions, which saves cookies and cache in the client's device and make it accessible to them in the state which is left. HTTP connection works on port number 80

HTTP messages are how data is exchanged between a server and a client. There are two types of messages: requests sent by the client to trigger an action on the server, and responses, the answer from the server.



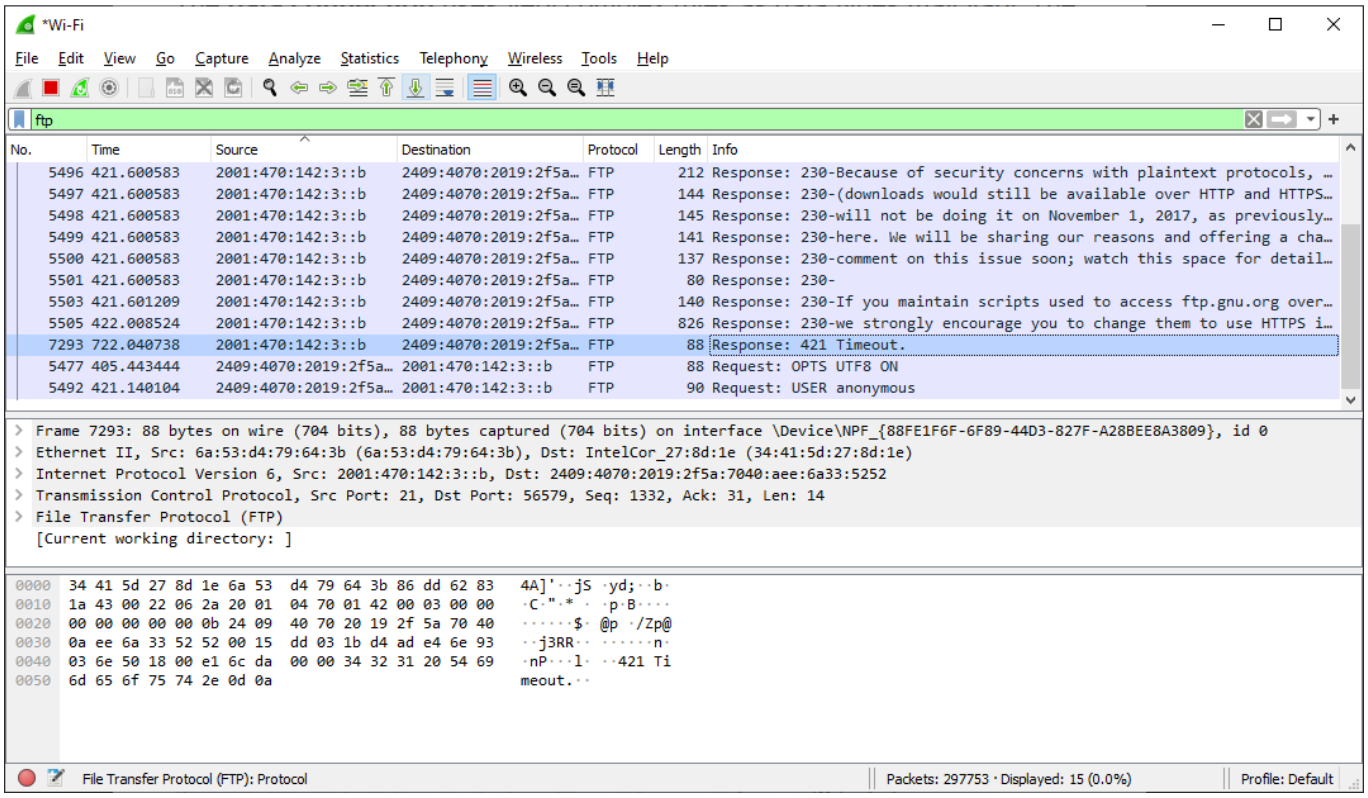
Q2) Use FTP to transfer some files, Use Wireshark to capture some packets. Show that FTP uses two separate connections: a control connection and a data-transfer connection. The data connection is opened and closed for each file transfer activity. Also show that FTP is an insecure file transfer protocol because the transaction is done in plaintext.

Details:

FTP is an application layer protocol that uses TCP for the transport layer similar to HTTP protocol. This is used for transferring files. Two TCP connections are used in parallel and are reliable for sharing confidential information, as port number 21 can be used to establish a controlled connection. The file-sharing usually takes place on port number 20.

When an FTP session is started between a client and a server, the client initiates a control TCP connection with the server-side. The client sends control information over this. When the server receives this, it creates a data connection to the client-side. Only one file can be sent over one data connection. But the control connection remains active throughout the user session. As we know, HTTP is stateless, i.e. it does not have to keep track of any user state. But FTP needs to maintain a state about its user throughout the session

FTP is insecure as we can see that data is in plain text format. In the below output we can clearly read “Time OUT”



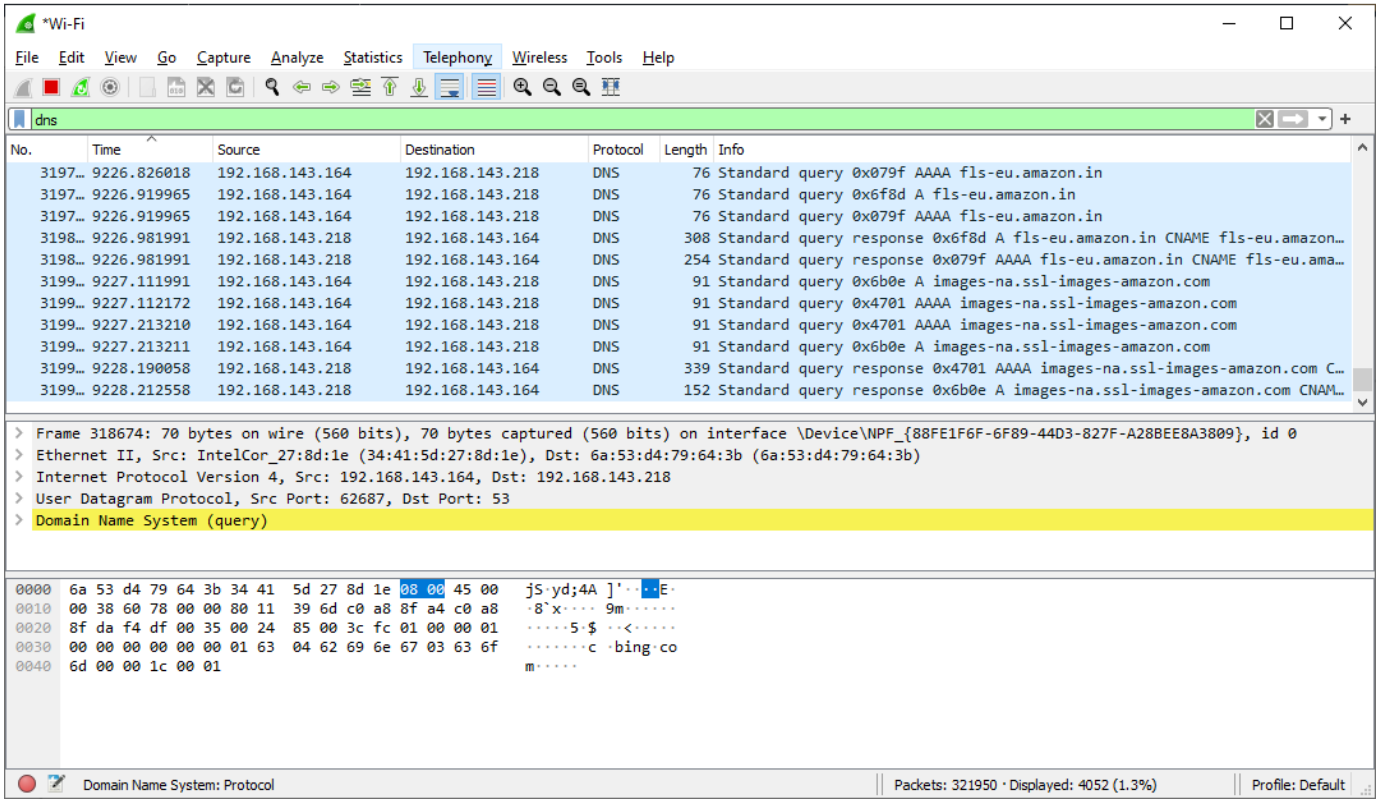
Q3) Analyze the behavior of the DNS protocol. In addition to Wireshark [Several network utilities are available for finding some information stored in the DNS servers. Eg.dig utilities (which has replaced nslookup). Set Wireshark to capture the packets sent by this utility.]

Details:

The Domain Name System (DNS) is the phonebook of the Internet. Humans access information online through domain names, like nytimes.com or espn.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Domain Name System helps to resolve the host name to an address. It uses a hierarchical naming scheme and distributed database of IP addresses and associated names

It is tough to find out the IP address associated with a website because there are millions of websites, and with all those websites, we should be able to generate the IP address immediately, there should not be a lot of delay for that to happen organisation of the database is very important. DNS helps in that regard


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
3197… 9226.826018 192.168.143.164 192.168.143.218 DNS 76 Standard query 0x079f AAAA fls-eu.amazon.in
3197… 9226.919965 192.168.143.164 192.168.143.218 DNS 76 Standard query 0x6f8d A fls-eu.amazon.in
3197… 9226.919965 192.168.143.164 192.168.143.218 DNS 76 Standard query 0x079f AAAA fls-eu.amazon.in
3198… 9226.981991 192.168.143.218 192.168.143.164 DNS 308 Standard query response 0x6f8d A fls-eu.amazon.in CNAME fls-eu.amazon…
3198… 9226.981991 192.168.143.218 192.168.143.164 DNS 254 Standard query response 0x079f AAAA fls-eu.amazon.in CNAME fls-eu.ama…
3199… 9227.111991 192.168.143.164 192.168.143.218 DNS 91 Standard query 0x6b0e A images-na.ssl-images-amazon.com
3199… 9227.112172 192.168.143.164 192.168.143.218 DNS 91 Standard query 0x4701 AAAA images-na.ssl-images-amazon.com
3199… 9227.213210 192.168.143.164 192.168.143.218 DNS 91 Standard query 0x4701 AAAA images-na.ssl-images-amazon.com
3199… 9227.213211 192.168.143.164 192.168.143.218 DNS 91 Standard query 0x6b0e A images-na.ssl-images-amazon.com
3199… 9228.190058 192.168.143.218 192.168.143.164 DNS 339 Standard query response 0x4701 AAAA images-na.ssl-images-amazon.com C…
3199… 9228.212558 192.168.143.218 192.168.143.164 DNS 152 Standard query response 0x6b0e A images-na.ssl-images-amazon.com CNAM…
Frame 318674: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{88FE1F6F-6F89-44D3-827F-A28BEE8A3809}, id 0
Ethernet II, Src: IntelCor_27:8d:1e (34:41:5d:27:8d:1e), Dst: 6a:53:d4:79:64:3b (6a:53:d4:79:64:3b)
Internet Protocol Version 4, Src: 192.168.143.164, Dst: 192.168.143.218
User Datagram Protocol, Src Port: 62687, Dst Port: 53
Domain Name System (query)
0000 6a 53 d4 79 64 3b 34 41 5d 27 8d 1e 08 00 45 00 jS·yd;4A]'····E·
0010 00 38 60 78 00 00 80 11 39 6d c0 a8 8f a4 c0 a8 ·8`x···· 9m····
0020 8f da f4 df 00 35 00 24 85 00 3c fc 01 00 00 01 ·····5·$ ··<·····
0030 00 00 00 00 00 00 01 63 04 62 69 6e 67 03 63 6f ·····c ·bing·co
0040 6d 00 00 1c 00 01 m·····
Domain Name System: Protocol
Packets: 321950 · Displayed: 4052 (1.3%)
Profile: Default