7/8/25

Exp:5 Experiment on packet capture tool: wireshark.

Aim:

Experiment on packet capture tool: wireshark.

wireshark:

A network analysis tool that captures real time network packet and displays them in human readable format.

key features:

1. Real time packet capture.
2. filtering
3. protocol decoding using dissectors
4. traffic browsing and smart statistics.

uses of wireshark:

1. Network Admin: Troubleshoot network issue.
2. Analyze security incidents
3. Debug network protocol implementation
4. understand protocols internals.

window: Download wireshark from official website.

a, capture packets:

Launch wireshark and double click a network interface to begin capturing packets.

Packets appear in real time and include all traffic of promiscous mode is enabled capture options > Enable promiscous mode.

b, coding colours:-

using of light purple to TCP.

Light blue for UDP.

Black refers to error packets view (or) customize colours:

view → coloring rule.

c, sample capture:-

* Load sample capture from wireshark | wifi via file > open.

* Save your own capture using file > save.

d, filtering packets:-

a, use the filter bar to isolate traffic

* press enter (or) click apply.

to use the filter.

* Access default/custom filters with Analyze → display filters.

c, following TCP streams:-

* Right click a packet → follow → TCP Stream

* close window auto apply a filter for that conversation.

Inspecting packets:-

* click a packet to see its details.

* Right click protocol fields → Apply a filter based on it.

Flow graph:-

* use statistics.

* visually traffic flow between devices flow graph.

Capturing and Analysing packets using wireshark tool:

Procedure:-

* Select Local Area Selection

* capture → options → set stop after 100 packets.

* click start
* save packets.

filter :- display TCP/UDP packets and show flow graph.

Procedure :-

* start capture as above.
* In filter bar, search tcp or udp.
* statistics > flow graph to views.
* save packets.

filter :- Display only ARP packets.

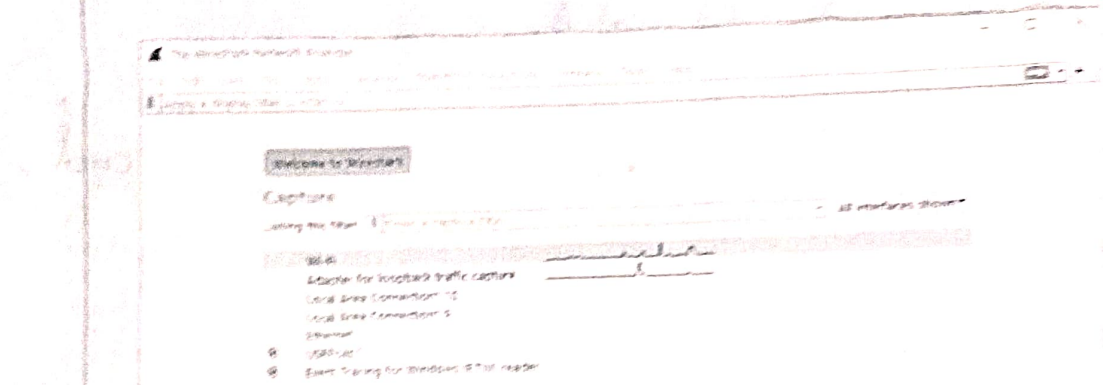
* short capture as above.
* In filter bar, type UDP.
* save packets.

filter :- Display only DNS packets and show flow graph.

* short capture as above
* In filter bar, type dns
* statistics > flow graph.
* save packets.

filter :- Display only HTTPS packets :-

* short capture as above
* in filter bar, type, HTTPS.
* save packets.



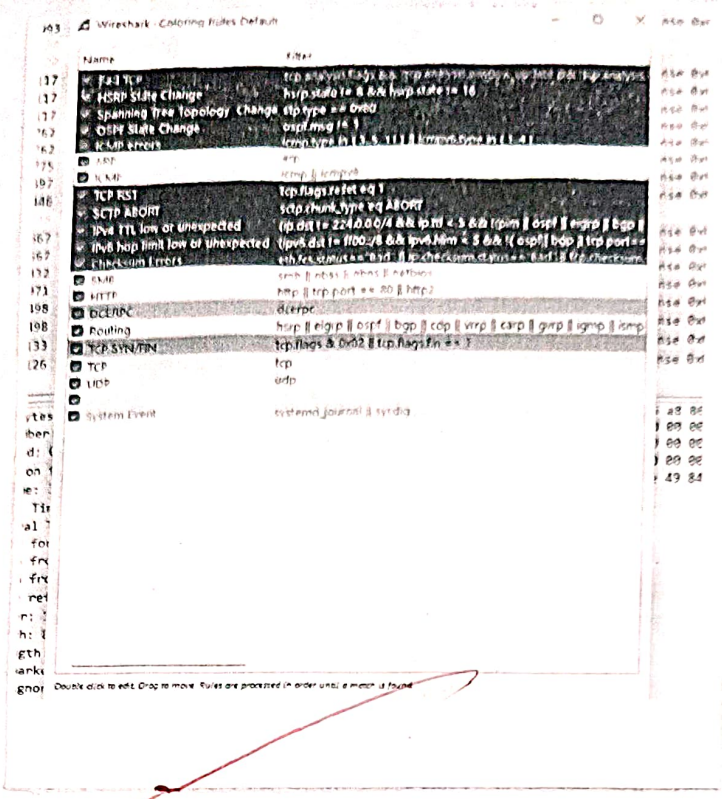
Capturing from Wi-Fi

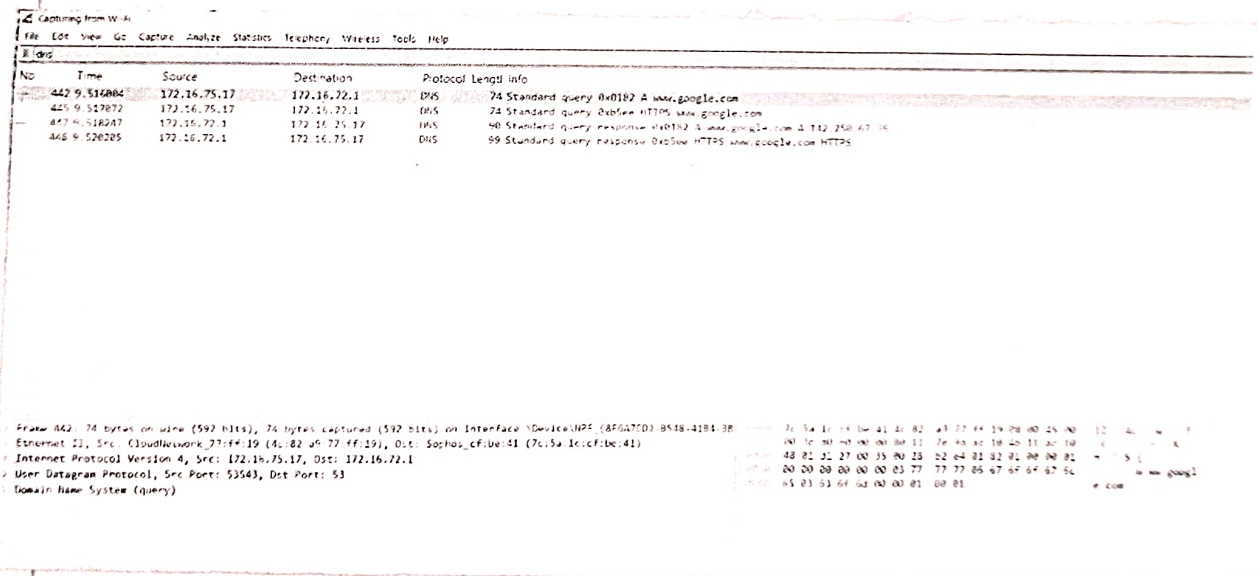
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

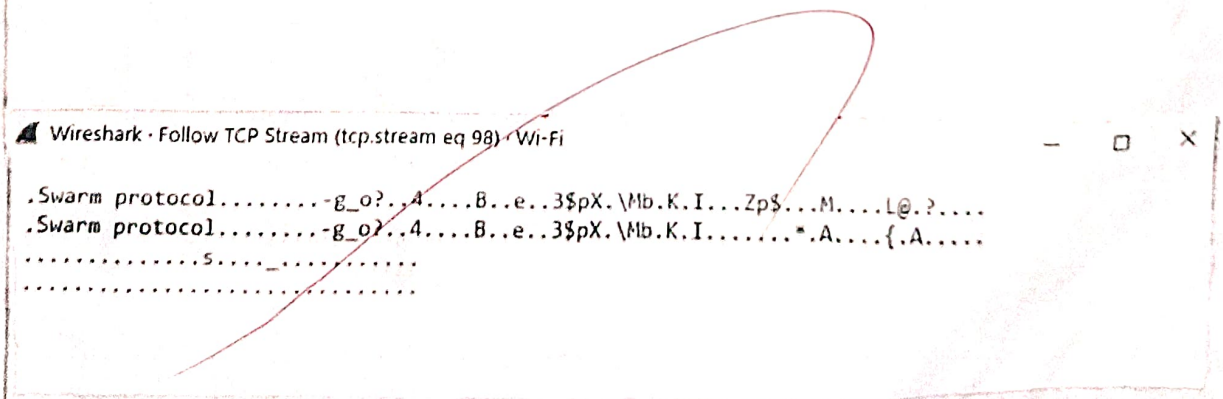
No.	Time	Source	Destination	Protocol	Length	Info
369	5.122991	fe80::e35e:b1ff:423…	ff02::fb	MDNS	319	Standard query response 0x0000 PTR DEL
370	5.122991	172.16.75.134	224.0.0.251	MDNS	299	Standard query response 0x0000 PTR DEL
371	5.122991	fe80::4983:8ee3:3c3…	ff02::fb	MDNS	328	Standard query response 0x0000 PTR DEL
372	5.124455	172.16.75.143	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR DEL
374	5.125749	172.16.75.138	224.0.0.251	MDNS	1177	Standard query response 0x0000 PTR DEL
375	5.125749	172.16.75.138	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR DEL
376	5.125749	172.16.75.151	224.0.0.251	MDNS	909	Standard query response 0x0000 PTR DEL
377	5.128353	172.16.75.134	224.0.0.251	MDNS	308	Standard query response 0x0000 PTR DEL
379	5.128353	fe80::ecf5:1acf:3c5…	ff02::fb	MDNS	319	Standard query response 0x0000 PTR DEL
380	5.129732	172.16.75.142	224.0.0.251	MDNS	1471	Standard query response 0x0000 PTR DEL
381	5.131317	fe80::51cd:5857:155…	ff02::fb	MDNS	1237	Standard query response 0x0000 PTR DEL
382	5.131317	fe80::3c3a:1528:8ea…	ff02::fb	MDNS	929	Standard query response 0x0000 PTR DEL
383	5.131317	fe80::422c:a4d1:845…	ff02::1:2	DHCPv6	128	Information-request XID: 0x5c2df0 CID:
384	5.147739	172.16.75.17	142.251.228.118	UDP	71	62039 → 443 Len=29
385	5.155736	142.251.228.118	172.16.75.17	UDP	68	443 → 62039 Len=26
386	5.157188	172.16.75.17	142.251.228.186	UDP	71	52994 → 443 Len=29
387	5.160145	142.251.228.186	172.16.75.17	UDP	68	443 → 52994 Len=26
388	5.388561	172.16.75.17	142.251.228.186	UDP	71	52994 → 443 Len=29

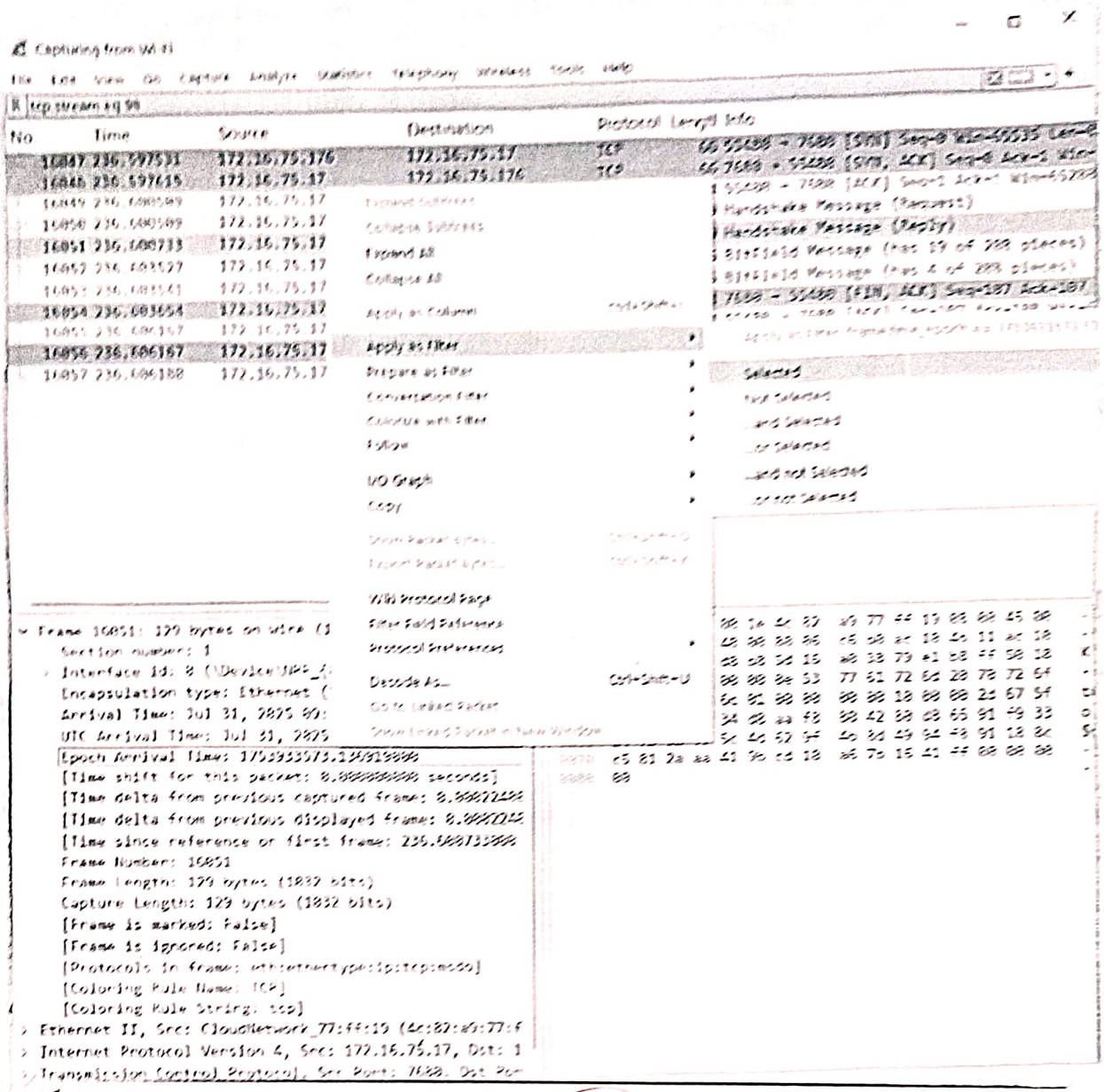
```
▸ Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (
▸ Ethernet II, Src: GigaByteTech_53:a5:a8 (e0:d5:5e:53:a5:a
▸ Internet Protocol Version 6, Src: fe80::e2d5:5eff:fe53:a5
▸ Internet Control Message Protocol v6
```

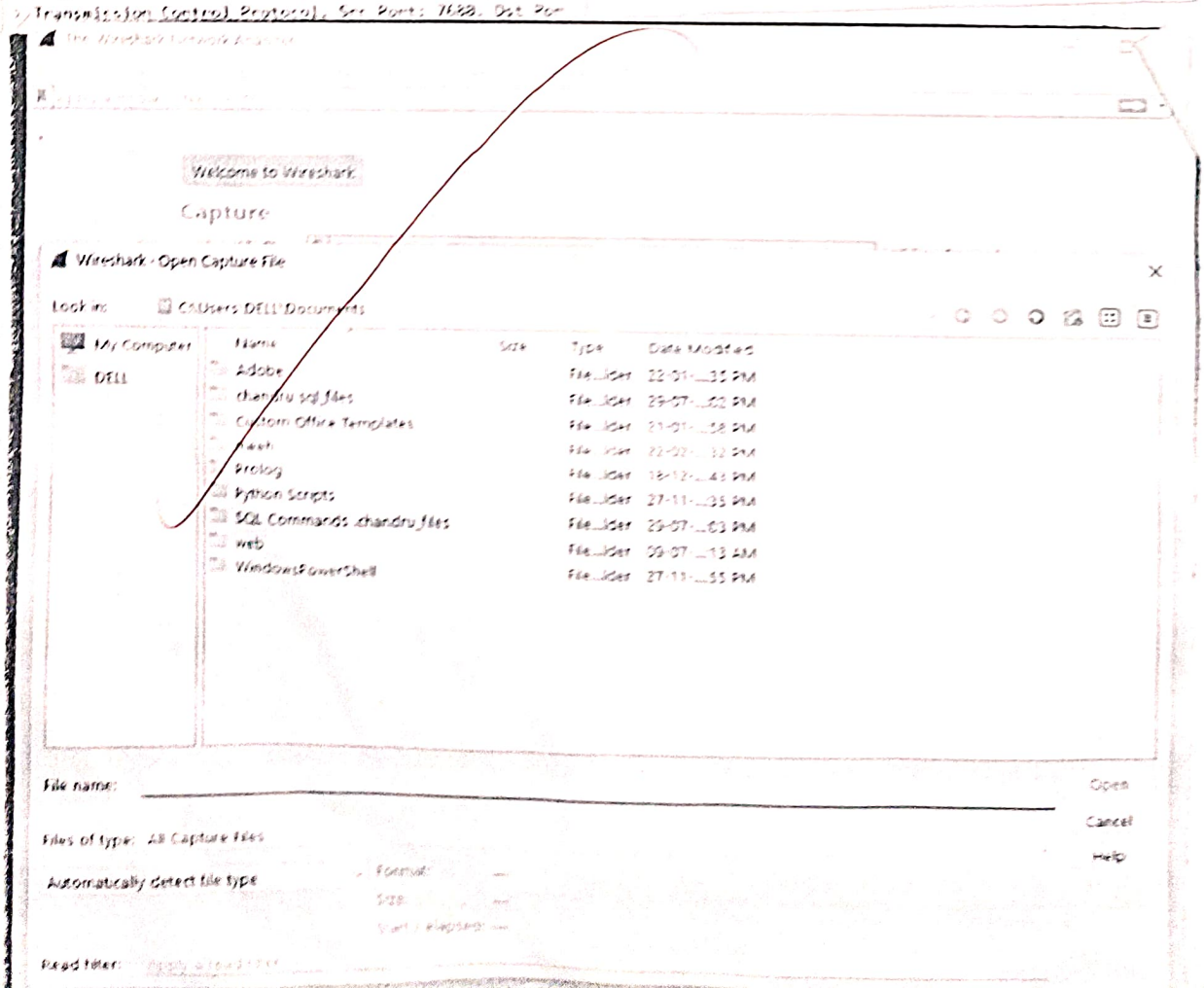
```
0000  33 33 ff 49 84 b2 e0 d5  5e 53 a5 a8 86 dd 60 00   33 I
0010  00 00 00 20 3a ff fe 80  00 00 00 00 00 00 e2 d5
0020  5e ff fe 53 a5 a8 ff 02  00 00 00 00 00 00 00 00
0030  00 01 ff 49 84 b2 87 00  cc 47 00 00 00 00 fe 80
0040  00 00 00 00 00 00 86 ba  d5 ff fe 49 84 b2 01 01
0050  e0 d5 5e 53 a5 a8
```


Wireshark · Coloring Rules Default
Name
Filter
TCP RST
tcp.flags.reset eq 1
SCTP ABORT
sctp.chunk_type eq ABORT
Routing
TCP SYN/FIN
tcp.flags & 0x02 && tcp.flags.fin == 1
TCP
tcp
UDP
udp
Double click to edit. Drag to move. Rules are processed in order until a match is found.


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
442 9.516884 172.16.75.17 172.16.72.1 DNS 74 Standard query 0x0182 A www.google.com
445 9.517872 172.16.75.17 172.16.72.1 DNS 74 Standard query 0xbfee HTTPS www.google.com
447 9.518247 172.16.72.1 172.16.75.17 DNS 90 Standard query response 0x0182 A www.google.com A 142.250.67.36
448 9.520205 172.16.72.1 172.16.75.17 DNS 99 Standard query response 0xbfee HTTPS www.google.com HTTPS
Frame 442: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{8F6A7C0D-B538-41B1-8F
Ethernet II, Src: CloudNetwork_77:ff:19 (4c:82:a9:77:ff:19), Dst: Sophos_cf:be:41 (7c:5a:1c:cf:be:41)
Internet Protocol Version 4, Src: 172.16.75.17, Dst: 172.16.72.1
User Datagram Protocol, Src Port: 53543, Dst Port: 53
Domain Name System (query)


Wireshark · Follow TCP Stream (tcp.stream eq 98) · Wi-Fi
.Swarm protocol.....-g_o?..4....B..e..3$pX.\Mb.K.I...Zp$...M....L@.?....
.Swarm protocol.....-g_o?..4....B..e..3$pX.\Mb.K.I.....*.A....{.A.....
.....s....._.....
.....


Capturing from Wi-Fi
tcp.stream eq 99
No Time Source Destination Protocol Length Info
16847 236.597531 172.16.75.176 172.16.75.17 TCP
16848 236.597615 172.16.75.17 172.16.75.176 TCP
16849 236.600589 172.16.75.17
16850 236.600589 172.16.75.17
16851 236.600733 172.16.75.17
16852 236.603527 172.16.75.17
16853 236.603541 172.16.75.17
16854 236.603654 172.16.75.17
16855 236.606167 172.16.75.17
16856 236.606167 172.16.75.17
16857 236.606180 172.16.75.17
Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
I/O Graph
Copy
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window
Selected
Not Selected
and Selected
or Selected
and not Selected
or not Selected
Frame 16851: 129 bytes on wire (1
Section number: 1
Interface id: 8 (\Device\NPF_{
Encapsulation type: Ethernet (
Arrival Time: Jul 31, 2025 09:
UTC Arrival Time: Jul 31, 2025
Epoch Arrival Time: 1753933573.235918000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000172000
[Time delta from previous displayed frame: 0.000172000
[Time since reference or first frame: 236.600733000
Frame Number: 16851
Frame Length: 129 bytes (1032 bits)
Capture Length: 129 bytes (1032 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:mssq]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: CloudNetwork_77:ff:19 (4c:89:89:77:f
Internet Protocol Version 4, Src: 172.16.75.17, Dst: 1
Transmission Control Protocol, Src Port: 7688, Dst Por


Welcome to Wireshark
Capture
Wireshark · Open Capture File
Look in: C:\Users\DELL\Documents
My Computer
DELL
Name Size Type Date Modified
Adobe File folder 22-01-... 3 PM
chandru sql files File folder 29-07-... 02 PM
Custom Office Templates File folder 21-01-... 58 PM
Flash File folder 22-02-... 12 PM
Proteus File folder 18-12-... 43 PM
Python Scripts File folder 27-11-... 35 PM
SQL Commands chandru files File folder 29-07-... 03 PM
web File folder 29-07-... 13 AM
WindowsPowerShell File folder 27-11-... 55 PM
File name:
Open
Cancel
Help
Files of type: All Capture Files
Automatically detect file type
Format:
Size:
Start / elapsed:
Read filter:

student observation:

1. What is promiscous mode?
   It allows a network device to capture all packets on the network not just those addressed to it.

2. Does ARP packets has transport layer headers? Explain?
   No, ARP operates at Data link and network layer and does not have a transport layer headers.

3. Which transport layer protocol is used by DNS?
   DNS user UDP by default and TCP for large queries like zone transfer.

4. What is the port number used by http protocol?
   Port 80 is used by Http protocol.

5. What is broadcast ip address?
   It is 255.255.255.255 used to send data to all hosts on a local network.

Result...
Thus the above experiment successfully completed and executed.