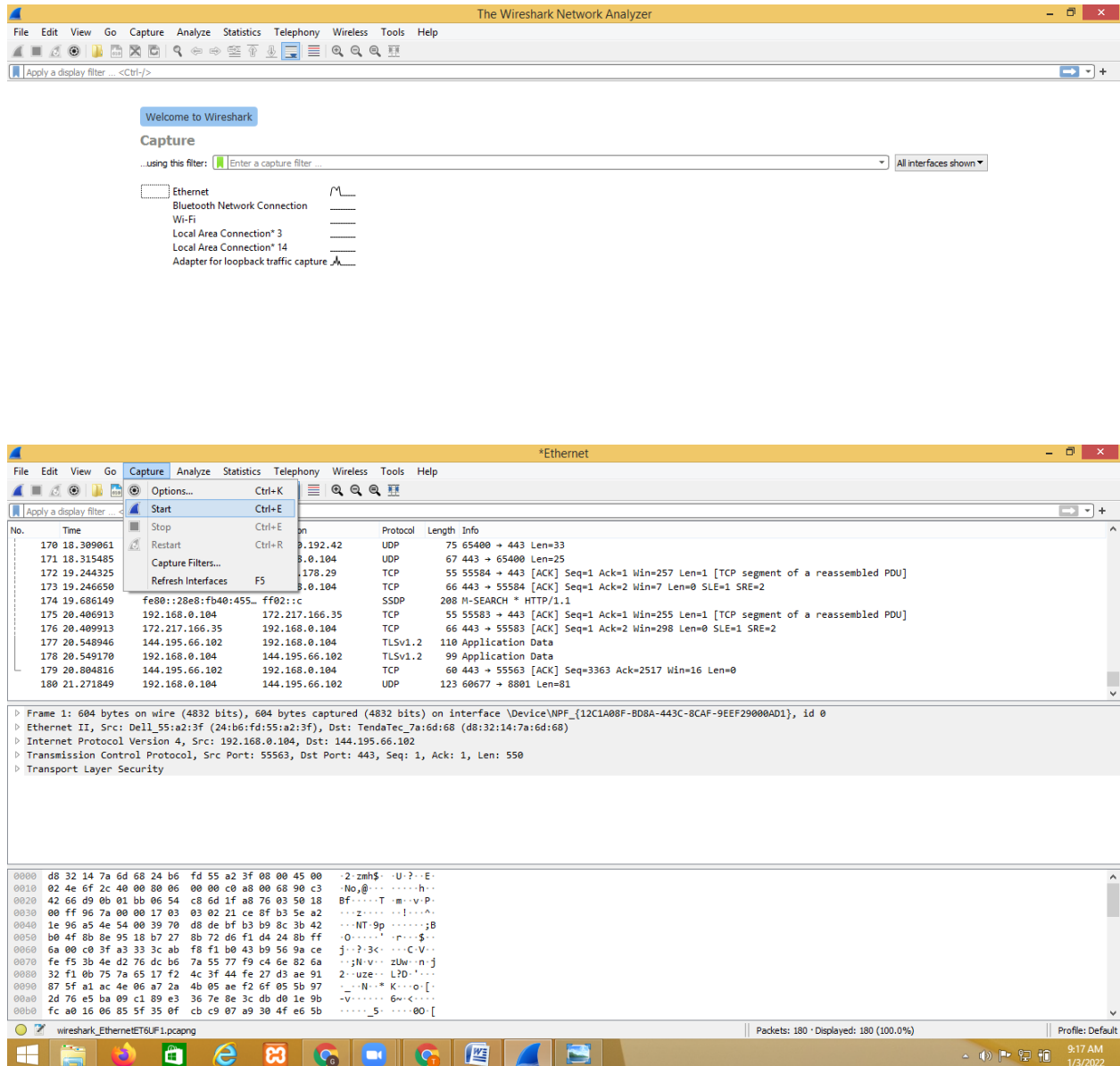


Practical:4

Aim: Capturing and analyzing network packets using Wireshark (Fundamentals):

- Identification the live network
- Capture Packets
- Analyze the captured packets

1. Open Wireshark



Practical:4

The screenshot shows a Wireshark capture titled "Capturing from Wi-Fi". The packet list on the left shows a series of SSDP and PNRP messages. The packet details pane on the right shows the structure of a frame, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Dynamic Host Configuration Protocol (Request). The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
2041	48.225900	fe80::28e8:fb40:455...	fe80::611f:77fa:cb4...	SSDP	453	HTTP/1.1 200 OK
2042	48.697963	fe80::28e8:fb40:455...	fe80::611f:77fa:cb4...	SSDP	453	HTTP/1.1 200 OK
2043	49.424370	fe80::611f:77fa:cb4...	fe80::28e8:fb40:455...	SSDP	452	HTTP/1.1 200 OK
2044	49.442680	fe80::611f:77fa:cb4...	fe80::28e8:fb40:455...	SSDP	452	HTTP/1.1 200 OK
2045	51.016571	fe80::611f:77fa:cb4...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2046	51.018063	fe80::611f:77fa:cb4...	fe80::28e8:fb40:455...	PNRP	98	PNRP SOLICIT Message [Malformed Packet]
2047	51.020164	fe80::28e8:fb40:455...	fe80::611f:77fa:cb4...	PNRP	150	PNRP ADVERTISE Message [Malformed Packet]
2048	51.020389	fe80::611f:77fa:cb4...	fe80::28e8:fb40:455...	PNRP	138	PNRP REQUEST Message [Malformed Packet]
2049	51.032899	fe80::28e8:fb40:455...	fe80::611f:77fa:cb4...	PNRP	82	PNRP ACK Message [Malformed Packet]
2050	51.032899	fe80::28e8:fb40:455...	fe80::611f:77fa:cb4...	PNRP	190	PNRP FLOOD Message [Malformed Packet]
2051	51.131342	fe80::28e8:fb40:455...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

Frame 1: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface \Device\NPF_{CC53721B-AE31-41C6-A8A9-1C9452174AFA}, id 0
Ethernet II, Src: HonHaiPr_a1:b0:2f (cc:af:78:a1:b0:2f), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)

Bytes 30-33: Destination Address (p.dst) | Packets: 2051 · Displayed: 2051 (100.0%) | Profile: Default

TCP package: search TCP package

The screenshot shows a Wireshark capture titled "*Ethernet". The packet list on the left shows a series of TCP and TLSv1.2 messages. The packet details pane on the right shows the structure of a frame, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Transport Layer Security. The packet bytes pane at the bottom shows the raw data of the selected packet.

No.	Time	Source	Destination	Protocol	Length	Info
3344	64.248338	193.123.149.194	192.168.0.104	TCP	60	443 → 55364 [ACK] Seq=4035 Ack=6718 Win=16 Len=0
3494	66.862140	192.168.0.104	193.123.149.194	TLSv1.2	132	Application Data
3507	67.059839	193.123.149.194	192.168.0.104	TCP	60	443 → 55364 [ACK] Seq=4035 Ack=6796 Win=16 Len=0
3508	67.059990	193.123.149.194	192.168.0.104	TLSv1.2	140	Application Data
3509	67.070213	192.168.0.104	193.123.149.194	TLSv1.2	104	Application Data
3521	67.273053	193.123.149.194	192.168.0.104	TLSv1.2	133	Application Data
3522	67.273450	192.168.0.104	193.123.149.194	TLSv1.2	104	Application Data
3537	67.510570	193.123.149.194	192.168.0.104	TCP	60	443 → 55364 [ACK] Seq=4200 Ack=6896 Win=16 Len=0
3538	67.518809	193.123.149.194	192.168.0.104	TLSv1.2	133	Application Data
3539	67.529968	192.168.0.104	193.123.149.194	TLSv1.2	104	Application Data

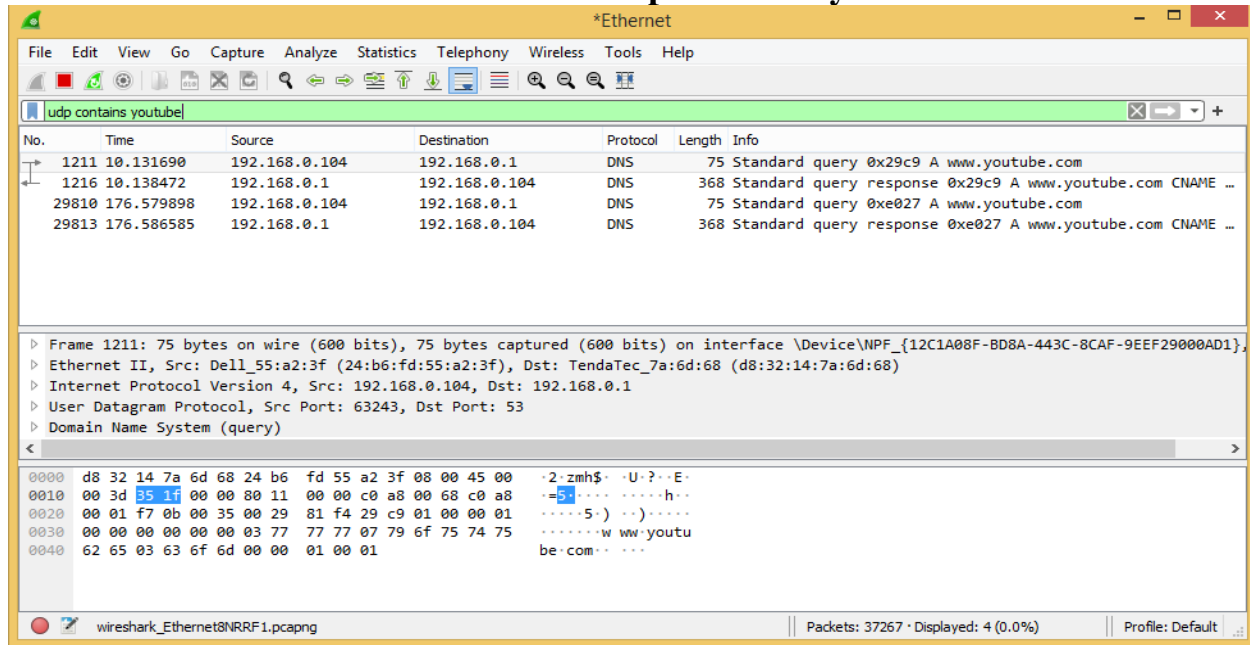
Frame 9: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{12C1A08F-BD8A-443C-8CAF-9EEF2900AD1}, id 0
Ethernet II, Src: Dell_55:a2:3f (24:b6:fd:55:a2:3f), Dst: TendaTec_7a:6d:68 (d8:32:14:7a:6d:68)
Internet Protocol Version 4, Src: 192.168.0.104, Dst: 193.123.149.194
Transmission Control Protocol, Src Port: 55364, Dst Port: 443, Seq: 1, Ack: 1, Len: 45
Transport Layer Security

wireshark_EthernetQOCsF1.pcapng | Packets: 3545 · Displayed: 253 (7.1%) | Profile: Default

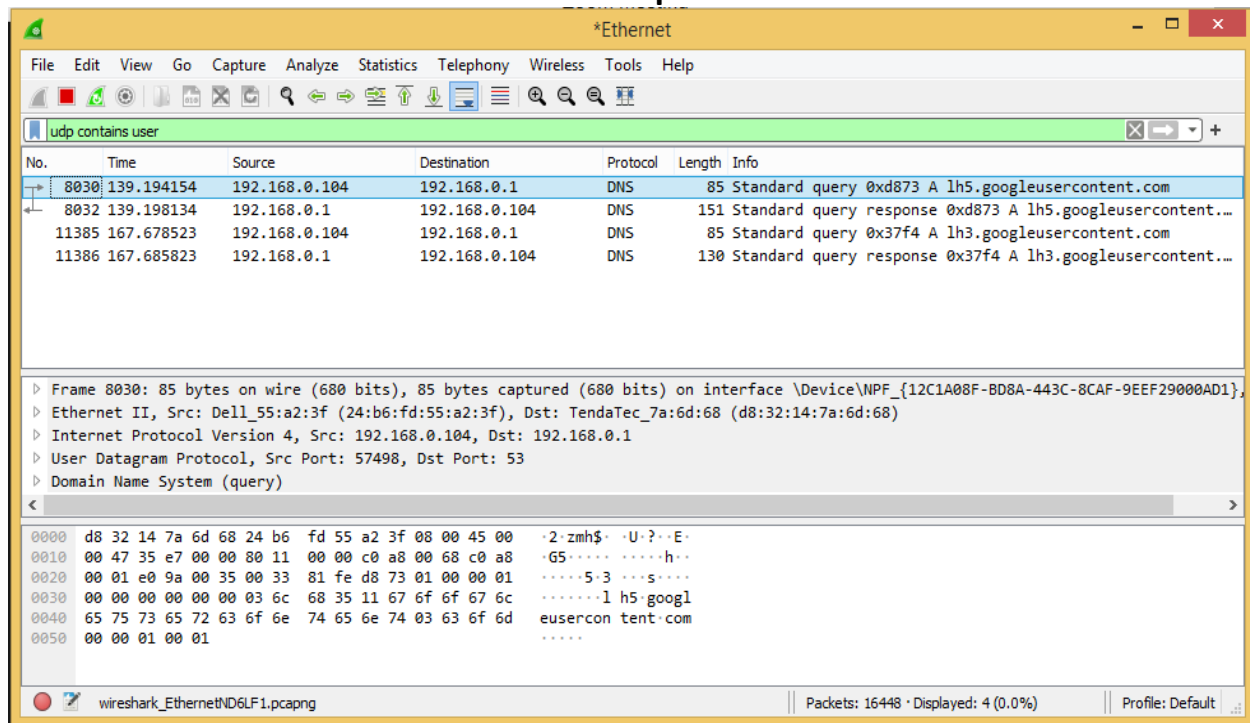
Practical:4

Analysis youtube data

Now go on browser and open youtube and perform some activity on the youtube
Now come back to Wireshark and enter **udp contains youtube** in the search bar.

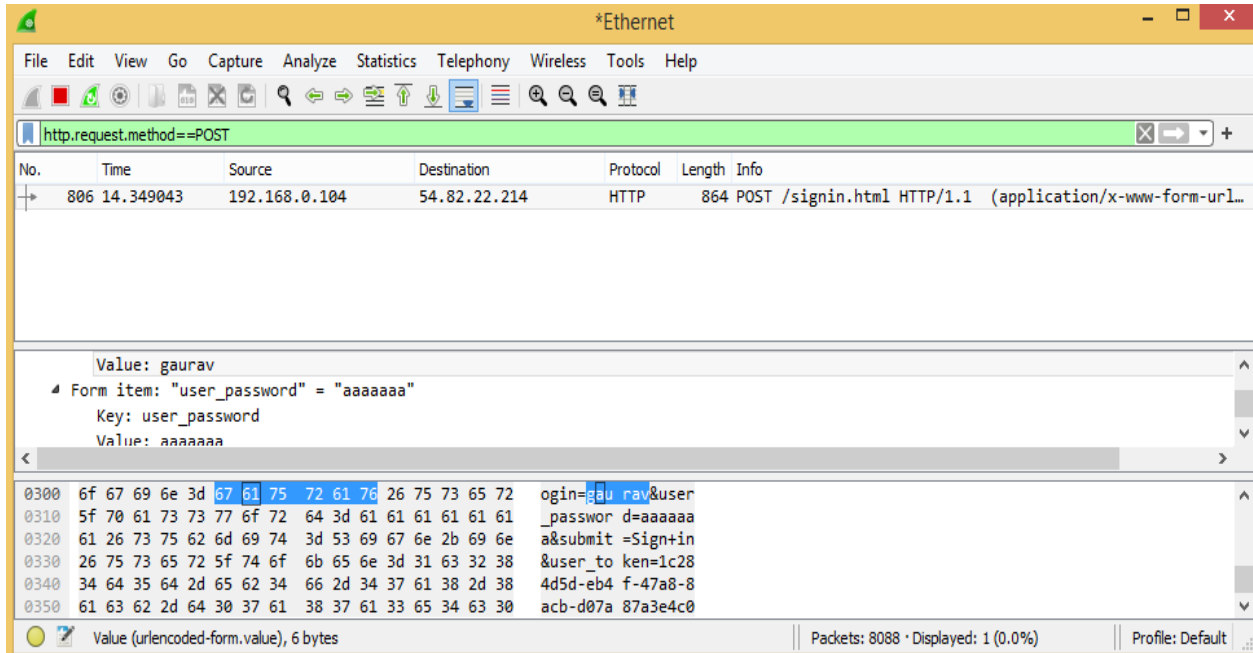


search udp contains user: Now go on browser, login in any secured website and
Now come back to Wireshark and enter **udp contains user** in the search bar.

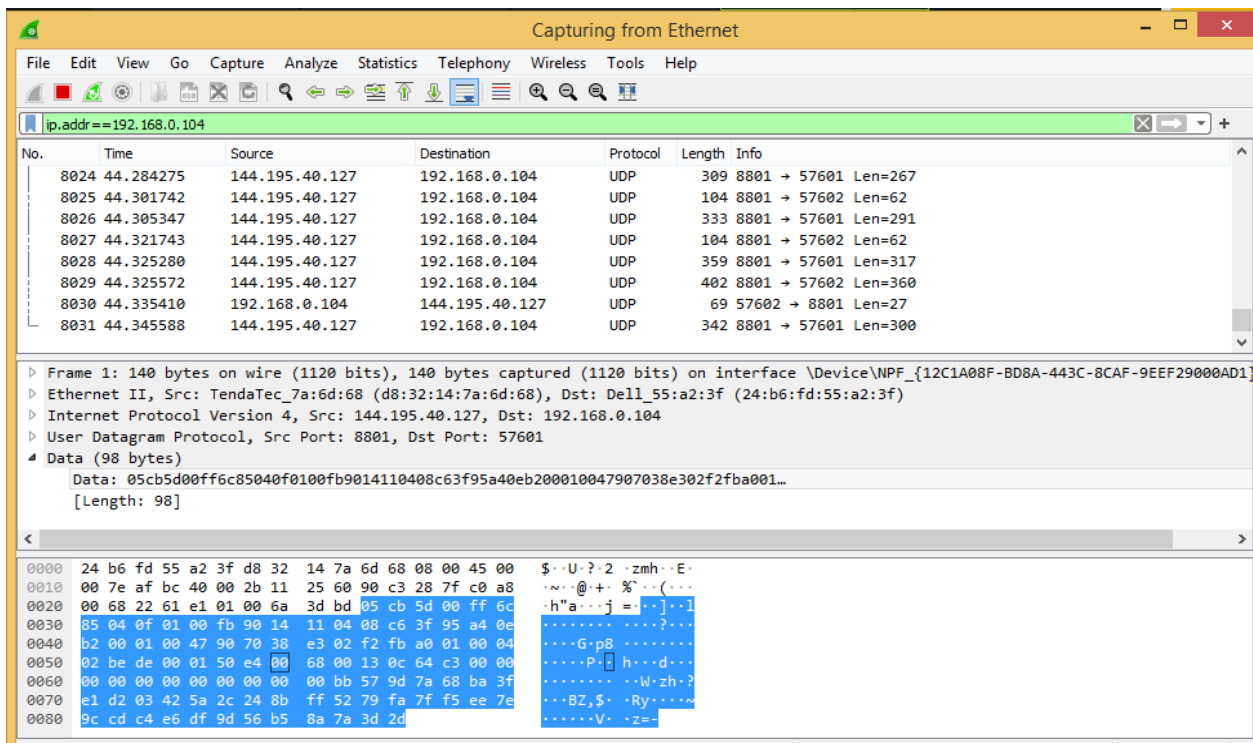


Practical:4

http website: go on browser, login in any unsecured website and Now come back to Wireshark and enter **http.request.method==POST** in the search bar. You can view the username and password because it is http website

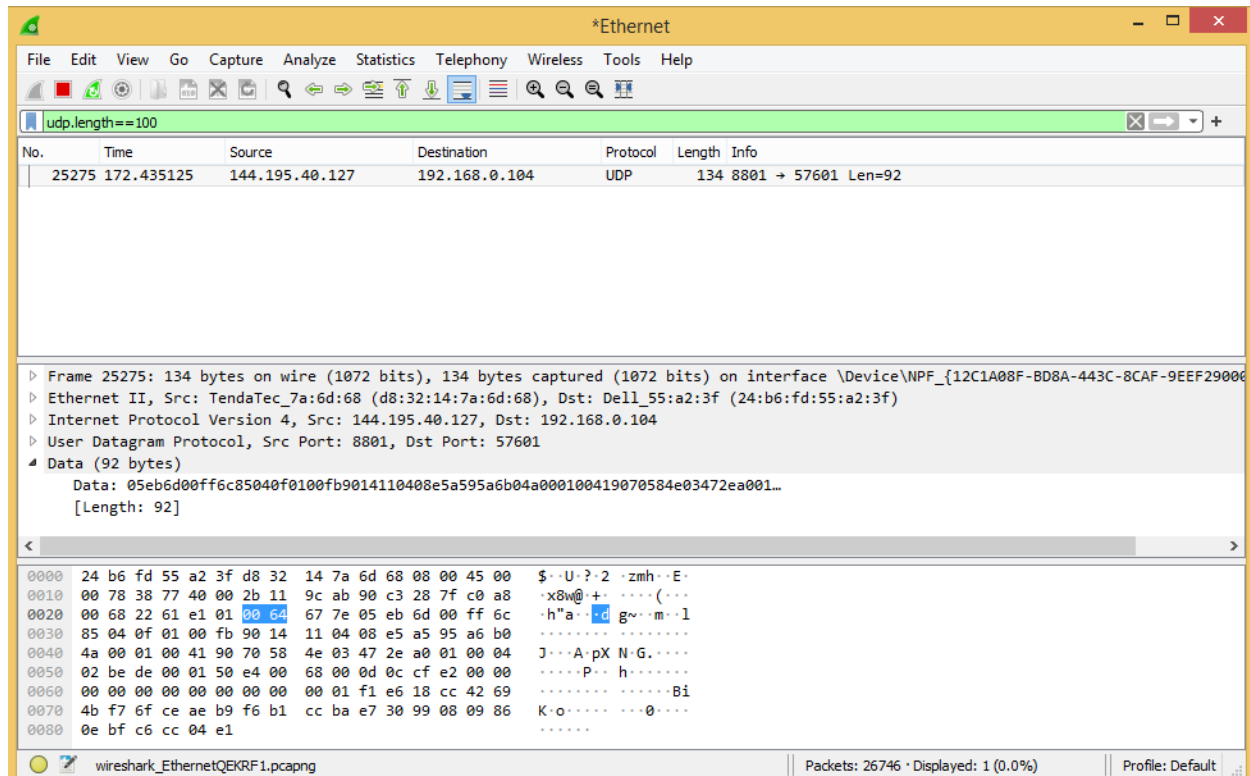


filter with ip: `ip.addr==192.168.0.104`



Practical:4

filter udp package with length : `udp.length==100`



Many other filter expression

