

St. Francis Institute of Technology
Department of Computer Engineering

COMPUTER NETWORK LAB

EXPERIMENT NO.5

AIM: Use Wire shark to understand the operation of TCP/IP layers:

- Ethernet Layer: Frame header, Frame size etc.
- Data Link Layer: MAC address, ARP (IP and MAC address binding)
- Network Layer: IP Packet (header, fragmentation), ICMP (Query and Echo)
- Transport Layer: TCP Ports, TCP handshake segments etc.

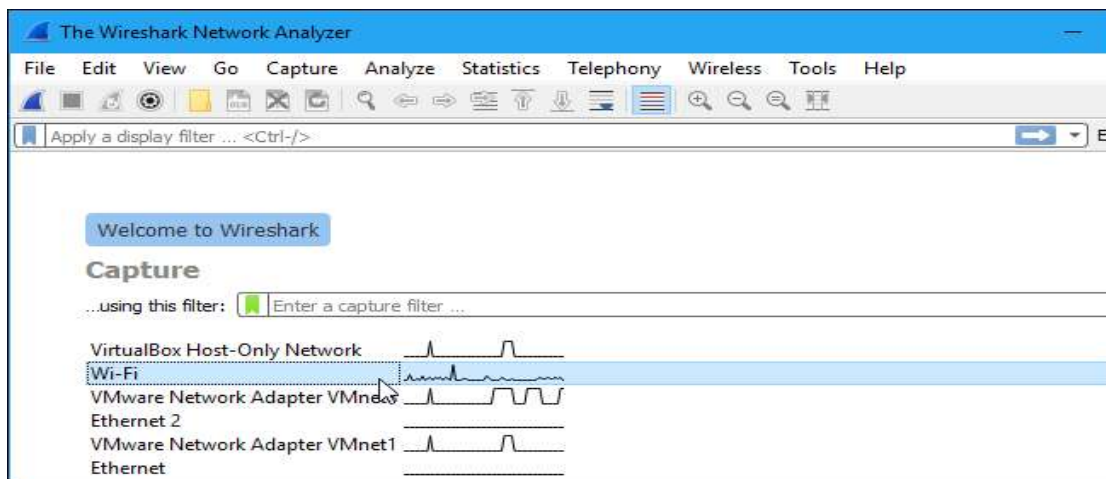
Application Layer: DHCP, FTP, HTTP header formats

THEORY:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

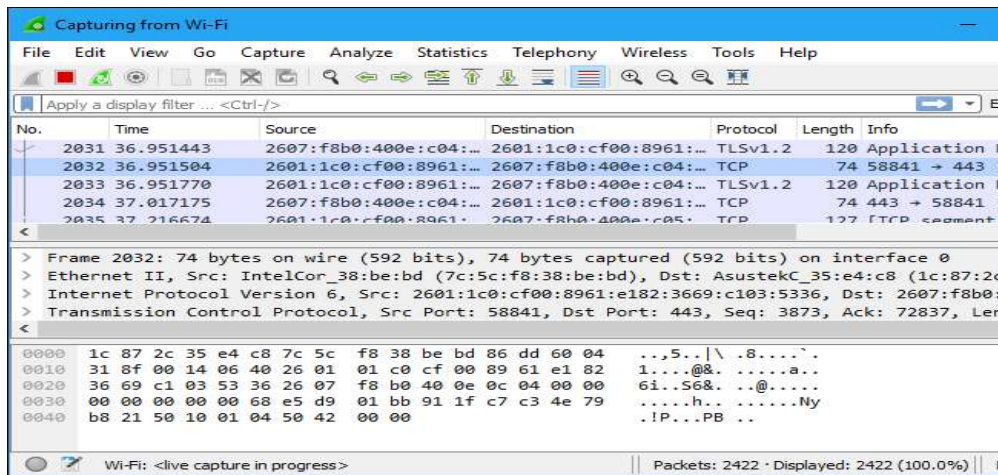
Capturing Packets

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn't necessary for now.

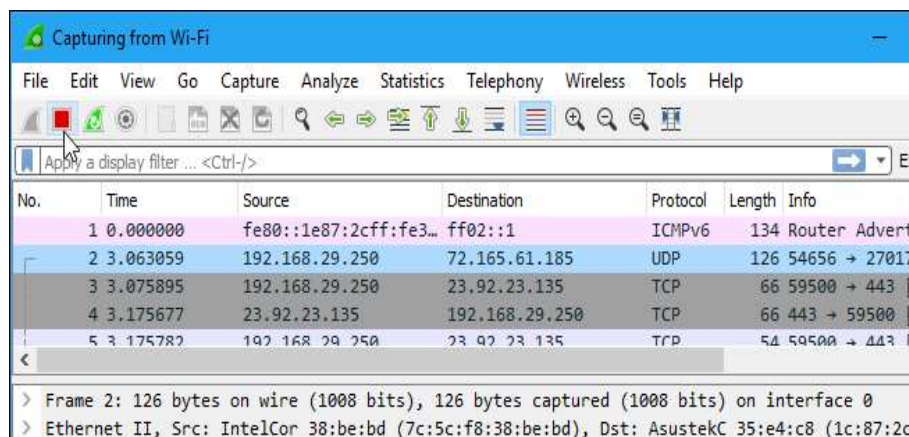


As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



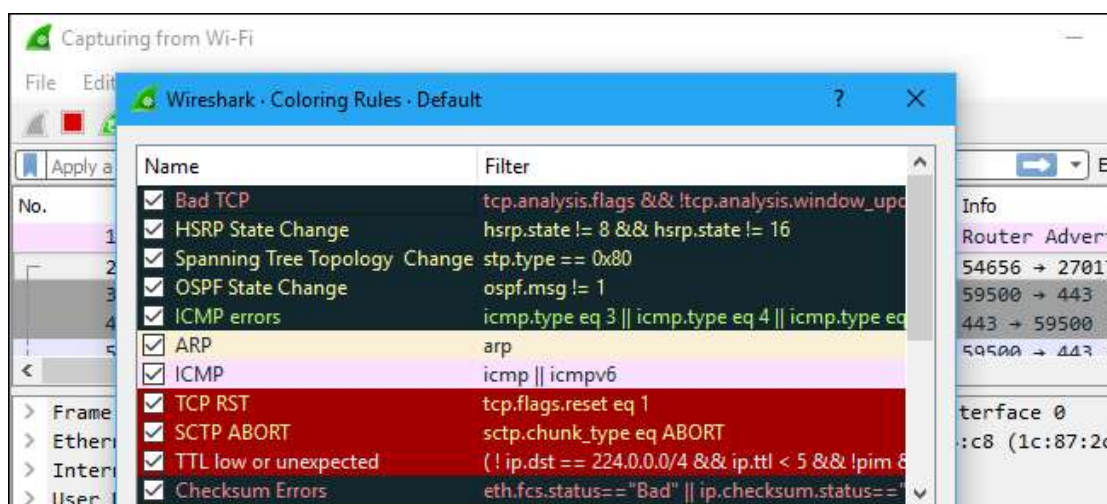
Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.



Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

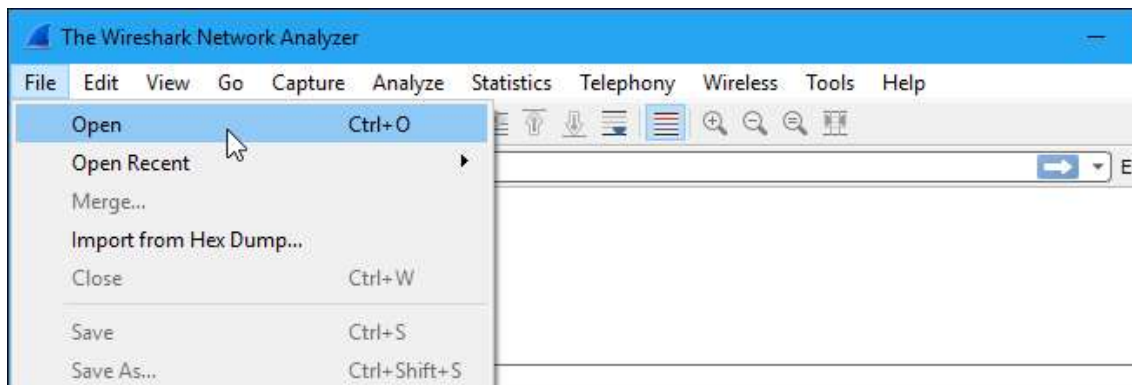
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

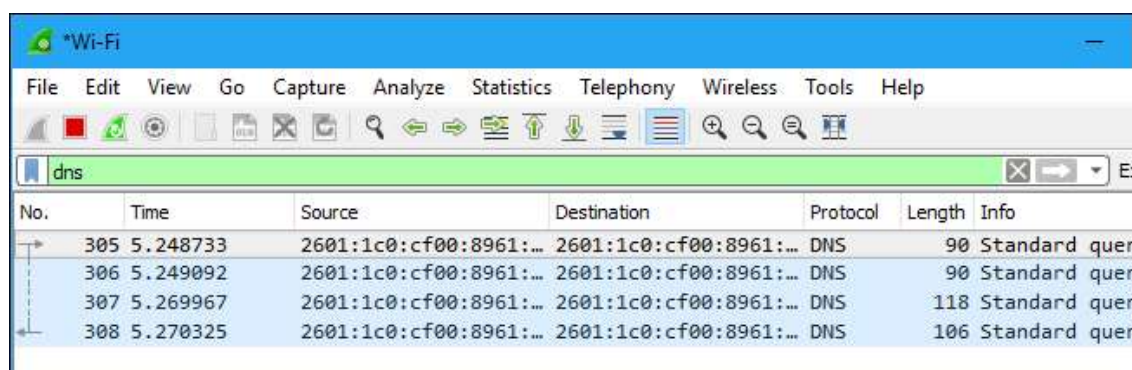
You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.



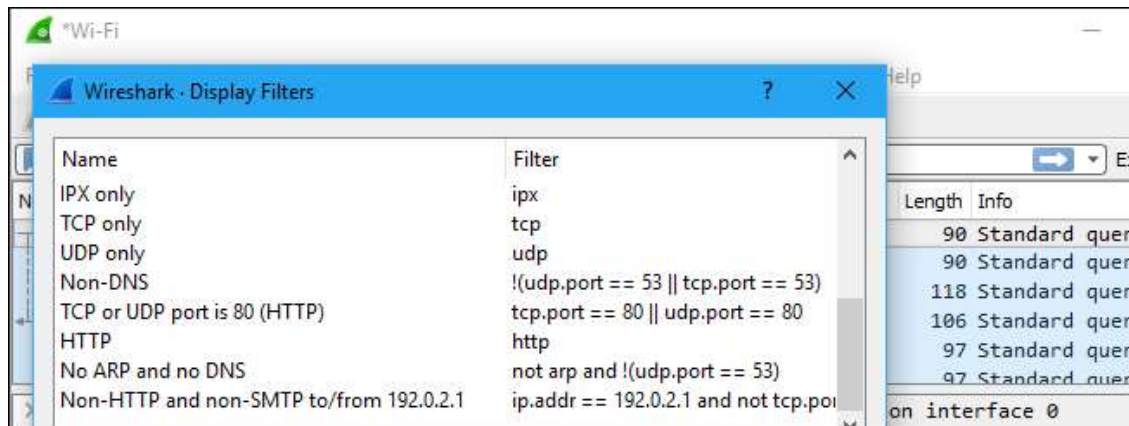
Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most **basic way** to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.

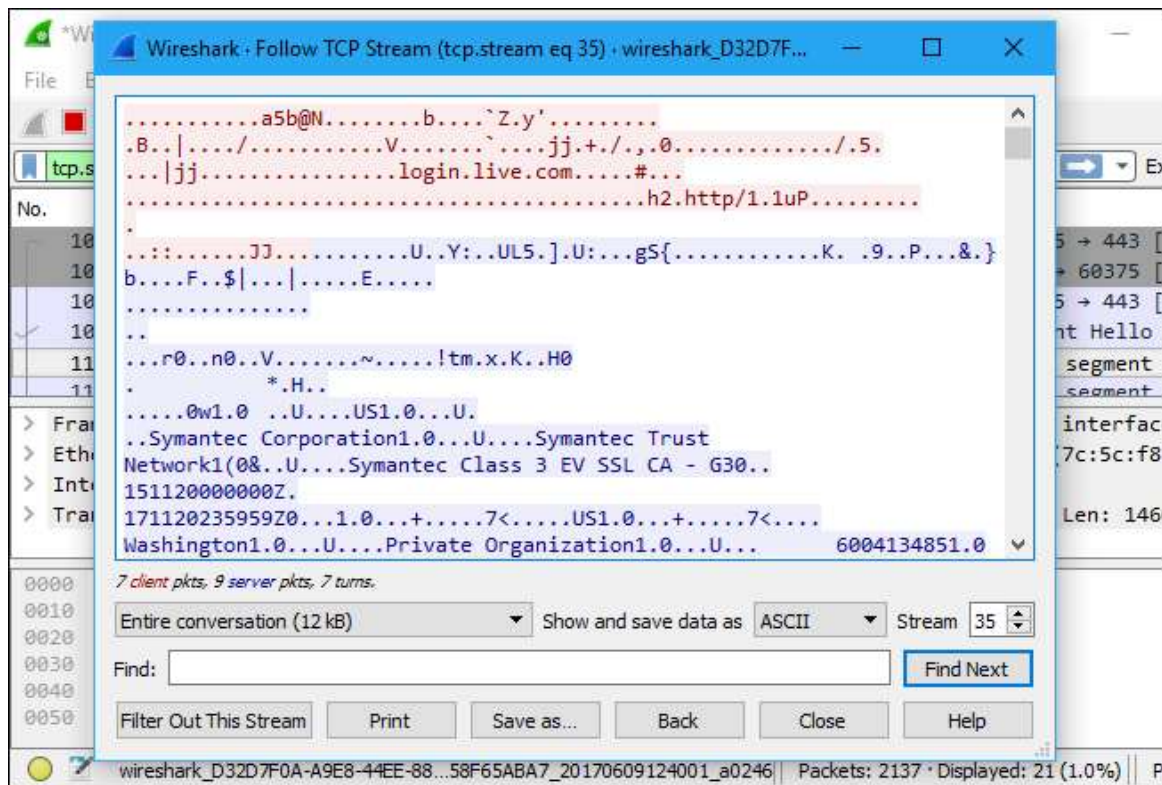


You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

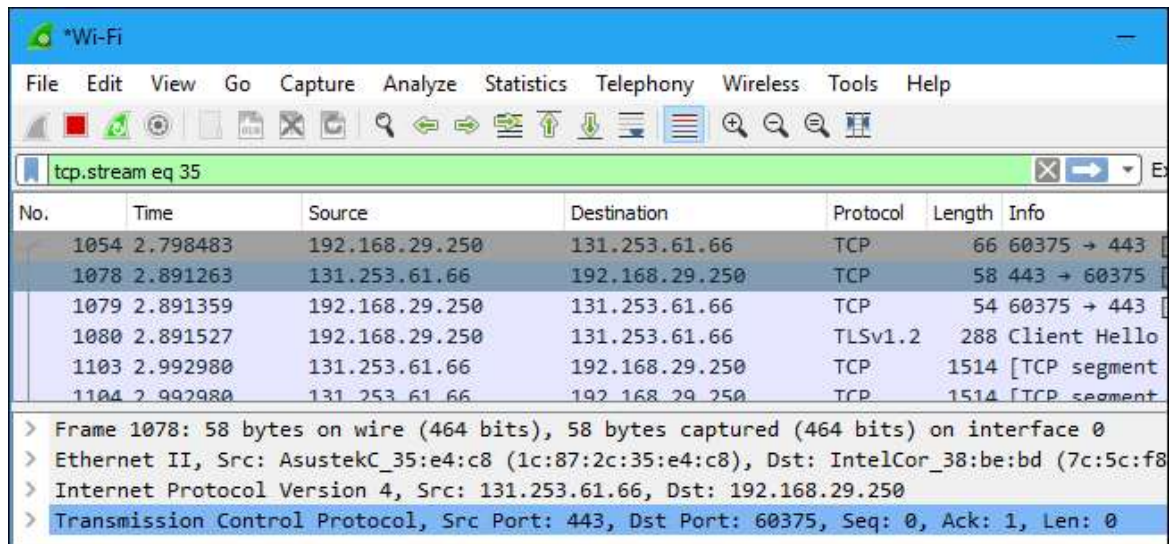


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.



Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello
1103	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment
1104	2.992980	131.253.61.66	192.168.29.250	TCP	1514	[TCP segment

> Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

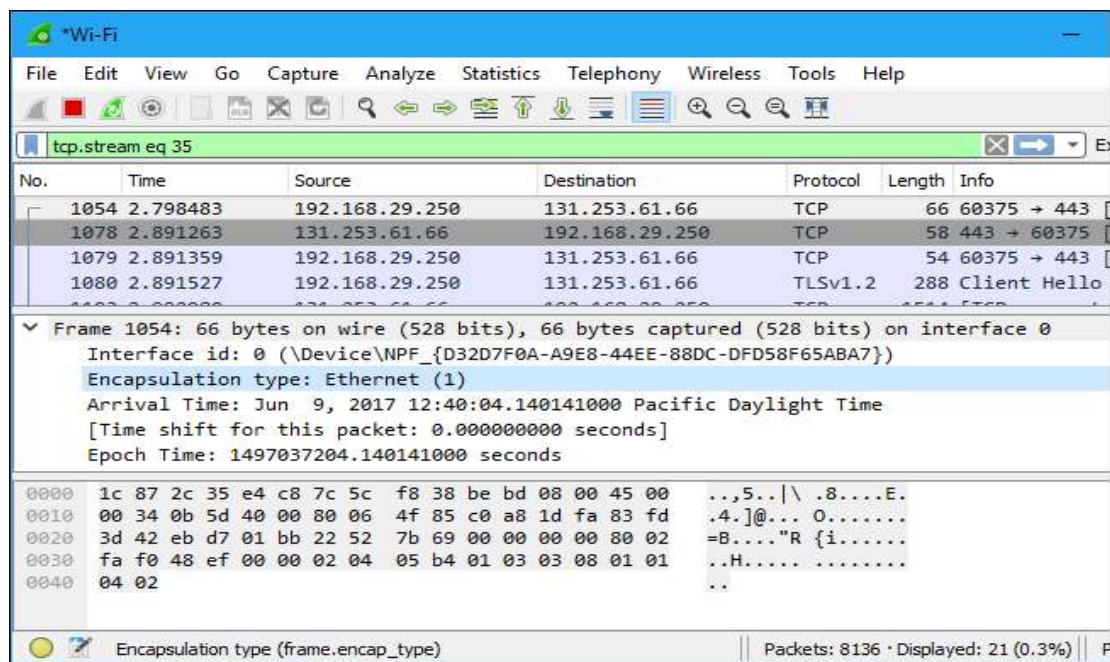
> Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c:f8:38:be:bd)

> Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250

> Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0

Inspecting Packets

Click a packet to select it and you can dig down to view its details.



No.	Time	Source	Destination	Protocol	Length	Info
1054	2.798483	192.168.29.250	131.253.61.66	TCP	66	60375 → 443
1078	2.891263	131.253.61.66	192.168.29.250	TCP	58	443 → 60375
1079	2.891359	192.168.29.250	131.253.61.66	TCP	54	60375 → 443
1080	2.891527	192.168.29.250	131.253.61.66	TLSv1.2	288	Client Hello

▼ Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0

Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time

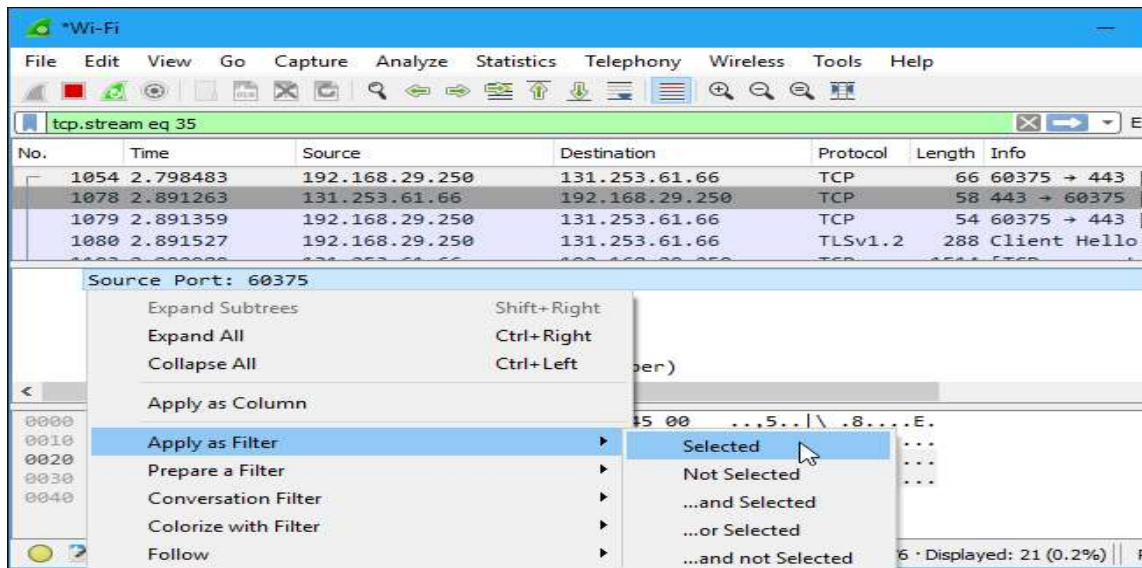
[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1497037204.140141000 seconds

Offset	Hex	ASCII
0000	1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00	..5.. \ .8....E.
0010	00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd	.4.]@... O.....
0020	3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 02	=B...."R {i.....
0030	fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01	..H.....
0040	04 02	..

Encapsulation type (frame.encap_type) | Packets: 8136 · Displayed: 21 (0.3%)

You can also create filters from here— just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



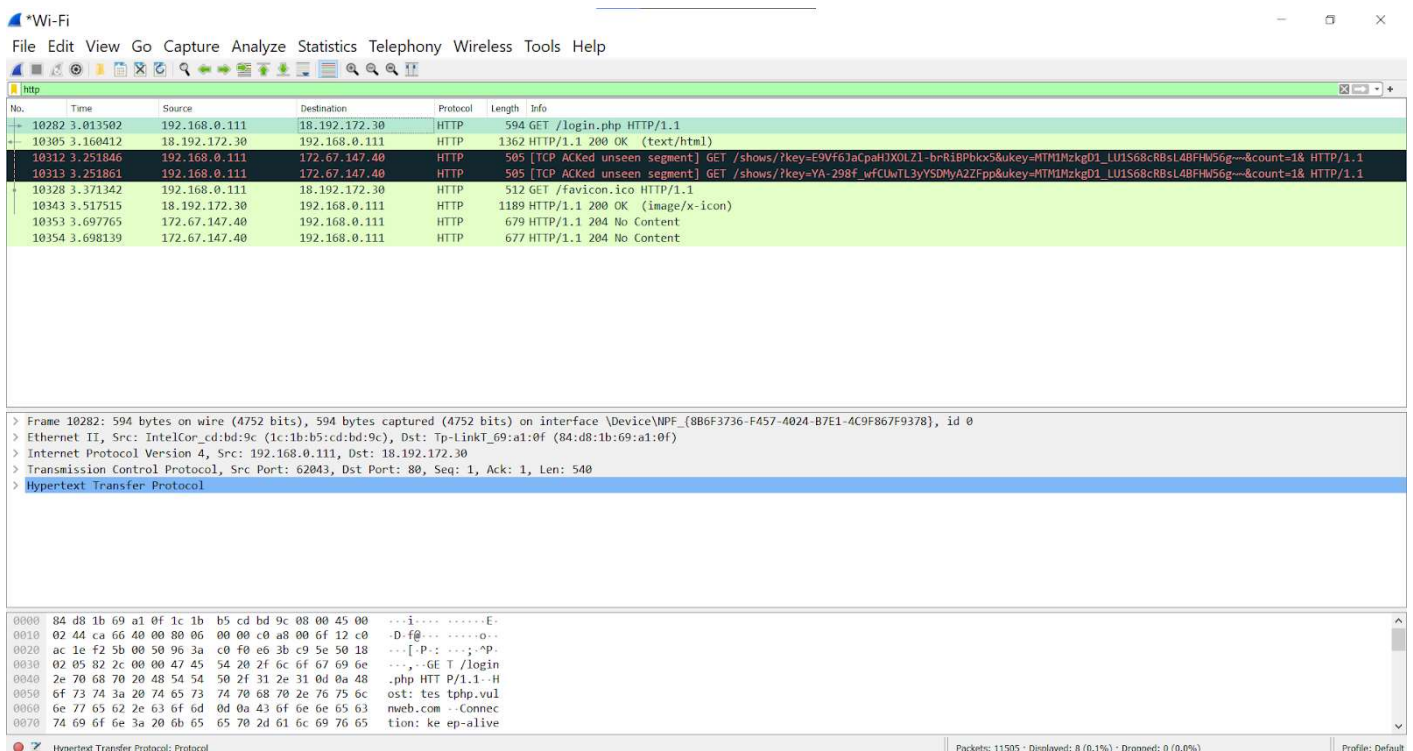
Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

INPUT and OUTPUT :- *(Apply all these filters and write the Steps and also paste Screen Shot)*

1. Which filter is used to check all incoming packets to HTTP web server?

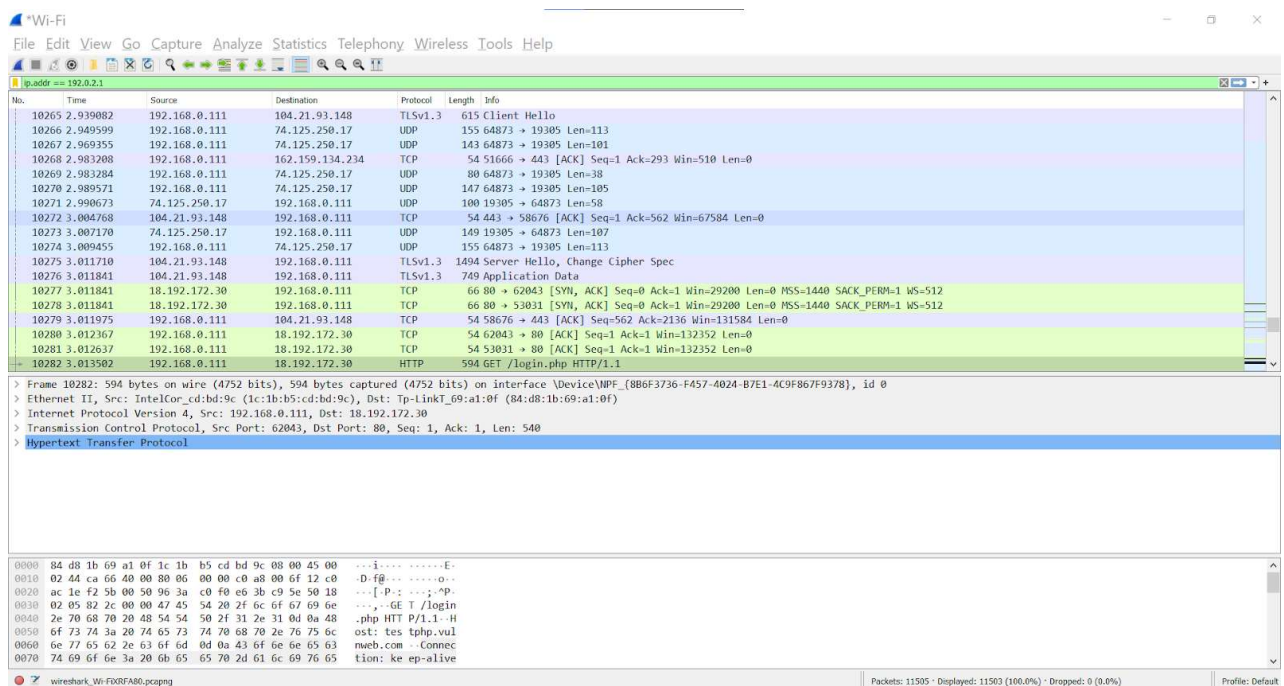
Step1: click the interface's name, packets start to appear in real time

Step2: To filter just type HTTP in the filter box at the top of the window and click Apply .



2. Which filter is used to monitor all outgoing packets from specific system on a network ?

ip.src==address



3. How to use wireshark to find password in any network.

HTTP typically runs on port 80/tcp and since it is a plain text protocol, it offers very little to no privacy to the communicating parties. Anybody who is in position to eavesdrop on the communication can capture everything over this channel, including password. Even though there has been a tremendous effort done by all major browser vendors to discourage usage of HTTP as much as possible, we can still see HTTP being used on internal networks during penetration tests. Here's an example of login credentials captured in a HTTP communication in a POST request

step1: Go to http website and try to login

step2: Open wireshark and type http in the filter bar.

step3: Now try to login on http website .

step4: Capture the post request in wireshark.

step5: click on it you will see the password you entered.

Meet - bxo-djnh-xv | Experiment 5 Lab manu | CN_Exp 5 - Google Doc | login page

Not secure | testphp.vulnweb.com/login.php

Apps | Gmail | Web Designing | input | WhatsApp | Canva | YouTube | Meet | Classroom | Reading list

acunetix acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

search art

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer

If you are already registered please enter your login information below:

Username :

Password :

You can also [signup here](#).
Signup disabled. Please use the username **test** and the password **test**.

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

No.	http	Source	Destination	Protocol	Length	Info
6395	http2	192.168.0.111	172.67.147.40	HTTP	505	GET /shows/?key=E9VF63aCpaHJXOLZ1-brRiBPbKx5&ukey=NTM1MzkgD1_LU1S68cRBsL4BFHw56g---&count=1& HTTP/1.1
8199	http3	18.192.172.30	192.168.0.111	HTTP	1216	HTTP/1.1 200 OK (text/css)
1340		172.67.147.40	192.168.0.111	HTTP	683	HTTP/1.1 204 No Content
299		3.776796	172.67.147.40	HTTP	687	HTTP/1.1 204 No Content
786	12.736655	192.168.0.111	18.192.172.30	HTTP	578	[TCP ACKed unseen segment] GET /login.php HTTP/1.1
799	12.884099	18.192.172.30	192.168.0.111	HTTP	1362	HTTP/1.1 200 OK (text/html)
806	12.967715	192.168.0.111	172.67.147.40	HTTP	505	GET /shows/?key=E9VF63aCpaHJXOLZ1-brRiBPbKx5&ukey=NTM1MzkgD1_LU1S68cRBsL4BFHw56g---&count=1& HTTP/1.1
807	12.967962	192.168.0.111	172.67.147.40	HTTP	505	GET /shows/?key=YA-298f_wfCLwL3yYSDMyA2Zfpp&ukey=NTM1MzkgD1_LU1S68cRBsL4BFHw56g---&count=1& HTTP/1.1
842	13.408447	172.67.147.40	192.168.0.111	HTTP	675	HTTP/1.1 204 No Content
843	13.413744	172.67.147.40	192.168.0.111	HTTP	679	HTTP/1.1 204 No Content
948	15.730775	192.168.0.111	18.192.172.30	HTTP	738	POST /userinfo.php HTTP/1.1 (application/x-www-form-urlencoded)
955	15.877793	18.192.172.30	192.168.0.111	HTTP	330	HTTP/1.1 302 Found (text/html)
956	15.885281	192.168.0.111	18.192.172.30	HTTP	594	GET /login.php HTTP/1.1
974	16.032568	18.192.172.30	192.168.0.111	HTTP	1362	HTTP/1.1 200 OK (text/html)
979	16.116340	192.168.0.111	172.67.147.40	HTTP	505	GET /shows/?key=E9VF63aCpaHJXOLZ1-brRiBPbKx5&ukey=NTM1MzkgD1_LU1S68cRBsL4BFHw56g---&count=1& HTTP/1.1
980	16.116521	192.168.0.111	172.67.147.40	HTTP	505	GET /shows/?key=YA-298f_wfCLwL3yYSDMyA2Zfpp&ukey=NTM1MzkgD1_LU1S68cRBsL4BFHw56g---&count=1& HTTP/1.1
998	16.541261	172.67.147.40	192.168.0.111	HTTP	679	HTTP/1.1 204 No Content
999	16.543849	172.67.147.40	192.168.0.111	HTTP	683	HTTP/1.1 204 No Content

> Frame 223: 881 bytes on wire (7048 bits), 881 bytes captured (7048 bits) on interface \Device\NPF_{8B6F3736-F457-4024-B7E1-4C9F867F9378}, id 0

> Ethernet II, Src: IntelCor_cd:bd:9c (1c:1b:b5:cd:bd:9c), Dst: Tp-LinkT_69:a1:0f (84:d8:1b:69:a1:0f)

> Internet Protocol Version 4, Src: 192.168.0.111, Dst: 18.192.172.30

> Transmission Control Protocol, Src Port: 64209, Dst Port: 80, Seq: 1, Ack: 1, Len: 827

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form-urlencoded

```
0000 84 d8 1b 69 a1 0f 1c 1b b5 cd bd 9c 08 00 45 00  ---i---E-
0010 03 63 ca 97 40 00 80 06 00 00 c0 a8 00 0f 12 c0  -c-@---o-
0020 ac 1e fa d1 00 50 7d 06 f1 da 76 84 e8 1b 50 18  -P}-v-P-
0030 02 05 83 4b 00 00 50 4f 53 54 20 2f 73 65 63 75  -K-PO ST /secu
0040 72 65 64 2f 6e 65 77 75 73 65 72 2e 70 68 70 20  red/newu ser.php
0050 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20  HTTP/1.1 -Host:
0060 74 65 73 74 70 68 70 2e 76 75 6c 6e 77 65 62 2e  testphp.vulnweb.
0070 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a  com-Connction:
```

Hypertext Transfer Protocol: Protocol

Packets: 1149 · Displayed: 22 (1.9%) · Dropped: 0 (0.0%)

Profile: Default


```

Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 2/3]
[Prev request in frame: 786]
[Response in frame: 955]
[Next request in frame: 956]
File Data: 35 bytes

```

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

```

> Form item: "uname" = "keegan"
> Form item: "pass" = "Y9A3xEiqXFpwh4@"

```

4. Explain wireshark coloring rules

There are two types of coloring rules in Wireshark: temporary rules that are only in effect until you quit the program, and permanent rules that are saved in a preference file so that they are available the next time you run Wireshark. Temporary rules can be added by selecting a packet and pressing the **Ctrl** key together with one of the number keys. This will create a coloring rule based on the currently selected conversation. It will try to create a conversation filter based on TCP first, then UDP, then IP and at last Ethernet. Temporary filters can also be created by selecting the Colorize with Filter → Color X menu items when right-clicking in the packet detail pane.



CONCLUSION: Thus, we have studied the working of Wire Shark Packet Capture.