Practical - 08

Title: - Introduction to Wireshark and its installation.

Aim: - To get familiar with network sniffing software - Wireshark.

Lab Objectives: -

Learn to capture network traffic using network sniffing software.

Description: -

Wireshark Introduction

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called a sniffer, network protocol analyzer, and network analyzer. It is also used by network security engineers to examine security problems.

Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Wireshark captures packets and lets you examine their contents.

Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- QA engineers use it to verify network applications.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

Wireshark can also be helpful in many other situations.

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- Save packet data captured.
- Export some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- Search for packets on many criteria.

- Colorize packet display based on filters.
- Create various statistics.

Here are some things Wireshark does not provide:

- Wireshark isn't an intrusion detection system.
- Wireshark will not manipulate things on the network, it will only "measure" things from it.
- Wireshark doesn't send packets on the network or do other active things (except domain name resolution, but that can be disabled).

Wireshark Installation

For windows

You can get the latest copy of the program from the Wireshark website at https://www.wireshark.org/download.html

The download page should automatically highlight the appropriate download for your platform and direct you to the nearest mirror.

For Ubuntu

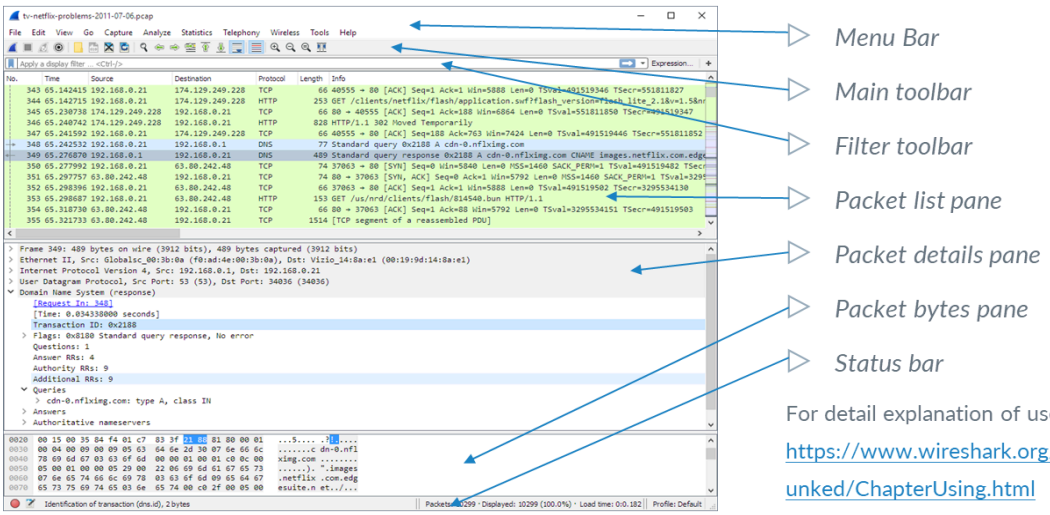
Enter following command at the terminal one after the other.

sudo apt-get install wireshark

sudo dpkg-reconfigure wireshark-common

sudo chmod +x /usr/bin/dumpcap

User Interface



For detail explanation of user interface, visit https://www.wireshark.org/docs/wsug_html_chunked/ChapterUsing.html

Capturing Live Network Data

Capturing live network data is one of the major features of Wireshark.

The Wireshark capture engine provides the following features:

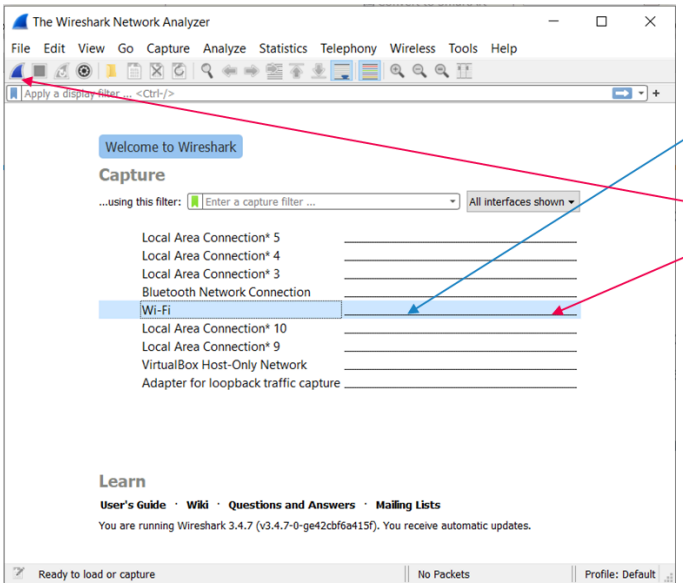
- Capture from different kinds of network hardware such as Ethernet or 802.11.
- Simultaneously capture from multiple network interfaces.
- Stop the capture on different triggers such as the amount of captured data, elapsed time, or the number of packets.
- Simultaneously show decoded packets while Wireshark is capturing.
- Filter packets, reducing the amount of data to be captured. See Section 4.10, “Filtering while capturing”.
- Save packets in multiple files while doing a long-term capture.

The following methods can be used to start capturing packets with Wireshark:

- You can double-click on an interface in the welcome screen.
- You can select an interface in the welcome screen, then select Capture → Start or click the first toolbar button.
- If you already know the name of the capture interface you can start Wireshark from the command line:

```
$ wireshark -i eth0 -k
```

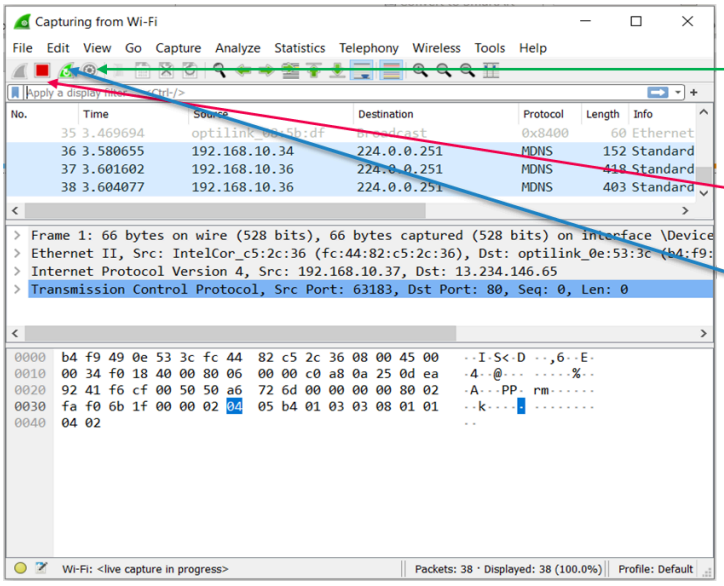
- This will start Wireshark capturing on interface eth0



You can double-click on an interface in the welcome screen.

or

You can select an interface in the welcome screen, then select Capture → Start or click the first toolbar button.



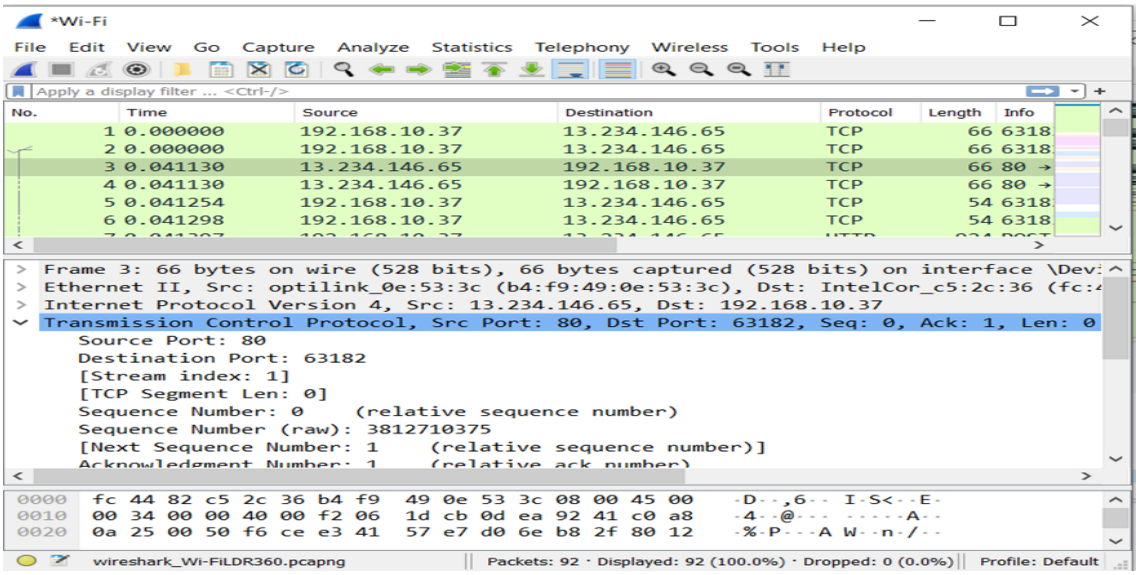
- You can configure capture option by clicking on **Capture options button.**
- You can stop capturing packets by clicking on **Stop button**.
- You can restart capture by clicking **Restart Capture** button
- You can save captured packets by using the File → Save or File → Save As... menu items. You can choose which packets to save and which file format to be used.

Viewing Captured Packets

Once you have captured some packets or you have opened a previously saved capture file, you can view the packets that are displayed in the packet list pane by simply clicking on a packet in the packet list pane, which will bring up the selected packet in the tree view and byte view panes.

You can then expand any part of the tree to view detailed information about each protocol in each packet.

Clicking on an item in the tree will highlight the corresponding bytes in the byte view.



Filtering Packets While Viewing

Wireshark has two filtering languages: **capture filters and display filters**.

- **Capture filters are used for filtering when capturing packets.**
- **Display filters are used for filtering which packets are displayed.**

Display filters allow you to concentrate on the packets you are interested in while hiding the currently uninteresting ones.

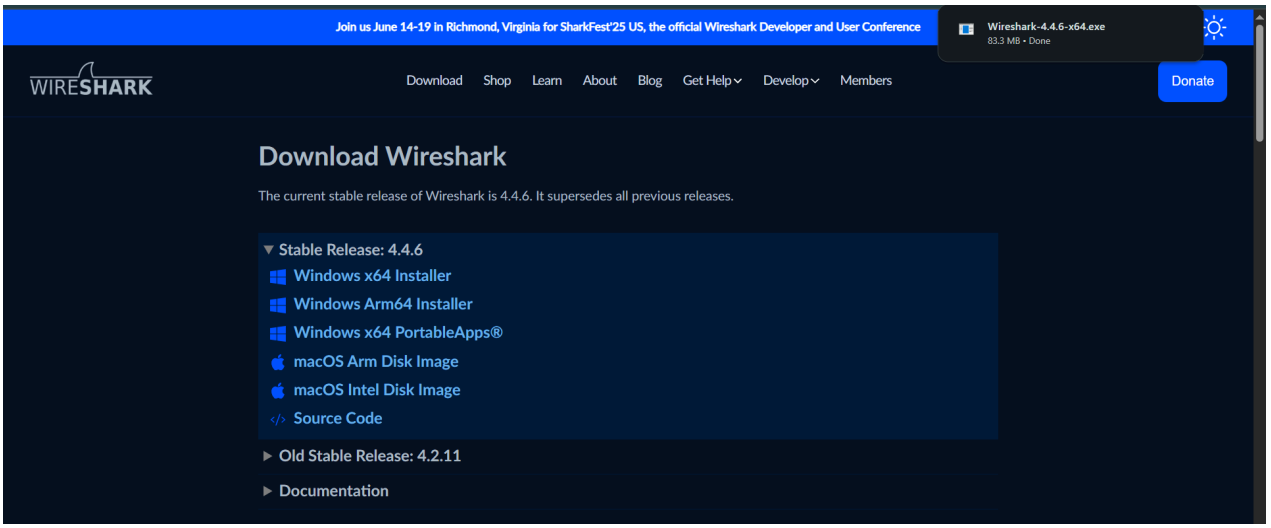
They allow you to only display packets based on:

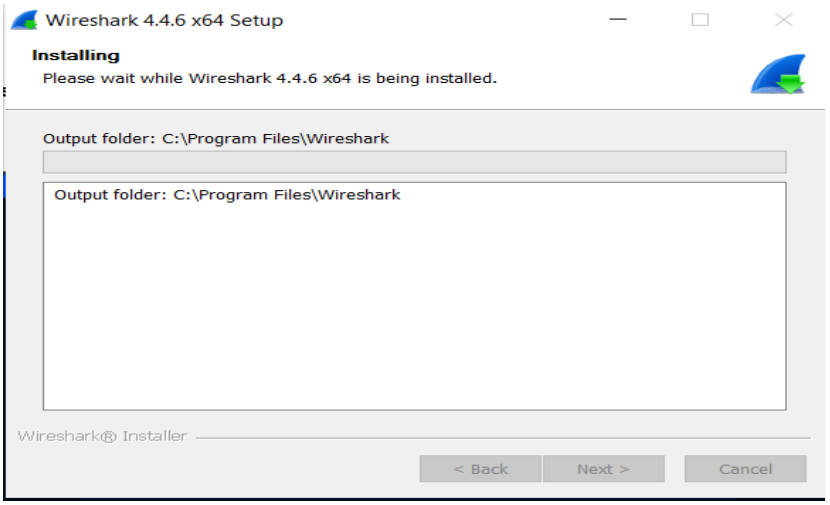
- Protocol
- The presence of a field
- The values of fields
- A comparison between fields

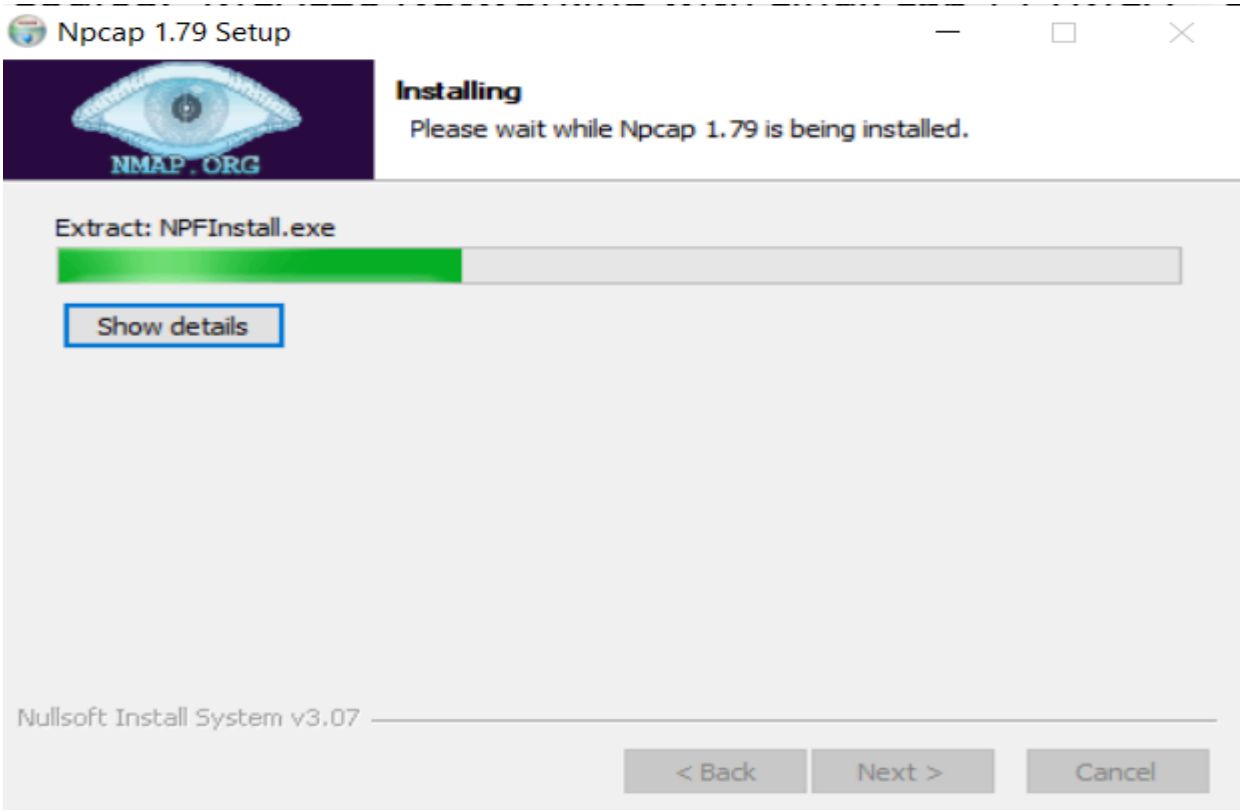
Exercise

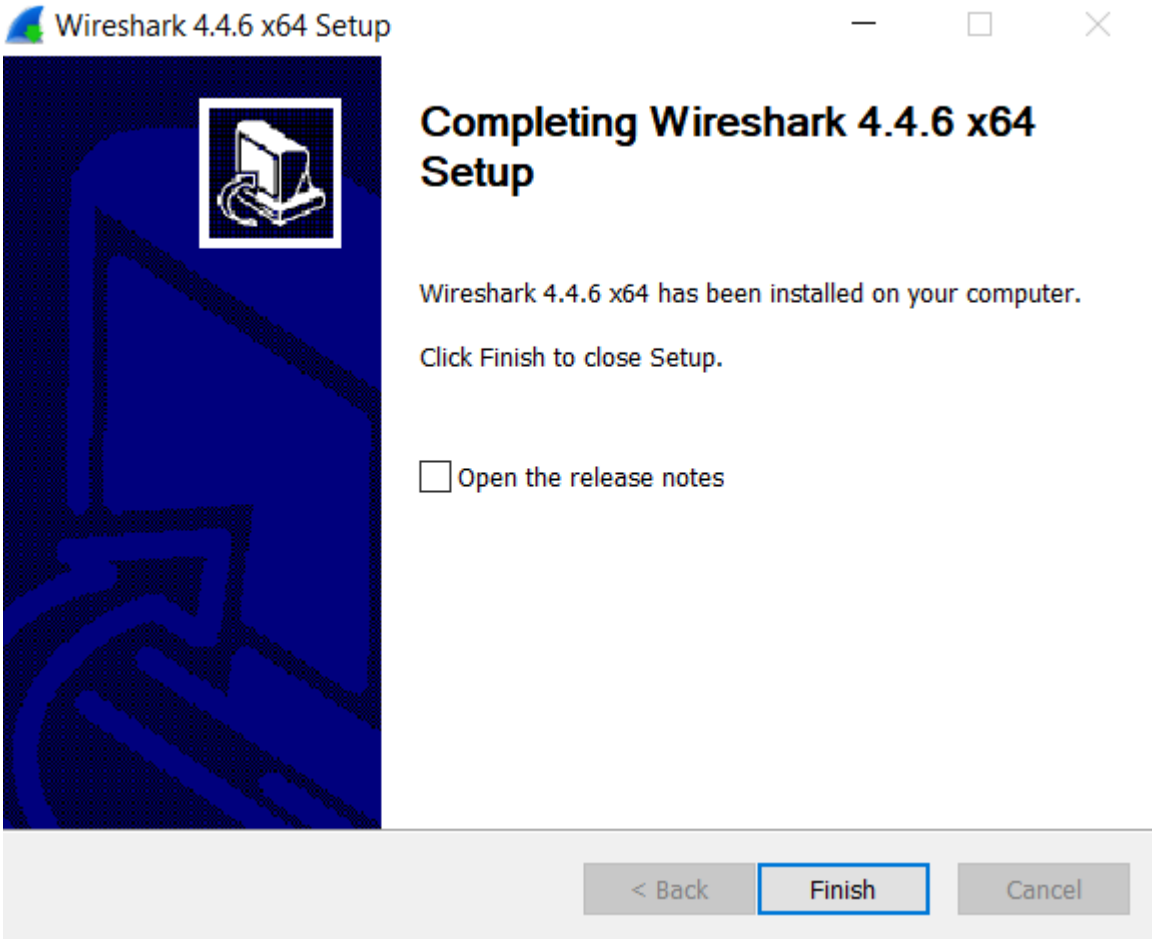
1. Install Wireshark on Windows and Linux operating systems.

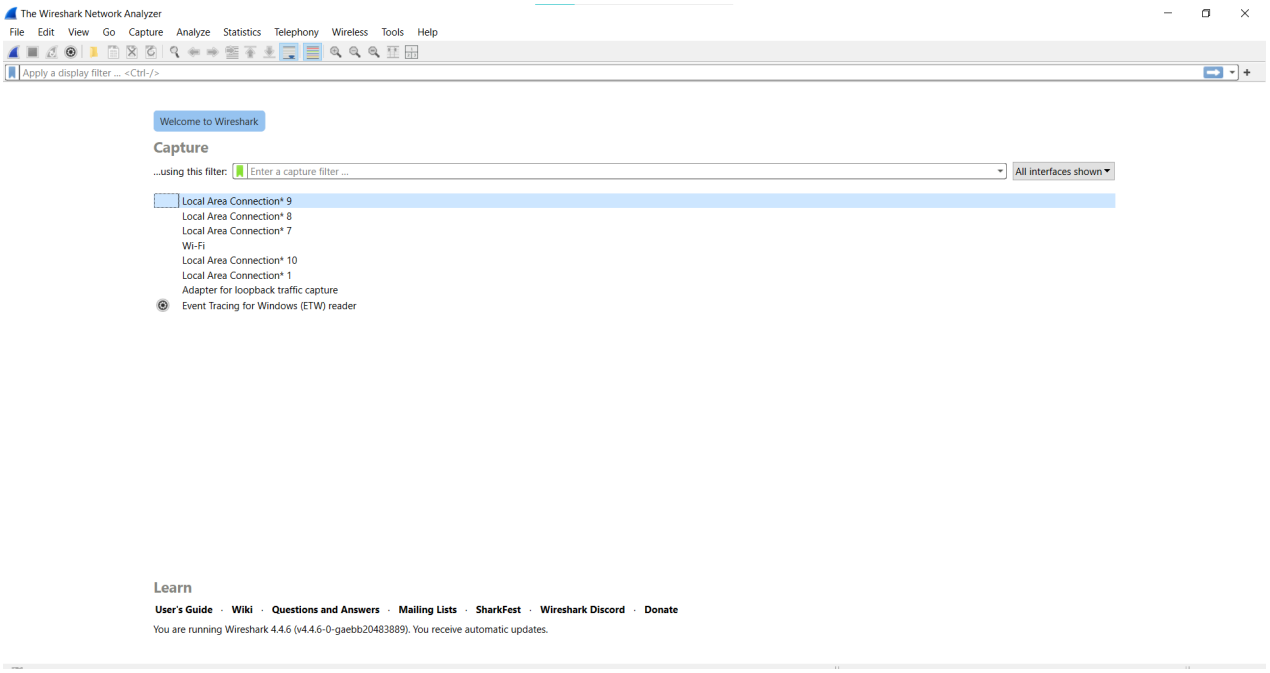
Output






Npcap 1.79 Setup
NMAP.ORG
Installing
Please wait while Npcap 1.79 is being installed.
Extract: NPFInstall.exe
Show details
Nullsoft Install System v3.07
< Back
Next >
Cancel

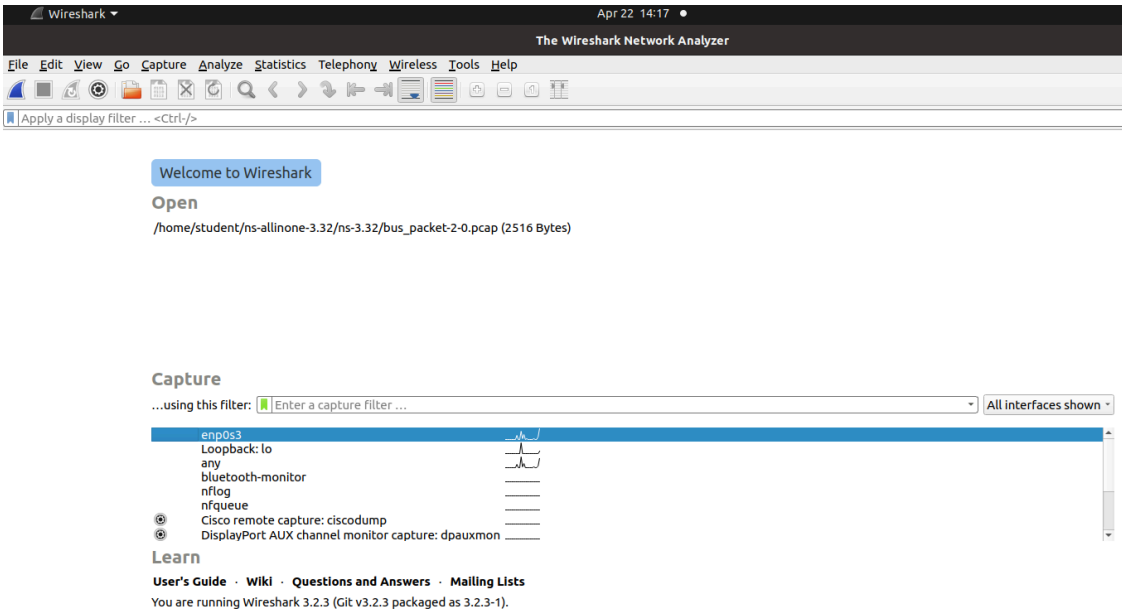

Wireshark 4.4.6 x64 Setup
Completing Wireshark 4.4.6 x64 Setup
Wireshark 4.4.6 x64 has been installed on your computer.
Click Finish to close Setup.
Open the release notes
< Back
Finish
Cancel



Using Linux

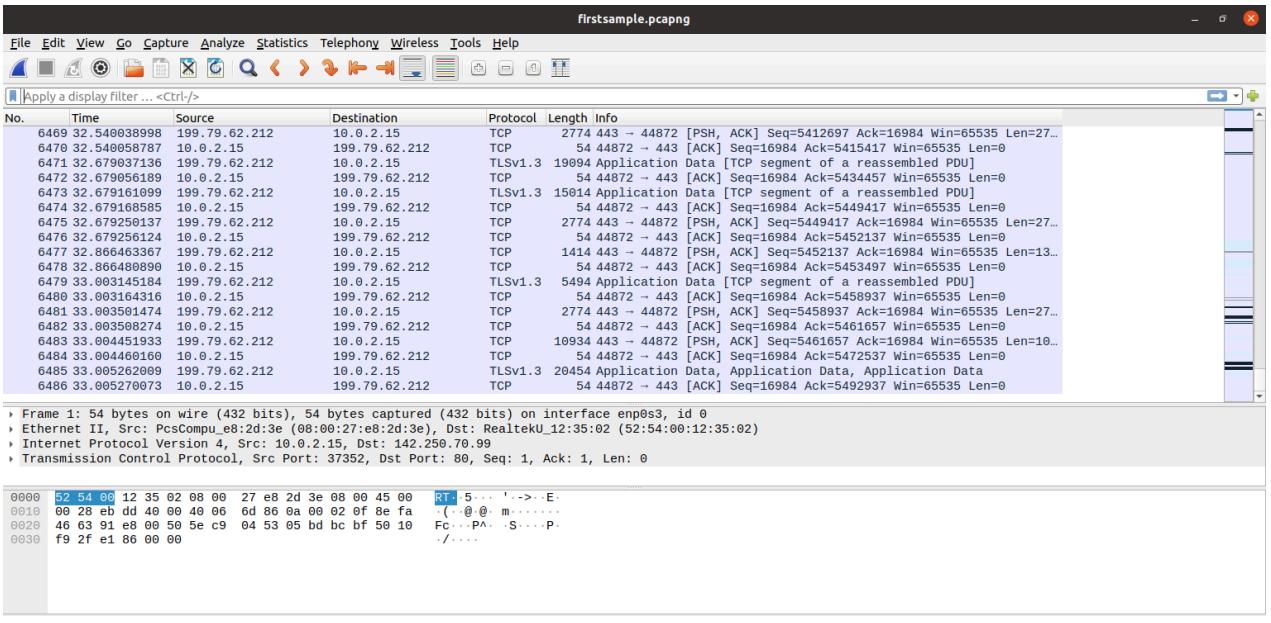
```
student@student-VirtualBox:~$ sudo apt update
[sudo] password for student:
Hit:1 http://in.archive.ubuntu.com/ubuntu focal InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu focal-updates InRelease
Hit:3 http://security.ubuntu.com/ubuntu focal-security InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu focal-backports InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
286 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

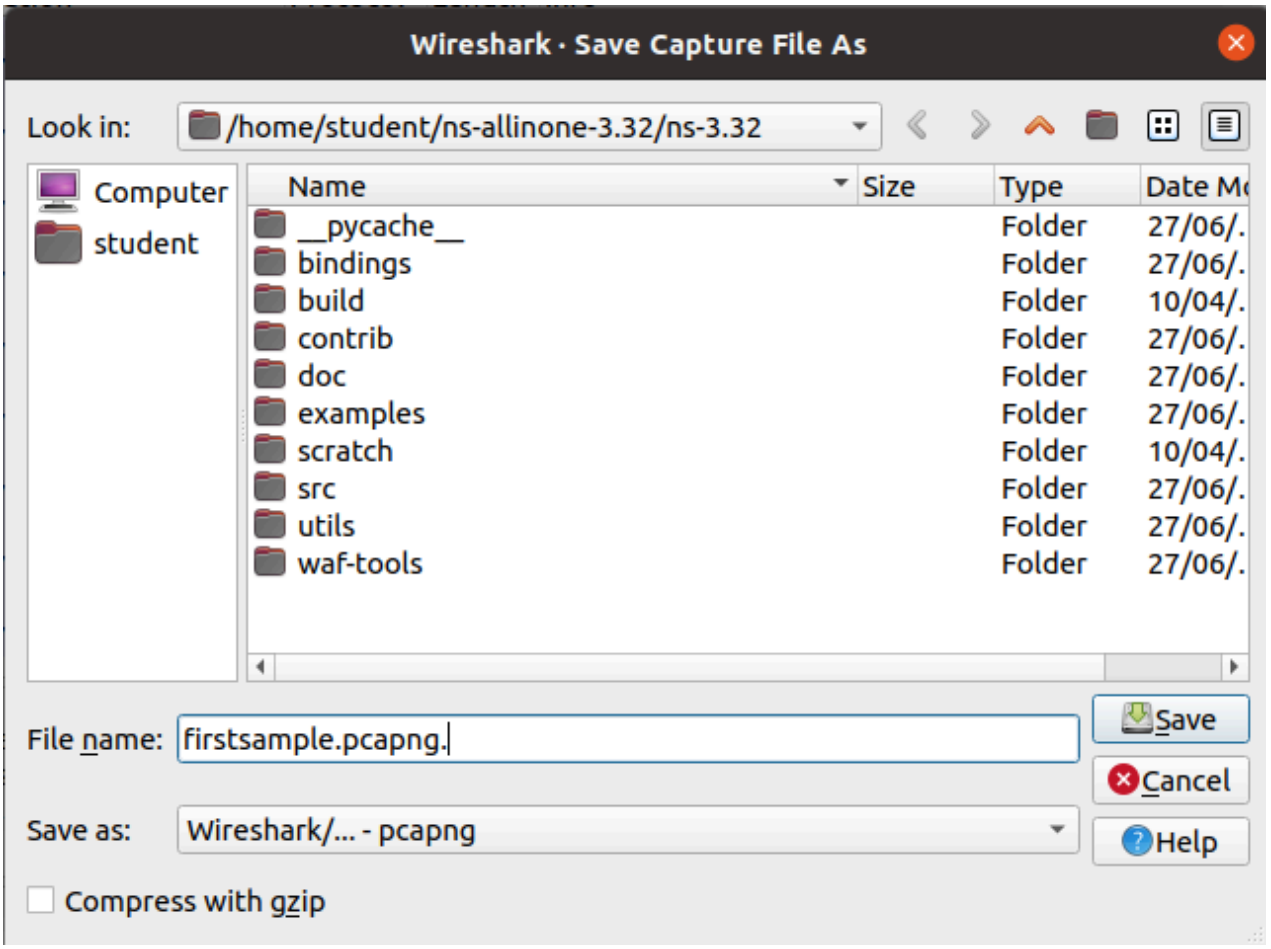
```
student@student-VirtualBox:~$ sudo apt install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
wireshark is already the newest version (3.2.3-1).
0 upgraded, 0 newly installed, 0 to remove and 286 not upgraded.
```

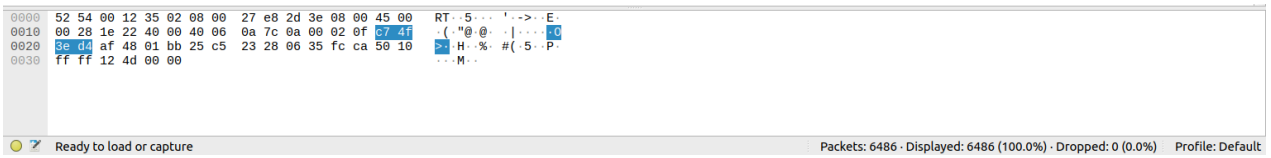


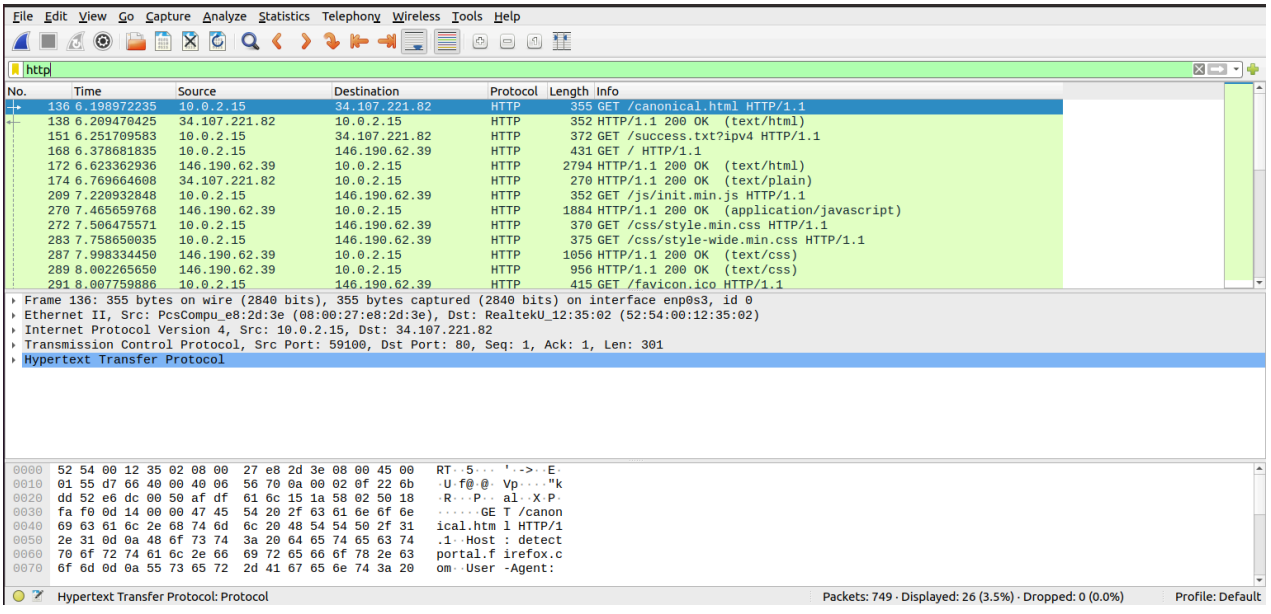
2. Start a sample capture on wireshark and browse https://famt.ac.in. Save the captured data as firstsample.pcapng. What is the total number of packets captured. Display http packets only.

Output



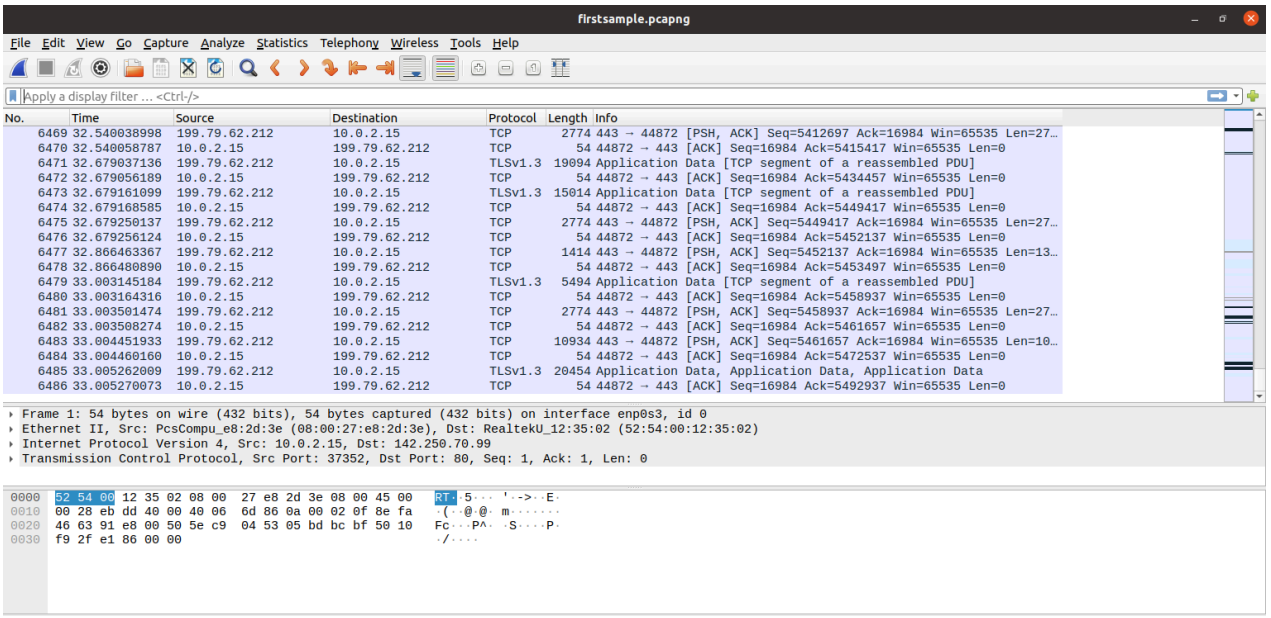


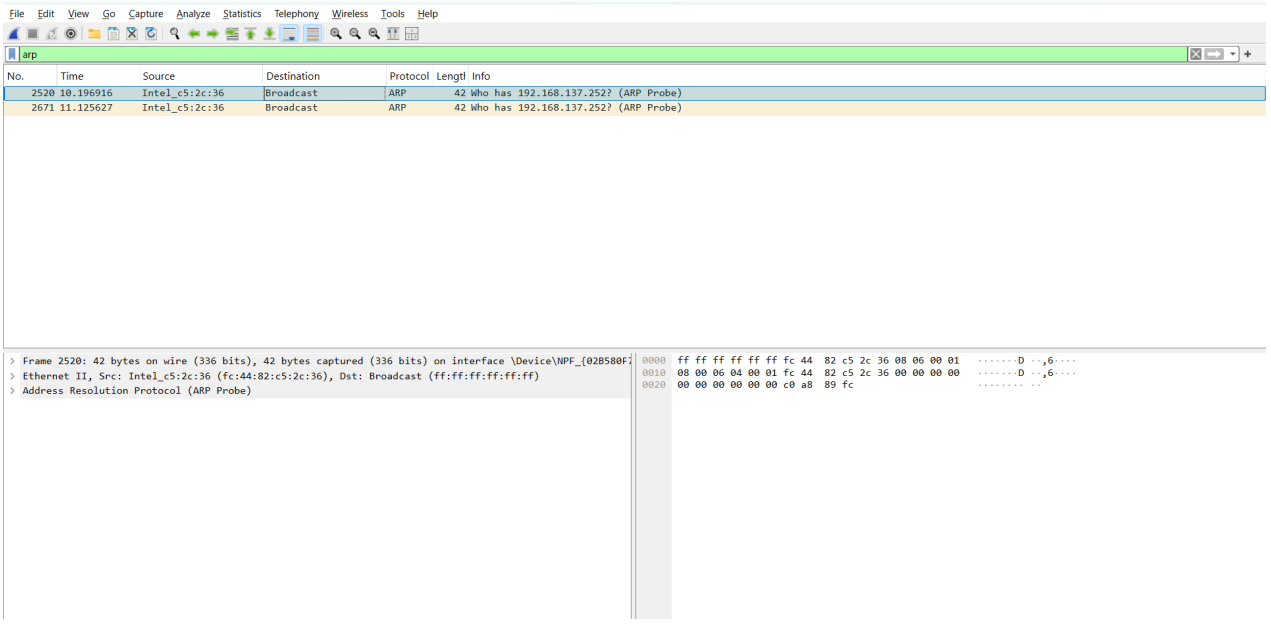




3. Start a sample capture on wireshark and browse your college website. Filter all ARP packets.

Output





Conclusion: Installed the Wireshark tool and learned to sniff and analyze the traffic on network.

References

https://www.wireshark.org/docs/wsug_html_chunked/index.html

https://www.freecodecamp.org/news/learn-wireshark-computer-networking/

https://www.lifewire.com/wireshark-tutorial-4143298