SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)

Department of CSE (ICB)

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJS22ICL402 **Course Name: Computer Networks Lab**

Name: Divy Arun Mav **SAP ID: 60019220133**

Experiment No: 8

Aim: To analyze different captured packets using Wireshark tool.

Theory:

Wire shark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

Here are some reasons people use Wire shark:

- 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 Features The

following are some of the many features Wire shark provides:

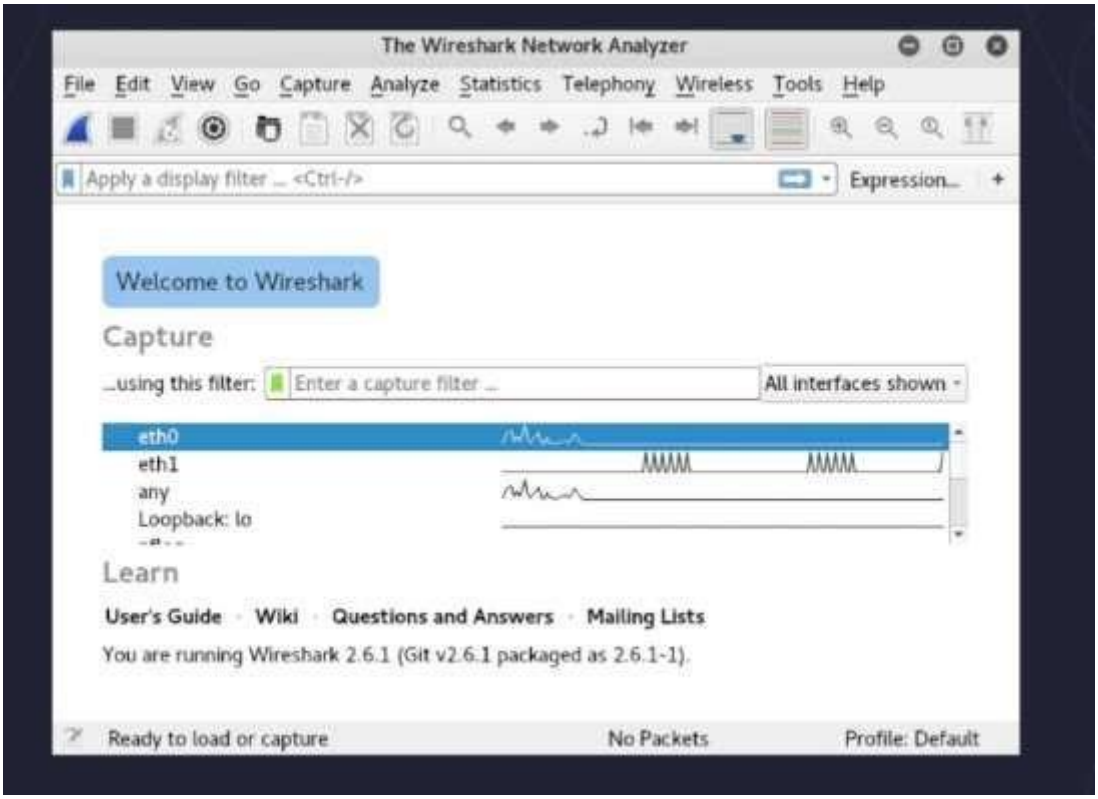
- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very 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.

Data Packets on Wireshark

Now that we have Wireshark installed let's go over how to enable the Wireshark packet sniffer and then analyze the network traffic.

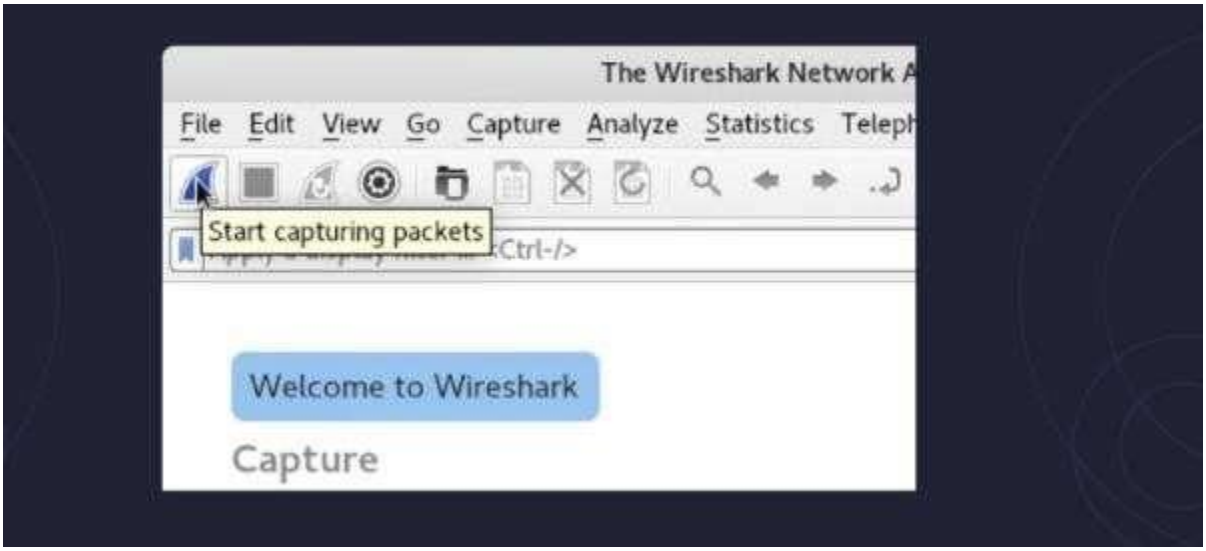
Capturing Data Packets on Wireshark

When you open Wireshark, you see a screen that shows you a list of all of the network connections you can monitor. You also have a capture filter field, so you only capture the network traffic you want to see



You can select one or more of the network interfaces using "shift left-click." Once you have the network interface selected, you can start the capture, and there are several ways to do that.

Click the first button on the toolbar, titled "Start Capturing Packets."



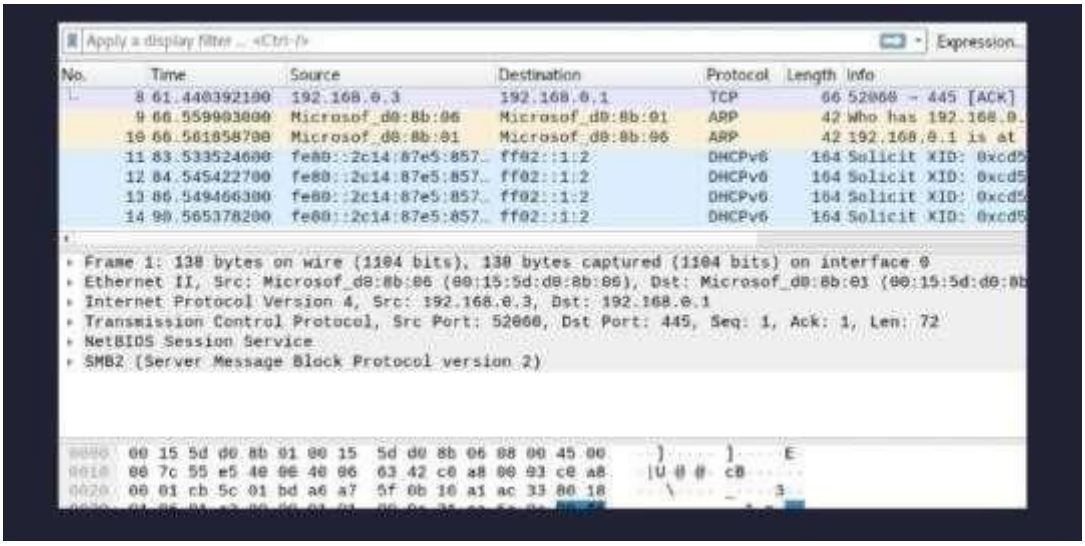
You can select the menu item Capture -> Start.

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJS22ICL402 **Course Name: Computer Networks Lab**

Or you could use the keystroke Control – E.

During the capture, Wire shark will show you the packets that it captures in real-time.

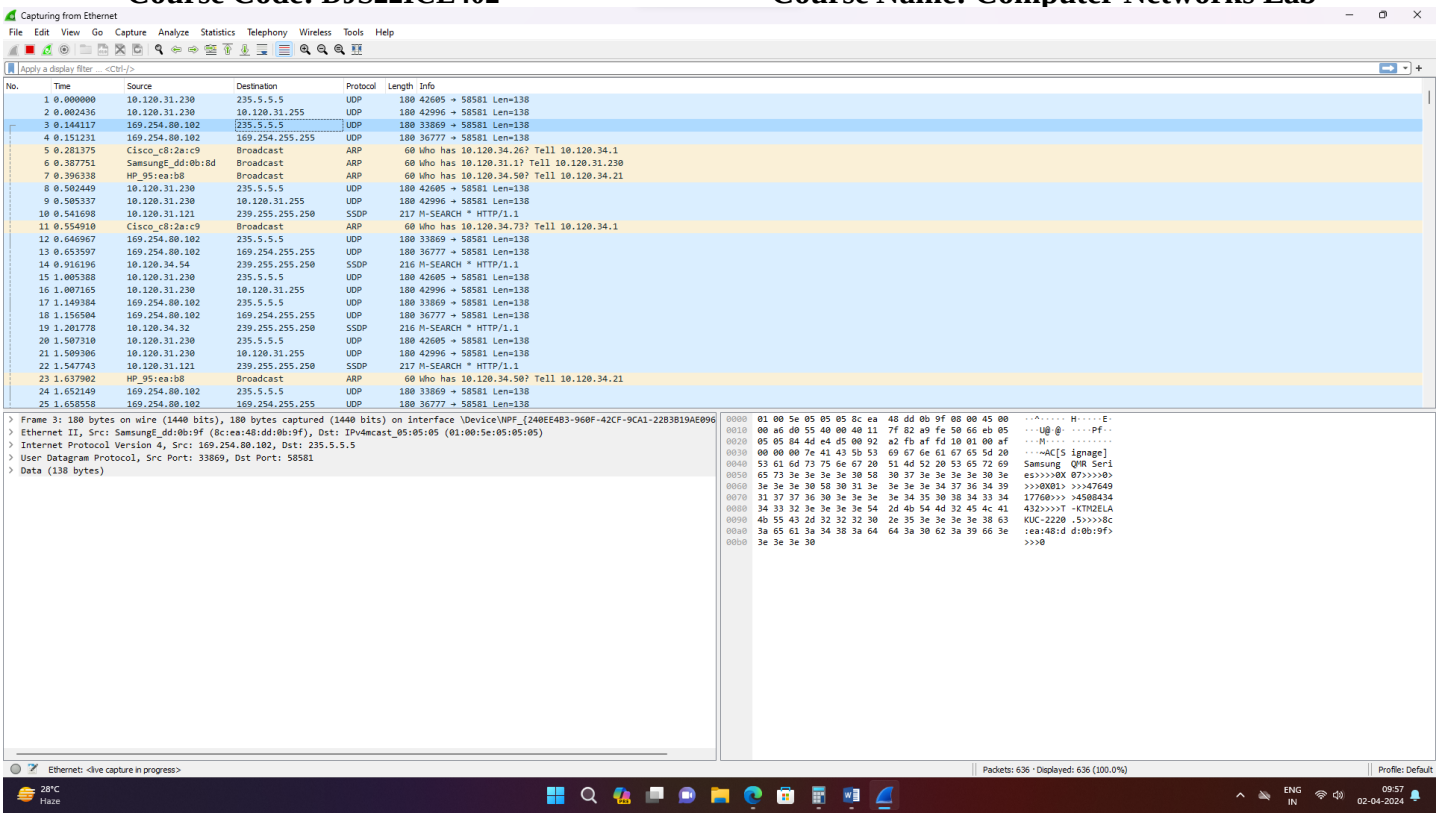


Student should Capture packet of TCP,UDP, HTTP, FTP using wireshark

SHRI VILEPARLE KELAVANI MANDAL'S
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
(Autonomous College Affiliated to the University of Mumbai)
NAAC ACCREDITED with "A" GRADE (CGPA : 3.18)
Department of Computer Science and engineering(IoT, Cyber security with block chain technology)

Class: S.Y. B.Tech. **Semester: IV**

Course Code: DJS22ICL402 **Course Name: Computer Networks Lab**



Conclusion: Successfully analyzed different captured packets using Wireshark tool.