Experiment No. 7

Aim: Study of packet sniffer tools: wireshark,

1. Download and install wire shark and capture icmp, tcp, and http packets in promiscuous mode.
2. Explore how the packets can be traced based on different filters

Objectives:

- Understand the need for traffic analysis.
- Understand the how packet sniffing is done using wire shark.
- Trace and understand various packets from dynamic traffic.

Outcomes: The learner will be able to

- Sniff network packets and study insights of packets to get detail network information.

Hardware / Software Required: Unix/Linux/Windows, wire shark

Theory:

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

Features of Wire shark:

- Available for UNIX and Windows.

- Capture live packet data from a network interface.

- Openfilescontainingpacketdatacapturedwithtcpdump/WinDump,Wireshark,anda

- Number of other packet capture programs.

- Import packets from text files containing hex dumps of packet data.

- Display packets with very detailed protocol information.

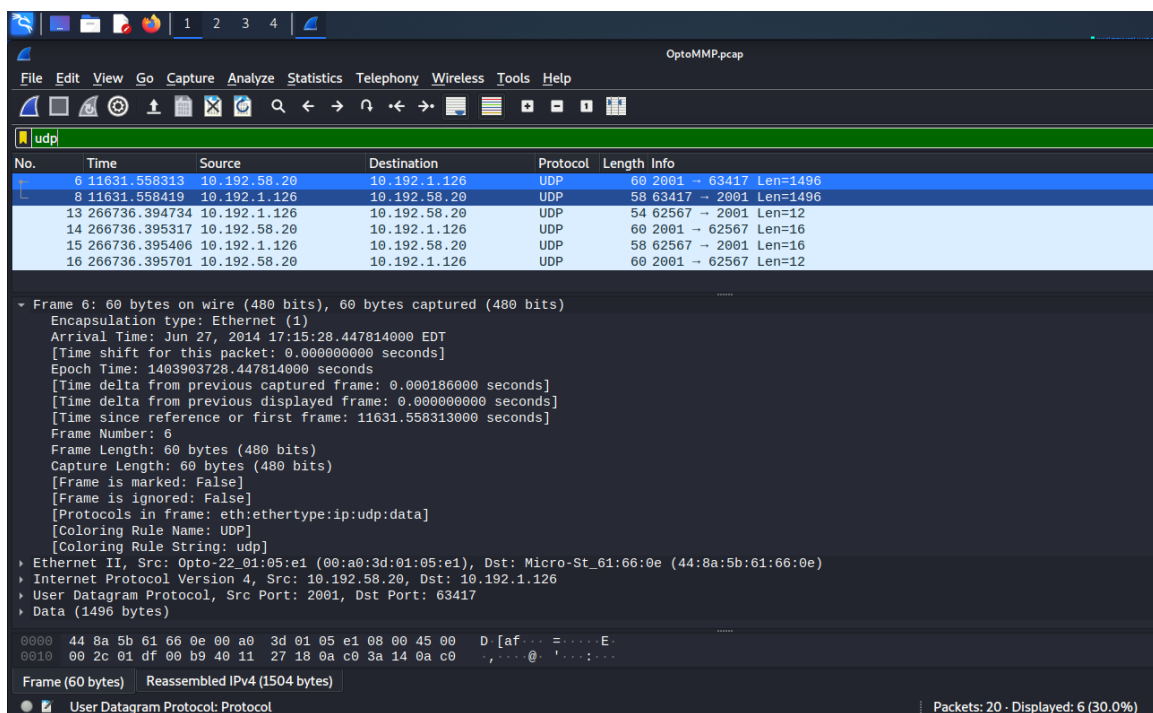- Export some or all packets in a number of capture file formats.

- Filter packets on many criteria.

- Search for packets on many criteria.

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

Capturing Packets

After downloading and installing wire shark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by clicking Capture Options.

As soon as you click the interface's name, you'll see the packets start to appearing real time.
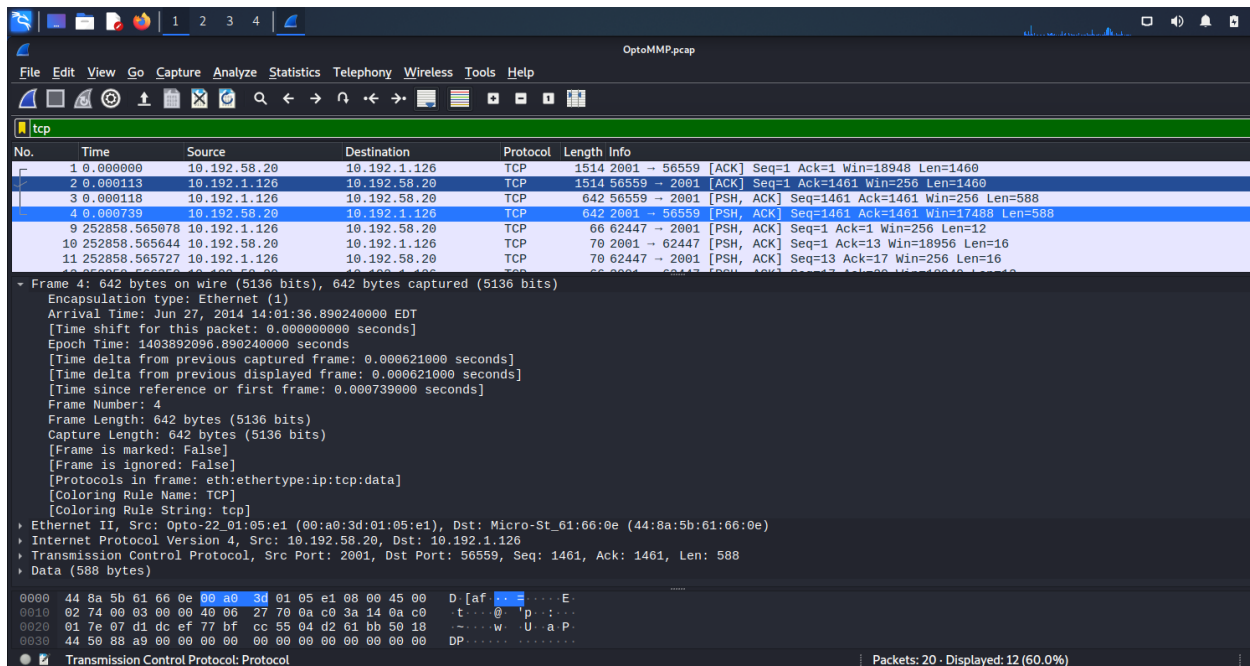
Wire shark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on the network

Wire shark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.

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 Wire shark'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 (oppressing Enter).

For example, type—dns ¦and you'll see only DNS packets. When you start typing, Wire shark will help you auto complete your filter.

Conclusion:

Wire shark installation and network traffic analysis using packet sniffing is done. Detailed information about packets is explored by applying filter.

For Faculty Use

Correction Parameters	Formative Assessment[40%]	Timely Completion of Practical [40%]	Attendance / Learning Attitude [20%]	Total
Marks Obtained				