

Experiment No. 7

Aim: Study of packet sniffer tools : wireshark, :

1. Download and install wireshark 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 how packet sniffing is done using wireshark.
- 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 detailed network information.

Hardware / Software Required: Unix/Linux/Windows, wireshark

Theory:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and displays 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.

Features of Wireshark :

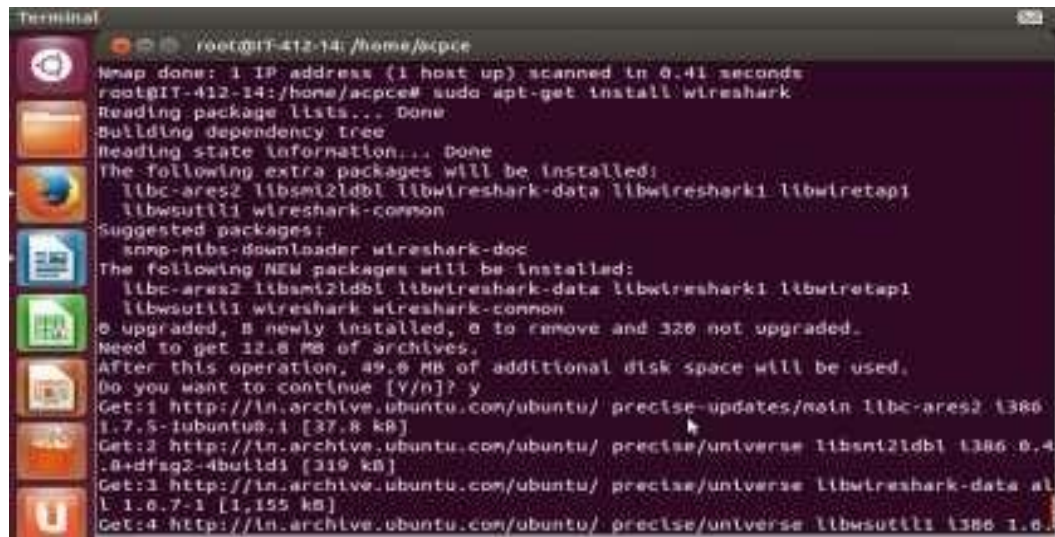
- Available for UNIX and Windows.
- Capture live packet data from a network interface.
- Open files containing packet data captured with tcpdump/Wireshark, and a number of other packet capture programs.
- Import packets from text files containing hex dumps of packet data.
- Display packets with very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

Installation of Wireshark:

```
sudo apt-get install wireshark
```

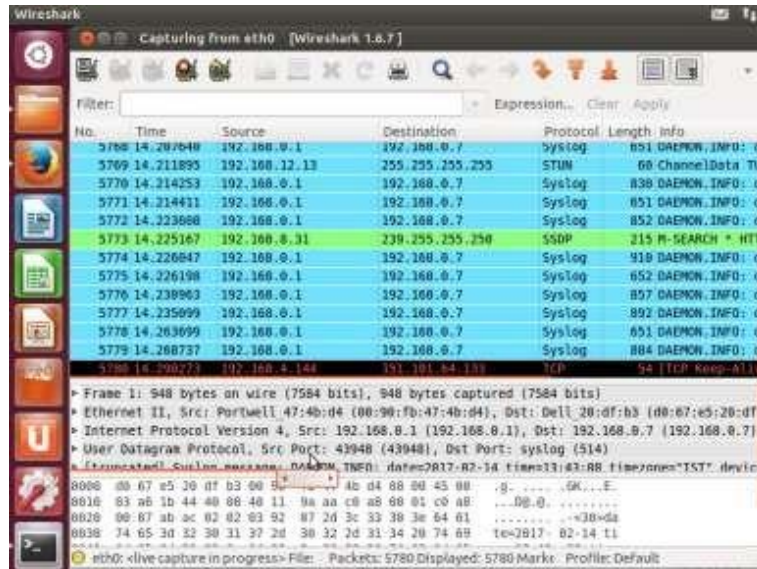


```
Terminal
root@IT-412-14: /home/acpce
nmap done: 1 IP address (1 host up) scanned in 0.41 seconds
root@IT-412-14: /home/acpce# sudo apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libbc-ares2 libbmi2ldbl libwireshark-data libwireshark1 libwireshark1
  libwsutil1 wireshark-common
Suggested packages:
  snmp-mibs-downloader wireshark-doc
The following NEW packages will be installed:
  libbc-ares2 libbmi2ldbl libwireshark-data libwireshark1 libwireshark1
  libwsutil1 wireshark-common
0 upgraded, 8 newly installed, 0 to remove and 320 not upgraded.
Need to get 12.8 MB of archives.
After this operation, 49.6 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://ln.archive.ubuntu.com/ubuntu/ precise-updates/main libbc-ares2 1.386
1.7.5-1ubuntu0.1 [37.8 kB]
Get:2 http://ln.archive.ubuntu.com/ubuntu/ precise/universe libbmi2ldbl 1.386 0.4
.0-dfsg2-4build1 [319 kB]
Get:3 http://ln.archive.ubuntu.com/ubuntu/ precise/universe libwireshark-data al
l 1.6.7-1 [1,155 kB]
Get:4 http://ln.archive.ubuntu.com/ubuntu/ precise/universe libwsutil1 1.386 1.6.7-1 [1,155 kB]
```

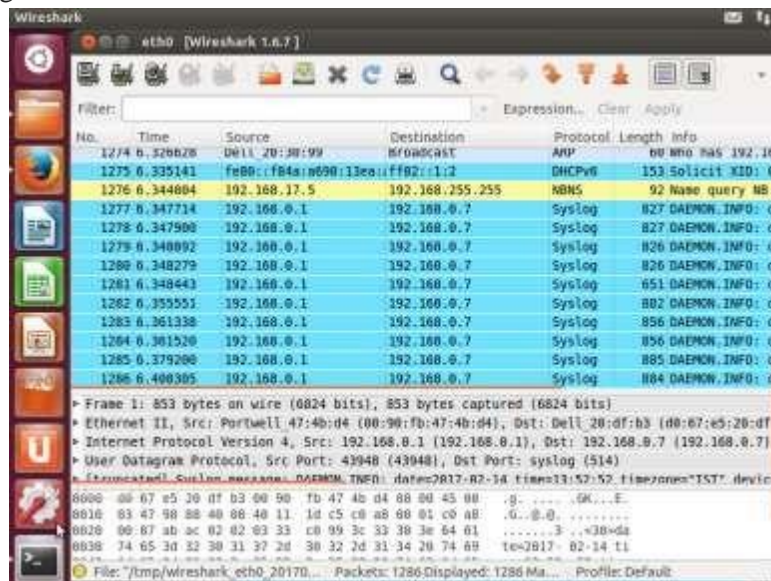
After downloading and installing wireshark, you can launch it and click the name of an interface under Interface List to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, click your wireless interface. You can configure advanced features by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



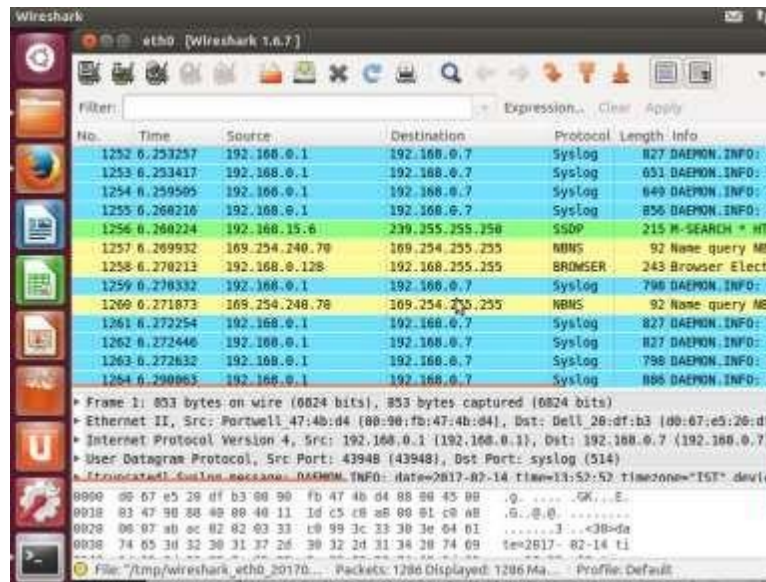
As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other the other packets on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



Click the stop capture button near the top left corner of the window when you want to stop capturing traffic.



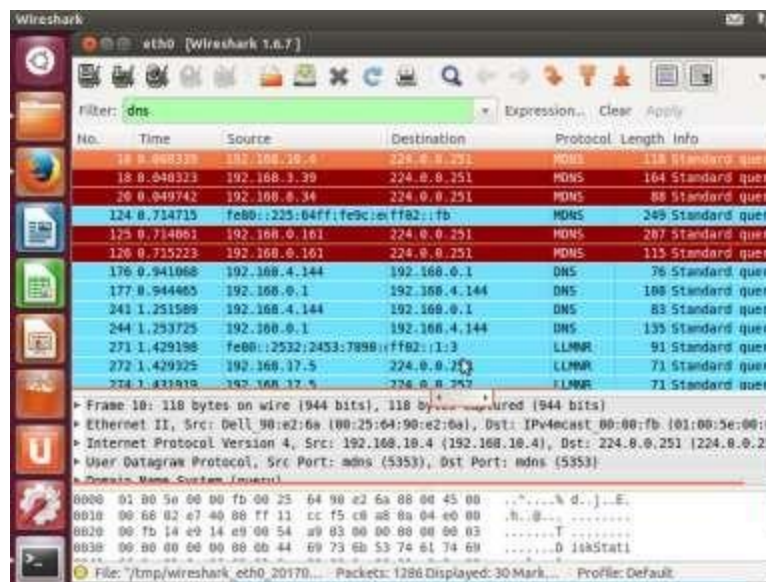
Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.



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 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.



Conclusion: Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet.