**Practical No 14**

**Aim: -** Analyze the network traffic using wireshark

**Objective: -**

* Understanging traffic analysis using wireshark

**Theory: -**

Wireshark 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).

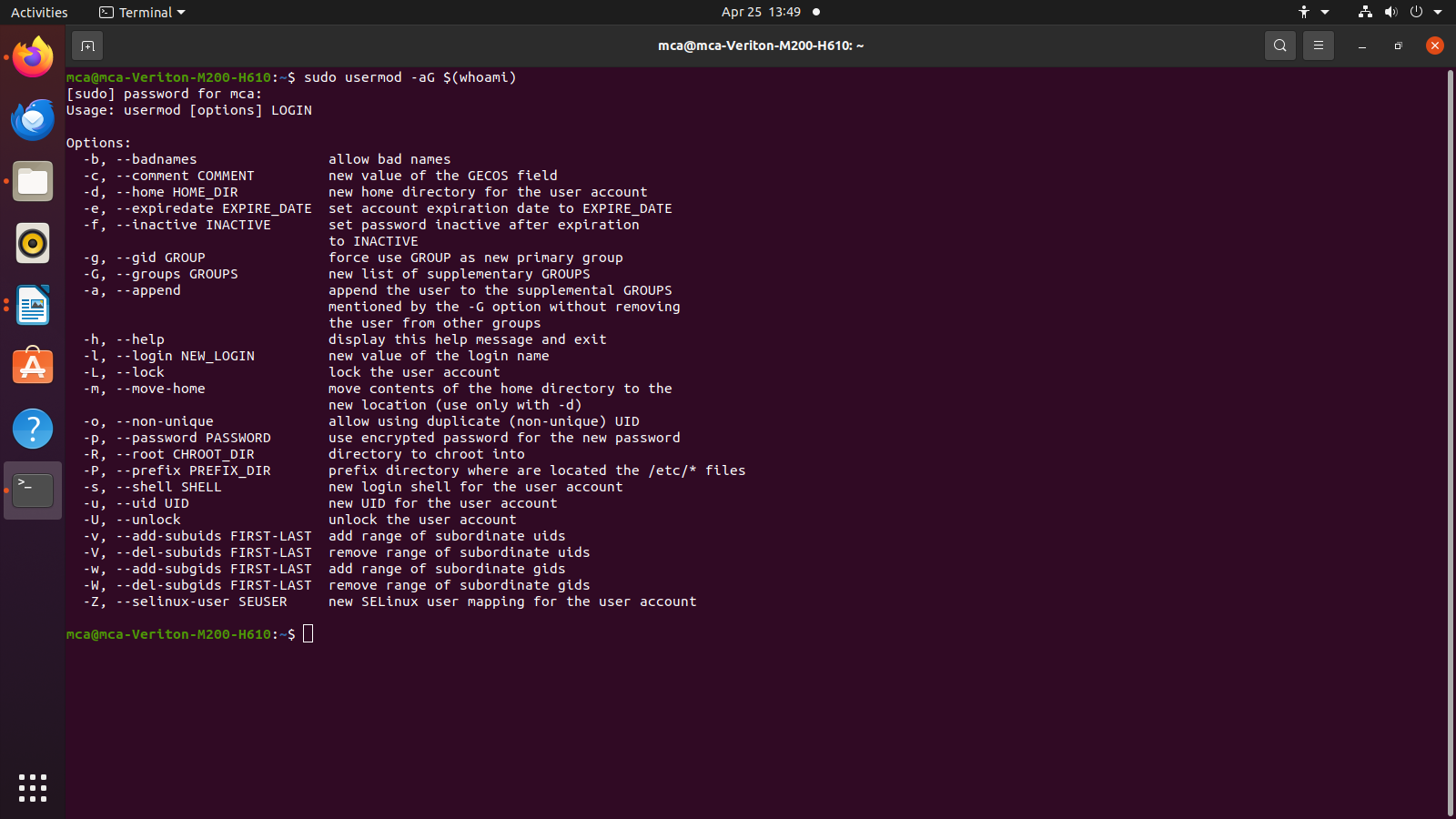
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

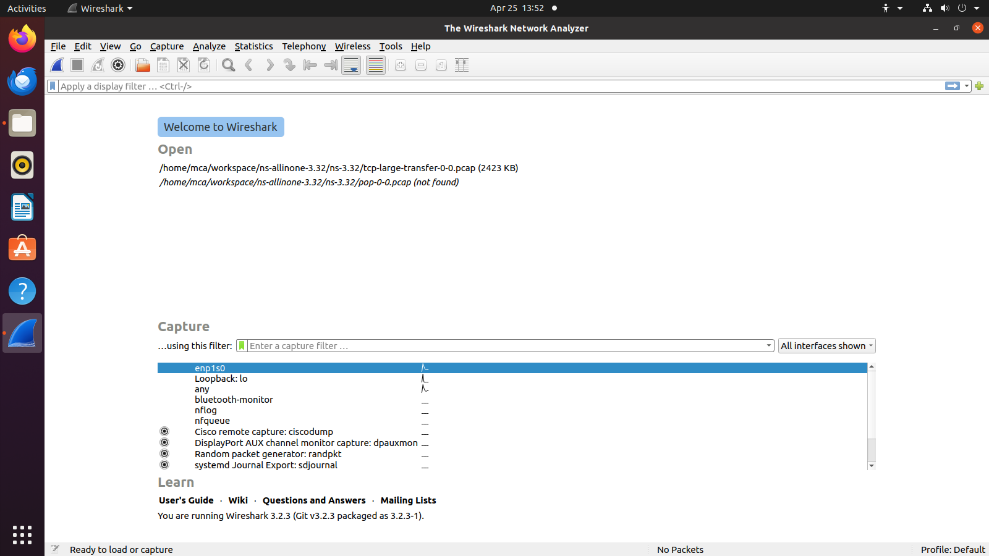
Some reasons people use Wireshark:

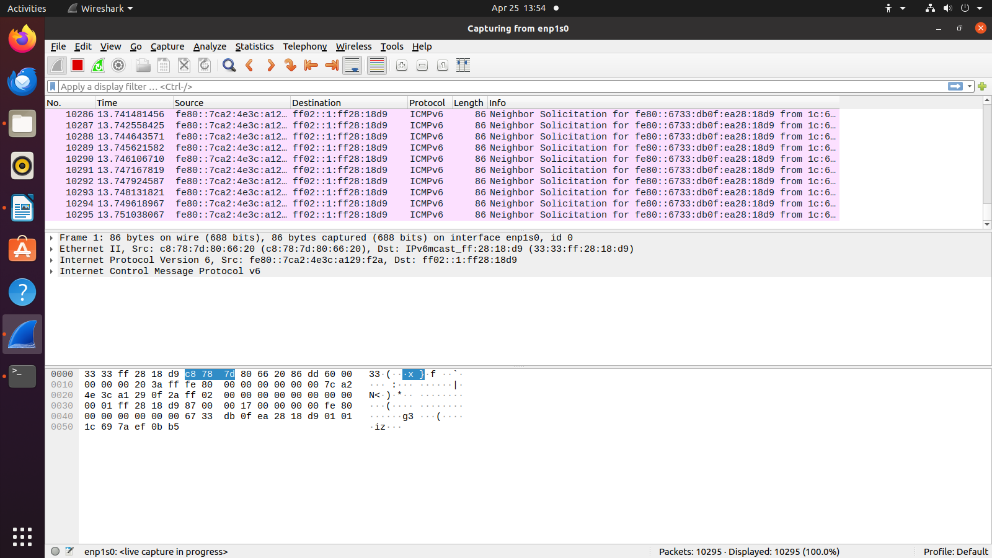
* Network administrators use it to troubleshoot network problems
* Network security engineers use it to examine security problems
* QA engineers use it to verify network applications
* Developers use it to debug protocol implementations
* People use it to learn network protocol internals

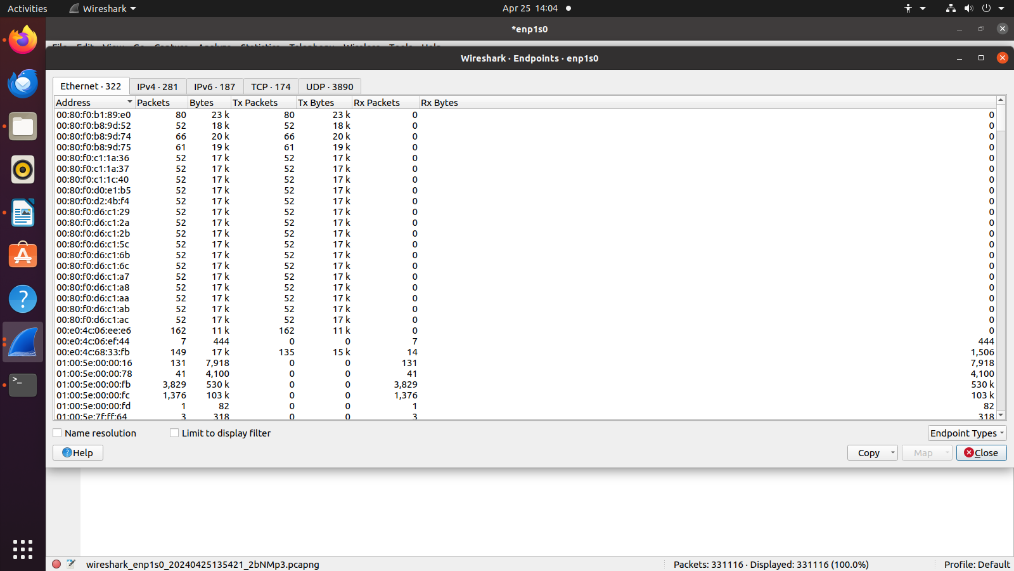
The following are some of the many features Wireshark provides:

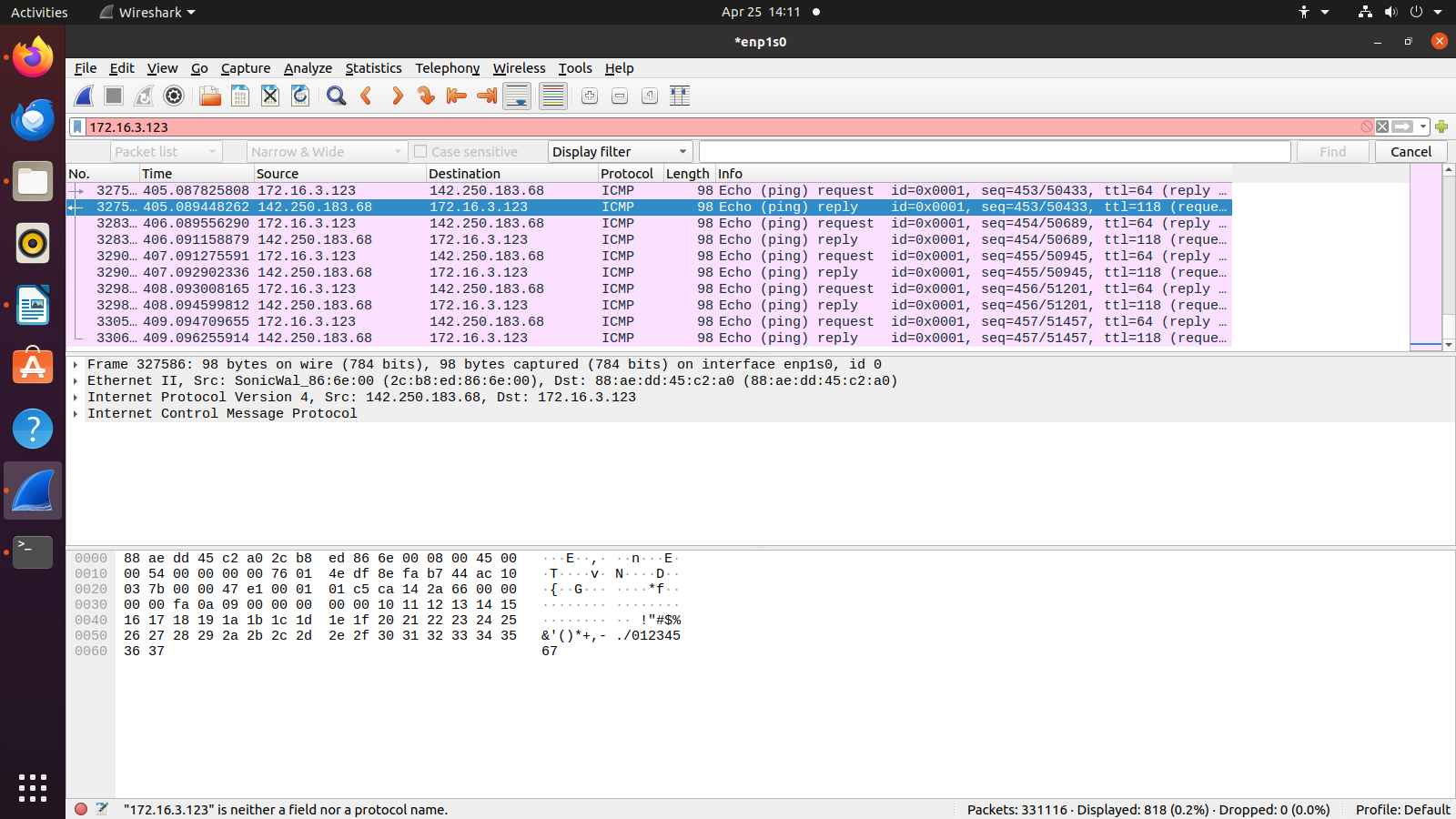
* Available for UNIX and Windows.
* Capture live packet data from a network interface.
* Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* Display packets with very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

**Output/Analysis: -**

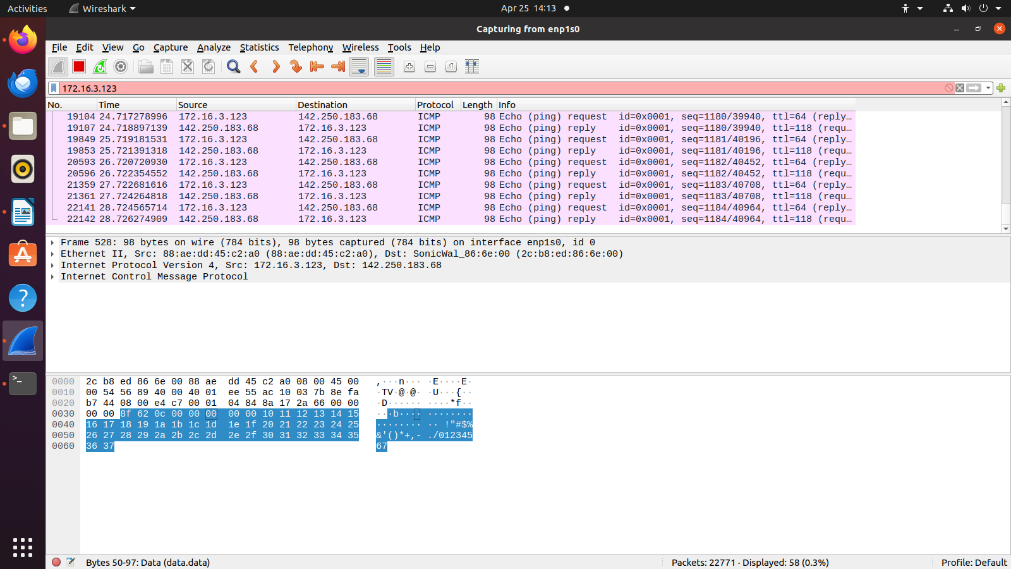
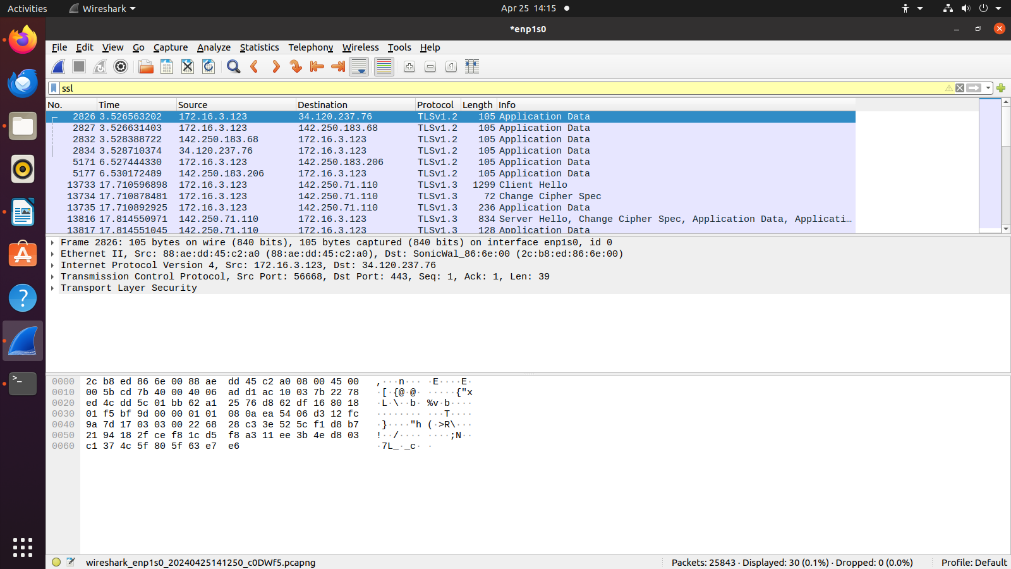
**Packet capturing**

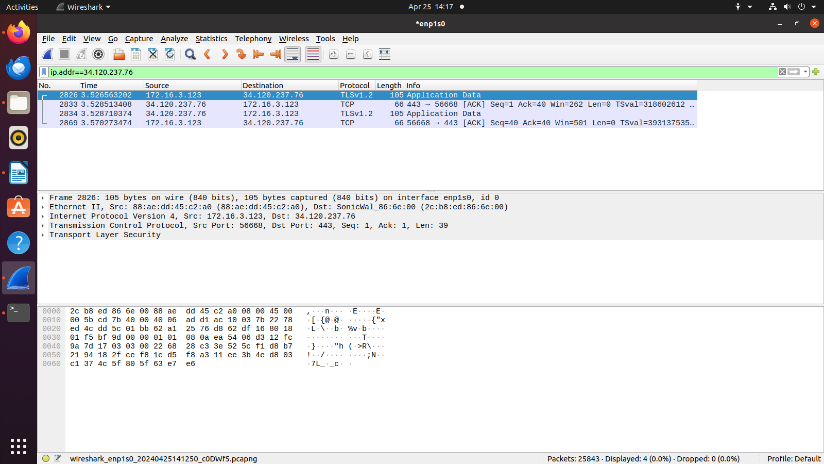
**Packet capturing process**

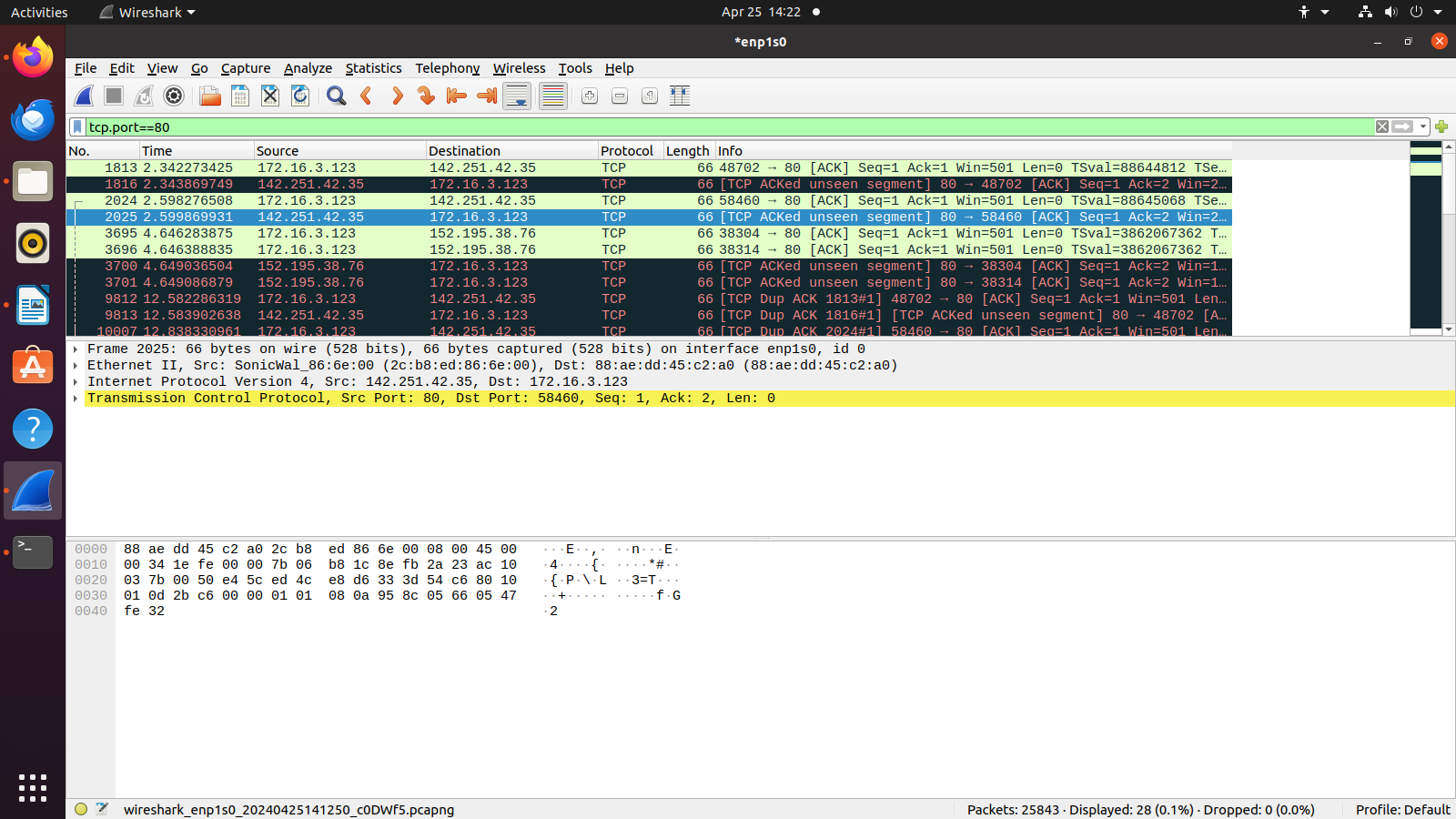
**Analyzing endpoints**

**ICMP Traffic analysis**

**HTTPS Traffic analysis**

<https://innovateindia.mygov.in/ppc-2024/>

****

**TCP traffic analysis**

**Conclusion: -**

Successful analyzed traffic of networks using wireshark.