**Experiment 3**

**Aim:** Use wireshark to understand the operation.

**Theory:**

## **What Is Wireshark?**

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. Packet is the name given to a discrete unit of data in a typical Ethernet network.

## **How Does It Work?**

Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

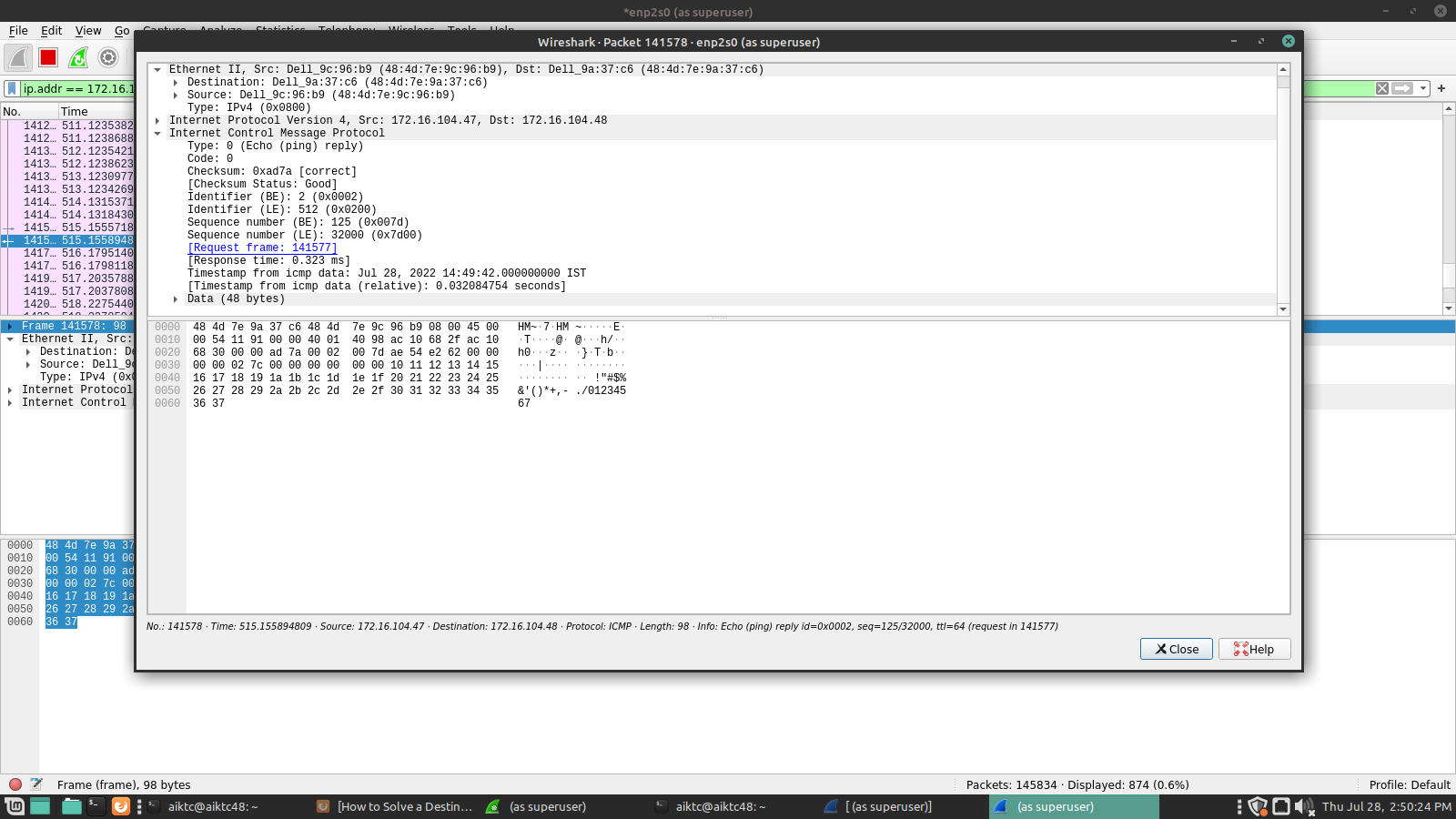
1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

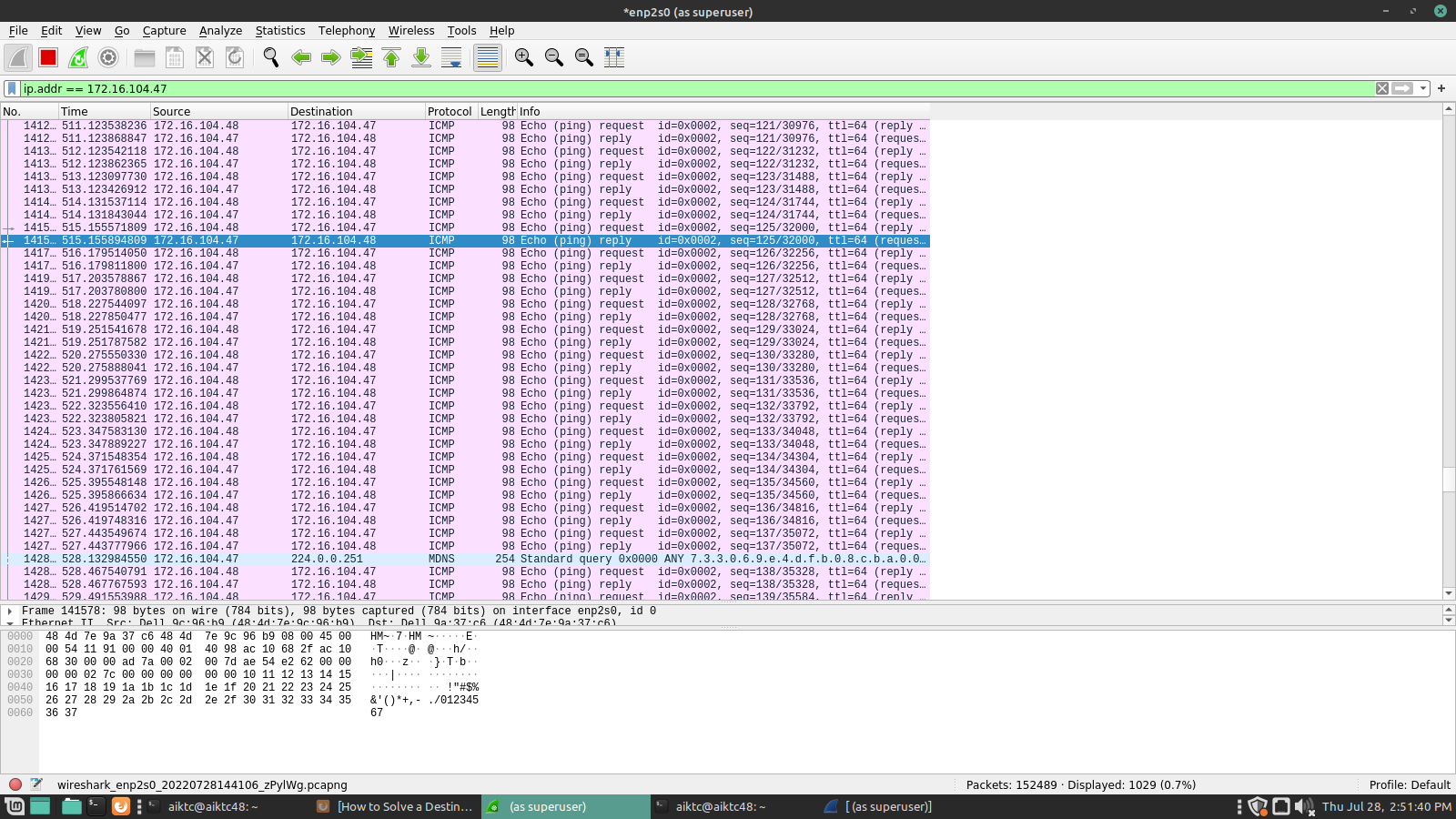
Wireshark has many uses, including [troubleshooting networks](https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting) that have performance issues. Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic. It’s a major part of any IT pro’s toolkit – and hopefully, the IT pro has the knowledge to use it.

## **Features of Wireshark?**

Wireshark consists of a rich feature set including the following:

* WiresLive capture and offline analysis
* Rich VoIP analysis
* Read/write many different capture file formats
* Capture compressed files (gzip) and decompress them on the fly
* Deep inspection of hundreds of protocols
* Standard three-pane packet browser
* Captured network packets can be browsed via a GUI or TShark utility
* Multi-platform easily ran on Linux, Windows, OS X, and FreeBSD
* Powerful display filters
* Output can be exported to XML, CSV, PostScript, or as a plain text
* Packet list can use coloring rules for quick and intuitive analysis





**Conclusion:** In this experiment we have connected our system with another system and analysed network traffic using Wireshark.