**Wireshark**

Wireshark is an open-source packet analyzer that is used for network troubleshooting, education, analysis, software development, and communication protocol creation.

It is used to track the packets so that each one is filtered to meet our specific needs. It is commonly called as a **sniffer, network protocol analyzer, and network analyzer**. It is also used by network security engineers to examine security problems.

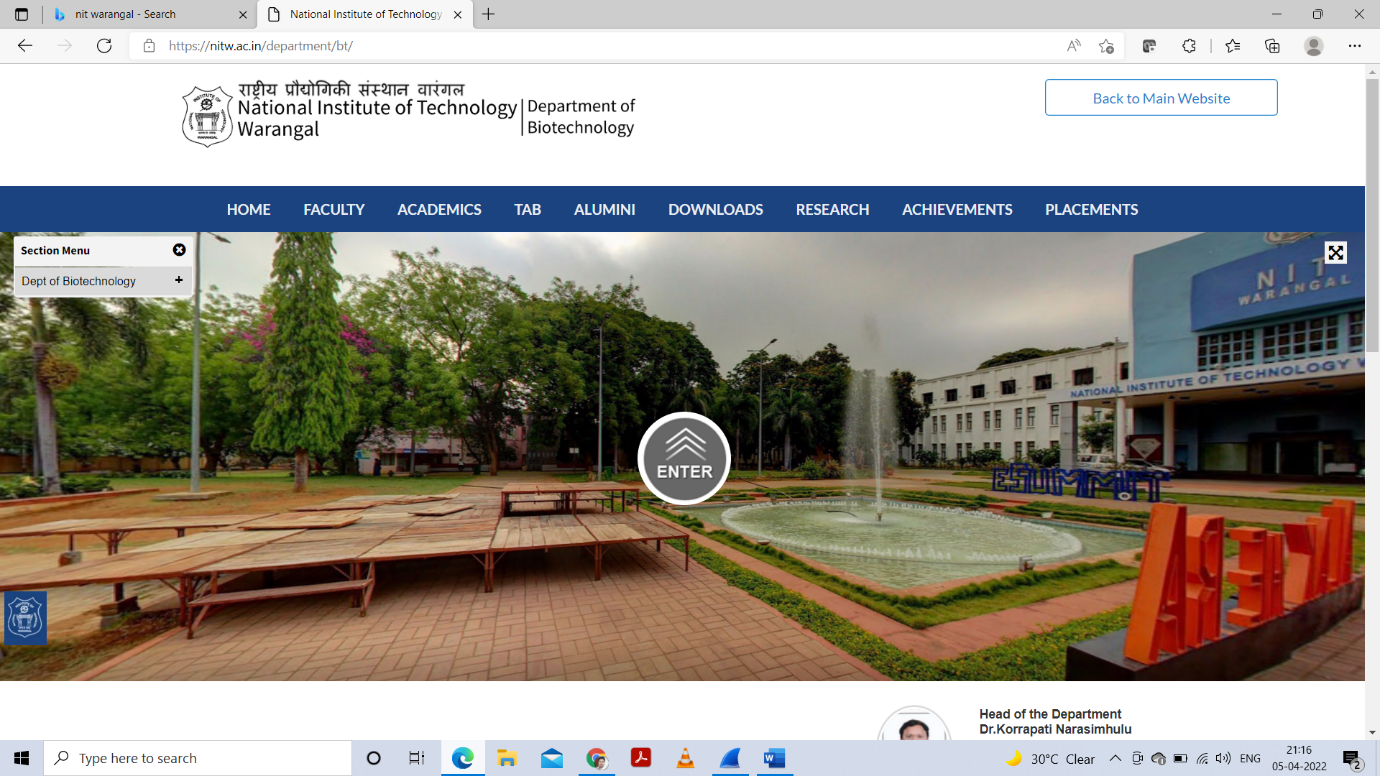
**Features of Wireshark**

* it can run on Linux, Windows, OS X, FreeBSD, NetBSD, etc.
* It performs deep inspection of the hundreds of protocols.
* It has sort and filter options which makes ease to the user to view the data.
* It can also capture raw USB traffic.
* Various settings, like timers and filters, can be used to filter the output.
* It can only capture packet on the PCAP (an application programming interface used to capture the network) supported networks.
* Wireshark supports a variety of well-documented capture file formats such as the PcapNg and Libpcap. These formats are used for storing the captured data.

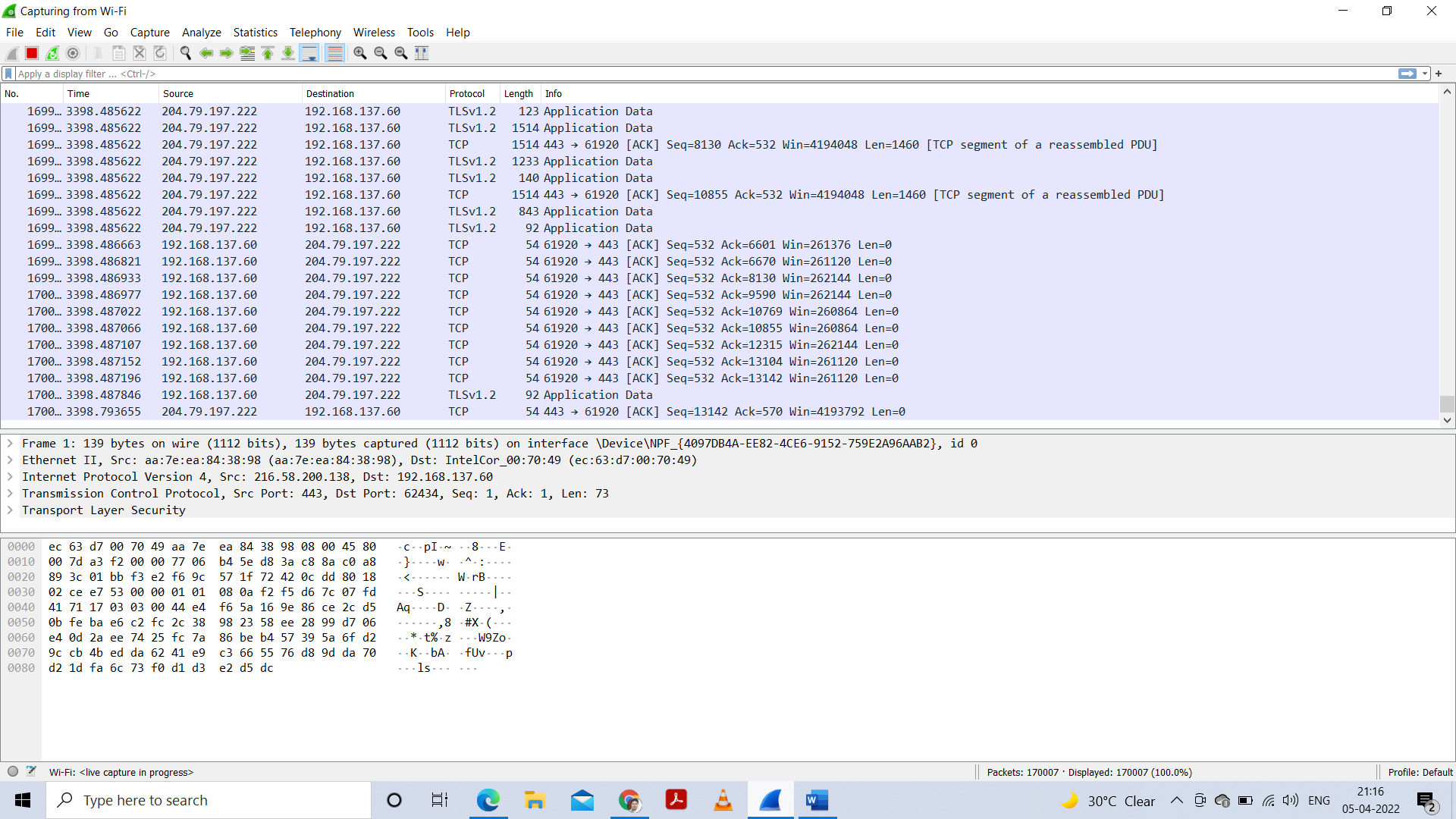
**Uses of Wireshark**

* Network security engineers use it to investigate security issues.
* It allows users to see all of the traffic that passes through the network.
* It also aids in the diagnosis of latency problems and malicious activity on your network.
* Network engineers use it to troubleshoot network issues.
* It can also examine packets that have been dropped.
* It enables us to understand how all devices, such as laptops, cell phones, desktop computers, switches, routers, and so on, connect inside a local network or with the rest of the world.

Visiting [National Institute of Technology | Warangal (nitw.ac.in)](https://nitw.ac.in/department/bt/) website.

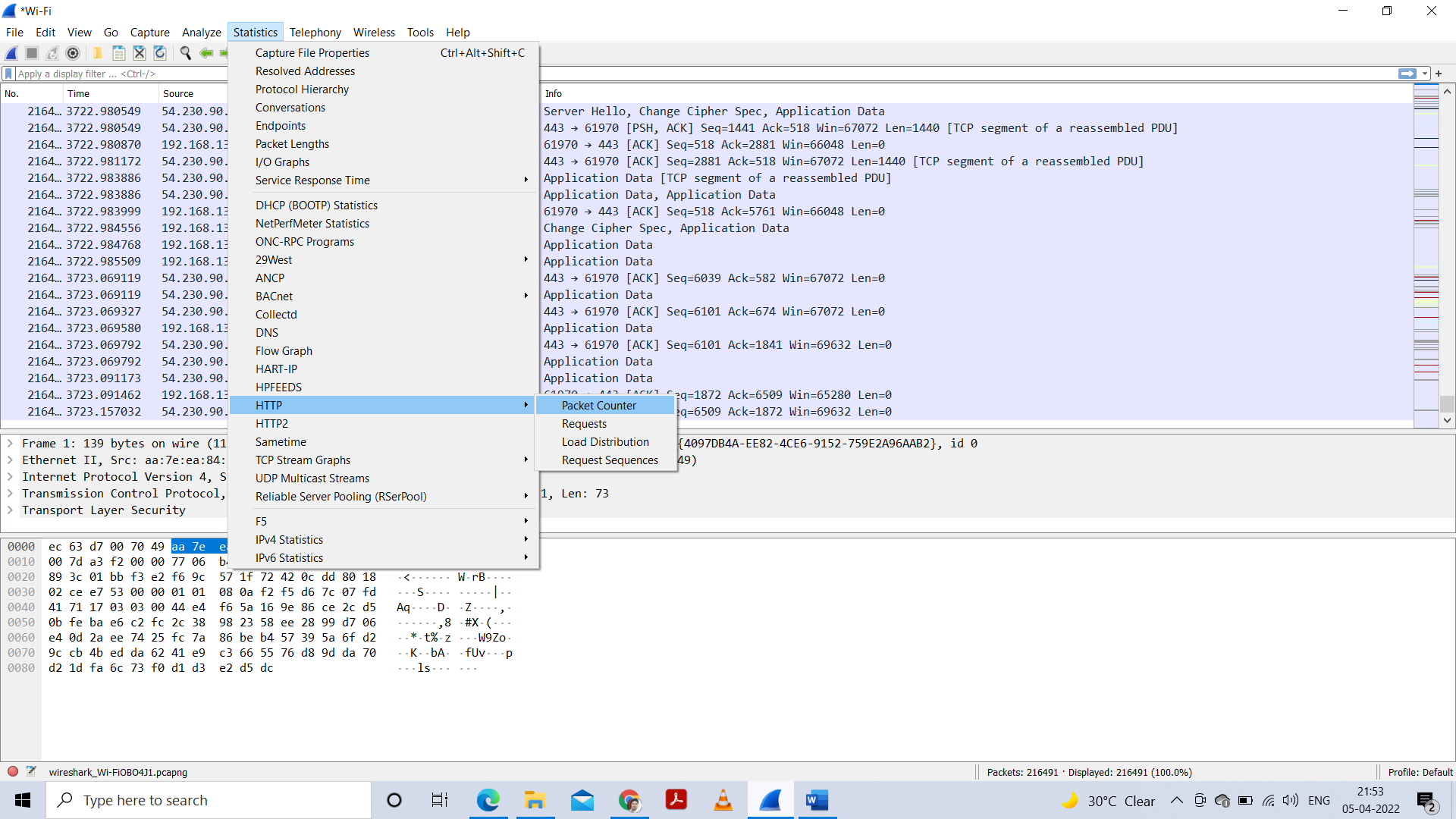


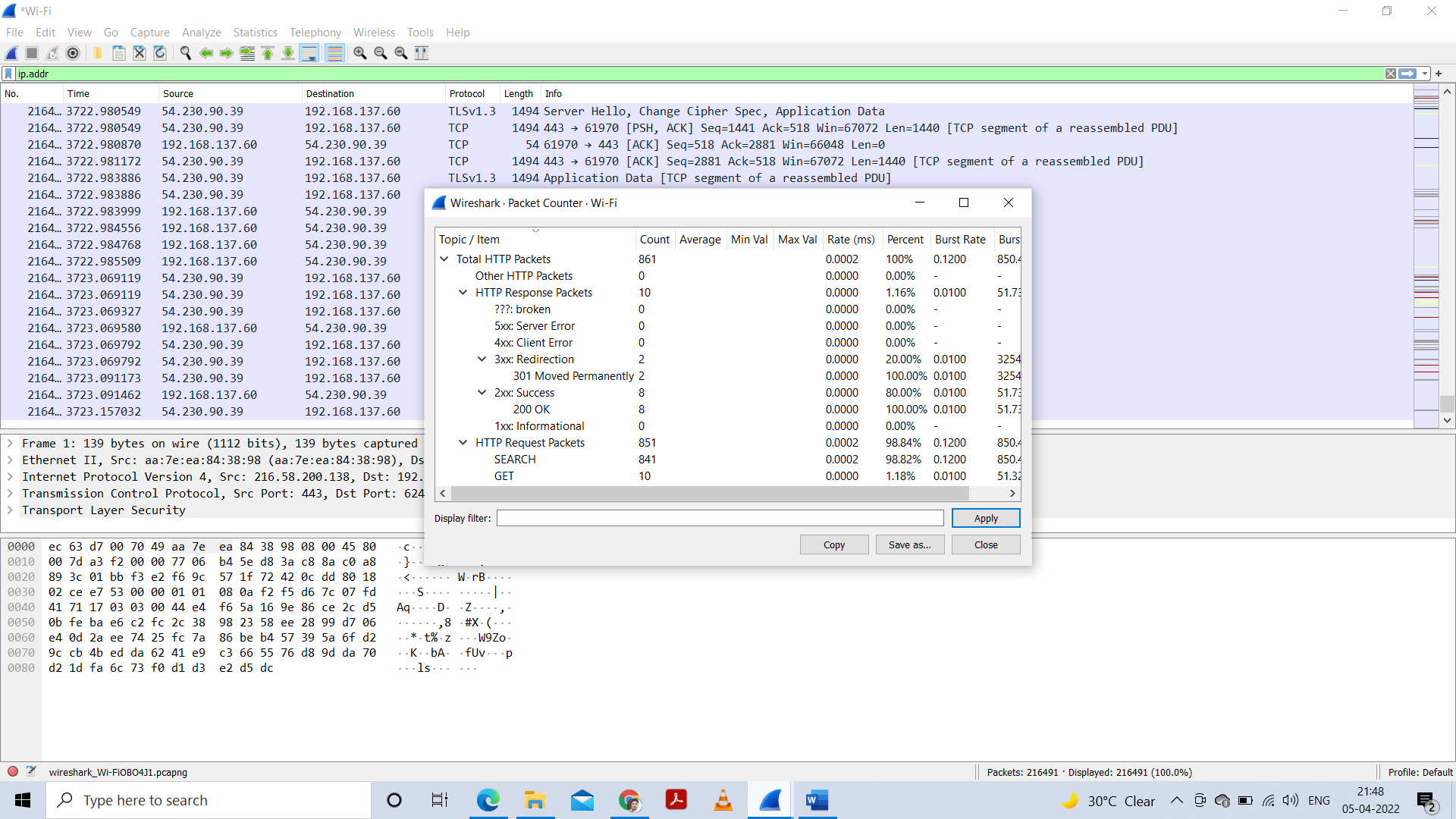
These(below) are the details of packets which are transferring. It contains information like source IP, Destination IP, Length of Packets and information about packets.

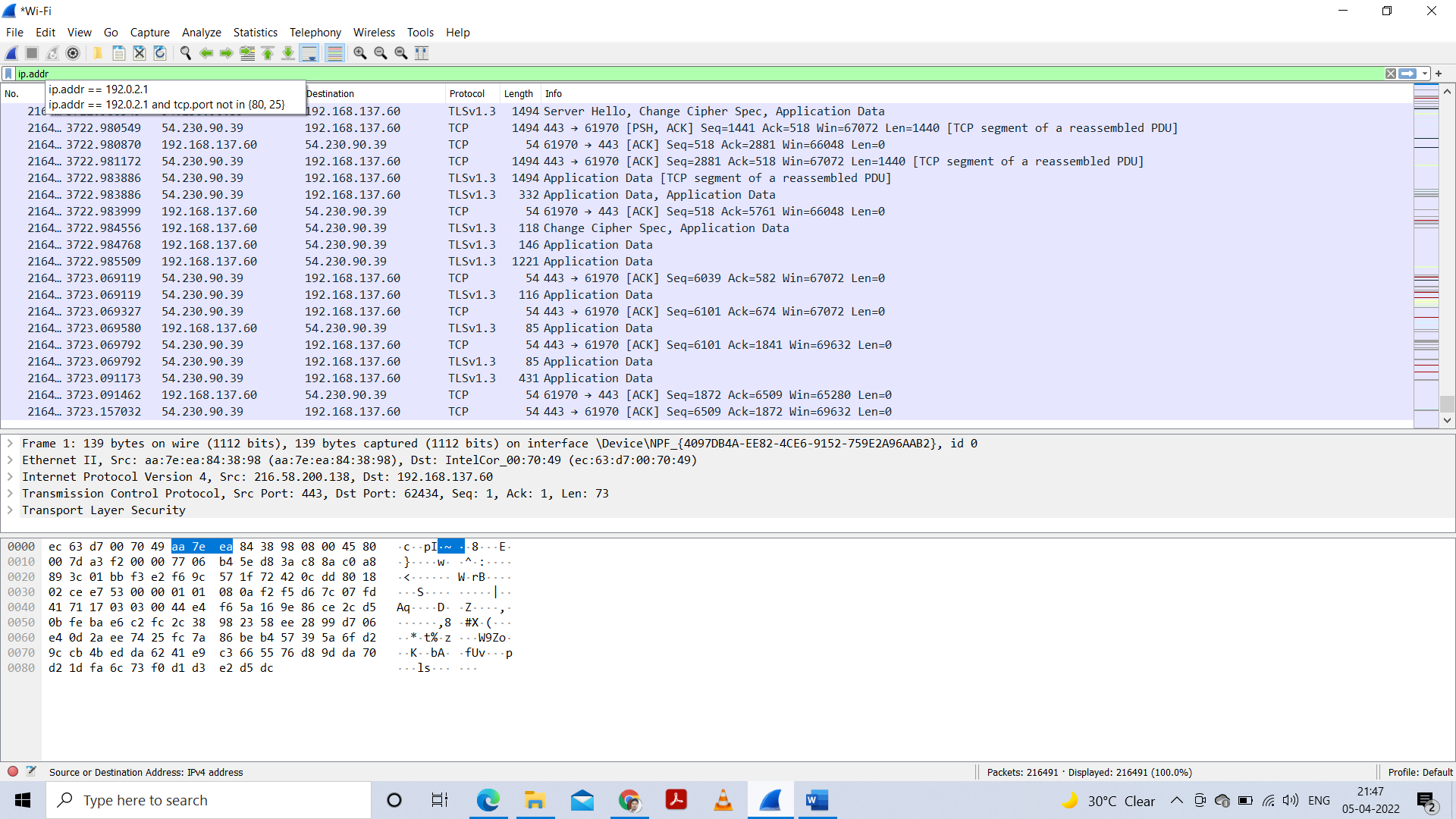


**Applying some filters**

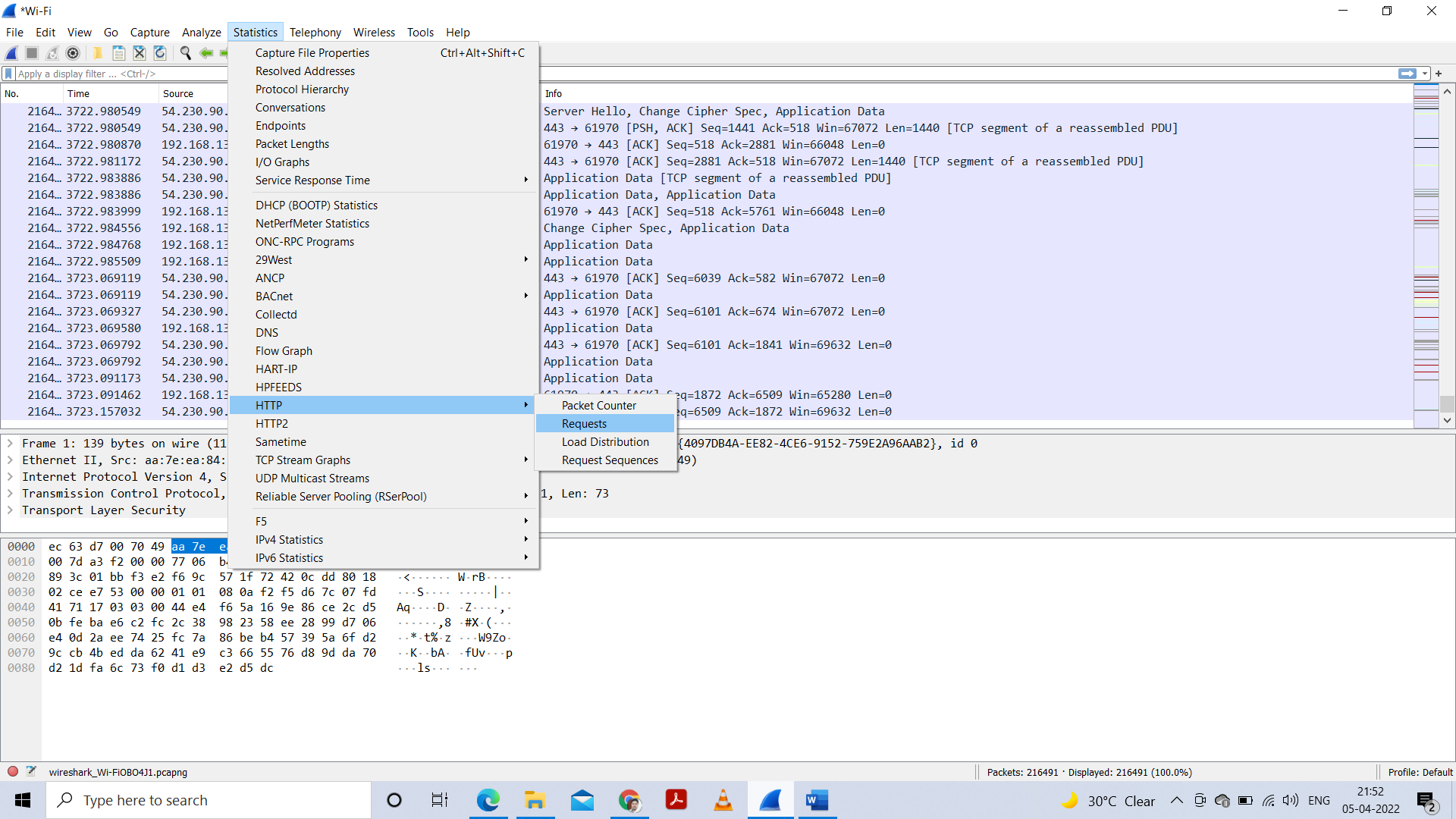
**1. Packet counter**

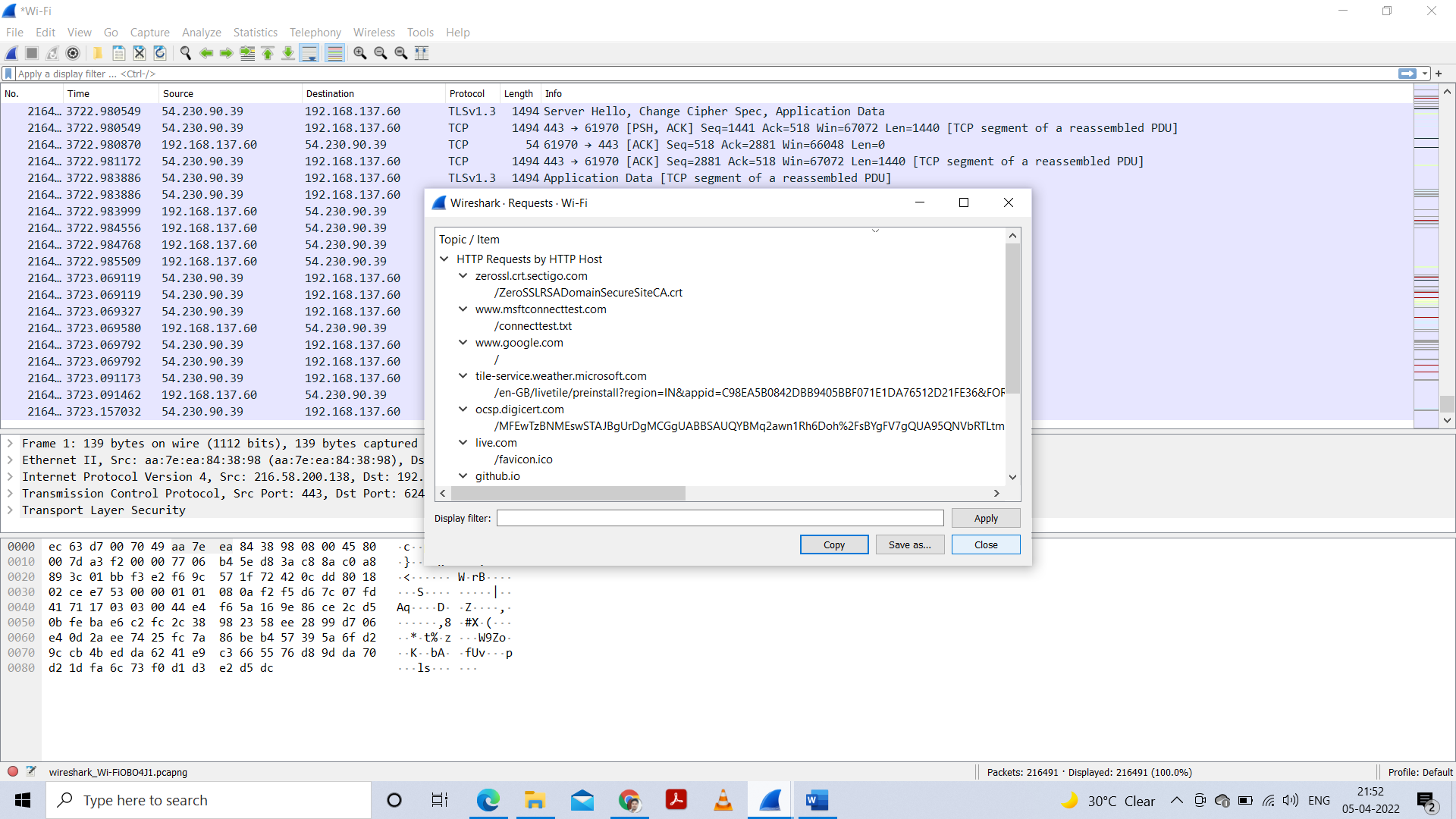


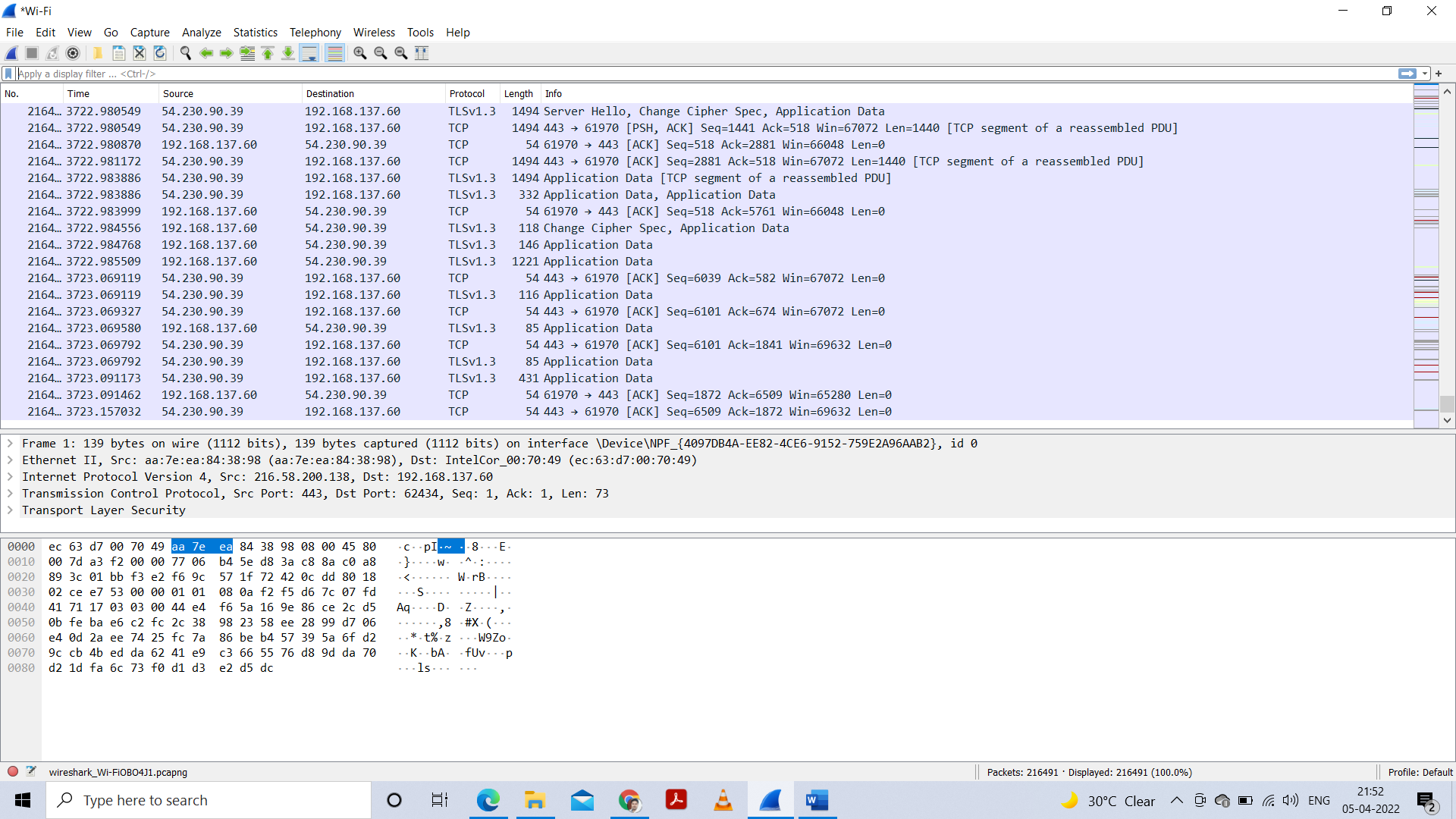




**2. Request packets**







**3. Load distribution**

