WIRESHARK PACKET ANALYSIS

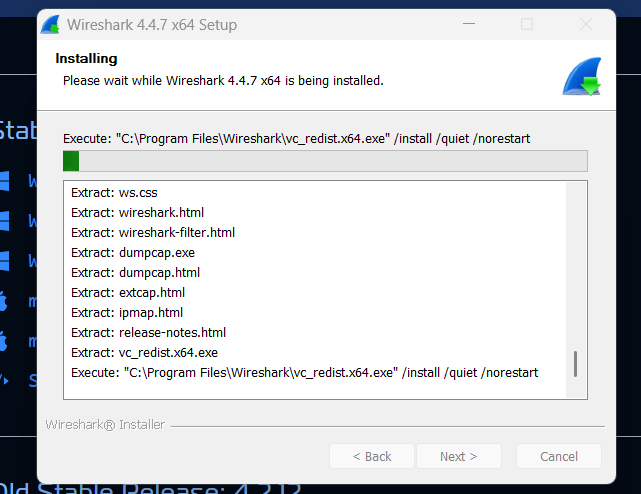
Submitted by

Rishikesh M

INSTALL WIRESHARK

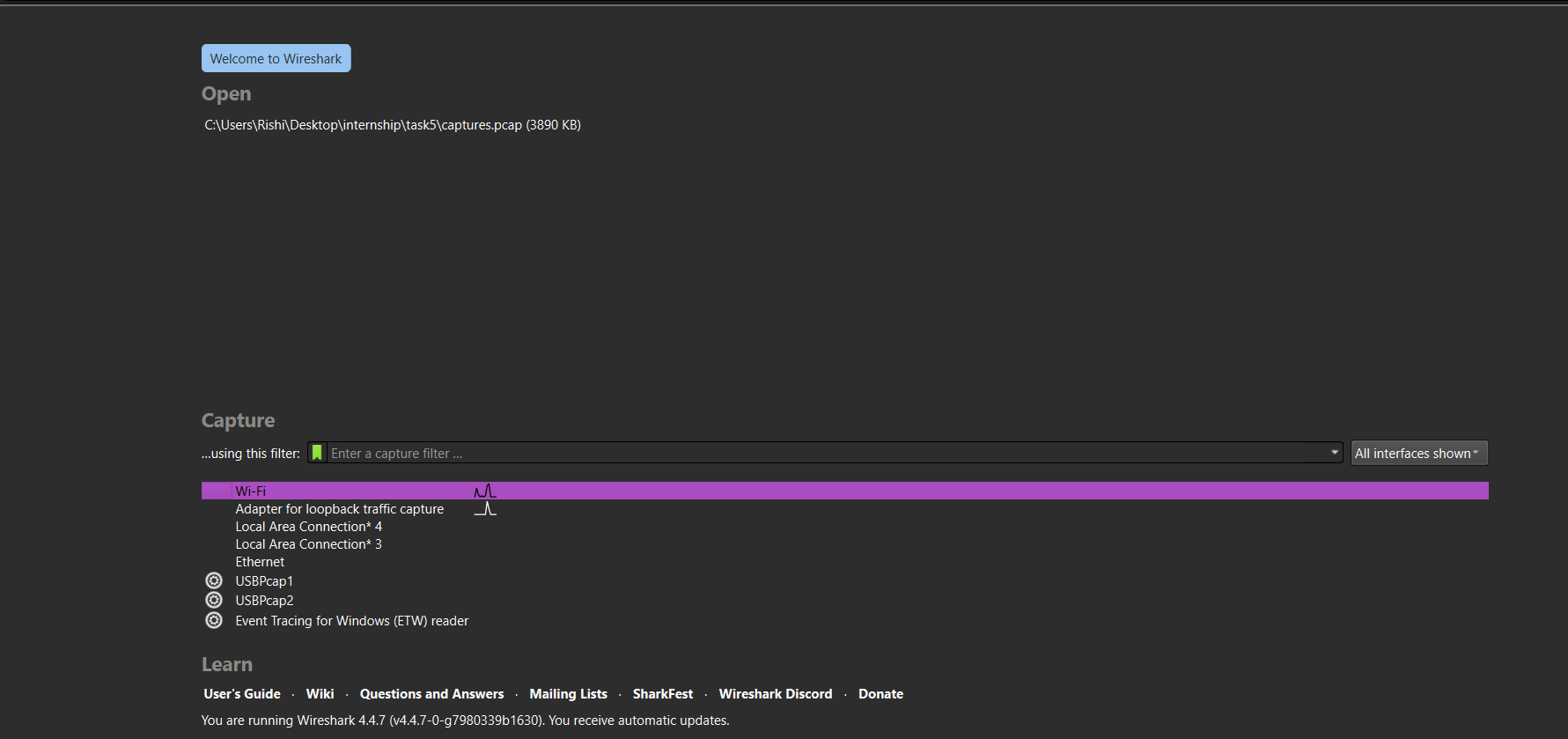
Operating sytem: Windows 11 23H2

Use the official website of wireshark to install the latest version.

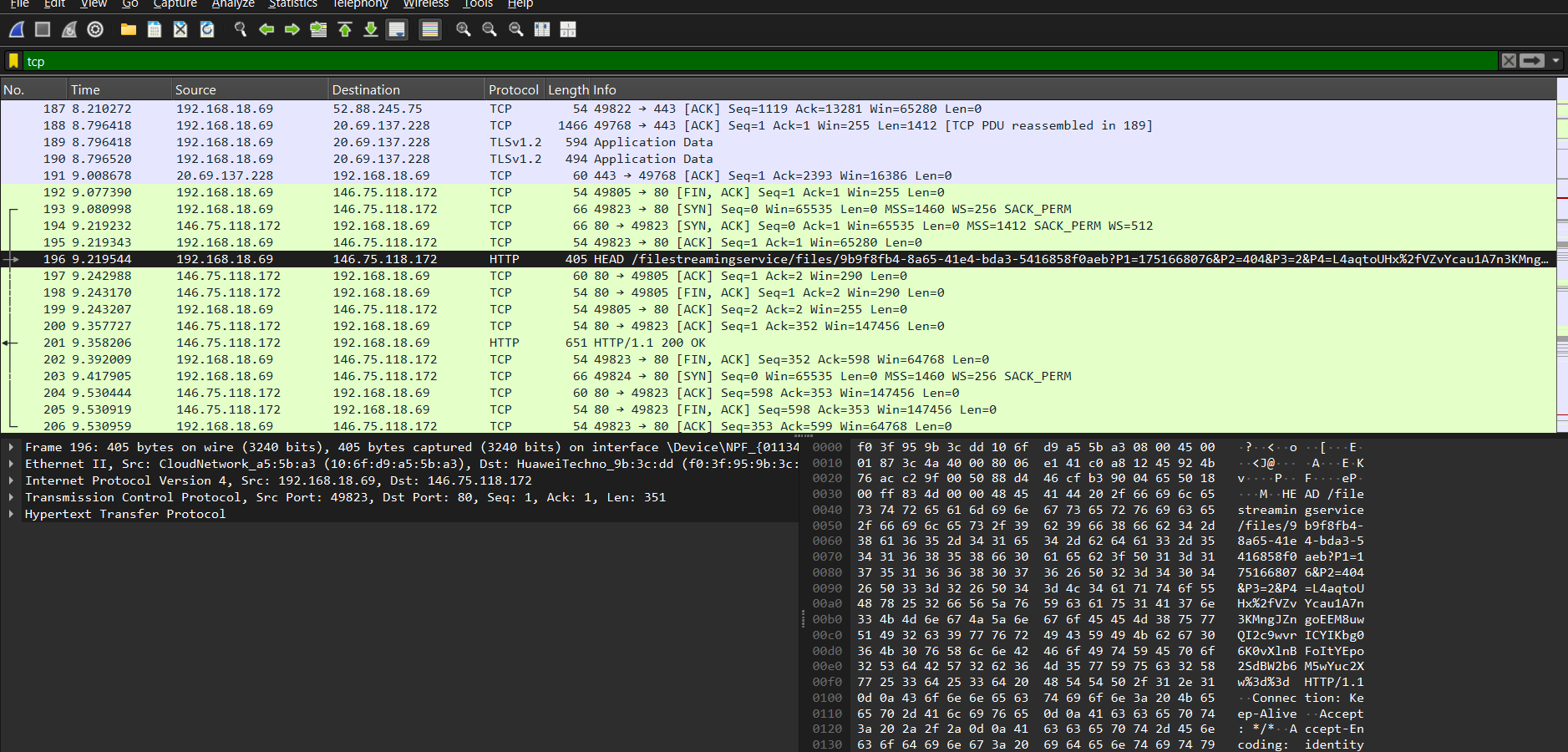


START CAPTURING PACKETS

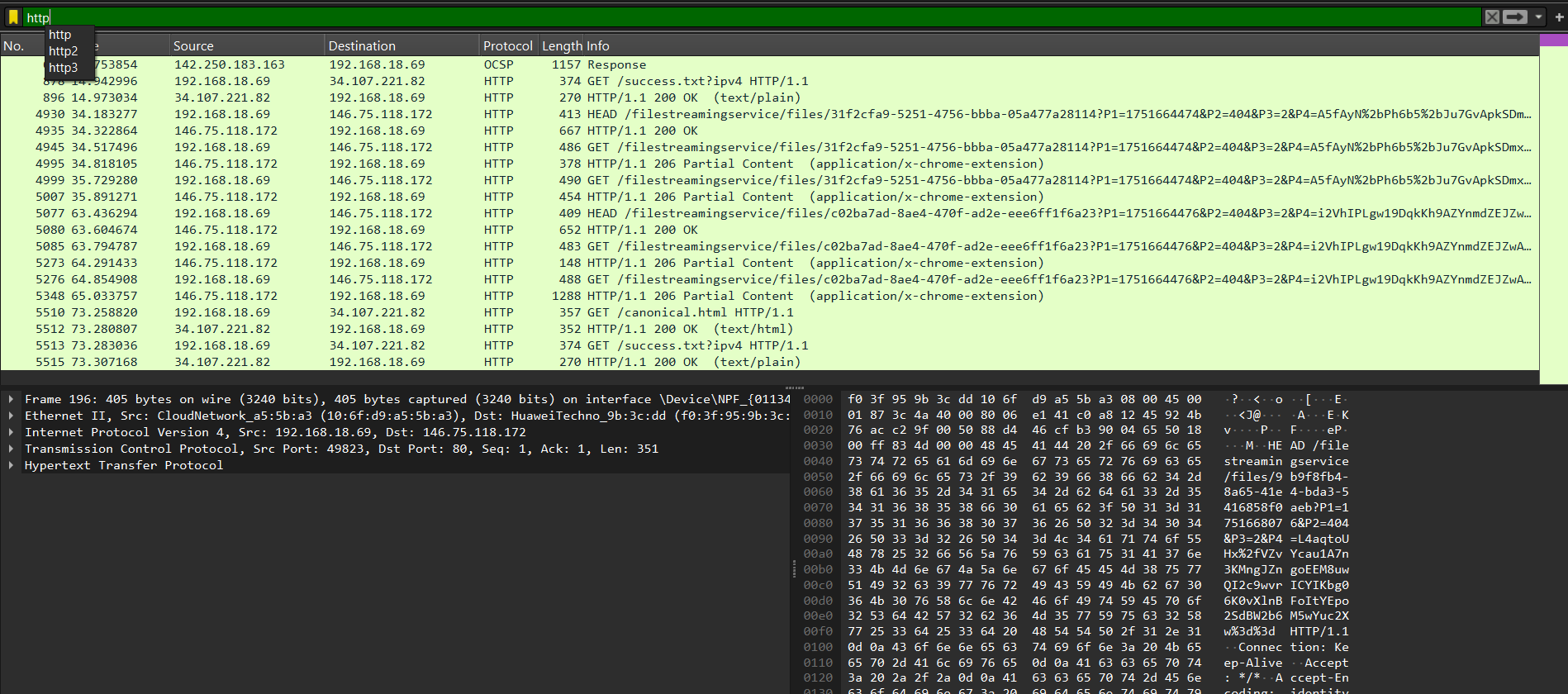
Use Start the packet capture and open a website eg: https://www.geeksforgeeks.com to capture the packets and analyze them.



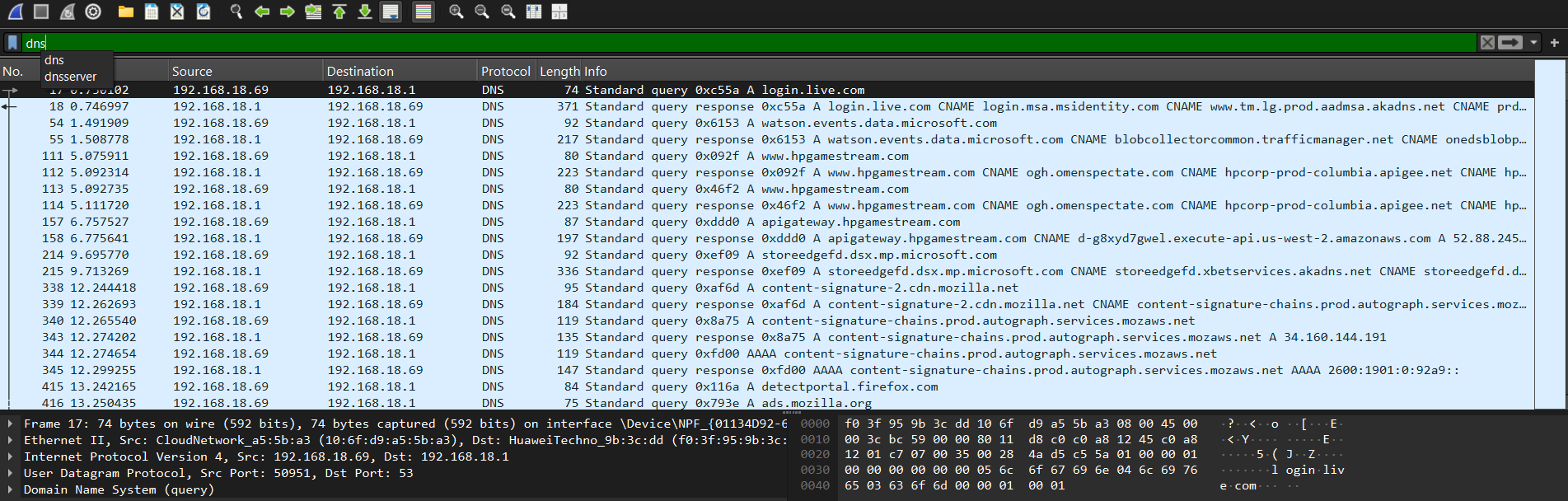
FILTER TCP PACKETS



FILTER HTTP PACKETS



FILTER DNS PACKETS



SUMMARY

Wireshark is an open source packet capture software that helps a security analyst to observe the different packets that travel through a network and analyze them for any kind of unusual or suspicious activity. The terminal version of wireshark is called t-shark. This software is also extremely useful in detecting the corporate attackers who might get access to the internal network and are already trying to attack the network internally.

REFERENCES

<https://www.wireshark.org/download.html>

<https://en.wikipedia.org/wiki/Wireshark>