**NETWORK ANALYSIS USING WIRESHARK**

**AIM**

To monitor different websites and their network protocols using Wireshark (network analysing tool)

**THEORY**

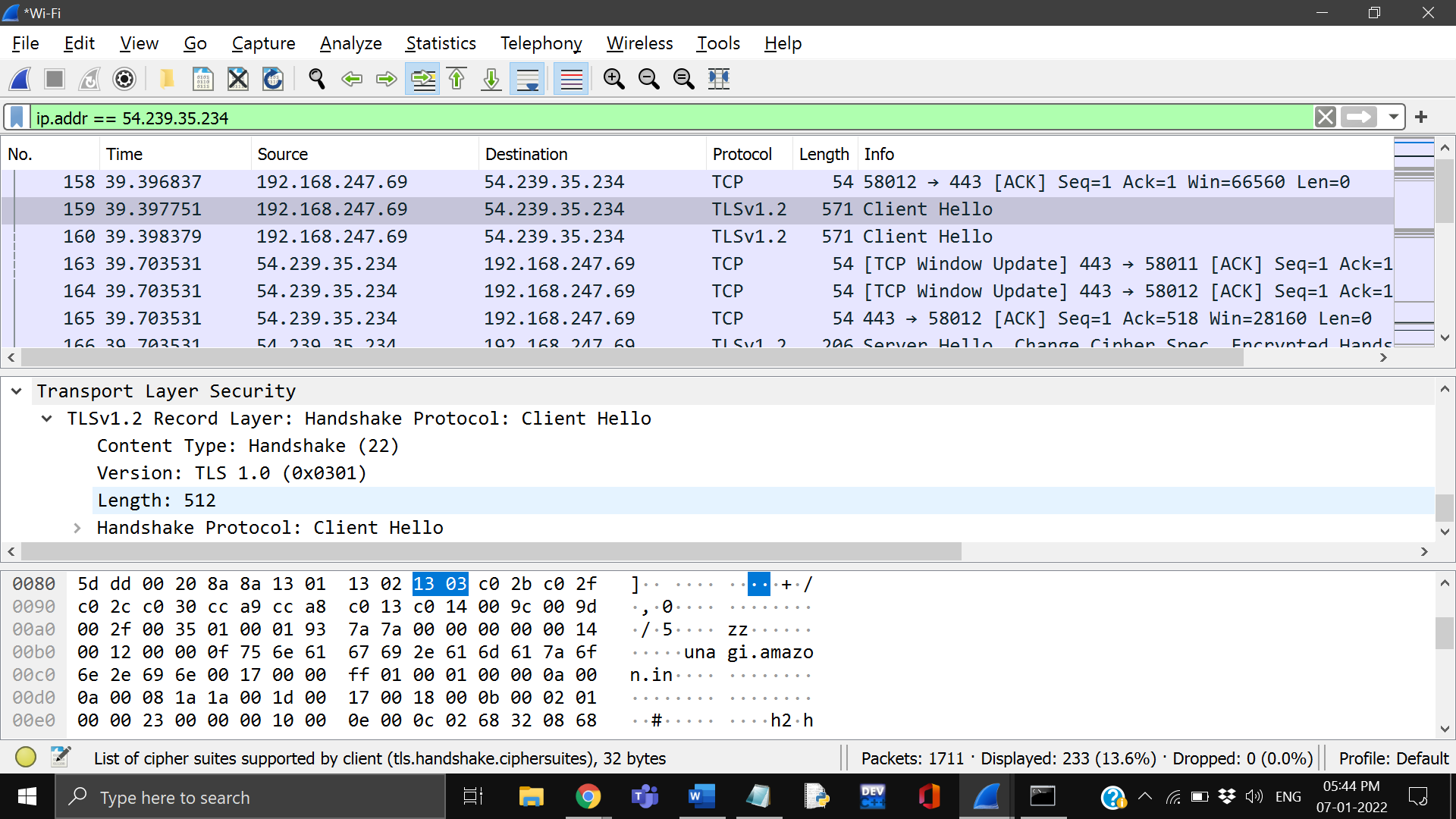
Wireshark is a free and open-source network protocol analyzer that enables users to interactively browse the data traffic on a computer network. The development project was started under the name Ethereal, but was renamed Wireshark in 2006.  
  
Many networking developers from all around the world have contributed to this project with network analysis, troubleshooting, software development and communication protocols. Wireshark is used in many educational institutions and other industrial sectors.

Wireshark is a network or protocol analyzer (also known as a network sniffer) available for free at the Wireshark website. It is used to analyze the structure of different network protocols and has the ability to demonstrate encapsulation. The analyzer operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing. Wireshark and other terminal-based free software versions like Tshark are released under the GNU General Public License.  
  
Wireshark shares many characteristics with tcpdump. The difference is that it supports a graphical user interface (GUI) and has information filtering features. In addition, Wireshark permits the user to see all the traffic being passed over the network.  
  
  
**Features of Wireshark include:**

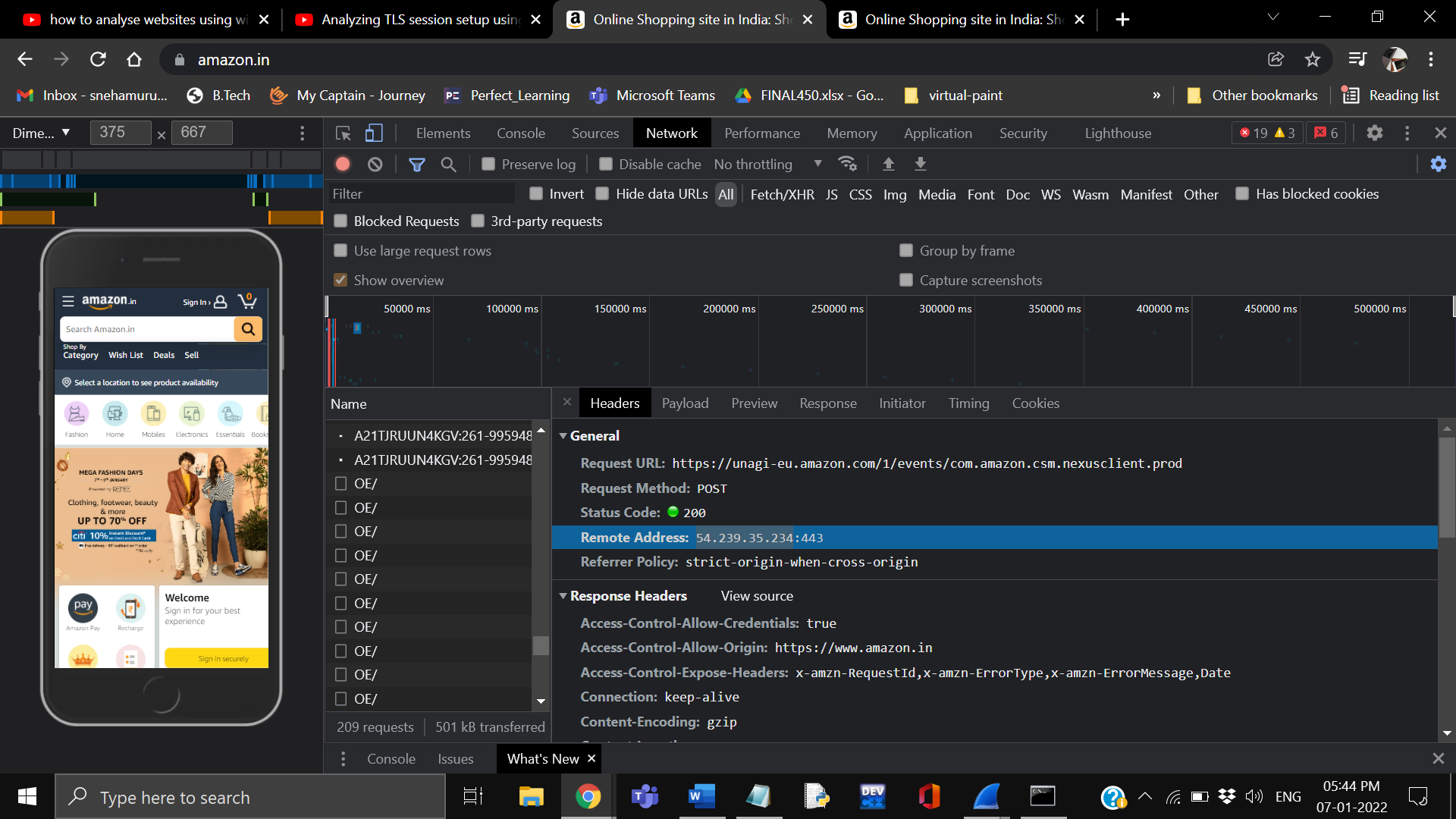
* Data is analysed either from the wire over the network connection or from data files that have already captured data packets.
* Supports live data reading and analysis for a wide range of networks (including Ethernet, IEEE 802.11, point-to-point Protocol (PPP) and loopback).
* With the help of GUI or other versions, users can browse captured data networks.

**OUTPUT SCREENSHOTS**

1. Website: <https://www.amazon.in/>

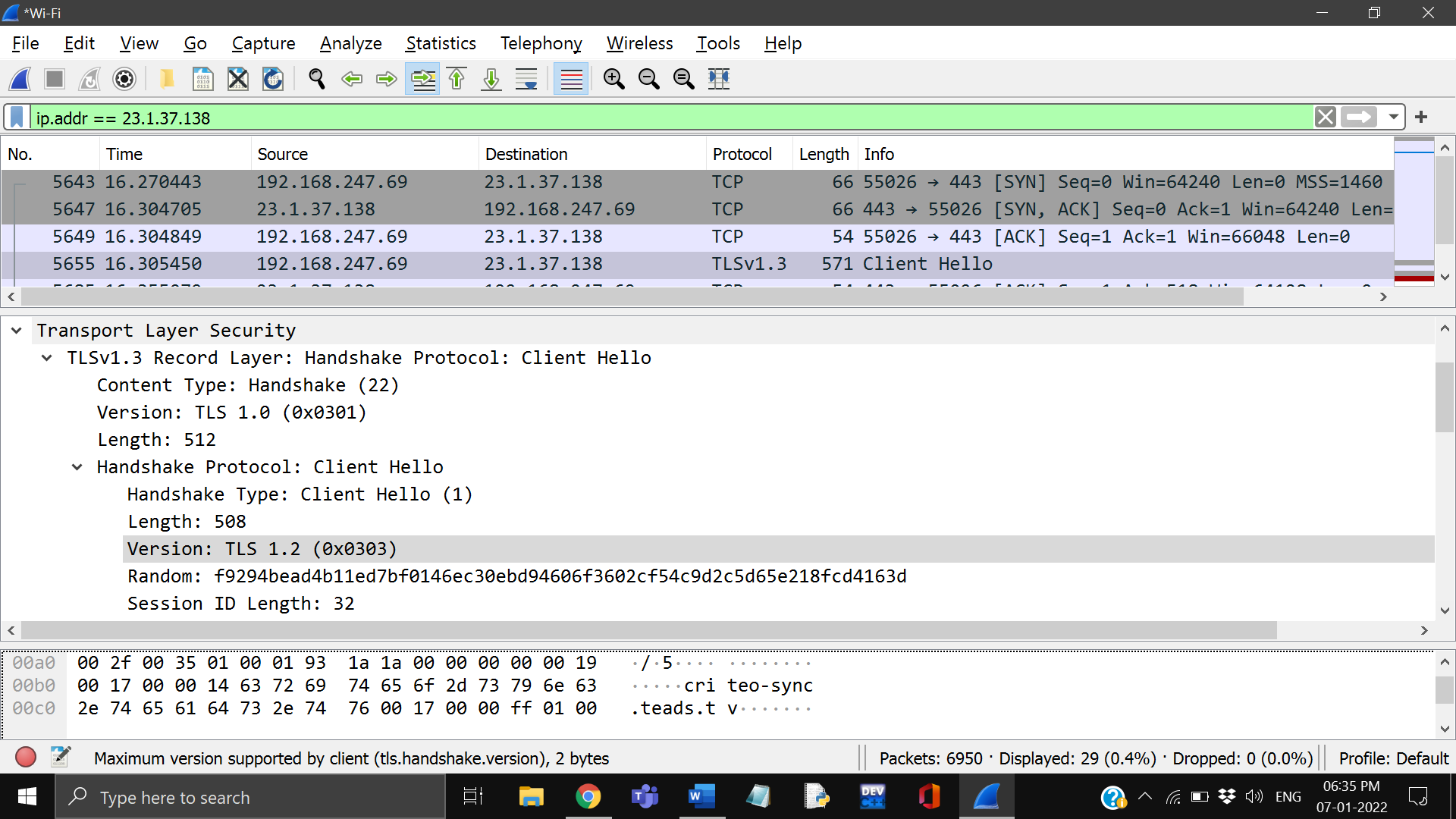




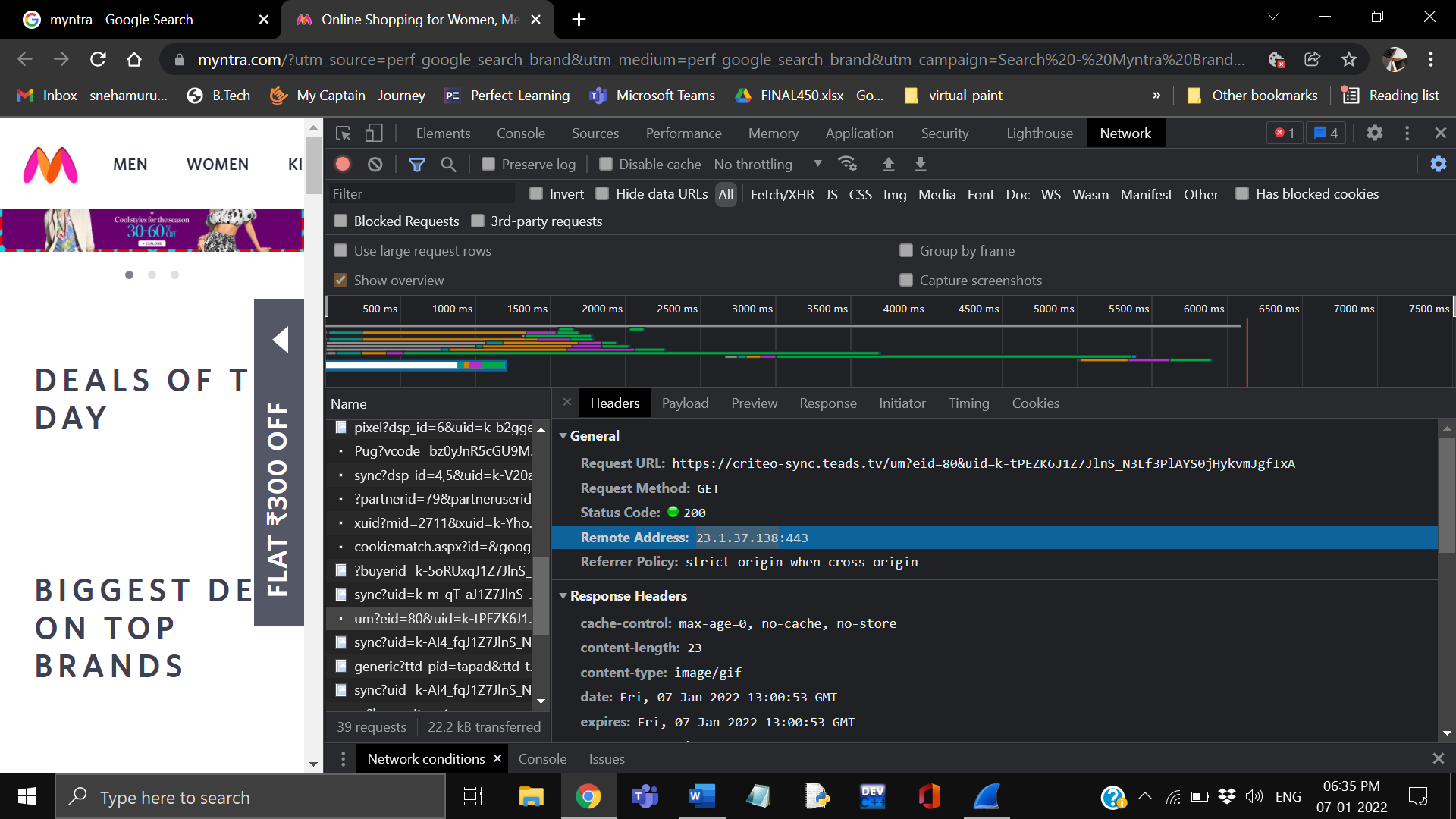




1. Website: <https://www.myntra.com/?utm_source=perf_google_search_brand&utm_medium=perf_google_search_brand&utm_campaign=Search%20-%20Myntra%20Brand%20(India)&gclid=CjwKCAiA5t-OBhByEiwAhR-hmwRCpgUJOVC-8Hm7CNtf-JQhnUIreGxWa3qgJ4wPFi6s-2eud5Ec3RoCEhMQAvD_BwE>

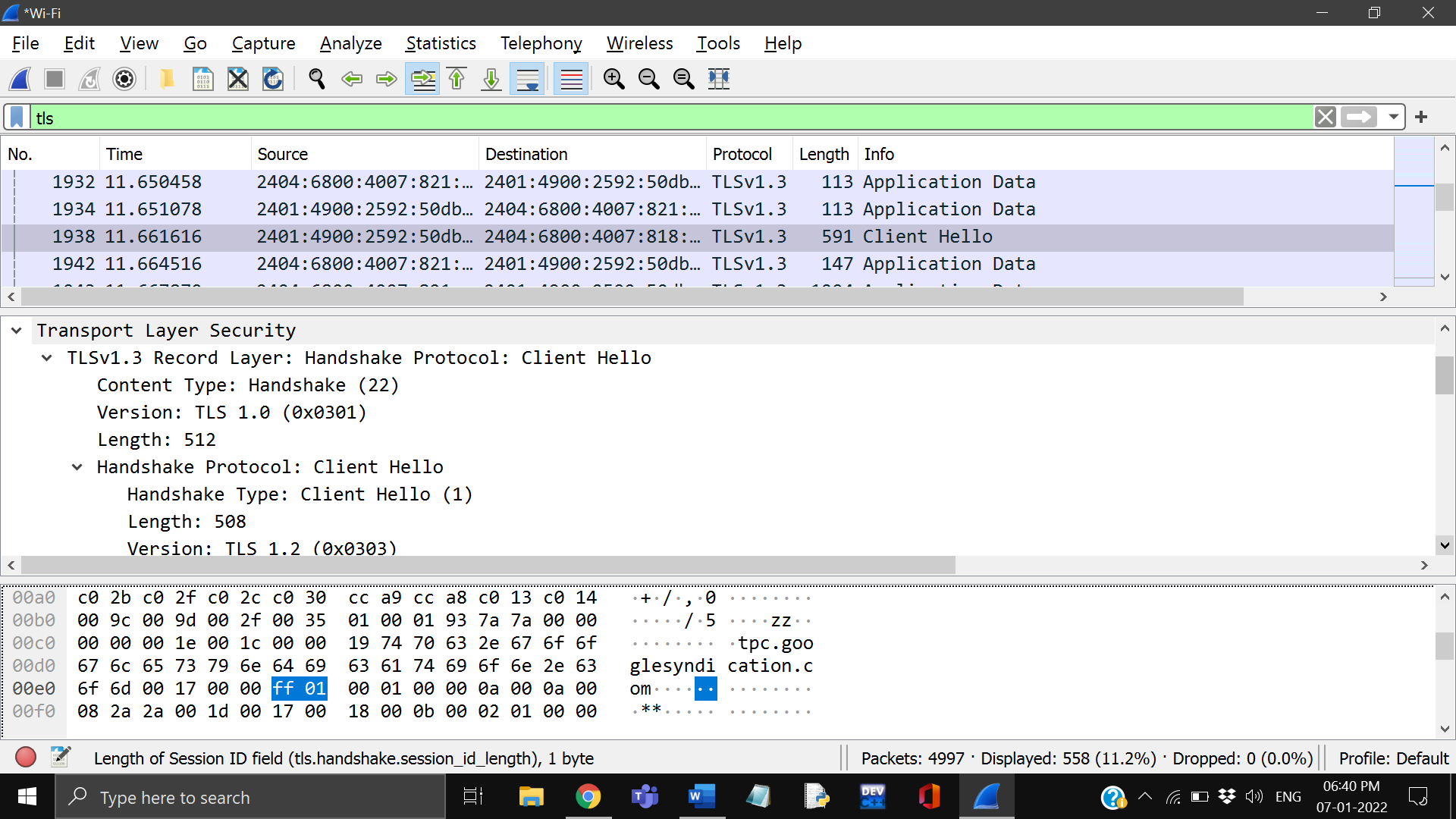




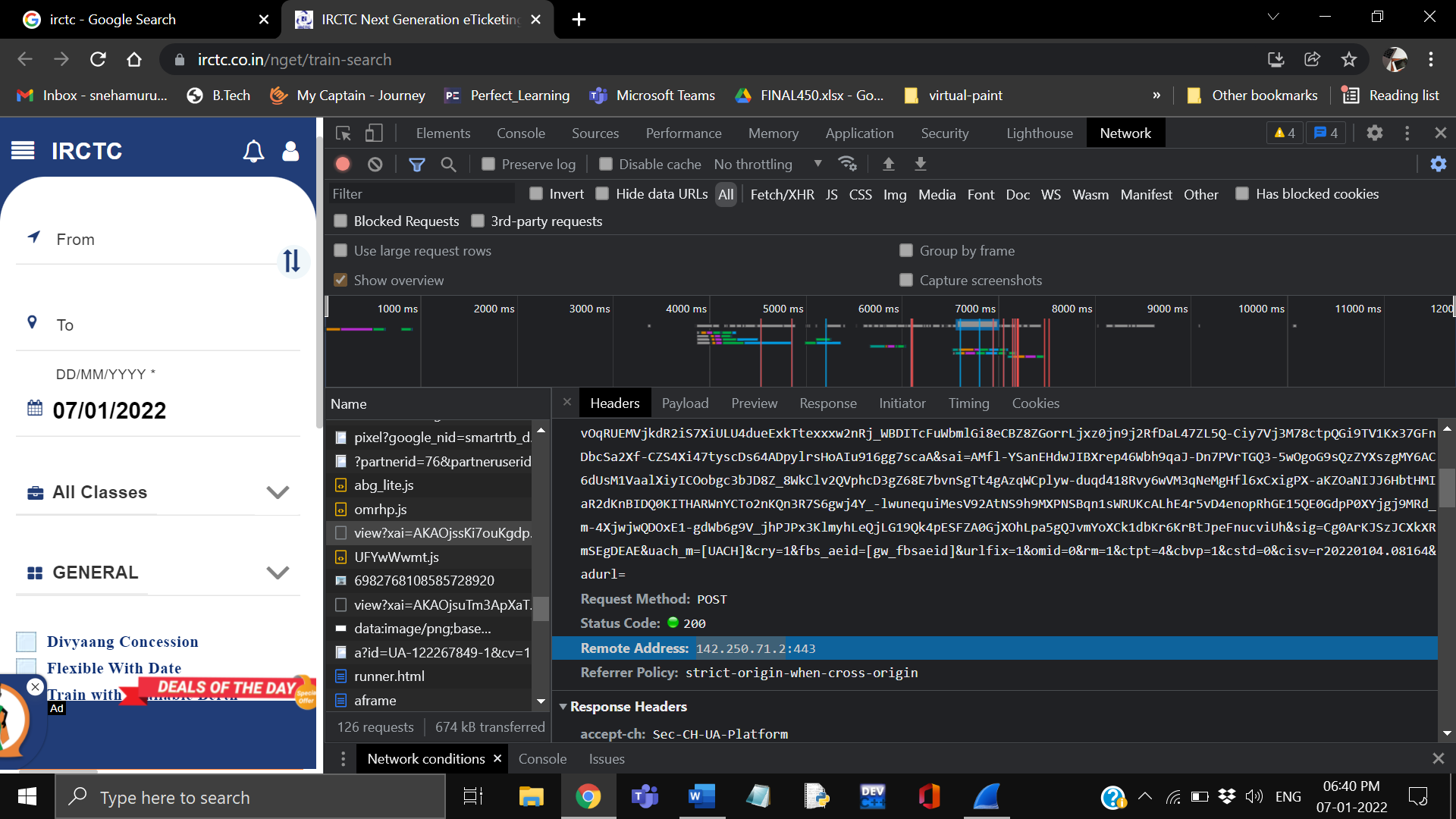




1. Website: <https://www.irctc.co.in/nget/train-search>









**RESULT**

Hence websites are monitored and respective network protocol is identified using Wireshark