**Experiment 6**

Rebecca Dias TECMPNA Pid:182027 19

**Aim:** Study of packet sniffer tools : wireshark

1. Download and install wireshark and capture icmp, tcp, and http packets in promiscuous mode

2. Explore how the packets can be traced based on different filters

**Theory:**

**a. What is Wireshark?**

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.

**b. Purpose of such softwares, which type of attack can it launch?**

Wireshark is a packet sniffer and analysis tool. It captures network traffic on the local network and stores that data for offline analysis. Wireshark captures network traffic from Ethernet, Bluetooth, Wireless Token Ring, Frame Relay connections, and more.Wireshark allows you to filter the log either before the capture starts or during analysis, so you can narrow down and zero into what you are looking for in the network trace. For example, you can set a filter to see TCP traffic between two IP addresses.

You can set it only to show you the packets sent from one computer. The filters in Wireshark are one of the primary reasons it became the standard tool for packet analysis.

Wireshark can launch various types of attacks few of them are ARP Spoof, DHCP Flooding, DNS Spoof, DDoS Attacks, VLAN Hopping, etc.Wireshark is used as the main support tool to help detect, or to a greater extent, analyse the problems generated by these attacks

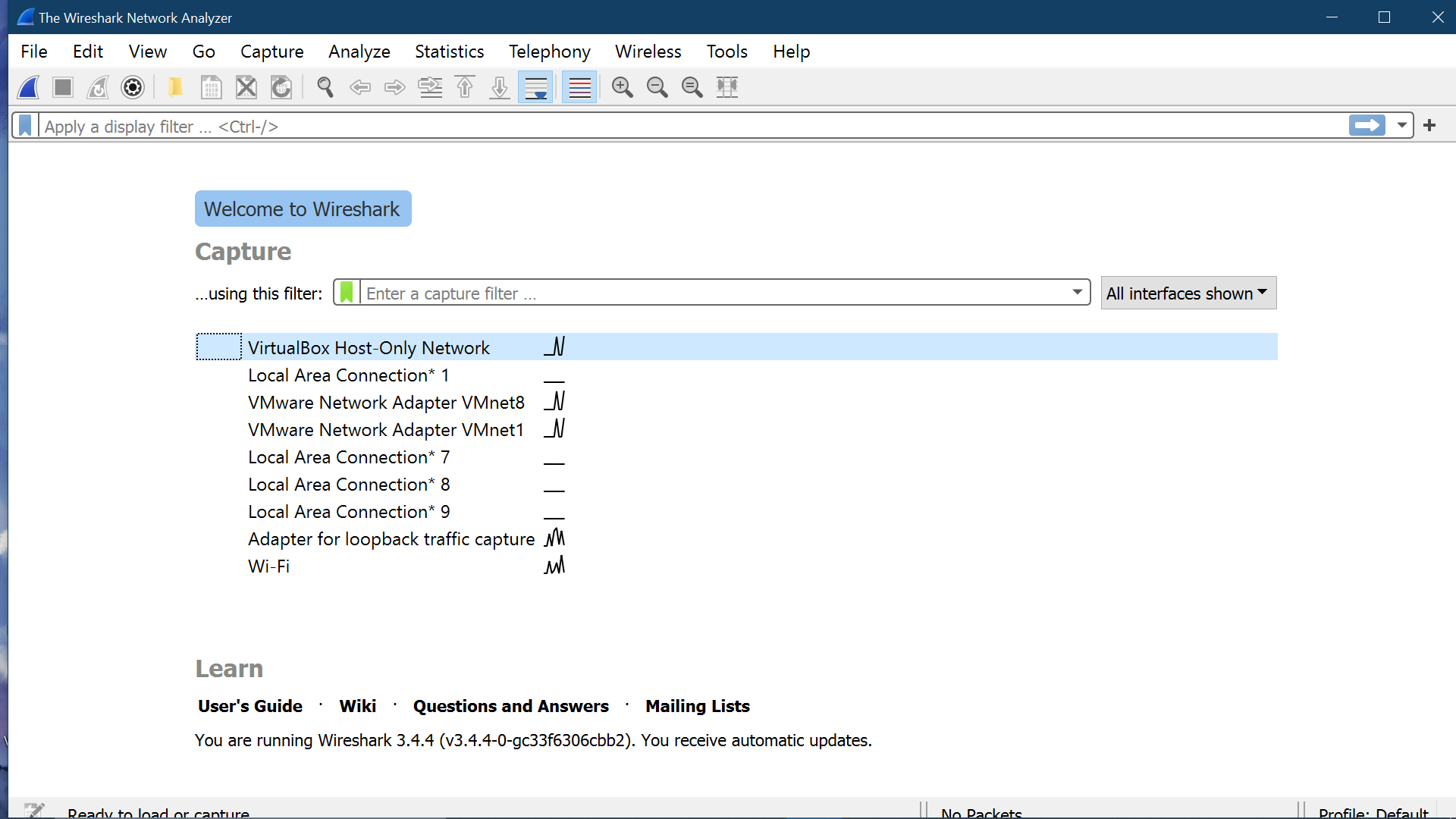
**c. Explain the features of Wireshark that you have studied.**

The following are some of the many features Wireshark provides:

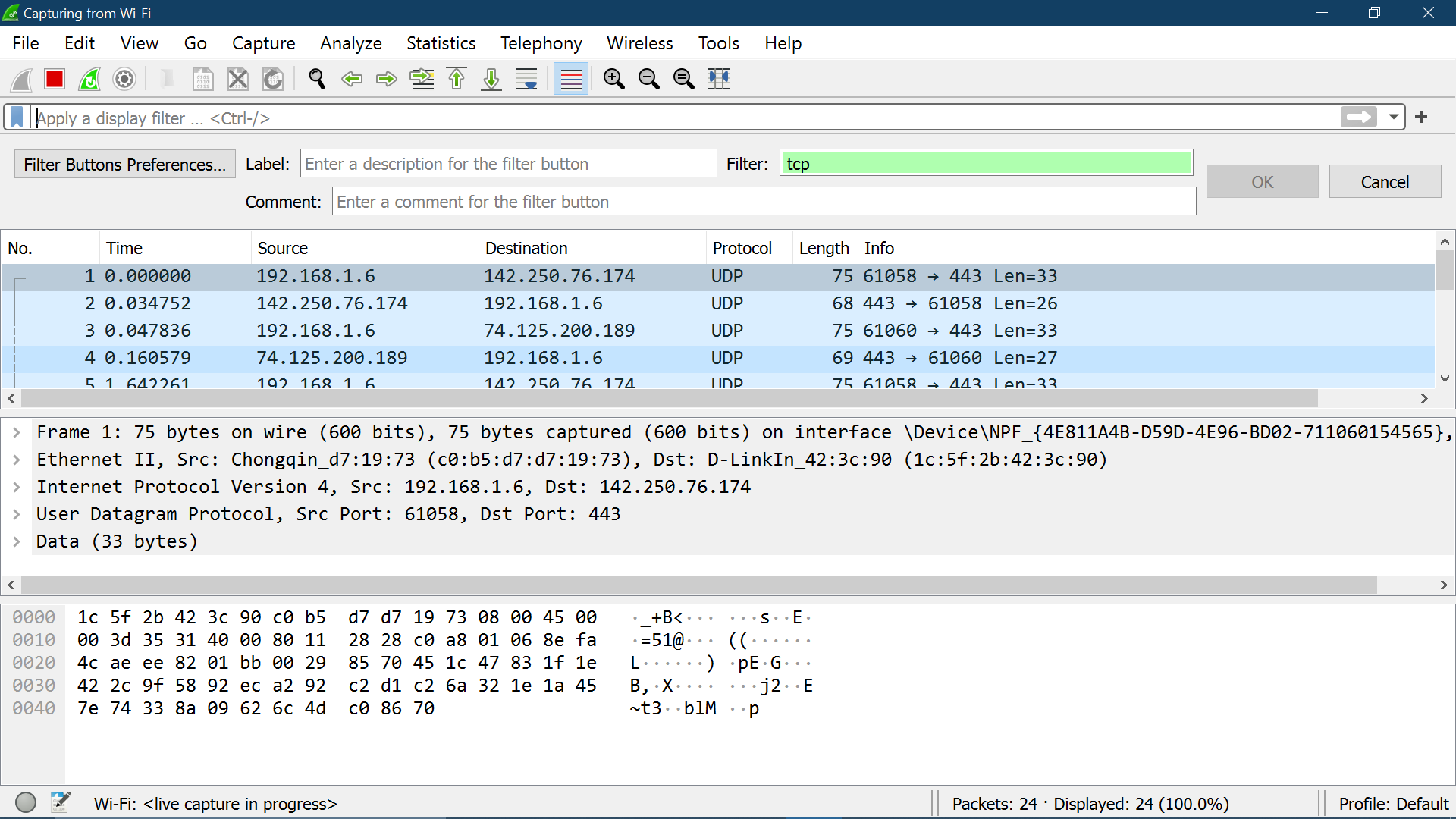
* Available for UNIX and Windows.
* Capture live packet data from a network interface.
* Open files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
* Import packets from text files containing hex dumps of packet data.
* Display packets with very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

**Implementation of Wireshark:**

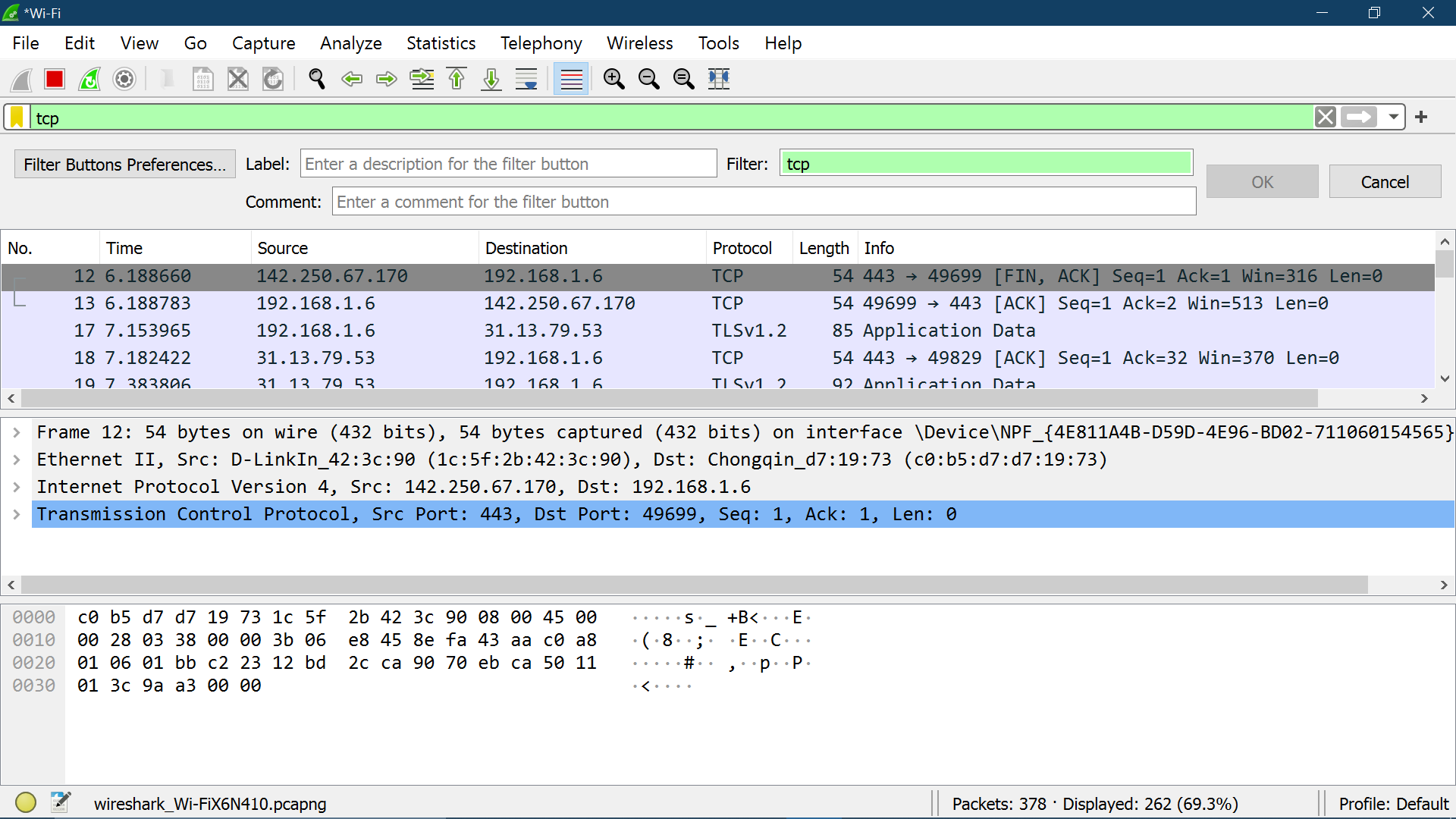
**a) Install Wireshark tool on the system.**



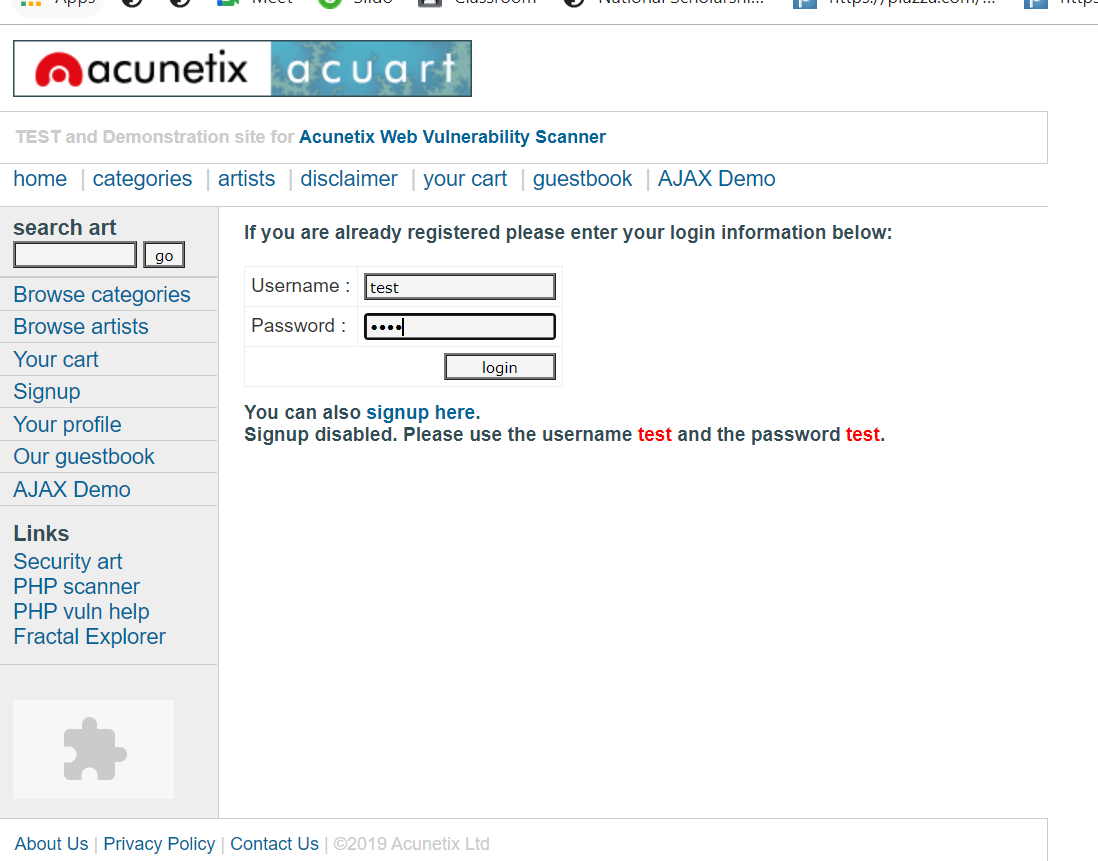
**b) Learn how to capture all the packets flowing through the network.**



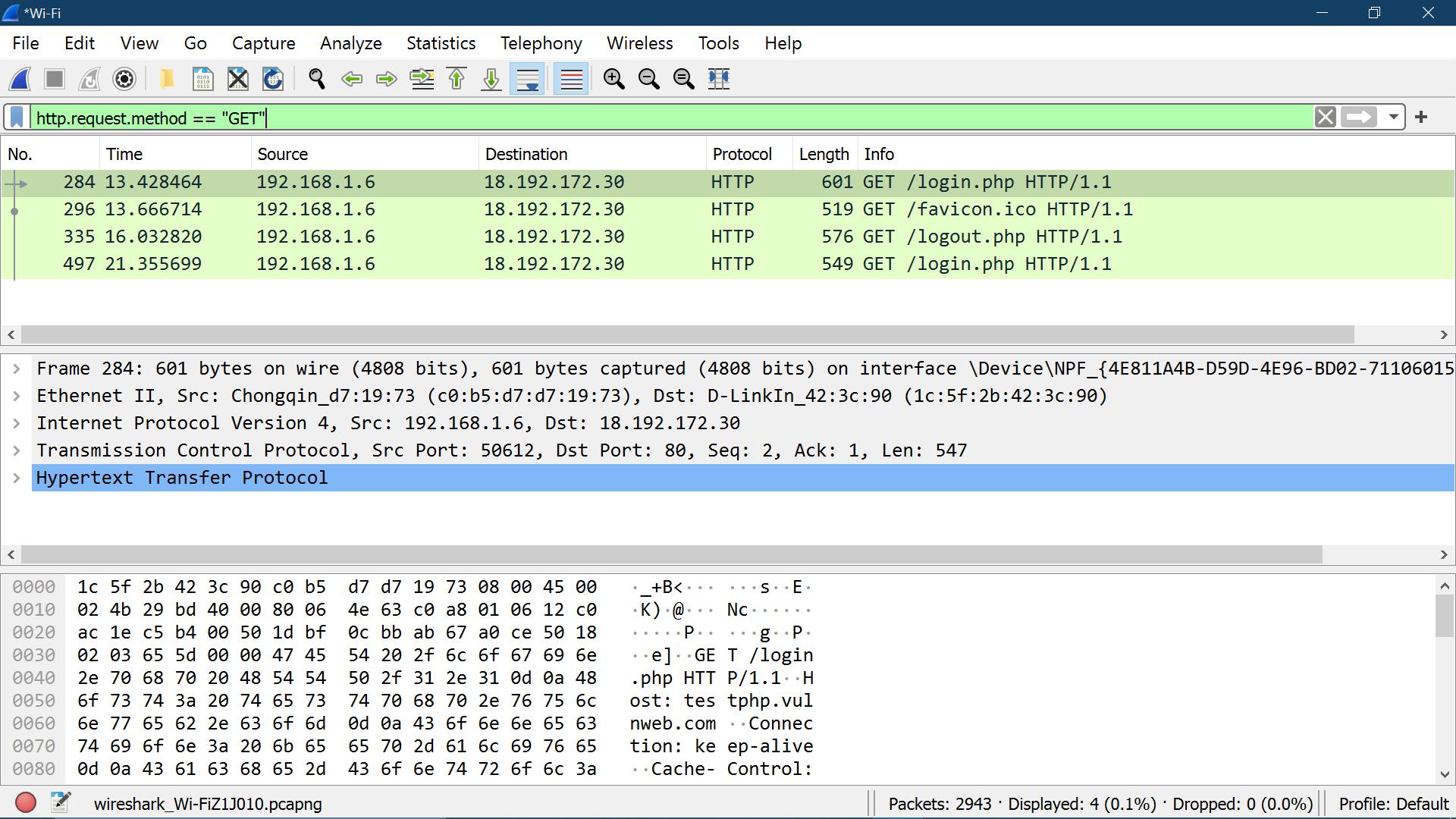
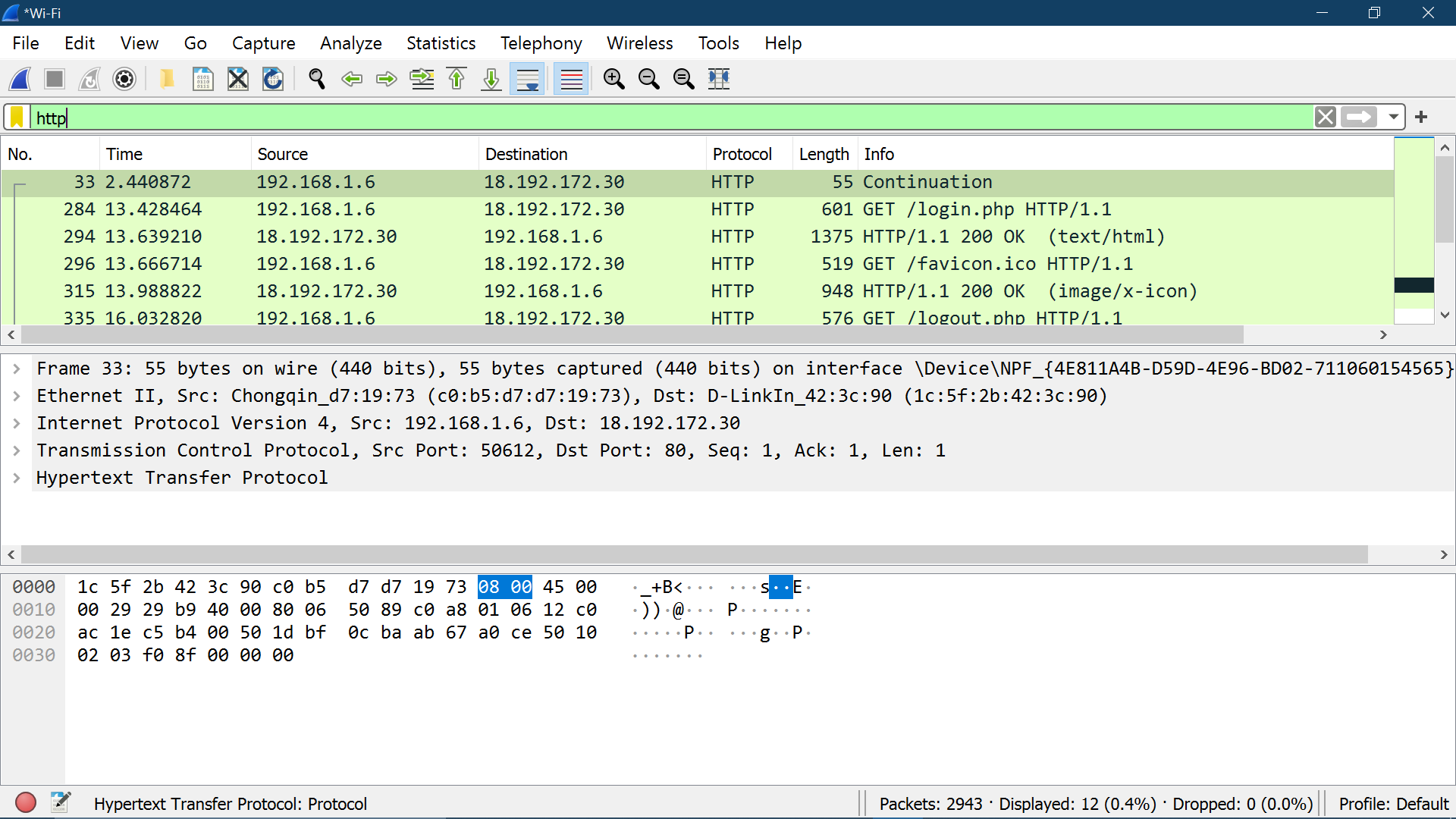
**c) Filter TCP packets.**

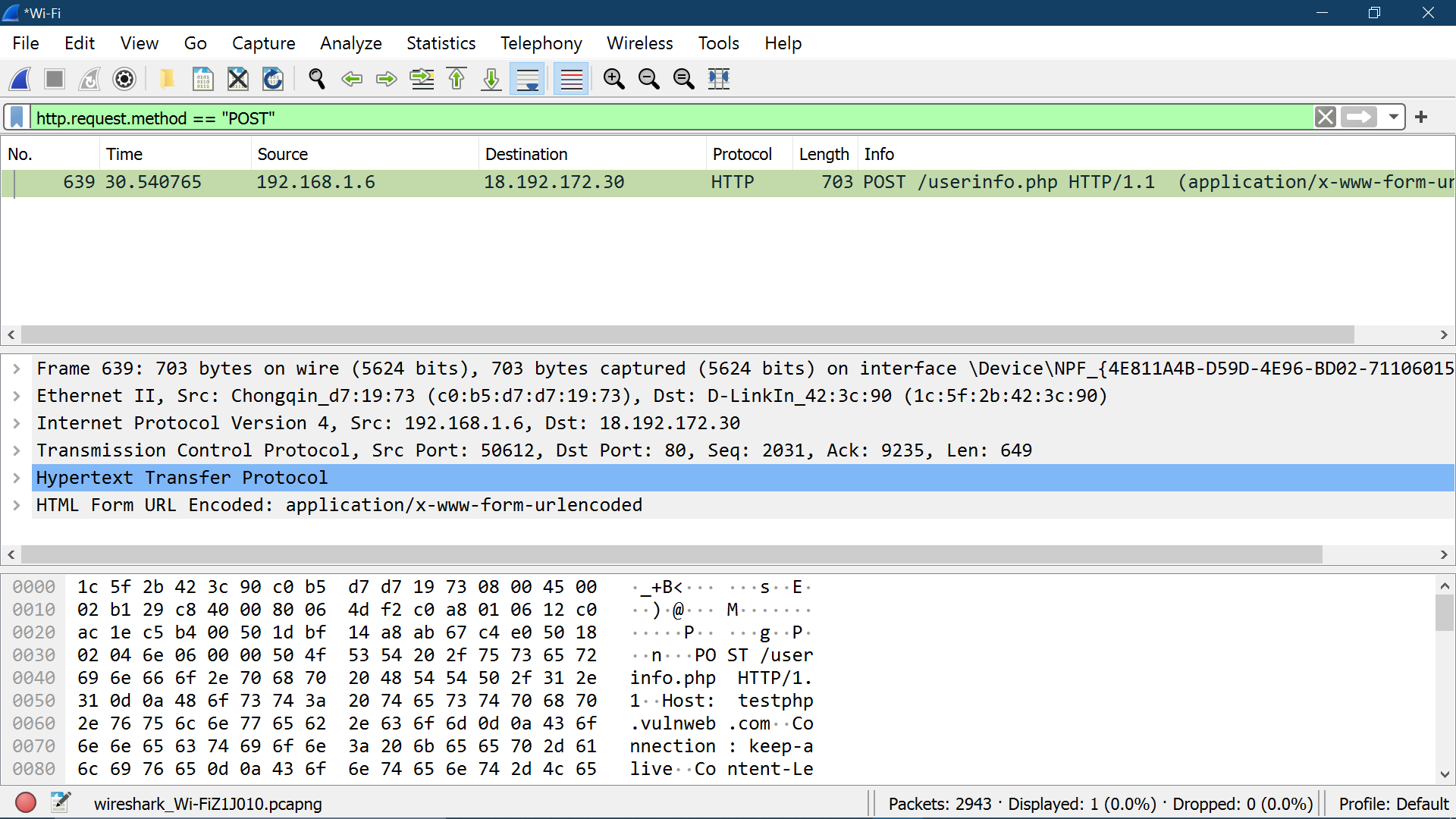


**d) Open a site and give username and password.**

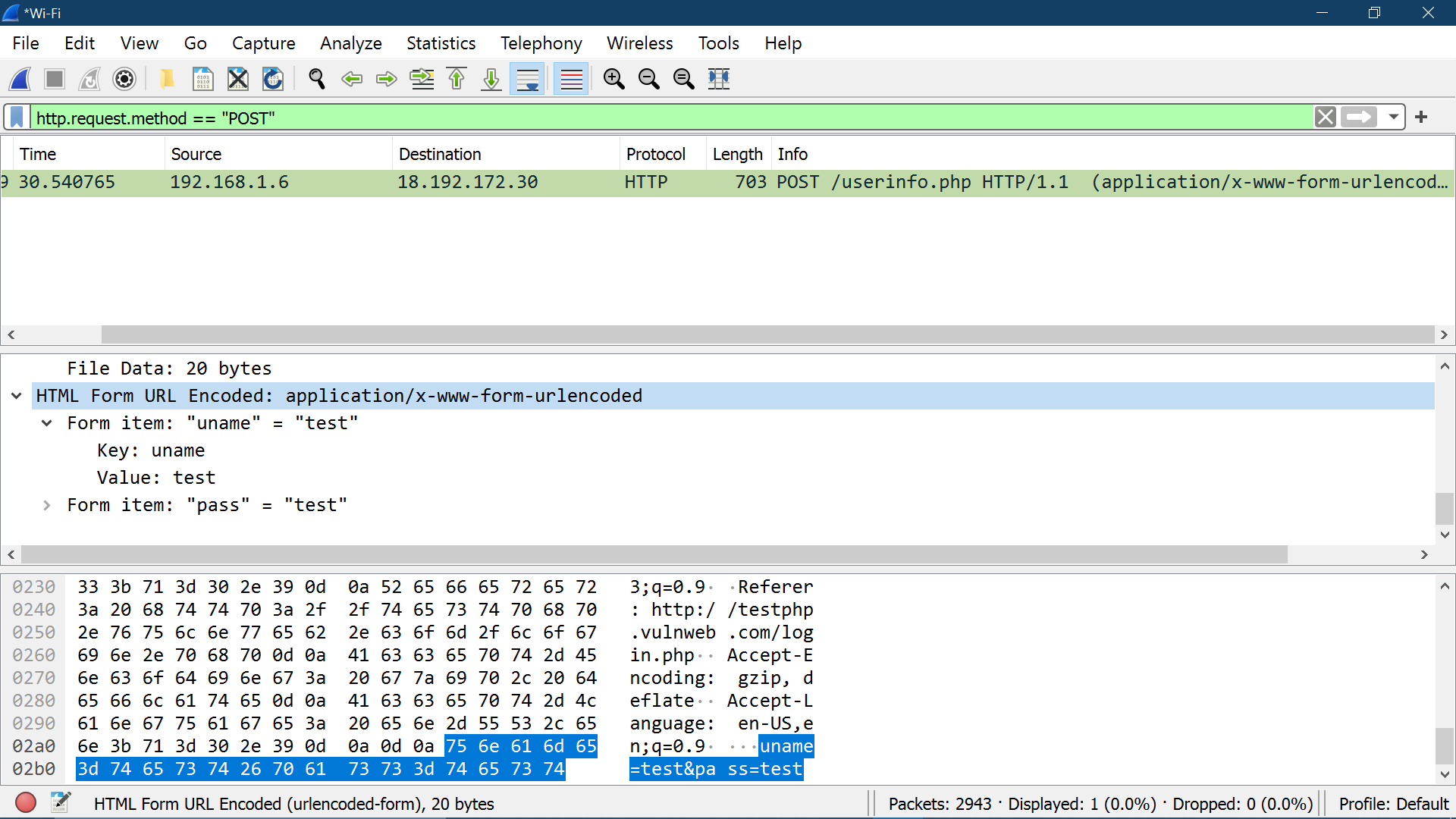


**e) Try to capture the username and password through Wireshark tool.**



****

**f) Capture TCP stream data revealing login credentials.**



**Conclusion:**

In this experiment we learnt about Wireshark that is a Packet Sniffing and Analyzer tool. We learnt about the interface of Wireshark and its features. After that, we tried to use Wireshark to hack the username and password from unsecure site. This is done by monitoring the packets of the website and then capturing that packet to know the Username and Password.For this process we used unsecure website i.e <http://testphp.vulnweb.com/>