**Aim:** To study the Packet Sniffer Tool-Wireshark Tool.

**Software Requirements:**

* Internet Connection
* Wireshark Program

**Theory:**

* 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.

* Features of Wireshark

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.

**Snapshots:**

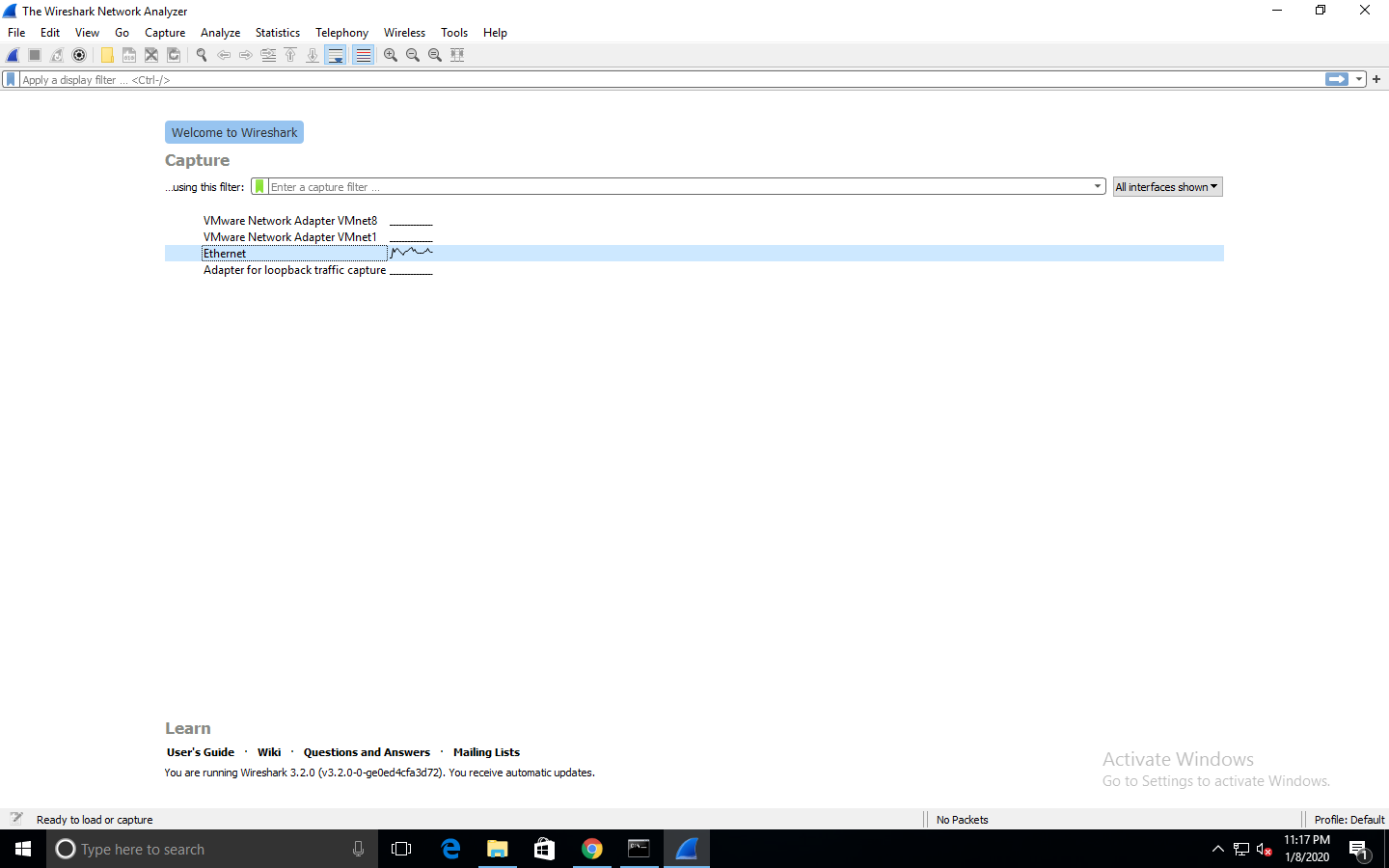


FIG 1: Start Window of Wireshark tool with Ethernet Interafce seelected.

The Wireshark software window is shown above in figure 1, and all the processes on the network are carried within this screen only. All the options given on the list are the Interface list options. The number of interface options will be present. Selection of any option will determine all the traffic. **For example,** from the above fig. select the Ethernet option. After this, a new window opens up, which will show all the current traffic on the network.

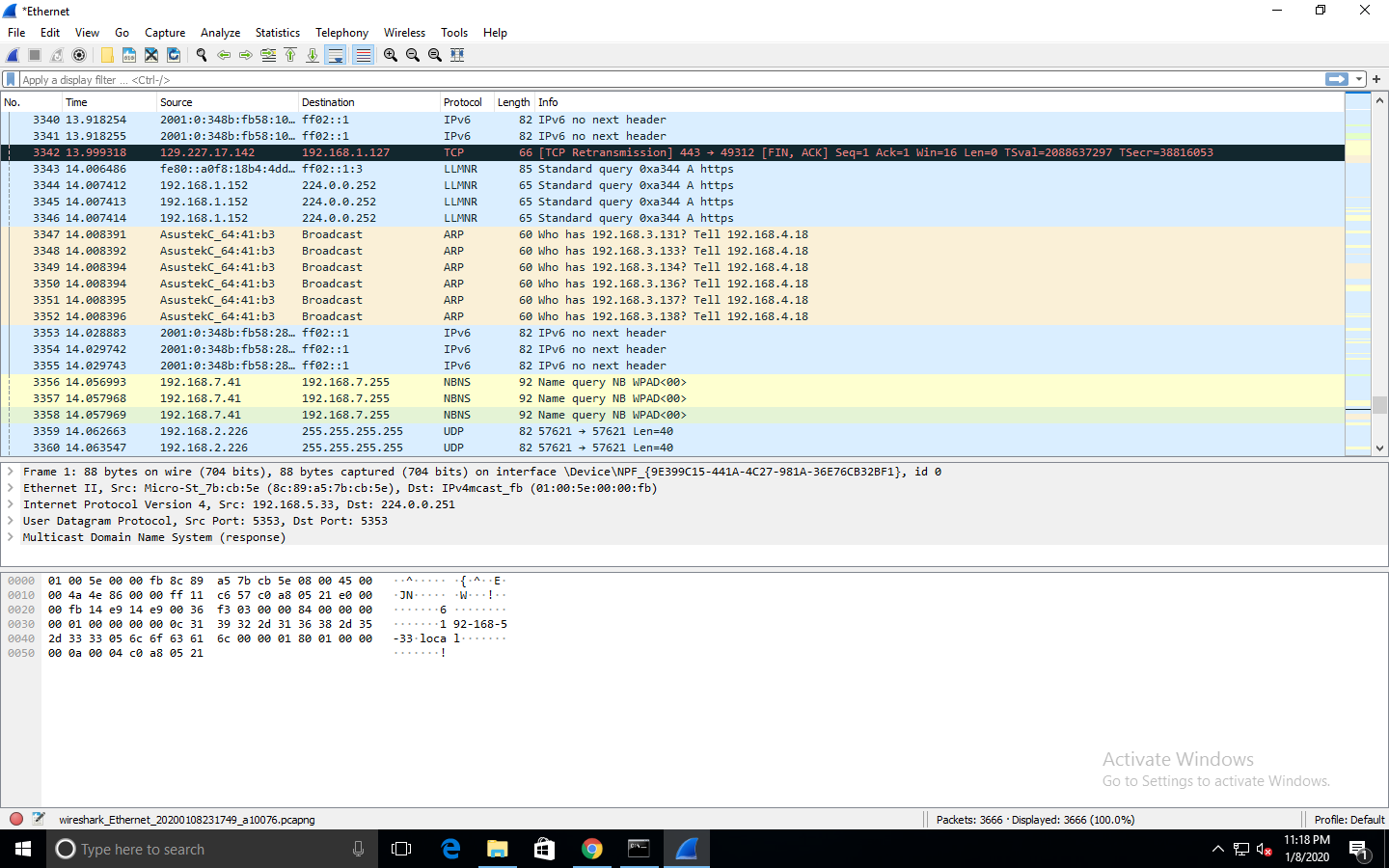


FIG 2: Wireshark’s main window consisting of three panes.

In the figure 2, we can see Wireshark’s main window with three panes: Packet list pane, Packet header-details pane and Packet bytes/contents pane. The packet list pane a summary of each packet captured. By clicking on packets in this pane you control what is displayed in the other two panes. The packet header-details pane displays the packet selected in the packet list pane in more detail. The packet bytes/contents pane displays the data from the packet selected in the packet list pane, and highlights the field selected in the packet details pane in ASCII and hexadecimal format.

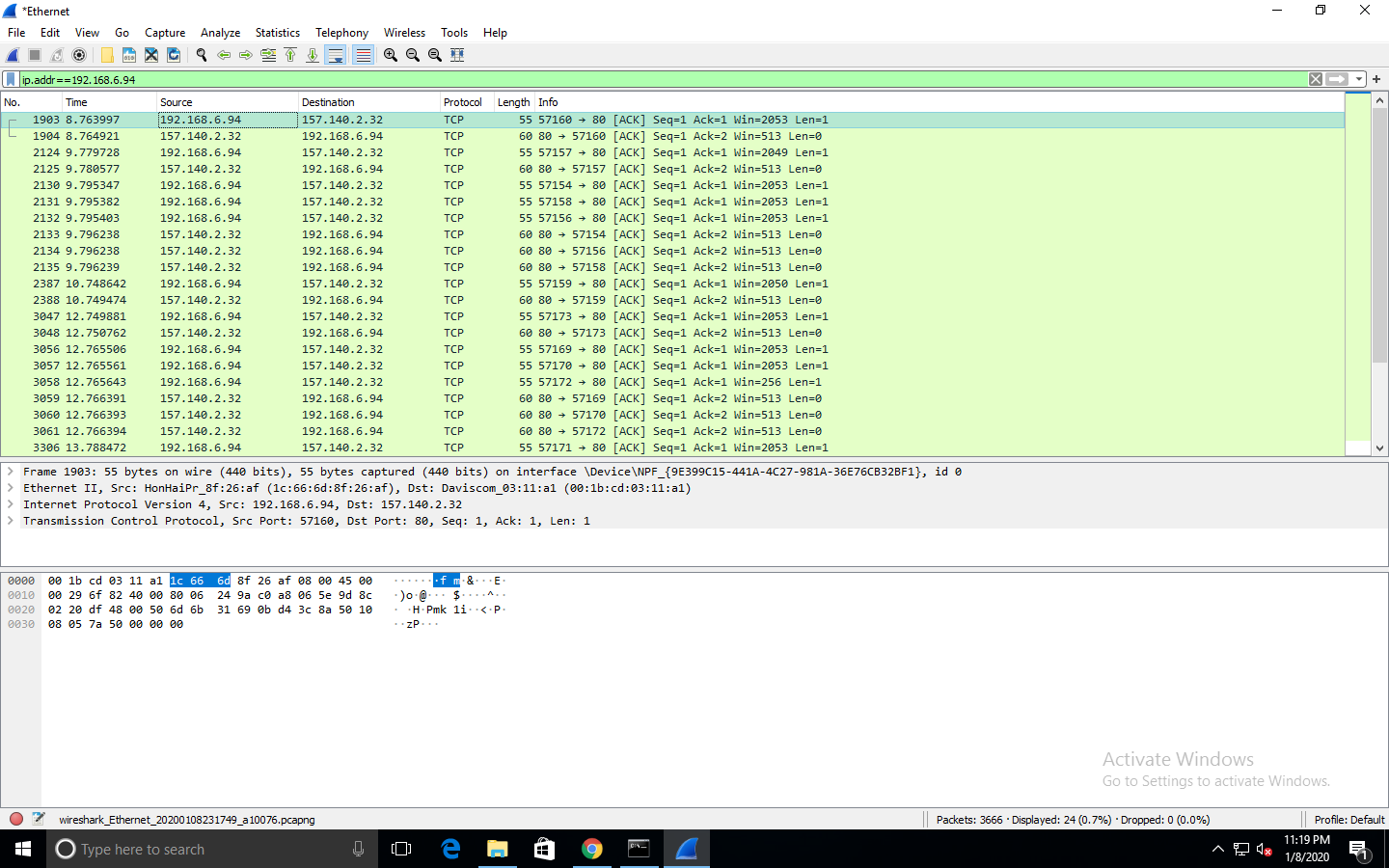


FIG 3: Applying display filter i.e. ip addr = = <ip address>

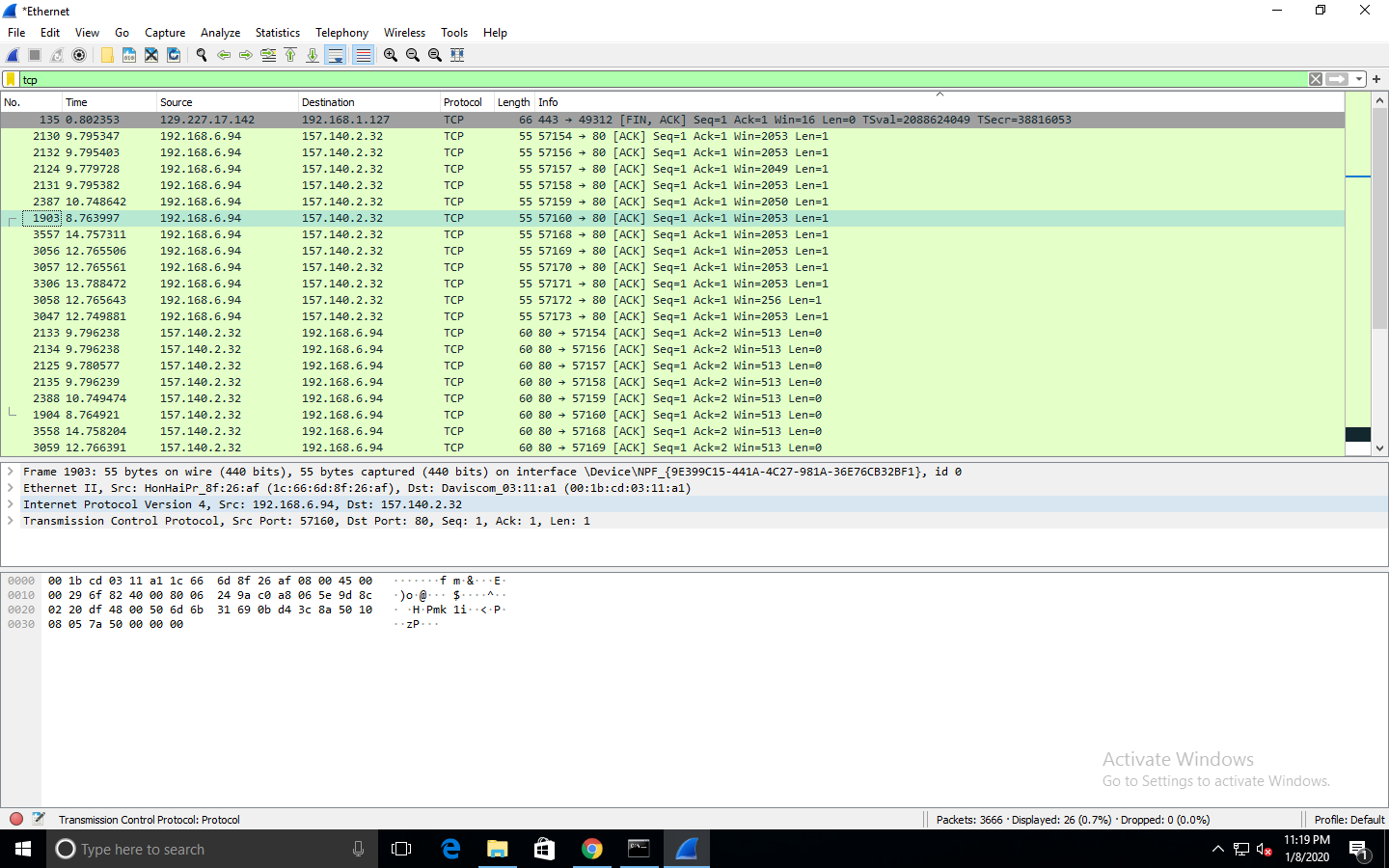


FIG 4: Applying display filter i.e. TCP.

The filter toolbar allows users to set display filters to filter which packets are displayed. For example, if we apply a filter for HTTP, only the interfaces with the HTTP will be listed. In the figure 3, we filtered the packet list using ip addr = = 192.168.6.94. All the packets with source ip address as mentioned are displayed. In the figure 4, we filtered the packet list using TCP and all the TCP packets were displayed.

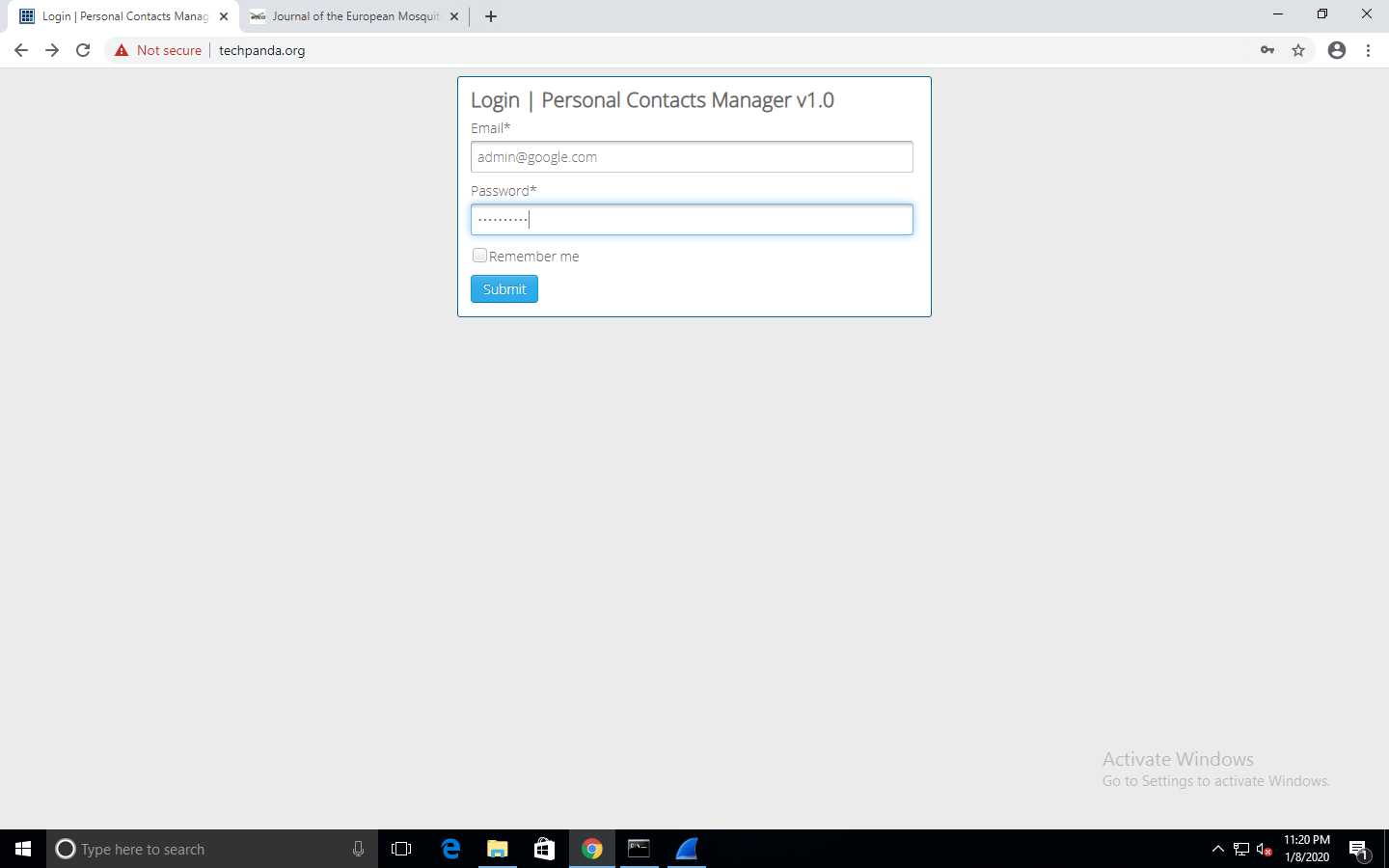


FIG 5: Logging in through Techpanda.org for hacking username and password.

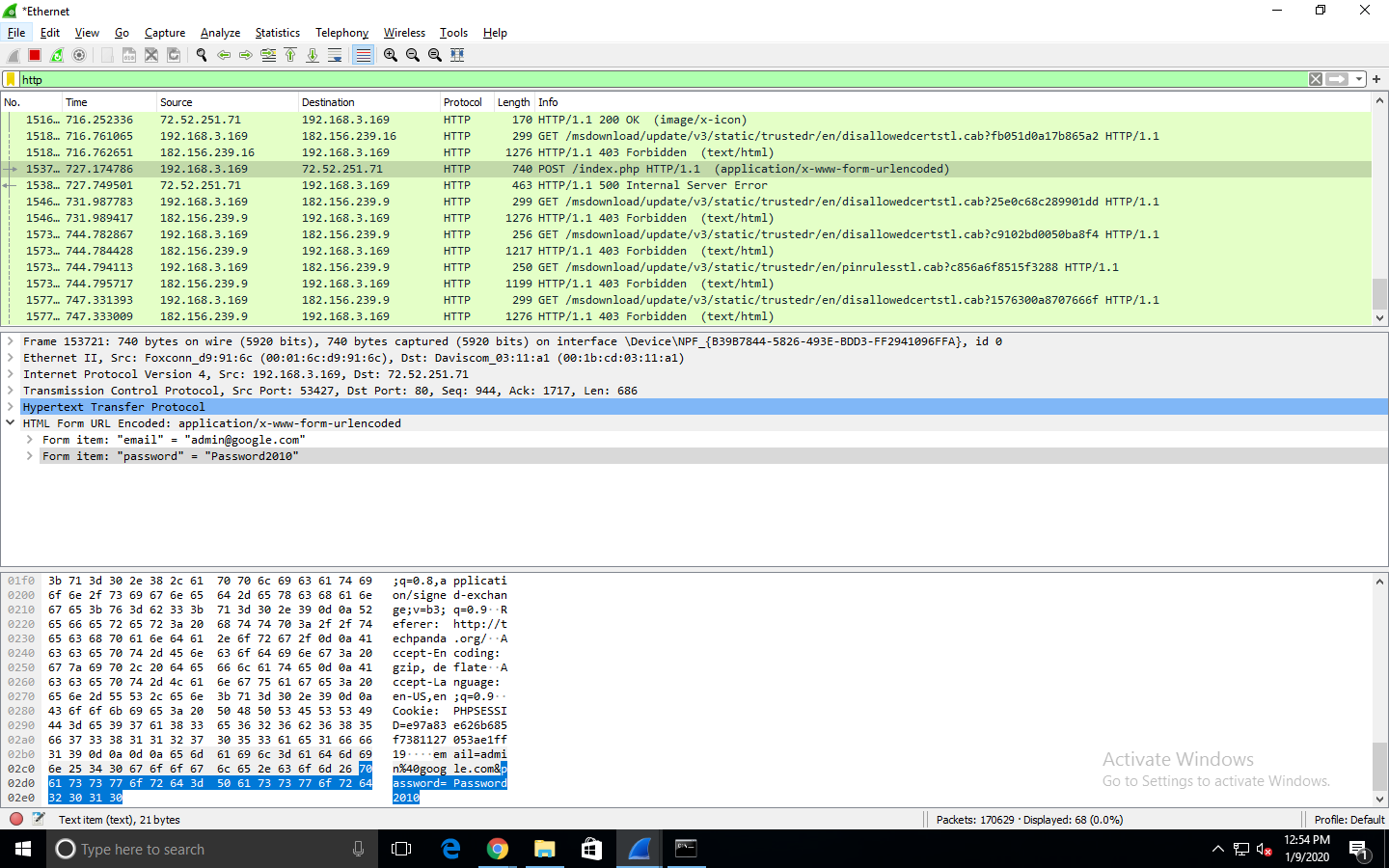


FIG 6: Username and Password Hacked after clicking on the captured packet.

In the figure 5, we login through the techpanda.org website as it is a not an encrypted website. Before clicking on the submit we click on start capturing the packets and as soon as the username and password are submitted, we stop capturing the packets. In the figure 6, we check the information bar and look for POST related information of the packet. We click it and the username and the password is obtained. Hence, the username and password submitted while performing login on the same PC or any other PC can be hacked.

**Conclusion:**

From 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 called Techpanda.org