Using Wireshark Tool to sniff the user's data

Wireshark is a network protocol analyzer, or an application that captures packets from a network connection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. **Wireshark** is the most often-used packet sniffer in the world.

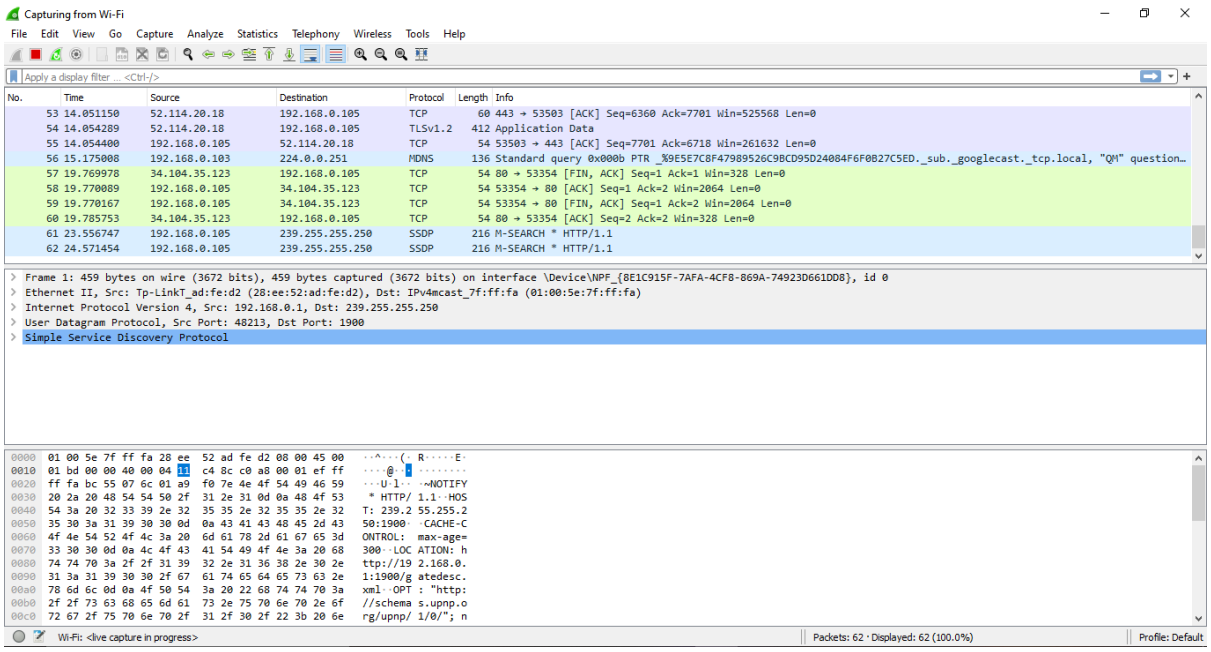
A hacker can use wireshark tool by getting into the same network as that of the victim's network by using a brute-force attack in order to get the password of wi-fi when the hacker has captured the packets of the network.

Being in the same network as the victim makes it easier for the hacker to get the victim's data. Hypertext Transfer Protocol (HTTP) runs on port 80/tcp and since it is a plain text protocol, it offers very little to no privacy to the communicating parties. Anybody who is in position to eavesdrop on the communication can capture everything over this channel, including passwords.

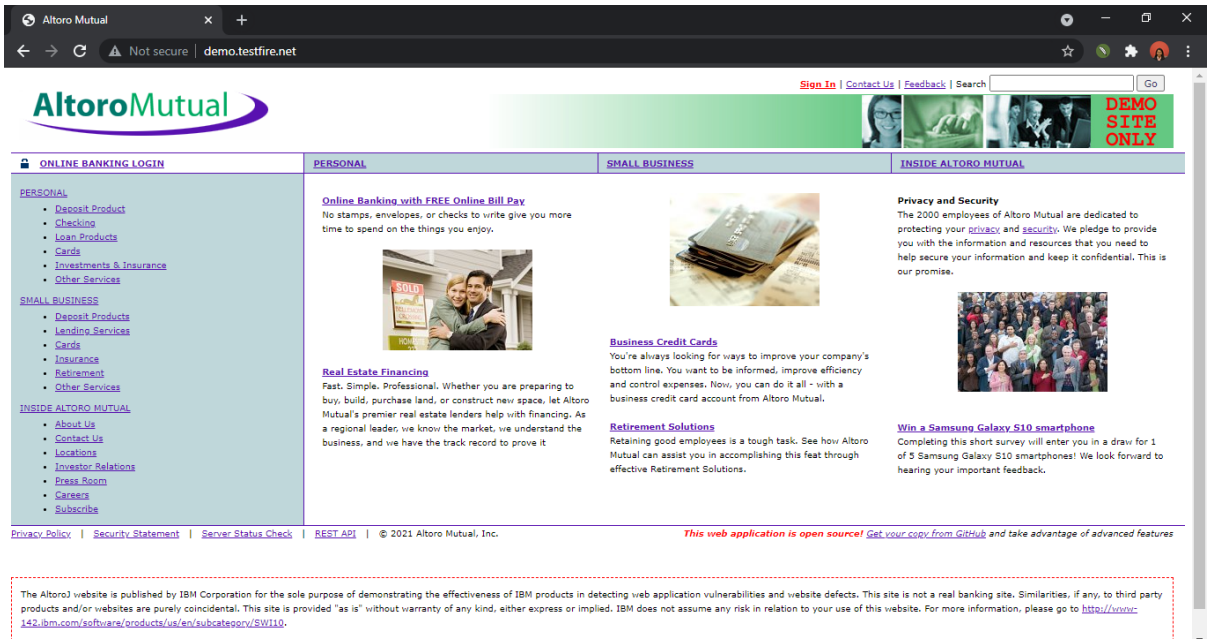
Even though there has been a tremendous effort done by all major browser vendors to discourage usage of HTTP as much as possible, we can still see HTTP being used on internal networks during penetration tests. By using Wireshark we can also easily extract files such as images, documents and audio files from the network traffic.

That is why is one must avoid connecting to free or public wireless connection. As it makes the device vulnerable to any of these attacks.

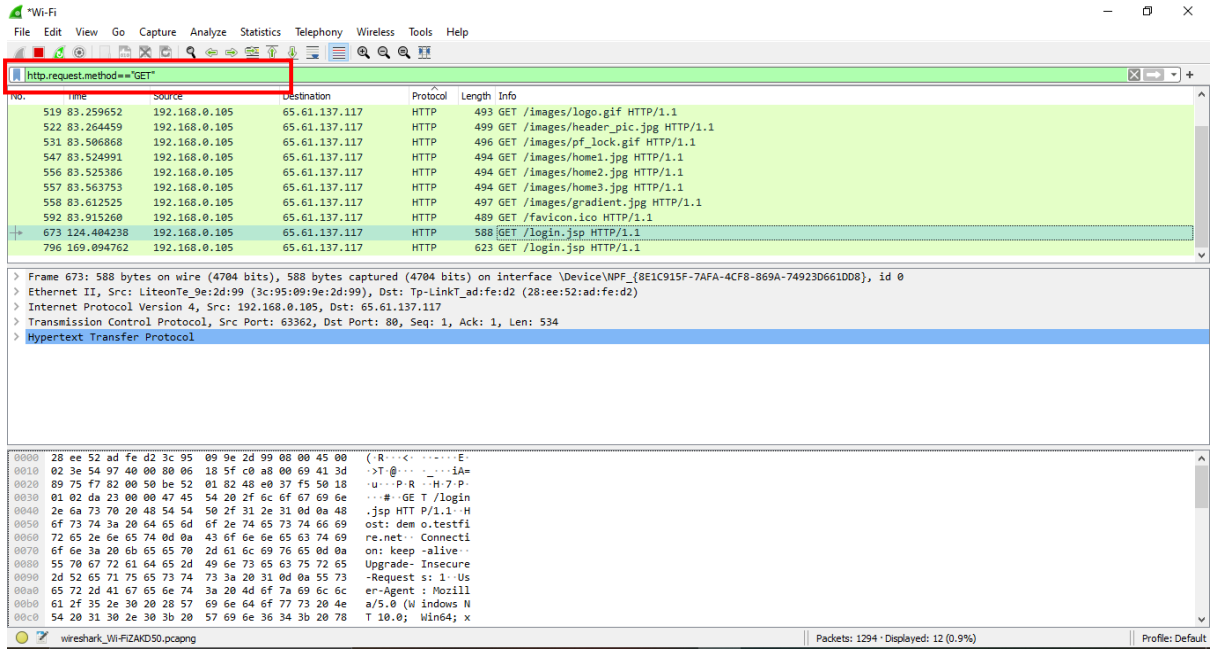
1.Opening wireshark tool and capturing data from the Wi-fi.



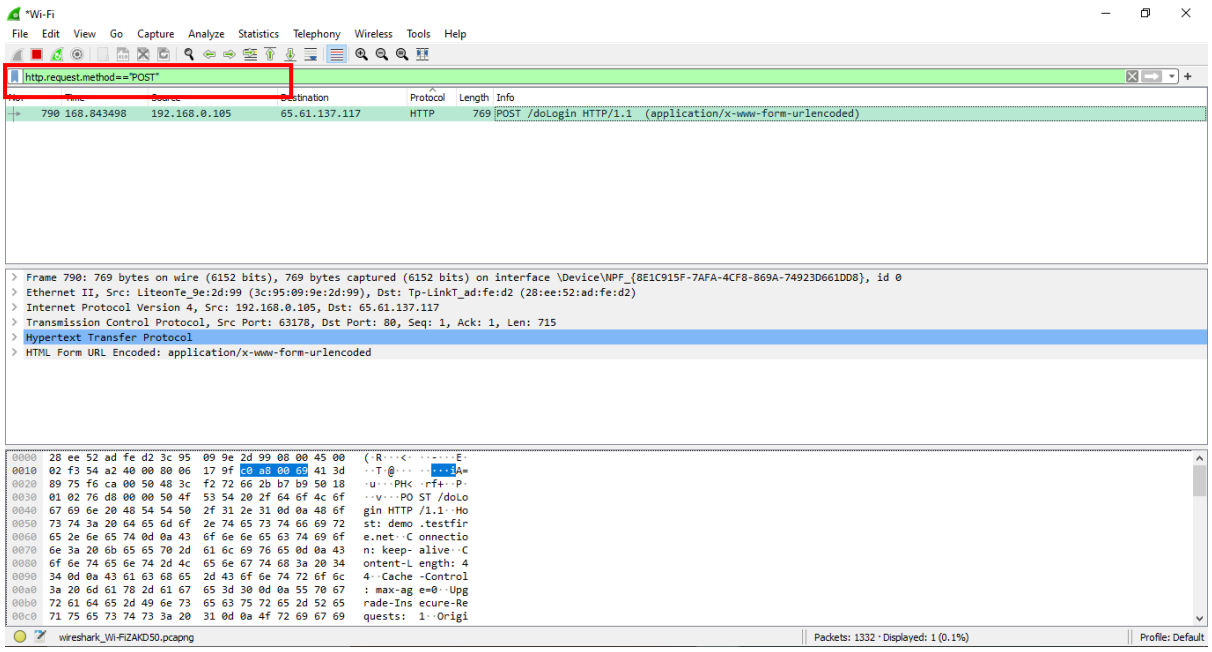
2.Suppose the victim is using his credentials to login to a website. We can capture that. Here we are testing it on http://demo.testfire.net/



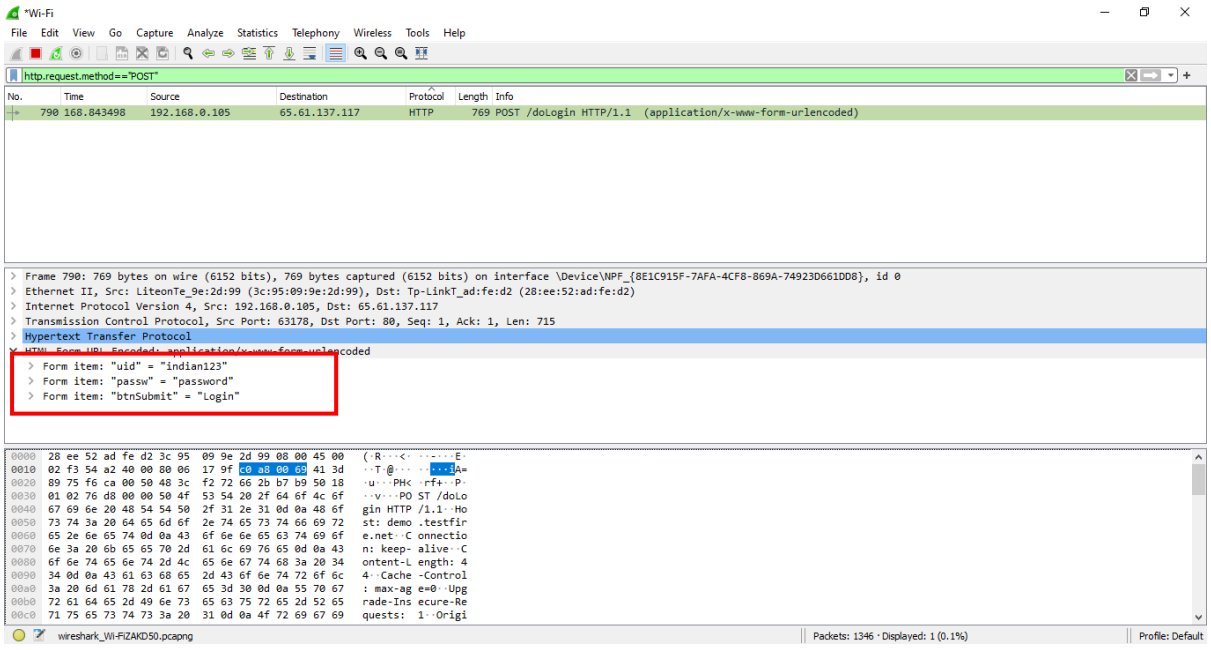
3.Checking for form submissions by using http.request.method==”GET”



4. Checking for values by using http.request.method==”POST”



5.We have successfully acquired the login name and password by packet sniffing and analysing.



In conclusion, here I have used the Wireshark tool and found out the victim’s user name and password on the demo website by capturing the data from the Wi-Fi.