

# 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.

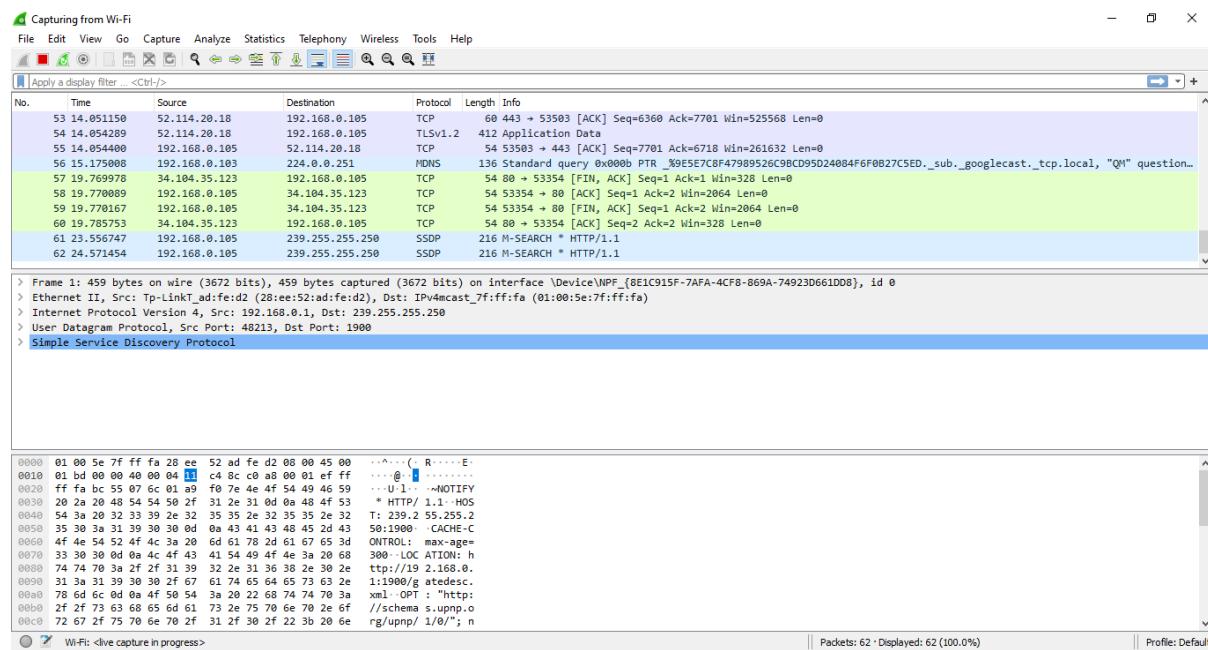
A hacker can use wireshark tool by getting into the same network as that of the victim's network by using a brute-force attack in order to get the password of wi-fi when the hacker has captured the packets of the network.

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 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/>

The Altoro website is published by IBM Corporation for the sole purpose of demonstrating the effectiveness of IBM products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. IBM does not assume any risk in relation to your use of this website. For more information, please go to <http://www.142.ibm.com/software/us/en/subcategory/SW10>.

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

```

Frame 673: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface \Device\NPF_{8E1C915F-7AFA-4CF8-869A-7492D661DD08}, id 0
> Ethernet II, Src: LiteonTe_9e:2d:99 (0c:95:09:9e:2d:99), Dst: Tp-LinkT_dfe:d2 (28:ee:52:ad:fe:d2)
> Internet Protocol Version 4, Src: 192.168.0.105, Dst: 65.61.137.117
> Transmission Control Protocol, Src Port: 63362, Dst Port: 80, Seq: 1, Ack: 1, Len: 534
> Hypertext Transfer Protocol

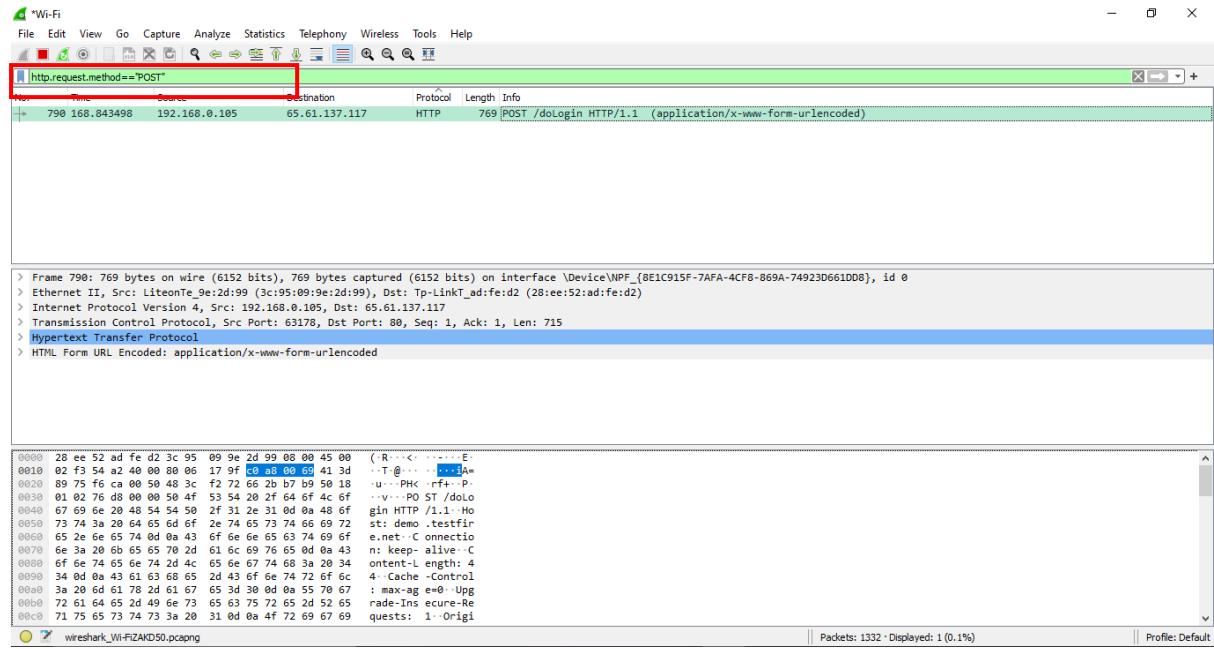
```

```

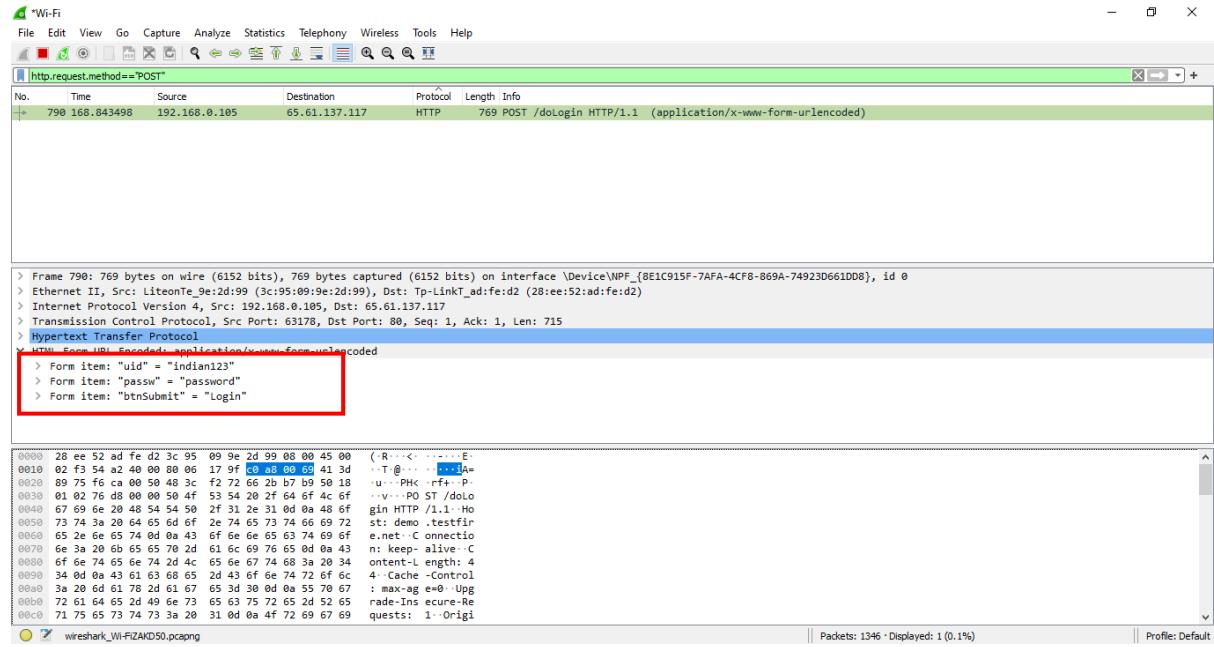
0000  28 ee 52 ad fe d2 3c 95 09 08 00 45 00  ( R-< -----E
0010  02 3e 52 97 40 00 00 06 18 5f c0 a8 00 69 41 3d  -> @... _-ia=
0020  89 75 f7 82 00 50 be 52 01 82 48 e0 37 f5 50 18  -u -P R -H 7 P
0030  01 02 d2 23 00 00 47 45 54 20 2f 6c 6f 67 69 6e  -> # -GE T /login
0040  2e 6a 73 70 20 40 54 50 2f 31 2e 31 00 48 48 48  .jpg HTTP/1.1 -H
0050  6f 73 70 20 40 54 50 2f 31 2e 31 00 48 48 48 48  .jpg HTTP/1.1 -H
0060  72 64 2e 6a 65 68 00 43 6f 6e 66 65 63 74 69 69  on:keepalive
0070  6f 6e 3a 20 6b 65 69 70 43 6f 6e 66 65 63 74 69  on:keepalive
0080  55 70 67 72 61 64 65 2d 49 6e 73 66 62 75 72 65  Upgrade: Insecure
0090  2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73  -Request s: 1; Us
00a0  65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c  er-Agent: Mozilla
00b0  61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e  a/5.0 (Windows N
00c0  54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 78  T 10.0; Win64; x

```

#### 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.