

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.

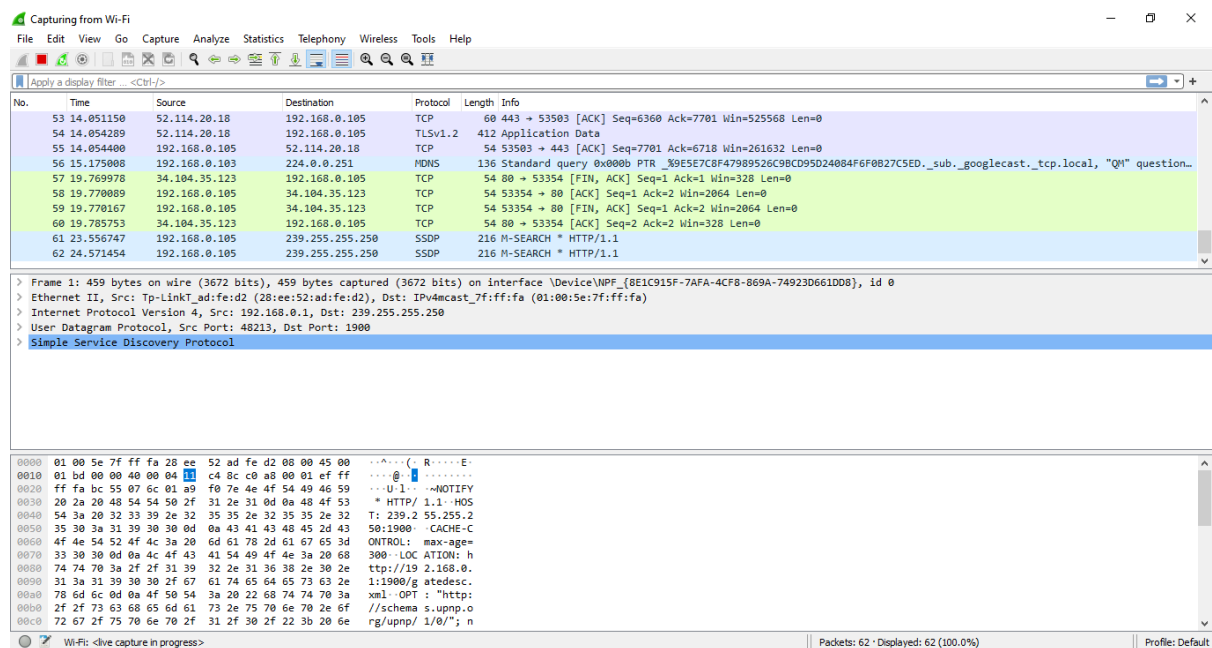
A hacker can use wireshark tool by getting into the same network as that of the victim's network by using a brute-force attack in order to get the password of wi-fi when the hacker has captured the packets of the network.

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/>

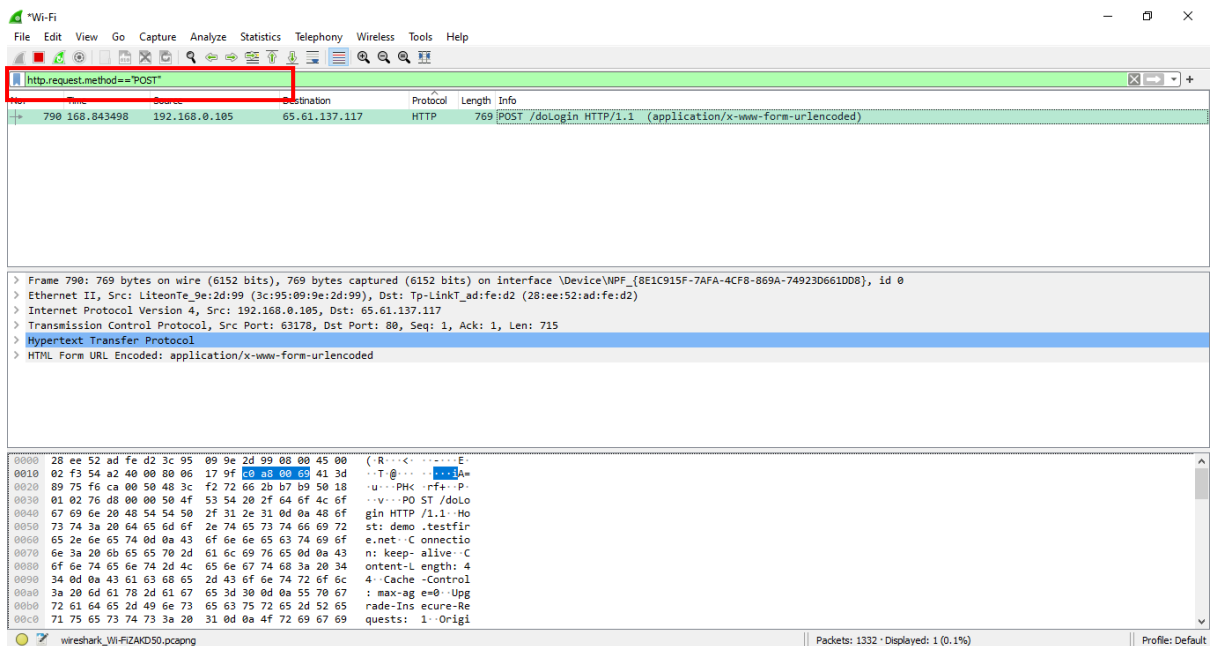
3. Checking for form submissions by using `http.request.method=="GET"`

No.	Time	Source	Destination	Protocol	Length	Info
519	83.259652	192.168.0.105	65.61.137.117	HTTP	493	GET /images/logo.gif HTTP/1.1
522	83.264459	192.168.0.105	65.61.137.117	HTTP	499	GET /images/header_pic.jpg HTTP/1.1
531	83.506868	192.168.0.105	65.61.137.117	HTTP	496	GET /images/pf_lock.gif HTTP/1.1
547	83.524991	192.168.0.105	65.61.137.117	HTTP	494	GET /images/home1.jpg HTTP/1.1
556	83.525386	192.168.0.105	65.61.137.117	HTTP	494	GET /images/home2.jpg HTTP/1.1
557	83.563753	192.168.0.105	65.61.137.117	HTTP	494	GET /images/home3.jpg HTTP/1.1
558	83.612525	192.168.0.105	65.61.137.117	HTTP	497	GET /images/gradient.jpg HTTP/1.1
592	83.915260	192.168.0.105	65.61.137.117	HTTP	489	GET /favicon.ico HTTP/1.1
673	124.404238	192.168.0.105	65.61.137.117	HTTP	588	GET /login.jsp HTTP/1.1
796	169.094762	192.168.0.105	65.61.137.117	HTTP	623	GET /login.jsp HTTP/1.1

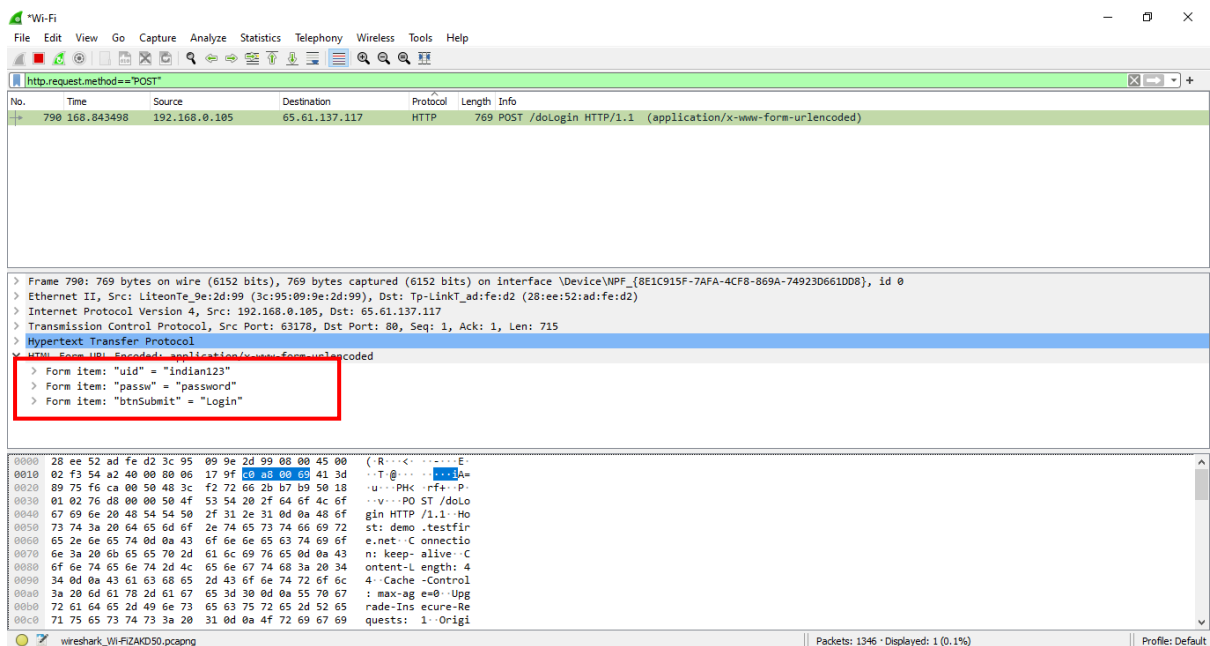
```
> Frame 673: 588 bytes on wire (4704 bits), 588 bytes captured (4704 bits) on interface \Device\NPF_{8E1C915F-7AFA-4CF8-869A-74923D661D08}, id 0
> Ethernet II, Src: LiteonTe_9e:2d:99 (3c:95:09:9e:2d:99), Dst: Tp-LinkT_ad:fe:d2 (28:ee:52:ad:fe:d2)
> Internet Protocol Version 4, Src: 192.168.0.105, 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 9e 2d 99 08 00 45 00  (R<...<...E-
0010 02 3e 54 97 48 00 00 06 18 5f c0 a8 00 69 41 3d  ->T.@...-IA=
0020 89 75 f7 82 00 50 be 52 01 82 48 e0 37 f5 50 18  -u...P.R...H?P
0030 01 02 da 23 00 00 47 45 54 20 2f 6c 6f 67 69 6e  -..#GE T /login
0040 2e 6a 73 70 20 48 54 50 2f 31 2e 31 0d 0a 48  -..jsp HTT P/1.1..H
0050 6f 73 74 3a 20 64 65 6d 6f 2e 74 65 73 74 66 69  -ost: dem o.testfi
0060 72 65 2e 6e 65 74 0d 0a 43 0f 6e 6e 65 63 74 69  -re.net... Connecti
0070 6f 6e 3a 20 6b 65 65 70 2d 01 6c 69 76 65 0d 0a  -on: keep-alive...
0080 55 70 67 72 61 64 65 2d 49 6e 73 65 63 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 6e  -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.