

# Forum:[Hack Forums](#)

Thread: [How to Use Wireshark to Steal Passwords](#)

**Pixel00** - September 12, 2019, 11:58 am

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level.

This tutorial can be an angel and also devil in the same time, it depends to you who use this tutorial for which purpose. Me as a writer of this tutorial just hope that all of you can use it in the right way ? , because I believe that no one from you want your password sniffed by someone out there so don't do that to others too ? ? ?

Requirements :

1. Wireshark Network Analyzer ([wireshark.org](https://www.wireshark.org))
2. Network Card (Wi-Fi Card, LAN Card, etc) fyi : for wi-fi it should support promiscuous mode

Step 1: Start Wireshark and capture traffic

In Kali Linux you can start Wireshark by going to

Application > Kali Linux > Top 10 Security Tools > Wireshark

In Wireshark go to Capture > Interface and tick the interface that applies to you.

Ideally you could just press Start button here and Wireshark will start capturing traffic. In case you missed this, you can always capture traffic by going back to Capture > Interface > Start

Step 2: Filter captured traffic for POST data

At this point Wireshark is listening to all network traffic and capturing them. I opened a browser and signed in a website using my username and password. When the authentication process was complete and I was logged in, I went back and stopped the capture in Wireshark.

When we typed in your username, password and press the Login button, it generates a a POST method (in short – you're sending data to the remote server).

To filter all traffic and locate POST data, type in the following in the filter section

```
http.request.method == "POST"
```

Step 3: Analyze POST data for username and password

Now right click on that line and select Follow TCP Stream.

There you go ? Hope this helped!

**XRVII I** - September 12, 2019, 2:20 pm

Got any software that can break into gmail accounts?

**Mike Echolas** - September 12, 2019, 10:18 pm

The principal thing you have to do is to catch the system parcels that contain the passwords (or other certification types, however suppose we're concentrating on passwords until further notice). Catching system bundles all in all is simple – you can do it on practically any PC where you have authoritative rights. "Typical" client rights aren't sufficient as a rule, since you have to empower Promiscuous Mode on the system card to have the option to catch bundles that are not intended to be gotten by your PC. This may sound muddled, however it fundamentally works this way:

1. Every one of the bundles on the system that really touch base at your PCs (or Mac) will be investigated to check on the off chance that they have a goal that matches the system card
2. in the event that the goal address is a match, the bundles are bound for your PC and will be left behind to the CPU and prepared
3. on the off chance that the goal address in the bundle doesn't coordinate the location of the system card the parcels will essentially be overlooked and disposed of

Investigate number 3 – this implies if your system card sees bundles that are sent from different PCs to different servers (without your PC being included by any means), your card won't even truly see them but to discover that it couldn't care less. So on the off chance that you need to get stuff that others are sending to one another, you have an issue.

Presently, in the event that you need to tell your system card "hello, acknowledge everything! Disregard the goal thing separating, I need everything!" you have to empower a unique mode on the system card. That mode is classified "Indiscriminate Mode", and Wireshark does it naturally of course

**tradingdude** - September 13, 2019, 10:24 am

thank you so much! very informative