PROJECT-6

**DEME SAIKIRAN**

**AZURE SKYNET**

WIRESHARK PACKET ANALYSING



**Contents :**

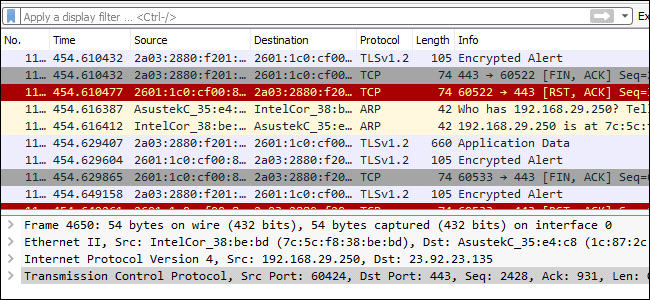
1. WIRE SHARK INTRO
2. Wire shark packet analyzing…..

# Introduction

## WIRESHARK TO CAPTURE , FILTER & INSPECTING THE PACKETS…

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets.

This tutorial will get you up to speed with the basics of capturing packets, filtering them, and inspecting them. You can use Wireshark to inspect a suspicious program’s network traffic, analyze the traffic flow on your network, or troubleshoot network problems



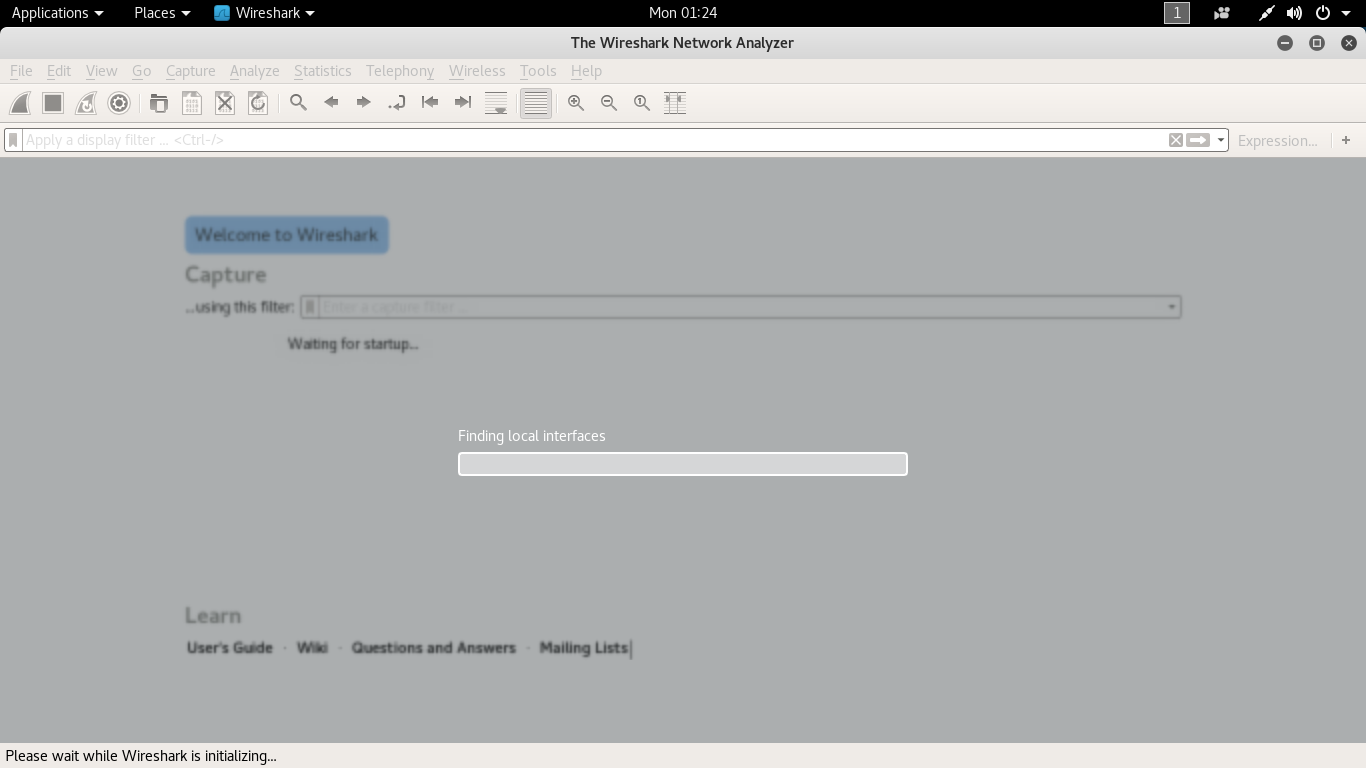
## **FEATURES OF WIRESHARK**

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

* Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
* Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
* Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
* Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
* Data display can be refined using a display filter.
* Plug-ins can be created for dissecting new protocols.
* VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
* Raw USB traffic can be captured.
* Wireless connections can also be filtered as long as they traverse the monitored Ethernet.[clarification needed]
* Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

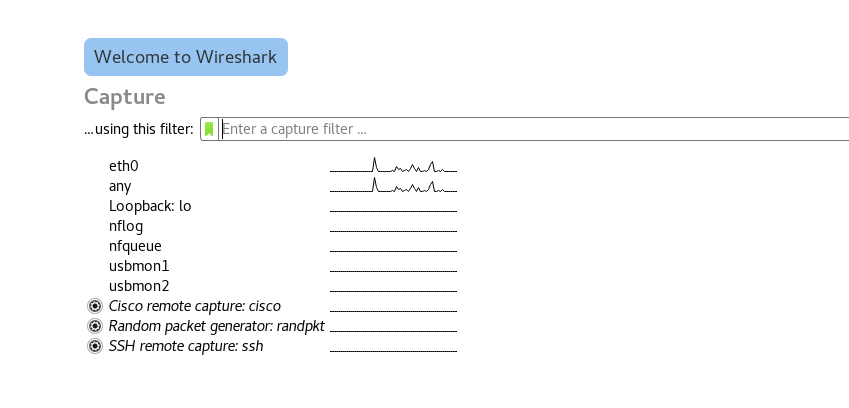
## **WIRESHARK PACKET ANALYSING…**



**Capturing Packets:**

After downloading and installing Wireshark, you can launch it and double-click the name of a network interface under Capture to start capturing packets on that interface. For example, if you want to capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture

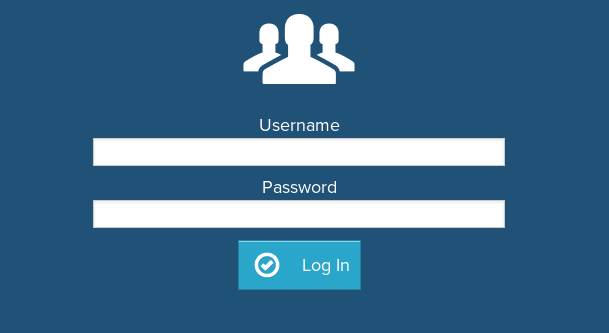
* Options, but this isn’t necessary for now
* Here the above picture indicates the wireshark is going to be started.
* Below mentioned picture indicates that the wireshark capturing the packets.



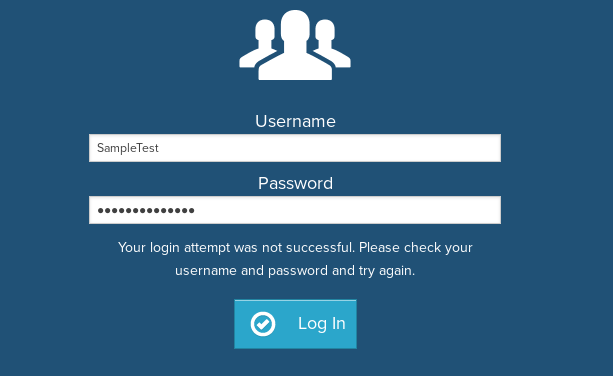
* As soon as you click the interface’s name, you’ll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.
* If you have promiscuous mode enabled—it’s enabled by default—you’ll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the “Enable promiscuous mode on all interfaces” checkbox is activated at the bottom of this window.
* Select the required network interface to start capturing the packets.



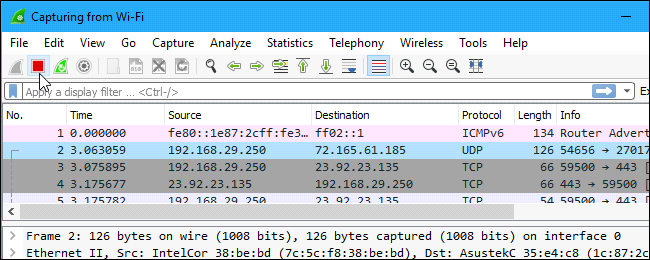
* Then it automatically captures the packets from the different sources connected to the same network interface.
* For example let the user uses to login into some page…..



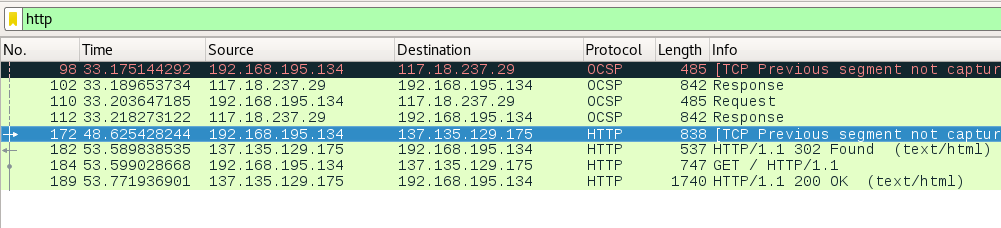
* Let the user will login into this login page as shown….. ☺



* Here in the wireshark it captures the packet related to the login website
* **Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.**



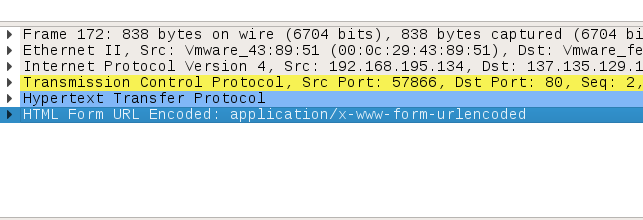
* After stopping capturing the packets let us filter the packets according the protocol(hypertext transfer protocol)
* It filters and shows the filtered packets as mentioned protocol that decreases the search compatability.



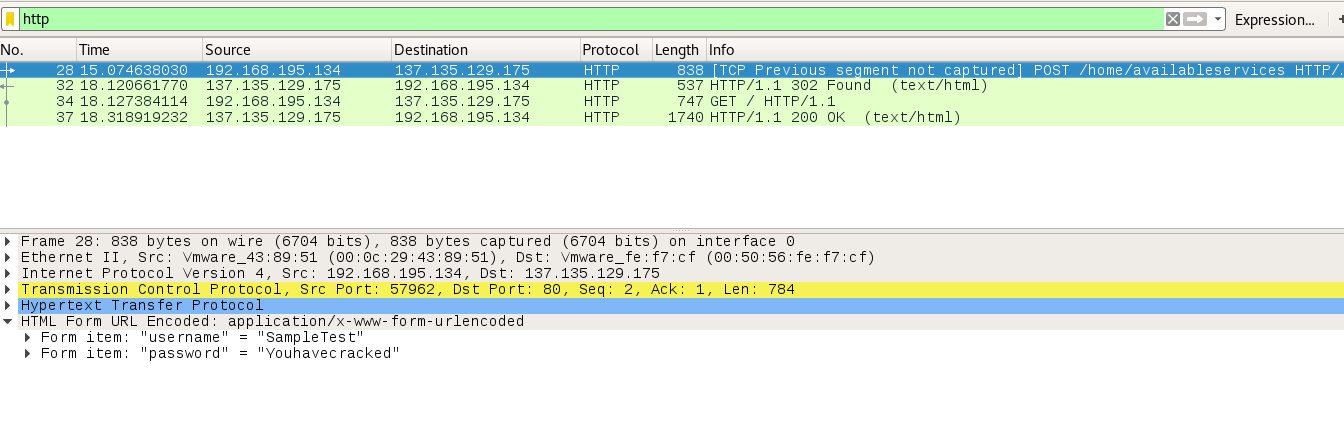
* Here is the list of packets captured according to our search.
* Follow the next process to ge the info of the packet.

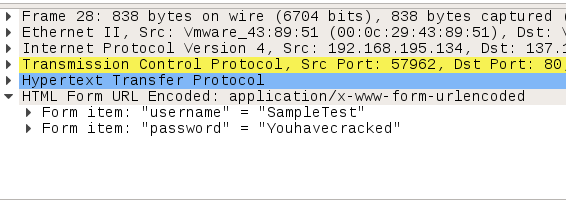
**Inspecting Packets:**

Click a packet to select it and you can dig down to view its details.



* Here search for the POST in the packet filtering then you will get the readable info of the related packet.





* As shown above the username is **Sampletest** & the password is given by **Youhavecracked**.

**HERE IS ALL ABOUT THE WIRESHARK PACKET ANALYSING ☺**