

What is Sniffing

Sniffing is **a process of monitoring and capturing all data packets passing through given network**. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.

Sniffing attack



Sniffing attack in context of network security, corresponds to theft or interception of data by capturing the network traffic using a packet sniffer. When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer.

Introduction to Wireshark

Wireshark is a software tool used to monitor the network traffic through a network interface. It is the most widely used network monitoring tool today. Wireshark is loved equally by system administrators, network engineers, network enthusiasts, network security professionals and black hat hackers.

The extent of its popularity is such, that experience with Wireshark is considered as a valuable/essential trait in a computer networking-related professional.

There are many reasons why Wireshark is so popular:

1. It has a great GUI as well as a conventional CLI (T Shark).
2. It offers network monitoring on almost all types of network standards (ethernet, wlan, Bluetooth etc)
3. It is open-source with a large community of backers and developers.
4. All the necessary components for monitoring, analysing and documenting the network traffic are present. It is free to use.

History of Wireshark

Wireshark was started with the intention of developing a tool for closely analysing network packets. It was started by Gerald Combez in 1997. Its initial name was Ethereal. It was initially released in July 1998 as version 0.2.0. Due to the support it got from the developer community, it grew rapidly and was released as version 1.0 in 2008, almost two years after it was renamed to Wireshark.

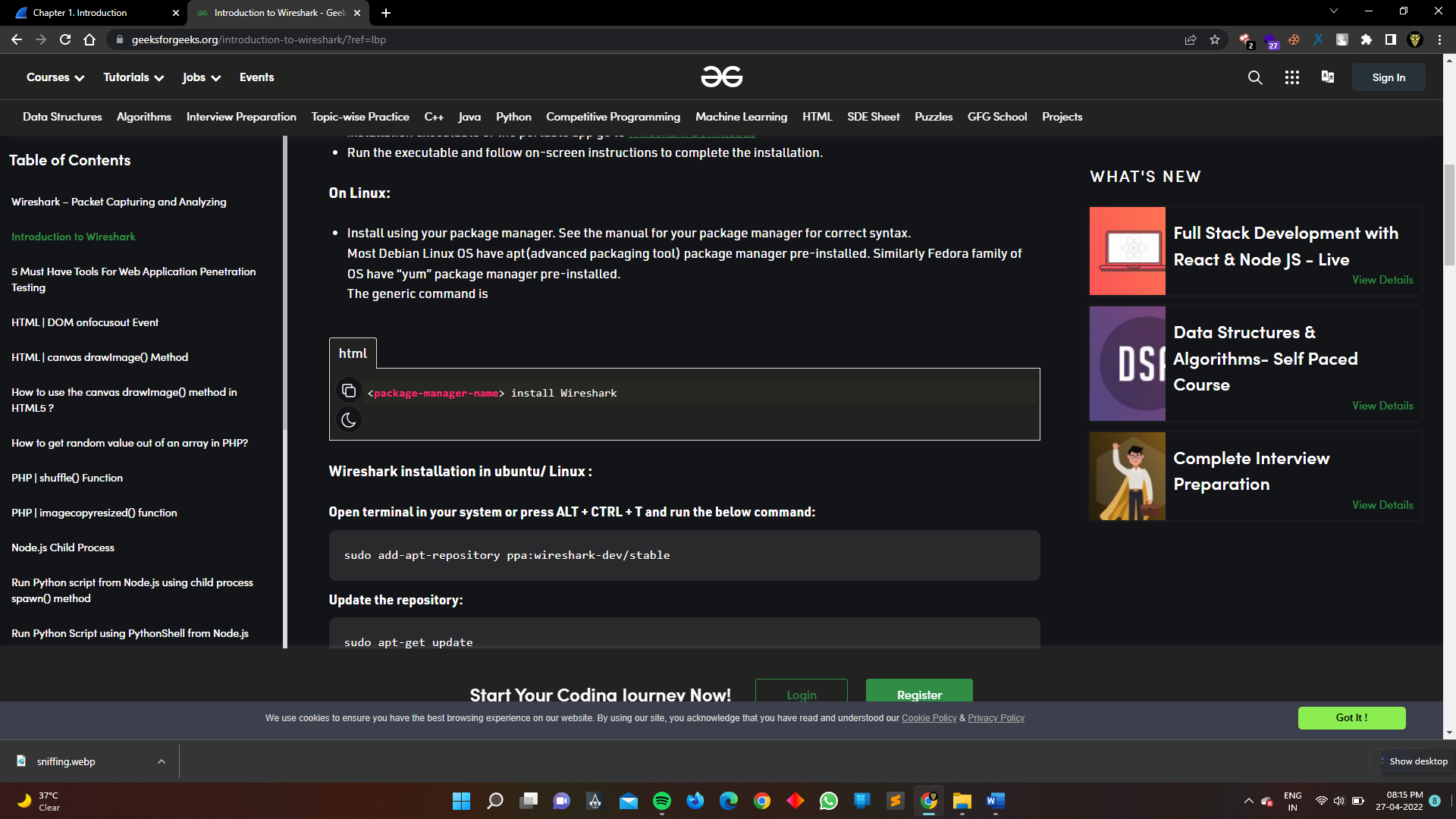
Wireshark installation:

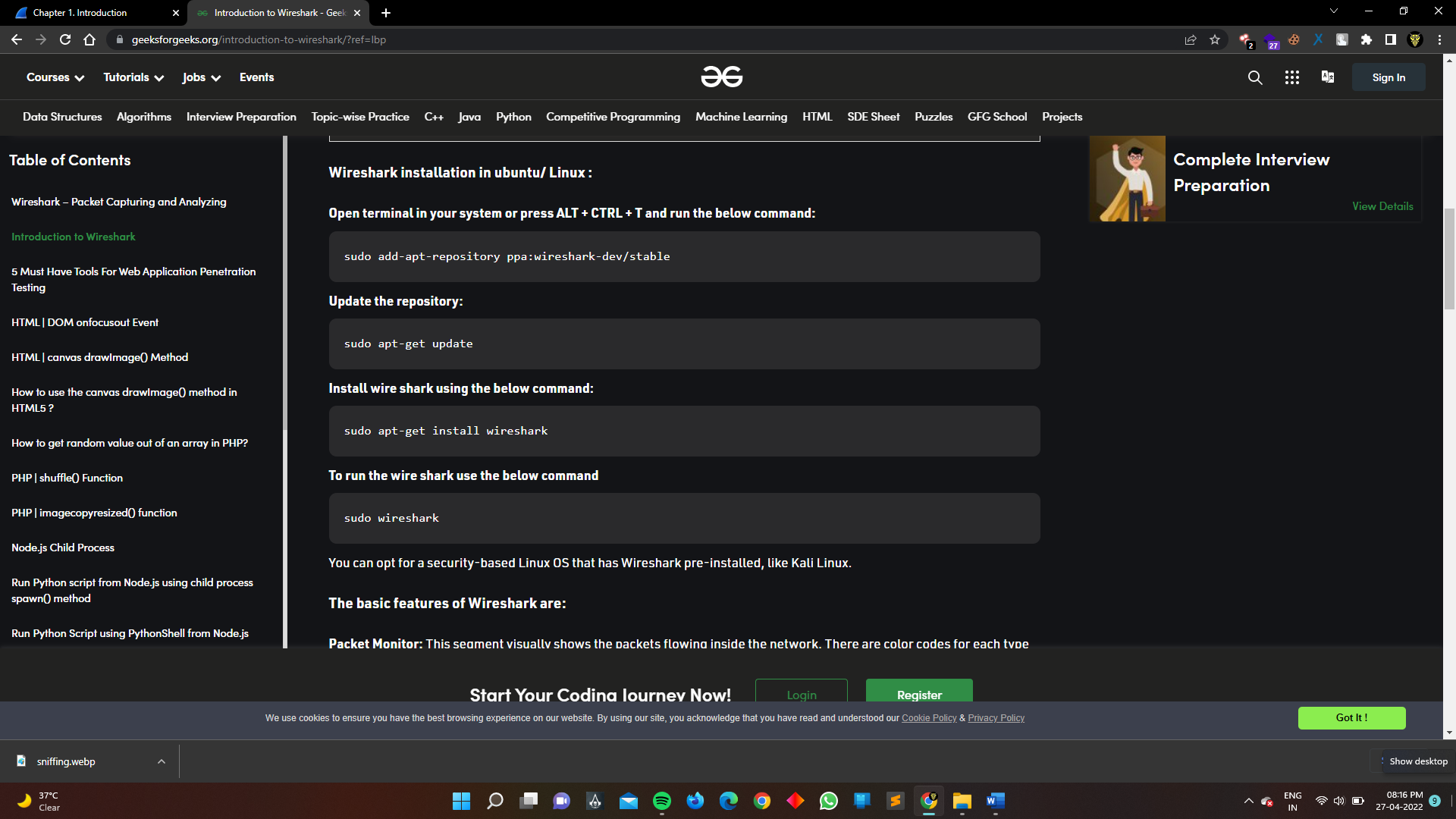
**Windows** :

* You can do a proper installation or run Wireshark as a portable app on your windows system. To download the installation executable or the portable app go to [Wireshark Downloads](https://www.wireshark.org/download.html)
* Run the executable and follow on-screen instructions to complete the installation.

**On Linux:**

* Install using your package manager. See the manual for your package manager for correct syntax.   
  Most Debian Linux OS have apt(advanced packaging tool) package manager pre-installed. Similarly Fedora family of OS have “yum” package manager pre-installed.   
  The generic command is

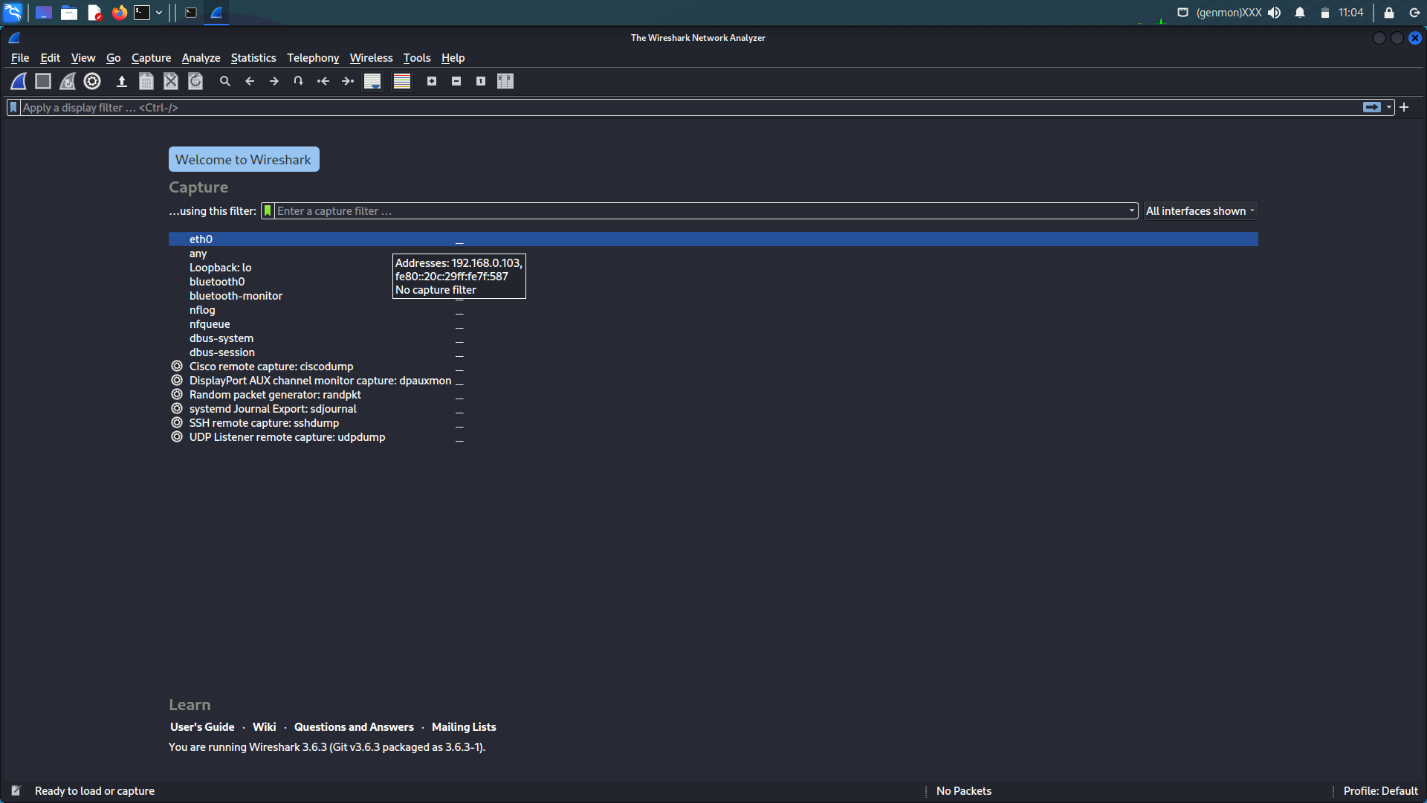




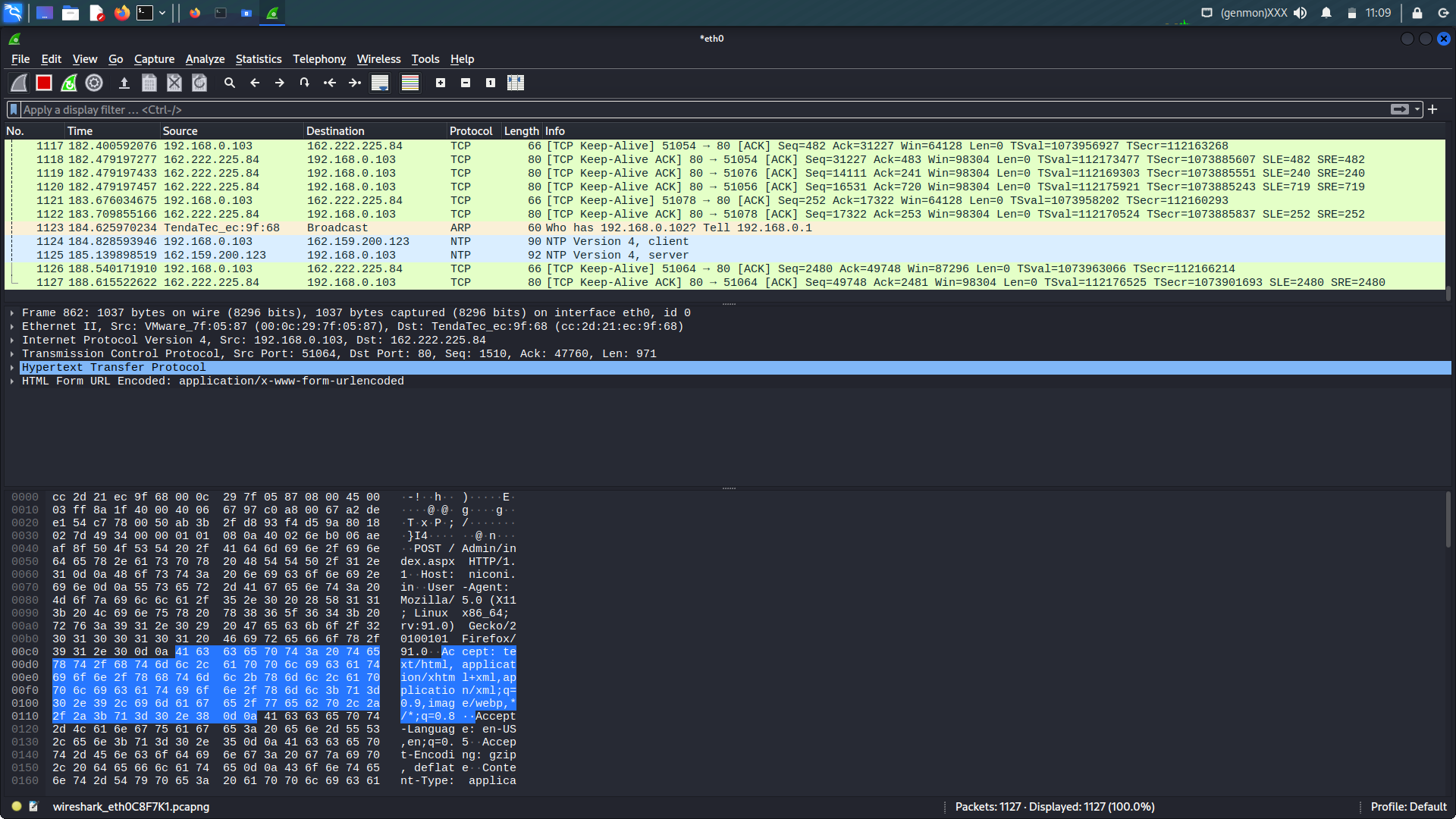
How we install Wireshark in Linux/Ubuntu

How we Use Wireshark (practical)

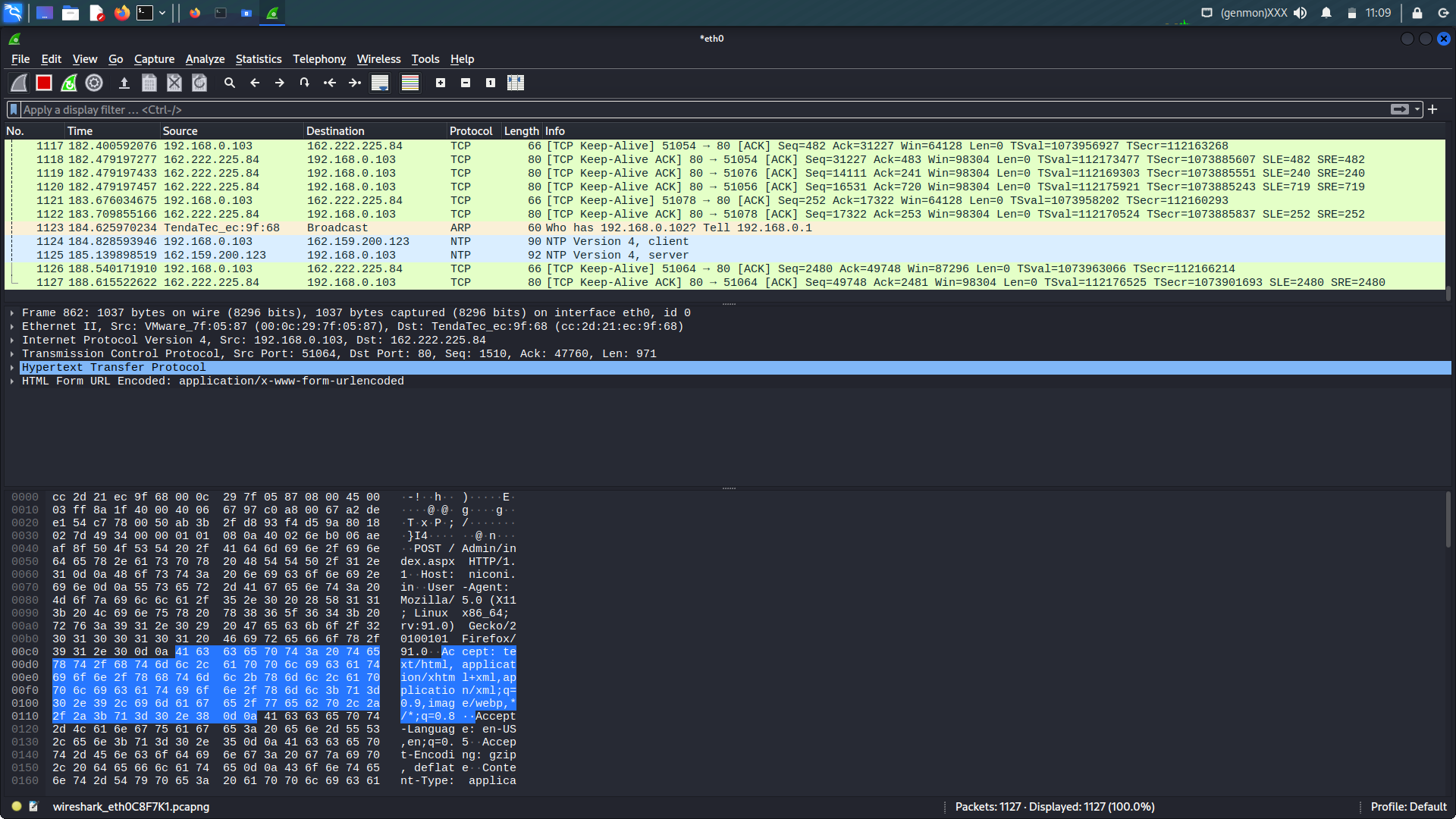
Open the wireshark in linux



Select the option etho



Packet capturing start automatically



Important point

1 Time

2 Source

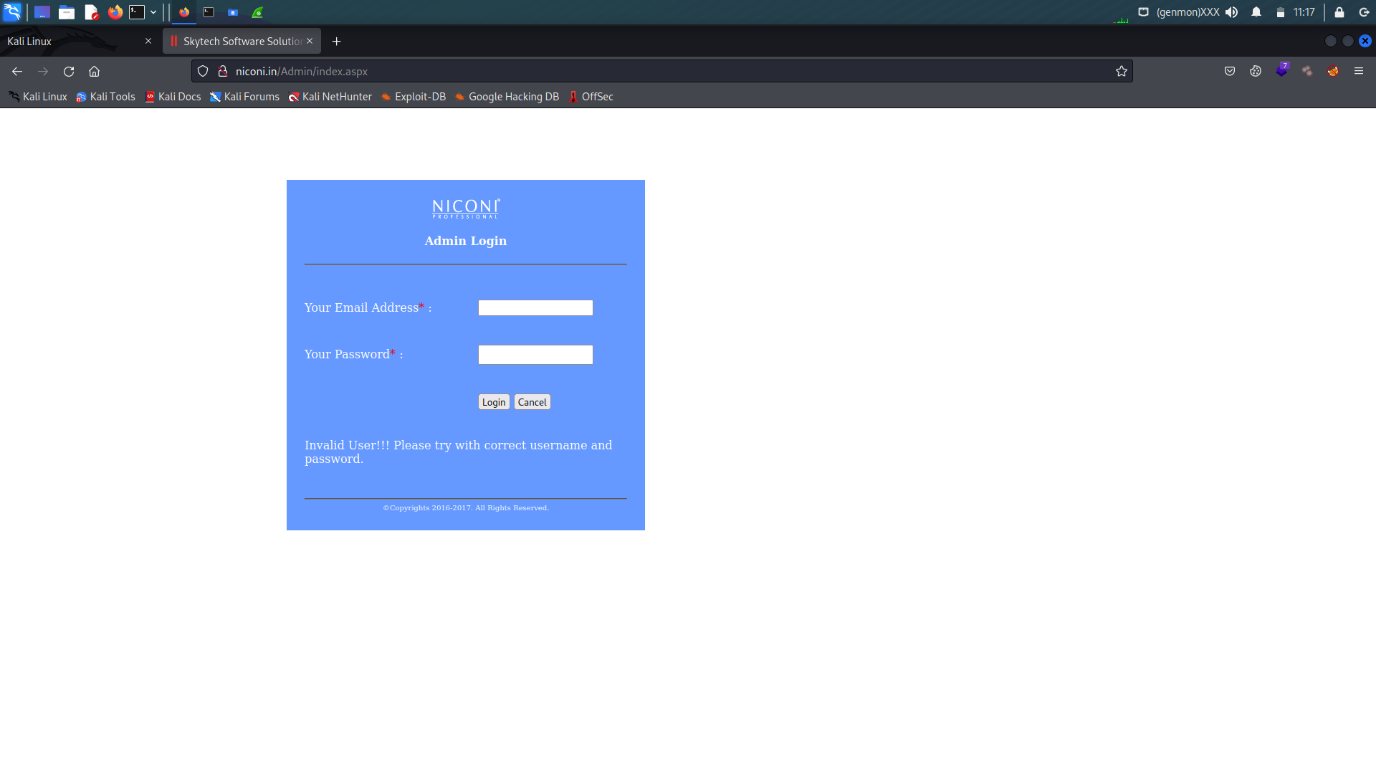
3 Destination

4 protocol

5 Length

6 info

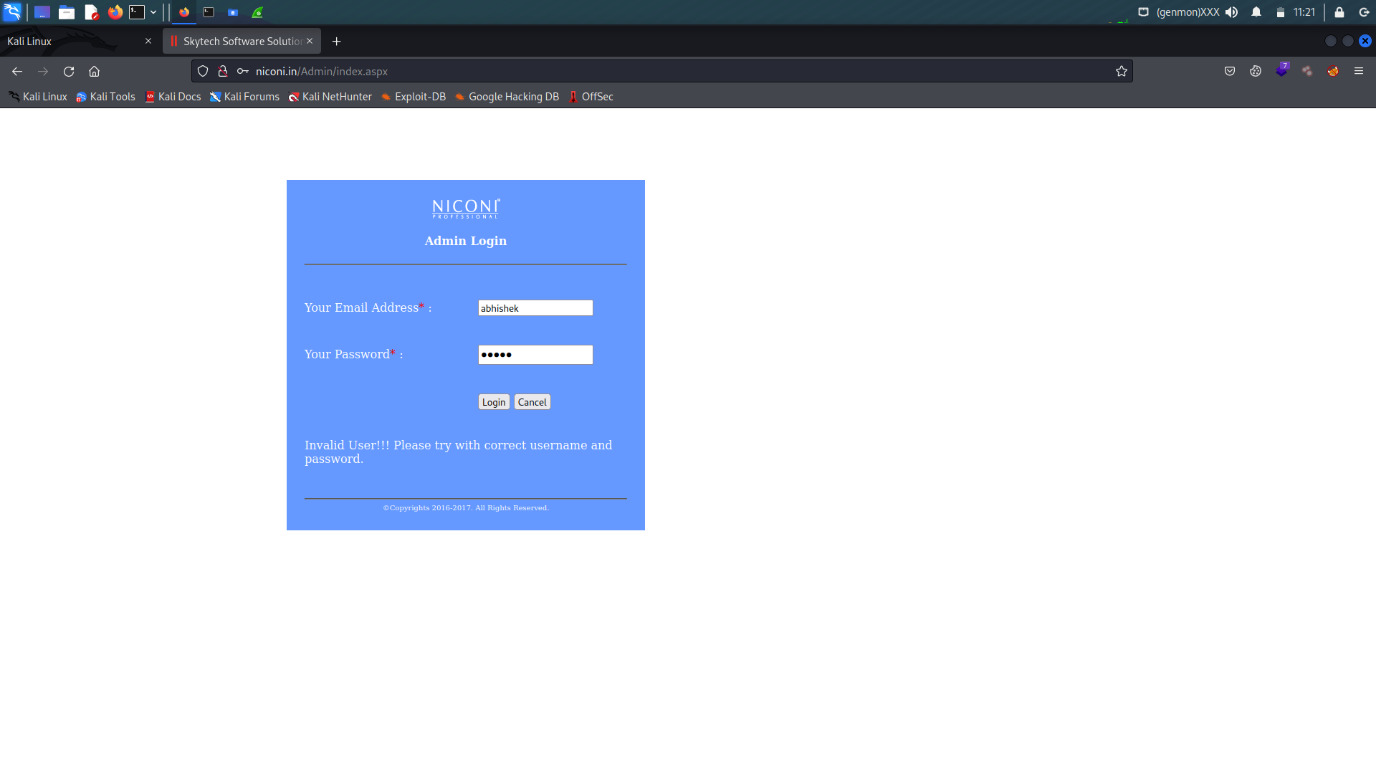
How we hack the password with the help of Wireshark ?



Visit any http website like this <http://niconi.in/Admin/index.aspx>

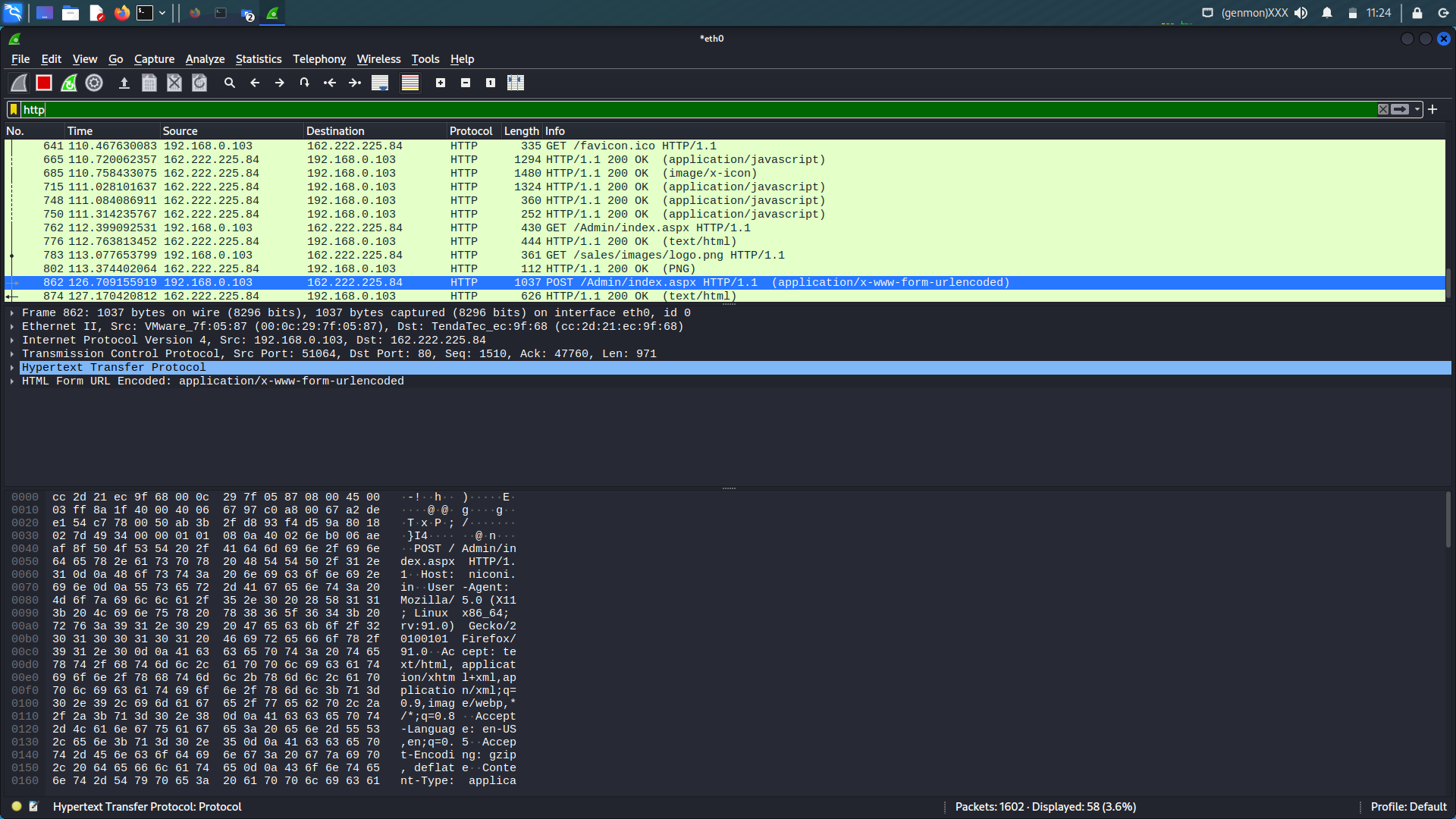
On the Wireshark tool before doing this

Fill the username and passwd in the form

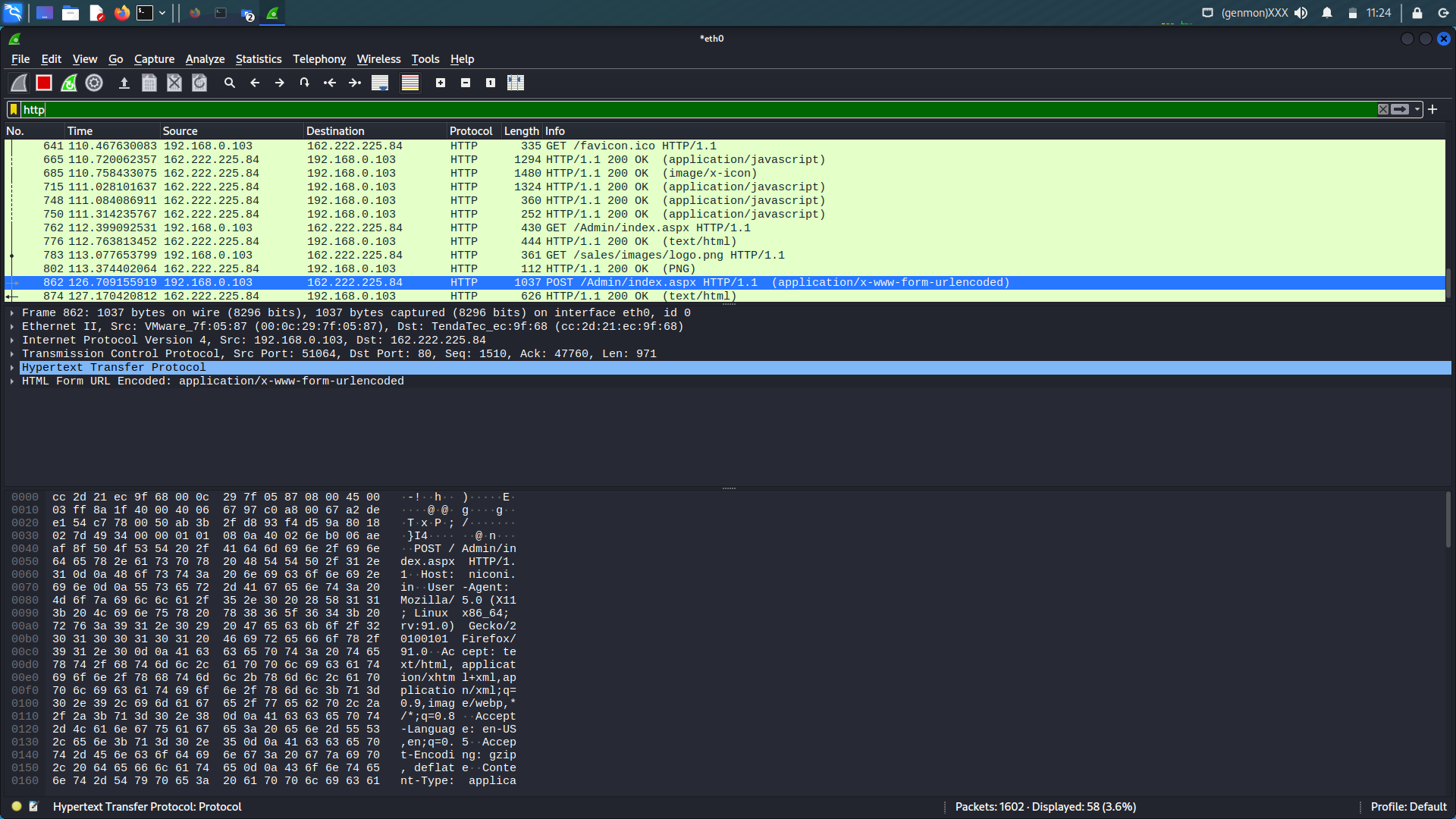


Click on the login

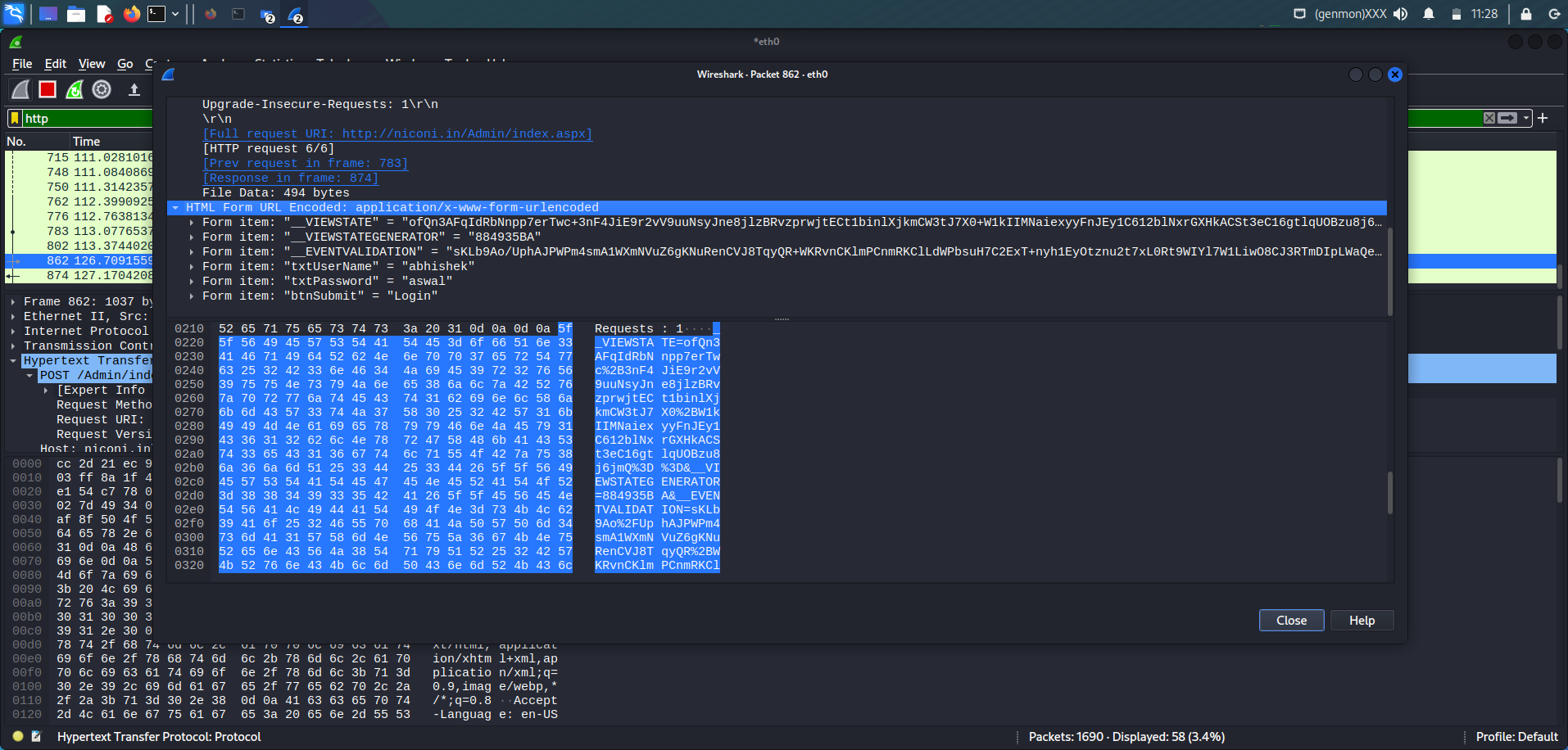
Open the Wireshark and check the request of the website which is capture



After doing this search in the filter “http” and check the website name..



Like this open the request



Here you can easily see the username and passwd

We clearly see the username and password

