Wireshark 0x01

Wireshark 0x01

0x01 aims at providing the basic introduction to get started with Wireshark. 0x01 is the first in the series of Wireshark!

[Task 1] Introduction to Wireshark

Wireshark is one of the greatest tools of the time and is currently being used everywhere wherever there are networks (Live/Offline).
It is used in wide range of fields ranging from Information Technology to Information Security. Wireshark is a network sniffing tool that
is capable of capturing all the network traffic going from and coming towards a particular network device/system.

Wireshark allows us to capture all those packets (Wired/Wireless) which can then be analyzed. This is what, known as "Packet Capturing"
and the process that is followed to analyze the packets is called "Packet Analysis".

In other words, Wireshark is a "Network Analyzer". With Wireshark, we can look for the most common to the most sensitive information
like PII (usernames and passwords, credit card details etc) which is being sent from client's browser to a web server.

Also Wireshark is used to analyze the network traffic for malicious activities. Different type of malware are controlled by C&C servers. Wireshark
plays a vital role here in capturing all those packets in which a particular malware tries to communicate with their server or with other machine's.

Wireshark also allows us to analyze packet captured files offline. We can simply load these files in Wireshark and can analyze them.

Wirehsark is a great tool to learn and it is widely used in performing "Network Forensics".

[#1] Read above

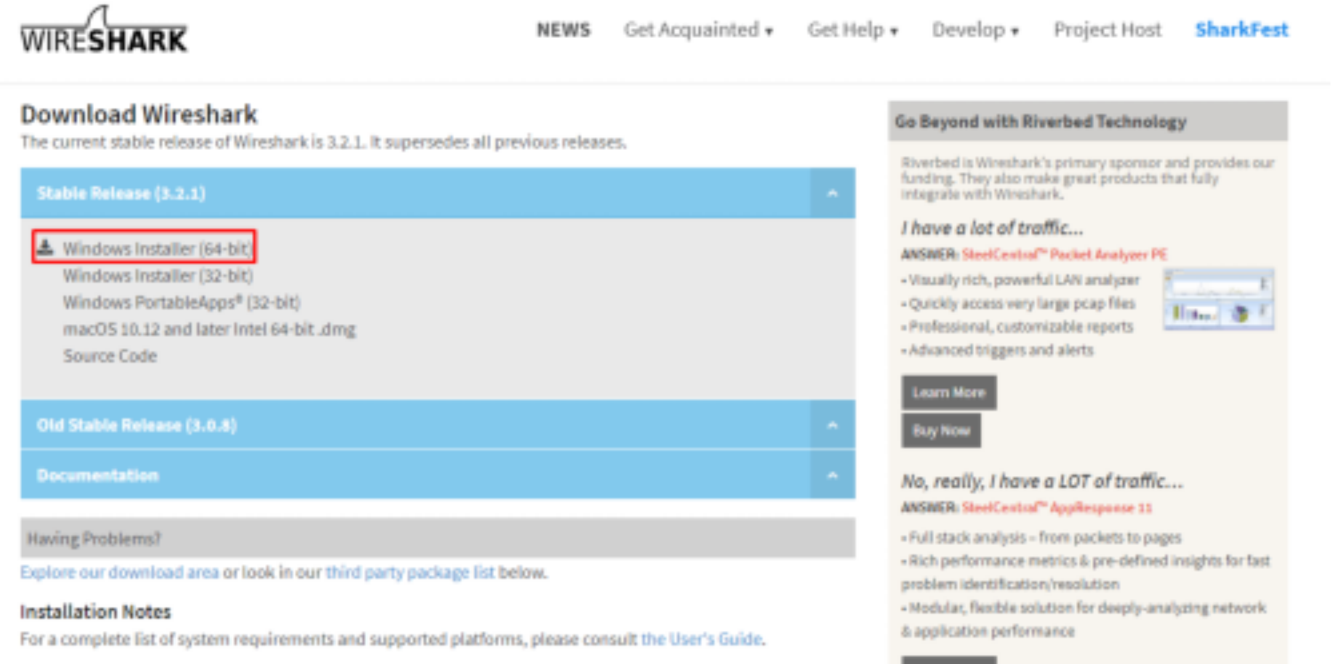
```
No answer needed
```

[Task 2] Downloading & Installing Wireshark - Windows

In order to utilize the Wireshark and its functionality. We first need to download the Wireshark from their official website. Wireshark is available for Windows, Mac and Linux distributions.

1. Downloading Wireshark

Go to the above link and download the Wireshark for Windows. In my case its Windows 10 - x64.
https://www.wireshark.org/download.html



Download Wireshark

The current stable release of Wireshark is 3.2.1. It supersedes all previous releases.

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.12 and later Intel 64-bit .dmg
- Source Code

Having Problems?

Explore our download area or look in our third party package list below.

Installation Notes

For a complete list of system requirements and supported platforms, please consult the User's Guide.

Go Beyond with Riverbed Technology

Riverbed is Wireshark's primary sponsor and provides our funding. They also make great products that fully integrate with Wireshark.

I have a lot of traffic...

ANSWER: SteelCentral™ Packet Analyzer PE

- Visually rich, powerful LAN analyzer
- Quickly access very large pcap files
- Professional, customizable reports
- Advanced triggers and alerts

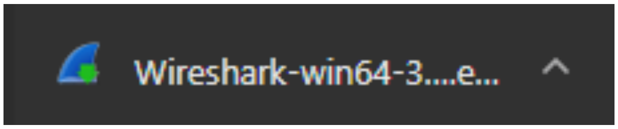
No, really, I have a LOT of traffic...

ANSWER: SteelCentral™ AppResponse 11

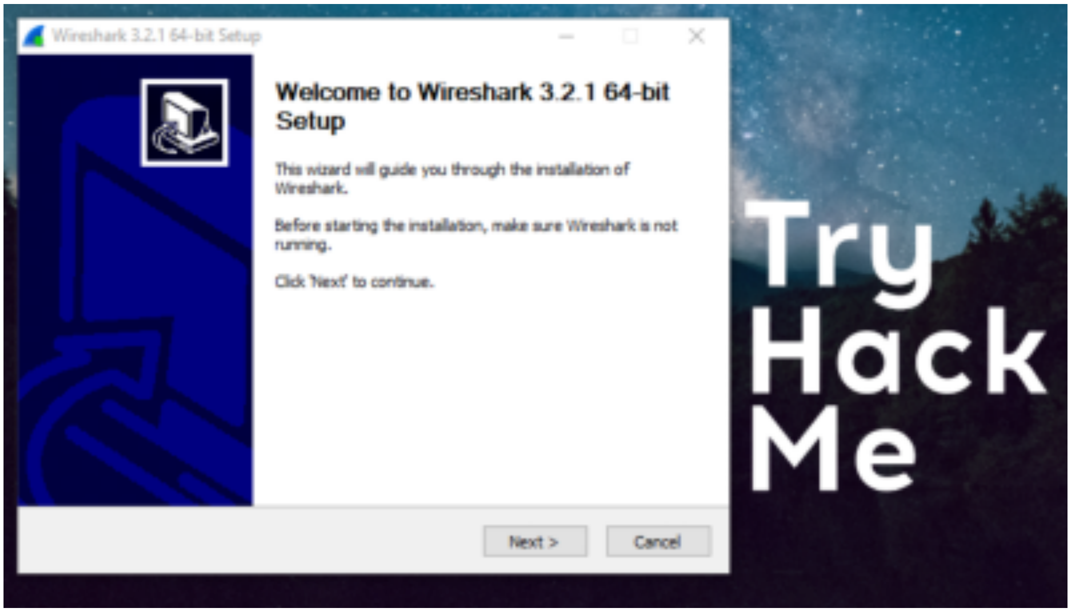
- Full stack analysis – from packets to pages
- Rich performance metrics & pre-defined insights for fast problem identification/resolution
- Modular, flexible solution for deeply-analyzing network & application performance

2. Installing Wireshark

Once the installer has been downloaded. Click on it to install the Wireshark on your system.



Once opened. Install it with the default settings.



Wireshark 3.2.1 64-bit Setup

Welcome to Wireshark 3.2.1 64-bit Setup

This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

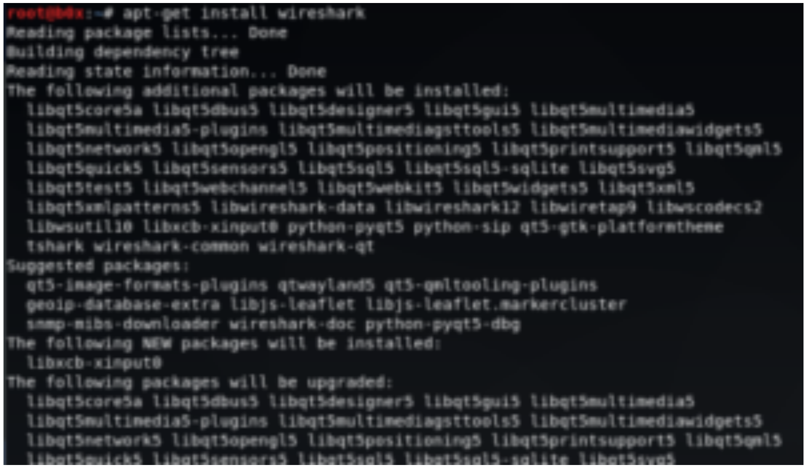
Click 'Next' to continue.

[#1] Download and install Wireshark.

`No answer needed`

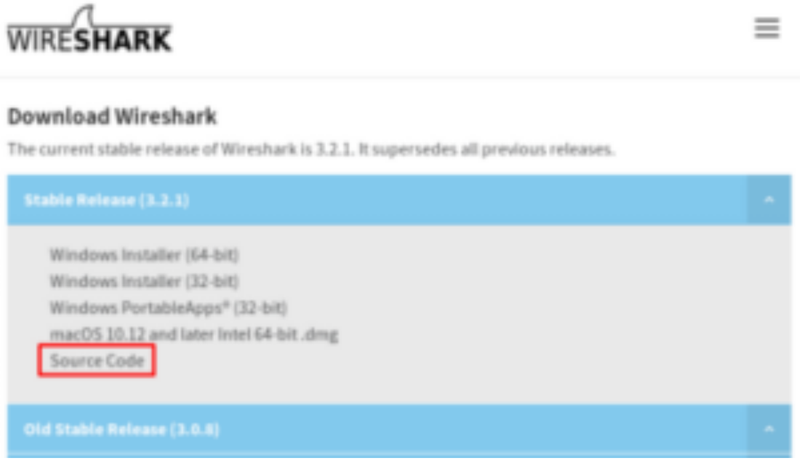
[Task 3] Downloading and Installing Wireshark - Linux

In order to install the Wireshark on Linux we have the two possibilities.
1. We can install it by using the source.
2. We can install it by using the apt-get utility.
Wireshark comes pre-installed with Kali Linux and can directly be run. Meanwhile,
1. Installing it via apt-get utility.
Open up your terminal and issue the following command.
`apt-get install wireshark`



```
root@box:~# apt-get install wireshark
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libqt5network5 libqt5opengl5 libqt5positioning5 libqt5printsupport5 libqt5qml5
  libqt5quick5 libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5
  libqt5test5 libqt5webchannel5 libqt5webkit5 libqt5widgets5 libqt5xml5
  libqt5xmlpatterns5 libwireshark-data libwireshark12 libwiretap9 libwscodecs2
  libwsutil10 libxcb-xinput0 python-pyqt5 python-sip qt5-gtk-platformtheme
  tshark wireshark-common wireshark-qt
Suggested packages:
  qt5-image-formats-plugins qtwayland5 qt5-qmltooling-plugins
  geoip-database-extra libjs-leaflet libjs-leaflet.markercluster
  snmp-mibs-downloader wireshark-doc python-pyqt5-dbg
The following NEW packages will be installed:
  libxcb-xinput0
The following packages will be upgraded:
  libqt5core5a libqt5dbus5 libqt5designer5 libqt5gui5 libqt5multimedia5
  libqt5multimedia5-plugins libqt5multimediagsttools5 libqt5multimediawidgets5
  libqt5network5 libqt5opengl5 libqt5positioning5 libqt5printsupport5 libqt5qml5
  libqt5quick5 libqt5sensors5 libqt5sql5 libqt5sql5-sqlite libqt5svg5
```

2. Installing it via source.
At first we need to download the source from the official website and download the "Source Code".



Download Wireshark

The current stable release of Wireshark is 3.2.1. It supersedes all previous releases.

Stable Release (3.2.1)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows PortableApps® (32-bit)
- macOS 10.12 and later Intel 64-bit .dmg
- Source Code

Old Stable Release (3.0.8)

Meanwhile we can also use the wget utility to download the source code.

```
wget "https://2.na.dl.wireshark.org/src/wireshark-3.2.1.tar.xz"
```

After that we need to unpack the tar file which can be done by utilizing the following command.

```
tar -xvf wireshark-3.2.1.tar.xz
```

Once done we need to crate a directory to build the Wireshark in.

```
mkdir build
cd build
```

Once done, we need to build the files and for this purpose we we utilize the cmake command. If it is not installed, you can install it by using the following command.

```
apt-get install cmake
```

Once done, issue the following command to build the Wireshark.

```
cmake ../wireshark-3.2.1
```

In the end run the make command and finally run wireshark.

```
make
wireshark
```

Finally, we have installed the Wireshark and you will have your Wireshark running.

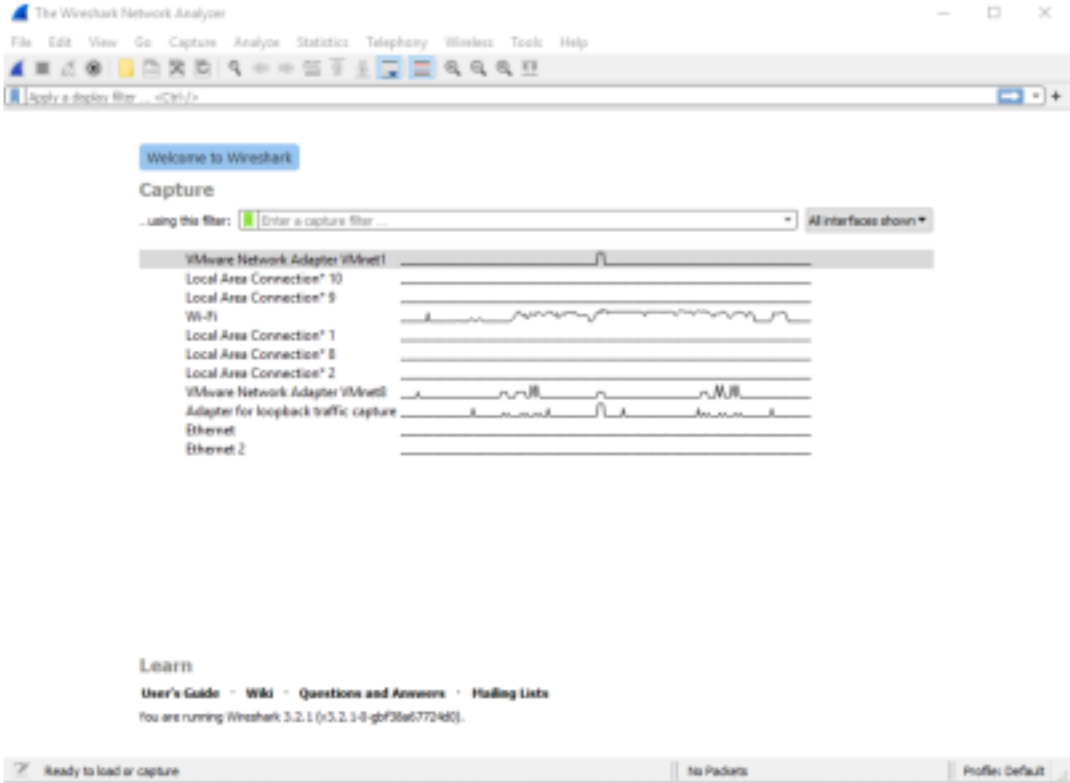
[#1] Download and install Wireshark.

No answer needed

[Task 4] Wireshark GUI - Basics

In this section we will look onto the basics of the Wireshark GUI. It is required that we shall know the different sections of the Wireshark as we will be utilizing all those sections when we will be interacting with the Wireshark.

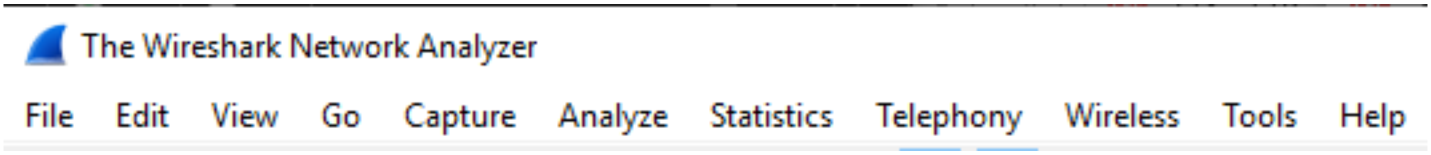
At first, we need to open up Wireshark. On Linux OS, open up your terminal, add "wireshark" and hit enter. The Wireshark will be opened. Meanwhile on Windows, locate the executable, double click on it and Wireshark will be opened. The GUI is same for Windows, Mac and Linux distributions and it looks like as above.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
VMware Network Adapter VMnet1
Local Area Connection* 10
Local Area Connection* 9
Wi-Fi
Local Area Connection* 1
Local Area Connection* 8
Local Area Connection* 2
VMware Network Adapter VMnet8
Adapter for loopback traffic capture
Ethernet
Ethernet 2
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 3.2.1 (v3.2.1-0-gbf38a67724d0).
Ready to load or capture
No Packets
Profile: Default

Now, we will look onto the section one by one!

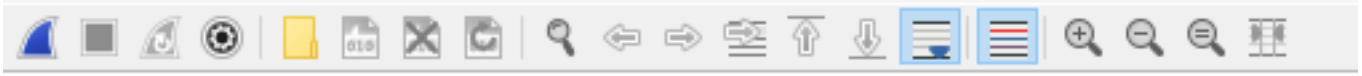
1. Menu

On the top we have the menu bar. It hosts all the features of the Wireshark which are categorized under their suitable titles.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

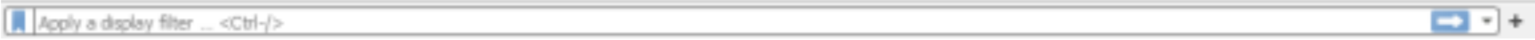
2. Main Toolbar

After that we have the "Main Toolbar" which contains all the actual functionalities which are thoroughly used when working with Wireshark.
Meanwhile you can see that few of the options available are grayed out. It is because they are not available within this context as we are
not capturing any sort of packets at the moment. We will see these options available when we will move further.



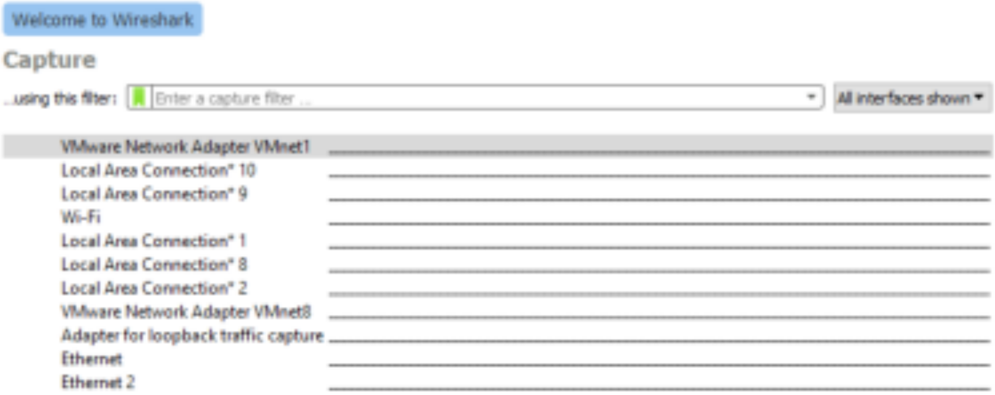
3. Filter Bar

This is the most important functionality in Wireshark. This allows us to filter/narrow down our results. It is because when we capturing the
packets there are hundreds and even thousands of packets coming in and going out from the system/device. So in order to narrow down
our search i.e. suppose we want to look for only HTTP packets we can filter HTTP packets from all other packets and by so we can narrow
down our search.

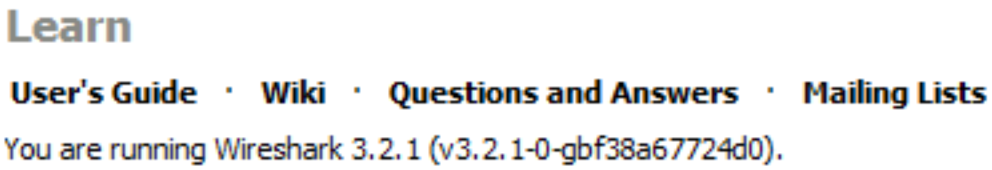


3. Capture Frame

This frame allows us to see which interfaces are available for Wireshark and also available on the system. We can then select a particular interface
to make the Wireshark particularly sniff on that interface. We will be utilizing this functionality in our next rooms more thoroughly and extensively.
Meanwhile you can see that we have bunch on interfaces available i.e. Virtual, eth0, WiFi etc.

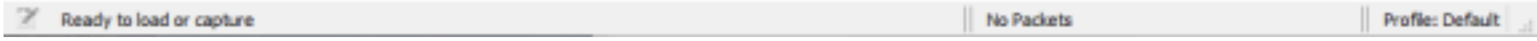


4. Wireshark Version
In the bottom we can find thee current version of the Wireshark which is currently being used. We can also find the User's Guide there.



You are running Wireshark 3.2.1 (v3.2.1-0-gbf38a67724d0).

5. Status Bar
In the end, we have the status bar where we can see the mode of the Wireshark. At this moment we are not capturing any packets so it states that it is ready to load or capture. Alongside on the right we can see the profile. We at the moment are using the default profile of Wireshark that comes pre-installed with it.



Ready to load or capture | No Packets | Profile: Default

[#1] Read above

```
No answer needed
```

[Task 5] Conclusion

So far, we have discussed about Wireshark, what it actually is and what does the different sections has to do on the GUI.
After all this you all will have a basic introduction to this tool and also you now know what does those sections means and have to do with the Wireshark.
The "Basic Introduction" has been covered in this room i.e. the first room of the Wireshark 0x0F series.In the upcoming rooms we will be looking onto using Wireshark in more details and you all will be able to get hand's on experience with this tool.
You can drop your feedback about this room/series on Discord.

[#1] Read above

```
No answer needed
```