Hacking Articles

Raj Chandel's Blog

Wireshark For Pentester: A Beginner's Guide

April 13, 2021 By Raj Chandel

Wireshark is an open-source application and it is the world's foremost and widely-used network protocol analyzer that lets you see what's happening on your network at a microscopic level. Just Because it can drill down and read the contents of each packet, it's used to troubleshoot network problems and test software.

Table of contents

What is Wireshark

Wireshark is an open-source widely used network packet or protocol analyzer. It is an essential tool for security professionals or system administrators. It is used to analyze the structure of different network protocols and has the ability to demonstrate application.

Wireshark can be operated in different platforms such as Windows, Unix, Linux and employs the GTK+ widget toolkit or PCAP for packet capturing. IT also has terminal-based free software versions like Tshark. Wireshark shares many characteristics with tcpdump only the difference is that it supports a graphical user interface (GUI) and has information filtering features.

Features

The following are the features that Wireshark provides:

- Can be operated on *UNIX and Windows*.
- *Capture live* packet data from a network interface.
- *Open files* containing packet data captured (PCAP Files) with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- *Import*packets from text files containing hex dumps of packet data.
- Display filters are used to filter and organize the data display.
- Display packets with *very detailed protocol information*.
- New protocols can be scrutinized by creating plug-ins.
- *Captured Traffic can also be trace Voice Over Internet (VOIP) calls over the network.*
- *Export some* or all packets in several capture file formats.
- *Filter packets on* many criteria.
- *Search for* packets on many criteria.
- *Colorize packet* display based on filters.
- Create various *statistics*.
- …and *a lot more!*

Installation of Wireshark

For Windows

Wireshark can be downloaded at no cost from the official website of Wireshark for both Windows and macOS. Here you can select and download the latest stable version of Wireshark

After downloading the Wireshark navigate to the downloads directory and run the Wireshark setup. During the installation process of Wireshark, choose to install Npcap if prompted as these include libraries required for live data capture.

After the installation of Wireshark, you must be logged in to the device as an administrator to use Wireshark. In Windows 10 simply search Wireshark and ***Run as administrator***. In macOS right-click the Wireshark app icon and select ***Get Info***. In the ***Sharing & Permissions*** settings, give the admin ***Read & Write*** privileges.

For Linux

Wireshark is also available for Linux and other UNIX like platforms including Red Hat, and FreeBSD.

To download Wireshark, open a terminal and type the following command to install Wireshark:

```
apt install wireshark
```

Press ‘Y’ when prompted to occupy additional space. During installation, Wireshark configuration will ask “should non-super users be able to capture the packets?”. For security purpose, it is not advisable to allow non-super users to access Wireshark. As of now, continue by pressing ‘yes’. Wireshark installation will continue and successfully install into the system.

Type the following code to verify the installation package of Wireshark:

```
apt show Wireshark
```

And to open the Wireshark run the following command and the Wireshark application will be visible as below:

```
Wireshark
```

Whenever you open Wireshark you will be prompted with the following screen.

Here you can see different network interfaces on your device. In the above image we can see there is a lot of traffic being communicated through the Wi-Fi interface. In most cases, you will only be able to see traffic going in and out of your own device, however, some wireless network cards can be set into monitor mode so that you will be able to see traffic from other wireless devices on the network.

Introduction to Wireshark UI Basics

As of this now you have installed Wireshark into your systems and likely excited to get started capturing your first packets. Without wasting of much time let's get started!!!

Now we're going to explore

- How Wireshark interface works
- How to view packets in Wireshark
- How to capture packets in Wireshark
- How to perform Trace Analysis in Wireshark
- How to filter packets in Wireshark
- ....and much more things!!

Wireshark can be started through windows program manager by searching Wireshark or also can be started through the command line by typing "Wireshark" in the directory of Wireshark.

The Main Window

Let's quickly take a look at the Wireshark user interface. Usually, you would see this similar scenario after some packets are captured or loaded.

Wireshark main window consists of these parts that are commonly called GUI programs.

1. The menu is used to start actions
2. The main toolbar quick access to frequently used items from the menu
3. Filter Toolbar allows user to set display filters to filter which packet should be displayed
4. The Packet list pane displays a summary of each packet captured.
5. The Packet details pane displays the packet selected in the packet list pane
6. The packet bytes pane displays the data from the packet selected in the packet list pane and highlights the field selected in the packet details pane
7. The status bar shows some detailed information about the current program state and the captured data.

The Menu

Wireshark main menu is located at the top of the main window (window, Linux).

The main menu contains the following Items:

File

This menu contains items to open and merge capture files, save, print, or export capture files in different Formats

Edit

This menu contains items to find a packet, time reference or mark one or more packets, handle configuration profiles, and set your preferences; (cut, copy, and paste are not presently implemented). The Wireshark Edit menu contains the fields as shown in the below image

View

This menu controls the display of the captured data, including colourization of packets, zooming the font, showing a packet in a separate window, expanding and collapsing trees in packet details.

Go

This menu contains items to go to a specific packet.

Capture

This menu allows you to start and stop captures and edit capture filters. Some of the important filters that make our capture more efficient are described below.

Analyze

This menu contains items to manipulate display filters, enable or disable the dissection of protocols, configure user-specified decodes and follow a TCP stream.

Statistics

This menu contains items to display various statistic windows, including a summary of the packets that have been captured, a display protocol hierarchy statistics and much more. Some of the important filters that make our Trace analysis more efficient are described below.

Statistics -> Protocol Hierarchy

- Presents descriptive statistics per protocol.
- Useful for determining the types, amounts, and relative proportions of protocols

within a trace

Statistics -> Conversations

- Generates descriptive statistics about each conversation for each protocol in the trace.

Statistics -> Flow Graph

- Generates a sequence graph for the selected traffic.
- Useful for understanding seq. and ack. calculations.

Telephony

This menu contains items to display various telephony related statistic windows, including a media analysis, flow diagrams, display protocol hierarchy statistics and much more.

Wireless

This menu contains items to display Bluetooth and IEEE 802.11 wireless statistics.

Tools

This menu contains various tools available in Wireshark, such as creating Firewall ACL Rules.

Help

This menu contains items to help the user, e.g. access to some basic help, manual pages of the various command-line tools, online access to some of the webpages, and the usual dialogue.

The Main Toolbar

The main toolbar provides quick access to frequently used items from the menu. This toolbar can customize by the user.

Actions of this filter toolbar are described below

Reference: –
https://www.wireshark.org/docs/wsug_html_chunked/ChUseMainToolbarSection.html

The Filter Toolbar

The filter toolbar lets you quickly edit and apply display filters.

Actions of this filter toolbar are described below

The packet list pane

The packet list pane displays all the packets in the order they were recorded.

Each line in the packet list corresponds to one packet in the capture file select the lines to get more details. More details will be displayed In the Packet details pane and packet byte panes.

There are lots of column available such as

- No: -The number of the packet in the capture file. This number won't change, even if a display filter is used.
- Time: -The timestamp of when the packet was captured is displayed in this column. The presentation format of this timestamp can be changed.
- Source: -The address where this packet is coming from.
- Destination: -The address where this packet is going.
- Protocol: -The highest-level protocol that Wireshark can detect.
- Length: -The length in bytes of each packet.
- Info: -Additional information about the packet content.

The packet details pane

The packet details pane shows the selected or current packet in a detailed form.

The above pane shows the protocols and protocol fields of the packet selected in the "packet list" pane. The protocols are shown in a tree which can be expanded and collapsed.''

The Packet Bytes pane

The packet bytes pane shows the data of the selected or current packet in hex dump style.

The packet bytes pane shows a canonical hex dump of the packet data. Each line contains the data offset, sixteen hexadecimal bytes and sixteen ASCII bytes. Non-printable bytes are replaced with period **"."**

The status bar

The status bar displays informational messages such as

The colourized bullet

The left side shows the highest expert information in the currently loaded capture file. Hovering the mouse on the colourized bullet will show you a description of the expert information level.

The edit icon

This allows you to add a comment to the capture file using the capture file properties dialogue.

The middle

It shows the current number of packets in the capture file. The following values are displayed:

Packets

The number of packets is being captured.

Displayed

The number of packets is being displayed.

Marked

The number of marked packets. Only displayed if you mark any packets in the capture.

Dropped

It shows the number of dropped packets. only displayed If Wireshark was unable to capture all packets.

Ignored

It shows the number of ignored packets and it will only be displayed if you ignore any of the packets.

The right side

it shows the selected configuration profile. Clicking on this part of the status bar will bring up a menu with all available configuration profiles, and selecting from this list will change the configuration profile.

Packet Capturing

The following methods can be used to start capturing packets

You can double-click on the interface in the welcome screen of Wireshark

If you already know the name of the capture interface then you can start Wireshark from the command line by running the following command:

```
wireshark -I eth0 -k
```

This will start Wireshark capturing on interface eth0

Once you have captured some packets you can view the packets that are displayed in the packet list pane by simply clicking on a packet on a packet list pane, which will bring up the selected packet in the tree view and byte view panes. As soon you capture some traffic then you need to apply some filter to make it easily understandable.

Wireshark has two filtering languages

- Capture filters
- Display filters

Capture filters are used for filtering when capturing packets and display filters are used for filtering which packets are displayed. Wireshark provides a display filter language that enables you to precise control which packets are displayed

Display filter fields

Wireshark's display filters a bar located right above the column display section. To only display packets containing a particular protocol, type the protocol into Wireshark's display filter toolbar Wireshark offers a list of suggestion based on the text that you typed.

For example, to only display TCP packets, type tcp into Wireshark's display filter toolbar.

Similarly, to only display packets containing a particular field, type the field into Wireshark's display filter toolbar. For example, to only display HTTP requests, type ***http.request*** into

Wireshark's display filter toolbar and it will accept the expression and works as intended

A similar example of Wireshark display filter accepting an expression but it does not work as intended such as type DNS and **ip.addr !=10.96.203.66**

As you saw above the expression works but not intended.

As we have noticed these packet captures have different colours. So, what are these colours intended for…?

Don't get confused with a different type of colour packets. These colours are intended for

- Gray – TCP packets
- Black with red letters – TCP Packets with errors
- Green – HTTP Packets
- Light Blue – UDP Packets
- Pale Blue – ARP Packets
- Lavender – ICMP Packets
- Black with green letters – ICMP Packets with errors

Note: – Colourings can be changed under View -> Colouring Rules

Building Display Filter expressions.

we can build display filters that compare values using a different type of comparison operator.

For example to only display packets to or from the IP address 10.96.200.253 use **ip.addr==10.96.200.253** . Wireshark display filter uses Boolean expressions, so we can specify values and chain them together. A complete list of available comparison operators is shown below.

Some Useful Filters

Here are some filter expressions that can be used as a way to quickly review web traffic.

Let's understand this with some sort of methods like how we are going to filter some infectious traffic.

Open the packet capture and apply the following filter: "http.request". This filter will show all

HTTP post requests. Also, you can find the total no. of packets at the bottom of the Wireshark screen that are 16 of these packets.

```
    http.request
```

After that to reveal all the URLs for HTTP requests, Domain names we can use the following expression as a way to quickly review web traffic

```
  http.request or ssl.handshake.type == 1
```

The value ***http.request*** reveals URLs for HTTP requests, and ***ssl.handshake.type == 1*** reveal domain names used in HTTPS or SSL/TLS traffic. Filtering with this display filter can outline the flow of events for the web traffic.

By modifying these types of filters, you can drill down the infectious traffic.

Hands-On Practice

Let's understand Wireshark with some sort of Questions

Q1. Find out the total no. of TCP syn packet for port 80

Answer: – To reveal all the TCP syn packets we can use the following expression as a way to quickly review web traffic for port 80. Also, you can find the total no. of packets at the bottom of the Wireshark screen that are 4 of these packets.

```
  tcp.flags.syn == 1 and tcp.flags.ack == 0 && tcp.port == 80
```

Q2. Filter out all the packet with the http response code 200.

Answer: – The value ***http.response*** reveals URLs for HTTP responses, and ***HTTP status code 200*** means success. The client has requested documents from the server. The server has replied to the client and given the client the documents. Filtering with this display filter can outline the flow of events for the web traffic.

```
http.response.code == 200
```

Q.3 Attacker try to download the malicious file from www.ethereal.com. Write down the filter to identify the http host.

Answer: – In this case, we have to find out the host who have visited the malicious website. As we know each website have own URL. So simply we can find out the host by using the following expression who have visited a malicious website.

```
http.host=="www.ethereal.com”
Or http.host=="URL”
```

Q4. Write down the filter to identify the destination port 23.

Answer: – Answer is quite simple… you can use the following expression to filter out the destination port 23

```
tcp.dstport == 23
```

Q5. Filter out the packets on behalf of the mac address.

Answer: – Apply the following expression to filter out the traffic for the specific mac address.

```
eth.addr == 00:a0:cc:3b:bf:fa
```

```
Or eth.addr == “mac addr”
```

Q6. Write down the filter to identify the IP address 10.96.203.66 for port 80 also including the IP address 10.121.1.161. find out the total no. of the packet.

Answer: – In this situation, we can create our custom filter for these types of random scenarios by using logical operators such as

```
ip.addr==10.96.203.66 and tcp.port==80 &&!(ip.addr==10.121.1.161)
```

By applying this filter, we can easily find out the total packets that are 3 of these packets.

Q7. Find out the flag hidden in the provided pcap file that contains the user name for

1. All users of the Ftp session
2. Find out the credentials used for the Telnet session
3. Find out which command is being executed during the telnet session.

Answer: – Do it by yourself. By getting the flag to submit the flag in the comment section.

All the best.

You can download the pcap file from **here**.

Source: **https://www.wireshark.org/**

Author – Vijay is a Certified Ethical Hacker, Technical writer and Penetration Tester at Hacking Articles. Technology and Gadget freak. Contact **Here**

FACEBOOK TWITTER PINTEREST LINKEDIN

PREVIOUS POST
Top Choices for Java Coding Practice

NEXT POST
Domain Persistence: DSRM

One thought on “Wireshark For Pentester: A Beginner’s Guide”

Reborn
April 14, 2021 at 6:38 pm

my mentor >,<

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *

Website

□ Notify me of follow-up comments by email.

□ Notify me of new posts by email.

Post Comment

Search

Search … | Search

Subscribe To Blog Via Email

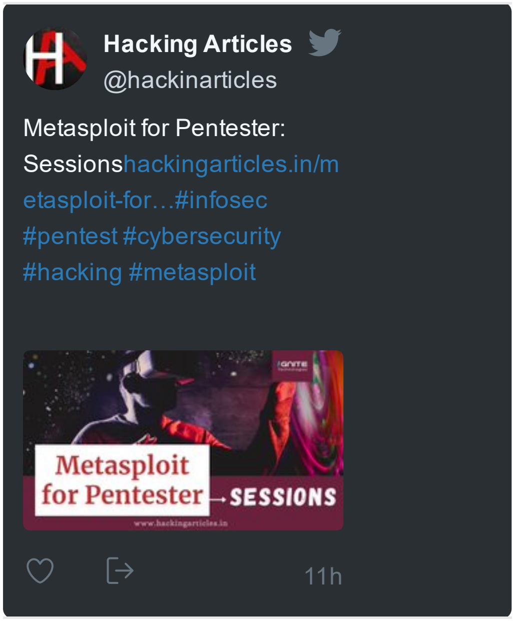
Email Address

Subscribe

Join Our Training Programs

iGNITE Technologies
JOIN OUR CYBER SECURITY TRAINING PROGRAMS
Enroll Today
www.ignitetechnologies.in

Follow Me On Twitter


Hacking Articles
@hackinarticles

Metasploit for Pentester: Sessionshackingarticles.in/metasploit-for…#infosec #pentest #cybersecurity #hacking #metasploit

Categories

- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Password Cracking
- Penetration Testing
- Pentest Lab Setup
- Privilege Escalation
- Red Teaming
- Social Engineering Toolkit
- Uncategorized
- Website Hacking

Window Password Hacking

Wireless Hacking

Wireless Penetration Testing

Articles

Select Month ▼

You may like

MSSQL for Pentester: Abusing Linked Database

September 11, 2021

MSSQL for Pentester: Abusing Trustworthy

September 7, 2021