**LAB - 4**

**WIRESHARK OBSERVATION**

**Objective:**

To observe the data packets the are transferred from one host to other using Wireshark.

**Introduction:**

A network packet is a formatted unit of data transferred from one host to another. A packet consists of control information and user data] which is also known as the payload. Control information provides data for delivering the payload, for example, source and destination network addresses, error detection codes, and sequencing information. Typically, control information is found in packet headers and trailers.

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and tries to display that packet data as detailed as possible. In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, all that has changed. Wireshark is perhaps one of the best open source packet analyzers available today.

**Experiment:**

In order to observe the network packets, the following steps are followed:

1. Set up an Apache server which hosts a text file on our local computer (or any other computer on the same network).
2. Secondly, we start Wireshark and choose to listen to the packets on localhost i.e., select *‘loopback:lo’.*
3. We then request the text file to the server and download it by using a tool called *‘wget’*.
4. And then observe/analyze the data packets in Wireshark.

**Step-1:**

1. Open a terminal and create a data file named data.txt and put some data in it.

|  |
| --- |
| $ nano data.txt |

1. Make apache is installed.
2. Move the file to the /var/www/html folder

|  |
| --- |
| $ sudo mv data.txt /var/www/html |

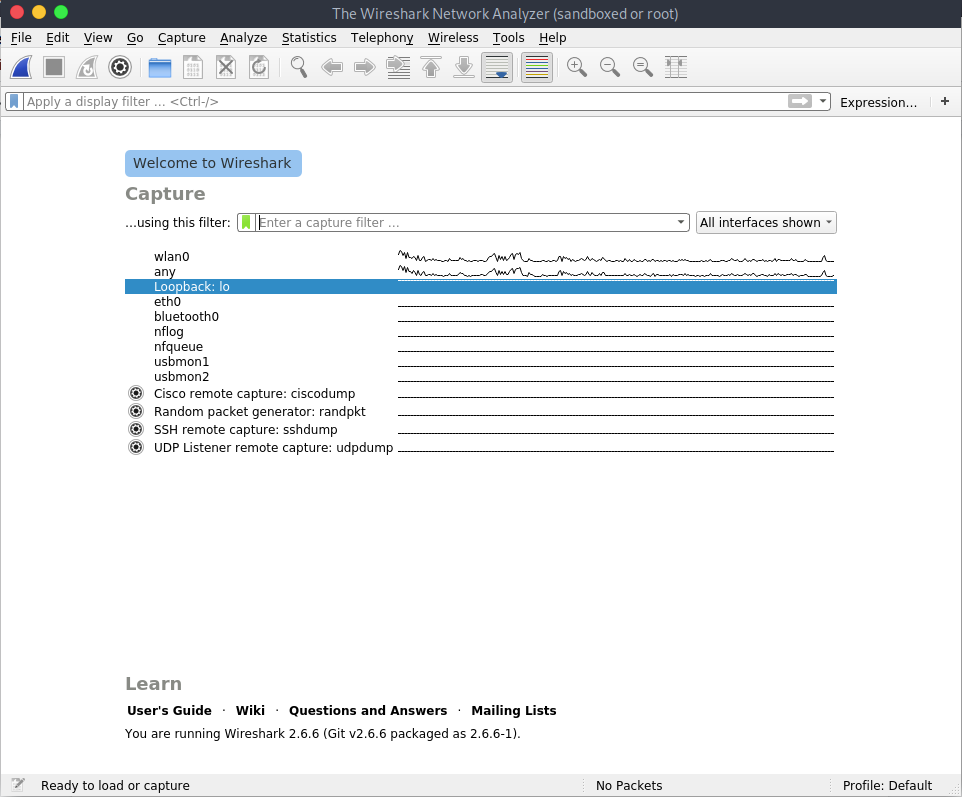
1. Now start the apache service

|  |
| --- |
| $ sudo service apache2 start |

1. Now open this link: <http://127.0.0.1/data.txt>. You will be seeing your content there. Hence the file is successfully hosted.

**Step-2:**

1. Open Wireshark and select loopback:lo option on start.



**Step-3:**

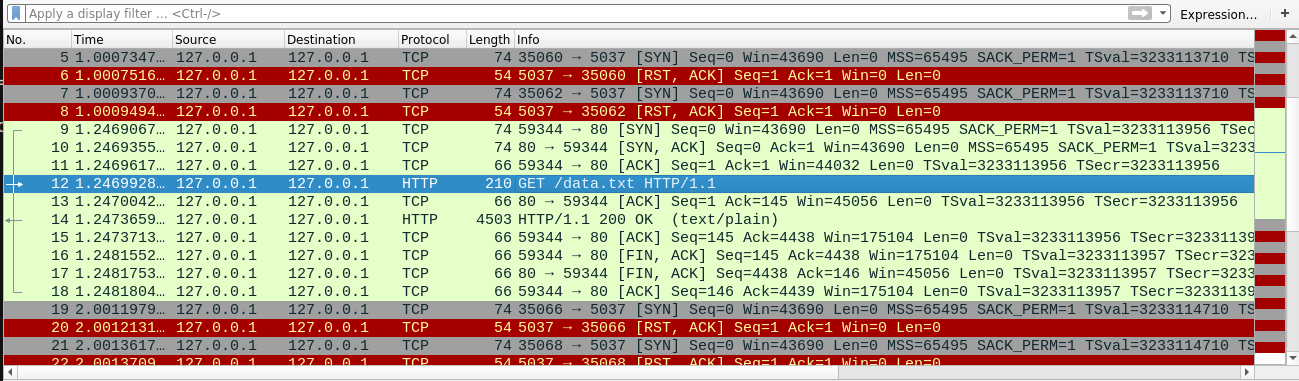
Wget is a computer program that retrieves content from web servers. It is part of the GNU Project. Its name derives from World Wide Web and get. It supports downloading via HTTP, HTTPS, and FTP. Its features include recursive download, conversion of links for offline viewing of local HTML, and support for proxies.

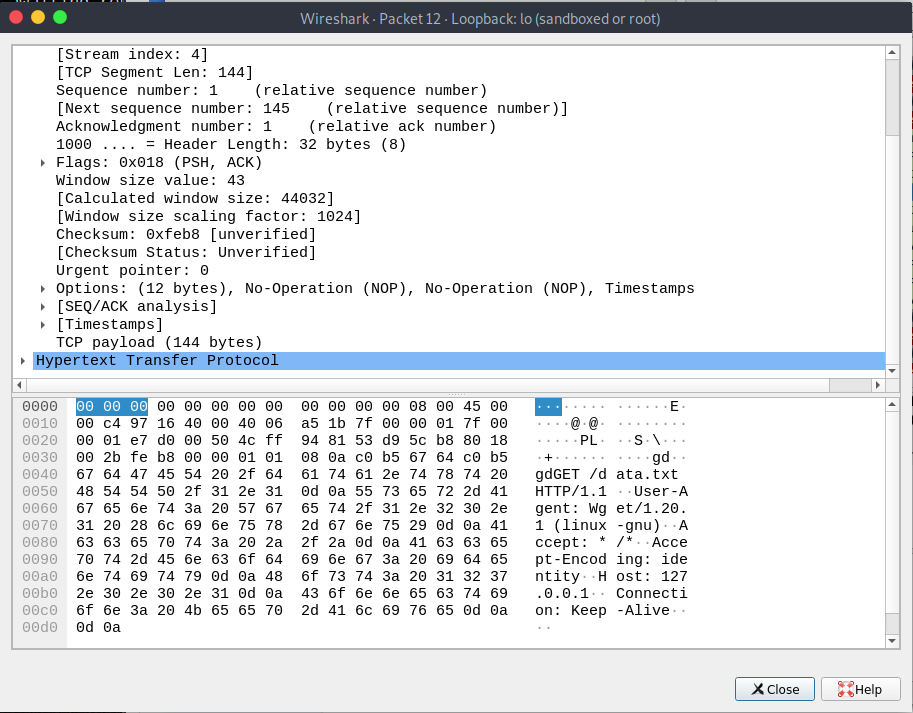
Type this command to request for the file hosted on 127.0.0.1

|  |
| --- |
| $ wget 127.0.0.1/data.txt |

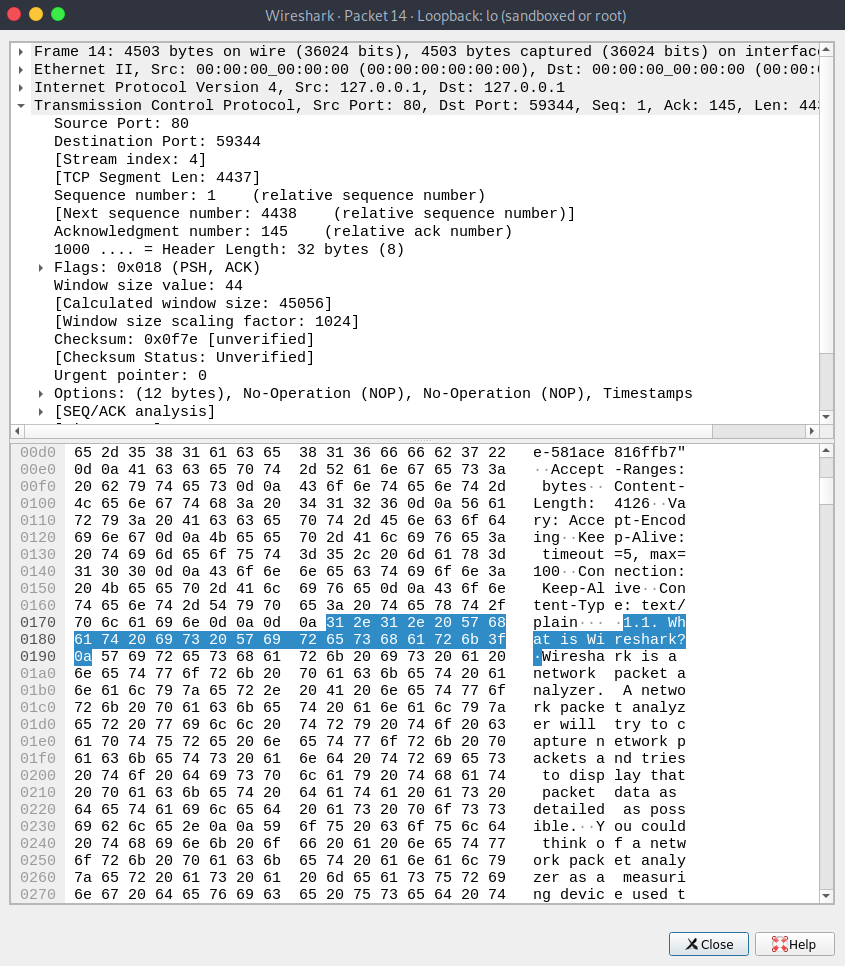
**Step-4:**

See Wireshark now, you will be seeing the packets from your computer requesting localhost for the data.txt file





The text file that is transferred is seen in the following packet



**Funtionalities:**

* Wireshark can capture traffic from many different network media types - and despite its name - including wireless LAN as well. Which media types are supported, depends on many things like the operating system you are using. An overview of the supported media types can be found at https://wiki.wireshark.org/CaptureSetup/NetworkMedia.
* It can open packets captured from a large number of other capture programs.
* When saved, the packets are usually stored in the format of pcap, pcap-ng etc., for offline analysis purposes. The packet data is usually in the Hexadecimal format.

Here are some things Wireshark does not provide:

* Wireshark isn’t an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn’t allowed to do. However, if strange things happen, Wireshark might help you figure out what is really going on.
* Wireshark will not manipulate things on the network, it will only “measure” things from it. Wireshark doesn’t send packets on the network or do other active things (except for name resolutions but even that can be disabled).

**Conclusion:**

Wireshark is a program that is used to capture data packets to allow a more precise analysis. The main focus of this tool is observing the data traffic within a network. This tool is

So powerful that it can be used for bad purposes also.

Signature