Subject: OPEN-SOURCE TECHNOLOGIES (INT-301)

Assignment 3 (Project)

Submitted by

Narala Likhith

Registration No: 11901982

Section: KE016

Roll NO: B35

GitHub Link : https://github.com/Likhith-likky/OpensourceCA3

School of Computer Science & Engineering

Lovely Professional University, Phagwara

Question No: 10

Suppose you are network analyst, working in Infotech department of LPU. You have been assigned the responsibility of inspecting HTTP Traffic and retrieve Username and password from BSNL website, using appropriate tool.

INDEX

Chapter-1

Introduction

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation ina court of law. The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

TYPES Of Forensics:

- **Network Forensics:** It is a sub-branch of Computer Forensics that involves monitoring and analyzing computer network traffic.
- **Disk Forensics:** It deals with extracting raw data from the primary or secondary storage of the device by searching active, modified, or deleted files.
- **Memory Forensics:** Deals with collecting data from system memory (system registers, cache, RAM) in raw form and then analyzing it for further investigation.
- **Malware Forensics:** It deals with the identification of suspicious code and studyingviruses, worms, etc.
- **Database Forensics:** It deals with the study and examination of databases and theirrelated metadata.
- **Email Forensics:** It deals with emails and their recovery and analysis, includingdeleted emails, calendars, and contacts.
- **Mobile Phone Forensics:** It deals with the examination and analysis of phones and smartphones and helps to retrieve contacts, call logs, incoming, and outgoing SMS,etc., and other data present in it. The project that I am doing is under Network Forensics and we will study it now.

My question is comes Under Network Forensic

Network forensics:

Network forensics is the process of analyzing and investigating network traffic to gather information about security incidents or any violations, or events that have occurred on a computer network. This involves capturing data packets and analyzing, logs, and other network traffic to determine the nature of an attack and to what extent an attack happened, and to identify the source of the problem. It can help organizations to understand how a security breach occurredand what data was compromised, and how to prevent similar incidents from happening in the future. It is the main component of computer and network security and is used by law enforcement agencies, businesses, and other organizations to investigate and solve crimes and other security incidents that have happened. Law enforcement will use network forensics to analyze network traffic data harvested from a network suspected of being used in criminal activity or a cyber-attack. Analysts will search for data that points towards human communication, manipulation of files, and the use of certain keywords. Unlike digital forensics, network forensics is more difficult to carry out as data is often transmitted across the network and then lost; in computer forensics data is more often kept in disk or solid-state storage making it easier to obtain.

1.1 OBJECTIVE OF THE PROJECT :

The objective of the project is to inspecting HTTP Traffic and retrieve Username and password from website, using appropriate tool. The objective of the project is also to gain insight into the network's and identify the network Traffic.

1.2 DESCRIPTION OF THE PROJECT

This project involves Inspecting HTTP traffic and retrieve username password from a website involves capturing and analyzing data transmitted between a client (such as a web browser) and a web server using the Hypertext Transfer Protocol (HTTP). To perform this task, specialized software tools are often used that can capture, decode, and analyze network packets.

One example of a tool that can be used for inspecting HTTP traffic and retrieve Username and password from a website is Wireshark. Wireshark is a free, open-source network protocol analyzer that allows users to capture and analyze traffic on a network. Wireshark can capture and decode HTTP traffic and provide detailed information about the data being transmitted, including the source and destination IP addresses, the type of request being made (e.g. GET, POST), headers, cookies, and any form data submitted by the user. By using Wireshark we can retrieve Username and password from a website.

1.3 SCOPE OF THE PROJECT :

The scope for inspecting HTTP traffic and retrieve username and password from a website depends on the specific goals and objectives of the analysis. HTTP traffic inspection can provide valuable insights into the behavior of web applications and services, and can be used to troubleshoot issues, monitor for security threats, optimize website performance, and analyze user behavior. Some examples of the scope of HTTP traffic inspection are:

- **Troubleshooting:** HTTP traffic inspection can be used to diagnose network connectivity issues, server configuration issues, or software compatibility issues. By analyzing HTTP traffic, it is possible to identify errors or anomalies in the network traffic that may be causing issues.
- **Security analysis:** HTTP traffic inspection can be used to identify potential security vulnerabilities, such as unencrypted transmission of sensitive data, injection attacks, or the presence of malicious code. By analyzing HTTP traffic, it is possible to identify potential security risks and take appropriate actions to mitigate those risks.

Performance optimization: HTTP traffic inspection can be used to optimize website performance by identifying bottlenecks or areas of slow performance. By analyzing

CHAPTER-2
SYSTEM AND SOFTWARE DESCRIPTION

2.1 TARGET SYSTEM DESCRIPTION:

To capture HTTP traffic of the network and retrieve Username and the password. the target system must have a network interface card that is capable of capturing network traffic. The target system must have software installed that can capture and analyze network traffic and also retrieve the username and password from the website. In addition, the target system must also have sufficient system resources, including System wifi, memory and storage to capture HTTP traffic and retrieve username and password from website.

2.2 ASSUMPTIONS AND DEPENDENCIES:

There are several assumptions and dependencies that you need to consider. These include that you need to have access to the HTTP network and retrieve there username and password using the software, a compatible network interface, sufficient system resources, proper configuration of the software, knowledge of networking protocols and tools,and the time and expertise to carry out the process.

2.3 FUNCTIONAL/NON-FUNCTIONAL DEPENDENCIES:

Functional dependencies are those that relate to the features and capabilities of the open-source software you plan to use. Some of them are Compatibility with the network interface, Support for the network protocols, Ability to filter traffic, Ease of use. Non-functional dependencies are those that relate to the operational and performance requirements of the open-source software. Some non-functional dependencies to consider include System requirements, Performance and scalability, Security, Support and community.

2.4 SOFTWARE DESCRIPTION / SOFTWARE USED:

WIRESHARK

Wireshark is a network protocol analyzer, or an application that captures packets from a networkconnection, such as from your computer to your home office or the internet. Packet is the name given to a discrete unit of data in a typical Ethernet network. Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

- **Packet Capturing:** Wireshark listens to a network connection in real time and then grabs entirestreams of traffic – quite possibly tens of thousands of packets at a time.
- **Filtering Information:** Wireshark is capable of slicing and dicing all this random live datausing filters. By applying a filter, you can obtain just the information you need to see.
- **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the verymiddle of a network packet. It also allows you to visualize entire conversations and network streams.

CHAPTER-3
ANALYSIS REPORT

3.1 SYSTEM SNAPSHOTS AND REPORT:

In this project we will use wireshark software. We will go through the steps of using Wireshark to capture HTTP traffic retrieve username and password from the website.

Installing and Configuring Wireshark:

The first step to install wireshark from the website https://www.wireshark.org/download.html

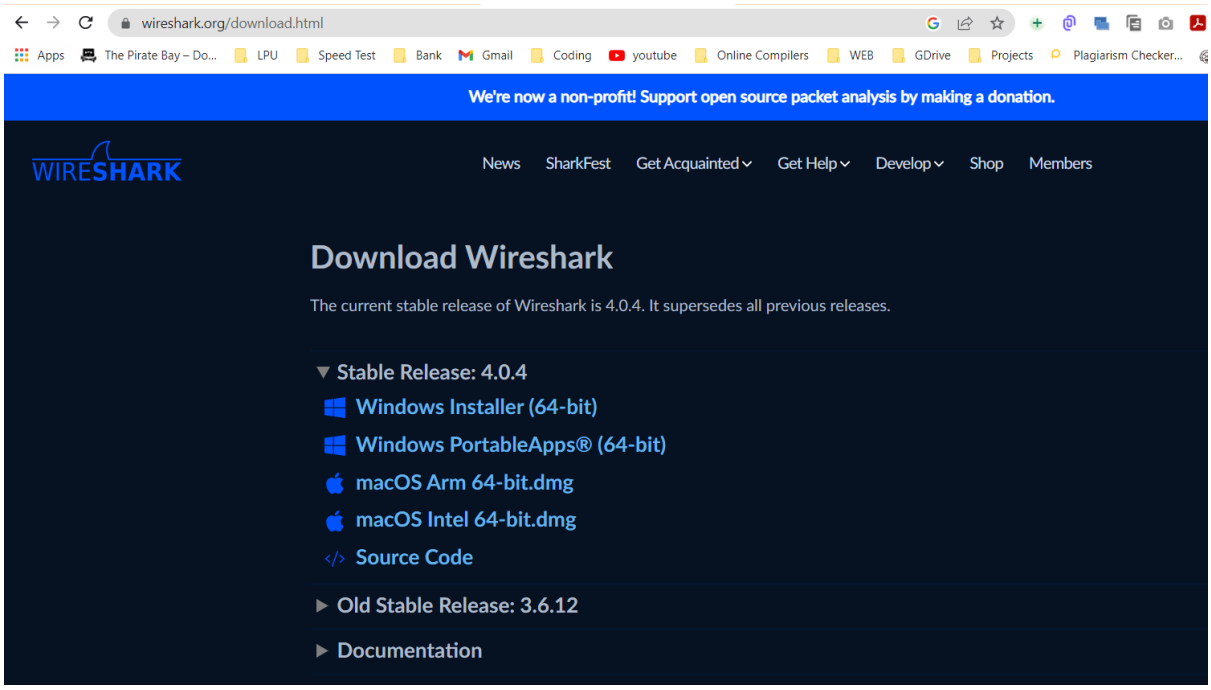


Fig 3.1 Different stable releases of software for different operating systems.

Retrive Username and password from HTTP Website

First open wireshark software

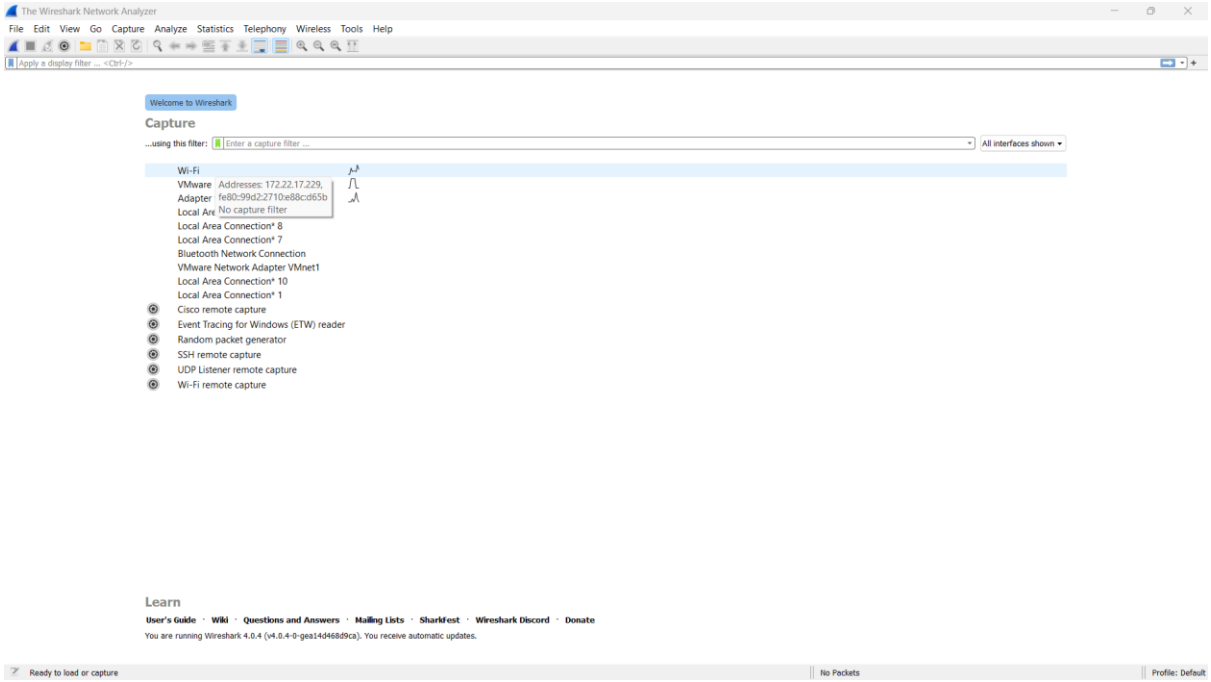


Fig 3.2 wireshark interface

Select wifi option and press capture

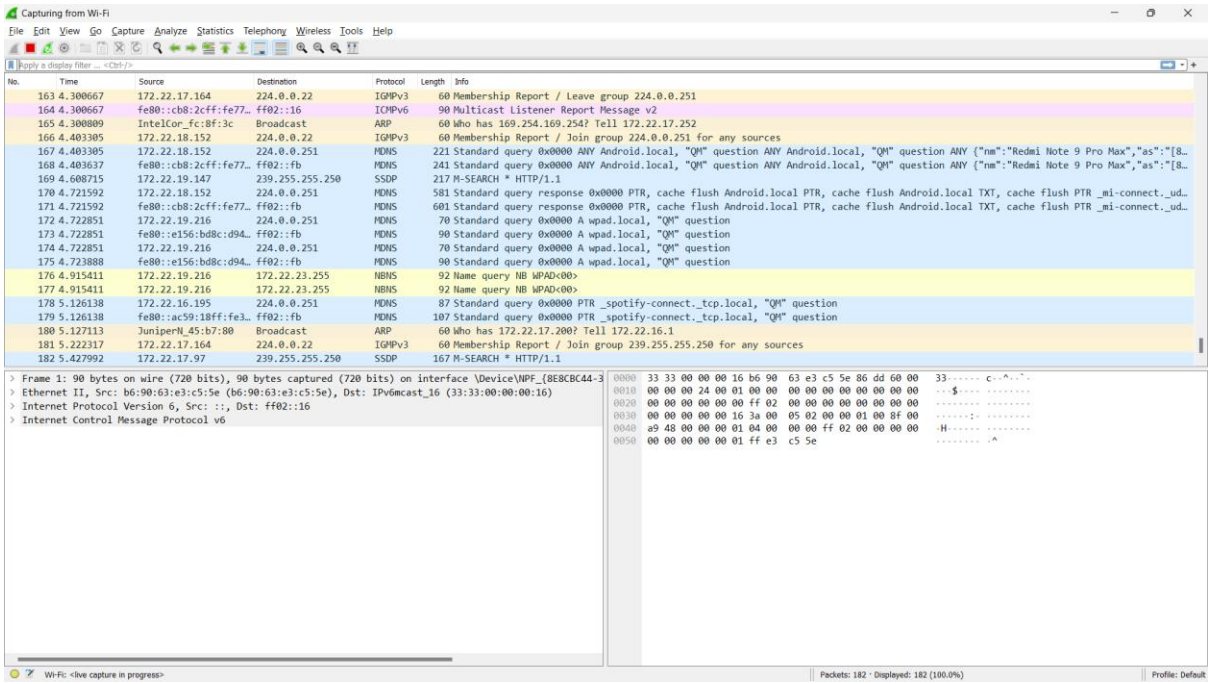


Fig 3.3 Stated wireshark

Open Browser and serach for HTTP login Websites and select a random http login website

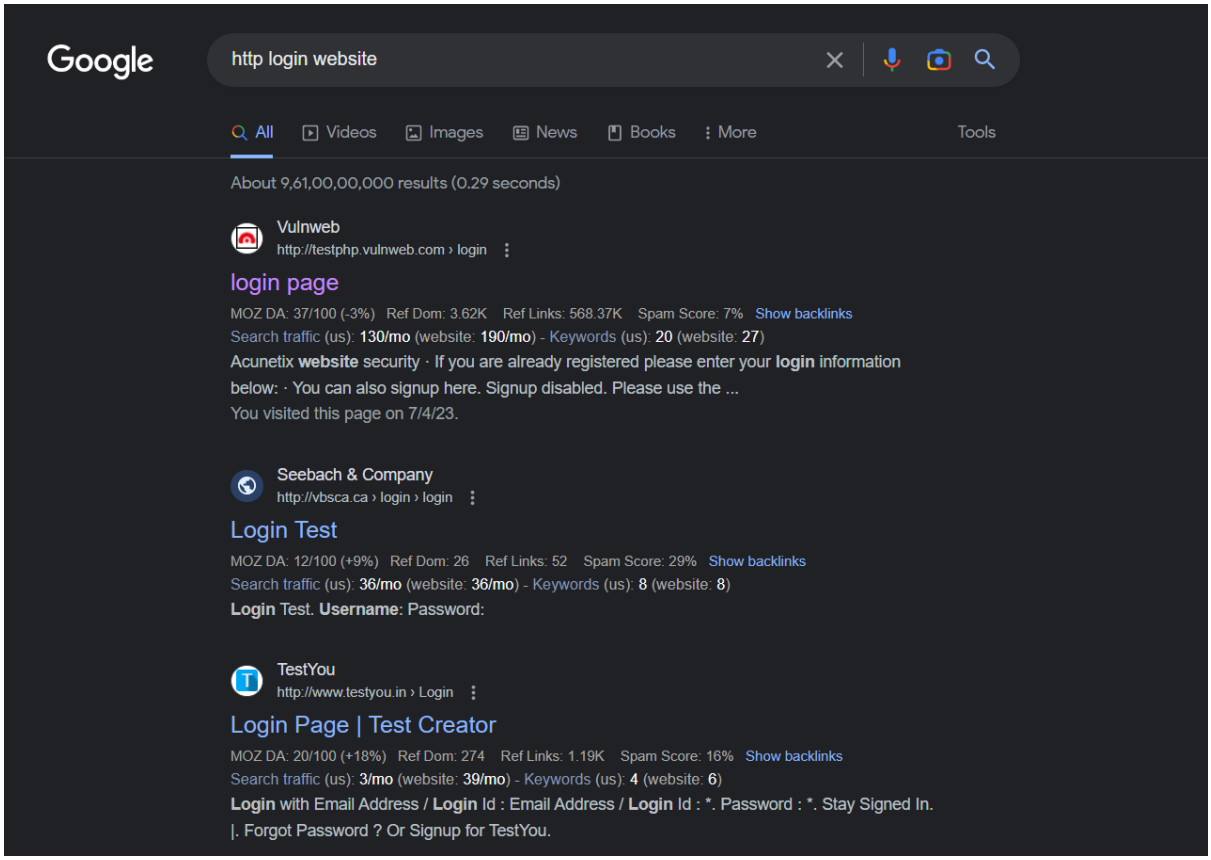
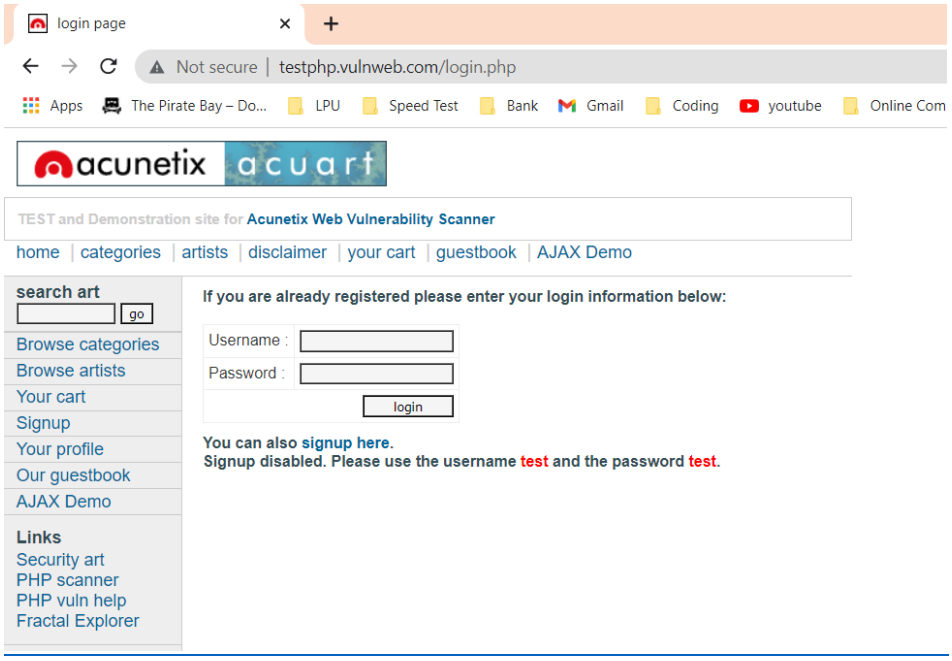


Fig 3.4 seraching for HTTP Website

Select any website you need to capture username and password

Website Link : http://testphp.vulnweb.com/login.php



Enter Username and password in the website

I have entered

Username : Likhith

Password: Likhith123

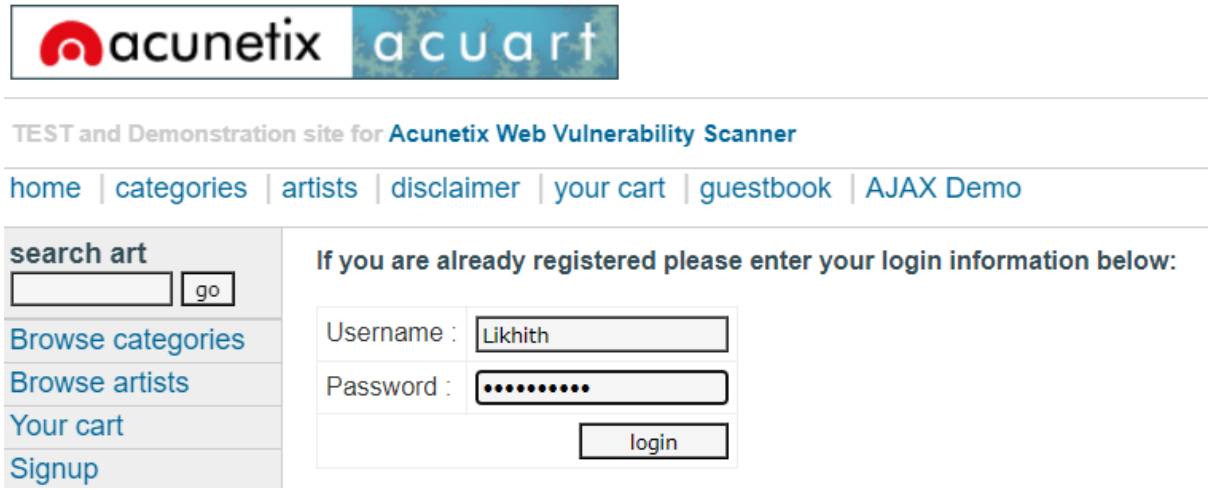


Fig 3.5 Entering username and password in the website

After entering click on login

Stop the wireshark:

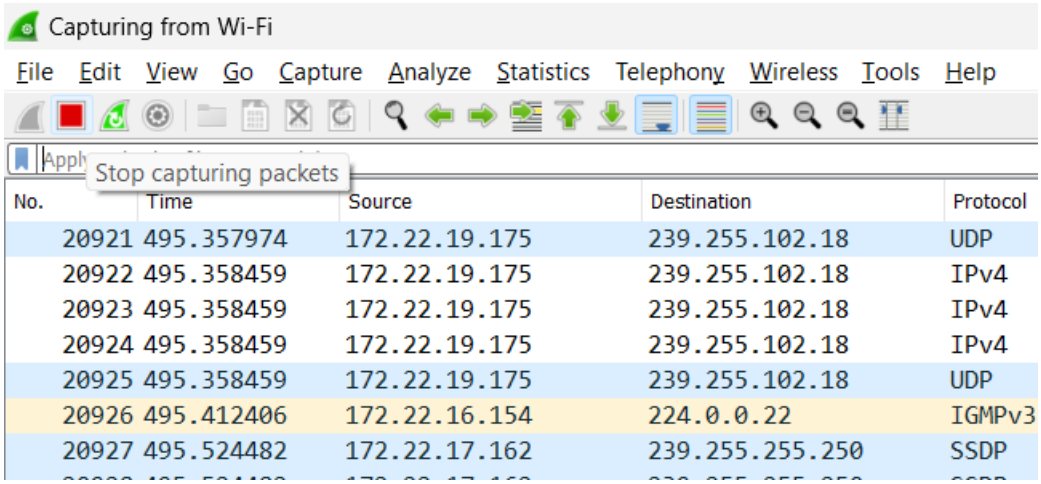


Fig 3.6 stoping wireshark

Type HTTP in the given Field

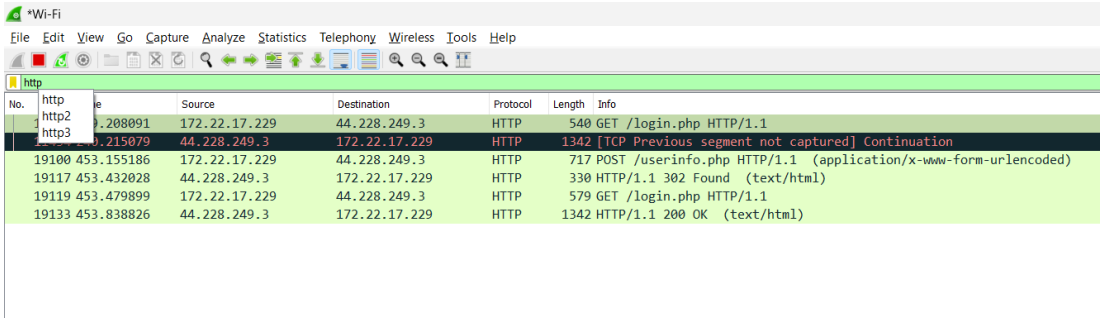


Fig 3.7 search for HTTP

Follow this Path : Follow-> HTTP Stream

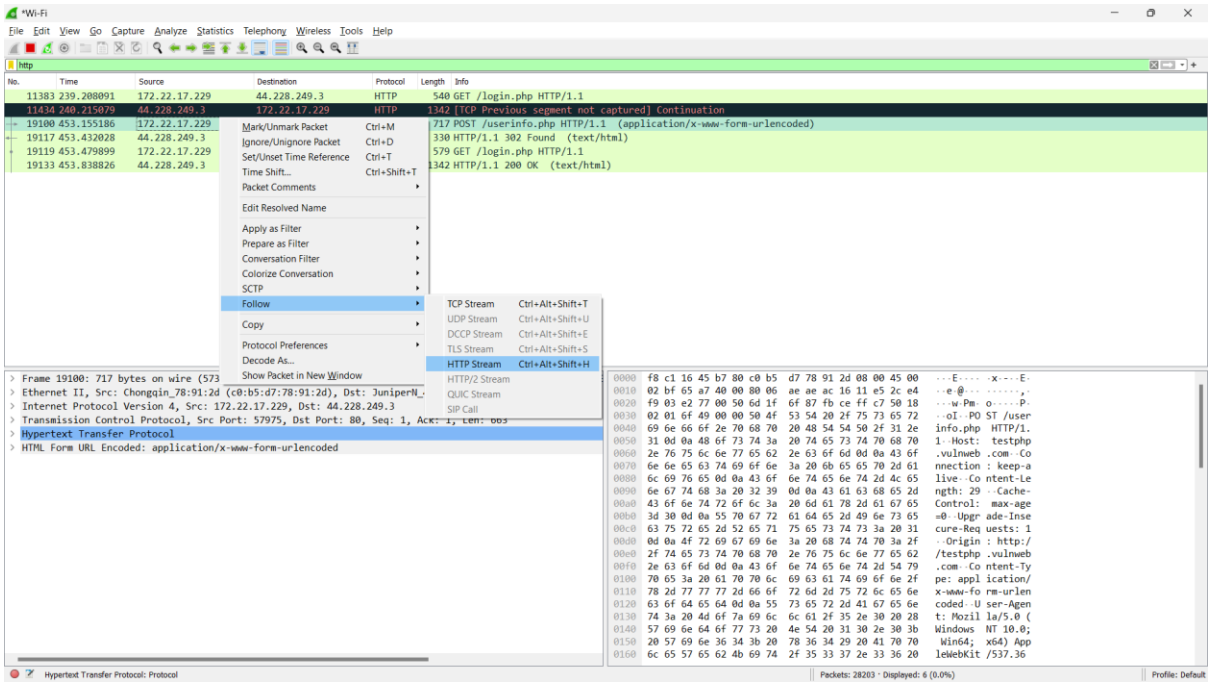


Fig 3.8 Steps for finding username and password

```
exchange;v=b3;q=0.7
Referer: http://testphp.vulnweb.com/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,te;q=0.8

uname=Likhith&pass=Likhith123HTTP/1.1 302 Found
Server: nginx/1.19.0
Date: Sat, 08 Apr 2023 18:06:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
Location: login.php
```

Fig 3.9 Showing Username and password

CHAPTER-4

CONCLUSION

In conclusion, capturing Username and password from HTTP traffic using open-source software can be useful for network administrators and security professionals. With the right tools and expertise, it is possible to gain insights into network traffic patterns, identify security threats, and optimize network performance. However, it is efficient to consider the assumptions, functional dependencies, and non-functional dependencies when working on such a project. Wireshark is anessential tool for network traffic analysis. It allows you to capture and analyze network traffic in real-time and troubleshoot network problems. In this report, we discussed the steps of using Wireshark to capture and analyze network traffic on your system. I hope this report has provided you with a good understanding how to retrieve username and password from http website using Wireshark.

REFERENCES :

[1] https://www.techtarget.com/searchsecurity/definition/computer-forensics

[2] https://www.geeksforgeeks.org/introduction-of-computer-forensics/

[3] https://www.cybrary.it/blog/0p3n/introduction-to-computer-forensics/