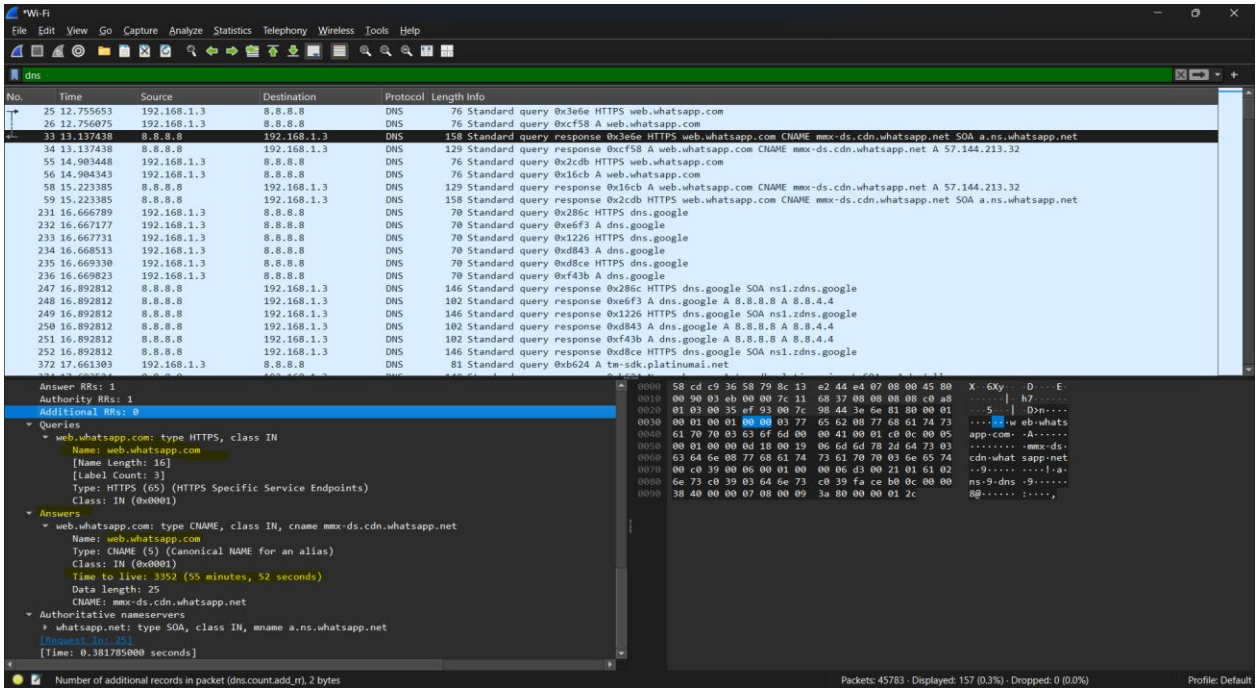
Traffic Analysis

Protocols:

Protocol is a set of rules which is used for communicating with two devices like computers, mobile ,..etc. Which devices are connected within a same network can communicate with each other using protocols.

IP (Internet Protocol) - A unique identifier number series used for communicate with other devices.
MAC (Media Access Control)-An unchangeable unique identifier for each device.
DNS (Domain Naming System)-Converts system understanding IP address to human understanding names.
TCP (Transfer Control Protocol)- Used for data transfer (reliable).
UDP (User Datagram Protocol)- Used for data transfer (unreliable).

DNS Traffic:



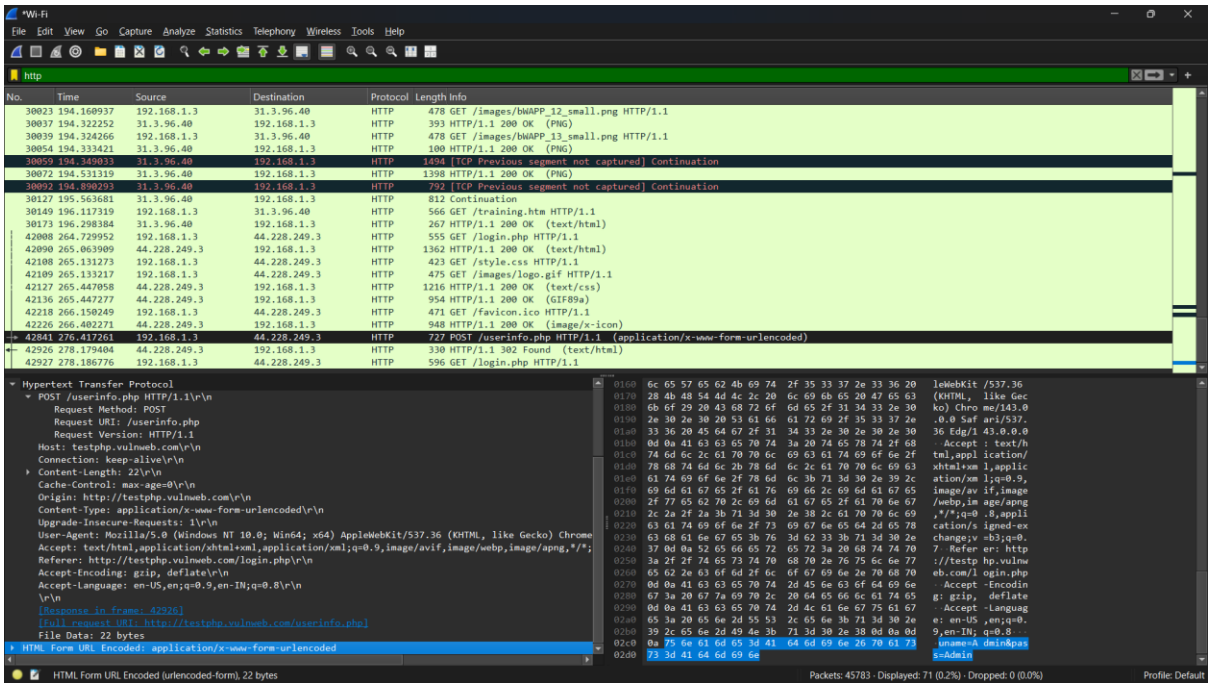
Own device-192.168.1.3

DNS Server-8.8.8.8

192.168.1.3 request for a website's IP to 8.8.8.8

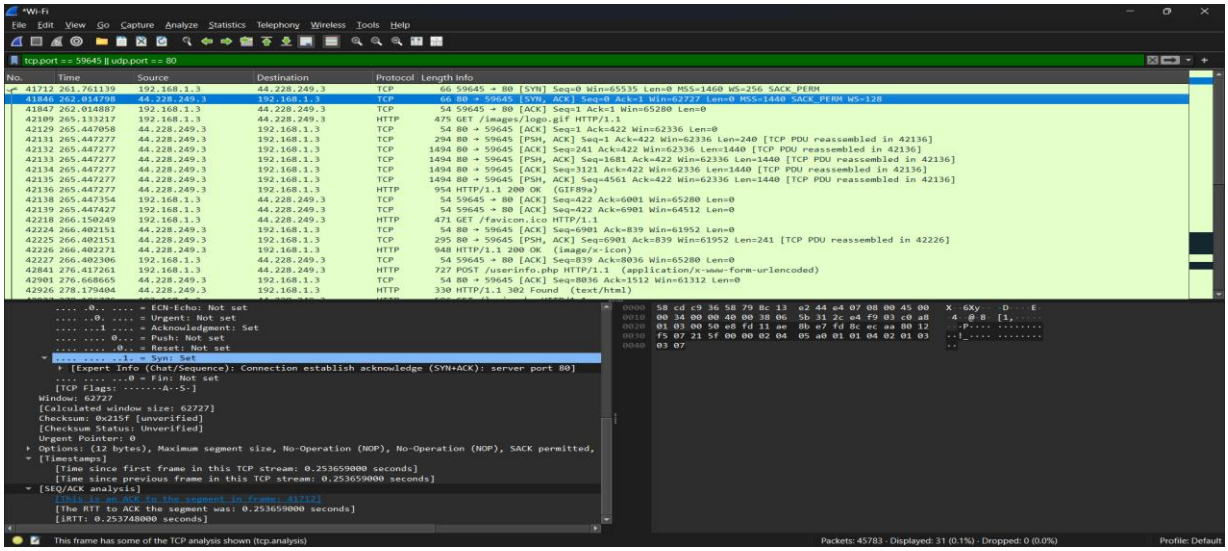
8.8.8.8 responded for the request from 192.168.13

HTTP Traffic:



HTTP stands for Hyper Text Transfer Protocol. It used for share html pages (Website). In this event, the user logged in the website named "vulnweb.com".

TCP Traffic:

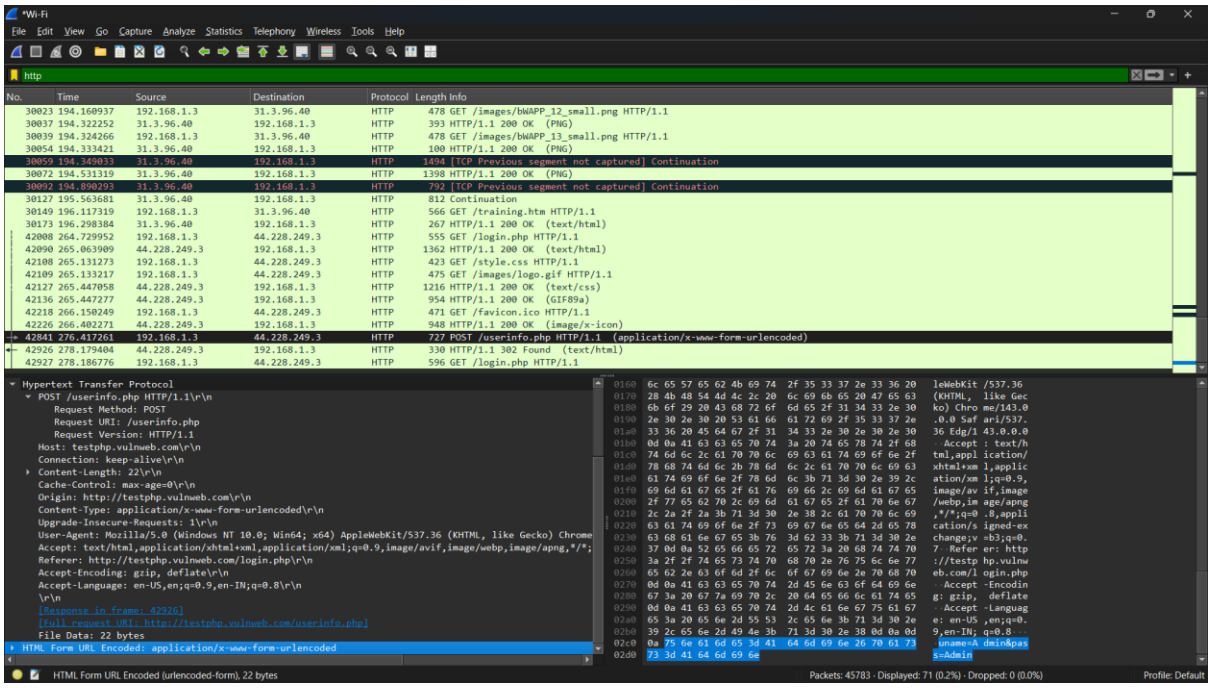


TCP is used for transfer data. In this event, the user device transferred data using port 80. The responder device (44.228.243.3) received the data using its port 59645. Port 80 was used for http protocol. So it might be a webpage activity.

Encrypted vs Plain data:

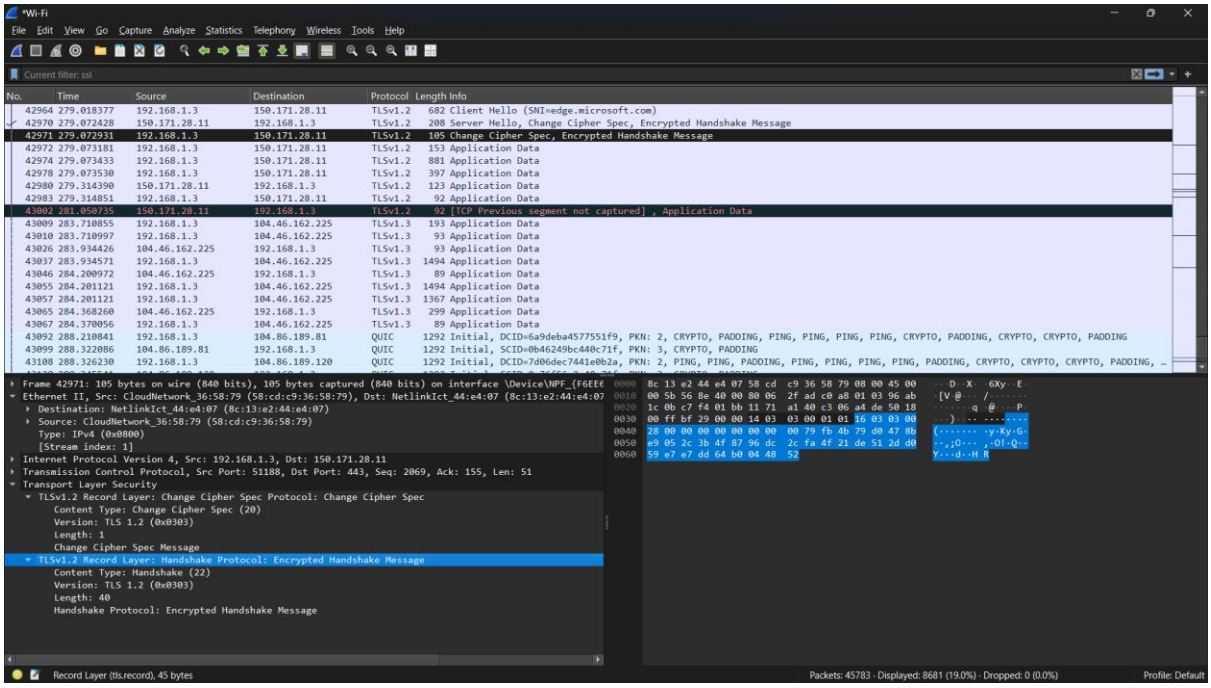
Encrypted Text	Plain Text
Hard to read it.	Easily read the data.
Non-vulnerable for man-in-middle attacks.	Vulnerable for man-in-middle attacks.
Data exposing might be difficult.	Data are exposed easily.
Most secured.	Unsecured

Plain Text:



Login credentials are exposed- Username: Admin, Password: Admin

Encrypted Text:



Login credentials are encrypted. We need to do some more works to find it.