**NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY**

**(AN AUTONOMOUS INSTITUTION, AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM, APPROVED BY AICTE & GOVT.OF KARNATAKA**

**Logo

Description automatically generated**

**LA-2 REPORT**

**on**

**DIGITAL INVESTIGATION**

***Submitted in partial fulfilment of the requirement for the award of Degree of***

***Bachelor of Engineering***

***in***

***Computer Science and Engineering***

***Submitted by:***

|  |  |
| --- | --- |
| **V VENKATA SREE HARSHA**  **SHUBHAM SINGH** | **1NT18CS181**  **1NT18CS157** |
|  |  |
|  |  |

**Under the Guidance of**

**MRS IMPANA**

**Associate Professor, Dept. of CS&E, NMIT**

****

**Department of Computer Science and Engineering**

**(Accredited by NBA Tier-1)**

**2020-21**

**NITTE MEENAKSHI INSTITUTE OF TECHNOLOGY**

**(AN AUTONOMOUS INSTITUTION, AFFILIATED TO VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM**

**, APPROVED BY AICTE & GOVT.OF KARNATAKA)**

**Department of Computer Science and Engineering**

**(Accredited by NBA Tier-1)**

**Logo

Description automatically generated**

**CERTIFICATE**

This is to certify that the Phase 2 Report on Digital Investigation is an authentic work carried out by V Venkata Sree Harsha (1NT18CS181), Shubham Singh (1NT18CS157) bonafide students of Nitte Meenakshi Institute of Technology, Bangalore in partial fulfilment for the award of the degree of *Bachelor of Engineering* in COMPUTER SCIENCE AND ENGINEERING of Visvesvaraya Technological University, Belagavi during the academic year *2020-2021.* It is certified that all corrections and suggestions indicated during the internal assessment has been incorporated in the report.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Internal Guide** | | **Signature of the HOD** | | **Signature of Principal** | |
|  | |  | |  | |
| **Mrs. Impana**  **Associate Professor, Dept. CSE,**  **NMIT Bangalore** | | **Dr. SarojaDevi**  **Professor, Head, Dept. CSE, NMIT Bangalore** | | **Dr. H. C. Nagaraj**  **Principal,**  **NMIT, Bangalore** | |
| **Signature of Examiners** | | | |
|  | |  | |
|  | |  | |
|  | |  | |

**DECLARATION**

We are hereby declare that

(i) The project work is our original work

(ii) This Project work has not been submitted for the award of any degree or examination at any other university/College/Institute.

(iii) This Project Work does not contain other persons’ data, pictures, graphs or other information, unless specifically acknowledged as being sourced from other persons.

(iv) This Project Work does not contain other persons’ writing, unless specifically acknowledged as being sourced from other researchers. Where other written sources have been quoted, then:

a) their words have been re-written but the general information attributed to them has been referenced;

b) where their exact words have been used, their writing has been placed inside quotation marks, and referenced.

(v) This Project Work does not contain text, graphics or tables copied and pasted from the Internet, unless specifically acknowledged, and the source being detailed in the thesis and in the References sections.

|  |  |  |
| --- | --- | --- |
| NAME | USN | Signature |
| V VENKATA SREE HARSHA | 1NT18CS181 | Text, letter  Description automatically generated |
| SHUBHAM SINGH | 1NT18CS157 | SHUBHAM SINGH |

Date: 06/01/2022

**ACKNOWLEDGEMENT**

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible, whose constant guidance and encouragement crowned our effort with success. I express my sincere gratitude to our Principal Dr. H. C. Nagaraj, Nitte Meenakshi Institute of Technology for providing facilities.

We wish to thank our HoD, Dr. Sarojadevi for the excellent environment created to further educational growth in our college. We also thank him for the invaluable guidance provided which has helped in the creation of a better project.

I hereby like to thank our *Mrs. Impana , Associate Professor*, Department of Computer Science & Engineering on her periodic inspection, time to time evaluation of the project and help to bring the project to the present form.

Thanks to our Departmental Project coordinators. We also thank all our friends, teaching and non-teaching staff at NMIT, Bangalore, for all the direct and indirect help provided in the completion of the project.

|  |  |  |
| --- | --- | --- |
| NAME | USN | Signature |
| V VENKATA SHREE HARSHA | 1NT18CS181 | Text, letter  Description automatically generated |
| SHUBHAM SINGH | 1NT18CS157 | SHUBHAM SINGH |

Date: 06/01/2022

**DIGITAL INVESTIGATION**

A digital investigation is **a process to answer questions about digital states and events**. The basic digital investigation process frequently occurs by all computer users when they, for example, search for a file on their computer.

**Some of the main types include the following:**

* Database forensics.
* Email forensics.
* Malware forensics.
* Memory forensics.
* Mobile forensics.
* Network forensics.

**Introduction**

A Digital Investigation means which we will check all types of malwares or any type of data which will be encrypted behind any type of file.

Here We are Investigating a packet to analyse whether that packet is having any types of images. And also, we will be checking the multiple images will be in unreadable format.

And We will be considering that unreadable format as RAW Format and we will be using a Editor to understand that data and we will be extracting the data.

**Tools Used Here**

* Wireshark
* HXD Editor
* Text Editor

**Wireshark:**

Wireshark is a network protocol analyser, or **an application that captures packets from a network connection**, 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.

* Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
* Live data can be read from different types of networks, including Ethernet, IEEE 802.11, [PPP](https://en.wikipedia.org/wiki/Point-to-Point_Protocol), and loopback.
* Captured network data can be browsed via a GUI, or via the terminal version of the utility, TShark.
* Captured files can be programmatically edited or converted via command-line switches to the "edit cap" program.
* Data display can be refined using a display filter.
* Plug-ins can be created for dissecting new protocols.
* VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
* Raw USB traffic can be captured.
* Wireless connections can also be filtered as long as they traverse the monitored Ethernet.
* Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

**HXD Editor:**

**HxD** is a hex editor, disk editor, and memory editor, and it can open files larger than 4 GiB and open and edit the raw contents of disk drives, as well as display and edit the memory used by running processes. Among other features, it can calculate various checksums, compare files, or shred files.

 Disk editor

 Data inspector

* Converts current data into many types, for editing and viewing
* Open-source plugin-framework to extend with new, custom type converters

 Multiple files are presented using a mixture of tabbed document interface and multiple document interface.

 Large files up to 8 EiB can be loaded and edited.

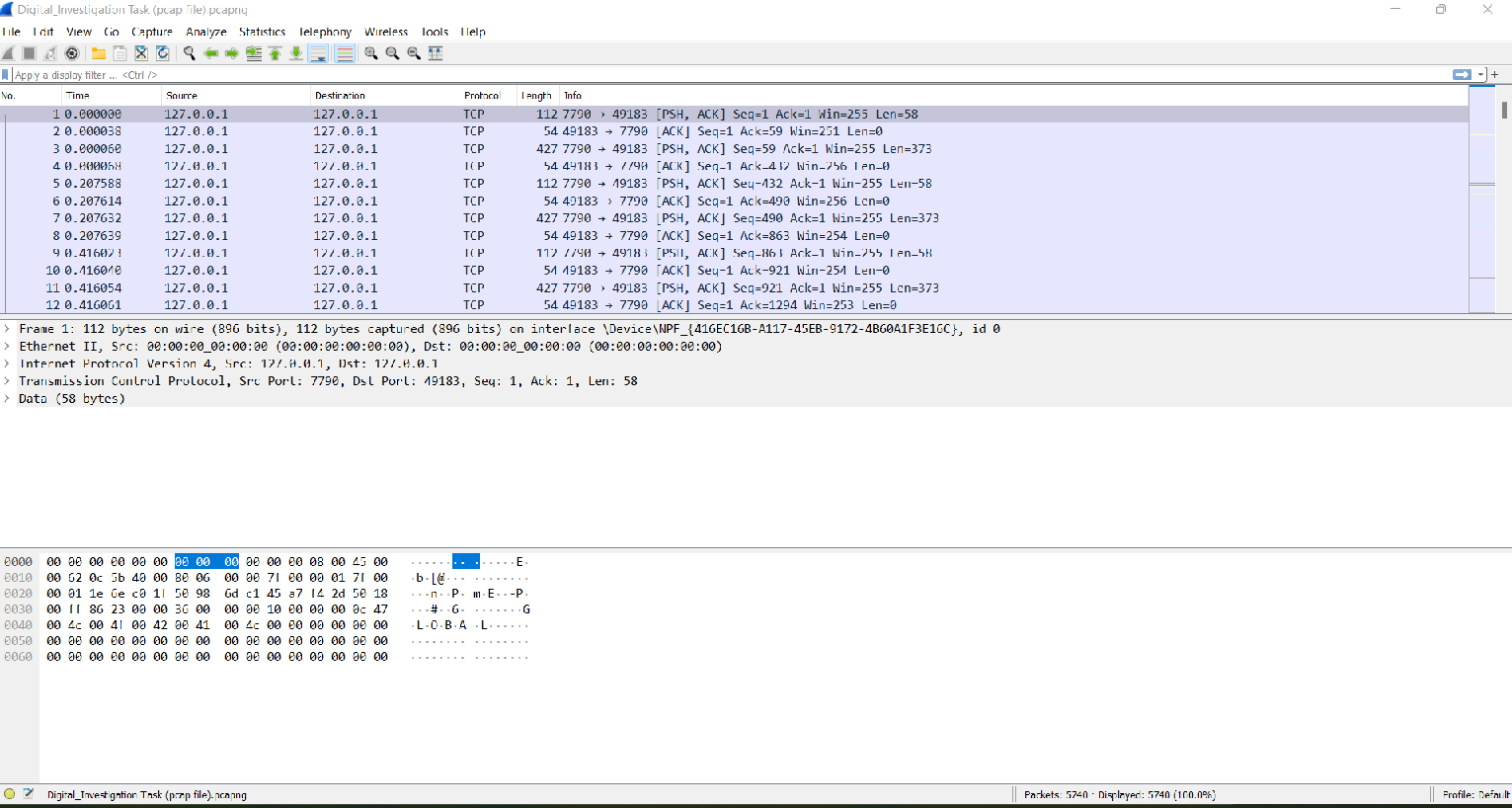
 Partial file loading for performance.

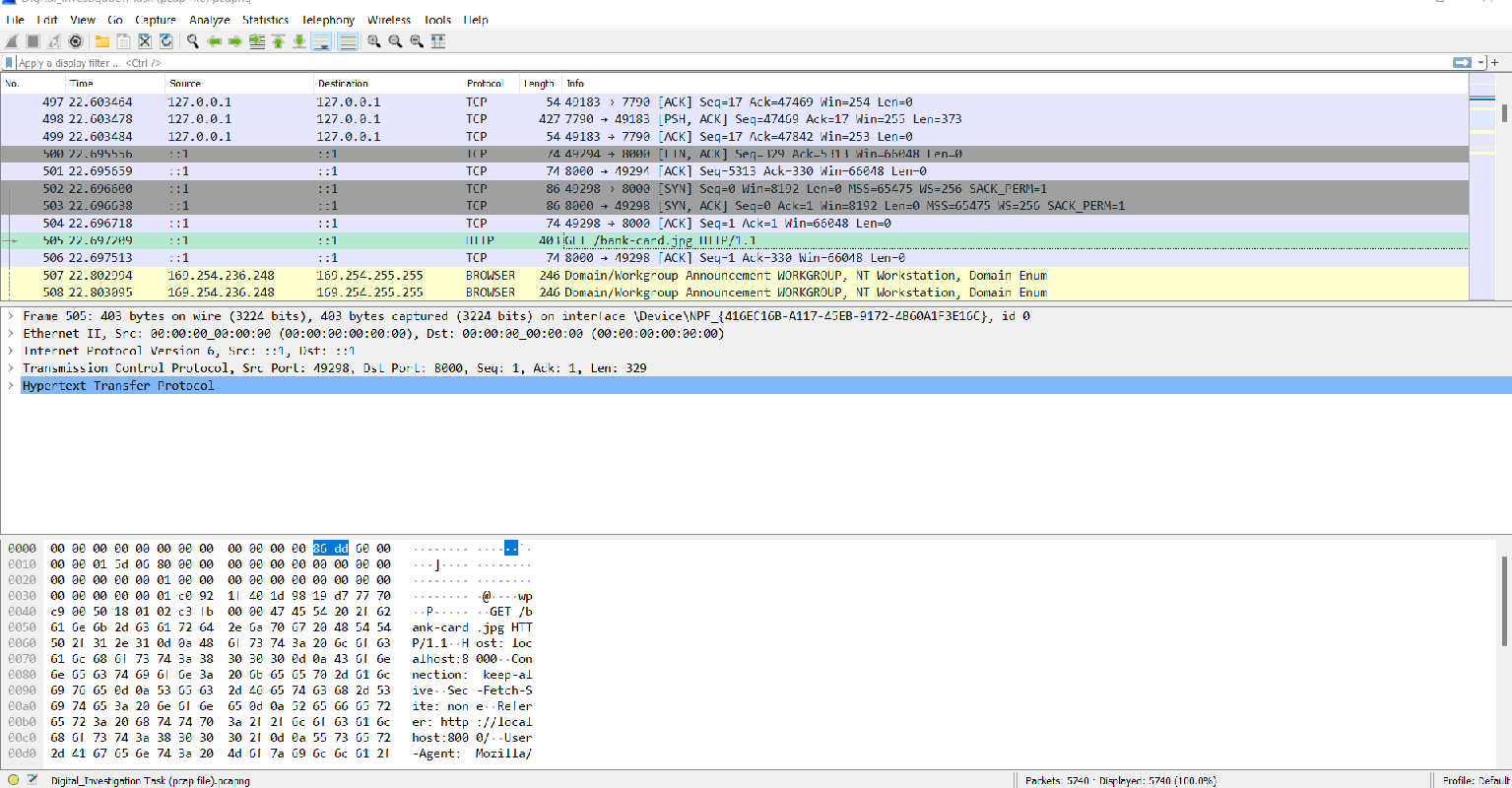
 Search and replace for several data types (including Unicode-strings, floats and integers).

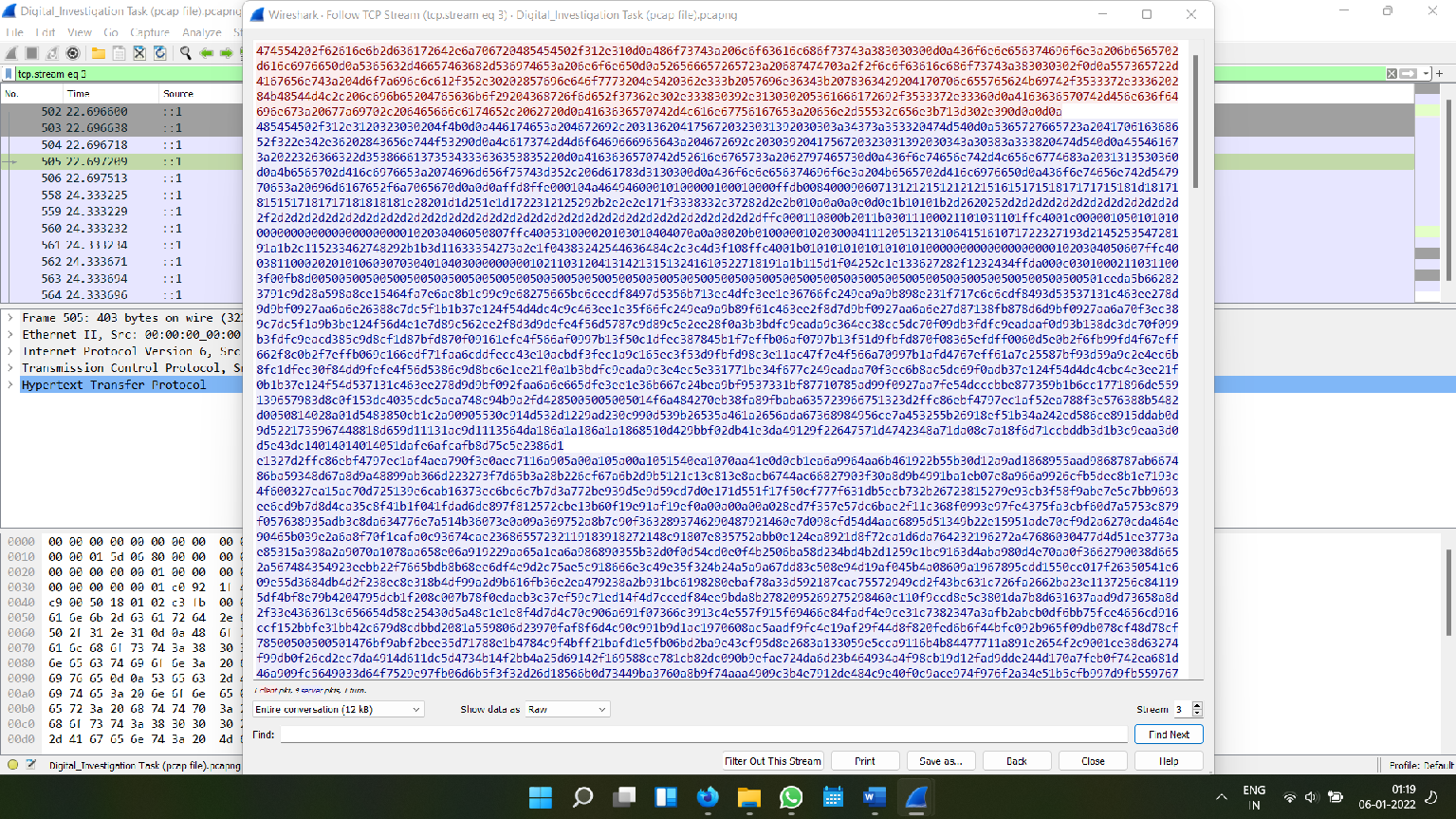
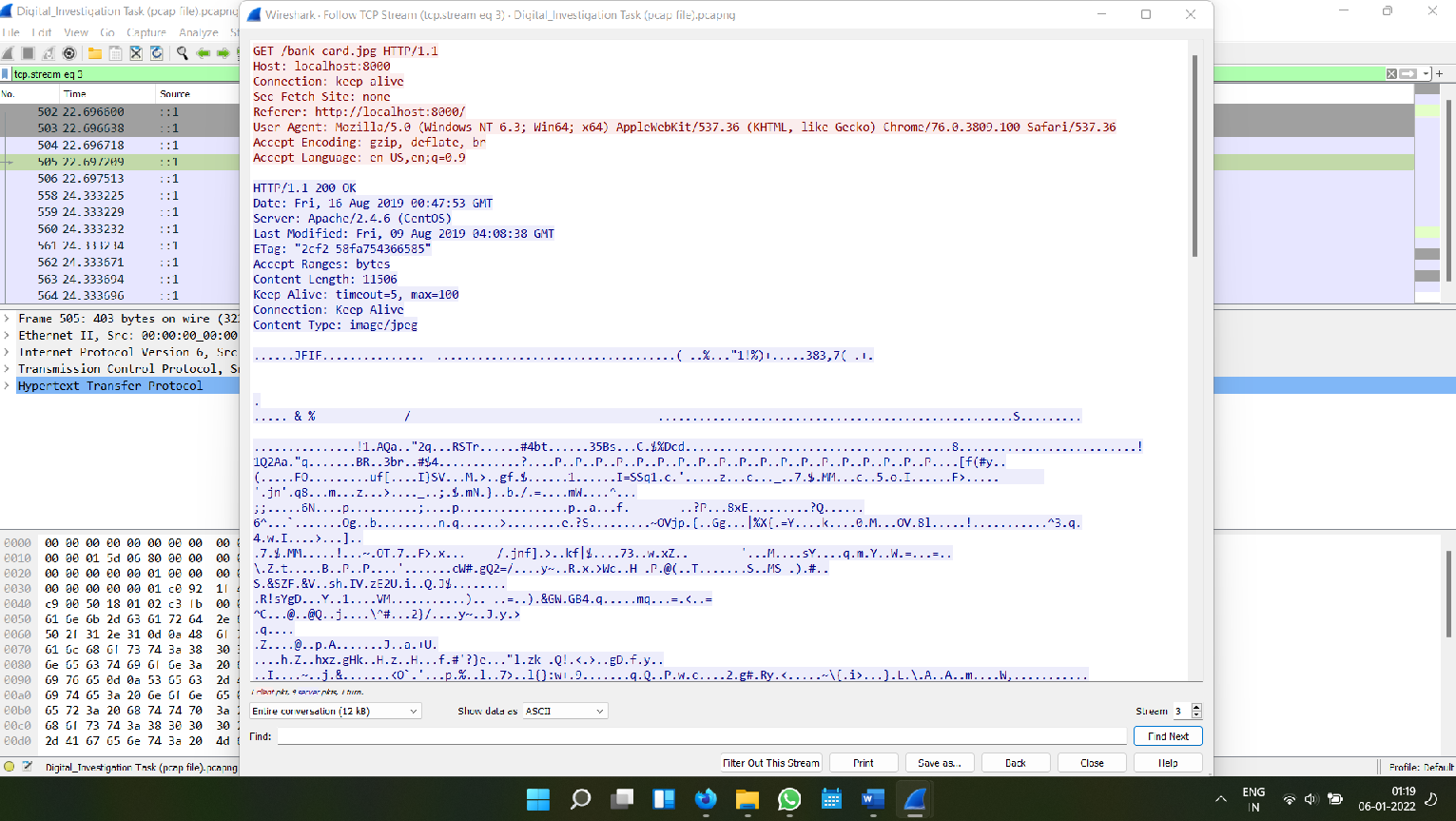
**Working:**

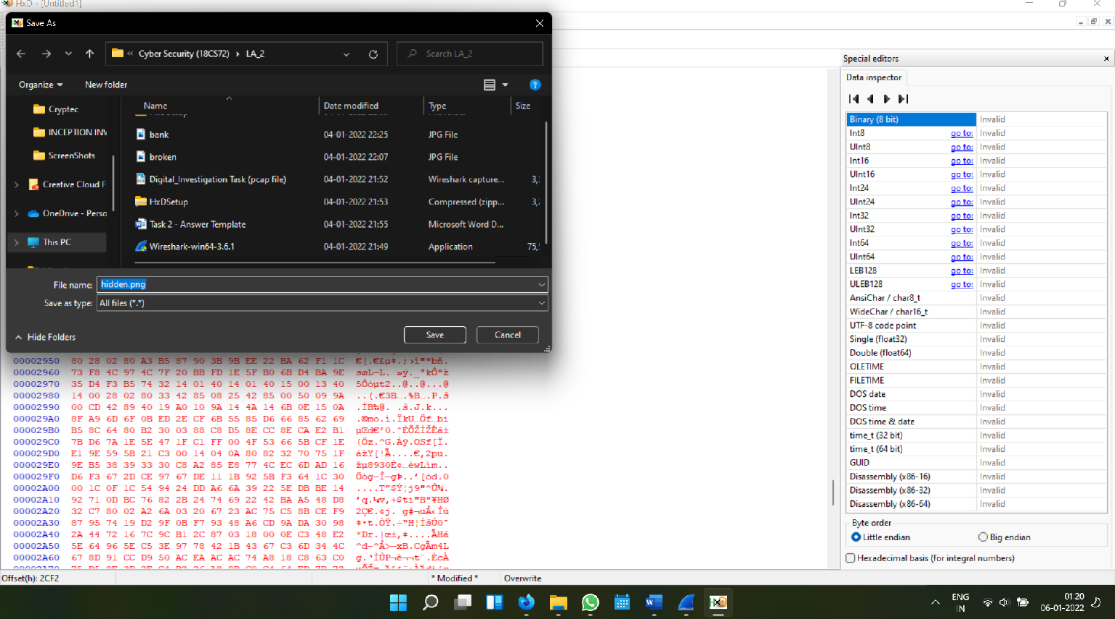
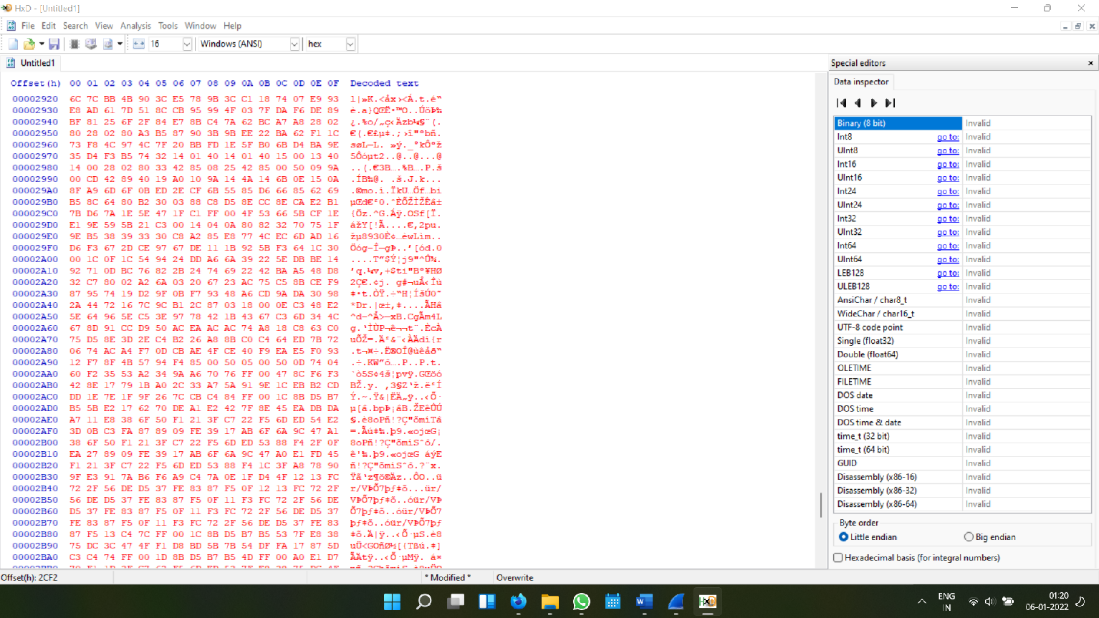
Firstly, we will be having a pcap file which we got from the network. Here we need to find the images which is behind the pcap file and we have to do digital investigation on this pcap file. So, this pcap file will be sending to the Wireshark tool. After sending to the Wireshark tool, it will be analysing the pcap file and it will be showing so many channels. And in these we need to search for the channel which is having .JPG Format because images are basically in .JPG Format. So after finding the .JPG channels we need to send to TCP Stream and after sending to the TCP Stream we will be having in the ASCII Format. And this ASCII Format must be changed to the RAW Format after converting this into RAW Format we need to copy the RAW Format from “ffd8” to “ffd9” because it is the encoding format of the images. So, we can use search tool to copy the ffd8 to ffd9. After copying the encoding text, we need to copy that and we need to open HxD Editor and create a new file and in that we need to paste that Encoding format data into this HxD Editor. After pasting we need to save the file by “image.jpg” format. After this has been saved, we need to locate the file where we have saved that file and if that file is having an image then the digital investigating what we are performing is successful.

**Screenshots:**

****

****

****

****

****

**The Above image is the hidden image in the Pcap file.**