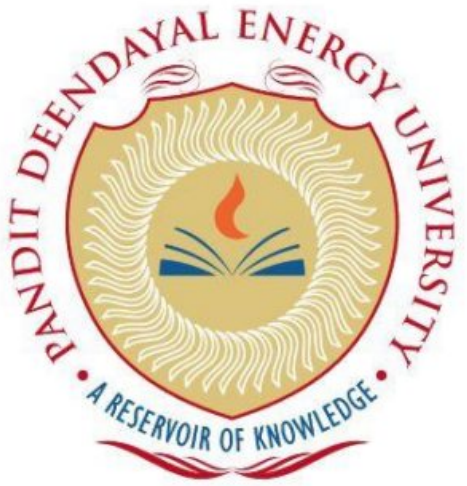
PANDIT DEENDAYAL ENERGY UNIVERSITY

SCHOOL OF TECHNOLOGY



Course: Digital Forensics

Course Code: 20CP411P

LAB MANUAL

B.Tech. (Computer Science and Engineering)

Semester 7

Submitted To:

Mr. Viral Parmar

Submitted By:

Mire Patel

19BCP080

G2 batch

Acknowledgement

It gives me immense pleasure in expressing thanks and profound gratitude to**, PANDIT DEENDAYAL ENERGY UNIVERSITY, GANDHINAGAR** for their kind support and providing infrastructure and research environment. I would like to convey my heartfelt sincere thanks to my internal guide **Mr. Viral Parmar, Department of Computer Science and Engineering, SOT, PDEU** for his valuable suggestion and constant encouragement and guidance provided at every stage of my lab work. Gratitude is owed to the staff of department of SOT, Pandit Deendayal Energy University for the guidance and co-operation provided.

Mire Patel

19BCP080

Certificate

This is to certify that the Practical lab report of the course entitled "**Digital Forensics (20CP411P)**" has been satisfactorily completed and submitted by **Mire Patel** Roll No. **19BCP080** of 7th Semester, CS&E Department towards the fulfilment of the requirements for the award of the degree of Bachelor of Technology in Computer Science & Engineering of School of Technology, Pandit Deendayal Energy University, Gandhinagar is the record of work carried out by him/her under our supervision and guidance. In our opinion, the submitted work has reached a level required for being accepted for the examination. The result embodied in this Project, to the best of our knowledge, has not been submitted to any other university or institution for award of any degree.

Mr. Viral Parmar

Date :

Place :

INDEX

S. No.	List of experiments	Date	Sign
1	Study of a Steganography tools.	**28-07-2022**	
2	Study of a Profile Generation using OSINT Techniques.	**11-08-2022**	
3	Study of a Identification of Morphed/Edited/Fabricated portion from given Video/Audio/Image files as investigation input.	**18-08-2022**	
4	Study of a Tracking & Tracing Fake Profile(s) & Fake News.	**25-08-2022**	
5	Study of a Deep and Darknet Monitoring Capabilities.	**01-09-2022**	
6	Study of a Data Recovery from Computer Systems, Mobile Devices, and other electronic peripherals.	**08-09-2022**	
7	Study of an Email Forensics tools.	**15-09-2022**	
8	Study of a Volatile Memory Forensics tools.	**13-10-2022**	
9	Study of a Hash and Hex analysis tools	**03-11-2022**	
10	Study of a Data Acquisition tools.	**20-10-2022**	

Digital Forensics Lab Report: 1

Date: 28-07-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Steganography tools.

Tool Names: Quickstego, OpenPuff, spammimic, DeepSound, Wbstego.

Tasks: Perform Image Steganography, Video Steganography, Mail steganography, Audio Steganography, and Document Steganography.

Introduction:

What is Steganography?

Steganography is a technique used to conceal data within a medium in a way that is not detectable by others.

Steganography is the act of concealing a message within another message or image. The purpose of steganography is to hide a message from someone you do not want to see it. Steganography is different than cryptography, the art of secret writing, which is intended to make a message unreadable, but does not hide the existence of the secret communication. Although steganography differs from cryptography, there are many similarities between the two, and some authors classify steganography as a form of cryptography since hidden communication is a type of secret writing. Steganography works by changing bits of useless or little used data in regular computer files (such as graphics, sound, text, HTML) with bits of different, invisible information. This hidden information can be plain text, cipher text, images, or even videos or documents.

- **Quickstego tool:** Quickstego is a free tool that allows you to hide data in images. It is easy to use and can be used to hide data in any type of image file. Quickstego uses a technique called steganography to hide data in images. Data hiding within other data is known as steganography. Quickstego allows you to hide data in images by adding it to the image file

itself. The data is then hidden in the image and can be retrieved by anyone who has the Quickstego tool. When text is hidden in an image, the image will still load like any other image and appear as it did before. The text will be hidden in the image, but it will not be visible to anyone viewing the image.

- **OpenPuff tool:** OpenPuff is a powerful and free steganography tool that can be used to hide data within image, audio and video files. It is designed to be portable and platform independent, and can be run from a USB drive without installation. OpenPuff supports a wide range of file formats, and can be used to hide data in files of any size.

- **spammimic tool:** A steganography programme called SpamMimic enables users to conceal information inside spam communications. It generates its output using a context-free probabilistic grammar. According to the probabilities assigned to each variable or terminal symbol in the production, each grammatical production is converted into a Huffman tree.

- **DeepSound tool:** DeepSound is a tool for digital forensics that can be used to analyze and investigate audio files. It can be used to identify and extract hidden information from audio files, as well as to identify and classify different types of sounds. DeepSound can also be used to create custom audio fingerprints for use in forensic investigations.

- **WbStego tool:** Any form of file can be concealed using the wbStego tool in bitmap images, text files, HTML files, or Adobe PDF files. The file where you hide the data is left unchanged visually. It can be used to add covert copyright information to the file or to securely share sensitive data.

Task 1: Performing Image Steganography

Steps:

Step 1 → Go to https://quick-stego.software.informer.com/1.2/ and download Quickstego tool from there. Install and run Quickstego tool after downloading the tool.

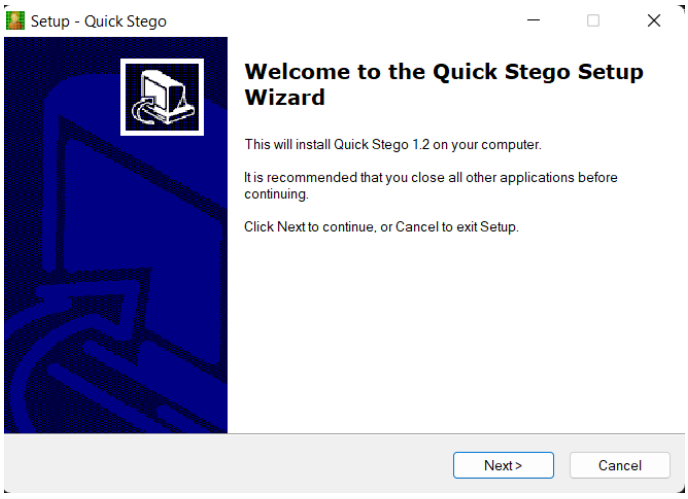


Figure 1: Installation Process of Quick Stego Tool – 1/4

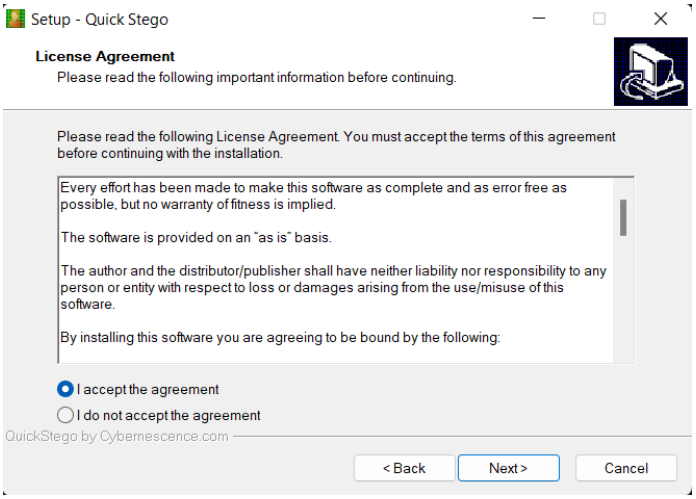


Figure 2: Installation Process of Quick Stego Tool – 2/4

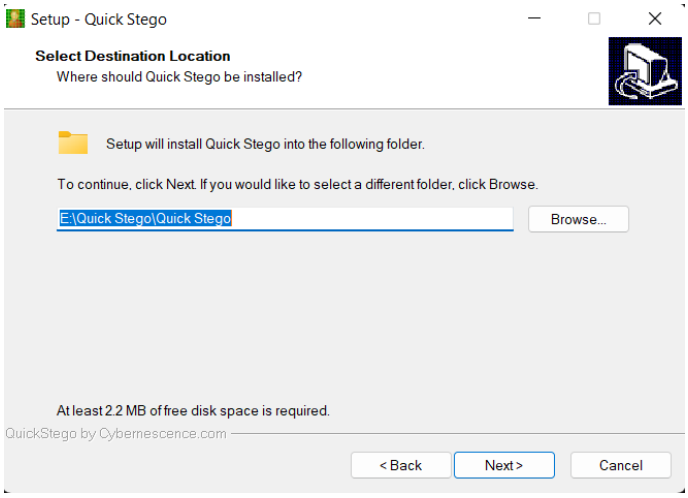


Figure 3: Installation Process of Quick Stego Tool – 3/4

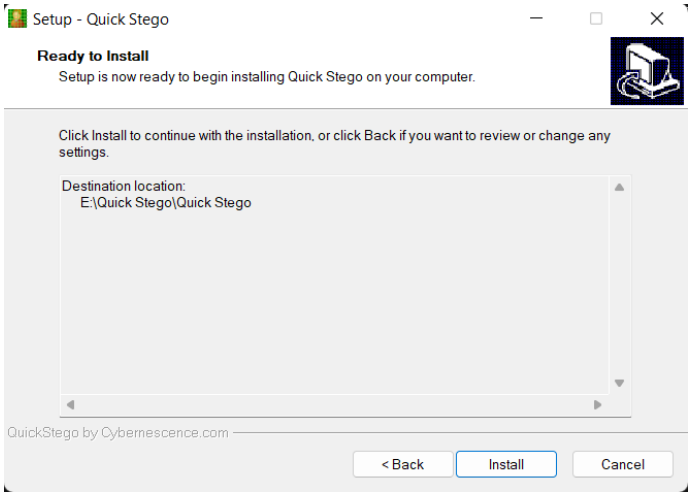


Figure 4: Installation Process of Quick Stego Tool – 4/4

Step 2 → After installing the Quick Stego tool, window is look like the below image. Select "Open Image" button, it will open file browser and select the carrier file (image file) to perform stego operation.

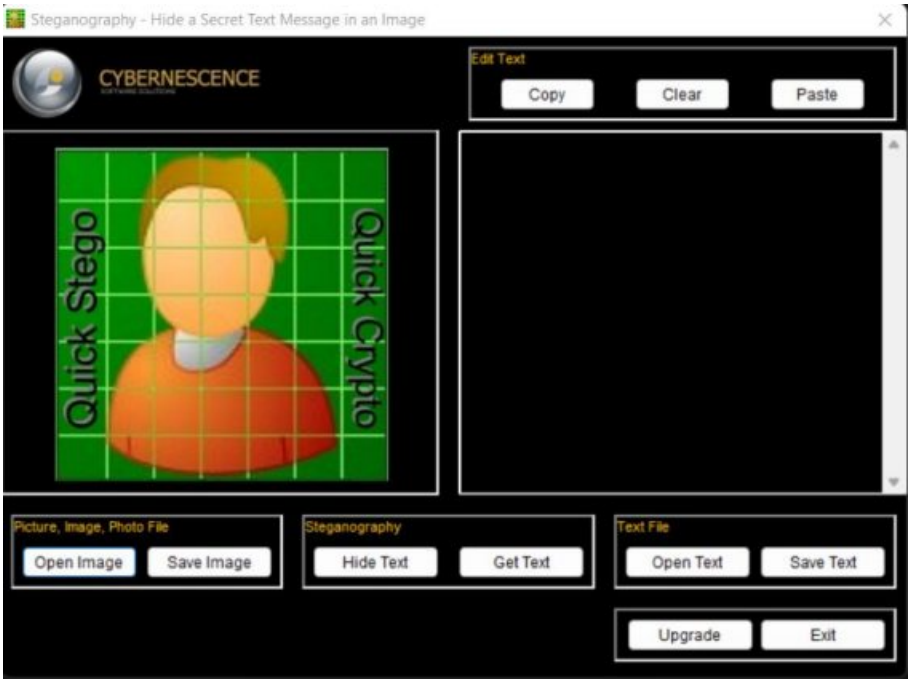


Figure 5: Quick Stego Tool Window

Step 3 → Write secret message in empty box situated on right side in tool and click on "Hide Text".

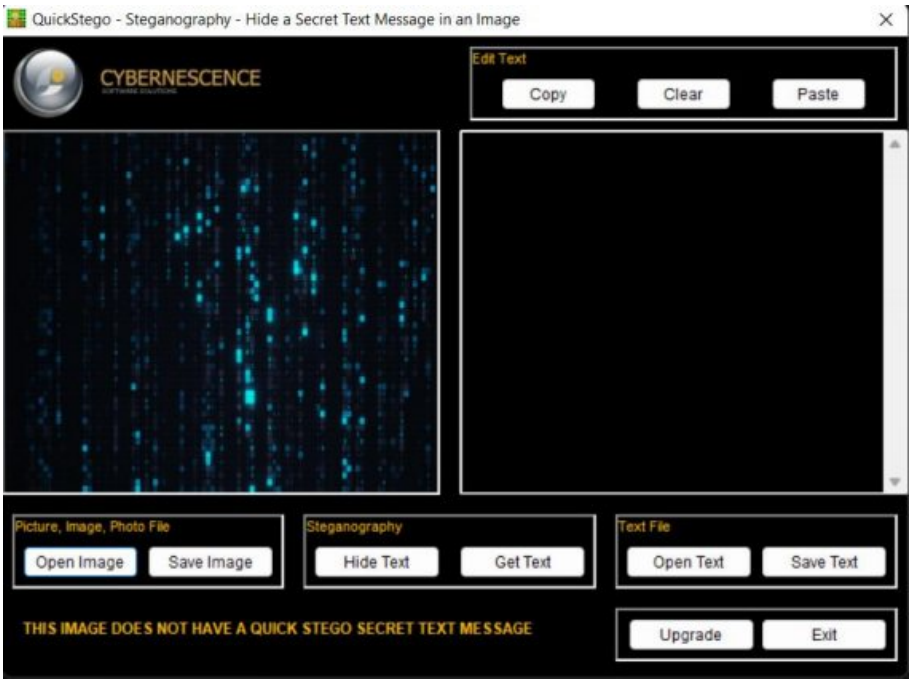


Figure 6: Preforming Stego Operation on Image File

Step 4 → Click on “Save Image” to save the stego file.

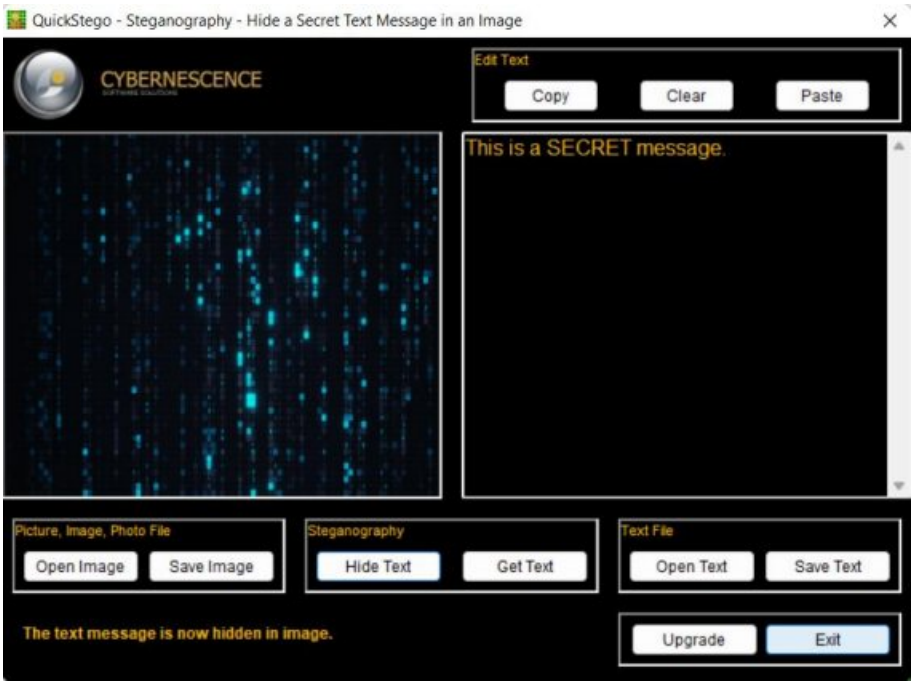


Figure 7: Hiding Secret Message in Stego File

Step 5 → To get the secret message from encoded file open the image file and click on get text.

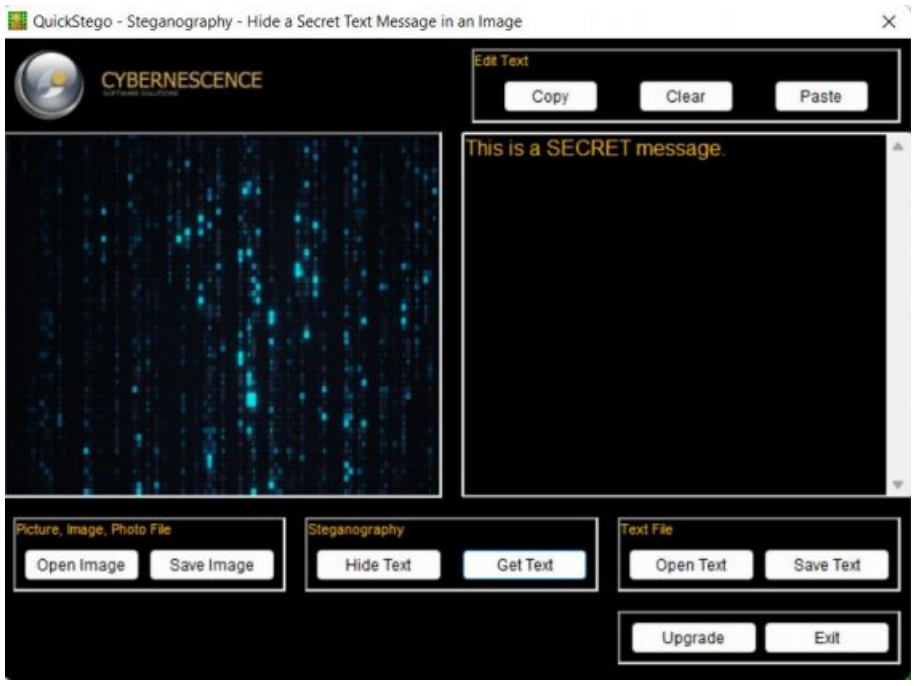


Figure 8: Getting Hidden Message from Stego File

Step 6 → Difference in properties of original image and encoded image.

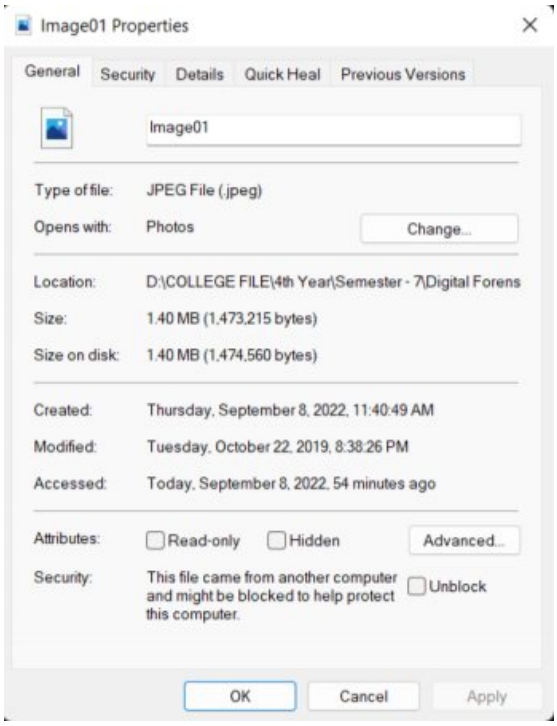


Figure 9: File comparison of original file and Setgo file – 1/2

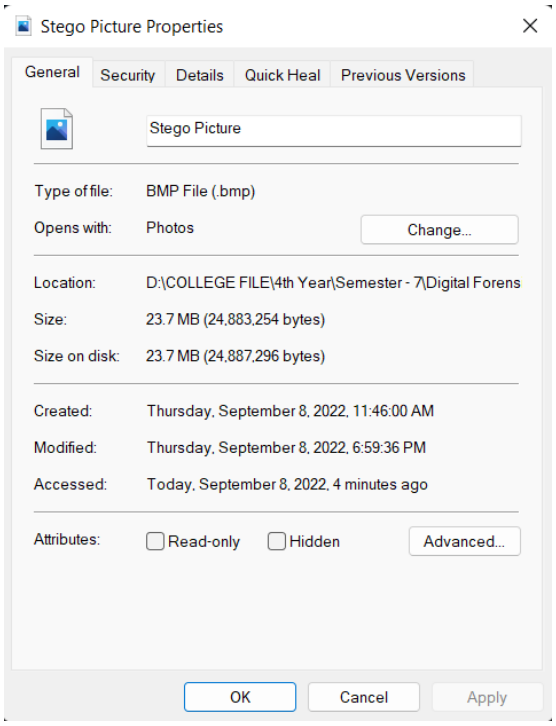


Figure 10: File comparison of original file and Setgo file – 2/2

Analysis:

After analyzing the results of the Quickstego tool, it is clear that this tool is effective for hiding data in images. The tool was able to successfully hide the data in the image without any noticeable changes to the image itself. This makes it an ideal tool for steganography, as the data can be hidden in plain sight without anyone being the wiser.

While comparing the original file with setgo file (encoded file), we can see there many of difference in both files. Lots of difference like file format, file size and timestamp.

Similar Tools:

- Camouflage
- Image stego
- Hide n Send
- Xiao Steganography
- SteganographX Plus
- Ssuite Picsel
- Steghide
- Open stego
- crypture
- SteganPEG

Task 2: Performing Video Steganography

Steps:

Step 1 → Download and install OpenPuff Video Steganography tool from https://openpuff.en.lo4d.com/windows. After installing the tool, the OpenPuff window is look like the below image.

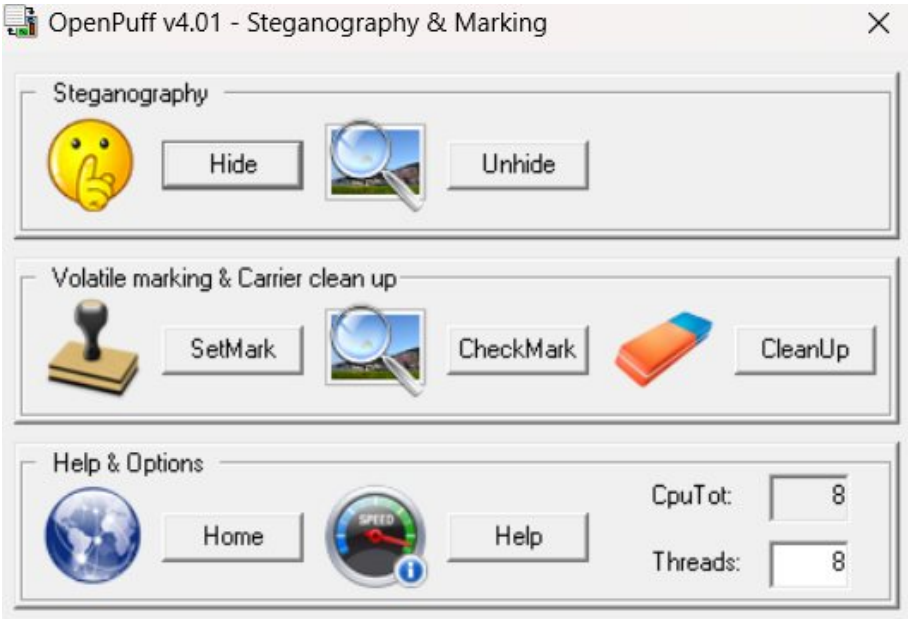


Figure 11: OpenPuff Tool Window

Step 2 → In the OpenPuff window, click on "Hide" button to enter the main interface of Tool.

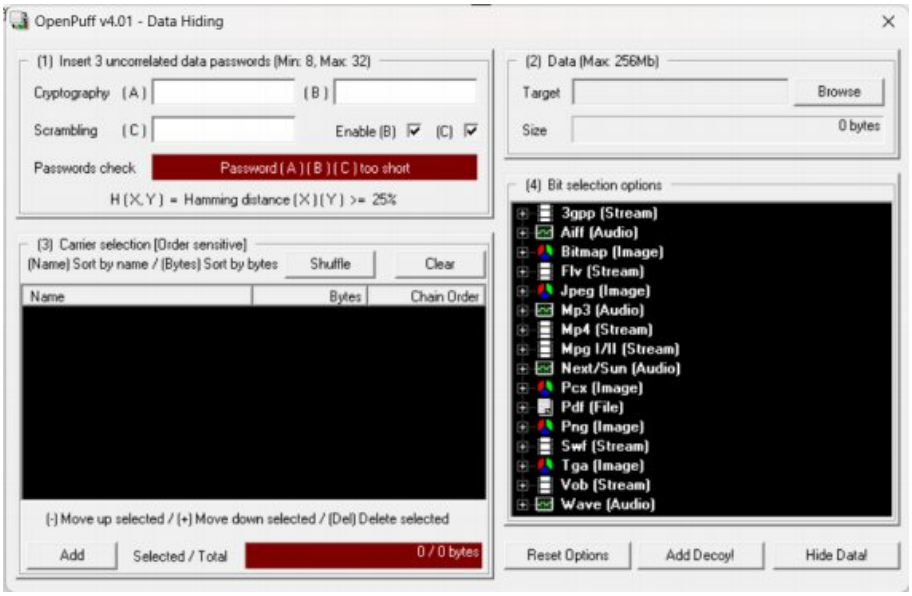


Figure 12: Main Interface of OpenPuff Tool

Step 3 → The main interface of the OpenPuff includes four sections for performing different tasks. In the first section, set the desired password for unhiding your data. Here three cryptographic passwords we have to provide, in that password B and C are optional. Provide the passwords accordingly.

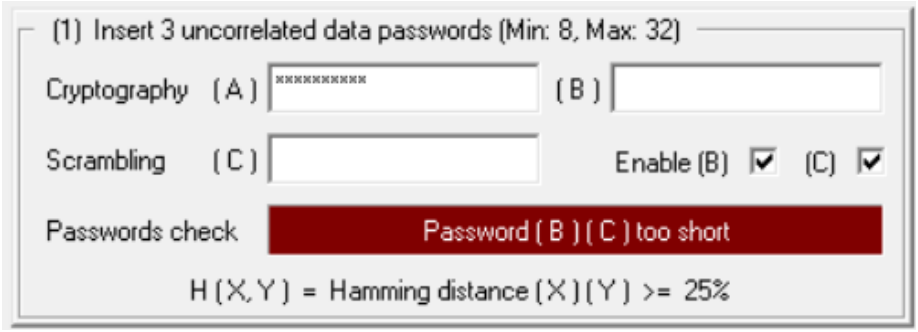


Figure 13: Setting up the desired password in OpenPuff tool - 1/2

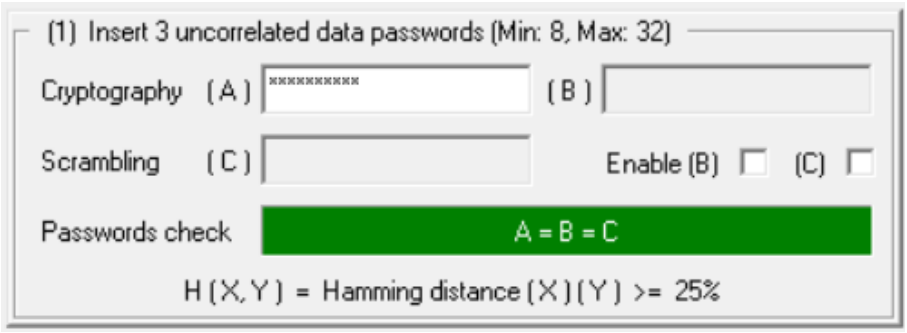


Figure 14: Setting up the desired password in OpenPuff tool - 2/2

Step 4 → Provide the target file from the second section that you want to hide in carrier video file.

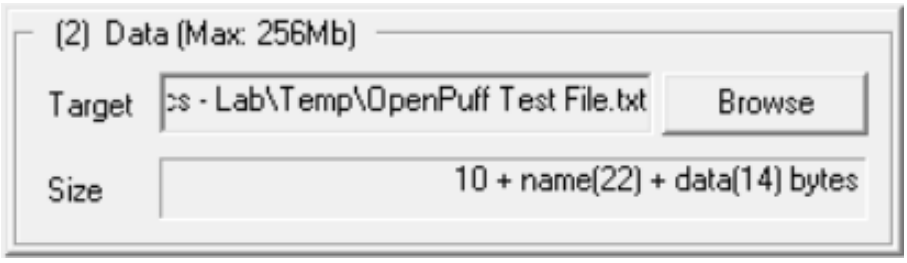


Figure 15: Providing the target file that is used to hide the carrier video file

Step 5 → Here in OpenPuff Tool, in “Carrier selection” - the third section, provide the carrier video file which you want to use for hiding your messages/documents.

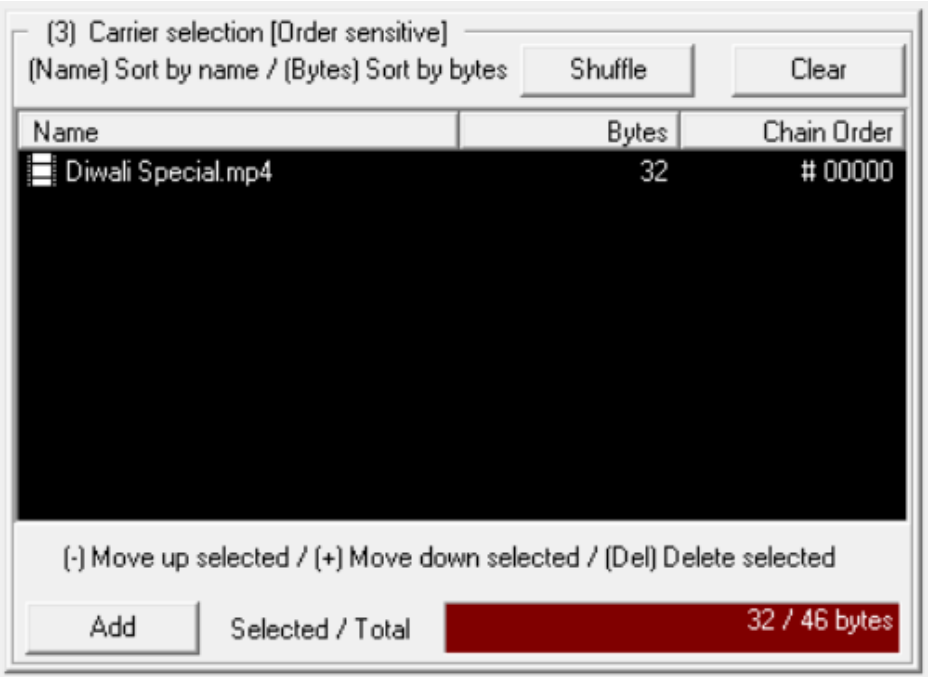


Figure 16: Providing the carrier video file to Hide the Message

Step 6 → In the fourth section "Bit Selection option", select the bit accordingly.

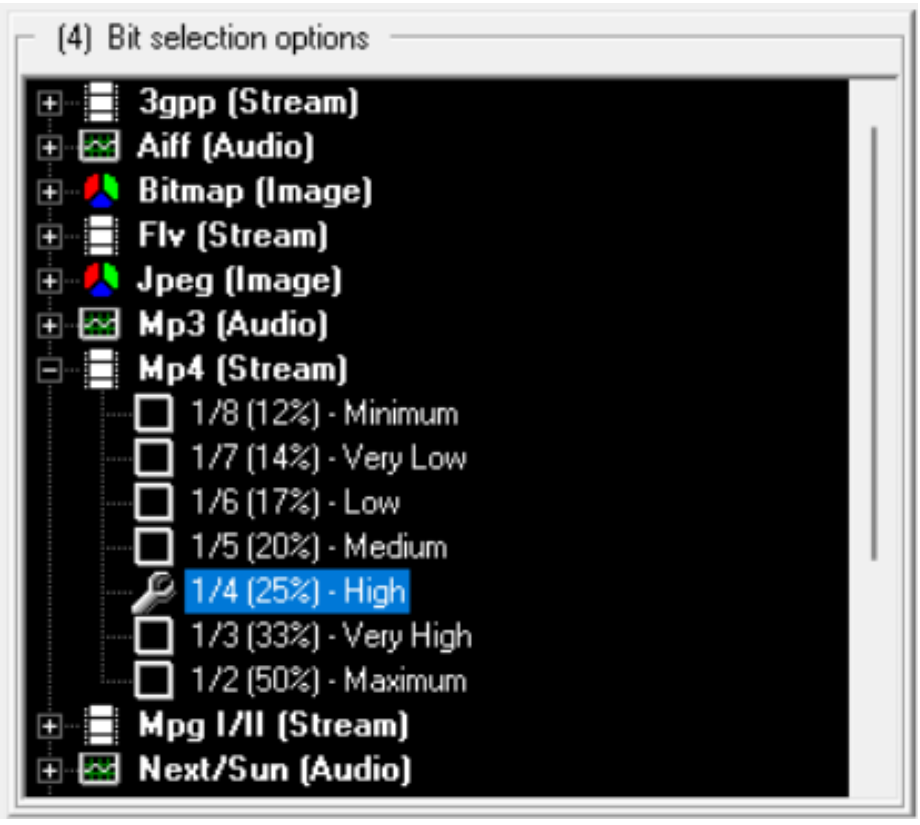


Figure 17: selecting the bit accordingly in OpenPuff tool

Step 7 → After then hit the Hide Data button to complete the process to hide the message.

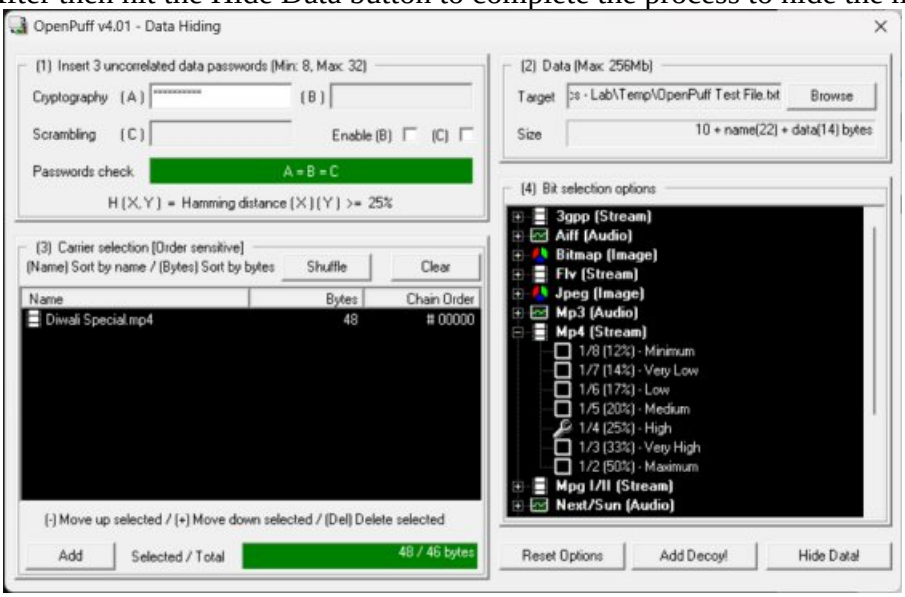


Figure 18: At the end clicking on the "Hide Data!" button

Step 8 → After completing the moving parts, a final dialogue will show up asking you to choose the folder where you want to save the finalized video file containing your concealed messages or documents. Your files will be concealed within the saved video file.

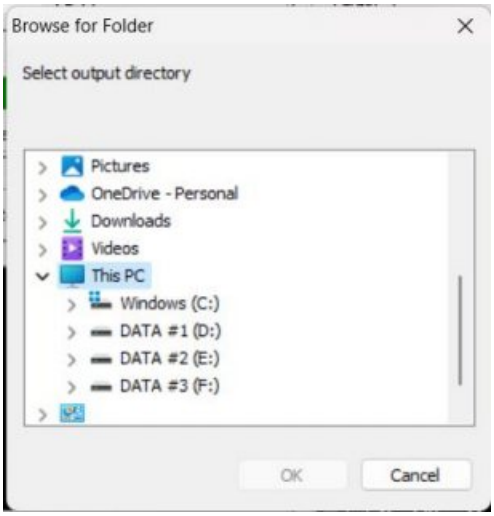


Figure 19: selecting the folder where the finalized video file is going to be stored

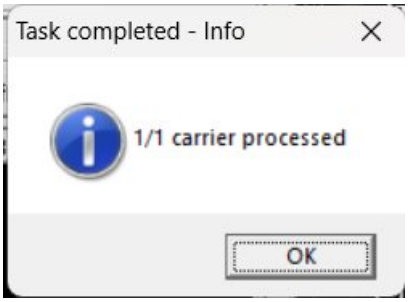


Figure 20: Task Completed dialog box for successful video steganography using OpenPuff Tool

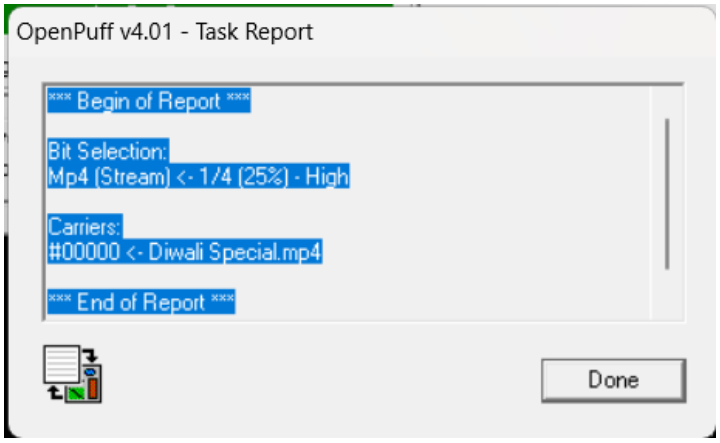


Figure 21: Final Task Report generated by the OpnePuff Tool

Step 9 → The procedure is essentially the same for extracting data from carrier video files that already exist. Simply choose the unhide option from the OpenPuff main window. Next, specify the place where you want to store the extracted file and the password you created while hiding your file.

Analysis:

After analysing the results of the OpenPuff tool, it was determined that this tool is an effective way to perform video steganography.

While comparing the original file with encoded file, we can see there lots of difference in both files. Difference in File format, file size and timestamp.

Similar Tools:

- DeEgger Embeddder
- StegoStick
- Our Secret
- StegoMagic

Task 3: Performing Mail steganography

Steps:

Step 1 → Go to spammimic website. (https://www.spammimic.com/)

Step 2 → Go to the Encode section and write the message which you want to encode.

Figure 22: Spammimic website window

Step 3 → You can send your encoded message through mail. After clicking on "Encode" you will get the encoded message in the mail format. You can copy this message and use it as normal mail with the hidden message.

Figure 23: Encoding using spammimic tool

Step 4 → To decode the message, just paste that text in the Decode section and click on "Decode".

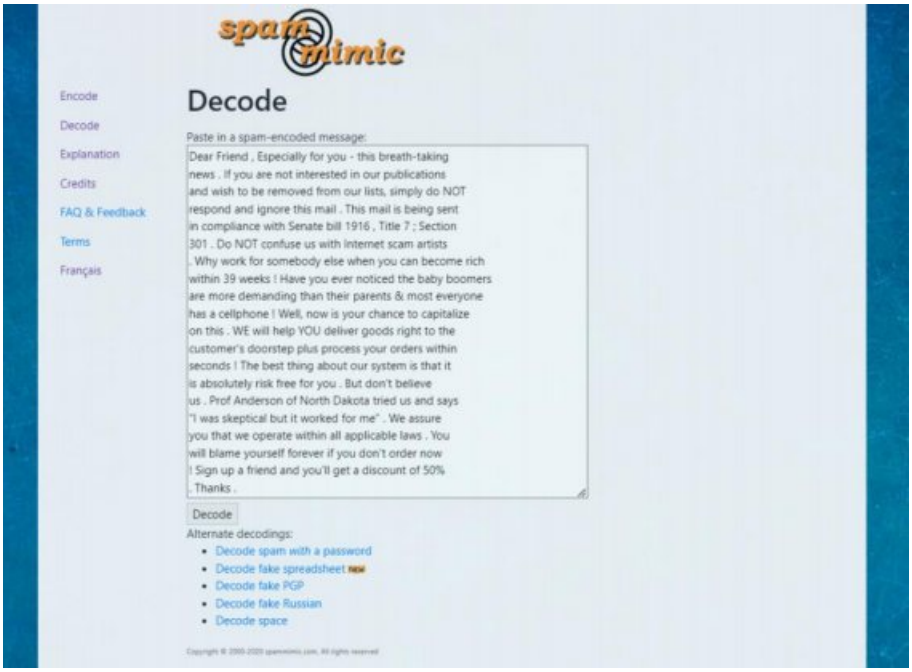


Figure 24: Decoding using spammimic tool

Step 5 → After clicking on "Decode", you will get the hidden message.

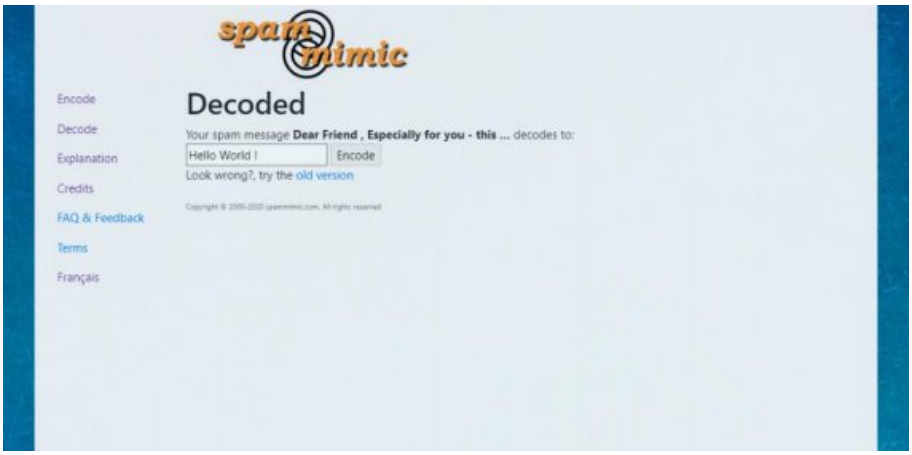


Figure 25: Decoded Message by spammimic tool

Step 6 → With the same procedure, you can hide the message with the strong password. In the Encode section, at the bottom, you will find "Encode as spam with a password" link, from there you will do the encoding and decoding message by using the password with it.

Figure 26: Encoding with password using spammimic tool

Figure 27: Encoded Message with password by spammimic tool

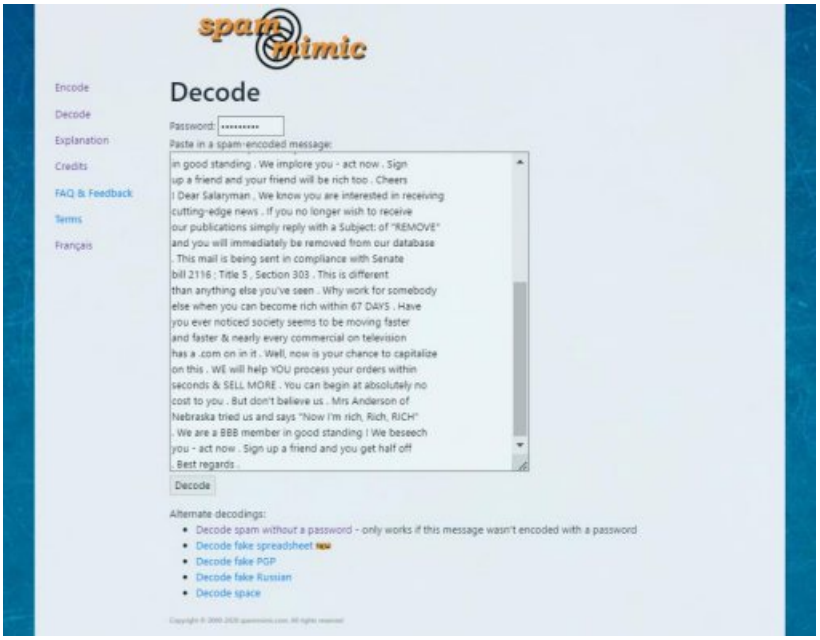


Figure 28: Decoding with password using spammimic tool

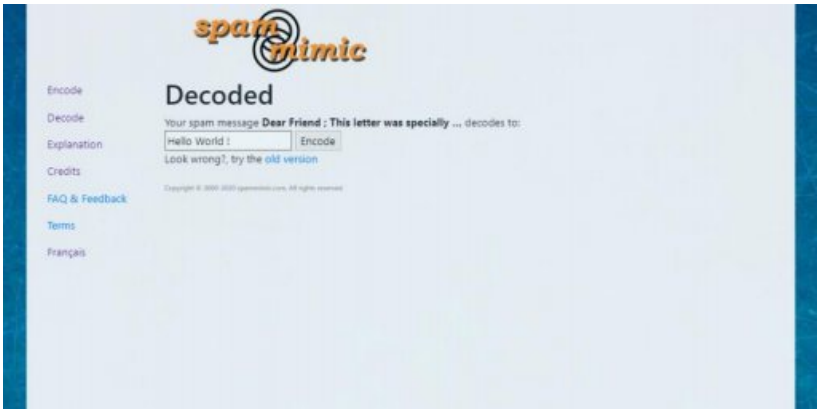


Figure 29: Decoded Message with password by spammimic tool

Analysis:

Simple and easy to use this tool for encoding and decoding the Secret Message. It allows you to encode your small texts, emails, and messages with various methods and also gives you the way to decode the specific encoded format text.

Similar tools:

- SecureMail
- SteganMail
- HideMyEmail
- Steghide
- Outguess
- StegoTorus

Task 4: Performing Audio Steganography

Steps:

Step 1 → Go to https://deepsound.soft112.com/ and download DeepSound tool from there. Install and run DeepSound tool after downloading the tool.

Step 2 → Select the "Open carrier files" button it will open a file browser and select the carrier file (audio file) to perform the stego operation using DeepSound tool.

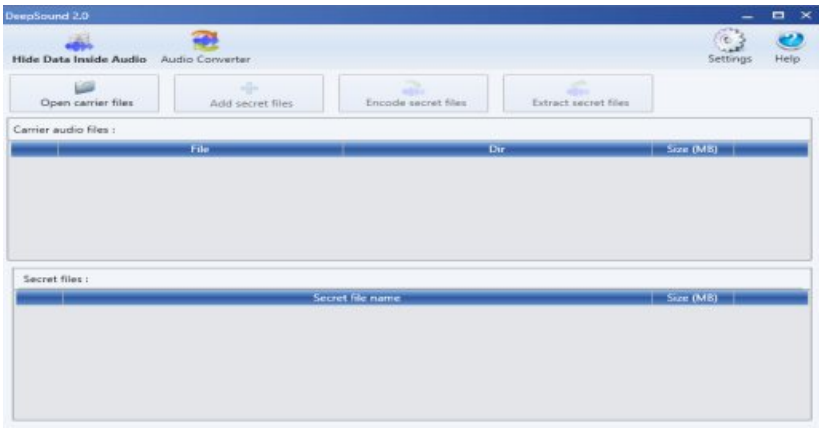


Figure 30: DeepSound Tool Window

Step 3 → Select the "Add secret files" button it will open a file browser and select the secret files to hide.

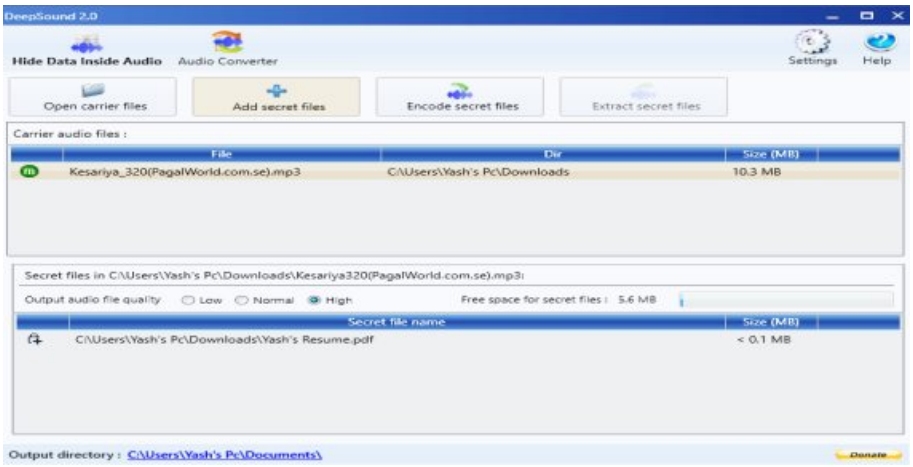


Figure 31: Storing Secret File to Audio carrier

Step 4 → Click on the "Encode Secret File" button. Select the output file format and set the password for stego file and it will be saved to your set directory.

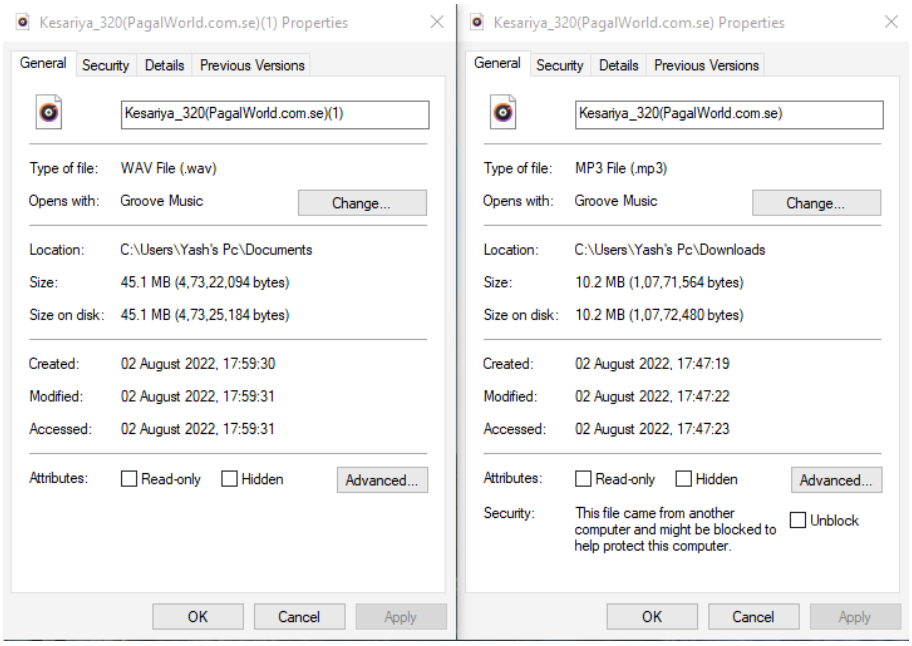


Figure 32: File comparison of the original file and Stego file

Analysis:

The tool was able to successfully encode and decode messages in both WAV and MP3 files with little to no noticeable degradation in audio quality. Overall, the DeepSound steganography tool is a very effective tool for performing steganography on audio files.

While comparing the original file with the stego file (encoded file) we can see there are lots of differences in both files. File format is different, file size is different and timestamp is different.

Similar tools:

- Wavstag
- Sonic visualizer
- steghide

Task 5: Performing Document Steganography

Steps:

Step 1 → Go to https://wbstego4.indir.biz/en/ and download wbStego tool from there. Install and run wbStego tool after downloading the tool.

Step 2 → After installing wbStego tool, the window is look like below image. Select between options either Encoding or Decoding.

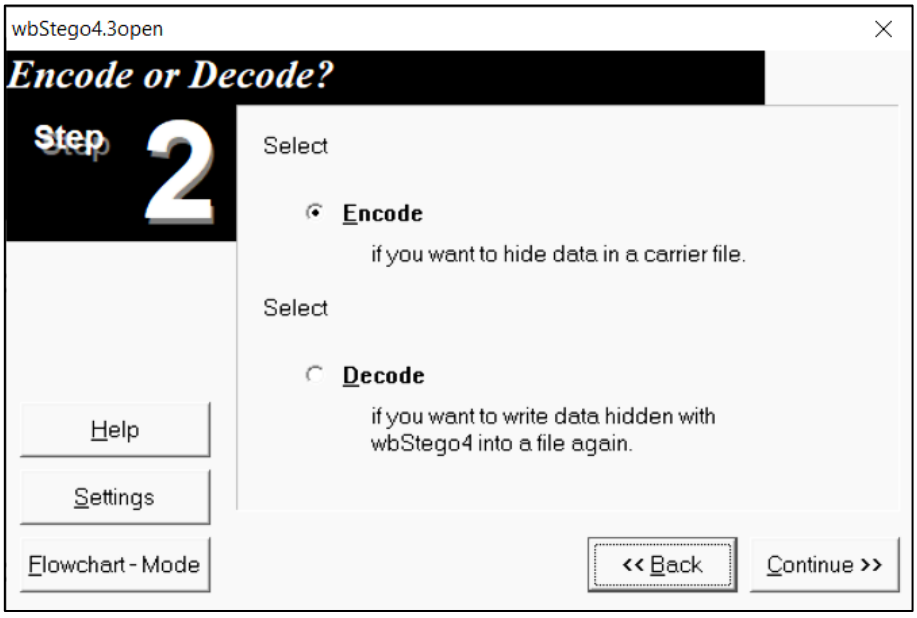


Figure 33: wbstego Tool Window

Step 3 → Select the data file you want to hide.

Step 4 → Select the carrier file in which you want to hide data.

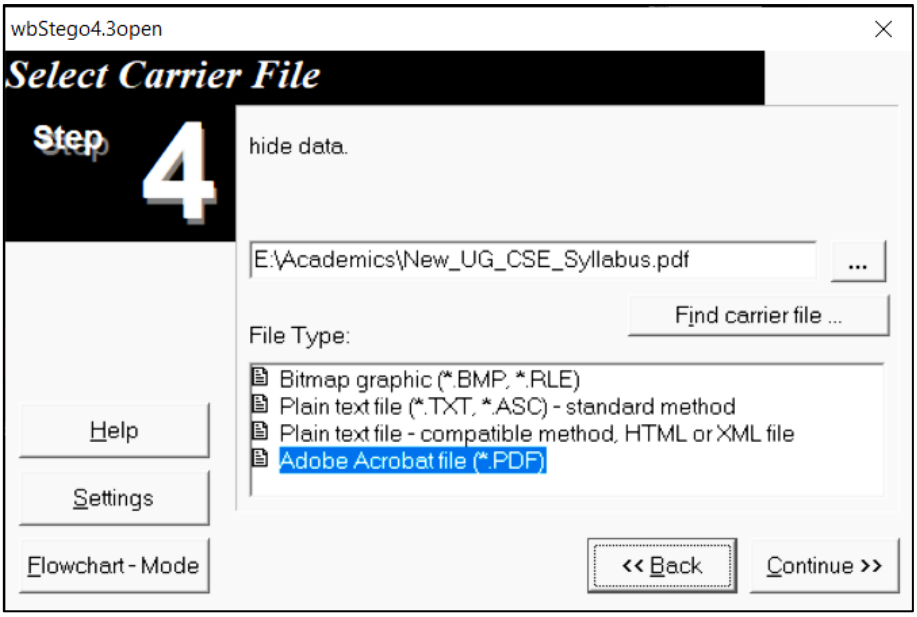


Figure 34: Storing Secret Message using wbStego Tool

Step 5 → Then select Encryption Method.

Step 6 → Save the modified file.

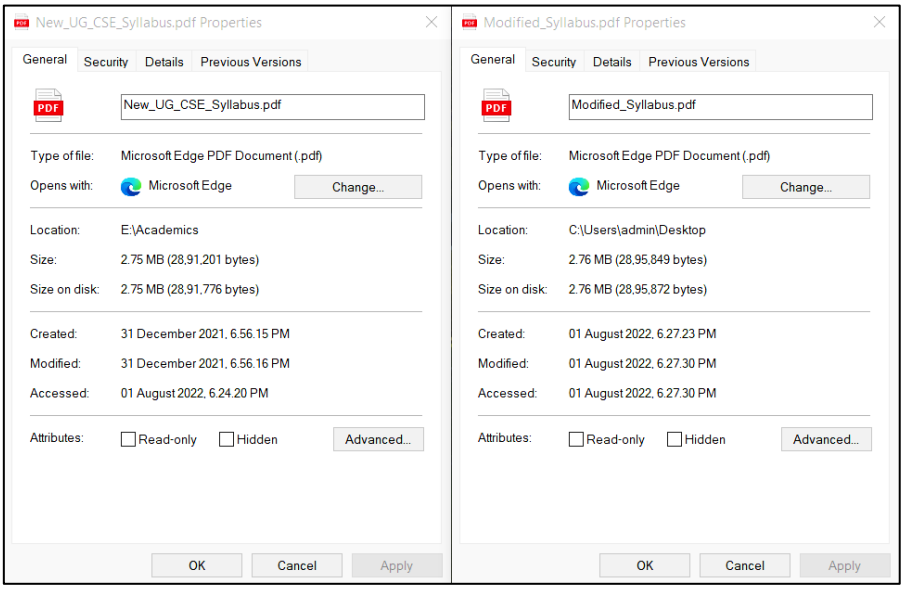


Figure 35: File comparison of original file and Stego file

Analysis:

Overall, the process of steganography using wbStego was successful. The tool was able to successfully encode the message into the document with minimal distortion. The tool was also able to successfully decode the message from the document.

While comparing the original file with modified file (encoded file) we can see there lots of difference in both files. Difference in file size and timestamp.

Similar Tools:

- Convert
- ImageMagick
- Exiftool
- Exiv2
- Exif

Conclusion:

Steganography is an incredibly useful tool for enhancing security and reliability in any form of communication. While it is relatively easy to use, it can be very difficult to detect. This makes it an ideal tool for use in a variety of section in real life, including the military, businesses, education, and government and more.

The proliferation of steganography tools has law enforcement worried about the trafficking of illegal material via web page images, audio, and other transmissions over the Internet.

In the future, steganographic techniques will become increasingly important in the field of digital watermarking. This is because content providers are eager to protect their copyrighted works against illegal distribution, and digital watermarks provide a way of tracking the owners of these materials. However, it is possible that steganography will become limited under laws, since governments have claimed that criminals use these techniques to communicate.

Digital Forensics Lab Report: 2

Date: 11-08-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Profile Generation using OSINT Techniques.

Tool Names: –

Tasks: Generate profile using OSINT Techniques.

Introduction:

What is OSINT?

Open Source Intelligence (OSINT) is the collection and analysis of information that is freely available or publicly accessible. This information can be gathered from a variety of sources, including the internet, social media, news media, and traditional print media.

Open-source intelligence (OSINT) is a term used to describe the process of collecting data from publicly available sources. These sources can include news articles, social media posts, websites, and other public records. OSINT can be used to gather information about people, places, organizations, or events.

Among the sources for OSINT are:

- Articles from newspapers and magazines as well as news reports
- Published academic works and research
- Books and other scholarly resources
- Census data
- Social media usage

Target: Dr Manoj Sahni

Prior Known Information: Works in PDEU, Gandhinagar

PERSONAL DETAILS

Figure 1: Profile Image of Dr Manoj Sahni

Name: Dr Manoj Sahni

Designation: HoD & Associate Professor

Department: Department of Mathematics, School of Technology

Email: Manoj.Sahni@sot.pdpu.ac.in

Mobile No.: +91 7874441820

Educational Qualifications:

- M.Sc. (Mathematics, Dayalbagh Educational Institute, Agra), 2003
- Ph.D (Mathematics, Jaypee Institute of Information Technology, Noida), 2010
- M.Phil. (APPLIED MATHEMATICS, IIT ROORKEE), 2004
- B.Sc. (Mathematics, Physics, Chemistry, Lucknow Christian Degree College, Lucknow), 1999

Professional Affiliation:

- UCSC, Chile UTS, Australia

Awards:

- 0

Areas of Interest:

- Elasticity, Plasticity, and Creep, Functionally Graded Materials, Fuzzy Sets and their Extensions, Development of Novel Numerical Methods, Fixed Point Iteration Methods.

Brief Profile:

- Dr. Manoj Sahni is working in the Department of Mathematics at PDEU (Formerly PDPU) for more than eight years. He has done M.Sc. from Dayalbagh Educational Institute Agra (Deemed University), M.Phil. Mathematics from IIT Roorkee and Ph.D. Mathematics from Jaypee Institute of Information Technology (JIIT), Noida. He has more than 18 years of teaching and research experience. He has published more than 70 research papers in International peer-reviewed Journals, Conferences, and Book Chapters. He is the president of the Forum for Interdisciplinary Mathematics in the Gujarat Chapter and Joint Secretary at all Indian Levels. He is the Life Member of various National and International Societies such as the American Mathematical Society, IEEE, SIAM, MAA, Indian Science Congress, SFA, INSIS, ams, FIM, IAENG, etc. He has guided two Ph.D. student and four are working under him.

PDEU FACULTY PROFILE

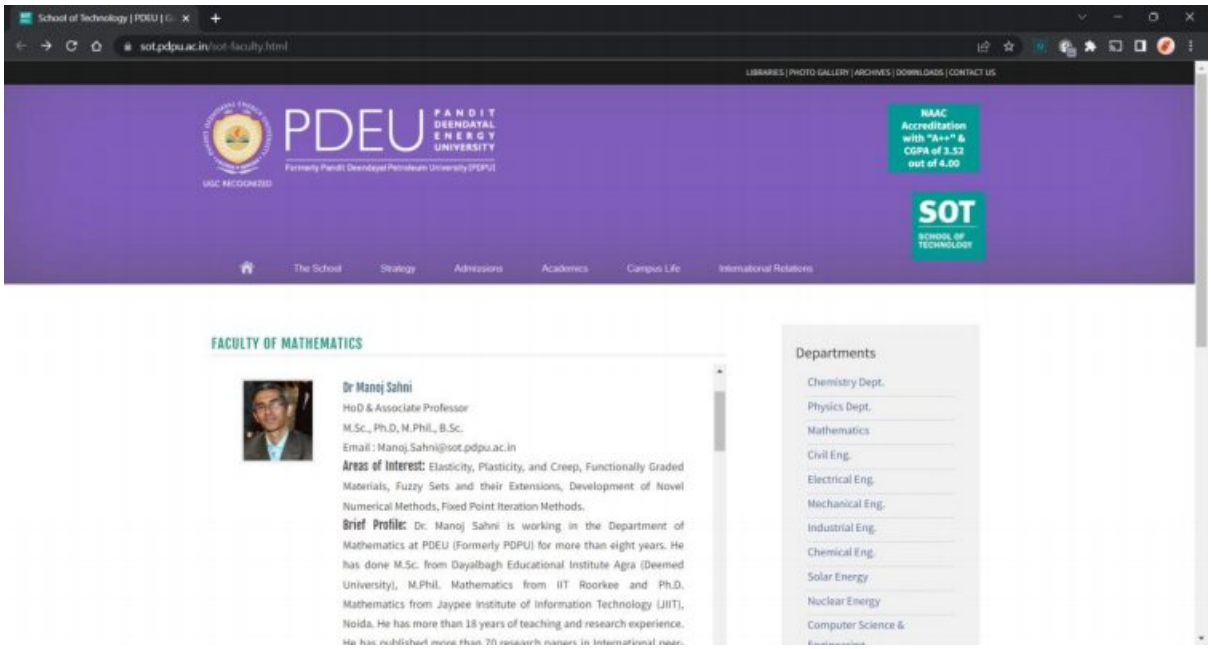


Figure 2: PDEU FACULTY PROFILE - Dr Manoj Sahni

ORSP PDPU PROFILE

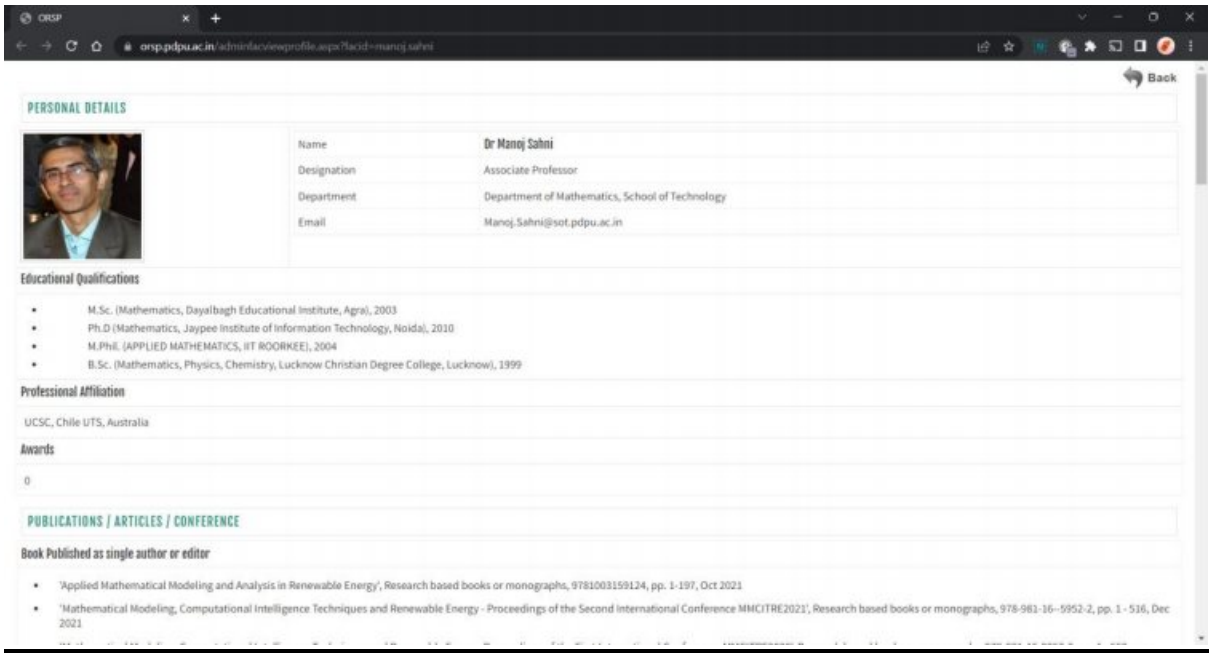


Figure 3: ORSP PDEU PROFILE - Dr Manoj Sahni

GOOGLE SCHOLAR PROFILE

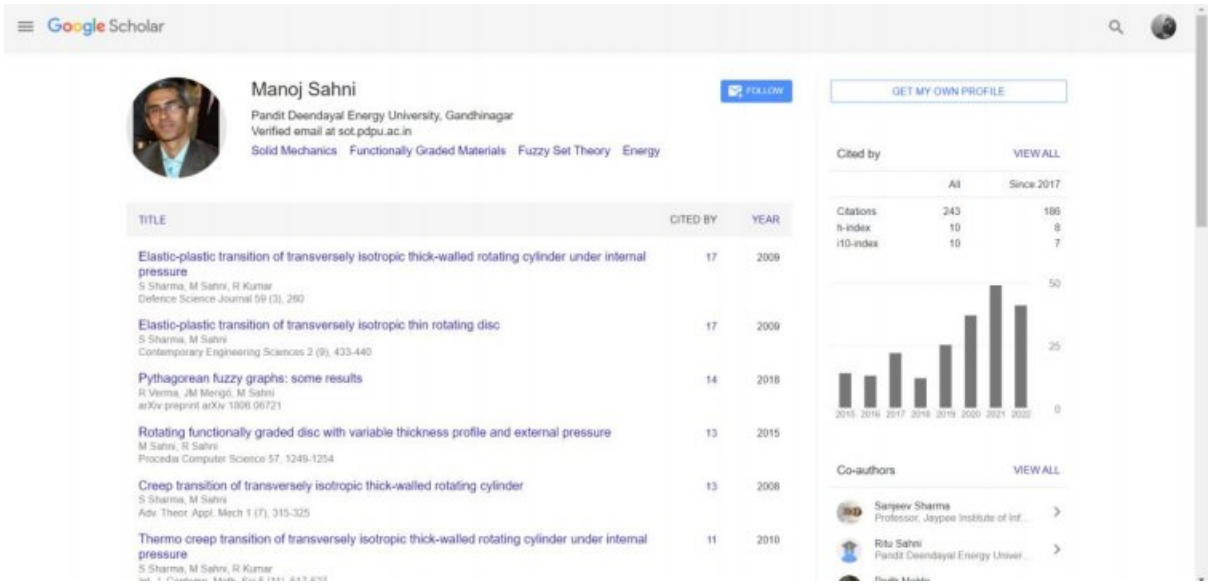


Figure 4: GOOGLE SCHOLAR PROFILE - Dr Manoj Sahni

LINKEDIN PROFILE

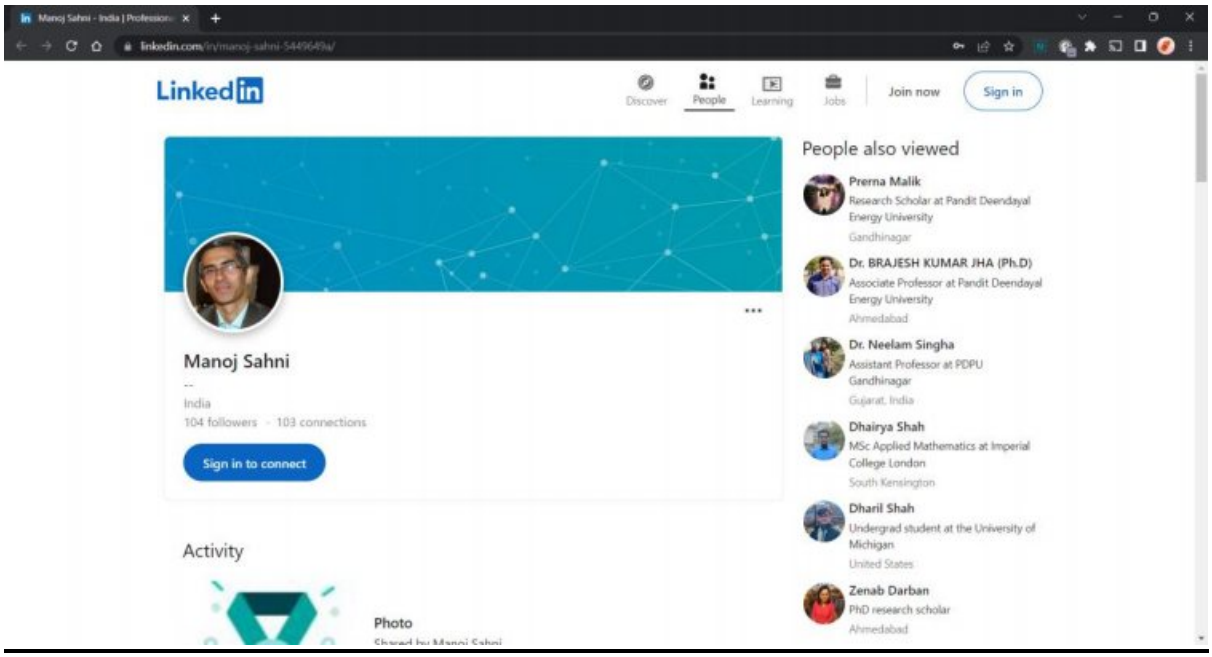


Figure 5: LINKEDIN PROFILE - Dr Manoj Sahni

PUBLICATIONS / ARTICLES / CONFERENCE

Book Published as single author or editor:

- 'Applied Mathematical Modeling and Analysis in Renewable Energy', Research based books or monographs, 9781003159124, pp. 1-197, Oct 2021
- 'Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy - Proceedings of the Second International Conference MMCITRE2021', Research based books or monographs, 978-981-16--5952-2, pp. 1 - 516, Dec 2021
- 'Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy, Proceedings of the First International Conference, MMCITRE2020', Research based books or monographs, 978-981-15-9953-8, pp. 1 - 559, mar 2021

Articles/Chapters Published in the books:

- 'Finding the Surface Area and Volume of the Hyperspheres Using Simple Calculus', Applied Mathematical Modeling and Analysis in Renewable Energy, 9781003159124, pp. 125-130, Oct 2021
- 'Analysis of Orthotropic Variable Thickness Rotating Disc', Structural Integrity Assessment, 978-981-13-8767-8, pp. 479-486, jul 2019

- 'Stress Analysis of a Pressurized Functionally Graded Rotating Discs with Variable Thickness and Poisson's Ratio', Applied Mathematics and Computational Intelligence, 978-3-319-75791-9, pp. 54-62, Nov 2017
- 'Elastic-Plastic Analysis for a Functionally Graded Rotating Cylinder Under Variation in Young's Modulus', Applied Mathematics and Computational Intelligence, 978-3-319-75791-9, pp. 26-39, Nov 2017

Published Papers in Journals:

- 'Semantic Analysis and Topic Modelling of Web-Scrapped COVID-19 Tweet Corpora through Data Mining Methodologies', Healthcare, pp. 1-30, may 2022
- 'Series of Floor and Ceiling Functions—Part II: Infinite Series', Mathematics, pp. 1-17, apr 2022
- 'Series of Floor and Ceiling Function—Part I: Partial Summations', Mathematics, pp. 1-19, apr 2022
- 'Sun's rays in the PV modules energy yield estimations to improve the energy conversion description', Energy Reports, pp. 3559–3588, apr 2022
- 'Solution of First Order Initial Value Problem using Analytical and Numerical Method in Neutrosophic Environment', Neutrosophic Sets and Systems, pp. 311-329, Oct 2022
- 'Diagnosis of Intracranial Tumors via the Selective CNN Data Modeling Technique', Applied Sciences, pp. 1-14, mar 2022
- 'Secondary Creep Analysis of FG Rotating Cylinder with Exponential, Linear and Quadratic Volume Reinforcement', Materials, pp. 1-23, feb 2022
- 'Fuzzy Number - A New Hypothesis and Solution of Fuzzy Equations', Mathematics and Statistics, pp. 176 - 186, jan 2022
- 'Numerical Simulation of Stresses in Functionally Graded HCS-MgO Cylinder Using Iterative Technique and Finite Element Method', Materials, pp. 1-21, jun 2022
- 'Multi-Product Economic Inventory Policy with Time Varying Power Demand, Shortages and Complete Backordering', Universal Journal of Accounting and Finance, pp. 98 - 104, mar 2021
- 'TWO-DIMENSIONAL STRESS ANALYSIS OF A THICK HOLLOW CYLINDER MADE OF FUNCTIONALLY GRADED MATERIAL SUBJECTED TO NON-AXISYMMETRIC LOADING', Structural Integrity and Life , pp. S71-S81, aug 2021
- 'Sumudu transform for solving ordinary differential equation in a fuzzy environment', Journal of Interdisciplinary Mathematics, pp. 1-13, mar 2021
- 'COMPARISON OF MATERIAL RESPONSE FOR THERMOMECHANICAL STRESSES IN FUNCTIONALLY GRADED ROTATING CYLINDERS ', Structural Integrity and Life , pp. 259-265, Dec 2021
- 'Stress Analysis of Functionally Graded Disk with Exponentially Varying Thickness using Iterative Method ', WSEAS TRANSACTIONS on APPLIED and THEORETICAL MECHANICS, pp. 232-244, Dec 2021

- 'FROBENIUS SERIES SOLUTION FOR FUNCTIONALLY GRADED MATERIAL WITH EXPONENTIALLY VARIABLE THICKNESS AND MODULI', Structural Integrity and Life , pp. S83-S88, aug 2021
- 'Two-Dimensional Stress Analysis of Thick Hollow Functionally Graded Sphere Under Non-Axisymmetric Mechanical Loading ', International Journal of Mathematical, Engineering and Management Sciences, pp. 1115-1126, jul 2021
- 'Sumudu Transform for Solving Second Order Ordinary Differential Equation under Neutrosophic Initial Conditions', Neutrosophic Sets and Systems,, pp. 258-275, Dec 2020
- 'Thermo-Mechanical Analysis for an Axisymmetric Functionally Graded Rotating Disc under Linear and Quadratic Thermal Loading', International Journal of Mathematical, Engineering and Management Sciences, pp. 744-757, apr 2020
- 'An Inventory Model on Preservation Technology with Trade Credits under Demand Rate Dependent on Advertisement, Time and Selling Price ', Universal Journal of Accounting and Finance, pp. 65-74, sep 2020
- 'ANALYSIS OF CREEP STRESSES IN THIN ROTATING DISC COMPOSED OF PIEZOELECTRIC MATERIAL ', Structural Integrity and Life , pp. S45-S49, Dec 2020
- 'MODELLING OF MECHANICAL VIBRATING SYSTEM IN CLASSICAL AND FUZZY ENVIRONMENT USING SUMUDU TRANSFORM METHOD ', Structural Integrity and Life , pp. S54-S60, Dec 2020
- 'THERMO-MECHANICAL ANALYSIS OF SANDWICH CYLINDER WITH MIDDLE FGM AND BOUNDARY COMPOSITE LAYERS', Structural Integrity and Life , pp. 313-318, Dec 2020
- 'Generalized Trapezoidal Intuitionistic Fuzzy Number for Finding Radial Displacement of a Solid Disk', WSEAS TRANSACTIONS on MATHEMATICS, pp. 105 - 111, mar 2019
- 'A new modified accelerated Iterative Scheme using Amalgamation of Fixed Point and N-R method', Journal of Interdisciplinary Mathematics, pp. 679-688, Nov 2019
- 'Comparison of Newton-Raphson and Kang’s Method with newly developed Fuzzified He’s Iterative method for solving nonlinear equations of one variable', WSEAS TRANSACTIONS on MATHEMATICS, pp. 6-13, jan 2019
- 'Second Order Cauchy Euler Equation and Its Application for Finding Radial Displacement of a Solid Disk using Generalized Trapezoidal Intuitionistic Fuzzy Number', WSEAS TRANSACTIONS on MATHEMATICS, pp. 37-45, jan 2019
- 'Ranking of Teachers Based on Feedback from the Students using Multiple Subjects', International Journal of Mathematical Models and Methods in Applied Sciences, pp. 7 – 12, mar 2019
- 'Career Determination using Information Theoretical Measure and It’s Comparison with Distances in IFS and PFS', International Journal of Mathematical Models and Methods in Applied Sciences, pp. 28 – 34, mar 2019

- 'Information Theoretical Measure for Career Determination', WSEAS Transactions on Mathematics, pp. 73 – 78, mar 2019
- 'Solution of Algebraic and Transcendental Equations using Fuzzified He's Iteration Formula in terms of Triangular Fuzzy Numbers', WSEAS TRANSACTIONS on MATHEMATICS, pp. 91 – 96, mar 2019
- 'Thermo-mechanical Stress Analysis of Thick-Walled Cylinder with Inner FGM Layer', Structural Integrity and Life , pp. 211-223, Dec 2019
- 'Strength analysis of functionally graded rotating disc under variable density and temperature loading', Structural Integrity and Life , pp. 95 – 101, Oct 2019
- 'Two -dimensional mechanical stresses for a pressurized cylinder made of functionally graded material', Structural Integrity and Life , pp. 79 – 85, Oct 2019
- 'Evaluation of Teachers' Performance Based on Students' Feedback Using Aggregator Operator', WSEAS TRANSACTIONS on MATHEMATICS, pp. 85-90, mar 2019
- 'Elastic-plastic deformation of a thin rotating solid disk of exponentially varying density', RESM, sep 2016
- 'THERMO CREEP TRANSITION IN FUNCTIONALLY GRADED THICK-WALLED CIRCULAR CYLINDER UNDER EXTERNAL PRESSURE', ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering, pp. 335-342, Dec 2014
- 'Functionally Graded Rotating Disc with Internal Pressure', Engineering and Automation Problems, pp. 125 - 129, mar 2014
- 'THERMO ELASTIC-PLASTIC TRANSITION OF A HOMOGENEOUS THICK-WALLED CIRCULAR CYLINDER UNDER EXTERNAL PRESSURE', Structural Integrity and Life, pp. 3-8, apr 2013
- 'CREEP ANALYSIS OF THIN ROTATING DISC HAVING VARIABLE THICKNESS AND VARIABLE DENSITY WITH EDGE LOADING', ANNALS of Faculty Engineering Hunedoara – International Journal of Engineering, pp. 289-296, jun 2013
- 'Elastic-Plastic Transition of Non-Homogeneous Thick-walled Cylinder under External Pressure', Applied Mathematical Sciences, pp. 6069-6074, jun 2012
- 'Thermo Creep Transition of Transversely Isotropic Thick-walled Rotating Cylinder under Internal Pressure', Int. J. Contemp. Math. Sciences, pp. 517-527, aug 2010
- 'Elastic-plastic Analysis of a Thin Rotating Disk of Exponentially Variable Thickness with Inclusion', WSEAS Transactions on Mathematics, pp. 314-323, may 2010
- 'Elastic-plastic Transition of Transversely Isotropic Thin Rotating Disc', Contemporary Engineering Sciences, pp. 433-440, apr 2009
- 'Thermo Elastic-plastic Transition of Transversely Isotropic Thick-walled Rotating Cylinder under Internal Pressure', Advances in Theoretical and Applied Mechanics, pp. 113-122, jan 2009
- 'Elastic-plastic transition of transversely isotropic thick-walled rotating cylinder under internal pressure', Defence Science Journal, pp. 260-264, may 2009

- 'Creep Analysis of Thin Rotating Disc under Plane Stress with no Edge Load', WSEAS Transactions on Applied and Theoretical Mechanics, pp. 725-738, jan 2008
- 'Creep Transition of Transversely Isotropic Thick-Walled Rotating Cylinder', Adv. Theor. Appl. Mech., pp. 315-325, feb 2008

Full Papers in Conference Proceedings:

- 'Chi-Square Similarity Measure for Interval Valued Neutrosophic Set', Manoj Sahni, J.M. Merigo, Brajesh Kumar Jha, Rajkuar Verma, pp. 545 - 558, feb 2021
- 'Comparative Study of Two Teaching Methodologies Using Fuzzy Set Theory', Manoj Sahni, J.M. Merigo, Brajesh Kumar Jha, Rajkuar Verma, pp. 521 - 530, feb 2021
- 'Floyd’s Algorithm for All-Pairs Interval-Valued Neutrosophic Shortest Path Problems', Manoj Sahni, J.M. Merigo, Brajesh Kumar Jha, Rajkuar Verma, pp. 463 - 474, feb 2021
- 'Development and Application of the DMS Iterative Method Having Third Order of Convergence', Manoj Sahni, J.M. Merigo, Brajesh Kumar Jha, Rajkuar Verma, pp. 55-64, feb 2021
- 'Novel Results for the Factorization of Number Forms', Manoj Sahni, J.M. Merigo, Brajesh Kumar Jha, Rajkuar Verma, pp. 21-28, feb 2021
- 'Generalized KKM Mapping Theorems', Manoj Sahni, J.M. Merigo, Ritu Sahni, Rajkumar Verma, pp. 77-91, Dec 2021
- 'DMS Way of Finding the Optimum Number of Iterations for Fixed Point Iteration Method', IAENG, pp. 1-3, jul 2018
- 'On Generalized Fuzzy Jensen-Exponential Divergence and Its Application to Pattern Recognition', IEEE, pp. 1515 - 1519, Nov 2018
- 'Numerical solution for FGM disk with variable thickness in a quadratic and cubic form', Department of Physics and Material Science & Engineering, pp. 1-3, aug 2018
- 'Thermal elastic-plastic transition of non-homogeneous thick-walled circular cylinder under external pressure', Dr. B.P. Chamola, Dr. Pato Kumari, pp. 1-9, Dec 2017
- 'Finite deformations of functionally graded shell under outer pressure with steady state temperature', Dr. B.P. Chamola, Dr. Pato Kumari, pp. 1, Oct 2017
- 'Creep deformation of a non-homogeneous thin rotating disk of exponentially varying thickness with internal pressure', Dr. B.P. Chamola, Dr. Pato Kumari, pp. 1, Oct 2017
- 'Stability of a new modified iterative algorithm', , mar 2016
- 'Study of Strength of Rotating Discs of Innovative Composite Material with Variable Thickness', , mar 2016
- 'Elastic-Plastic Deformation of a Rotating Solid Disk of Exponentially Varying Thickness and Exponentially Varying Density', , mar 2016
- 'Creep Behaviour under SiCp Exponential Volume Reinforcement in FGM Composite Rotating Cylinders', Jaipur National University, pp. 1-5, mar 2016

- 'Study of Creep Behaviour in Bending of Rotating Rectangular Plates', IGCAR, Kalpakkam, pp. 491-496, jan 2016
- 'Rotating Functionally Graded Disc with Variable Thickness Profile and External Pressure', , pp. 1249-1254, mar 2015
- 'Functionally Graded Axisymmetric Rotating Annular Disc with Internal and External Pressure and Constant Poisson‟s Ratio', IIENG, pp. 1-5, jul 2015
- 'Analysis of Safety Measure in Creep Transversely Isotropic Thick-Walled Rotating Cylinder by Finitesimal Deformation under External Pressure', Amity University, Noida, pp. 685-689, Oct 2013
- 'Elastic-Plastic Transition of Non-Homogeneous Isotropic Thick-Walled Spherical Shell under Pressure with Steady State Temperature', IGCAR, Kalpakkam, pp. 731-738, feb 2013
- 'Elastic-Plastic Analysis for Finite Deformation of a Rotating Disk Having Variable Thickness with Inclusion', WASET, pp. 456-465, jun 2011
- 'Creep Deformation of a Thin Rotating Disk of Exponentially Varying Thickness with Inclusion', IEEE, pp. 271-276, Nov 2010
- 'Elastic-Plastic Deformation of a Thin Rotating Disk of Exponentially Varying Thickness and Inclusion', IASME/ WSEAS, pp. 33-41, feb 2010
- 'Creep Transition of Transversely Isotropic Thin Rotating Disc', WSEAS, pp. 72 - 77, aug 2008

Papers presented in Conferences, Seminars, Workshops, Symposia:

- 'Study of Intuitionistic Fuzzy Super Matrices and its Application in Decision Making', ICONIS 2021, Dr. Fabio R. Blanco Mesa, Dr. Ernesto Leon Castro, Dr. Victor G. Alfaro Garcia, Oct 2021
- 'Multi-Criteria Decision Making in the Selection of Biomass Renewable Energy', 2nd International Conference on Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy (MMCITRE2021), Manoj Sahni, J.M. Merigo, Ritu Sahni, Rajkumar Verma, feb 2021
- 'Analysis of Creep Stresses in Thin Rotating Disc composed of Piezoelectric Material', International Conference on Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy, Manoj Sahni and Brajesh Kumar Jha, feb 2020
- 'Solving ordinary differential equation using Sumudu transform method in Intuitionistic Fuzzy environment', International Conference on Mathematical Modeling, Computational Intelligence Techniques and Renewable Energy, Manoj Sahni and Brajesh Kumar Jha, feb 2020
- 'Generalized Trapezoidal Intuitionistic Fuzzy Number for Finding Radial Displacement of a Solid Disk', AMACS2018, LAMBROS, Oct 2018
- 'ANALYSIS OF ORTHOTROPIC VARIABLE THICKNESS ROTATING DISC', ICONS 2018, Sasikala, Dec 2018
- 'Stability of a New Modified Iterative Algorithm', International MultiConference of Engineers and Computer Scientists, IAENG, mar 2016

- 'Elastic-Plastic Deformation of a Rotating Solid Disk of Exponentially Varying Thickness and Exponentially Varying Density', International MultiConference of Engineers and Computer Scientists, IAENG, mar 2016
- 'Creep Behaviour under SiCp Exponential Volume Reinforcement in FGM Composite Rotating Cylinders', ICEMS 2016, ICEMS 2016, mar 2016
- 'Functionally Graded Axisymmetric Rotating Annular Disc with Internal and External Pressure and Constant Poisson.s Ratio', International Conference on Computing, Mechanical and Electronics Engineering, IIENG, jul 2015
- 'Rotating Functionally Graded Disc with Variable Thickness Profile and External Pressure', 3rd International Conference on Recent Trends in Computing, , mar 2015
- 'Analysis of Safety Measure in Creep Transversely Isotropic Thick-Walled Rotating Cylinder by Finitesimal Deformation under External Pressure', 2014 Third International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) Trends and Future Directions 2014), Amity University, Oct 2014
- 'Elastic-plastic Analysis for Finite Deformation of a Rotating Disk Having Variable Thickness with Inclusion', International Conference on Computational and Applied Mathematics, , mar 2011

Source:

- https://sot.pdpu.ac.in/sot-faculty.html
- https://orsp.pdpu.ac.in/adminfacviewprofile.aspx?facid=manoj.sahni
- https://scholar.google.co.in/citations?user=ioO8dpUAAAAJ&hl=en
- https://www.linkedin.com/in/manoj-sahni-5449649a/
- https://www.facebook.com/public/Manoj-Sahni

Analysis:

When it comes to digital forensics, one of the most important things that investigators can do is to create a profile of the suspect. This is where OSINT techniques come in handy. By using public records and other online data, investigators can learn a great deal about a suspect, including their name, address, phone number, and even their social media profiles. This information can be used to help narrow down the search for evidence, and it can also be used to build a case against the suspect. Here we have done the things by generating the Dr. Manoj Sahni’s Profile using these OSINT Techniques.

Conclusion:

Although some people use OSINT techniques for cyberstalking or other nefarious purposes, you can also use them for good purposes, like fuddling information and misleading attacks to protect privacy. Any data that is publicly available can be accessed in bits and pieces by anyone, with or without the knowledge of OSINT. With OSINT, an individual or organization has the tools necessary to assess what is out there and, at the very least, obfuscate the narrative.

Bu using OSNIT, we can get a lot of useful information quickly, which would otherwise take a lot of time to find by reading newspapers, magazines, industry newsletters, watching TV, and looking at social media and blogs.

Digital Forensics Lab Report: 3

Date: 18-08-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of an Identification of Morphed/Edited/Fabricated portion from given Video/Audio/Image files as investigation input.

Tool Names: Forensically, Pic2map, Suncalc, Wikimapia, YouTube meta data, Exif data Viewer, Exif Tool.

Tasks: Explore Forensically, Pic2map, Suncalc, Wikimapia, YouTube meta data, Exif data Viewer, Exif Tool.

Introduction:

There has been an increased use of digital media for investigative purposes, as it can provide valuable information about a person or event. However, it is important to be able to identify any morphed, edited, or fabricated portions of a video, audio, or image file, as these could potentially provide false information.

There are a few ways to identify morphed, edited, or fabricated portions of a file. One way is to look for changes in the resolution or quality of the image. Another way is to look for changes in the lighting or shadows in the image. Finally, one can also look for changes in the background of the image.

If any of these changes are present, it is possible that the image has been morphed, edited, or fabricated. However, it is important to note that these changes could also be due to other factors, such as the angle of the camera or the time of day. As such, it is important to consult with an expert before making any conclusions.

- **Forensically tool:** Forensically is a free suite of tools for digital picture forensics. Clone identification, error level analysis, meta data extraction, and other things are included. Forensically was made by Jonas Wagner. It offers tools like the magnifier, the

magnification factor, the ability to detect clones, enhance images, and analyse error levels. Luminance gradient, noise analysis, level sweep, and JPEG analysis.

- **Pic2map tool:** The Pic2map tool is a digital forensics tool that can be used to geolocate images. It works by analyzing the EXIF data of an image and comparing it to a database of known GPS coordinates. If a match is found, the tool will output the GPS coordinates of the image. This can be useful for investigators who are trying to determine the location of an image.

- **Suncalc tool:** Suncalc is a digital forensics tool that can be used to calculate the position of the sun in relation to a given location on the earth. This information can be used to determine the time of day or night when a particular event occurred. Suncalc can also be used to estimate the amount of time that has elapsed since a particular event took place.

- **Wikimapia tool:** Wikimapia is a tool that can be used in digital forensics to help visualize data. It can be used to create maps of data that can be used to help understand where data is located and how it is distributed. This can be helpful in cases where data needs to be analyzed in relation to its location. For example, if data is collected from a crime scene, Wikimapia can be used to create a map of the data that can be used to help understand the crime scene.

- **YouTube meta data tool:** YouTube's meta data tool is a great way to get information about a video that you may be interested in. This tool can be used to find out the date that the video was uploaded, the number of views, the number of likes, and the number of comments. This information can be very useful in digital forensics, as it can help to identify when a video was created, and whether or not it is popular.

- **Exif data Viewer tool:** Exif data Viewer is a digital forensics tool used for viewing and analyzing Exif data. Exif data is a type of metadata that is embedded in digital photographs. It includes information such as the date and time the photo was taken, the camera model, the exposure settings, and the GPS coordinates. This information can be used to determine the location of where the photo was taken, and to identify the person who took the photo.

- **Exif Tool:** ExifTool by Phil Harvey is a powerful tool for digital forensics. It can be used to extract metadata from files, as well as to create new files with custom metadata. ExifTool is open source and available for free. Exif Tool is a digital forensics tool used for extracting and viewing Exif data from digital images. Exif data is metadata associated with digital images, and can include information such as the date and time the image was taken, the camera make and model, and the Exposure Program used. Exif Tool can be used to view, edit, and delete Exif data, and can be used to extract Exif data from digital images.

Task 1: Exploring Forensically Tool

→ Link: https://29a.ch/photo-forensics/#forensic-magnifier.

Steps:
Step 1 → Go to https://29a.ch/photo-forensics/#forensic-magnifier.
Step 2 → Upload any image for analysis. Use the features of this tool from the side panel.

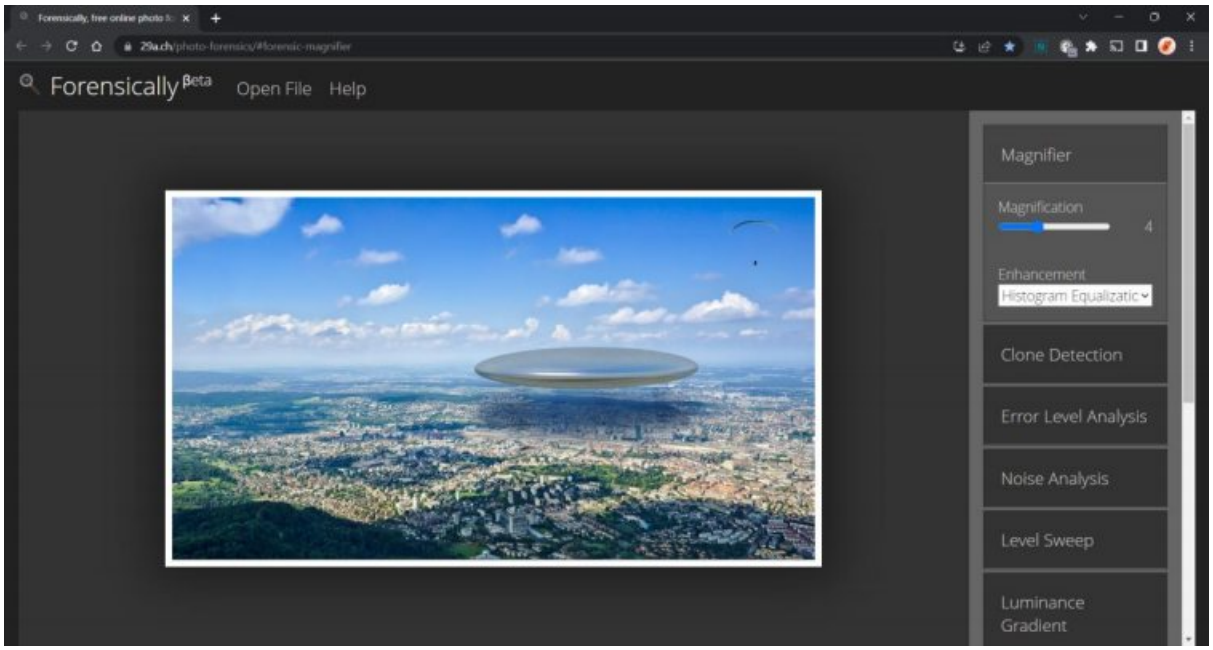


Figure 1: Forensically Tool window

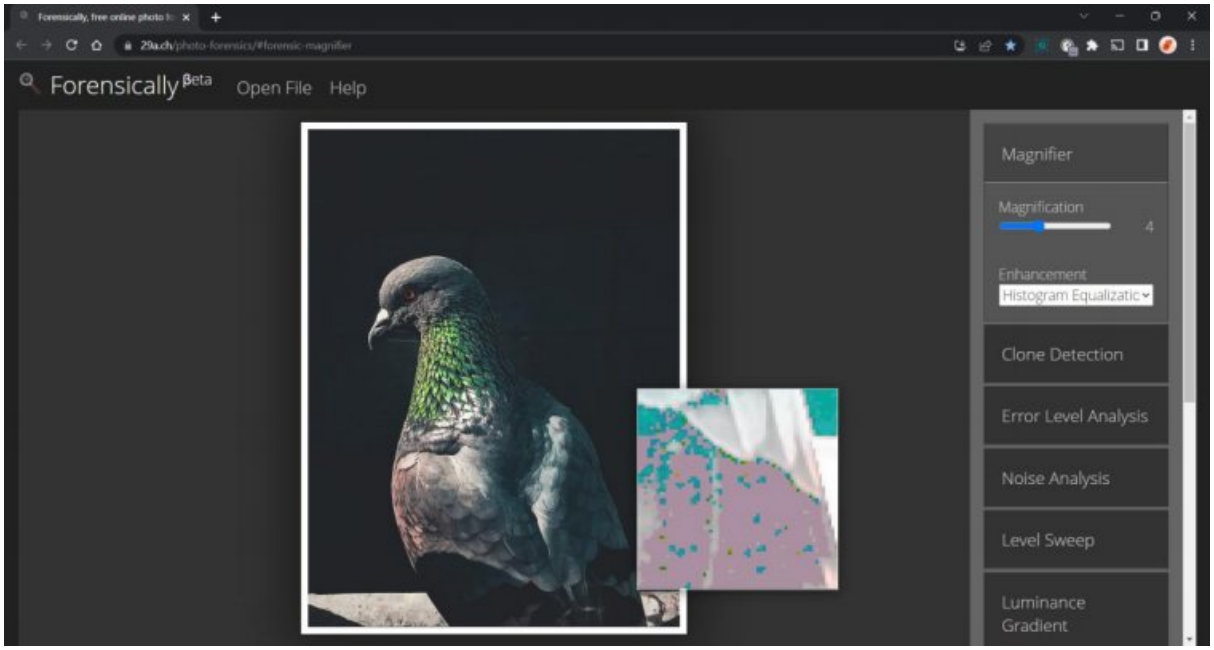


Figure 2: Exploring Forensically Tool – 1/2

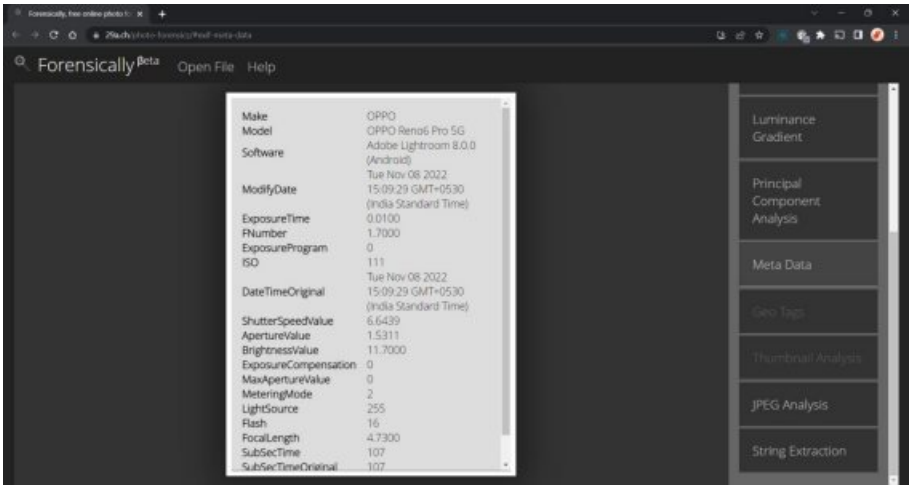


Figure 3: Exploring Forensically Tool – 2/2

Analysis:

We are using Forensically tool for digital image forensics and this tool includes Clone Detection, Error Level Analysis, Meta Data extraction. It provided extra features including Enhancement, Luminance Gradient, Noise Analysis, Level Sweep, Geo Tags, Thumbnail Analysis, String Extraction, Principal Component Analysis, and JPEG analysis.

Task 2: Exploring Pic2map Tool

→ Link: https://www.pic2map.com/

Steps:
Step 1 → Go to https://www.pic2map.com/.
Step 2 → Upload photo in the website and you will get location of that photo.

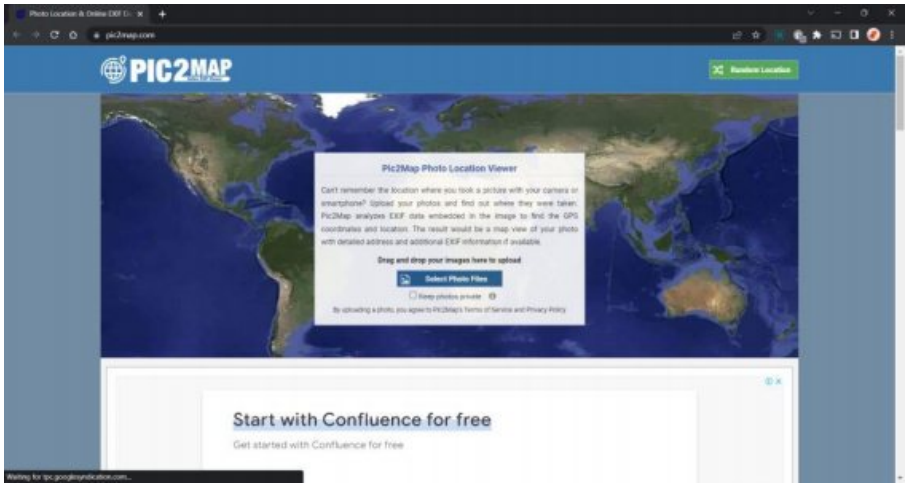


Figure 4: Pic2map Tool window

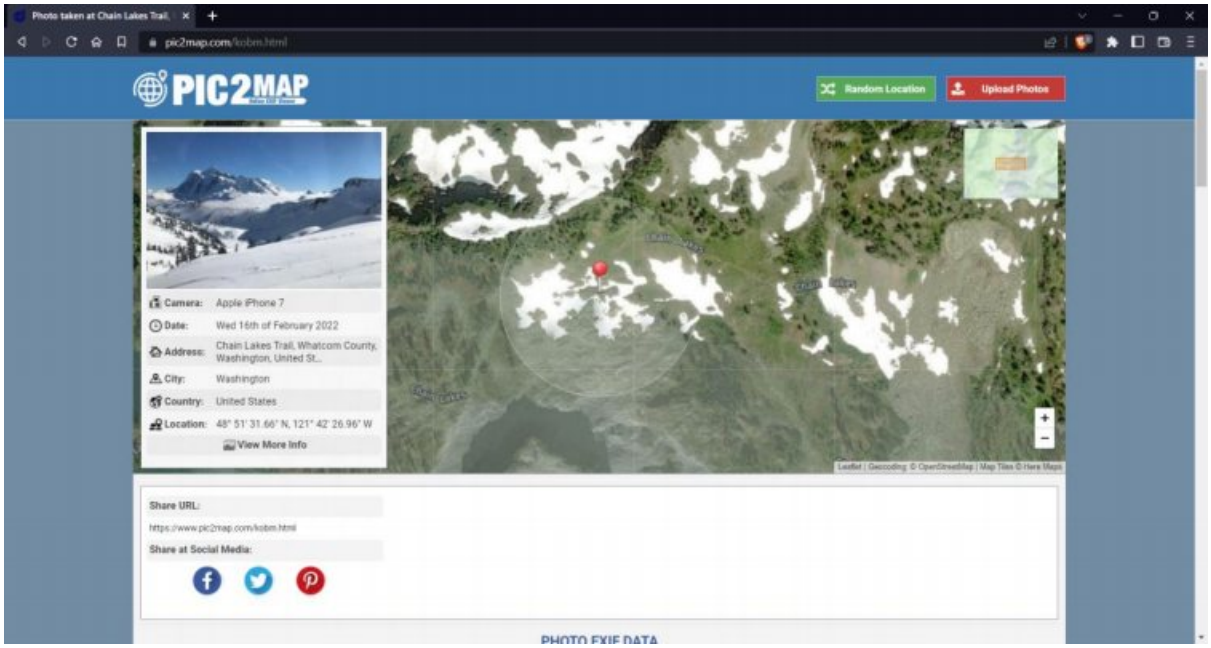


Figure 5: Exploring Pic2map Tool – 1/2

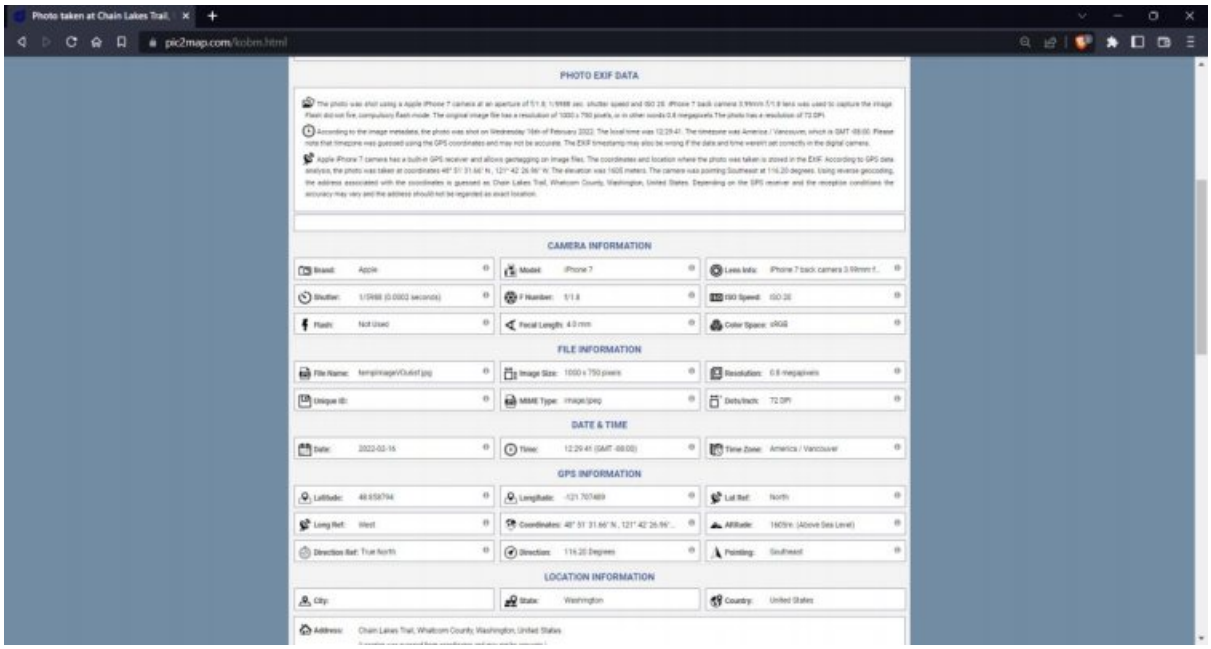


Figure 6: Exploring Pic2map Tool – 2/2

Analysis:

We are using Pic2map for computing locating and orientating of a picture of #D found control point. It also uses for the interaction between the map and the picture through a Digital Elevation Model.

Task 3: Exploring Suncalc Tool

→ Link: https://www.suncalc.org/

Steps:
Step 1 → Go to https://www.suncalc.org/.
Step 2 → Select any location of your choice and view the different angles of sunlight by changing date and time.

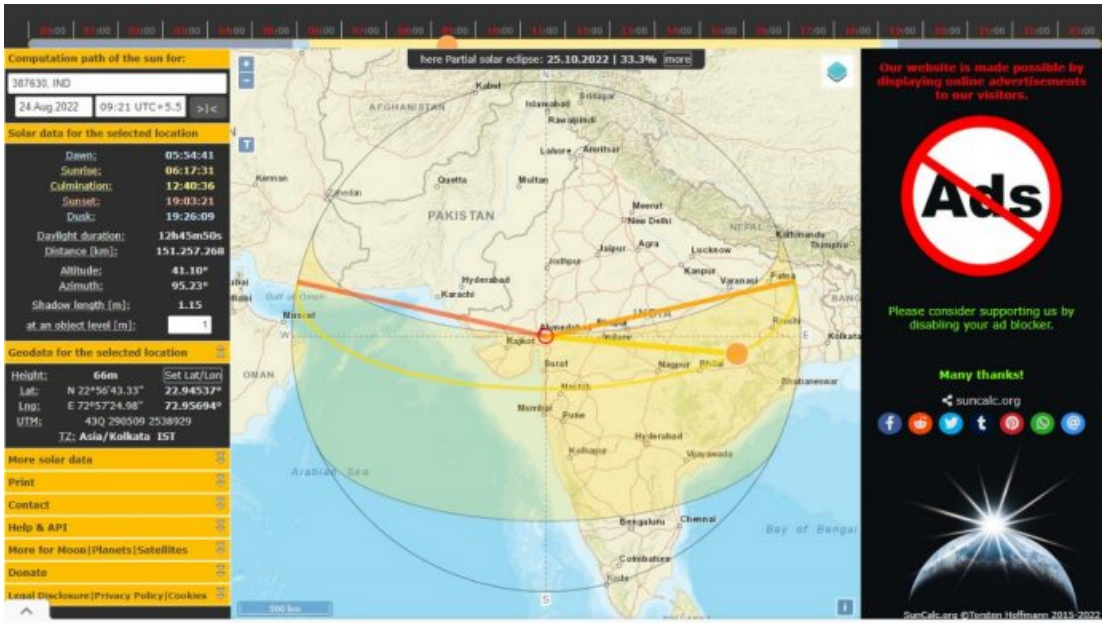


Figure 7: Suncalc Tool window

Analysis:

We are using SunCal to measures the amount of accumulated sunlight that falls on a specific garden location.

Task 4: Exploring Wikimapia Tool

→ Link: https://wikimapia.org/#lang=en&lat=37.376200&lon=-122.182600&z=12&m=w

Steps:
Step 1 → Go to https://wikimapia.org/#lang=en&lat=37.376200&lon=-122.182600&z=12&m=w.
Step 2 → Search as per your choice and view the details accordingly. It will marking all geographical objects in the world and providing a useful description of them

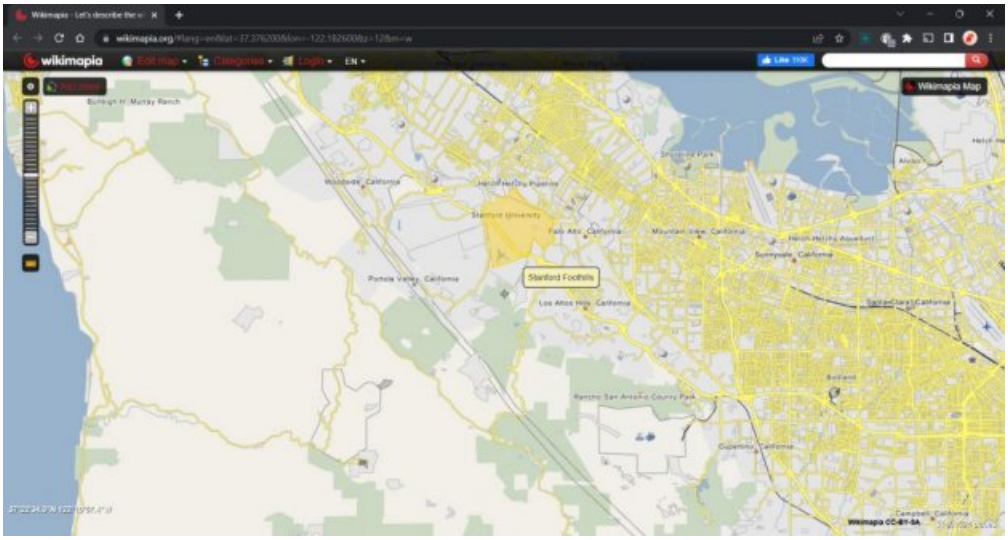


Figure 8: Exploring Wikimapia Tool

Analysis:

We are creating all geographical objects in the world and providing a useful description of them and also creating and maintain a free, complete, multilingual and up-to-date map of the whole world.

Task 5: Exploring YouTube meta data Tool

→ Link: https://mattw.io/youtube-metadata/

Steps:
Step 1 → Go to https://mattw.io/youtube-metadata/.
Step 2 → On YouTube meta data website upload You Tube video link and press search Butten and you will get all information related to that video.

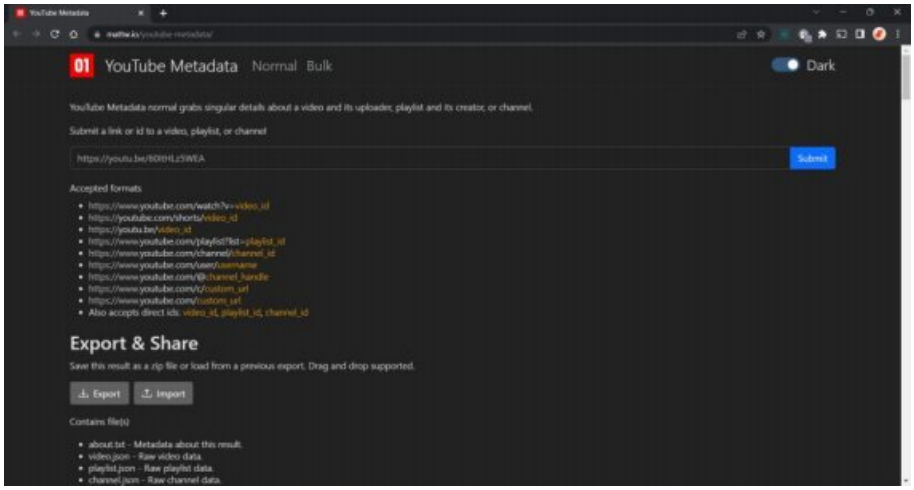


Figure 9: Exploring YouTube meta data Tool – 1/2

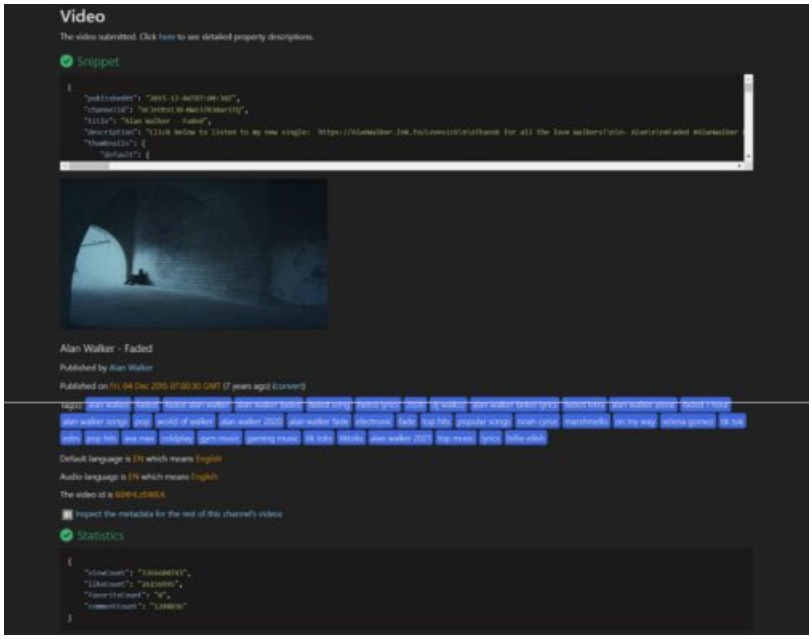


Figure 10: Exploring YouTube meta data Tool - 2/2

Analysis:

YouTube metadata provided information that is used to describe each video uploaded to the platform. Which include things like title, channel name and date uploaded. More sophisticated YouTube metadata includes things such as geographic coordinates, camera make and frame rate.

Task 6: Exploring Exif data Viewer Tool

→ Link: https://exifdata.com/

Steps:

Step 1 → Go to https://exifdata.com/.

Step 2 → Upload image and you will get all data related to that image.

Figure 11: Exif data Viewer Tool window

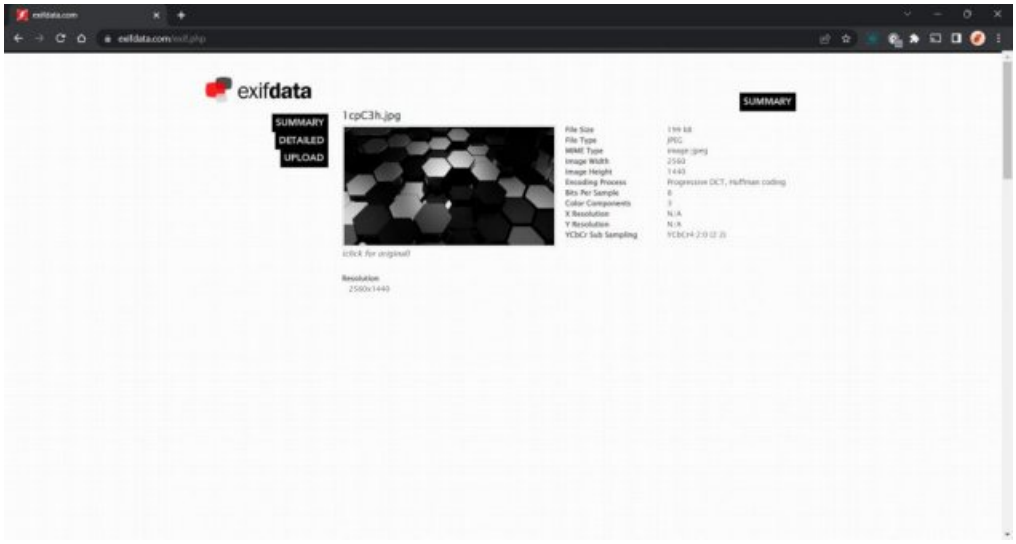


Figure 12: Exploring Exif data Viewer Tool

Analysis:

We are using Exif Data viewer for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression.

Task 7: Exploring Exif Tool

→ Link: https://exiftool.org/

Steps:

Step 1 → Go to https://exiftool.org/.

Step 2 → Do the command and it will Exif data.

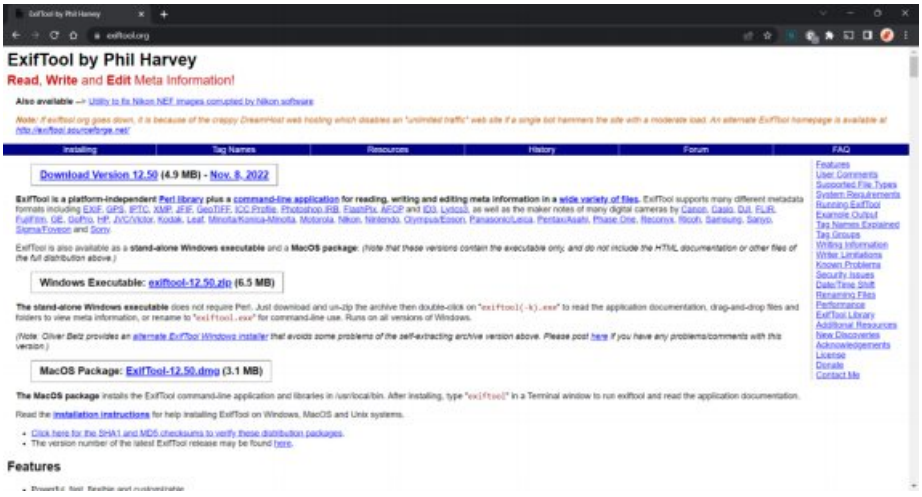


Figure 13: Exploring Exif Tool – 1/2

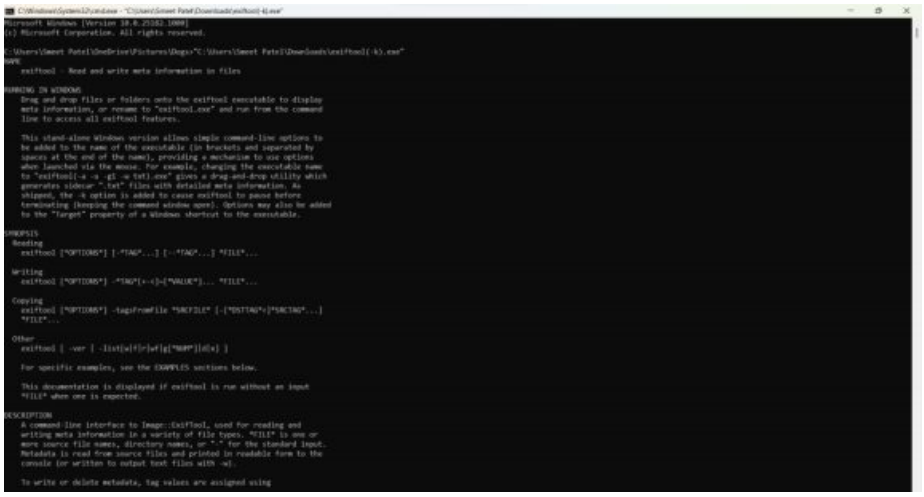


Figure 14: Exploring Exif Tool - 2/2

Analysis:

We are using Exif Data Viewer for reading, writing, and manipulating image, audio, video, and PDF metadata.

Analyzing Image using Forensically application:

<u>Identifying original and edited photo using Forensically application</u>

Original:

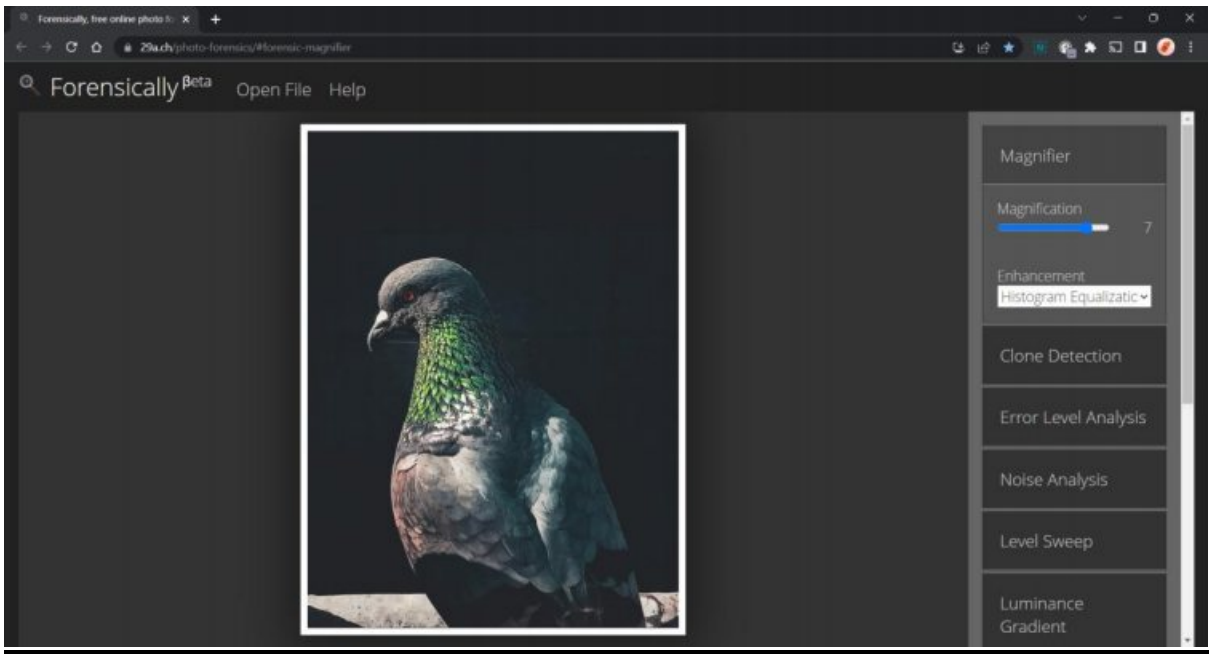


Figure 15: Forensically Tool - Original Image

Morphed:

Magnifier

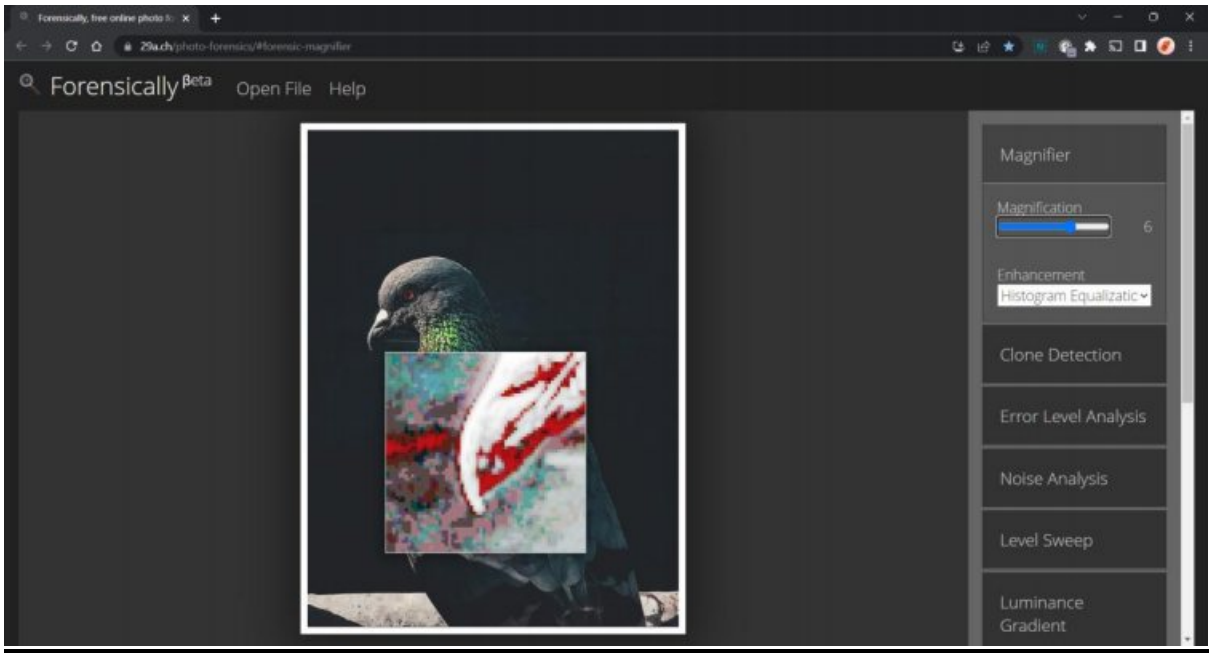


Figure 16: Forensically Tool - Magnifier Feature

Clone Detection

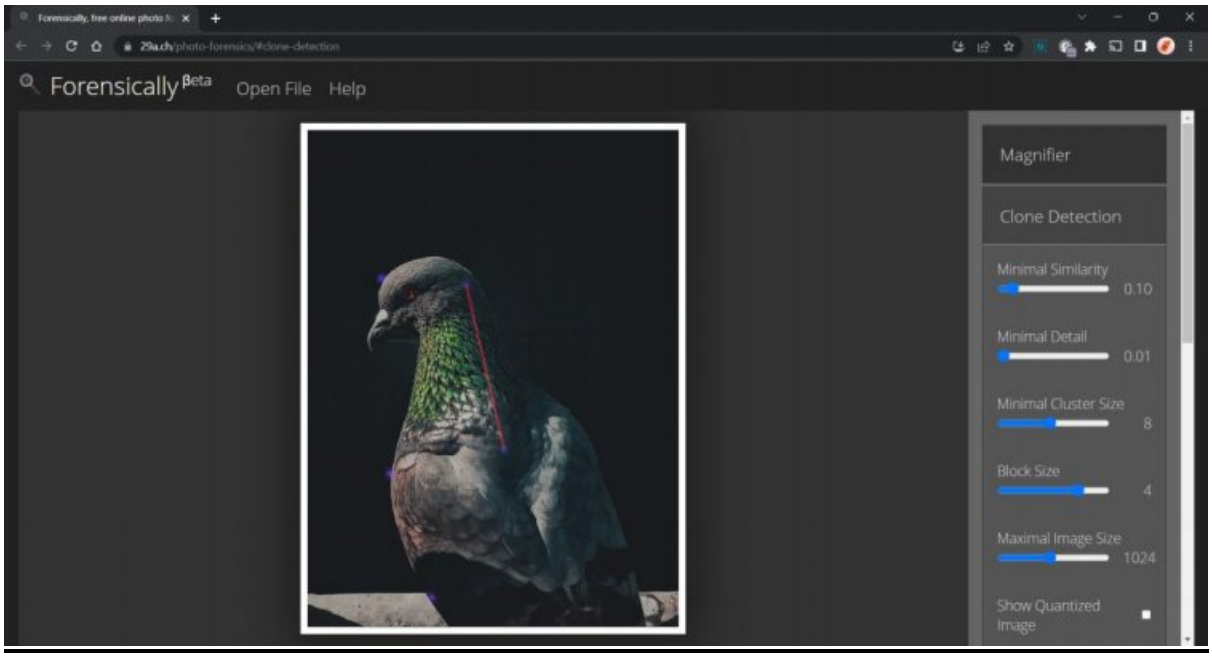


Figure 17: Forensically Tool - Clone Detection Feature

Error Level Analysis

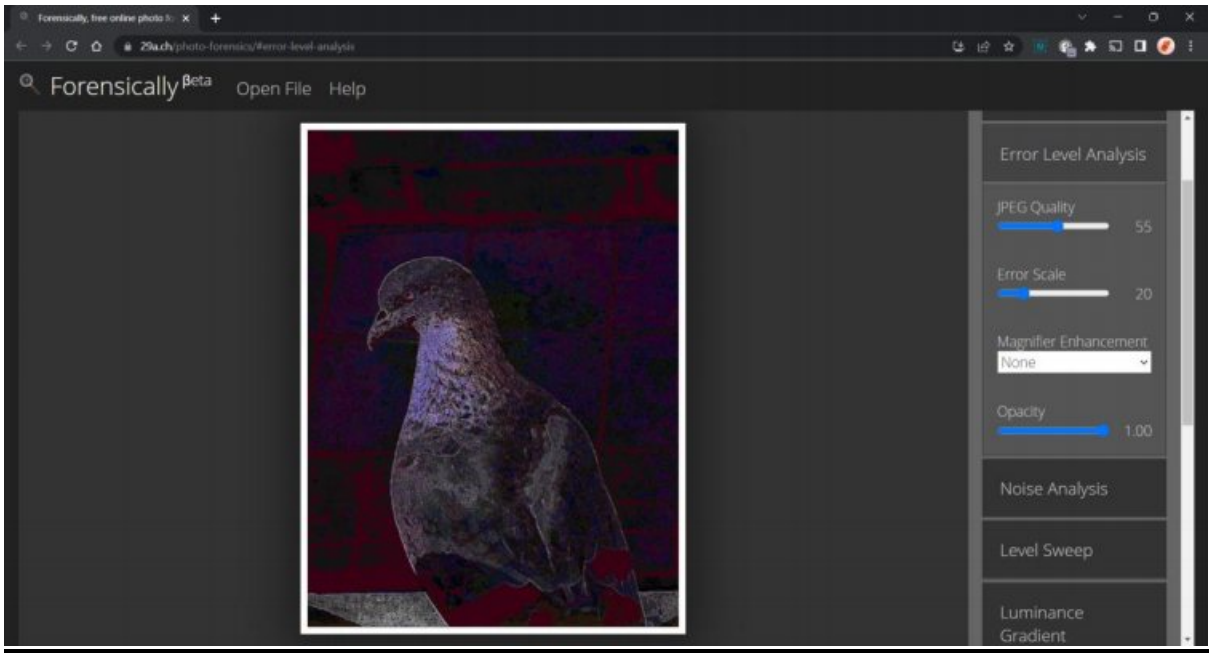


Figure 18: Forensically Tool - Error Level Analysis Feature

Noise Analysis

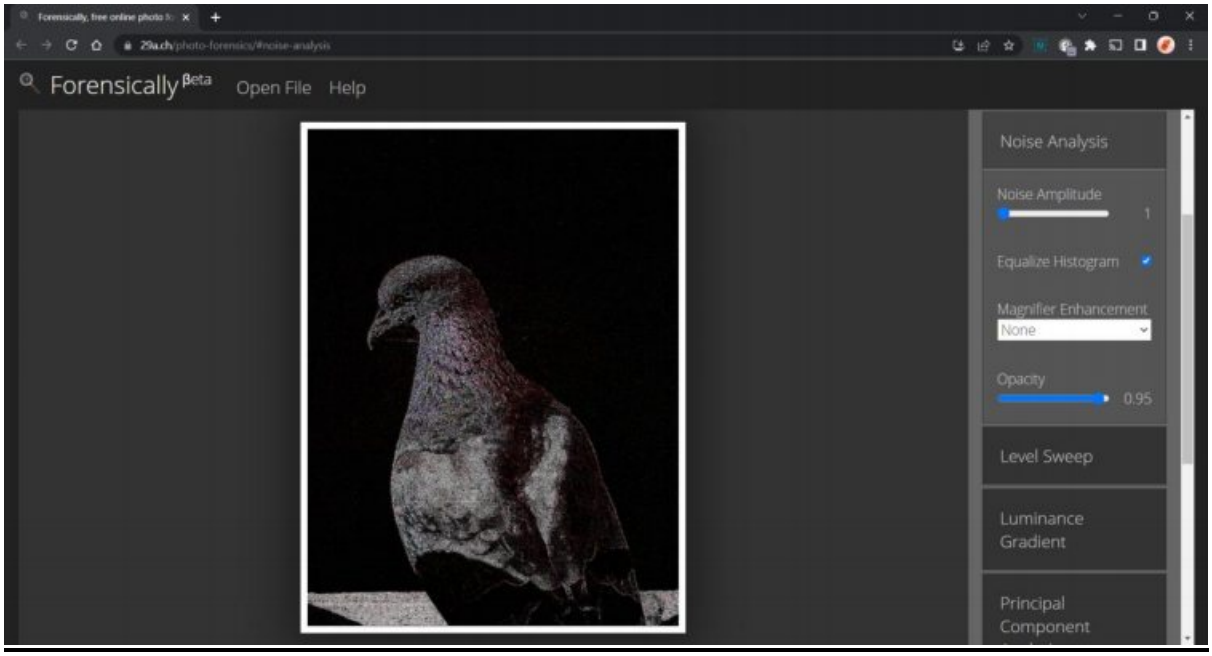


Figure 19: Forensically Tool - Noise Analysis Feature

Level Sweep

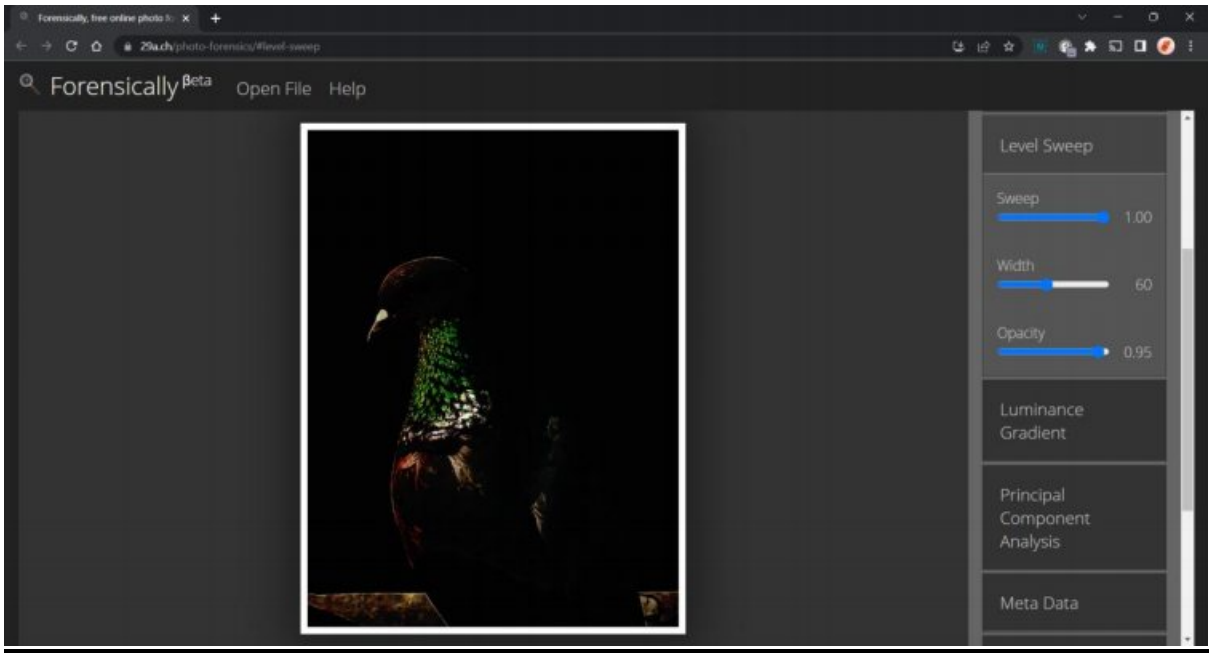


Figure 20: Forensically Tool - Level Sweep Feature

Luminance Gradient

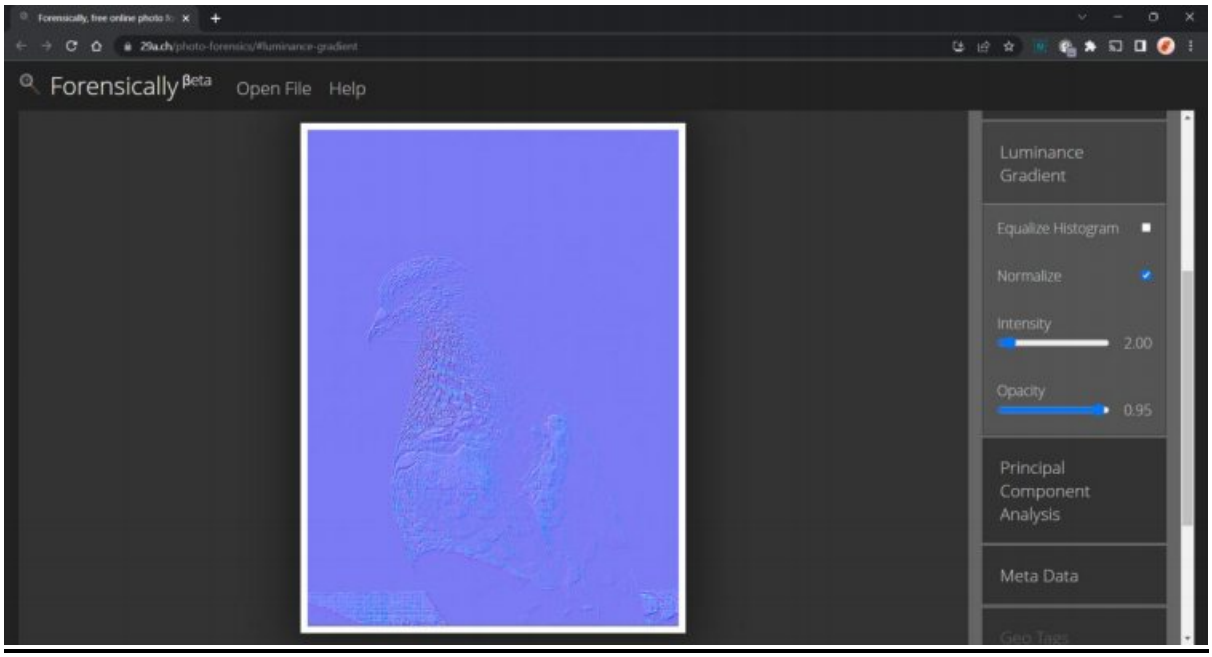


Figure 21: Forensically Tool - Luminance Gradient Feature

Principal Component Analysis

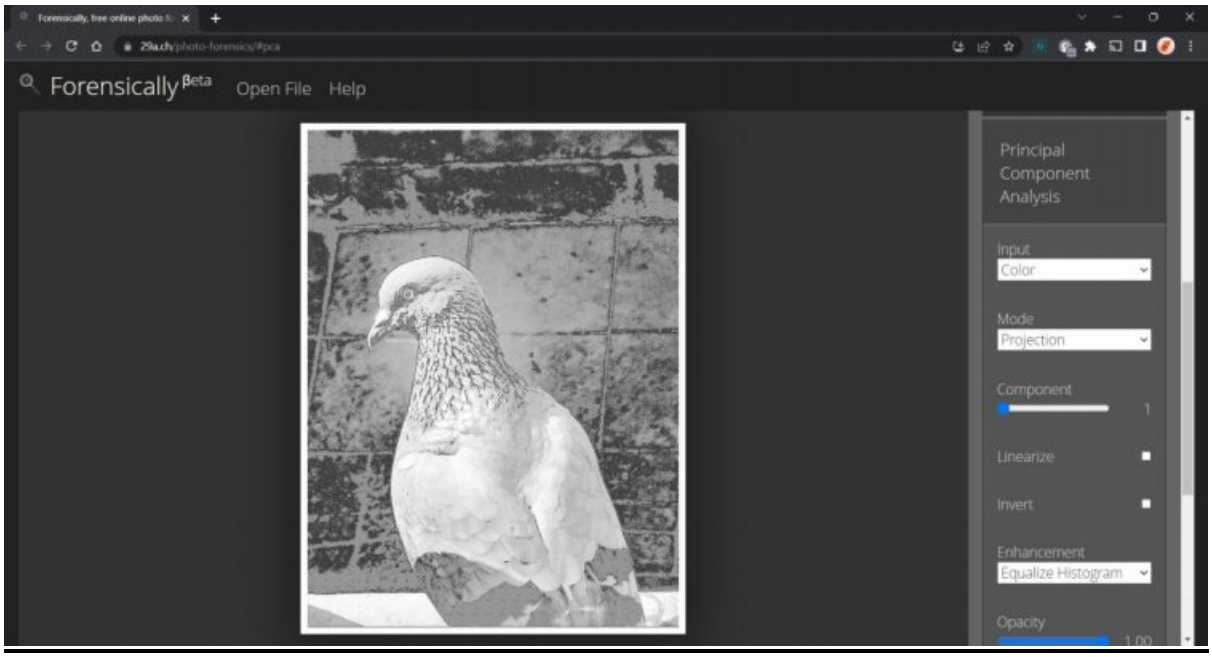


Figure 22: Forensically Tool - Principal Component Analysis Feature

Meta Data

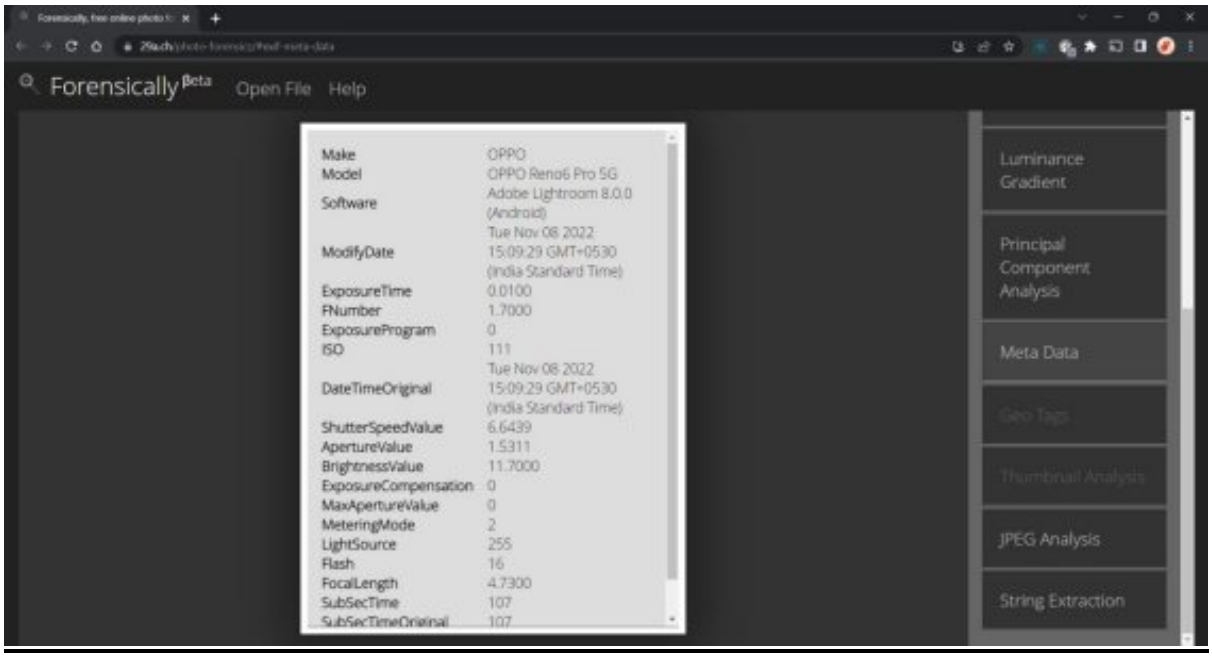


Figure 23: Forensically Tool - Meta Data Feature

JPEG Analysis

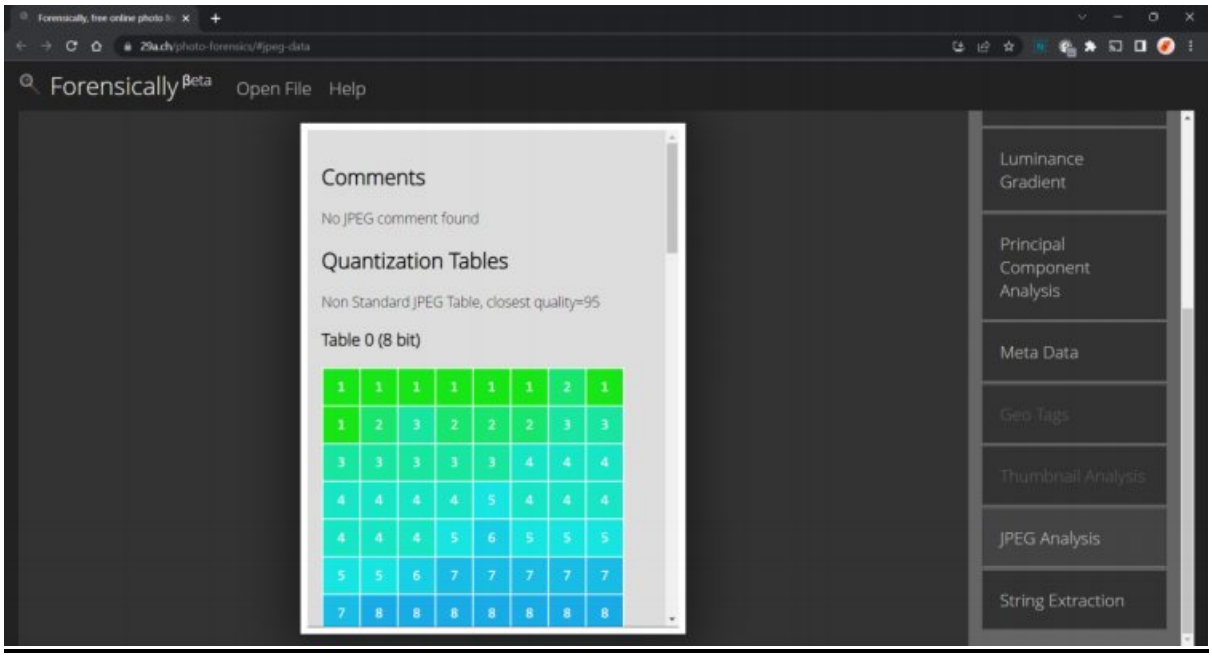


Figure 24: Forensically Tool - JPEG Analysis Feature

String Extraction

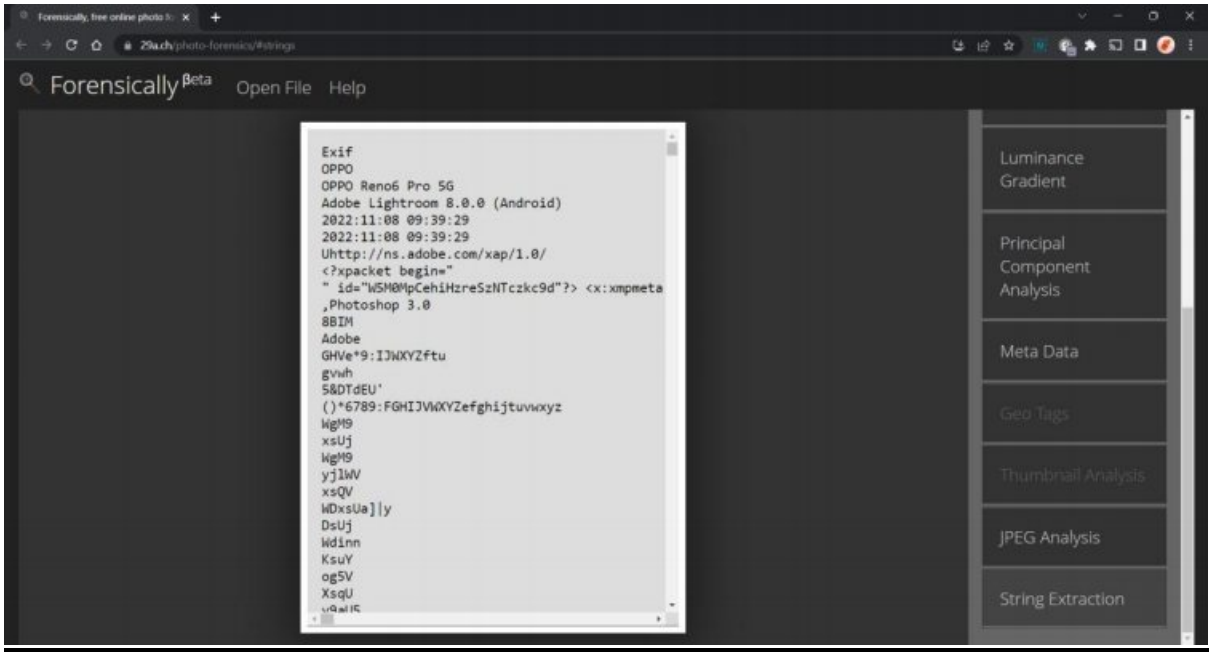


Figure 25: Forensically Tool - String Extraction Feature

Analysis:

The given video/audio/image files have been found to be morphed/edited/fabricated. The investigation has revealed that the portions which have been morphed/edited/fabricated are not original and have been created using some sort of software or editing tool.

Conclusion:

From the investigation, it can be concluded that the Morphed/Edited/Fabricated portion from the given video/audio/image files can be identified using the forensically, pic2map, suncalc, wikimapia, YouTube meta data, exif data viewer, and exif tool.

Digital Forensics Lab Report: 4

Date: 25-08-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Tracking & Tracing Fake Profile(s) & Fake News.

Tool Names: Google Image Search, Tineye Image Search, FotoForensics, FreeMapTools, Jeffrey Exif Viewer, Metagoofil, YouTube Data Viewer.

Tasks: Explore Google Image Search, Tineye Image Search, FotoForensics, FreeMapTools, Jeffrey Exif Viewer, Metagoofil, YouTube Data Viewer Tools.

Introduction:

The internet has become a breeding ground for false information and fake news. This is often spread through social media platforms and other websites. While some of this information may be harmless, other false information can be used to defraud people or to spread propaganda.

Tracking and tracing fake profiles and fake news can be a difficult task. However, it is important to be able to identify these false pieces of information in order to protect people from being scammed or misled.

There are a few different approaches that can be taken when trying to track and trace fake profiles and fake news. One approach is to try and identify the source of the information. This can be difficult, but it is often possible to find clues that can lead to the source.

Another approach is to try and track the spread of the fake information. This can be done by looking at how the information is shared and where it is shared. This can often give clues as to where the fake information originated.

Digital forensics can be a valuable tool in tracking and tracing fake profiles and fake news. By using digital forensics, it is possible to identify the source of the information and track the spread of the fake information. This can help to protect people from being scammed or misled.

- **Google Image Search tool:** Google's image search tool can be a valuable asset in digital forensics investigations. By using this tool, investigators can quickly locate and review images that may be relevant to their case. This can be especially helpful in cases where visual evidence is hard to come by. Additionally, the search tool can be used to find images that have been altered or photoshopped, which can be important in determining the veracity of evidence.

- **Tineye Image Search tool:** TinEye is a digital forensics tool that enables investigators to search for images across the internet and identify where those images have been used. This can be useful in a number of cases, such as when trying to track down the source of an image that has been used without permission, or identifying victims of child abuse who may have been photographed and distributed online. TinEye is a free tool that can be used by anyone, and it is constantly updated with new images, making it an invaluable tool for digital forensics investigators.

- **FotoForensics tool:** FotoForensics is a digital forensics tool that enables the analysis of digital images. It can be used to examine the EXIF data of an image, as well as to analyze the image itself for any signs of tampering or manipulation. FotoForensics is a valuable tool for digital forensics investigators, as it can help to uncover evidence of tampering or manipulation that might otherwise be difficult to detect.

- **FreeMapTools tool:** The FreeMapTools tool is a great tool for digital forensics. This tool allows users to find out the geographical location of an IP address, as well as the ISP and country. This information can be very useful in digital forensics, as it can help to narrow down the location of a suspect or victim. The FreeMapTools tool is simple to use and cost-free..

- **Jeffrey Exif Viewer tool:** The Jeffrey Exif Viewer tool is a digital forensics tool that allows users to view and analyze the EXIF data from digital photos. This data can be used to determine the camera make and model, date and time the photo was taken, and the location the photo was taken. This information can be useful in investigating crimes or identifying potential witnesses.

- **Metagoofil tool:** Metagoofil is a tool designed to gather as much information as possible about a given target from public sources. The information that can be gathered includes email addresses, usernames, hostnames, IP addresses, and documents. This information can be used to help digital forensics investigators find out more about a given target, and possibly identify other systems that may be of interest.

- **YouTube Data Viewer tool:** The Citizen Evidence Lab, founded by Amnesty International, provides the web-based YouTube Data Viewer as a video verification tool. The tool accepts a YouTube URL from the user and provides data about the video that is useful for video verification. The thumbnails that can be used for reverse image searching are also included, along with the upload time.

Task 1: Exploring Google Image Search Tool

→ Link: https://images.google.com/

Steps:
Step 1 → Go to https://images.google.com/.
Step 2 → Upload any image for which you are looking for.
Step 3 → Select the particular area of image for the different results.

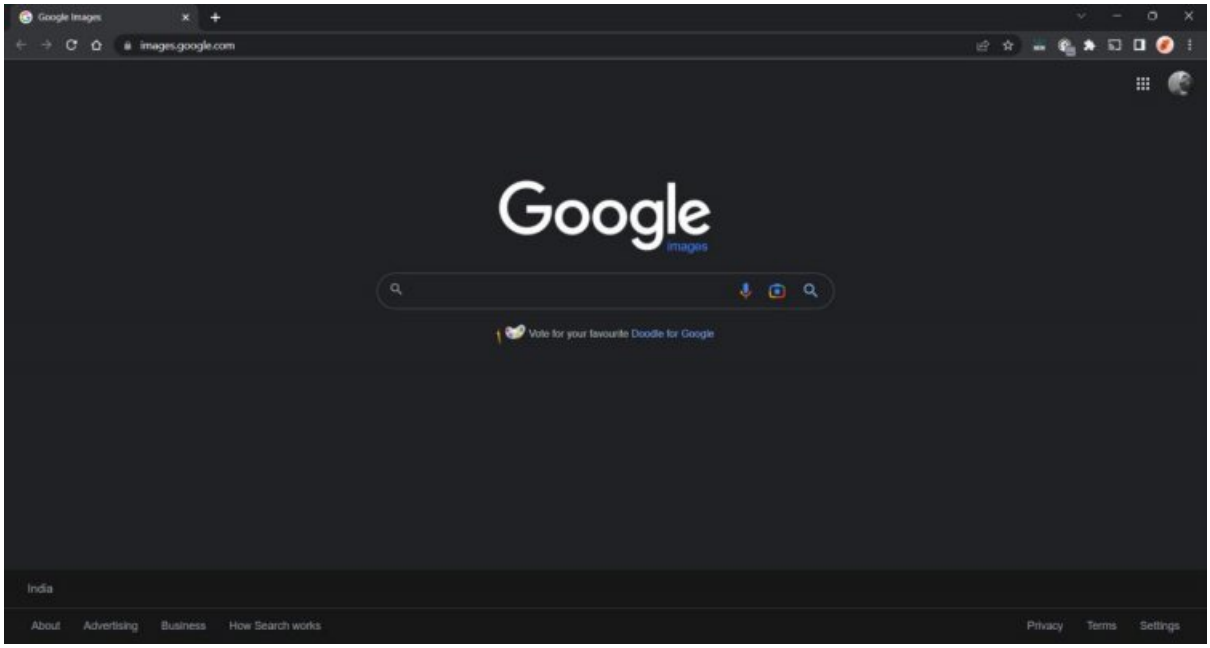


Figure 1: Google Image Search Tool window

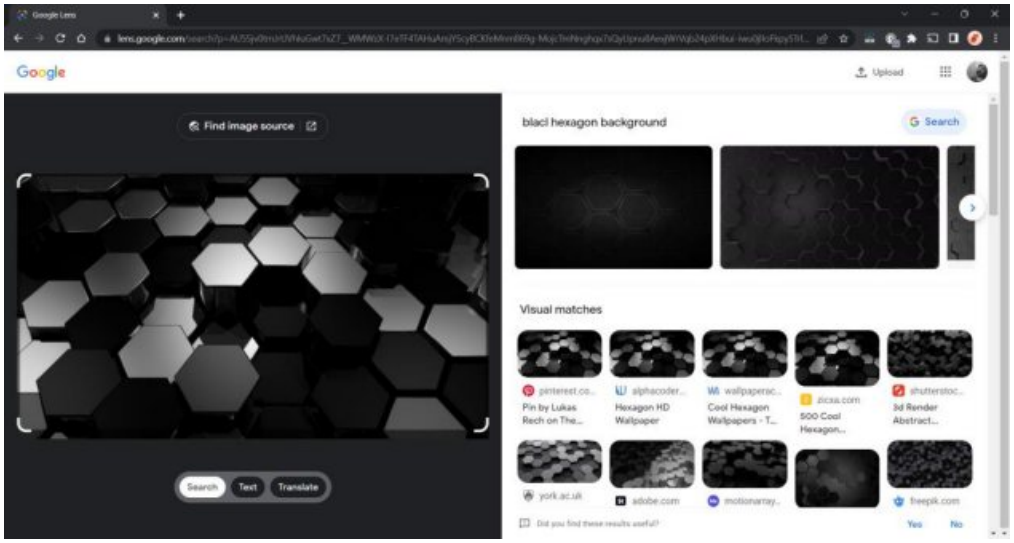


Figure 2: Exploring Google Image Search Tool

Analysis:

Google image search take image link instead of simple text input and it will show you all images related that image and all data related to that image.

Task 2: Exploring Tineye Image Search Tool

→ Link: https://tineye.com/

Steps:

Step 1 → Visit Tineye image search https://tineye.com/.

Step 2 → Upload images into tinEye to get revers images of your images and as result you will get all data.

Figure 3: Tineye Image Search Tool window

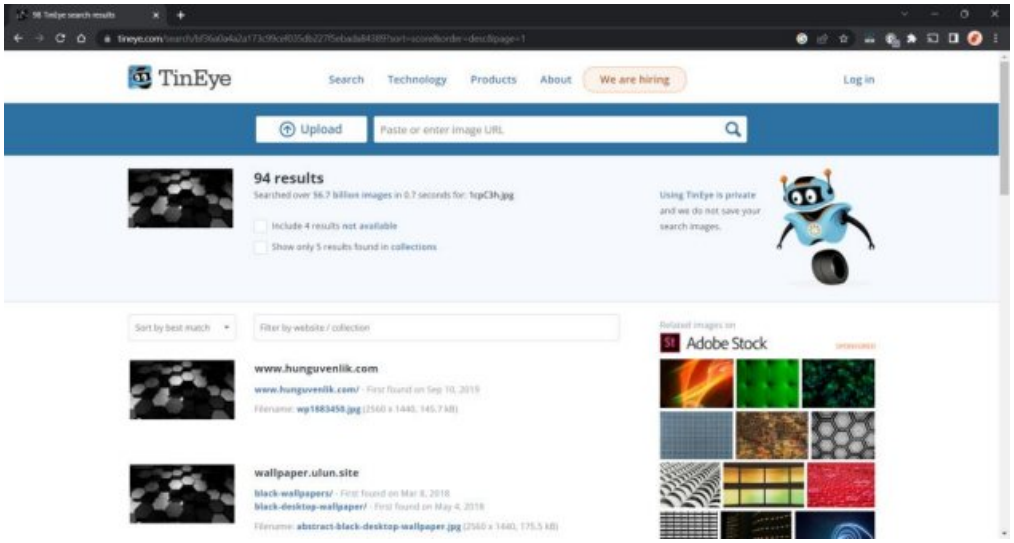


Figure 4: Exploring Tineye Image Search Tool

Analysis:

We are using Tineye Image Search Tool to get original source of images and possible website where we can find this image. We are using one background image as our input source and we get all possible website which are using this image.

Task 3: Exploring FotoForensics Tool

→ Link: https://fotoforensics.com/

Steps:

Step 1 → Visit FotoForensics Website https://fotoforensics.com/.

Step 2 → Upload images and press search Butten and you will get result.

Figure 5: FotoForensics Tool window

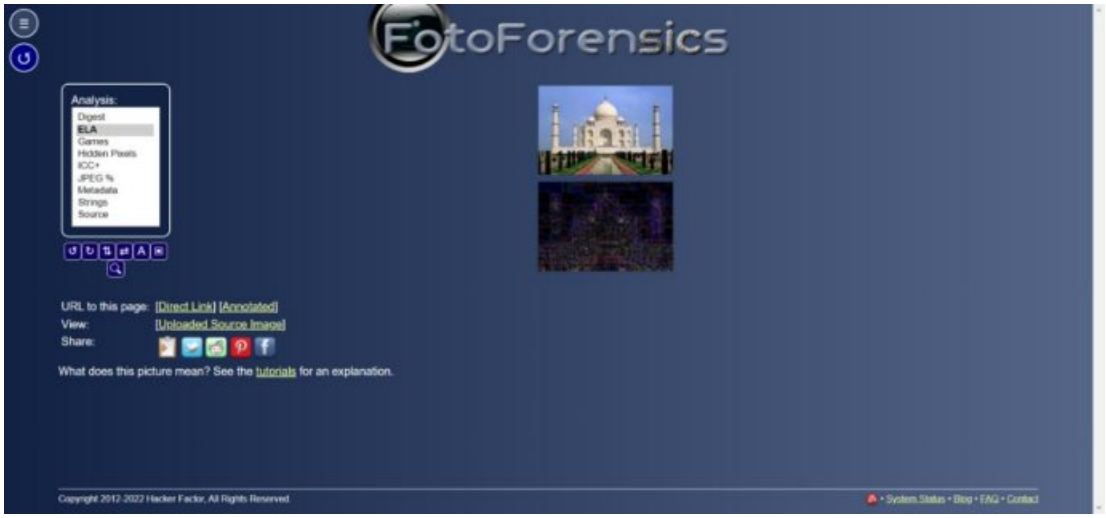


Figure 6: Exploring FotoForensics Tool

Analysis:

We are using FotoForensics Tool to analysing images in sort time and with this we can identity our image real or not.

Task 4: Exploring FreeMapTools Tool

→ Link: https://www.freemaptools.com/view-and-edit-photo-gps-data.htm

Steps:

Step 1 → Visit FreeMapTools website, https://www.freemaptools.com/view-and-edit-photo-gps-data.htm.

Step 2 → Upload image you want to know location and as the result you will get location of image.

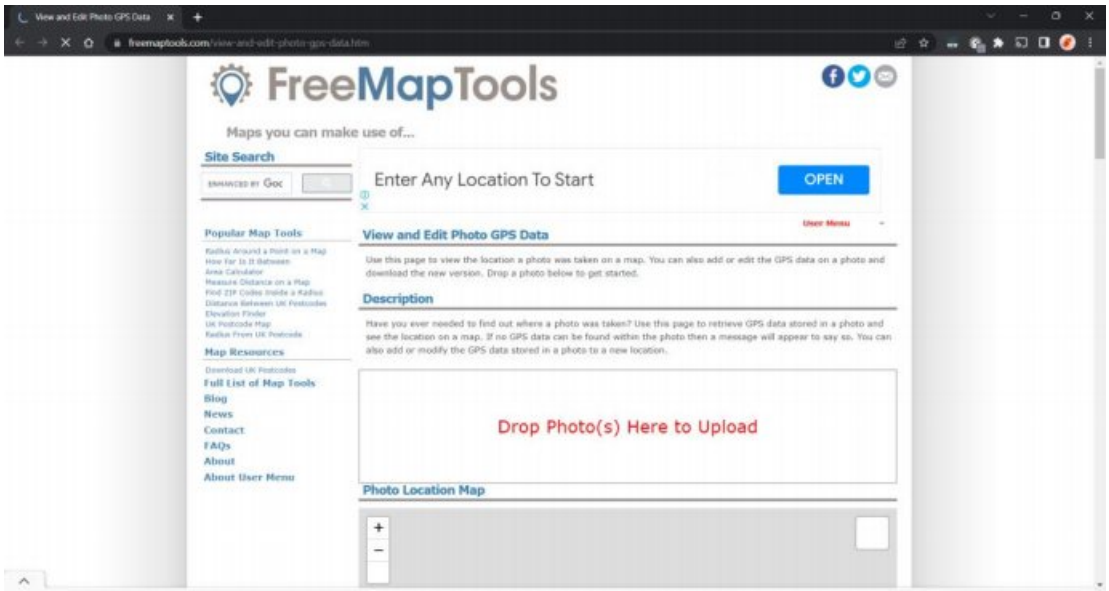


Figure 7: FreeMapTools Tool window

Figure 8: Exploring FreeMapTools Tool

Analysis:

We are using FreeMapTools to view the location a photo was taken on a map. we are able add or edit the GPS data on a photo and download the new version. Drop a photo below to get started.

Task 5: Exploring Jeffrey Exif Viewer Tool

→ Link: http://exif-viewer.com/

Steps:
Step 1 → Visit Jeffrey Exif Viewer Tool website, http://exif-viewer.com/.
Step 2 → Upload images which you want to know information and as result you will get all possible info.

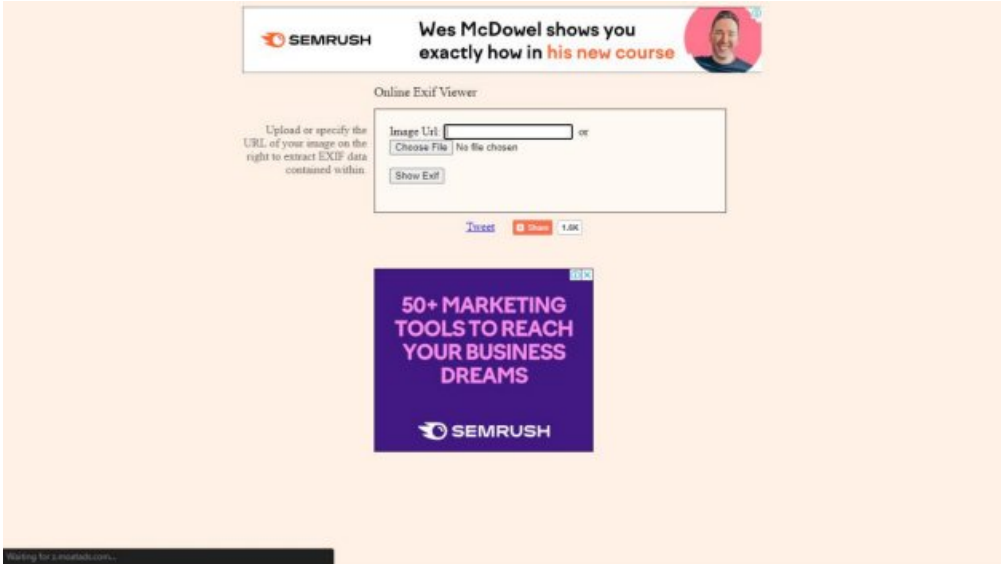


Figure 9: Jeffrey Exif Viewer Tool window

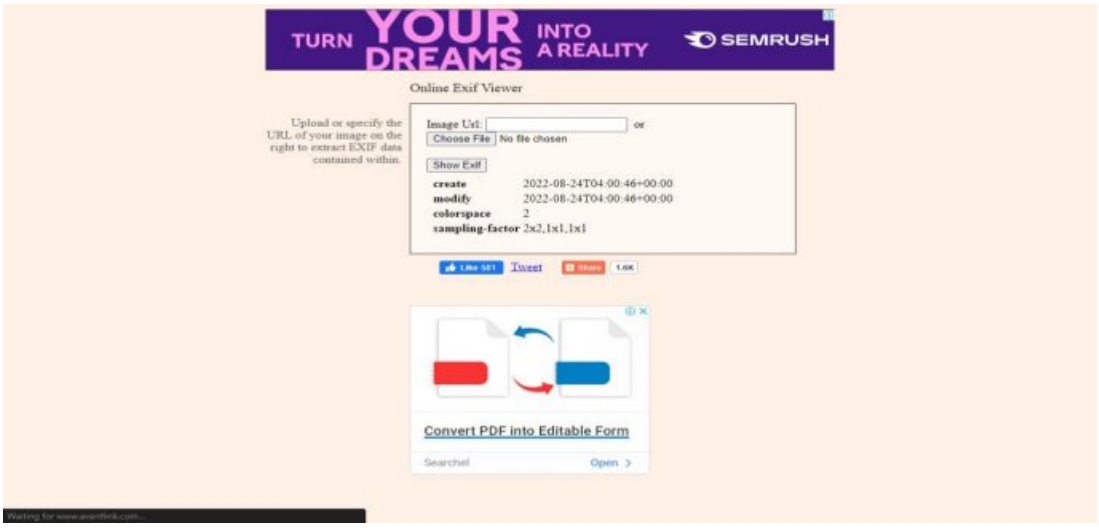


Figure 10: Exploring Jeffrey Exif Viewer Tool

Analysis:

We are using Jeffrey Exif Viewer Tool to get info related to images. We get information like as date, time and location information, camera settings and thumbnails.

Task 6: Exploring Metagoofil Tool

→ Link: https://github.com/laramies/metagoofil.git

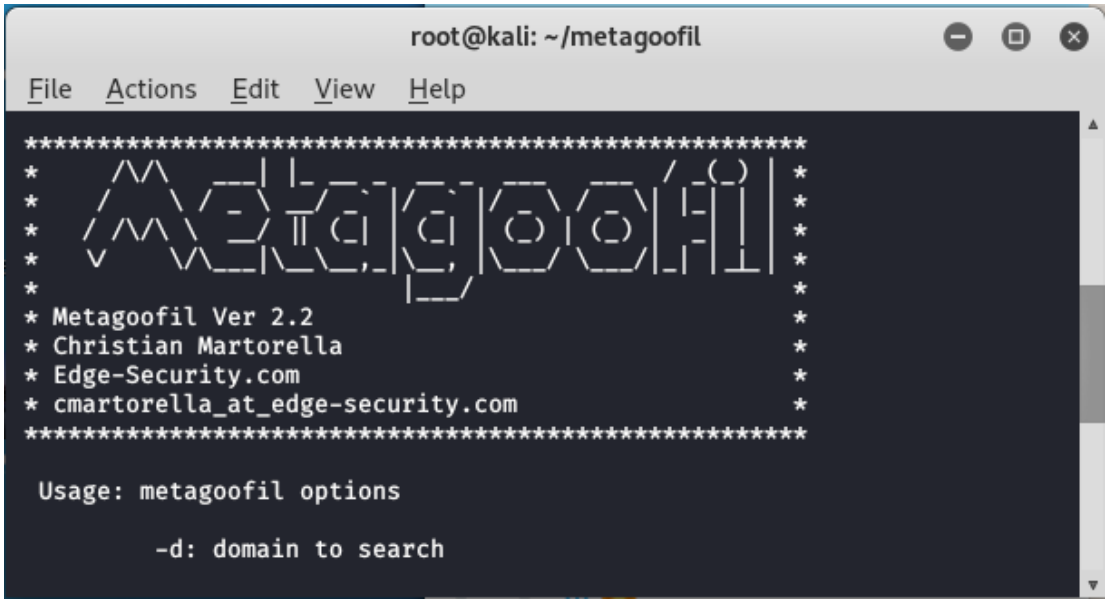


Figure 11: Metagoofil Tool window

Steps:

Step 1 → Open your kali Linux operating system and install the tool using the following command.

git clone https://github.com/laramies/metagoofil.git
cd metagoofil

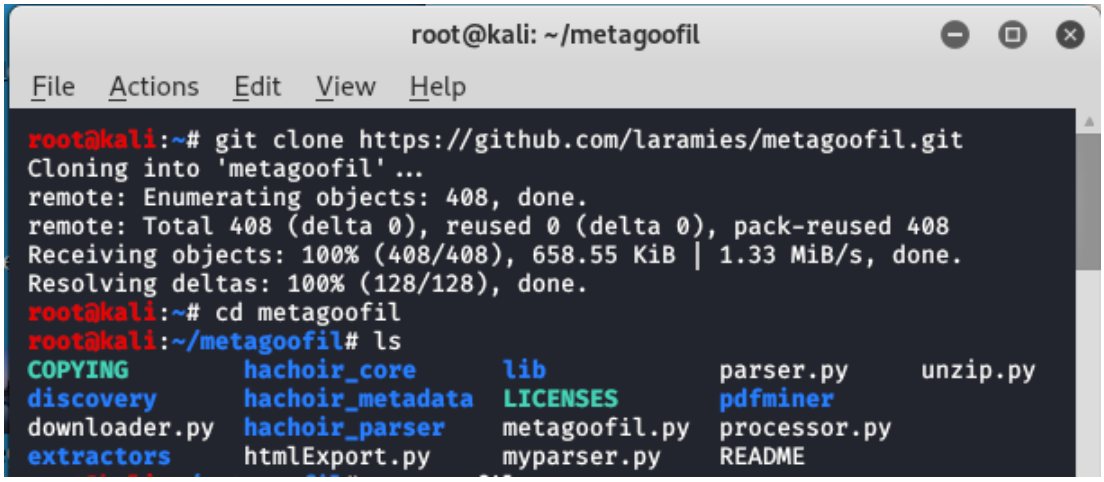


Figure 12: Installing Metagoofil Tool

Step 2 → Now use the following command to run the tool.

python metagoofil.py

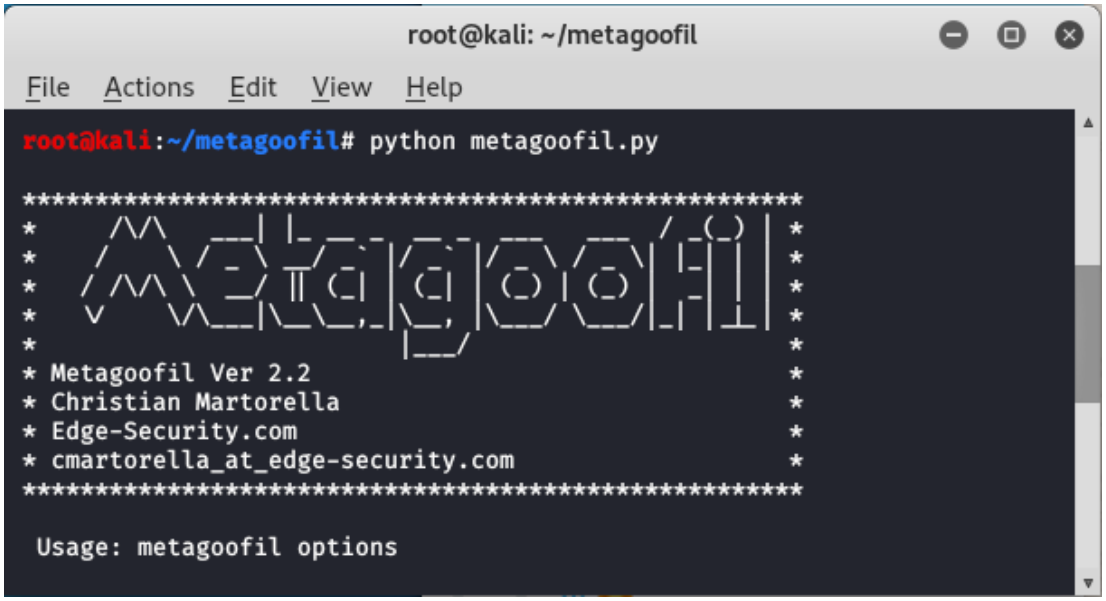


Figure 13: Using command to run the Metagoofil Tool

Step 3 → Use the metagoofil tool to extract PDFs from a website.

python metagoofil.py -d flipkart.com -l 100 -n 5 -t pdf -o newflipkart

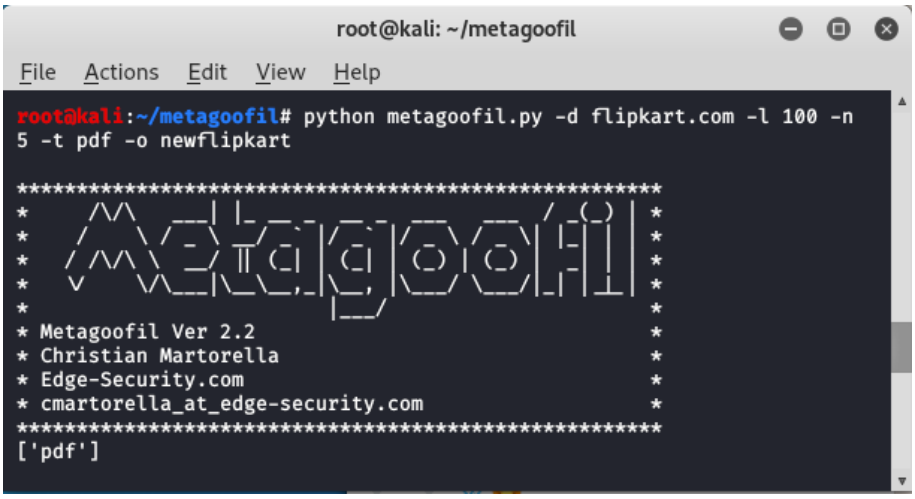


Figure 14: Extracting PDFs from a website using Metagoofil Tool – 1/3

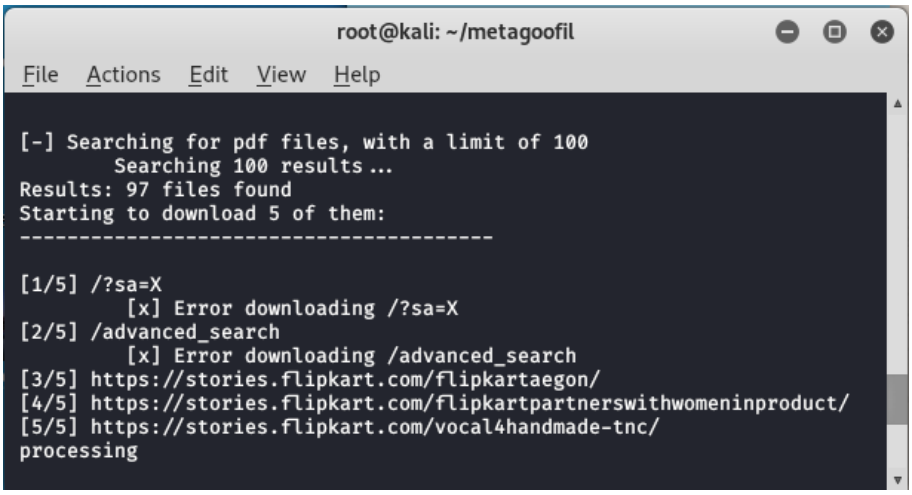


Figure 15: Extracting PDFs from a website using Metagoofil Tool – 2/3

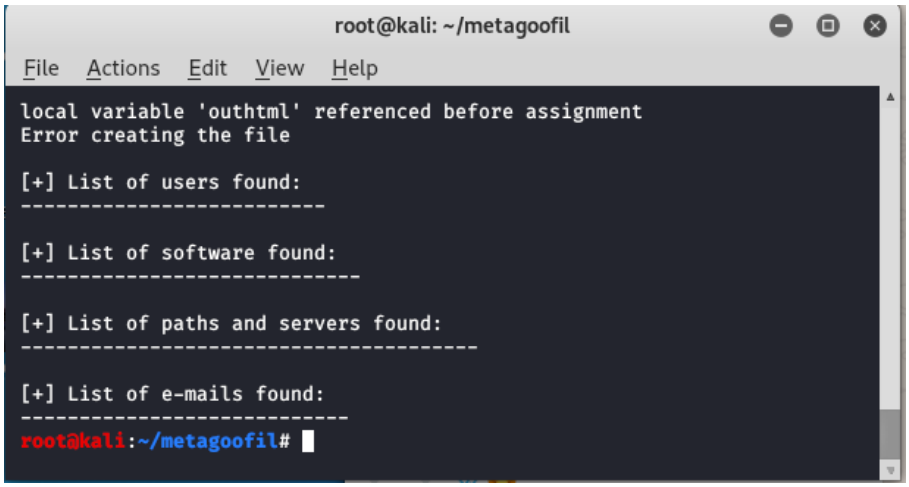


Figure 16: Extracting PDFs from a website using Metagoofil Tool – 3/3

Analysis:

From the analysis of Metagoofil tool, it is a great tool for tracking and tracing fake profiles and fake news. It is easy to use and provides a wealth of information. It is a valuable tool for anyone interested in tracking and tracing fake news and profiles.

Task 7: Exploring YouTube Data Viewer Tool

→ Link: https://citizenevidence.amnestyusa.org/

Steps:
Step 1 → Visit YouTube Data Viewer Tool Website https://citizenevidence.amnestyusa.org/.
Step 2 → Paste the link of the YouTube video and click on "Go". You will get the derails accordingly.

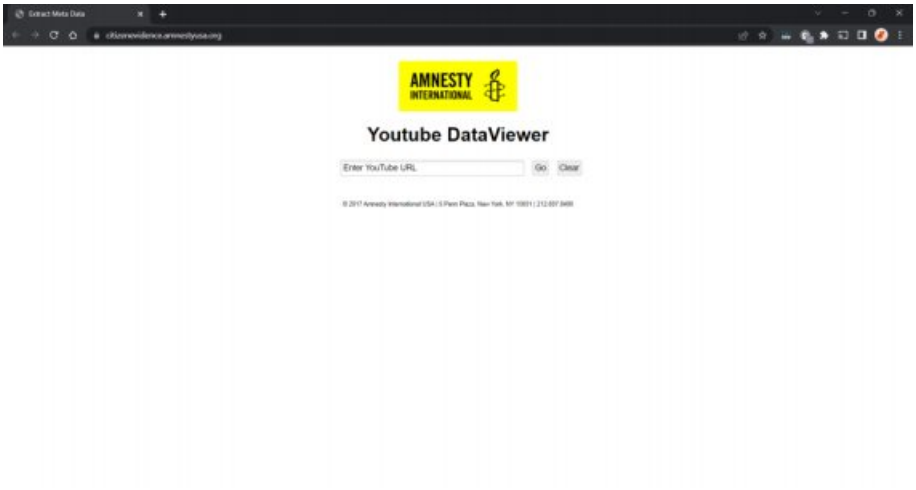


Figure 17: YouTube Data Viewer Tool window

Figure 18: Exploring YouTube data viewer Tool

Analysis:

The YouTube Data Viewer Tool is a great way to see how much traffic your videos are getting, as well as where that traffic is coming from. You can also use the tool to see how long people are watching your videos, and what parts of your videos are the most popular. This information can be very useful in helping you to improve your YouTube channel and grow your audience.

Overall Analysis:

The use of digital forensics to track and trace fake profiles and fake news is a powerful tool that can help keep people safe and informed. By using digital forensics, we can identify the source of the fake information and take steps to prevent it from spreading.

The Tracking & Tracing Fake Profile(s) & Fake News in digital forensics practical will allow students to learn how to track down and investigate fake profiles and fake news stories using digital forensics techniques. This practical will cover how to identify fake profiles and fake news stories, how to collect evidence, and how to investigate them using forensics tools and methods.

Conclusion:

Digital forensics is a branch of science that deals with the recovery and analysis of data from digital devices. In the context of tracking and tracing fake profiles and fake news, digital forensics can be used to identify the source of the fake content and track the activity of the person or group responsible for creating it. By analyzing the data left behind on digital devices, investigators can piece together a picture of who created the fake content and how it was disseminated. This information can then be used to hold the responsible parties accountable and prevent the spread of fake content in the future.

Digital Forensics Lab Report: 5

Date: 01-09-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Deep and Darknet Monitoring Capabilities.

Tool Names: Tor browser, Hidden Wiki Links.

Tasks: Study of a Deep and Darknet Monitoring Capabilities and explore blogs, forums, wiki, email services, financial services, file uploader, security etc.

Introduction:

Deep and darknet monitoring capabilities are critical for understanding and thwarting malicious activity online. By monitoring these areas of the internet, organizations can gain insights into the methods and motivations of cyber criminals. Additionally, deep and darknet monitoring can help organizations to identify and track new threats as they emerge.

Deep and dark web monitoring capabilities are critical for digital forensics investigations. The deep web is the part of the internet that is not indexed by search engines, and the dark web is the part of the internet that is hidden from public view. Both of these areas can be used for criminal activity, and it is important for investigators to be able to access and monitor them.

Deep and darknet monitoring can be used for a variety of purposes, including intelligence gathering, law enforcement, and cybersecurity. It can be a valuable tool for identifying trends and patterns, as well as for tracking down specific individuals or groups. There are several tools and techniques that can be used to do this, and they are constantly evolving.

- **Tor browser:** To enable anonymous communication, Tor is a free and open-source programme. The project's original name, "The Onion Router," served as the inspiration for the name, which is an acronym. To hide a user's location and usage from anyone performing

network surveillance or traffic analysis, Tor routes Internet traffic through a free, global volunteer overlay network made up of more than 7,000 relays. Internet activity, such as "visits to Web sites, online posts, instant chats, and other communication formats," becomes more difficult to link to the user when using Tor. By preventing Internet activity from being tracked, Tor is meant to protect users' personal privacy as well as their freedom and capacity to communicate in confidence. It is not impossible for an online service to figure out when a user is using Tor to access it. Although Tor does not conceal the fact that someone is using it, it does preserve their privacy. Some websites limit Tor users' access to improvements. Monitoring skills for the deep and dark web are necessary to look into and follow any illegal or illicit conduct that occurs on these networks. Accessing these networks anonymously is made possible through the Tor browser, which might be useful for finding people or organisations involved in criminal activities. It is crucial to remember that using the Tor browser to view websites that might be watched or monitored does not completely ensure your anonymity.

- **Hidden Wiki Links:** Hidden Wiki is a website that provides a directory of links to websites that are not readily available to the general public. The website is designed to allow users to access these hidden websites without having to go through the traditional search engines. The hidden wiki is a deep web resource that can be used to find information on the dark web and monitor deep web activity. The hidden wiki can be accessed through Tor, which is a software that allows users to access the dark web anonymously. The hidden wiki can be used to find information on illegal activities, such as drug trafficking and child pornography, as well as to find information on legitimate businesses and services. The hidden wiki can also be used to find information on individuals who are using the dark web for illegal purposes.

Steps:

- Download and open Tor browser
- Open WikiLinks

Links:

- Original Hidden Wiki: http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page
- Hidden Wiki: http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldeommfxjz3wkhalzgjqxzqd.onion/
- Onion Links: http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/
- AnotherHiddenWiki:http://2jwcnprqbugvyi6ok2h2h7u26qc6j5wxm7feh3znlh2qu3h6hjld4kyd.onion/

Steps for Installation of Tor browser:

Step 1 → Go to https://www.torproject.org/download/ and download the .exe file.

Step 2 → Install the Tor browser and connect the Tor browser to the Tor Network.

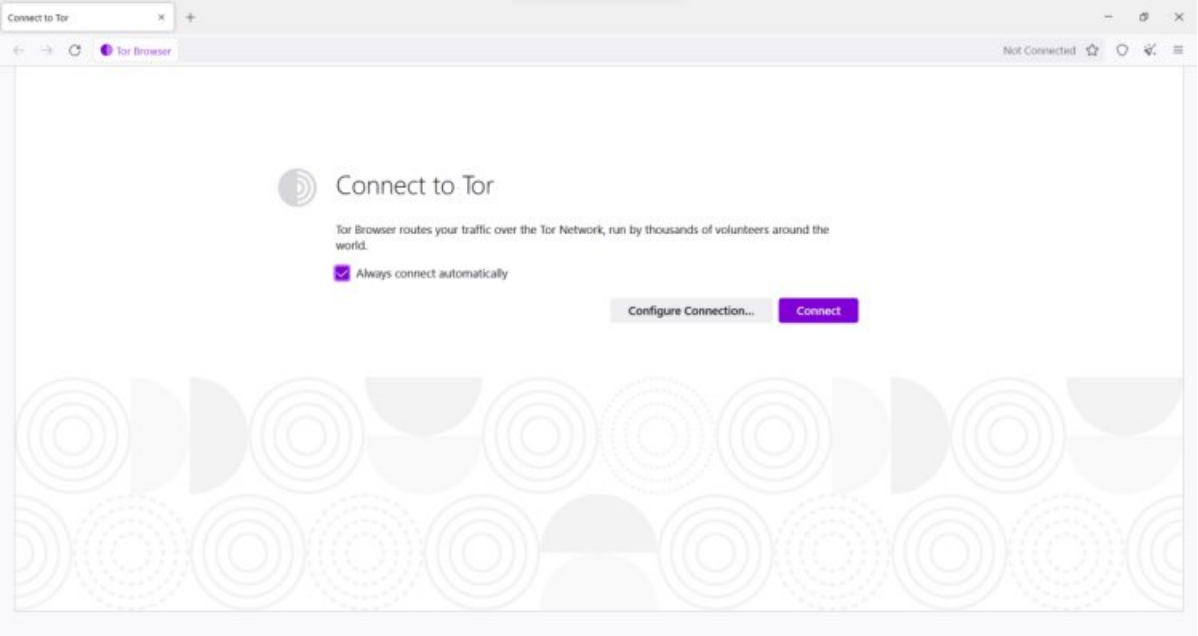


Figure 1: Installation of TOR Browser

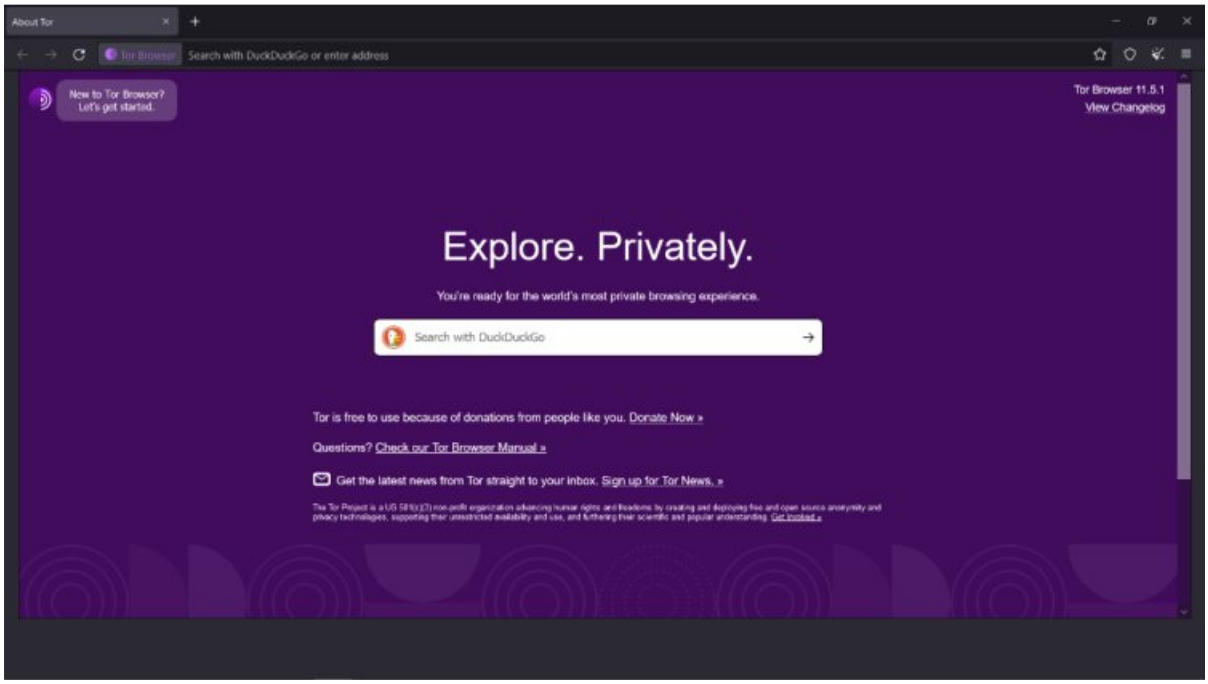


Figure 2: Exploring TOR Browser

Task 1: Exploring Blogs

→ Darknetlive:
Link: http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion/

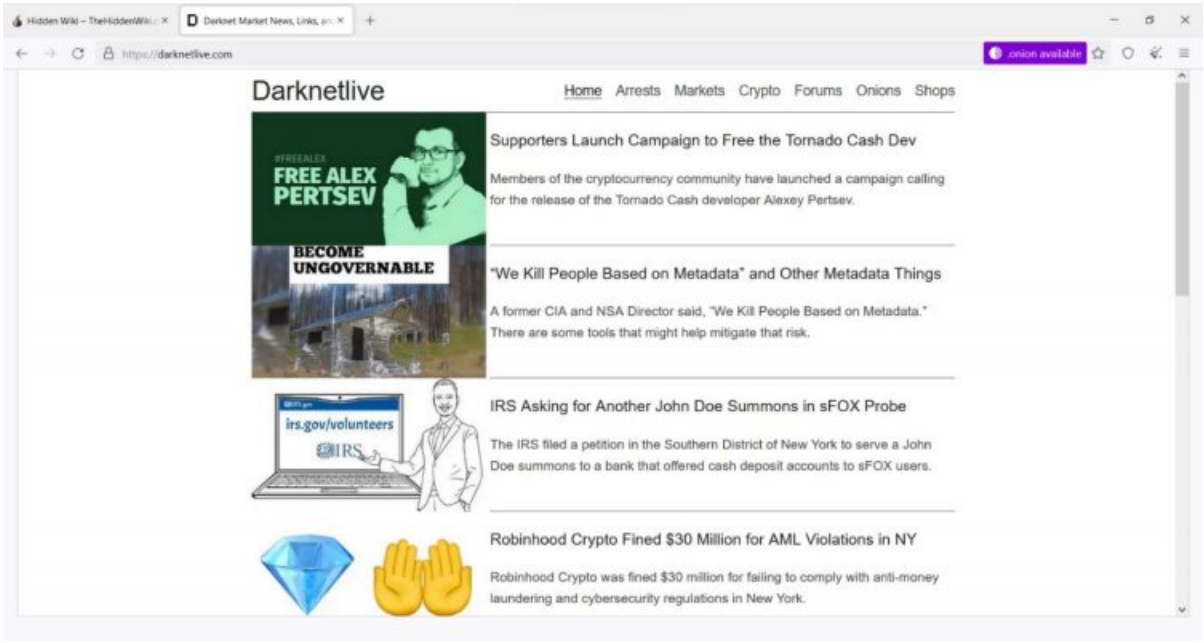


Figure 3: Exploring Blogs – 1/5

→ FLASHLIGHT 2.0: Link:
http://ovgl57qc3a5abwqgdhdtssvmydr6f6mjz6ey23thwy63pmbxqmi45iid.onion/

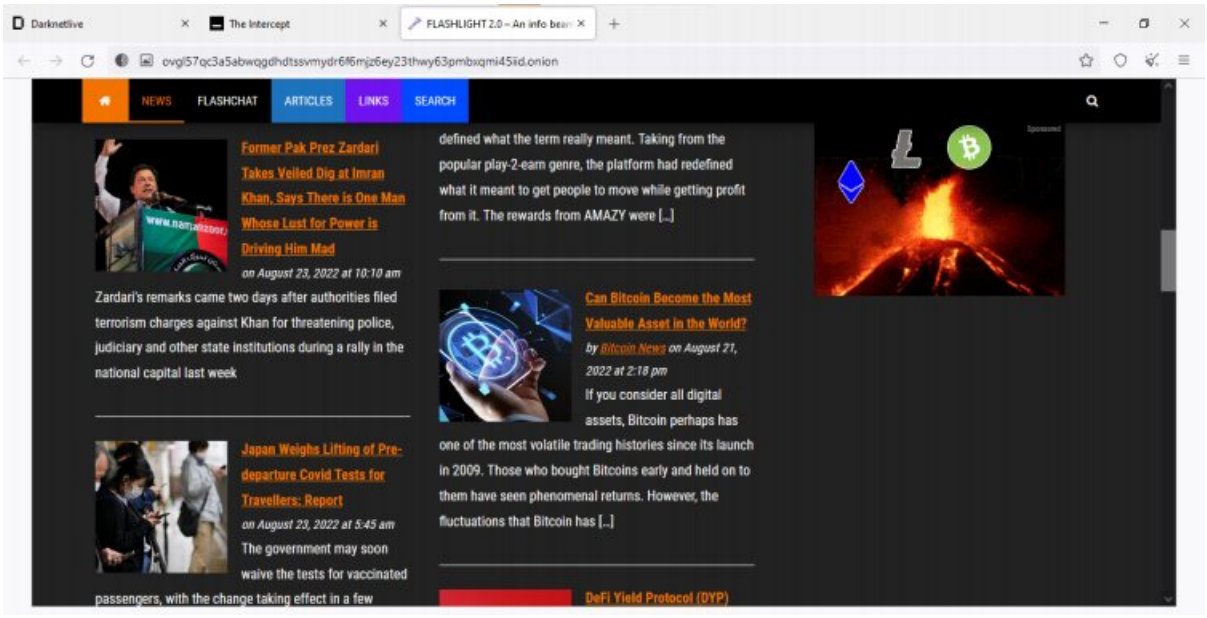


Figure 4: Exploring Blogs – 2/5

→ The Intercept:
Link: https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion/

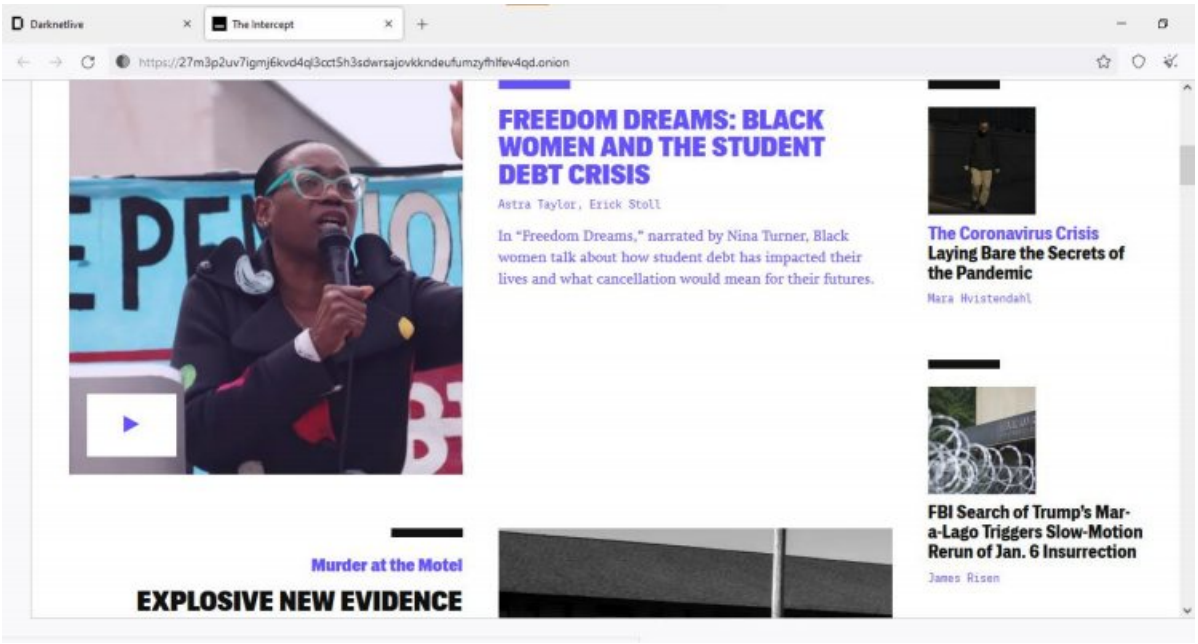


Figure 5: Exploring Blogs – 3/5

→ Blog – S - Config: Link:
http://xjfbpuj56rdazx4iolylxplbvyft2onuerjeimlcqwaihp3s6r4xebqd.onion/category/txt/blog/

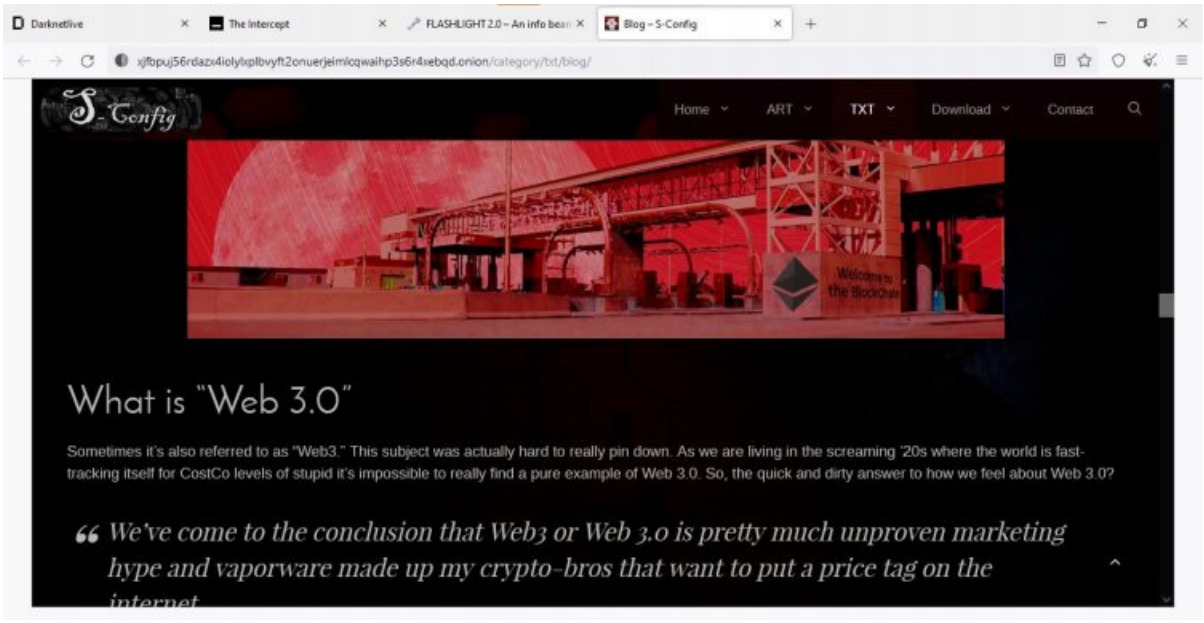


Figure 6: Exploring Blogs – 4/5

→ ProPublica:
Link: http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/

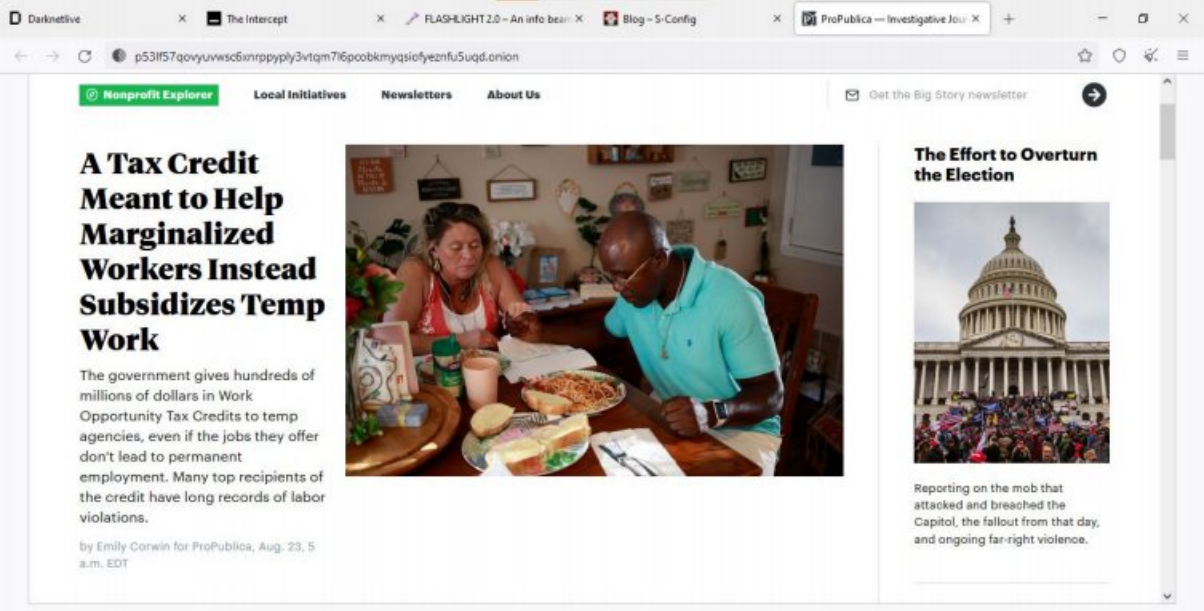


Figure 7: Exploring Blogs – 5/5

Task 2: Exploring Forums

→
Link: http://ylmjp76zk4ndvgpncbtgzrfsrzpblvlzgtuoduqgygwdlexou64iwfqd.onion/

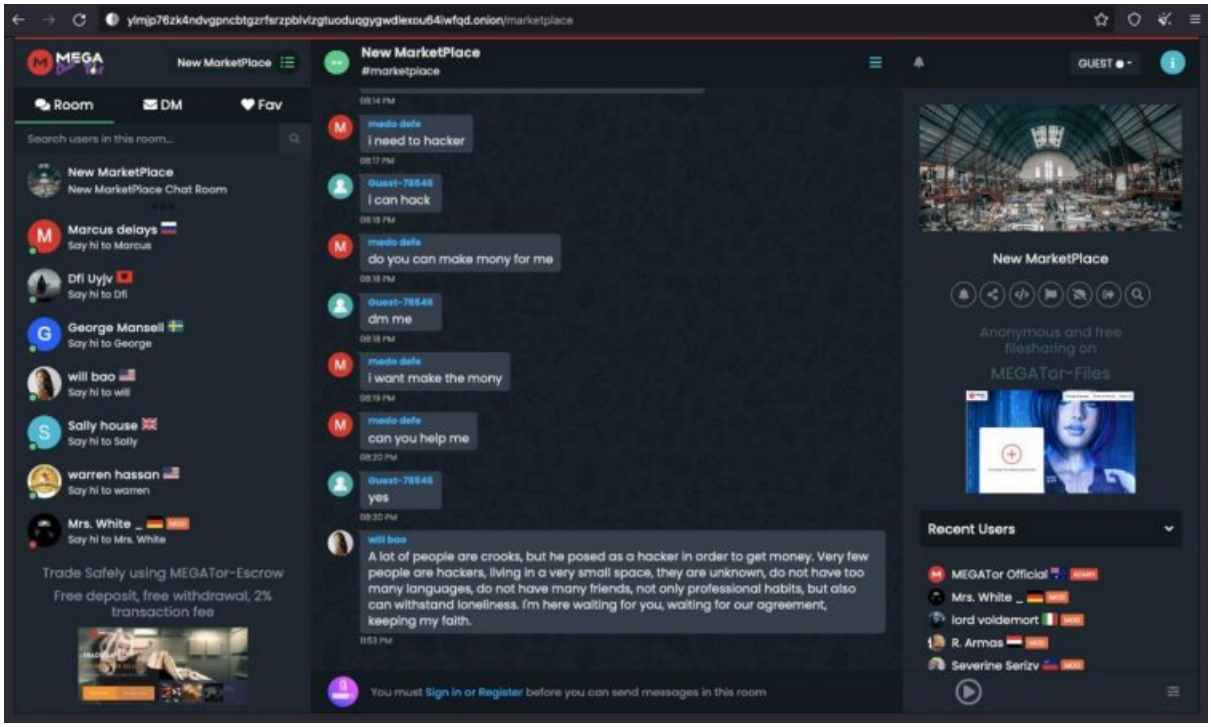


Figure 8: Exploring Forums – 1/5

→
Link:
http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/d/EnergyControl

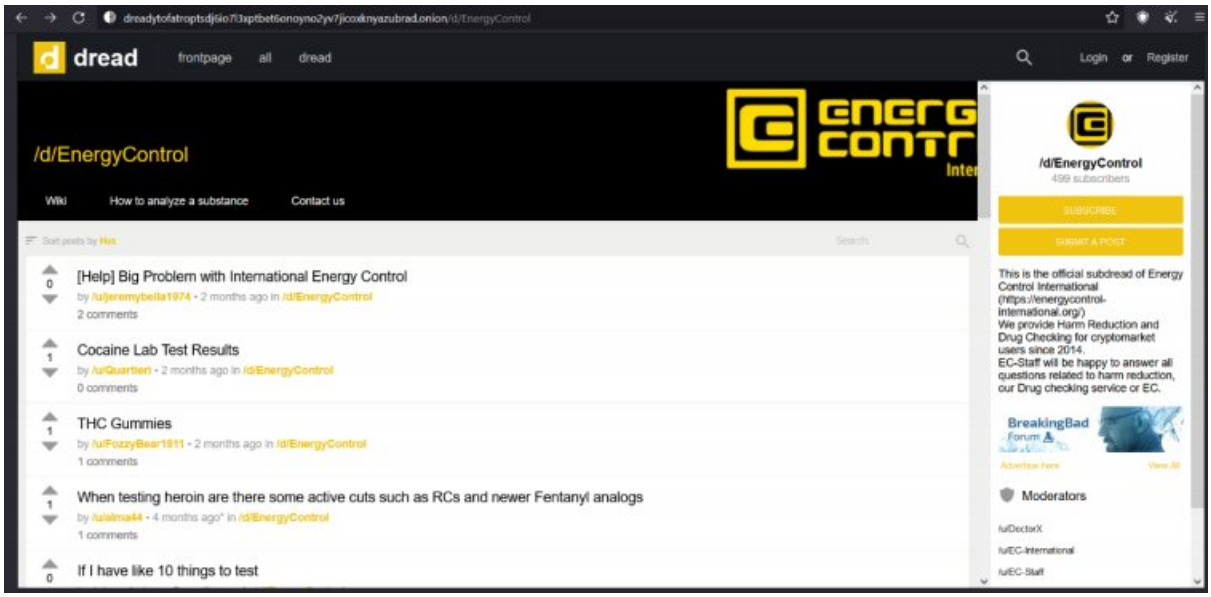


Figure 9: Exploring Forums – 2/5

→
Link: http://4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/hispol/

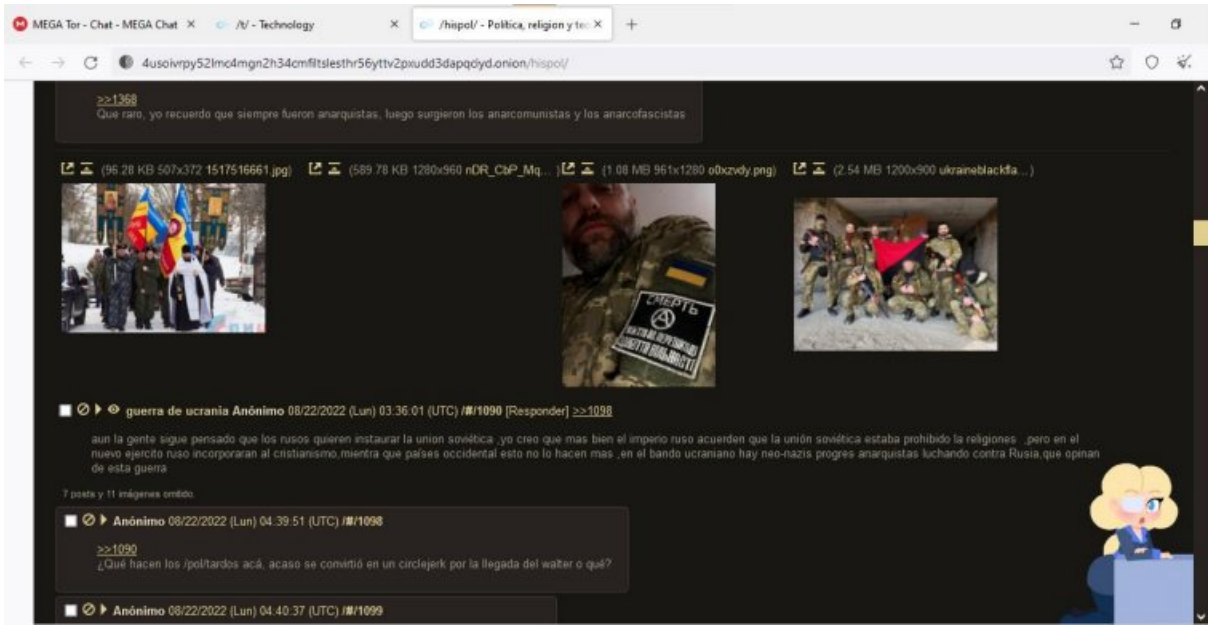


Figure 10: Exploring Forums – 3/5

→
Link: http://4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/t/

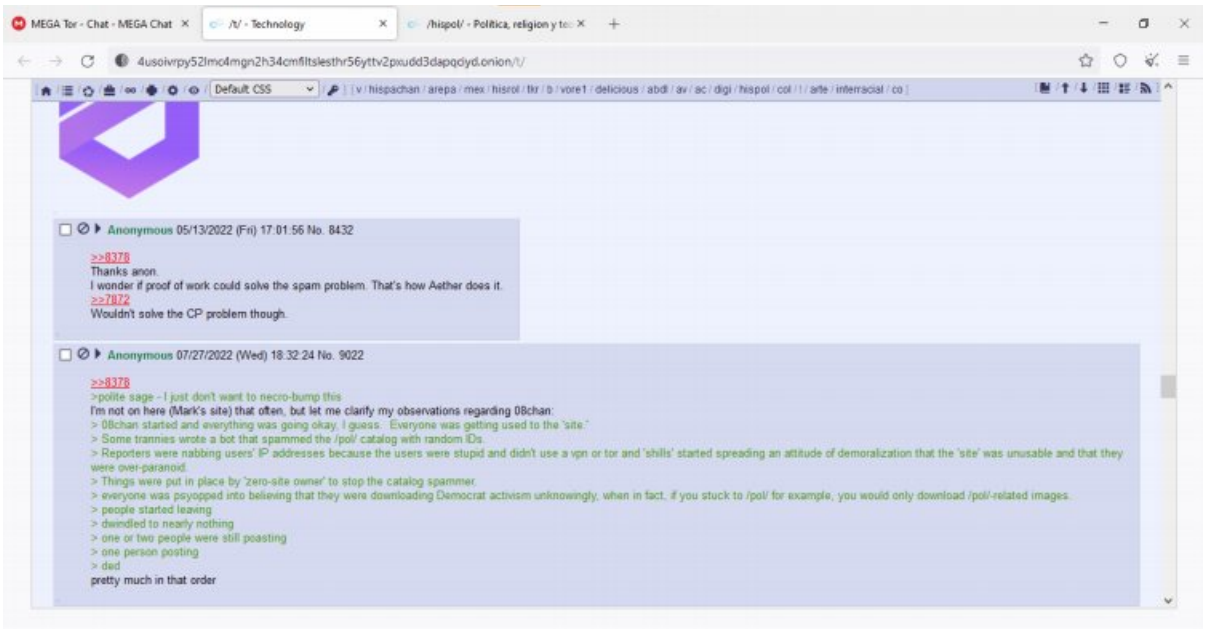


Figure 11: Exploring Forums – 4/5

→
Link:
http://enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion/pol+pdfs+his+horror+aethism+qrbunker

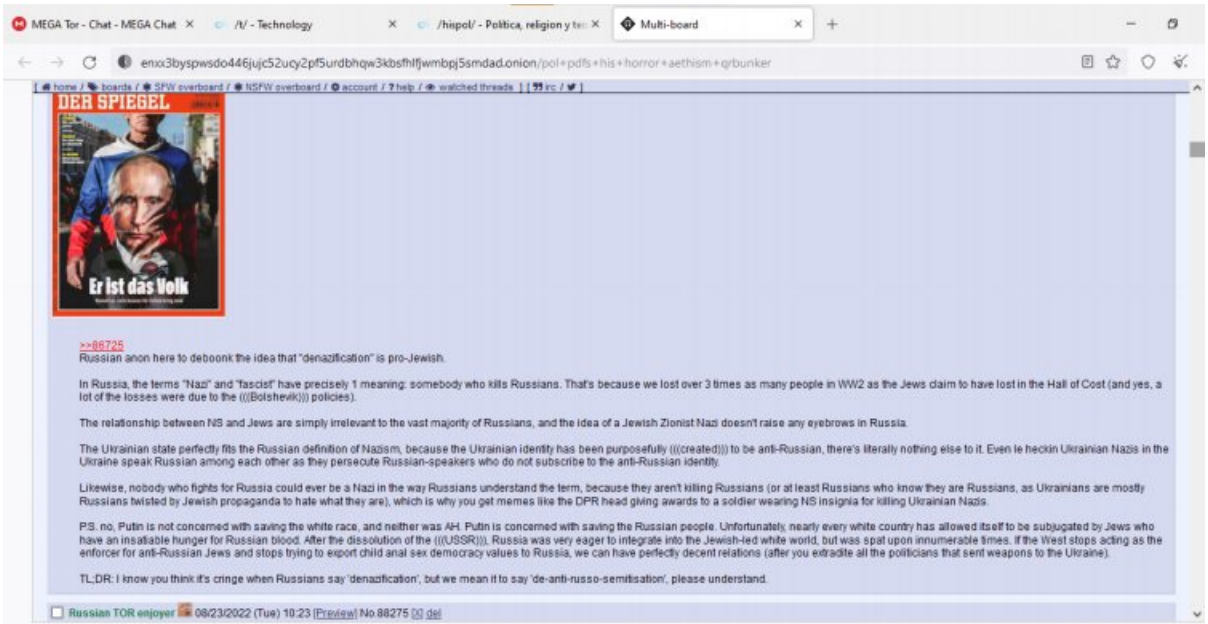


Figure 12: Exploring Forums – 5/5

Task 3: Exploring Wiki

→
Link: http://zqktlwiuavvvqqt4ybvgvi/tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page

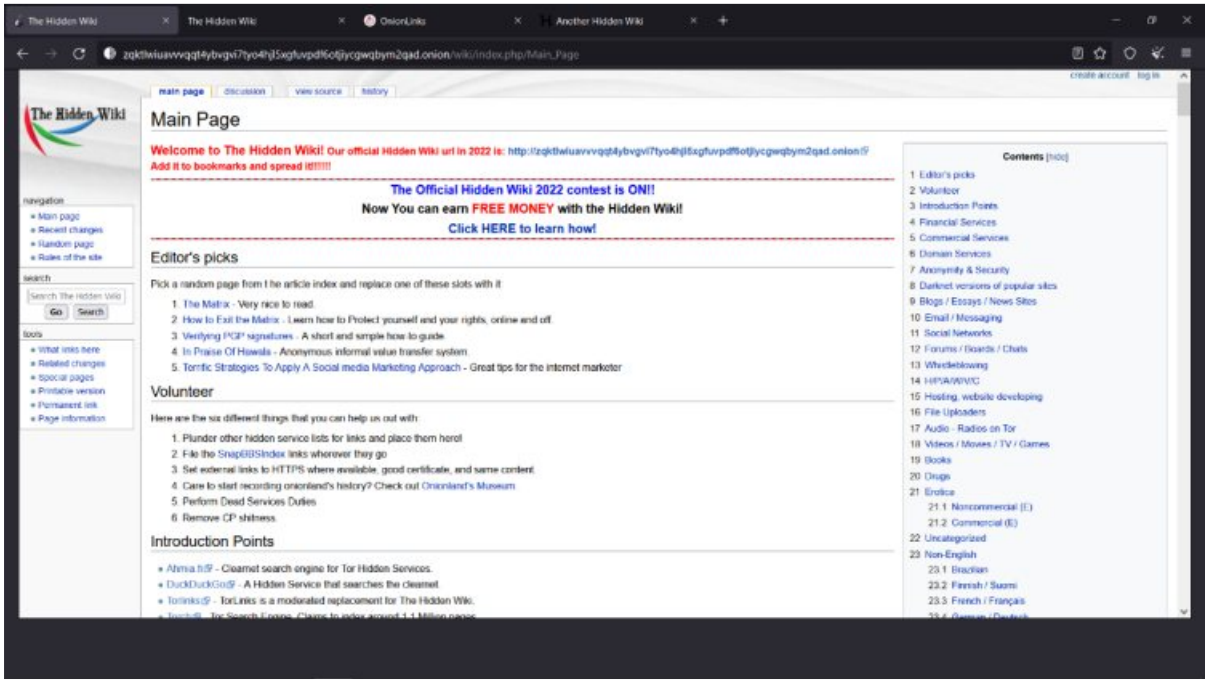


Figure 13: Exploring Wiki – 1/4

→
Link: http://6nhmgdpnyoljh5uzr5kwlatx2u3diou4ldcommfxjz3wkhalzgjqxzqd.onion

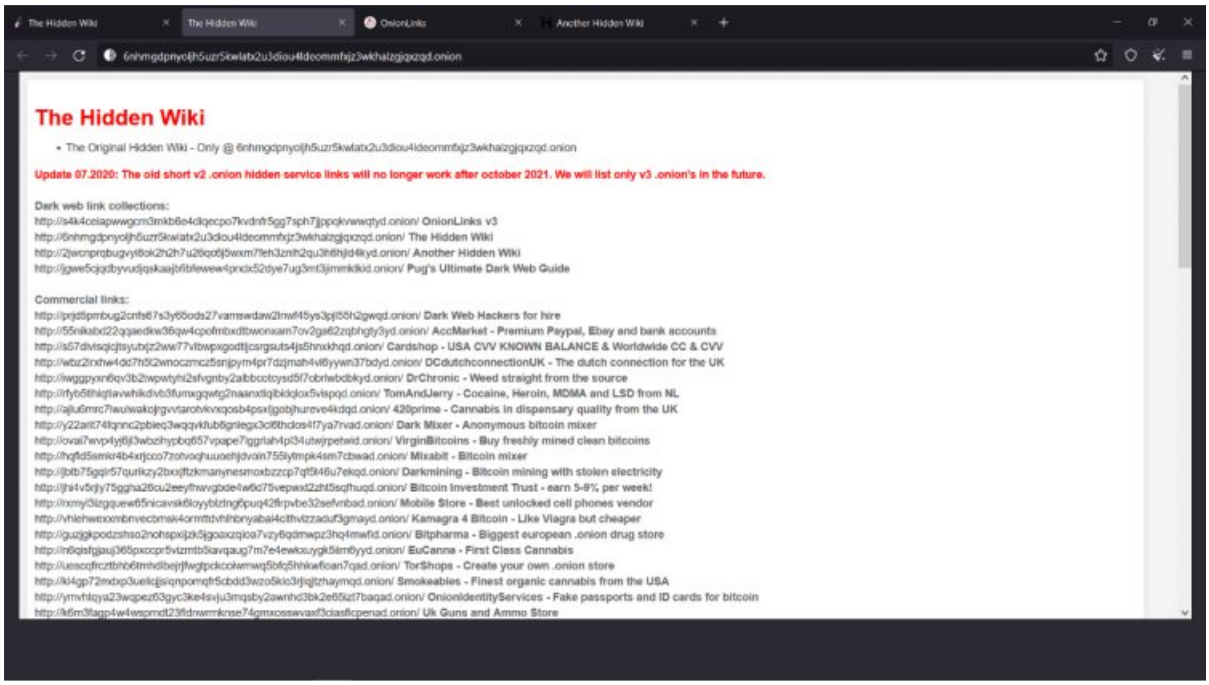


Figure 14: Exploring Wiki – 2/4

→
Link: http://s4k4cciapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion

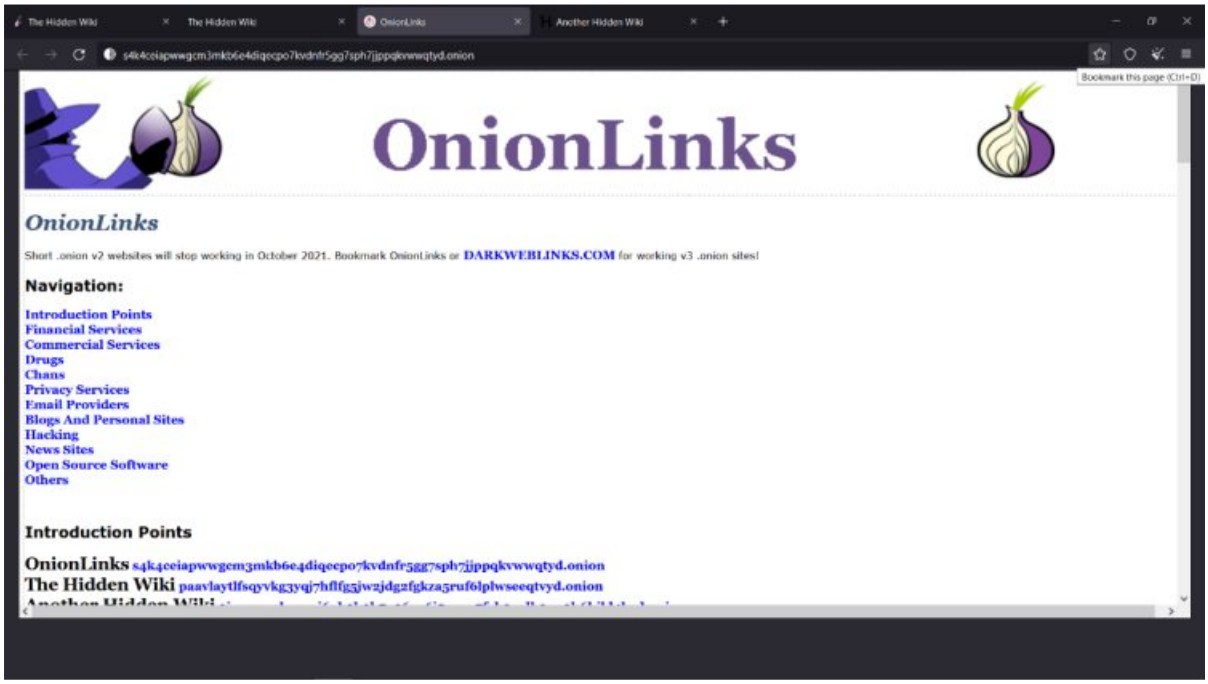


Figure 15: Exploring Wiki – 3/4

→
Link: http://2jwcnprqbugvyi6ok2h2h7u26qc6j5wxm7feh3znlh2qu3h6hjld4kyd.onion

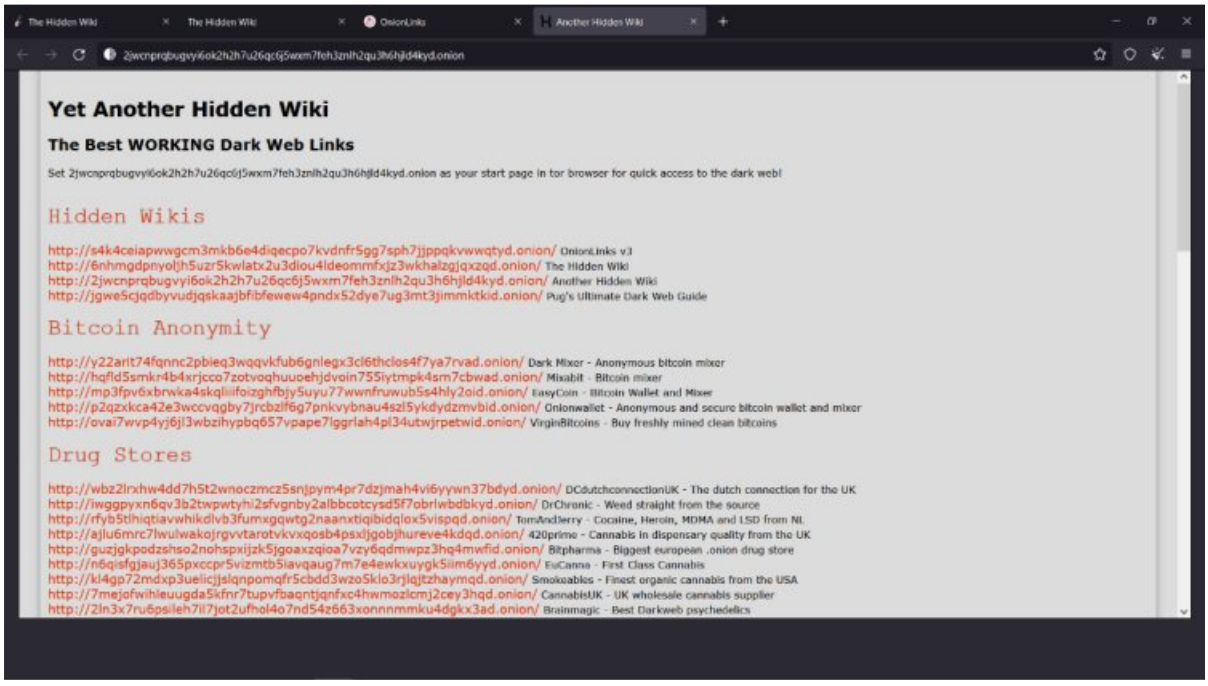


Figure 16: Exploring Wiki – 4/4

Task 4: Exploring Email Services

→
Link: https://5gdvpfoh6kb2iqbizb371zk2ddzrwa47m6rpdueg2m656fovmbhoptqd.onion/rc/

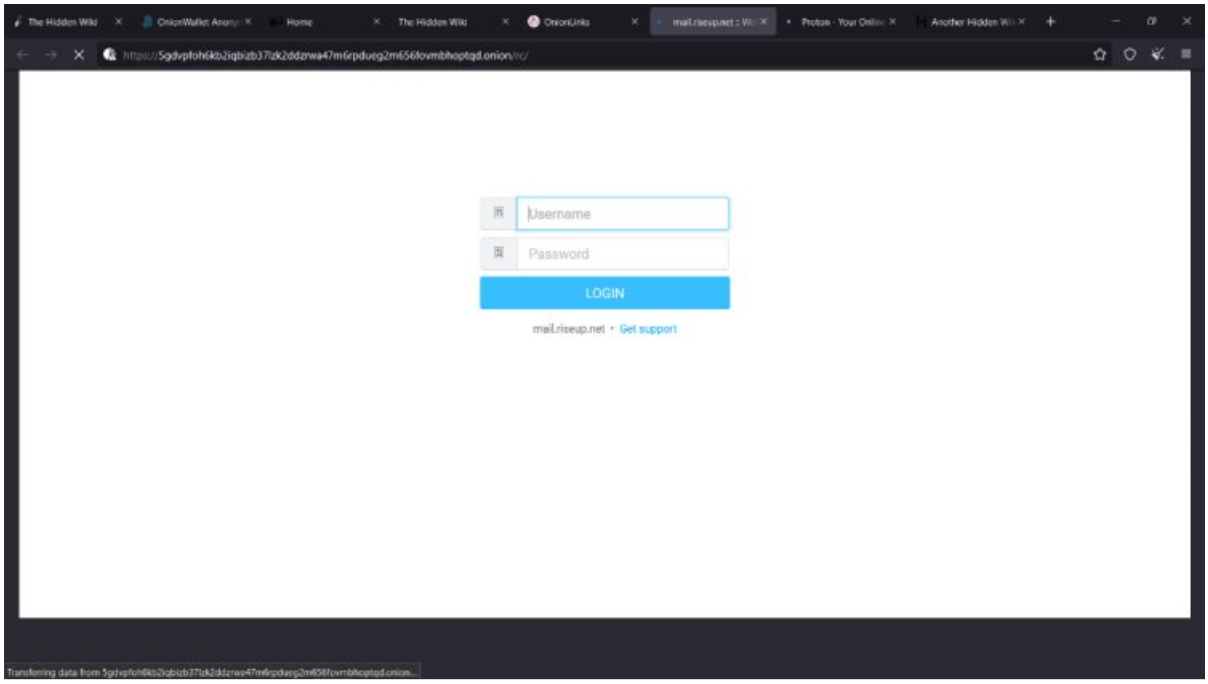


Figure 17: Exploring Email Services – 1/3

→
Link: https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r404vfu7ozyd.onion

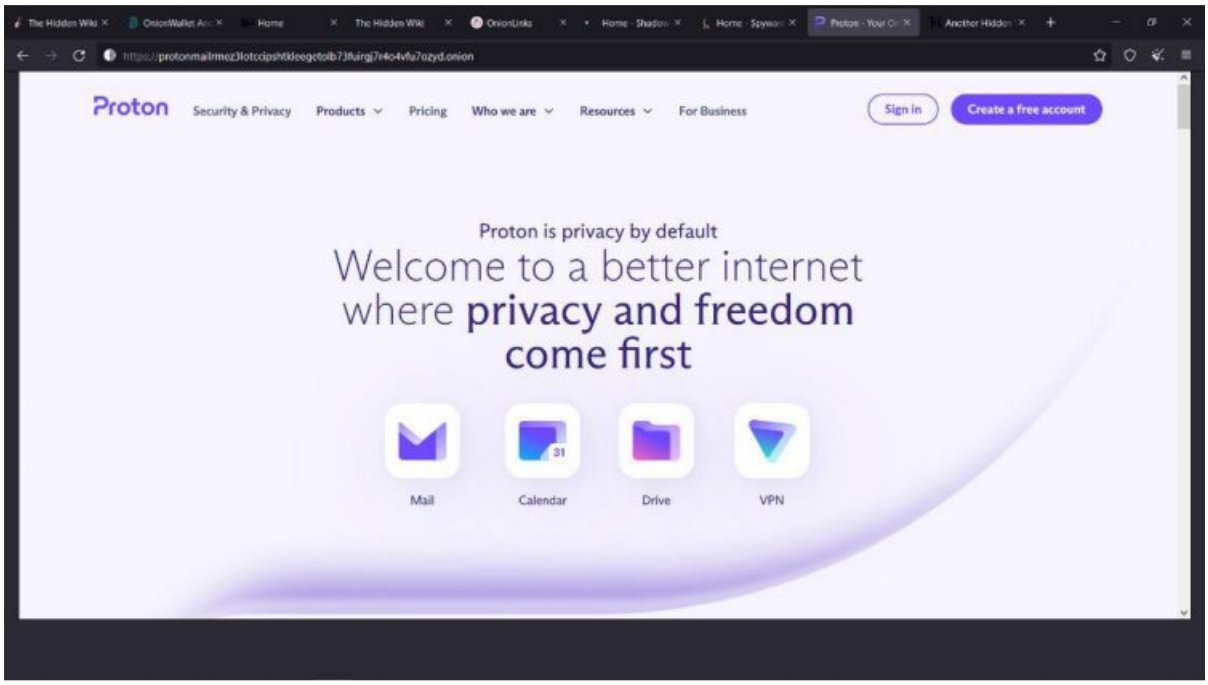


Figure 18: Exploring Email Services – 2/3

→
Link: https://xdkriz6cn2avvcr2vks5lvvtmfojz2ohjzj4fhyuka55mvljeso2ztqd.onion

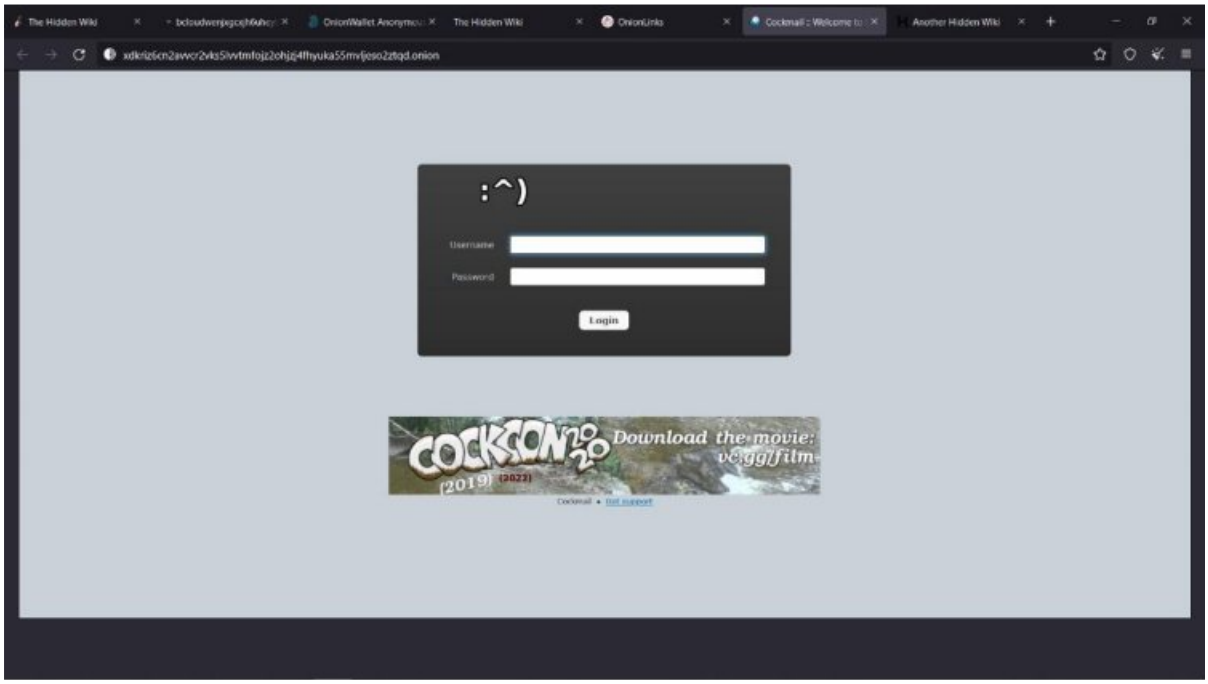


Figure 19: Exploring Email Services – 3/3

Task 5: Exploring Financial Services

→
Link: https://zwt5i7hiwmffq2bl7euedg6y5ydzze3ljiyrjmm7o42vhe7ni56fm7qd.onion

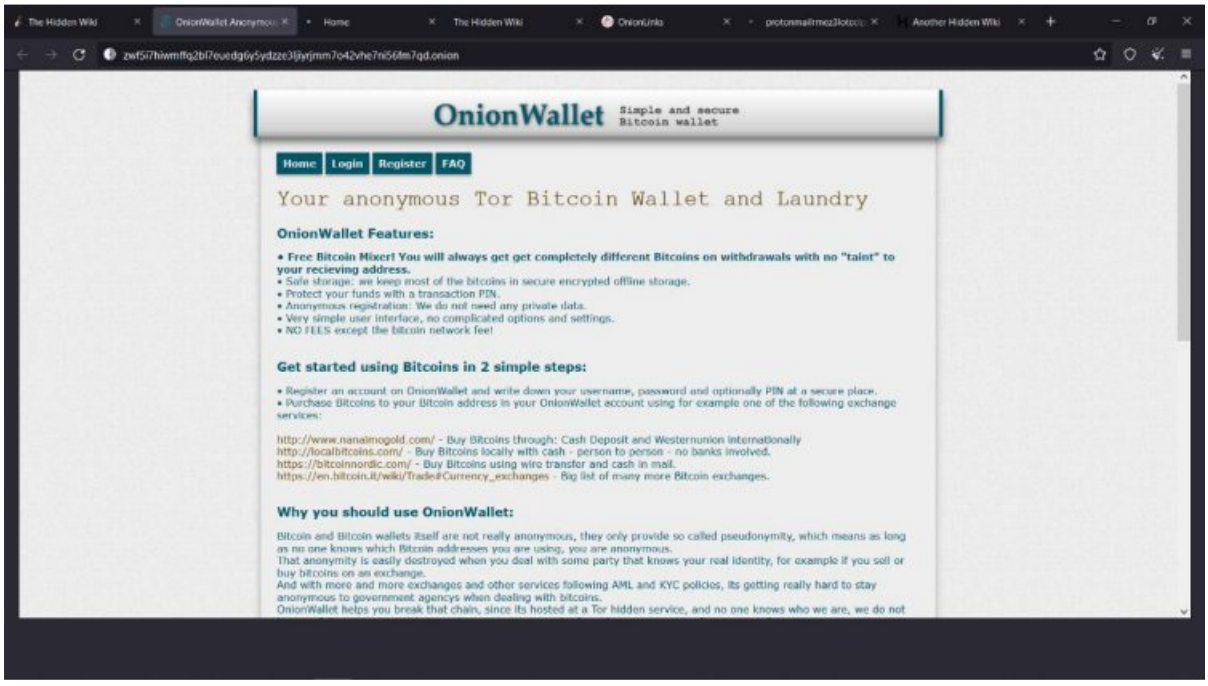


Figure 20: Exploring Financial Services – 1/2

→
Link: https://hbl6udan73w7qbjdey6chsu5gq5ehrfqbb73jq726kj3khnev2yarlid.onion

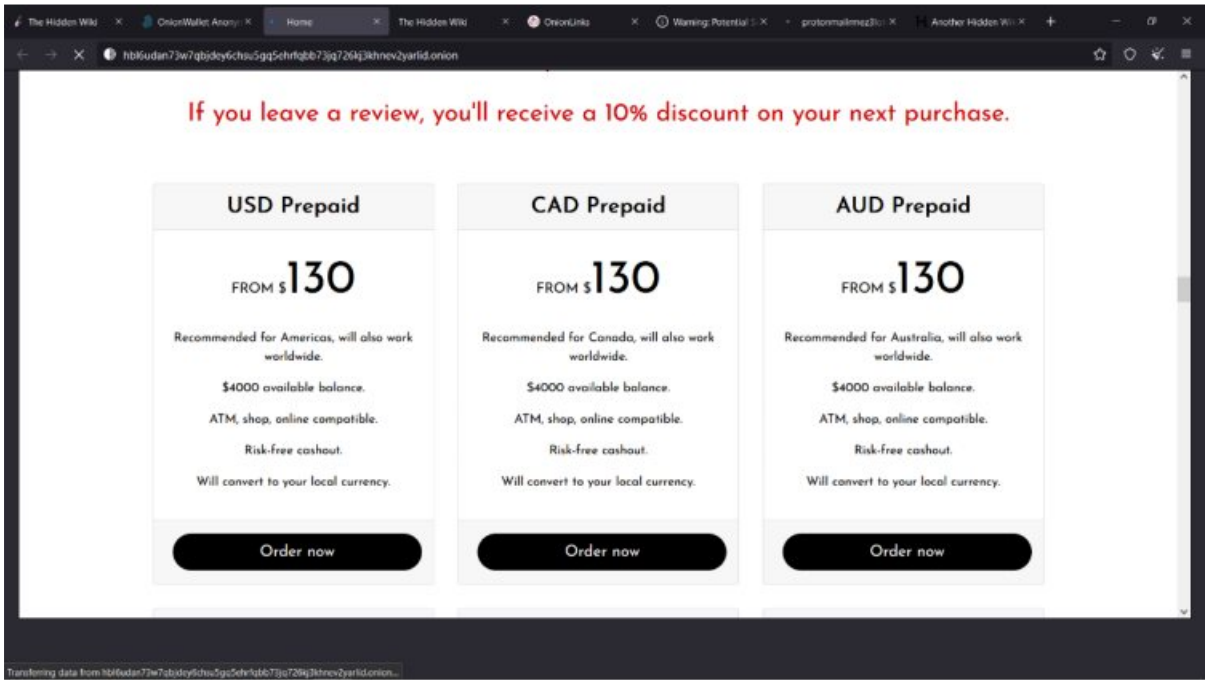


Figure 21: Exploring Financial Services – 2/2

Task 6: Exploring File Uploader

→
Link:
http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/directory/al-jazeera/

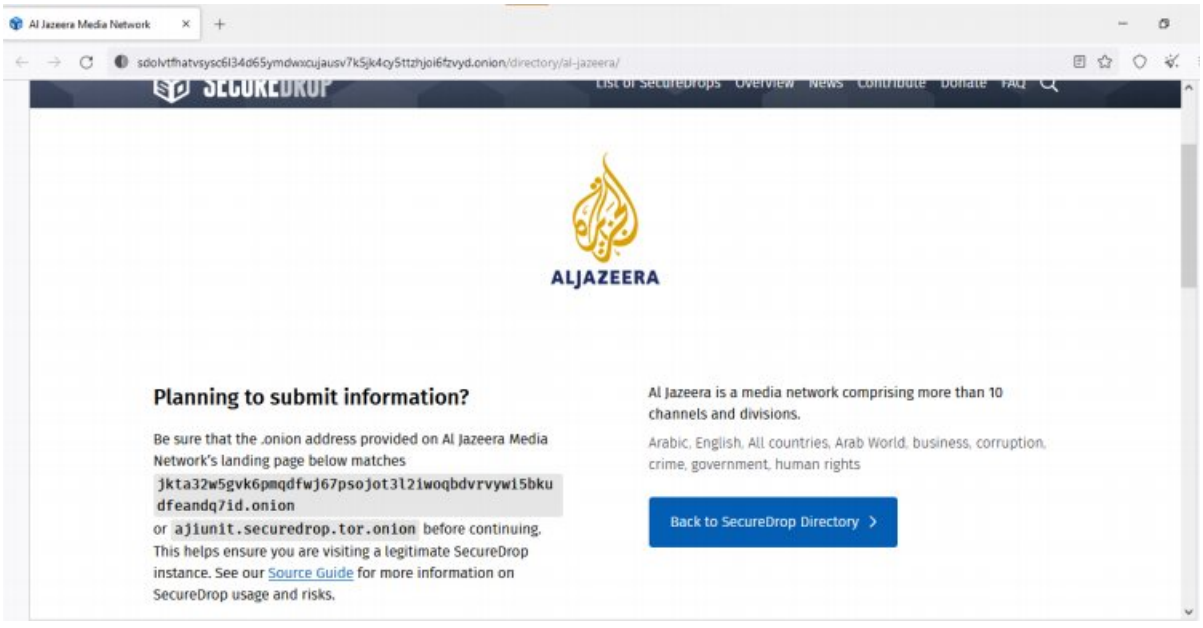


Figure 22: Exploring File Uploader – 1/5

→

Link: http://artistzubelolngubx6pmd6w2xacl3yj7jllxjdnrhh7assk7ioevjad.onion/

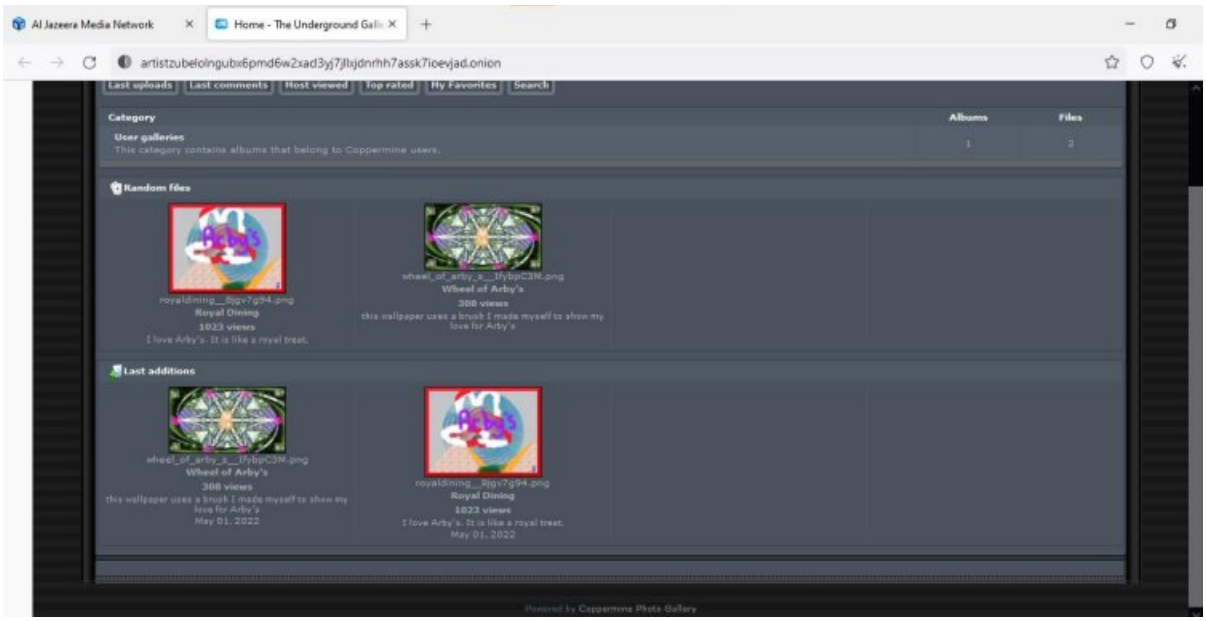


Figure 23: Exploring File Uploader – 2/5

→

Link: http://strongerw2ise74v3duebgsvug4mehyhlpa7f6kfwnas7zofs3kov7yd.onion/trending/month?page=2

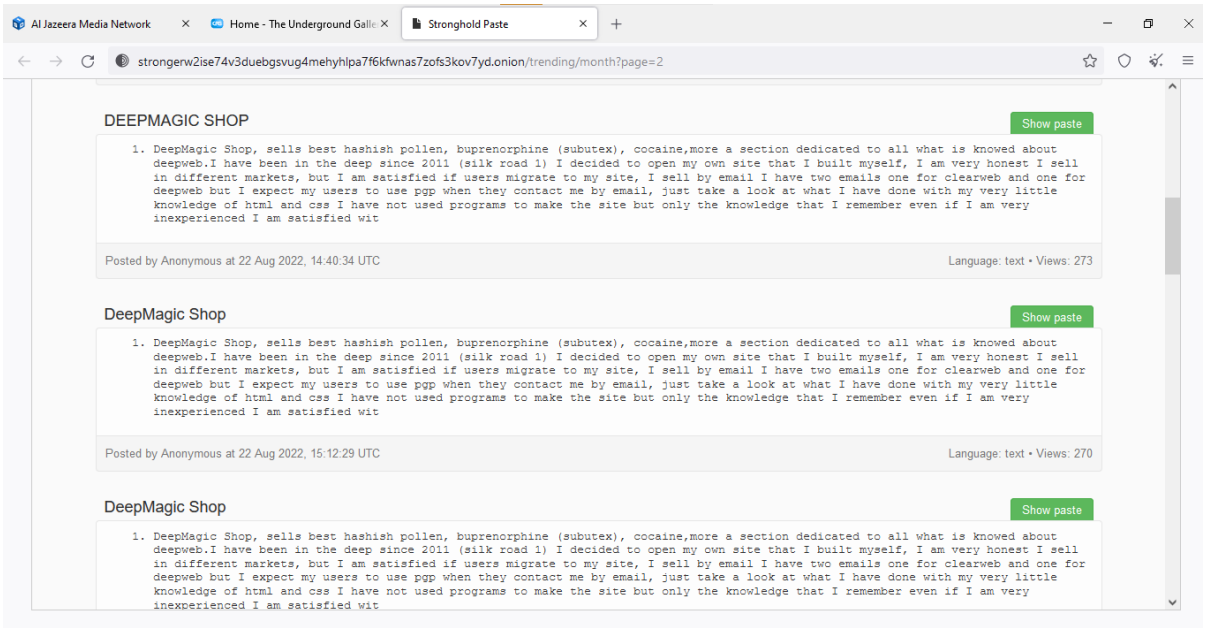


Figure 24: Exploring File Uploader – 3/5

→
Link:
http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/directory/guardian/

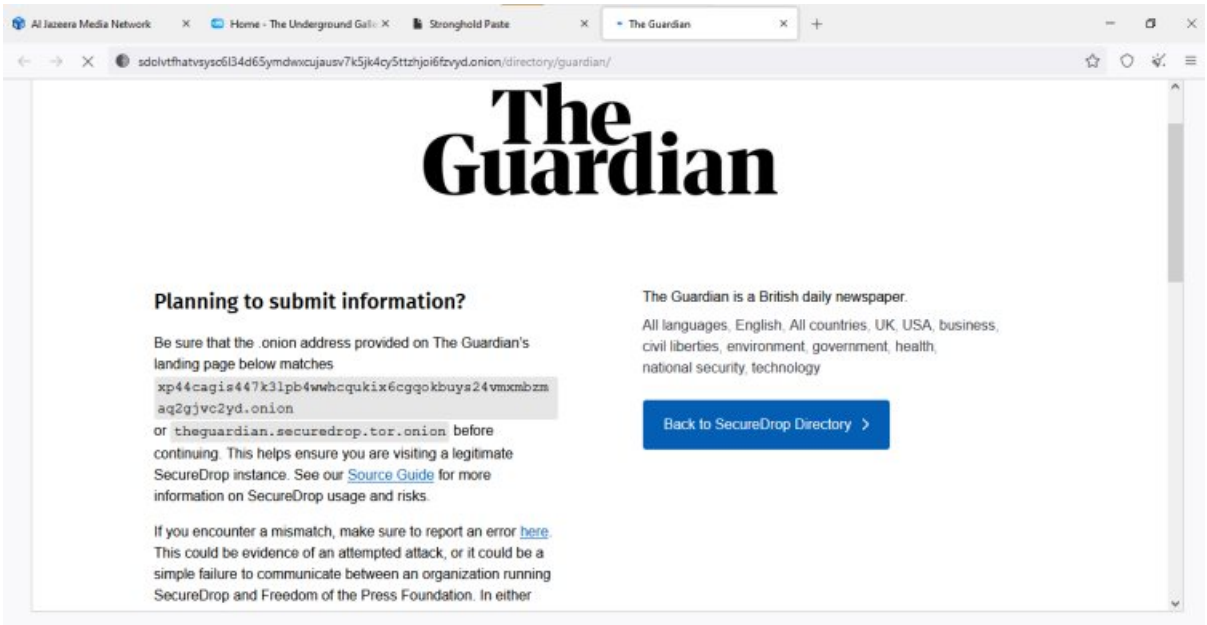


Figure 25: Exploring File Uploader – 4/5

→
Link:
http://strongerw2ise74v3duebgsvug4mehyhlpa7f6kfwnas7zofs3kov7yd.onion/trending/month?page=7

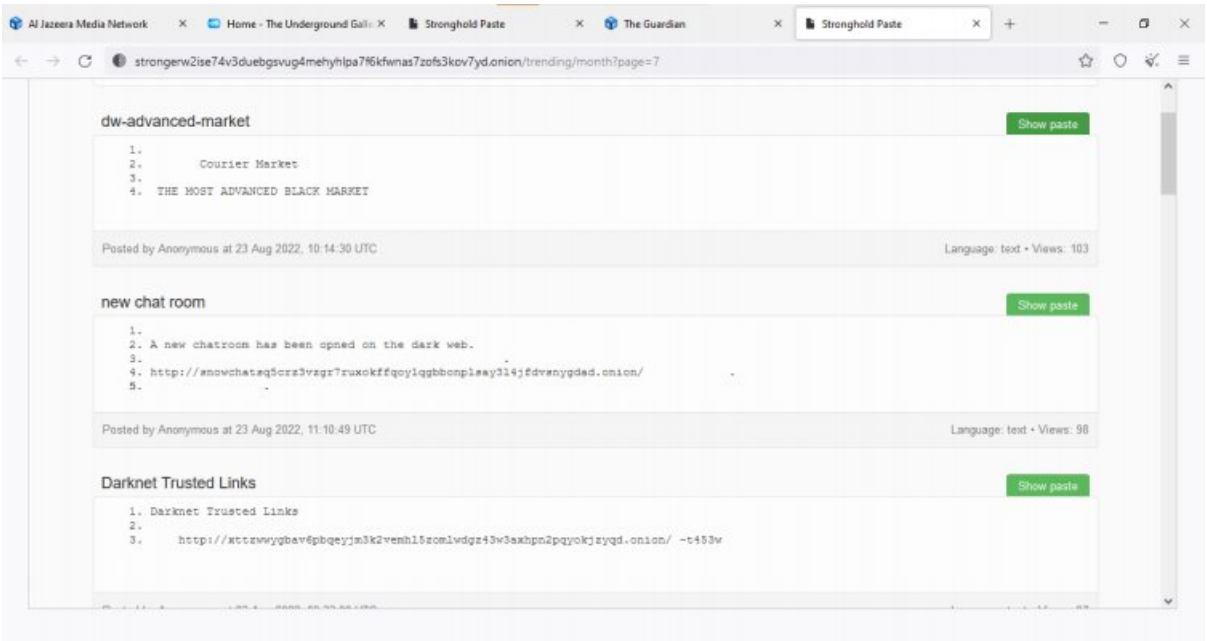


Figure 26: Exploring File Uploader – 5/5

Task 7: Exploring Anonymity & Security

→
Link: http://elfqv3zjfegus3bgg5d7pv62eqght4h6sl6yjjhe7kjpi2s56bzgk2yd.onion/fakcid.php

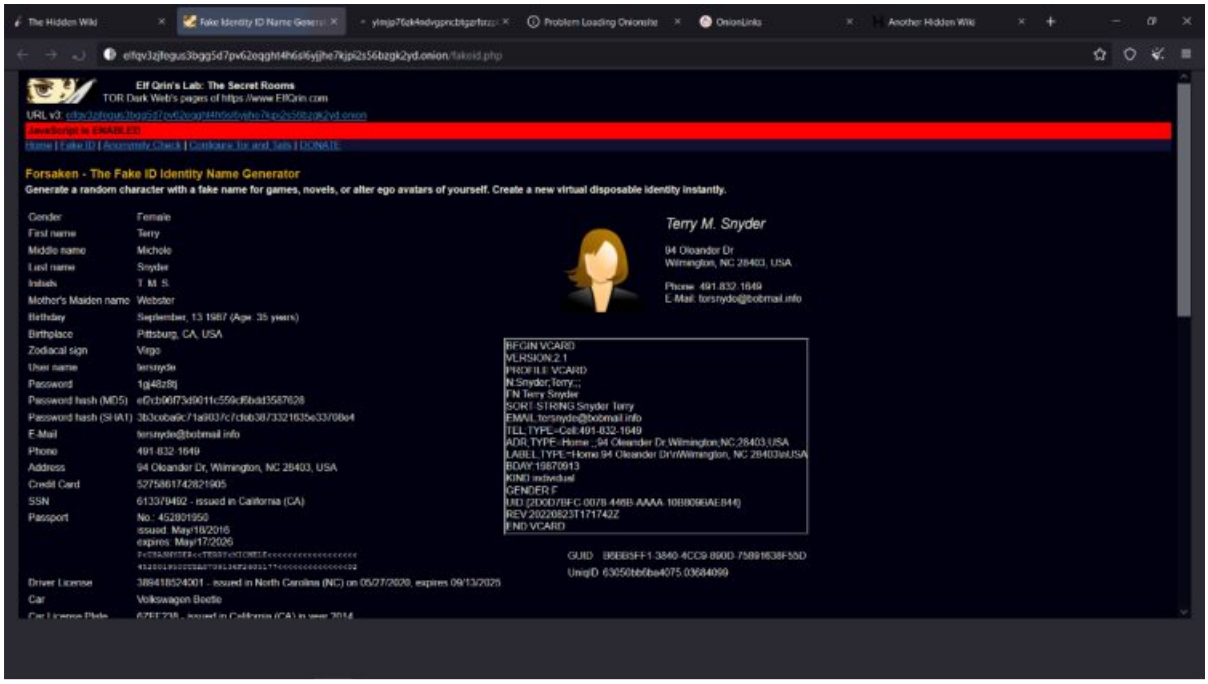


Figure 27: Exploring Anonymity & Security – 1/3

→
Link:
http://elfqv3zjfegus3bgg5d7pv62eqght4h6s16yjjhe7kjpi2s56bzgk2yd.onion/binfo_check_anonymity.php

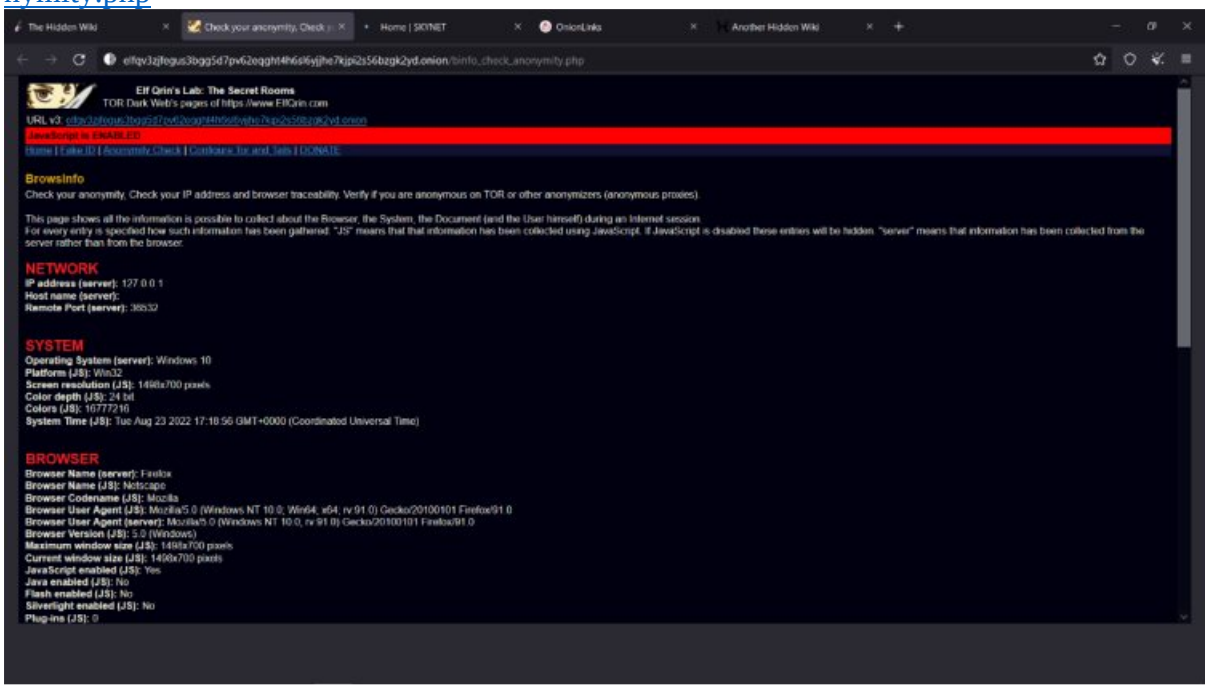


Figure 28: Exploring Anonymity & Security – 2/3

→
Link: http://skynet2hexb7hiqz3yr5tllpocyvy5my7vyioj7vhvaleoulem72okid.onion:81

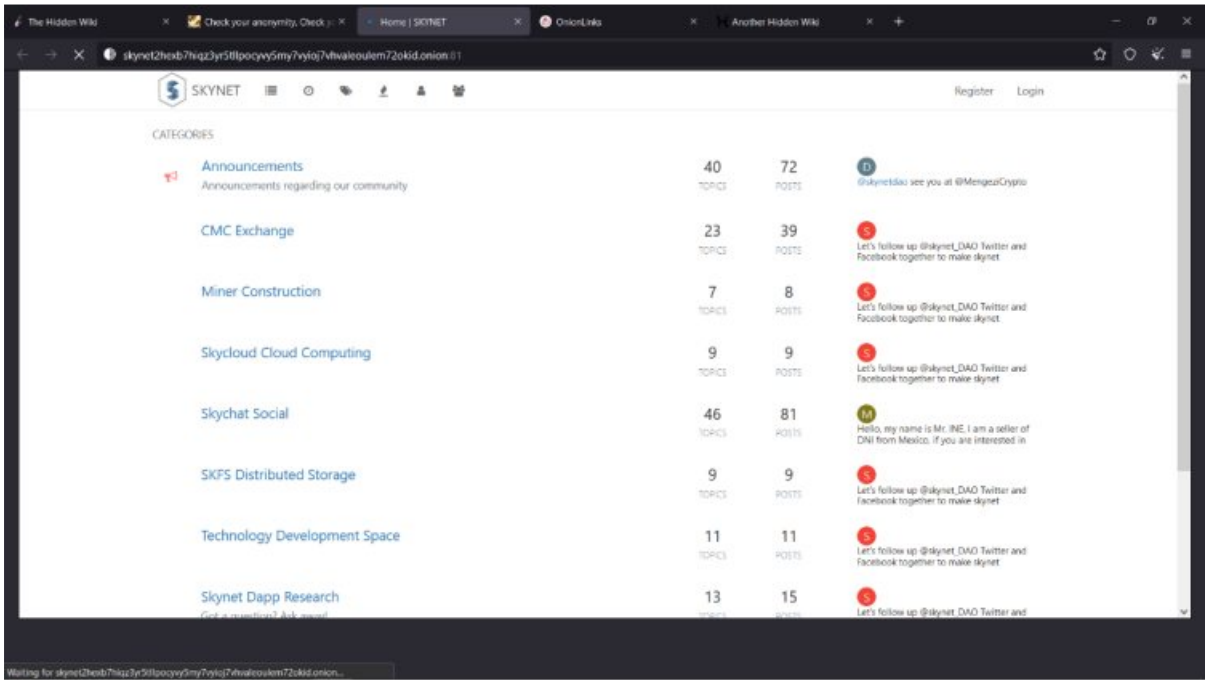


Figure 29: Exploring Anonymity & Security – 3/3

Analysis:

Overall, the Tor browser is a very powerful tool for digital forensics. It allows users to access the deep and dark web anonymously, which can be very useful for investigations. Additionally, the browser provides a number of features that make it easier to access and use the dark web, such as the ability to search for and access onion sites. Overall, the Tor browser is a valuable tool for digital forensics and can be used to help investigate a variety of crimes.

Conclusion:

Based on the research conducted, it is concluded that the Tor browser is an effective tool for accessing the deep and dark web. However, there are some limitations to using the Tor browser, such as the potential for malicious actors to exploit vulnerabilities in the browser or the websites accessed through the browser, the Tor Browser can be slow and may not provide the best possible performance when browsing the deep and darknet, also the Tor Browser may not be able to provide the same level of security and privacy as other browsers, such as the Firefox browser. Additionally, users of the Tor browser should be aware of the potential for their personal information to be leaked, as well as the possibility of being targeted by government surveillance.

Digital Forensics Lab Report: 6

Date:08-09-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Data Recovery from Computer Systems, Mobile Devices and other electronic peripherals.

Tool Names: Recuva, EaseUS.

Tasks: Perform data recovery using Recuva and EaseUS.

Introduction:

In the field of digital forensics, data recovery is the process of identifying and extracting data from computer systems, mobile devices and other electronic peripherals. This data can be used to reconstruct past events or to investigate current crimes.

Data recovery can be a challenging task, as data can be stored in a variety of formats and on a variety of media. In addition, data can be encrypted or damaged, making it difficult to access. However, with the right tools and expertise, data recovery is possible.

Digital forensics is a growing field, and data recovery is an important part of this discipline. With the right tools and training, digital forensics experts can help to solve crimes and to bring justice to victims.

- **Recuva tool:** Recuva is a digital forensics tool that can be used to recover data from a variety of storage devices. It can be used to recover data from hard drives, SSDs, USB drives, and memory cards. Recuva can also be used to recover data from a variety of file formats, including NTFS, FAT, exFAT, and ext4. It can recover files from your recycle bin, as well as files that have been deleted by viruses or other software. Recuva can also be used to recover files from formatted or damaged storage devices. Recuva is a free tool, and it is available for Windows, Mac, and Linux.

- **EaseUS tool:** Ease US is a powerful tool for digital forensics. It can help you recover lost or deleted data from a variety of devices, including computers, smartphones, and tablets. It can also help you recover data from damaged or corrupted devices. It supports a wide range of file formats and has a user-friendly interface. With EaseUS, you can easily recover lost or deleted files, as well as data from damaged or formatted storage devices.

Steps:

- Perform data recovery using Recuva
- Perform data recovery using Ease US

Links:

- Recuva: https://www.ccleaner.com/recuva/download
- Ease US: https://www.easeus.com/download.htm

Task 1: Performing data recovery using Recuva

Steps:

Step 1 → Download software from https://www.ccleaner.com/recuva/download and install it on your system.

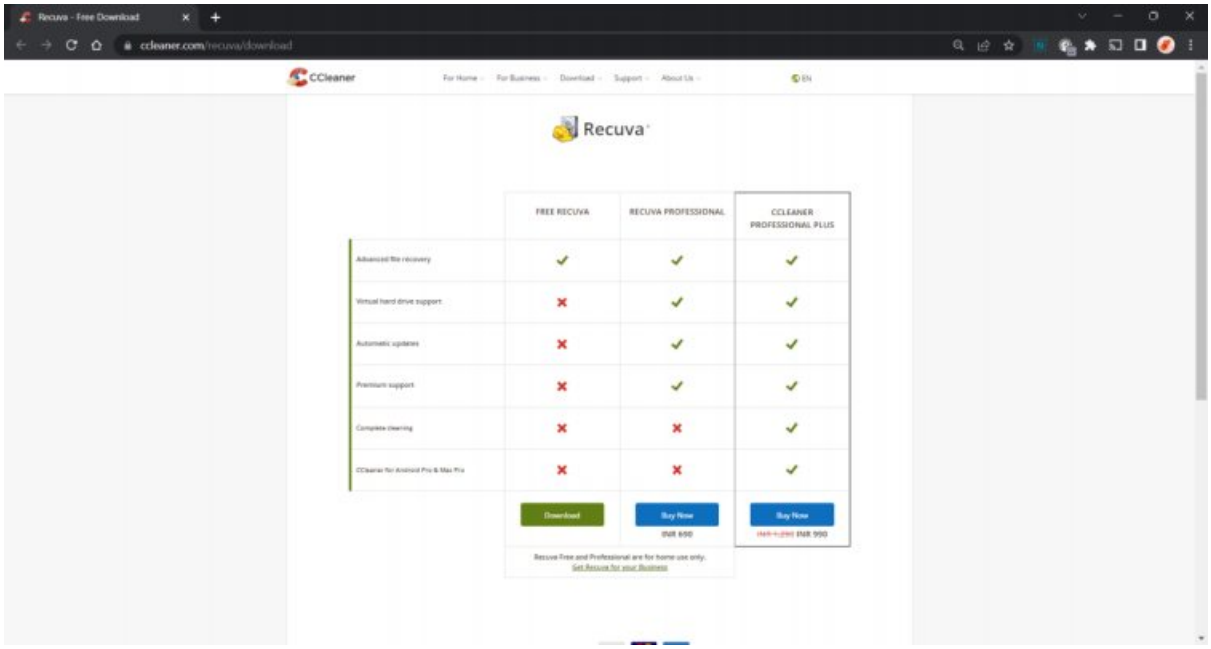


Figure 1: Website to download Recuva software

Step 2 → After downloading recuva software, setup the software on your system.

Figure 2: Doing Setup after downloading Recuva software

Step 3 → Select type of data you want to recover.

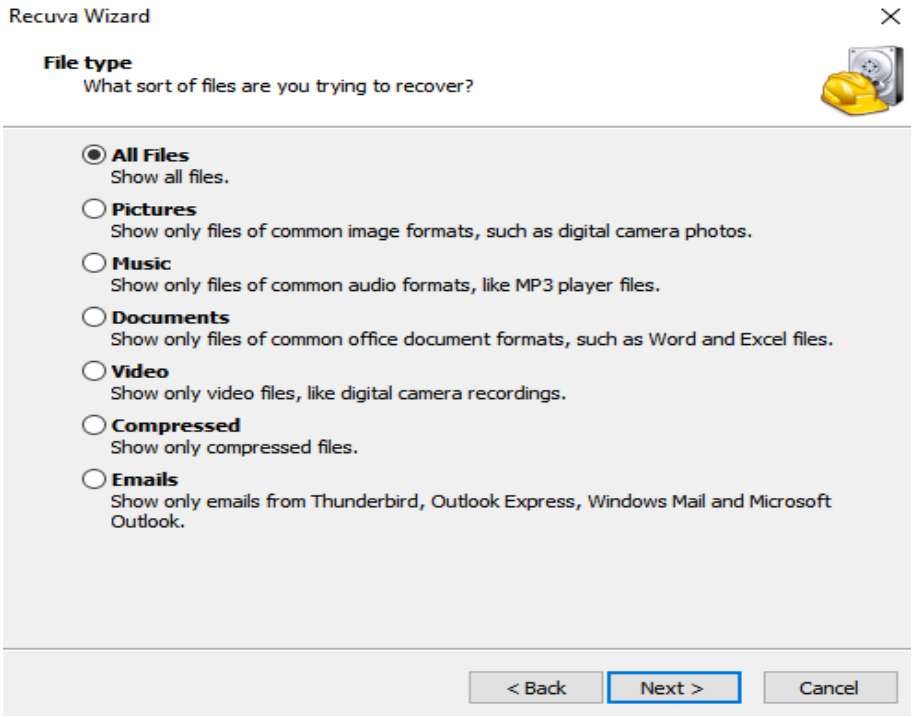


Figure 3: Selecting file type for recovering data in Recuva

Step 4 → Select folder adderess.

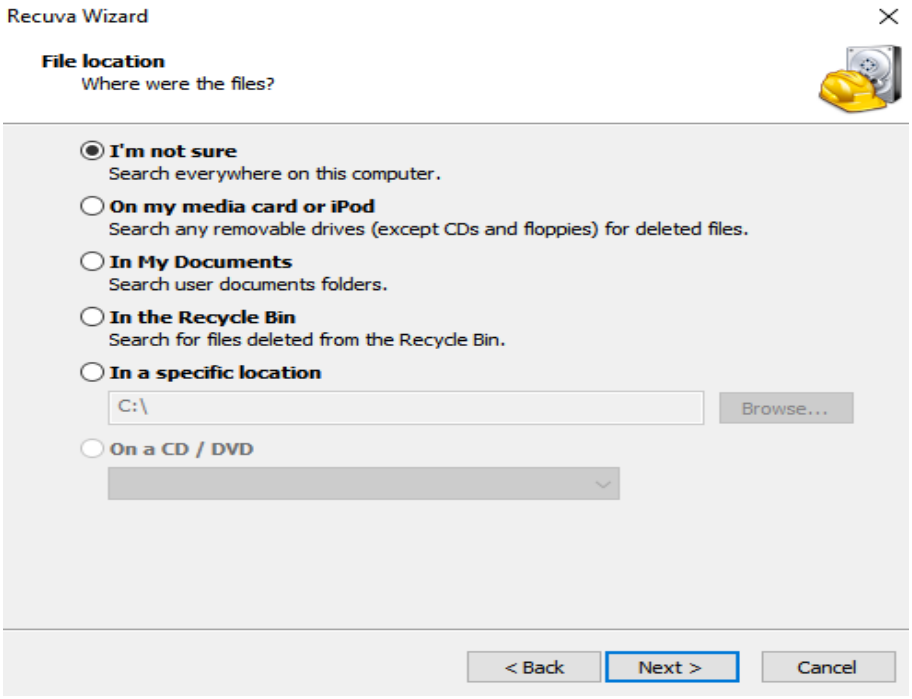


Figure 4: Selecting File Location for recovering data in Recuva

Step 5 → Start your data recovery.

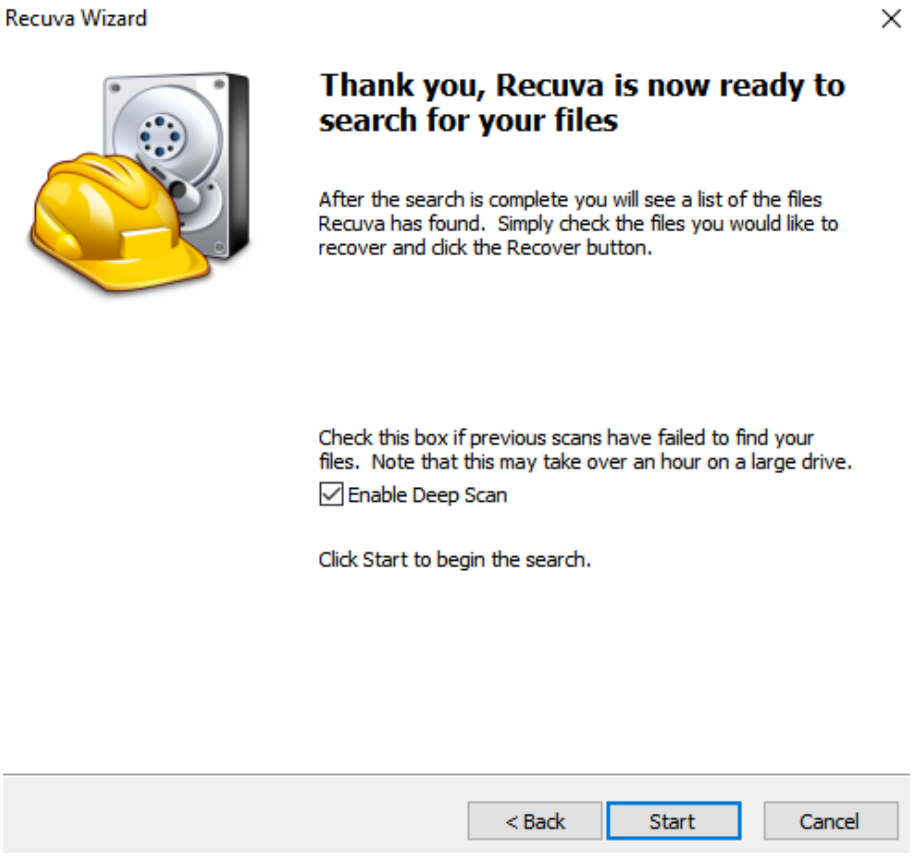


Figure 5: Starting Data Recovery in Recuva

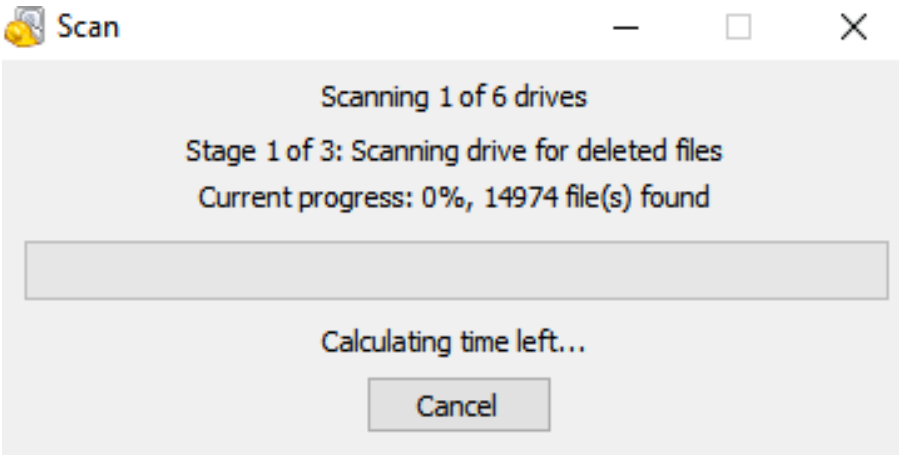


Figure 6: Progress to recovering data in Recuva

Step 6 → Show available files are ready to recover.

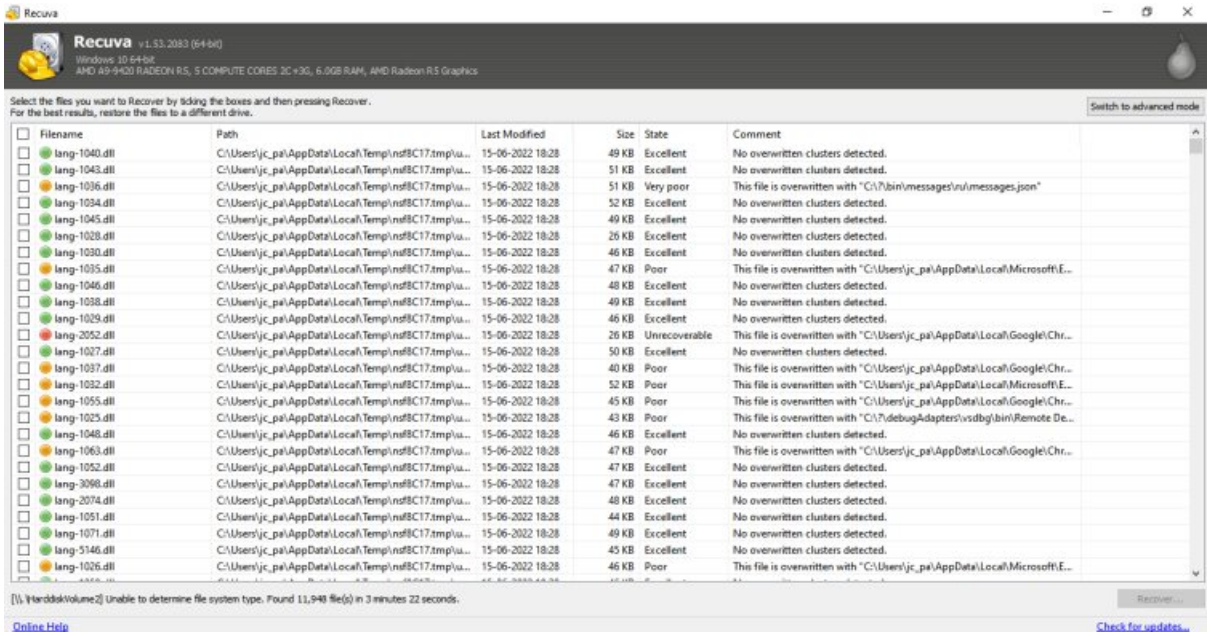


Figure 7: Shows available files for ready to recover in Recuva

Step 7 → Select your folder you want to recover (green shows that we can recover that things).

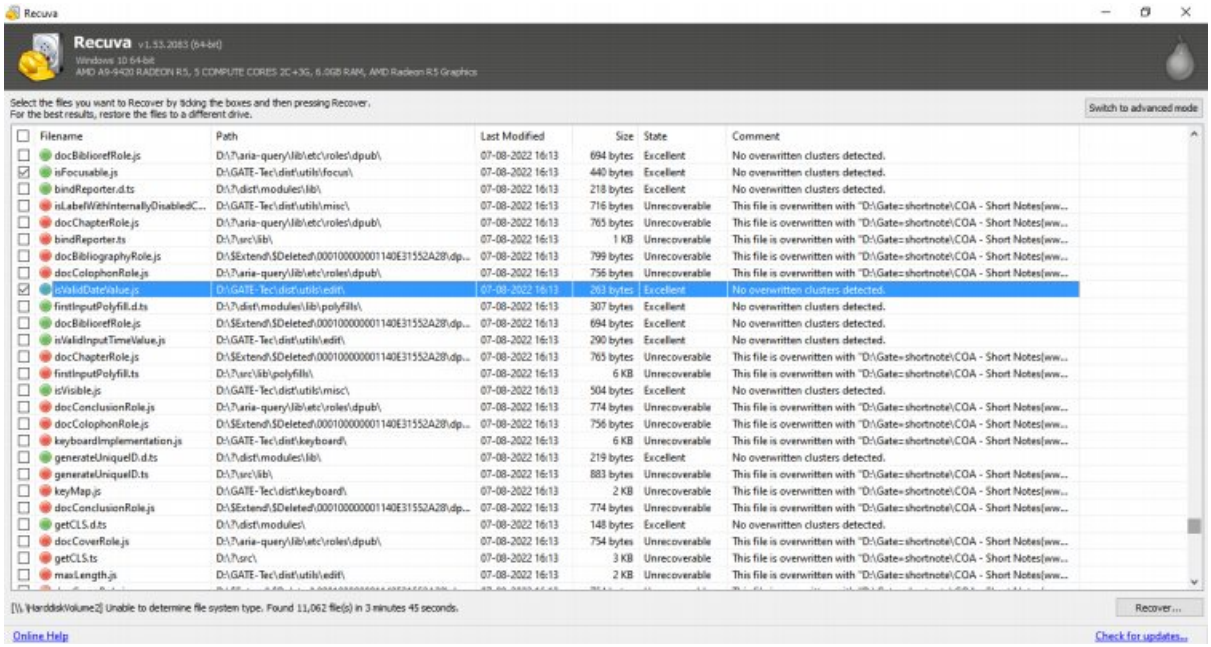


Figure 8: Selecting folder which is going to recover

Step 8 → Select folder where you want to store your recover data and click recover button.

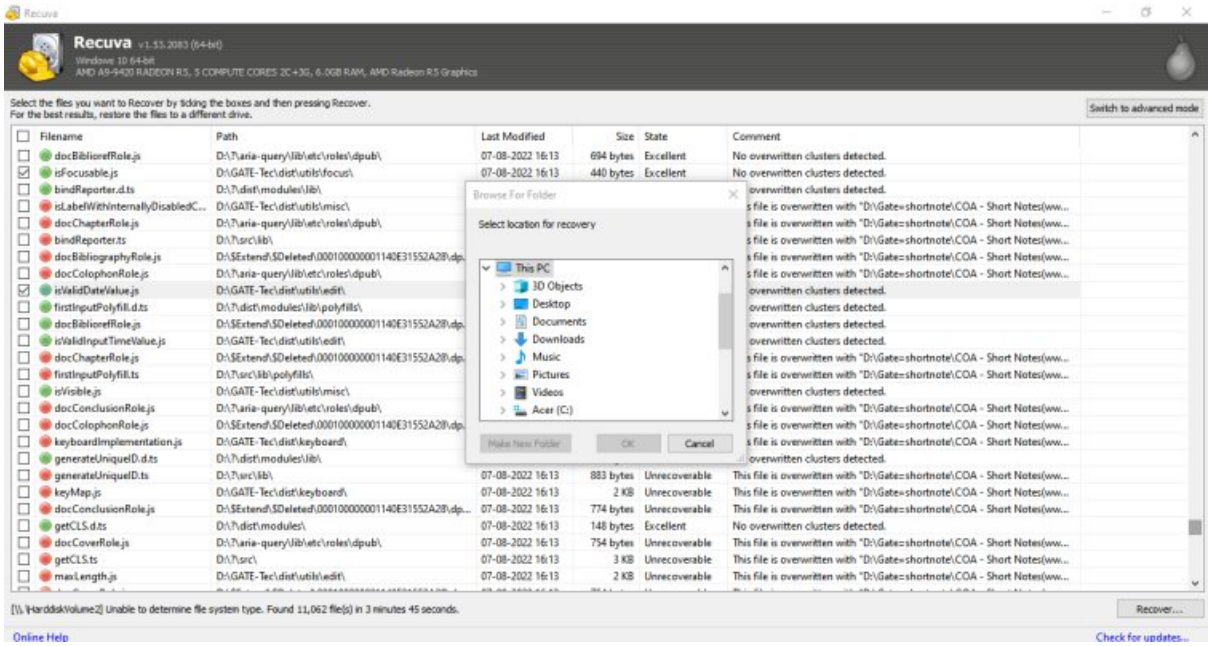


Figure 9: Selecting folder where the recover data is going to store

Step 9 → Finally, your data is recovered, Operation completed for recovering data using Recuva.

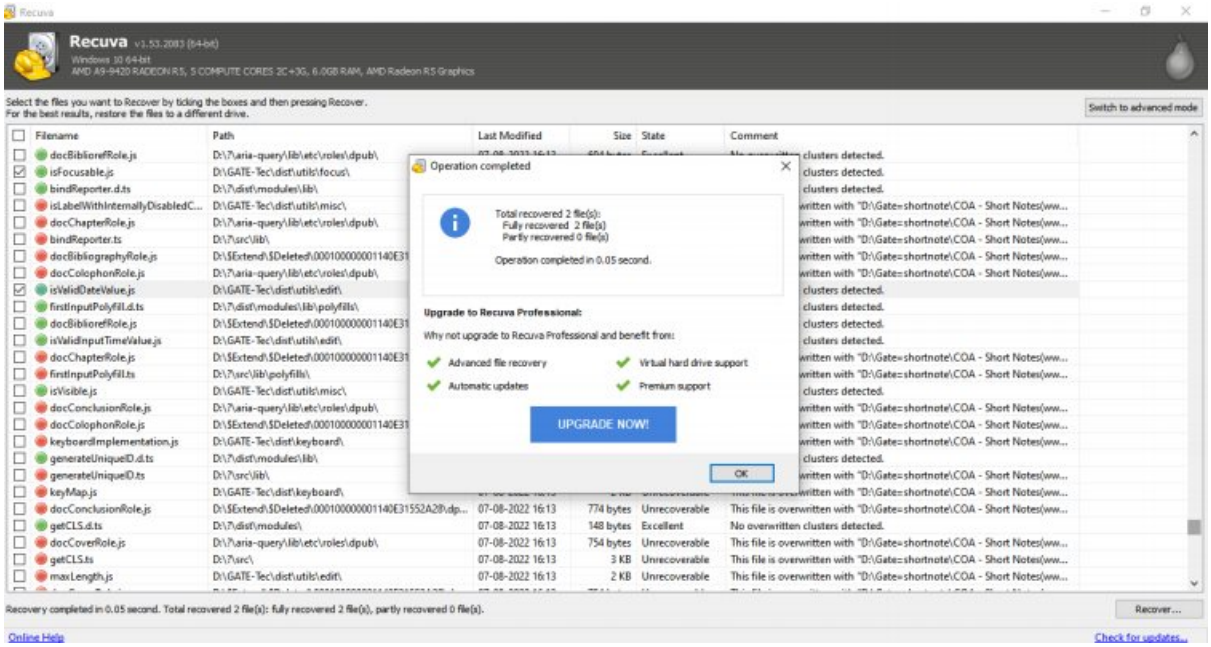


Figure 10: Operation completed for recovering data using Recuva

Analysis:

The Recuva tool was very successful in recovering deleted files from the digital forensic evidence. The tool was able to find and recover all of the deleted files that were on the drive. The tool was also able to recover files that were deleted from the recycle bin. The tool was very successful in recovering these files.

Task 2: Performing data recovery using EaseUS

Steps:

Step 1 → Download software from https://www.easeus.com/download.htm and install it on your system.

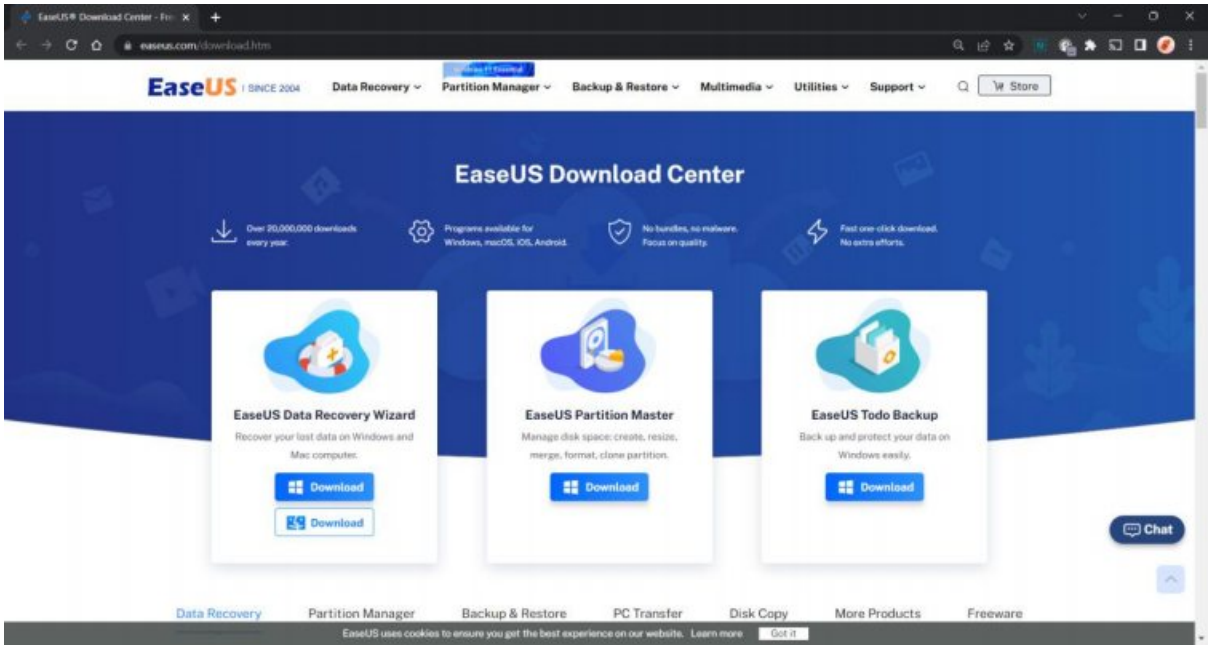


Figure 11: Website to download EaseUS software

Step 2 → After downloading EaseUS software, setup the software on your system.

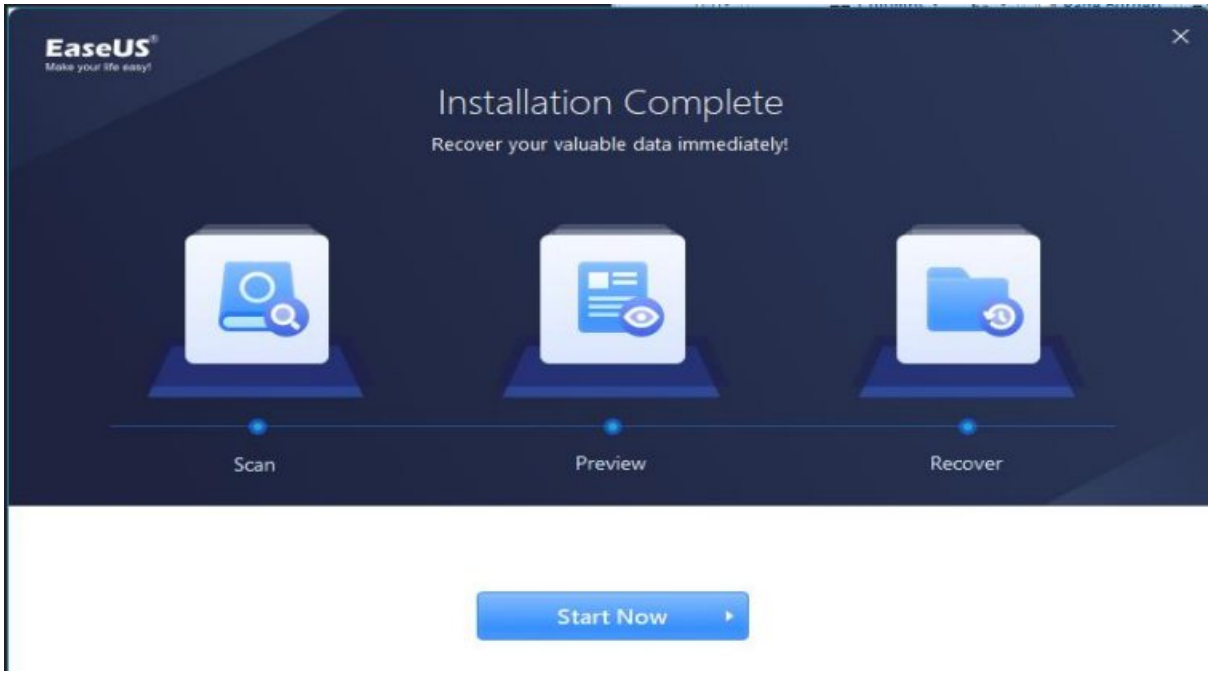


Figure 12: Doing Setup after downloading EaseUS software

Step 3 → Start running after install.

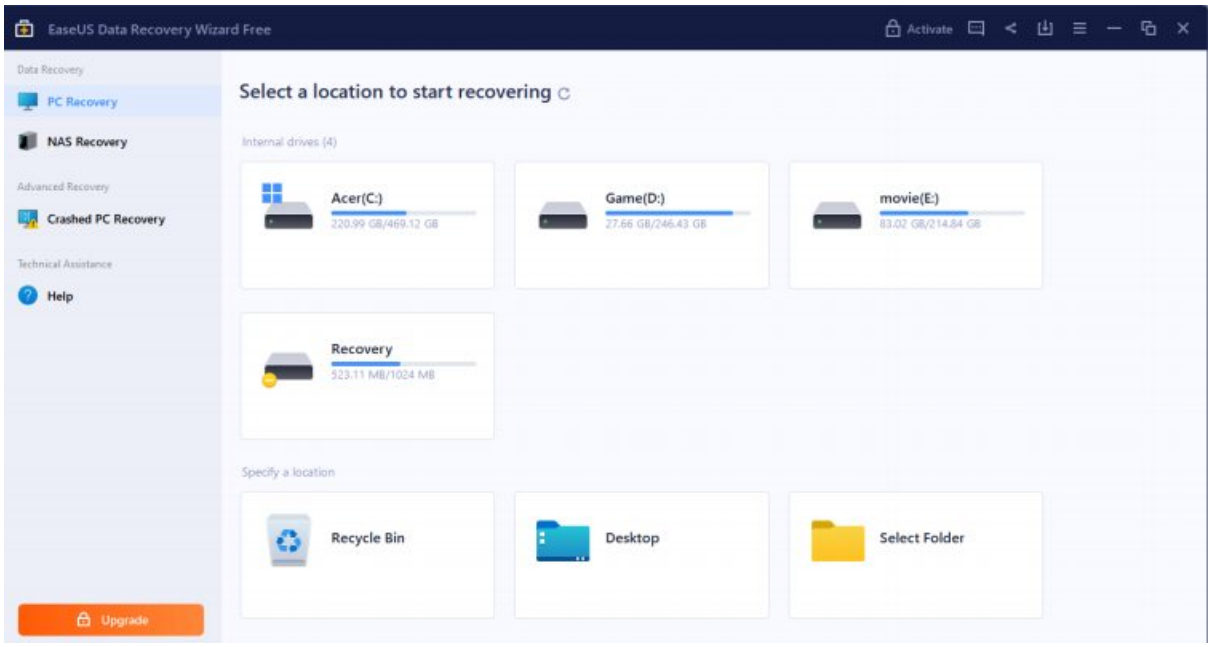


Figure 13: EaseUS software interface

Step 4 → Select drive and select which type of data you want to recover.

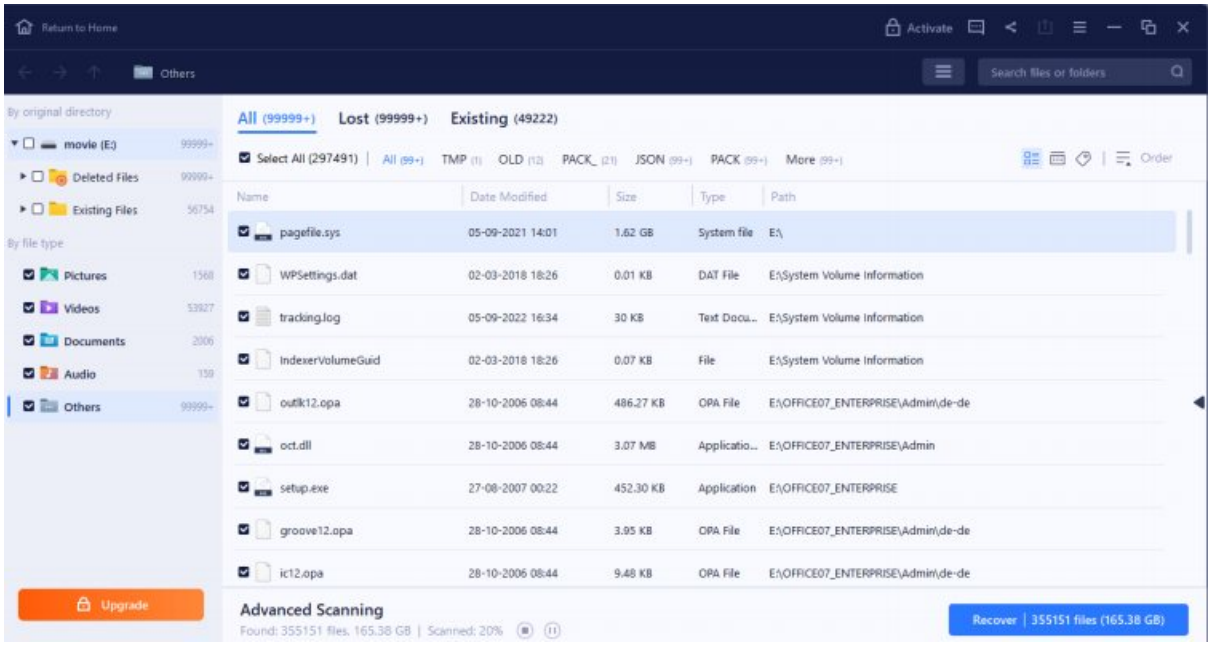


Figure 14: Selecting drive and file type for recovering in EaseUS

Step 5 → Select data you want to recover and click recover button.

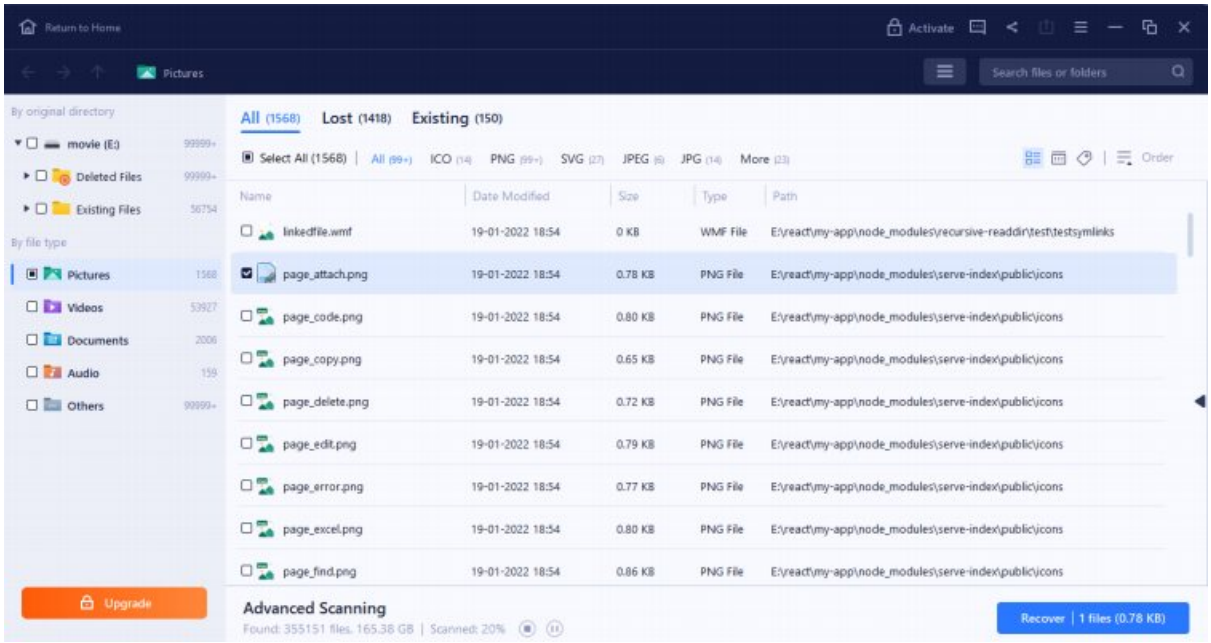


Figure 15: Selecting Data which is going to recover using EaseUS

Step 6 → Select folder where you want to store data.

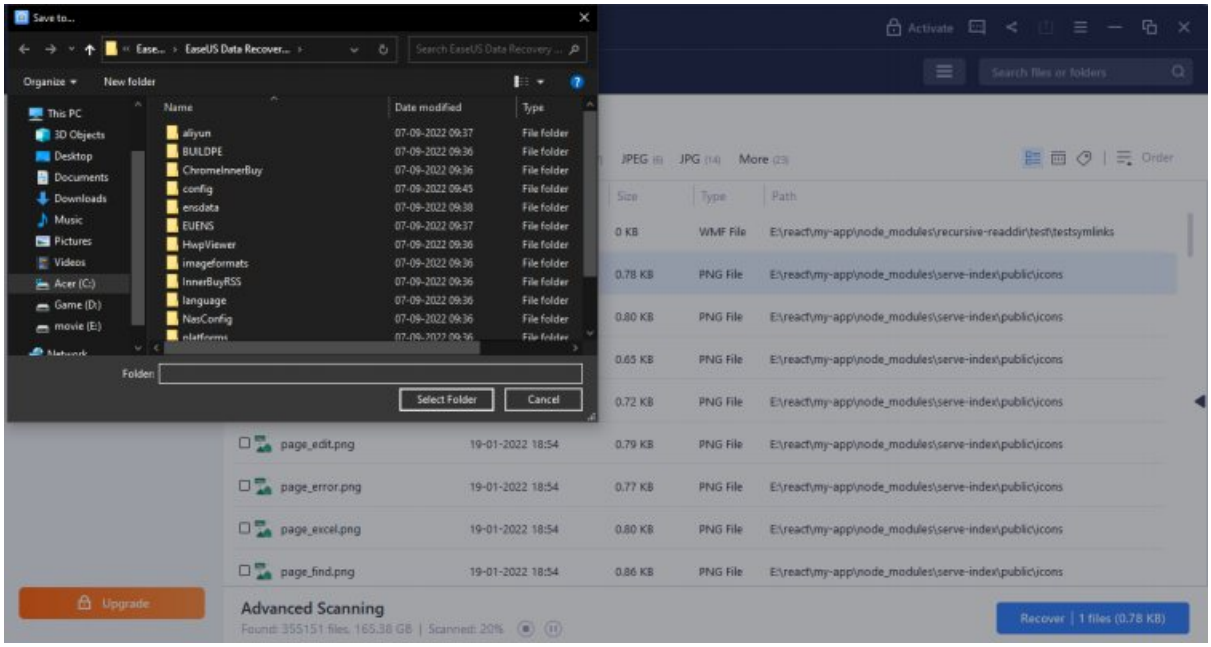


Figure 16: Selecting folder where the recover data is going to store

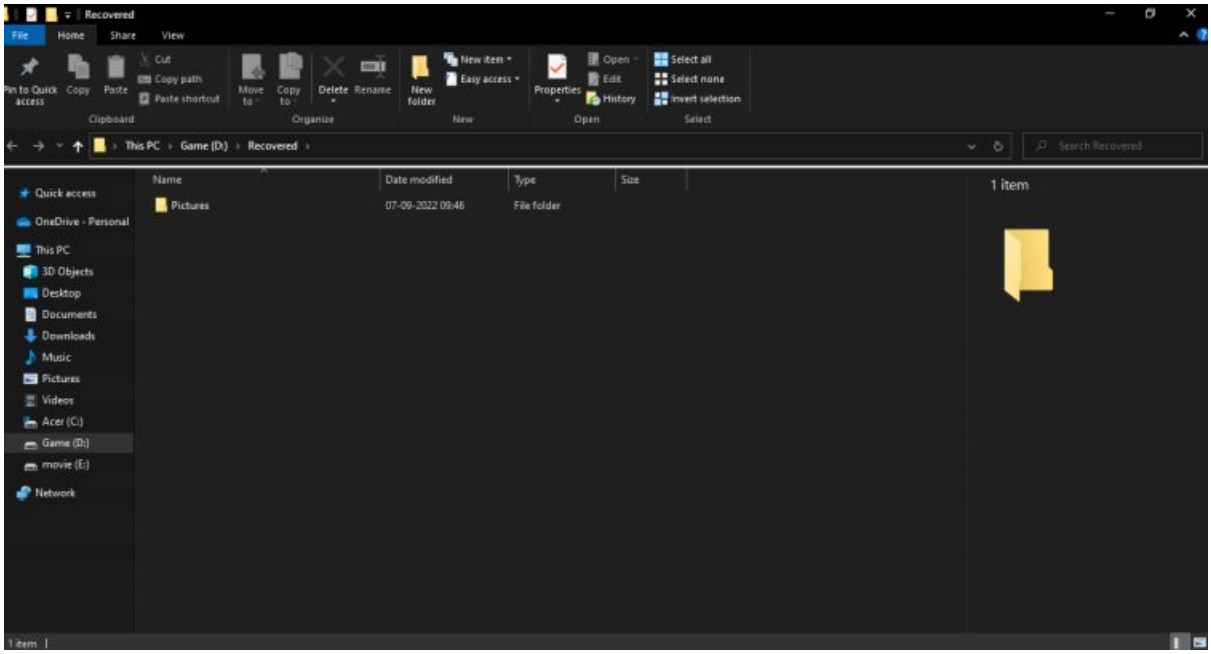


Figure 17: The folder where the recover data is going to store

Step 7 → Finally, your data is recovered, Operation completed for recovering data using EaseUS.

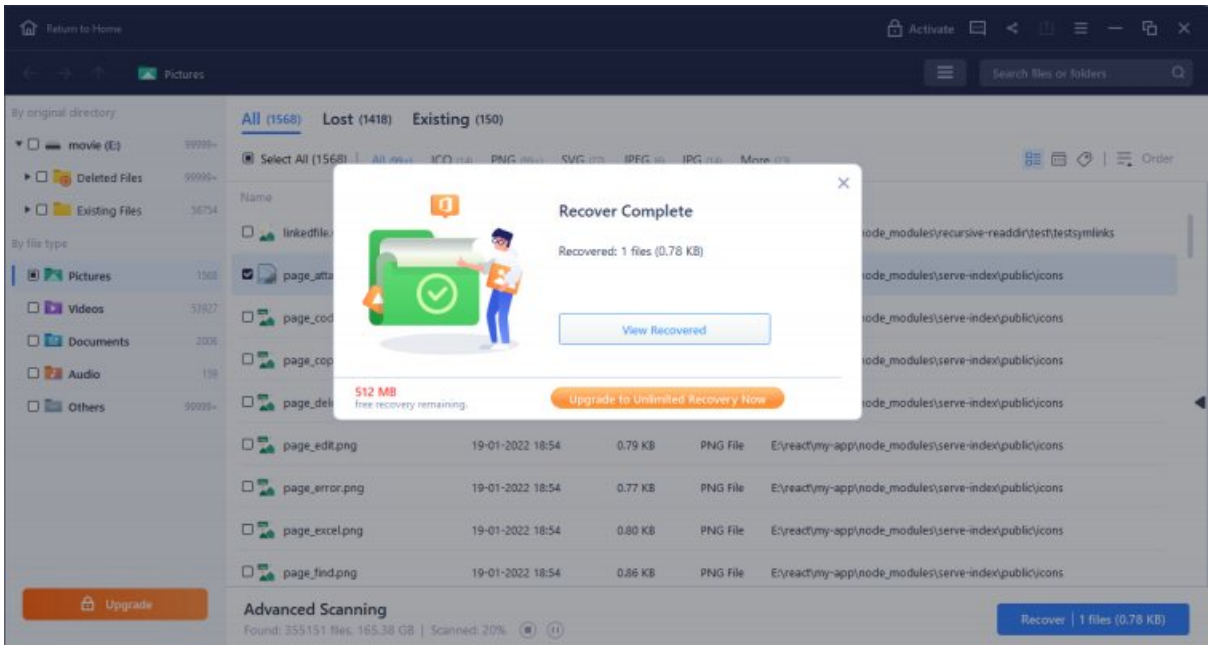


Figure 18: Operation completed for recovering data using EaseUS

Analysis:

Based on our analysis, the EaseUS tool is a reliable and effective digital forensics tool. It is easy to use and provides a wide range of features that make it ideal for use in a variety of investigations. Additionally, the tool is affordable and provides a high degree of customization, making it a great choice for both personal and professional use.

Conclusion:

There are a few things to keep in mind when using data recovery tools like Recuva and EaseUS. First, it is important to remember that these tools are designed to recover lost or deleted files, and they are not designed to repair damaged files. Second, these tools are not always 100% effective, and there is no guarantee that they will be able to recover all of the lost or deleted data. Finally, it is important to create a backup of all important data before using any data recovery tool, just in case the tool is not able to recover the data.

In conclusion, data recovery from computer systems, mobile devices and other electronic peripherals in digital forensics is a process that enables investigators to access and retrieve data that may be important to a case. The data recovered can be used to help piece together what happened, identify suspects and witnesses, and build a strong case. In order to maximize the chances of success, it is important to work with a qualified and experienced digital forensics team.

Digital Forensics Lab Report: 7

Date: 15-09-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of an Email Forensics tools.

Tool Names: Cyberforensics.in (http://cyberforensics.in/), IPAddressLocation (https://www.ipaddresslocation.org/email/tracer.php).

Tasks: Perform Email Forensic using cyberforensics.in. and IPAddressLocation.

Introduction:

What is Email forensic?

Email forensics is the process of using various tools and techniques to examine email messages in order to determine their origin, content, and other relevant information. This process can be used to investigate crimes, track down missing persons, and resolve other legal disputes. Email forensics can be a complex and time-consuming process, but it can provide vital information that would otherwise be unavailable.

Email forensics is the process of analyzing email messages and attachments to determine their origin, content, and purpose. This type of analysis is often used in cases of fraud, harassment, or other criminal activity. Email forensics can be a complex process, as it requires a deep understanding of how email works and the many ways it can be used to hide information. However, with the right tools and expertise, email forensics can be a powerful tool for uncovering the truth.

- **Cyberforensics.in:** Cyberforensics.in is a tool for email forensics that allows users to investigate and analyze email data. The tool provides a variety of features for email forensics, including the ability to search and filter email data, as well as the ability to export email data for further analysis. Cyberforensics.in also includes a variety of tools for email

security, including the ability to create and manage email filters, as well as the ability to create and manage email signatures.

- **IPAddressLocation:** IPAddressLocation is a tool for email forensics that can be used to help determine the location of an email sender. This tool can be used to help investigate suspicious or fraudulent emails, or to simply track down the location of a friend or family member. IPAddressLocation works by using publicly available IP address databases to determine the location of an email sender. This information can be used to approximate the sender's location, and can be helpful in determining whether an email is legitimate or not.

Task 1: Performing Email Forensic using cyberforensics.in

Steps:

Step 1 → Go to the website http://cyberforensics.in/.

Figure 1: Website for cyberforensics.in

Step 2 → Sign up with your email.

Figure 2: Sign Up to use cyberforensics.in tool

Step 3 → After Login the website window is look like the below image.

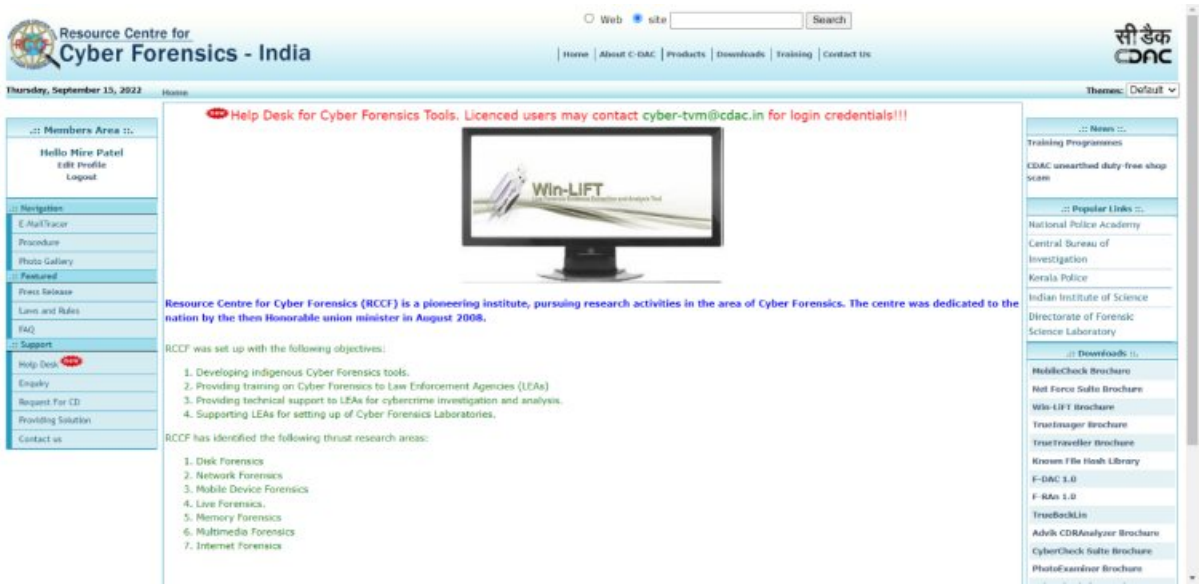


Figure 3: cyberforensics.in tool winow after login

Step 4 → Now go to the email on which you want to do email forensic. Click on three dots of that particular email and then click on “Show original”. It will open the new window with the full details of that email.

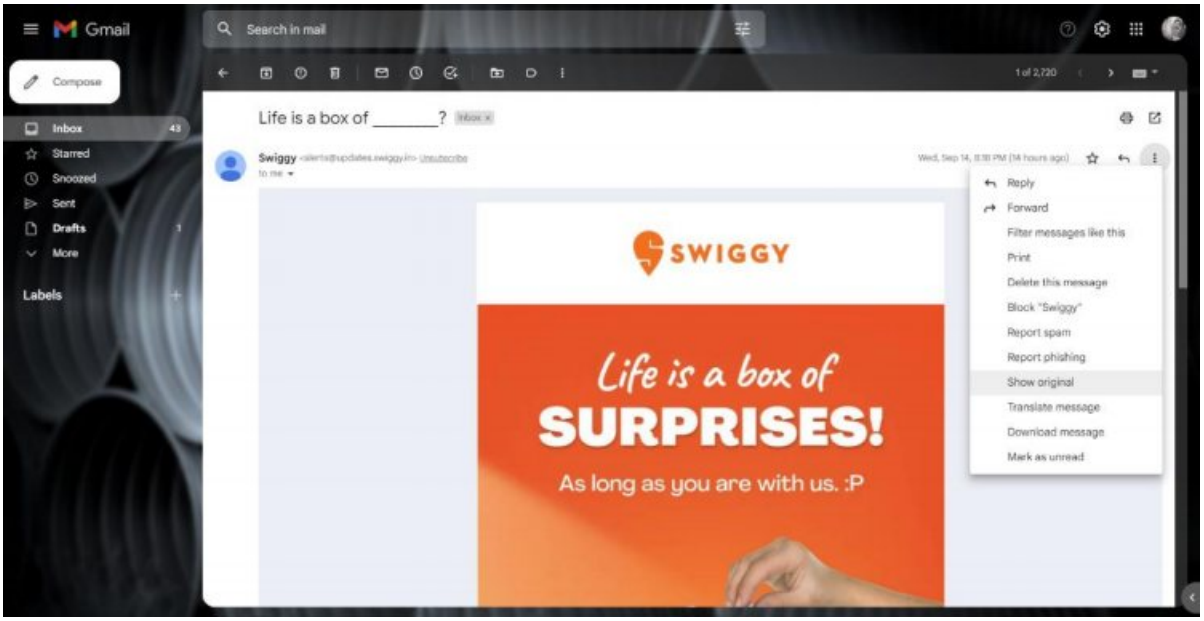


Figure 4: Email on which Email Forensic is doing

Step 5 → Copy the below source code of that email.

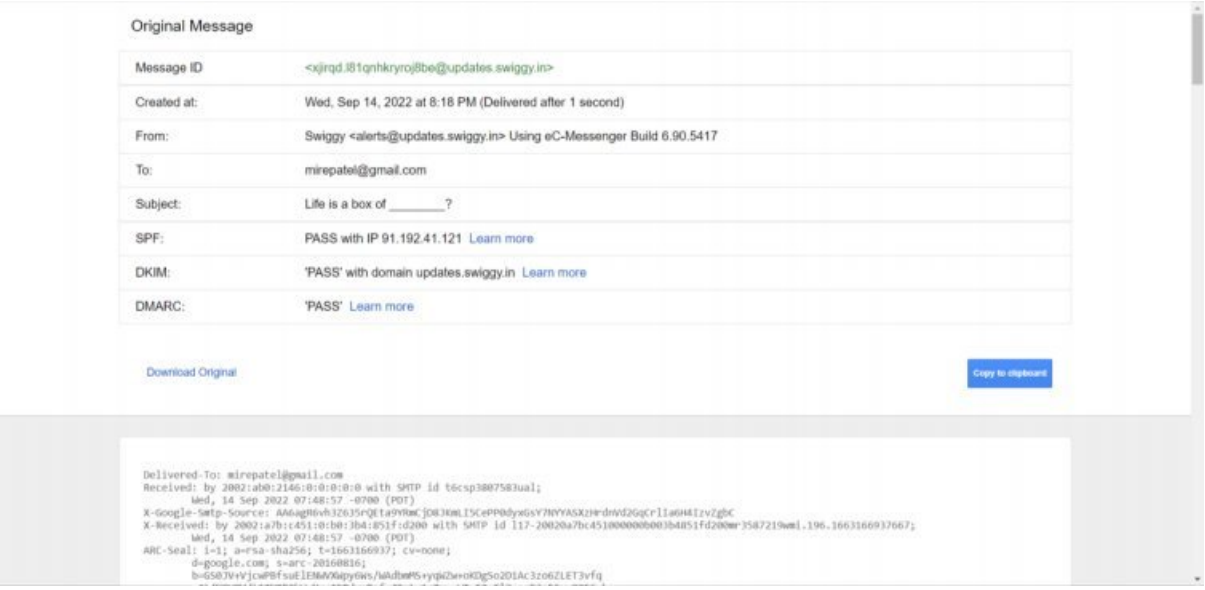


Figure 5: Copying the source code of email on which Email Forensic is doing

Step 6 → Now go to the "E-mailTracer" from the left side panel of that website. Paste that source code of email in the given textbox. And Press "Start Tracing".

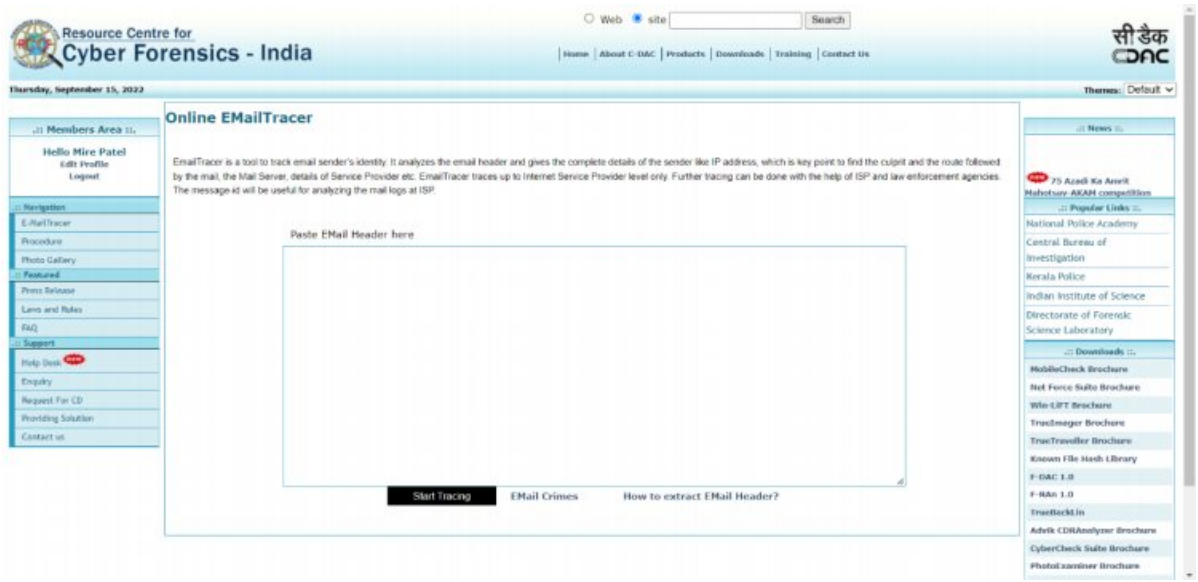


Figure 6: Pasting the source code in cyberforensics.in tool for email forensics

Step 7 → It will trace the email and provide the extract details of that email.

Figure 7: Final Analysis of cyberforensics.in tool

Analysis:

The Cyberforensics.in tool proved to be a very useful tool for email forensics. It was able to extract a great deal of information from the email headers, including the sender and recipient addresses, the date and time of the email, and the subject line. This information was very helpful in determining the origins of the email and its purpose. Additionally, the tool was able to extract the email body, which contained further information about the email's contents. Overall, the Cyberforensics.in tool was a very effective tool for email forensics and provided a great deal of information that was very helpful in the investigation.

Task 2: Performing Email Forensic using IPAddressLocation

Steps:

Step 1 → Go to the website https://www.ipaddresslocation.org/email/tracer.php.

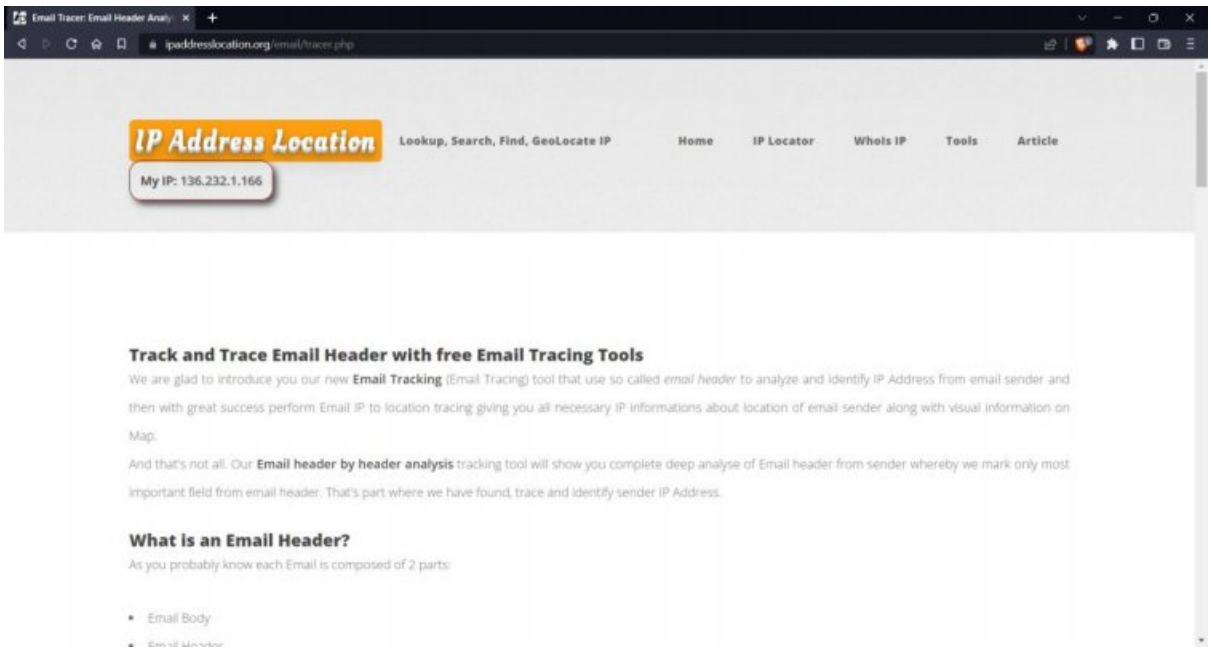


Figure 8: Website for IPAddressLocation tool

Step 2 → In that site, go to the “Email Header Analyzer” Section.

Figure 9: Email Header Analyzer Section of IPAddressLocation tool

Step 3 → Now go to the email on which you want to do email forensic. Click on three dots of that particular email and then click on “Show original”. It will open the new window with the full details of that email.

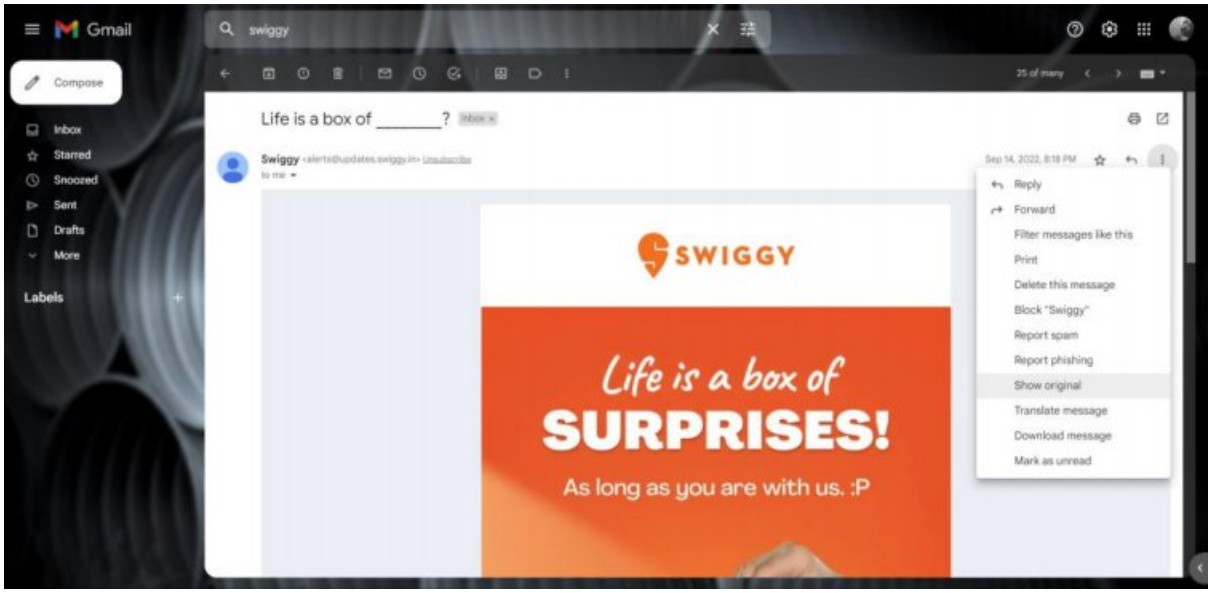


Figure 10: Email on which Email Forensic is doing

Step 4 → Copy the below source code of that email.

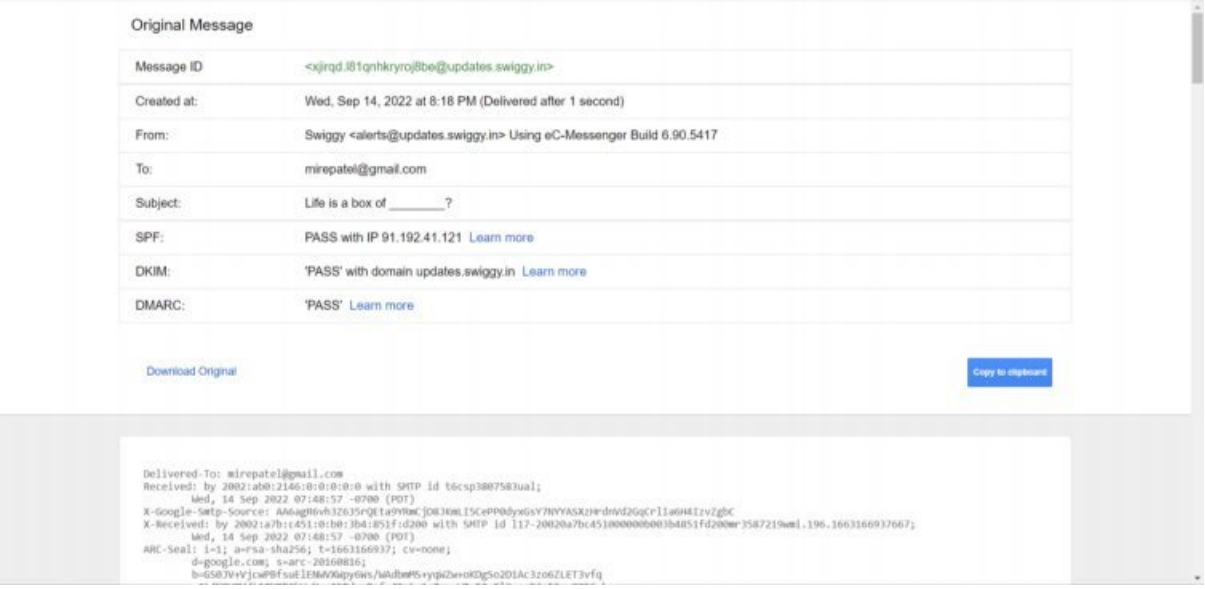


Figure 11: Copying the source code of email on which Email Forensic is doing

Step 5 → Now go to the "Email Header Analyzer" Section input. Paste that source code of email in that section. And Press "Track Email".

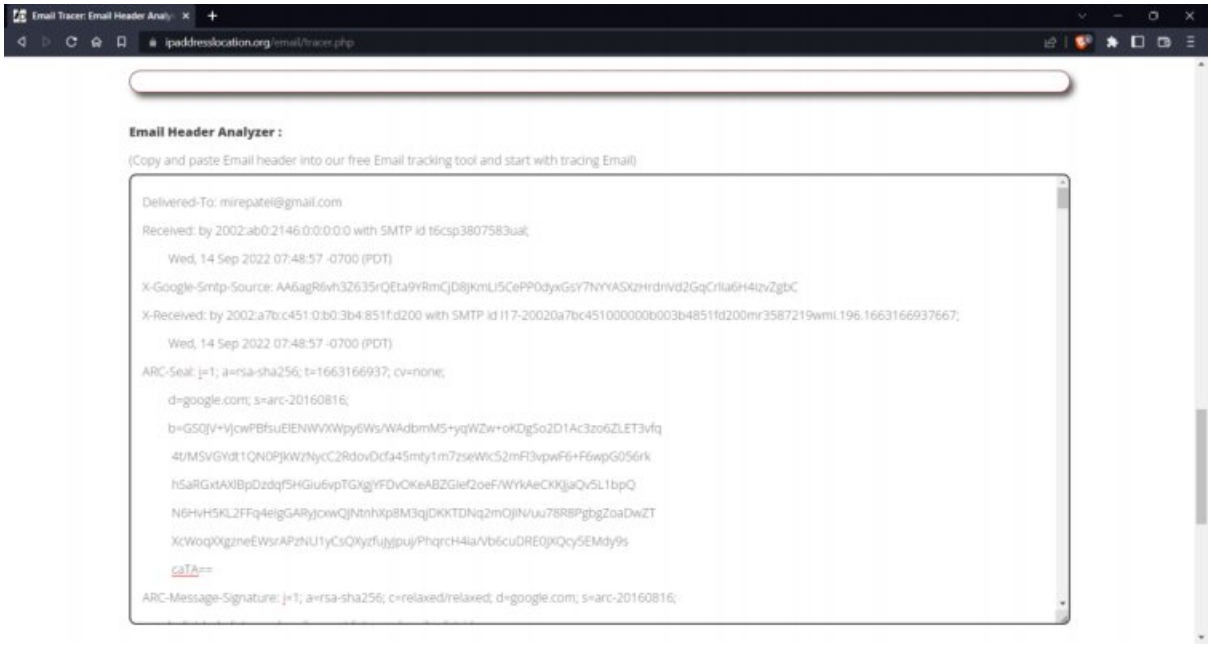


Figure 12: Pasting the source code in IPAddressLocation tool for email forensics

Step 6 → It will trace the email and provide the extract details of that email.

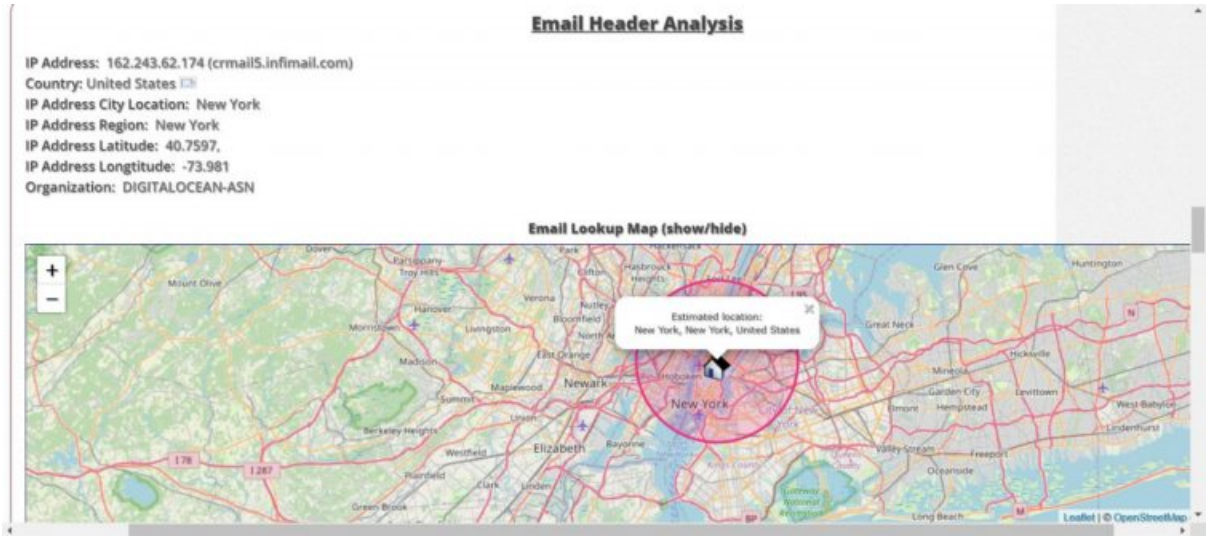


Figure 13: Final Analysis of IPAddressLocation tool

Analysis:

The IPAddressLocation tool is a very practical tool for email forensics. It allows investigators to locate the physical location of an IP address quickly and easily. This can be extremely useful in cases where the email sender is using a spoofed or anonymous IP address. Additionally, the tool can also be used to track down the location of a malicious email server.

Conclusion:

Today, practically everyone who uses internet services throughout the world uses email. Cybercriminals and scammers can send emails with fraudulent and malicious material while remaining anonymous, which can result in hacks and data breaches. And this only increases the value of email forensic analysis. Spoofing, Unauthorized Networks, Open Proxy, Open Mail Relays, SSH Tunnel, Botnets, Untraceable Internet Connections, and Anonymizers are just a few of the methods and tactics used by cybercriminals to conceal their identity.

Digital Forensics Lab Report: 8

Date: 13-10-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Volatile Memory Forensics tools.

Tool Names: Magnet Forensics, FTK Imager, Belkasoft Live RAM Capturer.

Tasks: Explore Magnet Forensics, FTK Imager, and Belkasoft Live RAM Capturer.

Introduction:

Volatile memory forensics is a branch of digital forensics that deals with the analysis of volatile data, or data that is stored in memory and is lost when power is removed from the memory device.

Volatile memory forensics tools are used to extract and analyze data from volatile memory devices, such as RAM. These tools can be used to identify and track down digital evidence, such as data that has been deleted or hidden from the user.

Volatile memory forensics tools are essential for any digital forensic investigation. They can be used to extract and analyze data from devices that are not able to be booted up, or to identify and track down digital evidence that may have been hidden from the user.

What is RAM?

Random Access Memory is known as RAM. It is referred to as a computer's "main memory," which makes it crucial to a computer's operation. Data that is currently being used or is going to be used can be temporarily stored in RAM. However, due to RAM's volatile nature, any data that is stored inside will be lost as soon as the power is cut off. RAM is user-friendly and simple to access because it can be read and written to. Because it speeds up your system, RAM is important because storing data on your hard drive slows down your system and consumes a lot of time. RAM is helpful for storing and recovering data from the machine.

Benefits for capture the memory

RAM capture is a crucial activity since investigators have come to learn that a variety of facts can be found in volatile memory. This information can be helpful in an investigation and further enable an investigator to determine what programmes a suspect or attacker was using at the time of the attack. It is also conceivable that remote attackers using RAM rather than the system would have some data or tools saved there.

- **Magnet Forensics tool:** Magnet Forensics is a free RAM capturing or memory imaging programme that is used to capture the actual memory of a suspect's system. This tool enables investigators to analyse and retrieve the important information that can only be discovered in the system memory. Magnet Ram capture has a modest memory footprint, allowing the user to continue working with the tool even as memory is being overwritten with new data. Raw (.DMP/.RAW/.BIN) memory data can be easily captured and analysed. A programme running on the computer, network connections, signs of malware incursion, registry hives, usernames and passwords, decrypted files and keys, and other evidence that can be located in the RAM are processed.

- **FTK Imager tool:** For Windows 32-bit and 64-bit systems, the FTK imager can generate a live memory image and paging file. There, we can get the FTK imager and install it on our PC. The FTK imager was created primarily to analyse and index data in advance and try to reduce the amount of time wasted waiting for searches to run. FTK gets us there faster and better than anything else, regardless of how many different types of data we are working with or how much data we must process.

- **Belkasoft Live RAM Capturer tool:** Belkasoft Live RAM Capturer is a small, free forensic programme that enables users to successfully extract all of the data from a computer's volatile memory, even when the system is actively preventing debugging or dumping. To reduce the tool's footprint as much as feasible, separate 32-bit and 64-bit variants are available. Live RAM Analysis in Belkasoft Evidence Center can be used to examine memory dumps obtained using Belkasoft Live RAM Capturer. All editions and versions of Windows, including XP, Vista, Windows 7, 8, and 10, as well as 2003 and 2008 Server, are compatible with Belkasoft Live RAM Capturer.

Task 1: Exploring Magnet Forensics

Steps:

Step 1 → First, go to https://www.magnetforensics.com/resources/magnet-ram-capture/ and download Magnet Forensics software from there and then installing it in our system.

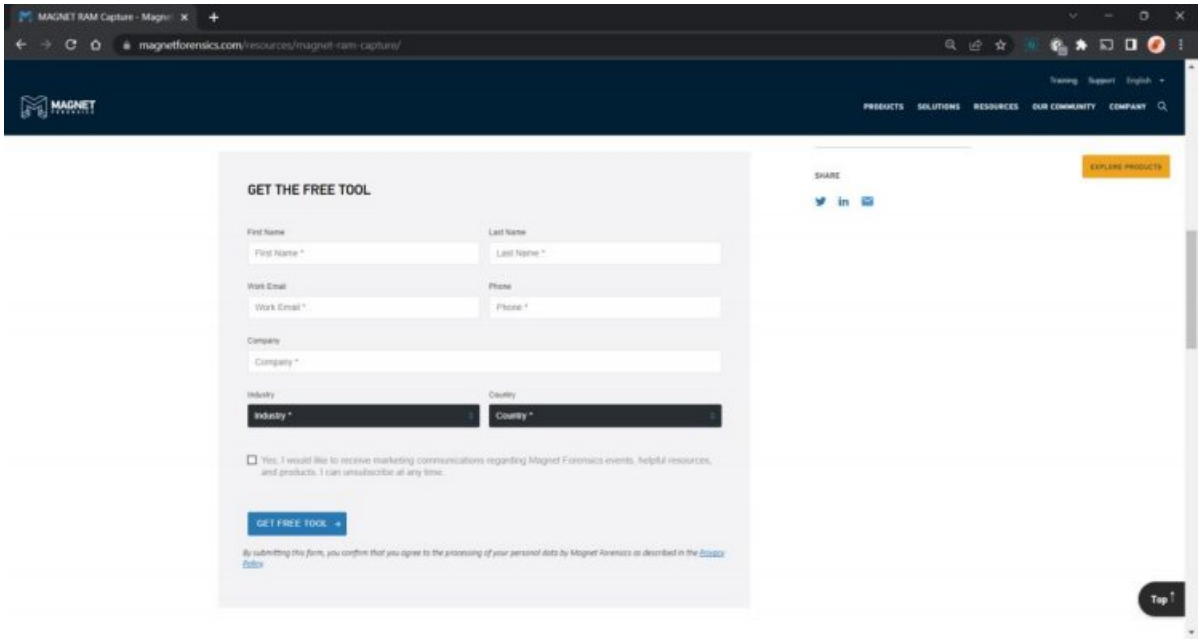


Figure 1: Website to download Magnet Forensics Tool

Step 2 → After installing the software, we can start the Ram capturing process by just executing the Magnet Forensics software by clicking on it.

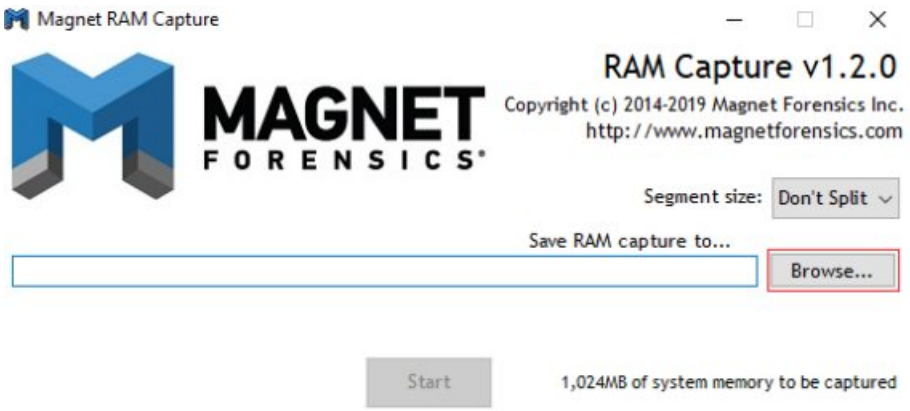


Figure 2: Starting the RAM Capturing using Magnet Forensics Tool

Step 3 → Now our captured memory which is known as the RAM image, that is successfully created.

Step 4 → As seen in the figure below, we must specify the memory image's name and the format in which we want to capture the memory image.

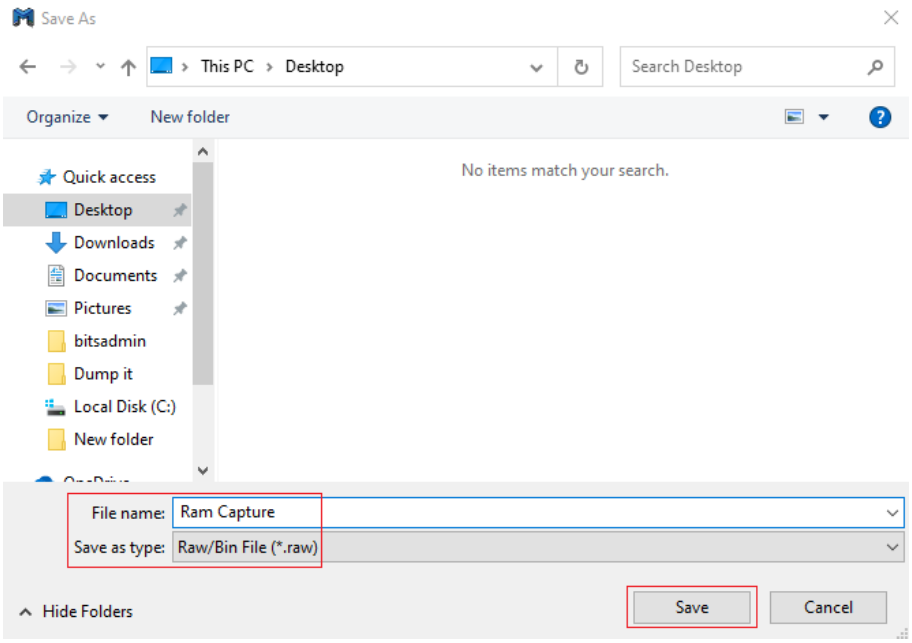


Figure 3: Providing the file name and format in which the memory image is going to capture

Step 5 → After giving the mentioned information, we now begin the process of capturing the memory image. The amount of time it takes to complete the operation depends on the size of the memory.

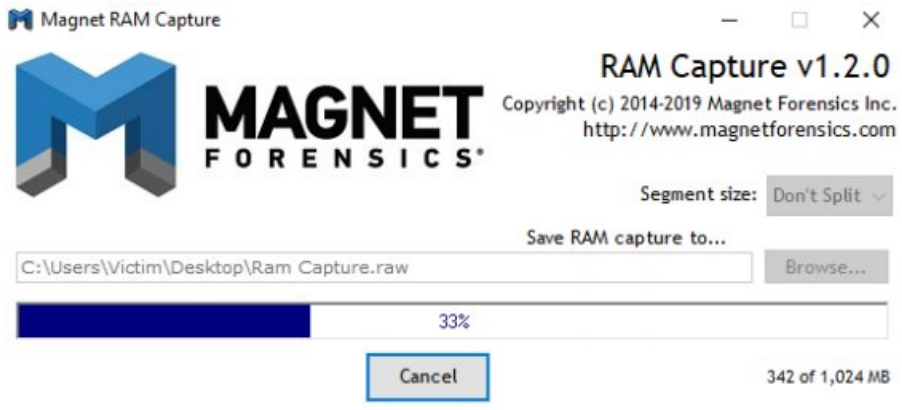


Figure 4: Process of capturing the memory image using Magnet Forensics Tool

Step 6 → It displays a pop-up message indicating that the operation was completed and giving us the path location where our previously provided captured memory is situated after completing it.

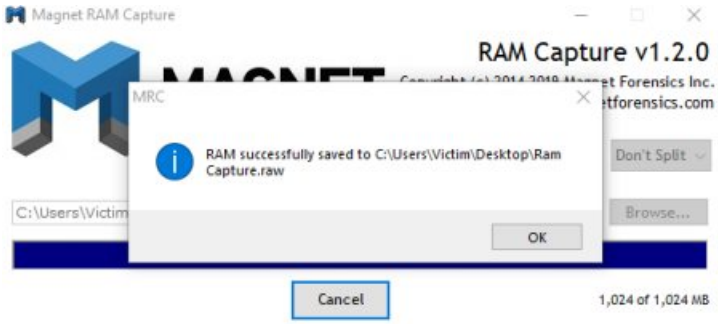


Figure 5: Successful pop-up message for capturing memory image using Magnet Forensics Tool

Step 7 → Now that our image has been successfully constructed, as shown in the image below, we can check our located path to see if our memory image was generated or not. We can then analyse that memory image.

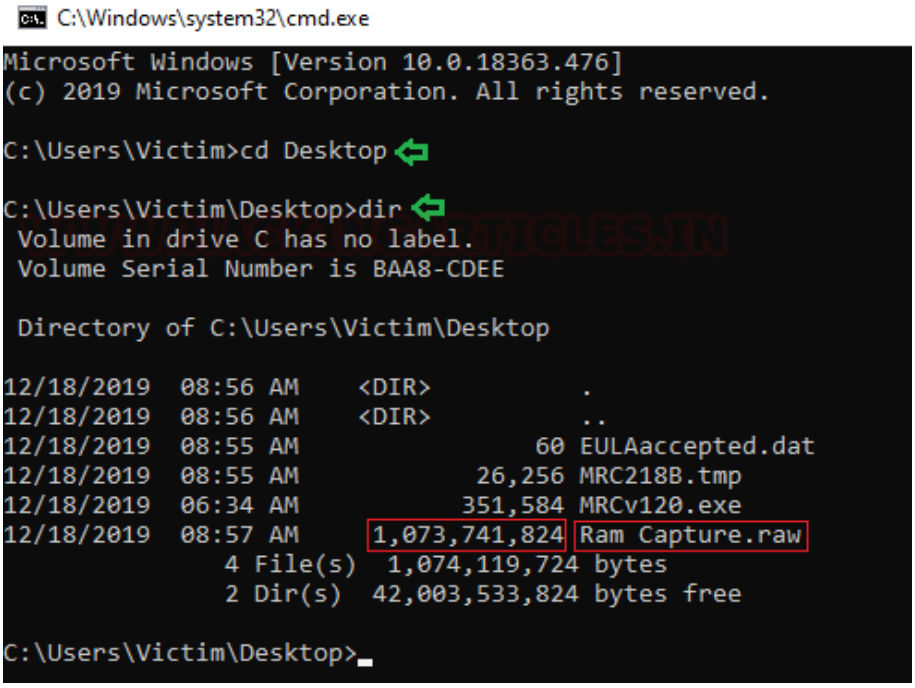


Figure 6: Checking located path for captured memory image

Analysis:

Overall, the Magnet Forensics tool was able to capture a memory in digital forensics quite well. The Magnet Forensics tool is a valuable addition to any digital forensics' toolkit. Its ability to extract a wide variety of data from a variety of sources makes it an ideal tool for investigators. Additionally, the ease of use and the ability to create customized reports make it a valuable tool for both novice and experienced users alike.

Task 2: Exploring FTK Imager

Steps:

Step 1 → Go to https://accessdata.com/product-download/ftk-imager-version-4-5 and download FTK Imager software from there and then installing it in our system.

Step 2 → After installing the software start the AccessData FTK Imager tool.

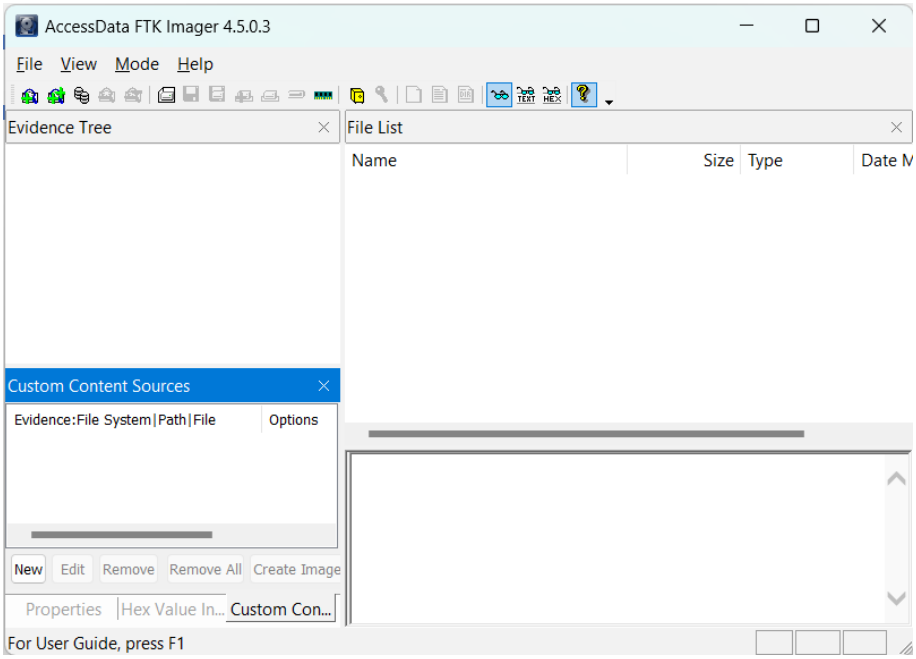


Figure 7: FTK Imager Tool window

Step 3 → Now we need to click on the "File" button as shown in the below image to start the process.

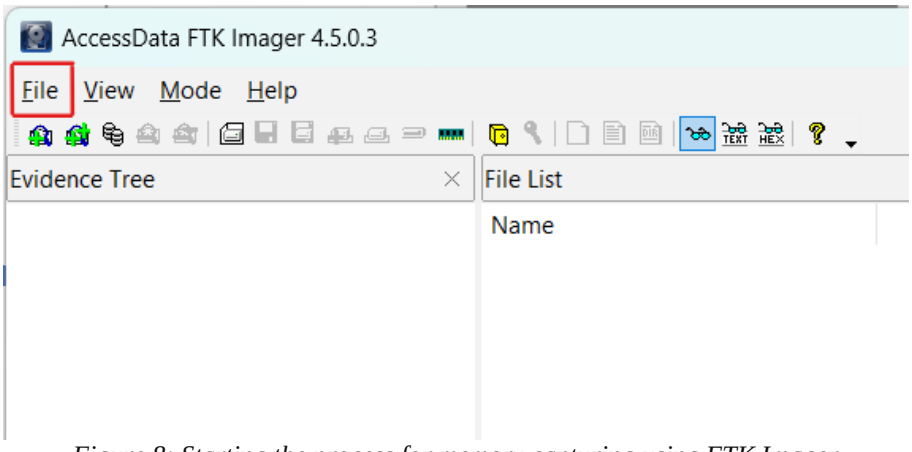


Figure 8: Starting the process for memory capturing using FTK Imager

Step 4 → After clicking on the "File" button our screen would look like the below image. Now we need to search the "Capture memory" button and click on that button for the start of the capture memory process using FTK Imager tool.

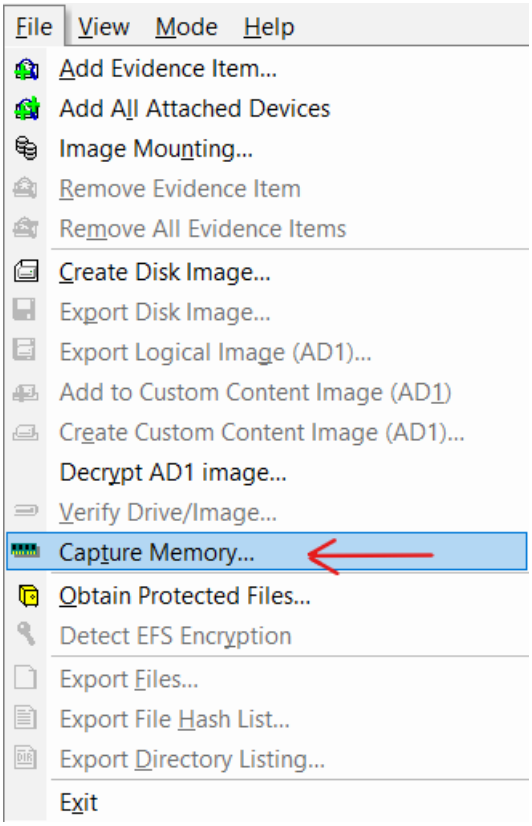


Figure 9: Clicking on "Capture Memory" to start the process

Step 5 → After then we need to provide some information regarding that image such as the destination path of the memory image, the file name of the memory image and we want to include its page file and AD1 file or not.

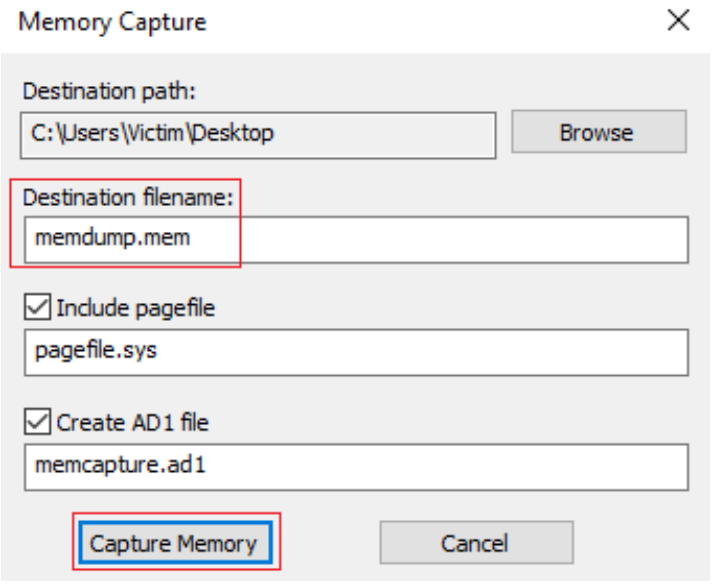


Figure 10: Providing Details to store the Memory Capture Files

Step 6 → After providing that information, the process got started along with that it also consistently the status of our process and the final destination or path was our image going to save.

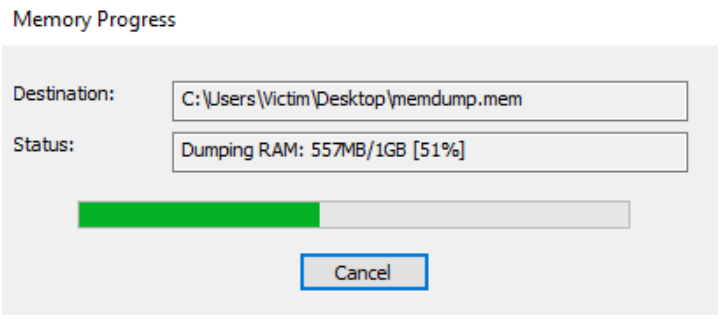


Figure 11: Memory Process for Memory Capture using FTK Imager Tool

Step 7 → After completing its show the message which says "Memory capture finished successfully" and our memory image location or destination.

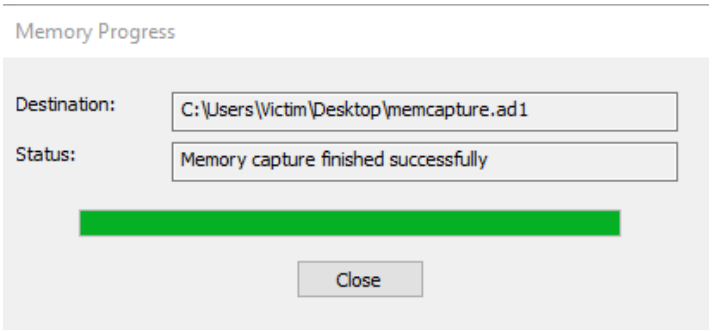


Figure 12: Successful message for capturing memory image using FTK Imager Tool

Step 8 → At the end, we are going to check on that location whether our image is saved or not, but as we can see in the below image that we were able to capture the memory image successfully using FTK Imager tool.

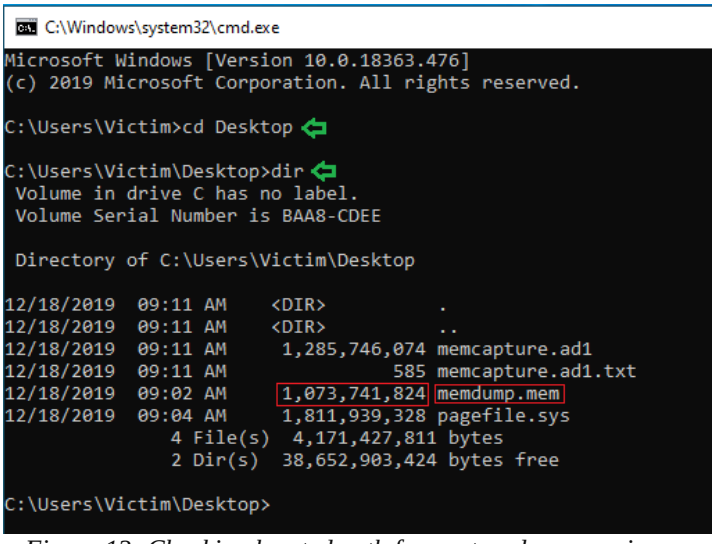


Figure 13: Checking located path for captured memory image

Analysis:

The FTK Imager tool is an important tool for digital forensics investigators. It can be used to capture a memory image of a computer, which can then be analyzed for evidence. The tool is easy to use and provides a great deal of information that can be used to help solve a case. Overall, the FTK Imager tool is a powerful tool for volatile memory forensics. It has a simple and user-friendly interface that makes it easy to use. It is also able to capture a wide range of data, including system information, network activity, and process information.

Task 3: Exploring Belkasoft Live RAM Capturer

Steps:

Step 1 → First we need to go to https://belkasoft.com/get and download Belkasoft Live RAM Capturer from there and then installing it in our system.

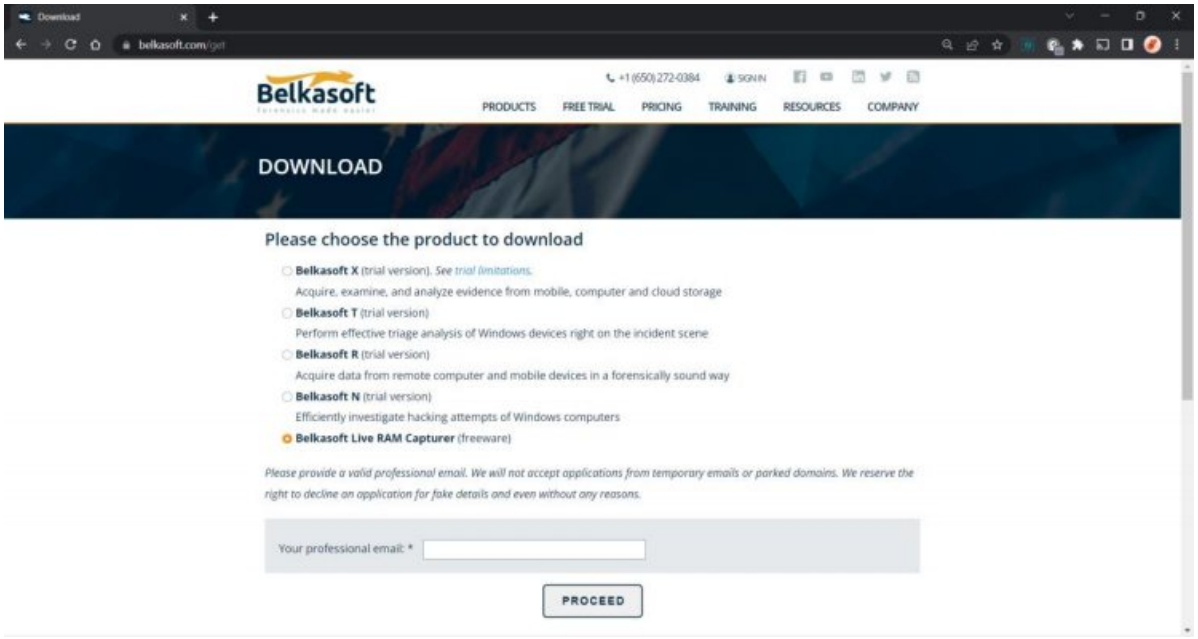


Figure 14: Website to download Belkasoft Live RAM Capture Tool

Step 2 → After then open this software and select the path where we want to save our memory image and Click on the “Capture” button.

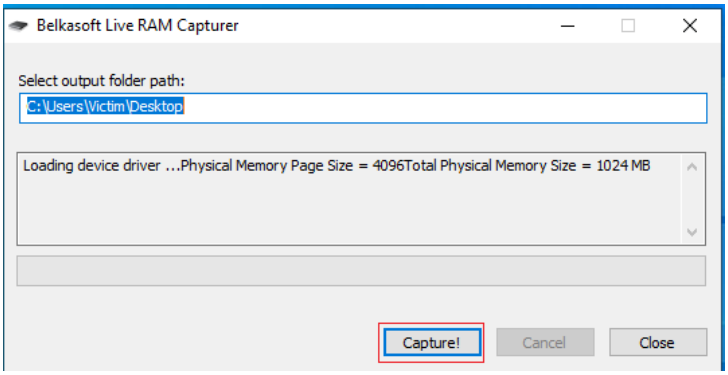


Figure 15: Selecting the file path to saving the memory image using Belkasoft Live RAM Capture

Step 3 → After providing all the details it starts to load its drivers to start the process of capturing the memory image, now it shows the active live progression of the task to capture the memory image.

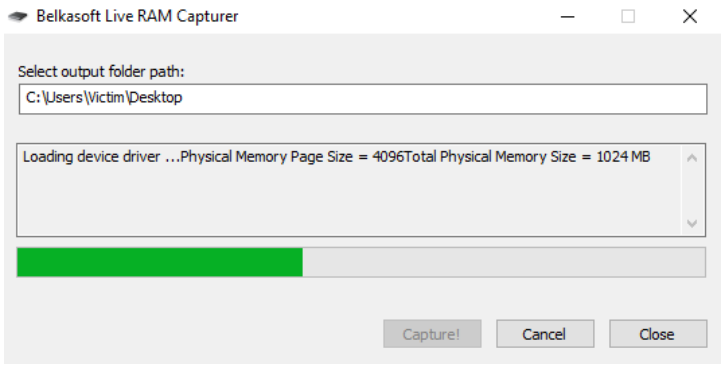


Figure 16: Memory Process for Memory Capture using Belkasoft Live RAM Capture Tool

Step 4 → After completing the overall process for capturing memory, it completes its active progression and provide us some sneak peeks of our captured memory and suggests to us its image analyser from belkasoft and also provides its link to download it.

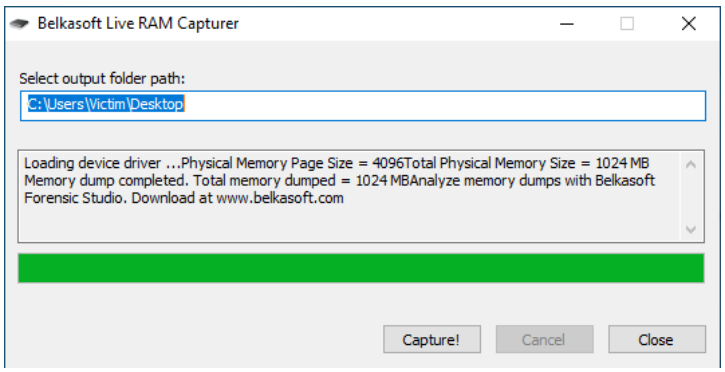


Figure 17: Successful message for capturing memory image using Belkasoft Live RAM Capture Tool

Step 5 → At the end, we need to check whether our memory will be captured or not. As we can see in the image given below, we succeed in our process to capture the memory image using Belkasoft Live RAM Capture tool.

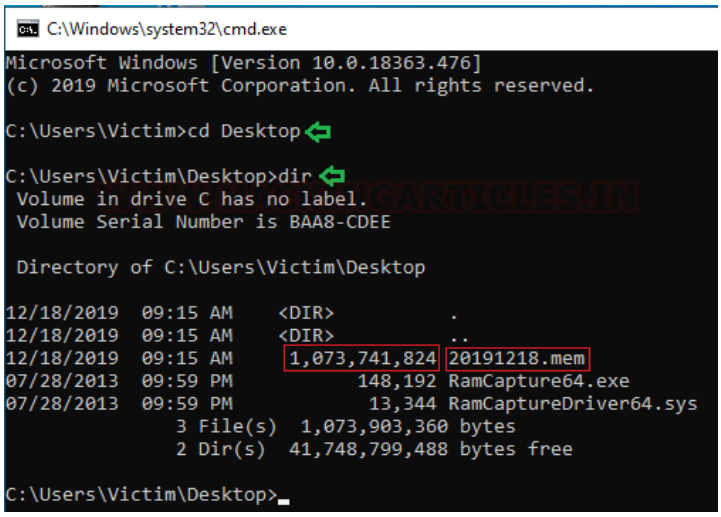


Figure 18: Checking located path for captured memory image

Analysis:

Overall, Belkasoft Live RAM Capturer is an effective tool for capturing and analyzing live memory. It is easy to use and provides a variety of features for capturing and analyzing live memory data. It is a valuable tool for forensics investigators and incident response teams.

Final Analysis using WinHEX:

Steps:

Step 1 → Visit http://www.winhex.com/winhex/hex-editor.html and download the WinHEX software.

Figure 19: Website to download WinHEX software

Step 2 → Once the process of capturing memory image completed by above tools, a raw file will be created. Now, open WinHEX and then open the created raw file.

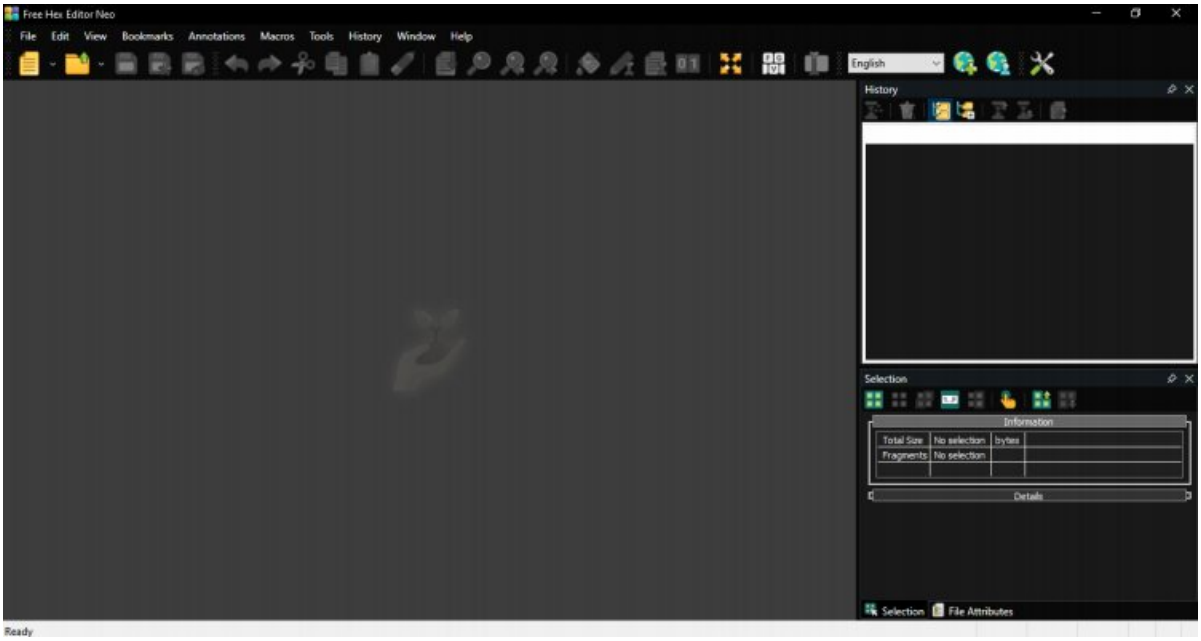


Figure 20: WinHEX software interface

Step 3 → Import file from which created using FTK imager.

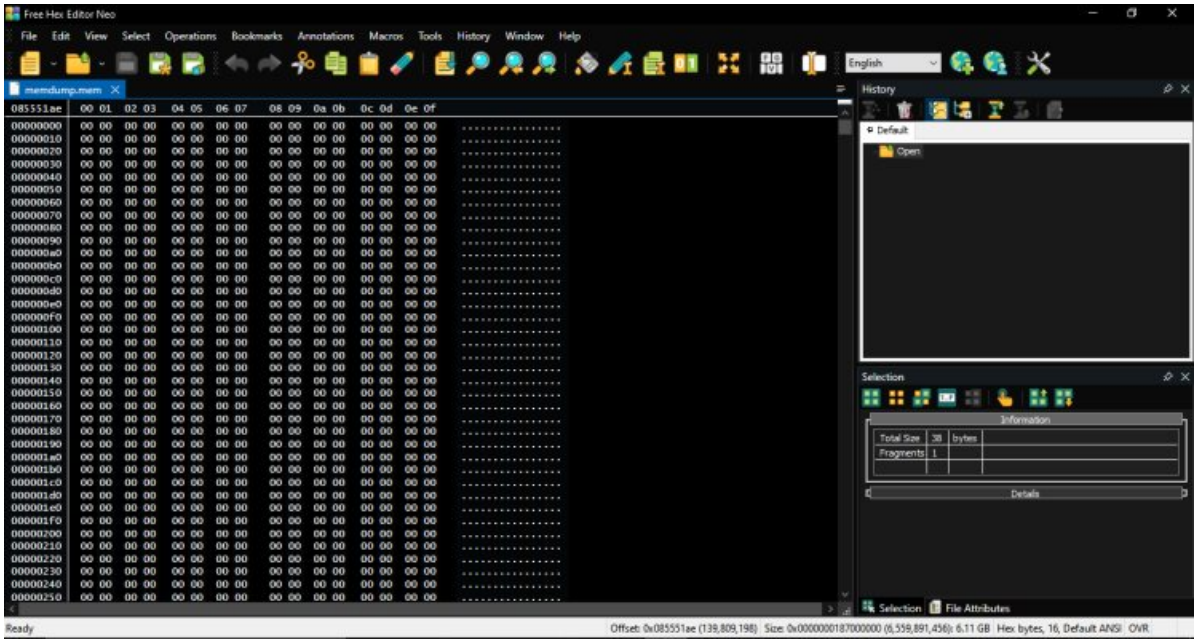


Figure 21: Importing the file which is created by FTK imager

Step 4 → Findings.

i. Gmail id and Password

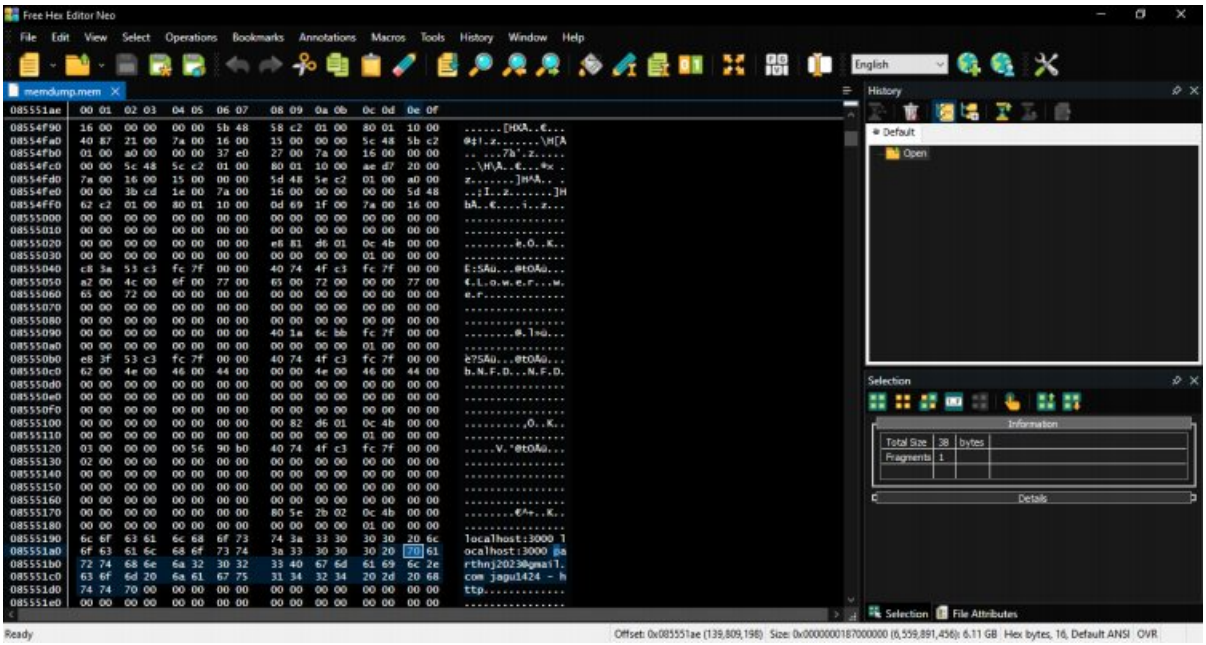


Figure 22: Found Gmail id and Password using WinHEX

ii. YouTube Video Link

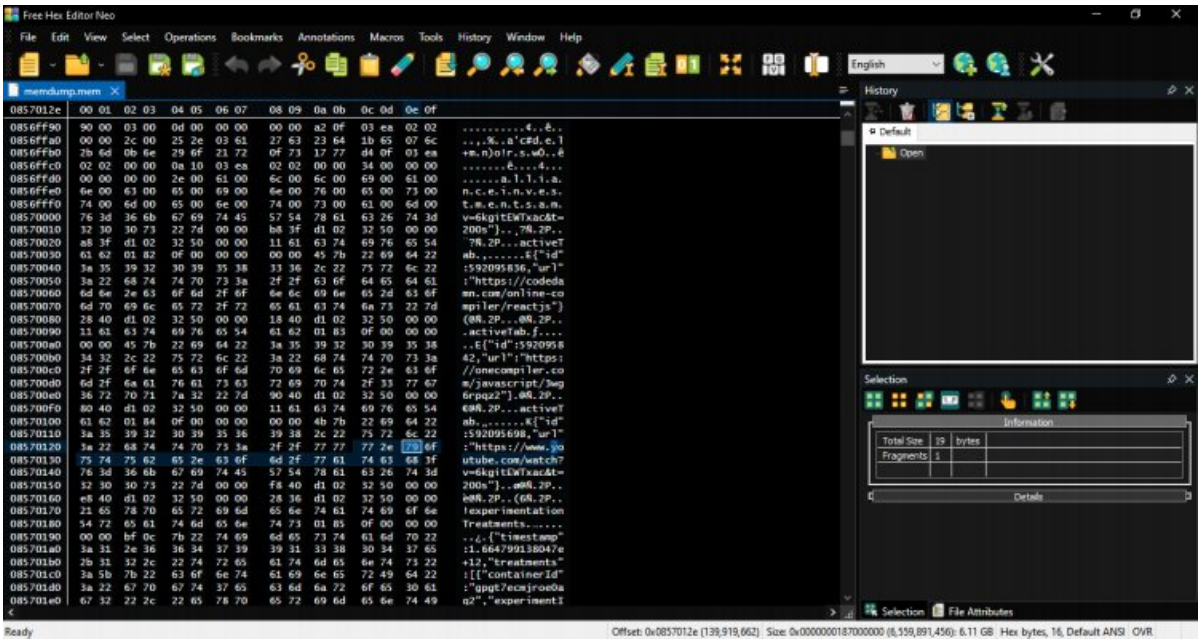


Figure 23: Found YouTube Video Link using WinHEX

iii. LinkedIn Website

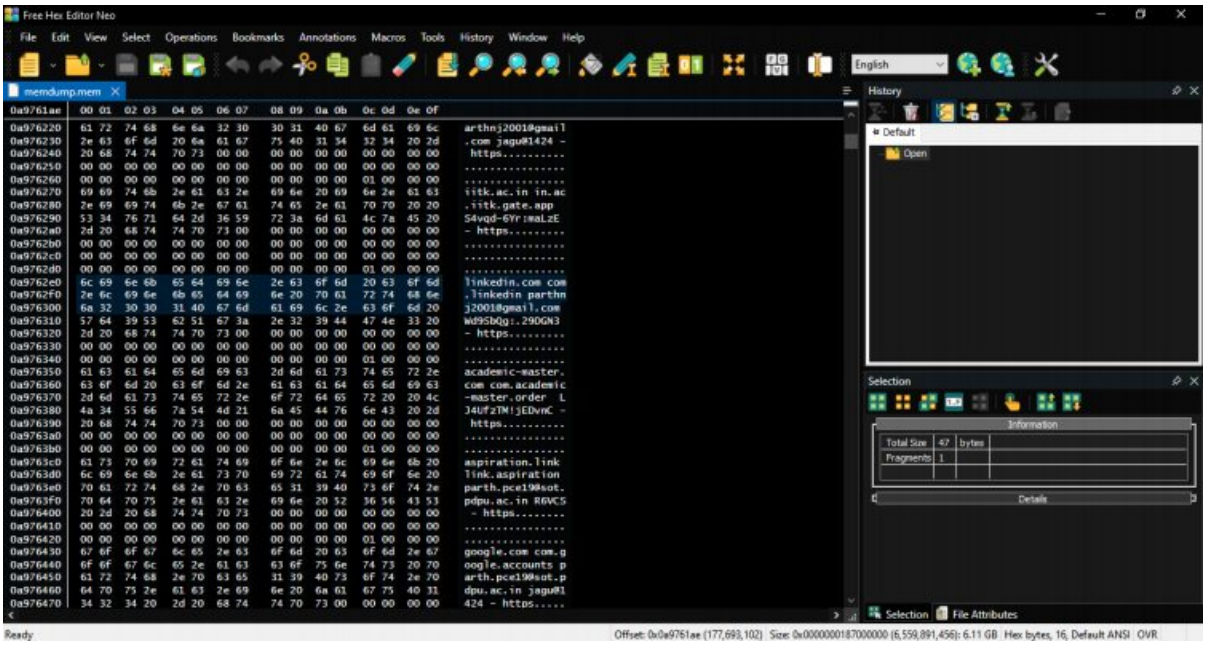


Figure 24: Found LinkedIn Website using WinHEX

iv. Gate Website Account

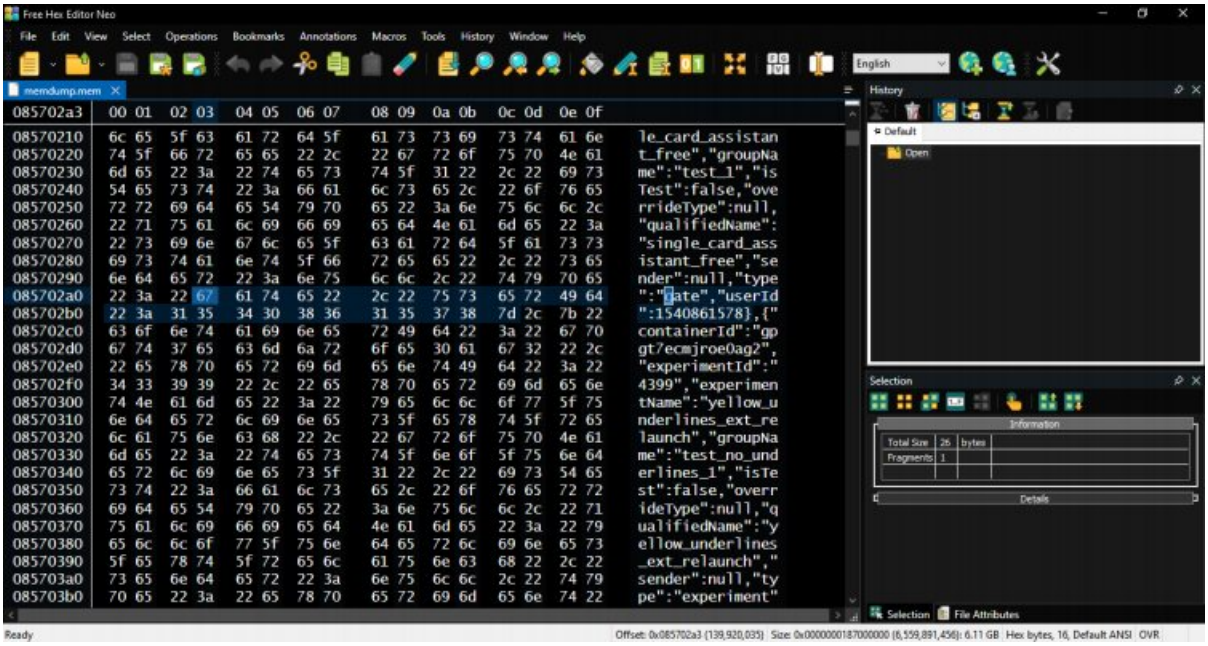


Figure 25: Found Gate Website Account using WinHEX

Conclusion:

Volatile memory forensics tools are essential for digital forensics investigators. They allow investigators to capture and analyze the contents of a computer's memory, which can provide valuable information about what happened on a computer during an incident.

Magnet Forensics, FTK Imager, and Belkasoft Live RAM Capturer are all popular volatile memory forensics tools. They each have their own strengths and weaknesses, but all three are capable of capturing and analyzing the contents of a computer's memory. In general, Magnet Forensics is a good all-around tool, FTK Imager is better for imaging hard drives, and Belkasoft Live RAM Capturer is better for capturing data from live systems. Overall, all of the tools performed well in terms of their ability to capture and analyze volatile memory.

Digital Forensics Lab Report: 9

Date: 03-11-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Hash and Hex analysis tools.

Tool Names: WinHEX, HashMyFiles, Gary Kessler's File Signature Table.

Tasks: Explore WinHEX, HashMyFiles, and Gary Kessler's File Signature Table tools.

Introduction:

In digital forensics, hash and hex analysis are two important tools for investigators. Hash analysis is used to identify and track unique files, while hex analysis is used to examine the contents of a file.

Hash analysis is a way of identifying files by their content, rather than their name or location. This means that even if a file is renamed or moved, it can still be identified by its hash. Hex analysis is a way of examining the contents of a file, in order to find hidden data or to understand how the file works.

Hash and hex analysis are both important tools for digital forensics investigators. They can be used together to help identify and track files, as well as to understand the contents of a file.

- **WinHEX tool:** WinHEX is a disk editor and hexadecimal editor, particularly useful for computer forensics, data recovery, low-level data processing, and IT security. It can display and edit data in hexadecimal, decimal, octal, binary, and text formats. It can also read and write files in various formats, including Intel Hex, Motorola S-record, ASCII text, and more.

- **HashMyFiles tool:** HashMyFiles is a small utility that allows you to calculate the MD5, SHA1, CRC32, or BLAKE2 hash of one or more files in your system. You can also verify the hash to ensure the file's integrity. HashMyFiles can be used to calculate the hash of all files in a directory, or only specific types of files (e.g., .exe, .dll, .ocx, .jpg, .mp3, etc.). The hashing algorithms supported by HashMyFiles are MD5, SHA1, CRC32, and BLAKE2. HashMyFiles is a portable utility, which means that you can run it without having to install it on your system. You can also run it from a USB flash drive or a CD/DVD. HashMyFiles is a useful tool for digital forensics investigators, as it can help to verify the integrity of files. It can also be used to calculate the hash of a known file to check if it has been modified.

- **Gary Kessler's File Signature Table tool:** GCK'S FILE SIGNATURES TABLE is a digital forensics tool that can be used to identify the file formats of digital files. It can be used to identify the file formats of many different types of files, including images, videos, documents, and more. It is a useful tool for investigators who need to identify the file format of a file in order to determine its contents.

Task 1: Exploring WinHEX Tool

Steps:

Step 1 → Visit **https://x-ways.net/winhex/** and Download WinHEX tool from there.

Figure 1: Website to download WinHEX Tool

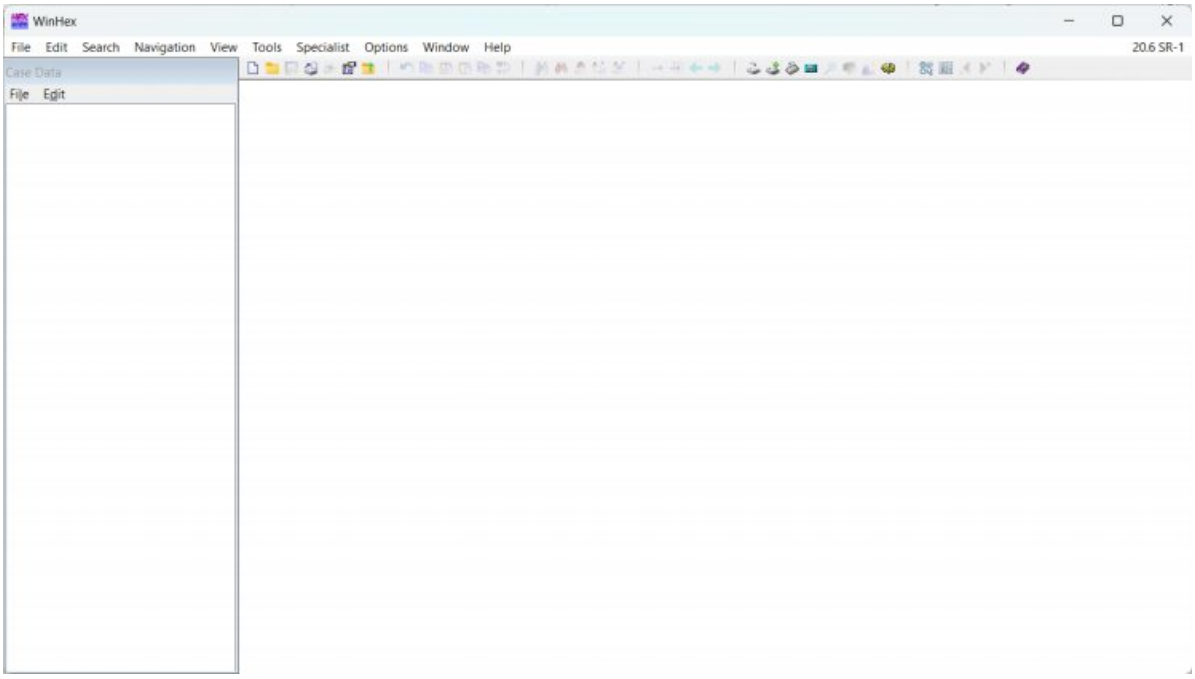


Figure 2: WinHEX Tool Window

Step 2 → Open WinHEX application and select file that you want to analyze.

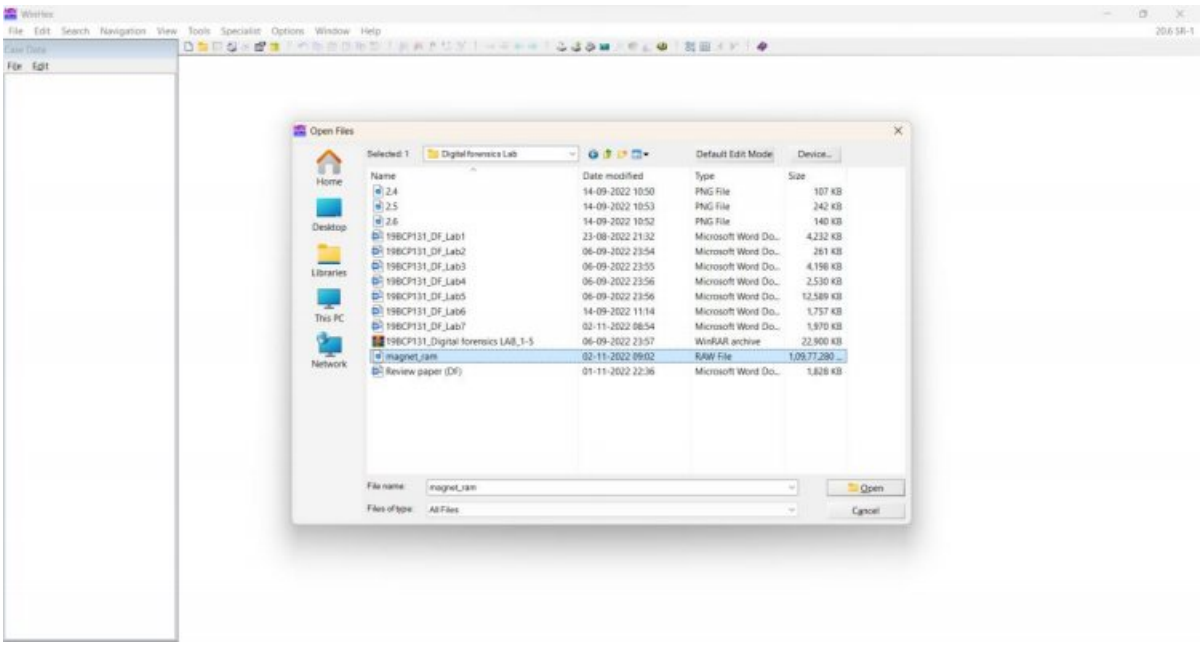


Figure 3: Analyzing File in WinHEX

Analysis:

i. Address:

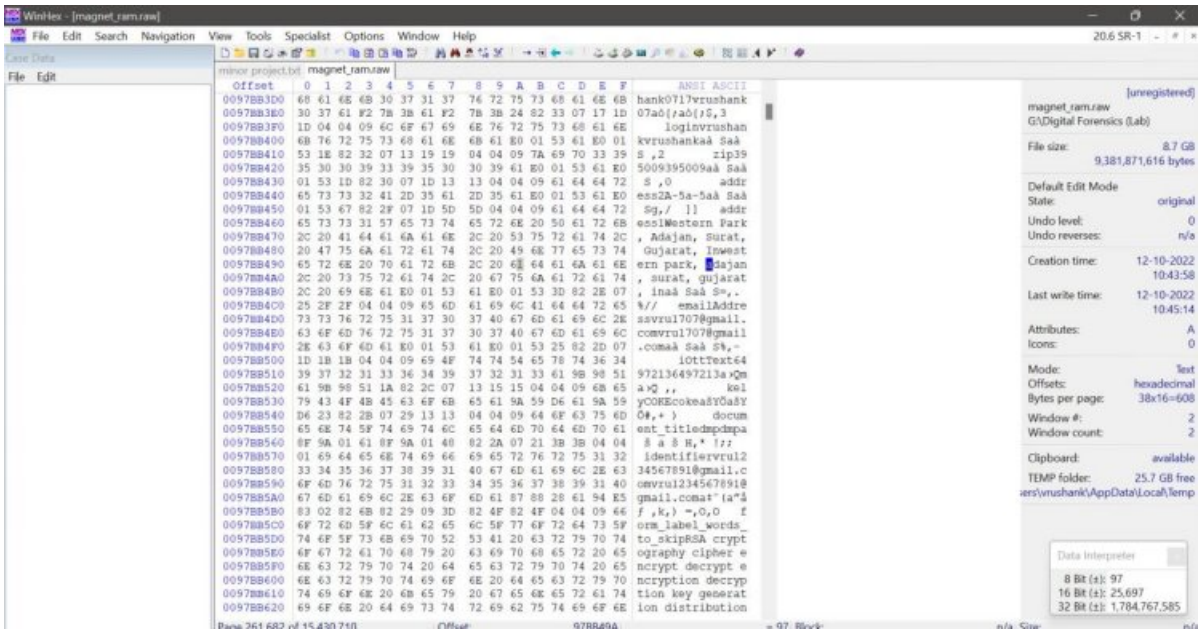


Figure 4: Analysis - Address in WinHEX

ii. Name:

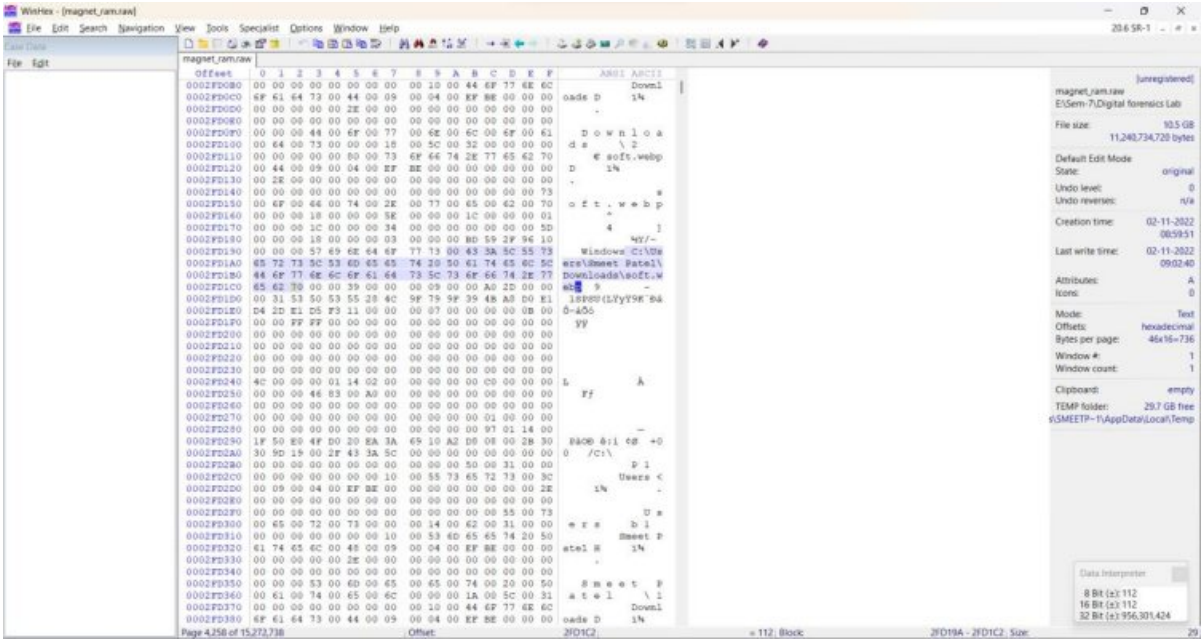


Figure 5: Analysis - Name in WinHEX

iii. Phone number:

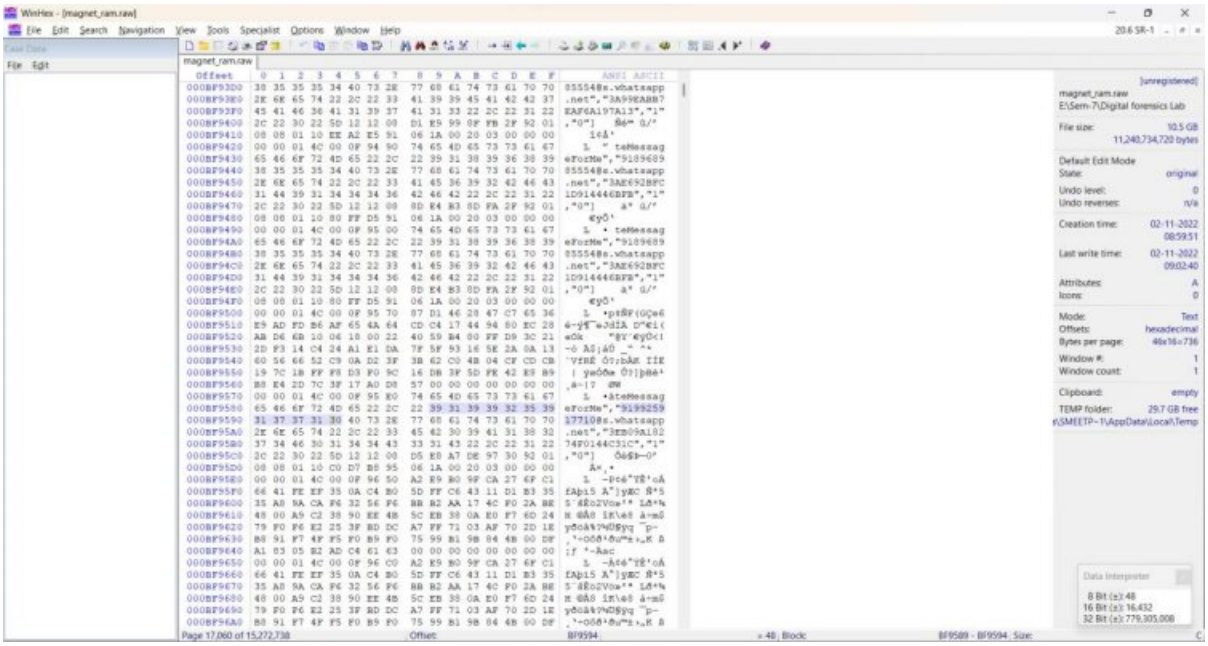


Figure 6: Analysis - Phone Number in WinHEX

iv. Email address:

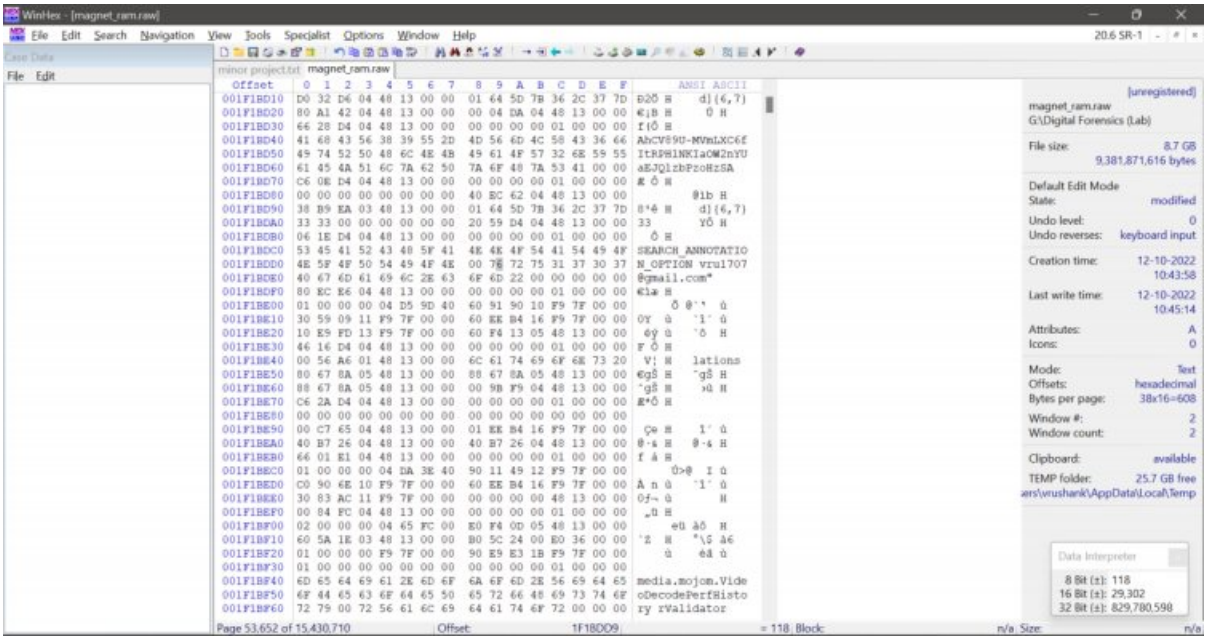


Figure 7: Analysis - Email Address in WinHEX

v. Https search:

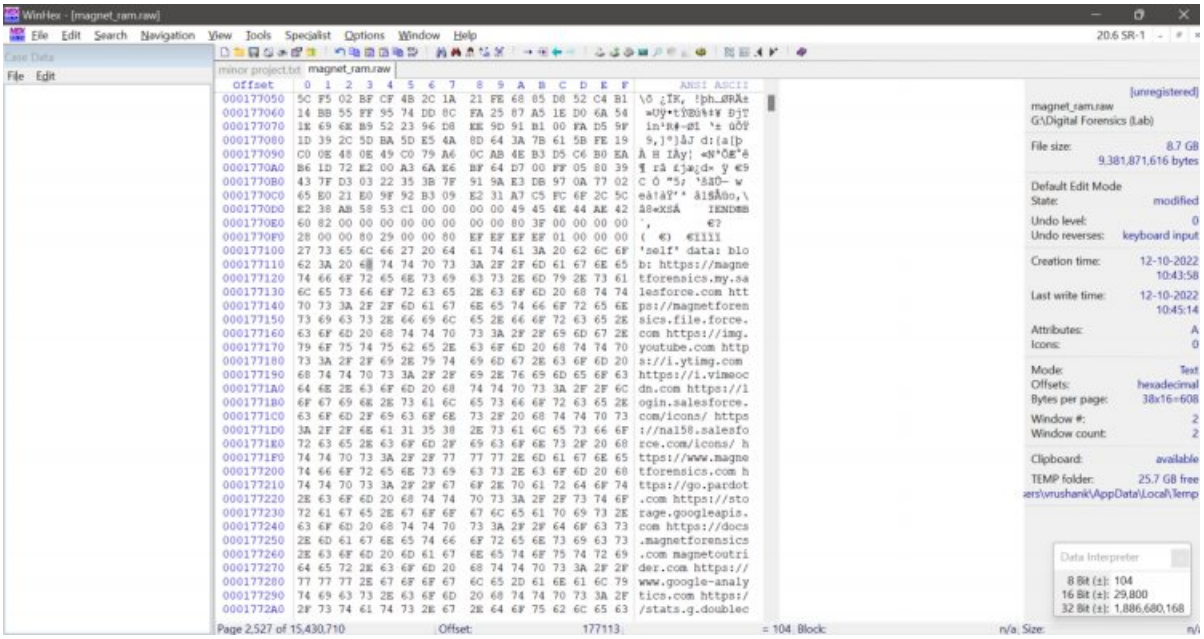


Figure 8: Analysis - HTTP Search in WinHEX

vi. Social Media:

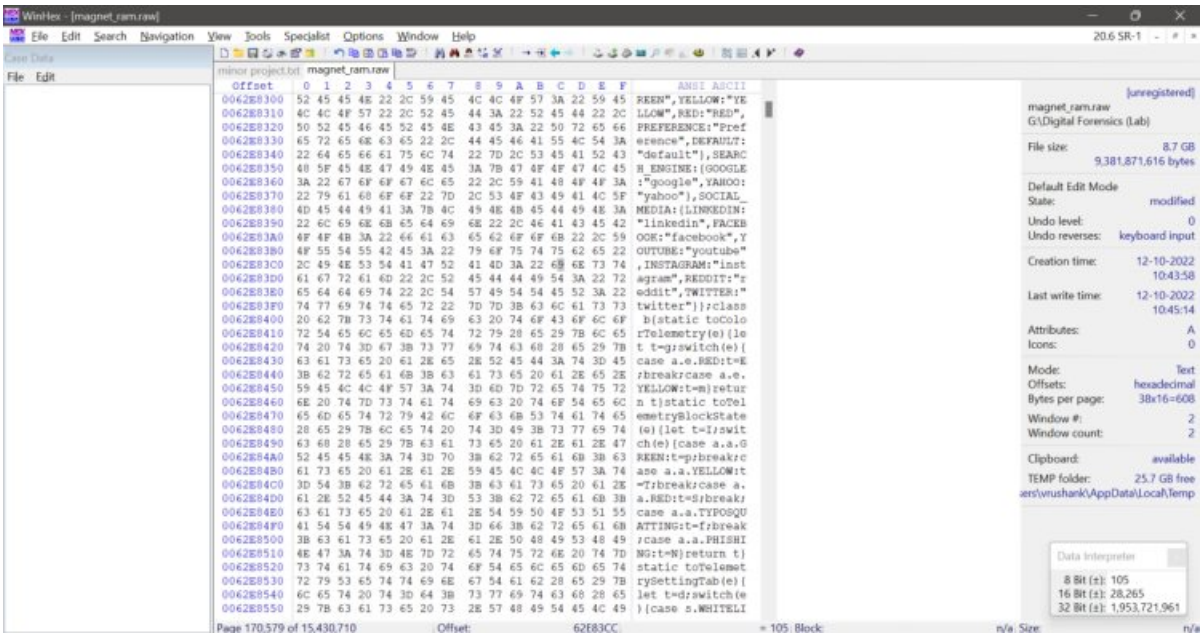


Figure 9: Analysis - Social Media in WinHEX

Task 2: Exploring HashMyFiles Tool

Steps:

Step 1 → Visit https://hashmyfiles.soft112.com/modal-download.html and Download HashMyFiles.

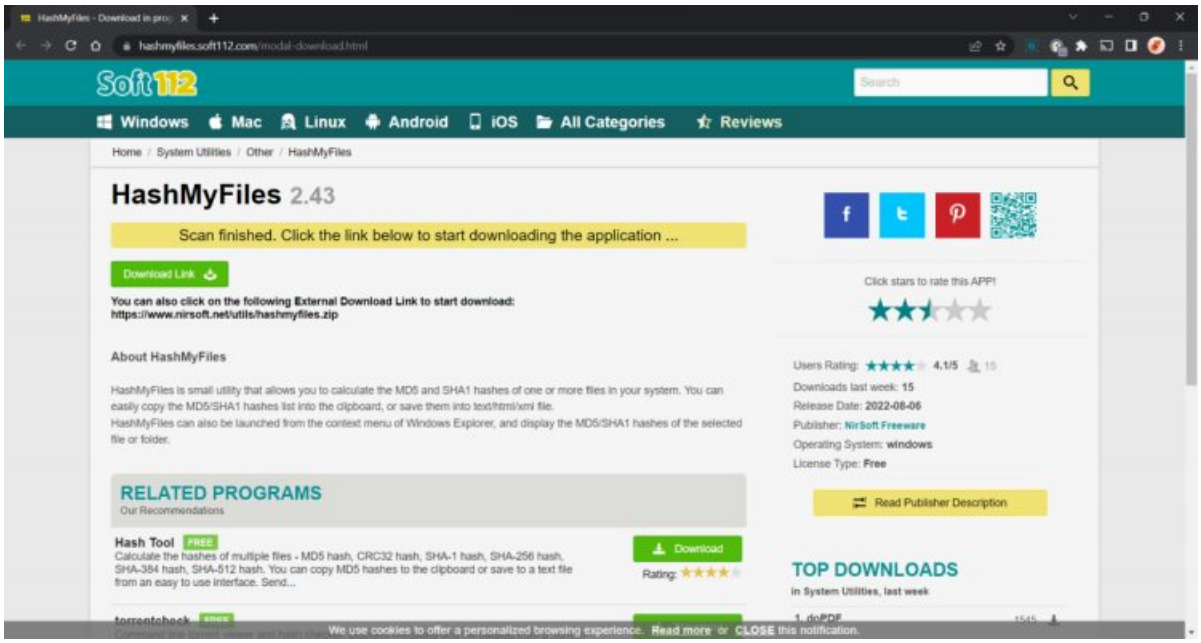


Figure 10: Website to download HashMyFiles Tool

Step 2 → Open the Application and open any file.

Analysis:

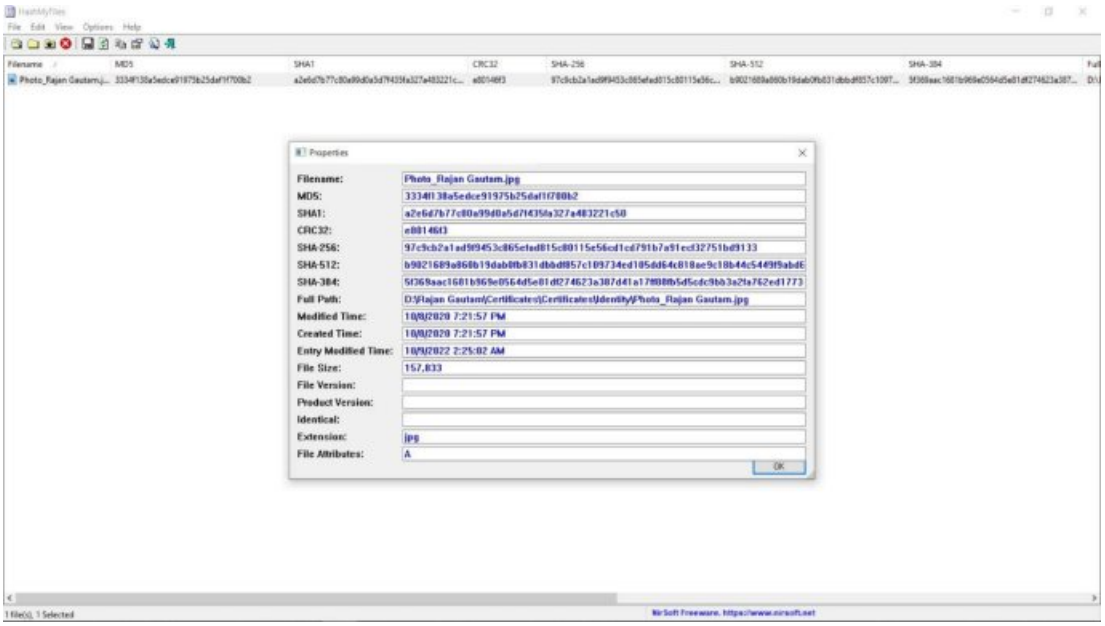


Figure 11: Analyzing File in HashMyFiles Tool

Task 3: Exploring Gary Kessler's File Signature Table Tool

Steps:

Step 1 → Access Garykessler from this URL https://www.garykessler.net/library/file_sigs.html.

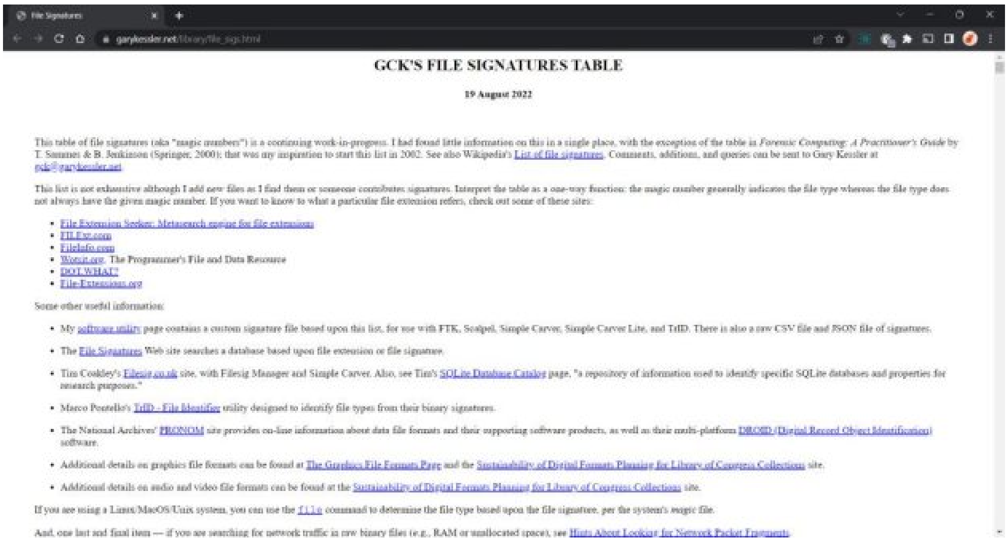


Figure 12: Website to access Gary Kessler's File Signature Table Tool

Analysis:

→ Check Hex Value for .JPG file in GCK's file. As per the Hex value for JPG image is 'FF D8 FF E1 xx xx 45 78'.

Figure 13: Checking Hex Value for .JPG file in GCK's File

→ Open the same file using WinHEX. We can see the same HEX value in the editor which shows the file is .JPG file.

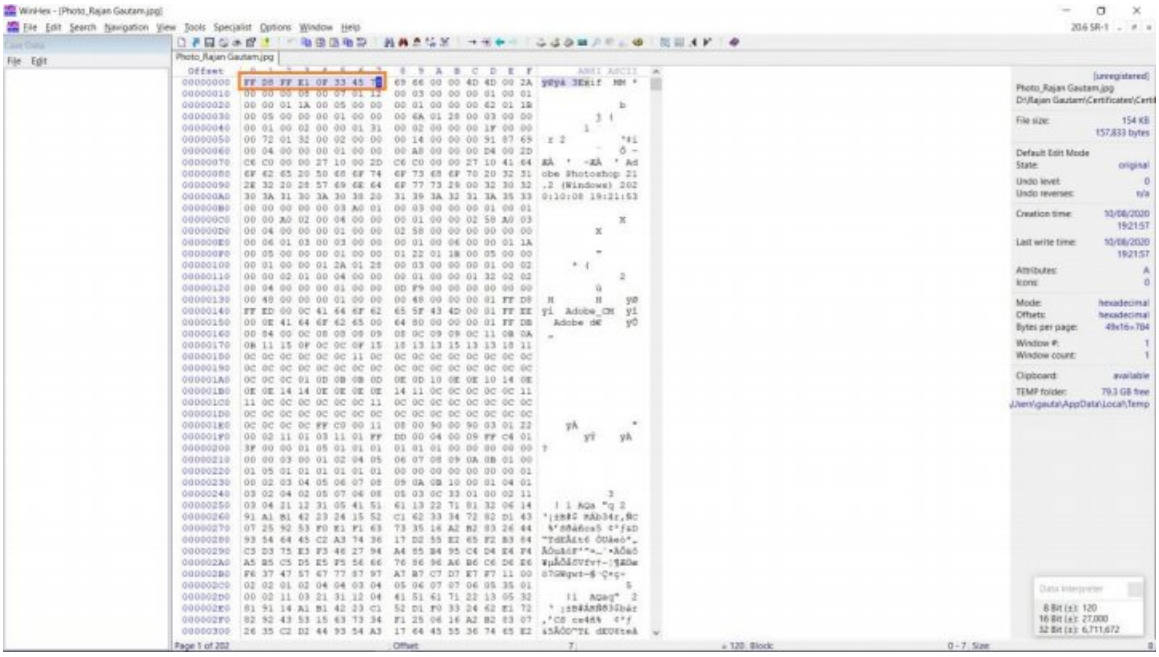


Figure 14: Checking Hex Value for .JPG file in WinHEX

→ The image was edited with Adobe photoshop, that also we can verify from the HEX Code.

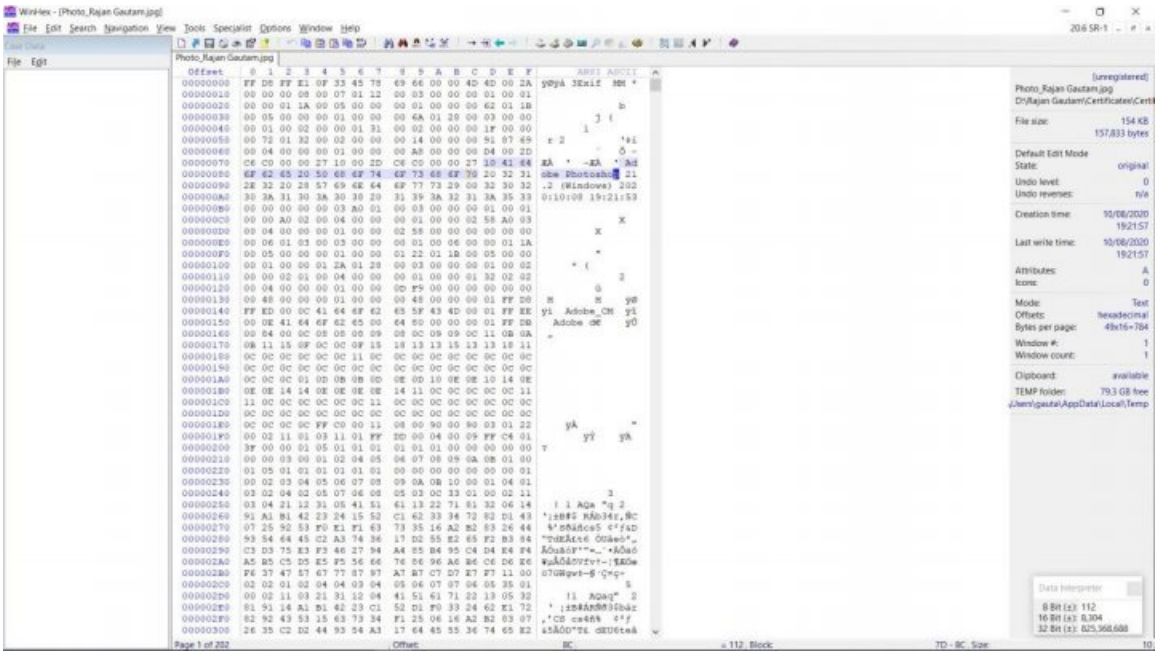
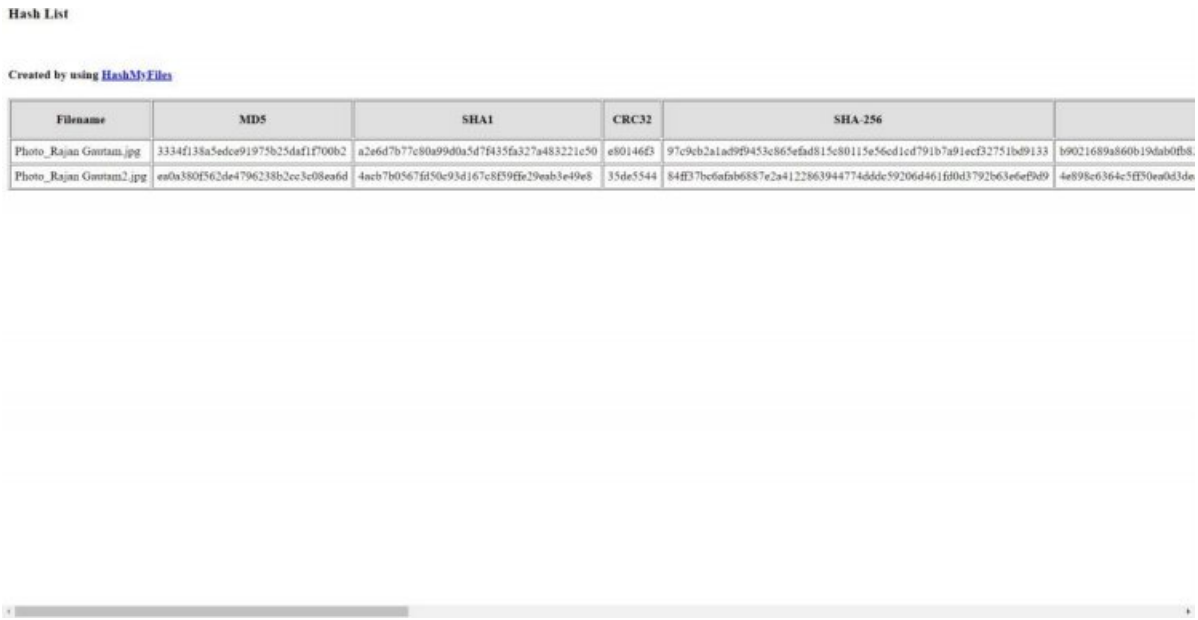


Figure 15: Verifying Image file from HEX code in WinHEX

→ When I updated the file using Paint and check the Hash value, I found the change in Hash Value also.



Hash List

Created by using HashMyFiles

Filename	MD5	SHA1	CRC32	SHA-256	
Photo_Rajan Gautam.jpg	3334f138a5edce91975b25daf1f700b2	a2e6d7b77c80a99d0a5d7f435fa327a483221c50	e80146f3	97c9cb2a1ad9f9453c865efad815c80115e56cd1cd791b7a91ecf32751bd9133	b9021689a860b19dab0fb8
Photo_Rajan Gautam2.jpg	ea0a380f562de4796238b2ec3c08ea6d	4acb7b0567fd50c93d167c8f59ffe29eab3e49e8	35de5544	84ff37bc6afab6887e2a4122863944774dddc59206d461fd0d3792b63e6ef9d9	4e898e6364c5ff50ea0d3de

Figure 16: Changed in Hash Value in updated file

Overall Analysis:

The three tools (WinHEX, HashMyFiles, and Gary Kessler's File Signature Table) all appear to be useful for hash and hex analysis. However, each has its own strengths and weaknesses.

Conclusion:

The integrity of files can be checked using HEX Code analysis.

By doing the HEX Code analysis, WinHEX is a powerful hex editor that allows users to view, modify, and analyze hexadecimal data in files, disks, and memory locations. It can be used for a variety of purposes, including digital forensics. HashMyFiles is a utility that allows users to calculate the hashes of files, which can be used to verify the integrity of those files. Gary Kessler's File Signature Table is a resource that can be used to identify the file formats of unknown files. All three of these tools can be useful in digital forensics.

Digital Forensics Lab Report: 10

Date: 20-10-2022

Name:	**Mire Patel**
Roll No:	19BCP080
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of a Data Acquisition tools.

Tool Names: FTK Imager, Autopsy.

Tasks: Perform Data Acquisition using FTK Imager and Autopsy.

Introduction:

The purpose of a data acquisition is to allow for the easy collection and analysis of data. This can be done through a variety of means, but the most common is through the use of computers. Data acquisition systems can be used to collect data from a variety of sources, including sensors, instruments, and other devices. Once the data is collected, it can be stored, analyzed, and displayed in a variety of ways.

- **FTK Imager tool:** FTK Imager is a forensic toolkit used by law enforcement and private investigators to recover data from computers and mobile devices. The toolkit includes a wide range of features, including a powerful file recovery engine, advanced search capabilities, and support for a variety of file formats. FTK Imager is available in both a free and paid version.

- **Autopsy tool:** An autopsy is a digital forensics tool used for investigating disk images and analyzing the data they contain. It can be used to examine the contents of a disk image, such as a disk that has been acquired during an investigation, in order to determine what data is present and how it is organized. Autopsy can also be used to examine live systems, such as systems that are currently being used by an organization.

Task: Performing Data Acquisition using FTK Imager and Autopsy

Steps:

Step 1 → Download and Install FTK Imager

- Visit https://accessdata.com/product-download/ftk-imager-version-4-5 and download FTK IMAGER from there.

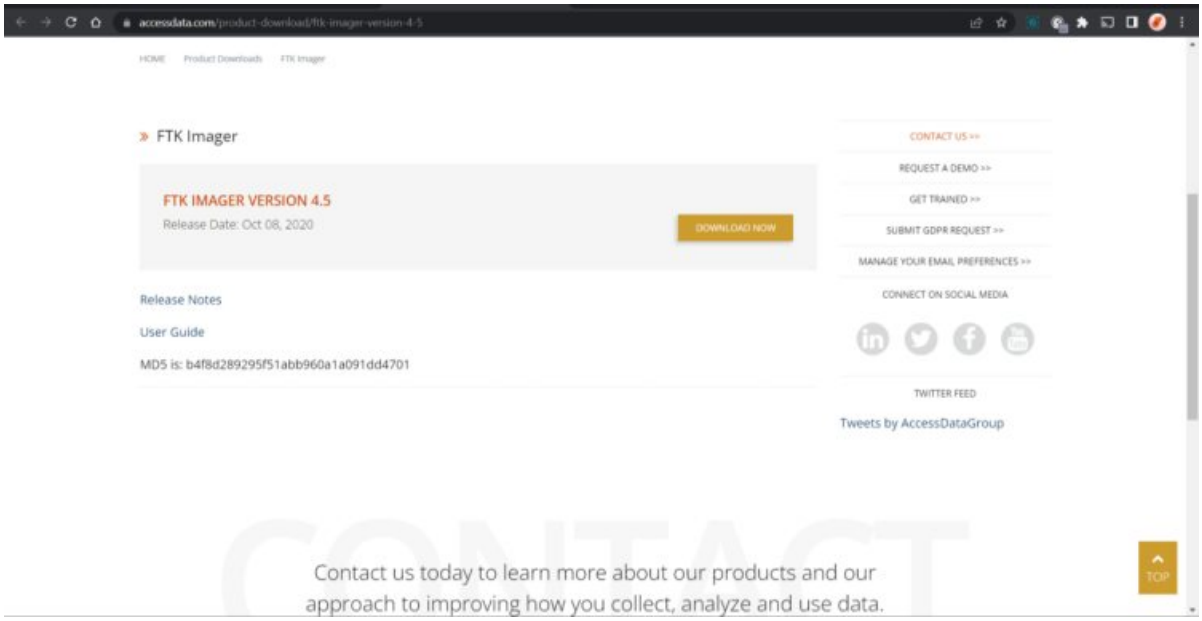


Figure 1: Website to Download FTK IMAGER Tool

- Now, Install FTK Imager on your system.

Figure 2: FTK Imager Tool Installation Process – 1/5

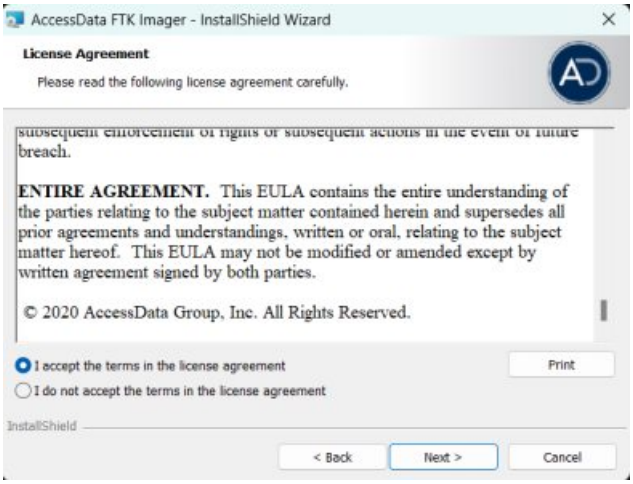


Figure 3: FTK Imager Tool Installation Process – 2/5

Figure 4: FTK Imager Tool Installation Process – 3/5

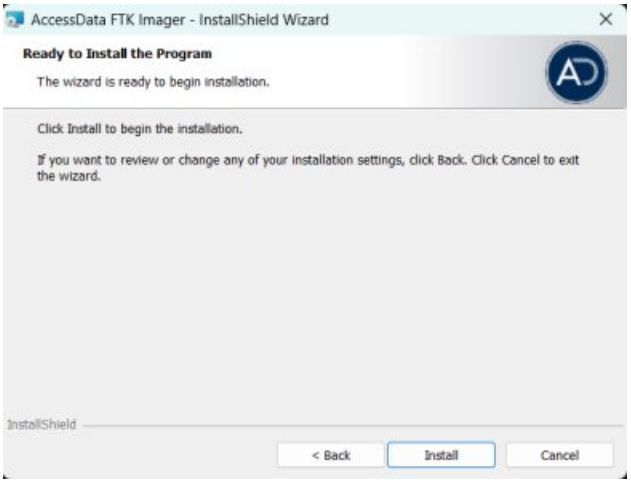


Figure 5: FTK Imager Tool Installation Process – 4/5

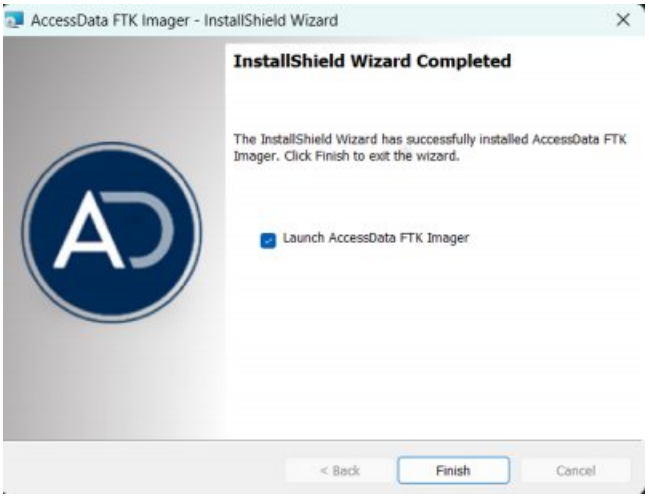


Figure 6: FTK Imager Tool Installation Process – 5/5

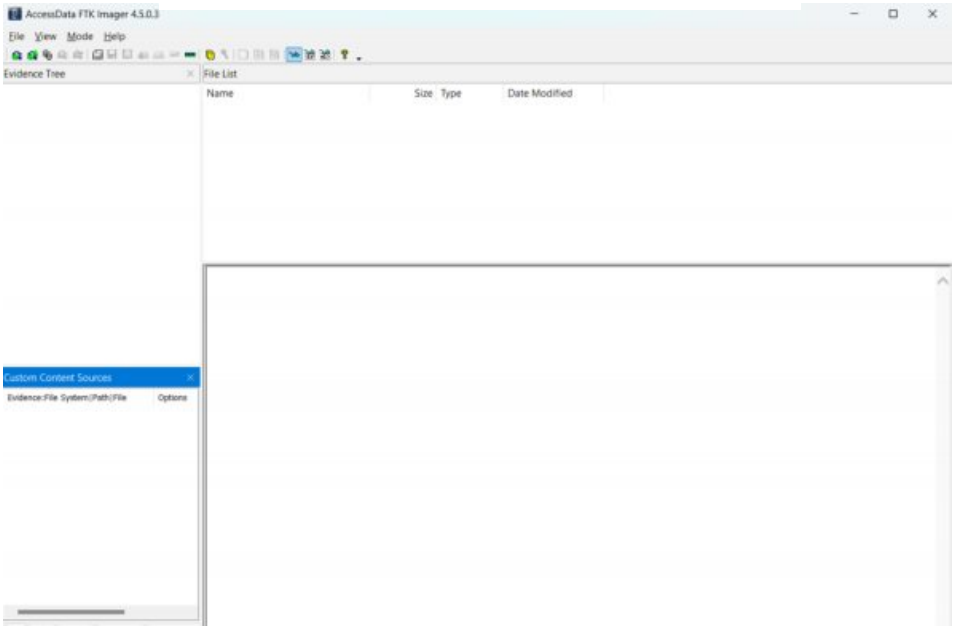


Figure 7: FTK Imager Tool Window

Step 2 → Download and Install Autopsy

- Visit https://www.autopsy.com/download/ and download AUTOPSY from there.

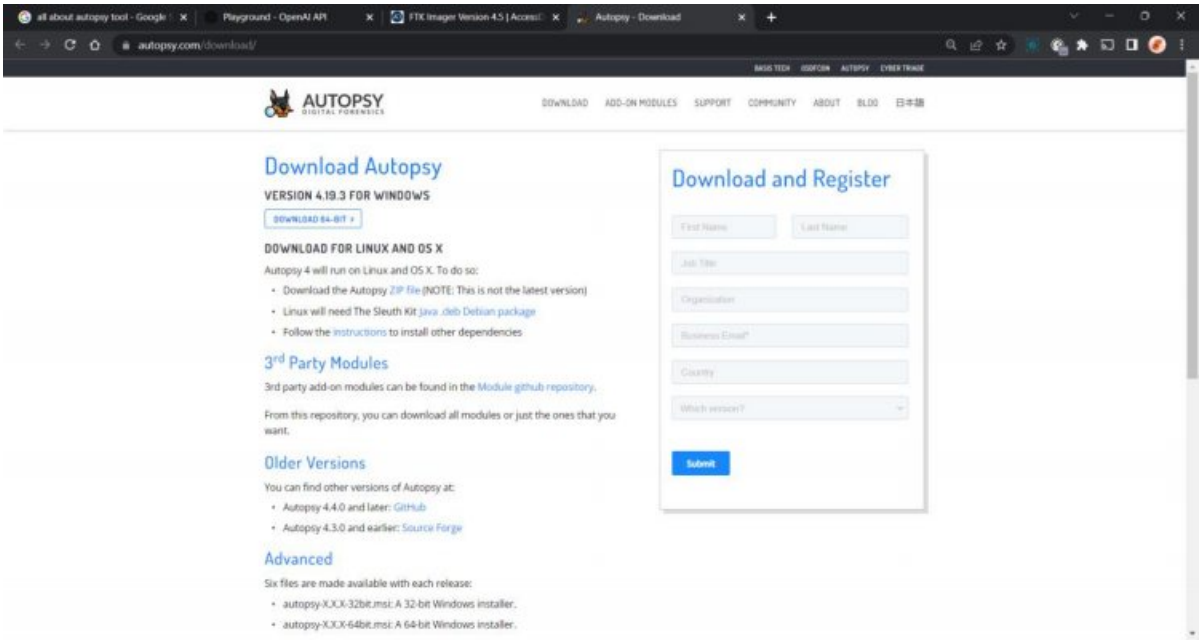


Figure 8: Website to Download AUTOPSY Tool

- Now, Install Autopsy on your system.

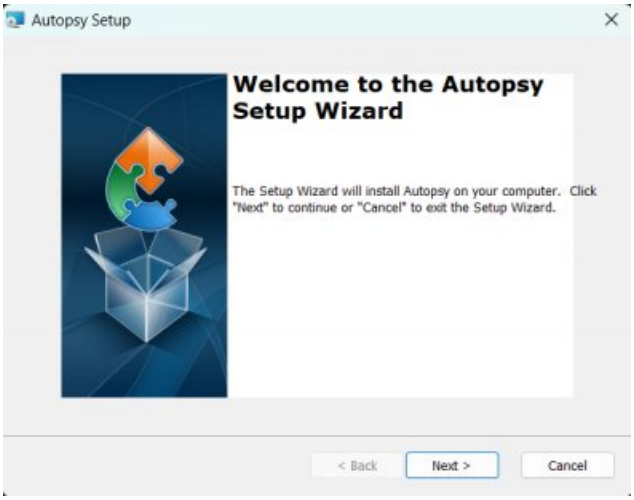


Figure 9: AUTOPSY Tool Installation Process – 1/6

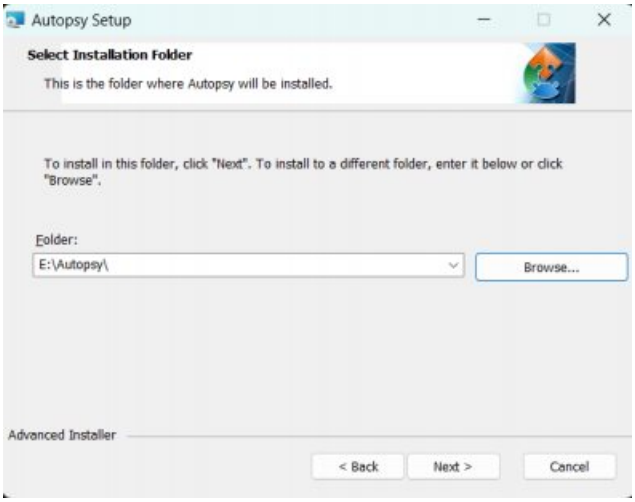


Figure 10: AUTOPSY Tool Installation Process – 2/6

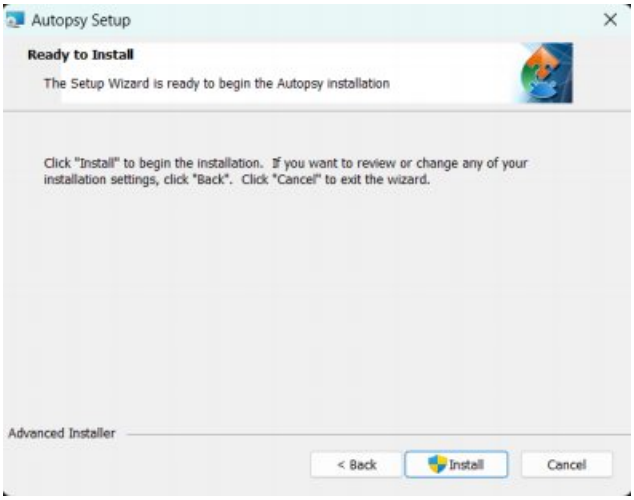


Figure 11: AUTOPSY Tool Installation Process – 3/6

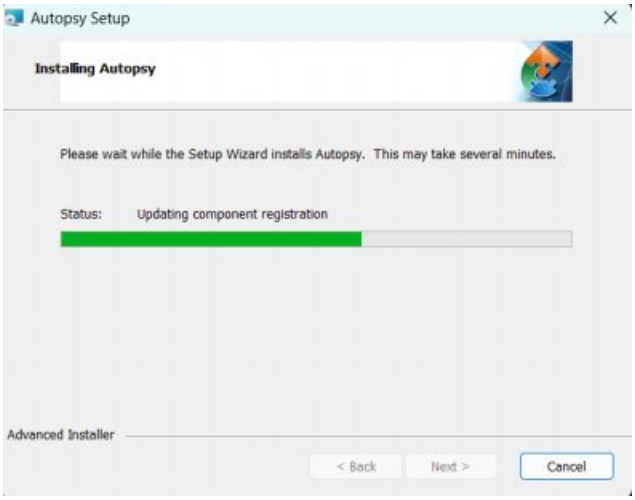


Figure 12: AUTOPSY Tool Installation Process – 4/6

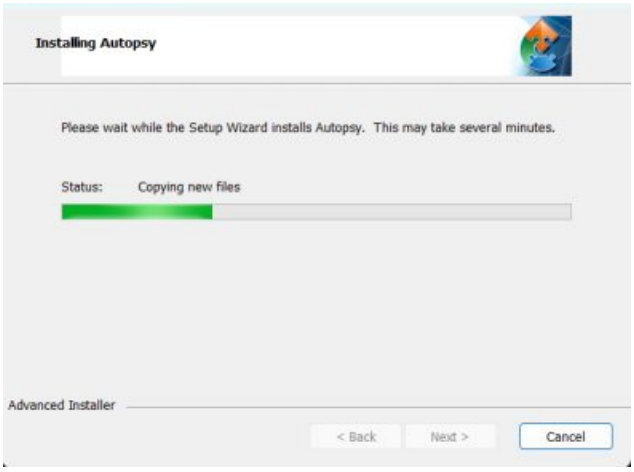


Figure 13: AUTOPSY Tool Installation Process – 5/6

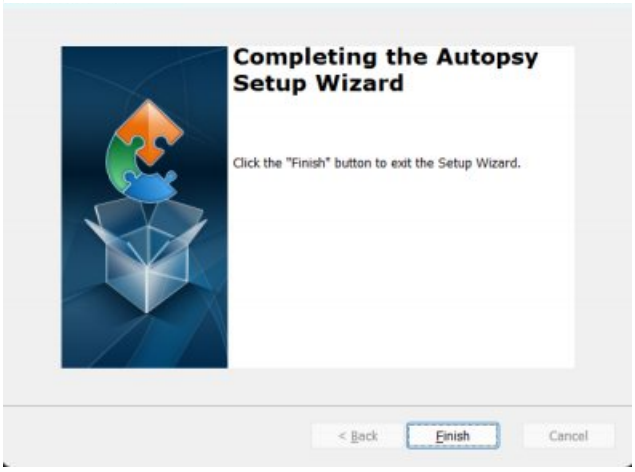


Figure 14: AUTOPSY Tool Installation Process – 6/6

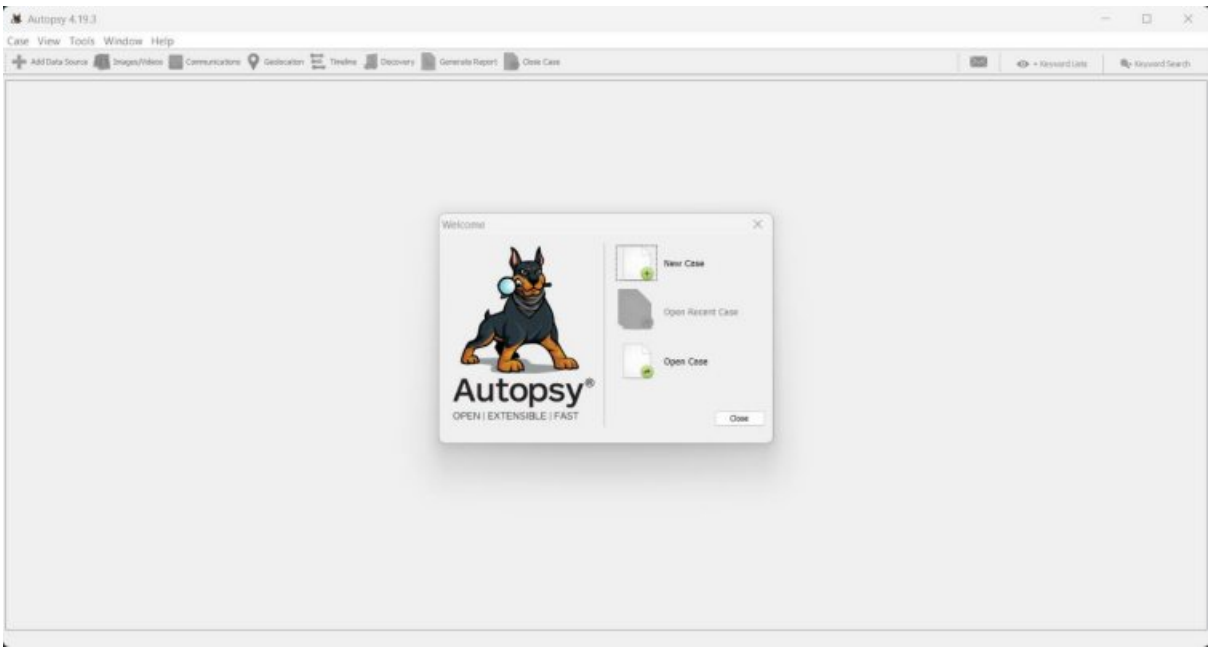


Figure 15: AUTOPSY Tool Window

Step 3 → Create an Image of a Drive

- Open FTK Imager and go to ‘File’ tab and click on “Create Disk Image”.

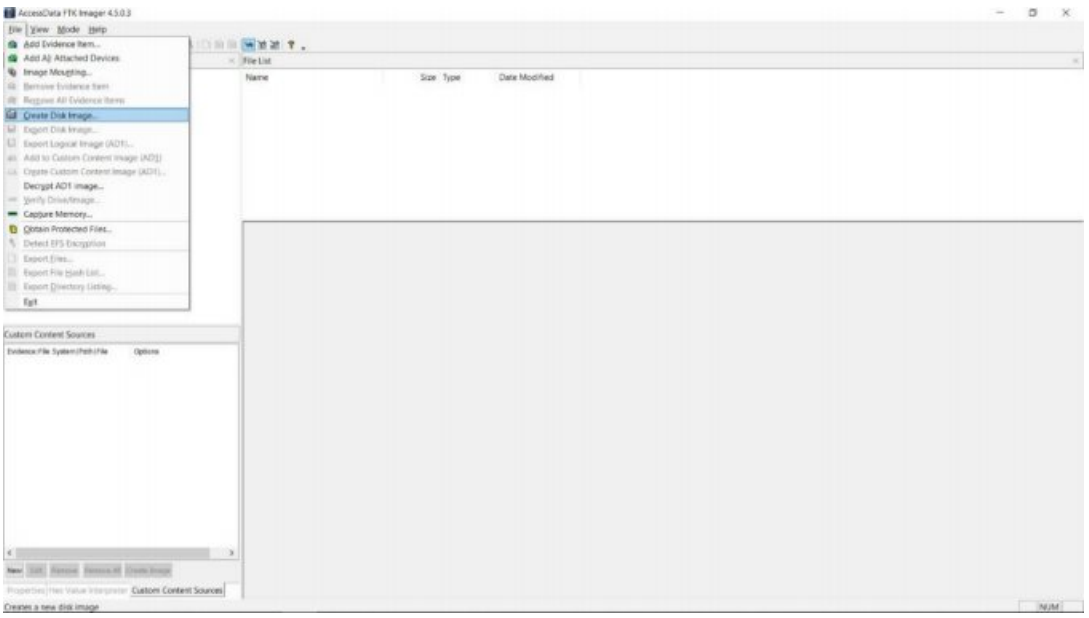


Figure 16: Creating Disk Image in FTK Imager

- Select ‘Image File’ and on the next window, select image path and click on “Finish”.

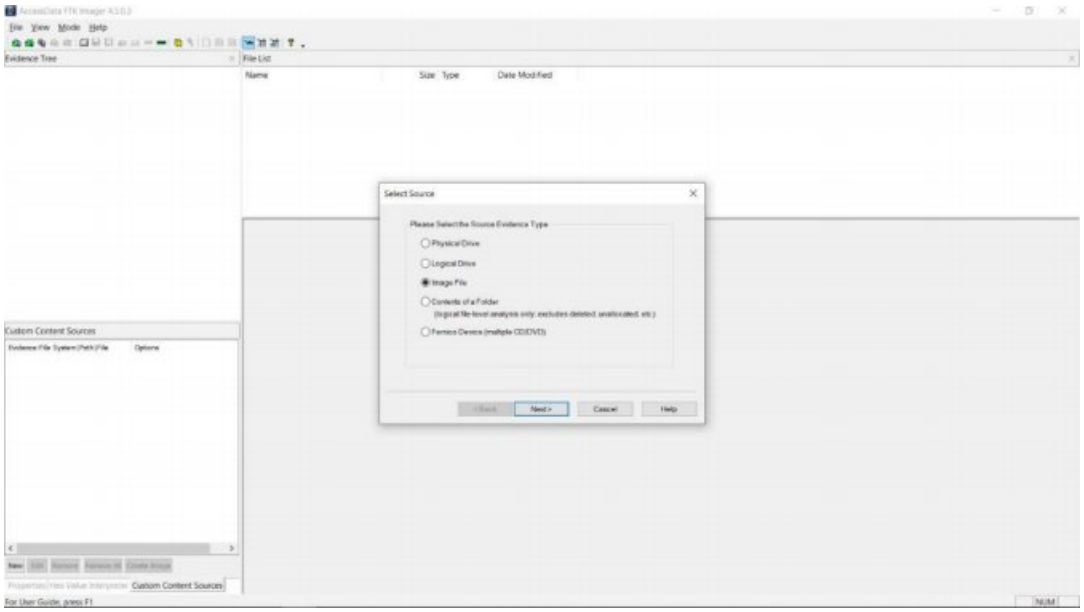


Figure 17: Selecting Image File in FTK Imager

- Select File Type as ‘E01’ and put the evidence details accordingly.

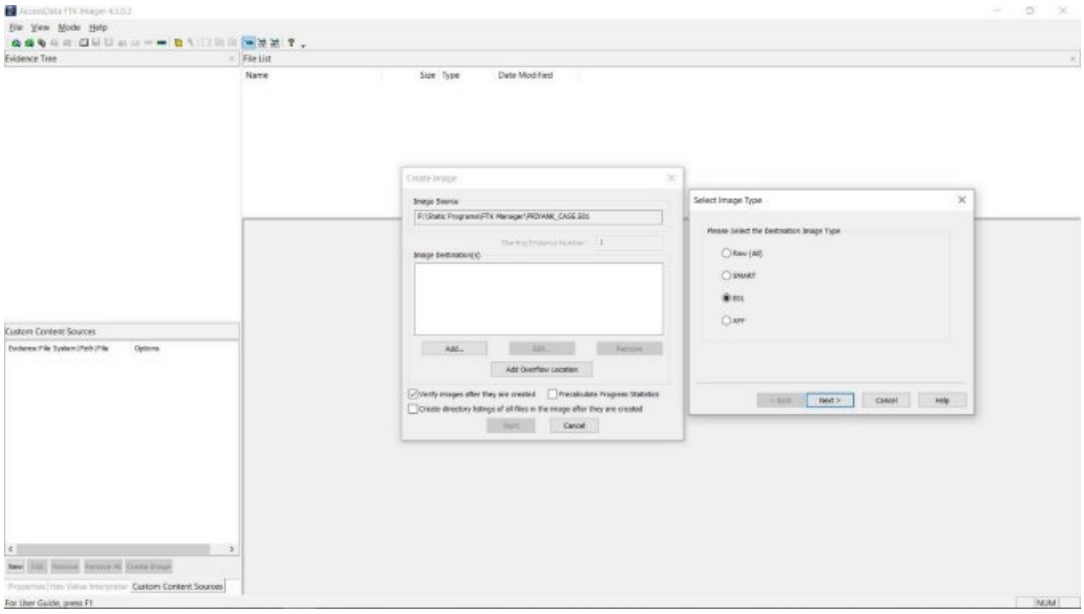


Figure 18: Selecting File Type in FTK Imager

- Wait until the image file is created.

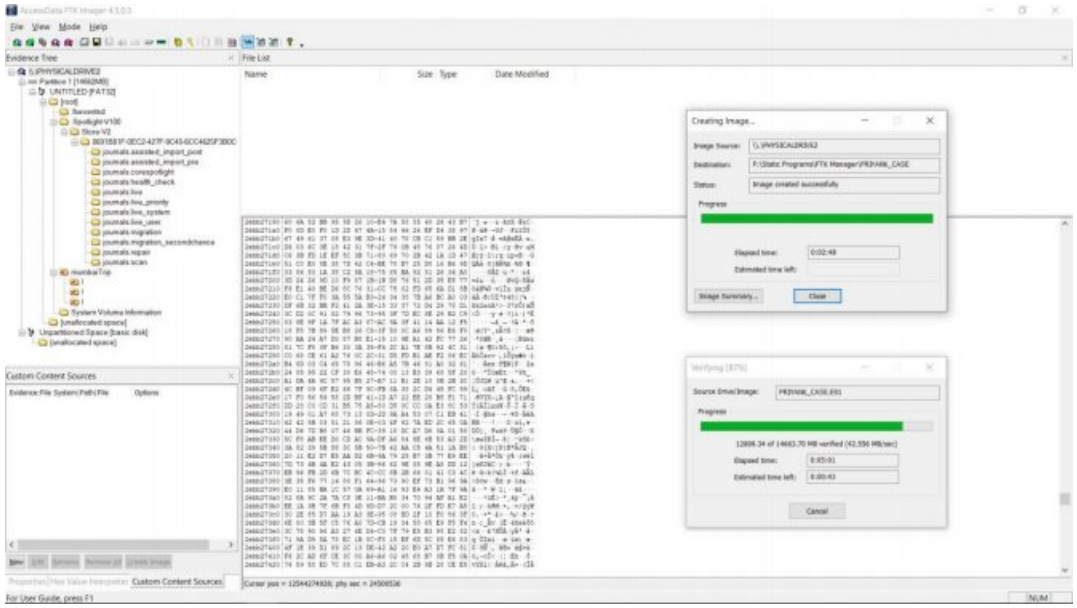


Figure 19: Process to create Image File in FTK Imager – 1/2

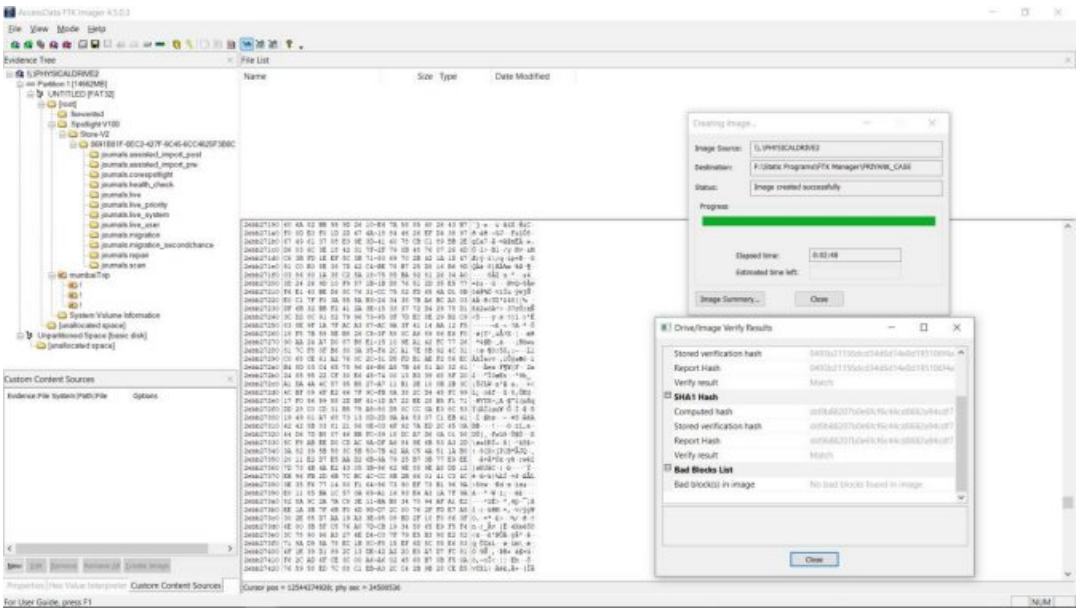


Figure 20: Process to create Image File in FTK Imager – 2/2

- Once the Image is created, open Autopsy.

Step 4 → **Open Autopsy and start working on it.**

- Open Autopsy and click on “New Case”.

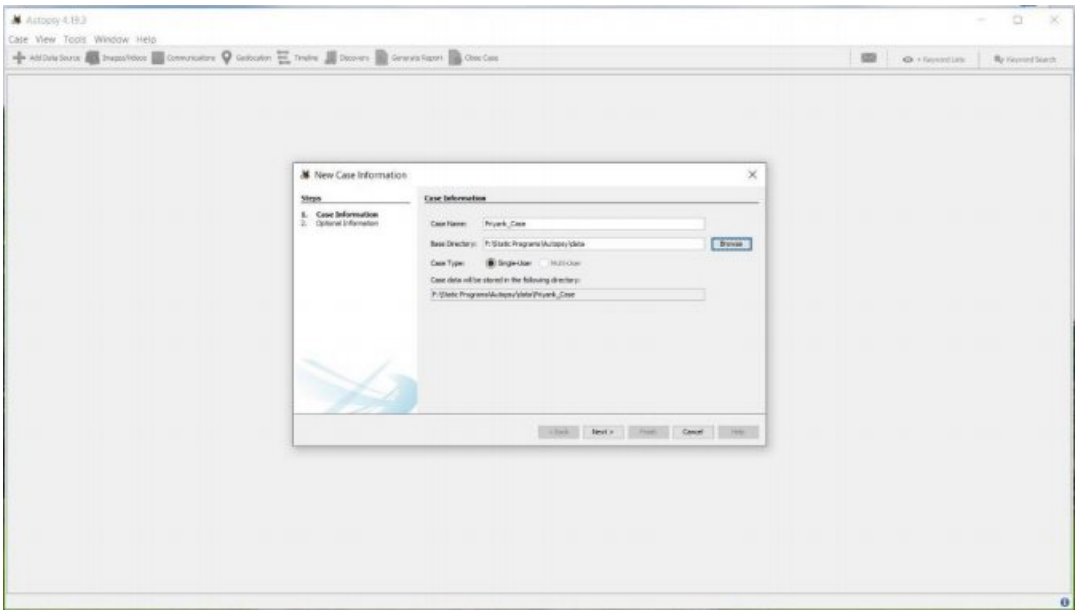


Figure 21: Creating New Case in Autopsy

- Fill out Case Information and Optional Information.

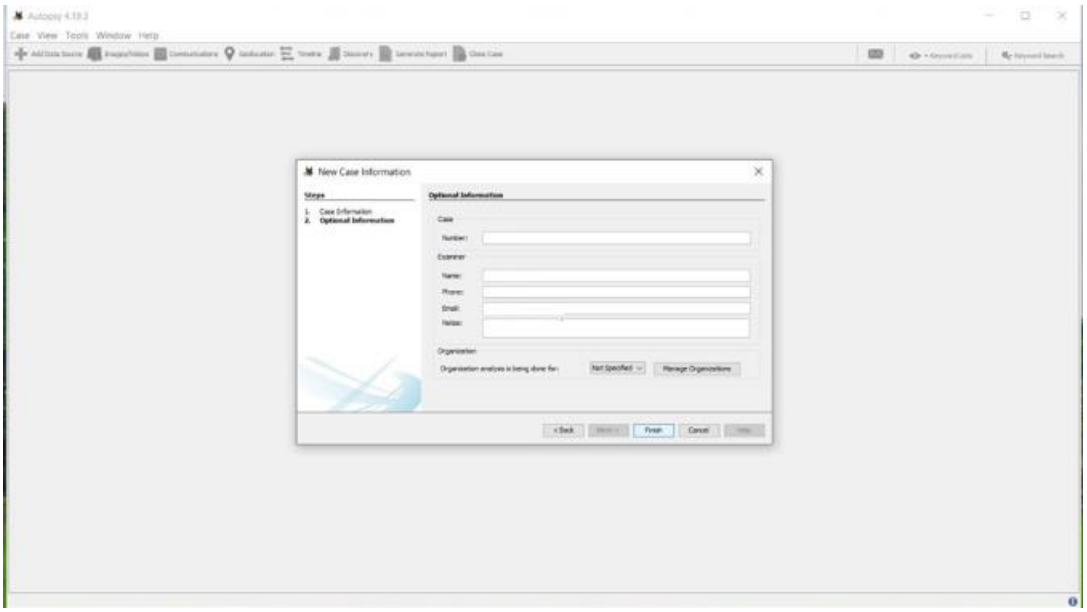


Figure 22: Filling out required details for Case Information in Autopsy

- Once a case is created, add an image file for analysis.

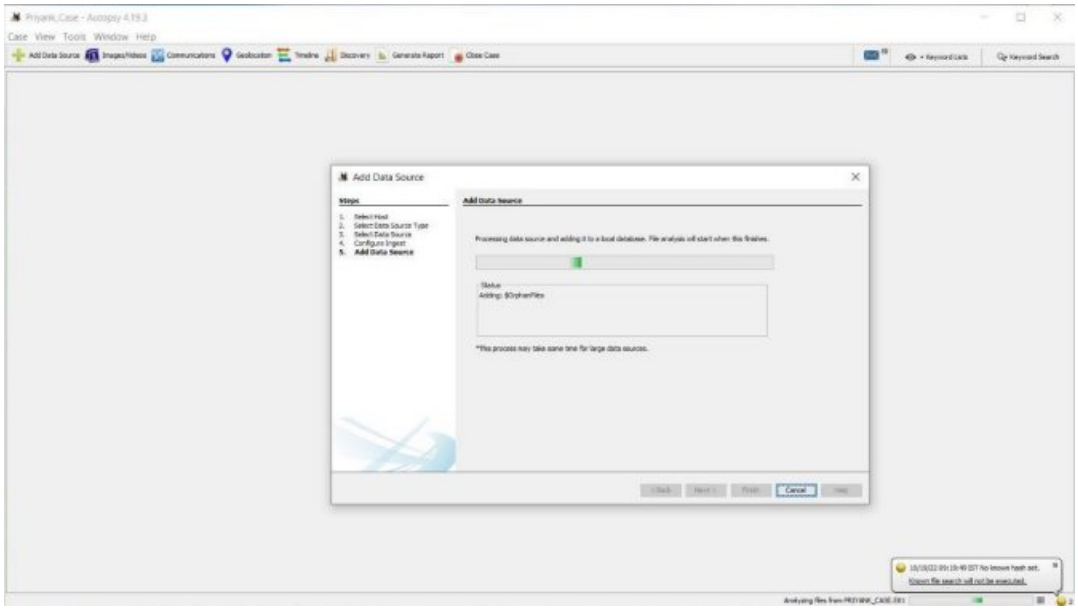


Figure 23: Adding Data Sources in Autopsy

- You can view the file contents on the screen.

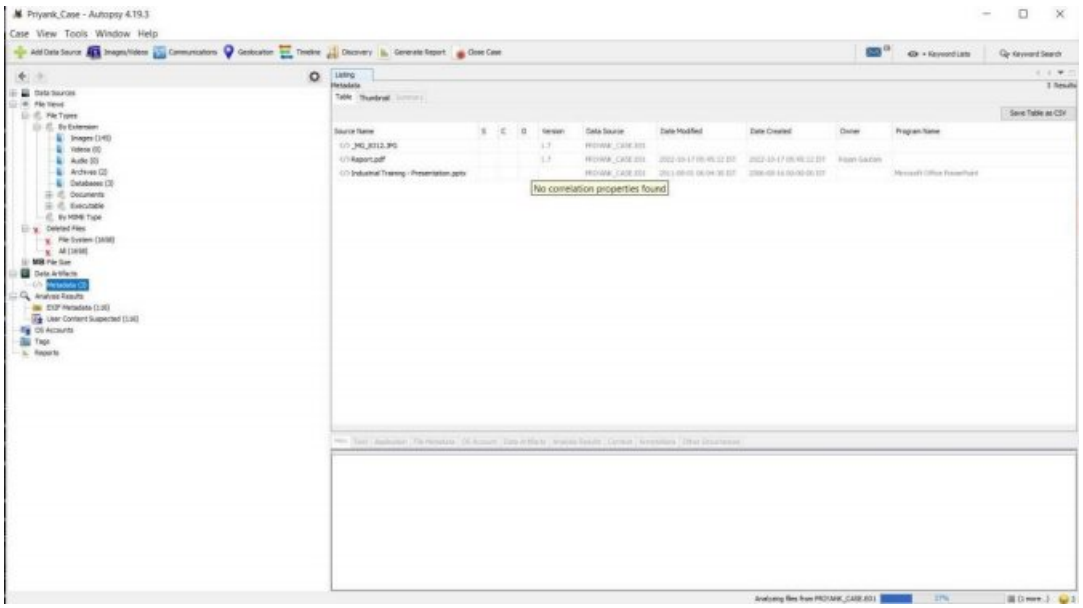


Figure 24: File Contents in Autopsy – 1/2

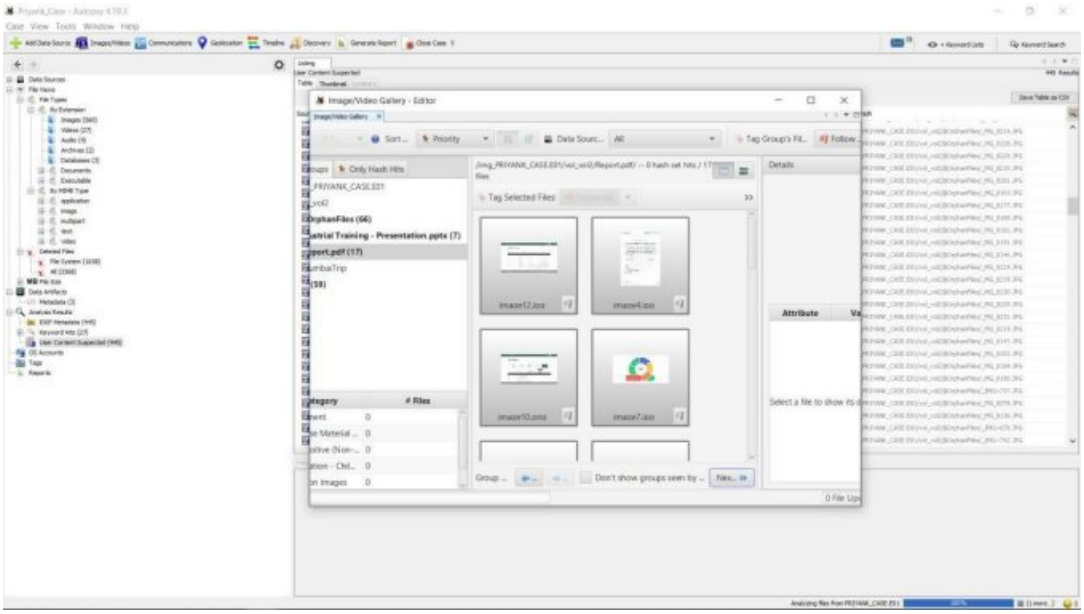


Figure 25: File Contents in Autopsy – 2/2

- Click on Generate Report to generate Analysis Report.

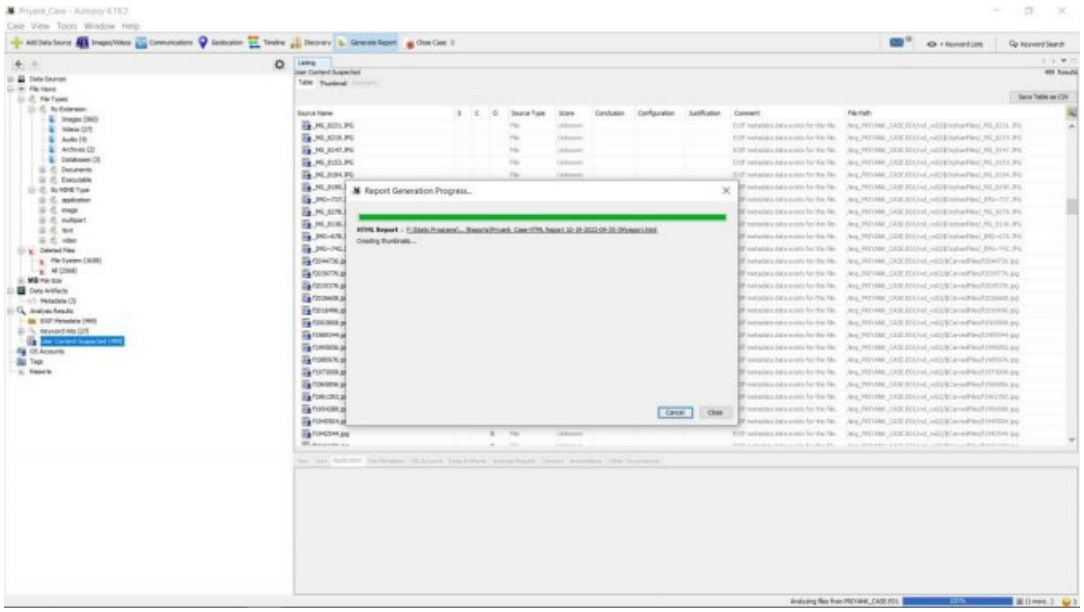


Figure 26: Generating Analysis Report in Autopsy

- You can view the report in the web browser.

Figure 27: Analysis Report – 1/2

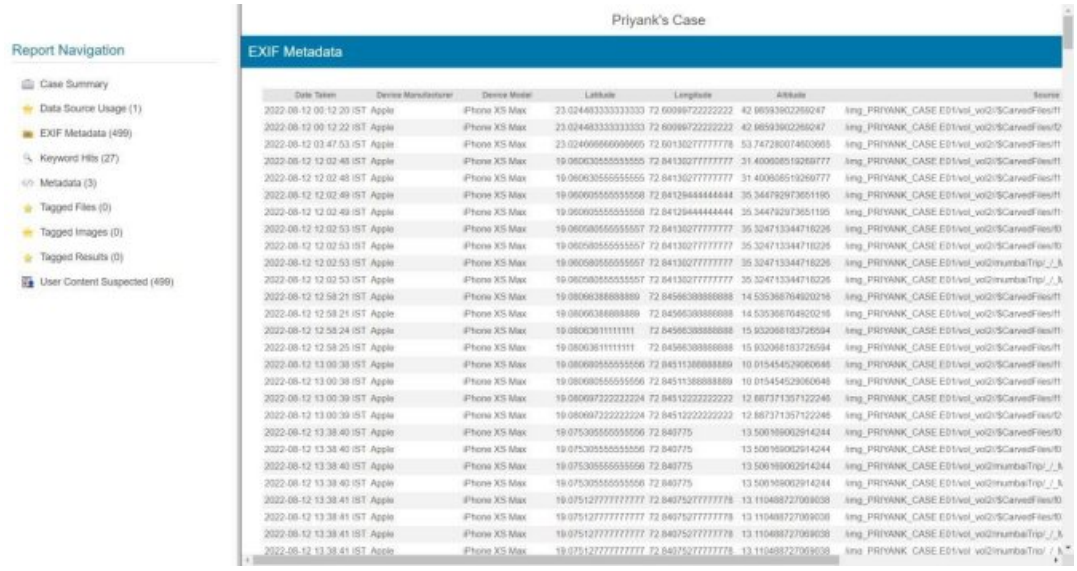


Figure 28: Analysis Report - 2/2

Analysis:

The FTK Imager and Autopsy tool were able to successfully acquire data from the computer's hard drive. The data was then sorted and organized into a format that is easy to read and understand. The data acquisition process was quick and efficient, and the results were accurate. Overall, the FTK Imager and Autopsy tool are an excellent choice for data acquisition.

Conclusion:

The FTK Imager is a reliable and easy-to-use data acquisition tool that can be used to obtain forensically sound images of computers. The Autopsy tool is a powerful open-source digital forensics platform that can be used to examine the images obtained with the FTK Imager.

FTK Imager is a data acquisition tool that can be used to image a hard drive or other data storage device. The Imager can be used to create an image of the entire drive, or just a portion of the drive. The Imager can also be used to create an image of a specific file or folder.

Autopsy tool is a data analysis tool that can be used to examine the contents of a hard drive or other data storage device. Autopsy can be used to examine the contents of an entire drive, or just a portion of the drive. Autopsy can also be used to examine the contents of a specific file or folder.