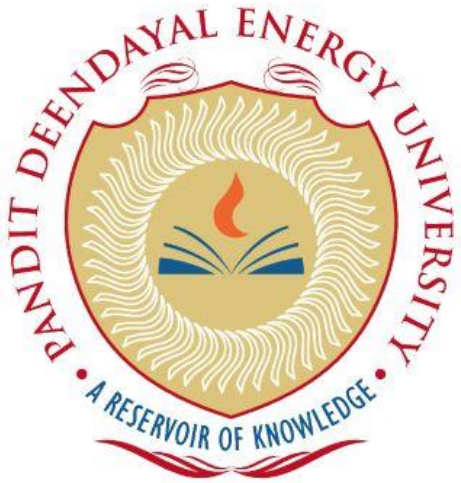
PANDIT DEENDAYAL ENERGY UNIVERSITY

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:

PATEL PARTH N

19BCP091

G3- CE19

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.

PATRL PARTH N

19BCP091

Certificate

This is to certify that the Practical lab report of the course entitled "**Digital Forensics (20CP411P)**" has been satisfactorily completed and submitted by PATEL PARTH N. Roll No. 19BCP091 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.	27-07-2022	
2	Studyof a Profile Generation using OSINT Techniques.	03-08-2022	
3	Study of a Identification of Morphed/Edited/Fabricated portion from given Video/Audio/Image files as investigation input.	17-08-2022	
4	Study of a Tracking & Tracing Fake Profile(s) & Fake News.	24-08-2022	
5	Study of a Deep and Darknet Monitoring Capabilities.	10-08-2022	
6	Study of a Data Recovery from Computer Systems, Mobile Devices, and other electronic peripherals.	07-09-2022	
7	Study of an Email Forensics tools.	14-09-2022	
8	Study of a Volatile Memory Forensics tools.	12-10-2022	
9	Study of a Hash and Hex analysis tools	26-10-2022	
10	Study of a Data Acquisition tools.	19-10-2022	

Digital Forensics Lab Report: 1

Date: 27-07-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Study of a Steganography tools.

Tool Names: -

- OpenPuff
- Spammimic
- QuickCrypto
- Pelock
- STEGONAUT

Links:

- Text Steganography:- spammimic - encode
- Images Steganography- Steganography Online Codec - Hide Message in Image (pelock.com)
- Audio Steganography :- STEGONAUT - Audio Steganography Tool
- Folder Steganography:-Download QuickCrypto - Free 15 Day Trial Period

Task 1: Perform Text Steganography using Spammimic

- **Website link :-** spammimic - encode
    - Spam Mimic is a popular steganography tool that allows users to hide information inside spam messages.
    - Spam Mimic works by using a context free probabilistic grammar to derive its output. Each production of the grammar is translated into a Huffman tree based on the probabilities assigned to each variable or terminal symbol in the production.

- **Original Text :-** I am here
- **Password:-** ***(123)
- **Decode Text :-**

Dear Friend ; This letter was specially selected to
be sent to you . If you no longer wish to receive our
publications simply reply with a Subject: of "REMOVE"
and you will immediately be removed from our mailing
list ! This mail is being sent in compliance with Senate
bill 2416 , Title 5 , Section 309 . This is not multi-level
marketing . Why work for somebody else when you can
become rich in 57 WEEKS . Have you ever noticed most
everyone has a cellphone & most everyone has a cellphone
. Well, now is your chance to capitalize on this !
We will help you increase customer response by 150%
and SELL MORE . You are guaranteed to succeed because
we take all the risk ! But don't believe us ! Mr Ames
of Washington tried us and says "Now I'm rich, Rich,
RICH" . This offer is 100% legal . Because the Internet
operates on "Internet time" you must hurry ! Sign up
a friend and you get half off . God Bless

Figure 1 Encrypted text of message

Steps:

1. Go to spammimic website. And select type of encoding

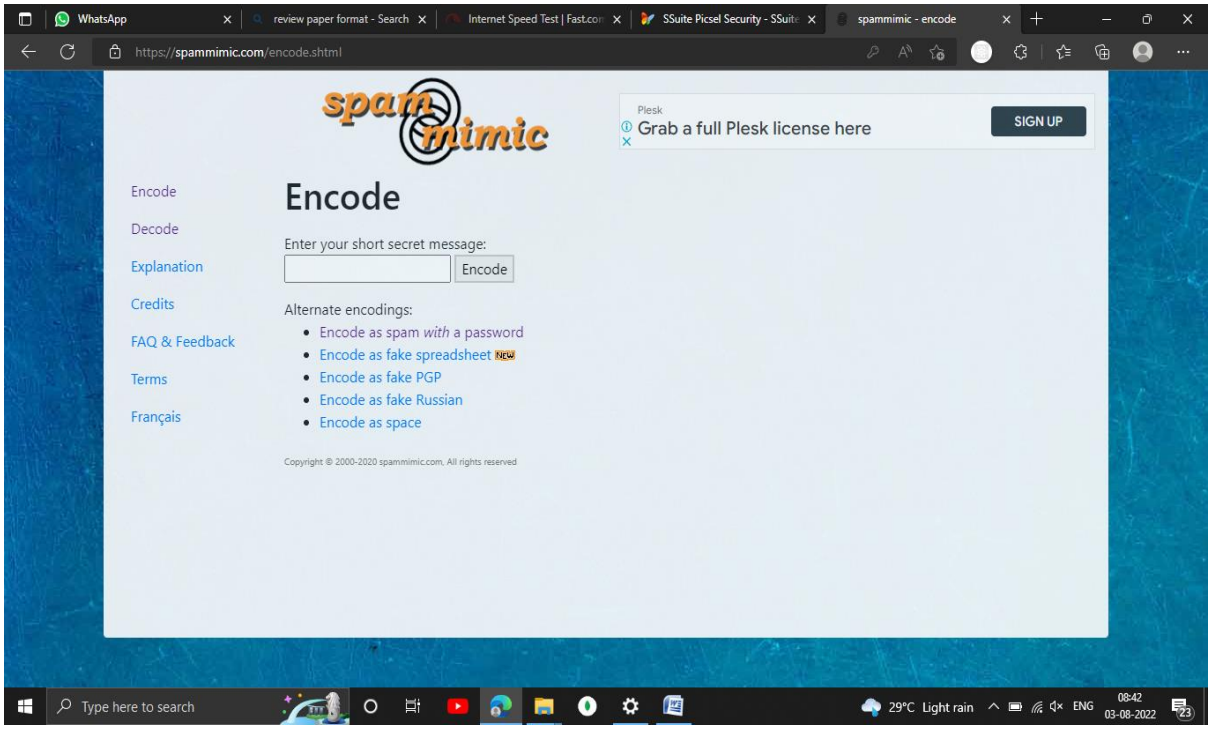


Figure 2 Text Steganography tool:- span mimic

2. Write the message you want to encode

Figure 3 Text Steganography tool:- span mimic

3. Press button and you will see encode message

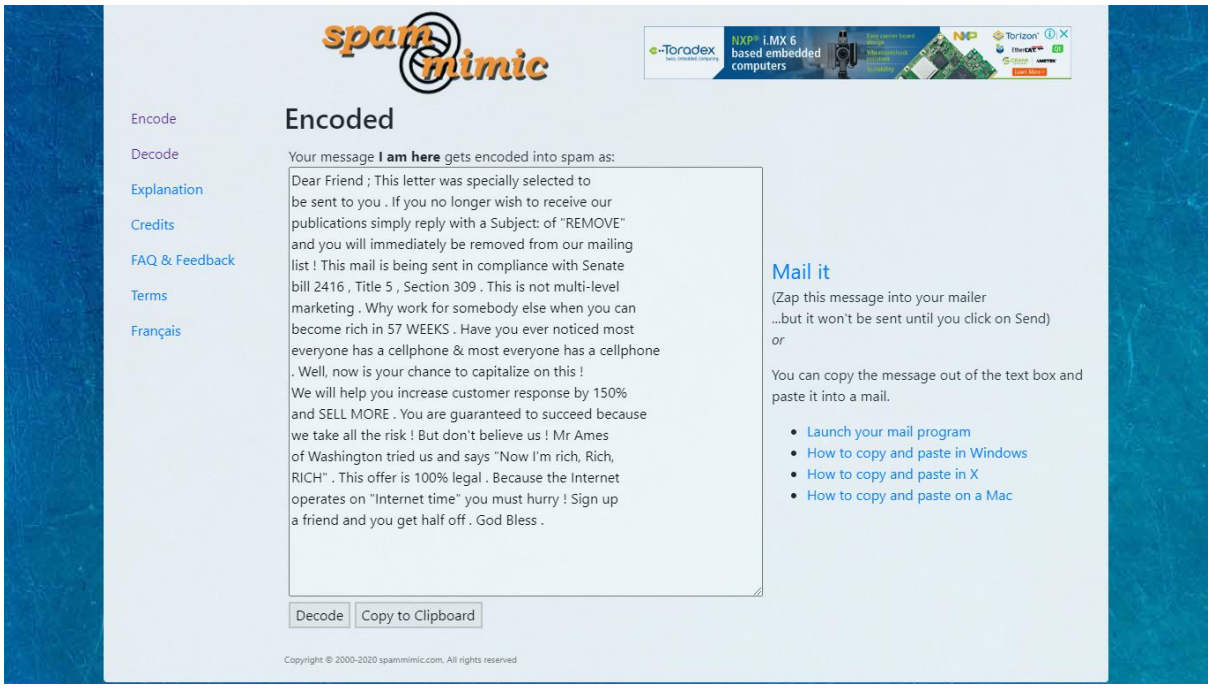


Figure 4 Text Steganography tool:- span mimic

4. Press button and you will see encode message

Figure 5 Text Steganography tool:- span mimic

5. Enter the password and encode message

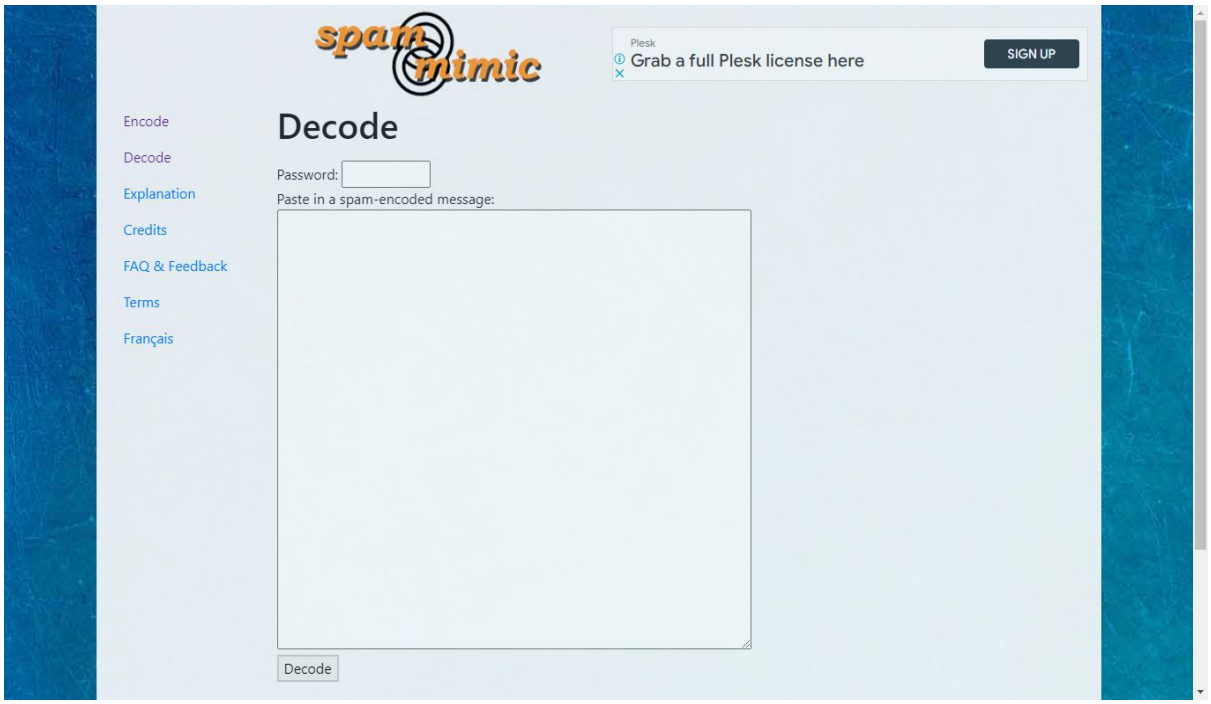


Figure 6 Text Steganography tool:- span mimic

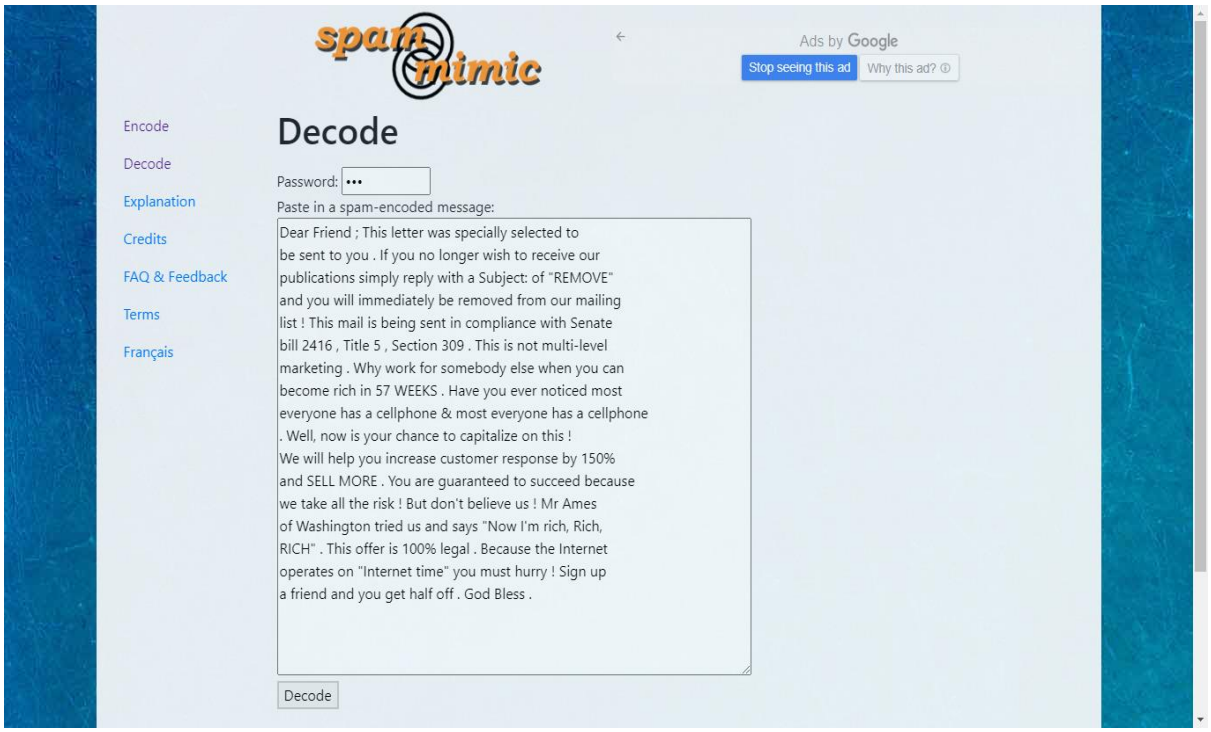


Figure 7 Text Steganography tool:- span mimic

6. Press button and you will get original text

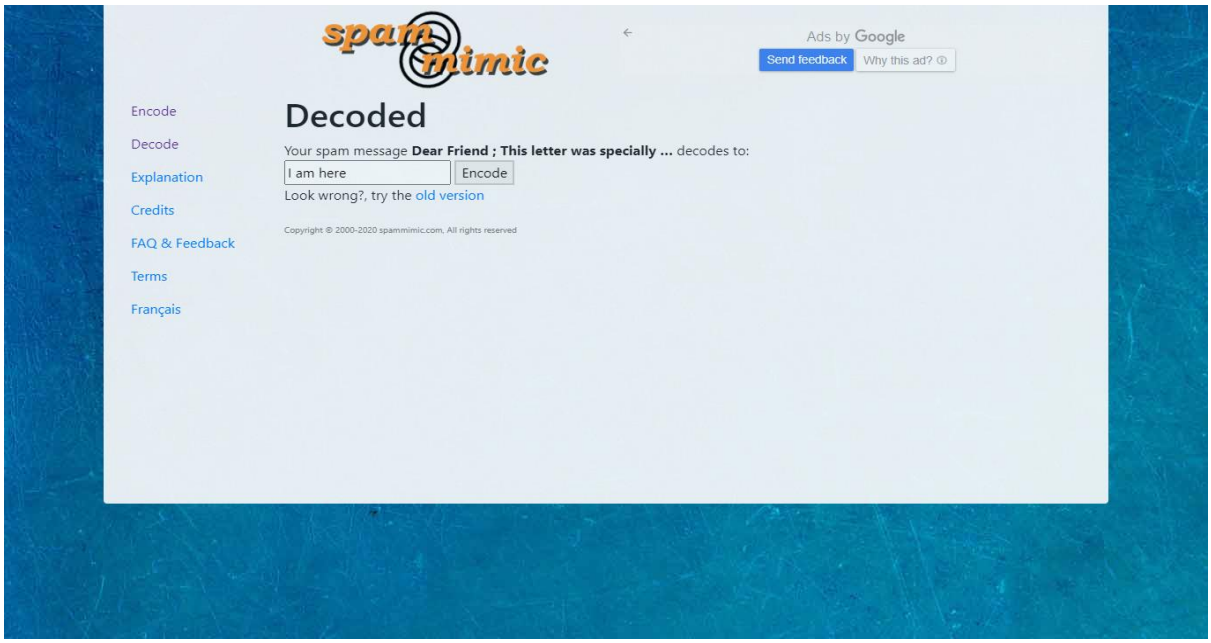


Figure 8 Text Steganography tool:- span mimic

Analysis:

1. We are able to use span mimic to encode your small texts, emails, and messages with various different methods and also gives you the way to decode the specific encoded format text.

Task 2: Perform Images Steganography using Pelock

- **Website link :-** [Steganography Online Codec - Hide Message in Image (pelock.com)]

    - Steganographic online codec allows you to hide a password encrypted message within the images & photos using AES encryption algorithm with a 256-bit PBKDF2 derived key.
    - The art and science of hiding information by embedding messages within other, seemingly harmless image files.
    - In this case, the individual bits of the encrypted hidden message are saved as the least significant bits in the RGB color components in the pixels of the selected image.
    - With our steganographic encoder you will be able to conceal any text message in the image in a secure way and send it without raising any suspicion. It will only be possible to read the message after entering the decryption password.

- **Original Text:-** hi i am here
- **Password**: - ***(123)
- **Original Images**

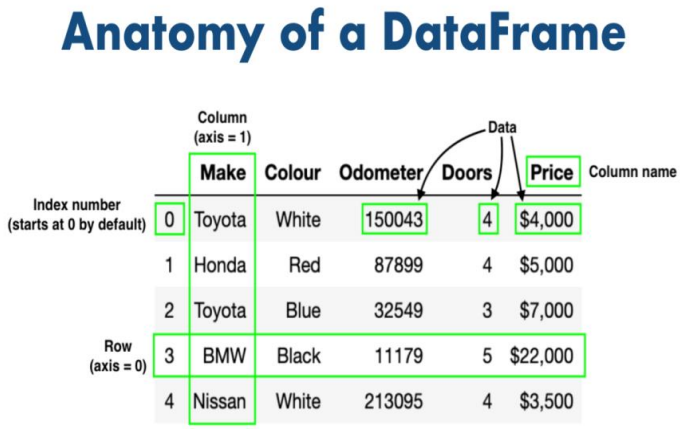


Figure 9 original image for encryption

Steps:

1. Website link :- [Steganography Online Codec - Hide Message in Image (pelock.com)]

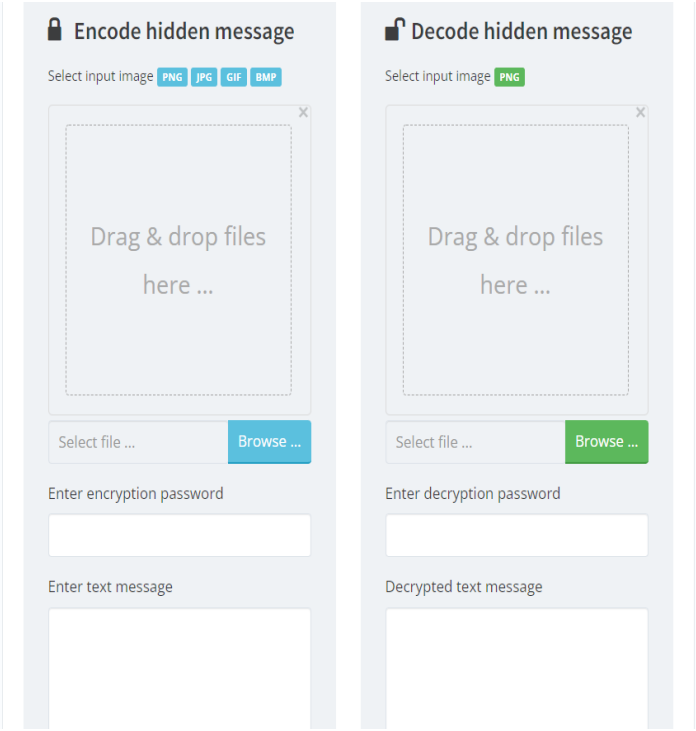


Figure 10 Images Steganography tool :- pelock

2. Original Images

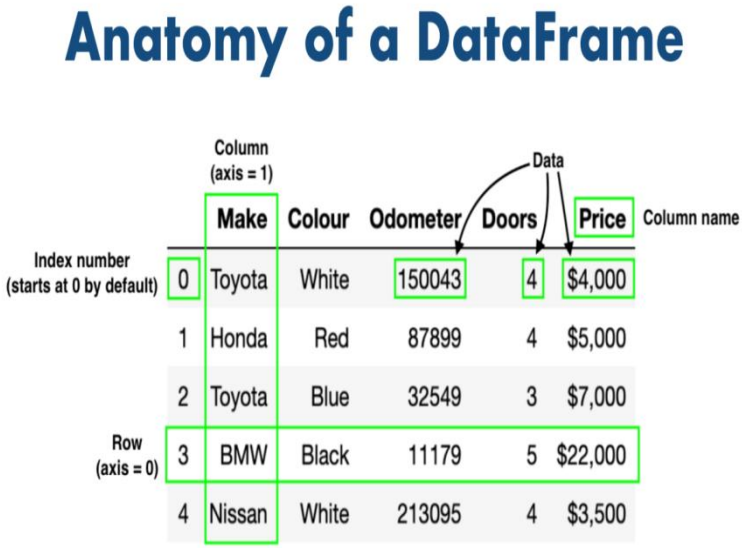


Figure 11 Images Steganography tool :- pelock

3. **Click on brows and upload images and add encode message you want to add**

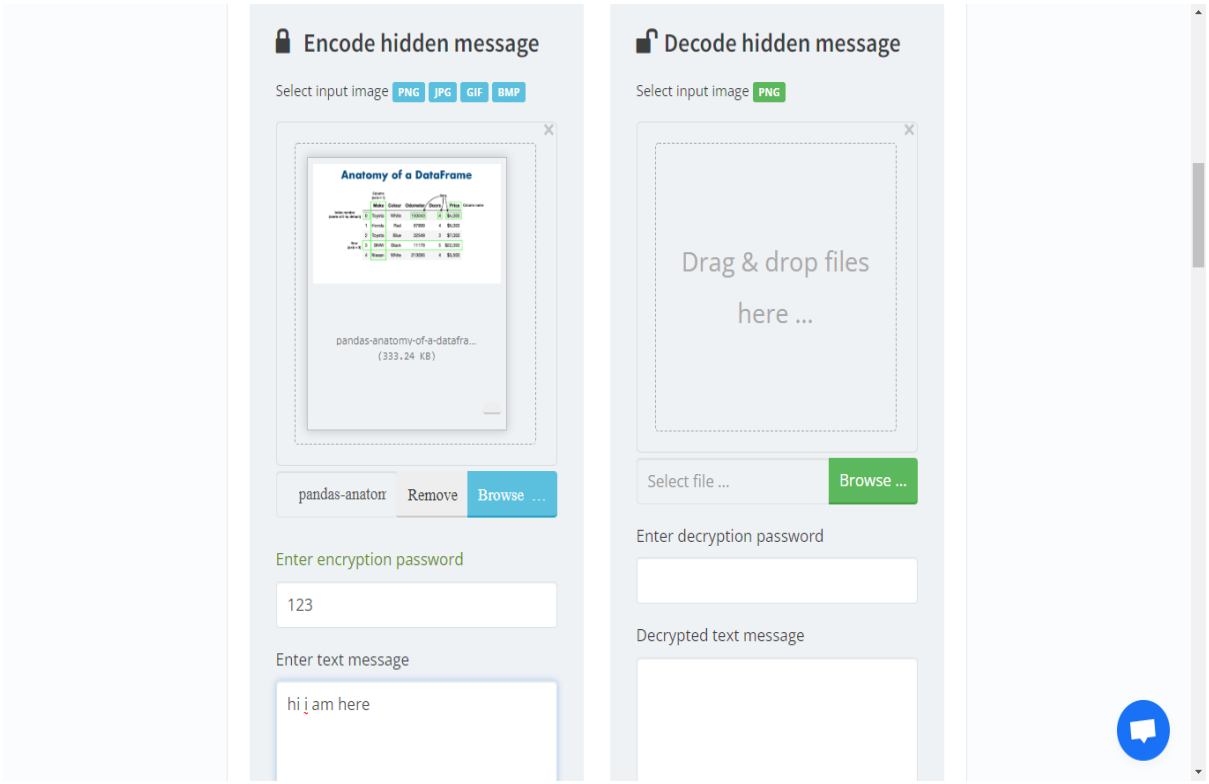


Figure 12 Images Steganography tool :- pelock

4. After encrypted you can download images

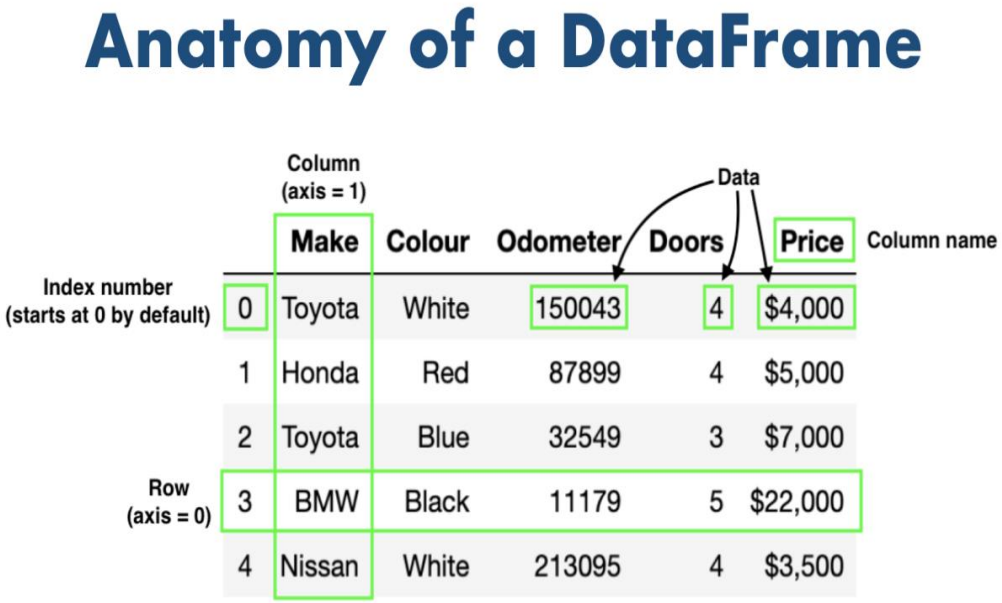


Figure 13 Images Steganography tool :- pelock

5. **Click brows and add encoded image and write password and you will get message**

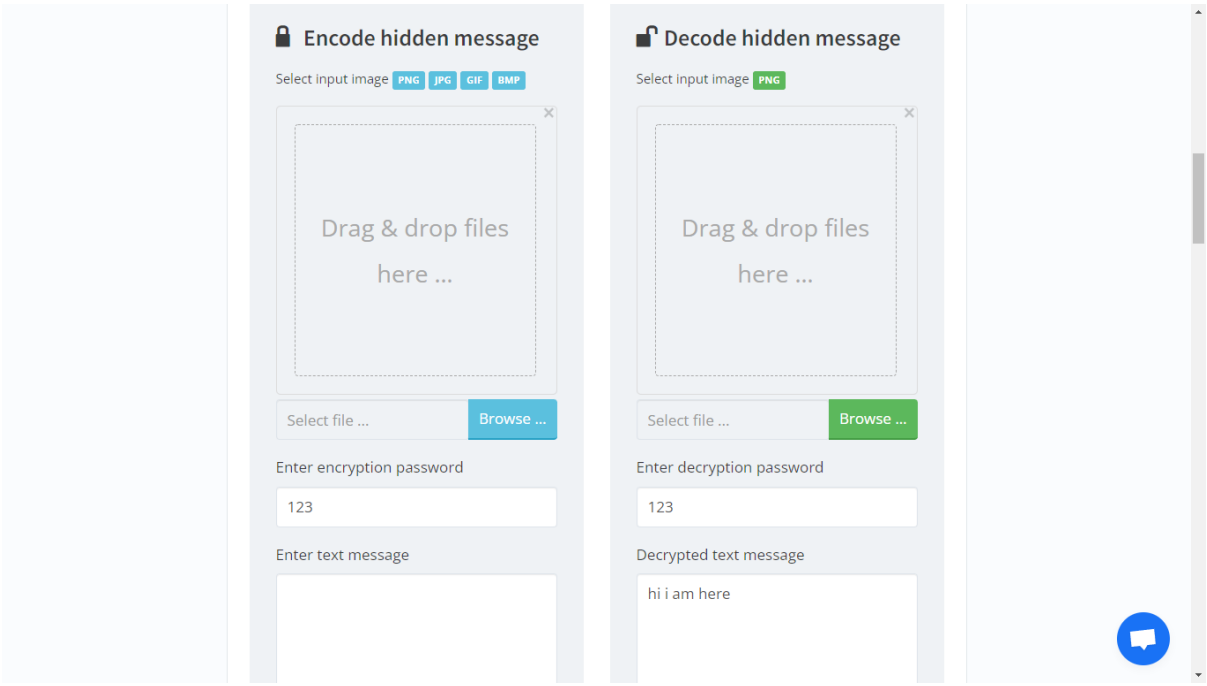


Figure 14 Images Steganography tool: - pelock

Analysis:

1. While comparing the original file with setgo file (encoded file) we can see there lots of difference in both file
2. File format is different, file size is different and timestamp is different

Similar Tools:

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

Task 3: Perform Audio Steganography using STEGONAUT

- Website link :- STEGONAUT - Audio Steganography Tool
    - STEGONAUT use for hide information in audio
    - Hide secret text messages inside MP3 files. Just choose an MP3 of your choice, type in your message, and a new MP3 file will be created. To uncover the message, load the newly created file again. Optionally, you can choose to encrypt the message with a password for additional layer of security.

Steps:

- Visit Website link :- STEGONAUT - Audio Steganography Tool

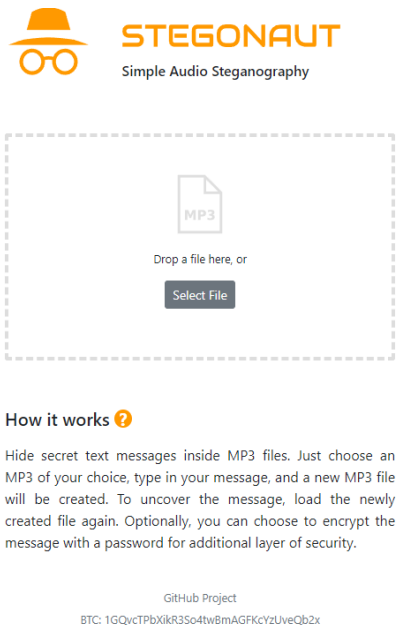


Figure 15 Audio Steganography tool: - STEGONAUT

1. Upload your audio and write down password and message

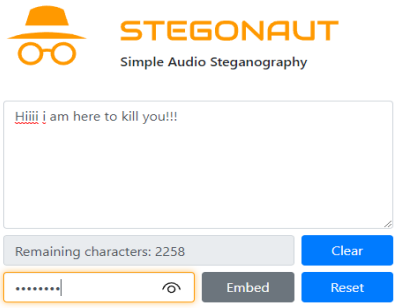


Figure 16 Audio Steganography tool: - STEGONAUT

2. Go to extract selection and write down password and you will get your meassage

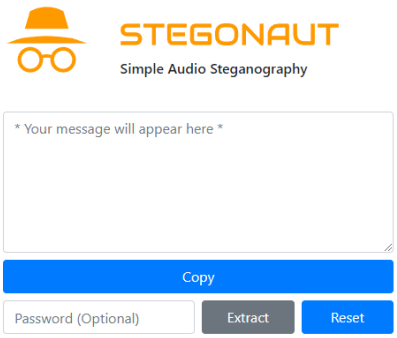


Figure 17 Audio Steganography tool: - STEGONAUT

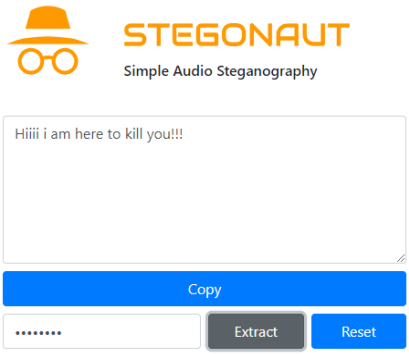


Figure 18 Audio Steganography tool: - STEGONAUT

Analysis:

1. We are using STEGONAUT for Audio Steganography. With this tool we can Hide secret text messages inside MP3 files with password and when can see different in MP3 file size.
2. When we need hide text we can use encrypted MP3 file to get hidden message.

Similar tools:

- Wavstag
- Sonic visualizer
- Steghide

Task 4: Perform Video steganography using OpenPuff

- Download link **:- Video steganography tool OpenPuff**
- Open Puff Steganography tool which use for video steganography. Open Puff is a freeware data encryptor app that's been categorized by our editors under the data encryption software category and made available by Cosmo Oliban for Windows

Step: -

1. Download and install OpenPuffVideo Steganography tool.

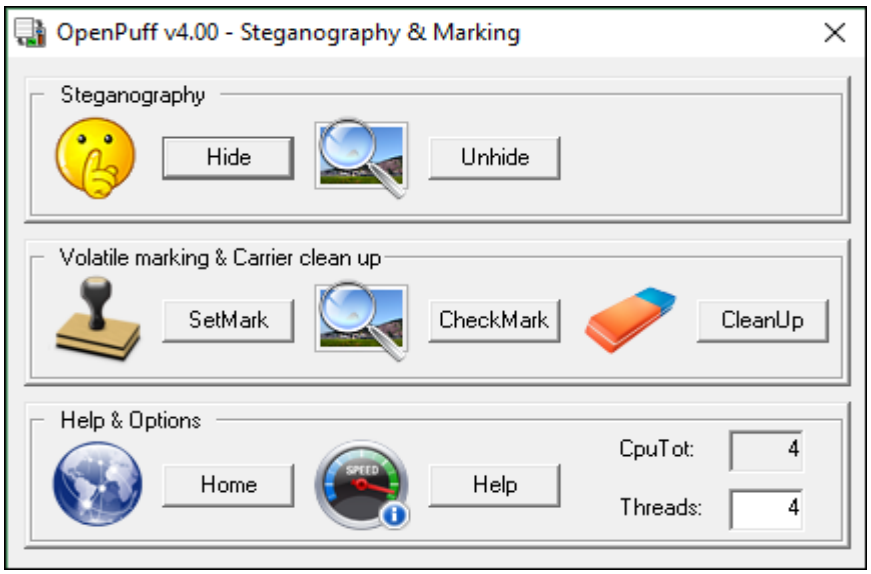


Figure 19 Video steganography tool:- Open Puff

2. click on Hide button to enter the main interface of Open Puff.

3. Here in this window the interface is divided into 4 sections for performing different tasks. In the first section set the desired password for unhiding your data.

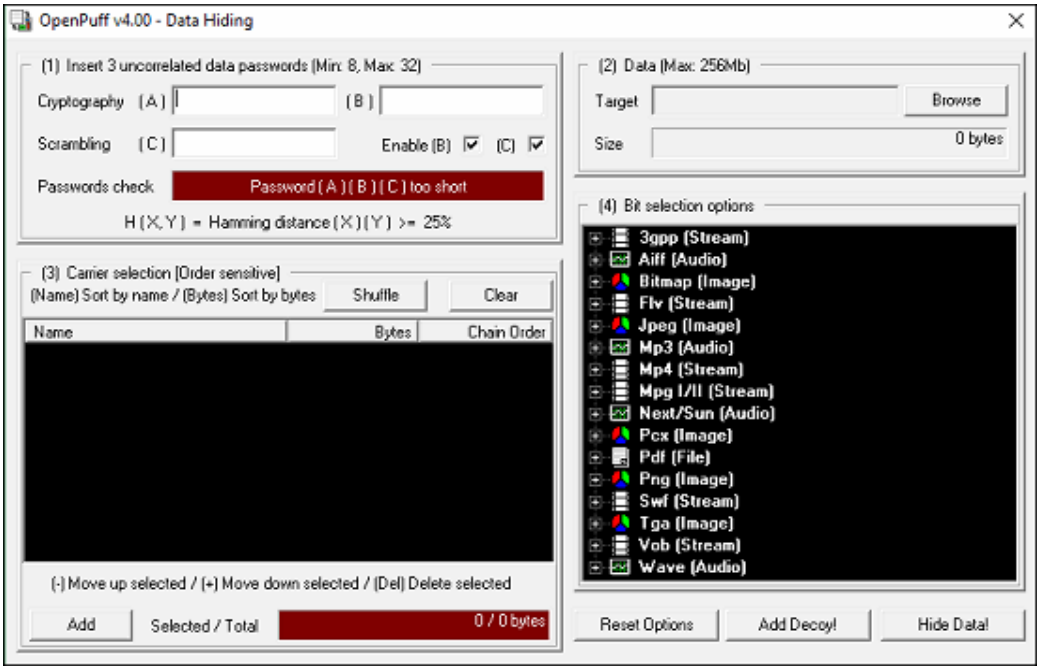


Figure 20 Video steganography tool:- Open Puff

4. In Carrier Selection provide the carrier video file that you want to use for hiding your messages/documents.

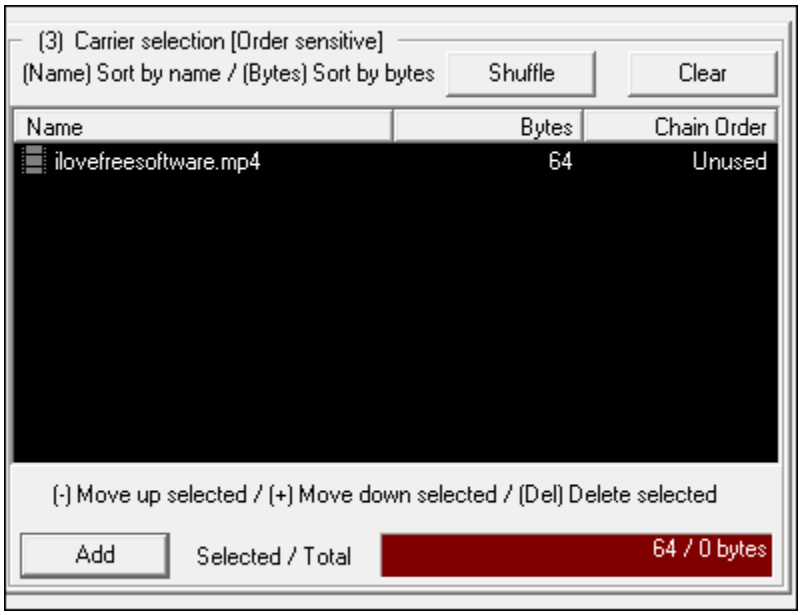


Figure 21 Video steganography tool:- Open Puff

5. Provide the target file that you want to hide in carrier video file and then hit the Hide Data button to complete the process.

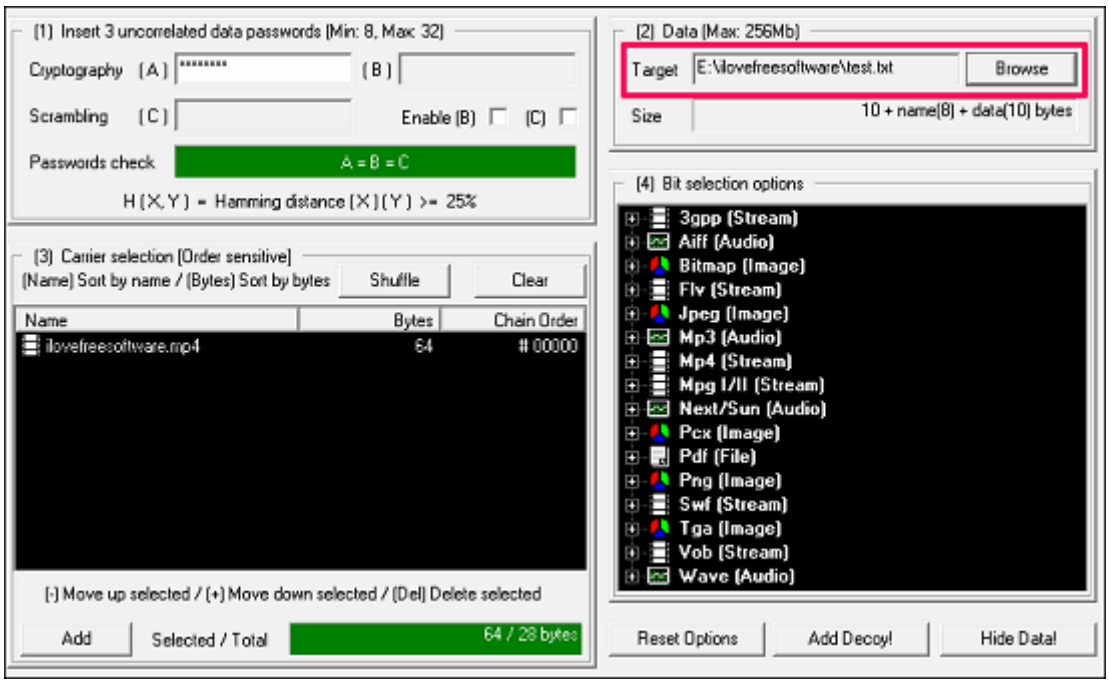


Figure 22 Video steganography tool:- Open Puff

6. After going through the above steps, a final dialog will appear, asking you to specify the folder where you want to save the final video file that contains your hidden messages and documents. This will save the video file, with your files hidden in it.

7. For extracting the data from an existing carrier video file/files that you created, the process is almost the same. You just have to select the unhide option from the main window of OpenPuff. Next, provide the password that you set during hiding your file and provide the location where you want to store the extracted file.

Analysis:

1. OpenPuff is a prevailing data hiding application made easy, safe and free that allows you to hide data into encrypted files in order to send it to other users.
2. In this we are using Video to hide our message

Similar Tools:

- Our Secret
- DeEggerEmbeddder
- StegoMagic

Task 5: Perform Folder Steganography using QuickCrypto

- Website link to download tool :-Download QuickCrypto - Free 15 Day Trial Period

- QuickCrypto is advanced Windows based privacy and encryption software. It uses the most powerful algorithms and techniques to ensure your email communication, passwords, all confidential files and information are kept completely secure

Steps:

1. Website link to download tool :- Download QuickCrypto - Free 15 Day Trial Period

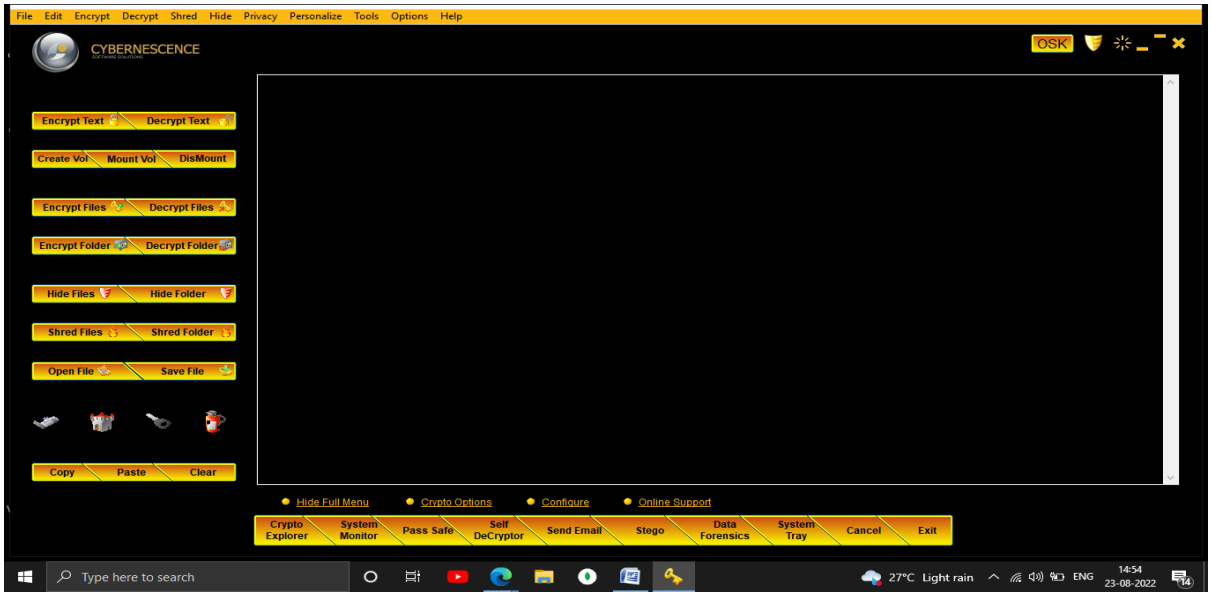


Figure 23 Folder Steganography tool:- Quick Crypto

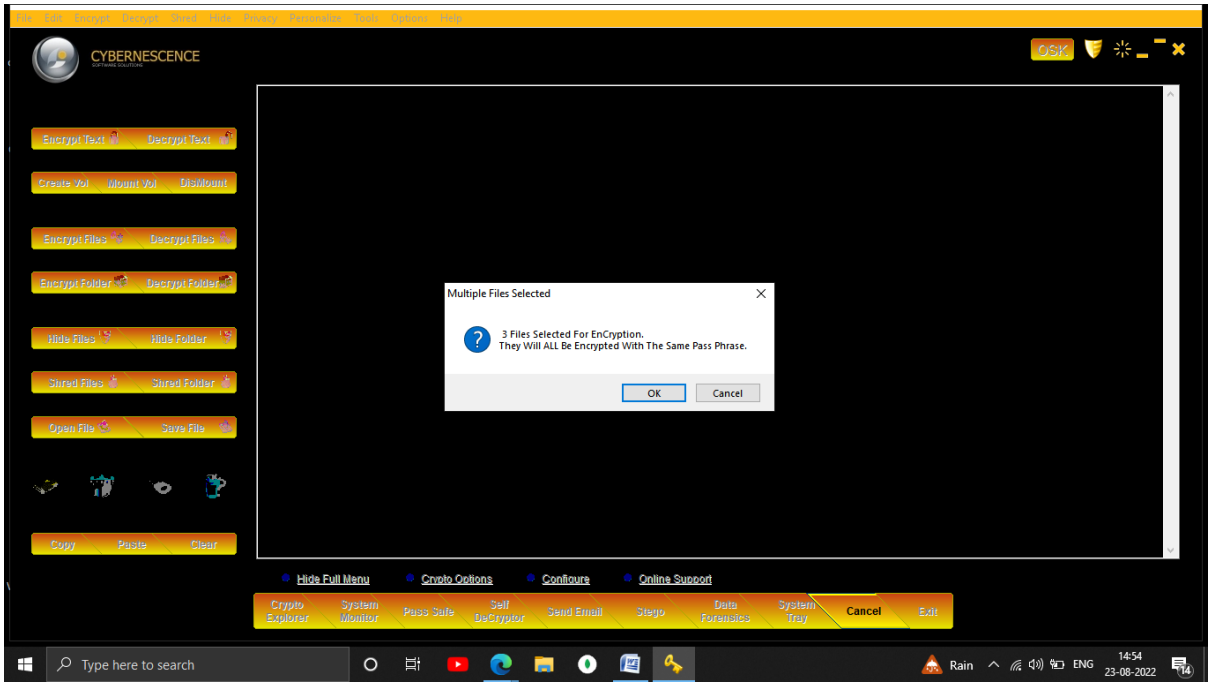


Figure 24Folder Steganography tool:- Quick Crypto

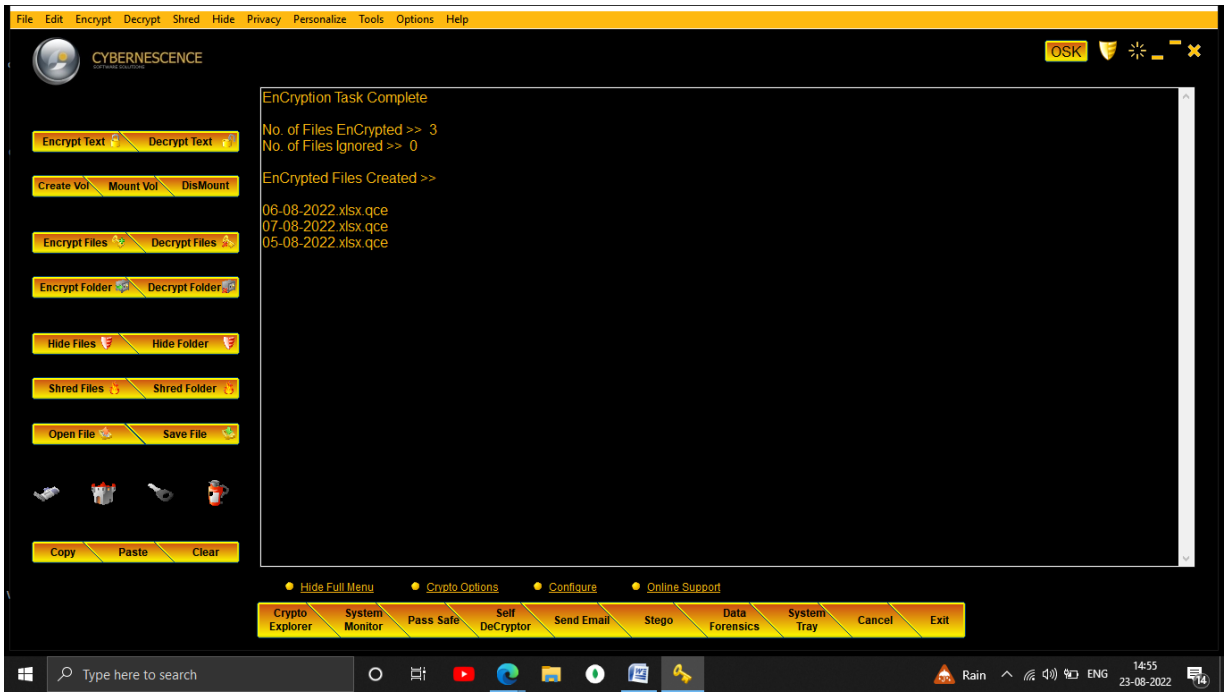


Figure 25 Folder Steganography tool:- Quick Crypto

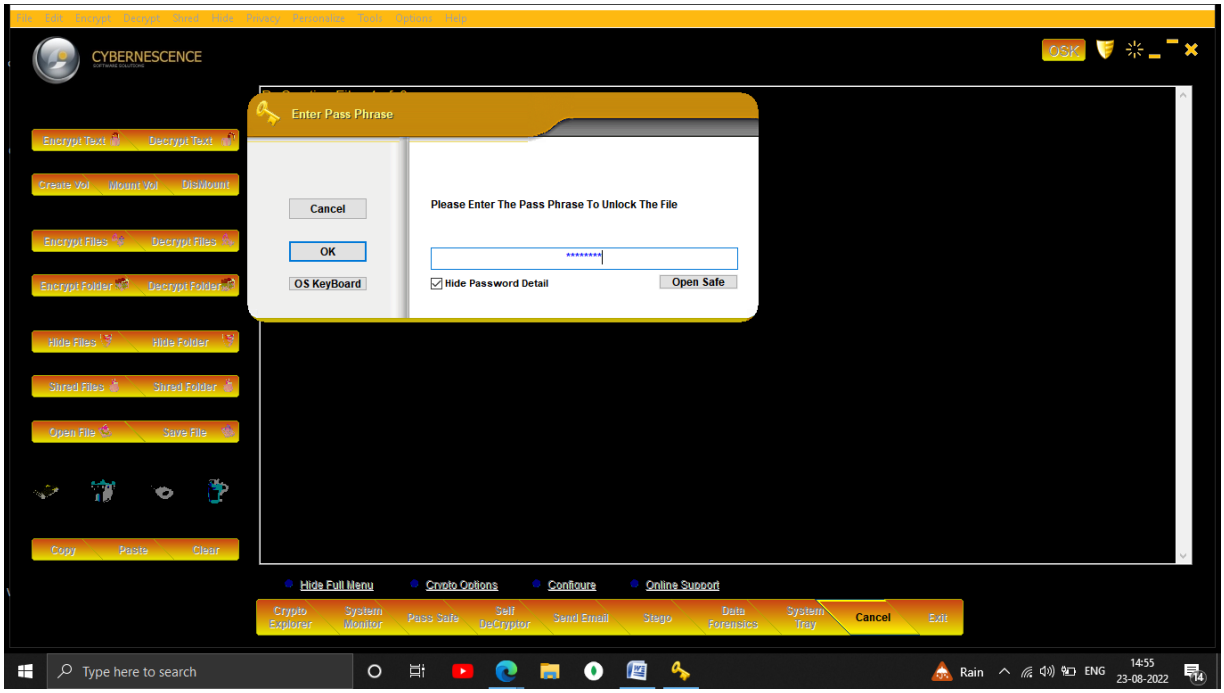


Figure 26 Folder Steganography tool:- Quick Crypto

Analysis:

1. With the help of quick crypto we are able to do Folder Steganography and it refers to hiding one or more files in a folder. During this we are able to hide folder but still keeps the associated files in its original folder for recovery.

Conclusion:

- Steganography is an effective way of secure communication. You can first encrypt a confidential file and then hide it inside an image of another kind of file before sending it to some other. It will decrease the chances of being intercepted.
- If you just send the file by encrypting it, the attacker will try to decrypt it by various ways. However, if he only finds a normal image file, he'll have no clue.
- This technique is very easy to use but very difficult to detect. It can be used by government organizations to use as the way to send and receive files securely

Digital Forensics Lab Report: 2

Date: 03-08-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

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

What is OSINT?

Open-source data is any information that is readily available to the public or can be made available by request. OSINT sources can include:

- Newspaper and magazine articles, as well as media reports
- Academic papers and published research
- Books and other reference materials
- Social media activity
- Census data

Target: Dr Manoj Sahni

Prior Known Information: Works in PDEU, Gandhinagar

PERSONAL DETAILS

Name	Dr Manoj Sahni
Designation	Associate Professor
Department	Department of Mathematics, School of Technology
Email	Manoj.Sahni@sot.pdpu.ac.in

Figure 1 Dr Manoj Sahni

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
Areas of Interest
Elasticity, Plasticity, and Creep, Functionally Graded Materials, Fuzzy Sets and their Extensions, Development of Novel Numerical Methods, Fixed Point Iteration Methods.
Mobile No.: +91 7874441820

PUBLICATIONS / ARTICLES / CONFERENCE

'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

'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

'Diagnosis of Intracranial Tumors via the Selective CNN Data Modeling Technique', Applied Sciences, pp. 1-14, mar 2022

'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

'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 ordinary differential equation in a fuzzy environment', Journal of Interdisciplinary Mathematics, pp. 1-13, 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

'FROBENIUS SERIES SOLUTION FOR FUNCTIONALLY GRADED MATERIAL WITH EXPONENTIALLY VARIABLE THICKNESS AND MODULI', Structural Integrity and Life , pp. S83-S88, aug 2021

'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

'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

'Sumudu Transform for Solving Second Order Ordinary Differential Equation under Neutrosophic Initial Conditions', Neutrosophic Sets and Systems,, pp. 258-275, Dec 2020

'ANALYSIS OF CREEP STRESSES IN THIN ROTATING DISC COMPOSED OF PIEZOELECTRIC MATERIAL ', Structural Integrity and Life , pp. S45-S49, Dec 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

'Generalized Trapezoidal Intuitionistic Fuzzy Number for Finding Radial Displacement of a Solid Disk', WSEAS TRANSACTIONS on MATHEMATICS, pp. 105 - 111, mar 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

'Thermo-mechanical Stress Analysis of Thick-Walled Cylinder with Inner FGM Layer', Structural Integrity and Life , pp. 211-223, Dec 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

'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

'Two -dimensional mechanical stresses for a pressurized cylinder made of functionally graded material', Structural Integrity and Life , pp. 79 – 85, Oct 2019

'Strength analysis of functionally graded rotating disc under variable density and temperature loading', Structural Integrity and Life , pp. 95 – 101, Oct 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

'Information Theoretical Measure for Career Determination', WSEAS Transactions on Mathematics, pp. 73 – 78, mar 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

Google Scholar:

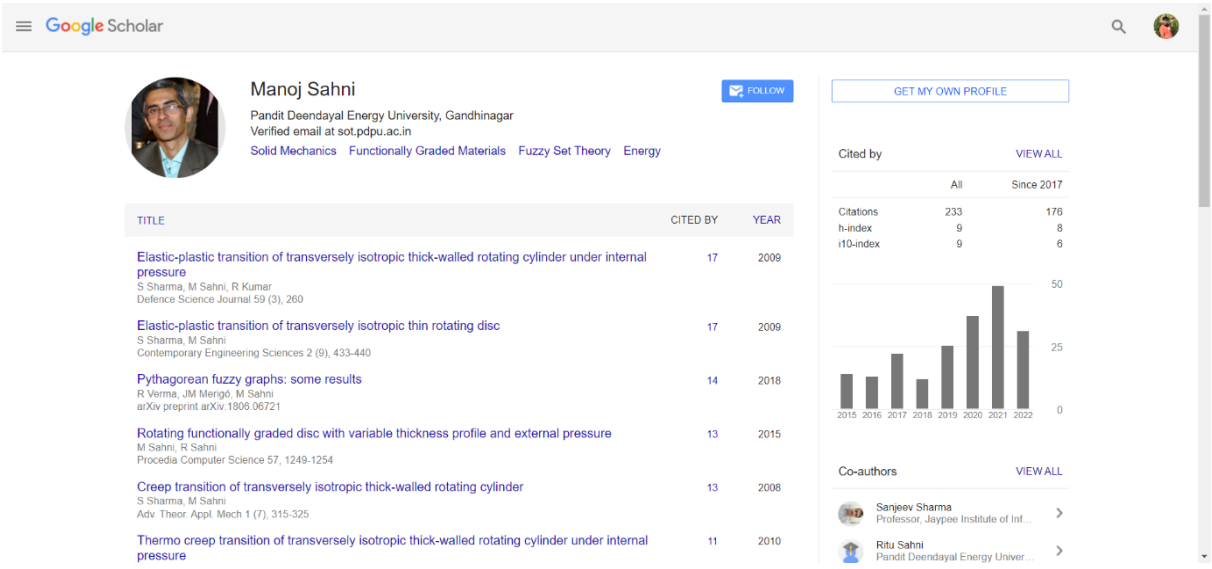


Figure 2 Dr Manoj Sahni google scholer profile

Source:

1. **https://orsp.pdpu.ac.in/adminfacviewprofile.aspx?facid=manoj.sahni**
2. **https://scholar.google.co.in/citations?user=ioO8dpUAAAAJ&hl=en**
3. **https://www.facebook.com/public/Manoj-Sahni**

Analysis:

1. With the help of OSINT we are able to profiling Dr Manoj Sahni and able to find their person information and other information like research paper, contact number etc.

Conclusion:

1. Open Source Intelligence software, abbreviated as OSINT software, are tools that allow the collection of information that is publicly available or open-source. The goal of OSINT software is mainly to learn more about someone or a business. 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

2. With the help of OSINT we are able to gather data of PDEU professor Dr Manoj Sahni and able to find their person information and other information like research paper, contact number etc.

Digital Forensics Lab Report: 3

Date 17-08-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

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

Tool Names:

1. **Forensically :-** Forensically, free online photo forensics tools - 29a.ch
2. **YouTube meta data:-** YouTube Metadata (mattw.io)
3. **Wikimapia:-** **https://www.google.com/search?q=wikimapia&rlz=1C1ZKTG_enIN914IN919&oq=Wikimapia&aqs=chrome.0.0i131i433i512j0i512l9.20776j0j4&sourceid=chrome&ie=UTF-8**
4. **Pic2map :-** Photo Location & Online EXIF Data Viewer - Pic 2 Map
5. **Suncalc :-** SunCalc - sunrise, sunset, shadow length, solar eclipse, sun position, sun phase, sun height, sun calculator, sun movement, map, sunlight phases, elevation, Photovoltaic system, Photovoltaic
6. **Exif Data Viewer :-** EXIF Data Viewer
7. **Exif Tool:**

Task 1:- Use photo forensics tool :- Forensically

- Forensically:- Forensically, free online photo forensics tools - 29a.ch
- Forensically is a set of free tools for digital image forensics. It includes clone detection, error level analysis, meta data extraction and more. It is made by Jonas Wagner.
- It provide Tools like Magnifier, Magnification factor, Clone Detection, Enhancement, Error Level Analysis. Noise Analysis, Level Sweep, Luminance Gradient, JPEG Analysis

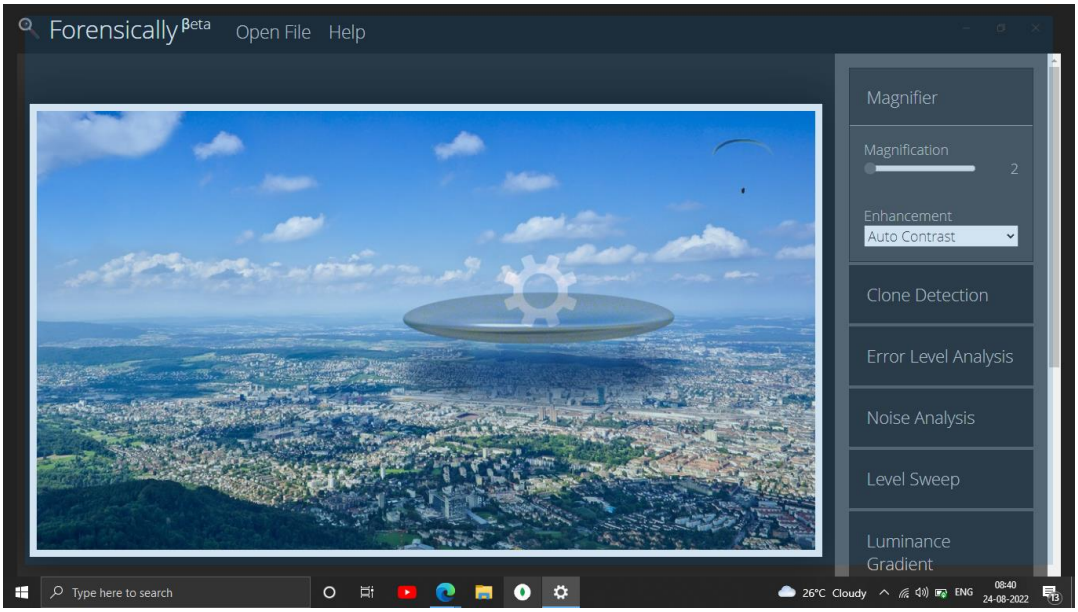


Figure 1 photo forensics tool :- Forensically

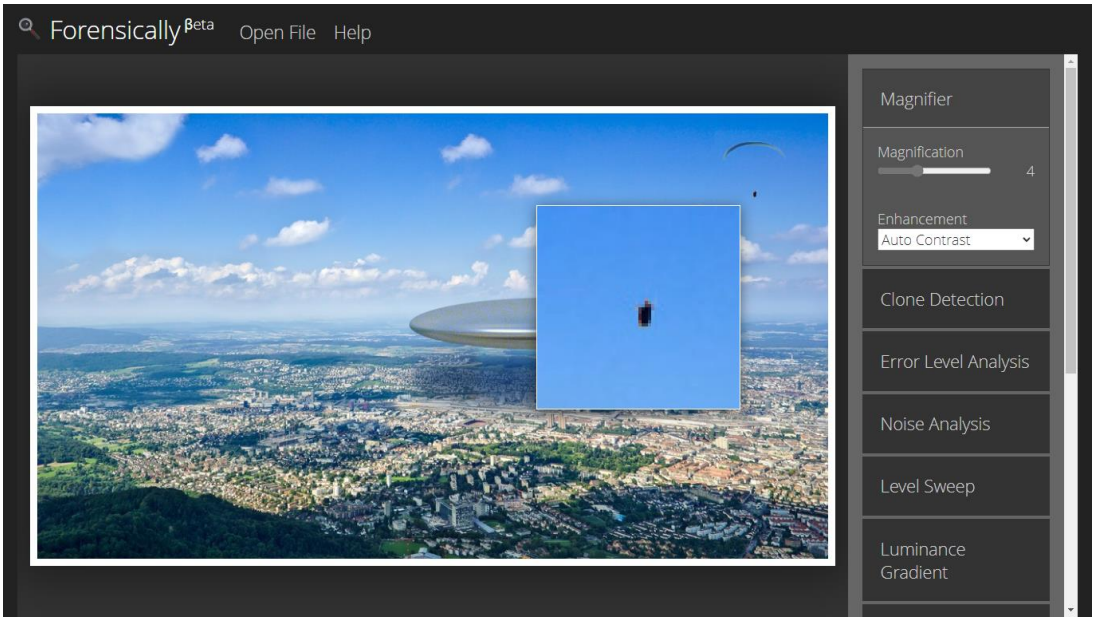


Figure 2 photo forensics tool :- Forensically

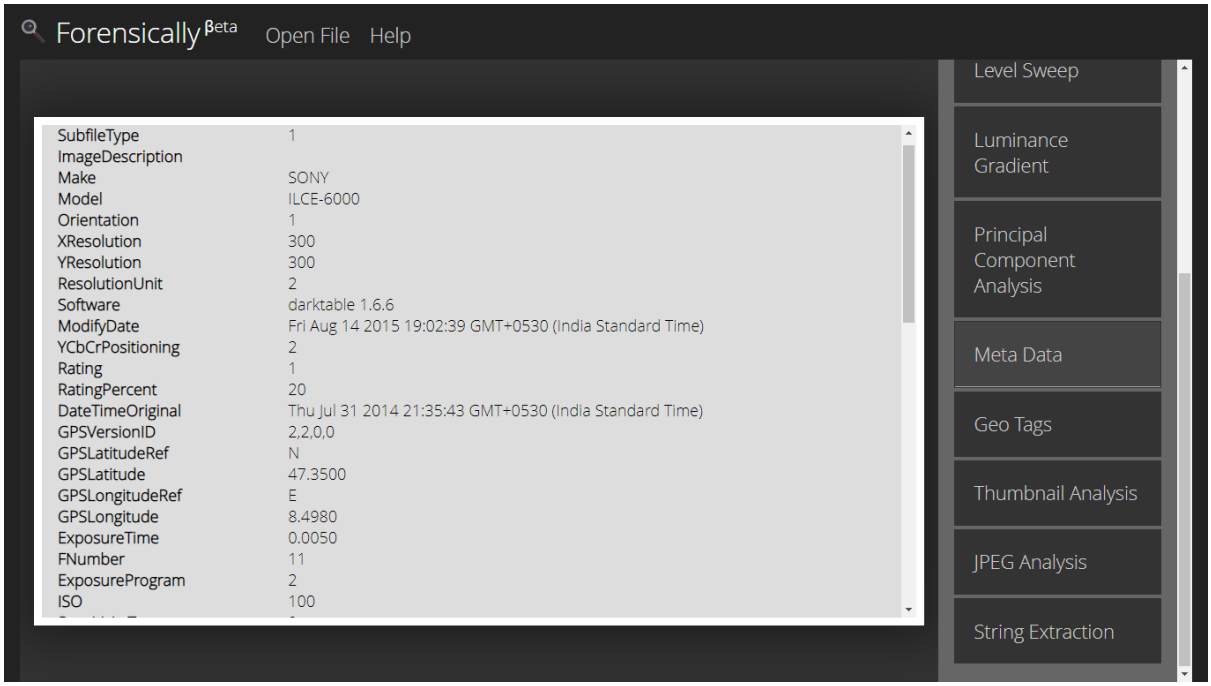


Figure 3 photo forensics tool :- Forensically

Analysis:

1. We are using forensics for digital image forensics and this tool includes clone detection, error level analysis, meta data extraction.
2. It also provided function like Enhancement, Error Level Analysis. Noise Analysis, Level Sweep, Luminance Gradient, JPEG Analysis

Task 2:- Exploring YouTube meta data tool

- YouTube meta data:- YouTube Metadata (mattw.io)
- The Youtube Dataviewer is a tool that allows users to extract metadata from Youtube videos.
- YouTube metadata is information that is used to describe each video uploaded to the platform. Basic examples include things like title, channel name and date uploaded. More sophisticated YouTube metadata includes things such as geographic coordinates, camera make and frame rate.

Steps

1. **Open** YouTube meta data:- YouTube Metadata (mattw.io)

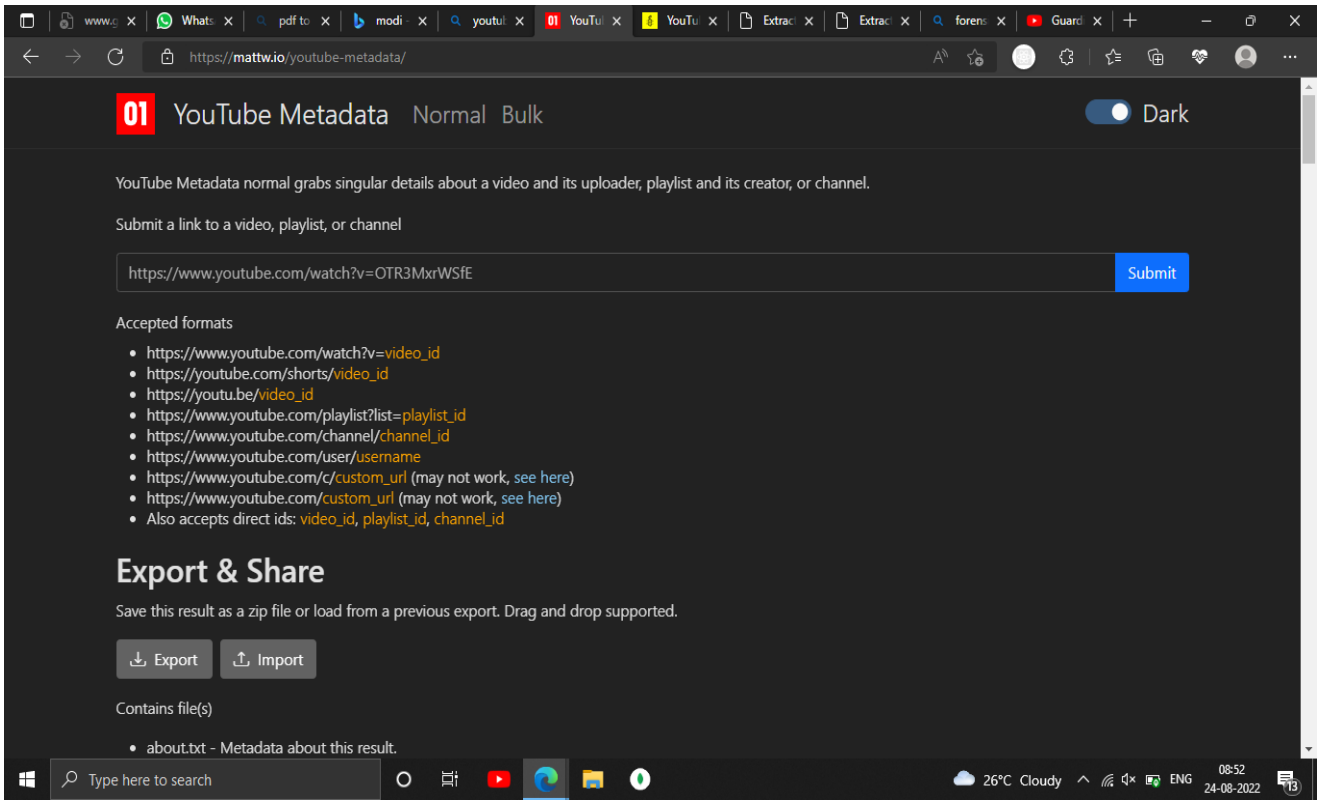


Figure 4 YouTube meta data tool

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.

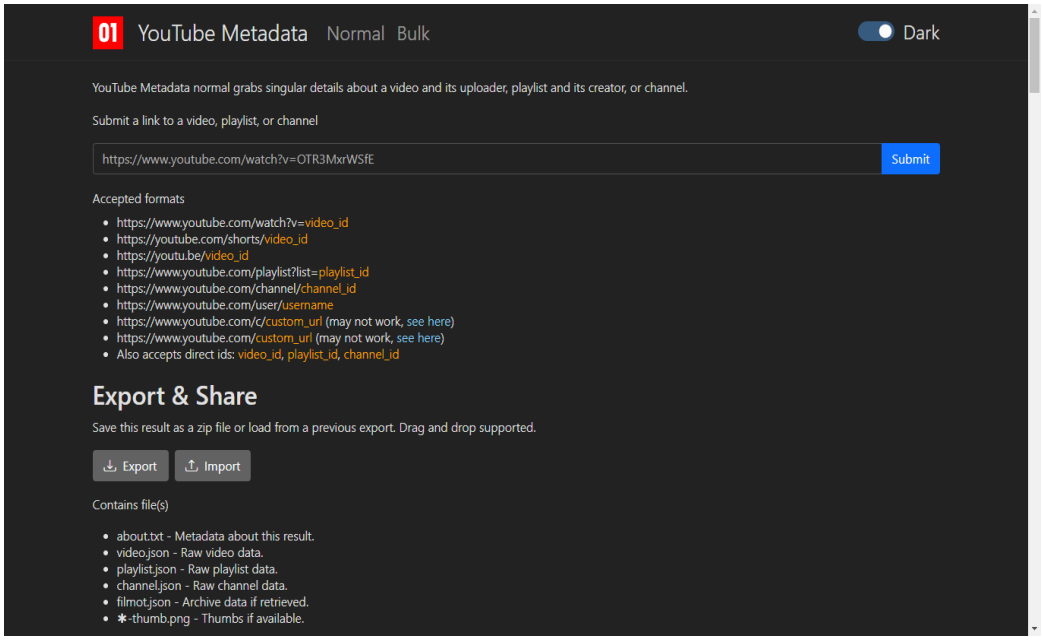


Figure 5 YouTube meta data tool

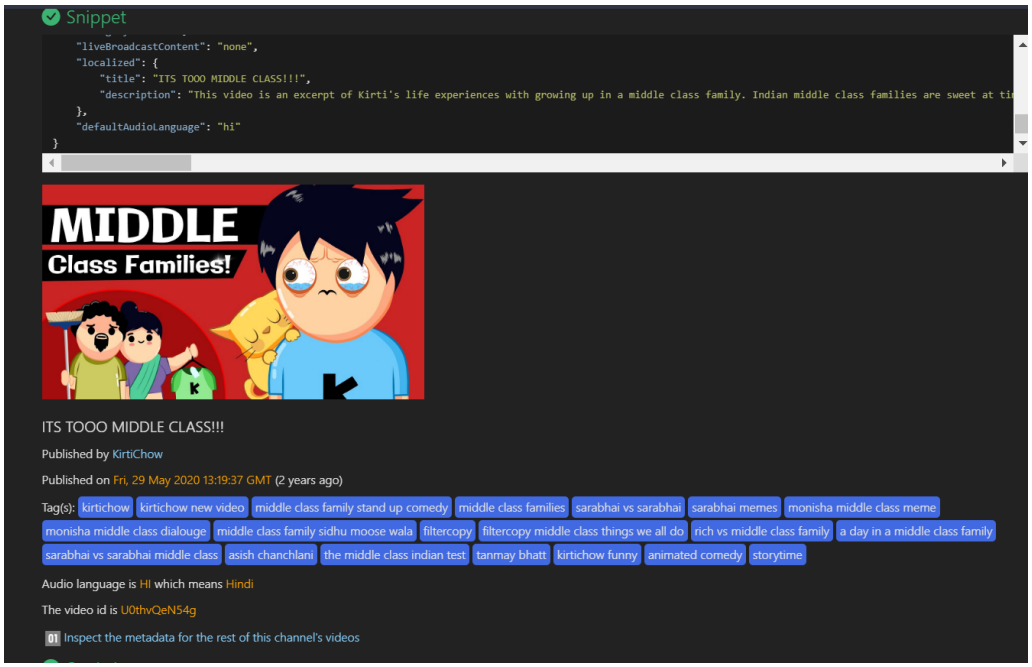


Figure 6 YouTube meta data tool

Analysis:

1. YouTube metadata provided information that is used to describe each video uploaded to the platform.
2. 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 3:- Exploring Wikimapia

- **Wikimapia:**https://www.google.com/search?q=wikimapia&rlz=1C1ZKTG_enIN914IN919&oq=Wikimapia&aqs=chrome.0.0i131i433i512j0i512l9.20776j0j4&sourceid=chrome&ie=UTF-8
- **Wikimapia** is a geographic online encyclopedia project. The project implements an interactive "clickable" web map that utilizes Google Maps with a geographically-referenced wiki system, with the aim to mark and describe all geographical objects in the world.
- Wikimapia was created by Alexandre Koriakine and Evgeniy Saveliev in May 2006. Wikimapia is an open-content collaborative mapping project, aimed at marking all geographical objects in the world and providing a useful description of them.[7] It aims to create and maintain a free, complete, multilingual and up-to-date map of the whole world. Wikimapia intends to contain detailed information about every place on Earth.

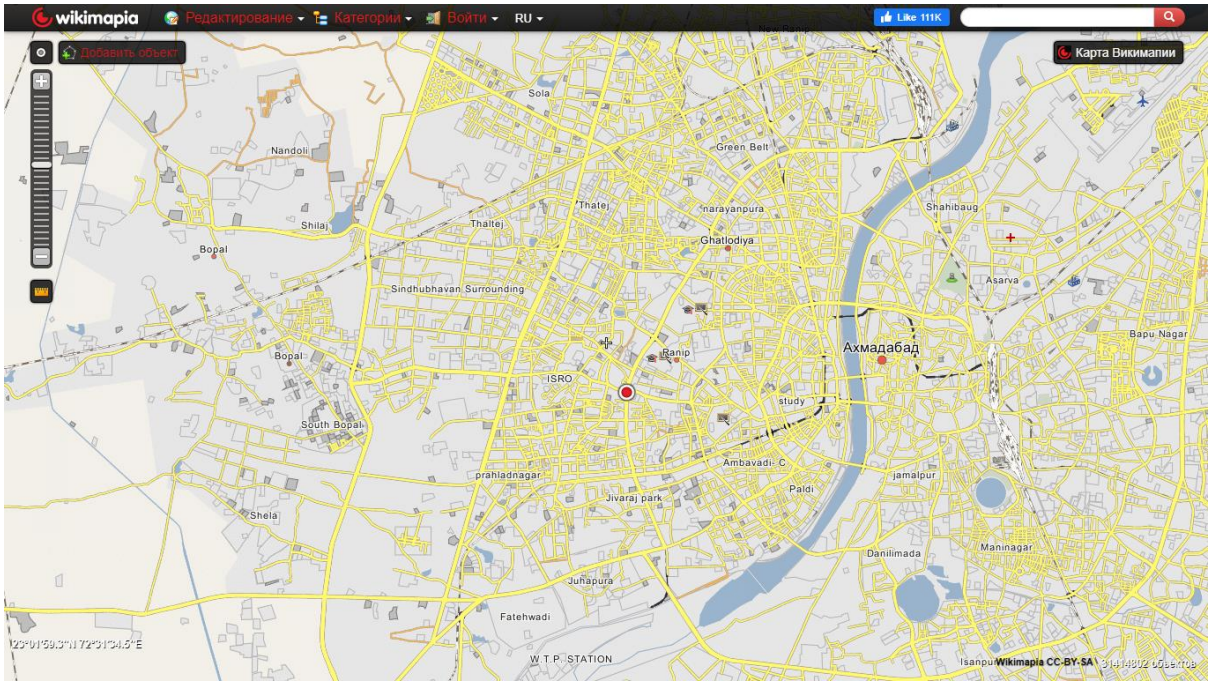


Figure 7 Wikimapia

Analysis:

1. 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 4 :- Exploring Photo Location & Online EXIF Data Viewer tool:- Pic2map

- **Pic2map :-** Photo Location & Online EXIF Data Viewer - Pic 2 Map
- Pic2Map is an online EXIF data viewer with GPS support which allows you to locate and view your photos on a map. Our system utilizes EXIF data which is available in almost all photos taken with digital cameras, smartphones and tablets.
- Even without GPS data, Pic2Map still serves as a simple and elegant online "EXIF" data viewer; which is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression.
- Depending on the brand and model of the camera; EXIF data includes information such as; shutter speed, exposure compensation, F number, ISO speed, flash usage, date and time the image was taken, whitebalance, auxiliary lenses that were used and resolution. Below, you can find a more detailed listing of all data Pic2Map provides

Steps:-

1. **Visit Pic2map :-** Photo Location & Online EXIF Data Viewer - Pic 2 Map

.

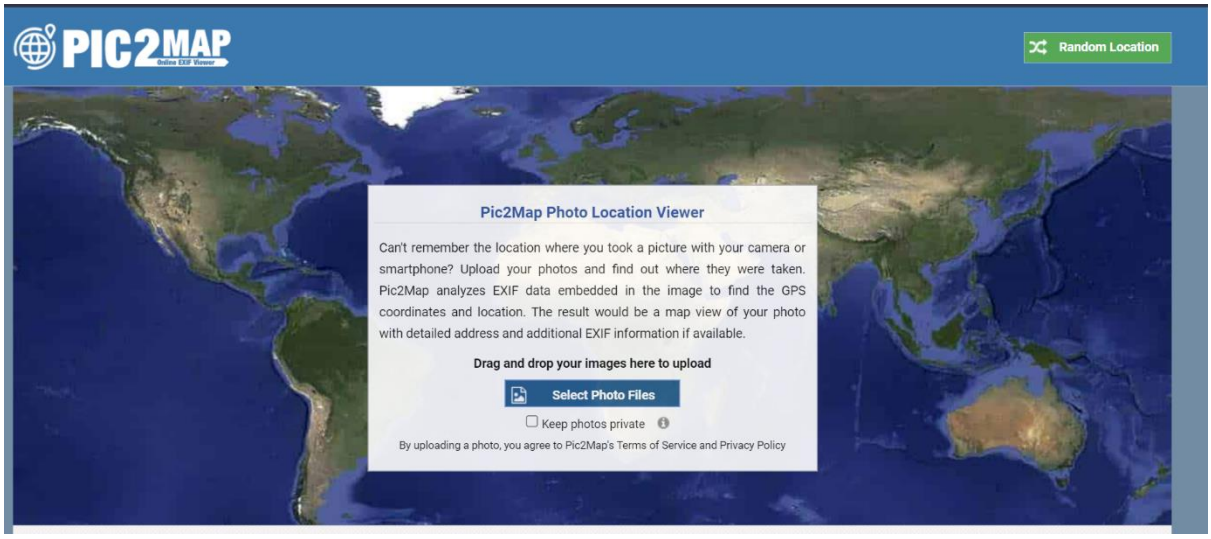


Figure 8 Photo Location & Online EXIF Data Viewer tool:- Pic2map

2. **Upload photo in the website and you will get location of that photo**

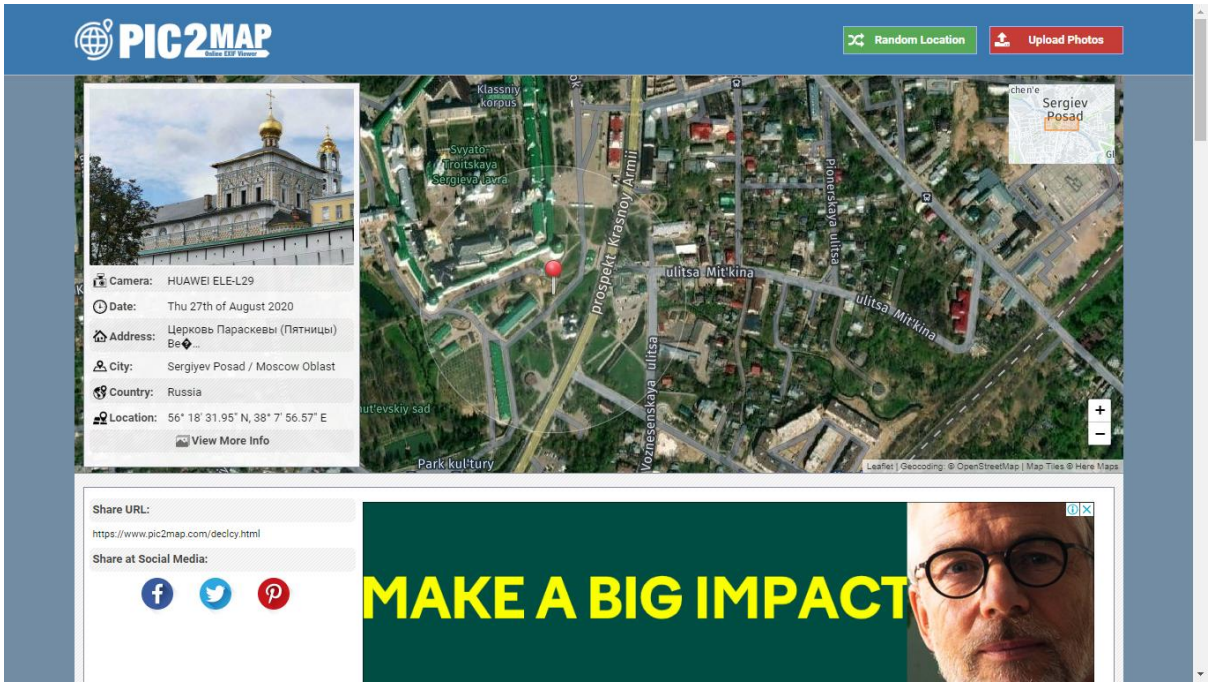


Figure 9 Photo Location & Online EXIF Data Viewer tool:- Pic2map

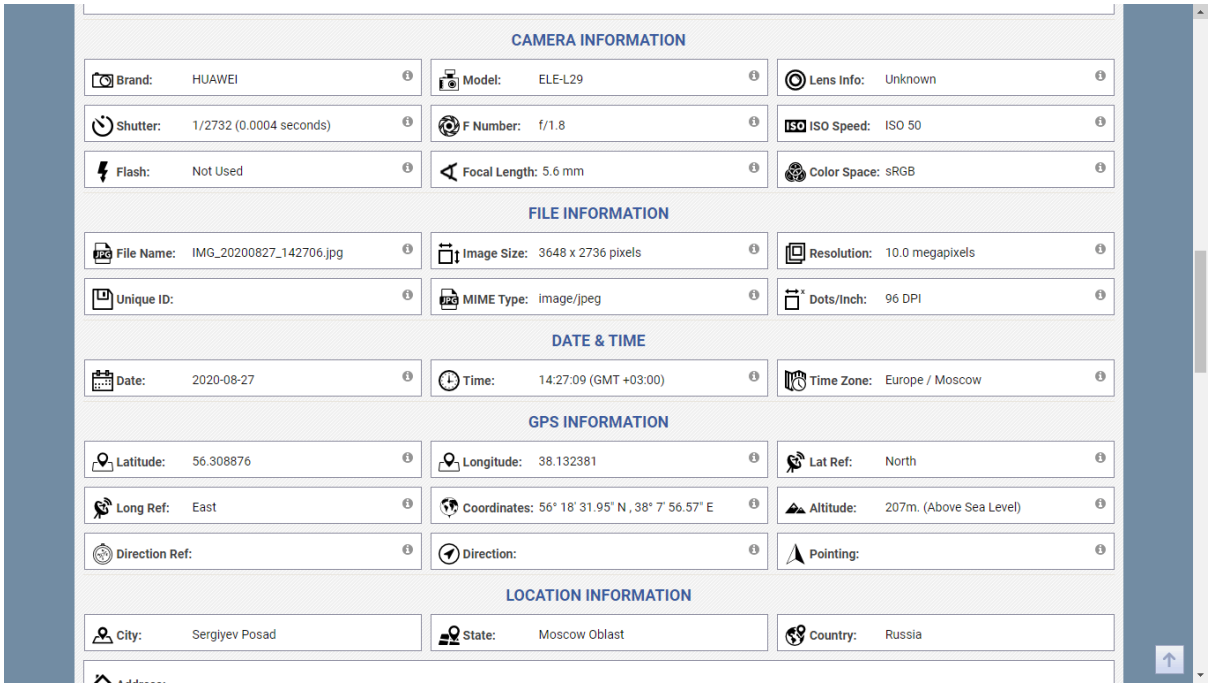


Figure 10 Photo Location & Online EXIF Data Viewer tool:- Pic2map

Analysis:

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

Task 5:- Exploring Suncalc

- Suncalc :- SunCalc - sunrise, sunset, shadow length, solar eclipse, sun position, sun phase, sun height, sun calculator, sun movement, map, sunlight phases, elevation, Photovoltaic system, Photovoltaic

- SunCalc is a little app that shows sun movement and sunlight phases during the given day at the given location. The user can see sun positions at sunrise, specified time and sunset. The thin orange curve is the current sun trajectory, and the yellow area around is the variation of sun trajectories during the year.

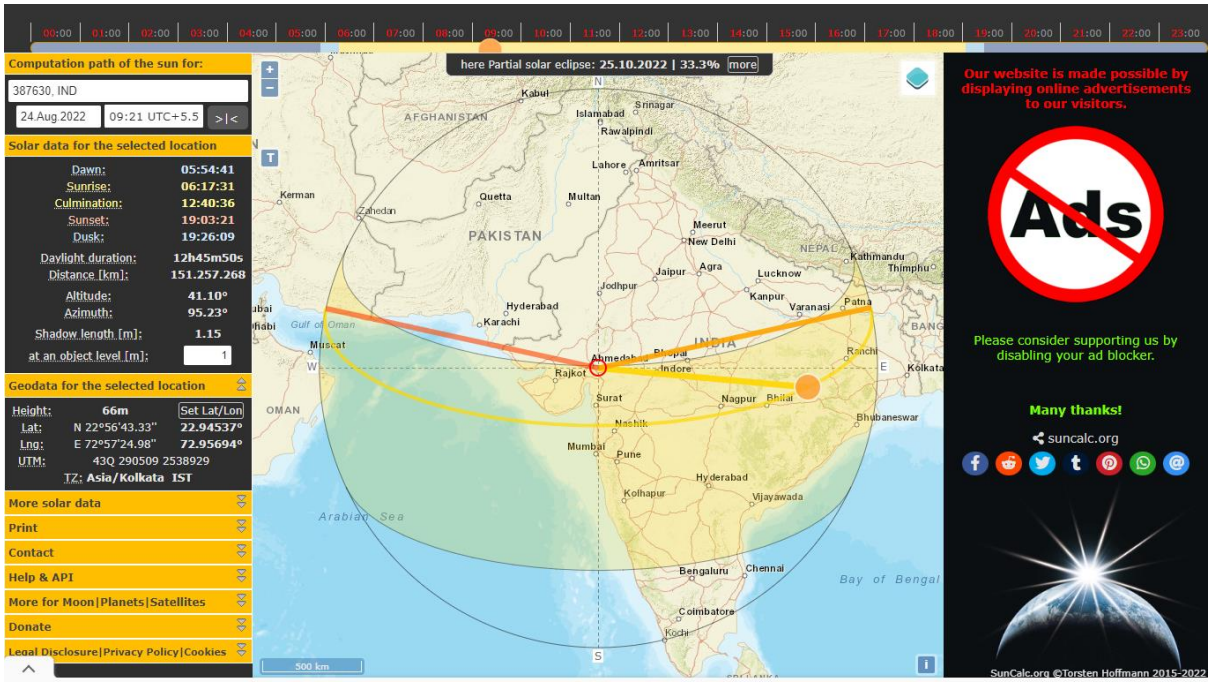


Figure 11 Suncalc

Analysis:

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

Task 6:- Exploring Exif Data Viewer

- **Exif Data Viewer :-** EXIF Data Viewer
- EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression.
- Almost all new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, F number, what metering system was used, flash, ISO number, date and time the image was taken, whitebalance, auxiliary lenses that were used and resolution.

Step 1: visit website Exif Data Viewer **:-** EXIF Data Viewer And upload image and you will get all data related to that image.

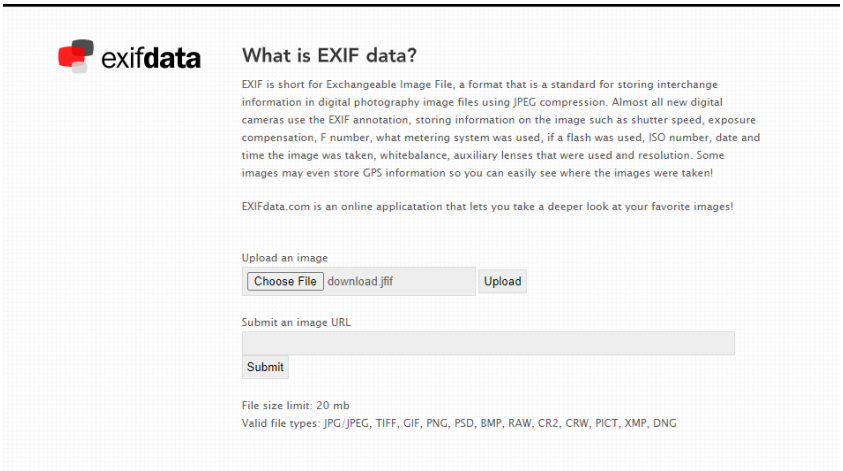


Figure 12 Exif Data Viewer

Figure 13 Exif Data Viewer

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

- Exif Tool is a free and open-source software program for reading, writing, and manipulating image, audio, video, and PDF metadata. It is platform independent, available as both a Perl library (Image::ExifTool) and command-line application. Exif Tool is commonly incorporated into different types of digital workflows and supports many types of metadata including Exif, IPTC, XMP, JFIF, GeoTIFF, ICC Profile, Photoshop IRB, FlashPix, AFCP and ID3, as well as the manufacturer-specific metadata formats of many digital cameras.

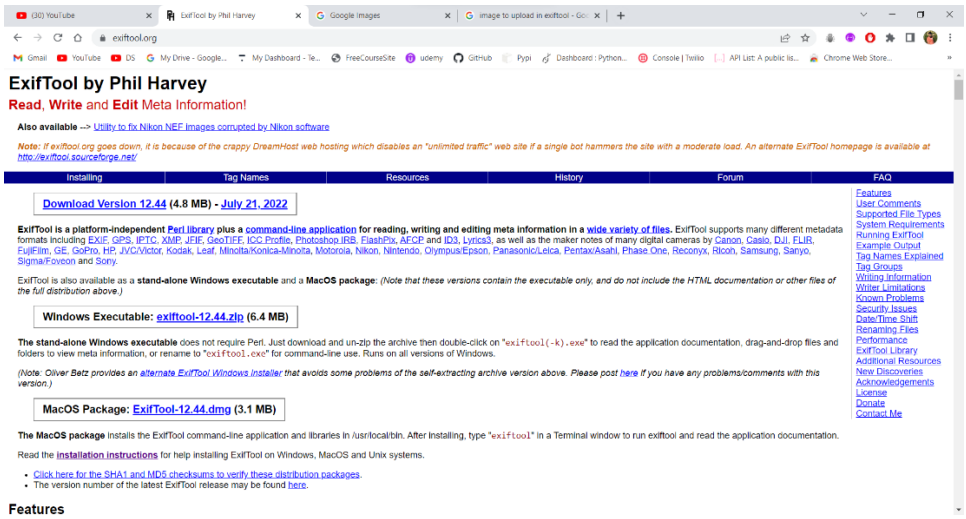


Figure 14 Exif tool

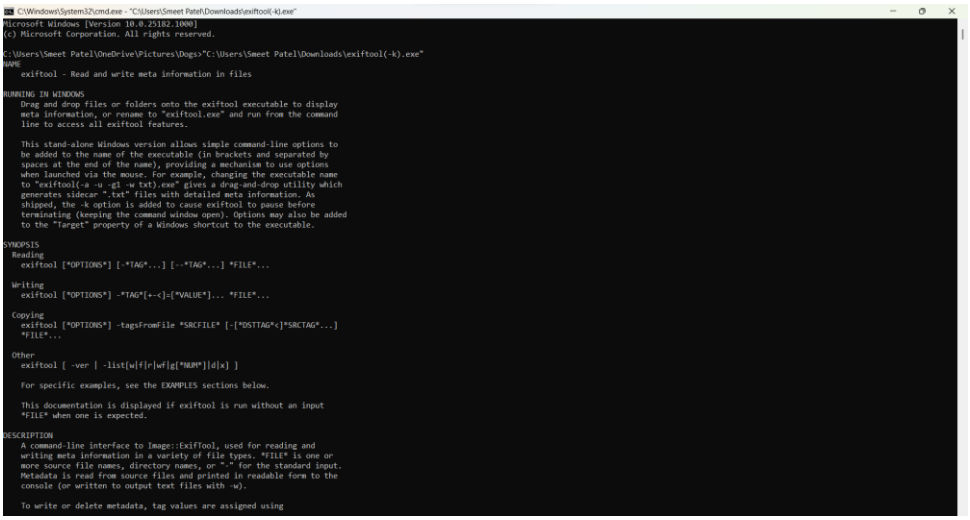


Figure 15 Exif tool

Analysis:

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

Identifying original and edited photo using forensically

1. **Magnification:** If we zoom the morphed image we can say that flowers are added in image.

Original:

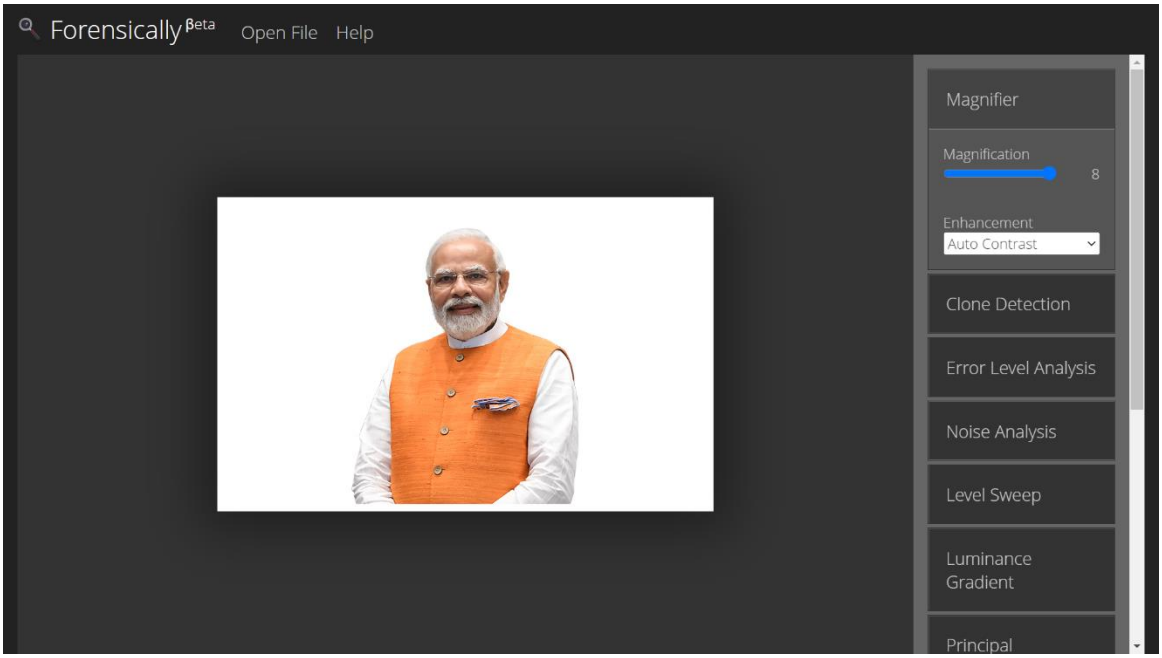


Figure 16 original image

Morphed:

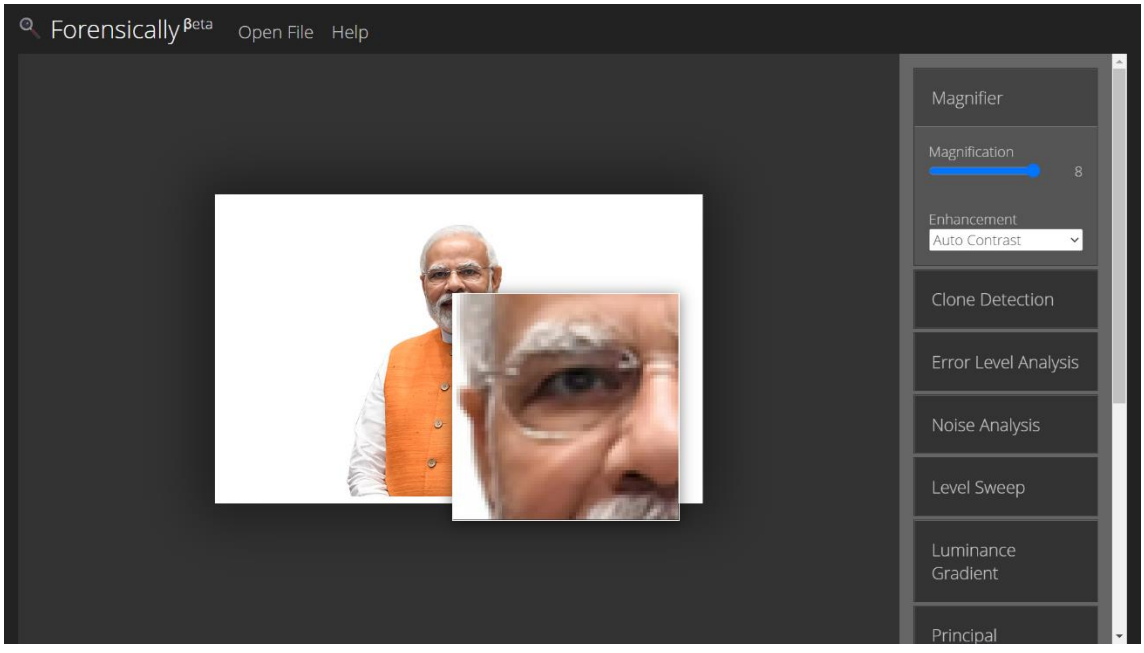


Figure 17 Morphed image

2. **Error Level Analysis:** if we set parameters of ELA same for both original and morphed photo you can easily classify the morphed photo.

Original:

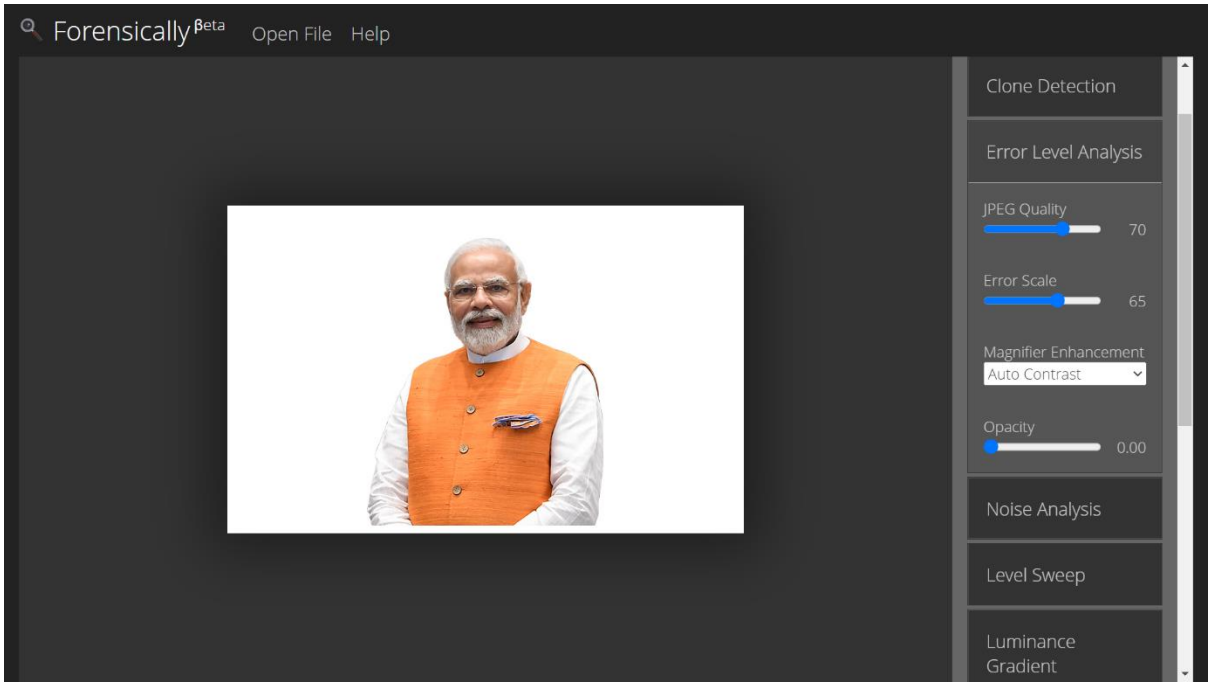


Figure 18 original image

Morphed:

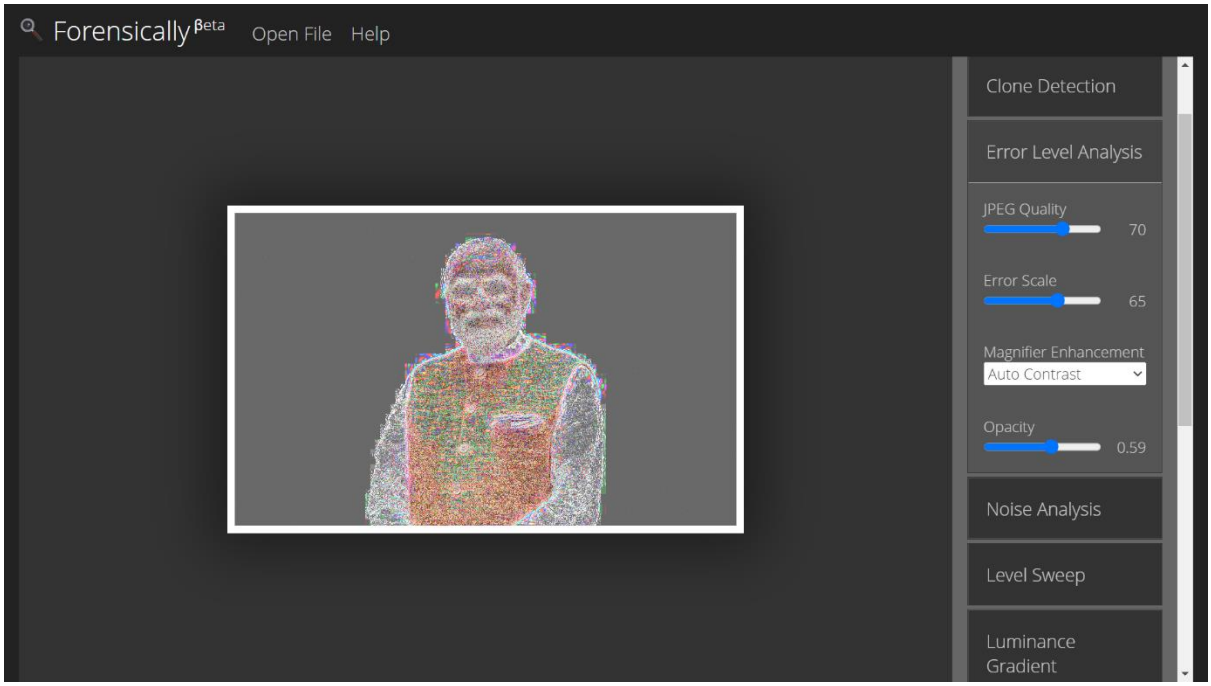


Figure 19 Morphed image

3. Noise Analysis: It is not that much helpful.

Original:

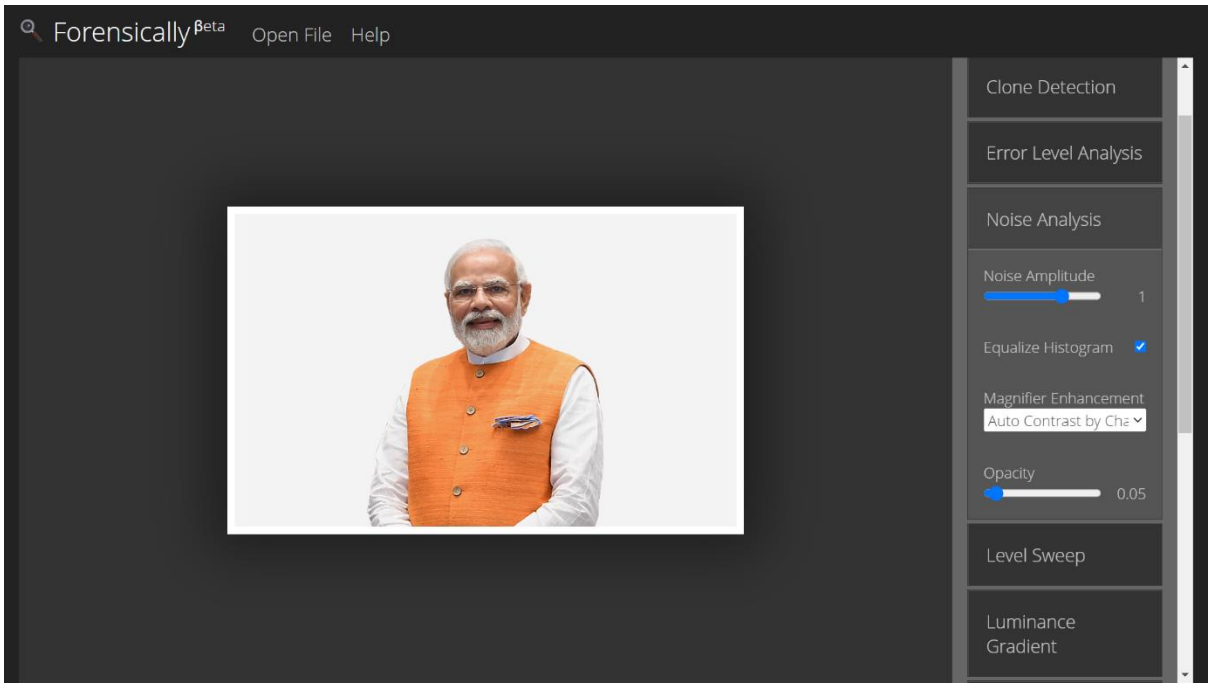


Figure 20 original image

Morphed:

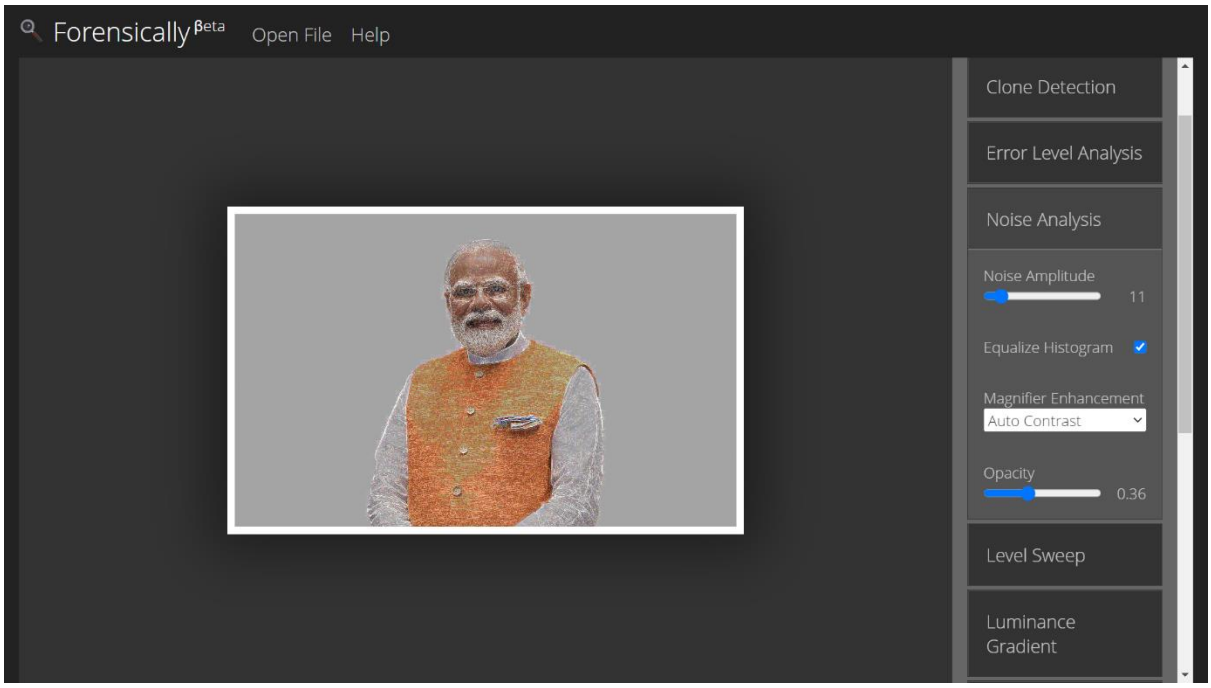


Figure 21 Morphed image

4.Meta Data: In original photo software is iOS 15.5 and in morphed photo software is Instagram.

Original:

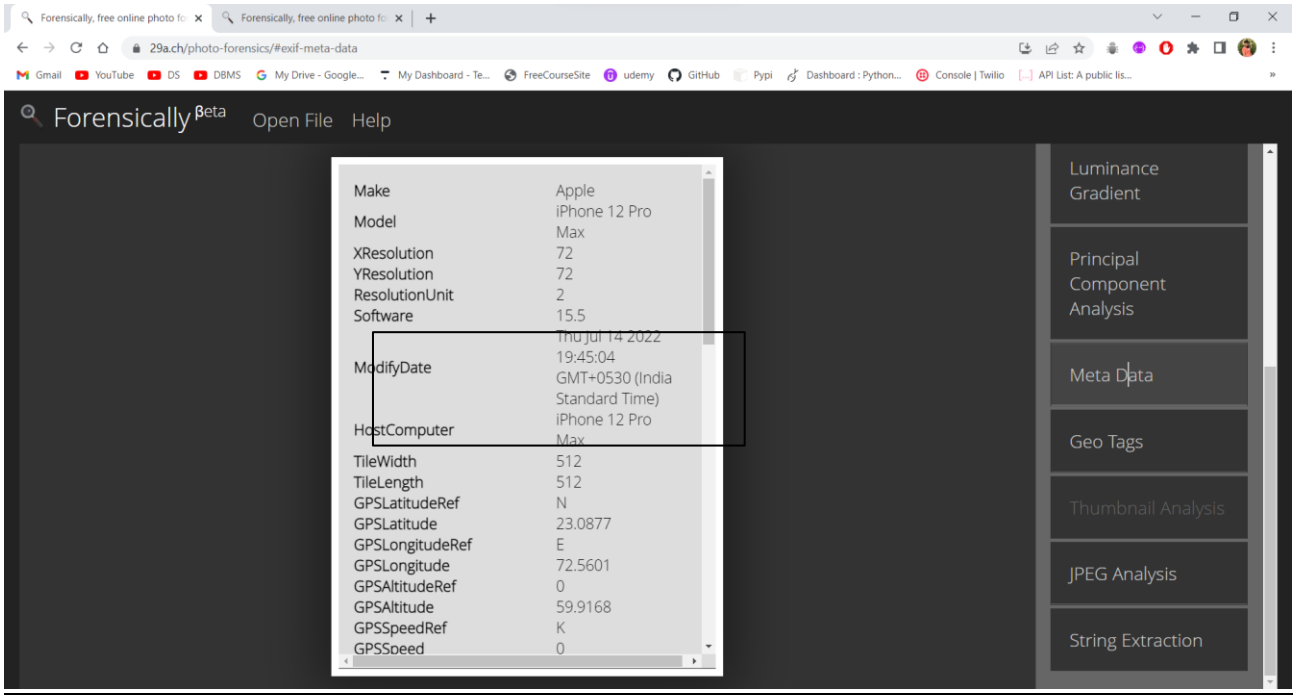


Figure 22 original image

Morphed:

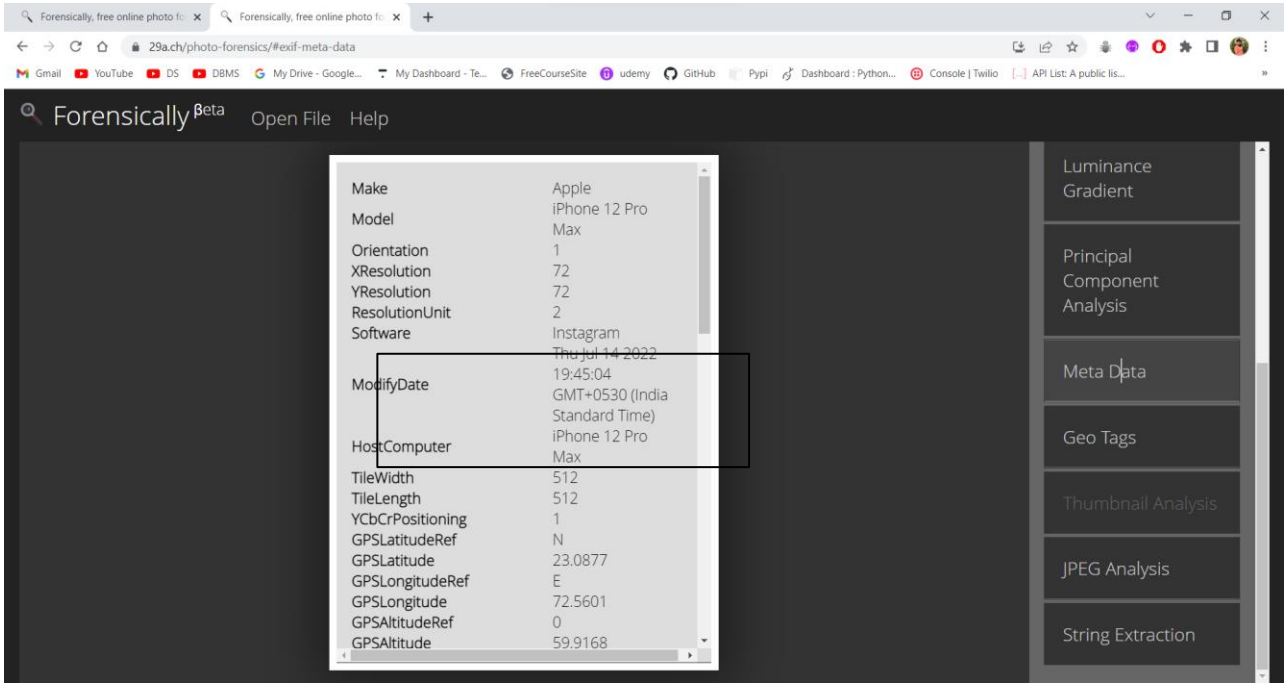


Figure 23 Morphed image

5. Geo Tags: I edited the photo from same location so details is same for both, but if some else has edited than the location maybe deferent.

Original:

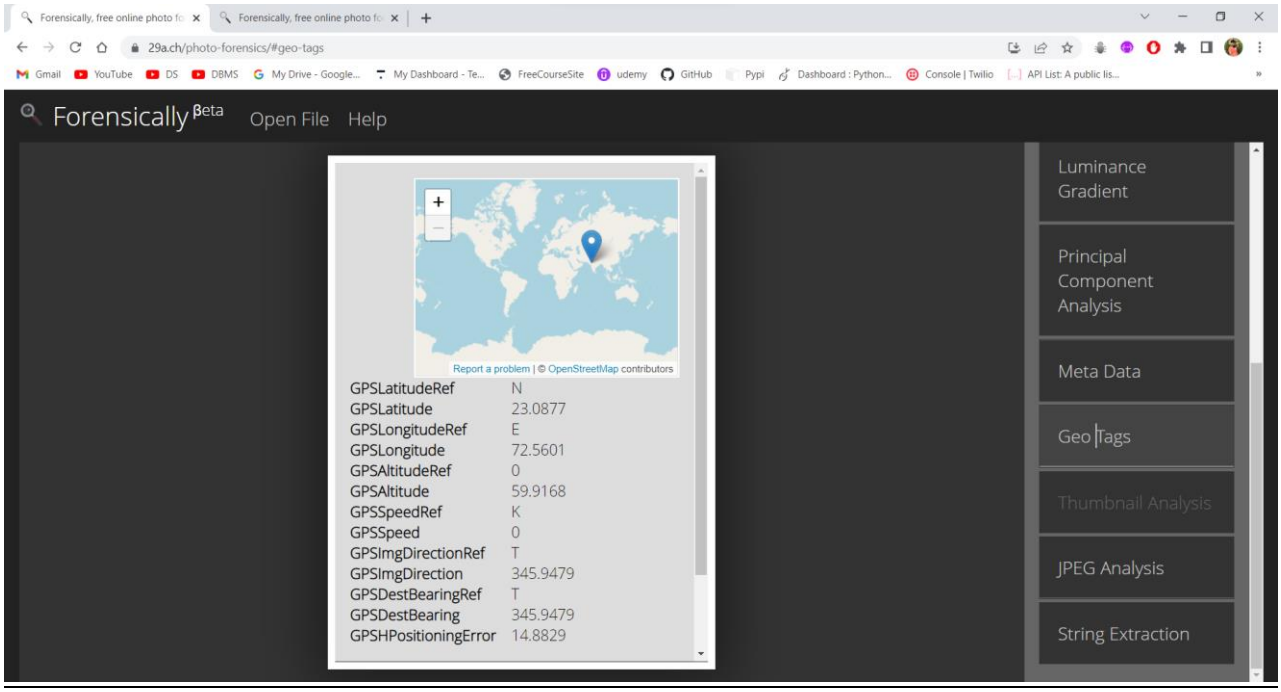


Figure 24 original image

Morphed:

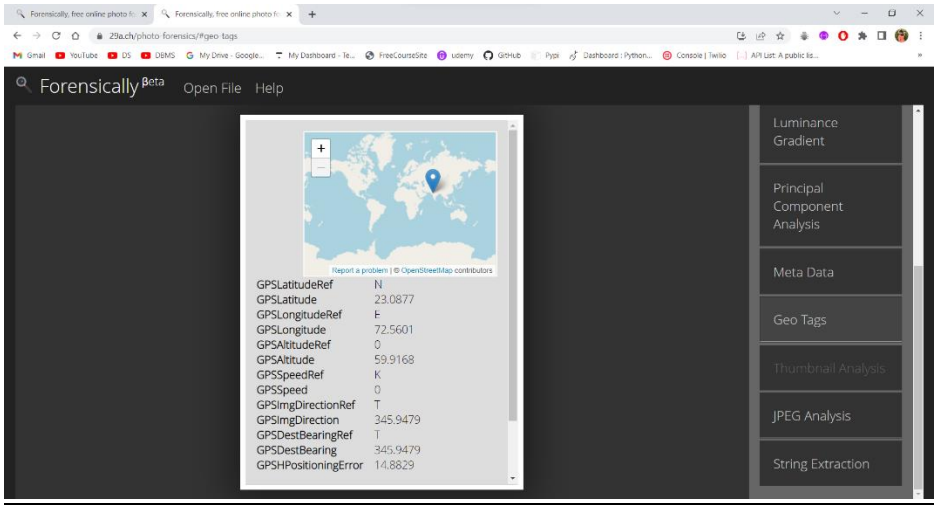


Figure 25 Morphed image

6. String Extraction:

Original:

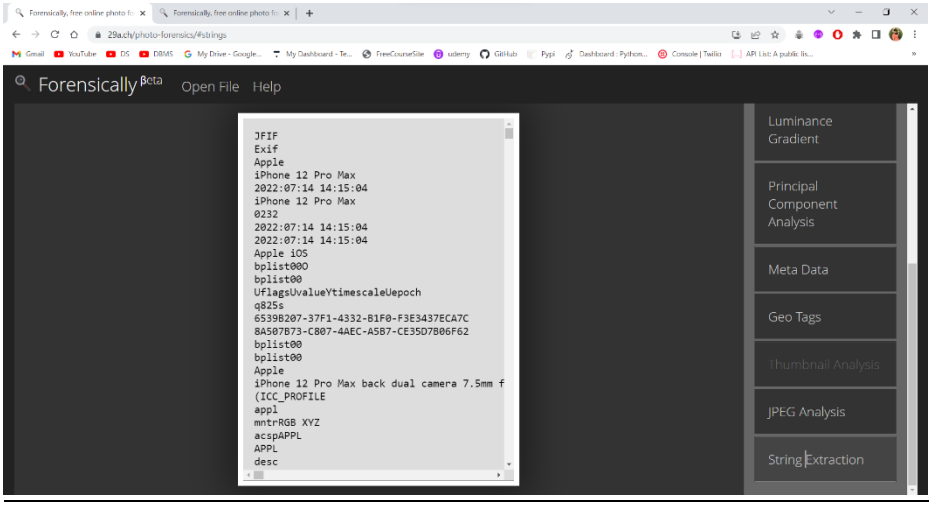


Figure 26 original image

Morphed:

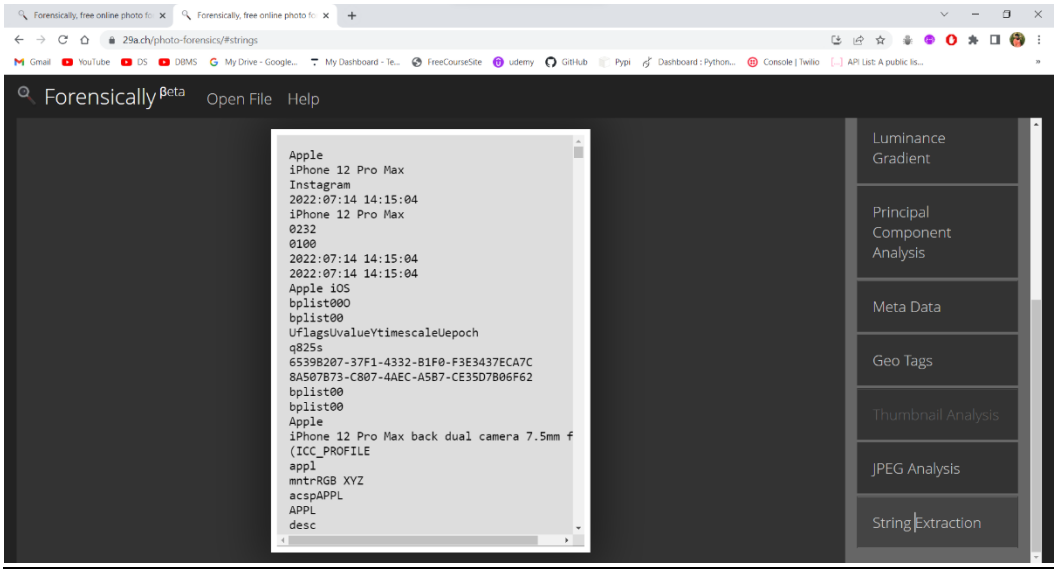


Figure 27 Morphed image

Conclusion:

1. We are using tool like forensically to Identifying original and edited photo.We are using YouTube metadata, Exif Data Viewer, Exif tool to find details or information related video or images. we are also using other like Suncalc and Pic2map

Digital Forensics Lab Report: 4

Date: 24-08-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

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

Tool Names:

1. **FreeMapTools :-** View and Edit Photo GPS Data (freemaptools.com)
2. **YouTube data viewer :-** Extract the tags from a Youtube Video (online-free-tools.com)
3. **Google image search :-** Google Images
4. **Tineye image search :-** **TinEye Reverse Image Search**
5. **Jeffrey exif viewer :-** Online Exif Viewer (exif-viewer.com)
6. **Foto forensic :-** FotoForensics
7. **DeepWare Website** :- https://scanner.deepware.ai/

Task 1 :- Exploring View and Edit Photo GPS Data tool :- FreeMapTools

- FreeMapTools :- View and Edit Photo GPS Data (freemaptools.com)
- An online resource that enables visitors to easily and quickly use maps in order to measure, search and overlay mark-up elements on maps for a wide range of useful applications.

Steps:

1. Visit FreeMapTools :- View and Edit Photo GPS Data (freemaptools.com)

Figure 1 View and Edit Photo GPS Data tool :- FreeMapTools

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

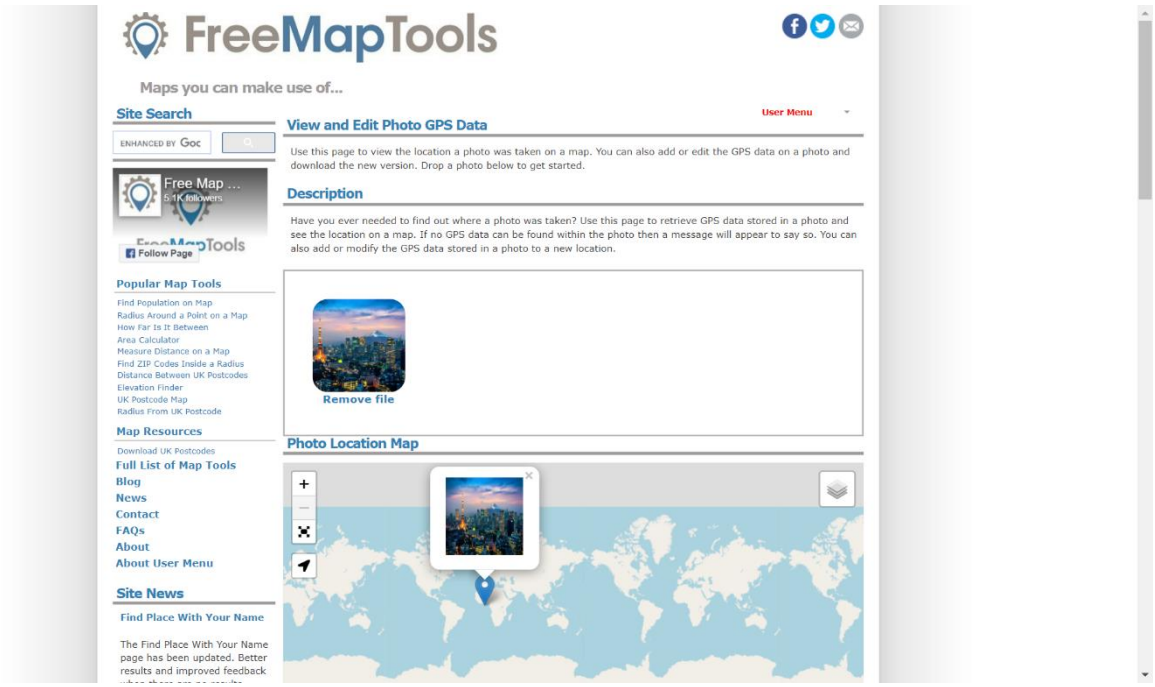


Figure 2 View and Edit Photo GPS Data tool :- FreeMapTools

Analysis:

1. We are using Free Map Tools 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 2:- Exploring and viewing YouTube data viewer

- YouTube data viewer :- Extract the tags from a Youtube Video (online-free-tools.com)

- The YouTube Data Viewer is a web-based video verification tool offered through The Citizen Evidence Lab, created by Amnesty International. Users input a YouTube URL, and the tool outputs information about the video that is helpful in verifying a video. This includes upload time and thumbnails that can be used for reverse image searching.

Steps:

1. **Visit YouTube data viewer :- Extract the tags from a Youtube Video (online-free-tools.com)**
2. Upload youtube video link to know information as a result you will get all data

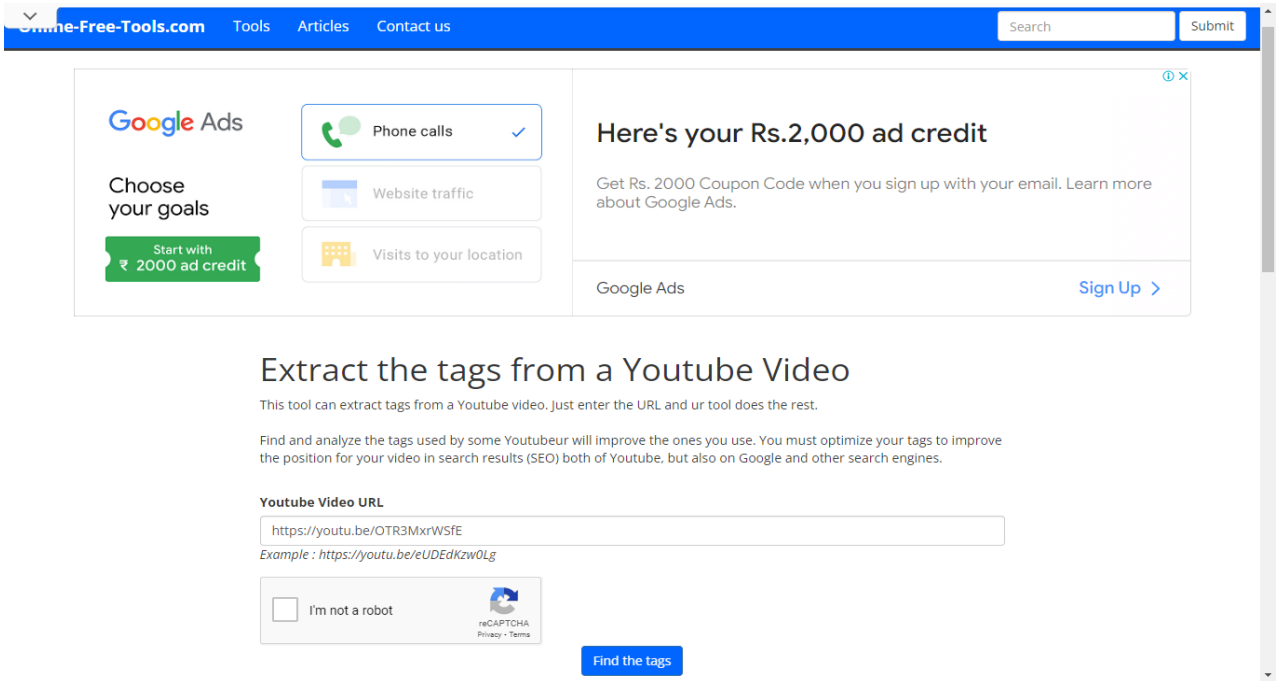


Figure 3 YouTube data viewer

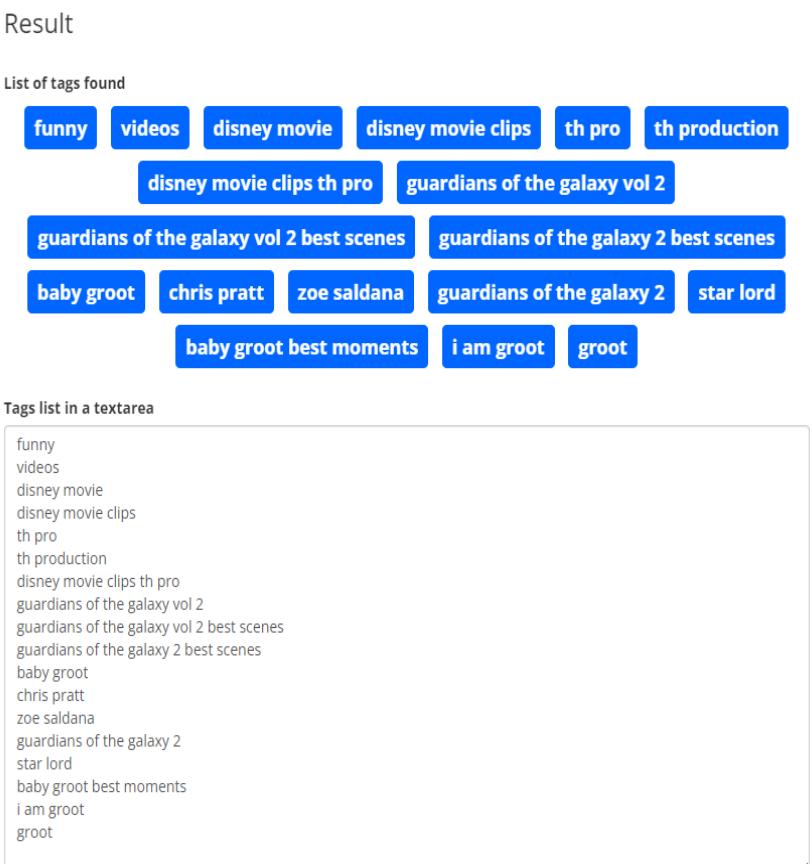


Figure 4 YouTube data viewer

Analysis:

1. We are using You Tube data viewer to know information related that video.
2. Using this tool we are able to extract all the tag related to that video

Task 3 :- Exploring Google image search

- Google image search :- Google Images
- Google reverse image search, officially called Google Search by Image, is a service provided by Google that allows a user to search for images using an image as the starting point, rather than a written or spoken search query.

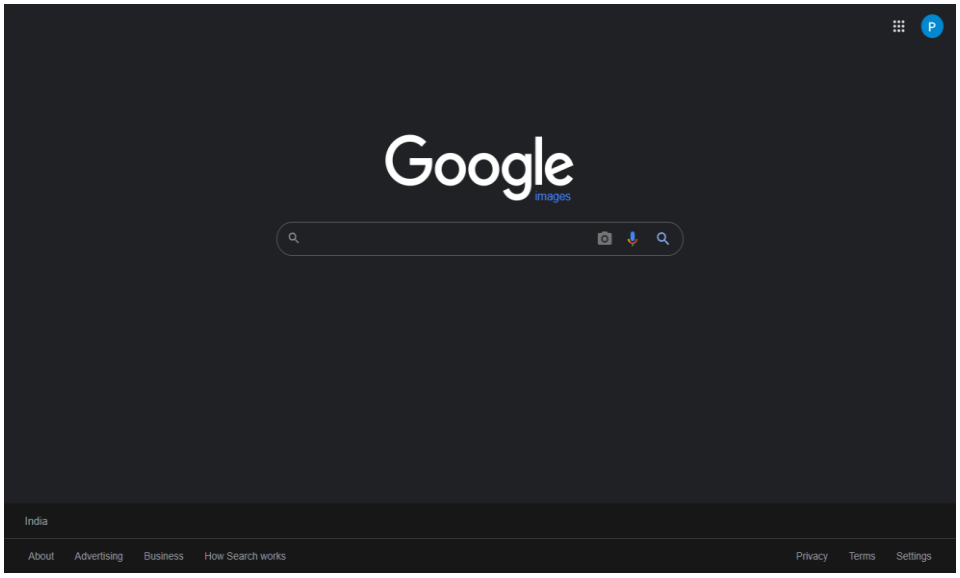


Figure 5 YouTube data viewer

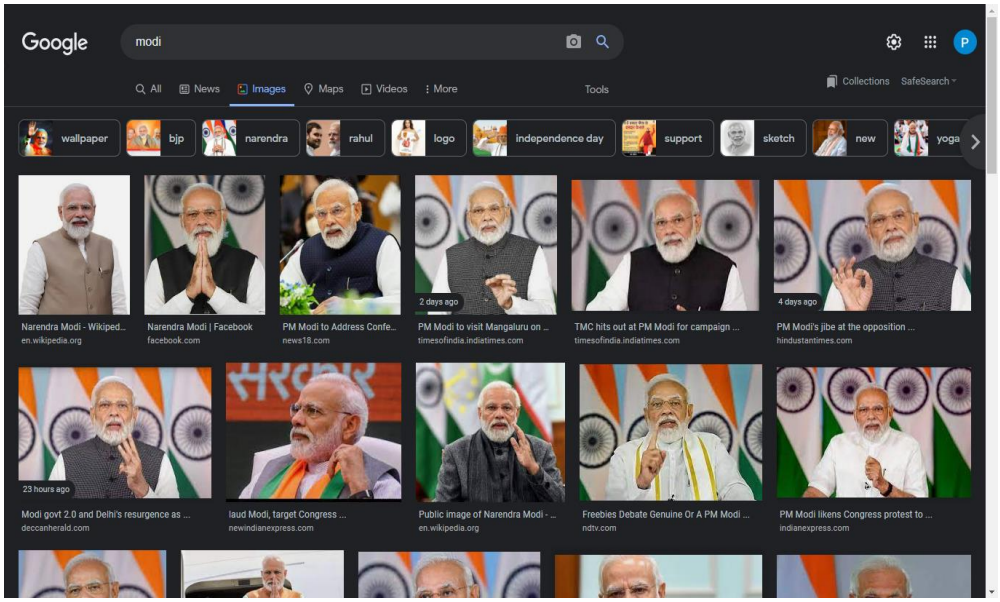


Figure 6 YouTube data viewer

Analysis:

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

Task 4:- Exploring Tineye image search :-

- Tineye image search :- TinEye Reverse Image Search

- TinEye is the original reverse image search engine, using image recognition with a growing index of billions of images. You can use TinEye to find out where an image came from, how it is being used, if modified versions of the image exist, or to find a higher resolution version.

Steps: -

1. Visit Tineye image search :- TinEye Reverse Image Search

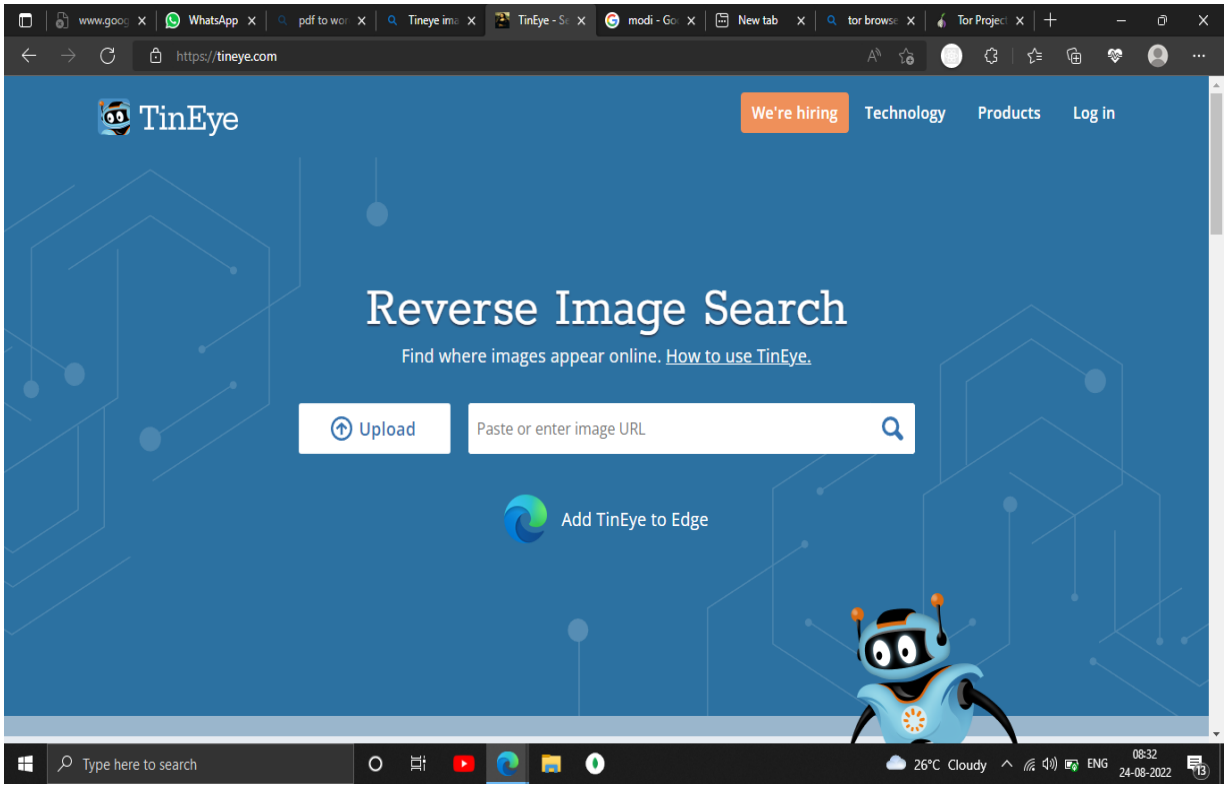


Figure 7 Tineye image search

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

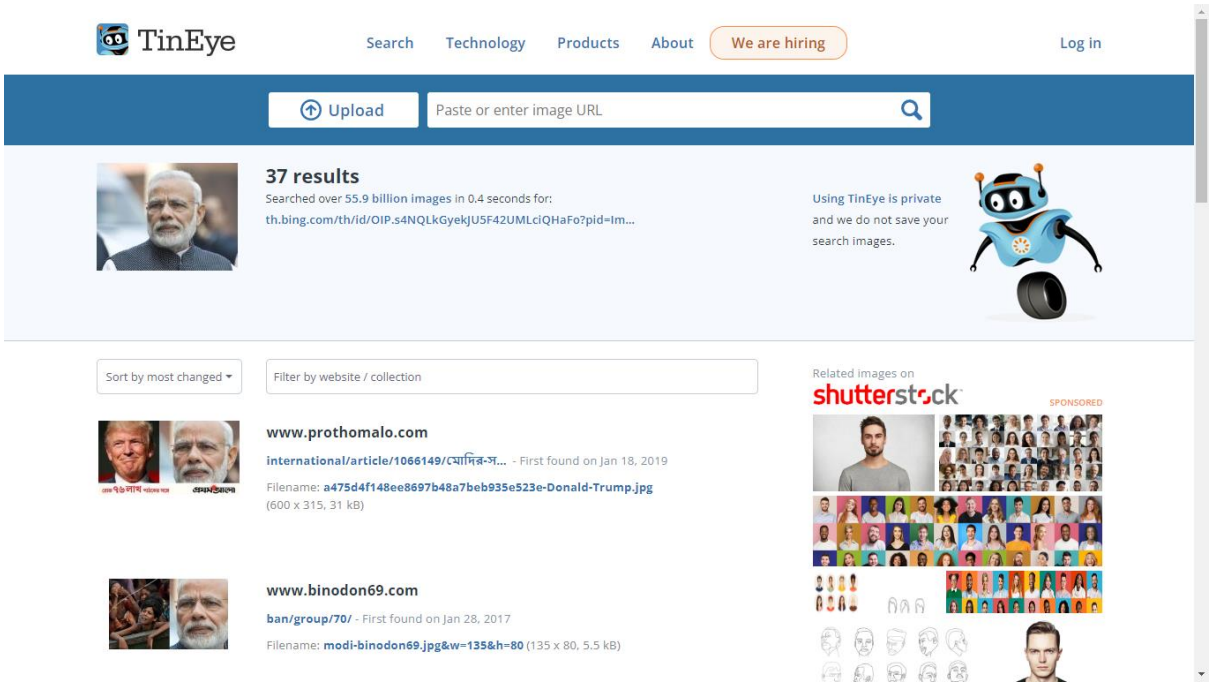


Figure 8 Tineye image search

Analysis:

1. We are using Tin Eye to get original source of images and possible website where we can find this image.
2. We are using modi images as our input source and we get all possible website which are using this image.

Task 5:- Exploring Jeffrey exif viewer

- Jeffrey exif viewer :- Online Exif Viewer (exif-viewer.com)
- Jeffrey's Image Metadata Viewer is an online tool for viewing image metadata or exchangeable image file format (EXIF) data such as date, time and location information, camera settings and thumbnails. The tool is free tu use and does not require subscription or payment.

Steps:-

1. Visit jeffrey exif viewer :- Online Exif Viewer (exif-viewer.com)

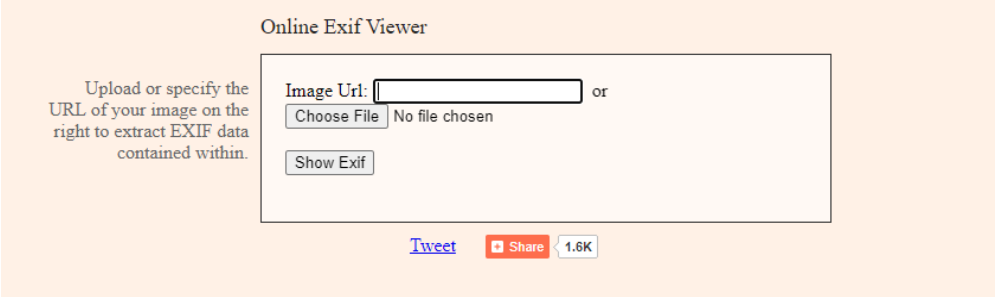


Figure 9 Jeffrey exif viewer

2. Upload images which you want to know information and as result you will get all possible info.

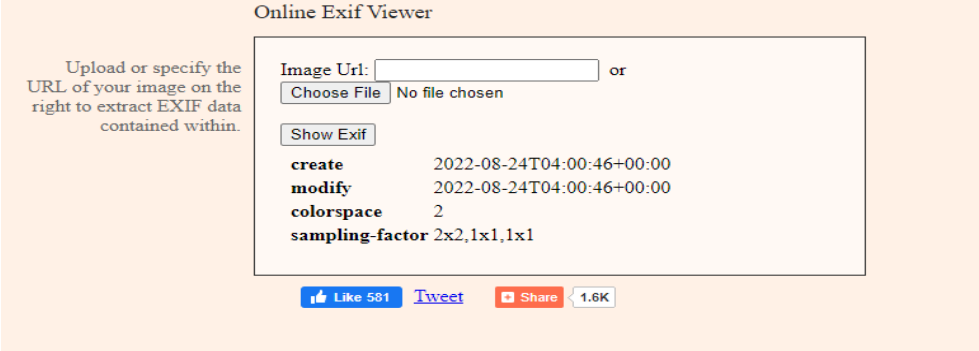


Figure 10 Jeffrey exif viewer

Analysis:

1. We are using jeffrey exif viewer to get info related to imgaes. We get information like as date, time and location information, camera settings and thumbnails.

Task 6:- exploring Foto forensic

- Foto forensic :- FotoForensics
- FotoForensics provides budding researchers and professional investigators access to cutting-edge tools for digital photo forensics. FotoForensics is designed and organized for rapid analysis. With a little experience, an analyst should be able to evaluate a picture in minutes.

Step 1: visit Foto forensic :- FotoForensics

Figure 11 Foto forensic

Step 2:Upload images and press search Butten an you will get result

Figure 12 Foto forensic

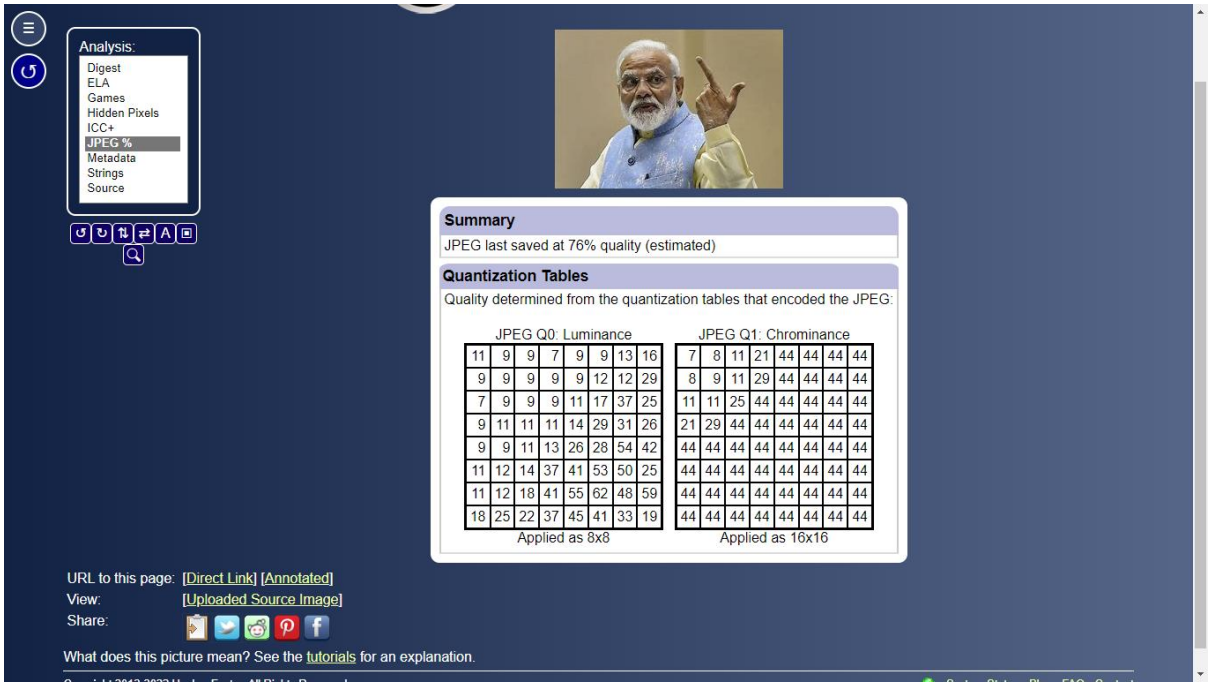


Figure 13 Foto forensic

Analysis:

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

Task 7:- exploring DeepWare

- DeepWare Website :- https://scanner.deepware.ai/

- Deepware, created by Zemana, develops deepfake detection technology designed to detect deepfake videos or, simply, any fake content in the areas of visual and audio communication. The company's cloud-based solution can scan a suspicious video to find out if it is synthetically manipulated.

Step:

1. Visit DeepWare Website :- https://scanner.deepware.ai/

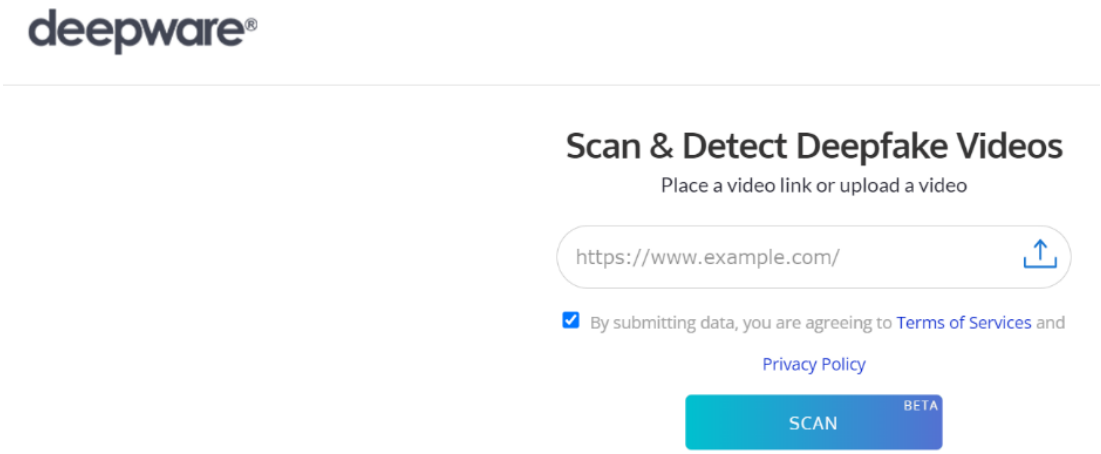


Figure 14 DeepWare

2. Upload Images into deepware to check your image is real or not as result it will show in blow image.

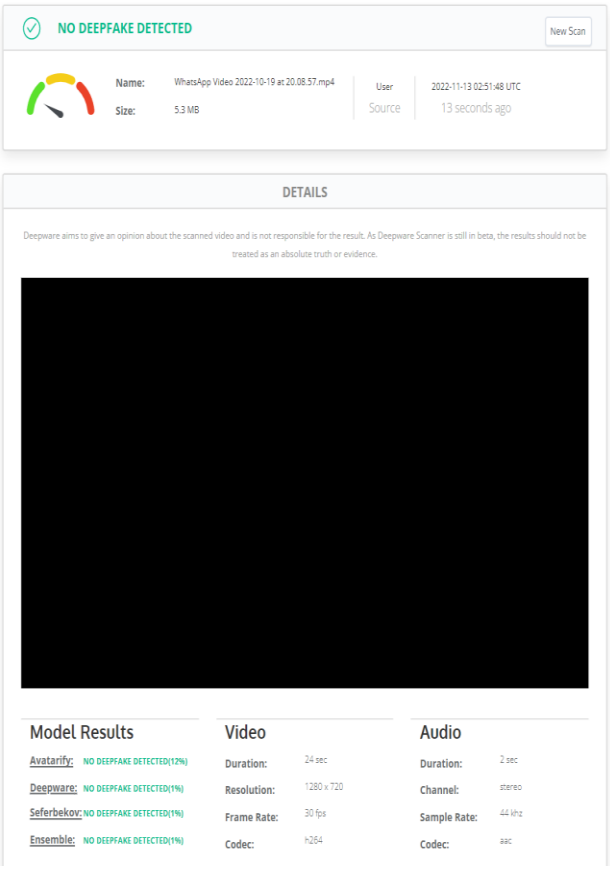


Figure 15 deepWare

Analysis:

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

Conclusion:

1. We are using tool like Free Map Tools, YouTube data viewer, Google image search, Tin Eye Reverse Image Search, Jeffrey exif viewer, Foto forensic, Deep Ware Website to identity if imago or video are face or not and also use to find related data and image to original image.

Digital Forensics Lab Report: 5

Date: 10-08-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
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: Explore blogs, forums, wiki, email services, financial services, file uploader, security etc

Steps for Installation of Tor browser:

1. Go to https://www.torproject.org/download/ and download the .exe file.
2. Install the Tor browser and connect it to the Tor Network.

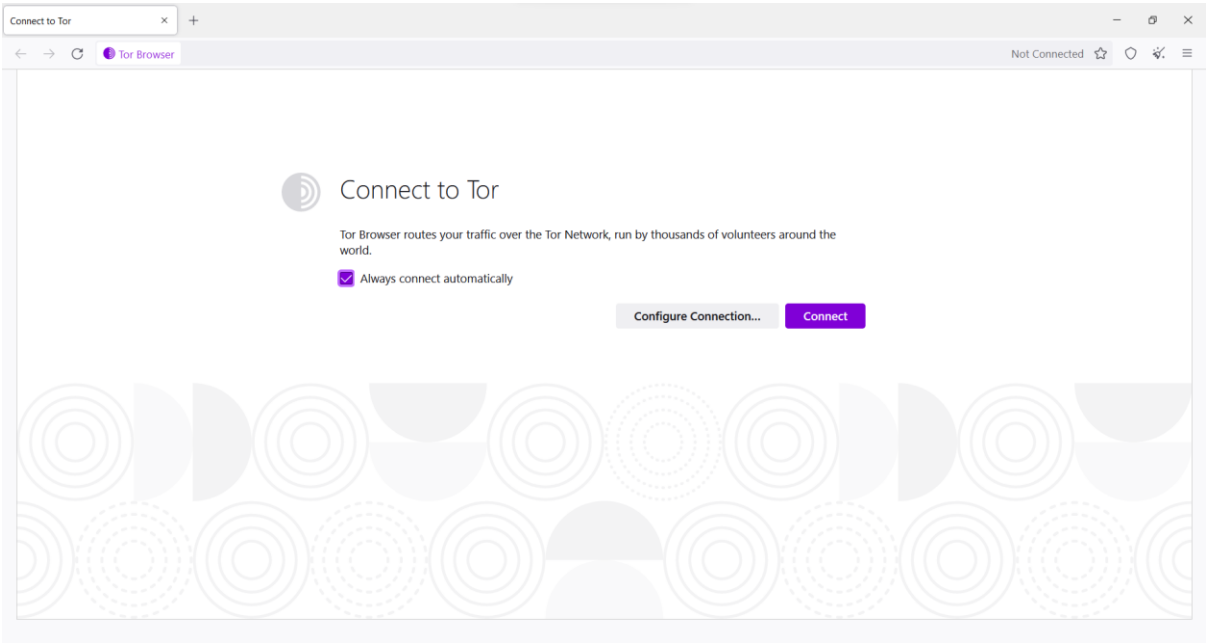


Figure 1 Tor browser

3. Go to the “Hidden Wiki” site.

Task 1 :- Exploring and Analyzing Blog:

1. Darknetlive:http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion/

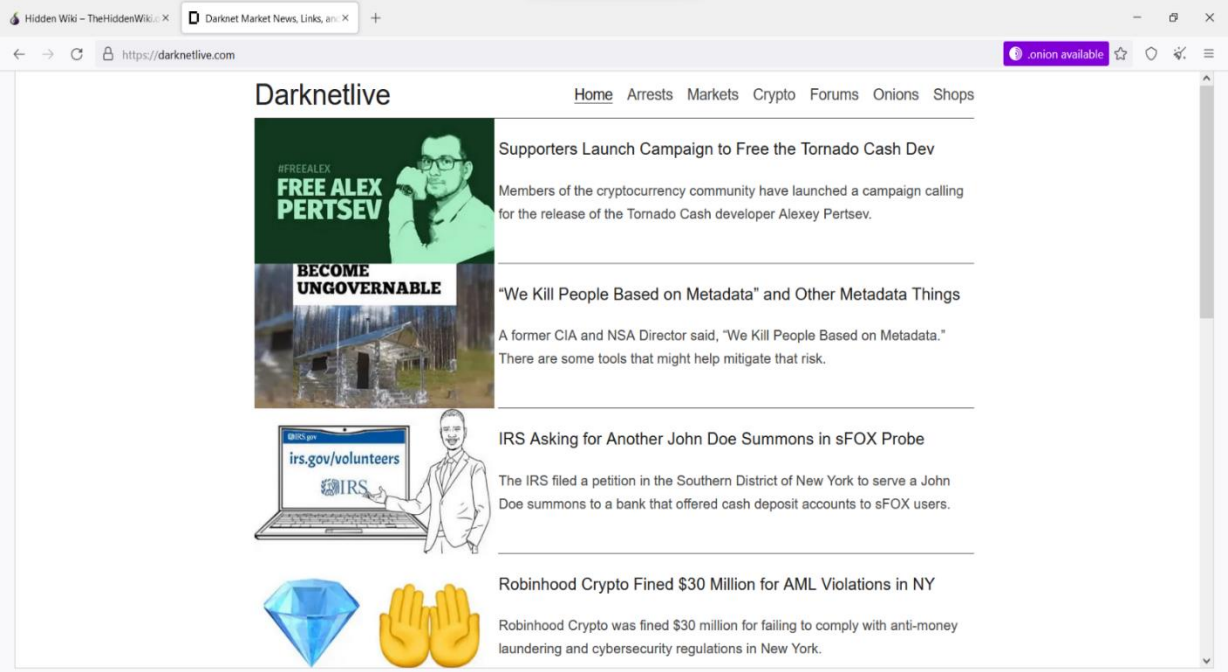


Figure 2 Blog on Darknet (Darknetlive)

2. Flashlight:http://ovgl57qc3a5abwqgdhdtssvmydr6f6mjz6ey23thwy63pmbxqmi45iid.onion/

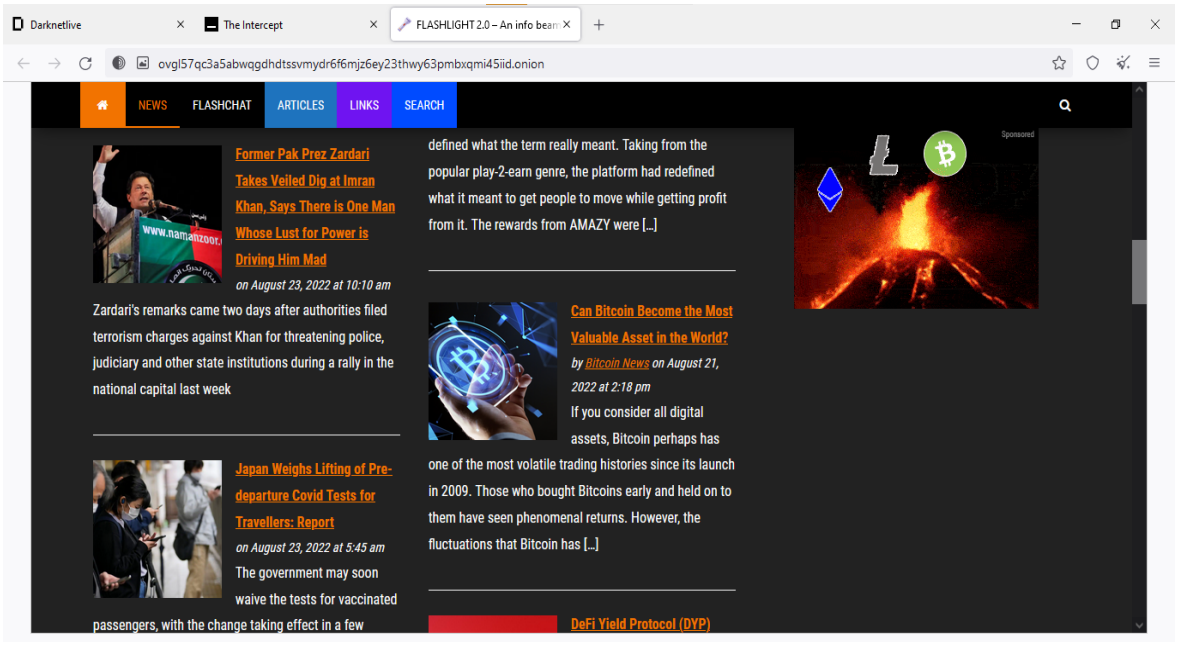


Figure 3 Flashlight

3. Intercept: https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion/

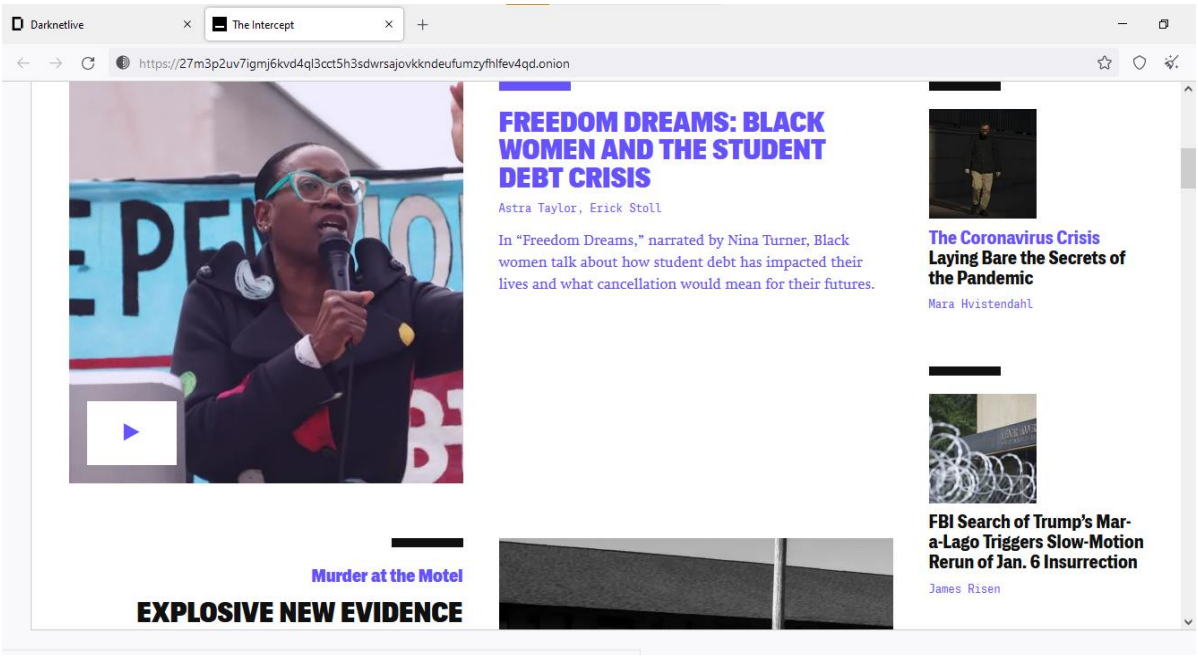


Figure 4 Blogs on Darknet(Intercept)

4. http://xjfbpuj56rdazx4iolylxplbvyft2onuerjeimlcqwaihp3s6r4xebqd.onion/category/txt/blog/

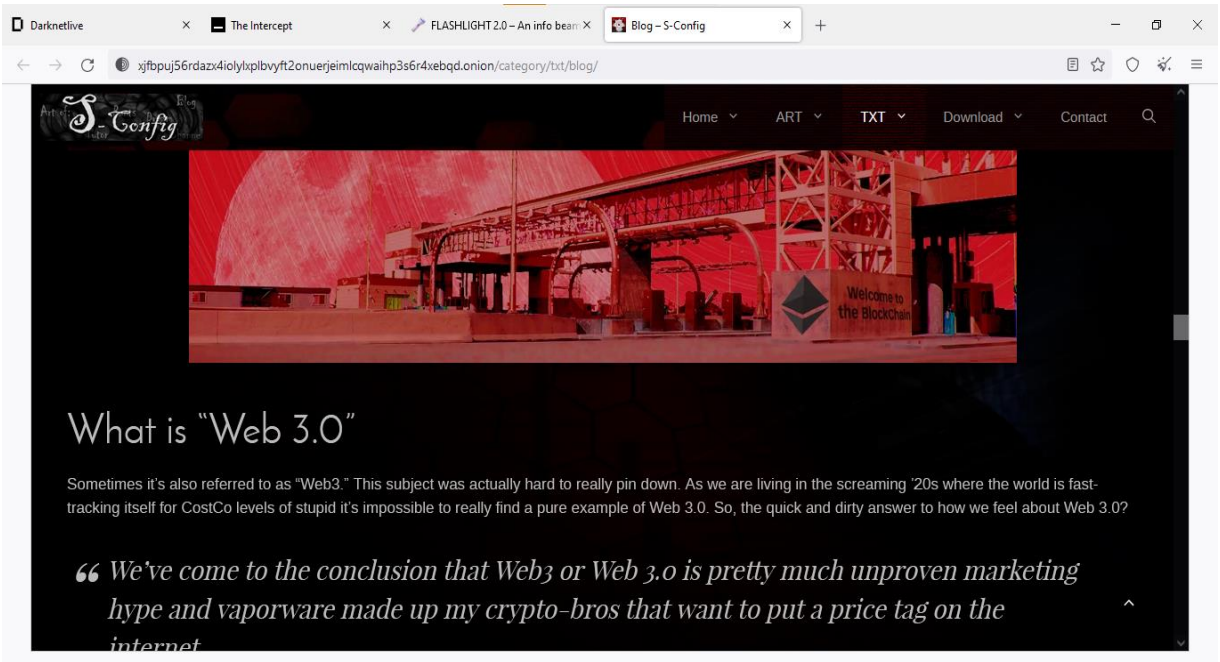


Figure 5 Blog website on Darknet

Task 2 :- Exploring and Analyzing Forums

1. http://ylmjp76zk4ndvgpncbtgzrfsrzpblvlzgtuoduqgygwdlexou64iwfqd.onion/

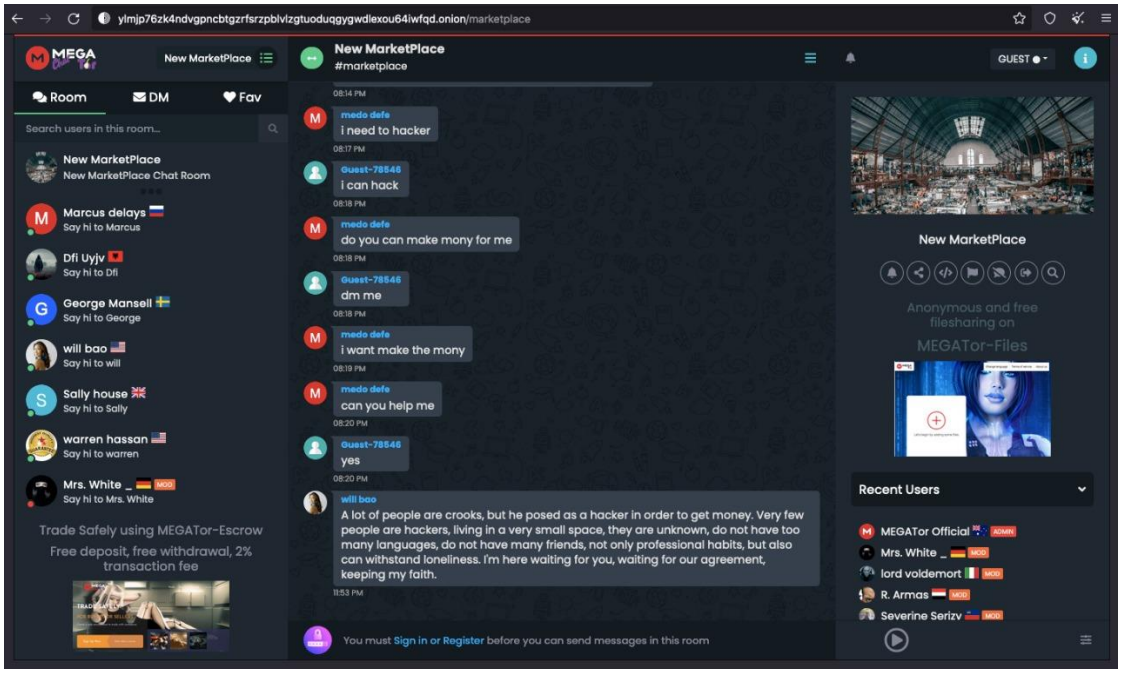


Figure 6 Forums on Darknet

2. http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/d/EnergyControl

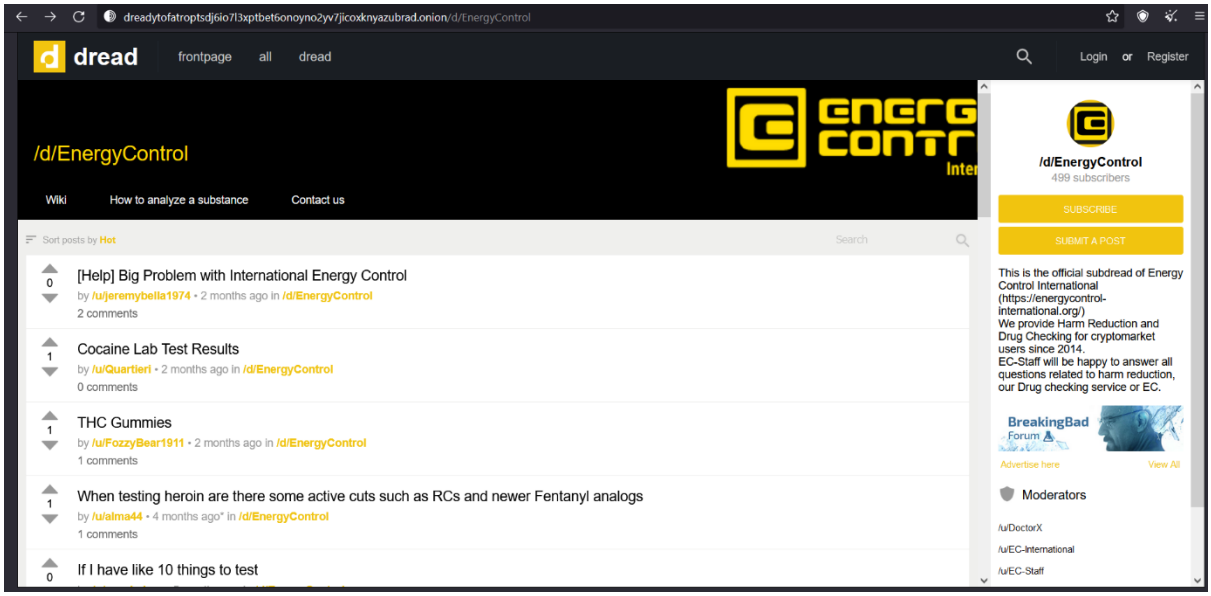


Figure 7 Forums on Darknet

3. http://4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/hispol/

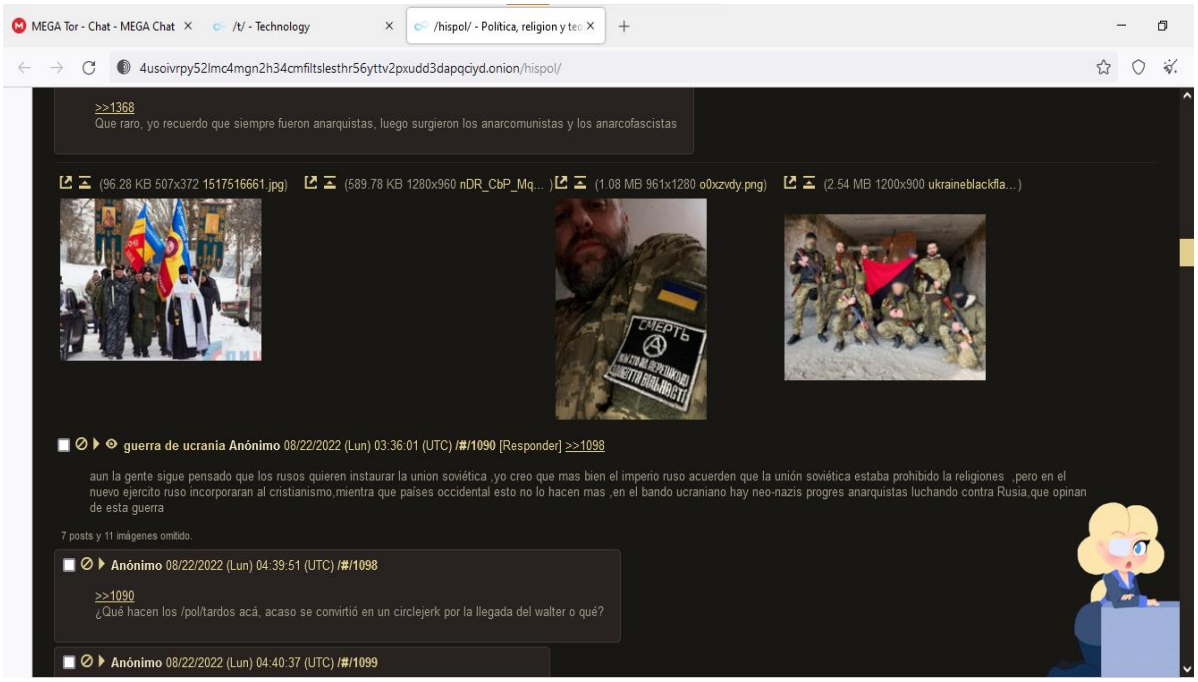


Figure 8 Forums on Darknet

http://4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/t/

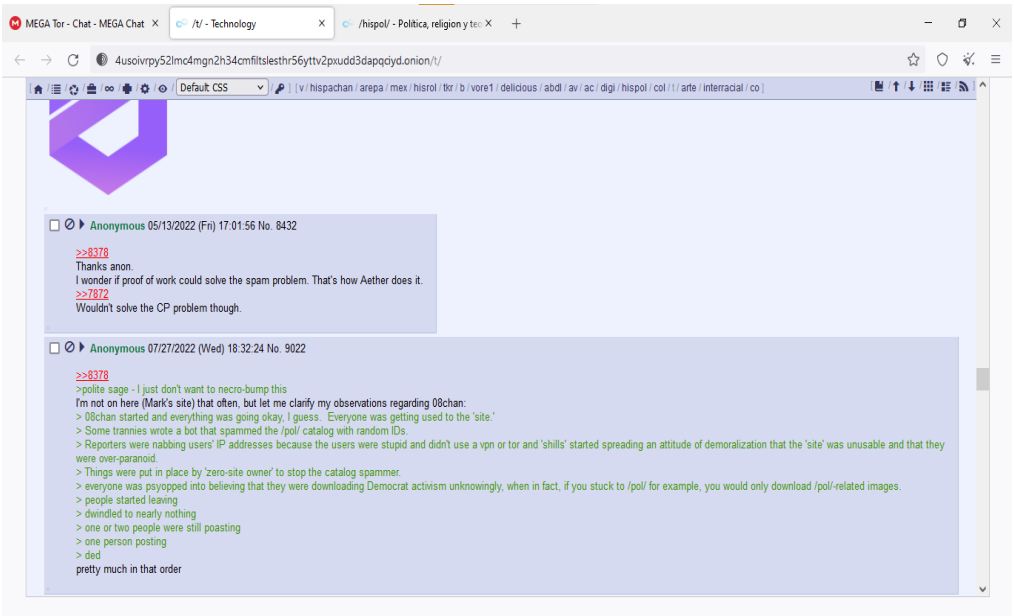


Figure 9 Forums on Darknet

Task 3 :- Exploring and Analyzing File Uploaders:

1. http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/directory/al-jazeera/

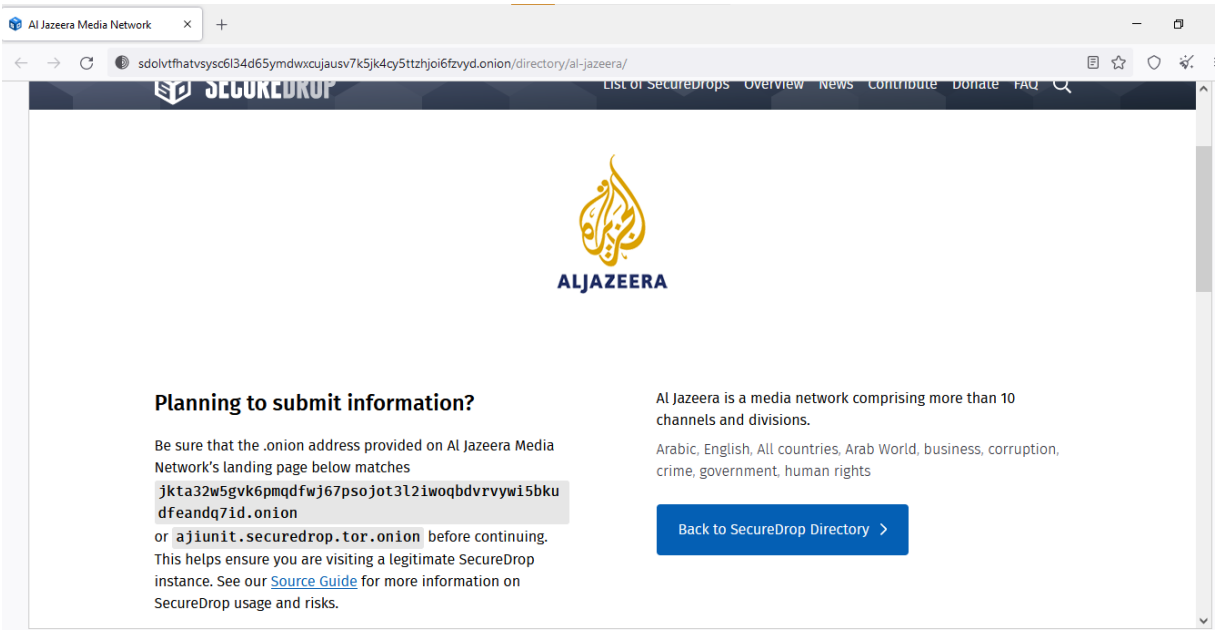


Figure 10 File Uploaders on Darknet(Aljzeera)

2. http://artistzubelolngubx6pmd6w2xacl3yj7jllxjdnrhh7assk7ioevjad.onion/

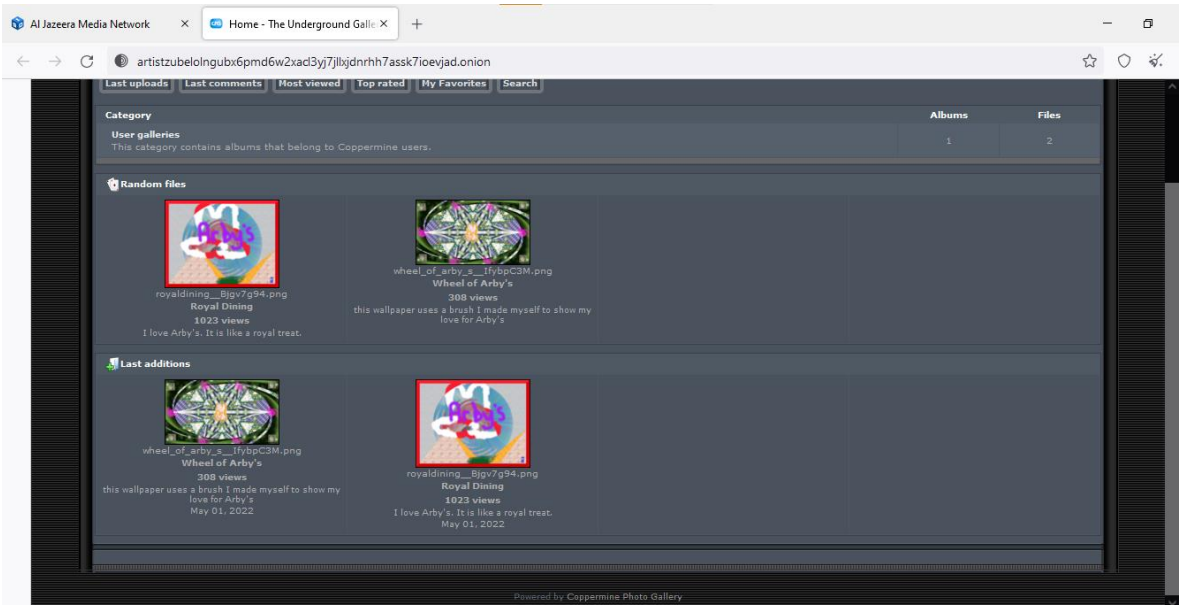


Figure 11 File Uploaders the underground gallery

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

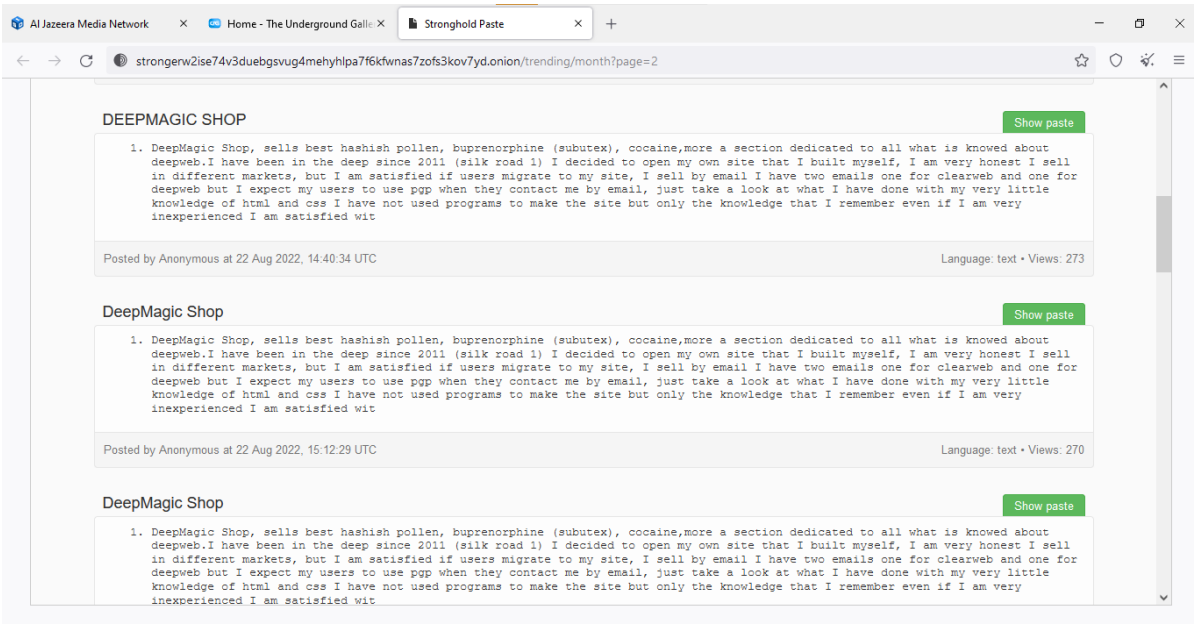


Figure 12 File Uploaders stronghold paste

4. http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/directory/guardian/

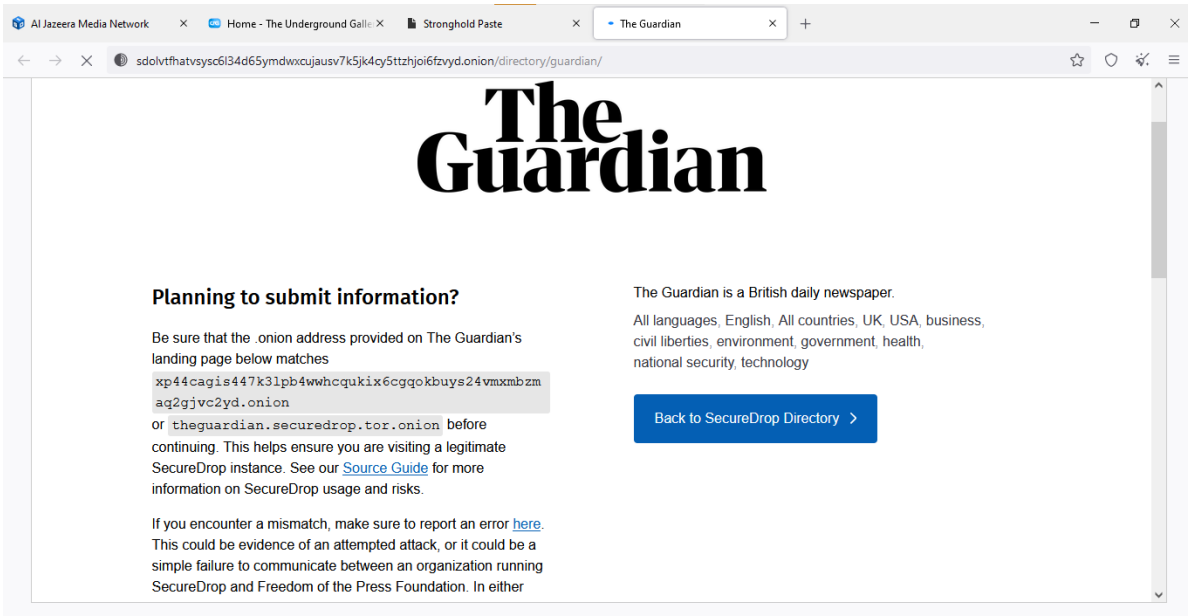


Figure 13 File Uploaders The Guardian

Task 4 :- Exploring and Analyzing Wiki:

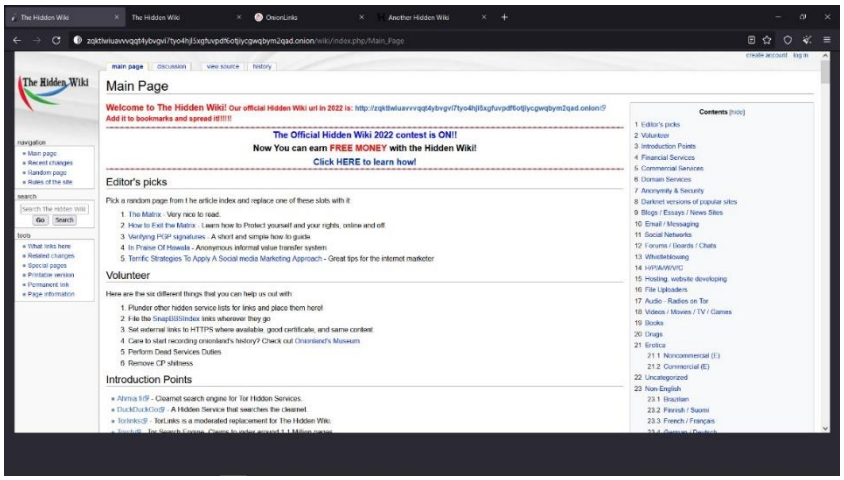


Figure 14 Exploring and Analyzing Wiki

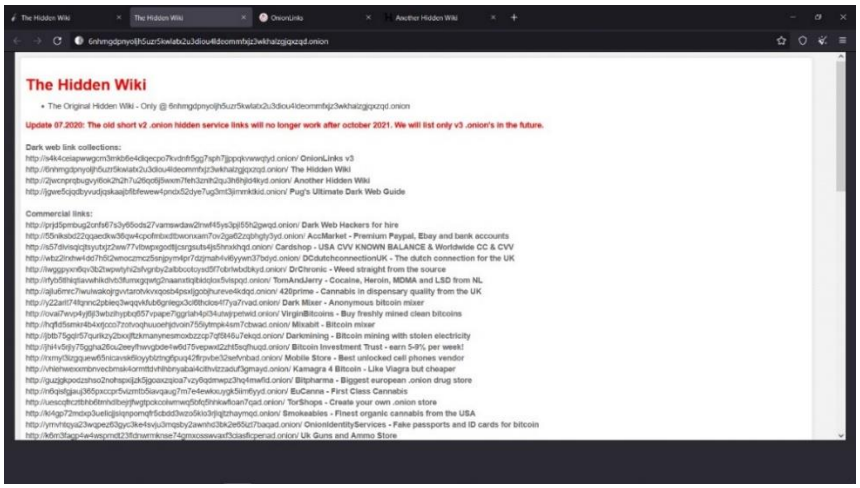


Figure 15 Exploring and Analyzing Wiki:

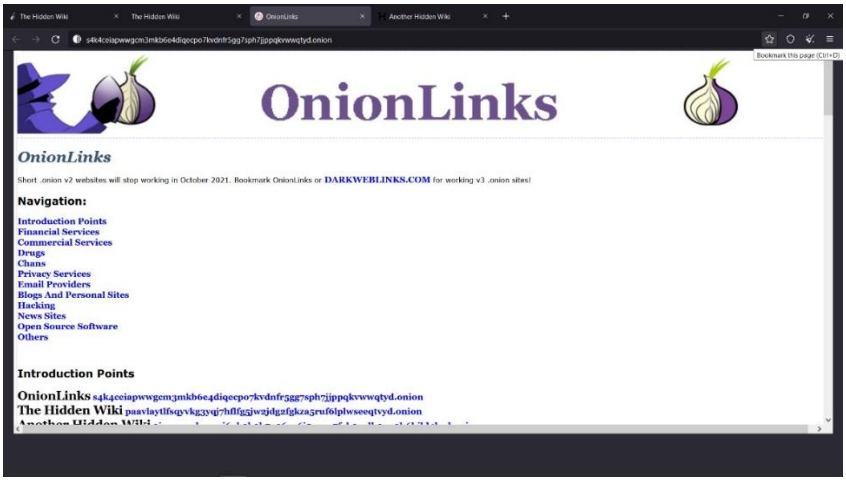


Figure 16 Exploring and Analyzing Wiki:

Task 5 :- Exploring and Analyzing Financial Services:

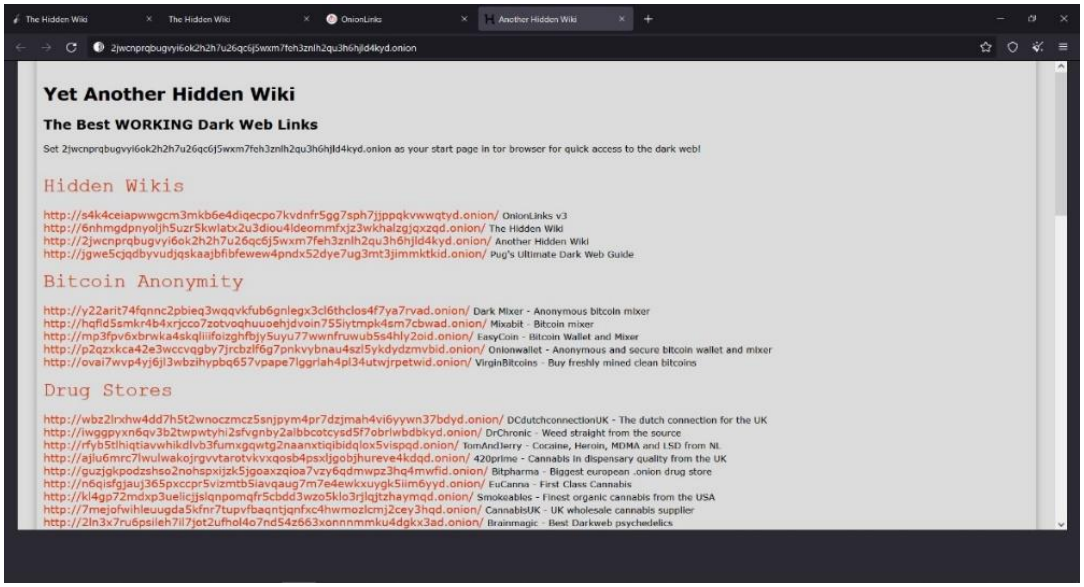


Figure 17 Exploring and Analyzing Financial Services

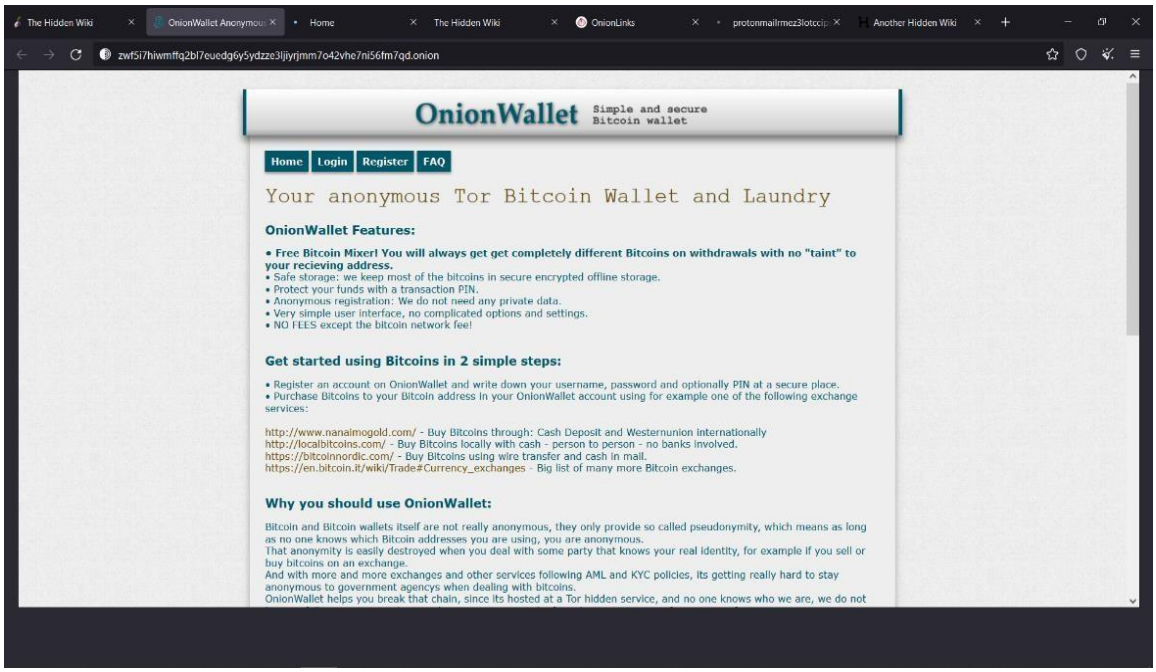


Figure 18 Exploring and Analyzing Financial Services

Task 6 :- Exploring and Analyzing Email Service:

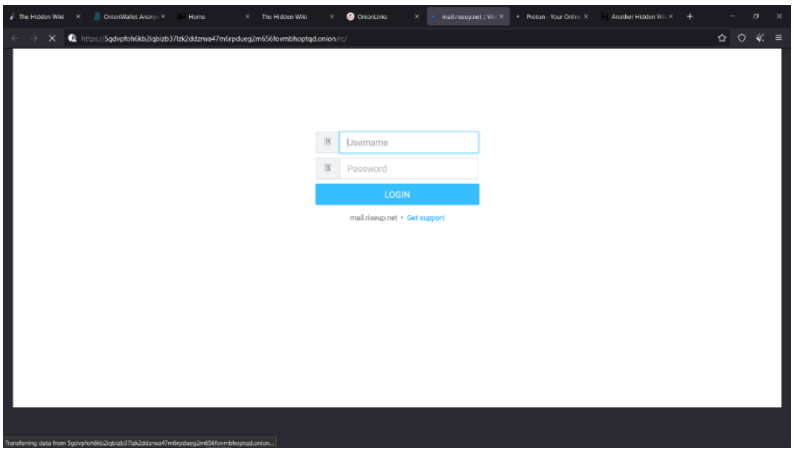


Figure 19 Exploring and Analysing Email Service

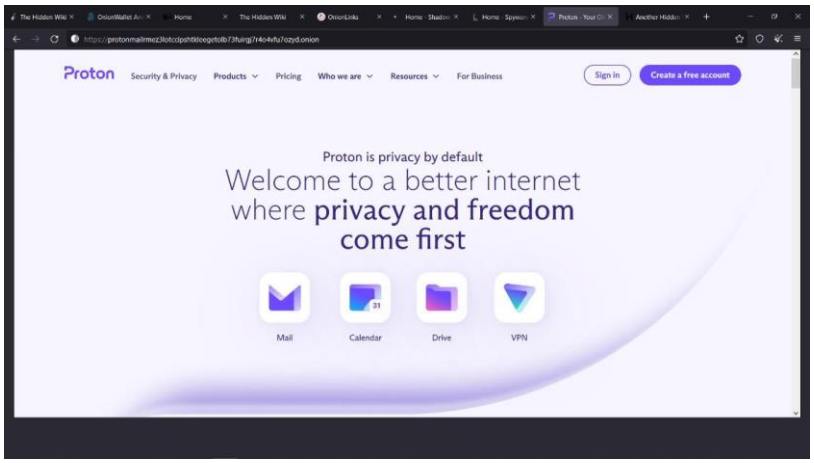


Figure 20 Exploring and Analyzing Email Service

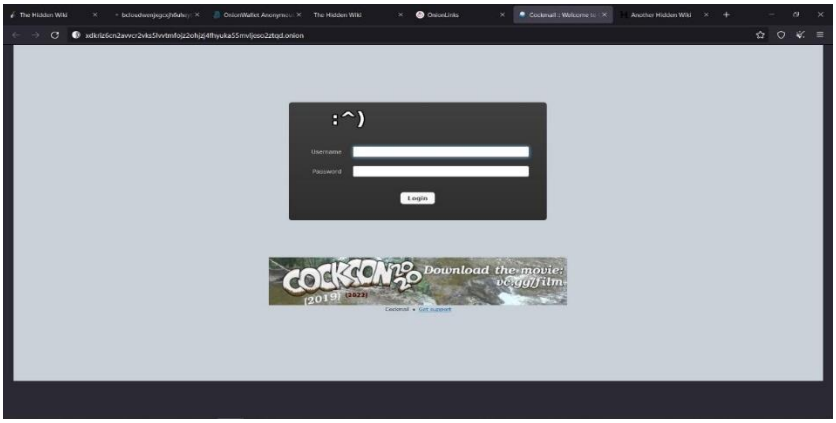


Figure 21 Exploring and Analyzing Email Service

Task 7 :- Exploring and Analyzing Anonymity & Security:

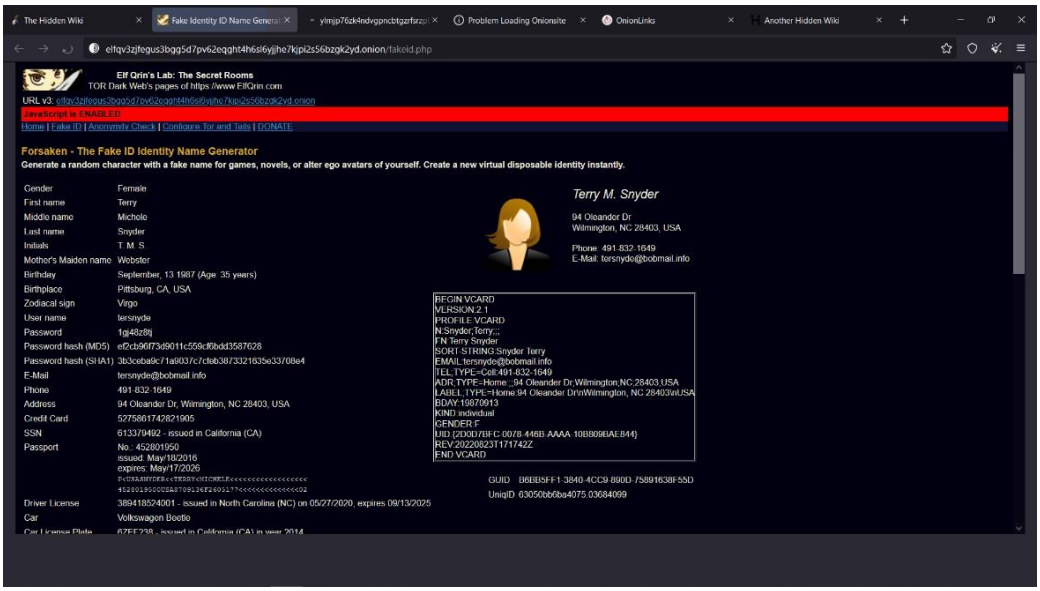


Figure 22 Exploring and Analysing Anonymity & Security

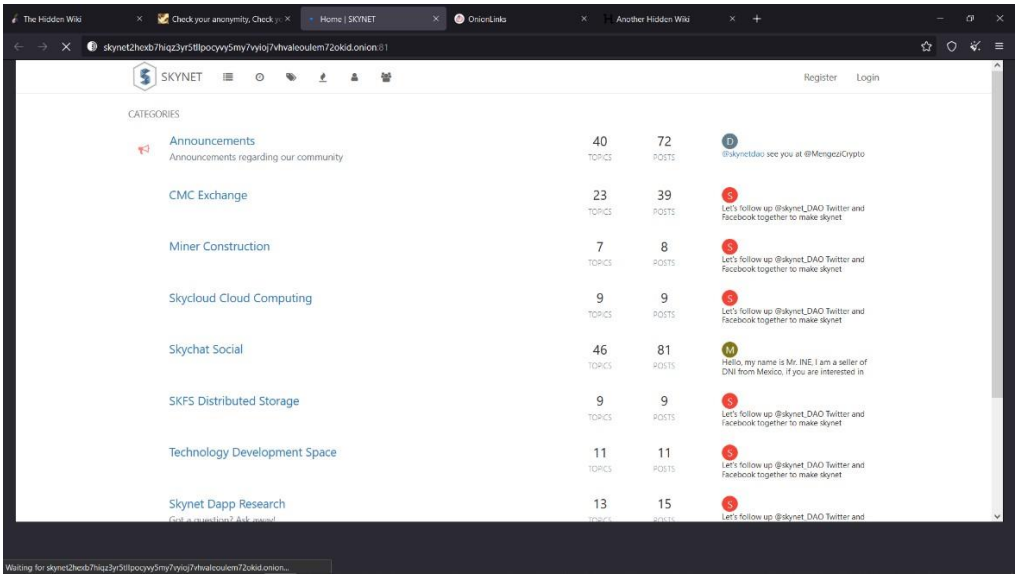


Figure 23 Exploring and Analysing Anonymity & Security

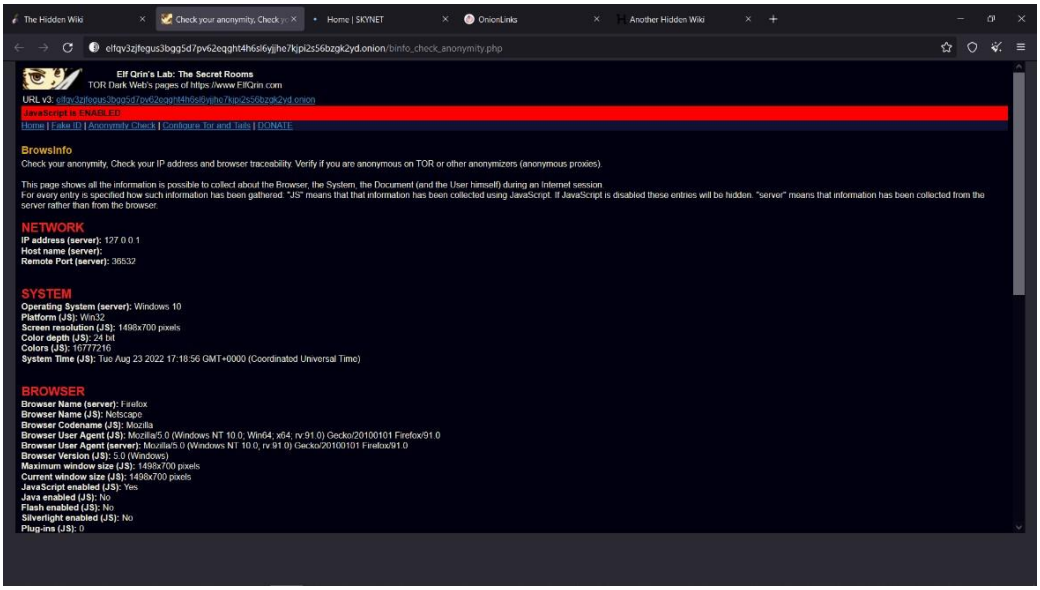


Figure 24 Exploring and Analysing Anonymity & Security

Analysis:

1. Exploring and analysing different darknet website like blogs, Anonymity & Security, Email service, Financial Services, wiki etc.

Conclusion:

1. We are using tor to connect with darknet website and we are exploring and analysing different darknet website like blogs, Anonymity & Security, Email service, Financial Services, wiki, Forums, File uploader and many more.

Digital Forensics Lab Report: 6

Date: 07-09-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
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:

1. **Recuva :- Recuva - Free Download (ccleaner.com)**
2. **Ease US :- Free Download Data Recovery Wizard - EaseUS®**

Task 1: Perform data recovery using Recuva

Steps:

1. Download software :- :- Recuva - Free Download (ccleaner.com) and setup your software
    1. Recuva is a small program you can use to recover pictures, music, documents, videos, or any other types of files on your hard drive, memory cards, floppy disks, MP3 player, or USB Flash drives.

Figure 1 Data recovery using Recuva

2. Select type of data you want to recover

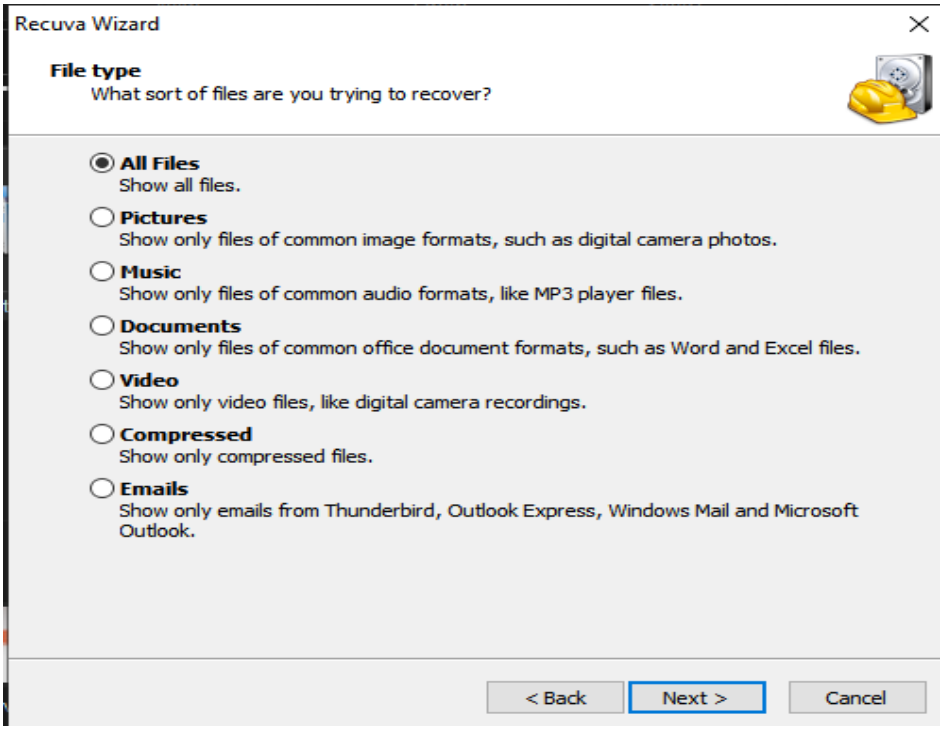


Figure 2 data recovery using Recuva

3. Select folder adderess

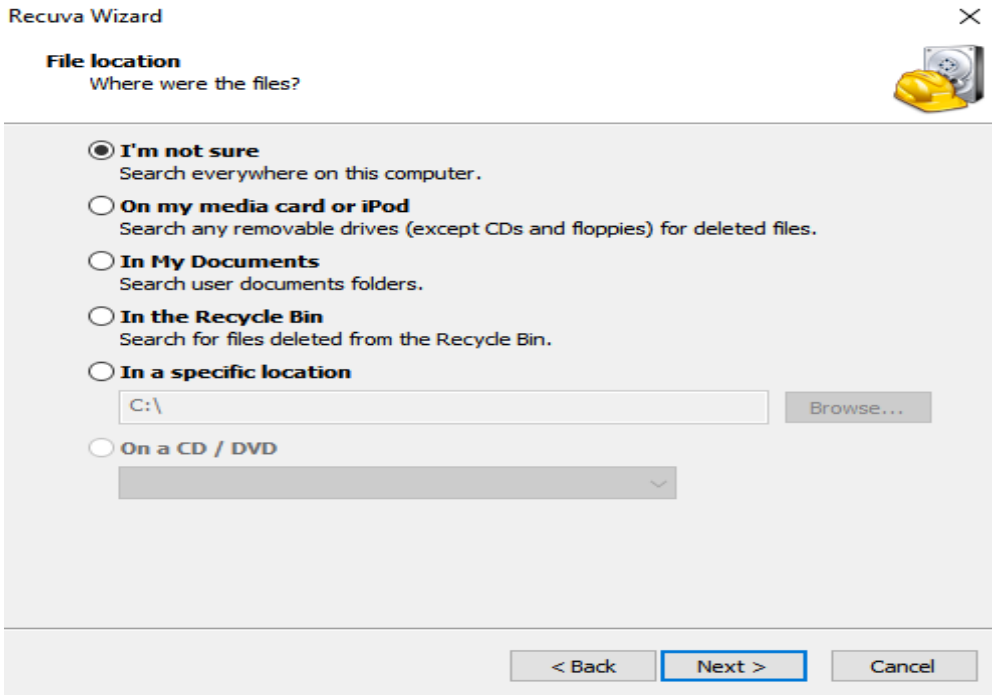


Figure 3 data recovery using Recuva

4. Start your data recovery

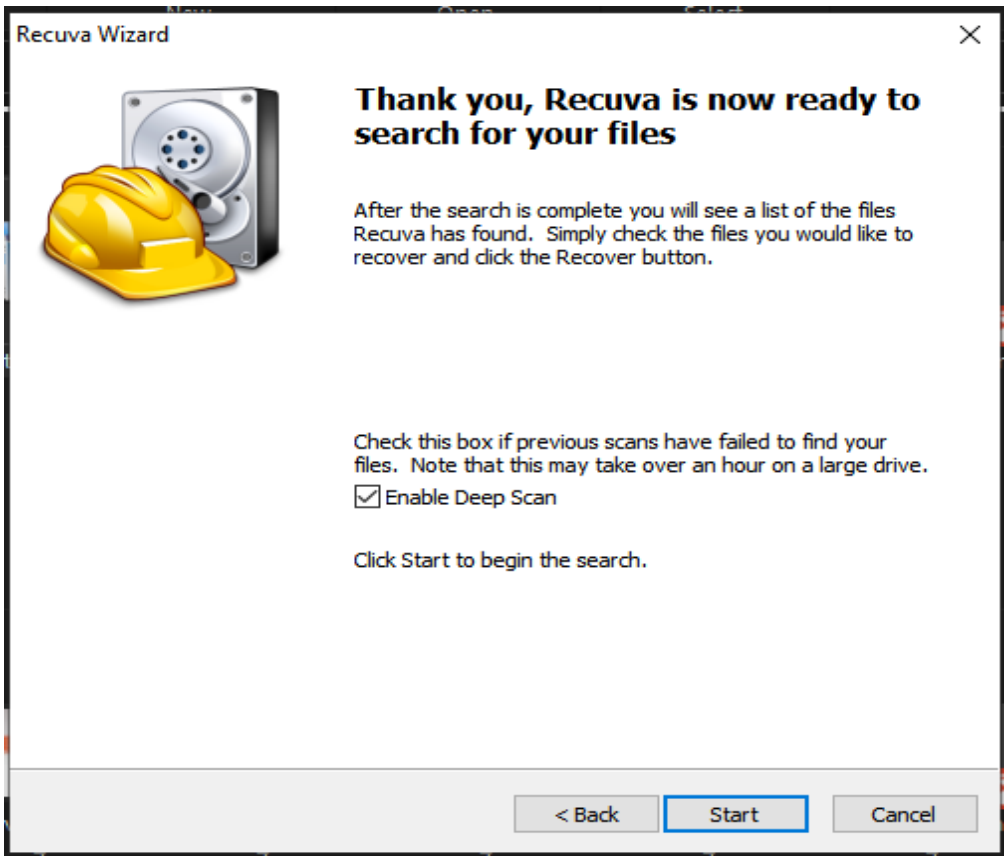


Figure 4 data recovery using Recuva

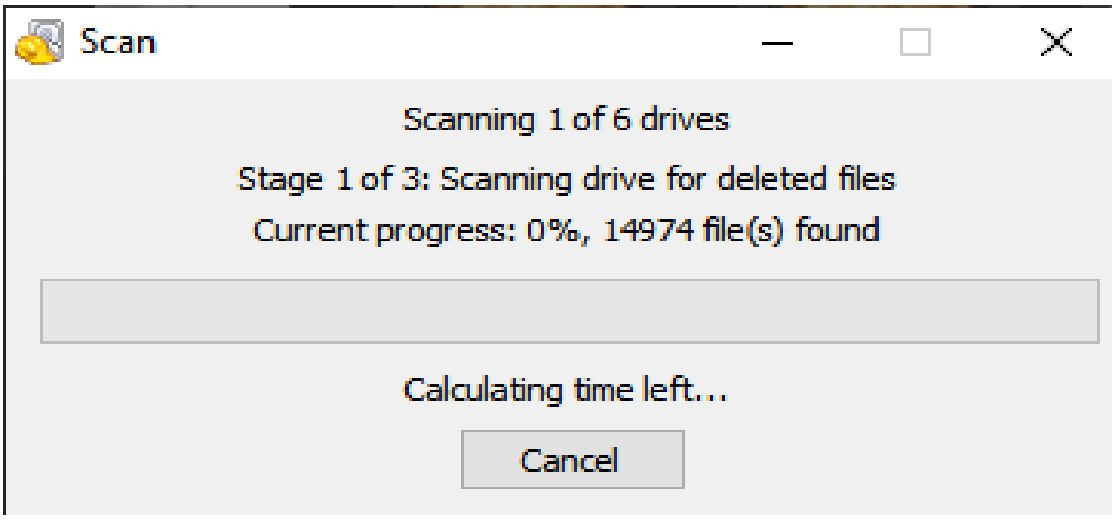


Figure 5 data recovery using Recuva

5. Show available file are ready to recover

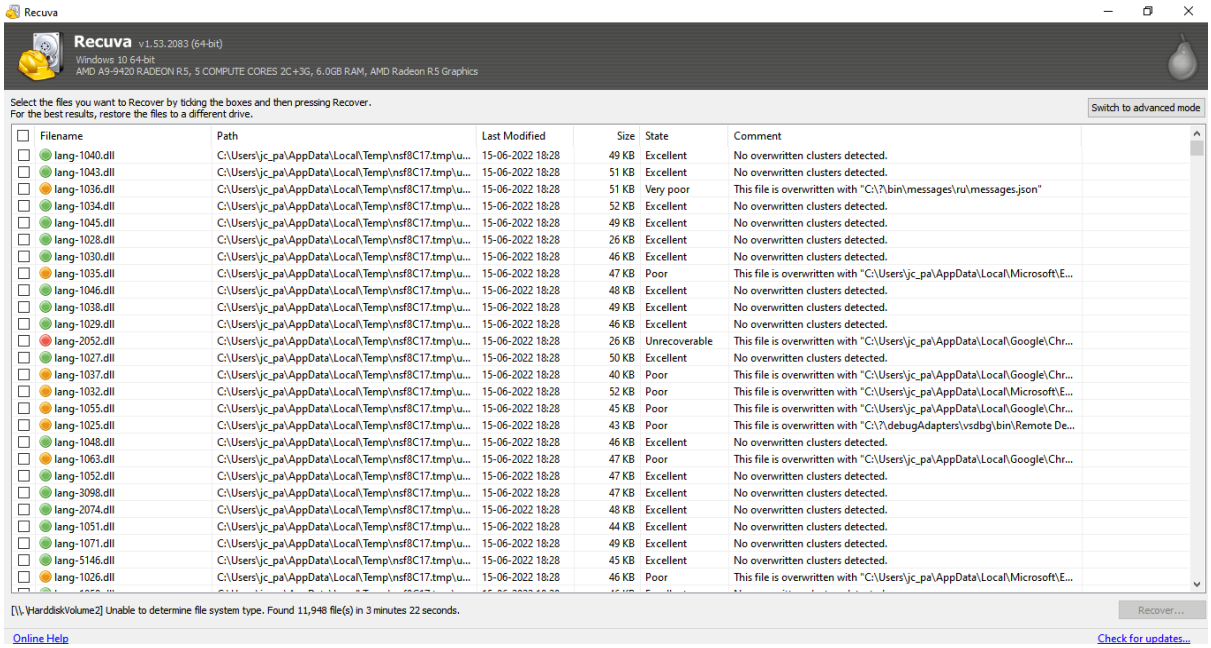


Figure 6 data recovery using Recuva

6. Select your folder you want to recover(green - > we can recover)

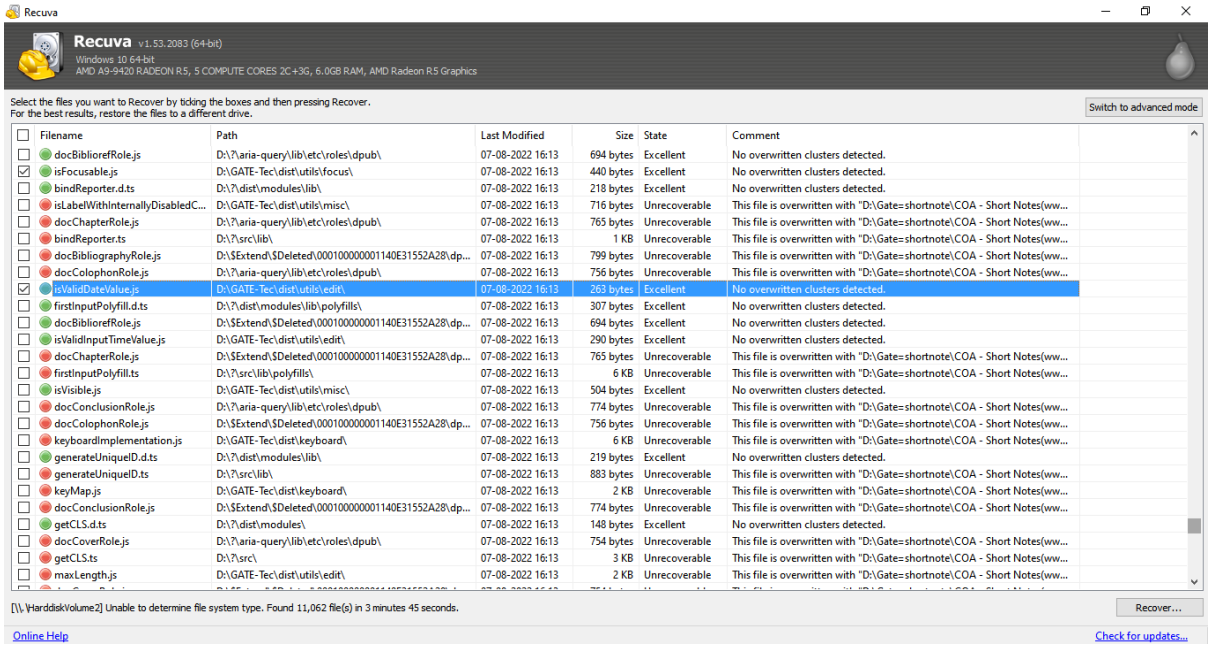


Figure 7 data recovery using Recuva

7. **Select folder where you want to store your recover data and click recover button**

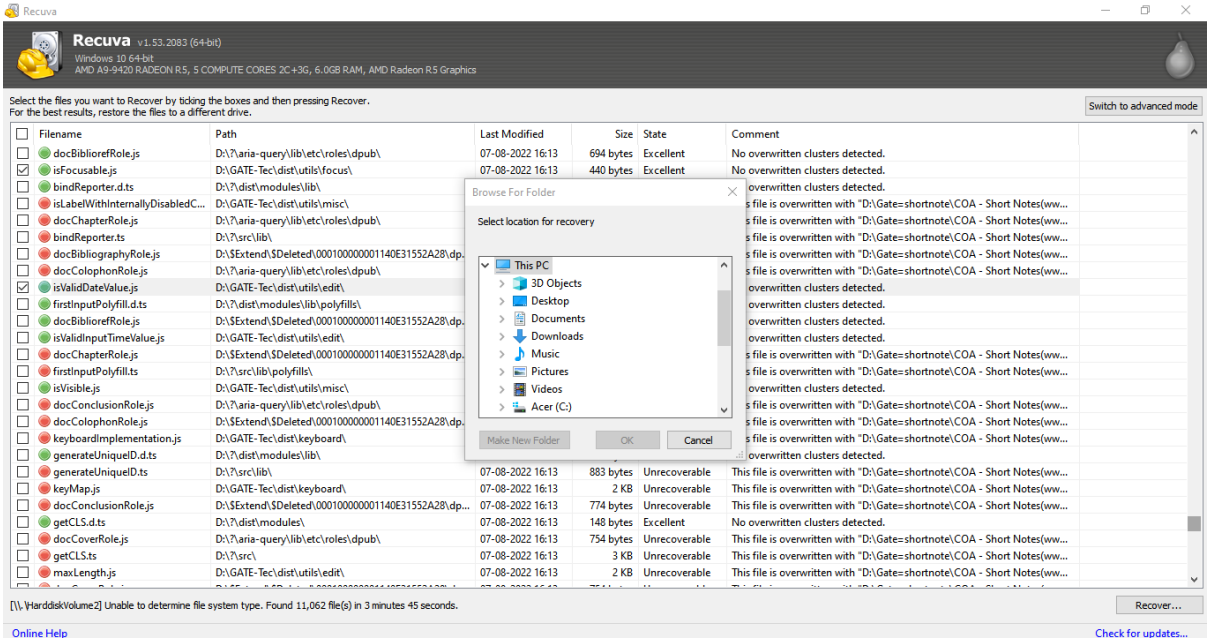


Figure 8 data recovery using Recuva

8. **Finally your data is recover**

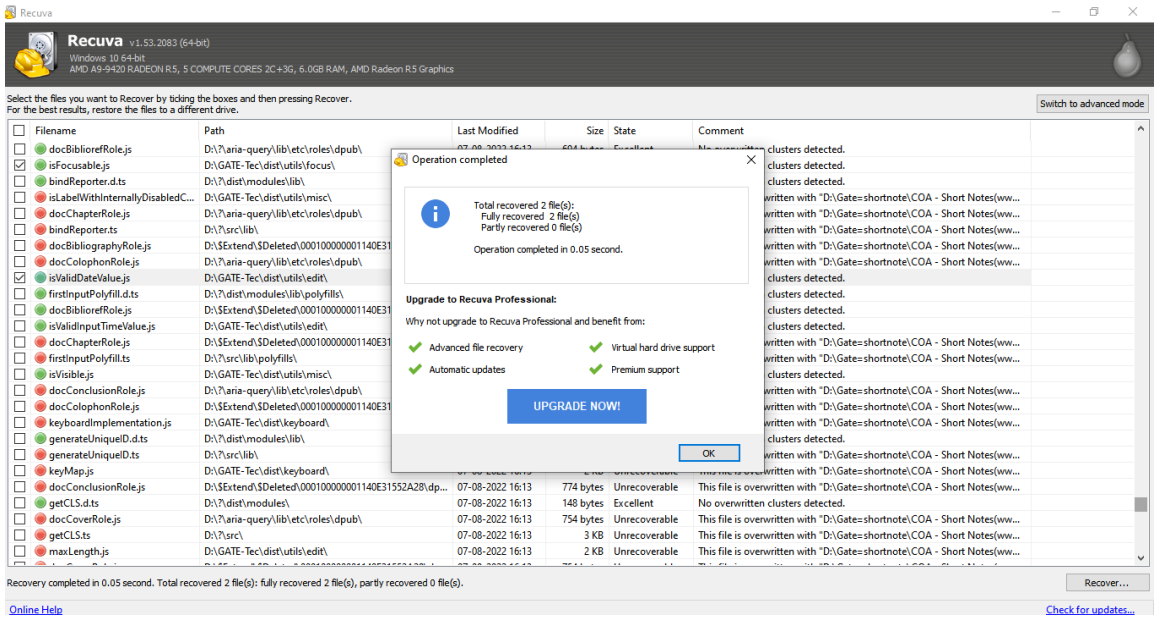


Figure 9 data recovery using Recuva

Analysis:

1. We are Recuva to recover deleted message, pictures, music, documents, videos, emails or any other file type you've lost.

Task 2: Perform data recovery using Ease US

Steps:

1. Download software :- [Free Download Data Recovery Wizard - EaseUS®] and setup your software
    2. EaseUS Data Recovery Wizard is a professional data recovery software for you to get what you have lost back simply. It is a handy and powerful tool for you to recover data in various situations, like format, virus attack, accidental file deletion, or sudden system crash.

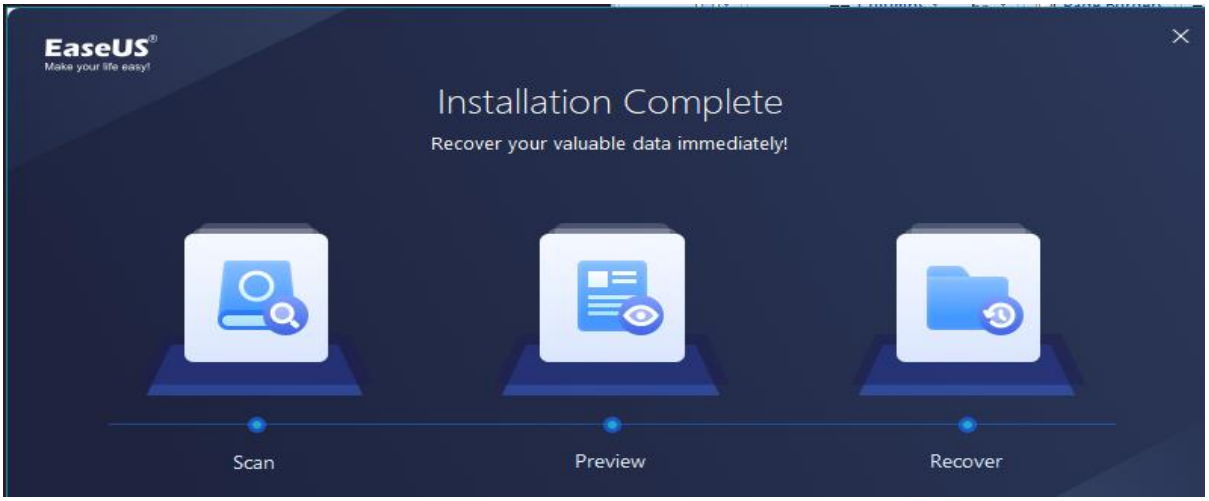


Figure 10 data recovery using Ease US

2. **Start running after install**

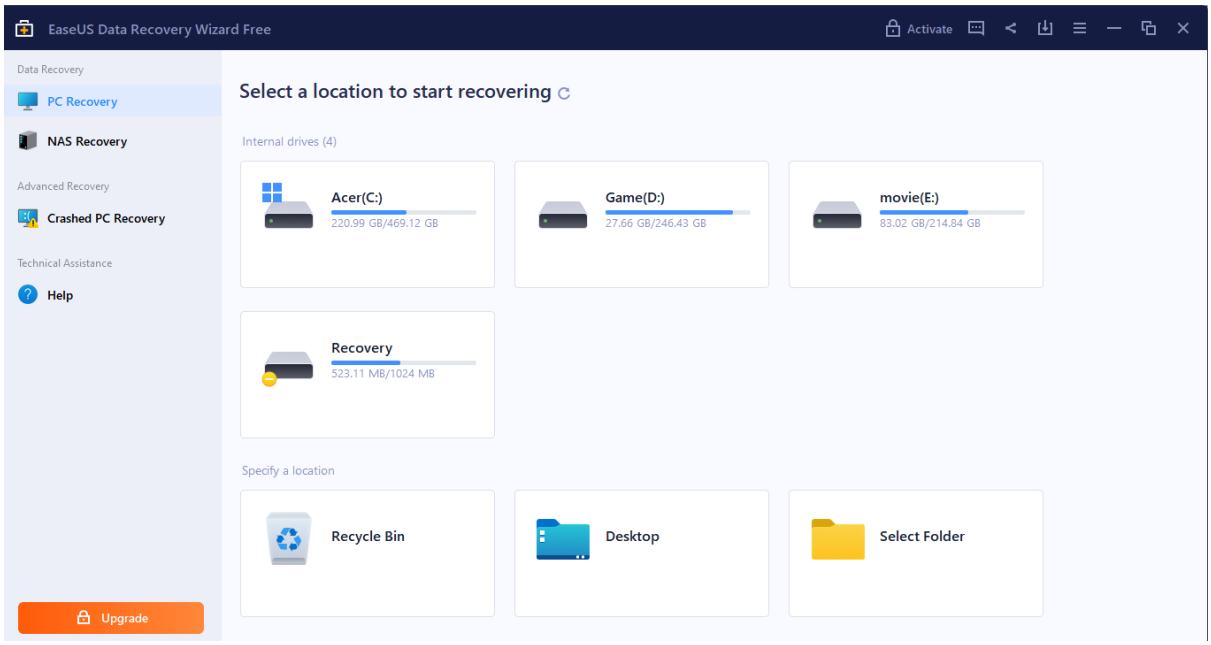


Figure 11 data recovery using Ease US

3. Select drive and select which type of data you want to recover

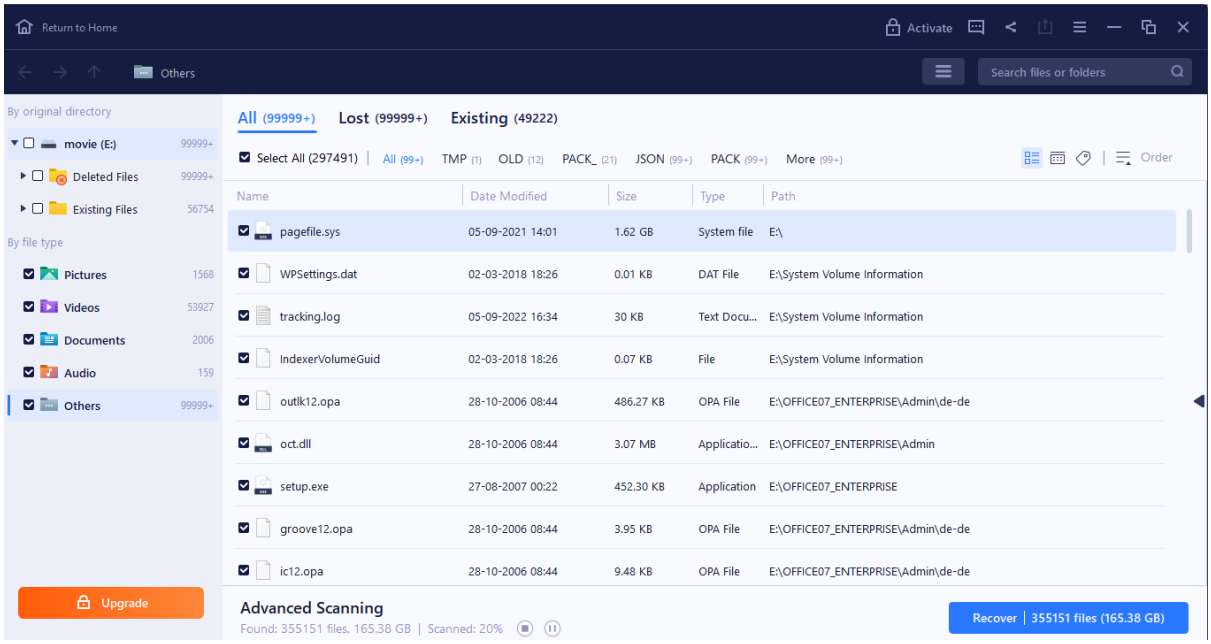


Figure 12 data recovery using Ease US

4. Select data you want ti recover and click recover button

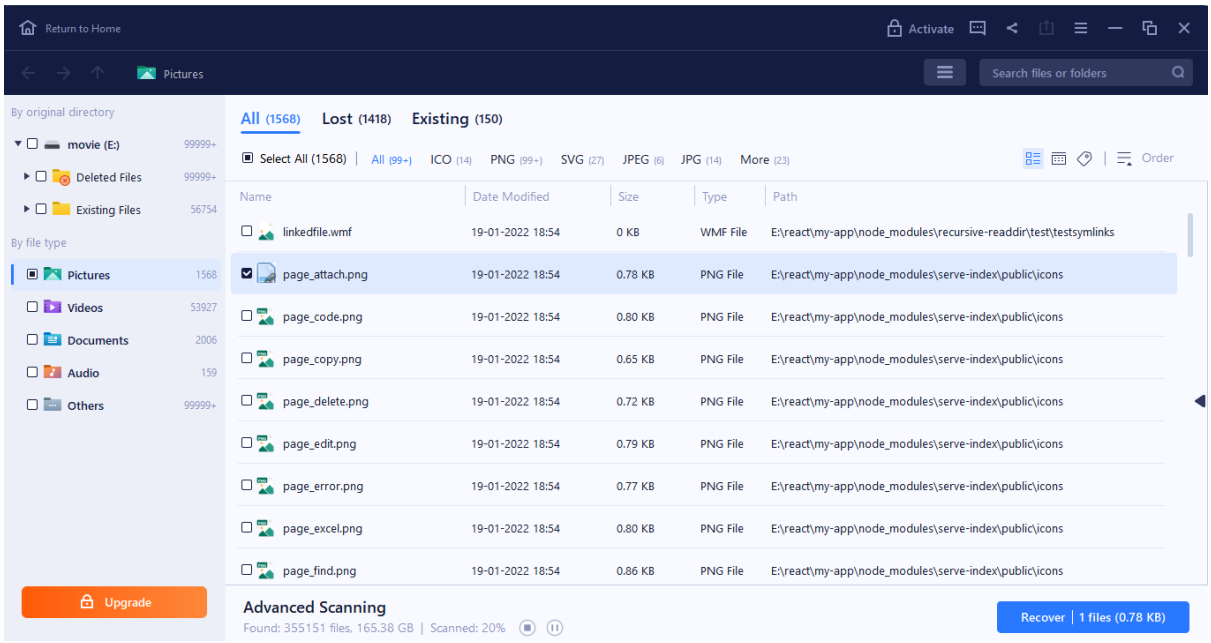


Figure 13 data recovery using Ease US

5. Select folder where you want to store data

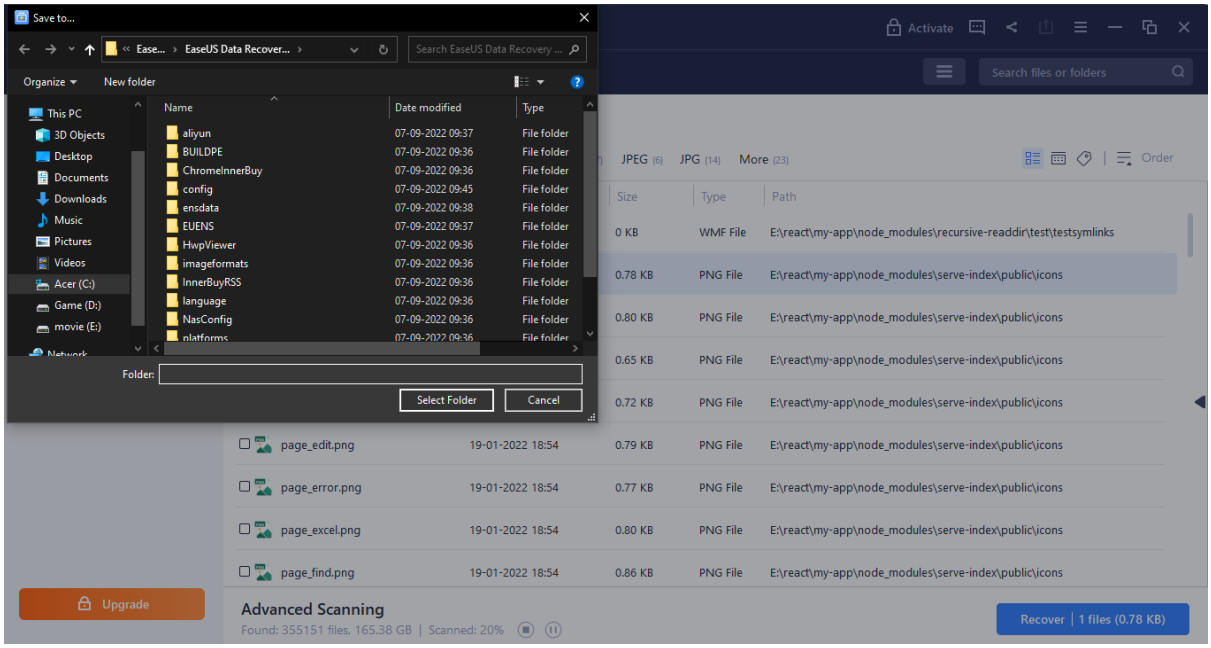


Figure 14 data recovery using Ease US

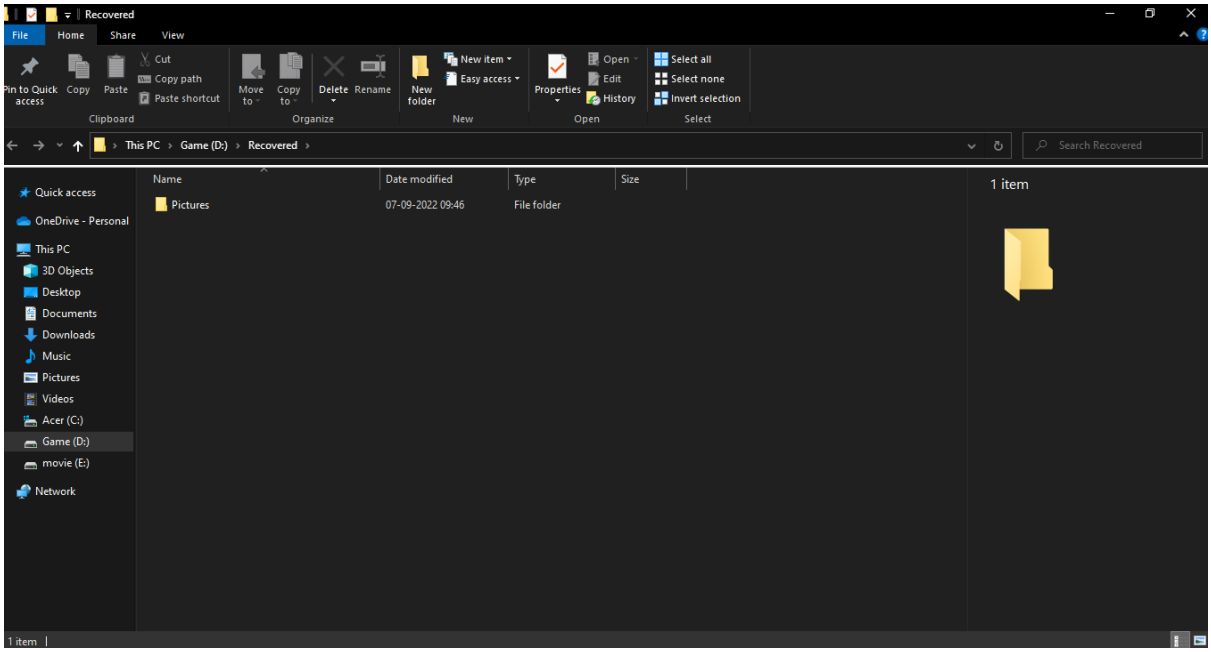


Figure 15 data recovery using Ease US

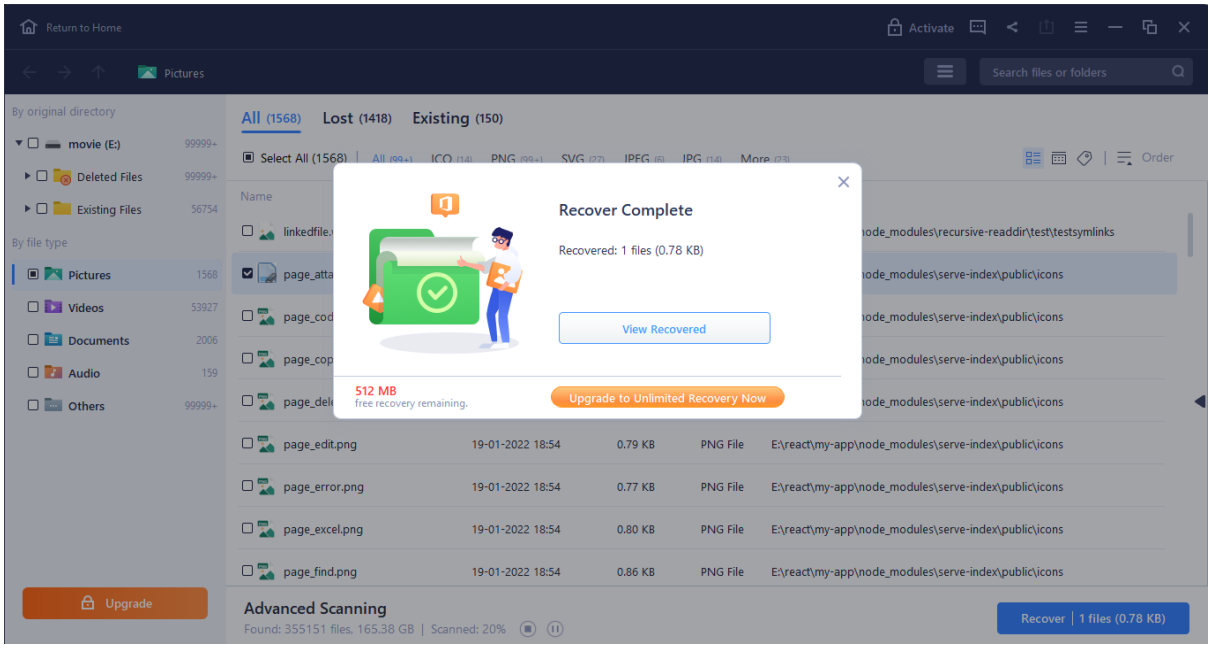


Figure 16 data recovery using Ease US

Analysis:

1. We are Ease US to recover deleted message, pictures, music, documents, videos, emails or any other file type you've lost.

Conclusion:

1. We are using Data recovery to tool like Recuva and Easy Us to recover deleted message, pictures, music, documents, videos, emails or any other file type you've lost.
2. There are other tool that we can use like NinjaOne Backup, Stellar Data Recovery, System Mechanic Ultimate Defense, AnyRecover, Aiseesoft Data Recovery, Advanced Disk Recovery. FonePaw Data Recovery

Digital Forensics Lab Report: 7

Date: 14-09-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Email Study of an Email Forensics tools.

Tool Names:-

- **Ipaddresslocation Website link :https://www.ipaddresslocation.org/email/tracer.php#email_headers**
- **Cyberforensics.in website link :- http://www.cyberforensics.in/OnlineEmailTracer/index.aspx**

Task 1:- use Ipaddresslocation.org for email Forensics

1. WebsiteLink:https://www.ipaddresslocation.org/email/tracer.php#email_headers
2. Email Tracking tool that use so called *email header* to analyze and identify IP Address from email sender and then with great success perform Email IP to location tracing giving you all necessary IP informations about location of email sender along with visual information on Map.
3. Our Email header by header analysis tracking tool will show you complete deep analyse of Email header from sender whereby we mark only most important field from email header. That's part where we have found, trace and identify sender IP Address.

Step1: Go to the ipaddresslocation.org website.In Email Header Analyzer section input original email address you want to track

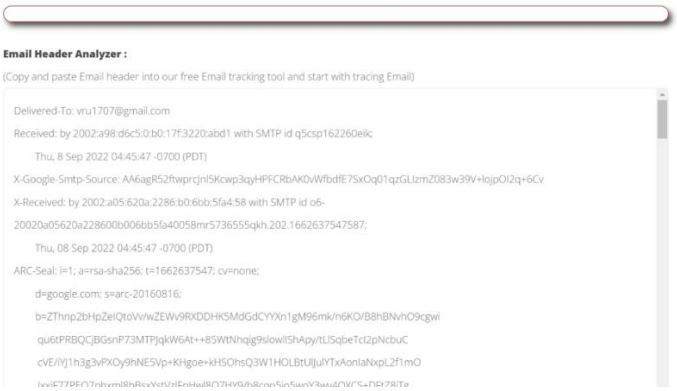


Figure 1 Email tracking using Ipaddresslocation

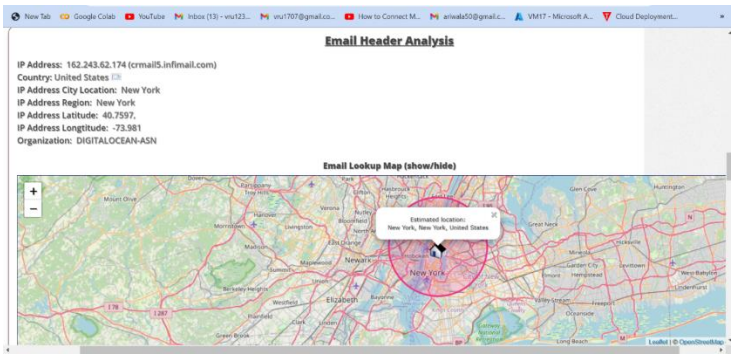


Figure 2 Email tracking using Ipaddresslocation

Figure 3 Email tracking using Ipaddresslocation

Analysis:

1. We are using Ipaddresslocation to tracking email. For email tracking we have to provide header and Ipaddresslocation track and show the path of email.

Task 2:- use Cyberforensics.in for email Forensics

- Link: http://www.cyberforensics.in/OnlineEmailTracer/index.aspx
- This is a free service to trace the email path from sender's location to recepient's mail server using IP addresses in the email header. Email Headers. Lookup. Sign up free demo account today to enjoy these benefits as registered users.

Step1: Go to the cyberforensics.in website and then click on E-MailTracer option.

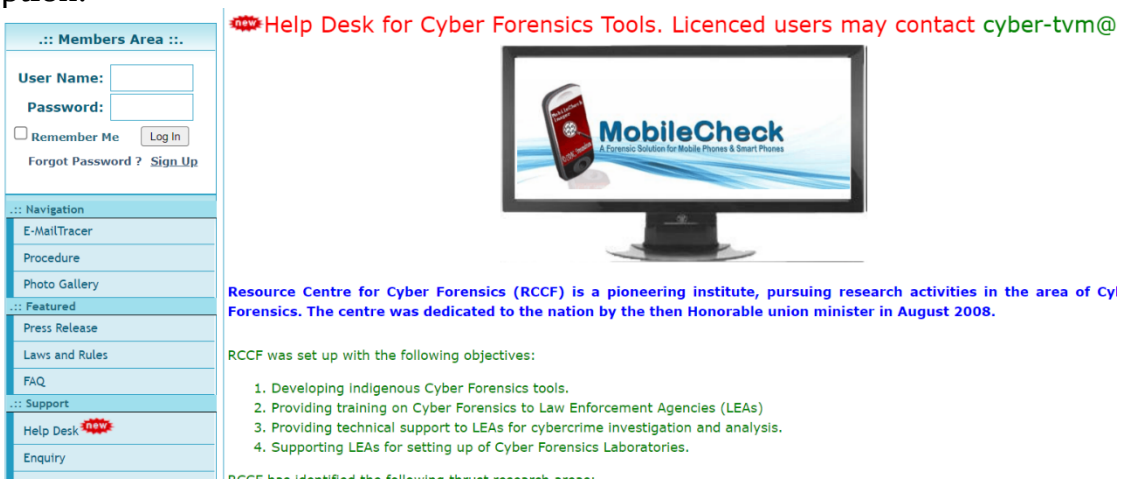


Figure 4 Online Email Tracer(cyberforensics)

Step 2:In Email Header Analyzer section input original email address you want to track.

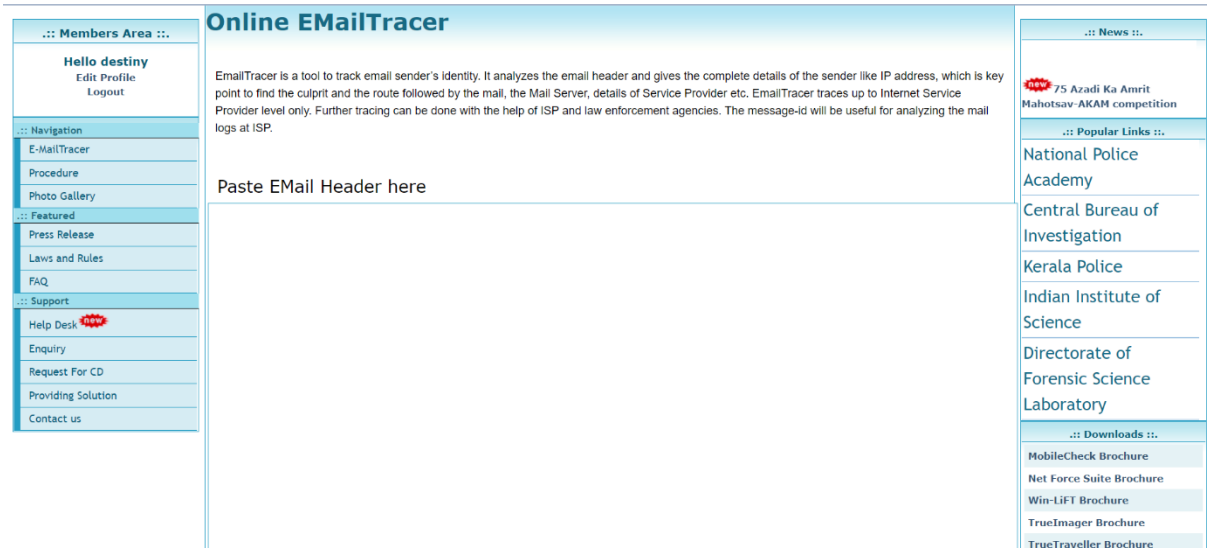


Figure 5 Online Email Tracer(cyberforensics)

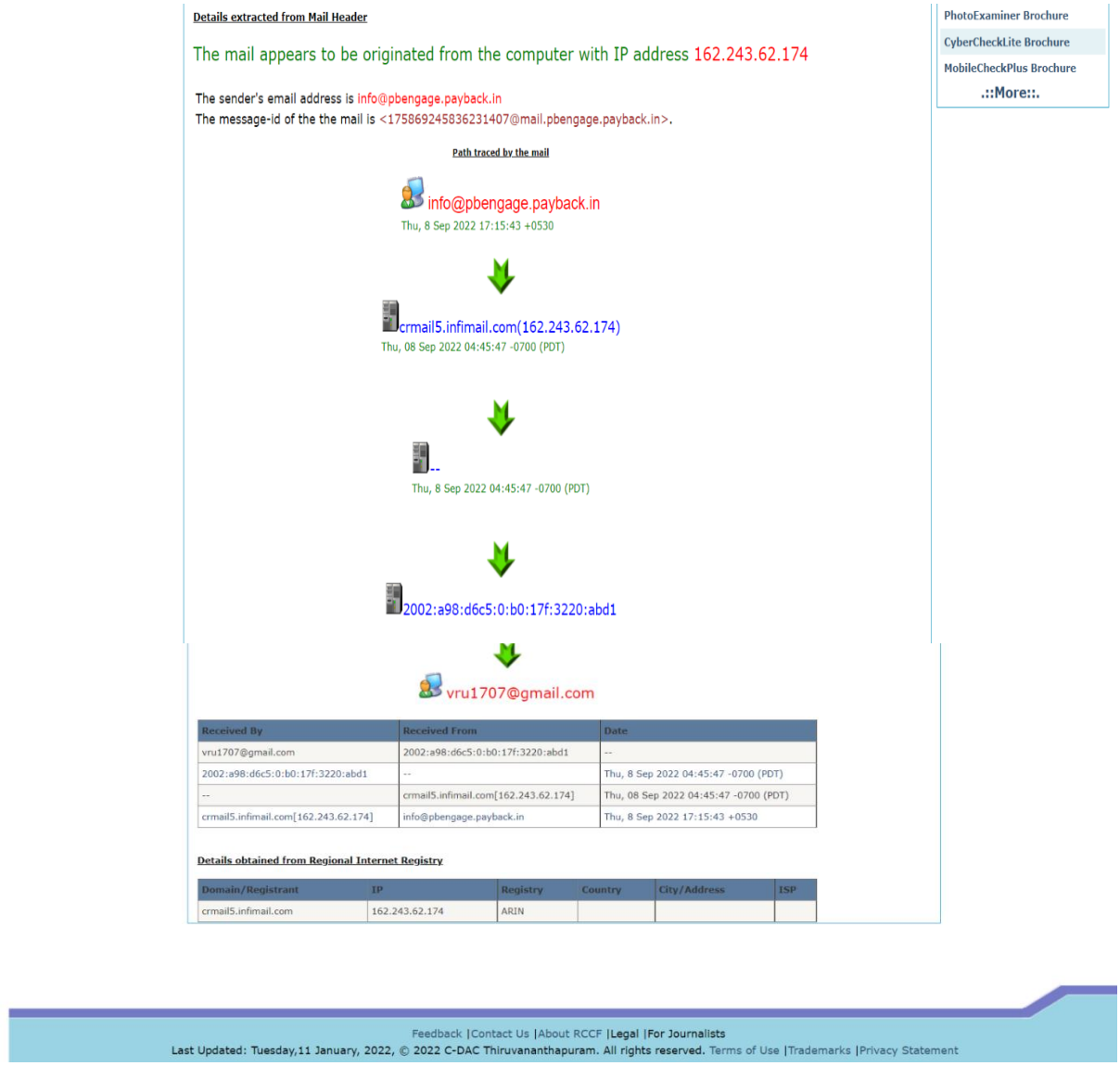


Figure 6 Online Email Tracer(cyberforensics)

Analysis:

We are using cyberforensics to tracking email. For email tracking we have to provide header and cyberforensics track and show the path of email.

Conclusion:

1. We are using cyberforensics and Ipaddresslocation to Email tracking.
2. Email tracking involves tracking emails sent to people and using the results to your benefit. Most email tracking tools can tell you who opened your emails, the time they opened them, locations, and other additional details.

Digital Forensics Lab Report: 8

Date: 12-10-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Study of volatile memory forensics tools

Tool Names:

1. FTK Imager link :- https://go.exterro.com/l/43312/2022-08-23/f7rytx
2. WinHex link :- http://www.winhex.com/winhex/hex-editor.html

Step 1:- Download FTK Imager

- FTK Imager Download link :- https://go.exterro.com/l/43312/2022-08-23/f7rytx click on get free tool. It will ask to fill the form in order to get the software link.
- FTK Manager is a powerful tool that can be used to manage forensics investigations. It provides a user-friendly interface that makes it easy to search and analyze forensic data. FTK Manager can be used to investigate a wide range of crimes, including child pornography, terrorism, and espionage.
- WinHex is a hexadecimal editor for the Windows operating system. It is used for forensics, data recovery, low-level data processing, and IT security. It allows the user to view files in hexadecimal format.
- Add your details and click on Get Free Tool, you will receive then a mail containing a software link.

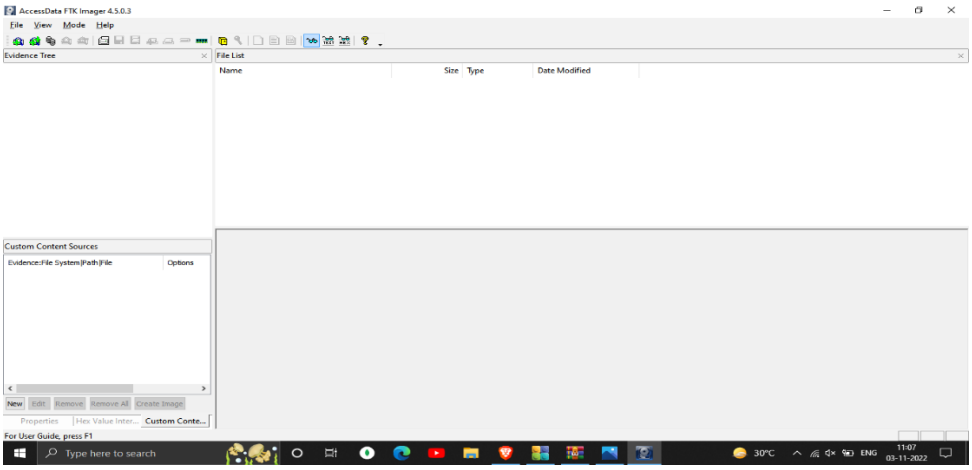


Figure 1 FTK Imager

Steps2: Download Winhex:

1. Visit http://www.winhex.com/winhex/hex-editor.html and click on Download.

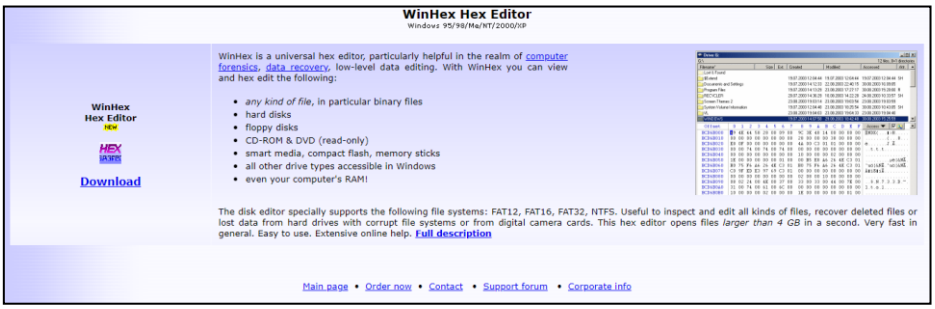


Figure 2 WinHex

Step 3: Make Image file in FTK imager Capture and open in Winhex.

Open Magnet Ram capture and choose directory and file name and click on start

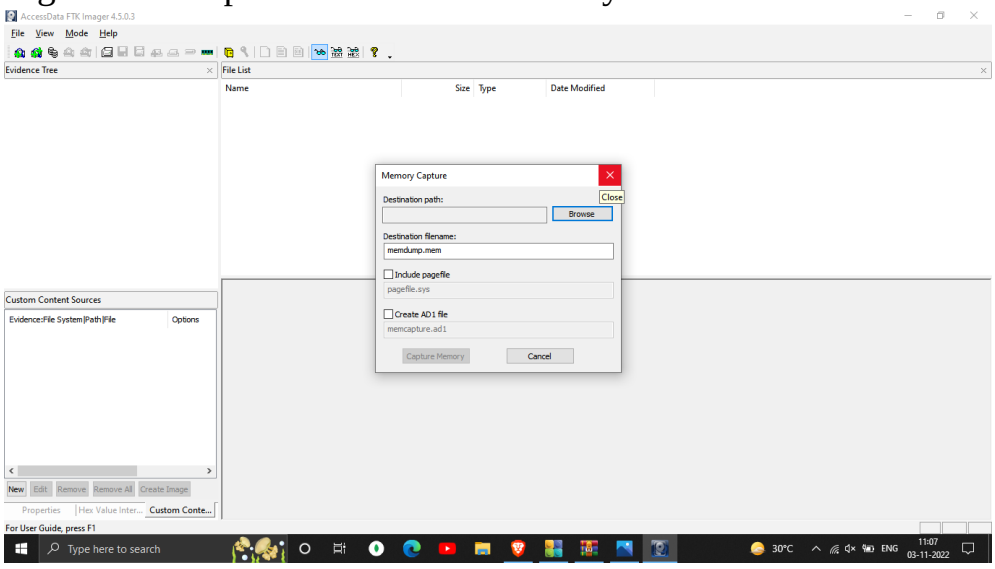


Figure 3 FTK Imager

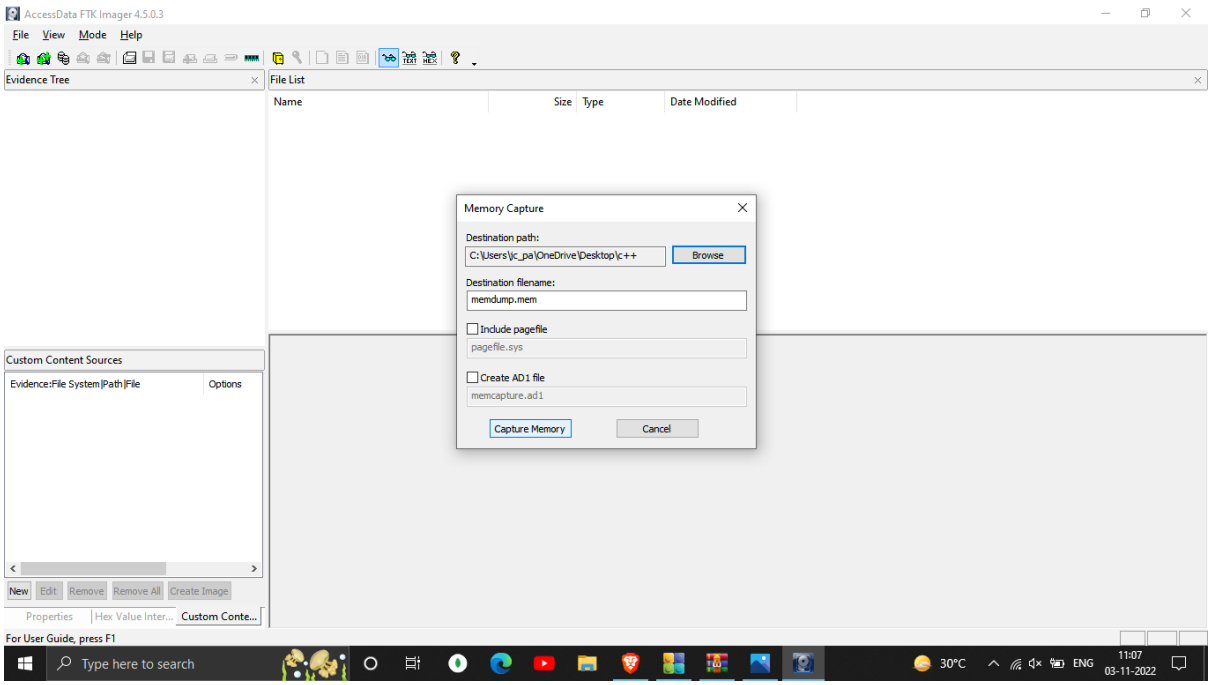


Figure 4 FTK Imager

2. 0nce completed, a raw file will be created Now, open winhex and then open the created raw file

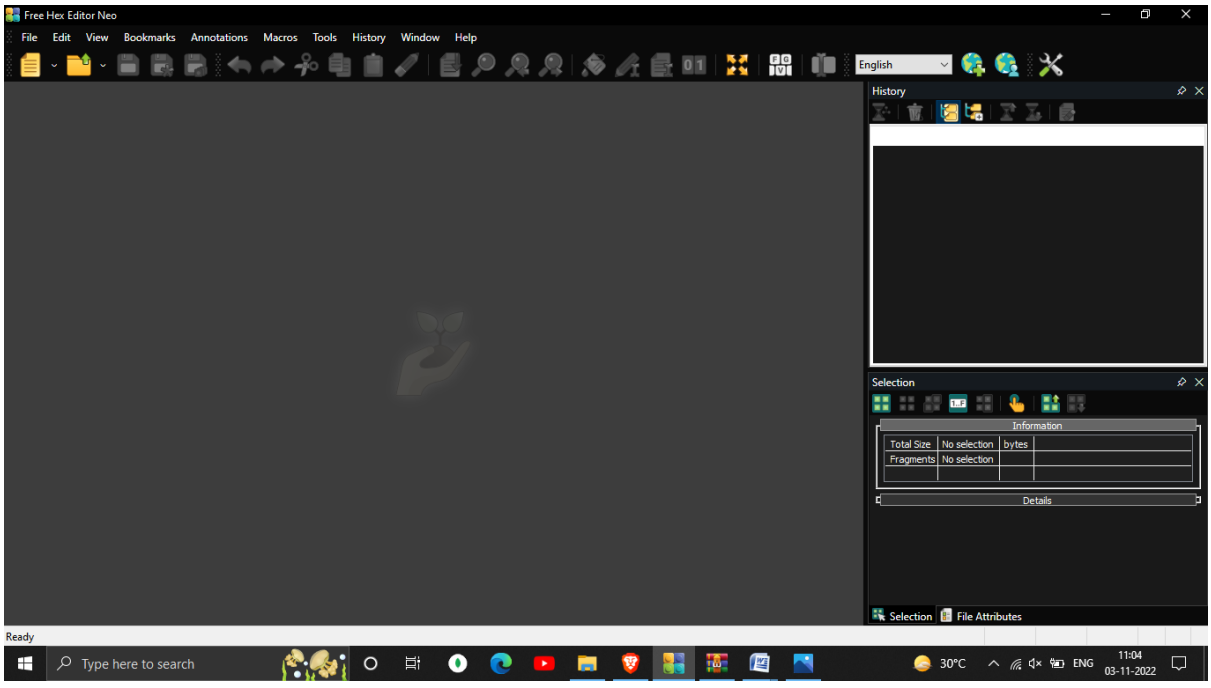


Figure 5 WinHex

3. Import fie from which creating using FTK imager

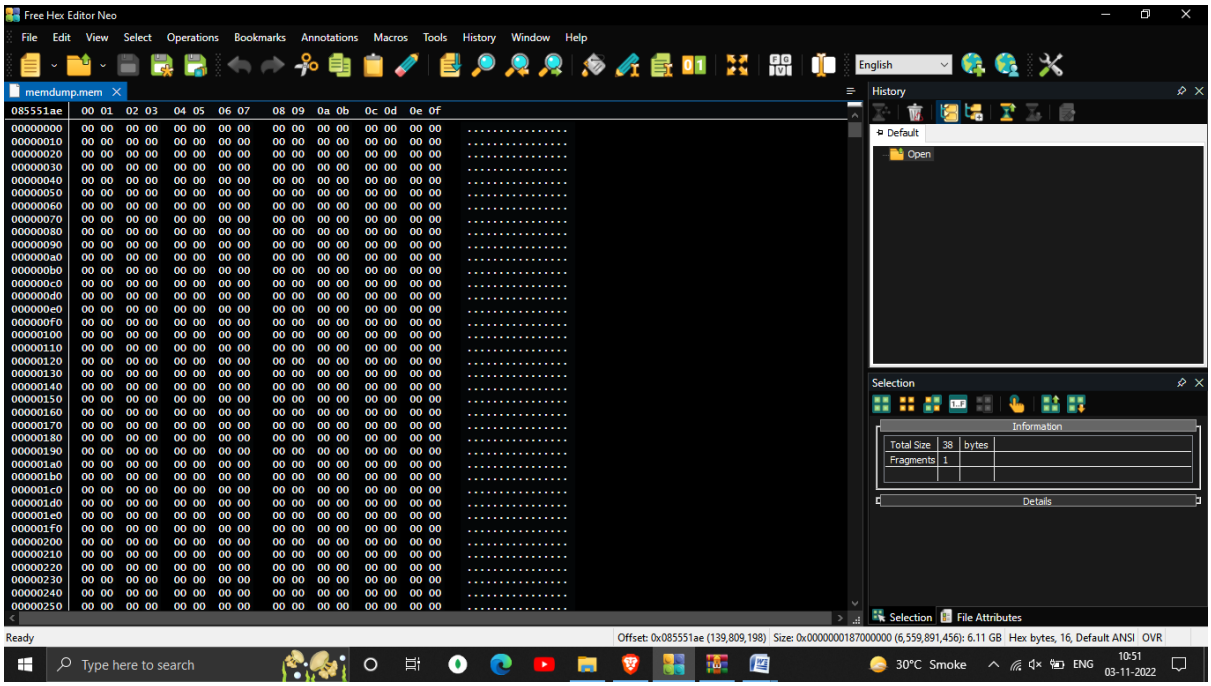


Figure 6 WinHex

4. Findings:

1. Found Gmail id and password :-

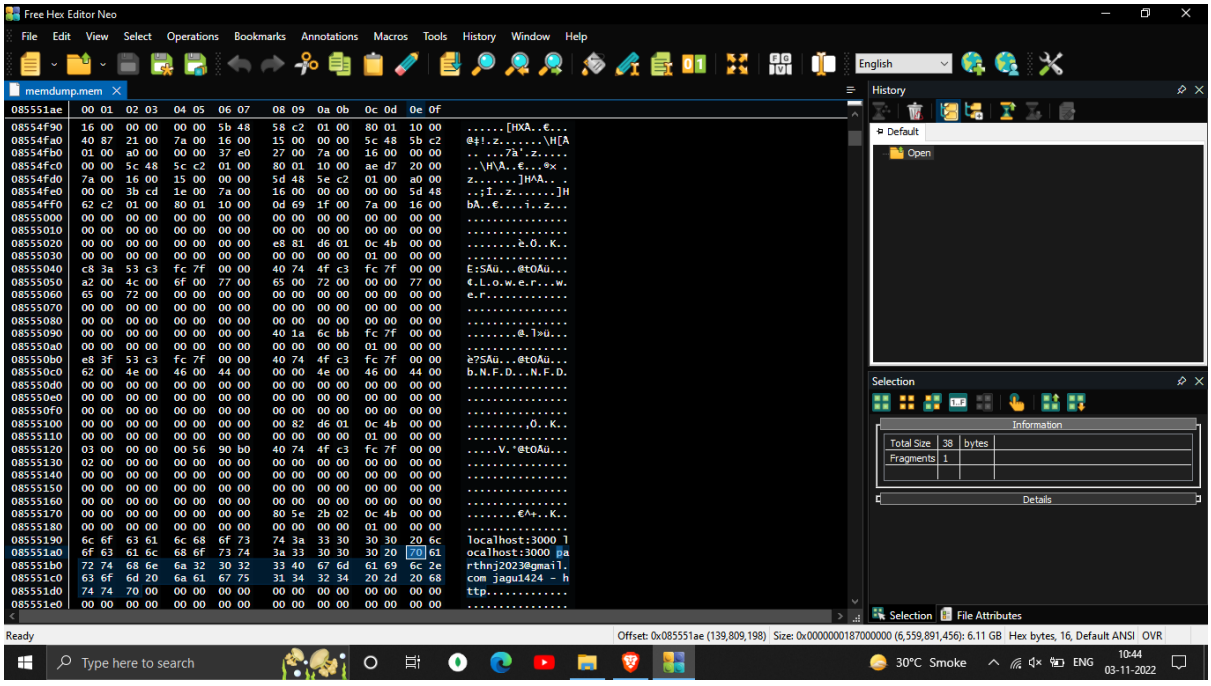


Figure 7 WinHex (Found :- Gmail ID and Password)

2. Found gate website account

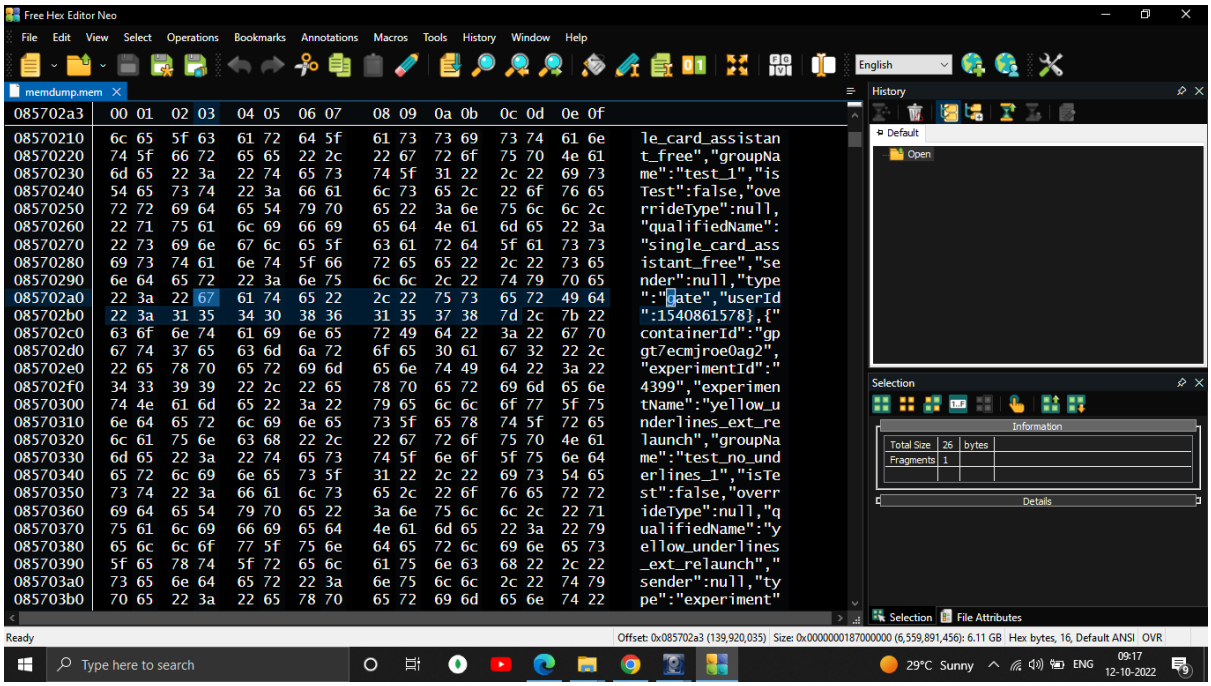


Figure 8 WinHex (Found :- gate website and account)

3. Find YouTube website

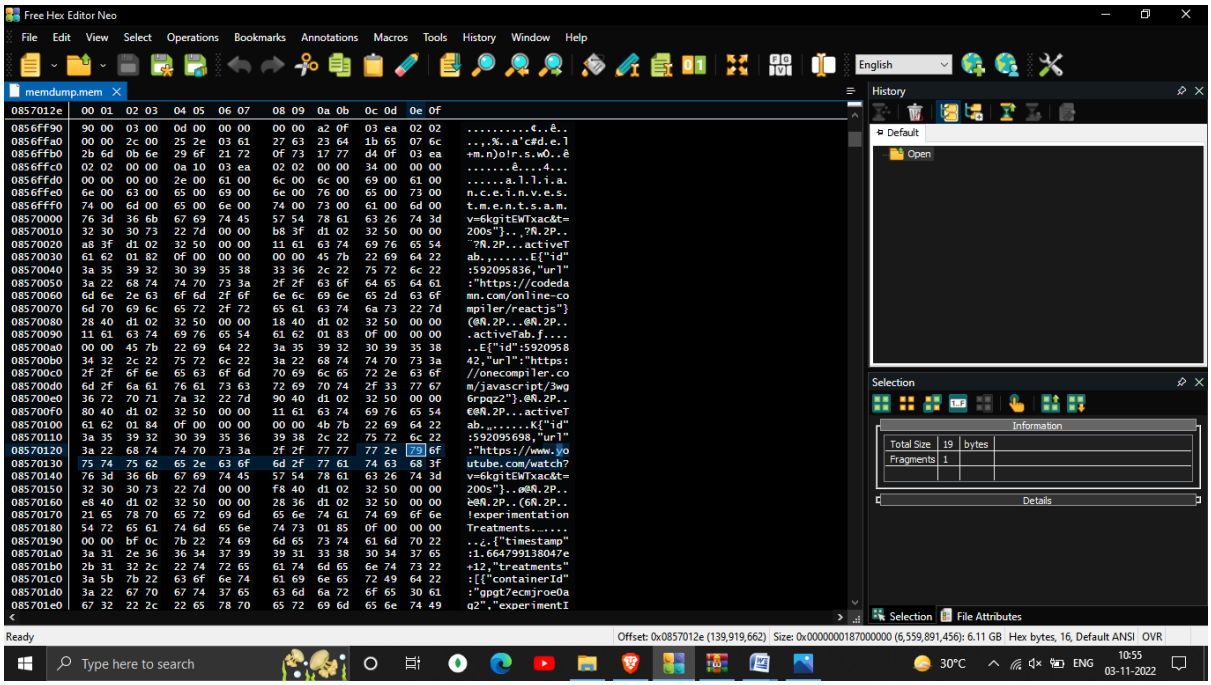


Figure 9 WinHex (Found :- Youtube)

4. Manga read website (1stkissmanga.io)

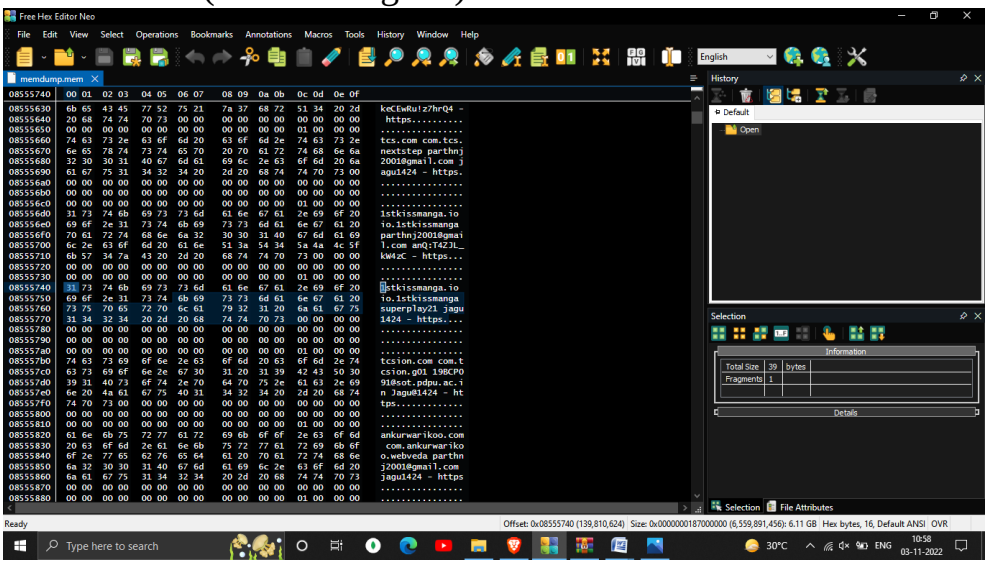


Figure 10 WinHex (Found :- 1stkissmanga)

5. LinkedIn

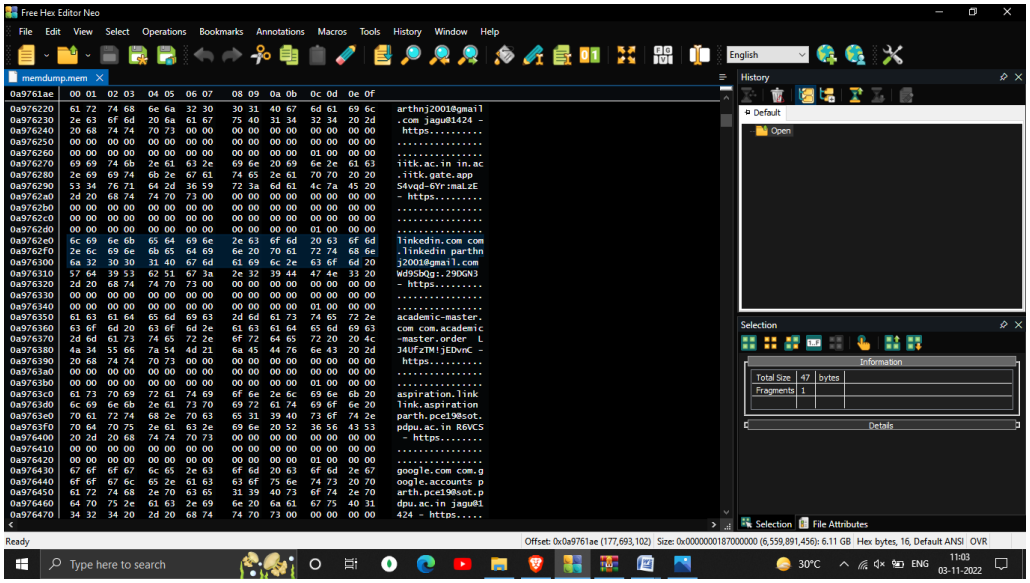


Figure 11 WinHex (Found :- LinkedIn)

Analysis:

1. We are using FTK imager to Capture memory and then using Win Hex to find data.

Conclusion:

1. We are using FTK imager to capture memory
2. We are using Win Hex to find data from FTK imager data may include like Gmail account and password , YouTube watch video other website password or other person phone number.

Digital Forensics Lab Report: 9

Date: 26-10-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

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

Tool Names:

1. WinHEX :- WinHex is a hexadecimal editor for the Windows operating system. It is used for forensics, data recovery, low-level data processing, and IT security. It allows the user to view files in hexadecimal format.

2. Garrykesler

3. Hashmefileignoreware:- HashMyFiles is small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system. You can easily copy the MD5/SHA1 hashes list into the clipboard, or save them into text/html/xml file.HashMyFiles can also be launched from the context menu of Windows Explorer, and display the MD5/SHA1 hashes of the selected file or folder.

Steps: -

Download and Install HashMyFiles :- https://hashmyfiles.soft112.com/modal-download.htmland Download HashMyFiles as ZIP. Extract the zip file to get the.exefile.

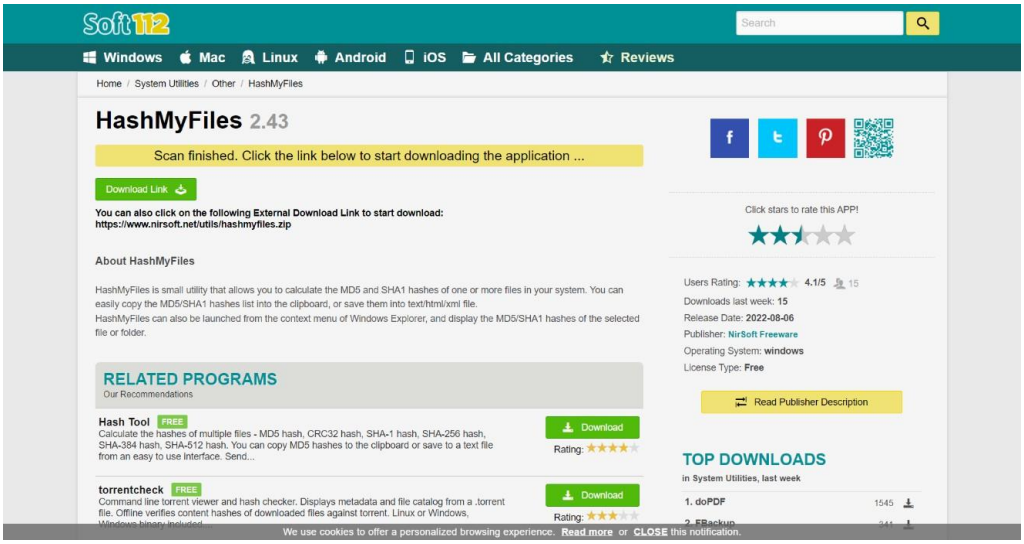


Figure 1 HashMyFiles download website

1. Open the Application and open any file.

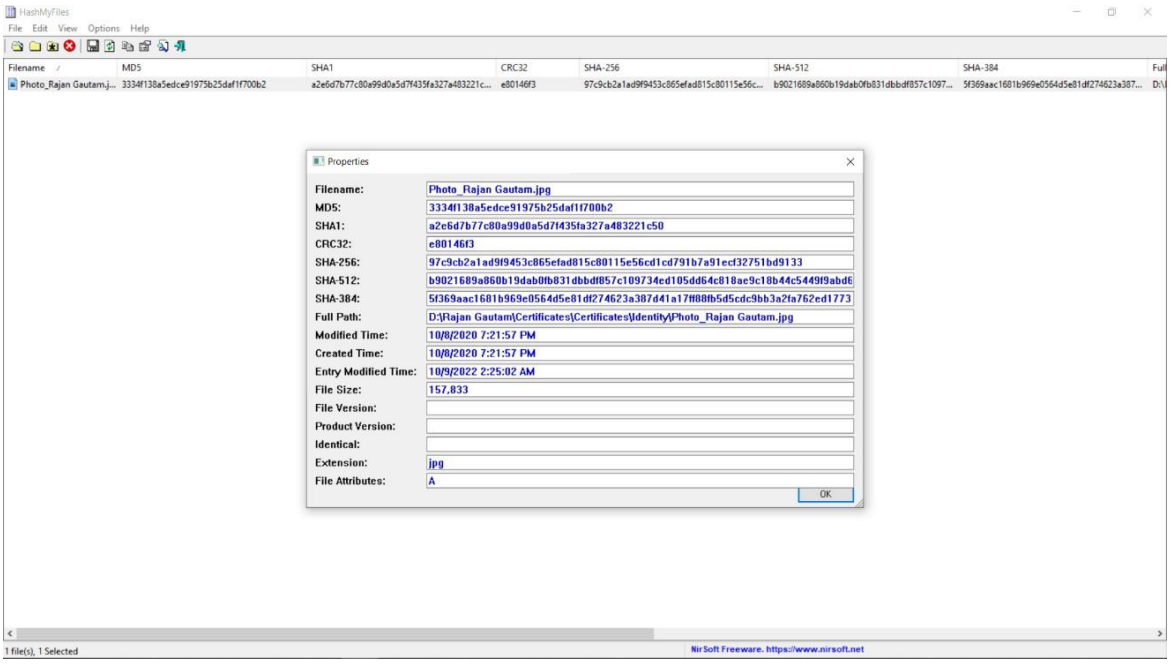
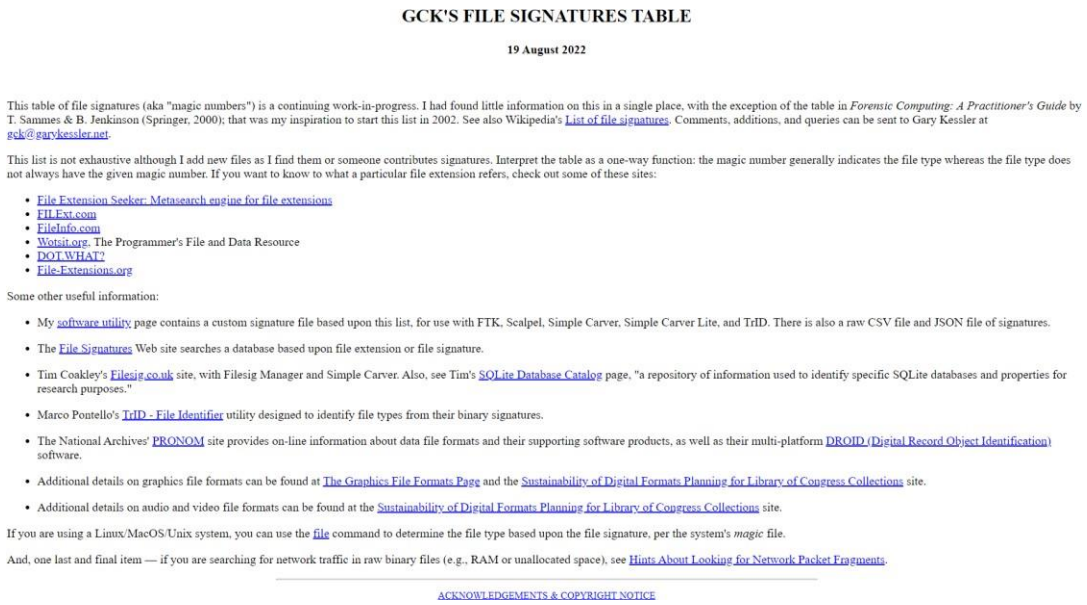


Figure 2 HasmyFiles

2. Access Garrykesler from this URLhttps://www.garykessler.net/library/file_sigs.html



GCK'S FILE SIGNATURES TABLE

19 August 2022

This table of file signatures (aka "magic numbers") is a continuing work-in-progress. I had found little information on this in a single place, with the exception of the table in *Forensic Computing: A Practitioner's Guide* by T. Sammes & B. Jenkinson (Springer, 2000); that was my inspiration to start this list in 2002. See also Wikipedia's List of file signatures. Comments, additions, and queries can be sent to Gary Kessler at gck@garykessler.net.

This list is not exhaustive although I add new files as I find them or someone contributes signatures. Interpret the table as a one-way function: the magic number generally indicates the file type whereas the file type does not always have the given magic number. If you want to know to what a particular file extension refers, check out some of these sites:

- File Extension Seeker: Metasearch engine for file extensions
- FILExt.com
- FileInfo.com
- Wotsit.org. The Programmer's File and Data Resource
- DOT.WHAT?
- File-Extensions.org

Some other useful information:

- My software utility page contains a custom signature file based upon this list, for use with FTK, Scalpel, Simple Carver, Simple Carver Lite, and TrID. There is also a raw CSV file and JSON file of signatures.
- The File Signatures Web site searches a database based upon file extension or file signature.
- Tim Coakley's Filesig.co.uk site, with Filesig Manager and Simple Carver. Also, see Tim's SQLite Database Catalog page, "a repository of information used to identify specific SQLite databases and properties for research purposes."
- Marco Pontello's TrID - File Identifier utility designed to identify file types from their binary signatures.
- The National Archives' PRONOM site provides on-line information about data file formats and their supporting software products, as well as their multi-platform DROID (Digital Record Object Identification) software.
- Additional details on graphics file formats can be found at The Graphics File Formats Page and the Sustainability of Digital Formats Planning for Library of Congress Collections site.
- Additional details on audio and video file formats can be found at the Sustainability of Digital Formats Planning for Library of Congress Collections site.

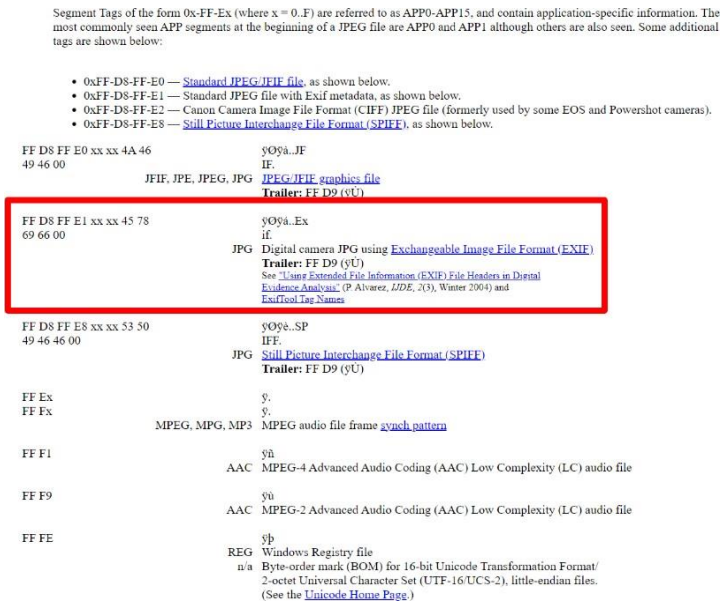
If you are using a Linux/MacOS/Unix system, you can use the file command to determine the file type based upon the file signature, per the system's *magic* file.

And, one last and final item — if you are searching for network traffic in raw binary files (e.g., RAM or unallocated space), see Hints About Looking for Network Packet Fragments.

ACKNOWLEDGEMENTS & COPYRIGHT NOTICE

Figure 3 Garrykesler

3. Check Hex Value for .JPG file in GCK's file. As per them Hex value for JPG image is 'FF D8 FF E1 xx xx 4578'.



Segment Tags of the form 0x-FF-Ex (where x = 0..F) are referred to as APP0-APP15, and contain application-specific information. The most commonly seen APP segments at the beginning of a JPEG file are APP0 and APP1 although others are also seen. Some additional tags are shown below:

- 0xFF-D8-FF-E0 — Standard JPEG/JFIF file, as shown below.
- 0xFF-D8-FF-E1 — Standard JPEG file with Exif metadata, as shown below.
- 0xFF-D8-FF-E2 — Canon Camera Image File Format (CIFF) JPEG file (formerly used by some EOS and Powershot cameras).
- 0xFF-D8-FF-E8 — Still Picture Interchange File Format (SPIFF), as shown below.

FF D8 FF E0 xx xx 4A 46 49 46 00	JFIF, JPE, JPEG, JPG	ÿØÿà..JF IF. JPEG/JFIF graphics file **Trailer:** FF D9 (ÿÙ)
FF D8 FF E1 xx xx 45 78 69 66 00	JPG	ÿØÿá..Ex if. Digital camera JPG using Exchangeable Image File Format (EXIF) **Trailer:** FF D9 (ÿÙ) See "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis" (P. Alvarez, *IJDE*, 2(3), Winter 2004) and ExifTool Tag Names
FF D8 FF E8 xx xx 53 50 49 46 46 00	JPG	ÿØÿè..SP IFF. Still Picture Interchange File Format (SPIFF) **Trailer:** FF D9 (ÿÙ)
FF Ex FF Fx	MPEG, MPG, MP3	ÿ. ÿ. MPEG audio file frame synch pattern
FF F1	AAC	ÿñ MPEG-4 Advanced Audio Coding (AAC) Low Complexity (LC) audio file
FF F9	AAC	ÿù MPEG-2 Advanced Audio Coding (AAC) Low Complexity (LC) audio file
FF FE	REG n/a	ÿþ Windows Registry file Byte-order mark (BOM) for 16-bit Unicode Transformation Format/ 2-octet Universal Character Set (UTF-16/UCS-2), little-endian files. (See the Unicode Home Page.)

Figure 4 Garrykesler

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

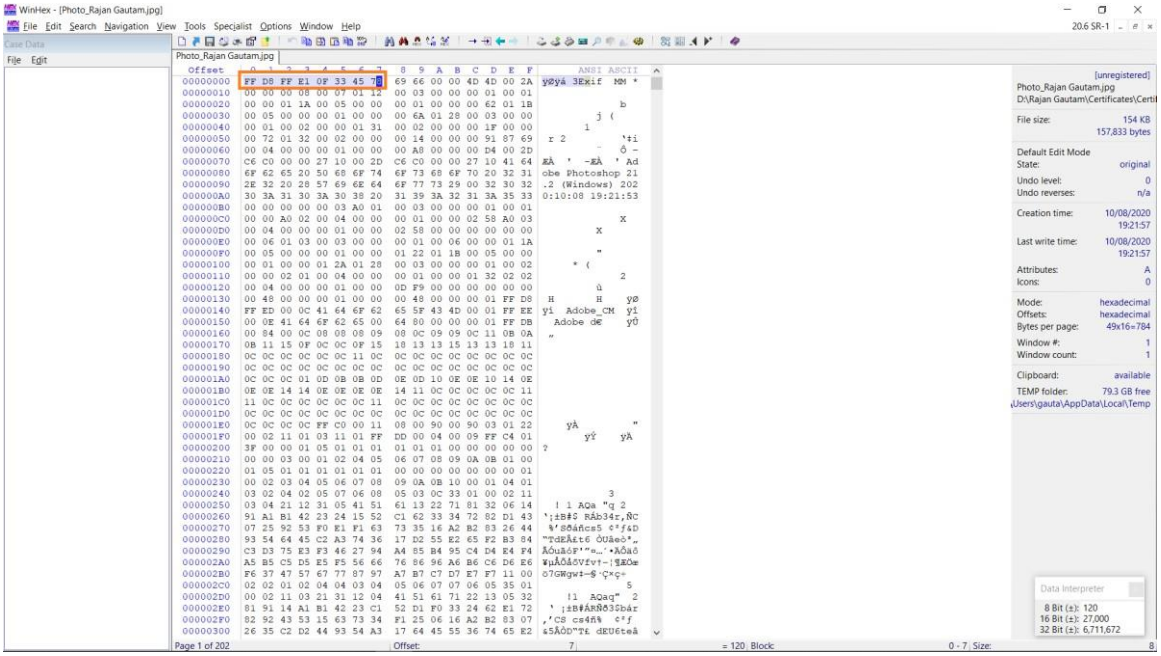


Figure 5 WinHex

5. The image was edited with Adobe photoshop, that also we can verify from the HEXCode.

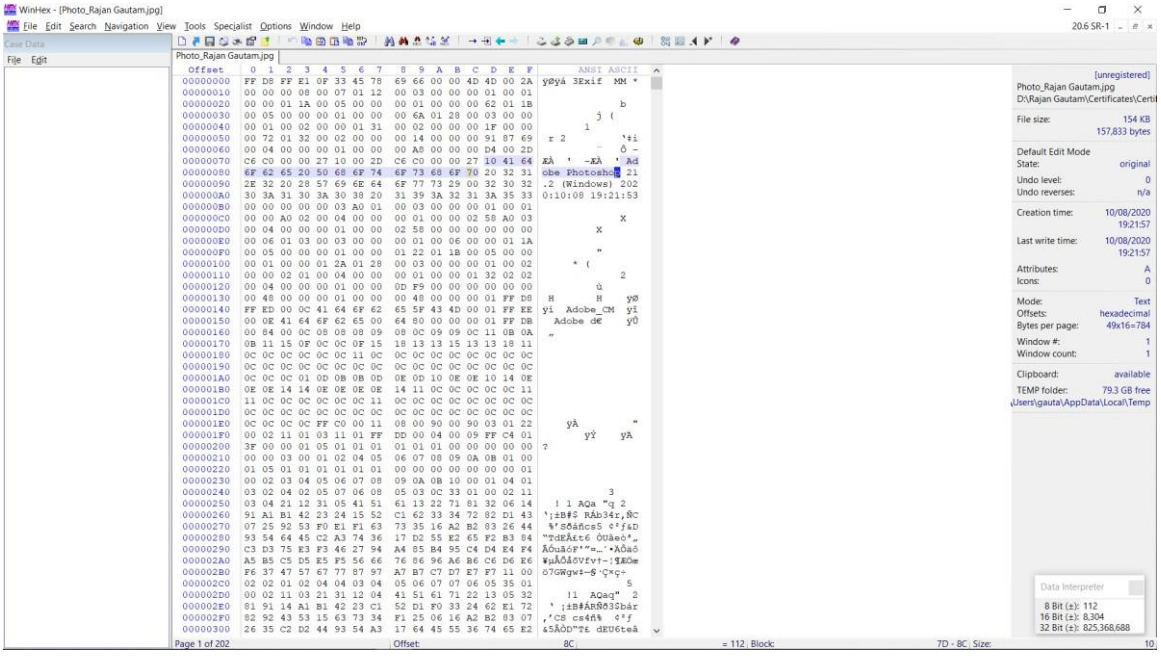
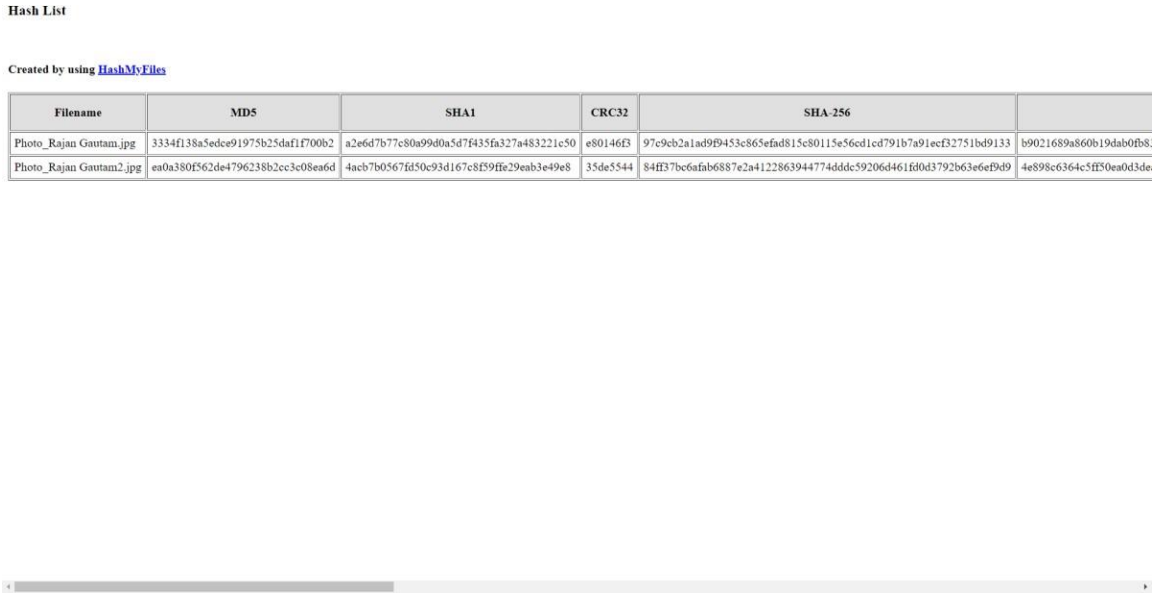


Figure 6 WinHex

6. When I updated the file using Paint and check the Hash value, I found the change inHash Valuealso.



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	ea0a380f562de4796238b2cc3c08ea6d	4acb7b0567fd50c93d167c8f59ffe29eab3e49e8	35de5544	84ff37bc6afab6887e2a4122863944774dddc59206d461fd0d3792b63e6ef9d9	4e898c6364c5ff50ea0d3de

Figure 7 Hash Valuealso.

Conclusion:

1. 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: 19-10-2022

Name:	**Parth Patel**
Roll No:	**19BCP091**
Subject Code:	**20CP411P**
Subject Name:	**Digital Forensics Lab**

Aim/Purpose: Study of a Data Acquisition tools

Tool Names:

1. FTK Manager

   FTK Manager is a powerful tool that can be used to manage forensics investigations. It provides a user-friendly interface that makes it easy to search and analyze forensic data. FTK Manager can be used to investigate a wide range of crimes, including child pornography, terrorism, and espionage.

2. Autopsy

   Autopsy is a digital forensics tool used to examine data stored on a computer. It can be used to examine data stored in a variety of formats, including images, text, and email. Autopsy can be used to investigate a variety of crimes, including murder, theft, and fraud.

Step 1: Download and Install FTK Imager

1. Visit https://accessdata.com/product-download/ftk-imagerversion-4-5 and click on Download button.

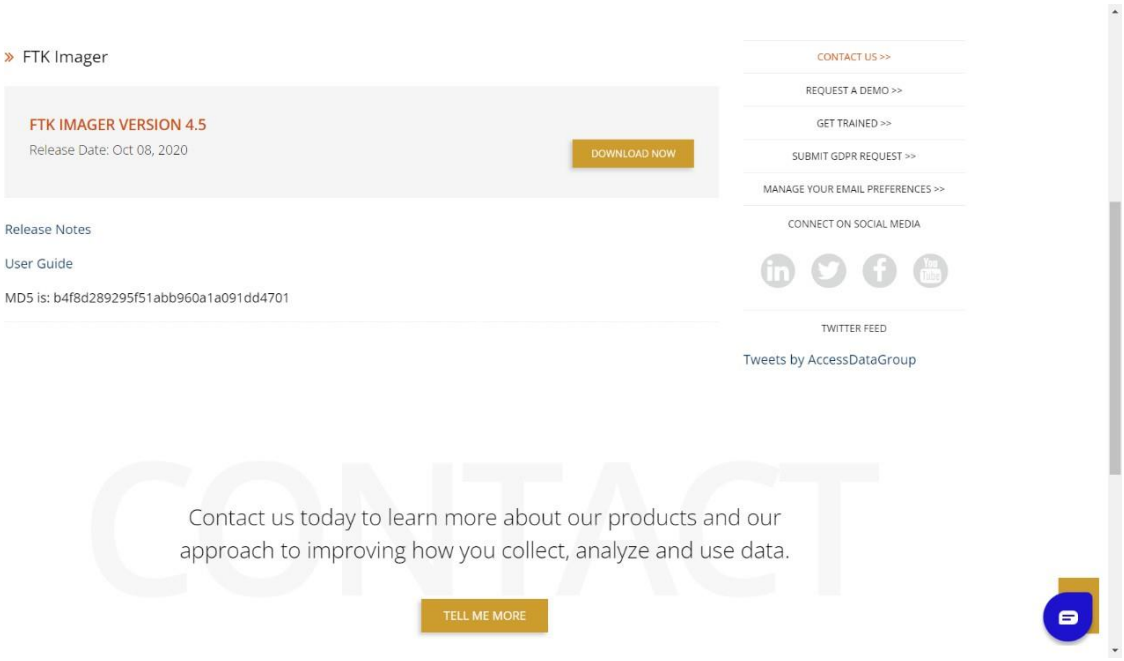


Figure 1 FTK imager

2. Install FTK Imager on your system.

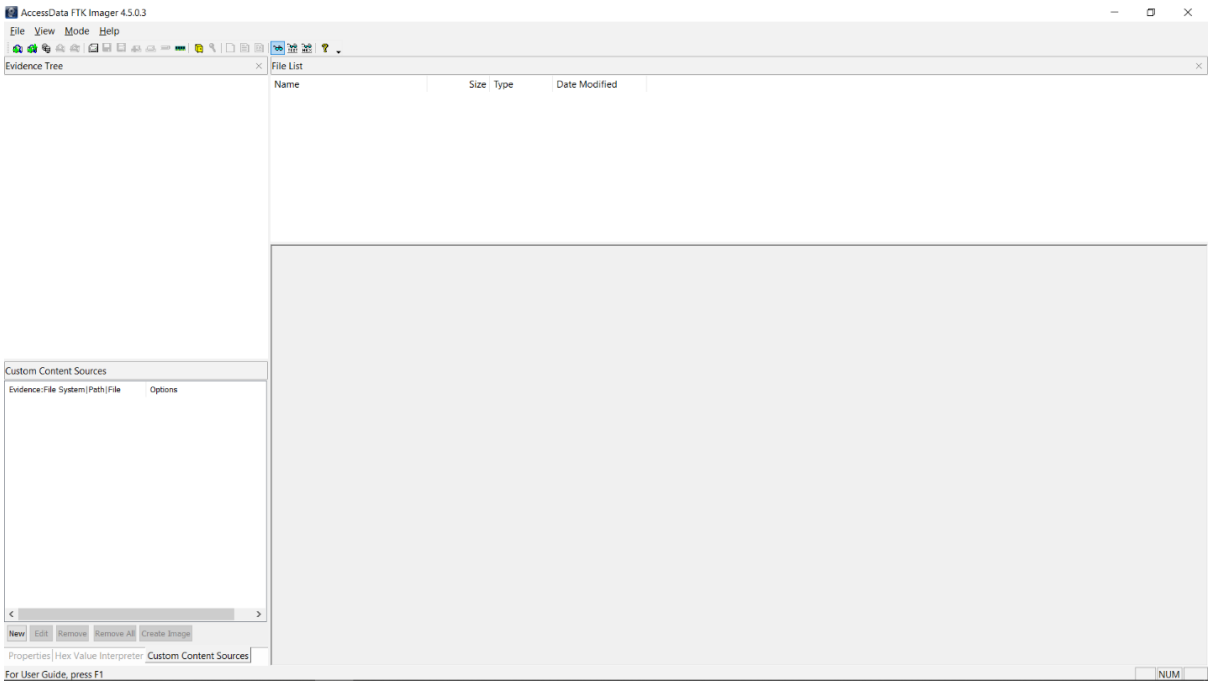


Figure 2 FTK Imager

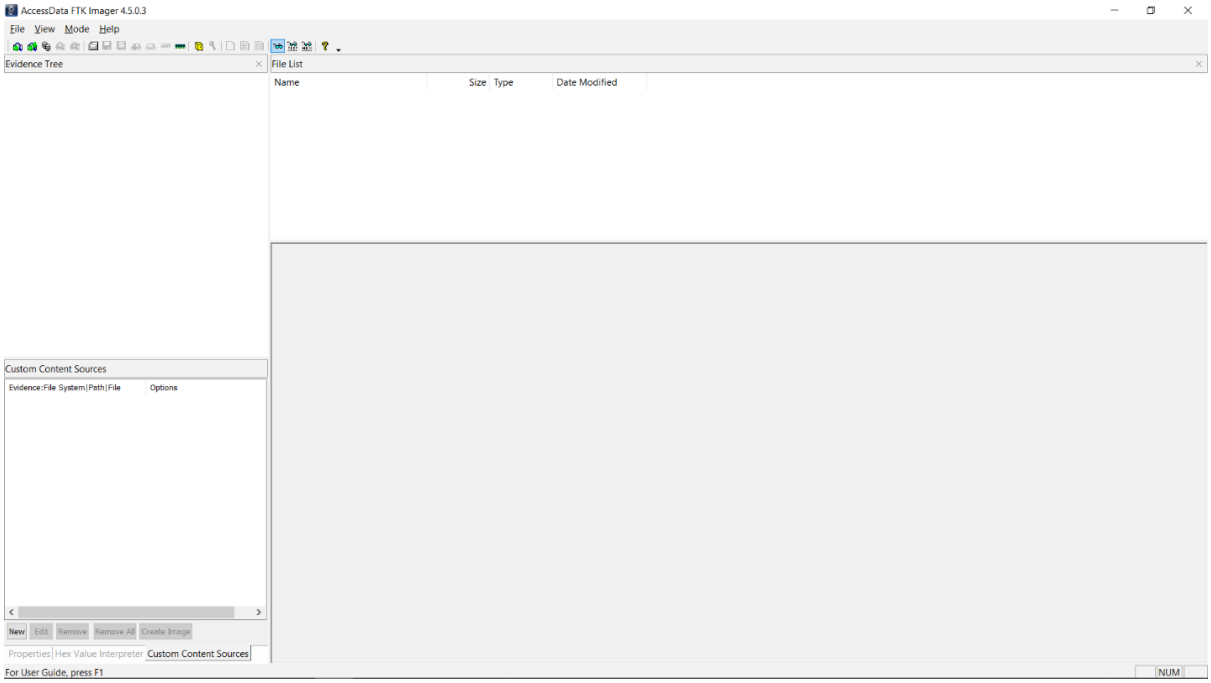


Figure 3 FTK imager

Step 2: Download and Install Autopsy

1. Visit https://www.autopsy.com/download/ and click on Download 64 – Bit.

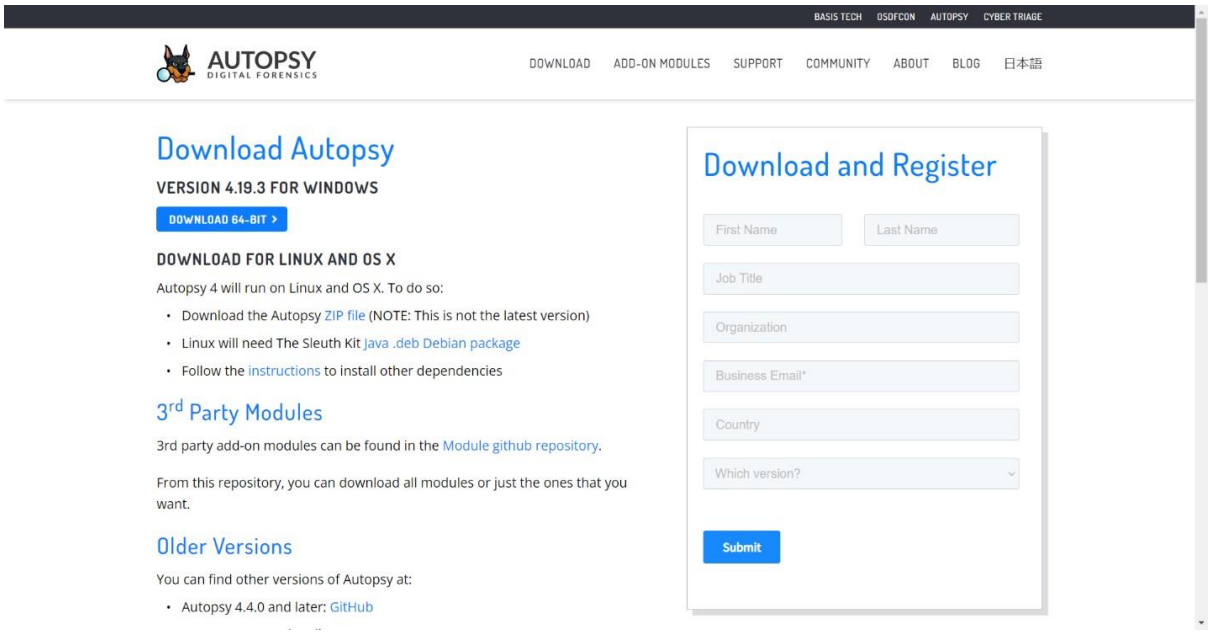


Figure 4 Autopsy

2. Install Autopsy on your system.

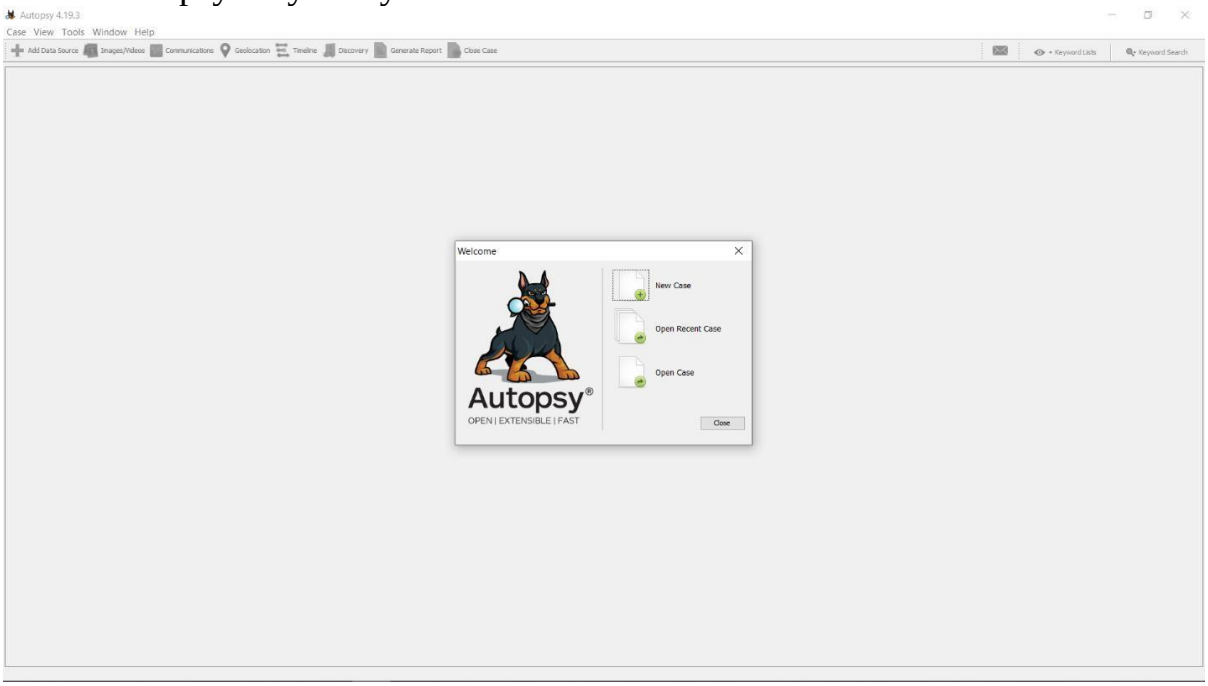


Figure 5 Autopsy

Step 3: Create Image of a Drive

1. Open FTK Imager and go to Files and Click on Create Disk Image.

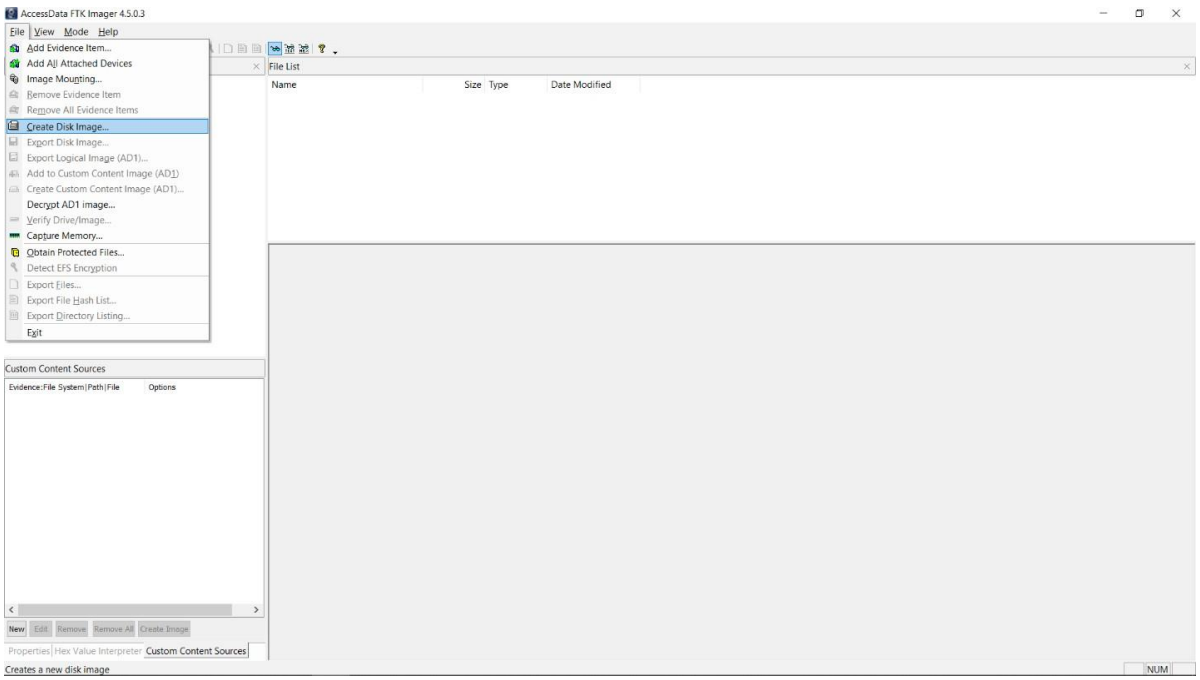


Figure 6 FTK imager

2. Select Image File and on the next screen, select image path and click on Finish

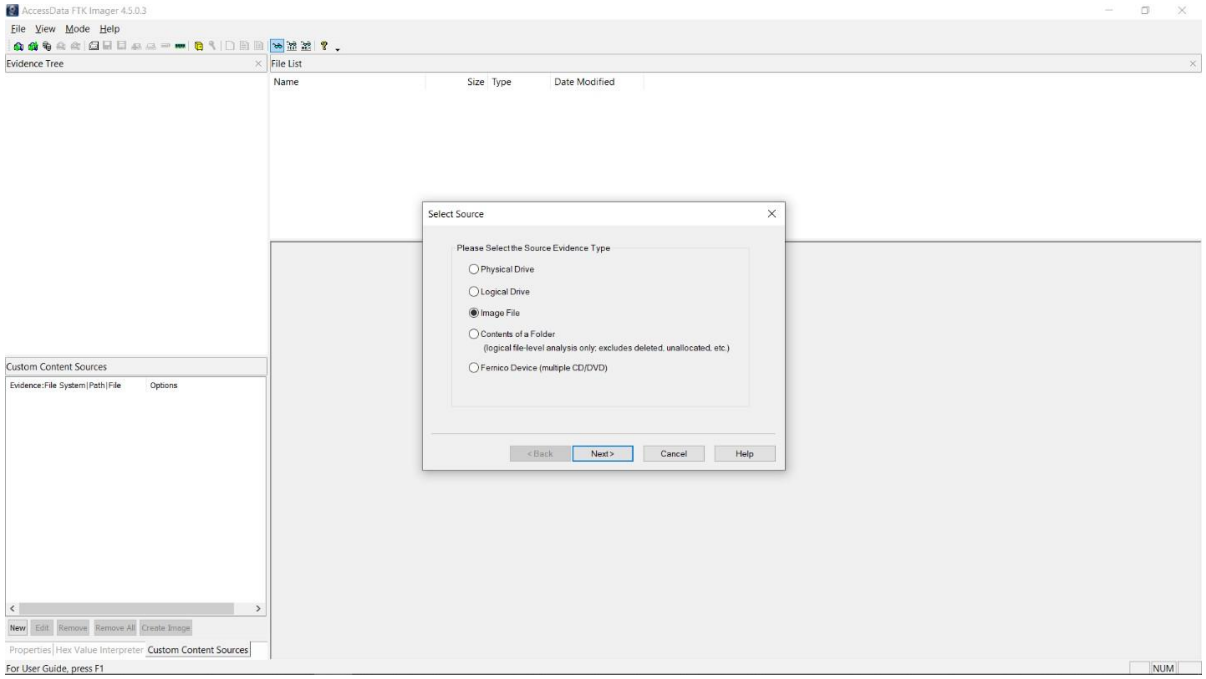


Figure 7 FTK imager

3. Select File Type as E01 and fill out the evidence details as asked.

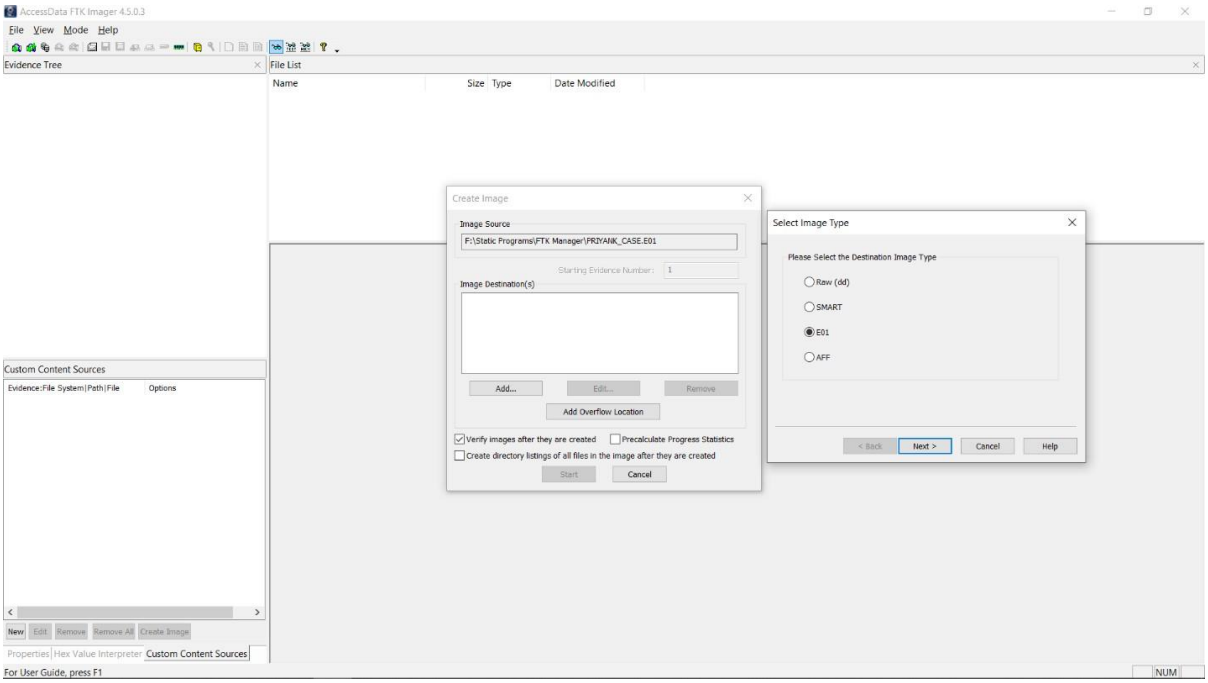


Figure 8 FTK imager

4. Wait until the image file is created

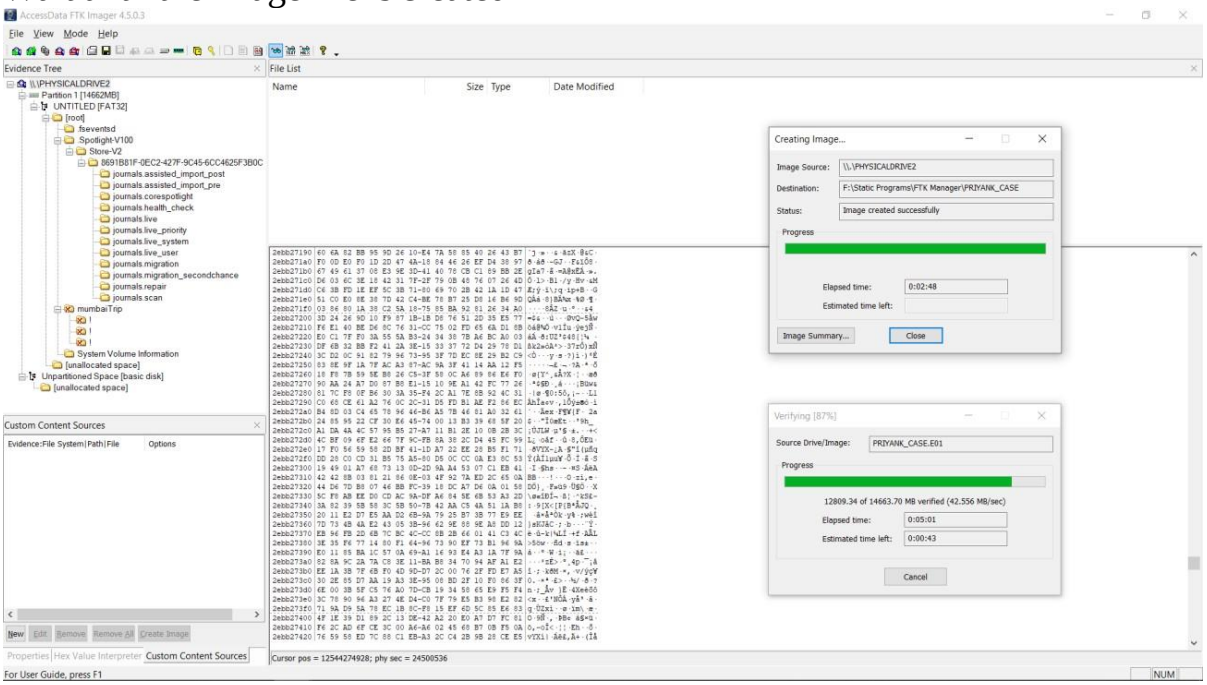


Figure 9 FTK imager

5. Once the Image is created, open Autopsy

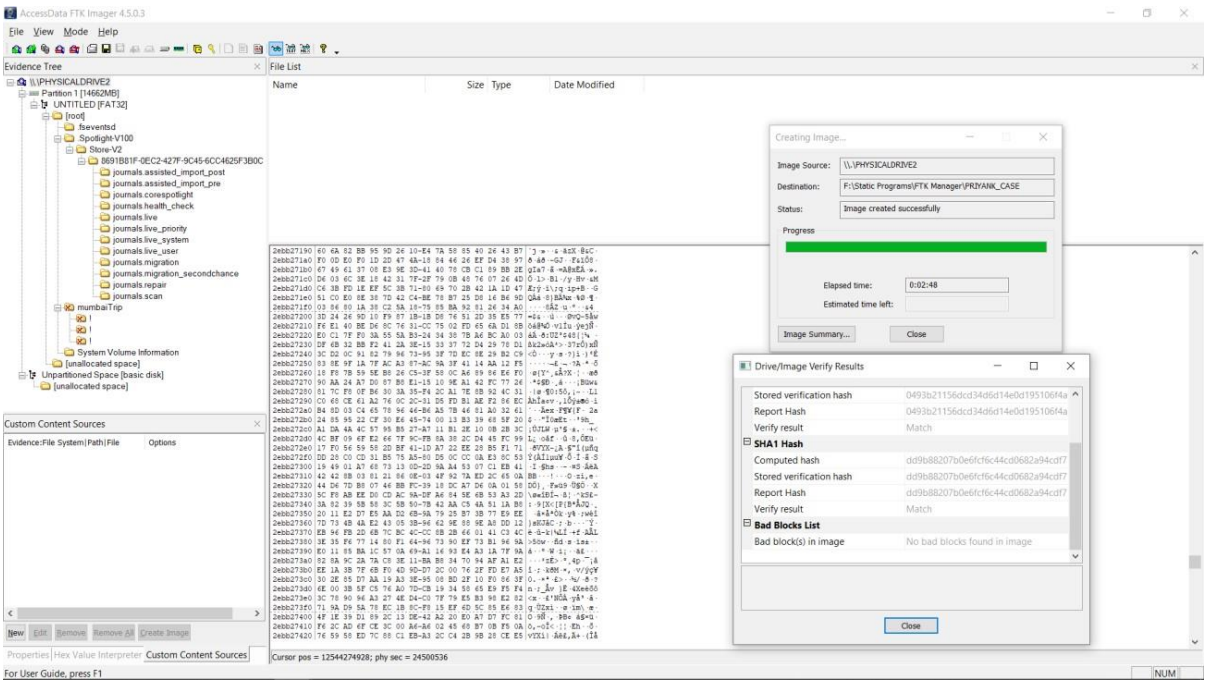


Figure 10 FTK imager

Step 4: Open Autopsy and start working on it.

1. Open Autopsy and click on New Case.

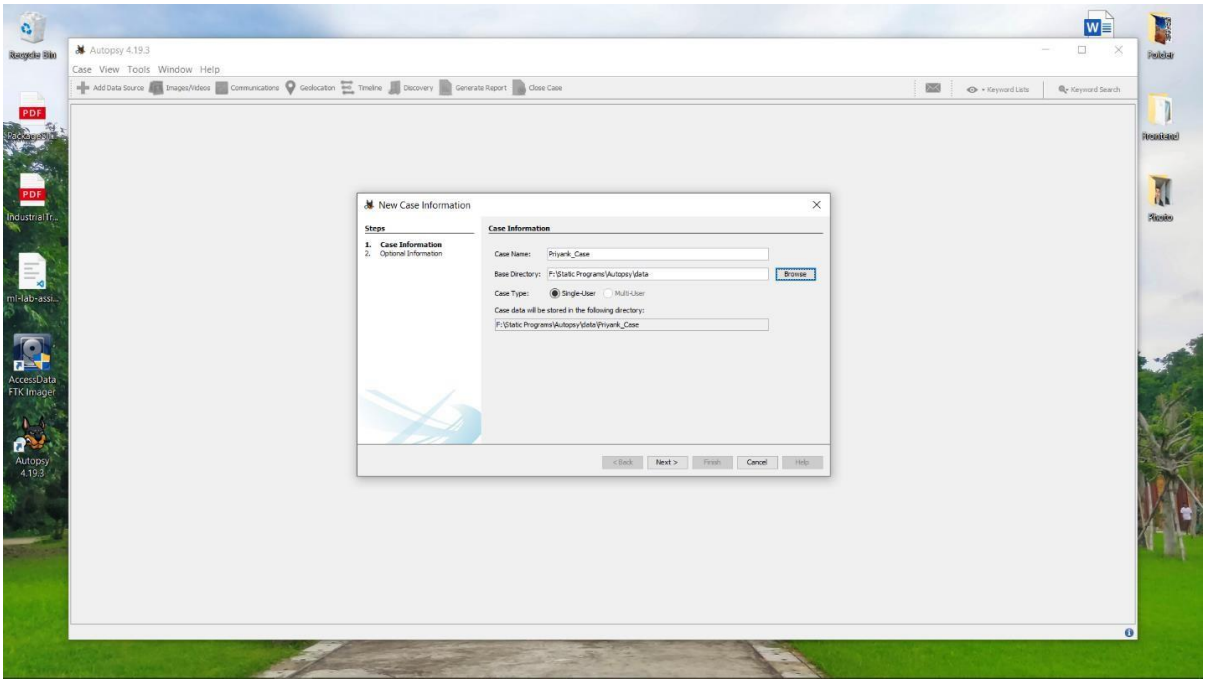


Figure 11 Autopsy

2. Fill out Case Information and Optional Information.

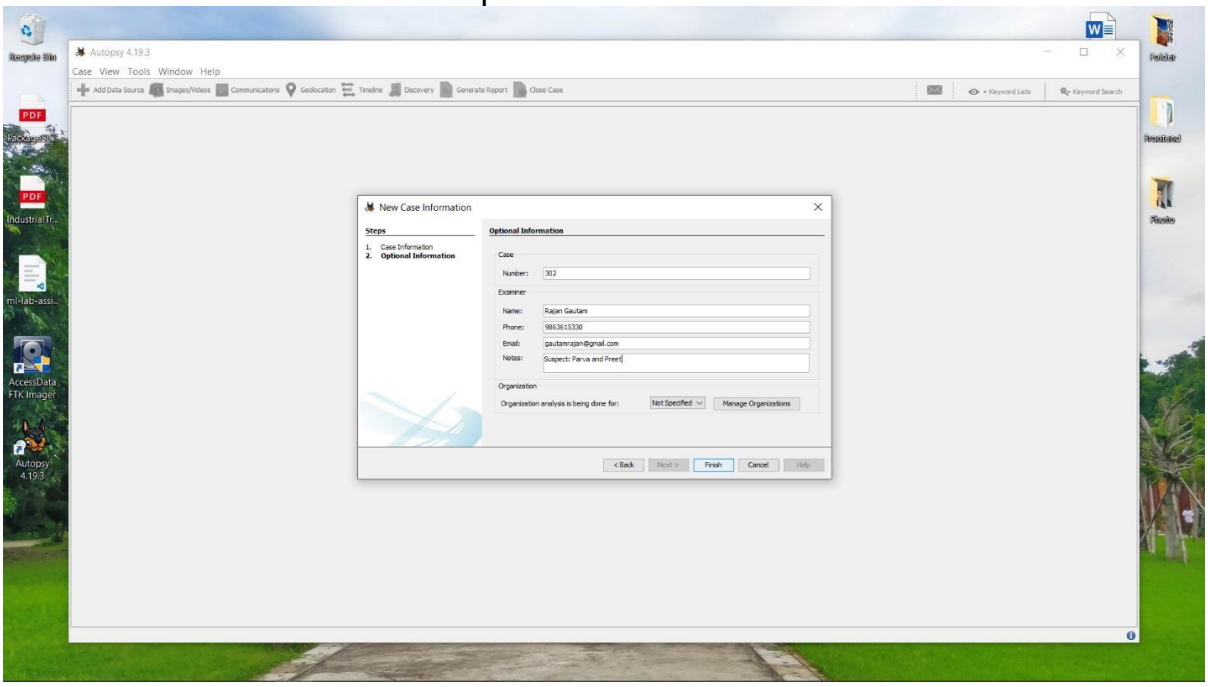


Figure 12 Autopsy

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

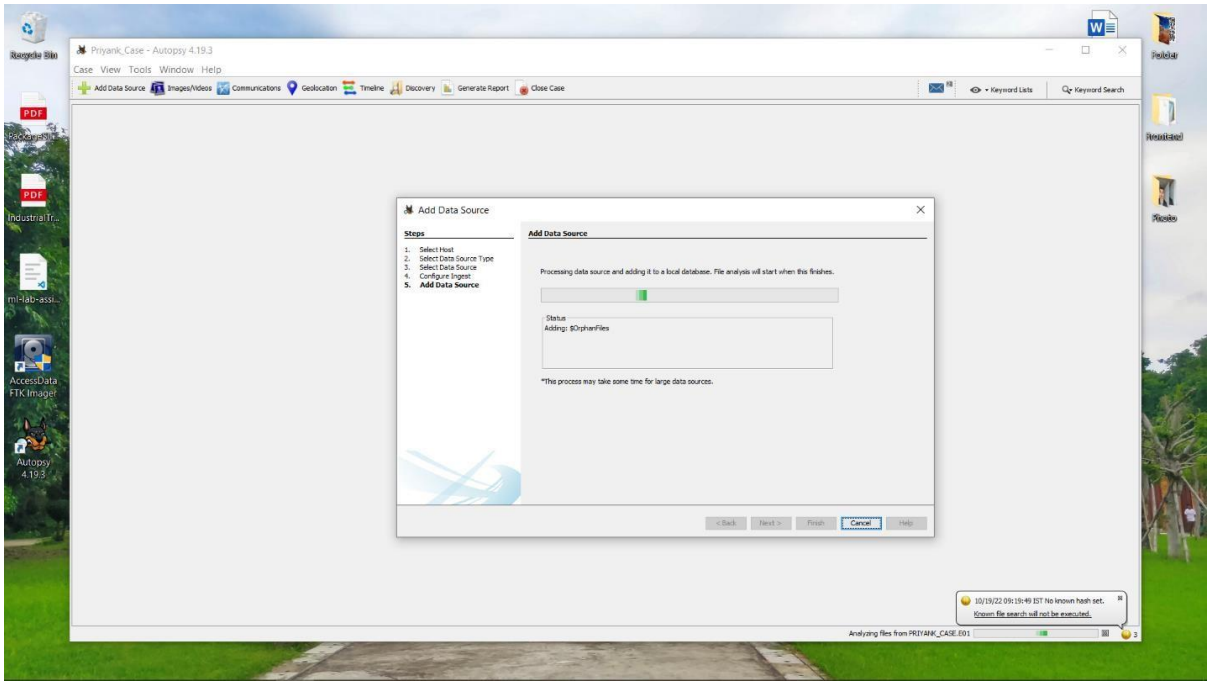


Figure 13 Autopsy

4. You can view the file contents on the screen.

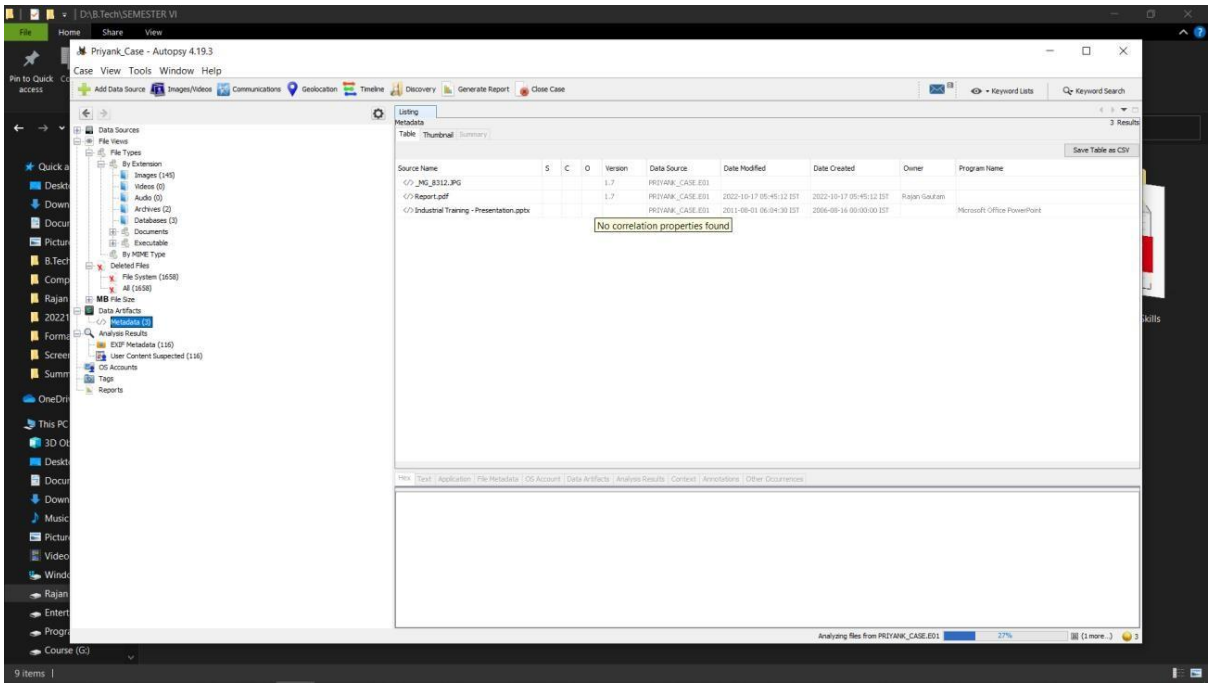


Figure 14 Autopsy

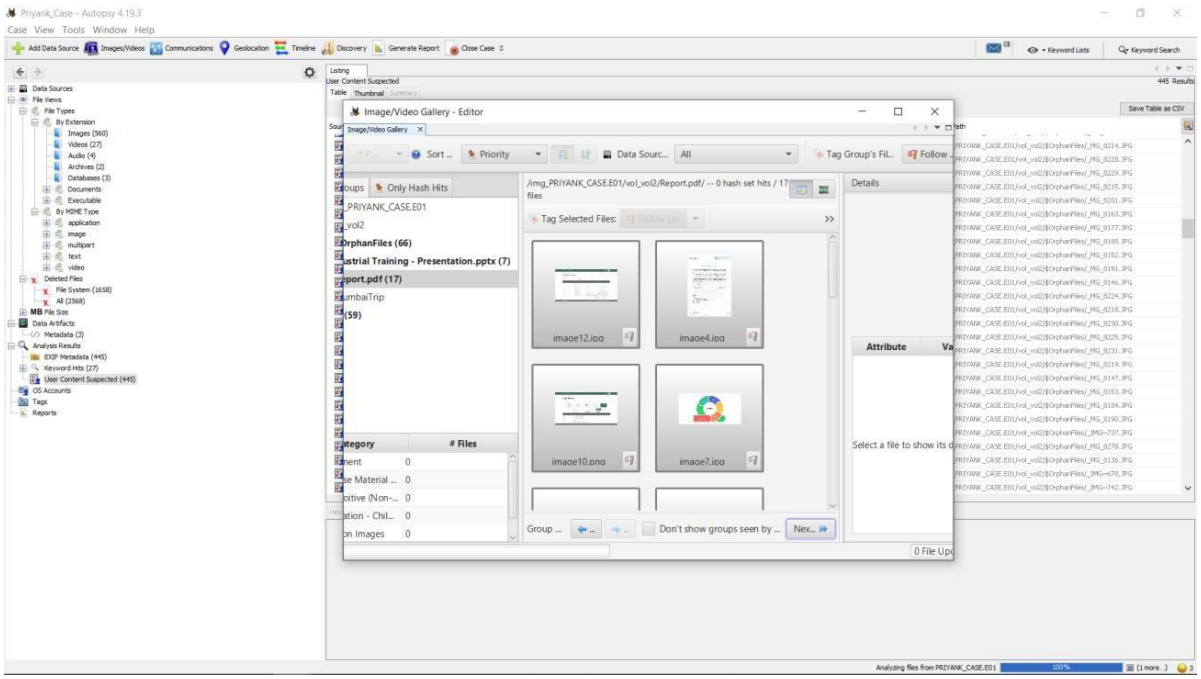


Figure 15 Autopsy

5. Click on Generate Report to generate Analysis Report.

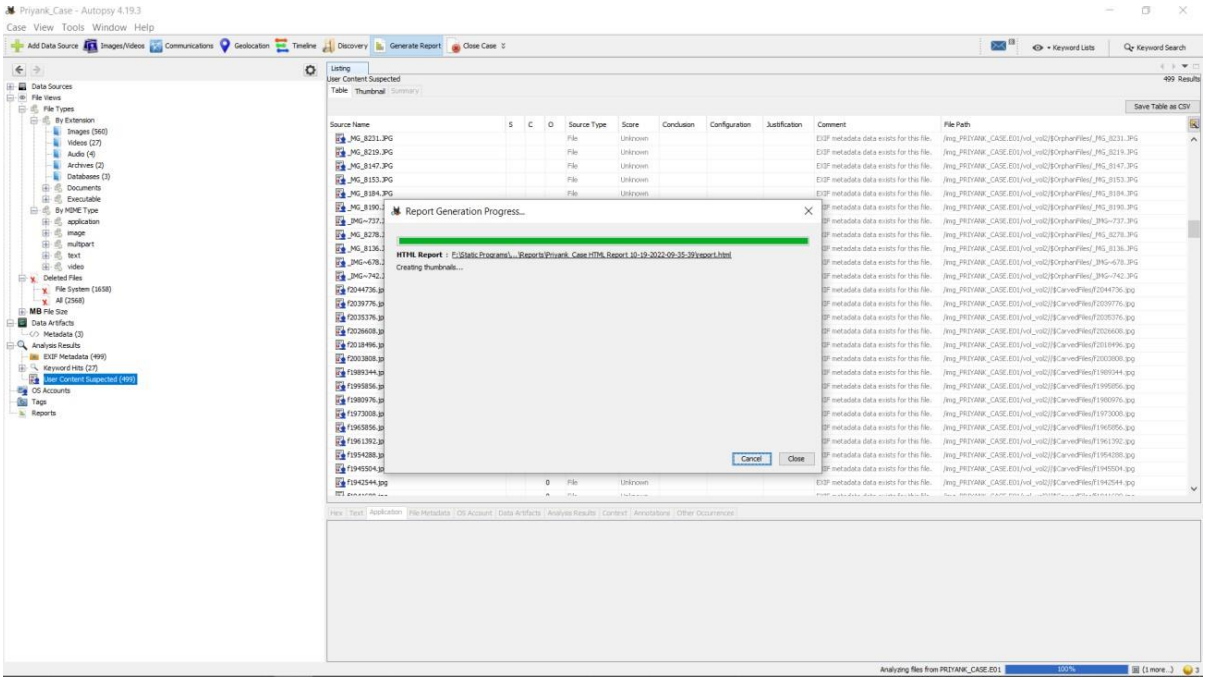


Figure 16 Autopsy

6. You can view the report in the web browser.

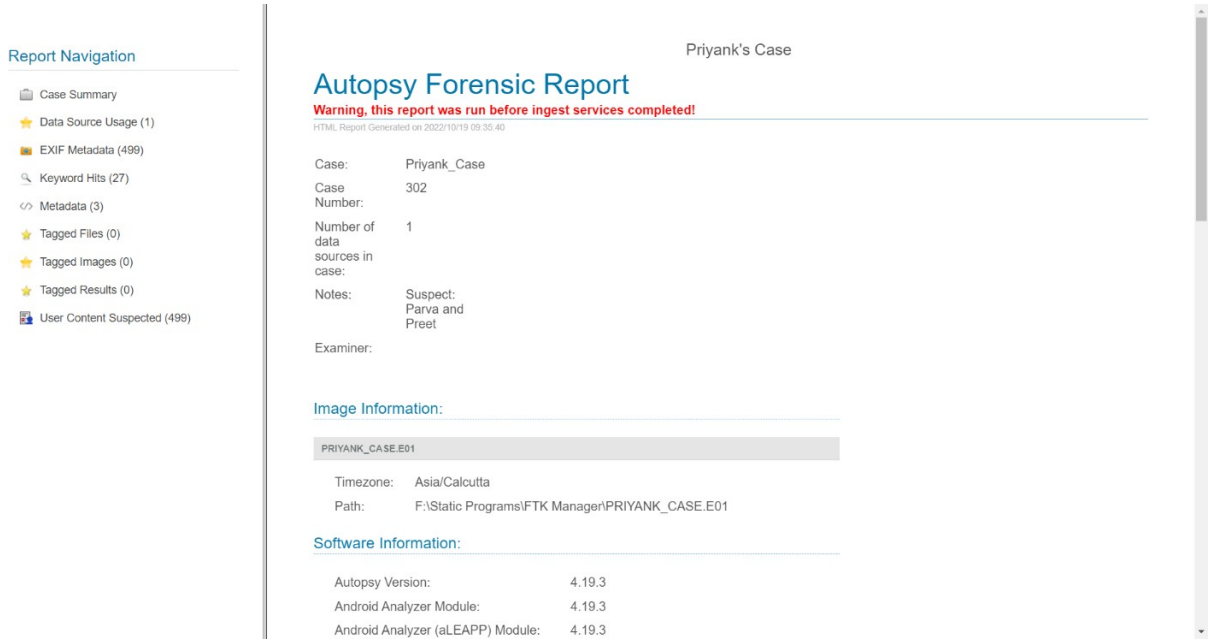


Figure 17 Autopsy

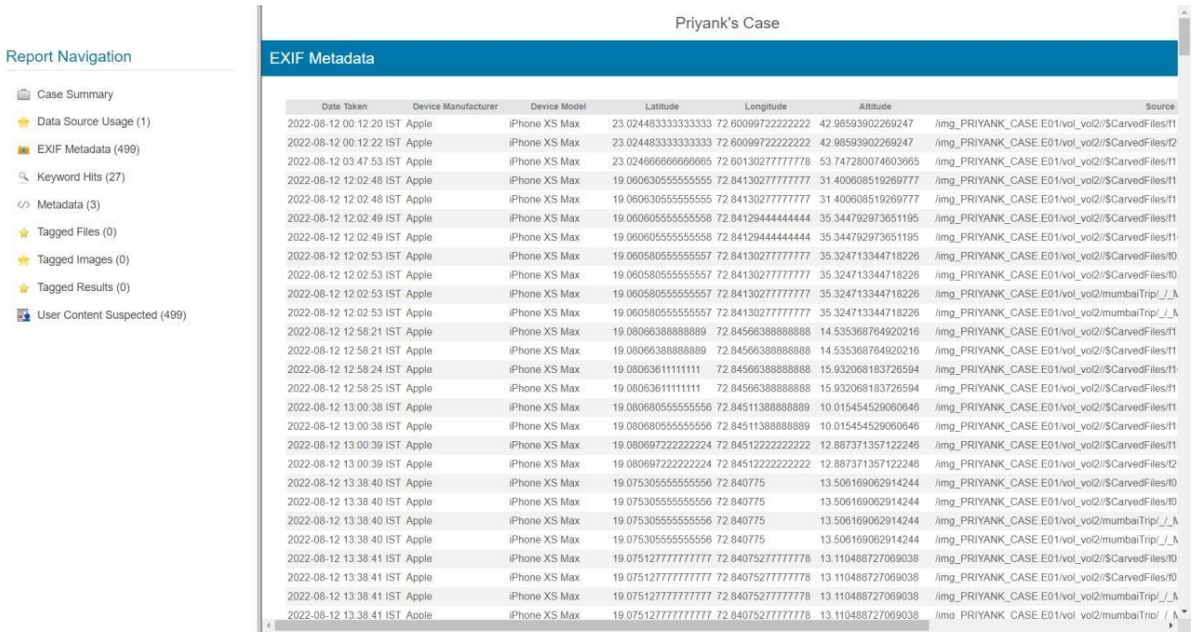


Figure 18 Autopsy

Conclusion:

1. 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.
2. 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.
3. 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.