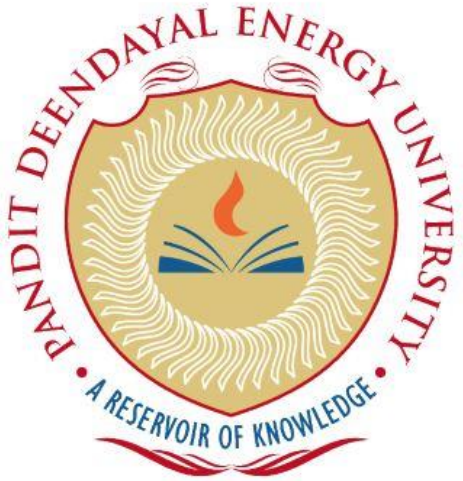
PANDIT DEENDAYAL ENERGY UNIVERSITY

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 Vedant Hareshbhai

19BCP138

G4 batch

Acknowledgement

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

Patel Vedant Hareshbhai

19BCP138

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 Vedant Hareshbhai** Roll No. **19BCP138** 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.		
2	Study of a Profile Generation using OSINT Techniques.		
3	Study of a Identification of Morphed/Edited/Fabricated portion from given Video/Audio/Image files as investigation input.		
4	Study of a Tracking & Tracing Fake Profile(s) & Fake News.		
5	Study of a Deep and Darknet Monitoring Capabilities.		
6	Study of a Data Recovery from Computer Systems, Mobile Devices, and other electronic peripherals.		
7	Study of an Email Forensics tools.		
8	Study of a Volatile Memory Forensics tools.		
9	Study of a Hash and Hex analysis tools		
10	Study of a Data Acquisition tools.		

Digital Forensics Lab Report: 1

Date: 27-07-2022

Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Perform Steganography using Stegano tools

Tool Names: Quick Stego, Deep Sound, Oursecret, Wbstego, Quickcrypto, spam mimic

Task 1: Perform Image Steganography

Steps:

1. Install and run the Quickstego tool
2. Select the “Open Image” button to open a file browser and select the carrier file (image) to perform the stego operation
3. Write a secret message in an empty box situated on the right side of the tool and click on hide text
4. Click on “Save Image” to save the stego file

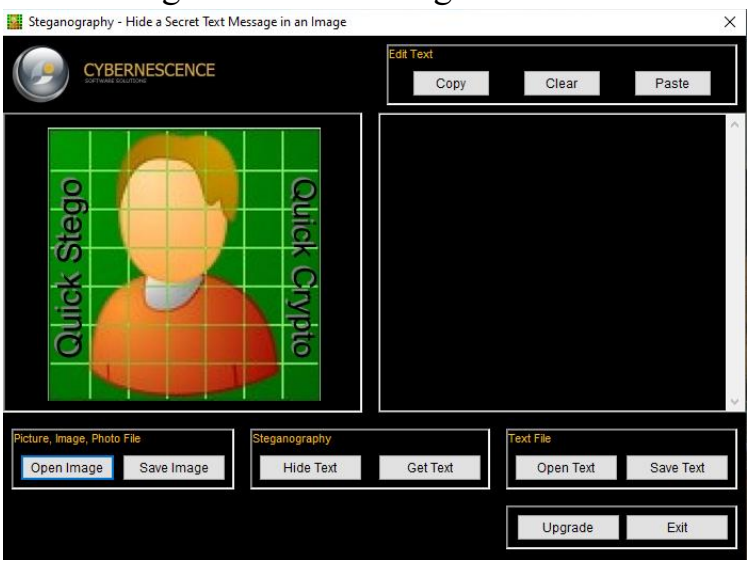


Fig **Quick Stego Tool**

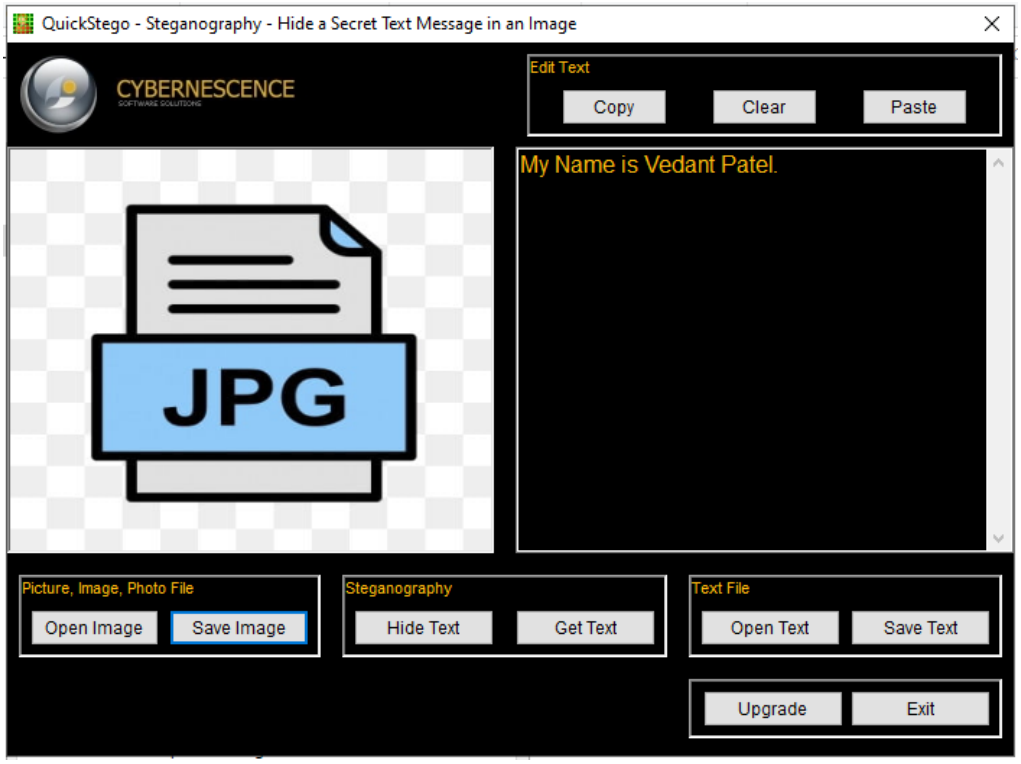


***Fig* Storing Secret Message**

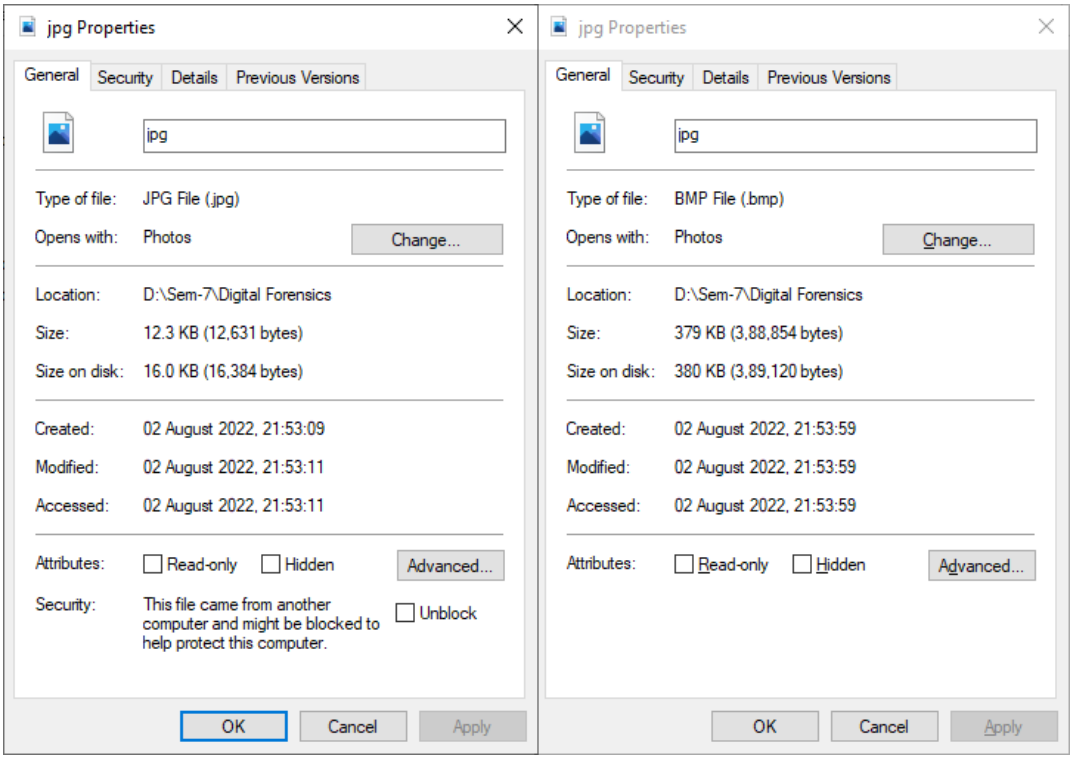


***Fig* File comparison of the original file and Stego file**

Analysis:

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

Similar Tools:

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

Task 2: Perform Video Steganography

Steps:

1. Download it from the link given above and after that run it from the directory where you have downloaded it.
2. Now, click on the Hide button to enter the main interface of OpenPuff.
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.
4. Navigate to the second section that is Carrier Selection, and provide the carrier video file that you want to use for hiding your messages/documents. Here you can also add multiple carrier video files to hide your data in them. And all the carrier videos that you use will play in the same manner as they were before. You will not be able to identify whether a video has any hidden file in it or not.
5. Provide the target file that you want to hide in the carrier video file and then hit the Hide Data button to complete the process.

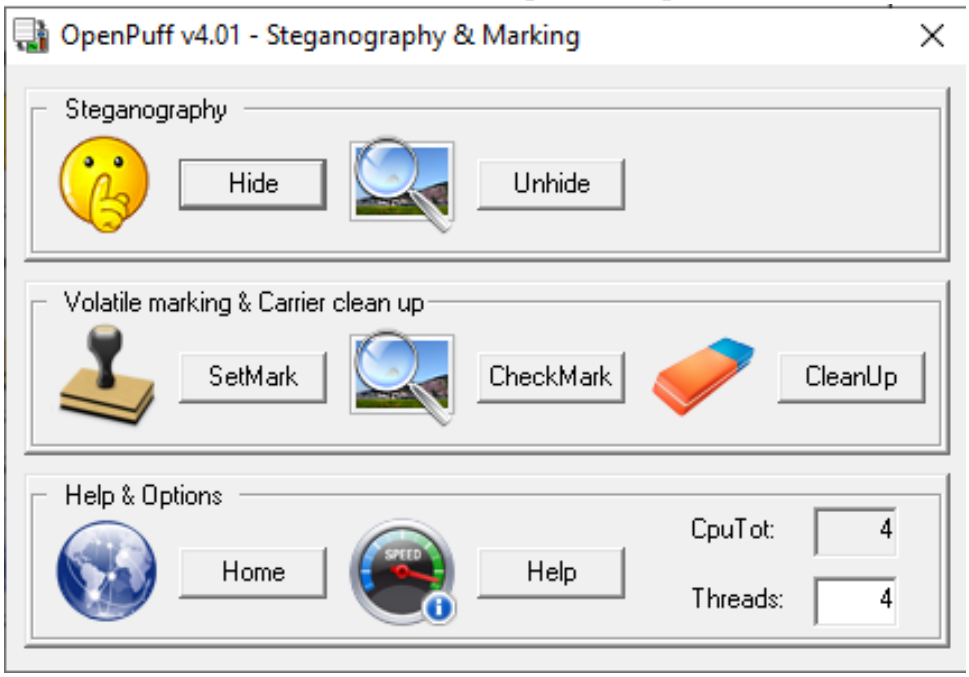


***Fig* OpenPuff tool**

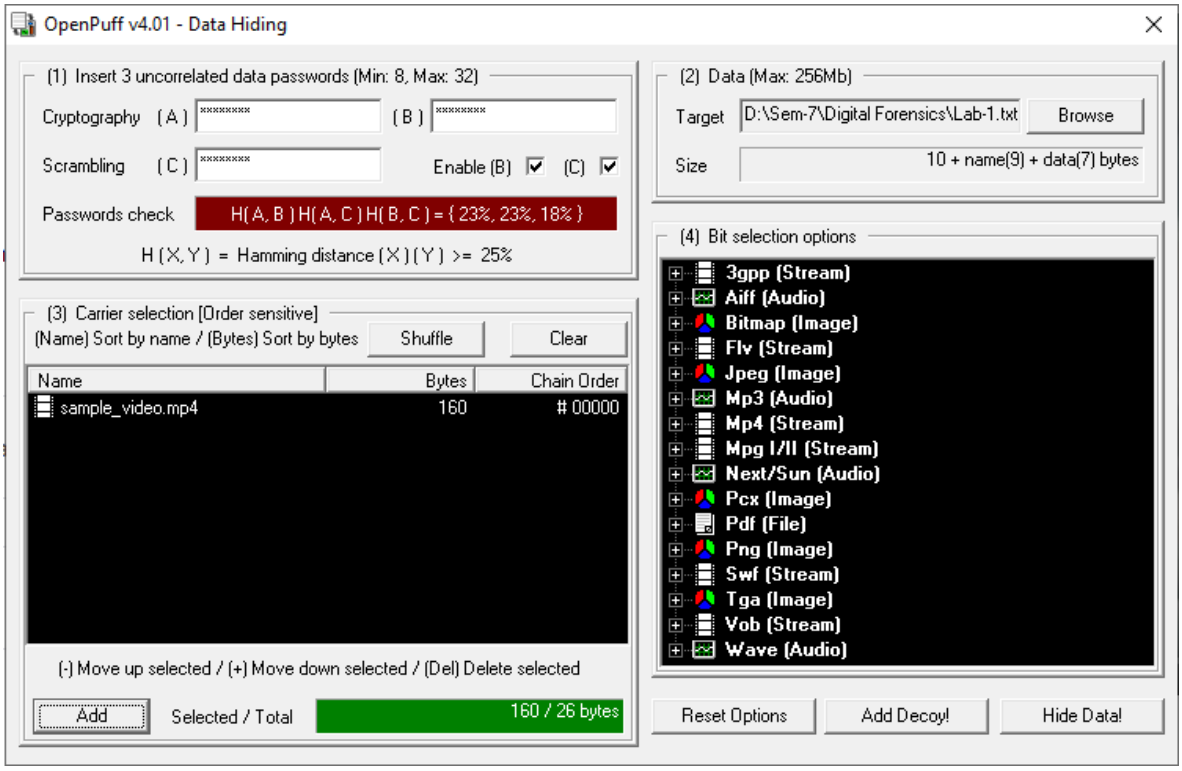


Fig **To encode video file to hide the text file**

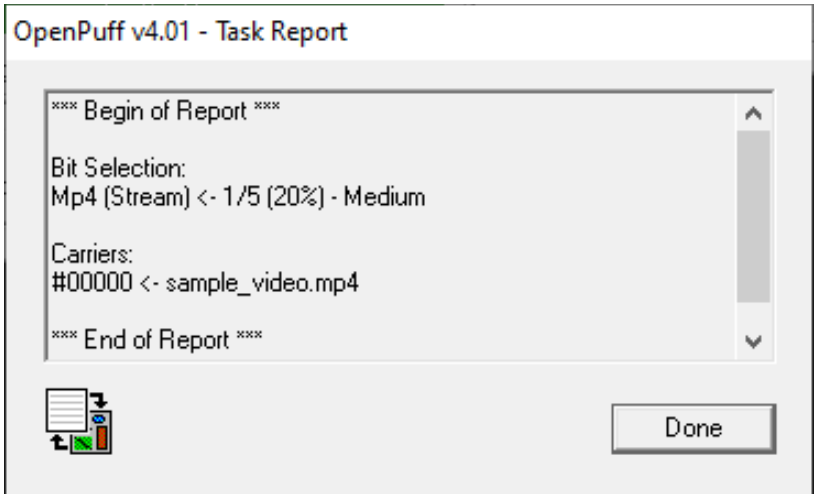


Fig Final report

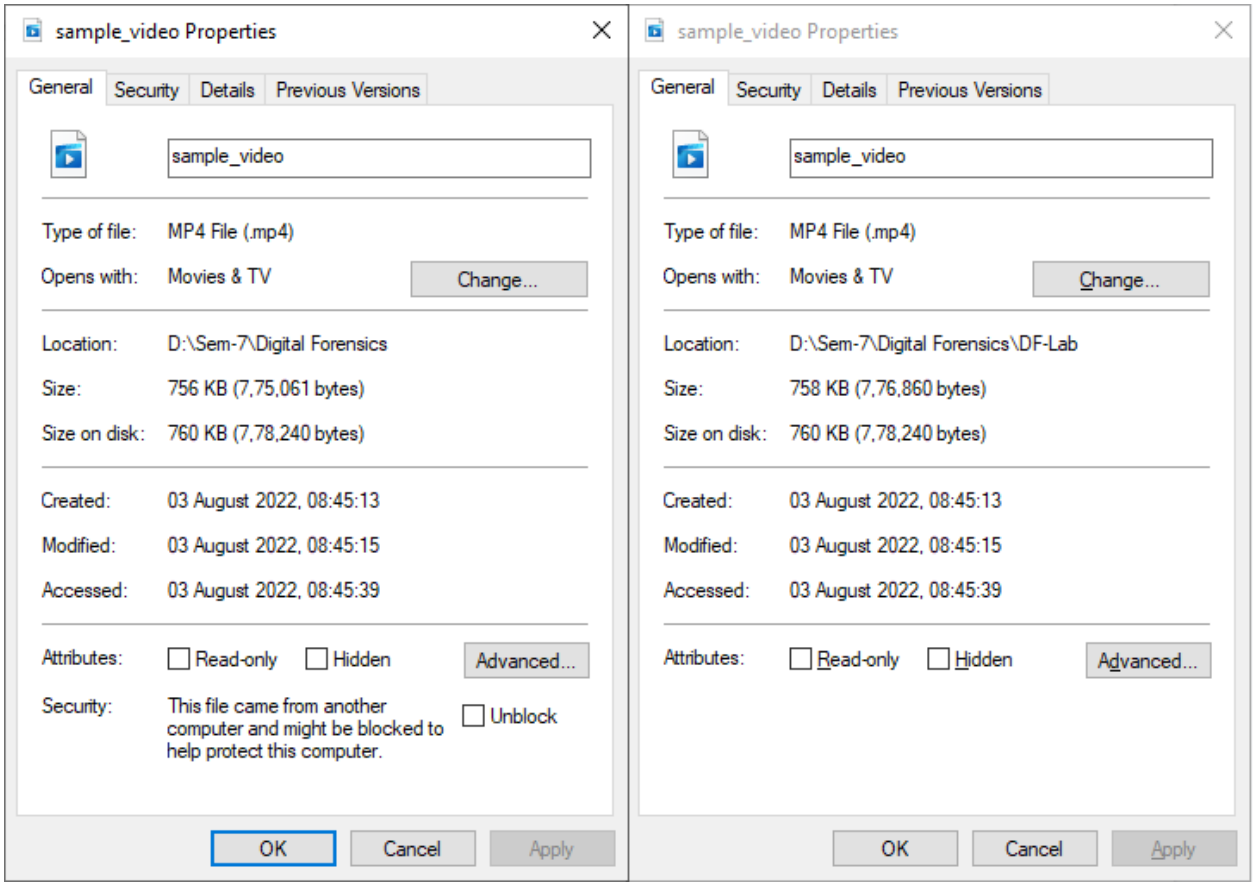


Fig Size difference between both file

Analysis:

1. A Prototype for Secure Information using Embedding Algorithm and Extracting Algorithm which decrease the discolor pixels in every frame, to increase the embedded Capacity in compressed video steganography.

Task 3: Perform Audio Steganography

Steps:

1. Install and run the Deep sound tool
2. Select the “Open Carrier File” button to open a file browser and select the carrier file (audio) to perform the stego operation
3. Select the “Add Secret Files” button to open a file browser and select the secret files to hide.
4. Click on the “Encode Secret File” button. Select the output file format and set the password for the stegno file and it will be saved to your set directory.

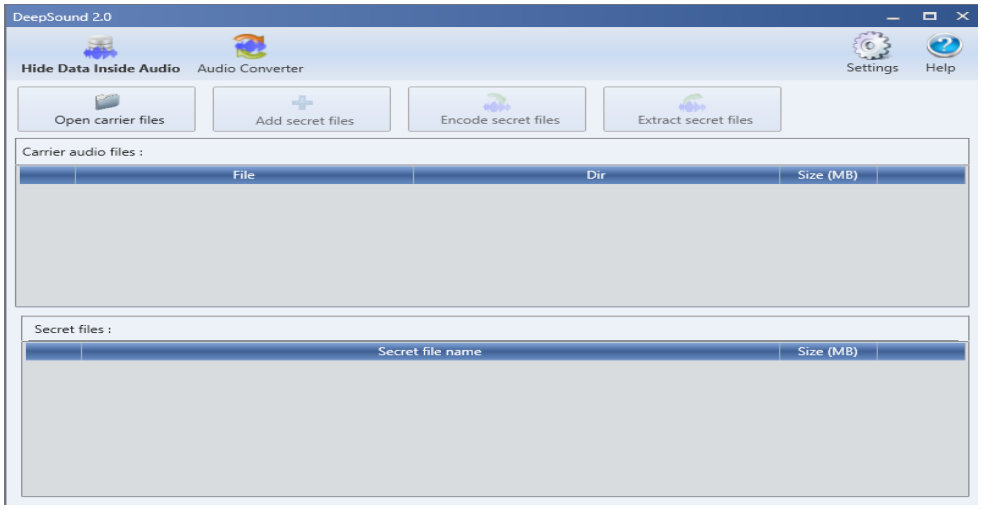


***Fig* DeepSound Tool**

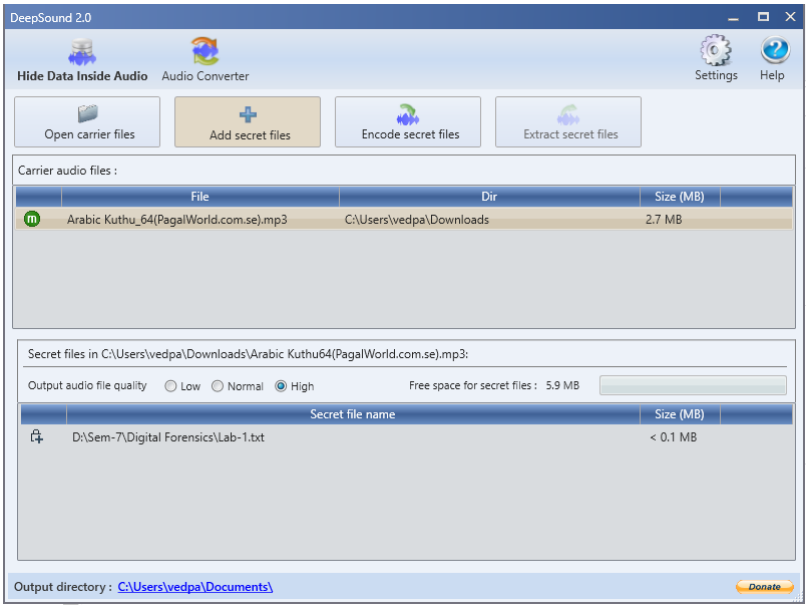


***Fig* Storing Secret File to Audio carrier**

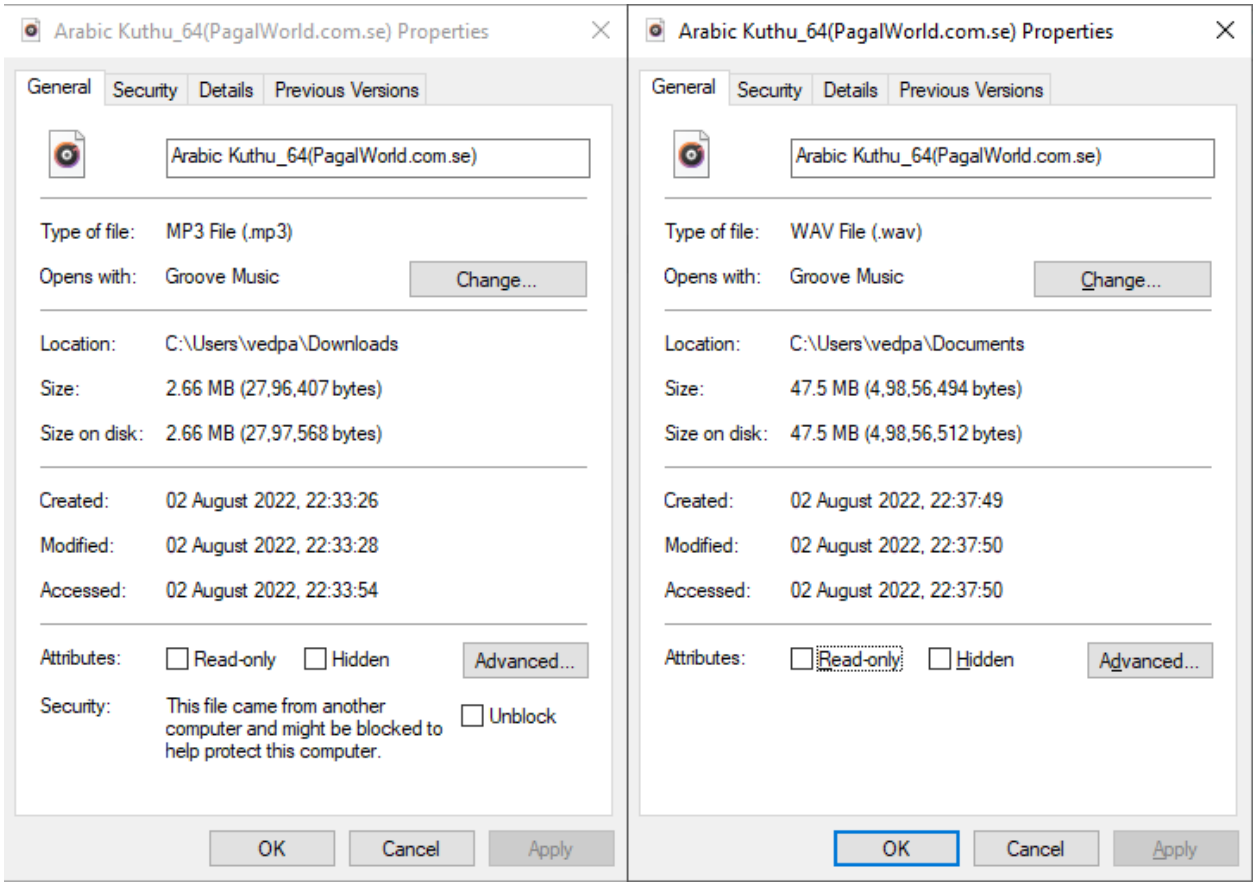


***Fig* File comparison of the original file and Stego file**

Analysis:

1. While comparing the original file with the stego file (encoded file) we can see many differences in both files
2. The file format is different, the file size is different and the timestamp is different.

Task 4: Perform Steganography using Quickcrypto Tool

Steps:

1. Install and run the Quickcrypto tool
2. Select the “Hide Folder” button to open a file browser and select the Folder to hide.
3. It will hide the folder and show messages as per figures.

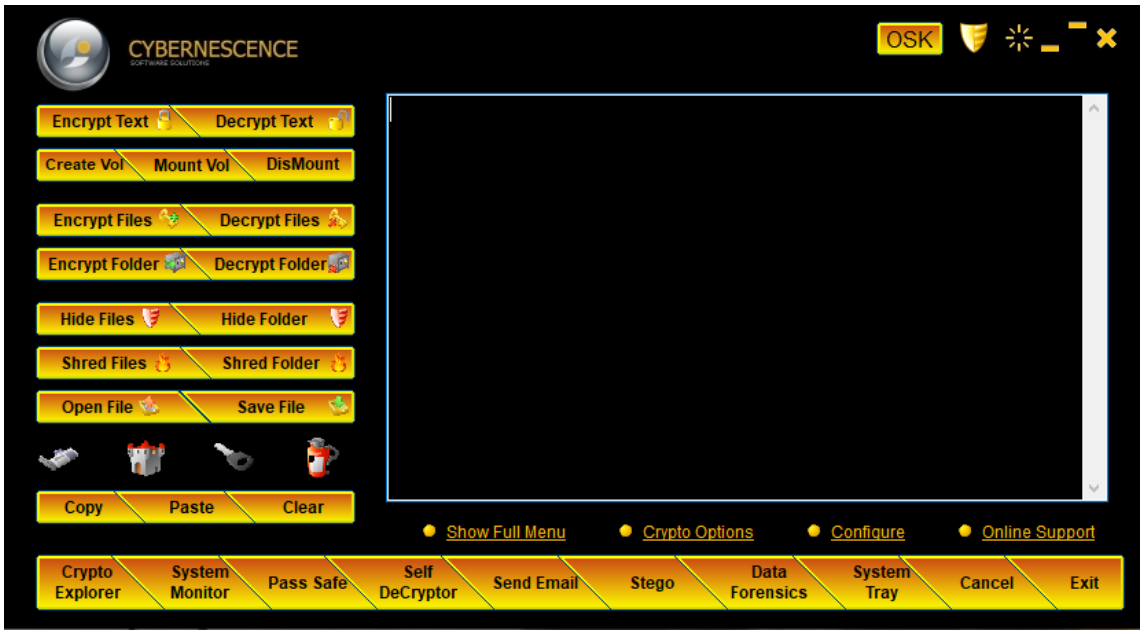


Fig **Quickcrypto Tool**

Fig **Hiding the secret folder**

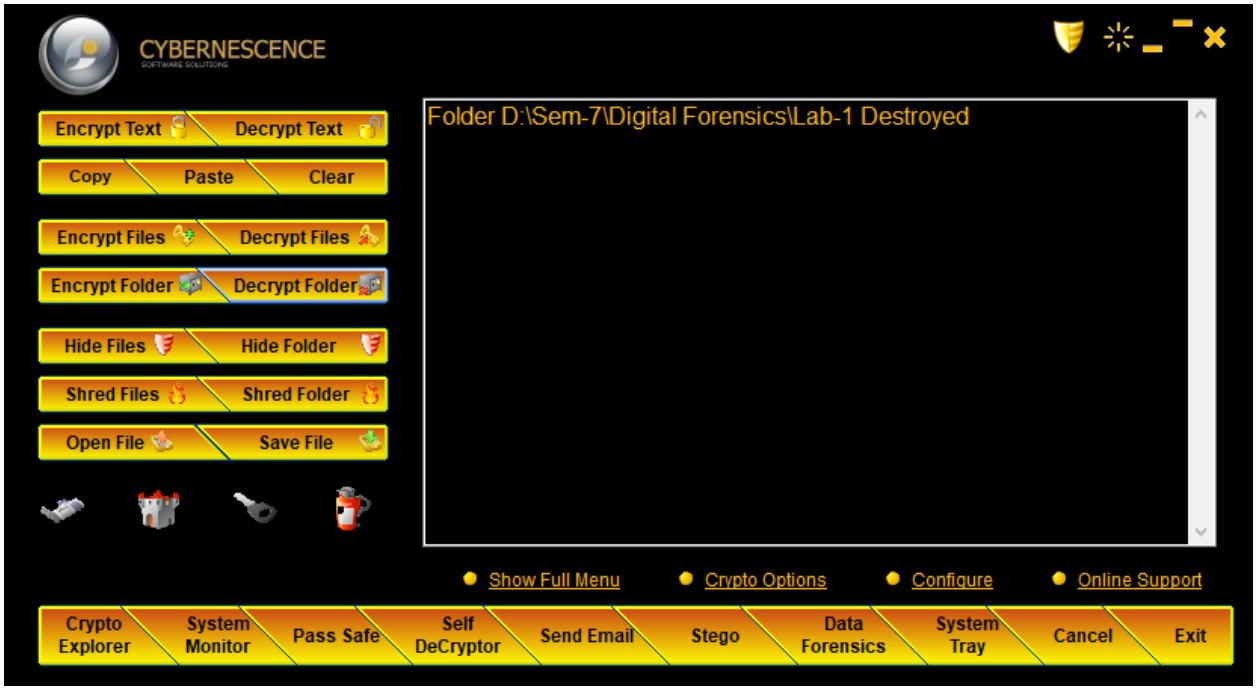


Fig **Folder Hidden**

Analysis:

1. It allows you to hide files on your system so only you can recover and use them.
2. Also conceal sensitive data (text and files of any type) into innocent 'carrier' files: JPEG, GIF, BMP, MP3, and WAV. Easily blend encrypted files and messages into many other files.

Task 5: Perform Steganography using Spammimic Tool

Steps:

1. Open the website: www.spammimic.com
2. Select the Encoding method to encode your secret message.
3. Write your secret message and click on the “Encode” button.
4. To decode your secret message click on the “Decode” button and select the encoded format to decode.
5. Write your encoded message and click on the "Decode" button it will show you the secret message.

***Fig* Spammimic Tool**

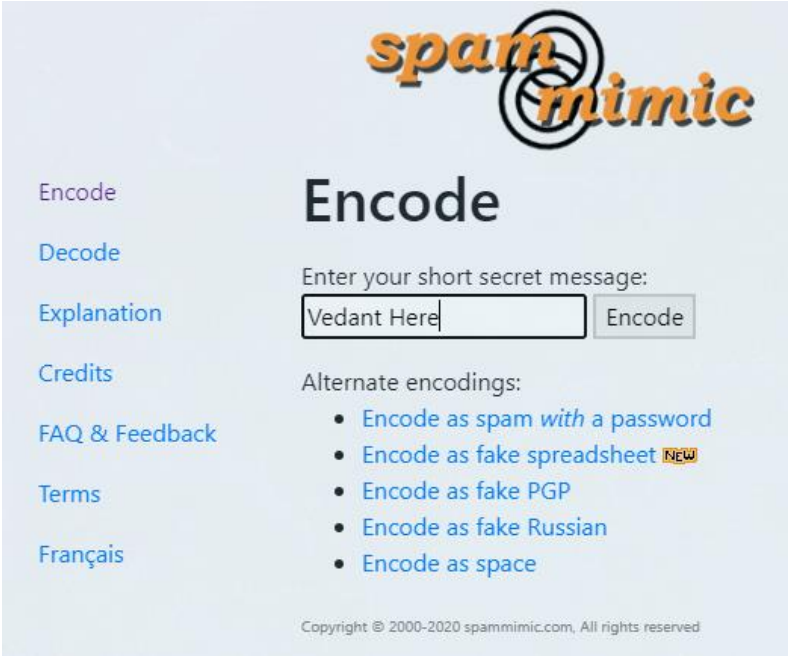


***Fig* Encode secret message**

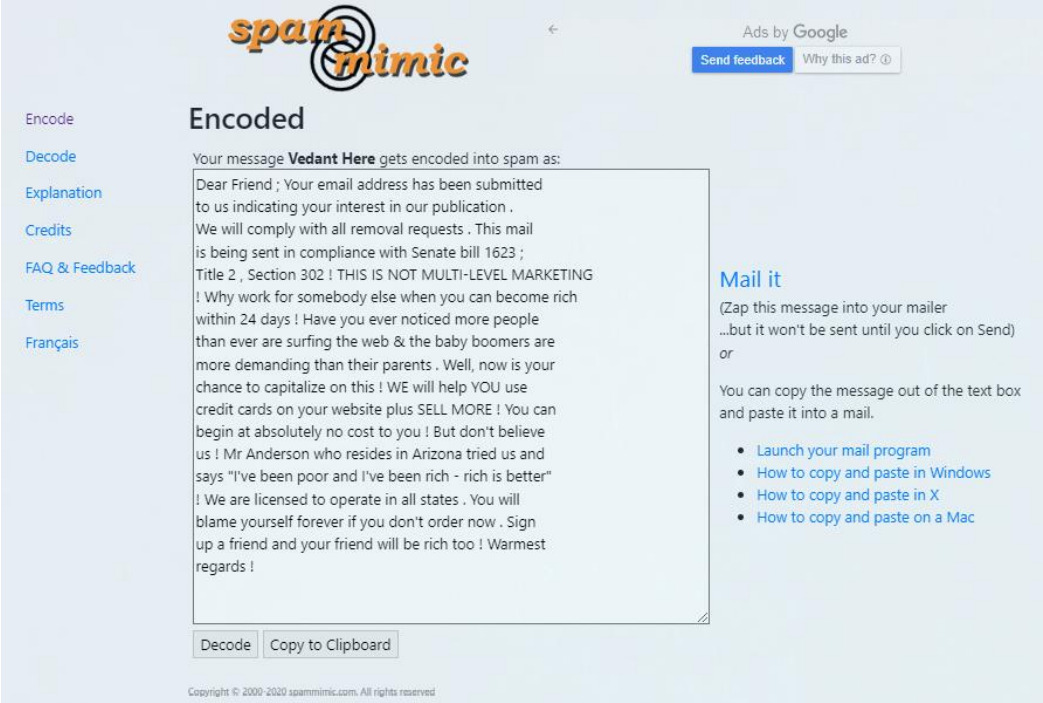


Fig **Encoded message**

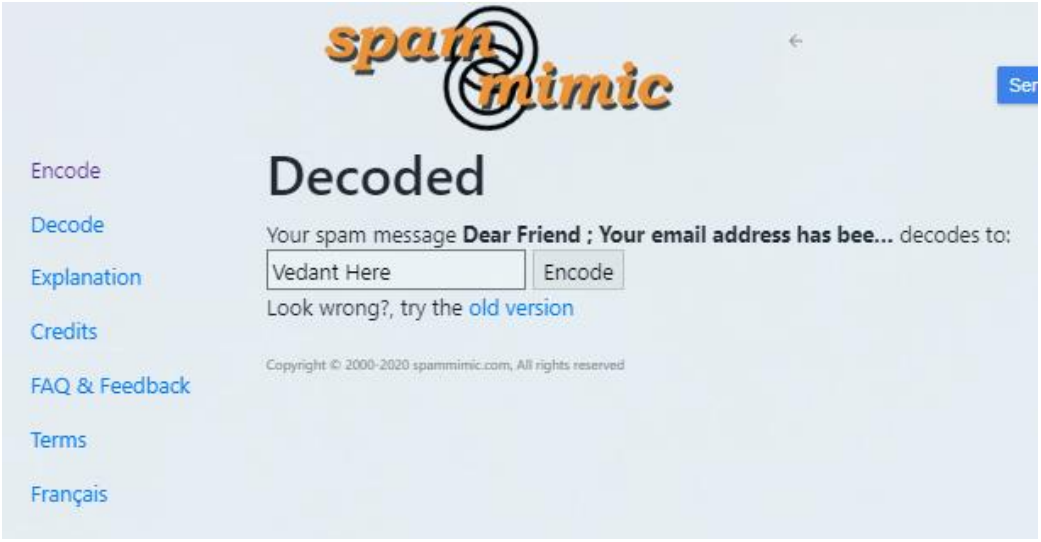


Fig **Decode secret message**

Analysis:

1. It allows you 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.

Other Steganography Tools:

- Camouflage (Imager Steganography)
- Ssuite Picsel (Imager Steganography)
- Hide n Send (Imager Steganography)
- OpenStego
- crypture
- Steghide
- Xiao Steganography (Imager Steganography)
- Quickstego (Imager Steganography)
- wbStego (Document Steganography)
- Our secret (Video Steganography)
- Quick crypto (Folder Steganography)
- Deep Sound
- Sonic visualizer
- Openpuff
- Netcross
- StegDetect
- Spammimic Web (Mail Steganography)

Digital Forensics Lab Report: 2

Date: 03-08-2022

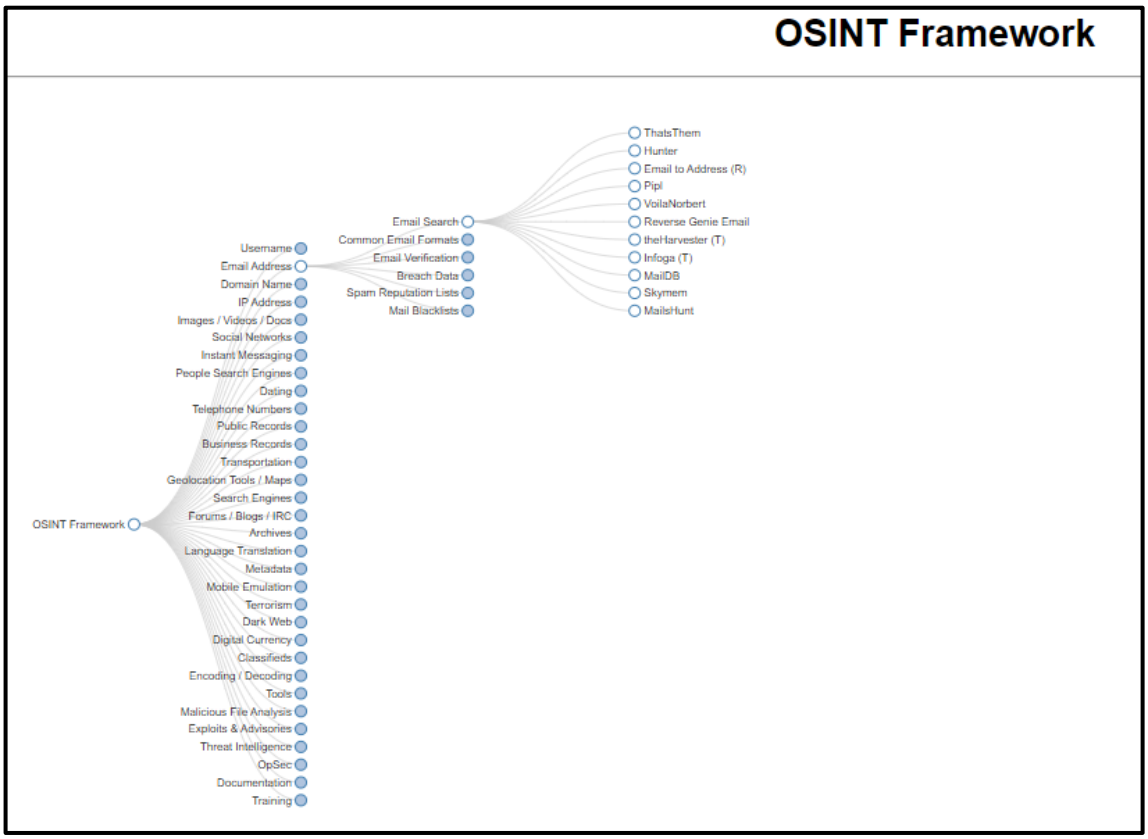
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

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

Tool Names: Have I been Pawned, True Caller, Teams.

What is OSINT?

- Open Source Intelligence
- Used for gathering publicly available target information.



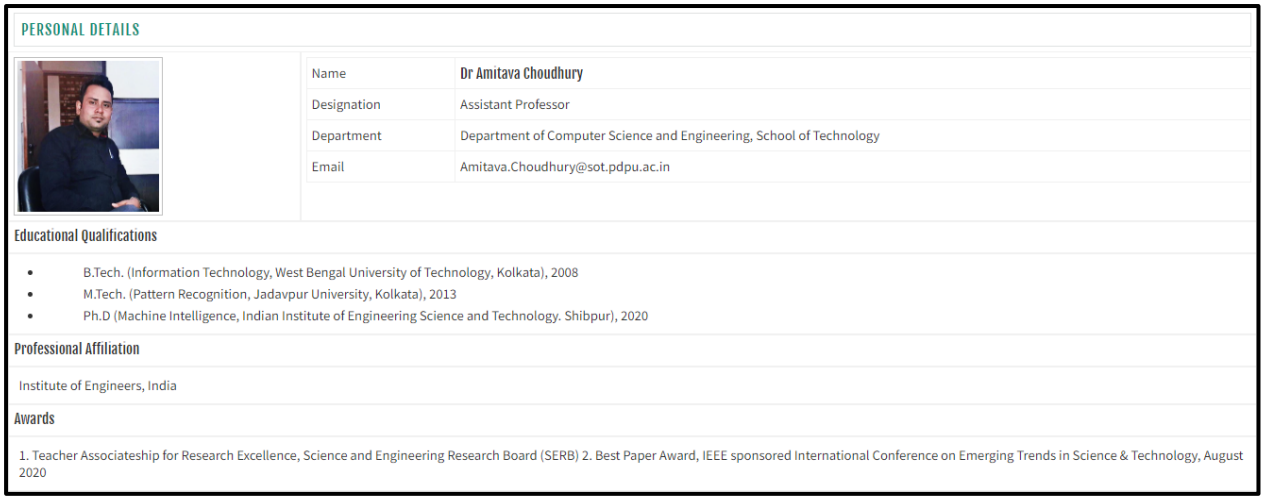
Target: Dr. Amitava Choudhury

- **Prior Known Information:** Works in PDEU, Gandhinagar
- **Photos:**

- **Designation:** Assistant Professor
- **University:** PDEU, Gandhinagar
- **Department:** Departments of Mathematics, School of Technology
- **Work Email:** **Amitava.Choudhury@sot.pdpu.ac.in**
- **Mobile No.:** +91 89026 91510
- **Sim Company:** BSNL
- **Sim Address:** Kolkata, India

Sources:

#1: https://orsp.pdpu.ac.in/adminfacviewprofile.aspx?facid=amitava.choudhury



PERSONAL DETAILS

Name	Dr Amitava Choudhury
Designation	Assistant Professor
Department	Department of Computer Science and Engineering, School of Technology
Email	Amitava.Choudhury@sot.pdpu.ac.in

Educational Qualifications

- B.Tech. (Information Technology, West Bengal University of Technology, Kolkata), 2008
- M.Tech. (Pattern Recognition, Jadavpur University, Kolkata), 2013
- Ph.D (Machine Intelligence, Indian Institute of Engineering Science and Technology. Shibpur), 2020

Professional Affiliation

Institute of Engineers, India

Awards

1. Teacher Associateship for Research Excellence, Science and Engineering Research Board (SERB) 2. Best Paper Award, IEEE sponsored International Conference on Emerging Trends in Science & Technology, August 2020

PUBLICATIONS / ARTICLES / CONFERENCE

Book Published as single author or editor

- 'Environmental Informatics', Textbooks published by International /National Publishers with an established peer review system with ISBN/ISSN numbers, 978-981-19-2083-7, pp. 300, jul 2022
- 'ADVANCES IN DATA SCIENCE AND COMPUTING TECHNOLOGY', Research based books or monographs, 978-1-77463-997-9 , pp. 450, aug 2022
- 'Smart Agriculture Automation Using Advanced Technologies', Research based books or monographs, 978-981-16-6123-5, pp. 228, Dec 2021
- 'Agricultural Informatics: Automation Using the IoT and Machine Learning', Research based books or monographs, 978-1-119-76884-5, pp. 271, mar 2021

Published Papers in Journals

- 'Phase Prediction in High Entropy Alloys by Various Machine Learning Modules Using Thermodynamic and Configurational Parameters.', Metals and Materials International , pp. -, jun 2022
- 'Prediction and Analysis of Mechanical Properties of Low Carbon Steels Using Machine Learning', Journal of The Institution of Engineers (India): Series D, pp. 1, feb 2022
- 'The Role of Machine Learning Algorithms in Materials Science: A State of Art Review on Industry 4.0', Archives of Computational Methods in Engineering , pp. 3361–3381, apr 2021
- 'Random Forest Regression-Based Machine Learning Model for Accurate Estimation of Fluid Flow in Curved Pipes', Processes, pp. 2095, Nov 2021
- 'CGI based syslog management system for virtual machines', Spatial Information Research, pp. 475–486, aug 2020
- 'Structure Prediction of Multi-principal Element Alloys Using Ensemble Learning', Journal of Engineering Computations, pp. 1003-1022, apr 2020
- 'Computer Vision Approach for Phase Identification from Steel Microstructure', Journal of Engineering Computations, pp. 1913-1932, aug 2019

Full Papers in Conference Proceedings

- 'Facial Recognition Based Attendance Monitoring System', 11th International Advanced Computing Conference on 18th & 19th December, 2021 at University of Malta, Malta, pp. 244-253, feb 2022
- 'Customized Human Mask-Face Recognition using Computer Vision', Bangalore, India, pp. 1-5, Oct 2021
- 'Cryptosystem using Facial Landmark for Authentication Pairing and Key Generation in Bluetooth Security', Bangalore, India, pp. 1-6, Oct 2021
- 'Efficient Human Feature Recognition Process Using Sclera', NIT Silchar, pp. 168-181, jun 2020
- 'Real-Time Inventory Management Using Hadoop', UPES, pp. 231-241, sep 2020
- 'Deep Neural Network based Place and Manner of Articulation Detection and Classication for Bengali continuous speech', NIT kurukshetra, pp. 895-901, Dec 2018
- 'Handwritten Bengali Numeral Recognition using HOG Based Feature Extraction Algorithm', Amity University, pp. 687-690, feb 2018
- 'Deep Neural Network Based Recognition and Classification of Bengali Phonemes: A Case Study of Bengali Unconstrained Speech', NGCT, pp. 750-760, jun 2018
- 'A New Zone Based Algorithm for Detection of License Plate From Indian Vehicle', Jaypee University, Wakhnaghat, pp. 370 - 374, Dec 2017
- 'Recognition of Handwritten Bangla Numerals using Adaptive Coefficient Matching Technique', visvesvaraya technological university, pp. 764 – 770 , aug 2016

Papers presented in Conferences, Seminars, Workshops, Symposia

- 'A Paradigm Shift towards Crowd-based Healthcare System', HCOMP/AAAI, AAAI, Nov 2021

#2: https://sot.pdpu.ac.in/sot-faculty.html

FACULTY OF COMPUTER SCIENCE & ENGINEERING

Dr Amitava Choudhury

Assistant Professor

B.Tech., M.Tech., Ph.D

Email : Amitava.Choudhury@sot.pdpu.ac.in

Areas of Interest: Computational Geometry in the field of micromechanical modelling, Pattern Recognition, Character Recognition, Machine Learning.

Brief Profile: Dr. Amitava Choudhury working as assistant professor in the Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gandhinagar, Gujrat. He received his Ph.D. from Indian Institute of Engineering Science and Technology, Shibpur and Master of Technology from Jadavpur University, West Bengal. He has 9 years of experience in teaching and research. Prior to join PDEU, he has worked at University of Petroleum and Energy Studies, Dehradun. He serves as a reviewer of IEEE biomedical transaction and Medical and biological engineering and Computing.

Name	**Dr Amitava Choudhury**
Designation	Assistant Professor
Department	Department of Computer Science and Engineering, School of Technology
Email	Amitava.Choudhury@sot.pdpu.ac.in

Educational Qualifications

- B.Tech. (Information Technology, West Bengal University of Technology, Kolkata), 2008
- M.Tech. (Pattern Recognition, Jadavpur University, Kolkata), 2013
- Ph.D (Machine Intelligence, Indian Institute of Engineering Science and Technology. Shibpur), 2020

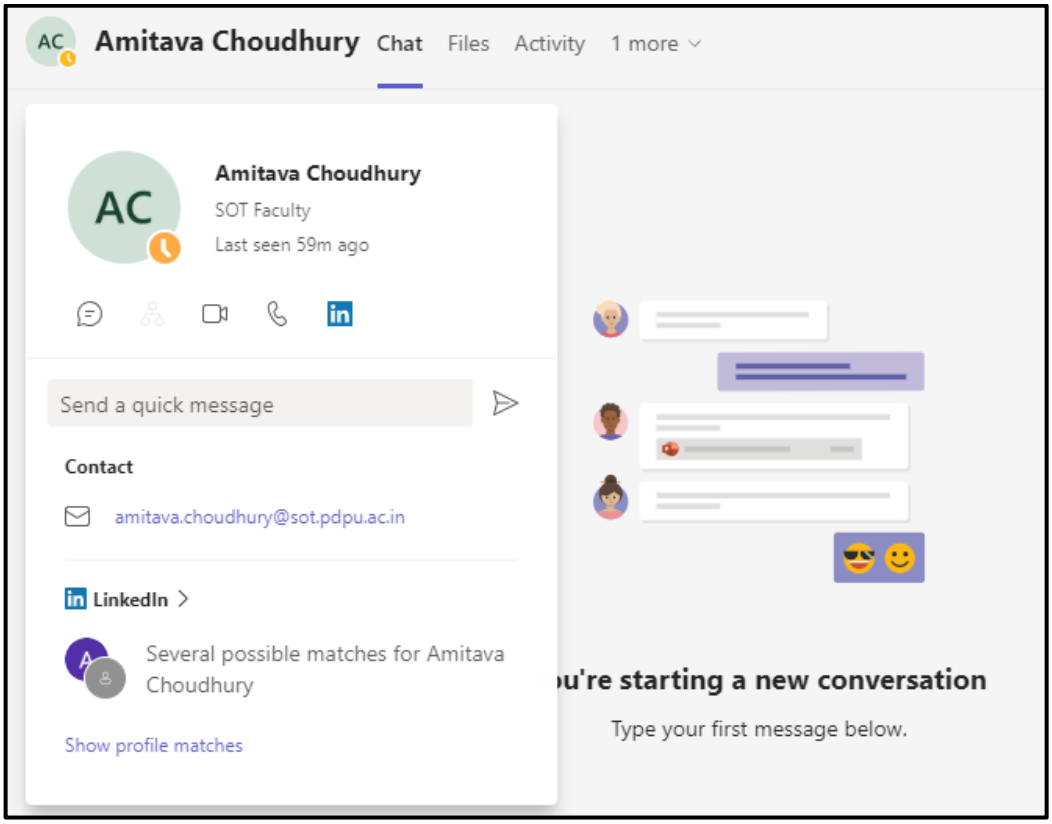
Professional Affiliation

Institute of Engineers, India

Awards

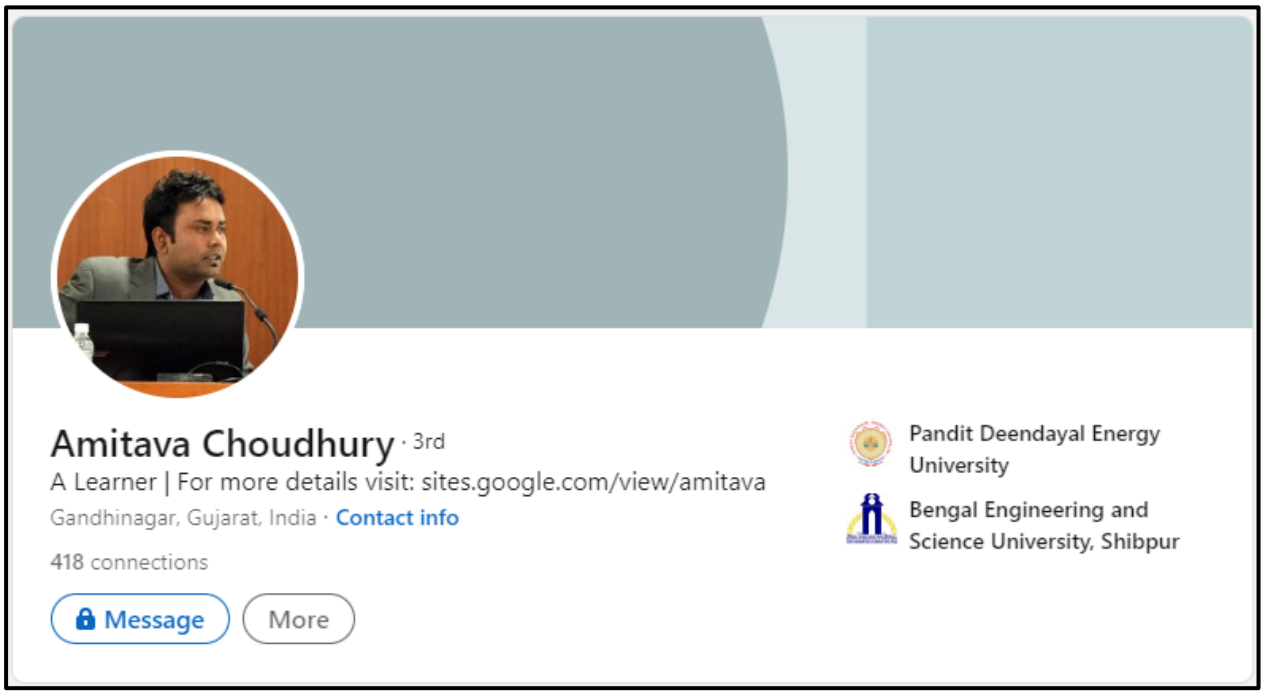
1. Teacher Associateship for Research Excellence, Science and Engineering Research Board (SERB) 2. Best Paper Award, IEEE sponsored International Conference on Emerging Trends in Science & Technology, August 2020

#3: Microsoft Teams



#4: **https://www.truecaller.com/search/in/89026%2091510**

#5: https://www.linkedin.com/in/amitava-choudhury-ds/



Experience

Assistant Professor
Pandit Deendayal Energy University · Full-time
Dec 2021 - Present · 9 mos
Gandhinagar, Gujarat, India

University of Petroleum and Energy Studies
5 yrs 4 mos

- **Assistant Professor**
  Sep 2016 - Dec 2021 · 5 yrs 4 mos
  India

  Home
  I am working as an Assistant Professor in University of Petroleum & Energy Studies, Dehradun, India and also pursuing my Ph.D from Indian Institute of Engineering science...

- **Assistant Professor**
  Full-time
  Sep 2016 - Dec 2021 · 5 yrs 4 mos
  Dehradun, Uttaranchal

Assistant Professor
IMS Unison University
Oct 2015 - Aug 2016 · 11 mos
Dehra Dun Area, India

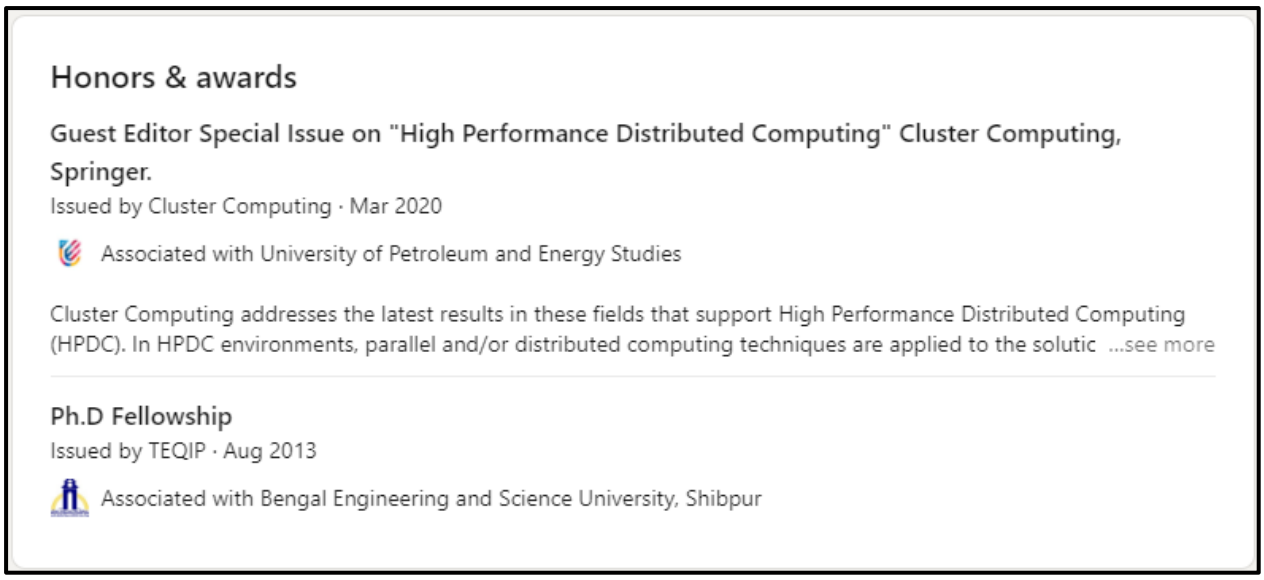
Research Scholar
Indian Institute of Engineering Science and Technology
Aug 2013 - Sep 2015 · 2 yrs 2 mos
Shibpur

Assistant Professor
Nimas College
Jun 2008 - Jul 2011 · 3 yrs 2 mos
Kolkata

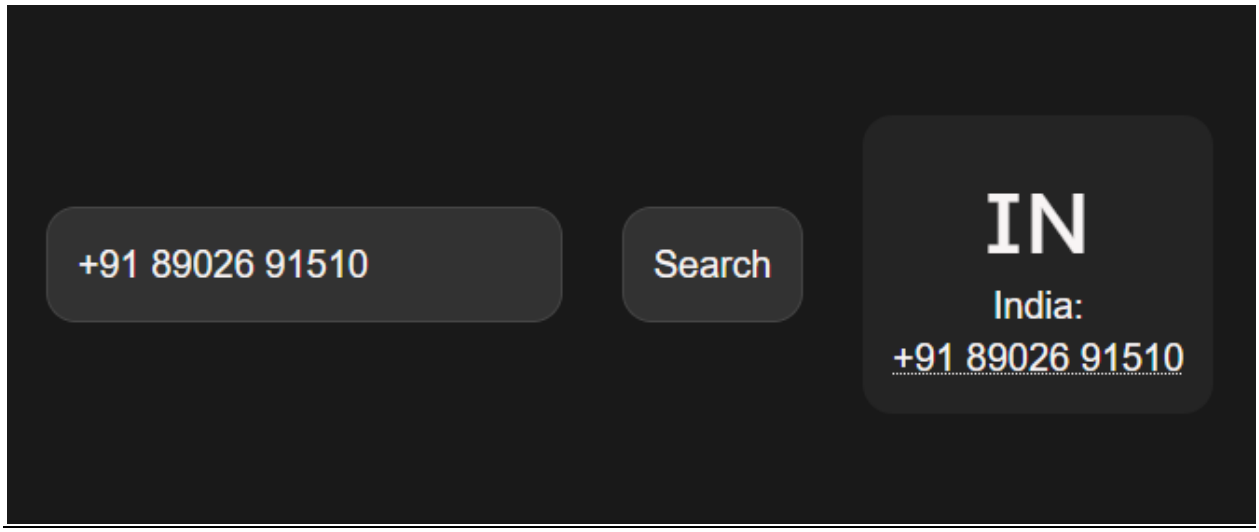
Education

IIEST, Shibpur
Doctor of Philosophy (Ph.D.), Research
2013 - 2020

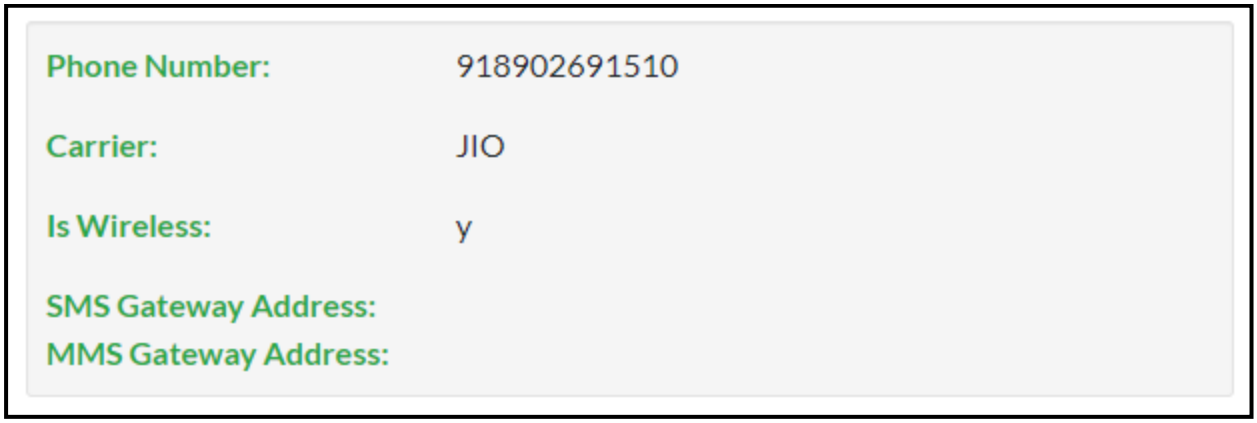
Jadavpur University
Master's degree, Information Technology
2011 - 2013



#6: https://whocalld.com/?p=%2B91+89026+91510



#7: **https://freecarrierlookup.com/**



Digital Forensics Lab Report: 3

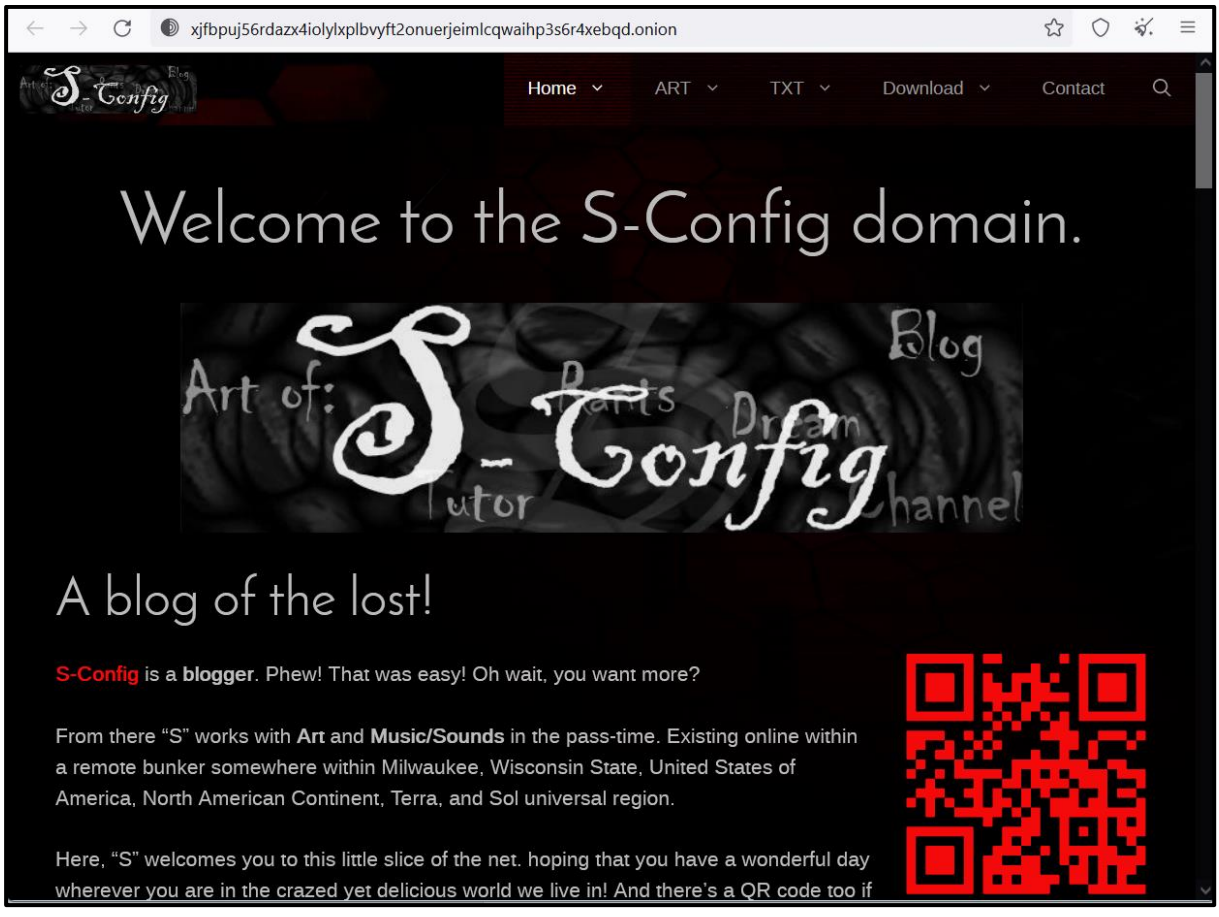
Date: 10-08-2022

Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Blogs, forums, and file uploader using the TOR browser.

Tool Names: TOR Browser

1. Blogs / Essays / News Sites



cgjzkysxa4ru5rhrtr6rafckhexbisbtxwg2fg743cjumioysmirhdad.onion

Coarse Enigma

About Code Links Webring

Coarse Enigma is ...

- A Privacy and Cybersecurity Blog
- A Repository for code
- A Space to Think

Posts

Dec 25, 2020

(Tr|b)ash - Thoughts on Unix Scripting

Nov 30, 2020

Introduction to DNS

Nov 23, 2020

Converting Writers Cafe Documents to Plaintext

Oct 19, 2020

Containers: FreeBSD Jails

p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion

Menu

PROPUBLICA

Investigative Journalism in the Public Interest

Donate

Nonprofit Explorer Local Initiatives Newsletters About Us

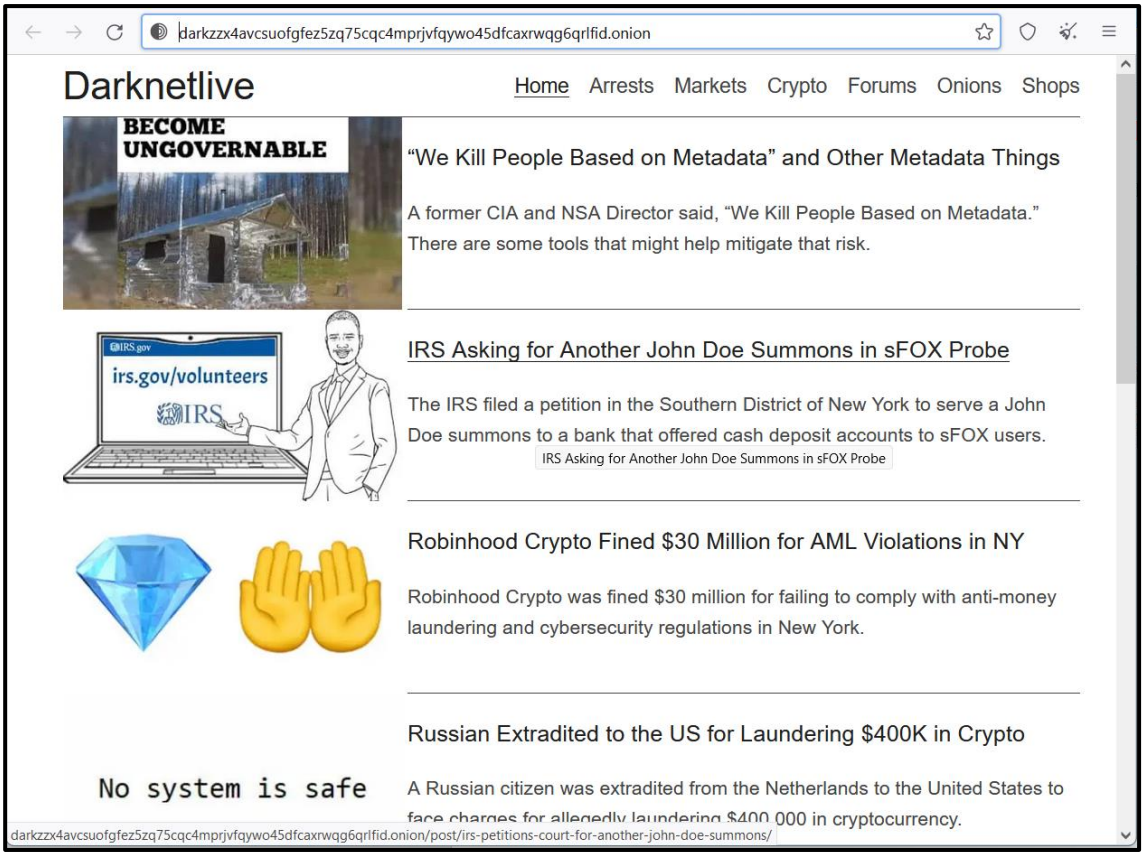
Get the Big Story newsletter

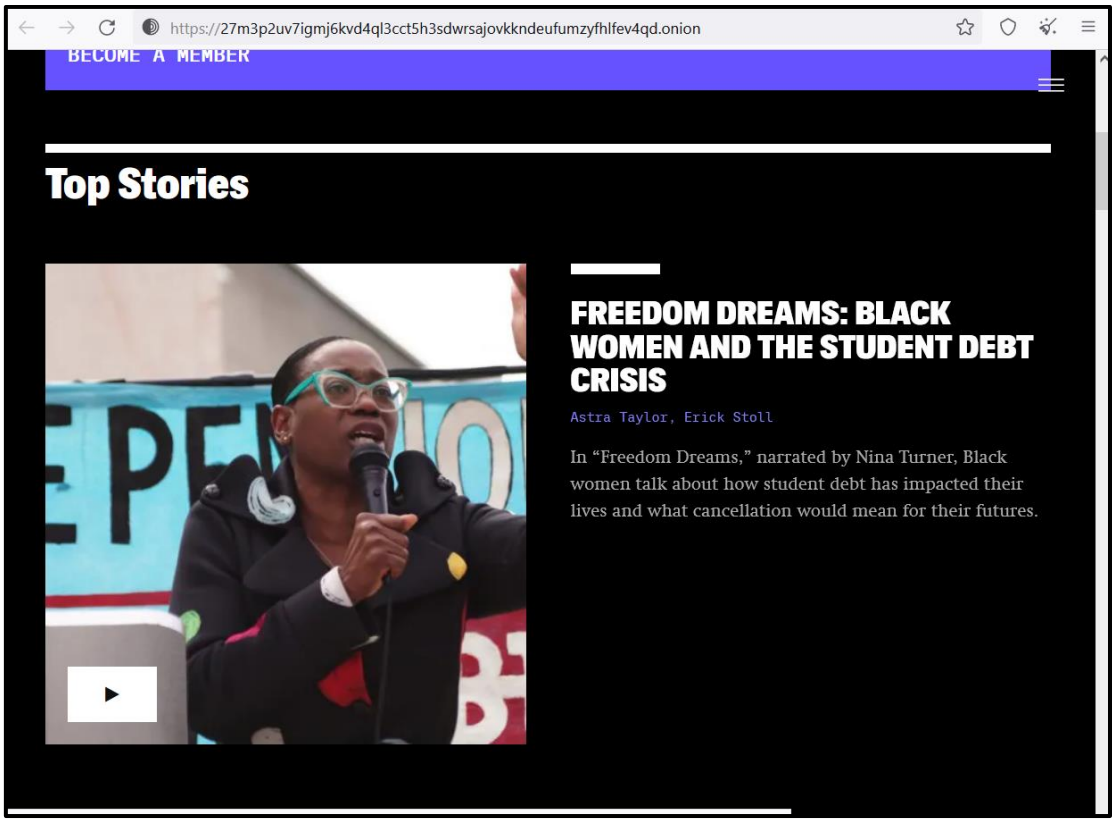
A Tax Credit Meant to Help Marginalized Workers Instead

The Effort to Overturn the Election

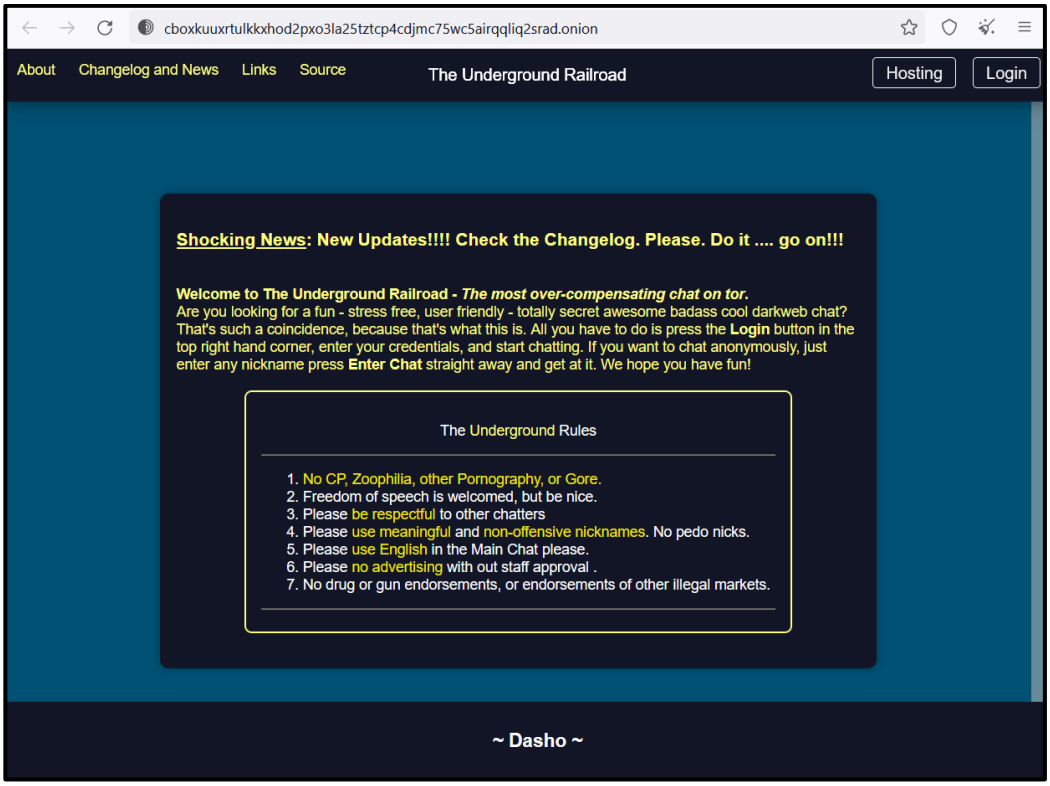
Reporting on the mob that attacked and breached the Capitol, the fallout from that day, and ongoing far-right violence.

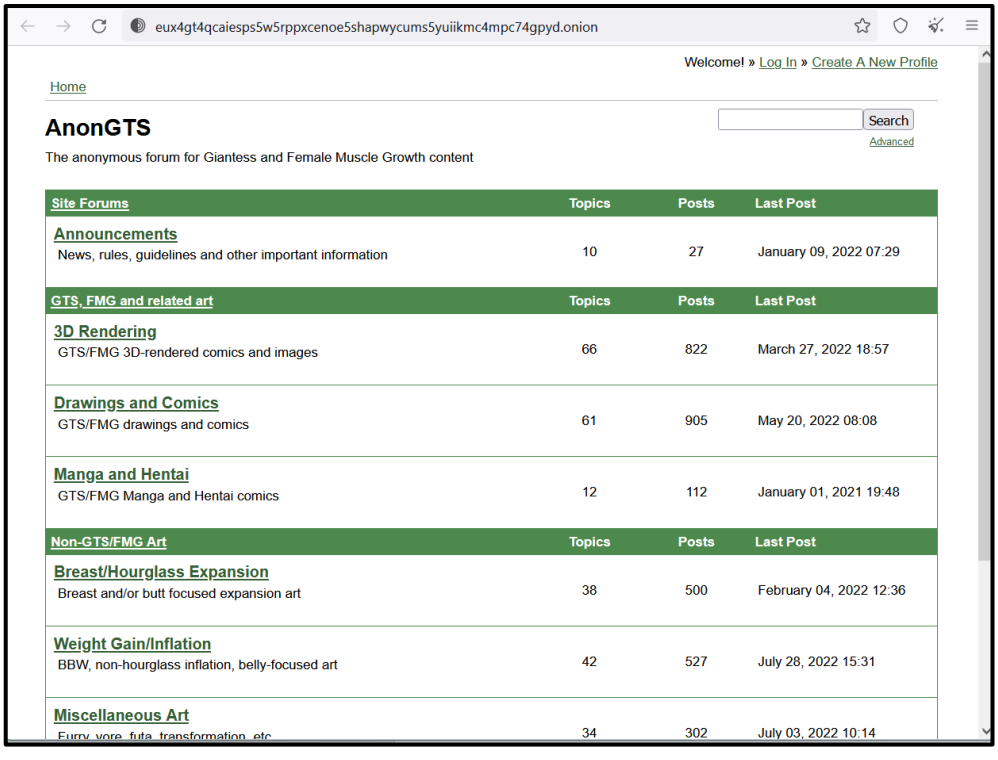
p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/article/work-opportunity-tax-credit-temp-permanent-employment

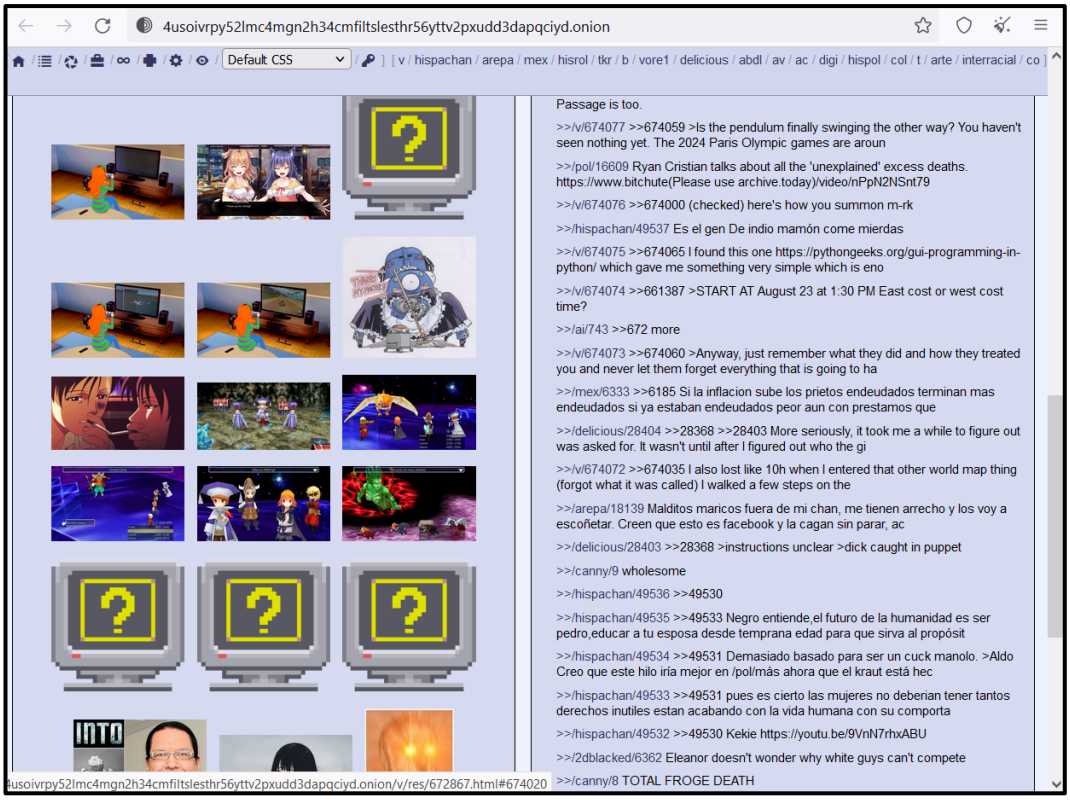

darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion
Darknetlive
Home Arrests Markets Crypto Forums Onions Shops
BECOME UNGOVERNABLE
"We Kill People Based on Metadata" and Other Metadata Things
A former CIA and NSA Director said, "We Kill People Based on Metadata." There are some tools that might help mitigate that risk.
IRS.gov
irs.gov/volunteers
IRS
IRS Asking for Another John Doe Summons in sFOX Probe
The IRS filed a petition in the Southern District of New York to serve a John Doe summons to a bank that offered cash deposit accounts to sFOX users.
IRS Asking for Another John Doe Summons in sFOX Probe
Robinhood Crypto Fined $30 Million for AML Violations in NY
Robinhood Crypto was fined $30 million for failing to comply with anti-money laundering and cybersecurity regulations in New York.
No system is safe
Russian Extradited to the US for Laundering $400K in Crypto
A Russian citizen was extradited from the Netherlands to the United States to face charges for allegedly laundering $400,000 in cryptocurrency.
darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion/post/irs-petitions-court-for-another-john-doe-summons/


https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion
BECOME A MEMBER
Top Stories
FREEDOM DREAMS: BLACK WOMEN AND THE STUDENT DEBT CRISIS
Astra Taylor, Erick Stoll
In "Freedom Dreams," narrated by Nina Turner, Black women talk about how student debt has impacted their lives and what cancellation would mean for their futures.

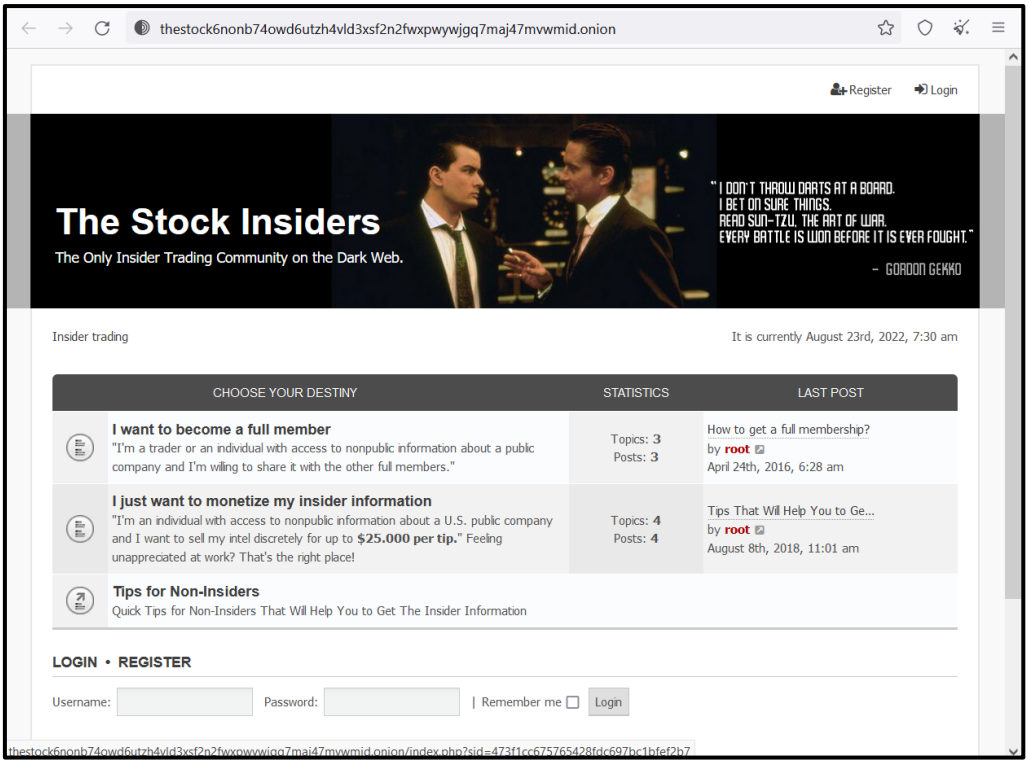
2. Forums / Boards / Chats



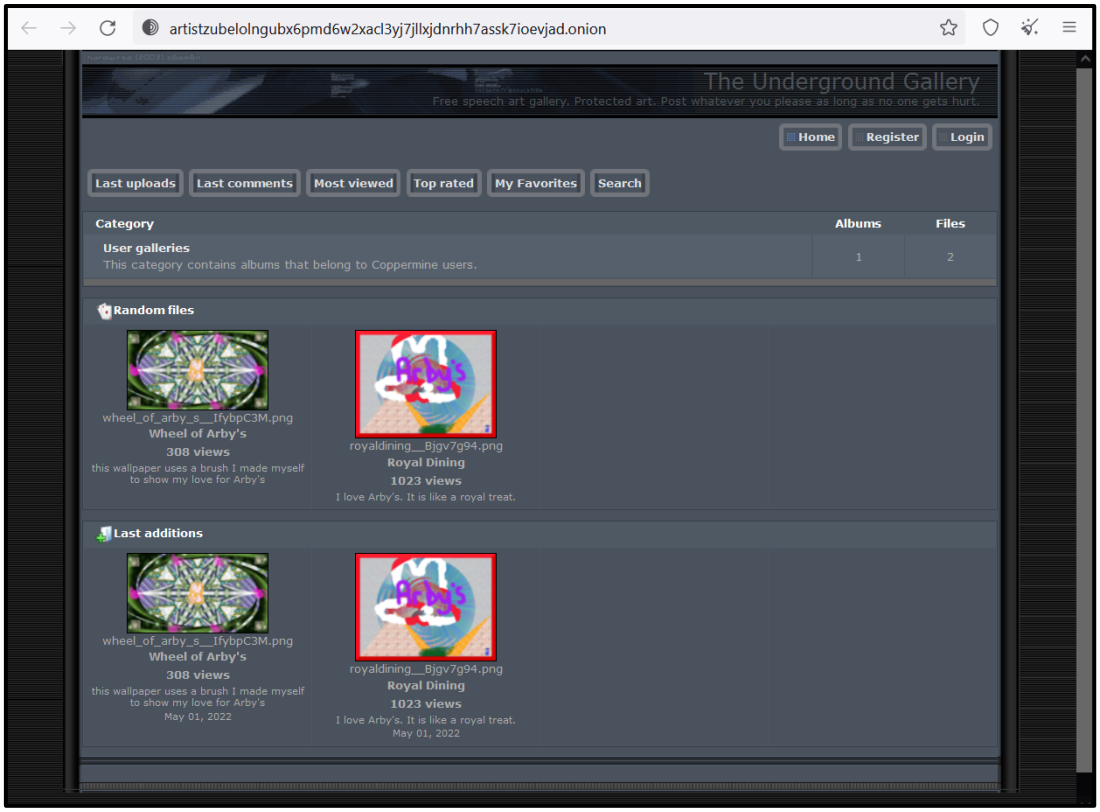


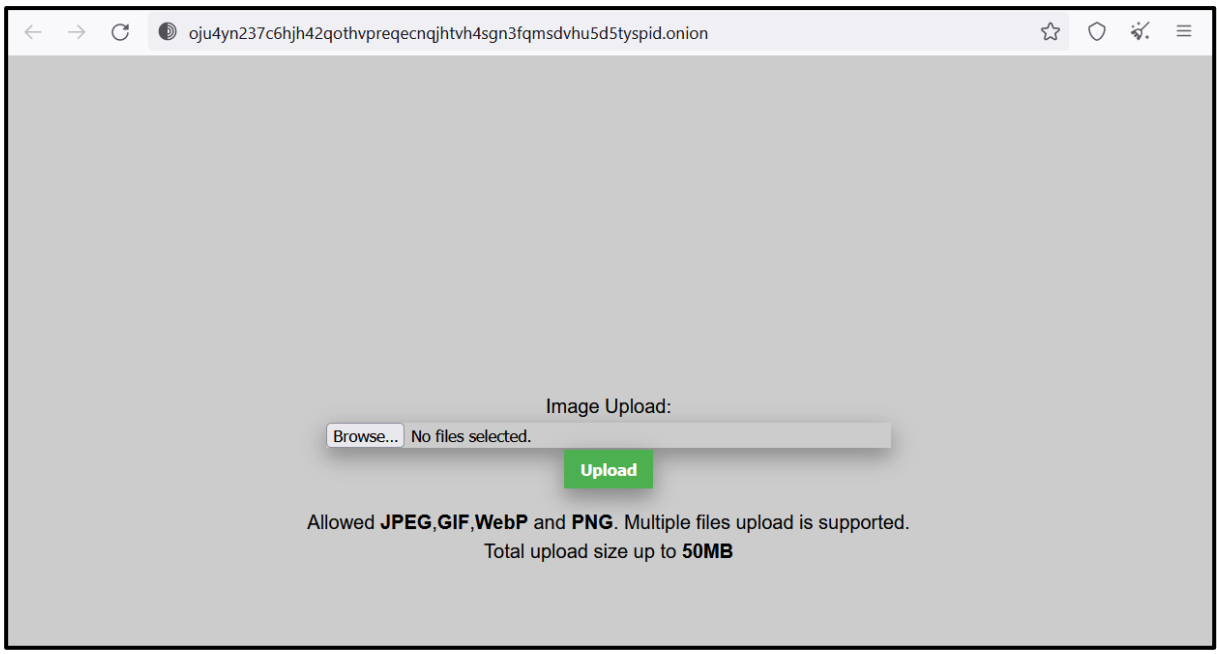

4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion
Default CSS
[v / hispachan / arepa / mex / hisrol / tkr / b / vore1 / delicious / abdl / av / ac / digi / hispol / col / t / arte / interracial / co]
Passage is too.
>>/v/674077 >>674059 >Is the pendulum finally swinging the other way? You haven't seen nothing yet. The 2024 Paris Olympic games are aroun
>>/pol/16609 Ryan Cristian talks about all the 'unexplained' excess deaths. https://www.bitchute(Please use archive.today)/video/nPpN2NSnt79
>>/v/674076 >>674000 (checked) here's how you summon m-rk
>>/hispachan/49537 Es el gen De indio mamón come mierdas
>>/v/674075 >>674065 I found this one https://pythongeeks.org/gui-programming-in-python/ which gave me something very simple which is eno
>>/v/674074 >>661387 >START AT August 23 at 1:30 PM East cost or west cost time?
>>/ai/743 >>672 more
>>/v/674073 >>674060 >Anyway, just remember what they did and how they treated you and never let them forget everything that is going to ha
>>/mex/6333 >>6185 Si la inflacion sube los prietos endeudados terminan mas endeudados si ya estaban endeudados peor aun con prestamos que
>>/delicious/28404 >>28368 >>28403 More seriously, it took me a while to figure out was asked for. It wasn't until after I figured out who the gi
>>/v/674072 >>674035 I also lost like 10h when I entered that other world map thing (forgot what it was called) I walked a few steps on the
>>/arepa/18139 Malditos maricos fuera de mi chan, me tienen arrecho y los voy a escoñetar. Creen que esto es facebook y la cagan sin parar, ac
>>/delicious/28403 >>28368 >instructions unclear >dick caught in puppet
>>/canny/9 wholesome
>>/hispachan/49536 >>49530
>>/hispachan/49535 >>49533 Negro entiende,el futuro de la humanidad es ser pedro,educar a tu esposa desde temprana edad para que sirva al propósit
>>/hispachan/49534 >>49531 Demasiado basado para ser un cuck manolo. >Aldo Creo que este hilo iría mejor en /pol/más ahora que el kraut está hec
>>/hispachan/49533 >>49531 pues es cierto las mujeres no deberian tener tantos derechos inutiles estan acabando con la vida humana con su comporta
>>/hispachan/49532 >>49530 Kekie https://youtu.be/9VnN7rhxABU
>>/2dblacked/6362 Eleanor doesn't wonder why white guys can't compete
>>/canny/8 TOTAL FROGE DEATH
4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/v/res/672867.html#674020

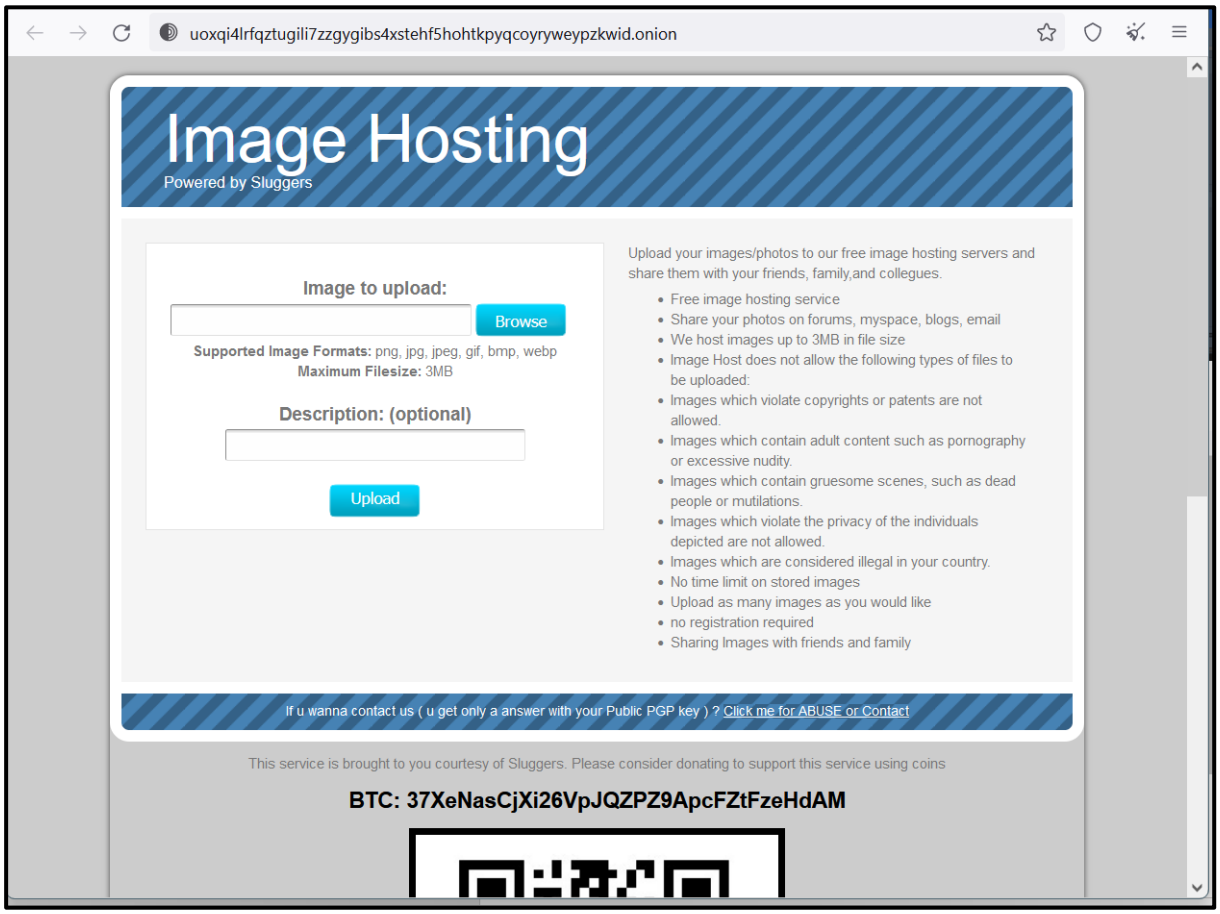

enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion
home / boards / overboard / account / help / watched threads] [irc / twitter / discord / telegram] [Tools] [F.A.Q. / logs]
THIS IS THE END
Endchan.
The imageboard at the end of the universe
The story so far: In 2015 Endchan was created. This has made a lot of people very angry and been widely regarded as a bad move
This is an anonymous imageboard that promotes ideas over identity. Here anyone can run their own boards. The only three global rules are:
1. Nothing illegal under US law.
2. No suggestive audio-visual content of underage children. Loli ok.
3. No spamming; no flooding that compromises normal operation of the site.
Last update: 2020-03-29 01:00am PST
We're actively working to improve the site. Any and all feedback is appreciated.
You must be 18 years or older to visit this site. This site is actively moderated by our team of volunteers.
Enable NSFW content:
Site Announcements
updated with desktop-first styling addressing many complaints.
Have questions or feedback?
UPDATE: 2022-04-09 01:24PM PDT - It has been brought to our attention that WebP image format and several others are still not working
UPDATE: 2021-12-20 1:46AM PDT - Happy 6th Birthday Endchan! View Magrathea. What's Magrathea?
Transferring data from enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion...

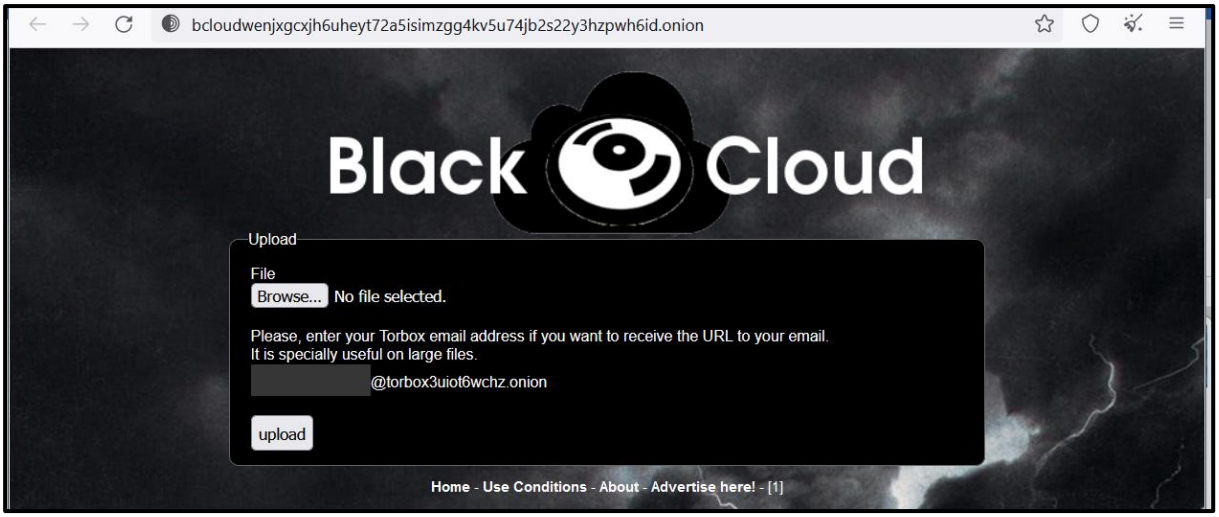


3. File Uploader




oju4yn237c6hjh42qothvpreqecnqjhtvh4sgn3fqmsdvhu5d5tyspid.onion
Image Upload:
Browse...
No files selected.
Upload
Allowed JPEG,GIF,WebP and PNG. Multiple files upload is supported.
Total upload size up to 50MB


uoxqi4lrfqztugili7zzgygibs4xstehf5hohtkpyqcoyryweypzkwid.onion
Image Hosting
Powered by Sluggers
Image to upload:
Browse
Supported Image Formats: png, jpg, jpeg, gif, bmp, webp
Maximum Filesize: 3MB
Description: (optional)
Upload
Upload your images/photos to our free image hosting servers and share them with your friends, family,and collegues.
Free image hosting service
Share your photos on forums, myspace, blogs, email
We host images up to 3MB in file size
Image Host does not allow the following types of files to be uploaded:
Images which violate copyrights or patents are not allowed.
Images which contain adult content such as pornography or excessive nudity.
Images which contain gruesome scenes, such as dead people or mutilations.
Images which violate the privacy of the individuals depicted are not allowed.
Images which are considered illegal in your country.
No time limit on stored images
Upload as many images as you would like
no registration required
Sharing Images with friends and family
If u wanna contact us (u get only a answer with your Public PGP key) ? Click me for ABUSE or Contact
This service is brought to you courtesy of Sluggers. Please consider donating to support this service using coins
BTC: 37XeNasCjXi26VpJQZPZ9ApcFZtFzeHdAM


bcloudwenjxgcxjh6uheyt72a5isimzgg4kv5u74jb2s22y3hzpwh6id.onion
Black Cloud
Upload
File
Browse...
No file selected.
Please, enter your Torbox email address if you want to receive the URL to your email.
It is specially useful on large files.
@torbox3uiot6wchz.onion
upload
Home - Use Conditions - About - Advertise here! - [1]

Digital Forensics Lab Report: 4

Date: 17-08-2022

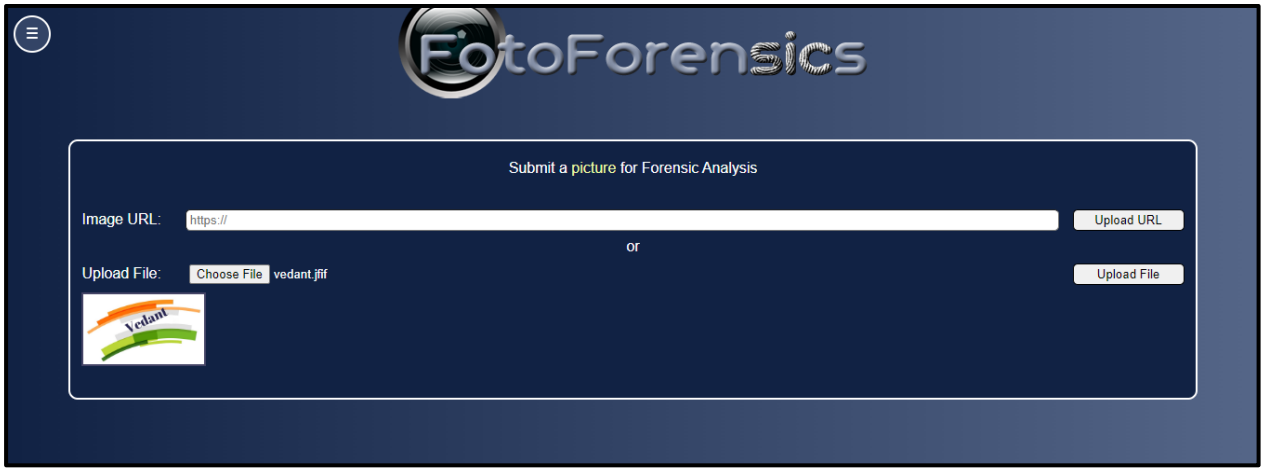
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Perform Steganography using Stegano tools

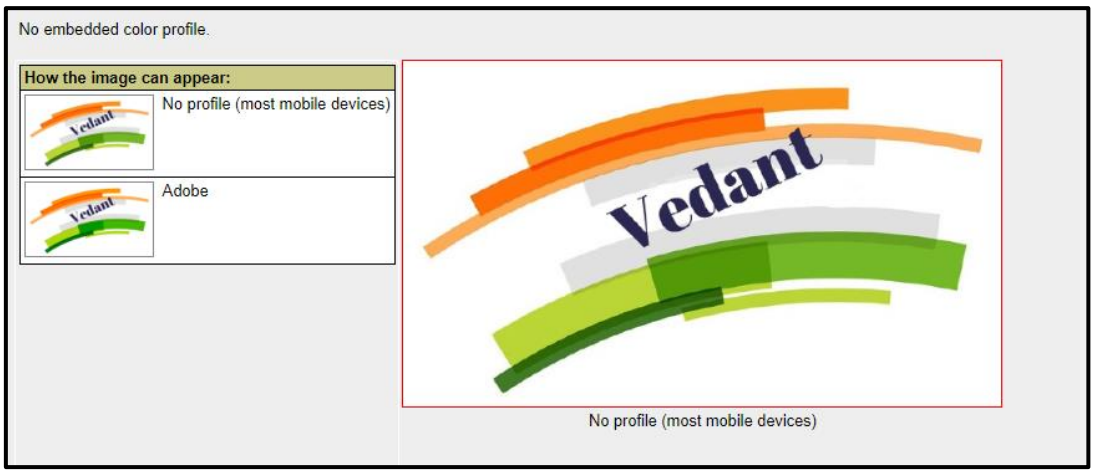
Tool Names: Google image search, Tineye image search, YouTube data viewer, Foto forensic, Forensically, Pic2map, Suncalc, Wikimapia, Exif Data Viewer, Jeffrey exif viewer, Exiftool, Metagoofil, YouTube metadata.

Task 1: Fotoforensics
Steps:

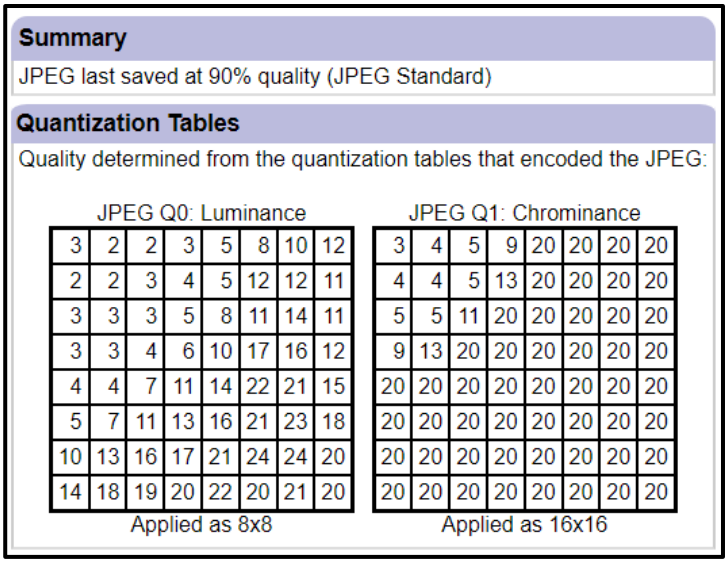
1. Open FotoForensics.
2. Select “Image URL” if you want to insert the image url or “Upload File” if you want to select the file from your local machine.
3. Then Click on upload url and upload image.
4. Then you get all data regarding images like ICC+, metadata, etc.



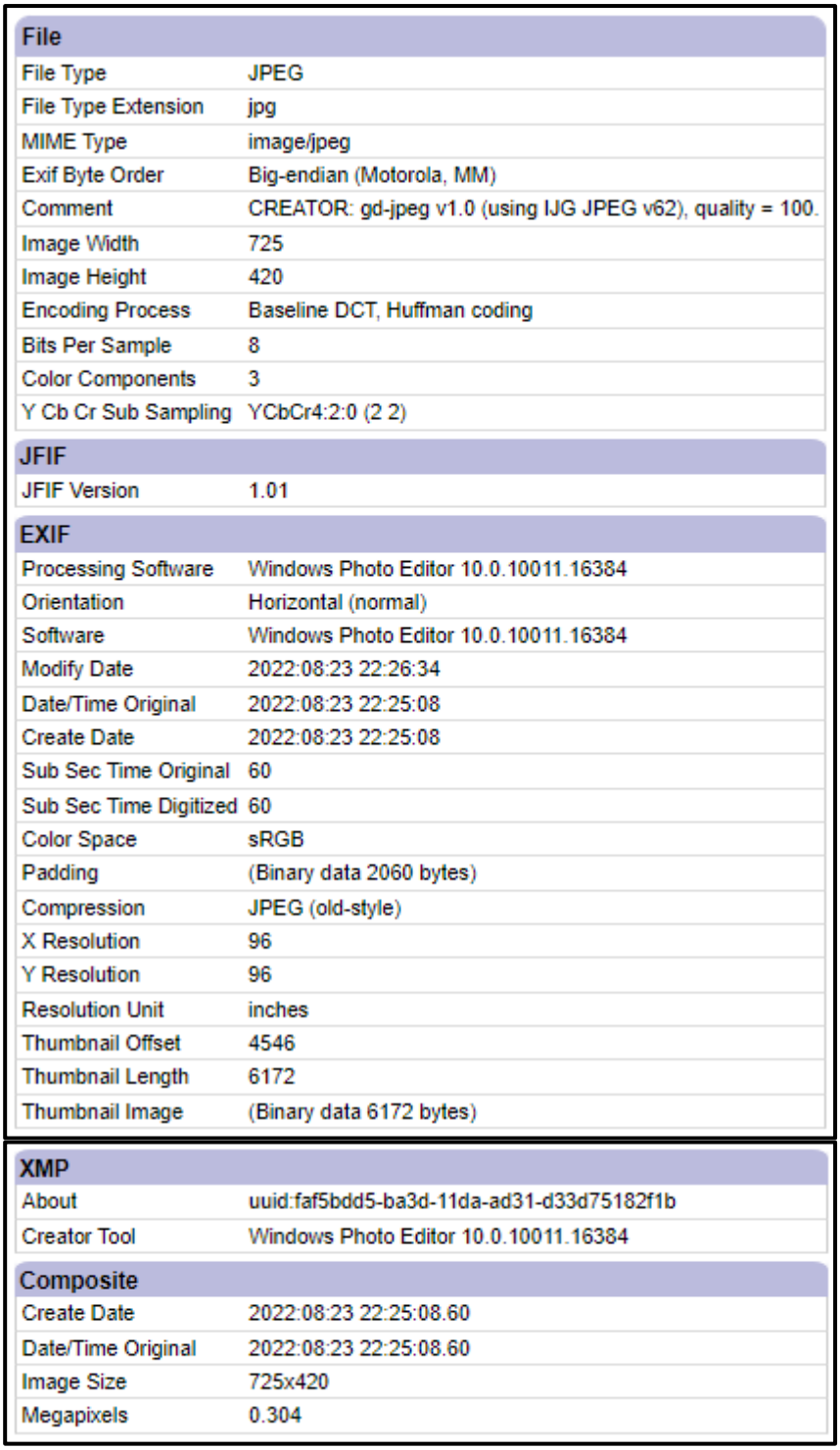
ICC:



JPEG:



MetaData:



File	
File Type	JPEG
File Type Extension	jpg
MIME Type	image/jpeg
Exif Byte Order	Big-endian (Motorola, MM)
Comment	CREATOR: gd-jpeg v1.0 (using IJG JPEG v62), quality = 100.
Image Width	725
Image Height	420
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
Y Cb Cr Sub Sampling	YCbCr4:2:0 (2 2)

JFIF	
JFIF Version	1.01

EXIF	
Processing Software	Windows Photo Editor 10.0.10011.16384
Orientation	Horizontal (normal)
Software	Windows Photo Editor 10.0.10011.16384
Modify Date	2022:08:23 22:26:34
Date/Time Original	2022:08:23 22:25:08
Create Date	2022:08:23 22:25:08
Sub Sec Time Original	60
Sub Sec Time Digitized	60
Color Space	sRGB
Padding	(Binary data 2060 bytes)
Compression	JPEG (old-style)
X Resolution	96
Y Resolution	96
Resolution Unit	inches
Thumbnail Offset	4546
Thumbnail Length	6172
Thumbnail Image	(Binary data 6172 bytes)

XMP	
About	uuid:faf5bdd5-ba3d-11da-ad31-d33d75182f1b
Creator Tool	Windows Photo Editor 10.0.10011.16384

Composite	
Create Date	2022:08:23 22:25:08.60
Date/Time Original	2022:08:23 22:25:08.60
Image Size	725x420
Megapixels	0.304

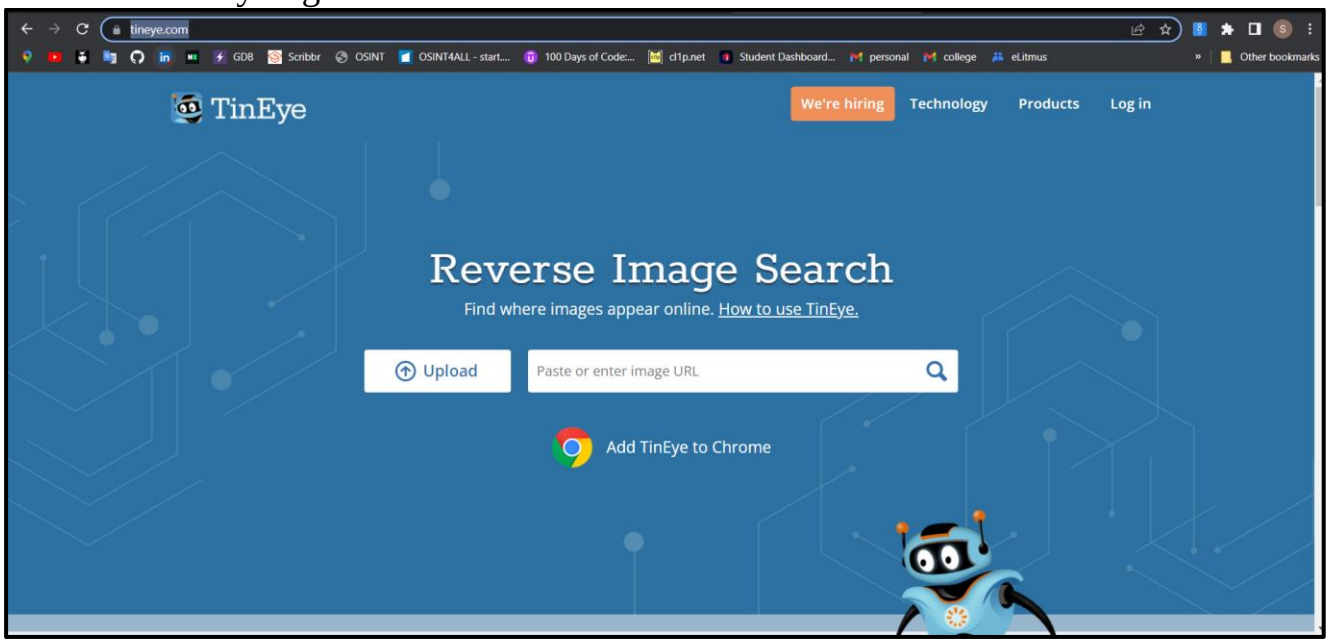
Analysis:

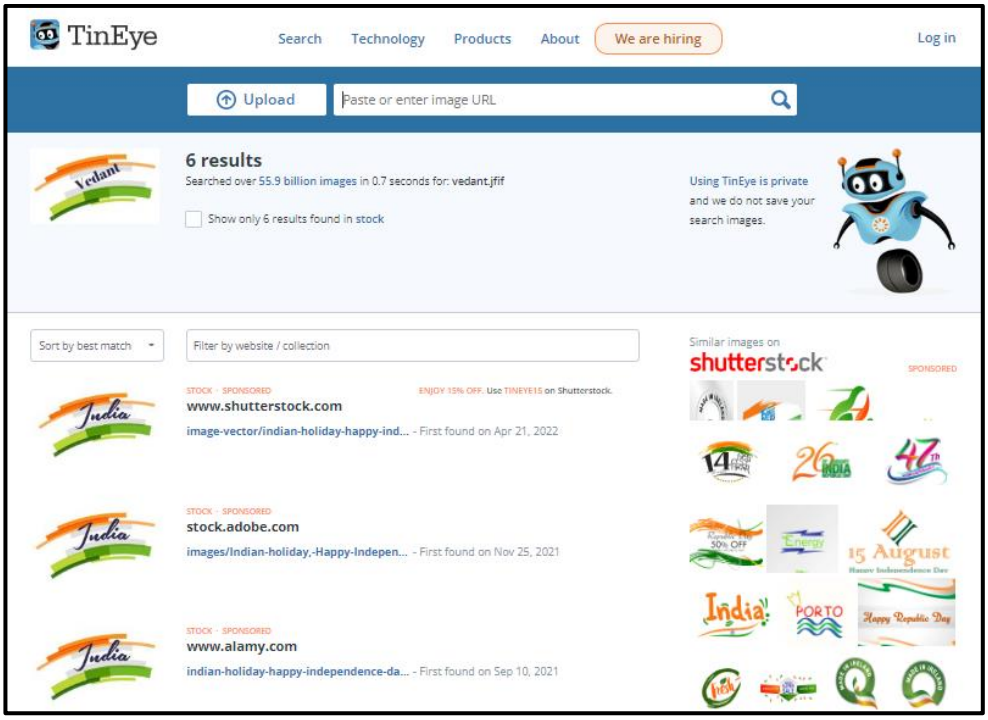
1. We can analyse the image by Hidden pixels or ELA. By using those modules we can easily get all information about the raw structure.

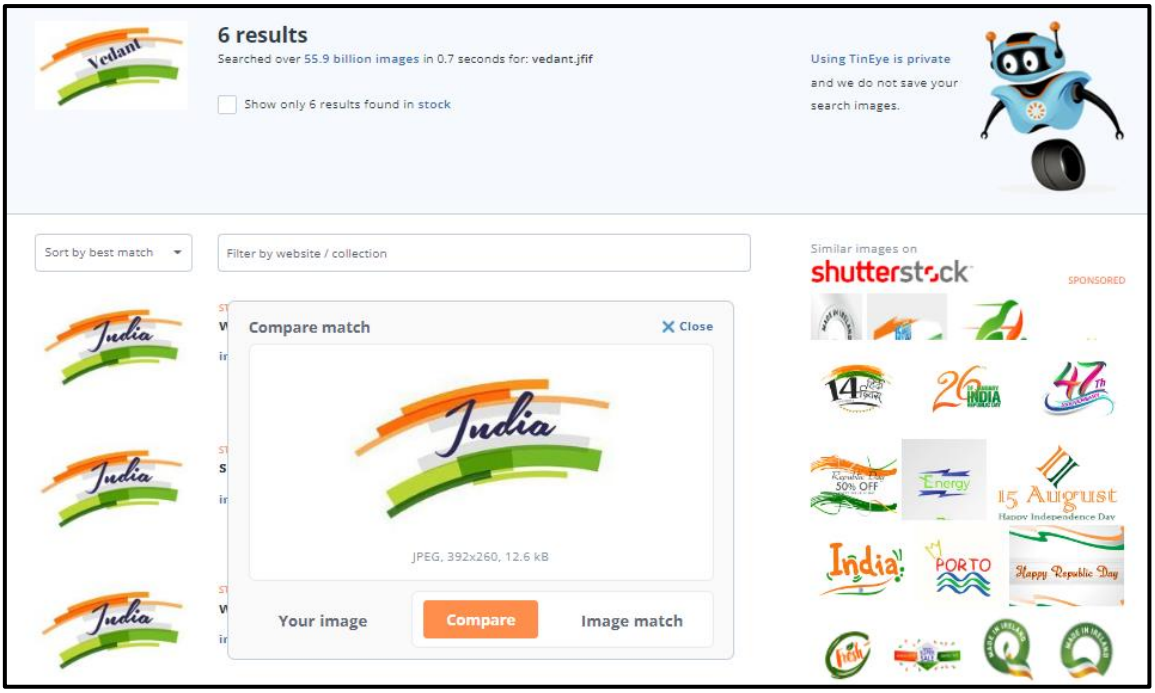
Task 2: TinEye

Steps:

1. Open https://tineye.com/
2. Then Select the Upload button and select the image from the local machine.
3. Then press enter click
4. After you get all related results







Analysis:

1. It is very useful when you have random images but you don't know and you get similar results so you will get to know about the images
2. It has features of comparing the input image and finding results so you can easily compare both images.

Tool 3: Pic2Map

Steps:

1. Open https://www.pic2map.com/
2. Upload the images of geographical location or you can select the images randomly too.
3. Then you will get all images and geographical information about that image's place.

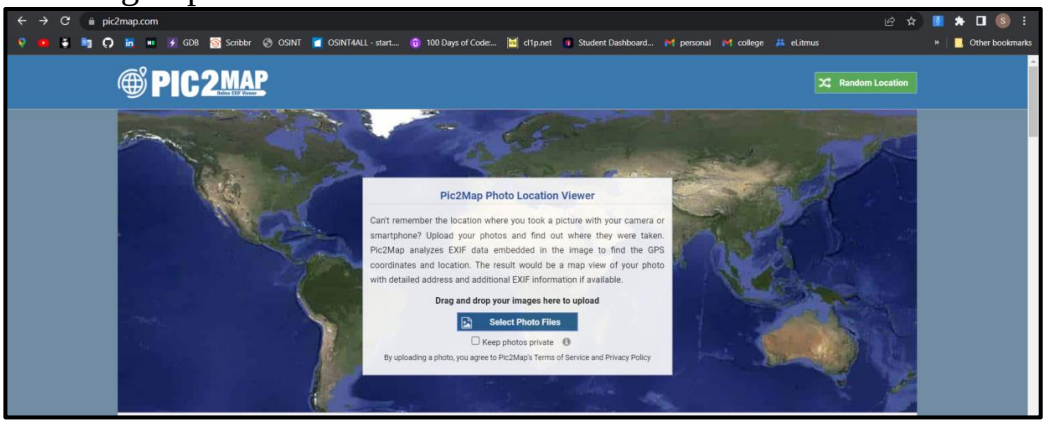


PHOTO EXIF DATA

The photo was shot using a Apple iPhone 3G camera at an aperture of f/2.8, sec. shutter speed and ISO 0. No flash function. The original image file has a resolution of 1600 x 1200 pixels, or in other words 1.9 megapixels.The photo has a resolution of 72 DPI.

According to the image metadata, the photo was shot on Saturday 22nd of October 2011. The local time was 16:18:01. The timezone was Europe / Istanbul, which is GMT +03:00. Please note that timezone was guessed using the GPS coordinates and may not be accurate. The EXIF timestamp may also be wrong if the date and time weren't set correctly in the digital camera.

Apple iPhone 3G camera has a built-in GPS receiver and allows geotagging on image files. The coordinates and location where the photo was taken is stored in the EXIF. According to GPS data analysis, the photo was taken at coordinates 39° 19' 52.80" N , 26° 39' 33.60" E. The elevation was 59 meters. Using reverse geocoding, the address associated with the coordinates is guessed as Mithatpaşa Mahallesi, Mevlana Caddesi, 10405 Ayvalık/Balıkesir, Turkey. Depending on the GPS receiver and the reception conditions the accuracy may vary and the address should not be regarded as exact location.

CAMERA INFORMATION

Brand: Apple	Model: iPhone 3G	Lens Info: Unknown
Shutter: (0. seconds)	F Number: f/2.8	ISO Speed: ISO 0
Flash: Not Used	Focal Length: mm	Color Space: sRGB

FILE INFORMATION

File Name: IMG_0897.JPG	Image Size: 1600 x 1200 pixels	Resolution: 1.9 megapixels
Unique ID:	MIME Type: image/jpeg	Dots/Inch: 72 DPI

DATE & TIME

Date: 2011-10-22	Time: 16:18:01 (GMT +03:00)	Time Zone: Europe / Istanbul

GPS INFORMATION

Latitude: 39.331333	Longitude: 26.659333	Lat Ref: North
Long Ref: East	Coordinates: 39° 19' 52.80" N , 26° 39' 33.60" E	Altitude: 59m. (Above Sea Level)
Direction Ref:	Direction:	Pointing:

LOCATION INFORMATION

City:	State: Balıkesir	Country: Turkey

Address: Mithatpaşa Mahallesi, Mevlana Caddesi, 10405 Ayvalık/Balıkesir, Turkey
(Location was guessed from coordinates and may not be accurate.)

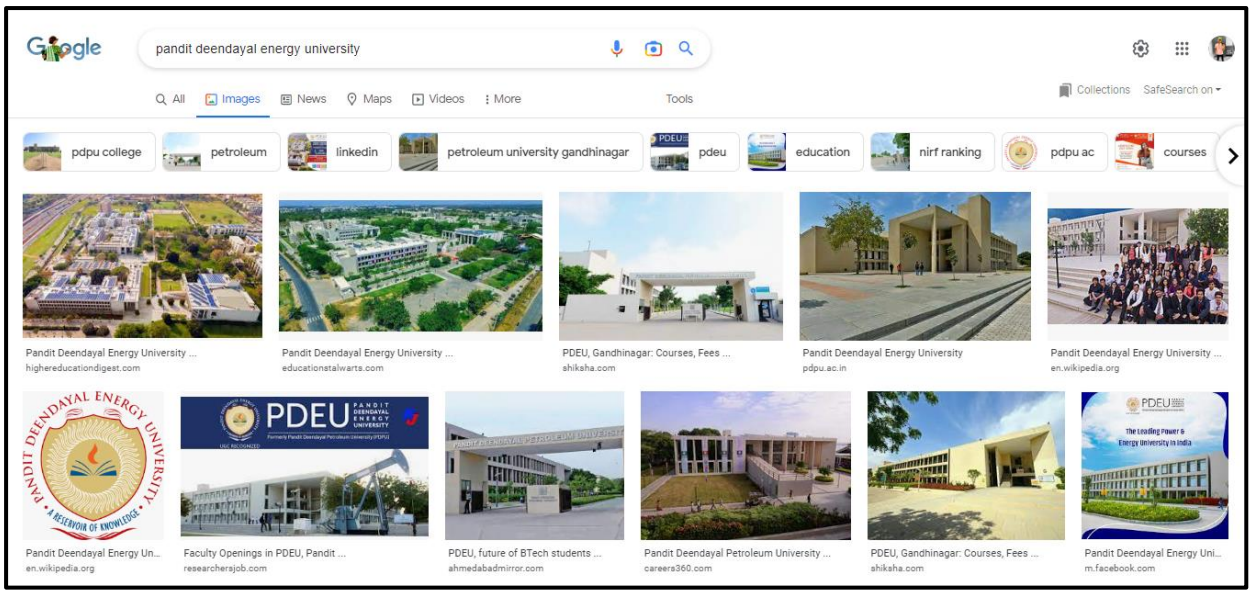
Analysis:

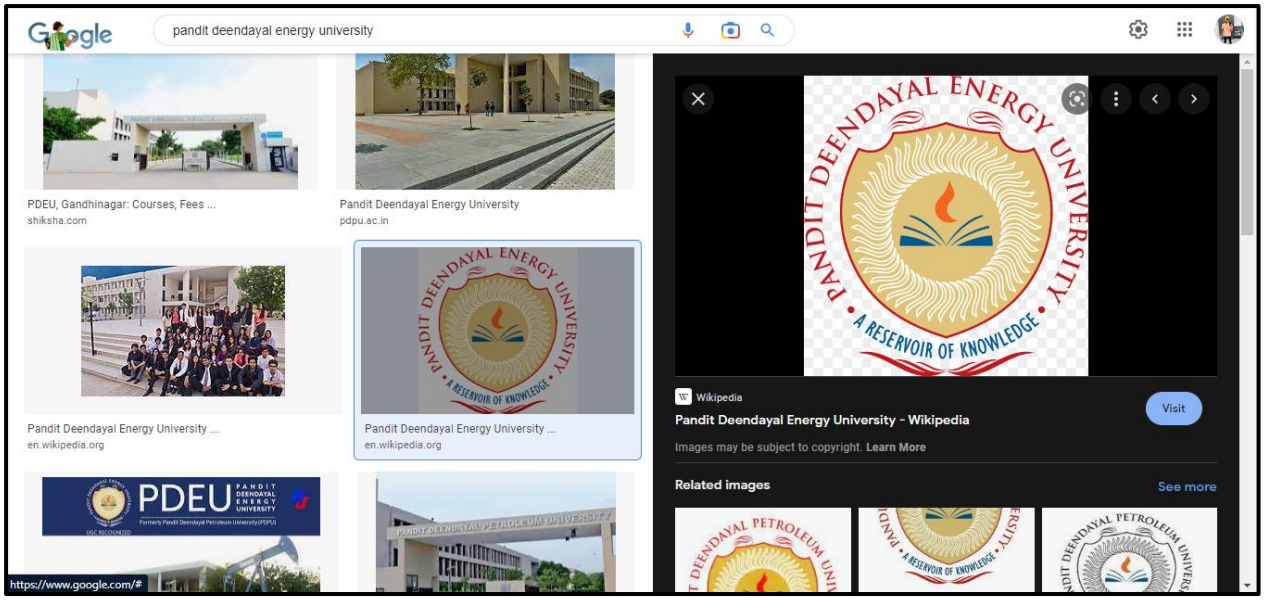
We can get lots of information about any geographical location by its photo and also you will find any random place by its photos and you will get the information about it.

Tool 4: Google image search

Steps:

1. Open https://images.google.com/
2. Click on the search bar and type whatever you want or you can also speak for searching.
3. Then you will get all image results.
4. By selecting any images you will get those images also you can save or download them and copy them or their url.





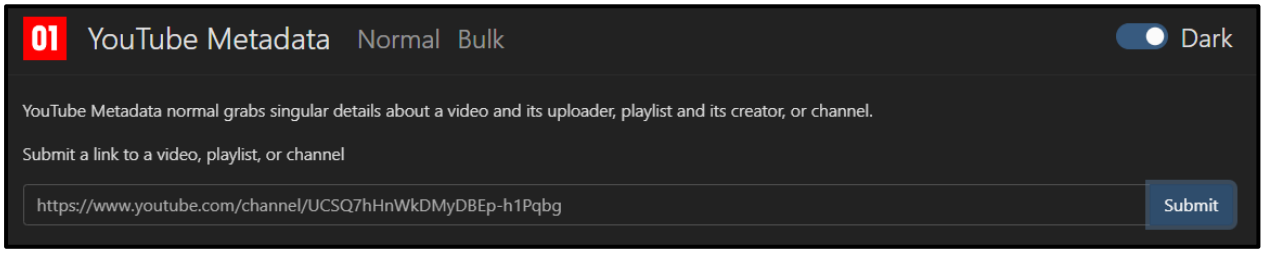
Analysis:

Very easy to access and you can also find lots of images shortly.

Tool 5: YouTube metadata

Steps:

1. Open https://mattw.io/youtube-metadata/
2. Click or search bar and copy the youtube link of that video which you want forensic.
3. Press on “submit”
4. Then you will get all image results, scripts codes or written information.



Channel

The video author, playlist creator, or channel submitted. Click here to see detailed property descriptions.

Snippet


```
{
    "title": "8bit Binks69",
    "description": "◆ ◆ ◆ ◆  About Me ◆ ◆ ◆ ◆ \n\nHi , I am Mithul Nayak, many of you know me as Binks.\nI play games on mobile and PC as well.\nI have joined 8bi
    "customUrl": "@8bitbinks69",
    "publishedAt": "2019-05-01T16:39:00Z",
    "thumbnails": {
        "default": {
```


8bit Binks69

Channel created on Wed, 01 May 2019 16:39:00 GMT (3 years ago)

The channel is associated with country code IN which is India

The channel has a custom url of value '@8bitbinks69'

The channel id is UCSQ7hHnWkDMyDBEp-h1Pqbg

Statistics


```
{
    "viewCount": "80454615",
    "subscriberCount": "218000",
    "hiddenSubscriberCount": false,
    "videoCount": "1095"
}
```


This channel's subscriber count qualifies for benefit level silver (100k-1m). Click here to learn more.

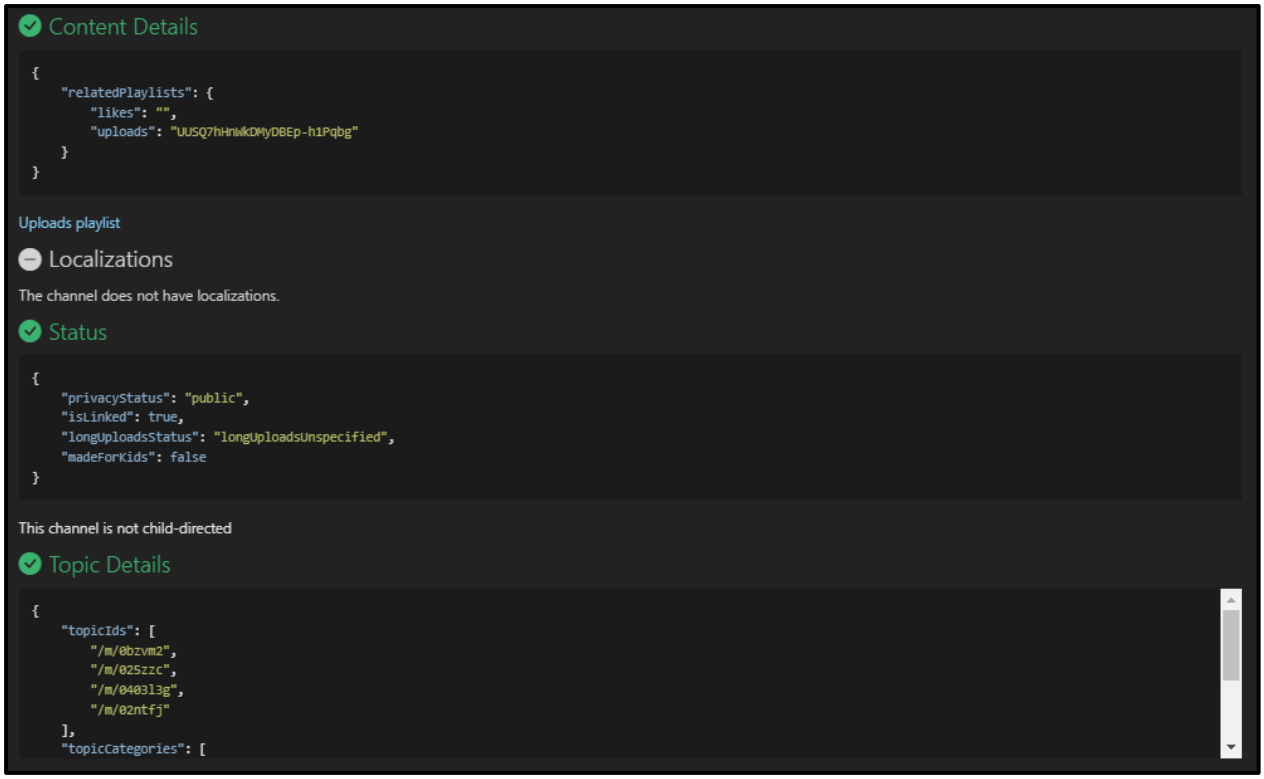
Check out this channel on SocialBlade.

01 Inspect the metadata for all of this channel's videos

Branding Settings


```
{
    "channel": {
        "title": "8bit Binks69",
        "description": "◆ ◆ ◆ ◆  About Me ◆ ◆ ◆ ◆ \n\nHi , I am Mithul Nayak, many of you know me as Binks.\nI play games on mobile and PC as well.\nI have joined
        "keywords": "binks69 blinks69 blinks binks paratroops 8bitbinks s8ul soul valorant T69 pinkcess india valorant gameplay \"valorant live\" \"valorant india\"
        "unsubscribedTrailer": "-NGeUF-nGsA",
        "country": "IN"
```


Channel Keyword(s): binks69 blinks69 blinks binks paratroops 8bitbinks s8ul soul valorant T69 pinkcess india valorant gameplay valorant live valorant india valorant india live live live stream live stream valorant india montage valorant gameplay fun funny facecam indian streamer valorantclips gaming valorantgame valorantgameplay gamer valoranthighlights riotgames pcgaming esports valorantplays valorant live stream 8bitbinks69 s8ul binks s8ul soul binks binks live binks valorant



Analysis:

With a single video link you can easily fetch all information and script code of that video web page when the video gets released who created a video in which language video is available and all.

You can also get the channel owner and channel details like when the channel is created or other video links or other playlist details.

Also, you can watch statistics of the channel like subscriber count and video count, and so on.

Digital Forensics Lab Report: 5

Date: 24-08-2022

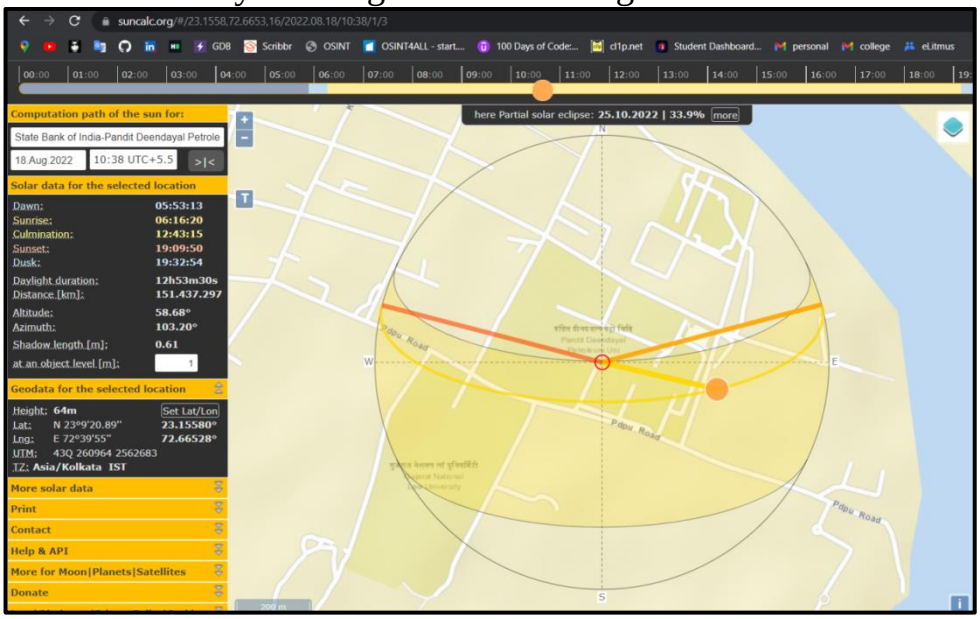
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

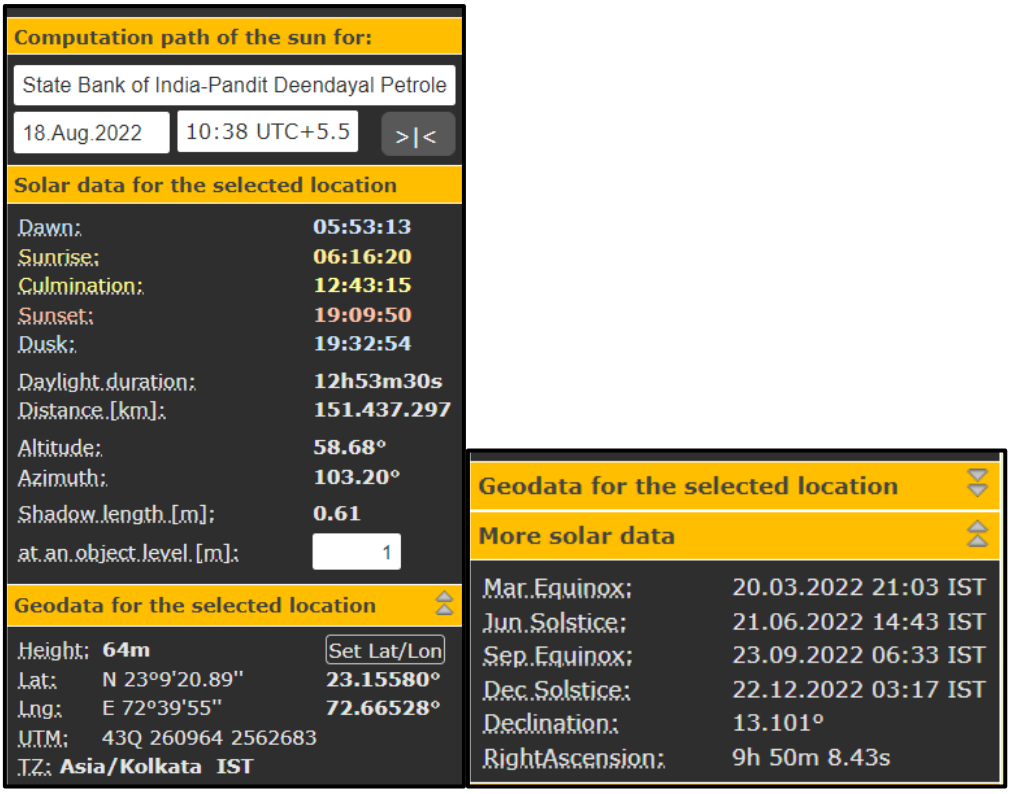
Aim/Purpose: Explore Fake news detection using different tools.

Tool Names: Google image search,Tineye image search, YouTube data viewer, Foto forensic, Forensically, Pic2map, Suncalc, Wikimapia, Exif Data Viewer, Jeffrey exif viewer, Exiftool, Metagoofil, YouTube metadata.

Tool 1:- Suncalc
Steps:

1. Open https://www.suncalc.org/#/49.2334,19.4414,3/2022.08.18/10:43/1/3
2. Now select the location by moving the pin on map or you can also type the description of that location on the left side text box and press enter
3. Then you will get a geographical map view of that location in center
4. And left side you will get solar data or geodata of that location.





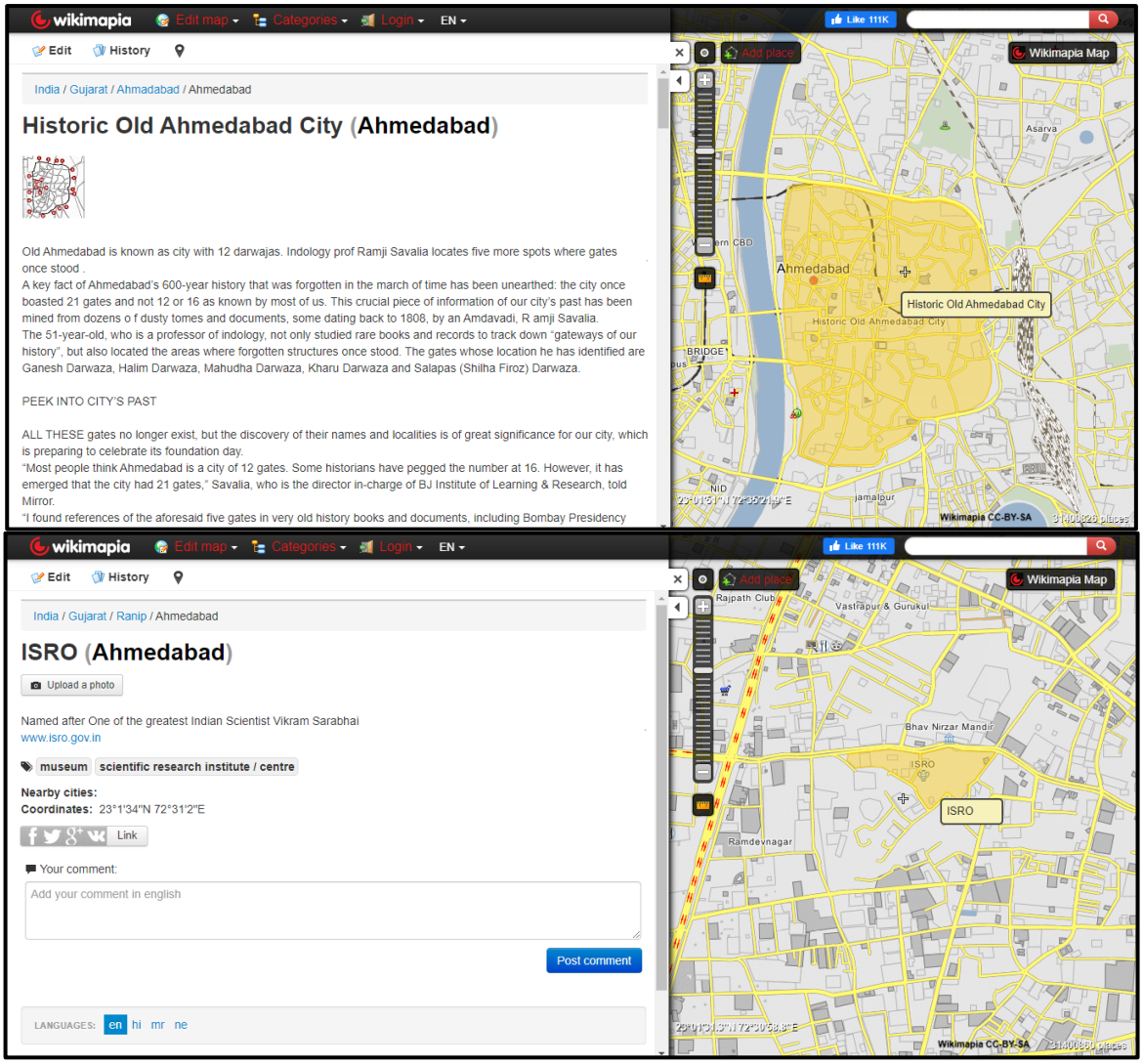
Analysis:-

You will get sunrise, sunset, Dusk, daylight duration and other information by its location description. And if you do not know the location description properly then you can go for map option and you can select the location from map.

Tool 2:- Wikimapia

Steps:-

1. Open https://wikimapia.org/
2. There is search bar on right topmost corner in that you can search anything that you want to search like Stadium, Shops, parks, Schools, etc.
3. In right Side you will all location of that query. Ex:- if you search stadium then you will get all stadium in geographical map.
4. Select the points one by one you will get the stadium details on the left side of page.



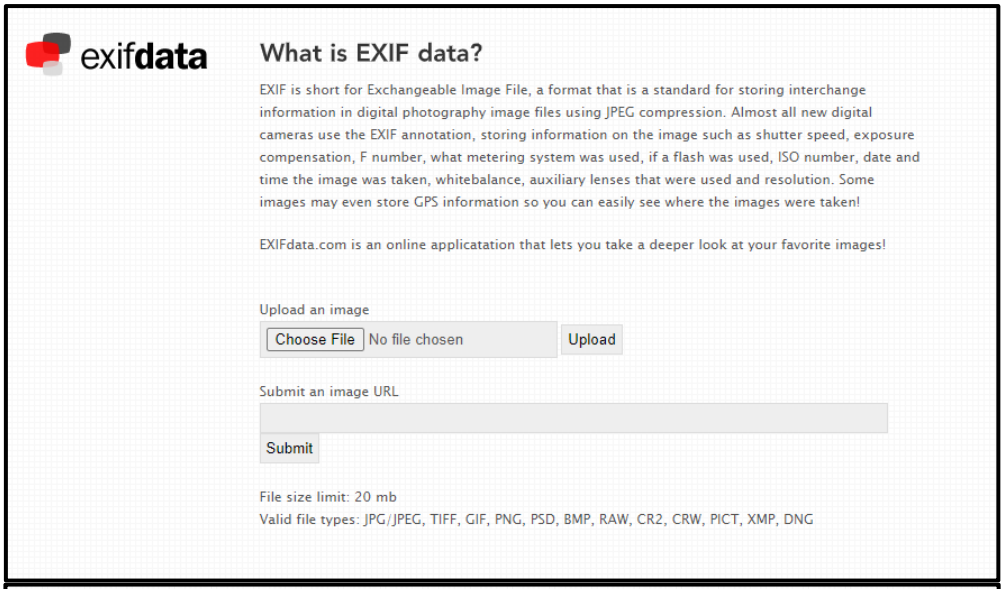
Analysis:-

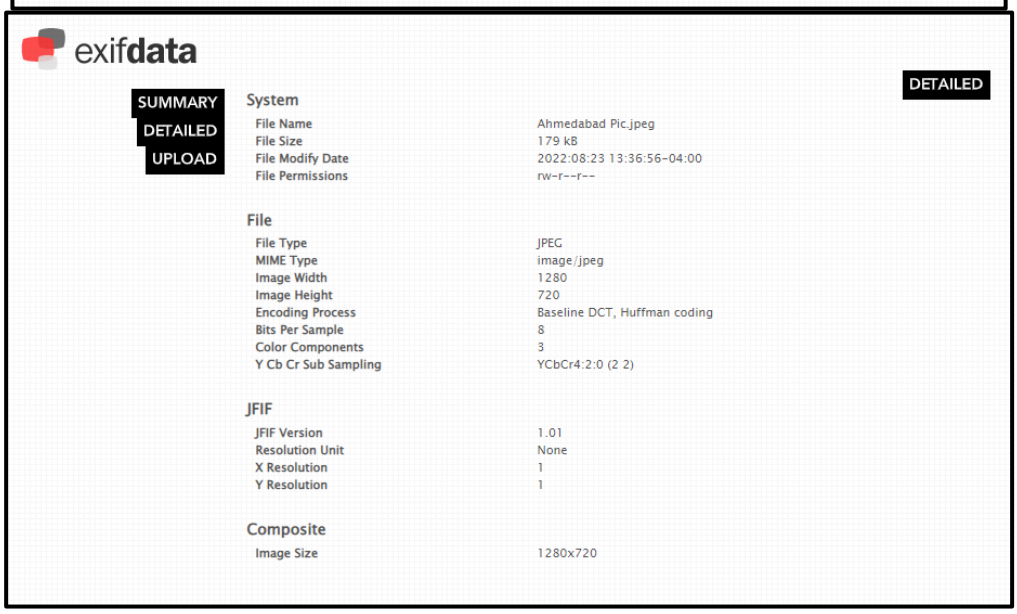
You will get the all locations of particular place by just its type name. Ex:- if want to know about the all shops of your city then just select the city and set the scale to city scan and press enter then you will get the all shops location and its available details.

Tool 3:- Exif Data Viewer

Steps:-

1. Open https://exifdata.com/
2. Press on the choose File for selecting the file from local machine and select the file and upload it
3. Also there is a option for image url if you want fetch details and summary by any online image
4. Press on "Submit" button
5. Then you will get summary and detailed of uploaded images





Analysis:-

You will get the file size, image width, or JFIF details of the images.

Tool 3:- Jeffrey exif viewer

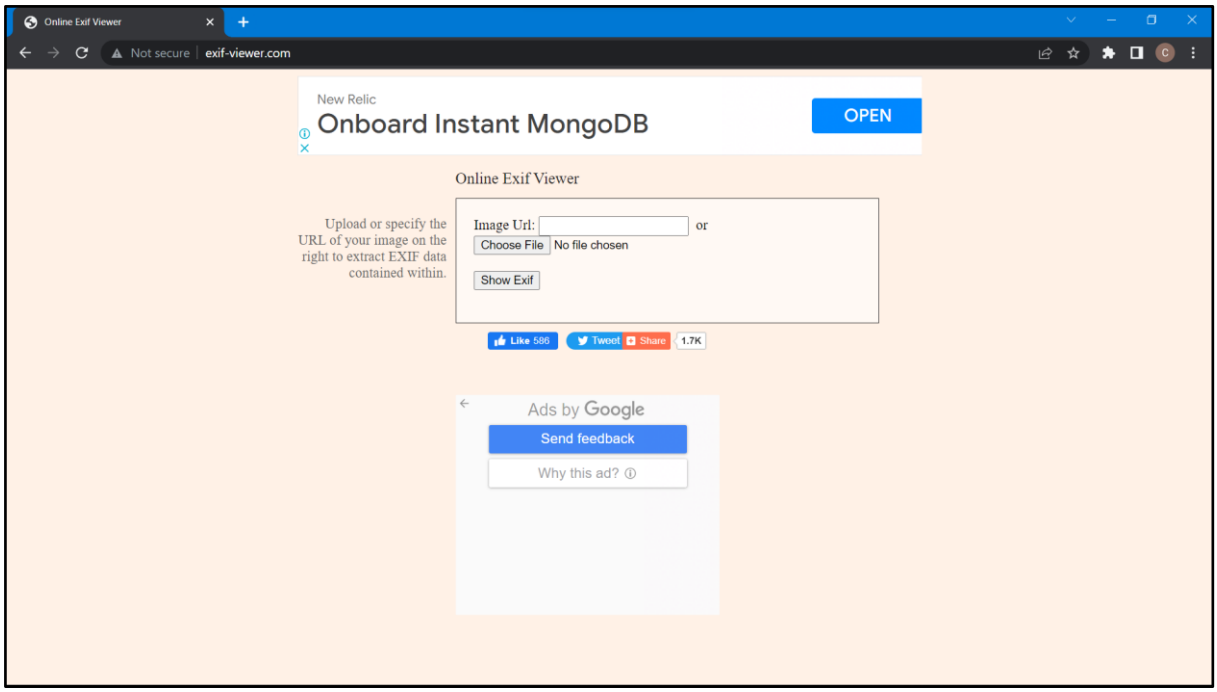
Steps:-

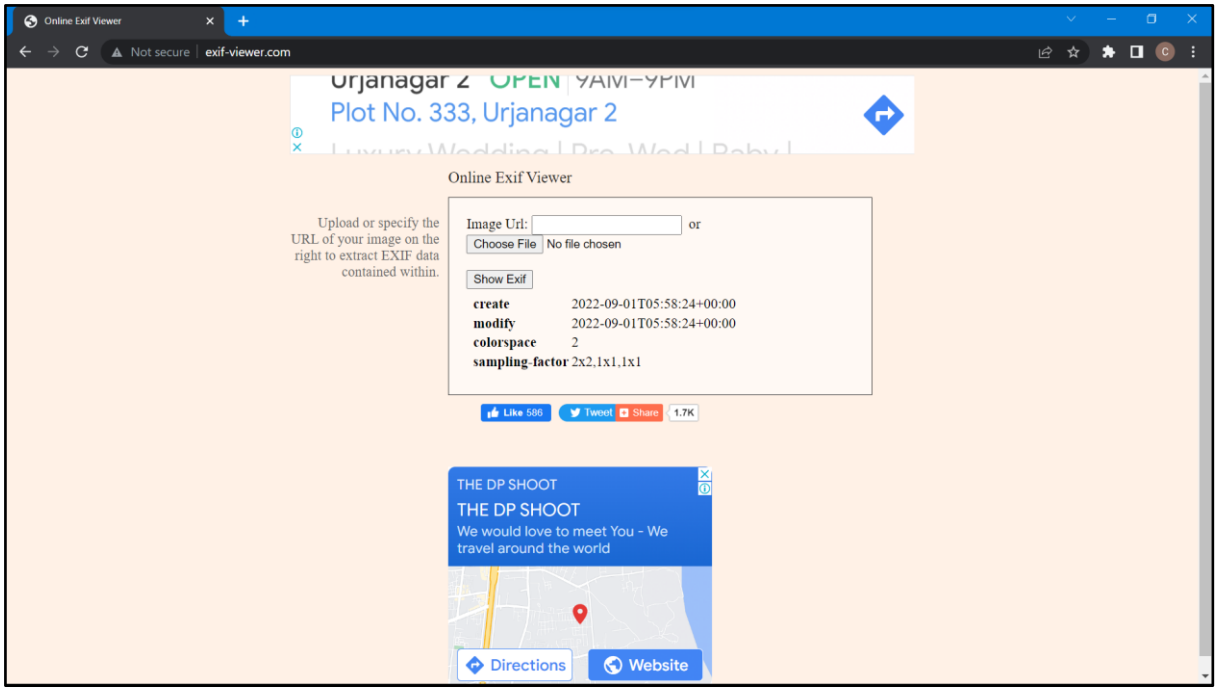
1. Open https://exifdata.com/
2. Press on the choose File for selecting the file from local machine and select the file and upload it
3. Also there is a option for image url if you want fetch details and summary by any online image
4. Press on “Submit” button

Tool 4:- Exif Viewer

Steps:-

1. Open http://exif-viewer.com/
2. Press on the choose File for selecting the file from local machine and select the file and upload it
3. Also there is a option for image url if you want fetch details and summary by any online image
4. Press on “Submit” button

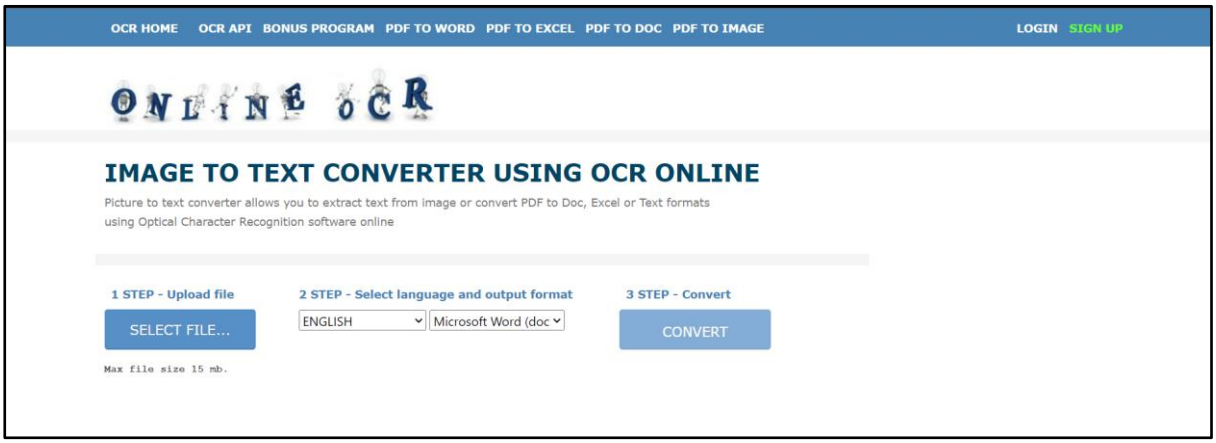


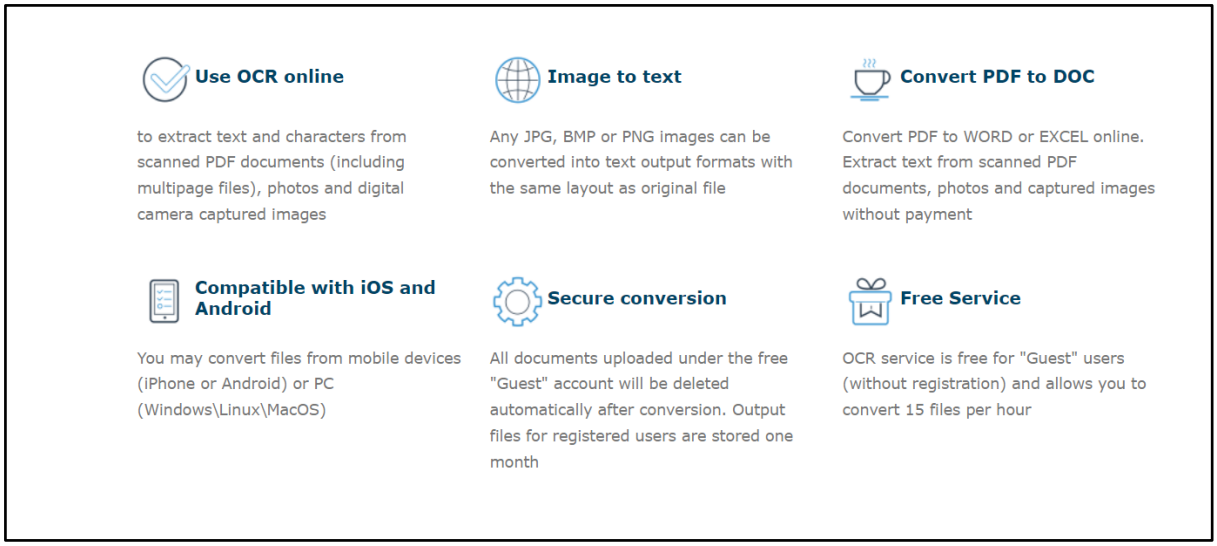


Tool 5:- Online OCR

Steps:-

1. Go to Online OCR
2. One can convert images to text here.
3. There are various other services available as well.



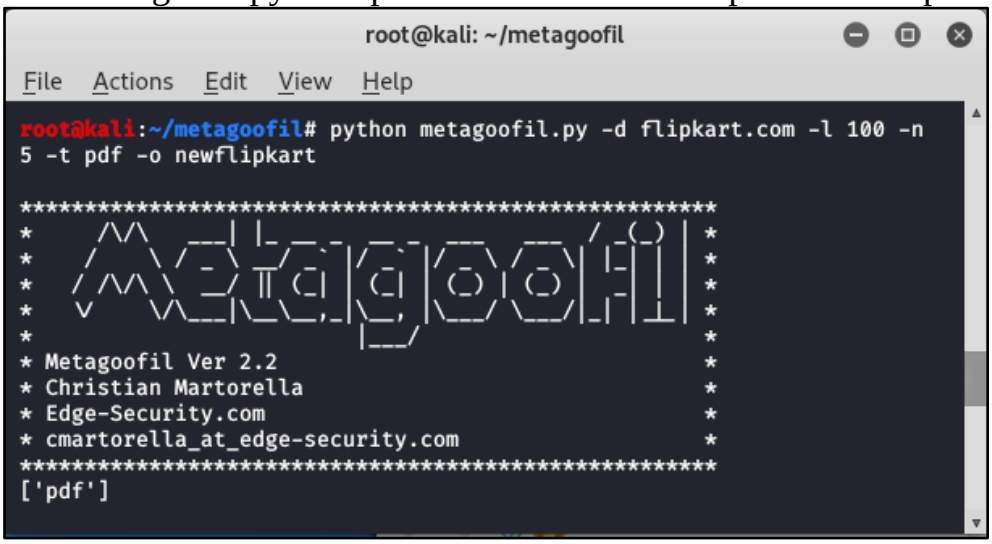


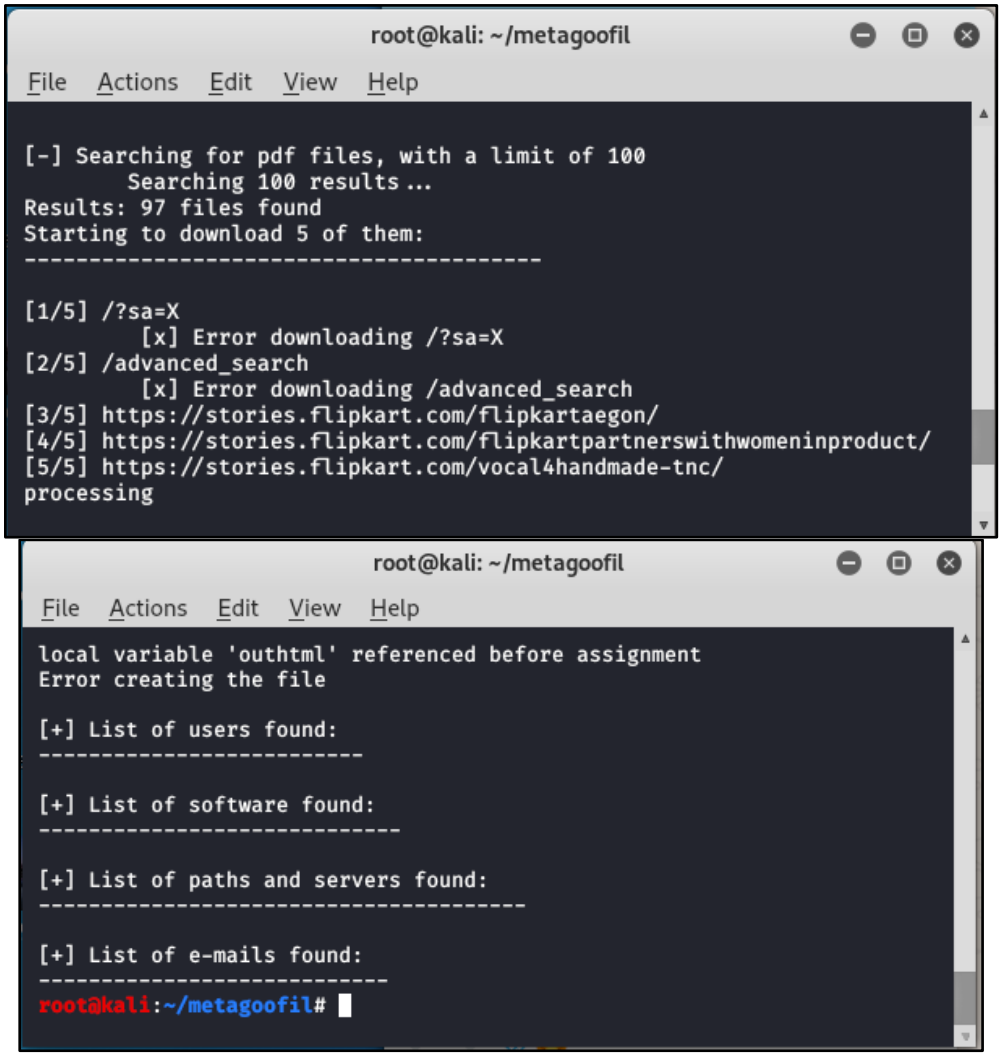
Tool 6:- Metagoofil

The **Metagoofil** is an information-gathering tool. This is a free and open-source tool designed to extract all the metadata information from public documents that are available on websites. This tool uses two libraries to extract data. These are Hachoir and PdfMiner. After extracting all the data, this tool will generate a report which contains usernames, software versions, and servers or machine names that will help Penetration testers in the information-gathering phase.

Steps:-

1. Open your kali Linux operating system and install the tool using the following command.
2. git clone https://github.com/laramies/metagoofil.git
   cd metagoofil
3. python metagoofil.py
4. Use the metagoofil tool to extract PDFs from a website.
5. python metagoofil.py -d flipkart.com -l 100 -n 5 -t pdf -o newflipkart.



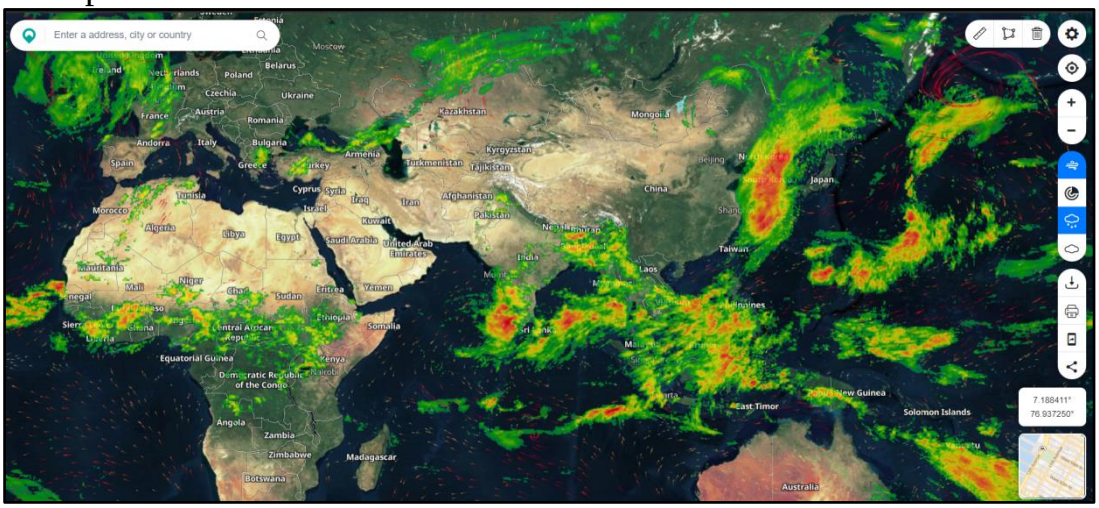


In this way, you can extract PDFsf and information on files from a website.

Tool 7:- Google Earth

Steps:-

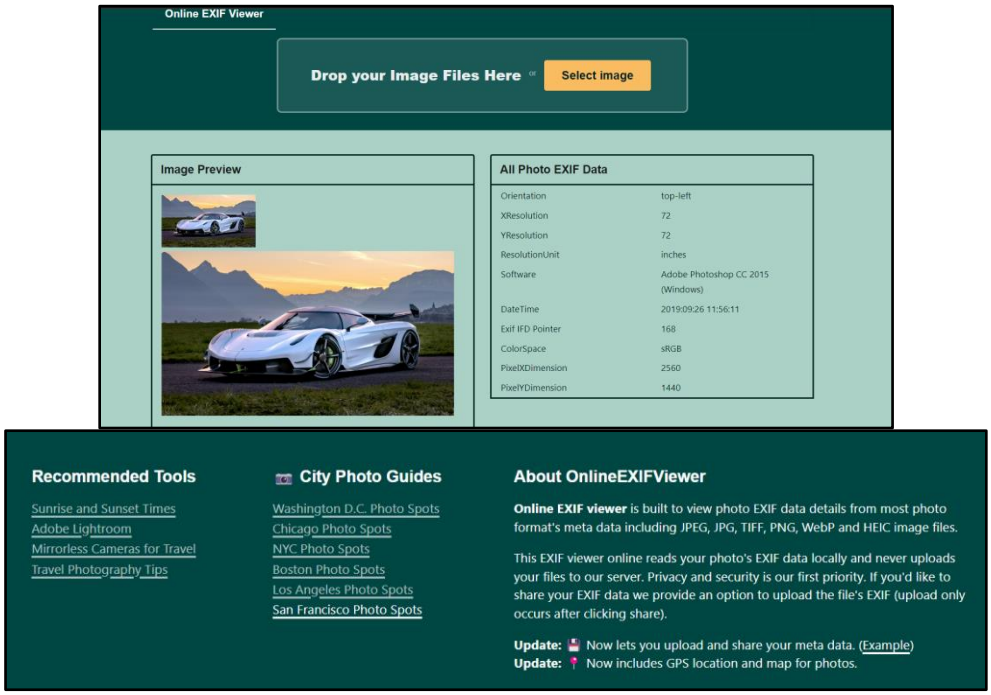
1. Go to Google Earth
2. Explore the website



Tool 8:- EXIF Viewer

Steps:-

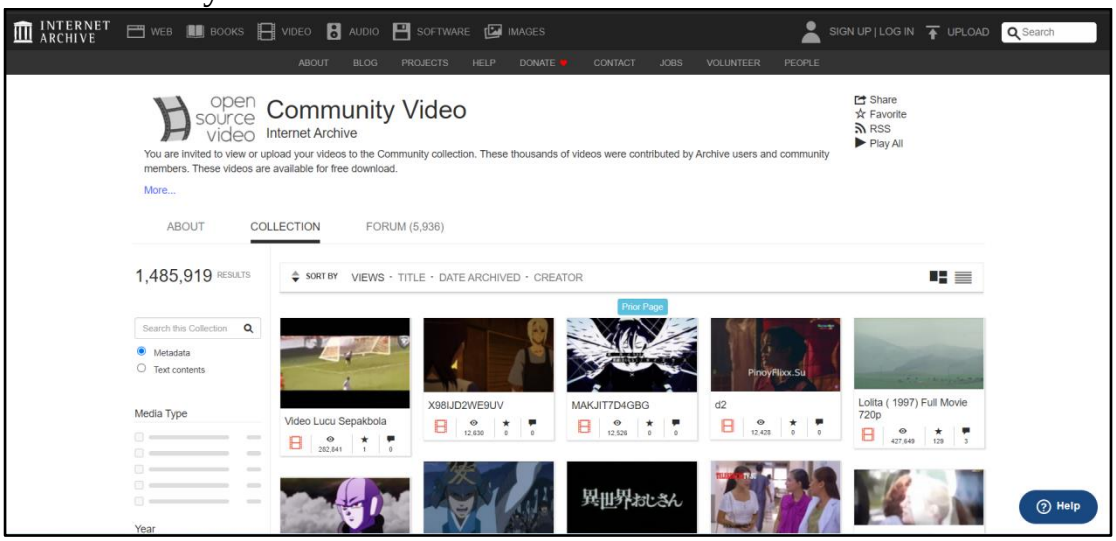
1. Go to EXIF
2. Upload your image
3. Get the exif data



Tool 9:- Internet Archive Videos

Steps:-

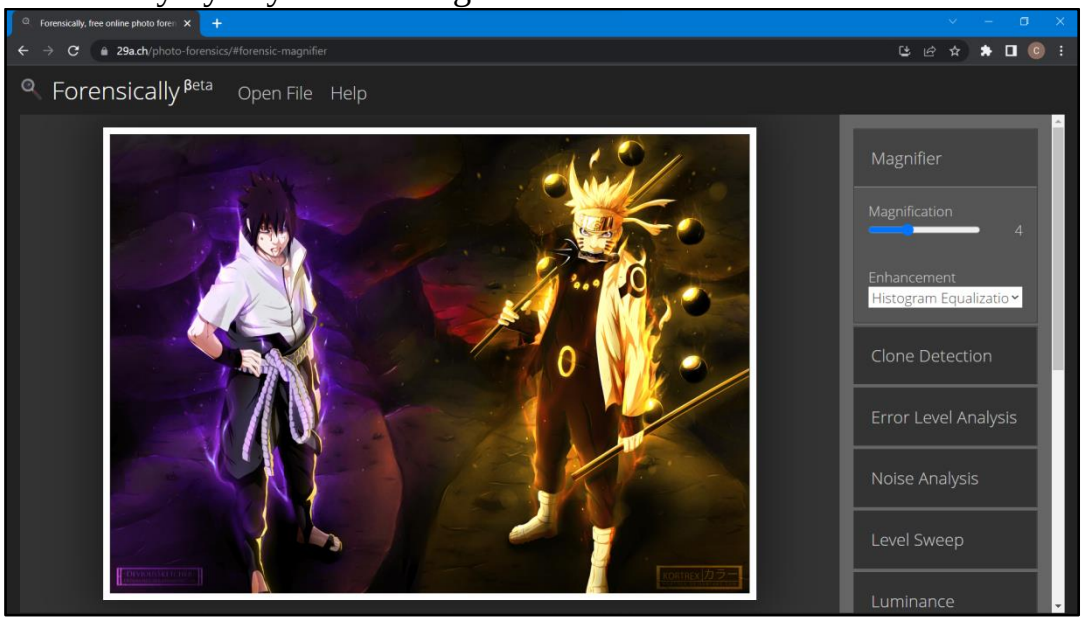
1. Go to Internet archive
2. Here you can get access to any images and videos uploaded by the community.

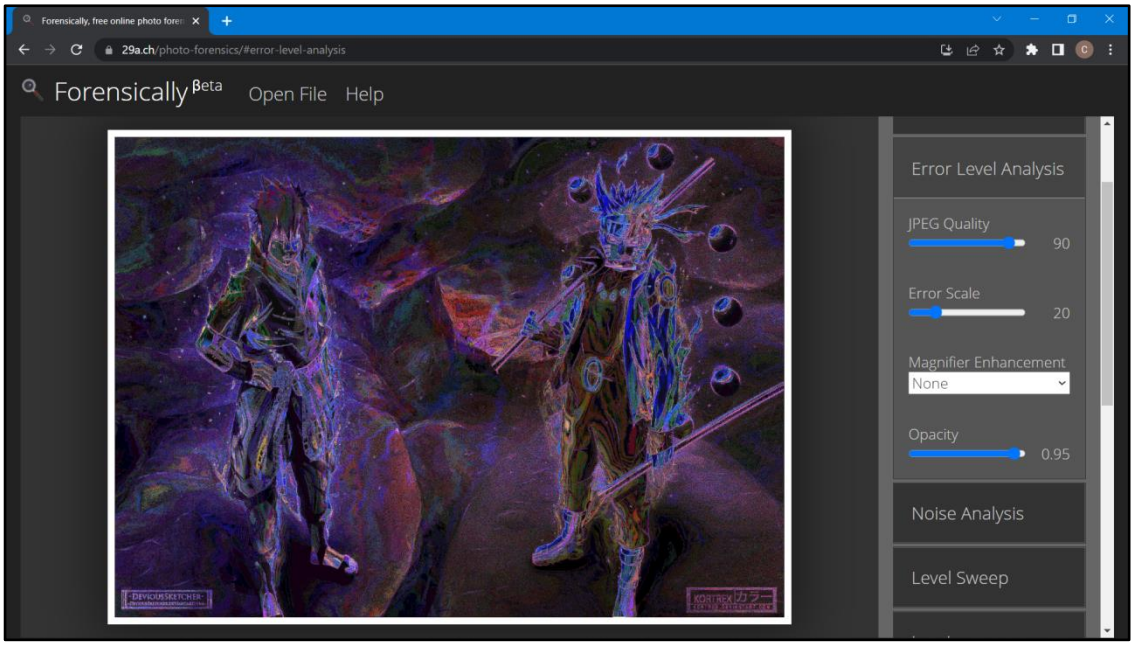


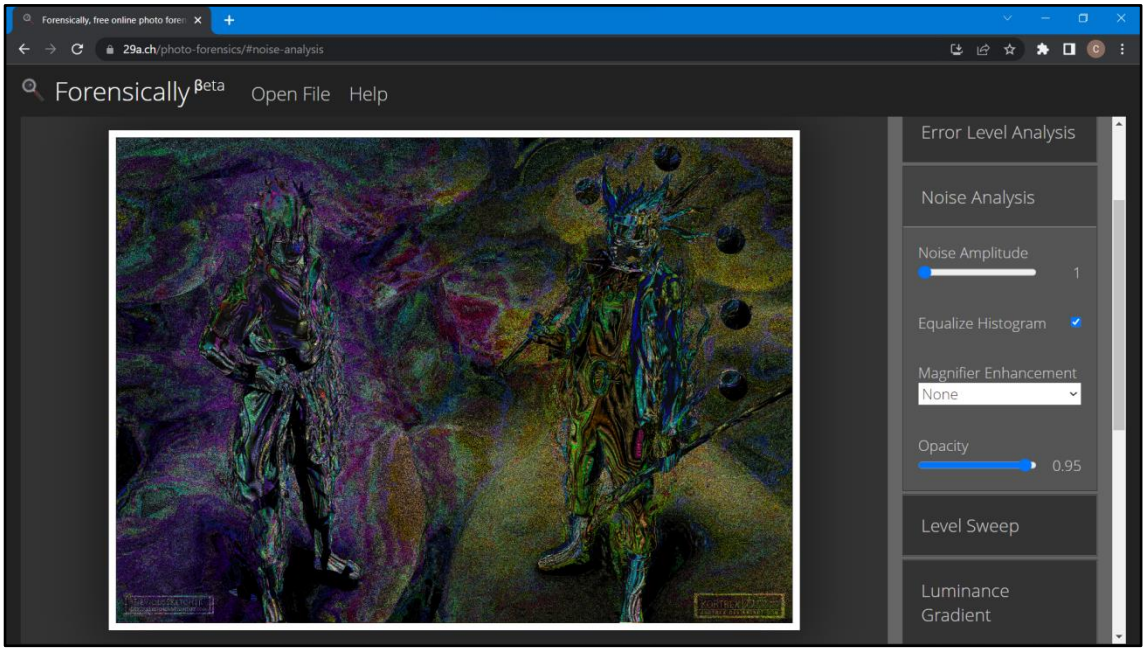
Tool 10:- Forensically

Steps:-

1. Open https://29a.ch/photo-forensics/#forensic-magnifier
2. Press on the open File for selecting the file from the local machine and select the file and upload it.
3. Also there is an option for image url if you want fetch details and summary by any online image.






Forensically, free online photo foren
29a.ch/photo-forensics/#noise-analysis
Forensically βeta
Open File
Help
Error Level Analysis
Noise Analysis
Noise Amplitude
1
Equalize Histogram
Magnifier Enhancement
None
Opacity
0.95
Level Sweep
Luminance Gradient

Digital Forensics Lab Report: 6

Date: 07-09-2022

Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

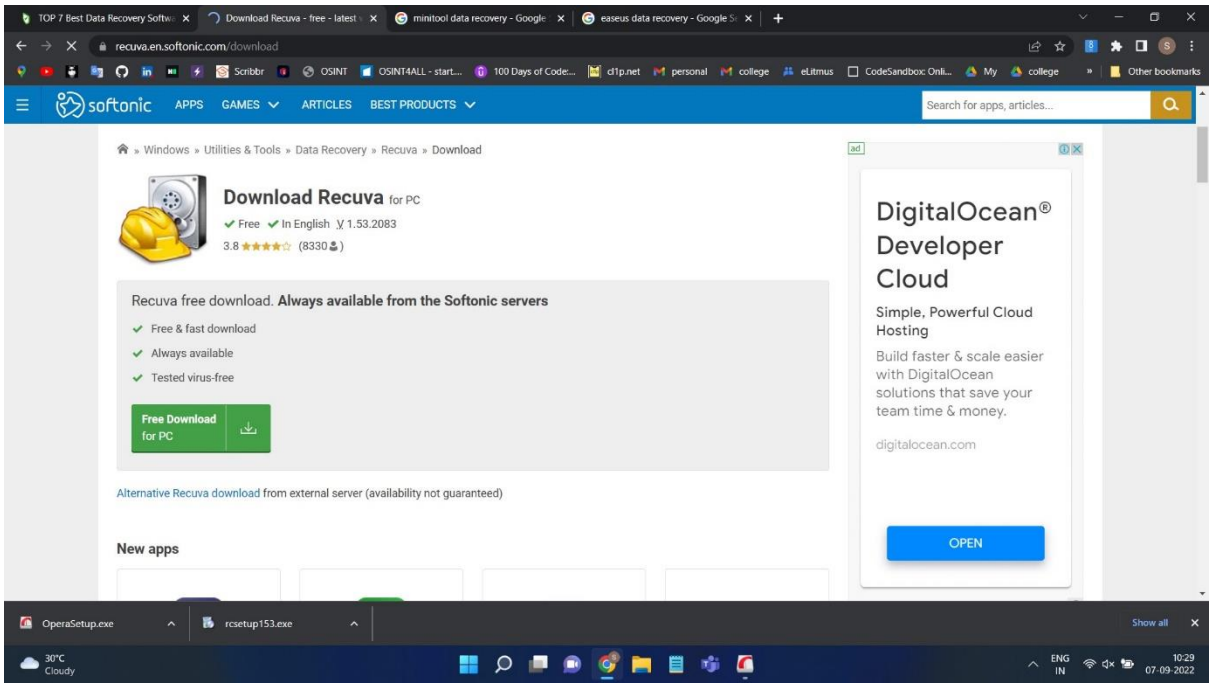
Aim/Purpose: Study of a Data Recovery from Computer Systems, Mobile Devices and other electronic peripherals.

Tool Names: Recuva Data Recovery Tool, EaseUS Data Recovery Tool

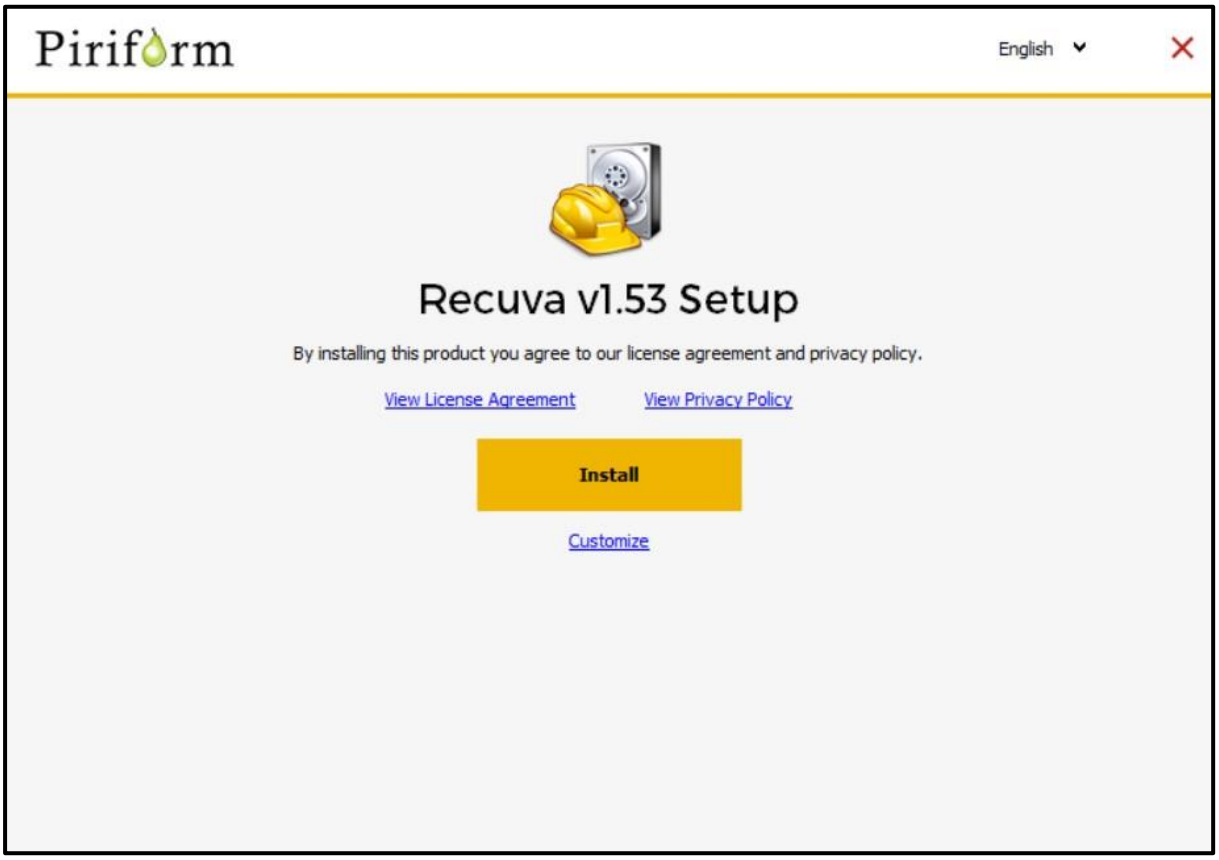
Task 1: Explore Recuva Data Recovery Tool

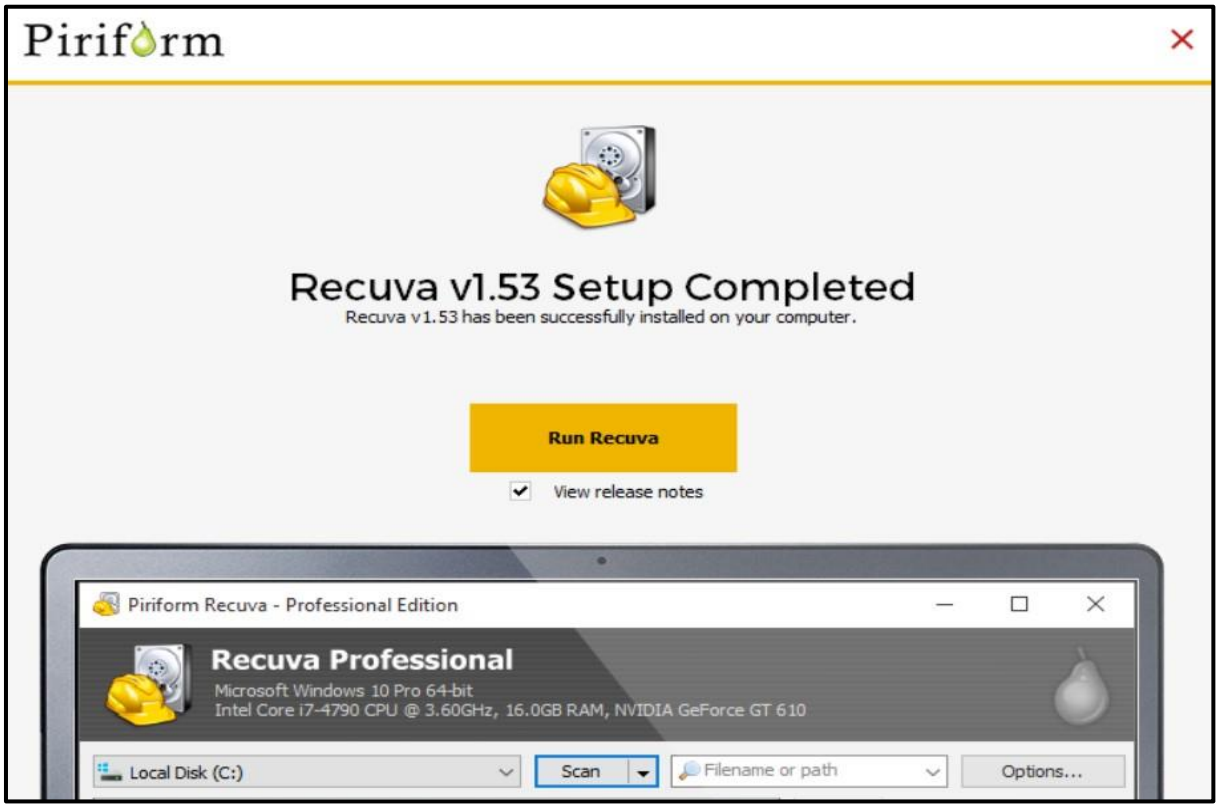
Steps:

1. Go to https://recuva.en.softonic.com/ and download the recuva tool.

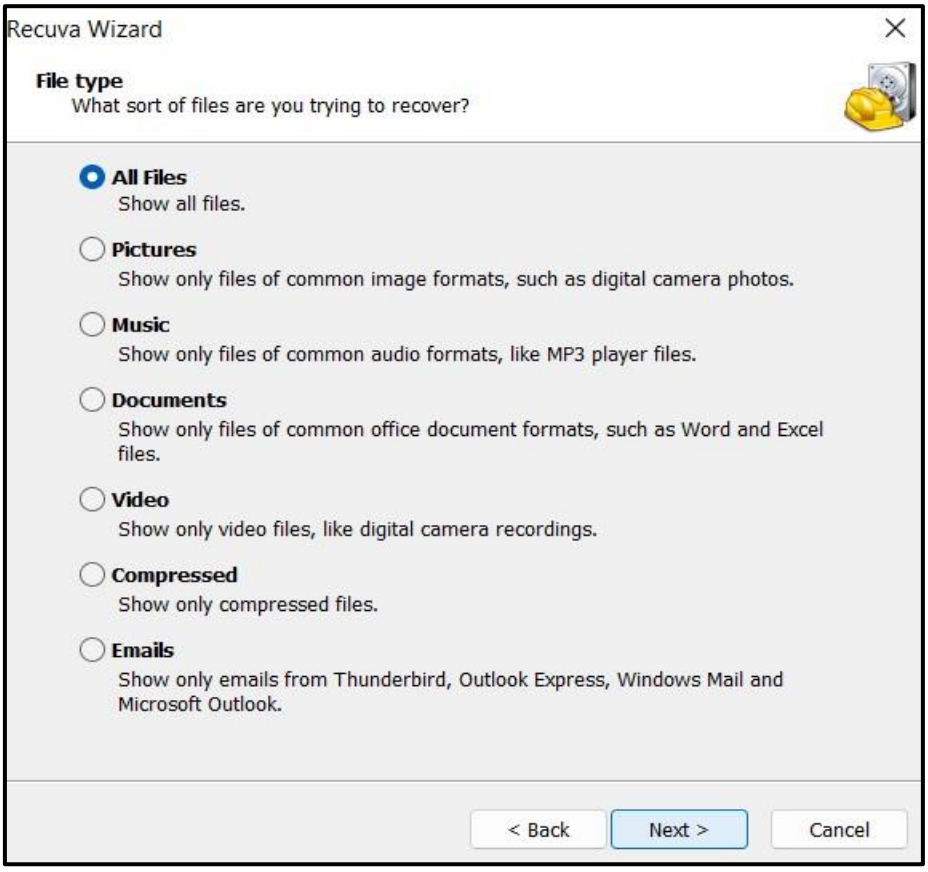


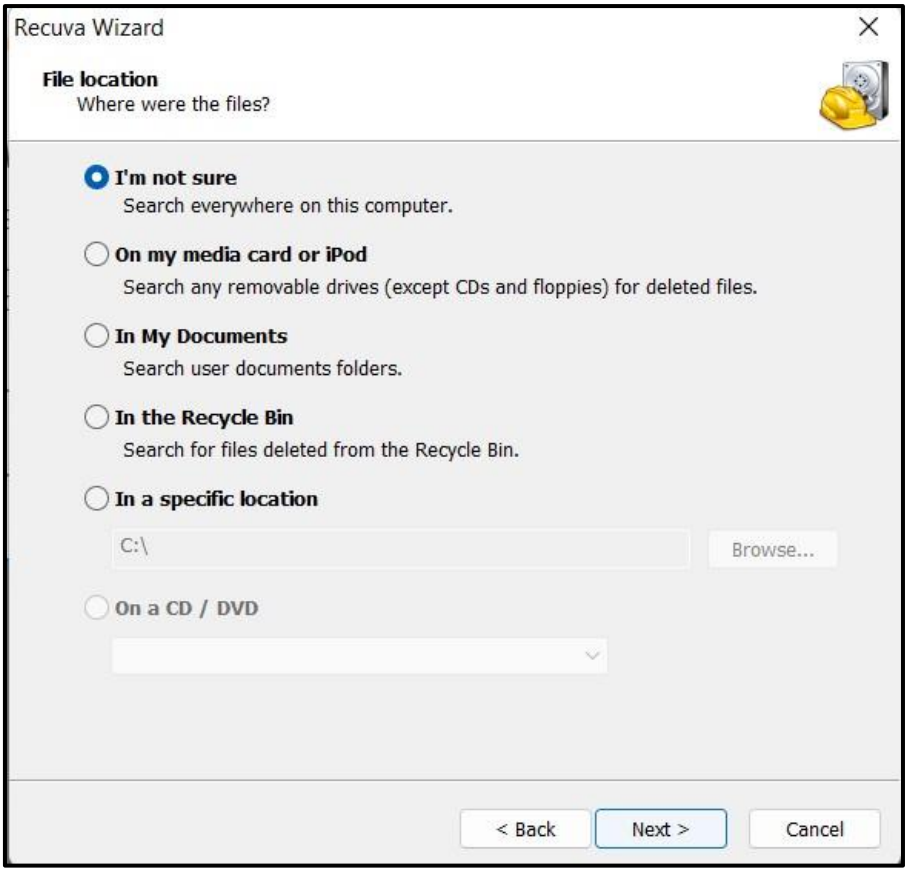
2. After Installing setup start installation process.

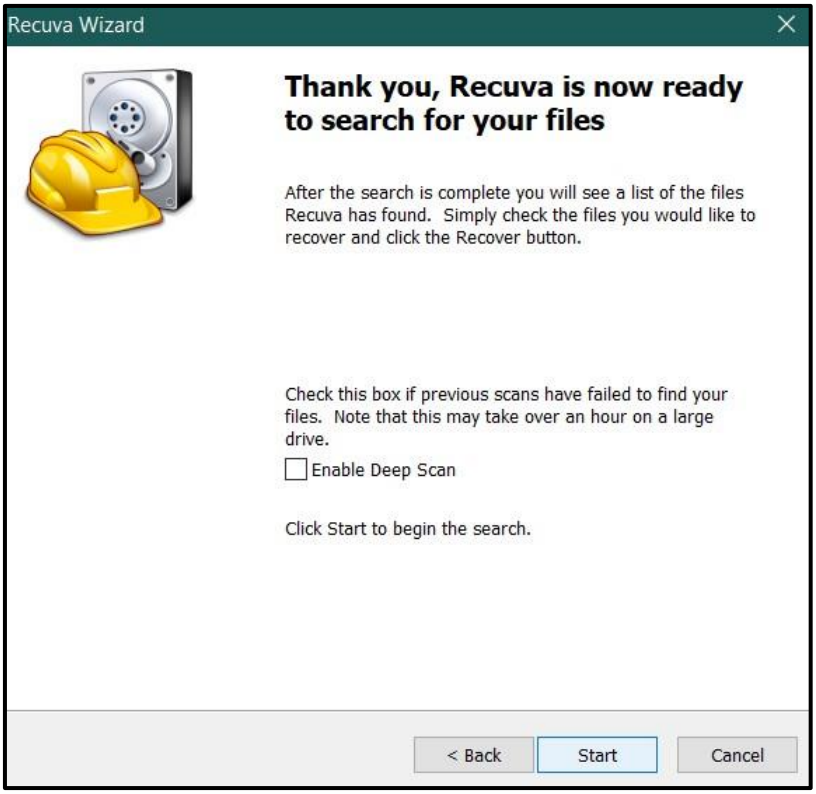


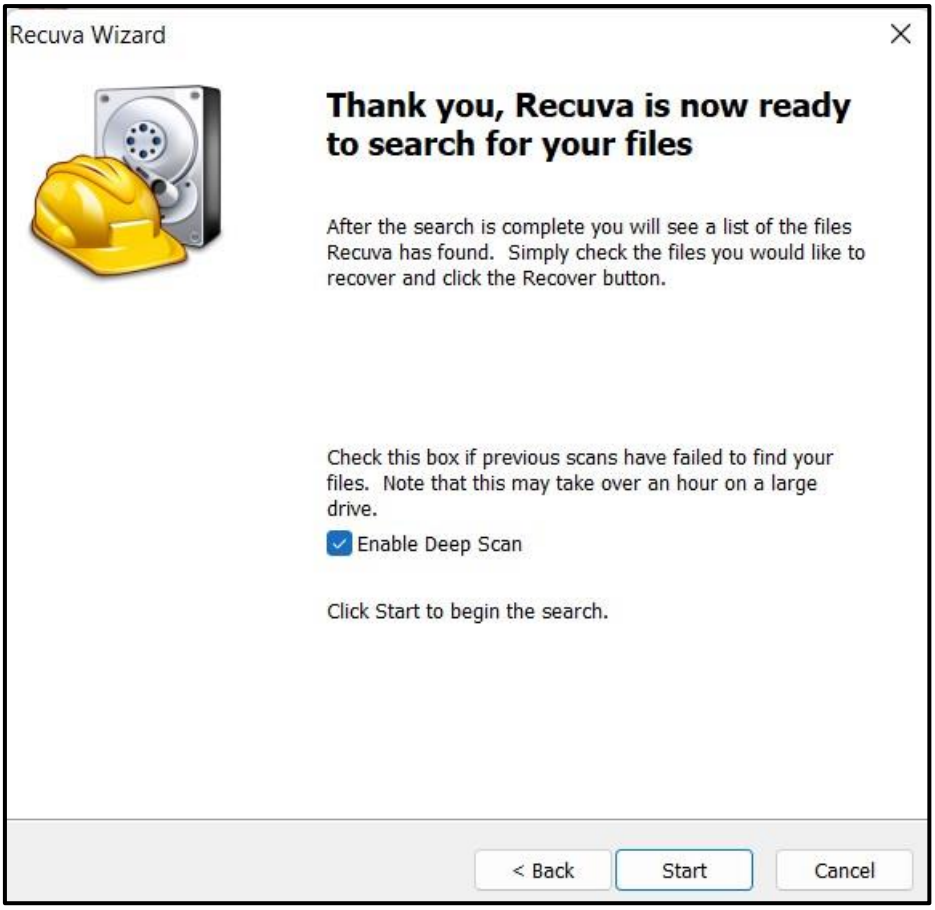



Recuva Wizard
Welcome to the Recuva Wizard
This wizard will help you recover your deleted files. Just answer a few simple questions and Recuva does the rest.
If you don't want to use this wizard, simply press Cancel and you will have access to the advanced features of Recuva.
Do not show this Wizard on startup.
< Back
Next >
Cancel

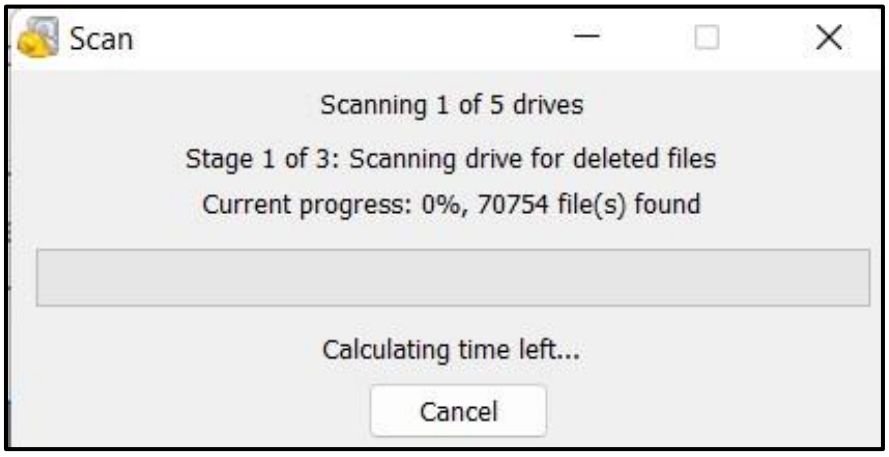

Recuva Wizard
File type
What sort of files are you trying to recover?
All Files
Show all files.
Pictures
Show only files of common image formats, such as digital camera photos.
Music
Show only files of common audio formats, like MP3 player files.
Documents
Show only files of common office document formats, such as Word and Excel files.
Video
Show only video files, like digital camera recordings.
Compressed
Show only compressed files.
Emails
Show only emails from Thunderbird, Outlook Express, Windows Mail and Microsoft Outlook.
< Back
Next >
Cancel


Recuva Wizard
File location
Where were the files?
I'm not sure
Search everywhere on this computer.
On my media card or iPod
Search any removable drives (except CDs and floppies) for deleted files.
In My Documents
Search user documents folders.
In the Recycle Bin
Search for files deleted from the Recycle Bin.
In a specific location
C:\
Browse...
On a CD / DVD
< Back
Next >
Cancel

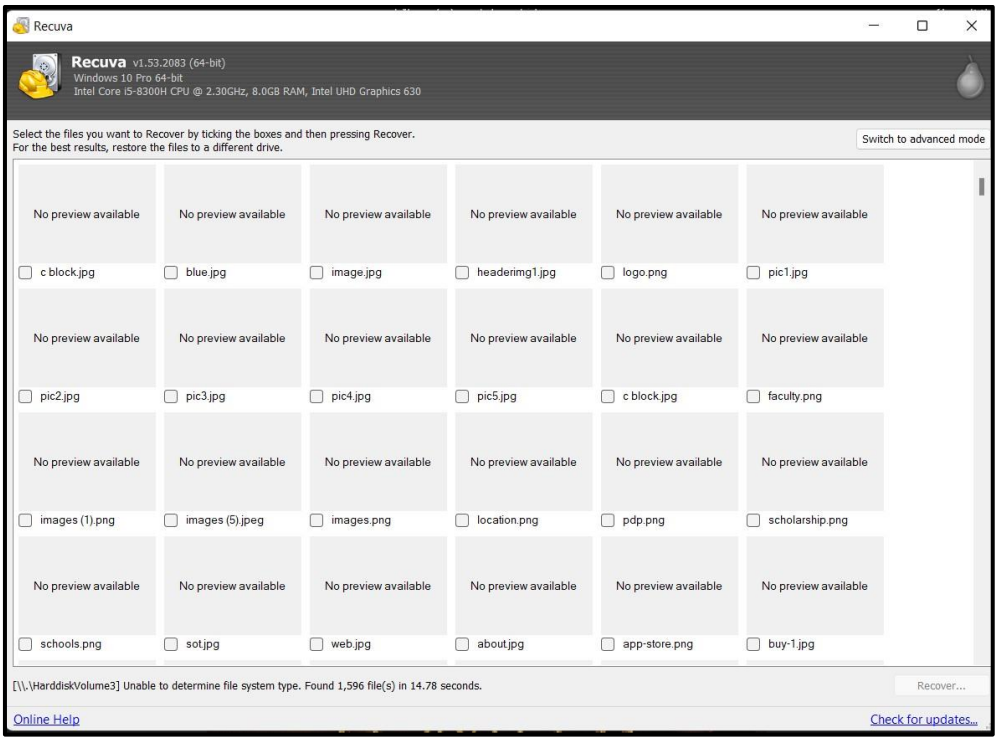

Recuva Wizard
Thank you, Recuva is now ready to search for your files
After the search is complete you will see a list of the files Recuva has found. Simply check the files you would like to recover and click the Recover button.
Check this box if previous scans have failed to find your files. Note that this may take over an hour on a large drive.
Enable Deep Scan
Click Start to begin the search.
< Back
Start
Cancel



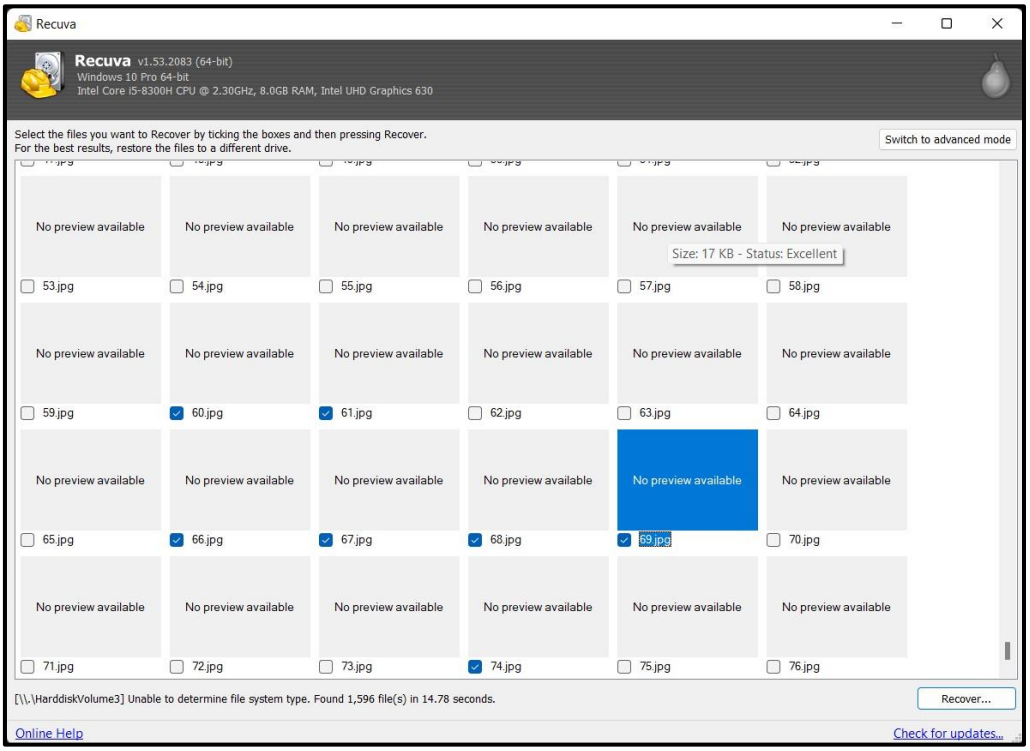
3. After Initializing the process of data recovery. You will be able to see scanning as below:

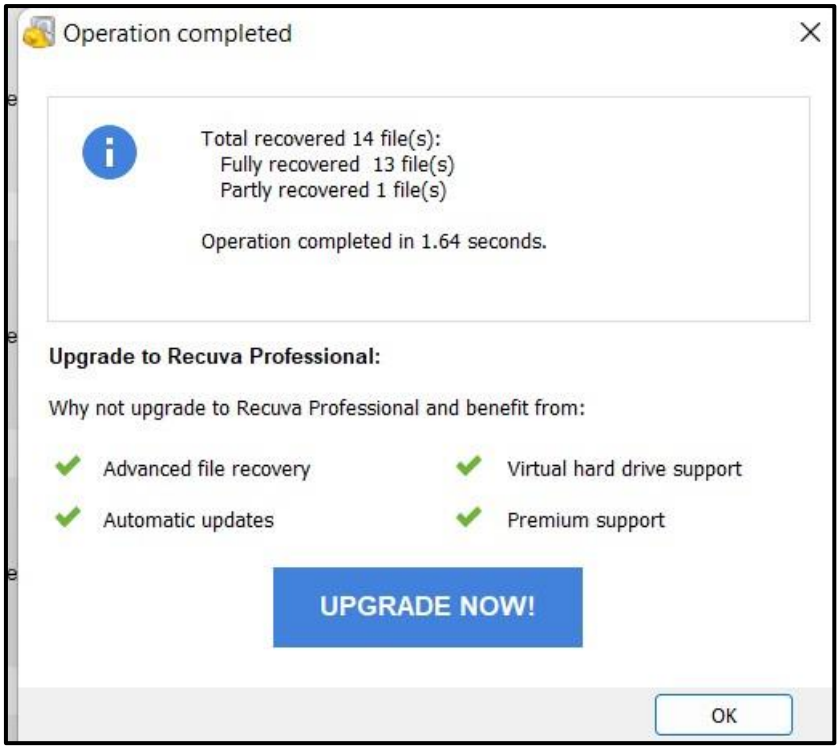


4. After Completion of data recovery scanning, you will be able to explore following results.

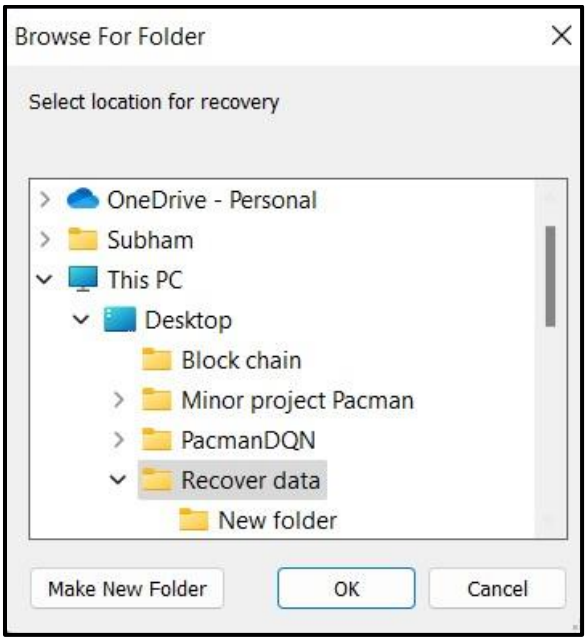


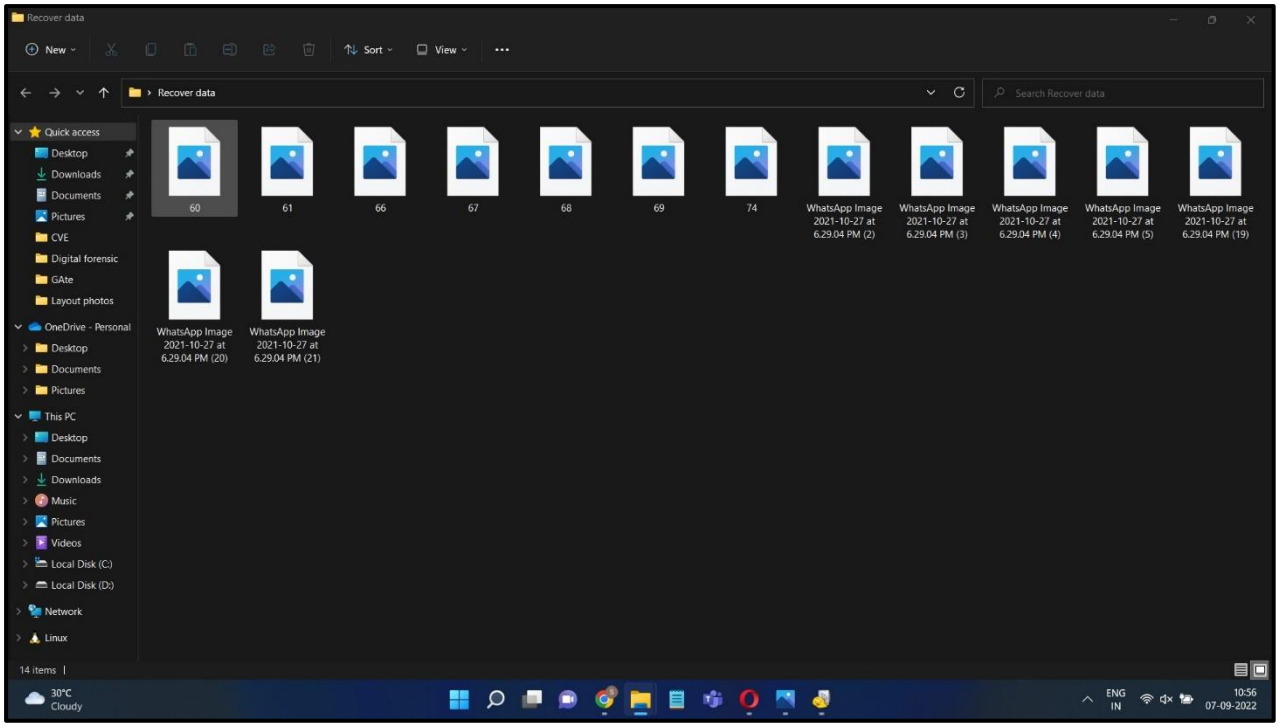
5. Now select the files/images that you want to recover



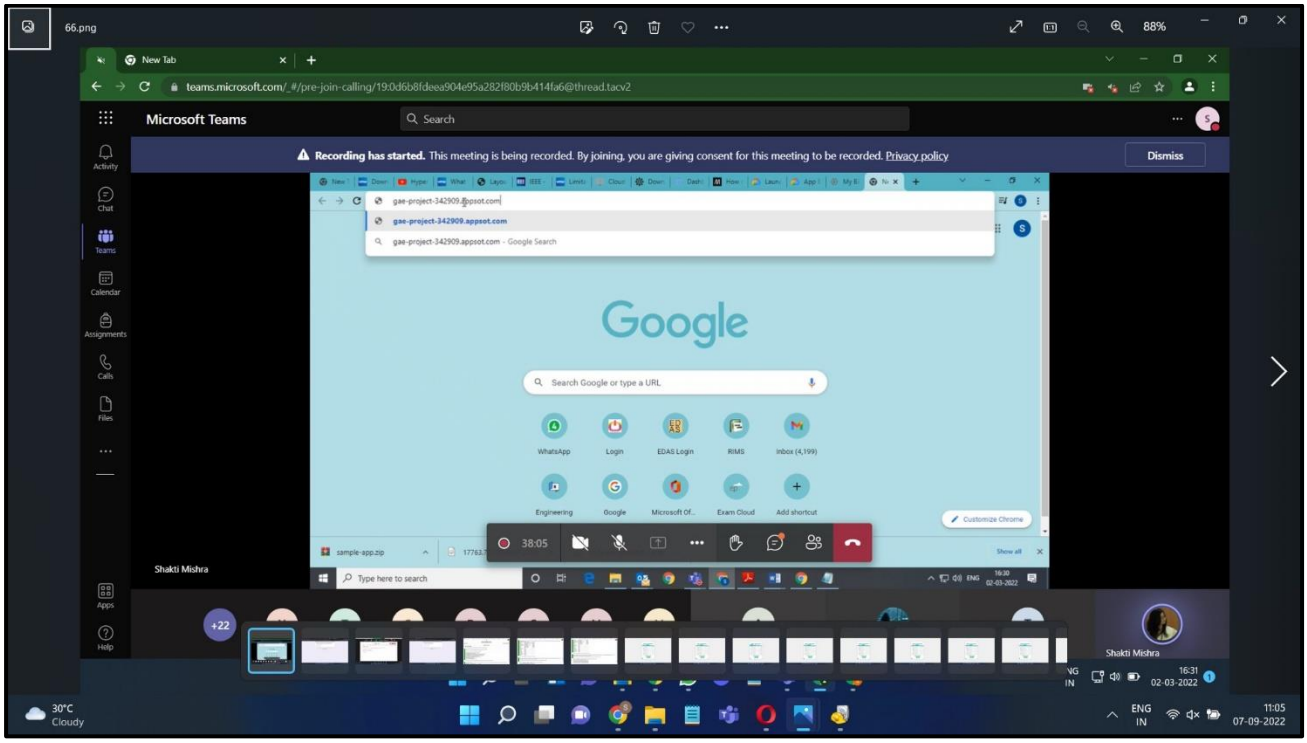


6. Select the file path for restoring the files





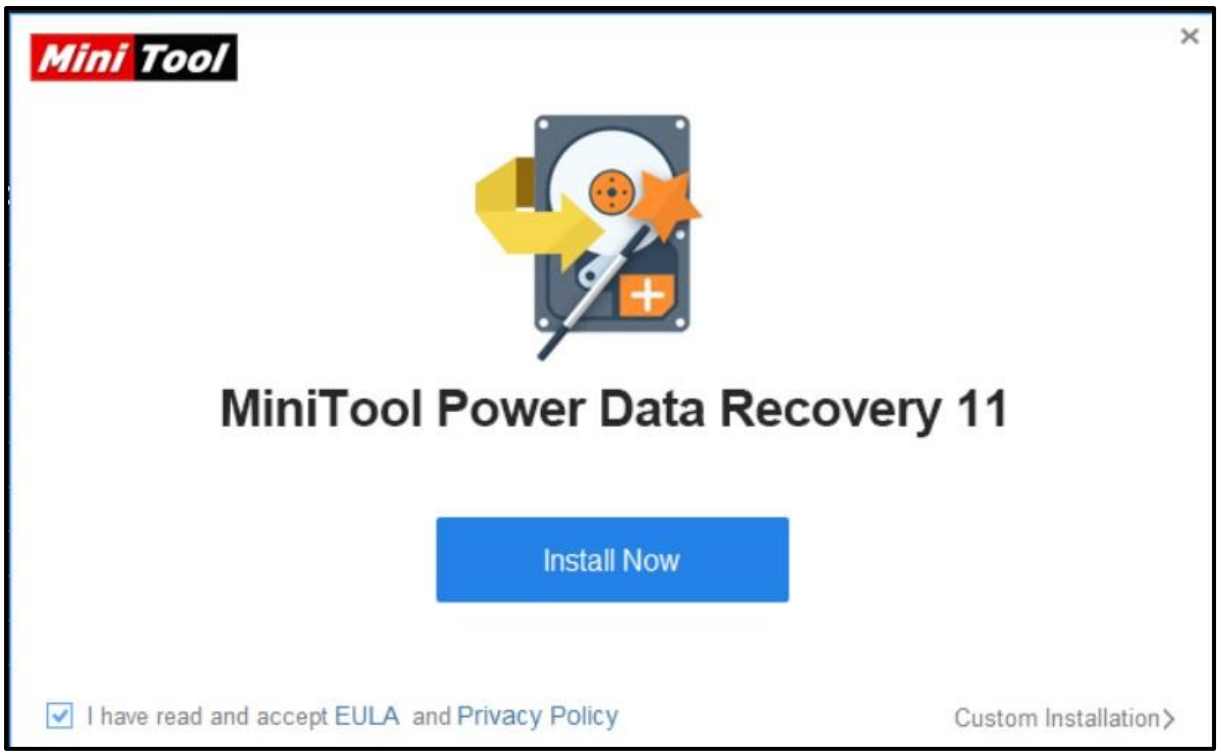
Deleted File/Image:



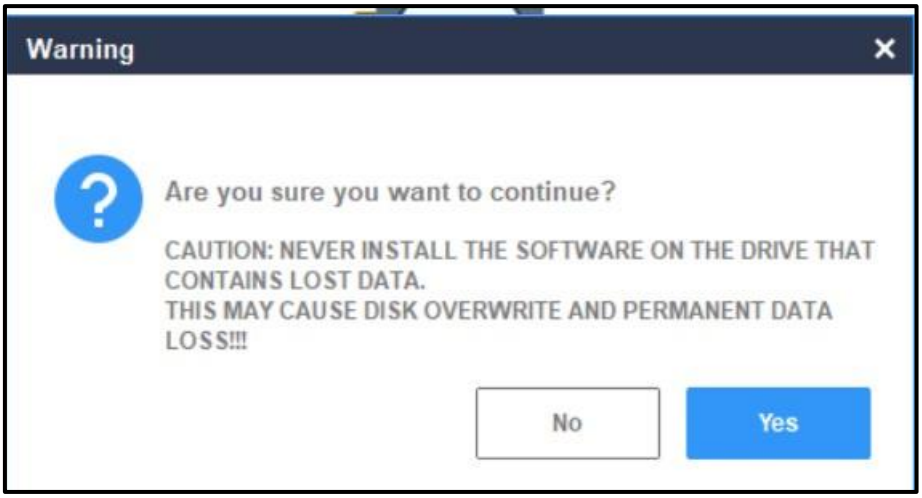
Task 2: Minitool

Steps:

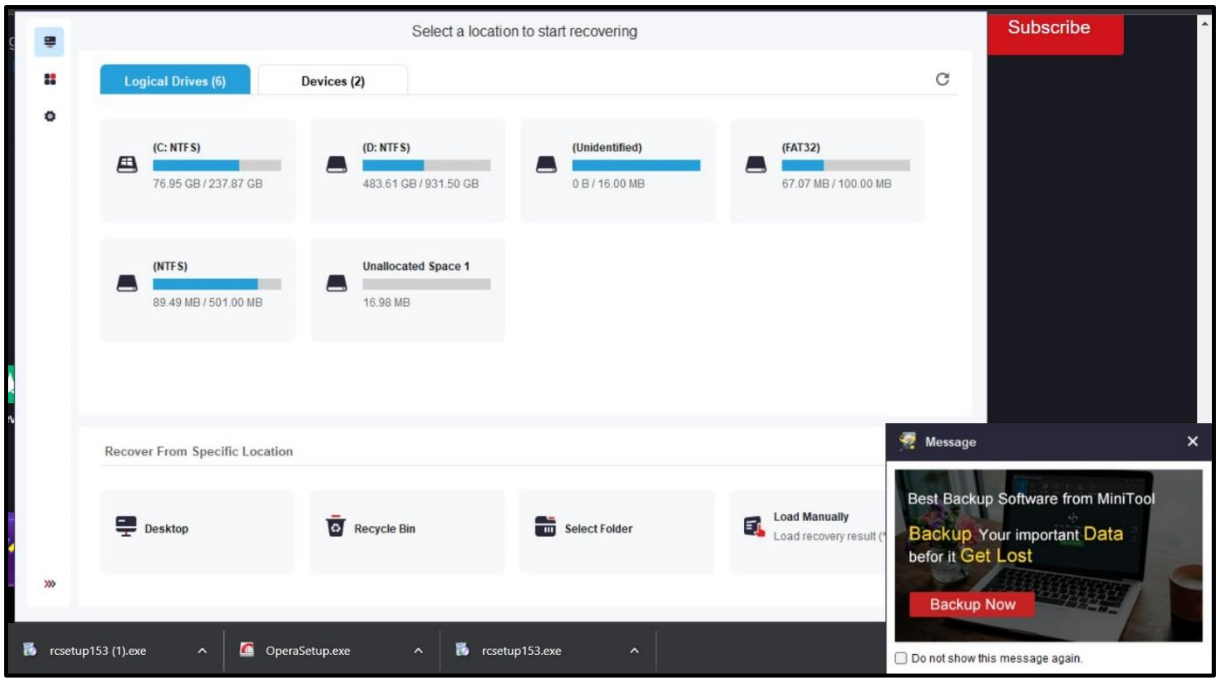
1. Go to https://www.minitool.com/data-recovery-software/ and download the Mini tool



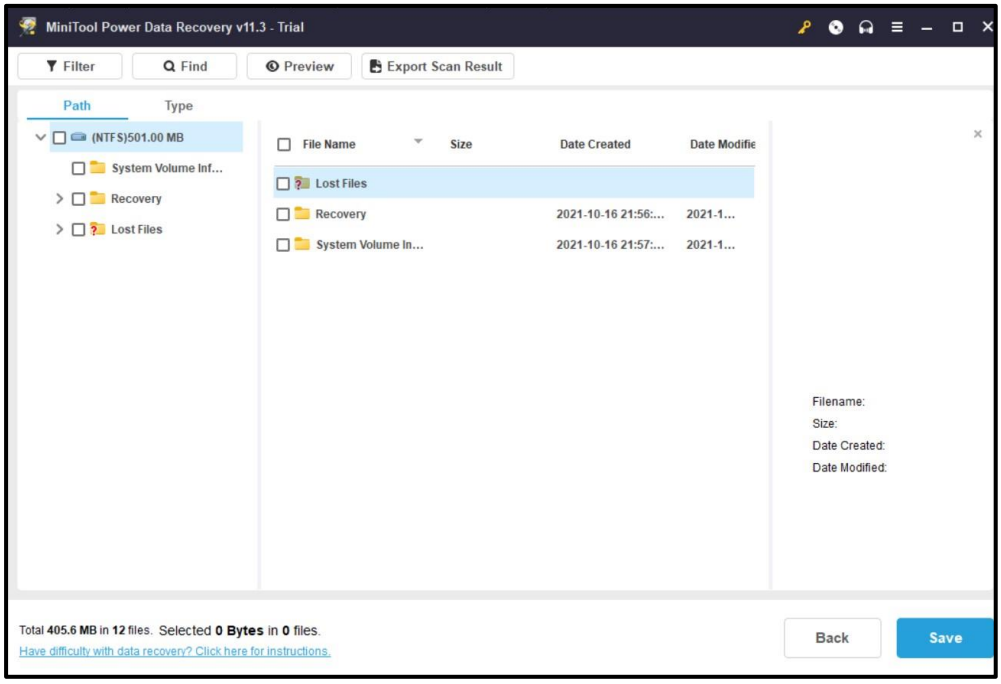
2. After Installing setup of the tool, following procedure will be followed to install the tool.

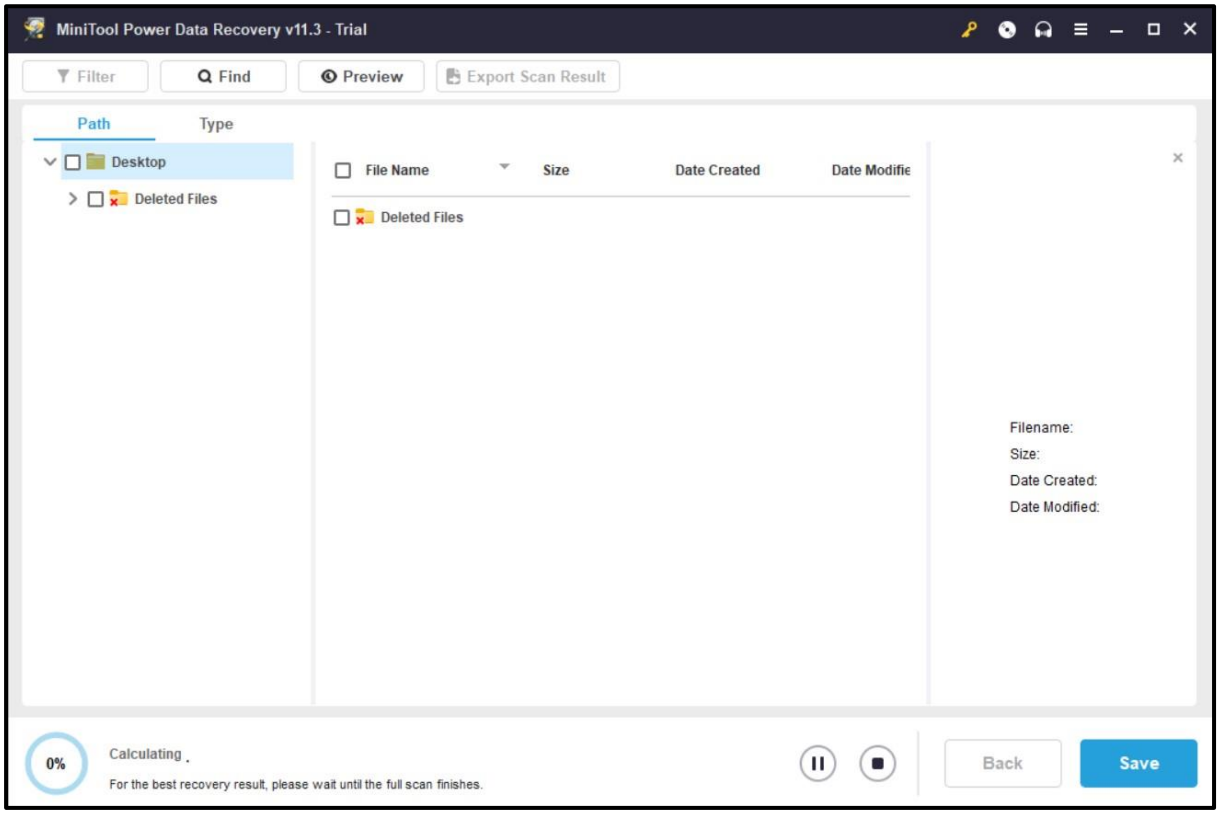


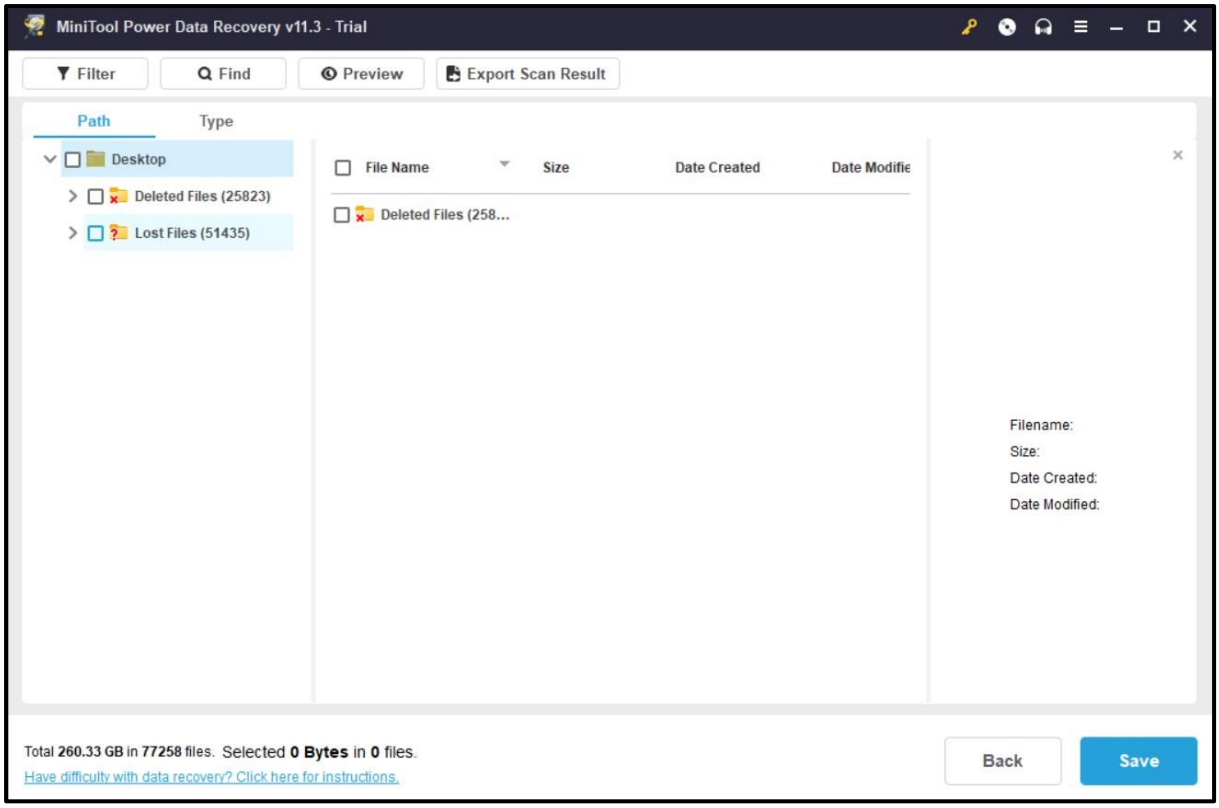
3. After completion of the installation of the tool, we can see preview of whole data file system of PC and select in which partition or folder we want to do data recovery scanning.



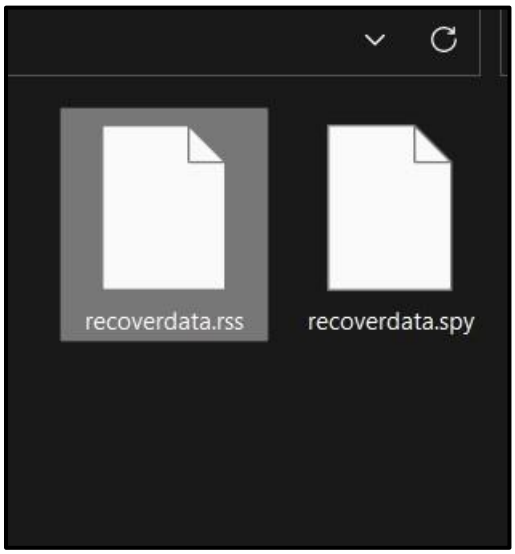
4. Choose in which folder you want to perform the scanning. It will show different previews of deleted files as well as existing files.







5. By clicking on “Save” you get your Recovered files.



Digital Forensics Lab Report: 7

Date: 14-09-2022

Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

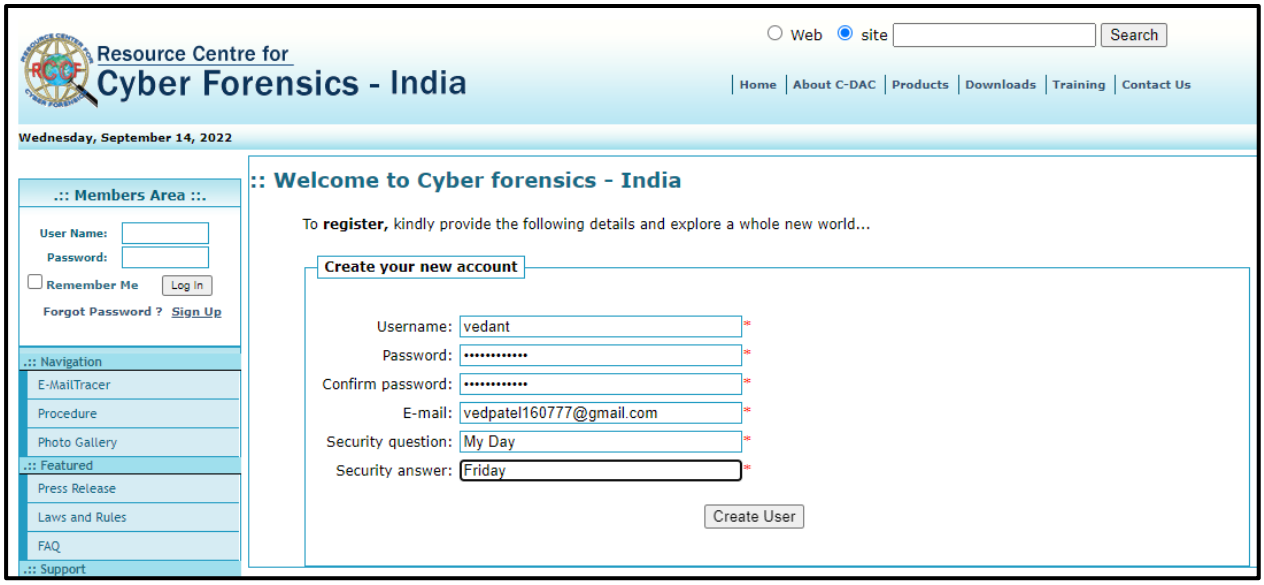
Aim/Purpose: Study of Email Forensics Tools.

Tool Names: Emailtracker Pro, politemail.com, cyberforensics.in, ipaddresslocation.org, pointofmail.com(Any 2 tools/website).

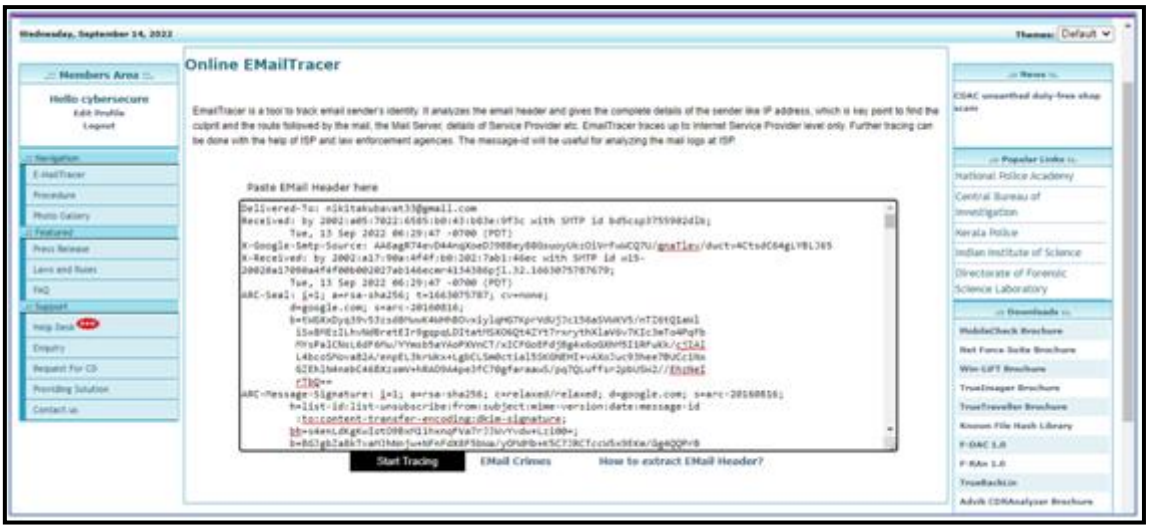
Task 1: CyberForensics.in

Steps:

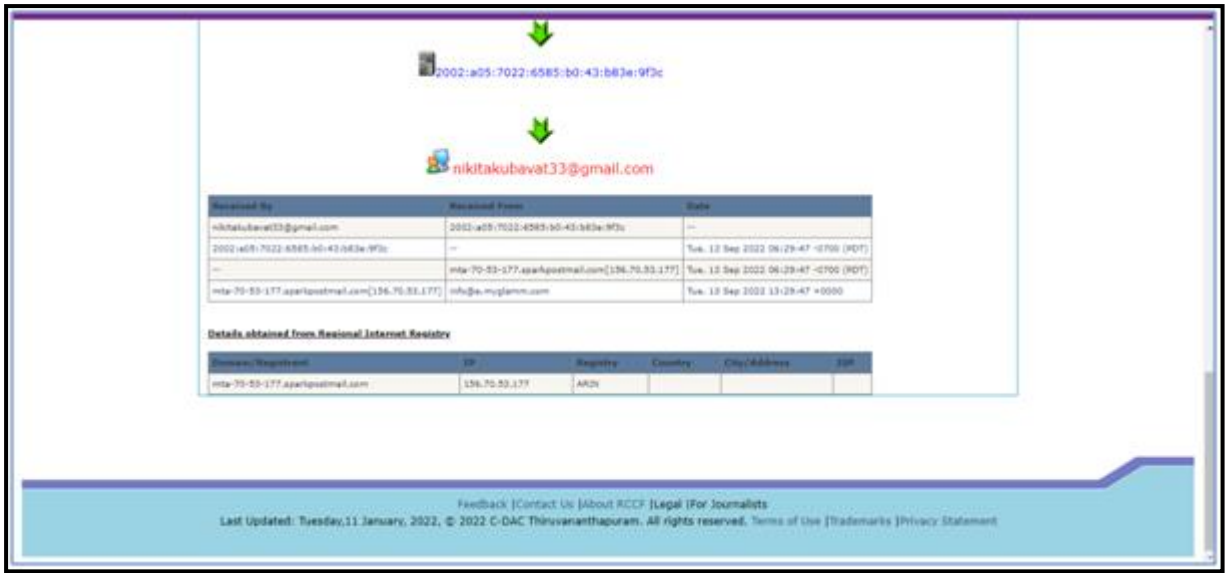
1. Open CyberForensics.in.
2. Select "Image URL" if you want to insert the image url or "Upload File" if you want to select the file from your local machine.
3. Then Click on upload url and upload image.
4. Then you get all data regarding images like ICC+, metadata, etc.




Resource Centre for
Cyber Forensics - India
Web
site
Search
Home | About C-DAC | Products | Downloads | Training | Contact Us
सी डैक
CDAC
Wednesday, September 14, 2022
Themes: Default
.:: Members Area ::.
Hello vedant1607
Edit Profile
Logout
.:: Navigation
E-MailTracer
Procedure
Photo Gallery
.:: Featured
Press Release
Laws and Rules
FAQ
.:: Support
Help Desk
Enquiry
Request For CD
Providing Solution
Contact us
Online EMailTracer
EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.
Paste EMail Header here
Start Tracing
EMail Crimes
How to extract EMail Header?
.:: News ::.
75 Azadi Ka Amrit Mahotsav-AKAM competition
Digital Evidence Handling during Covid-19
.:: Popular Links ::.
National Police Academy
Central Bureau of Investigation
Kerala Police
Indian Institute of Science
Directorate of Forensic Science Laboratory
.:: Downloads ::.
MobileCheck Brochure
Net Force Suite Brochure
Win-LiFT Brochure
TrueImager Brochure
TrueTraveller Brochure
Known File Hash Library
F-DAC 1.0
F-RAn 1.0
TrueBackLin


Wednesday, September 14, 2022
Themes: Default
.:: Members Area ::.
Hello cybersecure
Edit Profile
Logout
Online EMailTracer
EmailTracer is a tool to track email sender's identity. It analyzes the email header and gives the complete details of the sender like IP address, which is key point to find the culprit and the route followed by the mail, the Mail Server, details of Service Provider etc. EmailTracer traces up to Internet Service Provider level only. Further tracing can be done with the help of ISP and law enforcement agencies. The message-id will be useful for analyzing the mail logs at ISP.
Paste EMail Header here
Start Tracing
EMail Crimes
How to extract EMail Header?


Details extracted from Mail Header
The mail appears to be originated from the computer with IP address 156.70.53.177
The sender's email address is info@e.myglamm.com
The message-id of the the mail is
info@e.myglamm.com
mta-70-53-177.sparkpostmail.com(156.70.53.177)
2002:a05:7022:6585:b0:43:b83e:9f3c
.::More::.



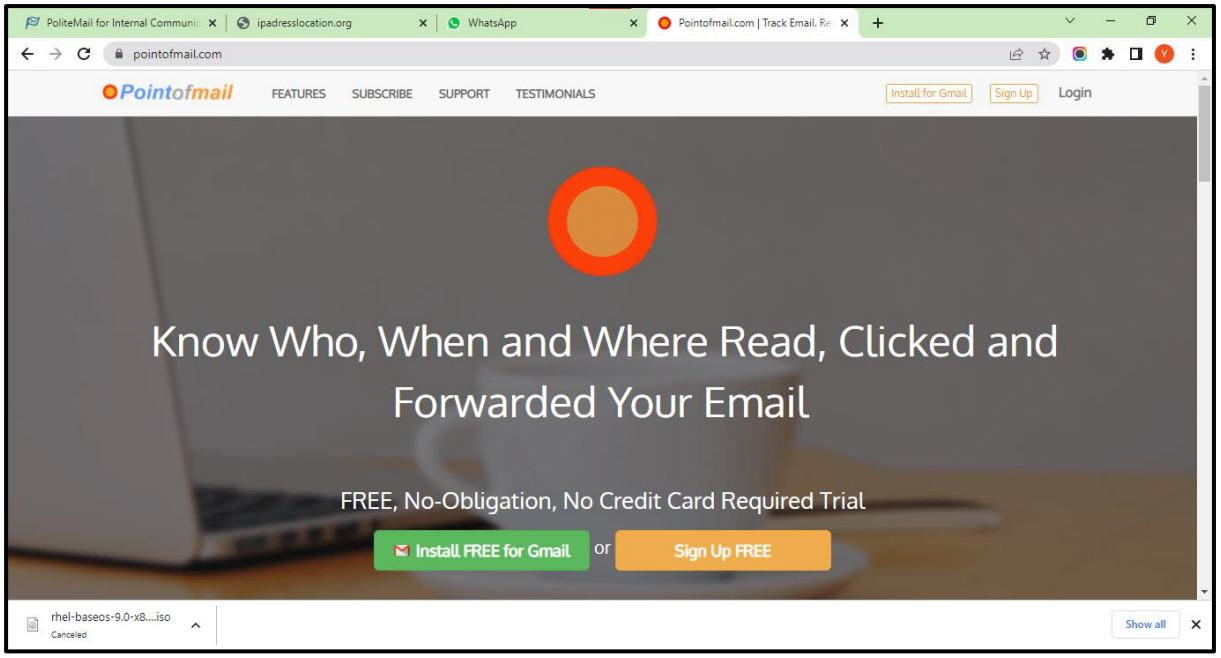
Analysis:

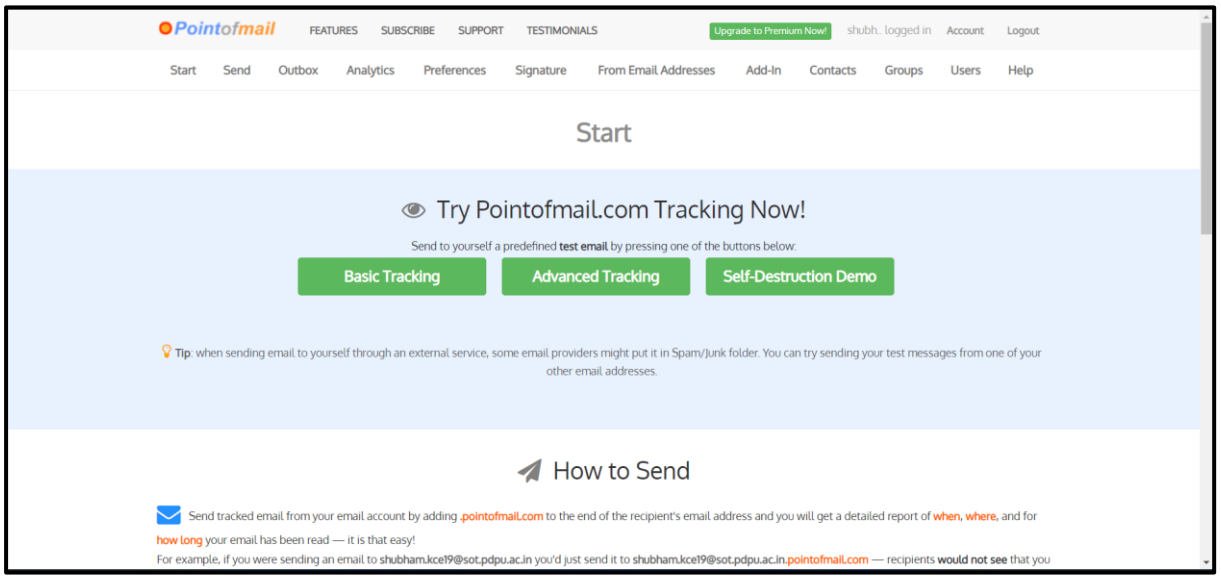
1. We can trace email easily. We can get all extracted details from email-header.

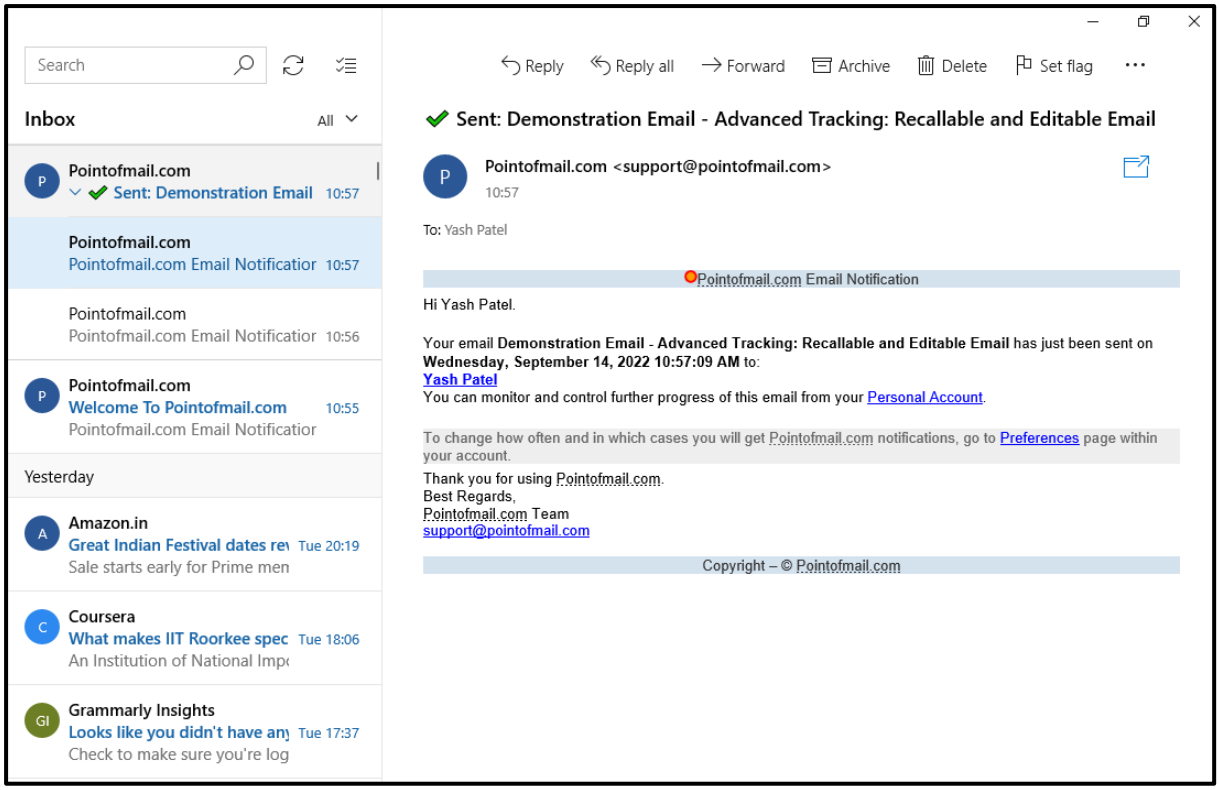
Task 2: Using Pointofmail

Steps:

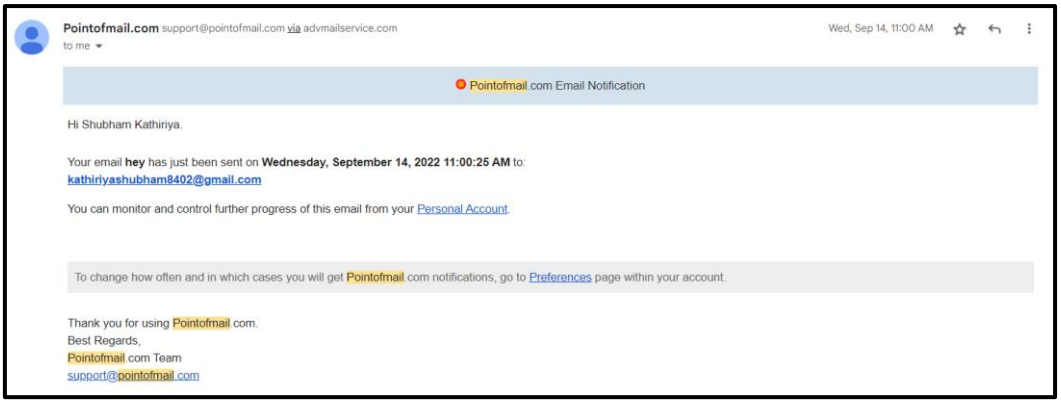
1. Go to https://www.pointofmail.com/
2. Create an account or login if you have already created account to use email tracer tool
3. After login go to pointofmail
4. It will take you to another page and ask to enter email header
5. Enter any email header of email you want to trace
6. Click on start tracing
7. It will show all the details of email such as sender email id, ip address, message id and path tracing info

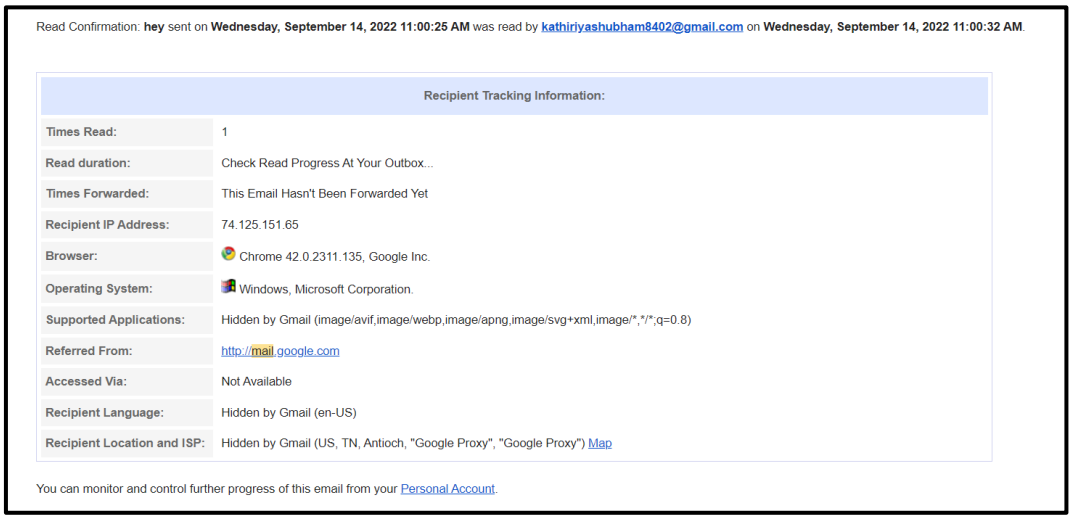

PoliteMail for Internal Communic
ipadresslocation.org
WhatsApp
Pointofmail.com | Track Email. Re
pointofmail.com
Pointofmail
FEATURES
SUBSCRIBE
SUPPORT
TESTIMONIALS
Install for Gmail
Sign Up
Login
Know Who, When and Where Read, Clicked and Forwarded Your Email
FREE, No-Obligation, No Credit Card Required Trial
Install FREE for Gmail
or
Sign Up FREE
rhel-baseos-9.0-x8....iso
Canceled
Show all

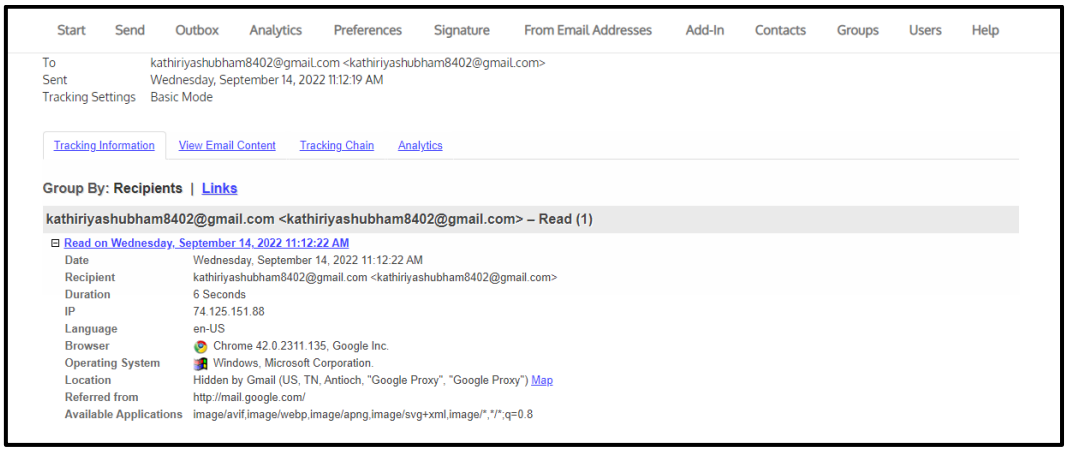

Pointofmail
FEATURES
SUBSCRIBE
SUPPORT
TESTIMONIALS
Upgrade to Premium Now!
shubh.. logged in
Account
Logout
Start
Send
Outbox
Analytics
Preferences
Signature
From Email Addresses
Add-In
Contacts
Groups
Users
Help
Start
Try Pointofmail.com Tracking Now!
Send to yourself a predefined test email by pressing one of the buttons below:
Basic Tracking
Advanced Tracking
Self-Destruction Demo
Tip: when sending email to yourself through an external service, some email providers might put it in Spam/Junk folder. You can try sending your test messages from one of your other email addresses.
How to Send
Send tracked email from your email account by adding .pointofmail.com to the end of the recipient's email address and you will get a detailed report of when, where, and for how long your email has been read — it is that easy!
For example, if you were sending an email to shubham.kce19@sot.pdpu.ac.in you'd just send it to shubham.kce19@sot.pdpu.ac.in.pointofmail.com — recipients would not see that you


Search
Inbox
All
Pointofmail.com
Sent: Demonstration Email 10:57
Pointofmail.com
Pointofmail.com Email Notificatior 10:57
Pointofmail.com
Pointofmail.com Email Notificatior 10:56
Pointofmail.com
Welcome To Pointofmail.com 10:55
Pointofmail.com Email Notificatior
Yesterday
Amazon.in
Great Indian Festival dates re\ Tue 20:19
Sale starts early for Prime men
Coursera
What makes IIT Roorkee spec Tue 18:06
An Institution of National Impc
Grammarly Insights
Looks like you didn't have an\ Tue 17:37
Check to make sure you're log
Reply
Reply all
Forward
Archive
Delete
Set flag
Sent: Demonstration Email - Advanced Tracking: Recallable and Editable Email
Pointofmail.com <support@pointofmail.com>
10:57
To: Yash Patel
Pointofmail.com Email Notification
Hi Yash Patel.
Your email Demonstration Email - Advanced Tracking: Recallable and Editable Email has just been sent on Wednesday, September 14, 2022 10:57:09 AM to:
Yash Patel
You can monitor and control further progress of this email from your Personal Account.
To change how often and in which cases you will get Pointofmail.com notifications, go to Preferences page within your account.
Thank you for using Pointofmail.com.
Best Regards,
Pointofmail.com Team
support@pointofmail.com
Copyright – © Pointofmail.com


To: kathiriyashubham8402@gmail.com.pointofmail.com;
Cc & Bcc
Subject
Study of email forensic tools:
emailtracker pro
politemail.com
cyberforensics.in
ipadresslocation.org
pointofmail.com
Sent from Mail for Windows
3







Analysis:

By using this tool, we can trace email. We can also find the location of Ip address and Ip related information.

Digital Forensics Lab Report: 8

Date: 12-10-2022

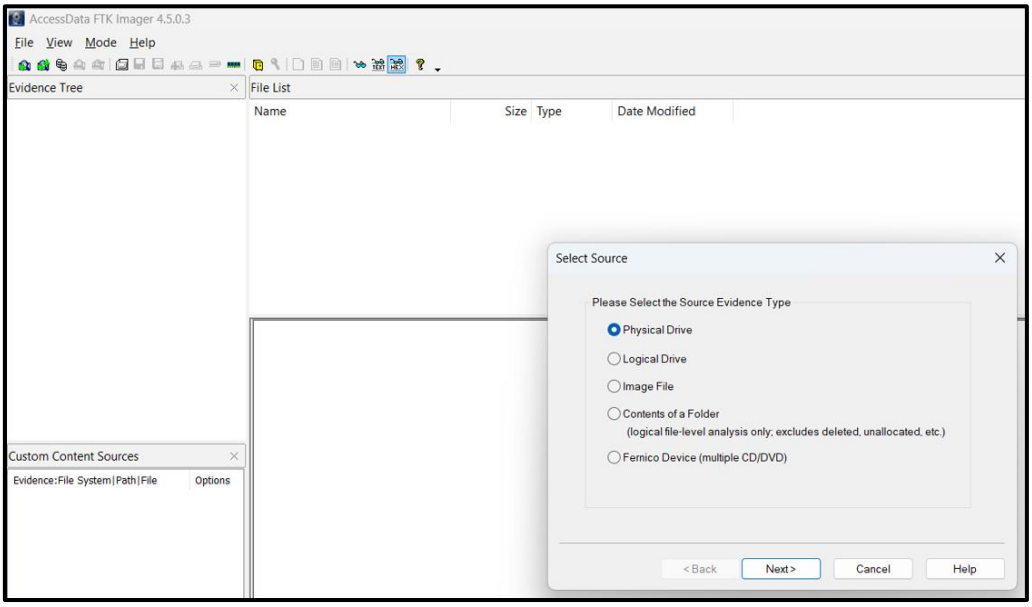
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: To create a disk image of a pen drive and studying it using Autopsy

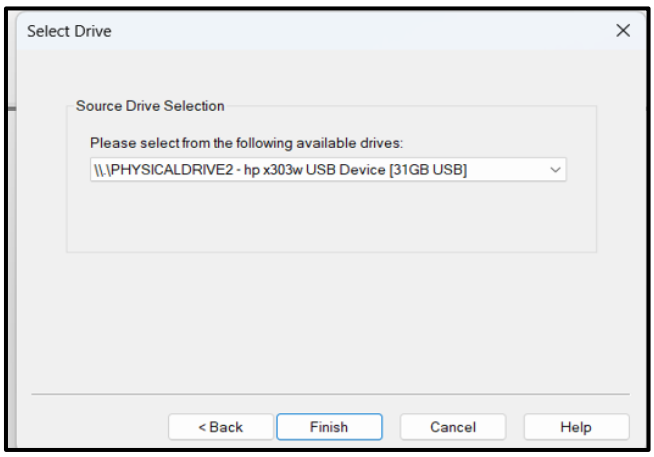
Task 1: FTK Imager

Step 1: Open Access Data FTK Imager and create a disk image of the pen drive.

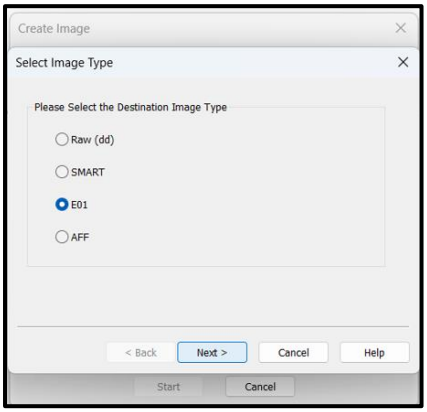
- Select Physical Drive



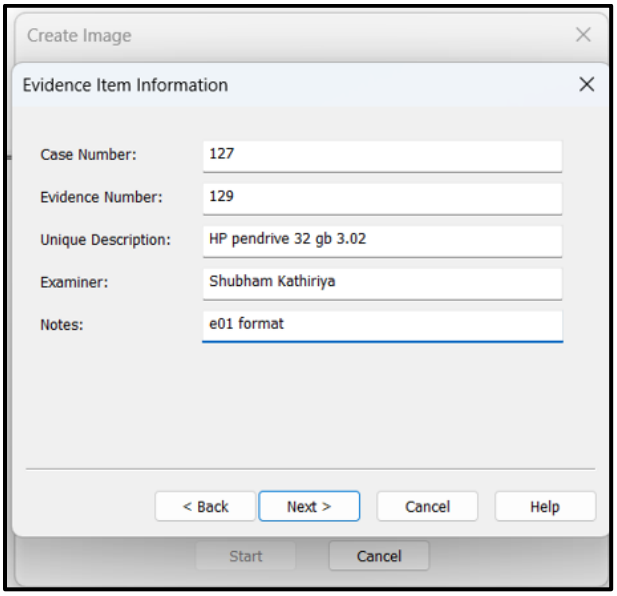
- Select Pen drive



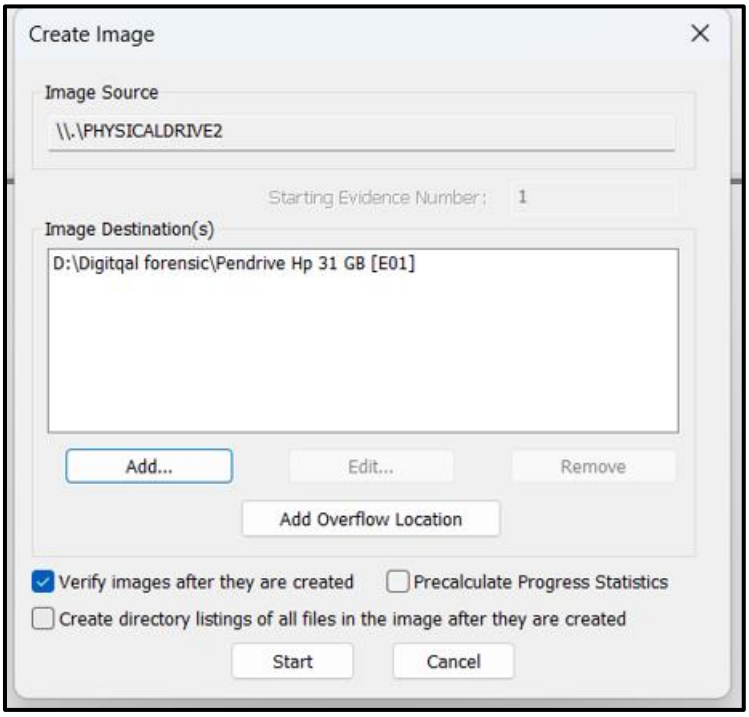
- Select the file format



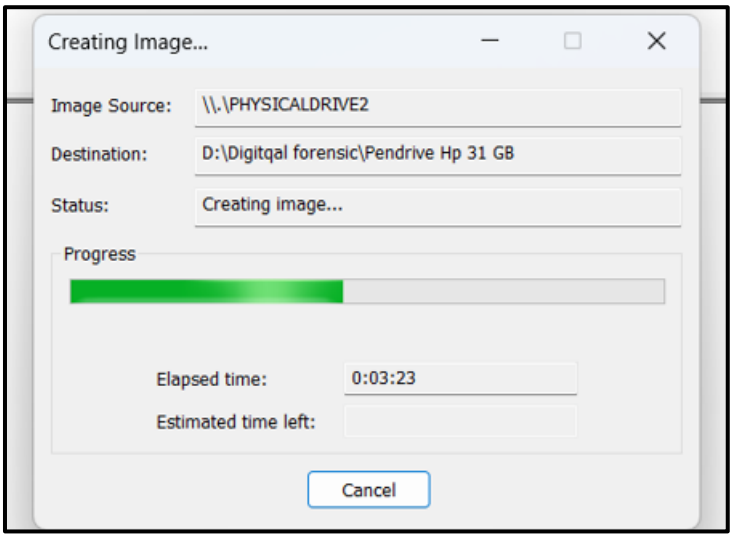
- Fill the following details



- Write the destination where you want to store and Click on the add

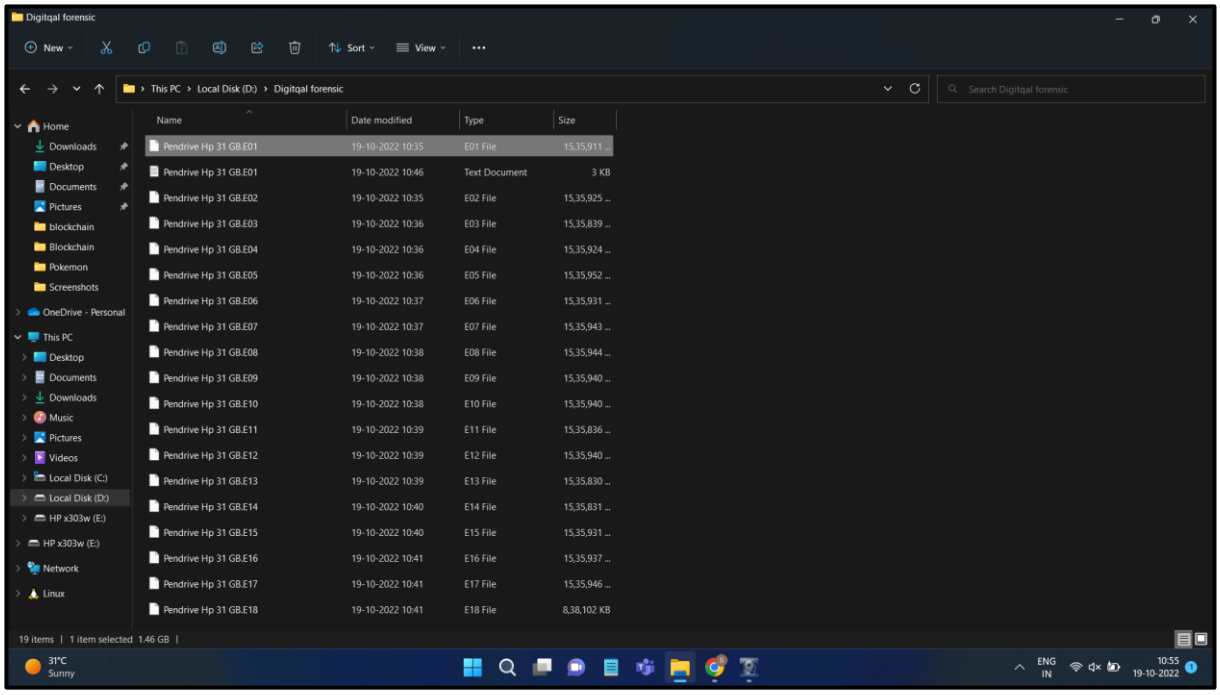


- Click on start button and then process will take place



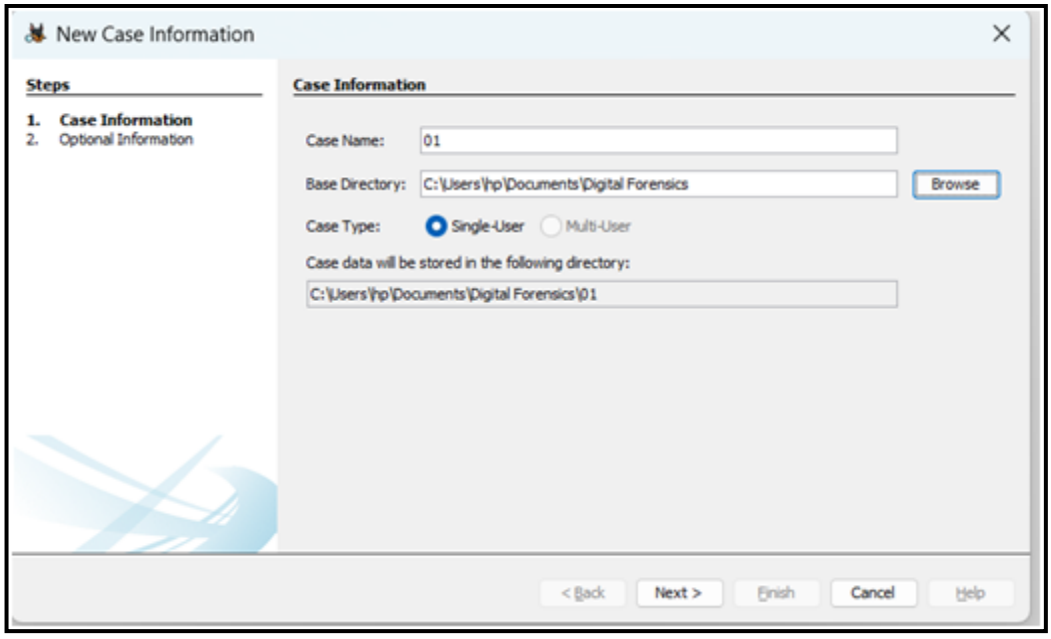
- Now after some time file has been created at your selected destination.

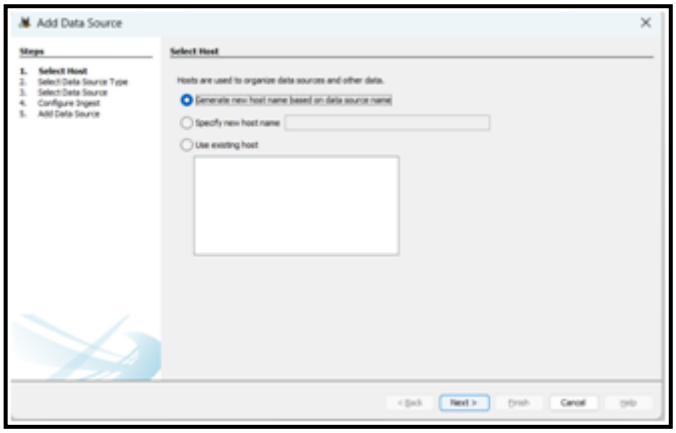
- Created file

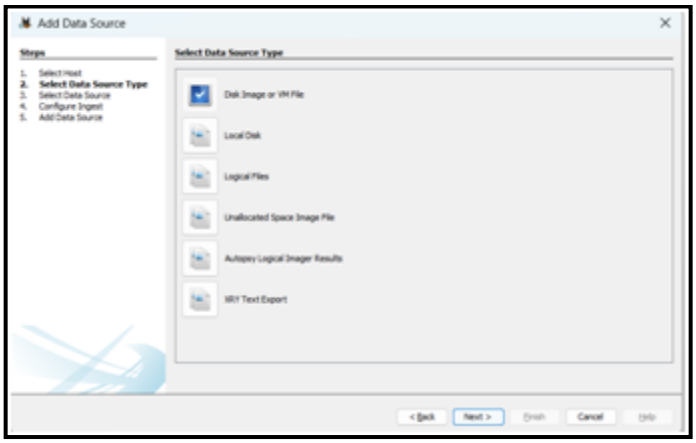


Step 2: Once the Disk image is created, open that disk imagefile in the Autopsy software.

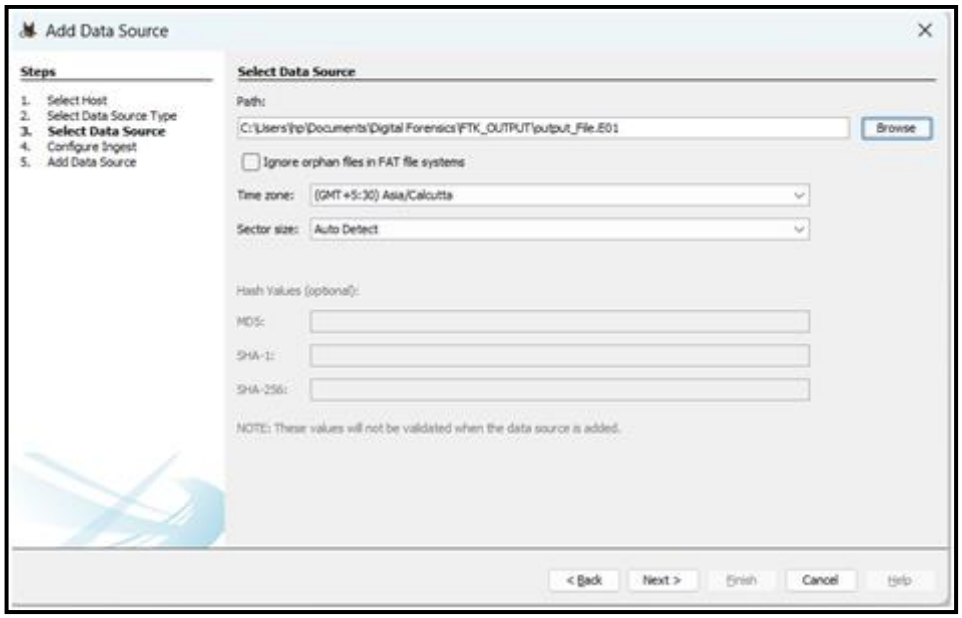
Select the following options.



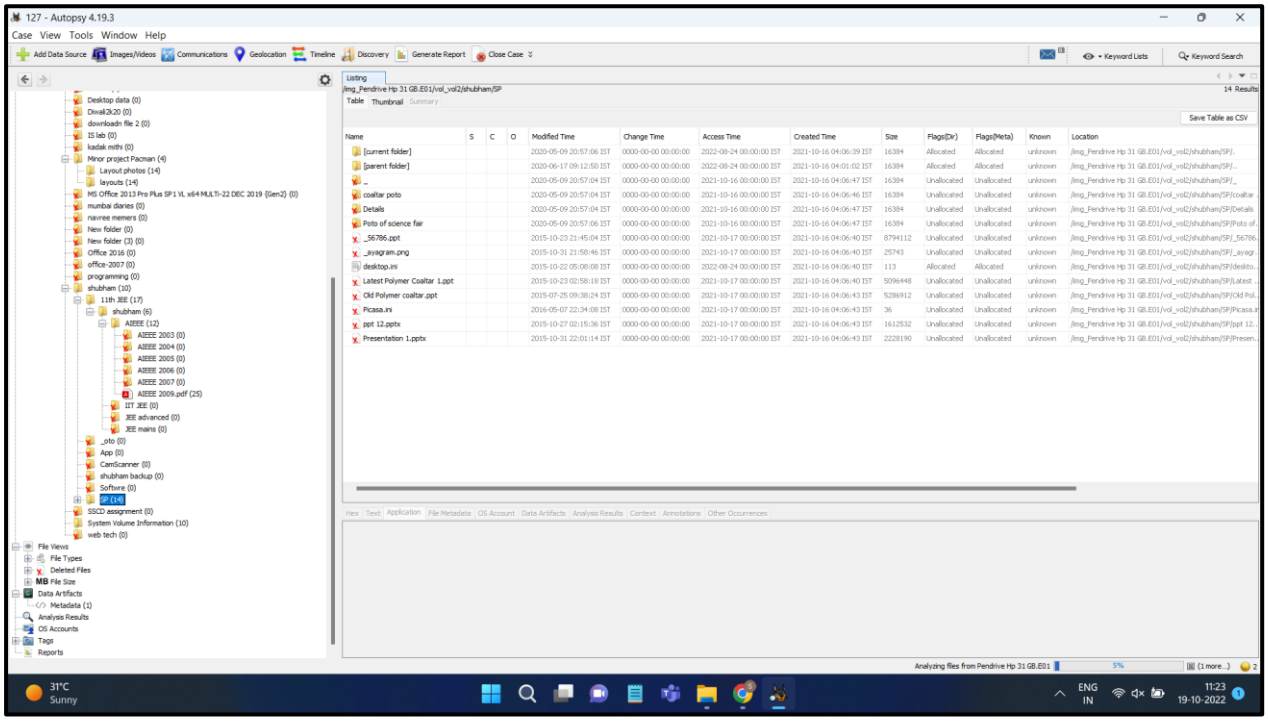




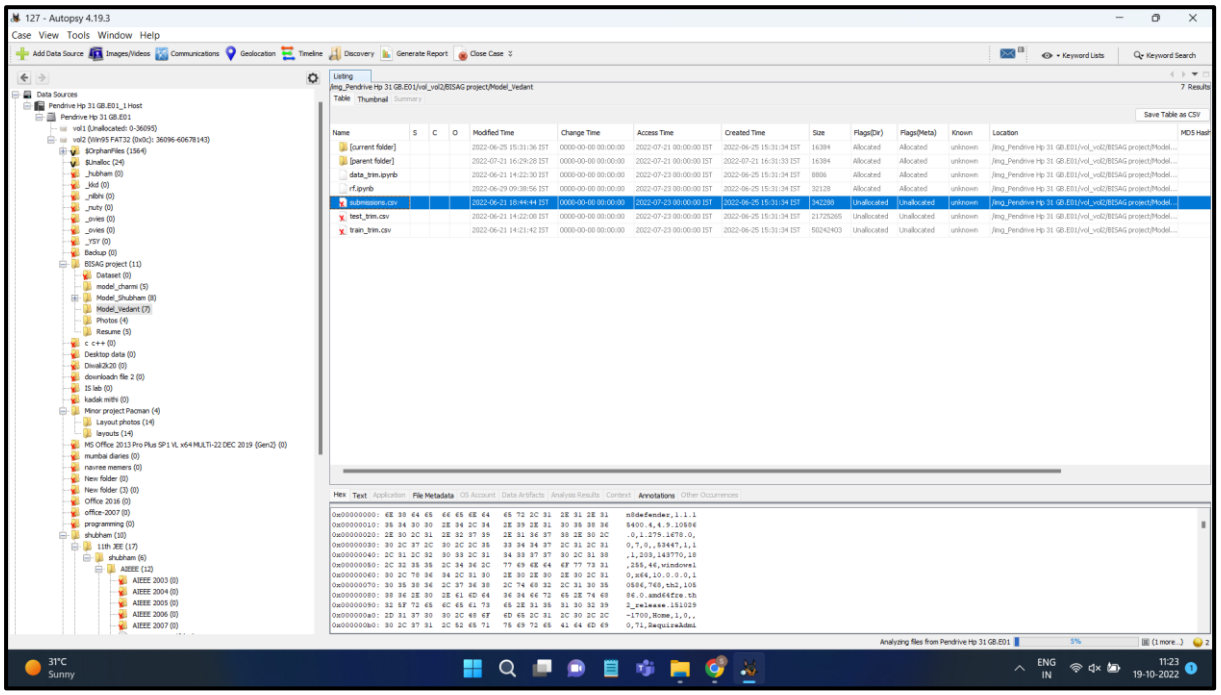
Select the FTK file that you have created priviously



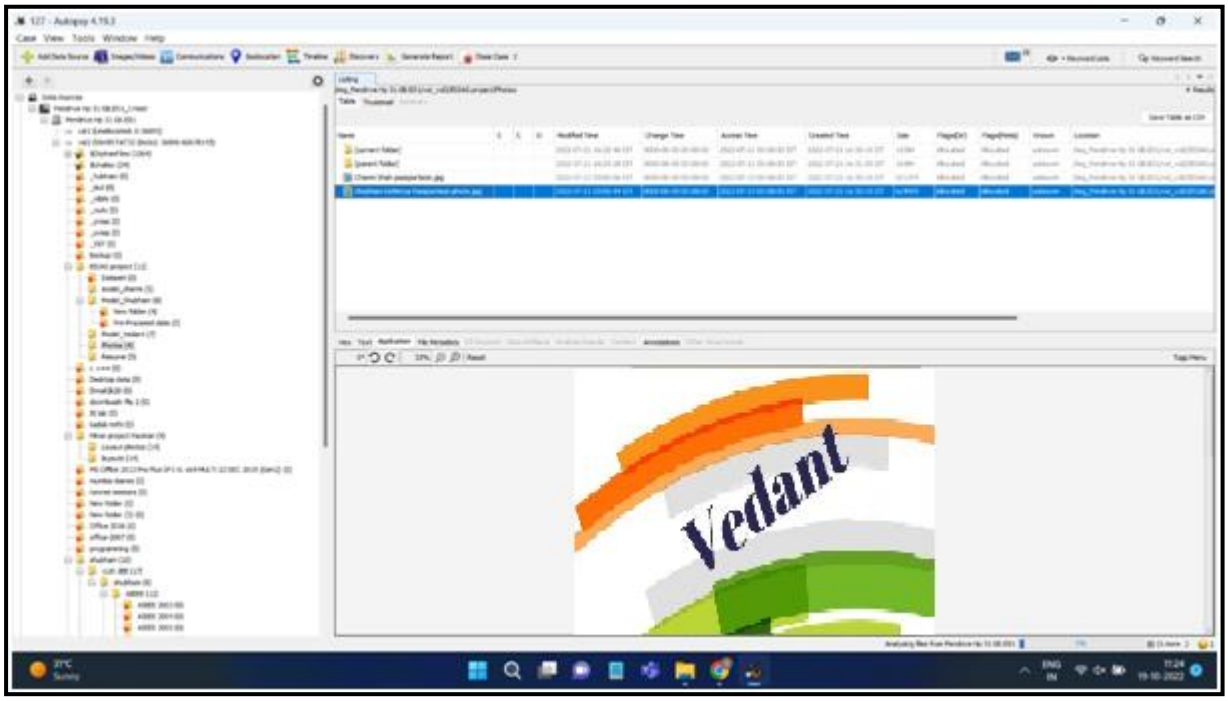
Click on “Next” button and then you can found the following details

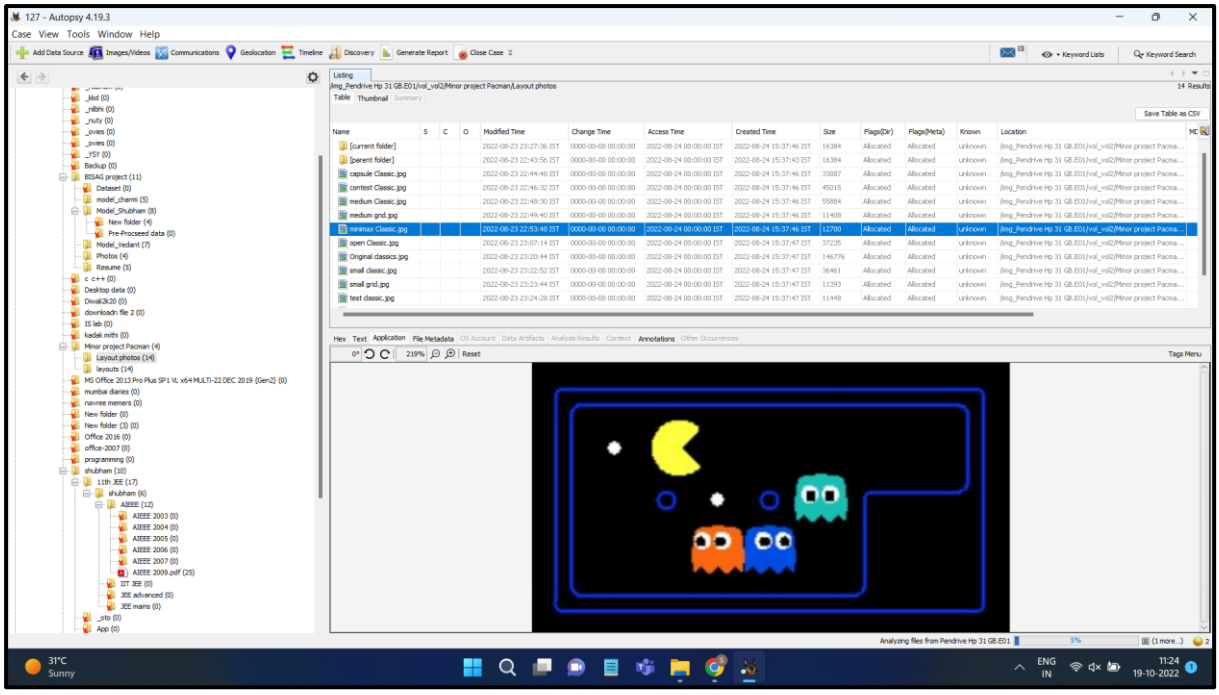


You can see the files as per below

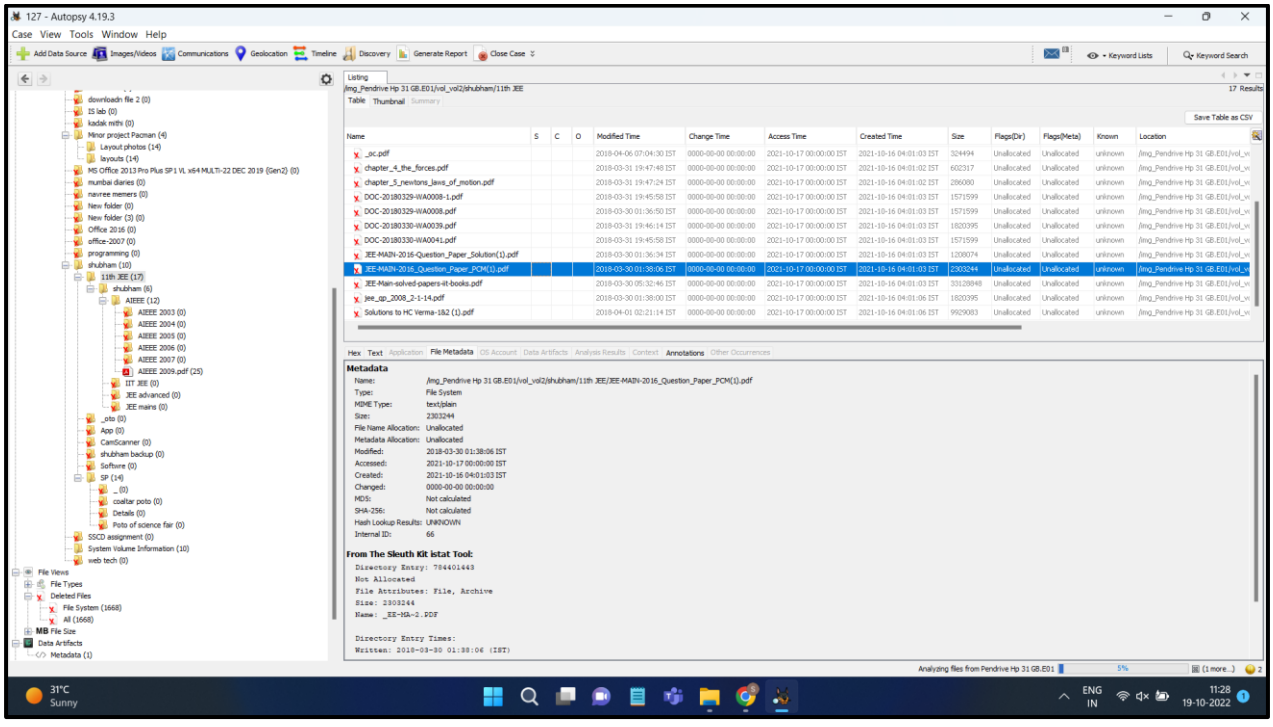


You can find the photos.

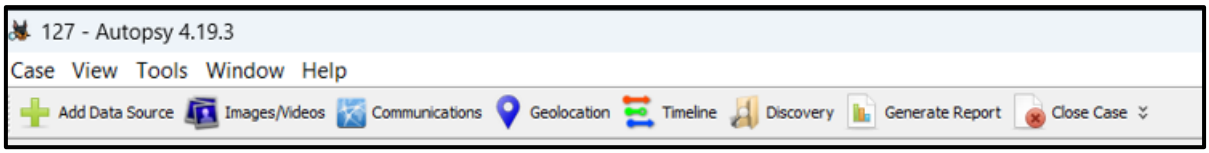




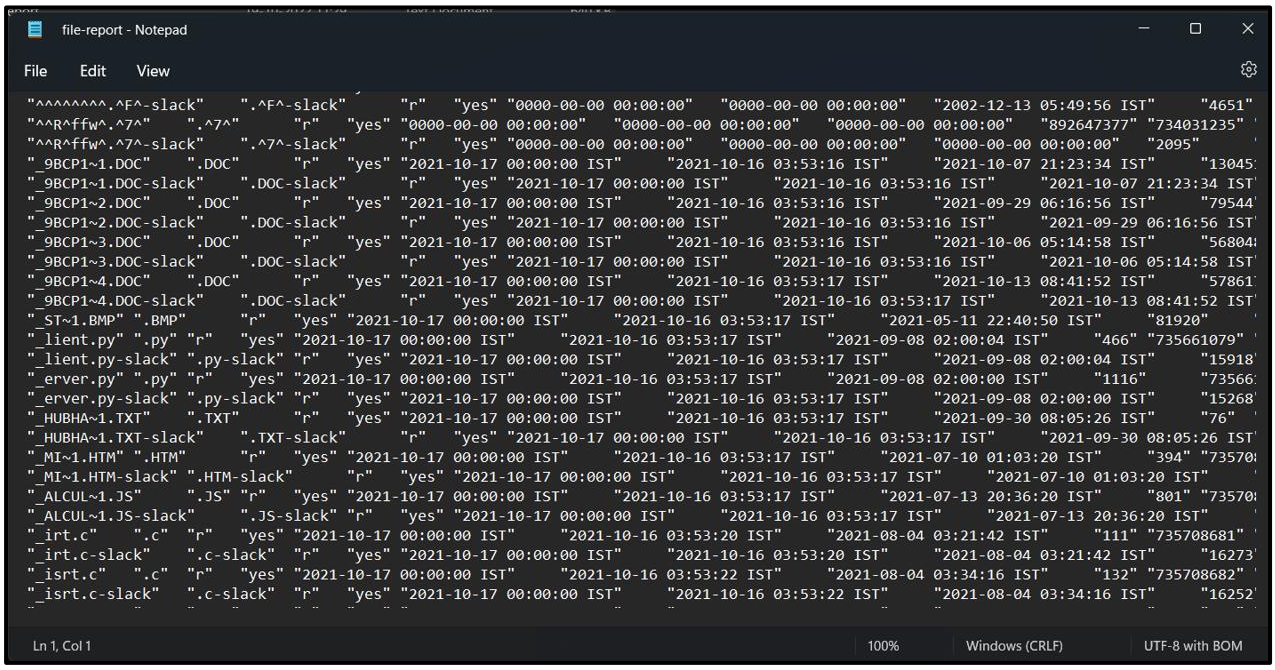
You can also see the metadata of the files



You can create the final report as given option click on the “generate report”



You can see the .txt file



Digital Forensics Lab Report: 9

Date: 26-10-2022

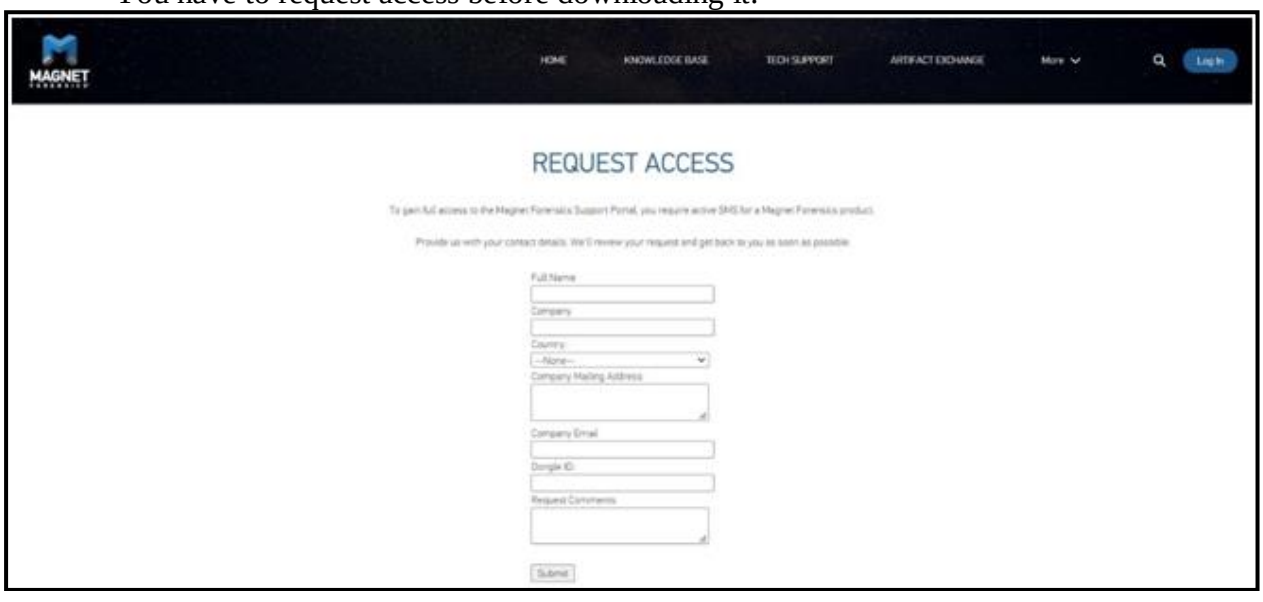
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of Volatile Forensics Tool.

Tool Names: Magnet RAM Capture, Balkasoft RAM Capture, WinHex

Step 1: Download Magnet RAM Capture

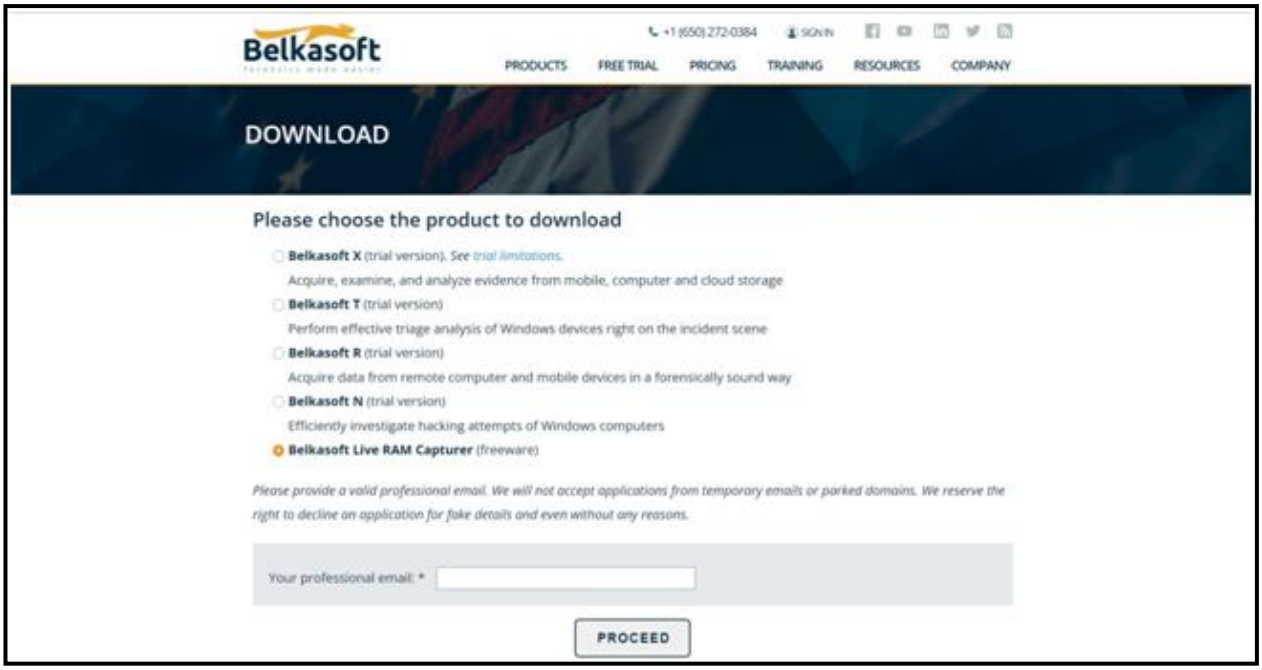
- Visit https://support.magnetforensics.com/s/article/Acquire-Memory-with-MAGNET-RAM-Capture and click on Software and Download
- You will have to download Magnet RAM Capture from the list of Software available inhttps://support.magnetforensics.com/s/software-and-downloads?productTag=free-tools
- You have to request access before downloading it.



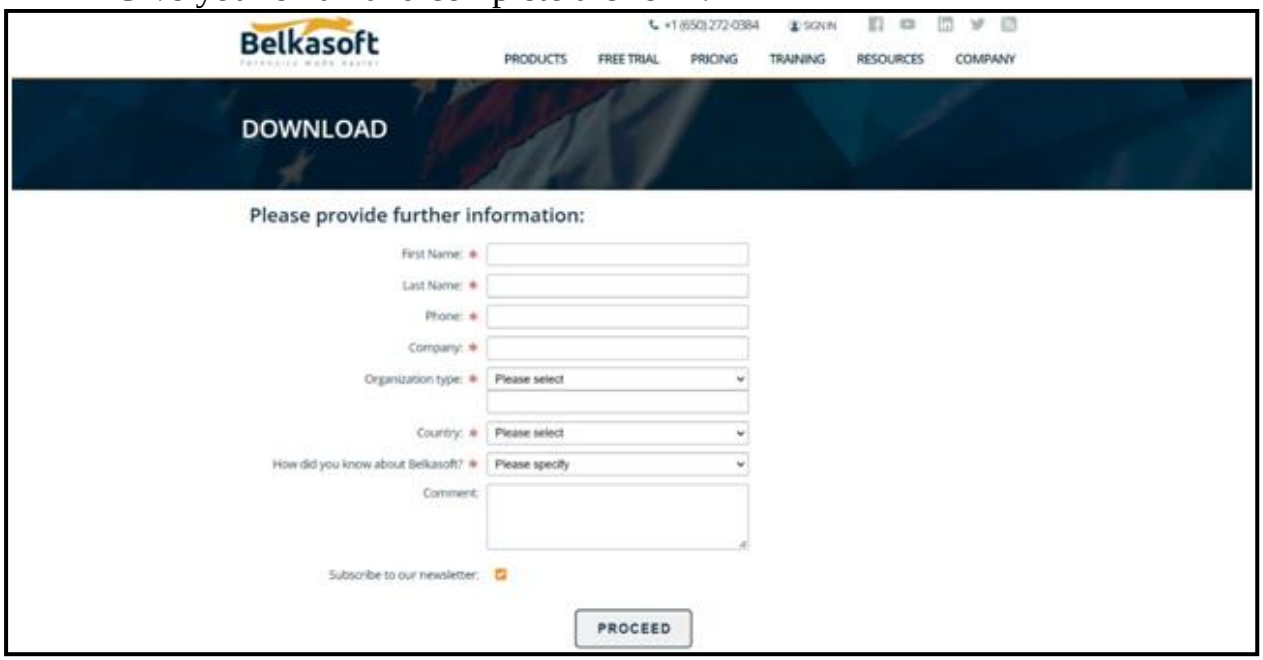
- You will get a link to download the file.

Step 2: Download BelkasoftSoftware

- Visit https://belkasoft.com/get



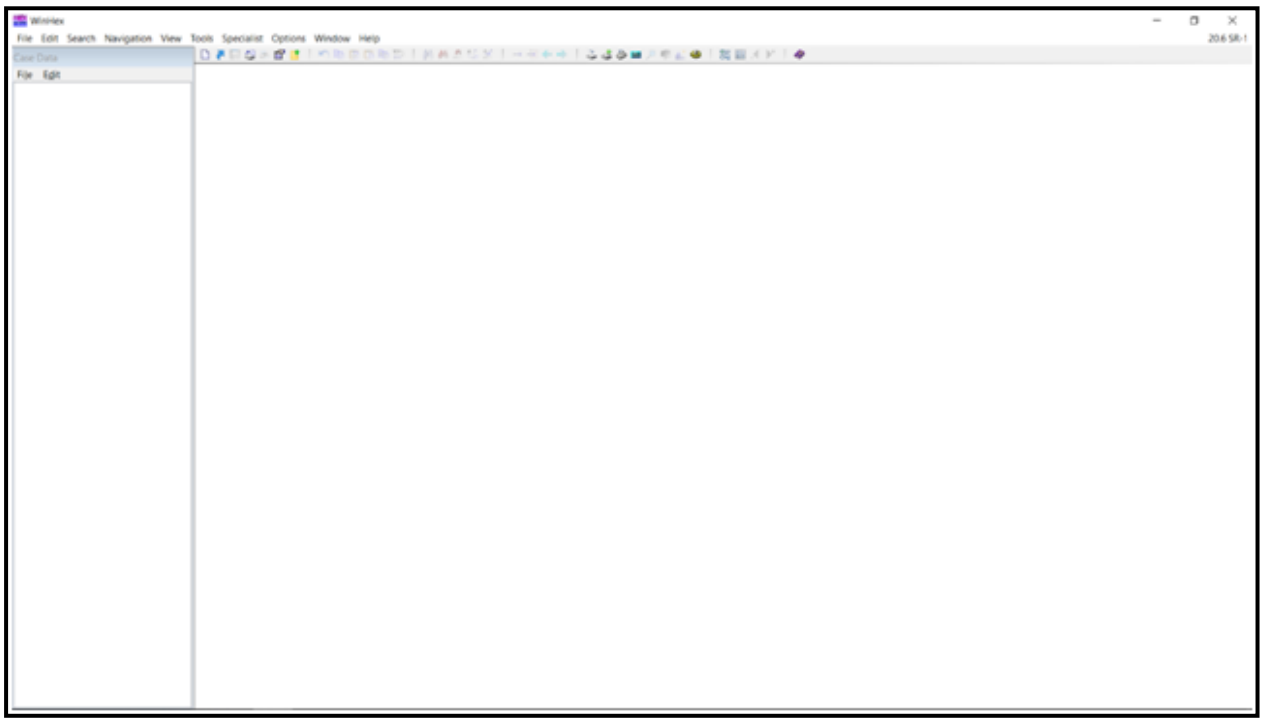
- Give your email and complete the form.



Step 3: Download and Install WinHEX

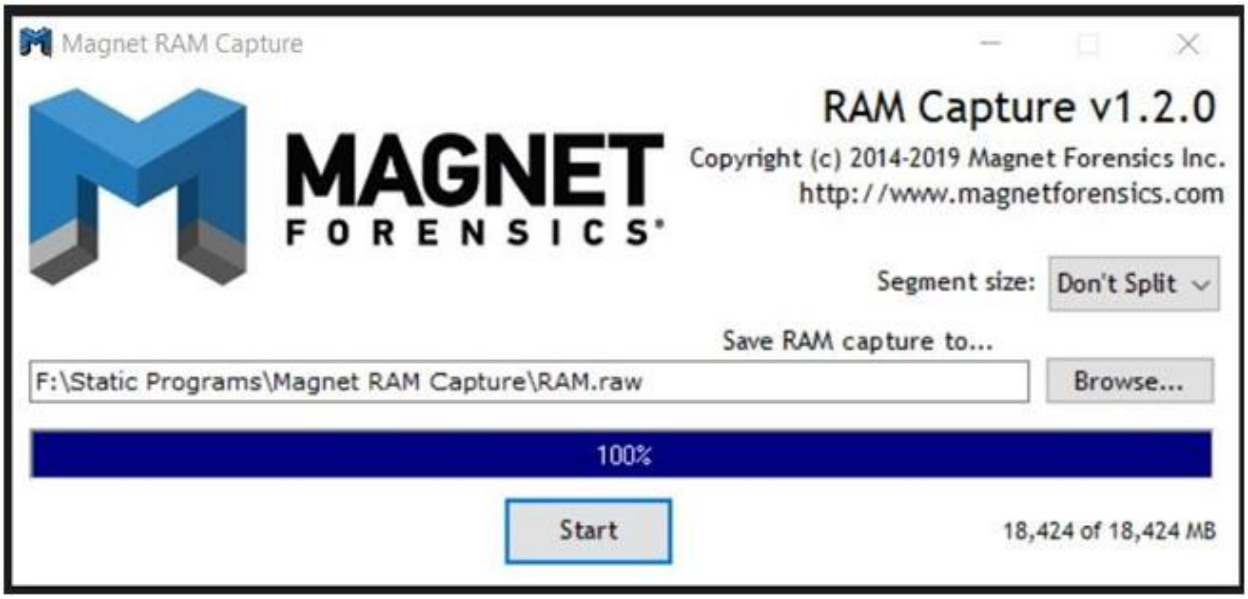
- Visit http://www.winhex.com/winhex/hex-editor.html and download and install.

- Open the application

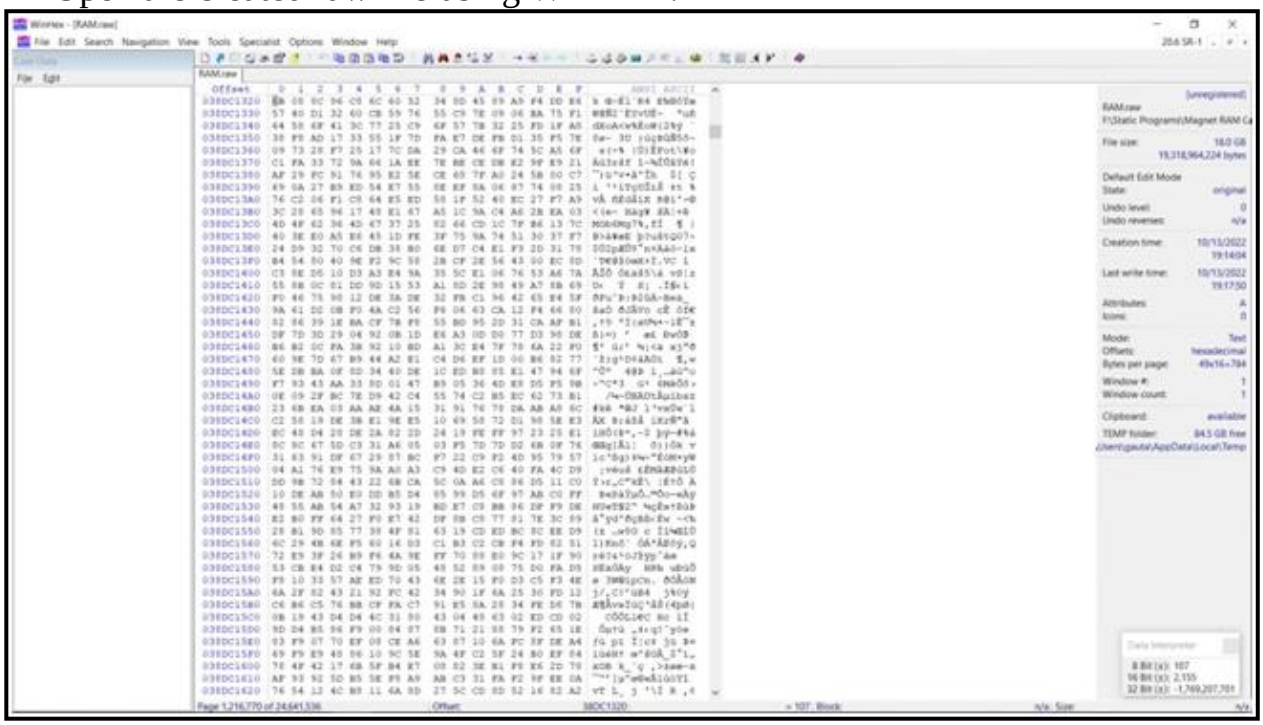


Step 4: Make Image File and Open in WinHEX

- Open Magnet RAM Capture, choose a directory and file name and click on start.
- Once completed, a raw file will be created.

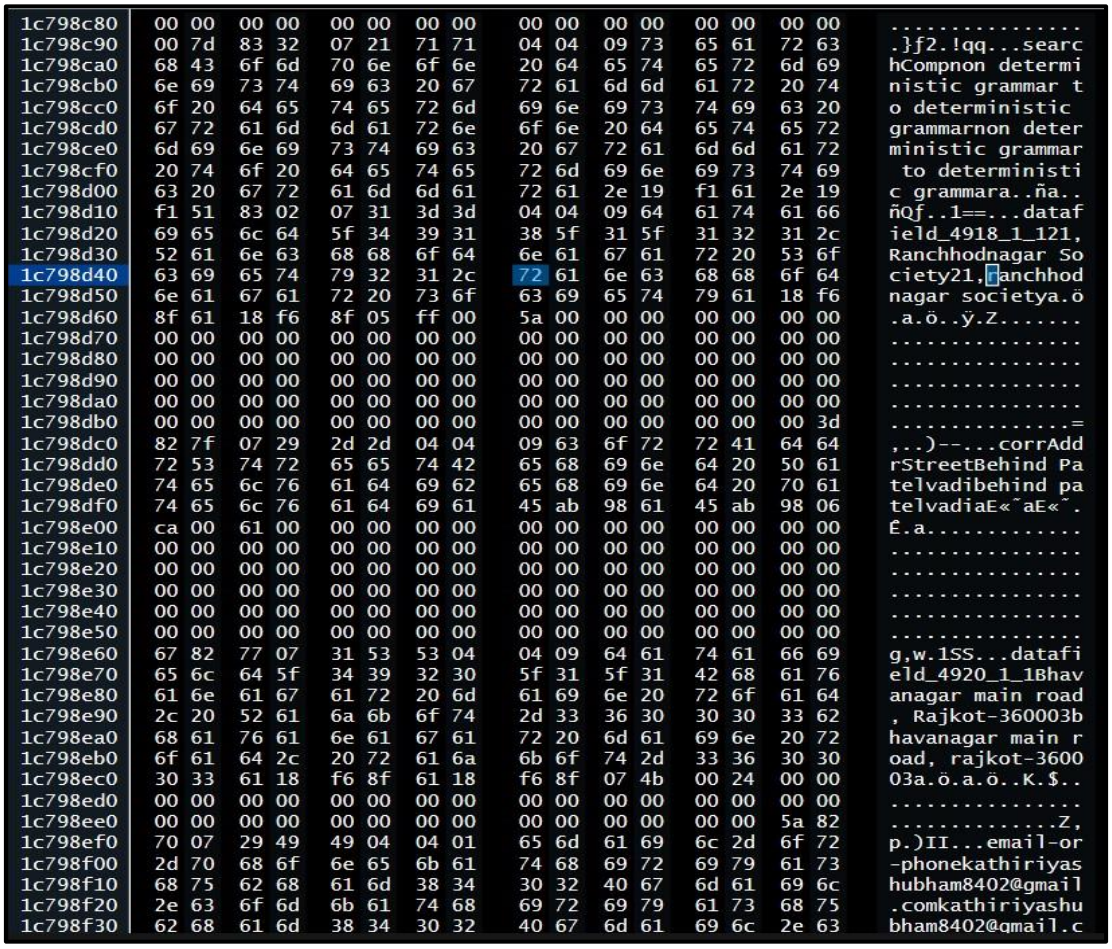


- Open the created raw file using WinHEX.



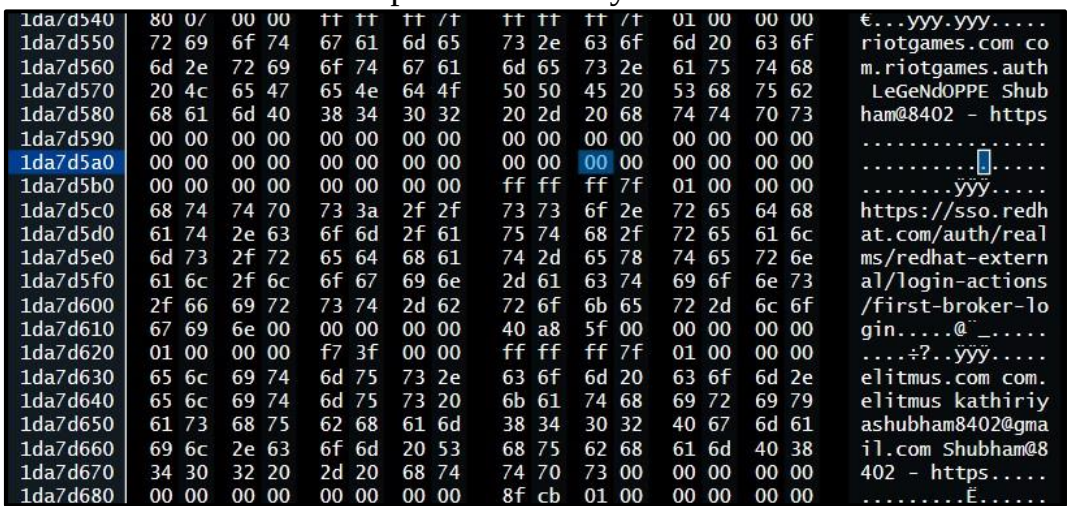
Findings:

1. Found the my address in website



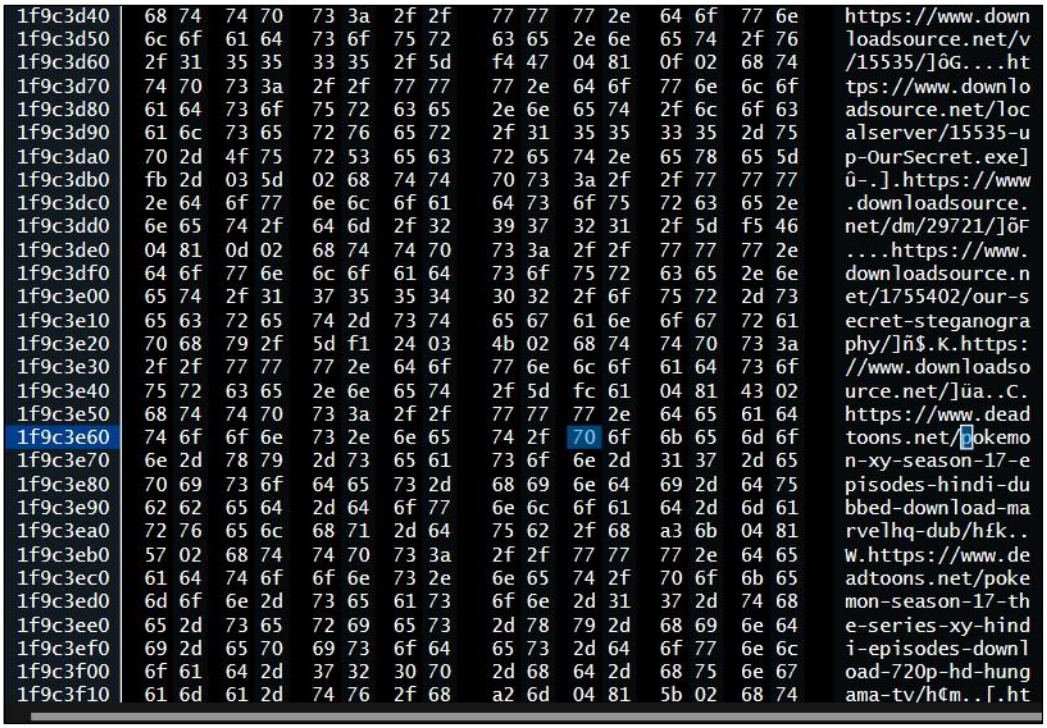
```
1c798c80  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798c90  00 7d  83 32  07 21  71 71  04 04  09 73  65 61  72 63  .}ƒ2.!qq...searc
1c798ca0  68 43  6f 6d  70 6e  6f 6e  20 64  65 74  65 72  6d 69  hCompnon determi
1c798cb0  6e 69  73 74  69 63  20 67  72 61  6d 6d  61 72  20 74  nistic grammar t
1c798cc0  6f 20  64 65  74 65  72 6d  69 6e  69 73  74 69  63 20  o deterministic
1c798cd0  67 72  61 6d  6d 61  72 6e  6f 6e  20 64  65 74  65 72  grammarnon deter
1c798ce0  6d 69  6e 69  73 74  69 63  20 67  72 61  6d 6d  61 72  ministic grammar
1c798cf0  20 74  6f 20  64 65  74 65  72 6d  69 6e  69 73  74 69   to deterministi
1c798d00  63 20  67 72  61 6d  6d 61  72 61  2e 19  f1 61  2e 19  c grammara..ña..
1c798d10  f1 51  83 02  07 31  3d 3d  04 04  09 64  61 74  61 66  ñQƒ..1==...dataf
1c798d20  69 65  6c 64  5f 34  39 31  38 5f  31 5f  31 32  31 2c  ield_4918_1_121,
1c798d30  52 61  6e 63  68 68  6f 64  6e 61  67 61  72 20  53 6f  Ranchhodnagar So
1c798d40  63 69  65 74  79 32  31 2c  72 61  6e 63  68 68  6f 64  ciety21,ranchhod
1c798d50  6e 61  67 61  72 20  73 6f  63 69  65 74  79 61  18 f6  nagar societya.ö
1c798d60  8f 61  18 f6  8f 05  ff 00  5a 00  00 00  00 00  00 00  .a.ö..ÿ.Z.......
1c798d70  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798d80  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798d90  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798da0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798db0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 3d  ...............=
1c798dc0  82 7f  07 29  2d 2d  04 04  09 63  6f 72  72 41  64 64  ,..)--...corrAdd
1c798dd0  72 53  74 72  65 65  74 42  65 68  69 6e  64 20  50 61  rStreetBehind Pa
1c798de0  74 65  6c 76  61 64  69 62  65 68  69 6e  64 20  70 61  telvadibehind pa
1c798df0  74 65  6c 76  61 64  69 61  45 ab  98 61  45 ab  98 06  telvadiaE«˜aE«˜.
1c798e00  ca 00  61 00  00 00  00 00  00 00  00 00  00 00  00 00  Ê.a.............
1c798e10  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798e20  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798e30  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798e40  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798e50  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798e60  67 82  77 07  31 53  53 04  04 09  64 61  74 61  66 69  g‚w.1SS...datafi
1c798e70  65 6c  64 5f  34 39  32 30  5f 31  5f 31  42 68  61 76  eld_4920_1_1Bhav
1c798e80  61 6e  61 67  61 72  20 6d  61 69  6e 20  72 6f  61 64  anagar main road
1c798e90  2c 20  52 61  6a 6b  6f 74  2d 33  36 30  30 30  33 62  , Rajkot-360003b
1c798ea0  68 61  76 61  6e 61  67 61  72 20  6d 61  69 6e  20 72  havanagar main r
1c798eb0  6f 61  64 2c  20 72  61 6a  6b 6f  74 2d  33 36  30 30  oad, rajkot-3600
1c798ec0  30 33  61 18  f6 8f  61 18  f6 8f  07 4b  00 24  00 00  03a.ö.a.ö..K.$..
1c798ed0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1c798ee0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  5a 82  ..............Z‚
1c798ef0  70 07  29 49  49 04  04 01  65 6d  61 69  6c 2d  6f 72  p.)II...email-or
1c798f00  2d 70  68 6f  6e 65  6b 61  74 68  69 72  69 79  61 73  -phonekathiriyas
1c798f10  68 75  62 68  61 6d  38 34  30 32  40 67  6d 61  69 6c  hubham8402@gmail
1c798f20  2e 63  6f 6d  6b 61  74 68  69 72  69 79  61 73  68 75  .comkathiriyashu
1c798f30  62 68  61 6d  38 34  30 32  40 67  6d 61  69 6c  2e 63  bham8402@gmail.c
```

2. I found the userID and password of my riot account for Valorant



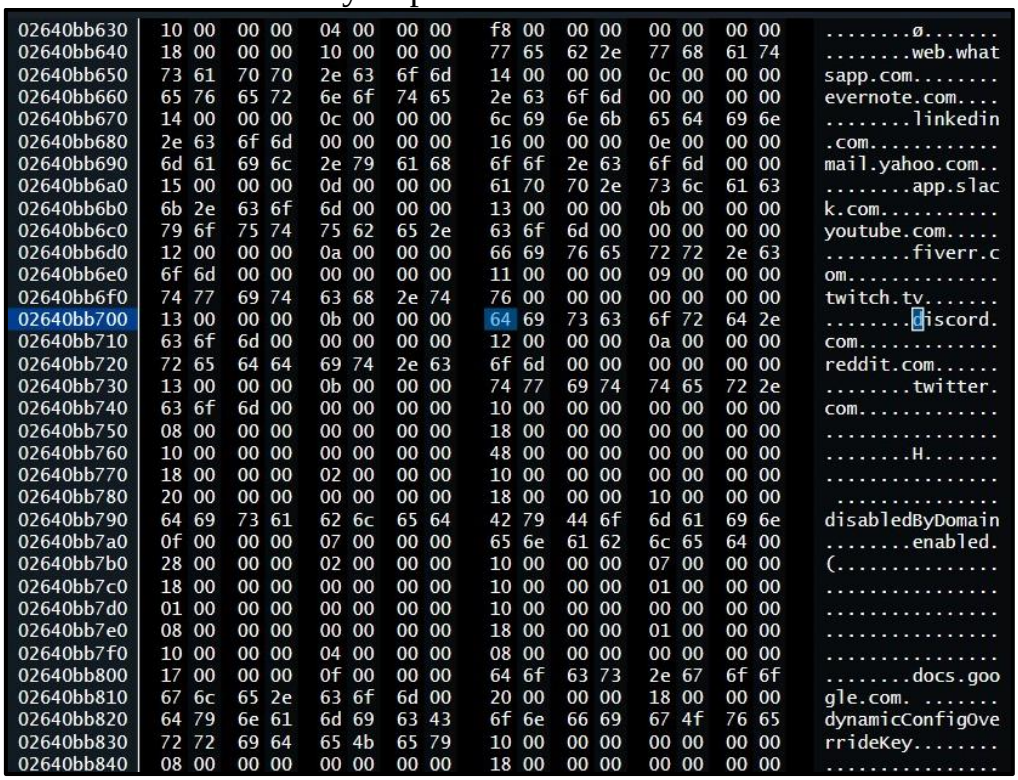
```
1da7d540  80 07  00 00  ff ff  ff 7f  ff ff  ff 7f  01 00  00 00  €...yyy.yyy.....
1da7d550  72 69  6f 74  67 61  6d 65  73 2e  63 6f  6d 20  63 6f  riotgames.com co
1da7d560  6d 2e  72 69  6f 74  67 61  6d 65  73 2e  61 75  74 68  m.riotgames.auth
1da7d570  20 4c  65 47  65 4e  64 4f  50 50  45 20  53 68  75 62   LeGeNdOPPE Shub
1da7d580  68 61  6d 40  38 34  30 32  20 2d  20 68  74 74  70 73  ham@8402 - https
1da7d590  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ................
1da7d5a0  00 00  00 00  00 00  00 00  00 00  00 00  00 00  00 00  ..........[.....
1da7d5b0  00 00  00 00  00 00  00 00  ff ff  ff 7f  01 00  00 00  ........ÿÿÿ.....
1da7d5c0  68 74  74 70  73 3a  2f 2f  73 73  6f 2e  72 65  64 68  https://sso.redh
1da7d5d0  61 74  2e 63  6f 6d  2f 61  75 74  68 2f  72 65  61 6c  at.com/auth/real
1da7d5e0  6d 73  2f 72  65 64  68 61  74 2d  65 78  74 65  72 6e  ms/redhat-extern
1da7d5f0  61 6c  2f 6c  6f 67  69 6e  2d 61  63 74  69 6f  6e 73  al/login-actions
1da7d600  2f 66  69 72  73 74  2d 62  72 6f  6b 65  72 2d  6c 6f  /first-broker-lo
1da7d610  67 69  6e 00  00 00  00 00  40 a8  5f 00  00 00  00 00  gin.....@¨_.....
1da7d620  01 00  00 00  f7 3f  00 00  ff ff  ff 7f  01 00  00 00  ....÷?..ÿÿÿ.....
1da7d630  65 6c  69 74  6d 75  73 2e  63 6f  6d 20  63 6f  6d 2e  elitmus.com com.
1da7d640  65 6c  69 74  6d 75  73 20  6b 61  74 68  69 72  69 79  elitmus kathiriy
1da7d650  61 73  68 75  62 68  61 6d  38 34  30 32  40 67  6d 61  ashubham8402@gma
1da7d660  69 6c  2e 63  6f 6d  20 53  68 75  62 68  61 6d  40 38  il.com Shubham@8
1da7d670  34 30  32 20  2d 20  68 74  74 70  73 00  00 00  00 00  402 - https.....
1da7d680  00 00  00 00  00 00  00 00  8f cb  01 00  00 00  00 00  .........É......
```

3. Found the download record which downloaded through chrome



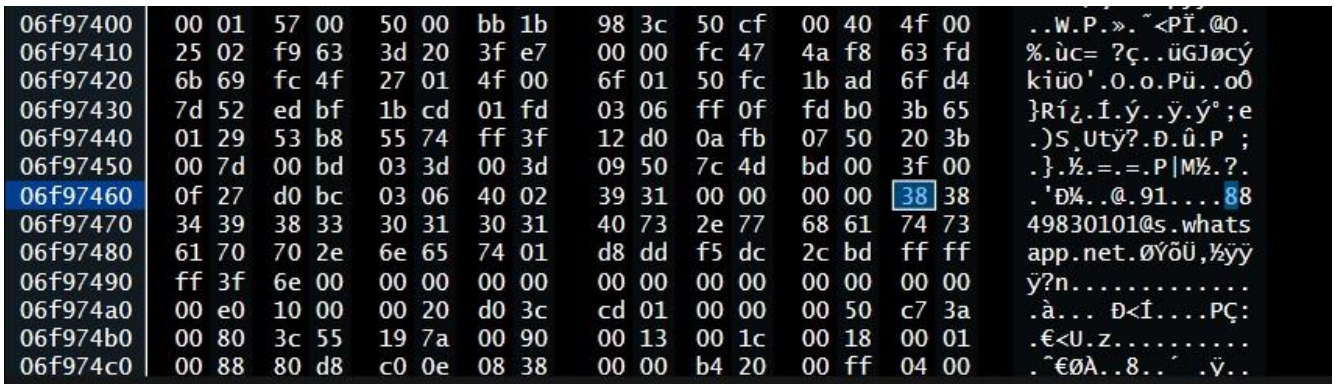
```
1f9c3d40  68 74  74 70  73 3a  2f 2f  77 77  77 2e  64 6f  77 6e  https://www.down
1f9c3d50  6c 6f  61 64  73 6f  75 72  63 65  2e 6e  65 74  2f 76  loadsource.net/v
1f9c3d60  2f 31  35 35  33 35  2f 5d  f4 47  04 81  0f 02  68 74  /15535/]ôG....ht
1f9c3d70  74 70  73 3a  2f 2f  77 77  77 2e  64 6f  77 6e  6c 6f  tps://www.downlo
1f9c3d80  61 64  73 6f  75 72  63 65  2e 6e  65 74  2f 6c  6f 63  adsource.net/loc
1f9c3d90  61 6c  73 65  72 76  65 72  2f 31  35 35  33 35  2d 75  alserver/15535-u
1f9c3da0  70 2d  4f 75  72 53  65 63  72 65  74 2e  65 78  65 5d  p-OurSecret.exe]
1f9c3db0  fb 2d  03 5d  02 68  74 74  70 73  3a 2f  2f 77  77 77  û-.].https://www
1f9c3dc0  2e 64  6f 77  6e 6c  6f 61  64 73  6f 75  72 63  65 2e  .downloadsource.
1f9c3dd0  6e 65  74 2f  64 6d  2f 32  39 37  32 31  2f 5d  f5 46  net/dm/29721/]õF
1f9c3de0  04 81  0d 02  68 74  74 70  73 3a  2f 2f  77 77  77 2e  ....https://www.
1f9c3df0  64 6f  77 6e  6c 6f  61 64  73 6f  75 72  63 65  2e 6e  downloadsource.n
1f9c3e00  65 74  2f 31  37 35  35 34  30 32  2f 6f  75 72  2d 73  et/1755402/our-s
1f9c3e10  65 63  72 65  74 2d  73 74  65 67  61 6e  6f 67  72 61  ecret-steganogra
1f9c3e20  70 68  79 2f  5d f1  24 03  4b 02  68 74  74 70  73 3a  phy/]ñ$.K.https:
1f9c3e30  2f 2f  77 77  77 2e  64 6f  77 6e  6c 6f  61 64  73 6f  //www.downloadso
1f9c3e40  75 72  63 65  2e 6e  65 74  2f 5d  fc 61  04 81  43 02  urce.net/]üa..C.
1f9c3e50  68 74  74 70  73 3a  2f 2f  77 77  77 2e  64 65  61 64  https://www.dead
1f9c3e60  74 6f  6f 6e  73 2e  6e 65  74 2f  70 6f  6b 65  6d 6f  toons.net/pokemo
1f9c3e70  6e 2d  78 79  2d 73  65 61  73 6f  6e 2d  31 37  2d 65  n-xy-season-17-e
1f9c3e80  70 69  73 6f  64 65  73 2d  68 69  6e 64  69 2d  64 75  pisodes-hindi-du
1f9c3e90  62 62  65 64  2d 64  6f 77  6e 6c  6f 61  64 2d  6d 61  bbed-download-ma
1f9c3ea0  72 76  65 6c  68 71  2d 64  75 62  2f 68  a3 6b  04 81  rvelhq-dub/h£k..
1f9c3eb0  57 02  68 74  74 70  73 3a  2f 2f  77 77  77 2e  64 65  W.https://www.de
1f9c3ec0  61 64  74 6f  6f 6e  73 2e  6e 65  74 2f  70 6f  6b 65  adtoons.net/poke
1f9c3ed0  6d 6f  6e 2d  73 65  61 73  6f 6e  2d 31  37 2d  74 68  mon-season-17-th
1f9c3ee0  65 2d  73 65  72 69  65 73  2d 78  79 2d  68 69  6e 64  e-series-xy-hind
1f9c3ef0  69 2d  65 70  69 73  6f 64  65 73  2d 64  6f 77  6e 6c  i-episodes-downl
1f9c3f00  6f 61  64 2d  37 32  30 70  2d 68  64 2d  68 75  6e 67  oad-720p-hd-hung
1f9c3f10  61 6d  61 2d  74 76  2f 68  a2 6d  04 81  5b 02  68 74  ama-tv/h¢m..[.ht
```

4. I found chrome history of previous window



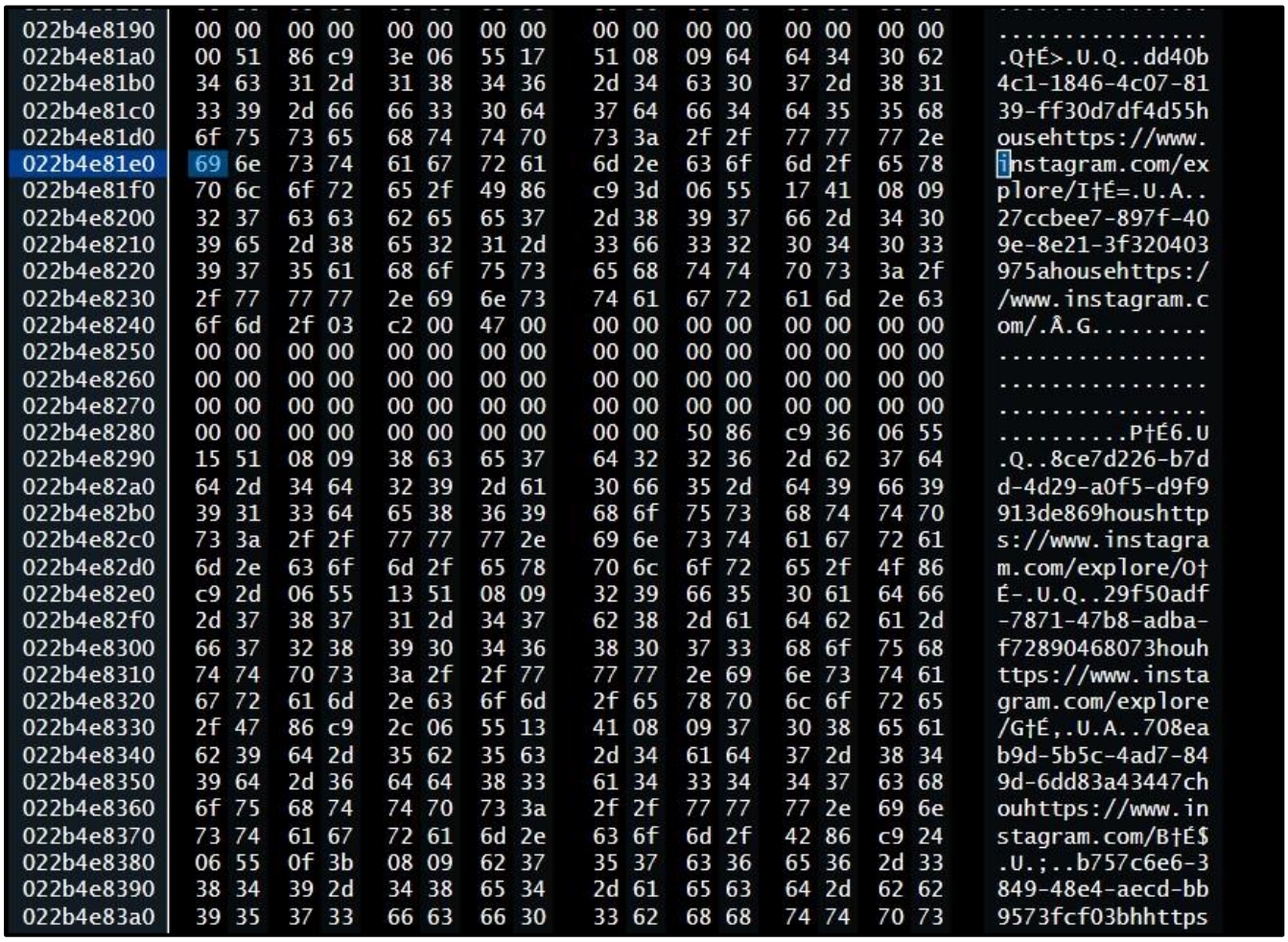
```
02640bb630  10 00  00 00  04 00  00 00  f8 00  00 00  00 00  00 00  ........ø.......
02640bb640  18 00  00 00  10 00  00 00  77 65  62 2e  77 68  61 74  ........web.what
02640bb650  73 61  70 70  2e 63  6f 6d  14 00  00 00  0c 00  00 00  sapp.com........
02640bb660  65 76  65 72  6e 6f  74 65  2e 63  6f 6d  00 00  00 00  evernote.com....
02640bb670  14 00  00 00  0c 00  00 00  6c 69  6e 6b  65 64  69 6e  ........linkedin
02640bb680  2e 63  6f 6d  00 00  00 00  16 00  00 00  0e 00  00 00  .com............
02640bb690  6d 61  69 6c  2e 79  61 68  6f 6f  2e 63  6f 6d  00 00  mail.yahoo.com..
02640bb6a0  15 00  00 00  0d 00  00 00  61 70  70 2e  73 6c  61 63  ........app.slac
02640bb6b0  6b 2e  63 6f  6d 00  00 00  13 00  00 00  0b 00  00 00  k.com...........
02640bb6c0  79 6f  75 74  75 62  65 2e  63 6f  6d 00  00 00  00 00  youtube.com.....
02640bb6d0  12 00  00 00  0a 00  00 00  66 69  76 65  72 72  2e 63  ........fiverr.c
02640bb6e0  6f 6d  00 00  00 00  00 00  11 00  00 00  09 00  00 00  om..............
02640bb6f0  74 77  69 74  63 68  2e 74  76 00  00 00  00 00  00 00  twitch.tv.......
02640bb700  13 00  00 00  0b 00  00 00  64 69  73 63  6f 72  64 2e  ........discord.
02640bb710  63 6f  6d 00  00 00  00 00  12 00  00 00  0a 00  00 00  com.............
02640bb720  72 65  64 64  69 74  2e 63  6f 6d  00 00  00 00  00 00  reddit.com......
02640bb730  13 00  00 00  0b 00  00 00  74 77  69 74  74 65  72 2e  ........twitter.
02640bb740  63 6f  6d 00  00 00  00 00  10 00  00 00  00 00  00 00  com.............
02640bb750  08 00  00 00  00 00  00 00  18 00  00 00  00 00  00 00  ................
02640bb760  10 00  00 00  00 00  00 00  48 00  00 00  00 00  00 00  ........H.......
02640bb770  18 00  00 00  02 00  00 00  10 00  00 00  00 00  00 00  ................
02640bb780  20 00  00 00  00 00  00 00  18 00  00 00  10 00  00 00   ...............
02640bb790  64 69  73 61  62 6c  65 64  42 79  44 6f  6d 61  69 6e  disabledByDomain
02640bb7a0  0f 00  00 00  07 00  00 00  65 6e  61 62  6c 65  64 00  ........enabled.
02640bb7b0  28 00  00 00  02 00  00 00  10 00  00 00  07 00  00 00  (...............
02640bb7c0  18 00  00 00  00 00  00 00  10 00  00 00  01 00  00 00  ................
02640bb7d0  01 00  00 00  00 00  00 00  10 00  00 00  00 00  00 00  ................
02640bb7e0  08 00  00 00  00 00  00 00  18 00  00 00  01 00  00 00  ................
02640bb7f0  10 00  00 00  04 00  00 00  08 00  00 00  00 00  00 00  ................
02640bb800  17 00  00 00  0f 00  00 00  64 6f  63 73  2e 67  6f 6f  ........docs.goo
02640bb810  67 6c  65 2e  63 6f  6d 00  20 00  00 00  18 00  00 00  gle.com. .......
02640bb820  64 79  6e 61  6d 69  63 43  6f 6e  66 69  67 4f  76 65  dynamicConfigOve
02640bb830  72 72  69 64  65 4b  65 79  10 00  00 00  00 00  00 00  rrideKey........
02640bb840  08 00  00 00  00 00  00 00  18 00  00 00  00 00  00 00  ................
```

5. Found whatsapp number



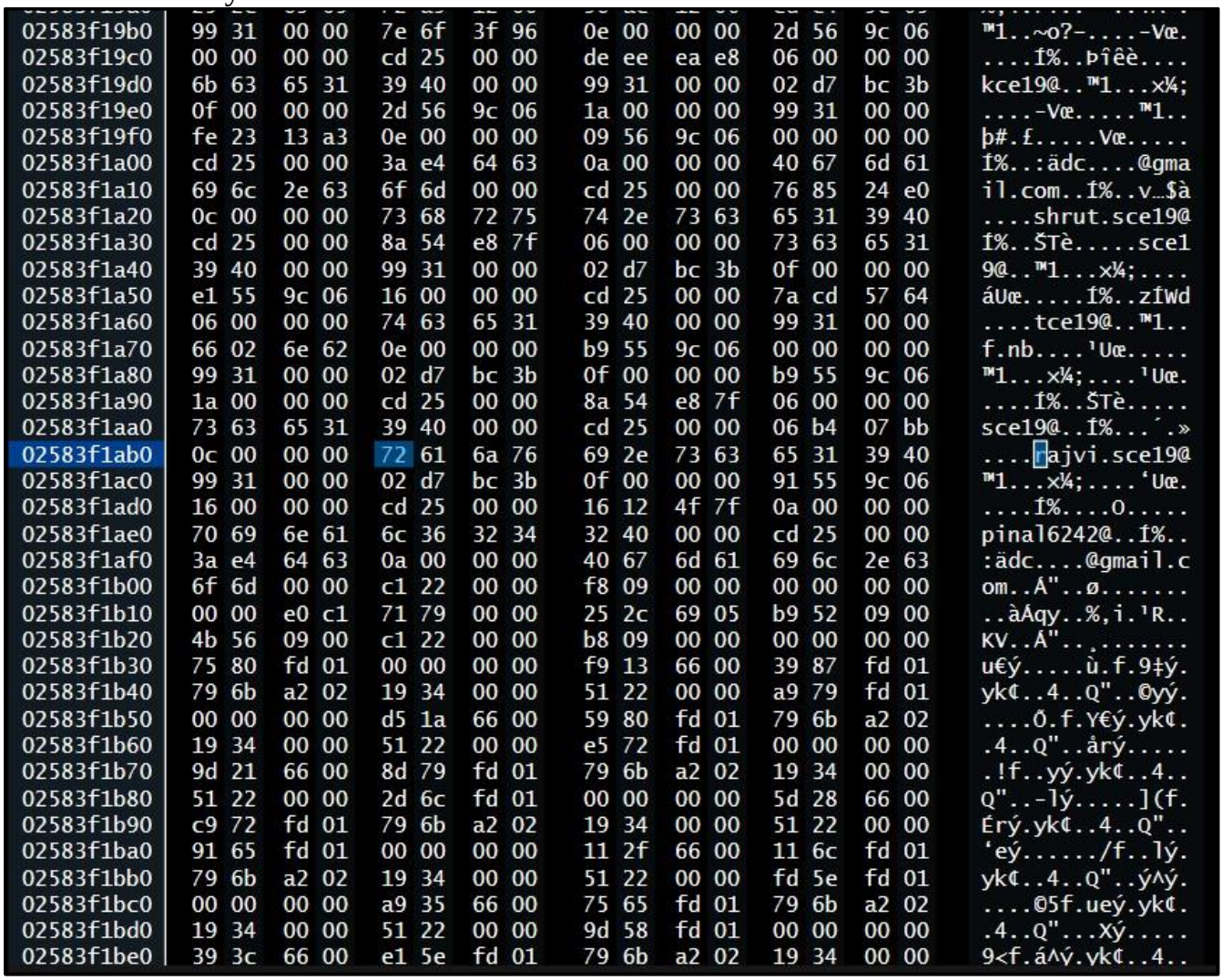
```
06f97400  00 01  57 00   50 00  bb 1b   98 3c  50 cf   00 40  4f 00   ..W.P.».˜<PÏ.@O.
06f97410  25 02  f9 63   3d 20  3f e7   00 00  fc 47   4a f8  63 fd   %.ùc= ?ç..üGJøcý
06f97420  6b 69  fc 4f   27 01  4f 00   6f 01  50 fc   1b ad  6f d4   kiüO'.O.o.Pü..oÔ
06f97430  7d 52  ed bf   1b cd  01 fd   03 06  ff 0f   fd b0  3b 65   }Rí¿.Í.ý..ÿ.ý°;e
06f97440  01 29  53 b8   55 74  ff 3f   12 d0  0a fb   07 50  20 3b   .)S¸Utÿ?.Ð.û.P ;
06f97450  00 7d  00 bd   03 3d  00 3d   09 50  7c 4d   bd 00  3f 00   .}.½.=.=.P|M½.?.
06f97460  0f 27  d0 bc   03 06  40 02   39 31  00 00   00 00  38 38   .'Ð¼..@.91....88
06f97470  34 39  38 33   30 31  30 31   40 73  2e 77   68 61  74 73   49830101@s.whats
06f97480  61 70  70 2e   6e 65  74 01   d8 dd  f5 dc   2c bd  ff ff   app.net.ØÝõÜ,½ÿÿ
06f97490  ff 3f  6e 00   00 00  00 00   00 00  00 00   00 00  00 00   ÿ?n.............
06f974a0  00 e0  10 00   00 20  d0 3c   cd 01  00 00   00 50  c7 3a   .à... Ð<Í....PÇ:
06f974b0  00 80  3c 55   19 7a  00 90   00 13  00 1c   00 18  00 01   .€<U.z..........
06f974c0  00 88  80 d8   c0 0e  08 38   00 00  b4 20   00 ff  04 00   .ˆ€ØÀ..8..´ .ÿ..
```

6. Found Instagram History



```
022b4e8190  00 00  00 00   00 00  00 00   00 00  00 00   00 00  00 00   ................
022b4e81a0  00 51  86 c9   3e 06  55 17   51 08  09 64   64 34  30 62   .Q†É>.U.Q..dd40b
022b4e81b0  34 63  31 2d   31 38  34 36   2d 34  63 30   37 2d  38 31   4c1-1846-4c07-81
022b4e81c0  33 39  2d 66   66 33  30 64   37 64  66 34   64 35  35 68   39-ff30d7df4d55h
022b4e81d0  6f 75  73 65   68 74  74 70   73 3a  2f 2f   77 77  77 2e   ousehttps://www.
022b4e81e0  69 6e  73 74   61 67  72 61   6d 2e  63 6f   6d 2f  65 78   instagram.com/ex
022b4e81f0  70 6c  6f 72   65 2f  49 86   c9 3d  06 55   17 41  08 09   plore/I†É=.U.A..
022b4e8200  32 37  63 63   62 65  65 37   2d 38  39 37   66 2d  34 30   27ccbee7-897f-40
022b4e8210  39 65  2d 38   65 32  31 2d   33 66  33 32   30 34  30 33   9e-8e21-3f320403
022b4e8220  39 37  35 61   68 6f  75 73   65 68  74 74   70 73  3a 2f   975ahousehttps:/
022b4e8230  2f 77  77 77   2e 69  6e 73   74 61  67 72   61 6d  2e 63   /www.instagram.c
022b4e8240  6f 6d  2f 03   c2 00  47 00   00 00  00 00   00 00  00 00   om/.Â.G.........
022b4e8250  00 00  00 00   00 00  00 00   00 00  00 00   00 00  00 00   ................
022b4e8260  00 00  00 00   00 00  00 00   00 00  00 00   00 00  00 00   ................
022b4e8270  00 00  00 00   00 00  00 00   00 00  00 00   00 00  00 00   ................
022b4e8280  00 00  00 00   00 00  00 00   00 00  50 86   c9 36  06 55   ..........P†É6.U
022b4e8290  15 51  08 09   38 63  65 37   64 32  32 36   2d 62  37 64   .Q..8ce7d226-b7d
022b4e82a0  64 2d  34 64   32 39  2d 61   30 66  35 2d   64 39  66 39   d-4d29-a0f5-d9f9
022b4e82b0  39 31  33 64   65 38  36 39   68 6f  75 73   68 74  74 70   913de869houshttp
022b4e82c0  73 3a  2f 2f   77 77  77 2e   69 6e  73 74   61 67  72 61   s://www.instagra
022b4e82d0  6d 2e  63 6f   6d 2f  65 78   70 6c  6f 72   65 2f  4f 86   m.com/explore/O†
022b4e82e0  c9 2d  06 55   13 51  08 09   32 39  66 35   30 61  64 66   É-.U.Q..29f50adf
022b4e82f0  2d 37  38 37   31 2d  34 37   62 38  2d 61   64 62  61 2d   -7871-47b8-adba-
022b4e8300  66 37  32 38   39 30  34 36   38 30  37 33   68 6f  75 68   f72890468073houh
022b4e8310  74 74  70 73   3a 2f  2f 77   77 77  2e 69   6e 73  74 61   ttps://www.insta
022b4e8320  67 72  61 6d   2e 63  6f 6d   2f 65  78 70   6c 6f  72 65   gram.com/explore
022b4e8330  2f 47  86 c9   2c 06  55 13   41 08  09 37   30 38  65 61   /G†É,.U.A..708ea
022b4e8340  62 39  64 2d   35 62  35 63   2d 34  61 64   37 2d  38 34   b9d-5b5c-4ad7-84
022b4e8350  39 64  2d 36   64 64  38 33   61 34  33 34   34 37  63 68   9d-6dd83a43447ch
022b4e8360  6f 75  68 74   74 70  73 3a   2f 2f  77 77   77 2e  69 6e   ouhttps://www.in
022b4e8370  73 74  61 67   72 61  6d 2e   63 6f  6d 2f   42 86  c9 24   stagram.com/B†É$
022b4e8380  06 55  0f 3b   08 09  62 37   35 37  63 36   65 36  2d 33   .U.;..b757c6e6-3
022b4e8390  38 34  39 2d   34 38  65 34   2d 61  65 63   64 2d  62 62   849-48e4-aecd-bb
022b4e83a0  39 35  37 33   66 63  66 30   33 62  68 68   74 74  70 73   9573fcf03bhhttps
```

7. Found my friends emailid



```
02583f19b0  99 31 00 00  7e 6f 3f 96  0e 00 00 00  2d 56 9c 06  ™1..~o?–....-Vœ.
02583f19c0  00 00 00 00  cd 25 00 00  de ee ea e8  06 00 00 00  ....Í%..Þîêè....
02583f19d0  6b 63 65 31  39 40 00 00  99 31 00 00  02 d7 bc 3b  kce19@..™1...x¼;
02583f19e0  0f 00 00 00  2d 56 9c 06  1a 00 00 00  99 31 00 00  ....-Vœ.....™1..
02583f19f0  fe 23 13 a3  0e 00 00 00  09 56 9c 06  00 00 00 00  þ#.£.....Vœ.....
02583f1a00  cd 25 00 00  3a e4 64 63  0a 00 00 00  40 67 6d 61  Í%..:ädc....@gma
02583f1a10  69 6c 2e 63  6f 6d 00 00  cd 25 00 00  76 85 24 e0  il.com..Í%..v…$à
02583f1a20  0c 00 00 00  73 68 72 75  74 2e 73 63  65 31 39 40  ....shrut.sce19@
02583f1a30  cd 25 00 00  8a 54 e8 7f  06 00 00 00  73 63 65 31  Í%..ŠTè.....sce1
02583f1a40  39 40 00 00  99 31 00 00  02 d7 bc 3b  0f 00 00 00  9@..™1...x¼;....
02583f1a50  e1 55 9c 06  16 00 00 00  cd 25 00 00  7a cd 57 64  áUœ.....Í%..zÍWd
02583f1a60  06 00 00 00  74 63 65 31  39 40 00 00  99 31 00 00  ....tce19@..™1..
02583f1a70  66 02 6e 62  0e 00 00 00  b9 55 9c 06  00 00 00 00  f.nb....¹Uœ.....
02583f1a80  99 31 00 00  02 d7 bc 3b  0f 00 00 00  b9 55 9c 06  ™1...x¼;....¹Uœ.
02583f1a90  1a 00 00 00  cd 25 00 00  8a 54 e8 7f  06 00 00 00  ....Í%..ŠTè.....
02583f1aa0  73 63 65 31  39 40 00 00  cd 25 00 00  06 b4 07 bb  sce19@..Í%...´.»
02583f1ab0  0c 00 00 00  72 61 6a 76  69 2e 73 63  65 31 39 40  ....rajvi.sce19@
02583f1ac0  99 31 00 00  02 d7 bc 3b  0f 00 00 00  91 55 9c 06  ™1...x¼;....'Uœ.
02583f1ad0  16 00 00 00  cd 25 00 00  16 12 4f 7f  0a 00 00 00  ....Í%....O.....
02583f1ae0  70 69 6e 61  6c 36 32 34  32 40 00 00  cd 25 00 00  pinal6242@..Í%..
02583f1af0  3a e4 64 63  0a 00 00 00  40 67 6d 61  69 6c 2e 63  :ädc....@gmail.c
02583f1b00  6f 6d 00 00  c1 22 00 00  f8 09 00 00  00 00 00 00  om..Á"..ø.......
02583f1b10  00 00 e0 c1  71 79 00 00  25 2c 69 05  b9 52 09 00  ..àÁqy..%,i.¹R..
02583f1b20  4b 56 09 00  c1 22 00 00  b8 09 00 00  00 00 00 00  KV..Á"..¸.......
02583f1b30  75 80 fd 01  00 00 00 00  f9 13 66 00  39 87 fd 01  u€ý.....ù.f.9‡ý.
02583f1b40  79 6b a2 02  19 34 00 00  51 22 00 00  a9 79 fd 01  yk¢..4..Q"..©yý.
02583f1b50  00 00 00 00  d5 1a 66 00  59 80 fd 01  79 6b a2 02  ....Õ.f.Y€ý.yk¢.
02583f1b60  19 34 00 00  51 22 00 00  e5 72 fd 01  00 00 00 00  .4..Q"..årý.....
02583f1b70  9d 21 66 00  8d 79 fd 01  79 6b a2 02  19 34 00 00  .!f..yý.yk¢..4..
02583f1b80  51 22 00 00  2d 6c fd 01  00 00 00 00  5d 28 66 00  Q"..-lý.....](f.
02583f1b90  c9 72 fd 01  79 6b a2 02  19 34 00 00  51 22 00 00  Érý.yk¢..4..Q"..
02583f1ba0  91 65 fd 01  00 00 00 00  11 2f 66 00  11 6c fd 01  'eý...../f..lý.
02583f1bb0  79 6b a2 02  19 34 00 00  51 22 00 00  fd 5e fd 01  yk¢..4..Q"..ý^ý.
02583f1bc0  00 00 00 00  a9 35 66 00  75 65 fd 01  79 6b a2 02  ....©5f.ueý.yk¢.
02583f1bd0  19 34 00 00  51 22 00 00  9d 58 fd 01  00 00 00 00  .4..Q"...Xý.....
02583f1be0  39 3c 66 00  e1 5e fd 01  79 6b a2 02  19 34 00 00  9<f.á^ý.yk¢..4..
```

Digital Forensics Lab Report: 10

Date: 02-11-2022

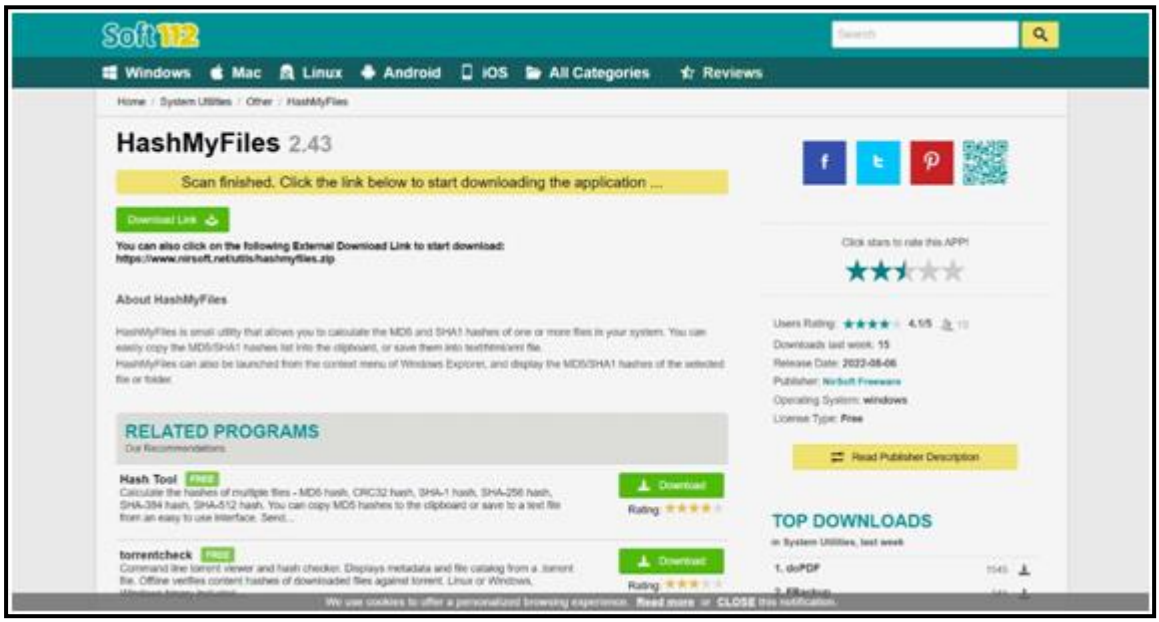
Name:	Vedant H. Patel
Roll No:	19BCP138
Subject Code:	20CP411P
Subject Name:	Digital Forensics Lab

Aim/Purpose: Study of Hash and Hack Analysis Tools.

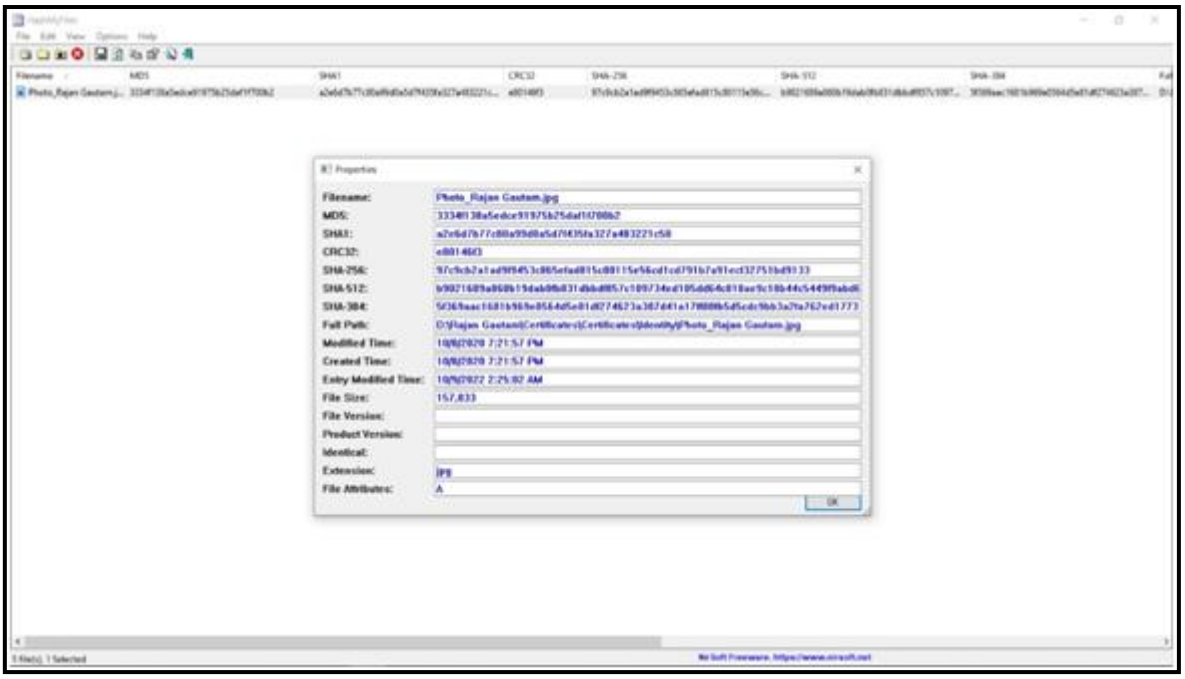
Tool Names: WinHEX, Garrykesler, hashmefile ignoreware.

Step 1: Download and Install HashMyFiles

- Visit https://hashmyfiles.soft112.com/modal-download.html and Download HashMyFiles as ZIP. Extract the zip file to get the .exe file.



- Open the Application and open any file.



- Access Garrykesler from this URL https://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 Extension.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 Conkley'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.

ACKNOWLEDGMENTS & COPYRIGHT NOTICE

- 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 45 78'.

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-D9-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 — ÿØÿà..JF IF. — JFIF, JPE, JPEG, JPG — JPEG/JFIF graphics file — **Trailer:** FF D9 (ÿÙ)

FF D8 FF E1 xx xx 45 78 69 66 00 — ÿØÿá..Ex if. — JPG — 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" (9 Advanced Computing and Digital Forensics Journal, 2(3), Winter 2004) and EndOfExif.Tag Pointer

FF D8 FF E8 xx xx 53 50 49 46 46 00 — ÿØÿè..SP IFF. — JPG — Still Picture Interchange File Format (SPIFF) — **Trailer:** FF D9 (ÿÙ)

FF Ex — ÿ.

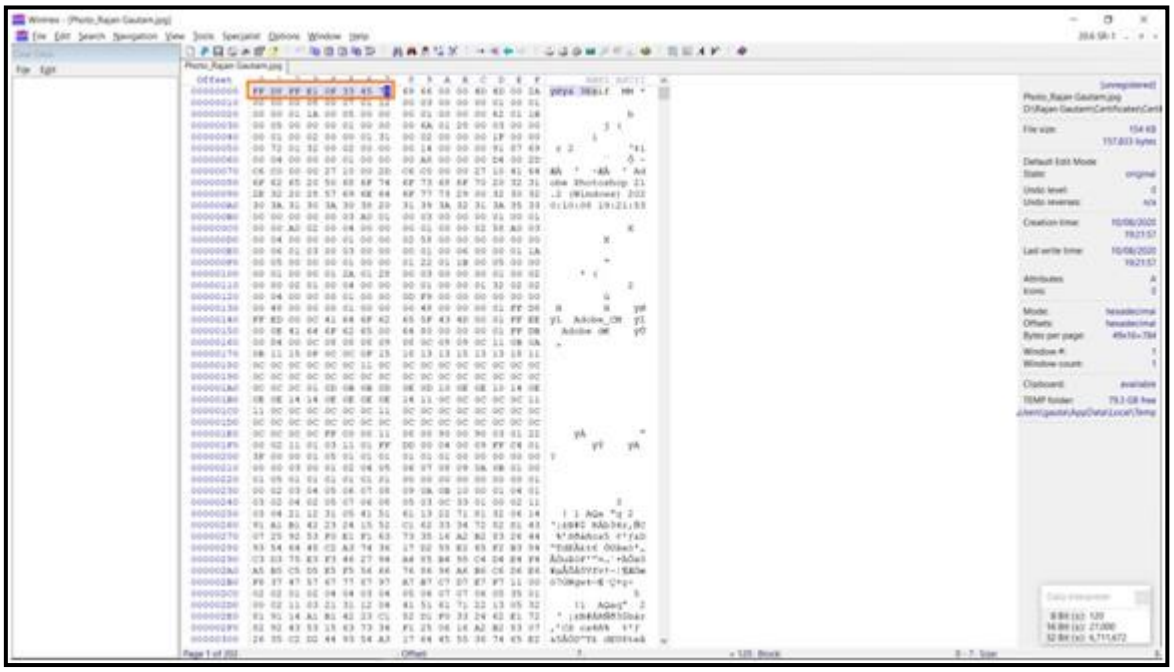
FF Fx — ÿ. — MPEG, MPG, MP3 — MPEG audio file frame sync pattern

FF F1 — ÿñ — AAC — MPEG-4 Advanced Audio Coding (AAC) Low Complexity (LC) audio file

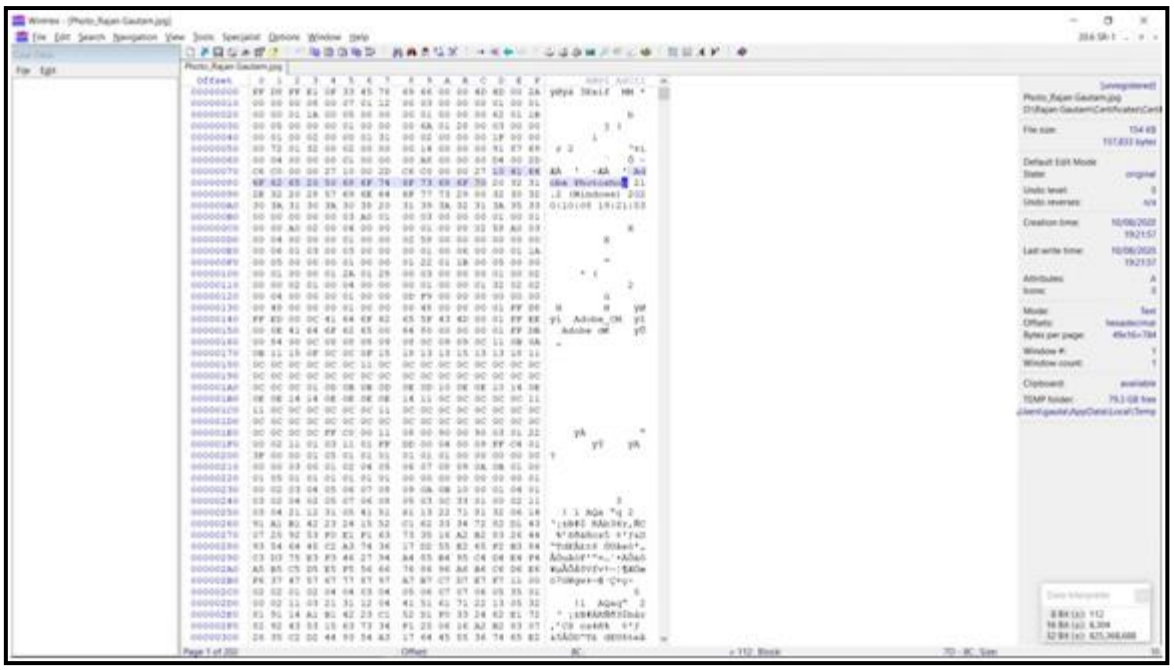
FF F9 — ÿù — AAC — MPEG-2 Advanced Audio Coding (AAC) Low Complexity (LC) audio file

FF FE — ÿþ — REG — Windows Registry file — n/a — 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 House Page.)

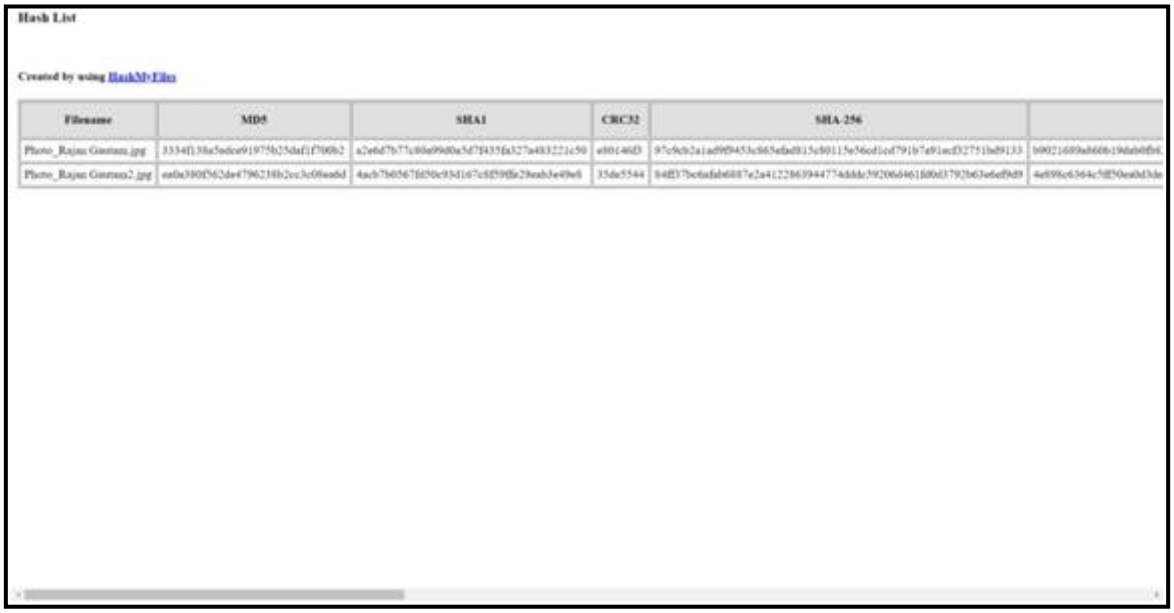
- Open the same file using WinHEX. We can see the same HEX value in the editor which shows the file is .JPG file.



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



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



Conclusion:

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

Thank You