International Journal of Innovation and Applied Studies
ISSN 2028-9324 Vol. 43 No. 2 Aug. 2024, pp. 261-271

http://www.ijias.issr-journals.org/

Digital Forensic Analysis of Social Media Platforms for Enhanced Investigation and Evidence Collection

***Kausik Maitra*[1-2]**

[1]Assistant Professor, Department of Cyber Science and Technology, Brainware University, Kolkata, 700125, India

[2]Ex-Technical Forensic Consultant in Central Bureau of Investigation Govt, India

ABSTRACT: Cybercrime in social media by definition is any harmful act committed from or against a computer or Network, is a crime committed in a virtual space and a virtual space is fashioned in a way that information about persons, objects, facts, events, phenomena or processes are represented in mathematical, symbol or any other way and transferred through local and global Networks. Digital forensic analysis of social media platforms has emerged as a vital tool for enhancing criminal investigations and evidence collection. With the increasing popularity of social media, criminals often use these platforms to plan, commit, and boast about their crimes. However, identifying and retrieving digital traces from social media can be challenging due to the complex nature of these platforms and the dynamic nature of the content.
This project aims to explore digital forensic techniques and methodologies for effectively analysing social media data, including user profiles, posts, messages, and metadata. And it can aid in determining cyber threats and fraud by examining evidence present in emails, social media, and other forms of digital communication that are part of cyber-attacks and financial crimes.

KEYWORDS: Cyber Investigation, IT ACT 2000, Web Scrapping, Cyberbullying, NLP, Privacy, Online Fraud, Digital Evidence.

1 INTRODUCTION

Social media crime has become a growing global issue due to the vast reach and accessibility of social media platforms in various forms.

- Fraud and Scams: Criminals have devised various schemes through fake messages from hijacked profiles. Offers for financial relief, "friend request" or message out of the blue, Completing quizzes and playing games, and online shopping fraud;
- Cyberbullying: Cyberbullying [11] is a serious and growing problem affecting many children and adults worldwide in social media, chat services, gaming platforms, and mobile devices. Cyberbullies revel in the “sense of anonymity” that the digital world offers them, while the majority of the bullied children and women are too traumatised to seek help and prefer to stay hidden. Like Spreading lies, sending hurtful messages, impersonating someone, sharing personal information, exclusion from online groups, and making fun of someone’s appearance, identity, abilities, beliefs, or interests on social media, causing humiliation;
- Cyberstalking: This is the act of persistent and unwanted contact from someone online. It may involve any number of incidents including threats, libel, defamation, sexual harassment, or other actions in which to control, influence, or intimidate their target. Stalking a person online may also involve stalking the person in real life. As per NCRB India, 1,823 cases of cybercrimes against children in 2022;
- Hate Speech & Extremism: Violence attributed to online hate speech has increased worldwide. Societies confronting the trend must deal with questions of free speech and censorship on widely used tech platforms. This trends in hate crimes around the world echo changes in the political climate, and that social media can magnify discord. Some key aspects include:

- Radicalization: Social media platforms are increasingly used by extremist groups to spread their message, recruit new members, and promote their ideology, often targeting vulnerable and impressionable individuals;
- Incitement to Violence: Hate speech on social media can lead to physical violence, as seen in cases of racially motivated attacks, anti-religious violence, and political extremism.

- Deepfakes for Social Engineering [13]: This is a threat to business as a vector for social engineering attacks. Criminals can use deepfakes to create realistic videos or audio recordings of public figures, CEOs, or even friends and family through Sharing sensitive information, Sending money, and Clicking on malicious links.

In a dynamic society that we live in technology and interpersonal connections are two things that keep on evolving. Digital forensics has had a significant impact on social media in India:

- Cyber Crime Detection: Indian law [10] enforcement agencies have benefited from the use of digital forensics in detecting and solving cybercrimes committed through social media platforms;
- Criminal Prosecution: Digital evidence retrieved from social media has been used in criminal prosecution and has helped secure convictions in several high-profile cases in India;
- Prevention of Fake News: The analysis of digital traces in social media has helped identify sources of fake news and misinformation, which have been a significant issue in India's political climate.

2 SCOPE

The research explores the intricate relationship between digitalization and white-collar crime in the context of India's evolving technological landscape. It examines the impact of digitalization on the dynamics of white-collar crime, investigating its purpose, methods, key findings, and implications. As people in India turned to the Internet after covid pandemic for their needs, it became more urgent to address cross-border data concerns to assist law enforcement investigations into criminal activity and to identify common cybersecurity attributes such as:

- User Perspective
  - Data Privacy [15]: Social media platforms collect and store vast amounts of personal information, which can be vulnerable to data breaches and hacking;
  - Account Security: Social media accounts are often targets for hacking and phishing attacks, with hackers trying to gain access to sensitive information or take over accounts for fraudulent purposes;
  - Discernment with Links & Attachments: Being cautious about clicking on links or opening attachments, especially from unknown senders, is vital to avoid malware and phishing scams;
  - Malware Distribution: Social media platforms can be used by hackers to distribute malicious software, such as viruses, worms, and ransomware, through fake profiles, links, or messages.
- Platform Security Measures
  - Security Protocols: Social media platforms use various security protocols, such as SSL (Secure Sockets Layer), [3] to encrypt user data and communications to prevent unauthorized access and eavesdropping;
  - Authentication and Authorization: Social media platforms implement authentication and authorization measures, such as passwords, two-factor authentication, and IP restrictions, to ensure that only authorized users can access accounts and data;
  - Regular Security Updates: Platforms should promptly address security vulnerabilities through regular updates to their systems;
  - Content Moderation: Having measures in place to identify and remove harmful content like hate speech or misinformation promotes a safer online environment;
  - User Reporting Mechanisms: Easy-to-use reporting tools allow users to flag suspicious activity or content for platform review and action.

3 OBJECTIVE

In the context of social media cyber space and digital environment has become one inextricable factor Social media can be defined as interactive computer-mediated technologies via virtual communities and social networking websites that simplify the creation and sharing of ideas, information, opinions, career interests, and other types of expression. With the increase in technology, there has been an inclination in crime rates and the crimes committed through this technology. The legal

framework is constantly evolving, and the impact of social media on the law of evidence cannot be ignored. The Indian Evidence Act stands amended now, especially to provide for the admissibility of electronic evidence (record) supplemented with paper-based documents as evidence in Indian Courts. Significant amendments grant the status of documents for adducing evidence to electronic records. The amendment to the Evidence Act is the introduction of Section 65A and 65B under the second schedule of the Information Technology Act. This provides for a procedure, that is different and special in nature for adducing evidence in relation to electronic records.

3.1 WHAT IS SOCIAL MEDIA EVIDENCE?

In the context of India, the term "social evidence" doesn't have a legal definition specifically related to social media. However, social media content can be considered electronic evidence under the Indian legal system. It also sets out conditions for the admissibility of evidence and all are to be satisfied. They are:

- At the time of creation of the electronic record, the computer output containing the relevant information was produced from a computer that was used there regularly to store and/or process information for any activities that are regularly carried on over that period by that person lawfully controlling the use of the computer;
- The type of information that is contained in the electronic record was regularly fed into the computer in the regular course of activities;
- The information that is contained by the electronic records is the reproduction of the original electronic record;
- During the material part of the period, the computer was operating properly or, if not, the the computer was out of operation for some period but did not have much to affect the electronic record.

3.2 TYPES OF SOCIAL MEDIA DIGITAL EVIDENCE

Social media digital evidence can be broadly classified into four types:

- Direct Evidence: This includes explicit content such as posts, comments, messages, and images that provide direct proof of a crime, civil dispute, or other incident;
- Indirect Evidence: This includes information that can be inferred from social media data, such as patterns of behaviour, associations with other people, or location data that can suggest someone's involvement in an event;
- Inferential Evidence: This includes data from social media platforms that can be used to build a case or support other evidence, such as login times, IP addresses, and user activity logs that can indicate someone's use of a particular account;
- Expert Witness Evidence: This includes expert opinions from social media or digital forensics experts who can provide insights on the authenticity, interpretation, or technical aspects of social media evidence.

3.3 WHAT CAN BE COLLECTED FROM SOCIAL MEDIA

- Text Content
  - Posts, comments, and messages on platforms like Facebook, Twitter, Instagram, and LinkedIn;
  - Private messages or direct messages.
- Multimedia Content
  - Photos, videos, and audio files shared publicly or privately;
  - Live streams and stories that are often time-limited.
- Metadata
  - Information such as timestamps, geolocation data, and user account details;
  - Data showing interactions, like who viewed or liked a post.
- Activity Logs
  - Records of account activity, including login times and IP addresses;
  - History of posts, edits, and deletions.

4 SCOPE OF PROJECT WORK

4.1 COLLECTION METHODS

Data from social media accounts can be collected via the following methods

- Cloud collections by using the application
  - Connect to social media accounts through provider API;
  - User credentials are needed for private accounts.
- Collection of mobile devices that have the social media account application installed
  - Apps like Snapchat can only be collected using this method;
  - Limited Datasets since most data is saved in the cloud rather than on the device itself;
  - User credentials can be obtained from a mobile device collection and used to log in to the accounts for a cloud collection.
- Collection of computers
  - Limited data sets since the majority of data is saved in the cloud rather than on the device itself;
  - Internet history, log files, and computer cache can provide insight and possibly relevant information;
  - User credentials can possibly be obtained from a mobile device collection and can be used to log in to the accounts for a cloud collection.
- Download of data from social media site
  - Sites like Facebook and Instagram provide a method of downloading all or selective data from a user's account;
  - Utilizing the self service 'download your data' option available on some cloud services will output the selected data in a format that is not easily readable or presentable but can be processed and decoded within application;
  - User credentials are needed to log into the account and access the selling to obtain the download of data.

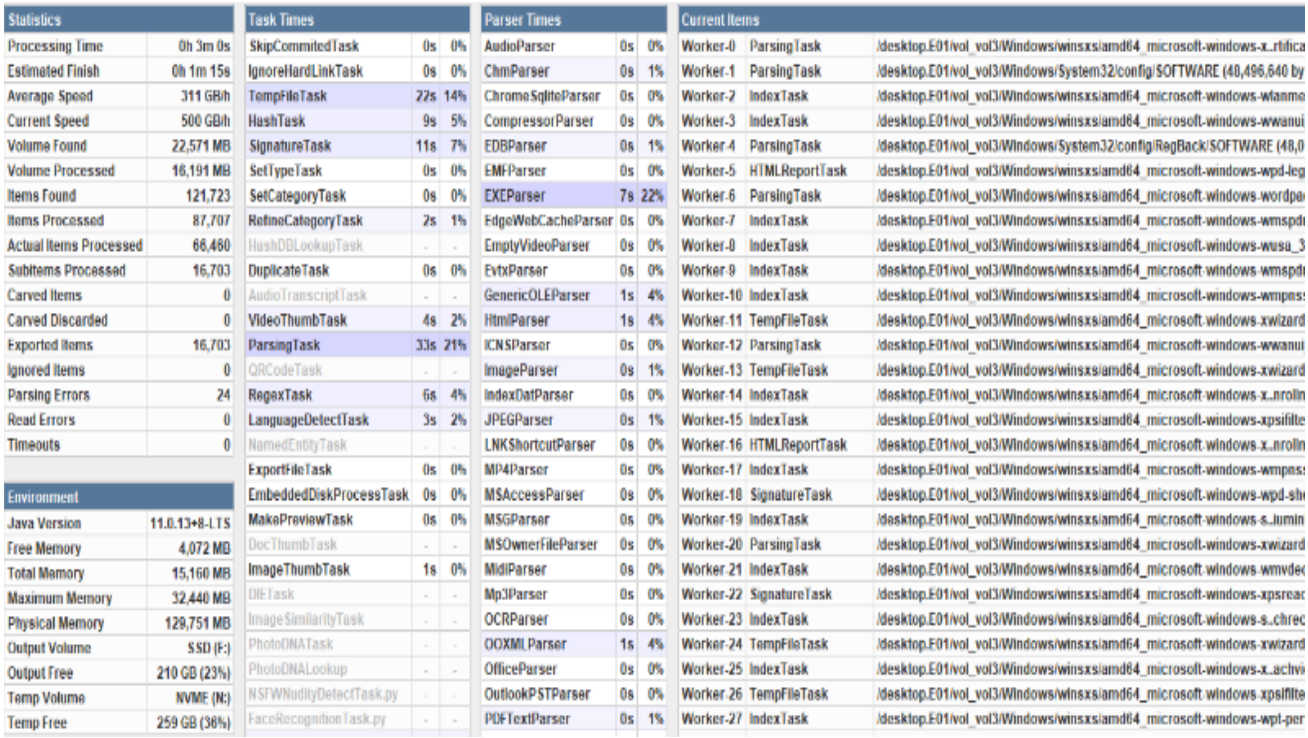
4.2 THE PROJECT WILL FOCUS ON THE FOLLOWING

- Criminal Investigations: Social media activity can be used to establish alibis, track down suspects, identify witnesses, and gather details about criminal activities;
- Civil Disputes: Social media posts can be evidence of contract breaches, defamation cases, intellectual property disputes, and even child custody battles;
- Impeaching Credibility: Inconsistent statements or contradictory posts can be used to challenge the credibility of witnesses or parties involved in a case.

4.3 FEATURES

- Supported hashes: md5, sha-1, sha-256, sha-512 and edonkey
- Supported hash sets: NIST NSRL, NIST CAID, standard CSV format
- Fast hash deduplication
- Signature analysis
- Categorization by file type and properties
- Recursive container expansion of dozens of file formats
- Embedded forensic/virtual disks expansion: supports splitted or single segment DD, E01, EX01, VHD, VHDX, VMDK (differential VMDKs are also supported)
- Image and video gallery for hundreds of formats
- Georeferencing of GPS data, using Google Maps, Bing or OpenStreetMaps
- Regex searches with optional script validation for credit cards, emails, urls, ip & mac addresses, money values, bitcoin, etc
- Embedded hex, Unicode text, metadata and native viewers
- File content and metadata indexing and fast searching, including unknown files and unallocated space
- Optical Character Recognition powered by tesseract 5
- Encryption detection for known formats and using entropy test
- Processing profiles: forensic, pedo (csam), triage, fastmode (preview) and blind (for automatic data extraction)
- Customizable filters based on any file metadata

- Similar document search with configurable threshold
- Similar image search, using internal or external image
- Similar face recognition, optimized to run without GPU, with configurable threshold
- Unified table timeline view and event filtering for timeline analysis
- Powerful file grouping (clustering) based on ANY metadata
- Extensible with javascript and python (including cpython extensions) scripts
- External command line tools integration for file decoding
- Browser history for IE, Edge, Firefox, Chrome and Safari
- Graph analysis for communications (calls, emails, instant messages...)
- Stable processing with out-of-process file system decoding and file parsing
- Web API for searching remote cases, get file metadata, raw content, decoded text, thumbnails and posting bookmarks
- Creation of bookmarks/tags for interesting data
- HTML, CSV reports and portable cases with tagged data



Statistics	
Processing Time	0h 3m 0s
Estimated Finish	0h 1m 15s
Average Speed	311 GB/h
Current Speed	500 GB/h
Volume Found	22,571 MB
Volume Processed	16,191 MB
Items Found	121,723
Items Processed	87,707
Actual Items Processed	66,460
Subitems Processed	16,703
Carved Items	0
Carved Discarded	0
Exported Items	16,703
Ignored Items	0
Parsing Errors	24
Read Errors	0
Timeouts	0

Environment	
Java Version	11.0.13+8-LTS
Free Memory	4,072 MB
Total Memory	15,160 MB
Maximum Memory	32,440 MB
Physical Memory	129,751 MB
Output Volume	SSD (F:)
Output Free	210 GB (23%)
Temp Volume	NVME (N:)
Temp Free	259 GB (36%)

Task Times		
SkipCommitedTask	0s	0%
IgnoreHardLinkTask	0s	0%
TempFileTask	22s	14%
HashTask	9s	5%
SignatureTask	11s	7%
SetTypeTask	0s	0%
SetCategoryTask	0s	0%
RefineCategoryTask	2s	1%
HashDBLookupTask	-	-
DuplicateTask	0s	0%
AudioTranscriptTask	-	-
VideoThumbTask	4s	2%
ParsingTask	33s	21%
QRCodeTask	-	-
RegexTask	6s	4%
LanguageDetectTask	3s	2%
NamedEntityTask	-	-
ExportFileTask	0s	0%
EmbeddedDiskProcessTask	0s	0%
MakePreviewTask	0s	0%
DocThumbTask	-	-
ImageThumbTask	1s	0%
DIETask	-	-
ImageSimilarityTask	-	-
PhotoDNATask	-	-
PhotoDNALookup	-	-
NSFWNudityDetectTask.py	-	-
FaceRecognitionTask.py	-	-

Parser Times		
AudioParser	0s	0%
ChmParser	0s	1%
ChromeSqliteParser	0s	0%
CompressorParser	0s	0%
EDBParser	0s	1%
EMFParser	0s	0%
EXEParser	7s	22%
EdgeWebCacheParser	0s	0%
EmptyVideoParser	0s	0%
EvtxParser	0s	0%
GenericOLEParser	1s	4%
HtmlParser	1s	4%
ICNSParser	0s	0%
ImageParser	0s	1%
IndexDatParser	0s	0%
JPEGParser	0s	1%
LNKShortcutParser	0s	0%
MP4Parser	0s	0%
MSAccessParser	0s	0%
MSGParser	0s	0%
MSOwnerFileParser	0s	0%
MidiParser	0s	0%
Mp3Parser	0s	0%
OCRParser	0s	0%
OOXMLParser	1s	4%
OfficeParser	0s	0%
OutlookPSTParser	0s	0%
PDFTextParser	0s	1%

Current Items		
Worker-0	ParsingTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-x..rtifica
Worker-1	ParsingTask	/desktop.E01/vol_vol3/Windows/System32/config/SOFTWARE (48,496,640 by
Worker-2	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wlanme
Worker-3	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wwanui
Worker-4	ParsingTask	/desktop.E01/vol_vol3/Windows/System32/config/RegBack/SOFTWARE (48,0
Worker-5	HTMLReportTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wpd-leg
Worker-6	ParsingTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wordpa
Worker-7	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wmspdi
Worker-8	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wusa_3
Worker-9	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wmspdi
Worker-10	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wmpnss
Worker-11	TempFileTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xwizard
Worker-12	ParsingTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wwanui
Worker-13	TempFileTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xwizard
Worker-14	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-x..nrolin
Worker-15	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xpsfilte
Worker-16	HTMLReportTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-x..nrolin
Worker-17	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wmpnss
Worker-18	SignatureTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wpd-sh
Worker-19	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-s..lumin
Worker-20	ParsingTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xwizard
Worker-21	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wmvdec
Worker-22	SignatureTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xpsreac
Worker-23	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-s..chrec
Worker-24	TempFileTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xwizard
Worker-25	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-x..aclvi
Worker-26	TempFileTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-xpsfilte
Worker-27	IndexTask	/desktop.E01/vol_vol3/Windows/winsxs/amd64_microsoft-windows-wpf-per

Fig. 1. Processing

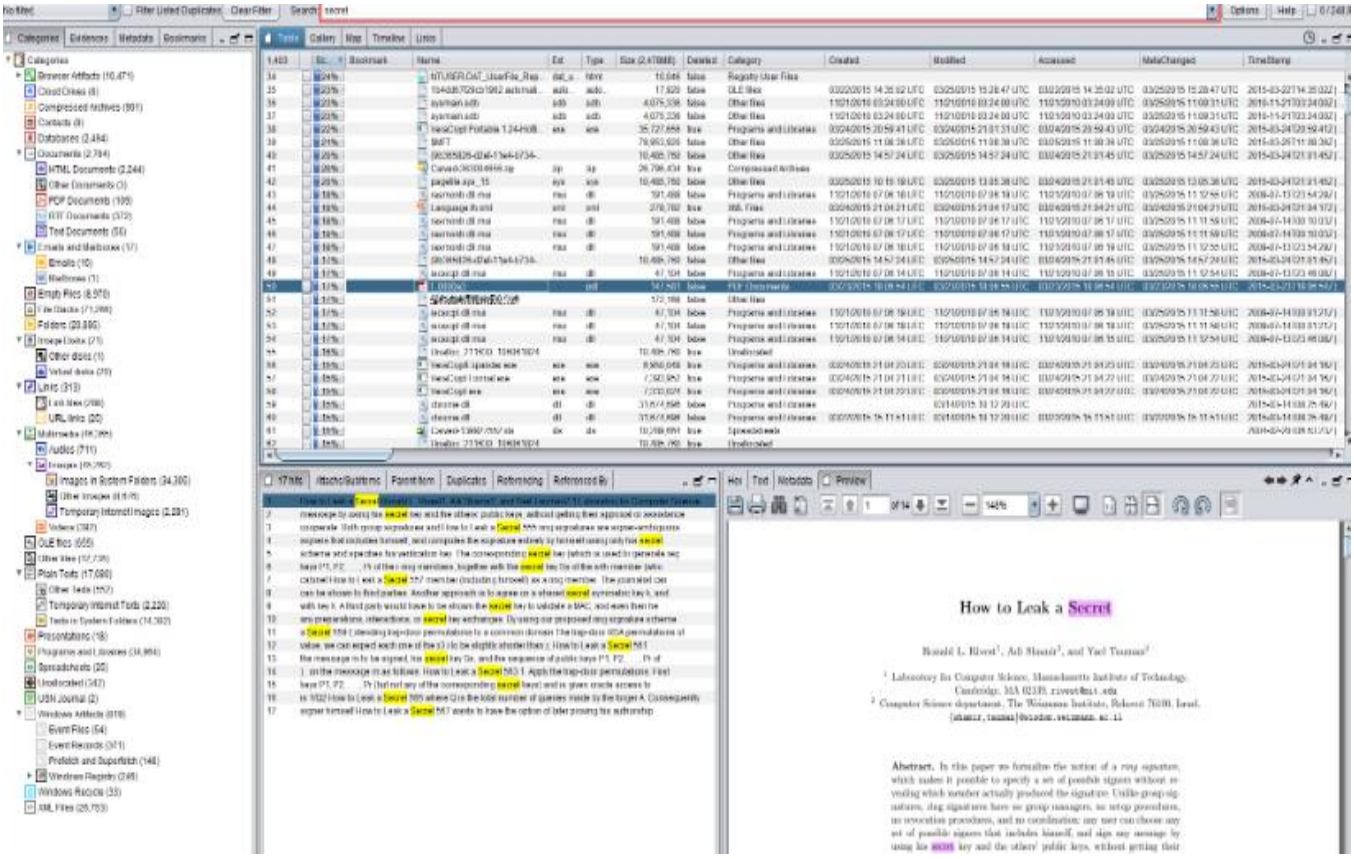


Fig. 2. Analysis

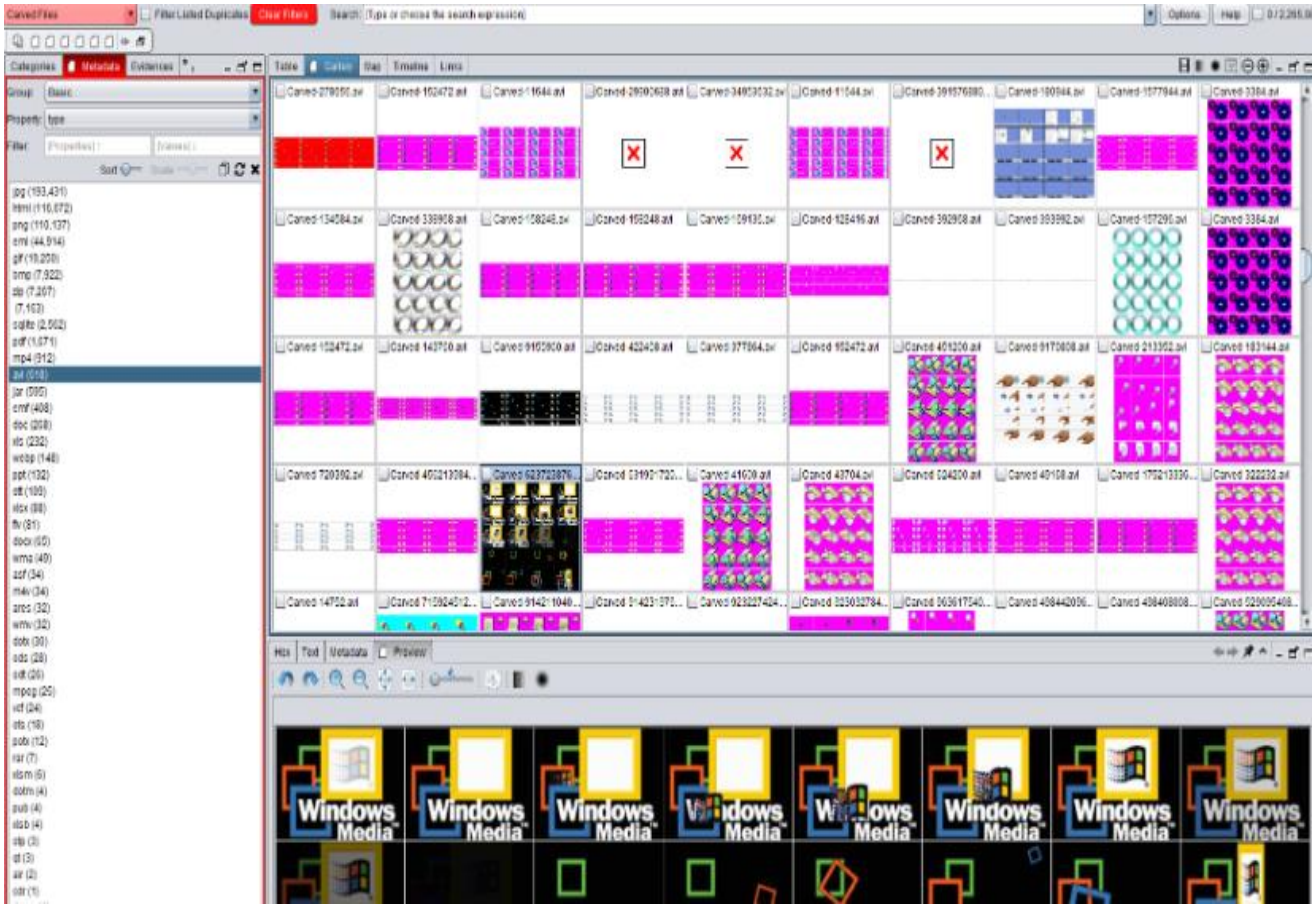


Fig. 3. Data Carving & Video Thumbnails

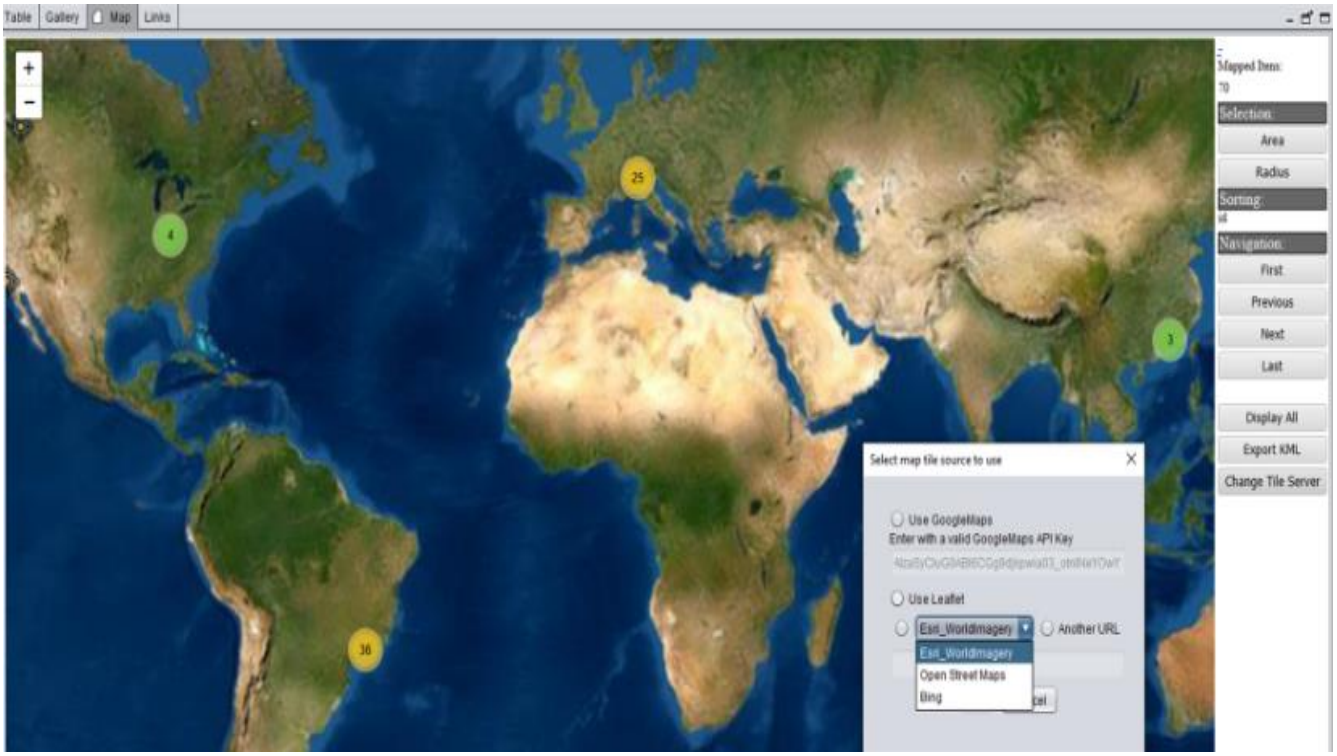


Fig. 4. Location

5 METHODOLOGY

- Literature review: Conduct a comprehensive review of existing research on social media-based expertise evidence, including current methodologies and best practices.
- Data collection and preprocessing: Gather relevant user-generated content from various social media platforms, including Twitter, LinkedIn, Facebook and Reddit, and preprocess the data for further analysis.
- NLP and sentiment analysis: Apply NLP [1] techniques to extract relevant information from user-generated content and use sentiment analysis [7] to assess the credibility of expertise claims and user endorsements.
- Network analysis: Analyze the relationships between users and their connections within professional networks to evaluate the influence and trustworthiness of expertise claims.
- Model development: Integrate the insights gained from social media analysis into a predictive model for assessing expertise levels in professional networking platforms.

This project will aim to propose a GUI for the argumentation analytics of social media content, taking advantage of the Large Language Models for argument relations prediction.

Social Media Case Investigation on:

- Analysis
- Information Bases
- Online Preservation and Collection
- Admissibility

The project will follow a multi-pronged approach:

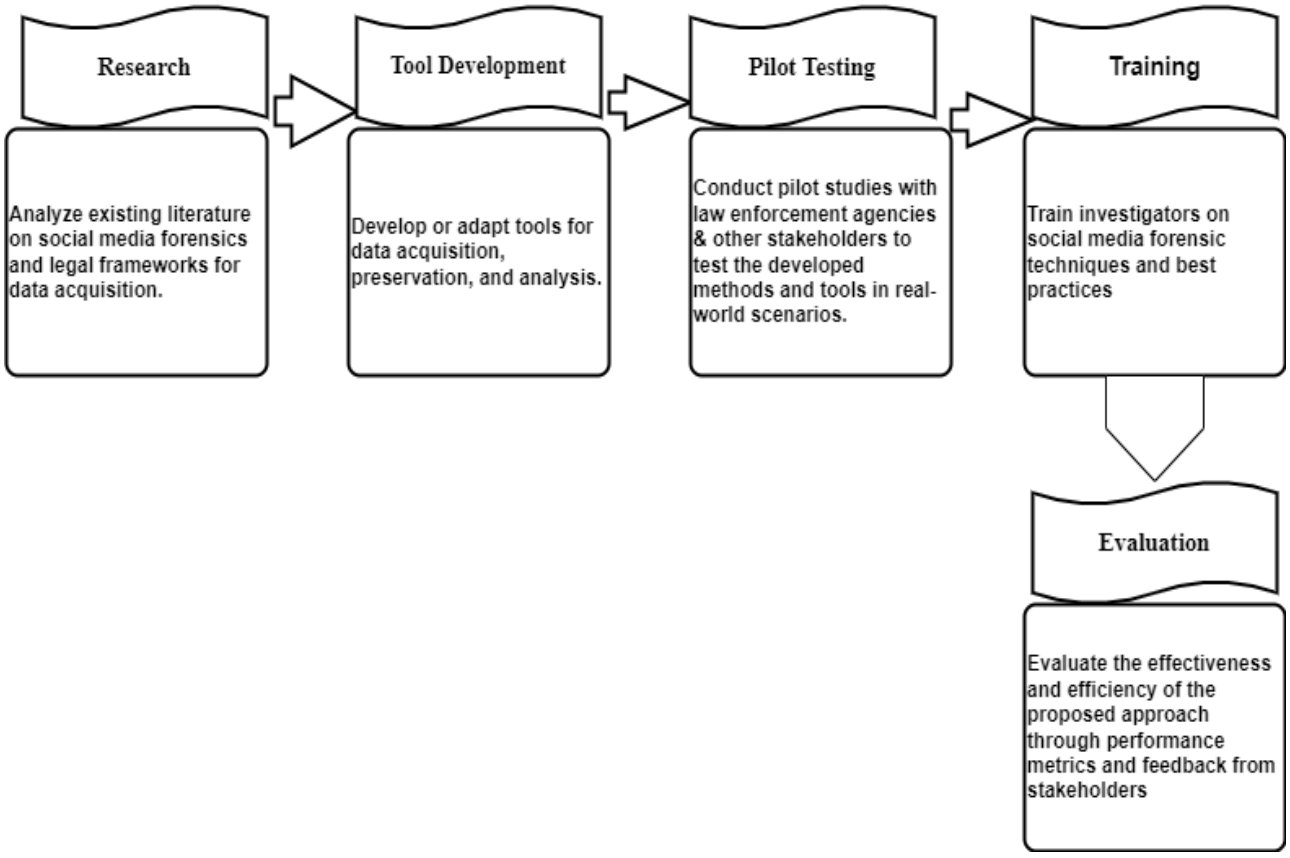


Fig. 5. Flow Chart of Methodology

6 EXPERIMENTAL SETUP

Social Media Harvesting Tools [12]: This tool is used to allow users to collect and analyze data from social media platforms through Hootsuite Insights, NetBase, and Social Bearing. The main objective of Social media harvesting tools to collect and store data from social media platforms for retrieve copies of public web pages removed in the past.

Online Preservation & Collection: Capture of dynamic content like video, audio, text, and animation. Capture of large size content and scrolling content, application & application data. To maintain the accuracy of the collection and proper documentation on consistent and repeatable methods used for capturing and securing content. Missing Metadata or references to authenticate.

7 LIMITATIONS AND CONSIDERATIONS

The IT Act [9] can have implications for collecting and handling electronically stored information (ESI) during legal proceedings or investigations involving electronic evidence.

- SECTION 43A & SECTION72A: This provision deals with data protection and privacy which govern the handling of personal and sensitive information and prescribe penalties for unauthorized access, disclosure, or misuse of such data. These provisions can be relevant when collecting, procession, and producing ESI during e-discovery, as privacy considerations and data protection obligations must be upheld.
- Cybercrimes and digital evidence: The IT Act addresses various cyber offenses, including hacking, identity theft, data theft, and unauthorized access to computer systems. When such offenses are committed, electronic evidence collected during e-discovery may be crucial in identifying and prosecuting the offenders. The IT Act provides a legal framework for investigating and prosecuting cybercrimes, and the electronic evidence collected can be presented in court to support the charges.
- Admissibility of electronic evidence: Section 65B of the Indian Evidence Act, which is often considered in conjunction with the IT Act, addresses the admissibility of electronic records as evidence. It sets certain requirements for the certification and production of electronic evidence in court. Compliance with the provisions of Section 65B is crucial to ensure the admissibility of electronic evidence during legal proceedings.

8 EXPECTED OUTCOMES

- An efficient methodology for extracting relevant information from user-generated content on social media platforms.
- A sentiment analysis framework for assessing the credibility of expertise claims and user endorsements on social media.
- Insights into the relationships between users and their connections within professional networks.
- A robust predictive model for assessing expertise levels in professional networking platforms based on social media data.

9 TECHNOLOGY STACK

Programming Languages: Python, JavaScript, PHP

Frameworks: PHP/HTML/CSS

Libraries: TensorFlow/PyTorch (machine learning), SpaCy (NLP), Scrapy (web scraping), panda

Databases: My SQL, Mongo

APIs: Different API for Social Media sites Twitter API, LinkedIn API, Facebook API etc.

Table 1. Phase of Implementation

Activity / Task	Description
Literature review	Conduct a comprehensive review of existing research on social media-based expertise evidence, including current methodologies and best practices.
Project plan development	Create a detailed project plan outlining the research objectives, methodology, and expected outcomes.
Data collection and Preprocessing	Gather relevant user-generated content from various social media platforms, including Twitter, LinkedIn, GitHub, and Reddit, and preprocess the data for further analysis.
Implementation of NLP	Apply advanced NLP techniques to extract relevant information from user-generated content on social media platforms.
Sentiment Analysis	Develop a sentiment analysis framework to assess the credibility of expertise claims and user endorsements on social media.
Network analysis	Analyze the relationships between users and their connections within professional networks to evaluate the influence and trustworthiness of expertise claims.
Development	Integrate the insights gained from social media analysis into a predictive model for assessing expertise levels in professional networking platforms.
Testing and Refinement	Evaluate the performance of the predictive model using relevant metrics and refine the model as needed.
Dissemination	Present the project results at conferences, workshops, or other relevant forums, and submit the final report to the institution or other interested stakeholders.
Documentation and archival	Properly document and archive all project materials, data, and outcomes for future reference and use.

Table 2. Risks and Mitigations

Risk	Likelihood	Impact	Mitigation Strategy
Data Privacy Concerns	High	High	Implement strict data anonymization and compliance with GDPR
API Access Restrictions	Medium	Medium	Develop backup web scraping methods, negotiate with platforms
Model Accuracy	Medium	High	Continuous model training and validation, incorporate feedback
User Adoption	Medium	Medium	Comprehensive user training and support, intuitive UI design
Technical Challenges	Medium	High	Regular technical reviews, employ experienced developers

10 CONCLUSION

Social media platforms serve as rich sources of evidence and intelligence, and investigators and analysts can effectively harness the power of social media for informed decision-making and investigative purposes. Digital forensic analysis of social media platforms is critical for investigating crimes in the digital age. This project offers a comprehensive approach to address current challenges and empower law enforcement with advanced investigative tools. By enhancing evidence collection and analysis, this project will contribute to a safer and more secure online environment.

REFERENCES

[1] Shahbazi Z, Byun Y-C, «NLP-based digital forensic analysis for online social network based on system security» Int J Environ Res Public Health 19: 7027. (2022) https://doi.org/10.3390/ijerph19127027.

[2] Khan AA, Zhang X, Hajjej F, Yang J, Ku CS, Por LY ASMF, Ambient social media forensics chain of custody with an intelligent digital investigation process using federated learning. Heliyon. 10 (1): e23254. https://doi.org/10.1016/j.heliyon.2023.e23254. (ISSN 2405-8440), (2024).

[3] Pour MS, Nader C, Friday K, Bou-Harb E, «A comprehensive survey of recent internet measurement techniques for cyber security», Comput Secur. 128: 103123. (2023) https://doi.org/10.1016/j.cose.2023.103123. (ISSN 0167–4048).

[4] Bandr F, « Digital forensics: crimes and challenges in online social networks forensics», J Arab American Univ. 6 (1): 2., (2020), https://digitalcommons.aaru.edu.jo/aaup/vol6/iss1/2.

[5] Horan C, Saiedian H, « Cyber crime investigation: landscape, challenges, and future research directions», J Cybersecur Priv 1: 580–596., (2021) https://doi.org/10.3390/jcp1040029.

[6] Arshad H, Jantan and A, Omolara E, « Evidence collection and forensics on social networks: Research challenges and directions.», Digit Invest. 28: 126–138. (2019) https://doi.org/10.1016/j.diin.2019.02.001. (ISSN 1742–2876).

[7] Dang NC, Moreno-García MN, De la Prieta F, «Sentiment analysis based on deep learning: a comparative study». Electronics 9: 483. https://doi.org/10.3390/electronics9030483.

[8] Nihal Shaikh and Dhaval M Chudasama, «Research on Cyber Offenses under Information Technology Act, 2000», May 2021 May 20218 (1): 2021 DOI: 10.37591/RTPC.

[9] Shikha Panwar, Dr. Mona Purohit Information Technology Act 2000: Overview, IJCRT | Volume 6, Issue 1 January 2018 | ISSN: 2320-2882, https://ijcrt.org/download.php?file=IJCRT1705227.pdf

[10] Dr. Swapnil Sudhir, Dr. Harita Swapnil, «IN-BUILT CHALLENGES FOR INFORMATION TECHNOLOGY LAW IN INDIA», International Journal of Advanced Research (2016), Volume 4, Issue 6, 652-657, https://www.journalijar.com/uploads/973_IJAR-10800.pdfw.

[11] Robert Slonje, Peter K. Smith, Ann Frisén «The nature of cyberbullying, and strategies for prevention», Computers in Human Behavior Volume 29, Issue 1, January 2013, Pages 26-32, https://www.sciencedirect.com/science/article/abs/pii/S0747563212002154.

[12] Man-pui Sally Chan, Alex Morales, Mohsen Farhadloo, Ryan Joseph Palmer, Dolores Albarraci.

[13] Murtaza Ahmed Siddiqi, Wooguil, Moquddam A. Siddiqi, «A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures», Appl. Sci. 2022, 12 (12), 6042; https://doi.org/10.3390/app12126042.

[14] Justin P. Murphy and Adrian Fontecilla,« Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues», Journal of Law and Technology, ISSN: 1091-7322, Volume 19, Issue 3 (2013), https://scholarship.richmond.edu/jolt/vol19/iss3/4/.

[15] H. Md and M. Warnier, Cyber Crime in Privately Held Information Systems: Personal Data at Stake, IEEE, 2014.