

Digital Forensic Framework for Social Media Crime Investigation using Authentication Technique to Preserve Digital Evidence Integrity

Rakhi Sunhare¹ & Dr. Yasmin Shaikh²

^{1,2}International Institute of Professional Studies, DAVV, Indore (M.P.)-INDIA

Abstract—With the rapid growth of social networking platforms, criminals increasingly exploit these environments to carry out illegal activities. The evidence associated with such crimes is often stored in cloud-based systems, where it can be easily altered or deleted. As a result, digital crime investigations have become more challenging due to the massive volume of data, varied data formats, multiple data sources, the volatile nature of digital evidence, and the limitations of traditional digital forensic frameworks, models and tools. To ensure that digital evidence remains reliable and legally admissible, it must be collected using a validated and approved forensic process that preserves its integrity. Consequently, there is a critical need to develop a digital forensic framework tailored specifically to online social networks in order to support effective investigations and obtain high-quality evidence.

The findings indicate that studies in existing literature focus mainly on general investigation approaches, many of which overlap in their processes. Furthermore, there is lack of comprehensive model specifically designed to conduct investigations within social networking environments. Several existing digital forensic models address either the investigation phase or the examination phase, but fail to integrate both. In this research paper, existing digital forensic models and frameworks related to social networks are analyzed. A novel framework titled Social Media Crime Investigation Using an Authentication Technique to Preserve Digital Evidence Integrity (SMI-ATPDEI) for the investigation of digital crimes committed on social networking platforms is proposed. The proposed framework includes both investigation and examination processes for preserving the integrity of digital evidence.

Keywords: Digital Forensics, Social Media Sites (SMSs), Digital Crime, Models & Digital Evidence.

1. INTRODUCTION

The rapid growth of social media has also resulted in an increase in its use for significant criminal activities, including identity theft, money laundering, deception, online sexual harassment, piracy, illegal trading, cyber stalking, and cyber terrorism [3]. The criminals use advanced technologies to commit digital crimes. The use of advanced technology make it difficult for investigating authorities to trace the criminals. Even if the criminal is traced, appropriate digital evidence are required to prove the crime. A massive amount of digital data is being created by a single person using electronic devices and social media. Social media evidence allows for near-real-time mining of an infinite amount of profile information about a possible victim or suspect [4]. Thus, analyzing and investigating the vast volumes of digital evidence without using suitable models or processes is a challenging and time-consuming task. It is crucial to understand the social media digital forensic models and frameworks currently in practice for the sake of active research. Digital Forensic is a process of collection, identification, extraction, and documentation of digital evidence from different digital devices and then use in a court of law as legal pieces of evidence [5-6]. Researchers have proposed various models over the past few years for digital forensic investigations and

examinations, although the limitation with these models is lack of functionality to preserve the integrity of digital evidence related to social network crime. The proposed model will combine the existing traditional frameworks and models and extend them in order to form a focused investigation as well as examination of digital evidence found on social networks while preserving the integrity of evidences.

The organization of this paper is as follows. Section 2 discusses current issues in digital forensics for social networks. Section 3 discusses related work focusing on existing models and frameworks. Section 4 presents the comparison of existing models and frameworks, and Section 5 presents our proposed model. Finally, Section 6 presents our conclusion and suggests future work.

II. CURRENT ISSUES IN SOCIAL MEDIA CRIME INVESTIGATIONS

According to available literature, it is difficult to preserve the integrity of evidence and meet the standards of scientific criteria in courts. The lack of trust in the digital forensic process and the absence of a well-known set of rules for examination provide a smooth and accessible path for defence legal representatives to challenge the evidence in courtrooms. They find several ambiguities in the process of evidence acquisition, analysis, and examination, which create doubts about the accuracy and reliability of the digital evidence. There is a need of standardized digital forensic framework that is specifically tailored for the investigation of social media platforms within the forensic community. It is important that the forensic community that intends to undertake such investigations do so in a manner that does not undermine the integrity and admissibility of any digital evidence found relating to SNSs(Social Networking Sites) misuse, especially if such may be required for a criminal investigation by investigation and examination agencies.

III. LITERATURE REVIEW

This section provides a background study on online social networks and digital forensic in order to have better understanding of the concepts related to digital evidence preservance and frameworks for digital forensics.

A. Social Networking Website:

In the world of Internet, millions of people regularly visit thousands of social media sites like; Facebook, YouTube, WhatsApp, Instagram, LinkedIn, Telegram, Snapchat, WeChat. These sites play a crucial role in formal and informal communications.

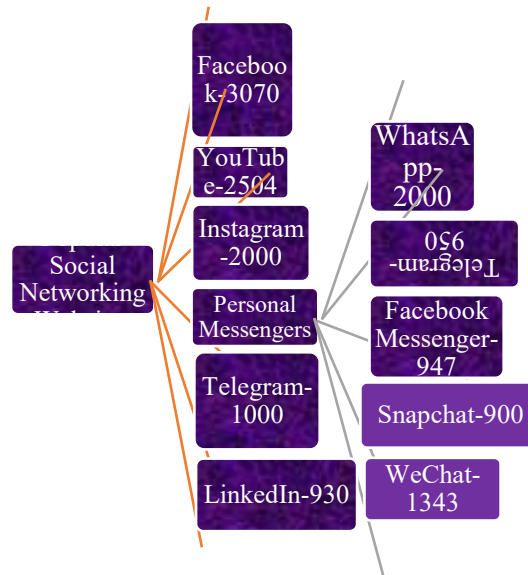


Figure 1: Popular Social Media Sites

The fundamental reason for the success of social networking is the increasing popularity of the Internet. There are several types of digital crime such as in cases of identity theft, honey traps, illegal trading, cyber stalking, fake profiling, social engineering, digital arrest and many more. Most of the digital evidences of such crime are either stored on the service provider's server or on the complainant's and suspect's devices,

According to the National Investigation Agency (NIA) chief, every sixth digital crime in India is committed through social media sites. By analyzing the basic facts and conditions prevailing in India, it can be said that there is a need to bring changes in the Information Technology Act to make it more effective in dealing with digital crime. SNW's help new structures of social communication, conversation, exchange and collaboration. They allow millions of users and institutions worldwide to exchange ideas, post updates and comments or participate in activities and events, while sharing their broader interests. At the same time, such a phenomenon has led to an increase in significant criminal activities by offenders who are becoming increasingly sophisticated in their attempts to deploy technology to circumvent detection [7]. Digital crime has become a critical issue over the last few decades. Factors such as age, gender, education, financial status, and prior victimization are associated with cybercrime victimization. Strong offline social networks serve as a protective factor against cyber harassment, particularly among females.

B. Digital Forensic:

Digital forensic has grown rapidly in a period of time to become an important part in many investigations in the digital world [8]. A computer forensic investigator defines computer forensics as simply the application of computer investigation and analysis techniques in the interest of determining potential legal evidence. INTERPOL defines digital forensic as digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically. [9].

Digital Forensic Investigation (DFI) is the process that explores digitally committed crimes

and intends to identify the culprit. Digital evidences play prominent role in the the process. Digital evidences are fragile in nature and can be easily destroyed, damaged and might be altered if unfortunately handed over to any surplus entity. In DFI, various available models focus on different aspects of digital evidence acquisition and analysis. Some focus mainly on data extraction. Others tend to be more concerned with the analysis of the data extracted from the digital media. There is an acute need for approaching digital forensic investigations in an integrated and formal manner that allows a flexible approach towards the changing environments of digital forensics, yet maintaining a strict procedural line to satisfy the courts in their scrutiny of the evidence. Not only is the evidence itself important in a digital forensic investigation, but the process followed in acquiring the evidence before final presentation is crucial.

Therefore, it is highly significant to use a systematic approach for digital forensic investigations to resolve cyber-crimes in SNSs, and to make sure that the valid digital evidence can be used in a court of law.

C. Digital Forensic Models & Frameworks:

In the past few years, several scientific communities have suggested several theories for digital crime investigations; these theories are needed to satisfy the legal and scientific demands to justify the facts derived from digital evidence [10]. The digital forensics investigators have to deal with volumes of data that are becoming increasingly large and distinct. Digital Forensic Frameworks and Models are used for examination and analysis of digital evidence [11-12].

Several forensic investigation models and structures have been proposed by various agencies, research communities, organizations and scientists for forensic investigation of digital crime [13-20]. The study of existing models revealed certain issues related to digital investigation. First, the proposed models are basically reforms of erstwhile models, with some improvements. Secondly, some of the models are generic and do not focus on the purpose of the digital investigation. There are various models and frameworks that have been defined and considered to ensure that the forensic data is valid and valuable in legal matters. The primary purpose of these models is to give guidelines for evidence gathering for human investigators. Likewise, some prior investigation process models are inappropriate for gathering evidence from social networks. SMS investigation models are limited in scope and do not cover all aspects of SMS investigation and digital evidence collection procedures.

The author proposed a model called Integrated Computer Forensic Investigation Process Model for computer crime investigation. This model includes eight phases namely readiness, identification, incident response, collection, examination, analysis, presentation and incident closure. This model has a generalized method that can be applied by non-technical observers [21]. Social networking has only been the subject of limited investigation process frameworks/models, including: The provenance management concept is taken into consideration when designing the multilayer semantic framework for OSN forensics. The framework is made up of four layers: Acquisition Layer, Knowledge Layer, Analysis Layer, and Interface Layer. The main objective is to collect and manage all relevant data and metadata. The goal is to preserve transparency in automated analysis procedures to avoid the disadvantages of data mining approaches. Despite this, there is no open way to preserve attribution [22].

David A et al, proposed a Framework for checking users' live activity on social media. This

framework is divided into four phases: Capture, Identify, Process, and Present. The command-line interface (CLI) is built around a command-line process used by investigators to conclude and assign actions to a user. It is not an easy task for investigators to use it [23]. Arshad H et al proposed a formal knowledge model for online social network forensics to explain the forensic process for social networks. This model aims to formulate a theoretical model to explain the evidence finding and analysis process by automated methods, and proposes an event-based knowledge model for automated forensic analysis of online social network data to retrieve evidence. This knowledge model is implemented through ontology [24].

In general observation, the investigation agencies face difficulty in preserving the integrity of evidence and meeting the standards of scientific criteria in courts. The lack of trust in the digital forensic process and the absence of a well-known set of rules for a smooth examination and an accessible path for the defence legal representative to challenge the evidence in courtrooms. Several ambiguities in the process of evidence acquisition, analysis and examination are found that create doubt on the accuracy and reliability of the digital evidence. Currently, it does not appear to be a commonly available digital forensic framework for the forensic community specifically aimed at the digital forensic investigation of SMS's. It is important that forensic community that intend to undertake such investigations do so in a manner that does not undermine the integrity and admissibility of any digital evidence found relating to SMS's misuse, especially if such may be required for a criminal case. However, there are limited number of models that have been specifically built with digital forensic investigation of SMS's but in contrast, digital crimes related to these networks are growing rapidly.

IV. ANALYSIS OF EXISTING MODELS

Several authors have suggested digital forensic investigation models and frameworks for social media sites. The existing models and frameworks are discussed in the previous section. In this section, specific digital forensic investigation models are analyzed and compared using some important parameters. The results are shown in the Table-1:

Table 1-Comparison of Models & Frameworks using Some Parameters

S. N	Model/ Framework Names	Branch Name	Identification Phase	Authentication Phase	Collection Phase	Preservation Phase	Analysis Phase	Examination Phase	Documentation Phase	Phase Reporting	Presentation	Decision Phase	Review Phase	Chain of custody report	Complexity Phase	Remark
1	An Extended Model of Cybercrime Investigations (2004)	Model	✓		✓	✓	✓	✓	✓							
2	Digital Forensic Model Based on Malaysian Investigation Process (2009)	Model	✓					✓		✓						
3	Integrated Computer Forensics Investigation Process Model (ICFIPM) (2016)	Model			✓		✓	✓		✓				✓		
4	Digital Forensic Investigation and Verification Model for Industrial Espionage (2019)	Model	✓		✓		✓	✓		✓				✓		
5	Multilayer Semantic framework for OSN forensics (2019)	Frame work	✓		✓		✓	✓		✓				✓		
6	Social Media User Relationship Framework (SMURF) (2020)	Frame work	✓		✓			✓	✓	✓						
7	Two-Stage Model for Social Network Investigations (2020)	Model	✓		✓		✓	✓		✓						
8	Formal knowledge model for online social network forensics (2020)	Model	✓		✓	✓		✓		✓						
9	OSN digital forensic investigation models	Model	✓	✓	✓	✓		✓		✓				✓		

As a result of the studies conducted on existing social media digital forensic models and frameworks, several critical issues have emerged that warrant discussion. Most of the proposed models and frameworks tend to follow generalized processes and exhibit a common structure. Consequently, they often fail to comprehensively address the wide range of current issues and challenges associated with digital forensic investigations.

These studies indicate that in order to develop a standardized model, it is essential to incorporate new features that can be utilized concurrently during both investigation and examination phases. Based on the above analysis, it becomes evident that there is a pressing need to design a standard digital forensic framework tailored specifically for the collection and examination of digital evidence related to crimes originating from social media platforms. This framework must also align with the newly enacted laws in the country.

V. Experimental Setup and Data Acquisition Using Commercial Tools

For the practical experimentation, two mobile devices - an iPhone 13 Pro and a Samsung SM-T255 were selected based on the popularity and widespread use of their respective operating systems. To ensure experimental reliability and eliminate remaining data, each device was subjected to seven factory resets. Subsequently, a controlled and standardized dataset was created on both devices for the purpose of forensic analysis.

The controlled dataset comprised multiple social media accounts, including three Facebook accounts, one WhatsApp account, and one Instagram account. A total of 1,200 application usage log records were generated, of which 1,000 were associated with Facebook, while WhatsApp and Instagram contributed 100 records each. Text-based communication data, encompassing SMS/MMS messages as well as messages exchanged through social media applications, amounted to 800 records in total. Among these, Facebook accounted for 500 messages, whereas WhatsApp and Instagram each contributed 150 messages.

Call log data were also generated to analyze communication patterns, with 100 call records collected from each of the three platforms - Facebook, WhatsApp, and Instagram - resulting in a total of 300 call log entries. Additionally, multimedia data in the form of photos and videos were collected uniformly across platforms, with 100 items obtained from each application, yielding a total of 300 multimedia files.

Furthermore, a substantial volume of data was extracted directly from social media applications. This included posts, comments, likes, shares, user profile information, and application-stored artifacts such as cached images and temporary files. In this category, 700 records were collected from Facebook, while WhatsApp and Instagram each contributed 150 records, resulting in a total of 1,000 items. Instances of forwarding and sharing other users' data were also identified, with 10 occurrences from Facebook and 5 occurrences each from WhatsApp and Instagram, totaling 20 records. Finally, unauthorized access events were deliberately introduced and documented across all three platforms, with one instance recorded for each application, resulting in a total of three unauthorized access cases.

After adding the above dataset to the social media accounts using the selected devices, a subset of data was deliberately deleted from all devices to simulate real-world user behavior and support forensic recovery analysis. As summarized one Facebook social media account was deleted, while no account deletions were performed on WhatsApp or Instagram. A total of 200 application usage log records were removed, comprising 100 records from Facebook and 50 records each from WhatsApp and Instagram, 100 text-based messages -including SMS/MMS and messages exchanged through social media applications - were deleted, of which 50 belonged to Facebook and 25 each to WhatsApp and Instagram. Call log deletions accounted for 50 records in total, including 22 from Facebook, 20 from WhatsApp, and 8 from Instagram, reflecting varied communication activity across platforms. Additionally, 50 multimedia items in the form of photos and videos were deleted, with 30 items from Facebook and 10 items each from WhatsApp and Instagram.

Further, 117 records related to social media application data such as posts, comments, likes, shares, user profiles, cached data, and temporary files - were deleted. Among these, Facebook contributed 80 records, WhatsApp 25 records, and Instagram 12 records. Instances of forwarding and sharing other users' data were also removed, totaling 10 records, including 5 from Facebook, 3 from WhatsApp, and 2 from Instagram. Finally, one unauthorized access record was deleted from Facebook, while no such deletions were observed for WhatsApp and Instagram. This controlled deletion process enabled the evaluation of forensic tools and techniques for recovering and analyzing deleted social media artifacts.

In the field of digital forensics, mobile device - specific data extraction and analysis were carried out using widely accepted commercial forensic tools, namely Cellebrite Physical Analyzer (UFED) version 7.72.0.10 and XRY Forensic version 10.10. These tools were employed to acquire, examine, and analyze social evidence from mobile devices in a forensically sound manner. The outcomes of the comparative analysis are summarized and presented as follows:

1. **iPhone 13 Pro:** Social media-related digital evidence from the iPhone 13 Pro was acquired using the Cellebrite Physical Analyzer (UFED) version 7.72.0.10 forensic tool is depicted in Figure 1.

Type	Included in report	Total
Activity Service Data	712	712
Aggregated Application Usage	2206	2206
Applications Usage Log	17671 (101 Deleted)	17671 (101 Deleted)
Autobill	15	15
Calendar	210	210
Call Log	758 (22 Deleted)	758 (22 Deleted)
Call Records	13 (12 Deleted)	13 (12 Deleted)
Chats	668 (3 Deleted)	668 (3 Deleted)
iMessage	40	40
Facebook Messenger	301	301
* 100021094712285	301	301
Instagram	188	188
* 11578761166	183	183
* 38288367628	21	21
* 8880802374	1	1
* 30515209464	1	1
* 5885309885	1	1
* 3880526673	1	1
Native Messages	10	10
Emails	1	1
Snapchat	2	2
* eyw8han01001	1	1
TikTok	2	2
* 656882811203E707F18	1	1
* 656552497930643047D	1	1
WhatsApp	128 (3 Deleted)	128 (3 Deleted)
* 916319217411@i.whatsapp.net	128 (3 Deleted)	128 (3 Deleted)
Contacts	15218 (7 Deleted)	15218 (7 Deleted)
Cookies	846	846
Device Connectivity	27	27
Device Events	16407	16407
Device Notifications	61	61
Devices	1	1
Emails	11	11
Installed Applications	281 (1 Deleted)	281 (1 Deleted)

Instant Messages	5		5	
Locations	8083	(571 Deleted)	8083	(571 Deleted)
Log Entries	2675		2675	
Notes	1		1	
Passwords	643		643	
Searched Items	984		984	
Social Media	883		883	
Uploads	52		52	
User Accounts	35		35	
Web Bookmarks	9		9	
Web History	2385	(1 Deleted)	2385	(1 Deleted)
Wireless Networks	249		249	
Timeline	58336	(900 Deleted)	58336	(900 Deleted)
Data Files	300932		300932	

Applications	2452		2452	
Archives	875		875	
Audio	8259		8259	
Configurations	176988		176988	
Databases	979		979	
Documents	281		281	
Exchange	32		32	
Images	83714		83714	
Text	15164		15164	
Videos	4230		4230	

Malware scanner	
Malware scan performed	False

Figure 1: Contents of iPhone 13 Pro

A graphical representation of the above data is presented in the following Figure 2.

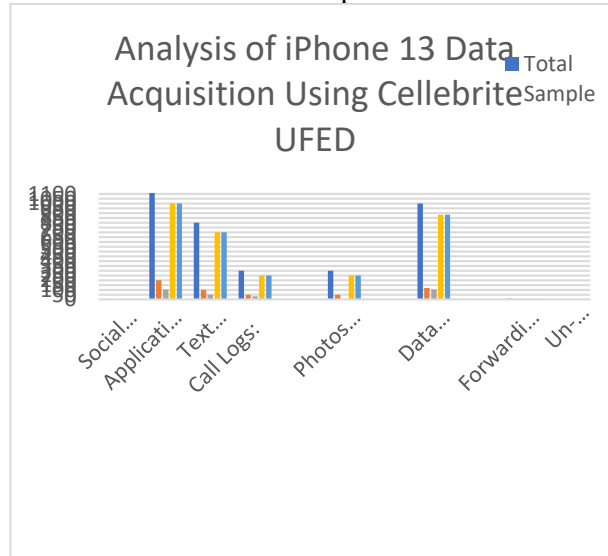


Figure 2: Acquired data Analysis of iPhone 13 Pro Using the Cellebrite Physical Analyzer (UFED) version 7.72.0.10

2. **Samsung SM-T225 Tablet:** Social media-related digital evidence from the 2. Samsung SM-T225 Tablet was acquired using the Cellebrite Physical Analyzer (UFED) version 7.72.0.10 forensic tool and is depicted in Figure 3.

Type	Included in report	Total
Applications Usage Log	7942 (99 Deleted)	7942 (99 Deleted)
Call Log	197	197
Chats	329 (1 Deleted)	329 (1 Deleted)
Facebook	7	7
@1581832217579	3	3
@1582159412365	4	4
Facebook Messenger	8	8
@1581832217579	2	2
@1582159412365	6	6
Instagram	1	1
77775639725	1	1
Native Messages	6	6
WhatsApp	307 (1 Deleted)	307 (1 Deleted)
@15825440859@w.whatsapp.net	307 (1 Deleted)	307 (1 Deleted)
Contacts	3704 (41 Deleted)	3704 (41 Deleted)
Cookies	204	204
Device Events	176	176
Device Notifications	1029	1029
Device Users	1	1
Emails	1	1
Installed Applications	215 (1 Deleted)	215 (1 Deleted)
Instant Messages	1	1
Locations	3	3
Network Usages	1829	1829
Notes	1	1
Passwords	247	247

Searched Items	30	30
Social Media	110	110
User Accounts	35	35
User Dictionary	2082	2082
Web Bookmarks	3	3
Web History	45	45
Wireless Networks	6	6
Timeline	17785 (99 Deleted)	17785 (99 Deleted)
Data Files	52077 (8 Deleted)	52077 (8 Deleted)
Applications	7415	7415
Archives	222	222
Audio	182	182
Configurations	157	157
Databases	806	806
Documents	9	9
Exchange	2515	2515
Images	30192 (8 Deleted)	30192 (8 Deleted)
Text	4527	4527
Videos	52	52

Malware scanner	False
-----------------	-------

Figure 2: Contains of Samsung SM-T225 Tablet

A graphical representation of the above data is presented in Figure 4:

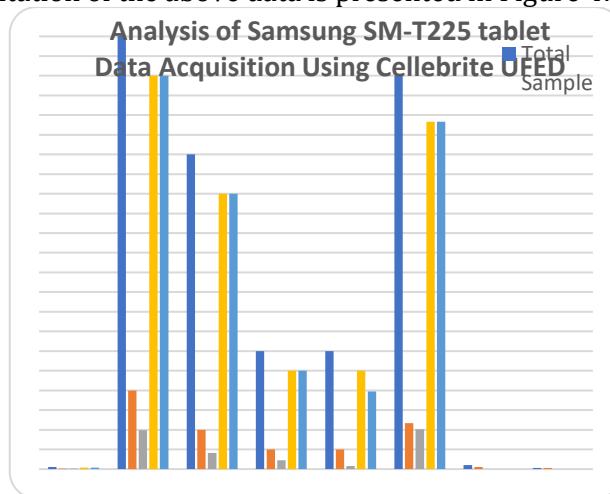


Figure 4: Acquired data Analysis of Samsung SM-T225 tablet Using the Cellebrite Physical Analyzer (UFED) version 7.72.0.10

3.iPhone 13 Pro: Social media-related digital evidence from the iPhone 13 Pro was acquired using the XRY 10.10 Forensic tool and is depicted in Figure 5

Categories	Artifacts	Deleted artifacts
Device / Network information	14	
Device / Event log	1	
Device / Installed apps	1050	
Device / Prescan	13	
Health / Log	610	
Security / Accounts	18	
Security / Secure storage	370	
Contacts / Contacts	383	
Contacts / Social groups	148	
Calls	18	
Organizer / Calendar events	219	
Messages / SMS	11	
Messages / Emails	14	
Messages / Chat	657	12
Places / Other	12431	
Places / Visited	82	
Web / History	149	
Web / Bookmarks	9	
Web / Searches	100	
Web / Cookies	43	
Files & media / Pictures	1938	
Files & media / Audio	22	
Files & media / Videos	32	
Files & media / Documents	4	
Files & media / Archives	16	
Files & media / Databases	2994	
Files & media / Readable files	23517	
Files & media / Unrecognized	1459	
User activity log / App activity	114	

Figure 5: Contains of iPhone 13

A graphical representation of the above data is presented in Figure 6

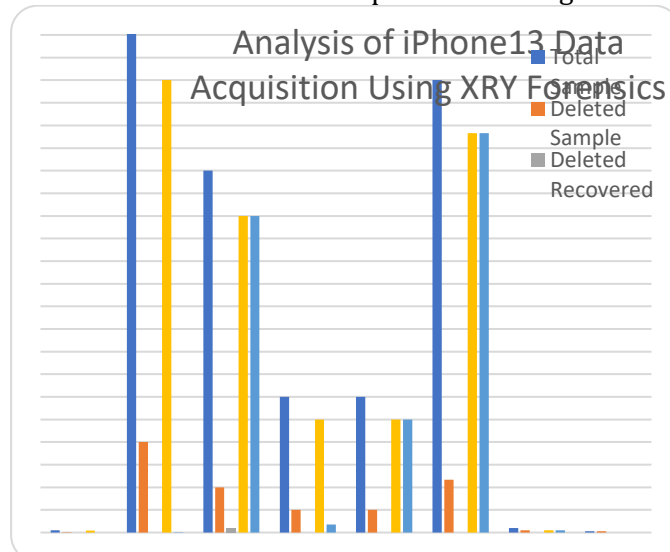


Figure 6: Acquired data Analysis of iPhone13 Using XRY Forensics

A graphical representation of the above data is presented in Figure 6

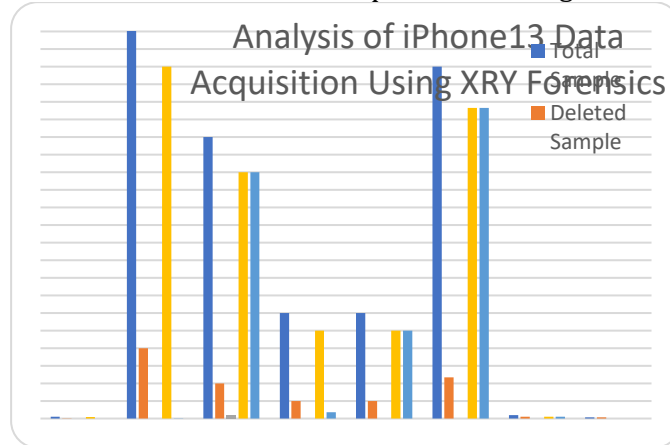


Figure 6: Acquired data Analysis of iPhone13 Using XRY Forensics

4. **Samsung SM-T225 Tablet:** Social media-related digital evidence from the Samsung SM-T225 Tablet was acquired using the XRY 10.10 forensic tool and is depicted in Figure 7.

Summary	
Date Created	27-10-2025 16:04:58 UTC+05:30
Locked	No
Manual Device Selection	Yes
Extraction Media	Cable
XRY Version	10.10
Lowest Module Version	10.10
File GUID	{4BB69178-C454-439A-8769-037D0F064D4B}
XryCore Version	1.0.157
Extraction result	Finished with warnings
Is File Subset	No
Is Encrypted	Yes
Extraction Action	Logical (Full read)
Decode Action	Logical (Full read)
Encryption level	AES-56
Is password protected	No

Categories	Artifacts
Device / Network information	0
Device / Event log	507
Device / Installed apps	349
Device / Device accounts	1
Device / Prescan	6
Security / Accounts	2
Contacts / Contacts	7
Calls	3
Messages / SMS	10
Files & media / Pictures	69360
Files & media / Audio	565
Files & media / Videos	47
Files & media / Documents	54
Files & media / Archives	1940
Files & media / Databases	14
Files & media / Application binaries	3148
Files & media / Readable files	6222
Files & media / Unrecognized	179725

Figure 7: Contents of Samsung SM-T225 Tablet

A graphical representation of the above data is presented in Figure 8:

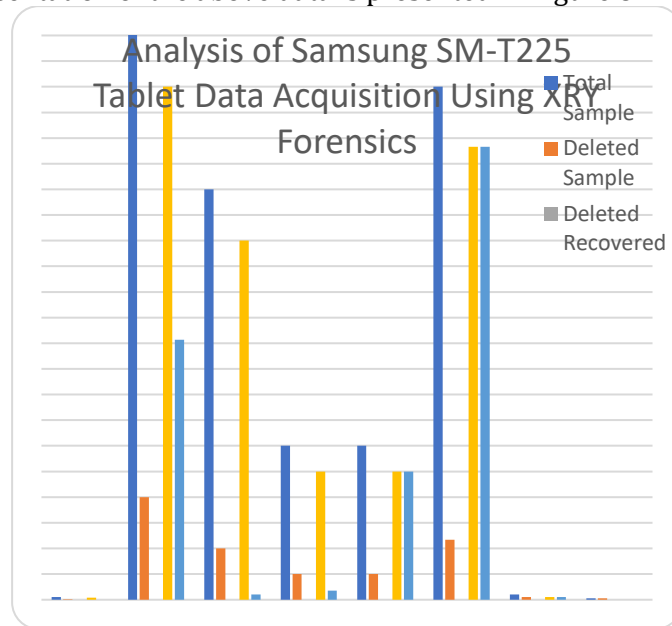


Figure 8: Acquired data Analysis of Samsung SM-T225 Tablet Using XRY 10.10. Forensics

5. iPhone 13 Pro: Social media-related digital evidence from the iPhone 13 Pro was acquired using the MOBILedit Forensic tool are shown in Figure 9:

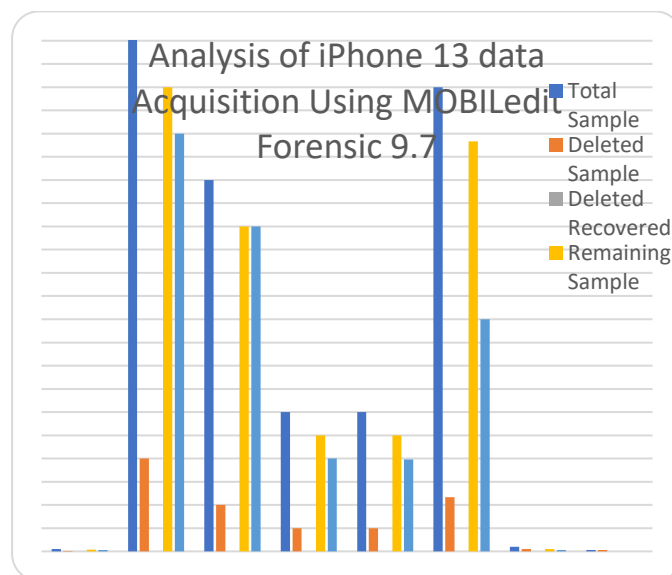


Figure 9: Acquired data analysis Using MOBILedit Forensic.

6. Samsung SM-T225 Tablet: Social media-related digital evidence from the iPhone 13 Pro was acquired using the MOBILedit Forensic tool are shown in the Figure 10:

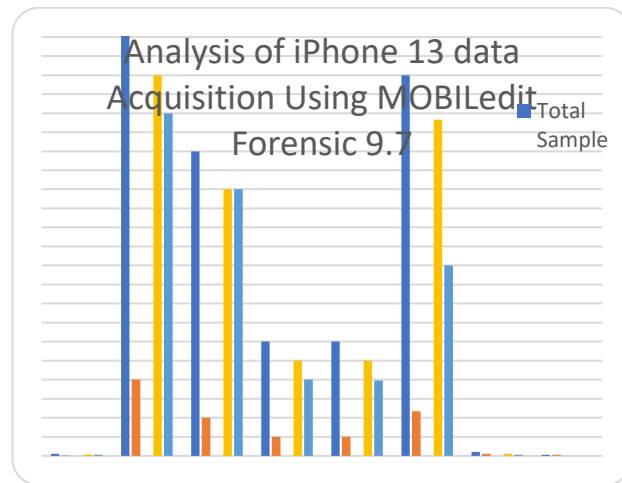


Figure 10: Acquired data and analysis Using MOBILedit Forensic.

VI. Tool Wise Comparative Analysis

The comparison of all three tools for data extraction is shown below:

1. **iPhone 13 Pro:** A comparative analysis of the iPhone 13 data acquisition results obtained using different forensic tools was conducted. The comparative results are presented in Table 2-

Table 2: Comparison of Samsung SM-T225 acquisition data result from different tool

iPhone 13 Pro	Commercial Cellebrite Analyzer (UFED) version		XRY 10.10 Forensic		MOBILedit Forensic 9.7	
Mobile Brand	iPhone 13		iPhone 13		iPhone 13	
Model	N104AP		N104AP		N104AP	
IMEI No	359564036422832					
Logical Extraction	Yes		Yes		Yes	
File System Extraction	Yes		No		No	
Physical Extraction	Yes		No		No	
	Remaining Recovered	Deleted Recovered	Remaining Recovered	Deleted Recovered	Remaining Recovered	Deleted Recovered
Social Media	4	1	0	1	3	0
Accounts						
Application Usage	1000	101	1	200	900	0
Text Messages (SMS/MMS messages and messages sent through social media apps)	700	50	700	100	700	0
Call Logs: (Phone records can show who a suspect has been in contact with, especially if linked to specific social media activities)	250	32	18	50	200	0
Photos and Videos: (These can be evidence of events, locations, or communications related to social media activity)	250	0	250	50	198	0
Data from Social Media Apps: (This includes posts, comments, likes, shares, and user profiles, as well as any data stored by the application, like cached images or temporary files)	883	101	883	117	500	0
Forwarding/sharing other user data	5	5	5	5	3	0
Un-Authorized Access	0	0	0	3	0	0

2. **Samsung SM-T225:** The Samsung SM-T225 mobile acquisition data results were compared using different forensic tools. Table 3 presents the comparative results-

Table 3: Comparison of Samsung SM-T225 acquisition data result from different tool

Samsung SM-T225	Commercial Cellebrite Physical Analyzer (UFED) version 7.72.0.10		XRY 10.10 Forensic		MOBILedit Forensic 9.7	
Mobile Brand	Samsung		Samsung		Samsung	
Model	SM-T225		SM-T225		SM-T225	
IMEI No	359364036422832					
Logical Extraction	Yes		Yes		Yes	
File System Extraction	Yes		No		No	
Physical Extraction	Yes		No		No	
	Remaining Recovered	Deleted Recovered	Remaining Recovered	Deleted Recovered	Remaining Recovered	Deleted Recovered
Social Media	4	1	0	0	0	0
Accounts						
Application Usage	1000	99	507	0	0	0
Logs						
Text Messages (SMS/MMS messages and messages sent through social media apps)	700	41	10	0	800	0
Call Logs: (Phone records can show who a suspect has been in contact with, especially if linked to specific social media activities)	250	33	18	0	18	0
Photos and Videos: (These can be evidence of events, locations, or communications related to social media activity)	197	08	250	0	240	0
Data from Social Media Apps: (This includes posts, comments, likes, shares, and user profiles, as well as any data stored by the application, like cached images or temporary files)	883	101	883	0	880	0
Forwarding/sharing other user data	0	0	5	0	5	0
Un-Authorized Access	0	0	0	0	0	0

The data in Table 2 and Table 3 presents the examination and analysis report of the iPhone 13 Pro and Samsung SM-T225, conducted using three commercial mobile forensic tools: Cellebrite Physical Analyzer (UFED) version 7.72.0.10, XRY 10.10 Forensic, and MOBILedit Forensic version 9.7. The commercial tool Cellebrite Physical Analyzer (UFED) version 7.72.0.10 extracted all the data from the both phones and supports physical as well as logical extraction. The analysis shows that some deleted data such as application usage logs, text messages (SMS/MMS messages and messages sent through social media apps), call logs (phone records can show who a suspect has been in contact with, especially if linked to specific social media activities) and forwarded/shared user data were also acquired but the deleted data of photos and videos (these can be evidence of events, locations, or communications related to social media activity), data from social media apps (This includes posts, comments, likes, shares, and user profiles, as well as any data stored by the application, like cached images or temporary files), un-authorized access recovered partially. However, XRY 10.10 Forensic and MOBILedit Forensic version 9.7 support only logical extraction; consequently, certain logical artifacts and all deleted data could not be recovered. Furthermore, both tools fail to present forwarded message origin ID information. In this study it found that none of the standard tools that have been considered for analysis, support all types of devices and acquire all remaining and deleted data. The origin information of forwarded messages could not be identified. The results shows that Cellebrite UFED is far better in acquiring data as compared to other two tools, XRY 10.10 Forensic and MOBILedit version 9.7.

VII. PROPOSED FRAMEWORK:

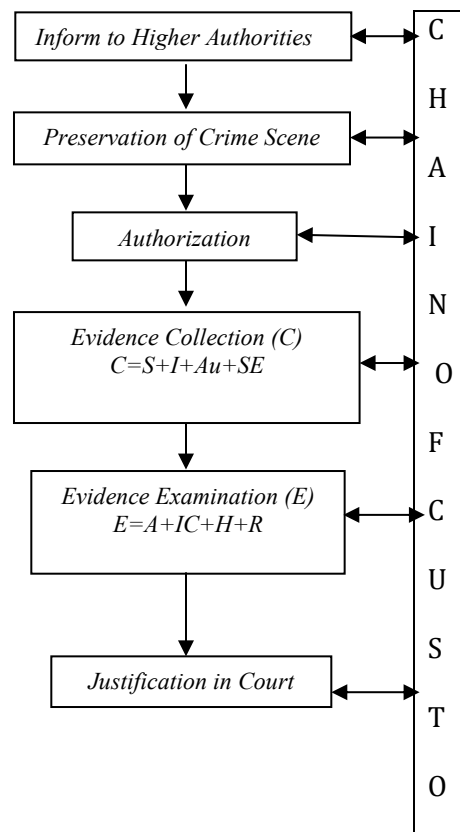
As identified in this research, one of the most significant challenges faced in the digital forensic investigation of social networking-related cases are the lack of standardization and the absence of a comprehensive theoretical framework specifically designed for social media related crimes. The dynamic nature of social media platforms, frequent changes in

application architectures, and the diversity of data formats further complicate the investigation process. In the absence of standardized procedures and a unified framework, evidence acquisition, preservation, and analysis are often inconsistent, which may adversely affect the integrity, reliability, and legal admissibility of digital evidence. Addressing this gap is therefore critical for developing effective and legally compliant social media forensic investigation framework.

On the basis of present and requirement of new criminal laws, two features of social media digital forensic investigation frameworks are identified as:

- ✓ Videography of all activities related to online and offline social media crime investigation and analysis should be made mandatory.
- ✓ There is a variety of digital data that can be obtained through a user's online social media account, and which is very useful for investigating agency.

To include these additional features and overcome existing limitations a comprehensive framework for social media crime investigation titled Social Media Crime Investigation Using an Authentication Technique to Preserve Digital Evidence Integrity (SMI-ATPDEI) is proposed as shown in Figure 11. The proposed framework focuses on systematic evidence acquisition, secure preservation, and robust analysis of social media based digital evidence, while maintaining a verifiable chain of custody and documenting any potential tampering at each stage of the investigation. By integrating technical forensic processes with legal compliance, the framework aims to bridge the gap between theoretical forensic models and practical investigative requirements, thereby enhancing the reliability, credibility, and admissibility of social media evidence in criminal investigations and judicial proceedings.



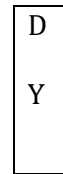


Figure-11: Social Media Crime Investigation Using an Authentication Technique to Preserve Digital Evidence Integrity (SMI-ATPDEI)

- ✓ S stand for Searching, I stand for Identification,
- ✓ Au stand for Authentication, SE stand for Secure Evidence,
- ✓ A stand for Analysis, IC stand for Integrity Check,
- ✓ H stand for Hypothesis Testing, R stand for Reporting

The details of the proposed models are as follows:

1. As soon as any information related to a social media crime is received, the forensic investigation team should take complete control of the crime scene to prevent any exchange or leakage of information. The crime scene must be secured, and simultaneously, gather as much information as possible regarding the factual circumstances of the scene. The purpose of this phase is to inform, authenticate, determine and plan the next approach that will be applied in the proceeding phases.
2. Collection: This phase involves several activities related to the investigation of online social media networks. The primary objective of this stage is to collect and preserve potential digital evidence and essential information to advance the investigation. During this phase, the following steps will be undertaken:
 - Investigating users or target profiles online, gather information about the links or connections between them that are related to the incident under investigation, as well as potential digital evidence and information associated with the user's profile.
 - Any possible digital evidence found will be collected in a digital forensic manner to make sure that the digital evidence is valid and presentable in a court of law or as a part of any other legal process.
 - If it becomes necessary to collect more detailed information and evidence from a profile or target, the above two phases will be repeated as needed.
 - Once the possible digital evidence has been recovered, it must be authenticated and stored in an appropriate storage device and sent to the forensic laboratory for examination.
3. Examination: The Analysis and Examination phase is a crucial component of the digital forensic investigation process. In this phase, the forensic investigator must verify that all digital evidence and information are directly related to the specific incident under investigation. In online social networking, digital forensics uses the following steps in digital forensic investigations-
 - Analyze the suspect's information by recording and digital evidence from the server, profile or system.
 - In some cases, it will be helpful to map connections of the suspect's profile data or network information with other suspects in order to get useful digital evidence.

4. The entire examination is over, and all the examined data are checked to determine whether they are admissible in the court of law. If not, then recheck the whole process. Hence, any document can be presented in the court is authentic and unique.

VIII. CONCLUSION

In this research paper, the main issues relating to social media crimes investigating and examination, such as long boundaries, hypothesis tests, collection of evidence, analysis of evidence, maintaining the integrity of evidence and fulfilling scientific criteria in the court are studied and analyzed. As a result of the above studies that have been conducted on social media digital forensic investigation models and frameworks that have been developed previously, there are several issues that can be discussed. Most of the models and frameworks that have been proposed are common models and frameworks with almost identical processes. In the scope of this analysis, a framework referred to as the Social Media Crime Investigation and Examination Framework, Social Media Crime Investigation Using an Authentication Technique to Preserve Digital Evidence Integrity (SMI-ATPDEI) is proposed.

This model will assist investigating officers in collecting digital evidence from social networking sites in accordance with the new laws, examining the digital evidence, and presenting it before the Hon'ble Courts without compromising its integrity, thereby maintaining the chain of custody of the digital evidence. In future the framework will be implemented and used to carry out investigations on different types of devices specifically addressing social media data.

REFERENCES

- [1] Rakhi Sunhare & Dr.Yasmin Shaikh, "Study of Security Vulnerabilities in Social Networking Websites", International Journal of Management, IT & Engineering, Vol. 9 Issue 6, June 2019, Impact Factor: 7.119
- [2] <https://datareportal.com/reports/digital-2025-global-overview-report>.
- [3] Salih K.M.M. & Ibrahim N.B. (2023), Digital Forensic Tools: A Literature Review, Journal of Education and Science, Vol. 32, No. 01, pp.-109-124, DOI: 10.33899/edusj.2023.137420.1304.
- [4] Muhammad Firdaus, Forensic Analysis of Social Media Data: Research Challenge and Directions, <https://doi.org/10.31219/osf.io/vn49u>.
- [5] Yiye J., Mustapha R., Ahmad A. M., & Bassi H (2022), Digital Forensic Investigation of Cyberstalking and Social Media Harassment using Network Forensic Analysis, JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(3), pp.1-10, www.atbuftejoste.com
- [6] Singh A, Singh S. K., Singh N. and Nayak S. K. (2022), NEED OF TECHNOSCIENCE AND DIGITAL FORENSIC IN EMERGING CRIME: A STUDY ON CYBERCRIME, YMER, VOLUME 21 : ISSUE 10 , pp-952-973, <https://ymerdigital.com>.
- [7] Montasari R., Hill R., Carpenter V. & Islamic M. (2019), "Digital Forensic Investigation of Social Media, Acquisition and Analysis of Digital Evidence", International Journal of Strategic Engineering, Volume 2, Issue 1, pp. 52-60, DOI: 10.4018/IJoSE.2019010105.
- [8] Harichandran V. S., Breitingner F. & Baggili I, (2016), "A Cyber Forensics Needs Analysis Survey: Revisiting the Domain's Needs a Decade Late", Electrical & Computer

- Engineering and Computer Science Faculty Publications, 01-10. DOI: 10.1016/j.cose.2015.10.007
- [9] Chabot Y., Bertaux A., Nicolle C., & Kechadi T. (2015), "An Ontology-Based Approach for the Reconstruction and Analysis of Digital Incidents Timelines", journal homepage: www.elsevier.com/locate/diin, pp-01-18, DOI:10.1016/j.diin. 2015.07.005.
- [10] Hargreaves C. & Patterson J. (2012), "An automated timeline reconstruction approach for digital forensic investigations, Digital Investigation", journal homepage: www.elsevier.com/locate/diin, S69-S79.
- [11] Carrier B. D. & Spafford E. H (2004), "An Event-Based Digital Forensic Investigation Framework", pp-01-12, at: <https://www.researchgate.net/publication/240788169>.
- [12] Ciardhuáin S. O. (2004), "An Extended Model of Cybercrime Investigations", International Journal of Digital Evidence, 3(1), pp-01-22, <https://www.researchgate.net/publication/220542517>.
- [13] Hargreaves C & Patterson J (2012), "An automated timeline reconstruction approach for digital forensic investigations", Digital Investigation (Elsevier Ltd.), vol. 9, pp-69-79. <https://doi.org/10.1016/j.diin.2012.05.006>.
- [14] Gupta A. (2013), "Privacy Preserving Efficient Digital Forensic Investigation Framework", IEEE, pp- 387-393, DOI:10.1109/IC3.2013.6612225.
- [15] Kebande V.K. & Ray I. (2016), "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)", IEEE 4th International Conference on Future Internet of Things and Cloud, DOI: 10.1109/FiCloud.2016.57, 356-362.
- [16] Chabot Y., Bertaux A., Nicolle C. & Kechadi M. T. (2014), "A complete formalized knowledge representation model for advanced digital forensics timeline analysis", Digital Investigation (Elsevier Ltd.), Vol.11, pp-95-105, <https://doi.org/10.1016/j.diin.2014.05.009>.
- [17] Ali M. M., Mohammed K. M. & Rajamani L (2014), "Framework for Surveillance of Instant Messages in Instant messengers and Social networking sites using Data Mining and Ontology," Proceeding of the 2014 IEEE Students' Technology Symposium, pp-297-302, 10.1109/TechSym.2014.6808064.
- [18] De Mendonça R. R, de Brito D. F., de Franco Rosa F., dos Reis J.C, & Bonacin R. (2020), "A Framework for Detecting Intentions of Criminal Acts in Social Media: A Case Study on Twitter", MDPI, Information 2020, 01-40, <https://doi.org/10.3390/info11030154>.
- [19] Arshad H., Jantan A., Hoon G. K., Butt A. S. (2019), "A multilayered semantic framework for integrated forensic acquisition on social media" Digital Investigation 29 (Elsevier), vol. 19, pp-147-158, www.elsevier.com/locate/diin.
- [20] David A., Morris S., & Thomas G. A. (2021), "Social Media User Relationship Framework (SMURF)", Journal of Digital Forensics, Security and Law, vol. 16 (1), pp.-01-30, DOI: <https://doi.org/10.15394/jdfsl.2021.1698>.
- [21] Dvid A., Morris S., & Thomas G. A. (2020), "A Two-Stage Model for Social Network Investigations in Digital Forensics", Journal of Digital Forensics, Security and Law, Vol. 15 (1), pp-01-36, <https://commons.erau.edu/jdfsl/vol15/iss2>.
- [22] Arshad H., Jantan A., Hoon G. K., & Abiodun I. O., (2020) "Formal knowledge model for online social network forensics", Computers & Security Vol. 89 (Elsevier), pp-01-11, www.elsevier.com/locate/cose.
- [23] David A., Morris S., & Thomas G. A. (2021), "Social Media User Relationship Framework (SMURF)", Journal of Digital Forensics, Security and Law, vol. 16 (1), pp.-01-30, DOI: <https://doi.org/10.15394/jdfsl.2021.1698>.

- [24]Arshad H., Jantan A., Hoon G. K, & Abiodun I. O., (2020) "Formal knowledge model for online social network forensics", Computers & Security Vol. 89 (Elsevier), pp-01-11, www.elsevier.com/locate/cose.