https://doi.org/ 10.33472/AFJBS.6.10.2024.4482-4493

Analyses of Social Media Networks Investigation in India – A Brief Overview

Bhoopesh Kumar Sharma[1*], Nitasha Singh[2], Sanyiam Beniwal[3], Mirza Tanweer Ahmad Beig[4], Pooja[5]

[1]Professor, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana – 122505*

[2,,3]Research Scholar, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana – 122505

[4]Assitant professor, Department of Physics, Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana – 122505

[5]M.Sc. Forensic Science, Department of Forensic Science, Shree Guru Gobind Singh Tricentenary University, Gurugram, Haryana – 122505

Corresponding Authors: [2]*Dr. Bhoopesh Kumar Sharma **(bhoopesh_fosc@sgtuniversity.org)**

Article History
Volume 6,Issue 10, 2024
Received:28 Apr 2024
Accepted : 25 May 2024
doi: 10.33472/AFJBS.6.10.2024.4482-4493

Abstract:
The primary purpose of social media was to facilitate communication between long-lost acquaintances and enable the exchange of personal thoughts, ideas, and insights. On the contrary, with the proliferation of social media users, a marginal alteration has occurred in the focus of the engaged audience on these platforms, transitioning from content sharing to data disclosures. The proliferation of Online Social Networks (OSNs) has facilitated global communication and interaction between individuals and organizations. Harassment of both individuals and businesses and infringements of intellectual property rights, identity theft, defamation, data privacy, and the transmission of personal information and viruses are all potential occurrences on social networking sites such as Facebook, Twitter, and LinkedIn. At the moment, there is a lack of publicly accessible business standards that are specifically designed for the computer forensic procedure of examining criminal activity on social networking platforms. The legal and computer forensic ramifications of obtaining digital evidence through social networking applications and programs are examined in this article. Additionally, the article proposes effective and comprehensive approaches to improving youth awareness regarding the detrimental consequences of cybercrime.

Keywords: Online Social Networks, Computer Forensics, Data Infringement, Legal Implications

1. Introduction:

The internet as a whole dates back to the 1960s, while the World Wide Web has existed since the 1990s. Presently, the internet is ubiquitous, influencing the lives of every individual on the planet. Electronic communication platforms—including microblogging and social networking websites—through which individuals establish virtual communities to exchange personal messages, information, and other types of content [1]. The primary purpose of social media was to facilitate communication between long-lost acquaintances and enable the exchange of personal thoughts, ideas, and insights. On the contrary, with the proliferation of social media users, a marginal alteration has occurred in the focus of the engaged audience on these platforms, transitioning from content sharing to data disclosures. For social and business interaction, social networking sites such as Facebook, LinkedIn, Myspace, and Twitter provide access to blogging, email, messaging, and photo sharing. Rapid growth has been observed in the utilization of social networking platforms by both individuals and enterprises [2]. There is an increasing trend among businesses to integrate Facebook and Twitter into their marketing strategies. While the primary purpose of social networking application usage is for personal gain, certain organizations encourage their employees to employ these platforms for work-related purposes, such as information transmission beyond the company network, which can boost productivity. Social media platforms can be utilized by personnel to establish both formal and informal relationships with external and internal information sources [3]. Conversely, certain organizations might remain entirely unaware of the potential for social networking applications to be utilized for malicious purposes. Harassment of both individuals and businesses and infringements of intellectual property rights, identity theft, defamation, data privacy, and the transmission of personal information and viruses are all potential occurrences on social networking sites such as Facebook, Twitter, and LinkedIn. The extent to which social media has significantly altered the lives of individuals for the better or for the worse is debatable. Criminal activities facilitated by social media have integrated seamlessly into our daily lives, much like the platform itself. The policy on computer utilization of an organization should specify whether social media applications are permitted for work-related purposes, so that employees are aware of the means to access these platforms. Morrison asserts that it is imperative for organizations to establish a policy that is unambiguous and forthright regarding the expectations that employees must uphold when utilizing both company-issued and personal social media accounts [3, 4, 31].

At the present time, defamation and abuse via social media misuse are two of the most prevalent illicit activities. Furthermore, both organizations and individuals are experiencing data loss due to the improper utilization of social media platforms. Cybercrime includes unauthorized system access, data manipulation, data destruction, and the plunder of intellectual property. As crime and the volume of crime-related data increase, the daily analysis of crime data becomes progressively more challenging [2,4]. A comprehensive forensic analysis of a social media account may be necessitated for a variety of reasons, including the collection of evidence for a criminal prosecution or disciplinary action against employees who violate company policies. Conversely, law enforcement agencies are inundated with a multitude of grievances originating from various social media platforms (e.g., Facebook and Twitter). The identity of the senders of these complaints frequently eludes explanation and necessitates additional inquiry.

At present, the number of universally accepted criteria for computer forensic investigations pertaining to social media networking programs is either minimal or non-existent. As per the Association of Chief Police Officers' (ACPO) in the United Kingdom, police forces conducting digital or cyber forensic investigations would consult the good practice guidelines for computer

and electronic evidence. This would provide an advantageous starting point for organizations and agencies conducting social media investigations [5]. A significant number of organizations across the globe lack guidance or direction regarding internal cyber forensic investigations, which ultimately compromises the integrity of digital evidence [6]. The prevalence of utilizing evidence obtained from social networking sites in criminal prosecutions has increased, as stated by O'Floinn and Ormerod [7]. The legal and forensic ramifications of obtaining digital evidence through the utilization of data from prominent social networking platforms are examined in this article. Additionally, the article proposes effective and comprehensive approaches to improving youth awareness regarding the detrimental consequences of cybercrime.

2. Criminal Activities Conducted Via Social Media:

Forbes estimates that there are approximately one billion social media user accounts in the world, and that these accounts connect virtually every nation on the planet. On websites such as Twitter and Facebook, users are able to communicate with one another and share information. Examples include pictures, movies, and letters sent via text message [8]. Users of social networking platforms frequently fail to remember that their privacy is put at jeopardy whenever they access the internet. This is due to the fact that a significant number of individuals refrain from utilizing the user settings of their social media accounts. The use of social media platforms can give rise to a wide range of different types of cybercrime activity. Several of these are explained in the following:

2.1 Phishing is a type of cybercrime that involves sending a bogus email that appears to be from a specific organization and asking for sensitive personal and financial information for malicious purposes. As a result, the user is deceived into disclosing their personal information, which they subsequently exploit to their advantage [9].

2.2 Identity theft: Occurrences of this nature are extremely common on social media. This type of criminal activity involves the assailant gathering confidential information about the target through social media platforms. This is done with the victim's information in order to obtain credit, loans, or other forms of financial assistance [10]. Additionally, it encompasses the compromise and theft of confidential data belonging to an organization or an individual with the intention of gaining access to their bank accounts. Such data is then utilized to perpetrate identity-based fraud against the intended victims. Four out of ten Indians have been victims of identity theft, according to an analysis in the Economic Times. The National Crime Records Bureau reports that in 2014, thirteen cases of identity theft under section 66 C and deception by personation under section 66 D of the Information and Technology Act were reported. The corresponding figures were 1545 and 1597 in 2016. In 2017, the corresponding figures for the number of reported cases were 3724 and 2296, respectively [11].

2.3 Prohibition of Obscene Content: Sharing or transmitting any form of obscene content is prohibited and punishable under section 67 of the Information Technology Act in India. Obscenity was defined by the Supreme Court of India in one of its landmark rulings as "the quality of being obscene, which signifies something that is revolting to modesty or decency; vulgar, unclean, and offensive." Additionally, the Supreme Court differentiated between pornography and obscenity [11]. Criminals also manipulate photographs discovered on social media via unauthorized accounts in order to generate explicit material, which they subsequently disseminate on the platform for amusement or retribution. This inflicts victim humiliation, defamation, and severe physical and mental harm [12].

2.4 Online Scams: In the current digital era, online scams are one of the greatest concerns. Internet-based fraudulent activities predominate when an individual's account is duplicated with the intention of acquiring personal information [13]. The individuals responsible employ the photographs and images to generate a fresh account, which they subsequently exploit to coerce family and friends into divulging sensitive data such as bank account information. As per the findings of the National Crime Reports Bureau, fraud-related offenses comprised 1,5051% of the total 27,248 cybercrime cases reported in 2018, which represents 55.2 percent of the overall cybercrime cases. The following are examples of significant online frauds: [14]

- corporate Frauds - Perpetrators perpetrate monetary frauds by intercepting corporate emails.
- Unauthorized online transactions can occur from a card-holder's bank accounts using debit or credit cards, e-wallets, or SIM swap fraud, without their knowledge or consent [13, 14].
- Vishing / Fraud Calls - In these instances, the target is contacted by deceptive phone calls, typically posing as their bank, with whom they hold accounts. The caller assumes the identity of a well-informed and trustworthy employee of a bank. This is done with the intention of acquiring the recipient's personal information, including Unique ID, Customer ID, Net Banking Password, ATM PIN number, One Time Passwords (OTPs), Card Expiration Date, CVV numbers, and other relevant details. Fraudulent calls encompass various forms of scams, including fake lottery and trip schemes [15].
- Internet Banking Fraud refers to the act of unlawfully withdrawing funds from a victim's bank account and transferring them to a specific targeted bank account using electronic technologies over the internet.
- India does not have a legislative framework to address fraud with cryptocurrency. Consequently, on the dark web, criminals utilize these currencies to initiate dubious Bitcoin business transaction requests.
- Salami attacks refer to a type of malicious activity that is specifically designed to commit financial crimes. These attacks involve making imperceptible alterations to facilitate concealment and evade discovery.

2.5 Cyber-Bullying: The act of subjecting a person to harassment and coercing them into performing actions against their will. Adolescents and young individuals are commonly targeted by cyber-bullying. It encompasses several actions such as making disparaging remarks against someone, sending degrading messages about them, sharing unnecessary photographs or videos of them, and so on. A survey done in India by the Delhi-based NGO Child Rights found that 9.2% of 630 minors experienced cyberbullying. Surprisingly, many of these teenagers chose not to report the incidents to their parents, teachers, guardians, police, cyber-cells, or any social media organizations. Many of these crimes go unsolved or are not treated with seriousness. Additionally, victims typically lack awareness of when to contact law enforcement authorities [16].

2.6 Fabricated Profile: Creating a fabricated profile of an individual and disseminating offensive material, such as manipulated images, on it [17].

2.7 Cyborg, sometimes known as cyber terrorism, is a highly dangerous type of cybercrime. It is utilized to perpetrate aggressive actions via the internet, such as purposeful and extensive interruptions. Terrorists are currently involved in cyber warfare targeting the human brain, utilizing brain computing to modify and manipulate human minds for their own advantage [18].

There are numerous other illicit activities that require prompt attention and solutions for the betterment of society.

3. Examination of social media offenses utilizing a computer forensic methodology:

Any person, whether they are an individual, an employee of a firm, or a police officer, has the ability to uncover a possible danger or misuse of any social media platform, as well as any proof pertaining to a suspected unlawful behavior. The investigation of social media crimes relies on various variables, including the timing of the complaint, the timing of the reported behavior, the device used to report the activity (such as a computer system or smartphone), and the identity of the person reporting the conduct [19]. Moreover, the Investigating Officers (IOs) face obstacles in identifying the victim, determining the purpose of the crime, and identifying the criminal.

3.1 The scope of investigation

The primary sources of digital evidence in a certain social networking application that is suspected of illegal behavior or misuse are the web pages or direct links. Acquiring vital digital evidence from an employee's computer is a necessary step in a police investigation about the misuse of a social networking program in a corporate setting. On the other hand, it is imperative to obtain digital proof from the computers of the victims who have been affected by the misuse. Given the wide range of computing devices available (such as laptops, desktop computers, tablets, mobile phones, gaming consoles, etc.), it is important to thoroughly and systematically examine these devices using specialized tools in order to investigate any potential criminal activity on social media platforms. During forensic and police investigations, authorities may request relevant digital data associated with suspected misuse from the social networking site's supplier or authorities. In some cases, forensic investigation of the servers that facilitate the social networking may also be necessary [20].

3.2 Acquiring digital evidence for the study of social media data in computer forensics

When it comes to obtaining digital evidence via social media platforms and similar networking programs, the following potential avenues of acquisition are commonly utilized [21]:

- Firstly, search for websites hosting social media programs that include the necessary and accessible information. Under such circumstances, investigators are required to examine any significant alterations made to a web page between the moment the content or post was generated and the time when the investigator attempts to recreate the page. For example, a victim may file a complaint of harassment utilizing a Facebook platform if there is a post containing abusive content and an inappropriate or undesirable image alongside it. However, when the investigator accesses that specific page and the message that was sent, the individual who posted the message has altered the symbol to a different image. In such instances, the investigator must possess adequate expertise, qualifications, and training to identify modifiable components and identify additional evidence of a crime that can be obtained from alternative sources.
- The suspect's equipment can be used to identify and locate him by utilizing IP addresses and other protocols. An obstacle that may arise while gathering evidence from the source is the wide accessibility of social media through various platforms such as laptops, tablets, mobile phones, iPads, e-readers, or traditional desktop computers, regardless of geographical location.

- Unlike inquiries conducted through email, the bulk of social media offenses generally involve the release of content and subsequent alterations to site pages or posts. In this situation, examining and investigating the victim's gadget could also be advantageous. The service provider's logs are likely to give the most compelling evidence in this instance.
- Typically, the server computers used by social networking services and relevant Internet Service Providers (ISPs) are only accessible for police investigations. Multiple sources are typically accessible for both internal and external investigative inquiries [22].

• When important evidence is found on a specific networking site, the best way to collect the evidence is to visit the site and immediately make copies and photographs of the relevant evidence and content.

When encountering such situations, it is imperative for the investigator to meticulously document the web address or URL of the suspected webpage within the specific website. It is imperative to carefully document an audit trail or activity log of all acts performed by the forensic investigator during the retrieval of the clues [23]. A widely used method for replicating the content of a website involves physically visiting the site and utilizing video capture software to record the relevant web pages. This allows for the creation of a visual representation of how the pages appeared at the specific moment of visitation, which can be useful for legal and reconstructive purposes. The pages can also be captured as screenshots whenever necessary for illustrative purposes. Additionally, it is advisable to save the individual web pages, either by utilizing website replication technologies or by doing it manually. Copying the web pages not only captures a visual record but also safeguards the exact code of those pages, allowing it to be utilized as a relevant source in the future.

In order to prevent the potential loss of evidence due to a delay in conducting investigative procedures, the person reporting the incident may be requested to create a duplicate of the evidence using any available means, such as saving pages, printing, or taking screenshots. In addition, the incident report can also be handled by the recipient. Prior to conducting any investigative operations, it is essential to get the assistance of a certified cyber forensics specialist. Failing to do so may result in the improper collection of evidence, which could potentially compromise the inquiry at a later stage [24].

4. Evidence Retrieval in Case of Social Media Crimes

Conventional computer forensic procedures can potentially retrieve data stored on the hard drive or other storage devices of a computer or smartphone that was used to carry out social media crimes. This data may include login information, usernames, web caches, internet history, and passwords related to specific social media applications. Considering that the data exchange being discussed primarily involves unstable data with no assurance of complete data recovery, any techniques used to extract SNS (Social Networking Sites) data as evidence must adhere to this requirement as a fundamental limitation [24]. The preservation of data generated through user engagement with social networking sites (SNSs) is not guaranteed. Accessing digital material kept on Internet service providers (ISPs) servers or social networking servers (SNS) can be challenging due to limited access, typically restricted to police investigations. If the social networking service (SNS) does not disclose IP addresses or account-related information, a comprehensive investigation can establish the involvement of a specific individual within the workplace or social circle in making an unlawful statement or committing

a specific crime [25]. Human intelligence, forensics, forensic linguistics, forensic psychologists, and Questioned Document Examiners are sometimes involved in this process.

Difficulties emerge when a message is sent from an individual's personal mobile phone, tablet, or laptop. In these circumstances, the organization does not have authority to view it. Generating a duplicate of the purported storage device is typically a component of the computer forensic investigation procedure. This guarantees the integrity of the original data, preventing any unauthorized modifications or corruption. Subsequently, the copy can be examined for pertinent evidence using a suitable computer forensic tool such as FTK or Encase. According to Haggerty et al, forensic tools are designed to analyze evidence obtained from storage media, not data from online sources like social media. This is problematic because the popularity of social media investigations has increased due to the valuable information they provide about a suspect [25].

To identify social media artifacts on a computer system, it is necessary to ascertain the specific social networking program or application and the operating system used on the device. Additionally, information regarding the suspicious internet browser to be used in the subsequent stage of investigation must be obtained. Facebook artifacts, such as data related to Facebook activities, can be located in several places on a computer, such as the browser cache, unallocated clusters, or system restore points [26].

However, analyzing data from mobile phones and tablets may pose more challenges due to the wide range of operating systems available. Furthermore, diverse social networking applications store digital data in distinct formats and locations within their memory. A database associated with the Facebook application is stored in the memory of mobile phones. The database stores comprehensive data about each individual on the list, including their names, unique identification numbers, and contact phone numbers. Twitter utilizes directories and other apps to store data pertaining to Twitter accounts, attachments transmitted with Tweets, user names, and date and time information. In order to acquire digital evidence pertaining to social media activities, one might employ either physical or logical methods. Nevertheless, there is a possibility that data stored in slack space may be disregarded during logical acquisitions [27].

Forensic software tools like Twitter investigator, Facebook forensics, and MacForensicsLab social agent can analyze certain computing devices to find evidence of social network activity. They can also identify the social networking web pages visited by the suspect, specifically on Apple Macs using the Apple Safari web browser. FTK and Encase are widely-used computer forensics software programs that provide capabilities for doing searches of your web history [28].

5. Analysis of Data

There are two items to contemplate: Primarily, has the account been compromised by hacking or has there been unauthorized access on another device? This requires scrutinizing all the devices and geographical locations that have had access to the device to determine if any of them exhibit any signs of malicious intent. For example, if we encounter a user originating from the United States and we detect access from Russia, it could suggest that the person is engaging in nefarious activities. By analyzing the forensic information pertaining to the method of account access, we can ascertain whether the account has been compromised [29].

The advent of rapidly advancing technology has greatly enhanced the investigative process by providing essential tools to aid in forensic computer inquiry. These tools enable the location, identification, examination, and analysis of digital evidence, so significantly benefiting the investigative process. To ensure efficient investigations, computer forensic examiners commonly conduct focused and precise exams utilizing specialized technologies. The majority of them are doing evidence analysis by selectively choosing particular files and disregarding unimportant files or categories of evidence and their contents [26, 28].

The development of advanced technologies such as FTK and EnCase has greatly enhanced the efficiency of digital forensic investigators in doing their responsibilities. The National Institute of Standard Technology (NIST) states that there are four main stages in any digital forensics case: identification, collection, organization, and presentation. The identification phase involves the recognition and acknowledgment of the incident or evidence. Data is gathered as evidence, then organized and streamlined by eliminating any duplications to lower its volume. During the organization step, carved data is carefully examined and cross-referenced with the crime scene to provide accurate and trustworthy conclusions. Ultimately, the presentation phase involves conveying the data in a manner that is comprehensible to the jury [28].

5.1. The process of analyzing heterogeneous social media data

A wide range of researchers have endeavored to bridge the divide between fragmented social media data and social media forensic applications in their studies. Their research proposes a unified framework to address the inconsistency across various social media sites and standardize the data. The architecture prioritizes security and enables functions such as data preservation, search, correlation, automated data analysis, and visualization. Their approach to social media analysis is based on a paradigm that involves three main steps: tracking, preparation, and analysis.

The preparation phase commences with the tracking of data utilizing platform-specific APIs provided by online social networks such as Twitter, LinkedIn, Facebook, and others. The majority of contemporary social media perceptions are mirrored and introduce a novel ontology known as the Unified Social Network Ontology (USNO). Various social media platforms have created plugins specifically designed to facilitate the implementation of the suggested method. The social media data is inputted into each plugin that is specific to the associated social media platform [29]. The USNO provides detailed information on the storage requirements for social media data in the graph database. The graph visualization showcases the node labels, node attributes, and the interconnections among the network's nodes/entities. The data from each social media site is analyzed to obtain implicit knowledge about the newly given unified taxonomy. Subsequently, the data is correlated with the United States Naval Observatory (USNO). During the subsequent phase, the data is stored in the graph database. To accurately assess the interaction between profiles, an inference technique has been devised to establish direct connections between profiles that communicate with each other, even if these connections are not explicitly stated. During the analysis phase, the cypher queries were constructed to retrieve information and establish connections pertaining to forensic research on profiles [29, 30].

Queries can utilize end-user inputs as parameters. Social Networking Analysis (SNA) techniques utilize predefined query placeholders to gain insights into the network structure and identify the most noteworthy profiles. In addition, any signal capable of providing social media

data will be promptly identified by law enforcement agencies. Automated data harmonization, archiving, and analysis will significantly decrease the cost of conducting an investigation [31].

Facebook artefacts encompass a range of data, such as activity logs, Facebook archives, profile information, locations and geo-locations, friends and family connections, applications, pages, groups, interests, text and links, timestamps of all activities, and details of friends involved in active chat sessions with the user. These are just a few examples of the extensive information that can be found on Facebook [25, 30, 32].

Twitter artefacts include user information, tweets posted, timestamps of the poster's tweets, and records of people followed by the subject and their tweets with timestamps.

6. The Difficulties of Forensic Analysis of Mobile Social Networking Apps

Smartphones, despite their capabilities, can provide several challenges for social media forensics investigators. Due to the perpetual connectivity and continuous data updates of smartphones, evidence is rapidly depleted. Furthermore, the proprietary operating systems used in smartphones (except Linux-based phones) prevent the use of specialized tools for extracting evidence [33].

Compounding the challenges for forensic professionals, smartphone makers frequently introduce new operating systems. Keeping pace with the latest technologies and investigation methodologies poses a challenge for experts in social media forensics [34].

Conclusion:

There is limited study on the forensic analysis and retrieval of actions conducted on mobile phones using social networking applications. These research have also been limited to acquiring fundamental data regarding the utilization of social networking programs. This study primarily focuses on the procedures and difficulties involved in obtaining data, retrieving evidence, and analyzing data in circumstances when a social networking application is used for illegal activities. Determining the primary origin of the current data or crime that has occurred anywhere in the world is always a challenging task. Nevertheless, by utilizing specialist tools and advanced forensic technologies, this issue can be effectively resolved through a systematic approach. Several studies have investigated whether the activities performed on social networking apps can be stored and retrieved from the internal memory of cell phones. Facebook, Twitter, WhatsApp, and Myspace are widely used social networking applications that have undergone testing on BlackBerry, iPhone, and Android devices [35]. Currently, there is a lack of generally available recommendations for organizations that specialize in computer forensic examinations of social networking programs. Organizations that intend to perform computer forensic investigations on social networking applications must ensure that they do not compromise the integrity and admissibility of any digital evidence related to the misuse of these applications. This is particularly important if such evidence is required for a police investigation [36]. Organizations that facilitate or encourage employees' utilization of social networking platforms at work should establish clear guidelines about acceptable (and unacceptable) usage, as well as the possible repercussions of such actions. There is an abundance of regulations that could be relevant to forensic investigations and the misuse of social media in the workplace.

Future Scope:

Uploaded evidence on the internet or a social media platform is subject to rapid changes and can be destroyed or modified at any given moment. Consequently, investigators must ensure that their data collection and preservation techniques are regularly updated to guarantee validity. Hence, further investigation in this field using state-of-the-art methods is necessary to get digital evidence in cybercrime cases.

References:

[1]. Harper, S., & Chen, A. (2011). Web accessibility guidelines. World Wide Web, 15(1), 61-88. doi: 10.1007/s11280-011-0130-8

[2]. Leng, H. (2013). Methodological Issues in Using Data from Social Networking Sites. Cyberpsychology, Behavior, And Social Networking, 16(9), 686-689. doi: 10.1089/cyber.2012.0355

[3]. Bevan, J. (2018). Social Networking Site Password Sharing and Account Monitoring as Online Surveillance. Cyberpsychology, Behavior, And Social Networking, 21(12), 797-802. doi: 10.1089/cyber.2018.0359

[4]. Flew, T. (2015). Social Media Governance. Social Media + Society, 1(1), 205630511557813. doi: 10.1177/2056305115578136

[5]. Muhammad, A., Wicaksono Y. S., & Sri R. A., (2021). Komparatif Anti Forensik Aplikasi Instant Messaging Berbasis Web Menggunakan Metode Association of Chief Police Officers (ACPO). JURISTIK (Jurnal Riset Teknologi Informasi Dan Komputer), 1(01), 8-15. doi: 10.53863/juristik.v1i01.341

[6]. ACPO (2012) Good practice guide for digital evidence, Version 5, The Association of Chief Police Officers of England, Wales and N. Ireland, http://www.acpo.police.uk

[7]. O'Floinn, M., Ormerod, D. (2011) Social networking sites, RIPA and criminal investigations, Criminal Law Review, 10, 766-792.

[8]. Marley, R., & Snow, N. (2014). An Empirical Investigation on Social Media Userss Demand for Accounting Information Distributed Via Social Media Platforms. SSRN Electronic Journal. doi: 10.2139/ssrn.2517037

[9]. Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. Journal Of Computer Security, 27(6), 581-612. doi: 10.3233/jcs-181253

[10]. Vijaya Geeta, D. (2011). Online identity theft – an Indian perspective. Journal Of Financial Crime, 18(3), 235-246. doi: 10.1108/13590791111147451

[11]. Wadje, A. (2013). Digital Obscenity: Issues & Challenges in India. SSRN Electronic Journal. doi: 10.2139/ssrn.2196473

[12]. Sharma, B., Joseph, M., Jacob, B., & Miranda, B. (2019). Emerging trends in Digital Forensic and Cyber security- An Overview. In Sixth HCT Information Technology Trends (ITT) (pp. 309-313). Ras Al Khaimah: IEE-Xplore. Retrieved from https://ieeexplore.ieee.org/document/9075101

[13]. Nyam, I. (2020). Tackling Online Dating Scams and Fraud. The International Journal Of Humanities &Amp; Social Studies, 8(11). doi: 10.24940/theijhss/2020/v8/i11/hs2011-065

[14]. Spaulding, T. (2010) How can virtual communities create value for business? Electronic Commerce Research and Applications, 9, 38-49.

[15]. Koteshwar, M., & Singh, B. (2019). Survey Report on Cyber Crimes and Cyber Criminals Get Protected from Cyber Crimes Review Paper. International Journal Of Computer Sciences And Engineering, 7(12), 99-109. doi: 10.26438/ijcse/v7i12.99109

[16]. Saenko, M., Savela, E., & Topolyansky, Y. (2021). International experience against cyber crime and cyber crime. Uzhhorod National University Herald. Series: Law, (64), 386-391. doi: 10.24144/2307-3322.2021.64.71

[17]. Asongu, S., & Odhiambo, N. (2018). Governance and Social Media in African Countries: An Empirical Investigation. SSRN Electronic Journal. doi: 10.2139/ssrn.3271787

[18]. Ajji, K. (2020). Cyborg finance mirrors cyborg social media. Big Data &Amp; Society, 7(1), 205395172093513. doi: 10.1177/2053951720935139

[19]. Craciunescu, C. (2015). Basic aspects concerning the evidence aquisition in digital forensic analysis. Forum Criminalistic / Forensic Science Forum, 8(17 (1/2015). doi: 10.18283/forum.viii.17.12015.315

[20]. Go, E., & You, K. (2016). But not all social media are the same: Analyzing organizations' social media usage patterns. Telematics And Informatics, 33(1), 176-186. doi: 10.1016/j.tele.2015.06.016

[21]. Adel, A. (2022). A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach. Forensic Sciences, 2(1), 111-129. doi: 10.3390/forensicsci2010009

[22]. Spindler, G., & Dorschel, J. (2005). Auskunftsansprüche gegen Internet-Service Provider. Computer Und Recht, 21(1). doi: 10.9785/ovs-cr-2005-38

[23]. Taylor M., Haggerty, J., Gresty, D. (2007) The legal aspects of corporate computer forensic investigations, Computer Law and Security Review, 23, 6, 562- 566.

[24]. Sundus Munir, S. (2018). Social Media and its Impact on our Privacy. International Journal For Electronic Crime Investigation, 2(3), 8. doi: 10.54692/ijeci.2018.020320

[25]. Moreno-García, M. (2020). Information Retrieval and Social Media Mining. Information, 11(12), 578. doi: 10.3390/info11120578

[26]. Wang, F., Cui, P., Sun, G., Chua, T., & Yang, S. (2012). Guest editorial: Special issue on information retrieval for social media. Information Retrieval, 15(3-4), 179-182. doi: 10.1007/s10791-012-9199-7

[27]. Haggerty, J., Casson, M., Haggerty, S., Taylor, M. (2012) A Framework for the forensic analysis of user interaction with social media, International Journal of Digital Crime and Forensics, 4, 4, 15-30.

[28]. Haenschen, K. (2016). Social Pressure on Social Media: Using Facebook Status Updates to Increase Voter Turnout. Journal Of Communication, 66(4), 542-563. doi: 10.1111/jcom.12236

[29]. Chhetri, A. (2020). Cyber Forensic Challenges: Escaping Holes for Cyber Attackers Series 01: Extracting Forensic Evidences from Non- Functional Computer Devices. Digital Forensics (4N6) Journal, 50-52. doi: 10.46293/4n6/2020.02.02.09

[30]. Mutawa, N. Baggili, I., Marrington, A. (2012) Forensic analysis of social networking applications on mobile devices, Digital Investigation, 9, 24-33.

[31]. Jordan, K. (2014). Academicss Awareness, Perceptions and Uses of Social Networking Sites: Analysis of a Social Networking Sites Survey Dataset. SSRN Electronic Journal. doi: 10.2139/ssrn.2507318

[32]. Guala, F., & Hindriks, F. (2014). A UNIFIED SOCIAL ONTOLOGY. The Philosophical Quarterly, 65(259), 177-201. doi: 10.1093/pq/pqu072

[33]. Greenspon, J. (2016). Social media and the art of intellectual property theft. Media Transformations, 12. doi: 10.7220/2029-8668.12.06

[34]. Morrison, T. (2014) Private eye: Legal update data privacy, The New Law Journal, 164, 7599, 164 NLJ 14

[35]. Murdoch, S. (2019). Transforming Cyber Incident Response. ITNOW, 61(1), 34-35. doi: 10.1093/itnow/bwz014

[36]. Hutcheson, G. (2011). Data coding, management and manipulation. Journal Of Modelling In Management, 6(1). doi: 10.1108/jm2.2011.29706aab.001