https://doi.org/10.29042/2020-10-4-32-38

Helix (2020) 10 (4): 32-38

Forensic Analysis of Third-party Mobile Application

[1] Majid ALThebaity, ✉ [2] Shailendra Mishra, [3] Manoj Kumar Shukla

[1] Department of Information Technology, College of Computer & Information Sciences, Majmaah University, Majmaah-11952, Saudi Arabia

MajidNayef@hotmail.com

[2] Department of Computer Engineering, College of Computer & Information Sciences, Majmaah University, Majmaah-11952, Saudi Arabia

s.mishra@mu.edu.sa

[3] Department of Electronics Engineering, Harcourt Butler Technical University, Kanpur

mkshukla@hbtu.ac.in

Received: 04th June 2020, Accepted: 19th June 2020, Published: 31st August 2020

Abstract

The expansion of the phone's memory space and processing power comprise some of the primary contributing factors to the evolution of digital crime. Therefore, wide adoption and reliance of third-party applications expose individuals to various digital crimes. In this research both qualitative and quantitative methods are used. The recovered data items from the phone's memory were classified and facilitate the description of the recoverable app and user information after the deletion of the social networking app like Facebook. The choice of Facebook as the subject app for investigation arises from the fact that it comprises one of the major social network platforms. Some of the recoverable data in both scenarios include but not limited to text messages, login information, friends' information, and user account details, among others. The research seeks to fill an existing gap concerning the establishment of the location and types of recoverable data after the uninstallation of the Facebook application from a smartphone device.

Keywords

Digital Forensic, Forensics Investigation; Third-Party Application; Social Networks; Digital Evidence.

Introduction

The advancements in mobile technology have multiple benefits as well as shortcomings to the consumers. One of the significant benefits of mobile phones includes enabling individuals to communicate efficiently with others across the globe. Primarily, mobile phone users rely on third-party applications to share information with efficiency; however, this has not been without crucial security concerns. Third-party applications have been a platform for digital crimes, especially social networks, which comprise one of the most relied upon mobile apps by persons for sharing information. Social networking apps leave a range of footprints, unlike other forms of mobile applications [1]. Therefore, mobile forensics of third-party smartphone apps can provide substantial and crucial digital evidence, especially to forensic investigators. However, numerous challenges hamper the success of forensic investigators. One of the significant obstacles challenging the acquiring of substantial digital evidence emanates from frequent updates of the operating system [2].

Mobile forensics is a branch of digital forensics that primarily deals with tablets, PDAs, and smartphones. Principally, digital forensics entails scientific driven and approved methods seeking to collect, preserve, validate, identify, analyze, interpret, and present electronic evidence acquired from digital devices. The principal reason for undertaking the above activities purposes to facilitate or further reconstructing events deemed criminal or actions that result in disruptions of operations. Therefore, mobile forensics entails the use of scientific methods intending to recover potential electronic pieces of evidence from mobile devices by relying on techniques similar to ones applied in digital forensics. Undertaking mobile forensics involves two main techniques, which comprise of physical and logical acquisition methods. In the logical acquisition, the investigator embarks on copying storage objects such as file system partition and directories bit-by-bit. Physical acquisition entails bit-by-bit copying of the entire physical store, such as memory chips [3].This research uses both the physical and logical evidence acquisition methods to ensure identification of areas where to retrieve third-party applications, especially Facebook data, after its deletion in a mobile device. Presently, the exchange of information between persons across the globe has undergone enhancement through the use of mobile apps. The portability of mobile phones comprises one of the leading factors for their wide adoption. Also, the provision of a range of features by installed apps on smartphones has had a significant effect on the efficiency of information sharing between individuals and groups of people across the world. Some of the features provided by these apps include but not limited to the capability to share images, text messages, and video files. However, third-party application platforms involve a significant security issue, as observed with the increase in digital crimes over the recent past [4].

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

There have been numerous studies intending to examine instant messaging apps like WhatsApp. WhatsApp has undergone digital forensic examinations to establish the application stores activity information in the phone's internal memory as well as establish recoverability of deleted data such as contact details [5]. Another study analyzed Instagram seeking to establish the storage location and the recoverable data from an Apple mobile device. The findings of the study established the availability of the app's data in the phone's internal memory. Also, the forensic examination recovered different types of data, such as username information, various data sharing dates, and deleted photos [6].Developers continuously release new versions of operating systems targeting to improve the user experience [7]. As a consequence, forensic investigators experience significant difficulties in establishing the meaning and locations of data during forensic investigations. Therefore, this paper presents a scenario-based methodology for undertaking forensic examination for Facebook social networking app on an Android mobile device. When implemented on Facebook security incidents, mobile forensics can offer investigators with substantial data to assist in the process of investigation. The need to investigate social network apps, especially Facebook, originate from its wide adoption by numerous individuals and the reliance to share information. At present, third-party apps comprise an essential part of the mobile phone environment. Consequently, both the Google Play and Apple app stores have increasingly experienced growth in the number of apps and downloads. These include the popular platforms from where electronic device users across the globe download apps for installations [8].

The increased adoption of the app by individuals for communication makes it the prime target by malicious persons whose main aim is to exploit users and acquire personal information [9]. The primary intention of gathering user data by malicious individuals is for personal gains, which may include financial and sexual exploitations, among others. Digital crimes have been on the rise, primarily via social networks, thus the need to establish additional methods to perform comprehensive mobile forensics to obtain considerable amounts of digital evidence.

The primary purpose of the forensic analysis in this research to determine the location of forensic artefacts left by the Facebook app on a smartphone upon the deletion of the app. So the analysis intended to establish whether the recoverable data provide meaningful artefacts for mobile forensics. Focus of the research concerns the Android smartphones and Facebook social network. Establishing Facebook's recoverable data and its location after the deletion of the app will significantly boost the efforts of forensic investigators in conducting a comprehensive investigation.

The paper was organized in various section, first section was introduction it includes background, purpose of the work and current state of the research in Forensic Analysis of third-party applications. Second section includes related work and literature review of peer-reviewed journals and books and their contribution to the field of mobile and digital forensics. The survey will be of significance in establishing the existing gap in the mobile forensics field, especially targeting third-party applications. The third section was the methodology part, identifying the methodological approach to the survey was considerably enhance the efforts towards the realization of the paper's goals. Section four includes the experimental analysis, validation, observations and key findings. Section five includes the discussion and conclusion. The conclusion in the paper would serve an essential role by establishing the procedures and relations underlining the study findings.

Related Work

Researchers and academicians have undertaken multiple research concerning the forensic analysis of third party applications. The unprecedented rise in the number of individuals using third party mobile applications exposes users to digital exploitations and attacks [10]. The high rate of digital crimes by using mobile phone for the intervention of forensic investigators in finding relevance and strong electronic evidence admissible in court. One of the significant reasons necessitating the involvement of digital forensic investigators includes the high volatility nature of the mobile device memory [11]. As a result, the high volatility leads to the erasure of data as the user continues to use the device for communication and other activities. In [12] authors used multiple methods to acquire information from the Android phone. The tools utilized in this research include (FTK) Forensic Tool Kit and CelleBrite UFED. The FTK tool enabled the recovery of call history, pictures, SMS/MMS, web history, email data, passwords, voice mails, and GPS information. The CelleBrite UFED tool, on the other hand, facilitated the recovery of SMS/MMS messages, call logs, videos, photos, and contact information.

In [13] authors undertook a study seeking to establish adaptable encryption standards to hide communication on instant messaging apps purposing to secure the exchanged message. These include symmetric and asymmetric algorithms. Symmetric includes algorithms such as AES (128 bits), Twofish (128 bits), and the serpent (128 bits) while asymmetric comprises RSA and Diffie-hellman, among others. The forensic process employed identification, acquisition, and examination methodology. The results indicated neither the presence of encryption nor encoding of Facebook messages, thus the need to ensure encryption of texts shared via the instant messaging app. Reference [14] deal with examining the Android memory through physical and logical approaches to inform on the process for adoption to obtaining sound forensic artefacts. Reference [15] researched mobile forensics and delivered significant findings and recommendations to follow in undertaking similar tasks, also investigated the evidence retrievable, the research involved laboratory experiments by working on three different models of

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

smartphones, iPhones, Android, and blackberry and some of the social networks investigated were Facebook, Twitter, LinkedIn and Google. These platforms comprise of the third-party mobile applications. In paper [16] authors conducted a forensic study on WhatsApp social network platform seeking to extract useful information on an Android phone. WhatsApp comprises one of the most popular third-party applications with a lot of users across the globe. The methodology utilized includes identifying, preserving, analyzing, and presenting digital evidence. The investigator employed a methodology by strictly following the identification, extraction, analyzing, and reporting process.

In [17] authors did a forensic investigation on Facebook photos to establish the trails left after renaming, compression, and resizing of the pictures. The necessary metadata established to remain on a photo includes the date, camera settings, time, and generic descriptions. The research finding provides a ground to conduct a comprehensive forensic investigation by identifying changes and trails left behind after uploading a picture via the Facebook app. In the reference [18], a standard process was identified to guide the extraction of evidence from mobile devices. The method defined by the authors chronologically includes intake, identification, preparation, isolation, processing, verifying, reporting/documenting, presenting, and archiving. In [19] authors conducted forensic research on Facebook seeking to establish the data that remains on Windows 8.1 OS and the corresponding locations on the hard drive. This investigation entailed residue information after the use of Facebook on windows and a computer. The study also seeks to identify the type of data that remains in RAM (random access memory) after the use of the Facebook app on a PC running on Windows 8.1 operating system. Another important research conducted in [20,21] was closely relates to Facebook forensics on a Windows 10 platform. The study focused on examining the locations for user information on the SQLite database. In [22] authors were reconstructed the past incidents in smartphones through forensic tool. The research established that data is retrievable from a device, backup files, on PCs, and the received as well as sent messages both from groups and individuals. Some of the identified sources of data necessary in incident forensics include SMS, e-mails, photos, MMS, call logs, audio files, videos, geo-locations, and other app information. In [23] authors conducted a study regarding mobile forensics by focusing on the operating system and forensic tools limitations. The research was of significance in establishing various factors that limit the capability of investigators to undertake mobile forensic investigation comprehensively. The study purposed to respond to the increased number of cybercrime incidents, which continues to escalate at a considerable pace since the establishment of the internet. The performance of a mobile forensic tool is measurable by its probability of successful extraction of specific digital evidence.

In [24] authors analyzed three third-party applications, namely Skype, Viber, and WhatsApp. The investigators intended to establish forensic artefacts retrievable from the apps data remnants concerning individuals. The investigation of these three apps revealed that phone numbers, video, images, contact information, and messages are recoverable from devices installed with the three apps, as mentioned above. The examination of the device in search of forensic artefacts followed a specific method that involves seizure, acquisition, analysis, and reporting process. The significant artefacts recovered by the investigators in [25] include app information, internet data information, multimedia, graphics, organizer information, call history, contact, and messages. Finding this information is of significance to any forensic investigation because they provide reach details that considerably facilitate the establishment of perpetrators of digital crimes. In [26] authors conducted a forensic investigation on WhatsApp instant messaging app seeking to obtain its latest forensic artefacts that utilize. crypt12 encryption.

The forensic investigation process employed collection, examination, analysis, and reporting methodology to conduct the exercise. Reference [27,28] dealt with a case study concerning the framework and methodology employable in investigating social network applications, especially the Facebook App. The study aimed at conducting a forensic analysis of cloud forensics and social network in an internet environment. The case study is in response to the numerous challenges faced by forensic investigators because of the increased identity theft, public defamation, compromise of personal data, and cyberstalking, amongst others.

The review of the related works carried out by digital forensic professionals and academicians is of significance as it has enabled the establishment of a research gap, which the study seeks to fill. Identifying the recoverable data and its location after the deletion of Facebook from the smartphone will facilitate the efforts of obtaining digital evidence efficiently. The review of related works has also provided adequate information and knowledge, especially regarding the methodology of adoption in the study to accomplish the research objectives. One of the most significant research gaps identified after close examination of various research articles includes a lack of a forensic study to establish the location and recoverable data after the deletion of a Facebook app or any social networking app from a smartphone. The identification of recoverable data and its probable location in a phone after the uninstallation of Facebook would significantly boost the capability of forensic investigators to conduct a comprehensive investigation concerning digital crimes. Therefore, this research will adhere to identification, acquisition, examination, and reporting methodological approach as informed by previous studies. Establishing Facebook's recoverable data and its location after the deletion of the app will significantly boost the efforts of forensic investigators in conducting a comprehensive investigation. Facebook comprises one of the most utilized

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

third-party applications across the globe. Facebook enjoys millions of users across the world, thus making it a principal target for exploitation.

Research Methodology

This study employed both qualitative and quantitative research methods. Qualitative is flexible structured it can be modified according to the facts collected and gathered. Starting with the qualitative research which mainly focuses on the hypothetical and theoretical data and not on numerical facts, figures and graphs. Qualitative provides insights and gets a hands-on understanding of the problem, mainly based on observations, anticipations, and interpretations. Coming towards the quantitative which is mainly concerned with the statistical and numeric data. It is a systematic and empirical investigation of observable phenomena via, statistical and mathematical techniques. It consists of large numerical data after that they conduct data analysis on that to find correlations. Quantitative approach in this research was used to ensure the accomplishment of the study objectives. The qualitative approach was used in this research for recovery of the data from the phone's memory using standard data recovery tool FTK. The recovered data items from the phone's memory required classification to their format and type to describe the recoverable app and user information after the deletion of the Facebook application.
The research design methodology outline was as follows:

- Wiping and restoring the devices factory defaults.
- Installing the Facebook app and configuring the created user accounts.
- The population of both devices with data through the created Facebook user accounts.
- Exchange data and allow the devices to update for several days.
- Isolate the devices by wrapping them in a faraday bag and activating airplane mode.
- Uninstall the Facebook app from one of the two devices.
- Root the devices separately.
- Perform a full acquisition of the file system on both the devices and store them separately on external drives.
- Analyze the results by Forensic tool kit (FTK)

Every device got populated with sample data through the exchange of text and other media formats via the created Facebook user accounts. On the bare minimum, both user profiles got filled with pictures, profile information, and location. The Facebook accounts were in frequent use during the initial phases of the research to ensure the presence of sufficient amounts of data exists for analysis.

Experimental Setup and Analysis

The implementation involved various steps to ensure the proper environment to conduct a comprehensive forensic investigation by setting up a workstation with the necessary forensic tools like FTK to facilitate the process of forensic examination along with two android smartphones installed with the Facebook app, a laptop running Windows 10 OS, two external disks, and USB data cables. After the setup, the first phase was accomplished with sending photos and texts between the two devices through the Facebook social network. After exchanging multiple media and text messages, switched the devices to airplane mode to isolate them from any communication as well as application updates. The next phase includes uninstalling Facebook from one of the two mobile devices. FTK was used to imaging (bit by bit copy) both phone's internal memory, storing them in different external drives subject for forensic examination. The two images were extracted and examined separately through the use of the FTK to establish the recoverable artefacts in both scenarios.
The experiment involved several task through the Facebook social network platform to ensure the generation of data for use in the forensic investigation and involved an exchange of a limited number of media and text. The process implemented the established forensic steps, which include identification, acquisition, examination, analysis, and reporting of findings. However, to ensure the establishment of massive forensic artefacts, the experiment required to include an extended exchange of media with multiple individuals and for a longer period. For purposes of verifying the results from the recovered data on the device with the uninstalled Facebook app, the experiment involved a comparison analysis. The analysis relied on the findings of the recovered artefacts from the equipment installed with the Facebook app (the receiver device). The comparison examined media metadata such as time, sender profile, ID, and content of the text received against those of the sender. The use of only two Facebook accounts facilitated the validation process by eliminating the confusion in verifying the actual sender in a real scenario, which involves multiple media and text exchange from different friends. The research intended to establish the recoverable artefacts from a deleted Facebook app on an Android phone. The outcome resulting from the practical implementation of the research achieved a significant proportion of the established overall objective. The acquired artefacts from both scenarios played a substantial role in determining the likelihood to recover Facebook data both before and after the deletion of the app. The acquisition of the app data through the use of FTK enabled the identification of three crucial SQLite database files, which provides substantive information regarding Facebook user activities on a mobile phone device. The three records obtained for this research in the deleted folder include;

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

i. analytics.SQLite database
ii. friends.SQLite database
iii. messages.SQLite database

The path to these database files on the target device is Program File\Apps\Deleted. Each of the records contains different details of a specific activity that took place via the use of the Facebook application. It includes the capability to recover substantive data even after the uninstallation of the Facebook app from an Android mobile phone platform. The deletion of the app from the target phone results in the relocation of the created folder during installation to Program File\Apps\Deleted. Obtaining the app database files from this folder provides an opportunity to gather details of user activities via the application. The recovered SQLite database files make available various user details that are crucial in forensic investigation. The analytics.sqlite database contains essential forensic data concerning the user activities among them, including the last time an individual logged in into their profile, as shown in table1.

Table 1: analytics.SQLite database

id	time	log_type	name	module	extra
Filter	Filter	Filter	Filter	Filter	Filter
1	142189831466	client_event	login	login_event	{ }

The recovered friends.SQLite database provided a significant amount of personal details that are crucial in the identification of persons during a forensic investigation. Among the most critical information about friends to a specific user within the file include the names, phone number, and email address. Other crucial detail about a friend to a particular user consists of the date of birth, as shown in table 2.

Table 2: friends.SQLite database

id	name	first_name	middle_name	last_name	contact_email	phones
Filter	Filter	Filter	Filter	Filter	Filter	Filter
100004911219827	Kelvin Sky	Kelvin		Sky	fbcctester@gmail.com	{ }

profile_url	is_pushable	has_messanger	communication	Birthday date
Filter	Filter	Filter	Filter	Filter
https://www.facebook.com/kelvin.sky.52	0	0	0.000848054885	1990-01-01

The messages. SQLite database provides meaningful forensic data concerning communication between the individuals. Among the details recovered in the file concerning the sender includes the time, message attachments, and name as shown in table 3.

Table 3: messages. SQLite database

id	thread_id	body	sender	tags	timestamp	attachment
Filter	Filter	Filter	Filter	Filter	Filter	Filter
m_mid.1421…	t_msg.e241a….		{“user_id”:”100000493581778 1”,”name”:”Jack Jaffry”,”e…… ……..}	[“inbox”,”read,” source:chat”]	1421644776796	{ “name”:”10934350_3842 3279175124 ……
m_mid.1421…	t_msg.e241a….	Here are some file for you	{“user_id”:”100000493581778 1”,”name”:”Jack Jaffry”,”e…… ……..}	[“inbox”,”read,” source:chat”]	1421644752737	{ }
m_mid.1421…	t_msg.e241a….	Hello Victim	{“user_id”:”100000493581778 1”,”name”:”Jack Jaffry”,”e…… ……..}	[“inbox”,”read,” source:chat”]	1421644744425	{ }

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Further investigations of the messages.SQLite file revealed the capability to retrieve additional content of text conversations. The revelation of the conversation content in this test case is of importance and meaning to forensic examinations as shown in table 4.

Table 4: Conversation Content

id	thread_id	body	sender	timestamp
Filter	Filter	Filter	Filter	Filter
m_mid.1 434780 ……	t_mid.14347806 …..	Check logs in db	{"user_id":"10000…..…. .	143478066271 5
m_mid.1 434780 …	t_msd.1434780 6……	Ok sure	{"user_id":"10000…… ……..	143478066857 4

Putting together these pieces of information would be of significance to forensic investigators when required to provide relevant evidence concerning a digital crime incidence that took place via the Facebook application. The installation process of the Facebook app in the two devices created a folder location in the phone's memory. However, the uninstallation process did not produce any file folder. As observed, the uninstallation process moved the installation folder created in the initial stages of the methodology implementation to the deleted app folder under the path: %Program File%Apps\Deleted. More so, the uninstallation process left app remnant footprints from the unallocated spaces, RAM, and system files, for example, shortcuts and event logs. The identification of the type of recoverable Facebook footprint remnants on an Android phone and their possible location on the device's memory is significant to the forensic investigation community. This will impact the practical capabilities of the investigation team to conduct similar tests more efficiently for the recovery of feasible and substantial digital evidence after the uninstallation of the Facebook app and other third-party applications. Concerning the theoretical implication, the study identifies an exciting area for a survey concerning the decryption of recovered data to determine the contained content for purposes of establishing the weight of digital evidence held. More so, the research outcomes sought to identify the recoverable data only; therefore, determining the type of information that cannot get recovered after the uninstallation of a Facebook app is of importance. The significance of this implication is to guide the process of extracting digital evidence efficiently.

Conclusions

The research outcome contributes significantly to the process of acquiring digital forensic, especially currently where the incidents concerning security issues via online platforms have been on the increase. One of the significant contributions made by the research is the identification of the recoverable and the path of Facebook files after the deletion of the app from a mobile device. Thus, the study sets a background upon which other investigations can refer to undertake similar tests on different types of third-party applications, especially on a smartphone platform. Literature surveys on other third-party applications seeking to identify the evidence left behind after the uninstallation of different apps on various platforms. Consequently, this would enhance the efforts of digital forensic investigators. Also, this would ease the process of gathering and identification of sufficient digital evidence, thus combating the widespread menace of crimes over the internet. The future works concerning the study should seek to expand its scope for purposes of establishing more digital evidence regarding third-party applications. One of the most important scopes of a target in future works includes factoring in more platforms such as different mobile models as well as computers. Another significant scope future works should seek to incorporate concerns the expansion of mobile applications subject for investigation. Future works should not only focus on third-party apps, but also other types of mobile applications that facilitate daily individual's activities.

References

[1] Thakur, K., Hayajneh, T., & Tseng, J, "Cyber security in social media: challenges and the way forward", IT Professional, vol.21(2), pp.41-49,2019.

[2] Krishnan, S., Zhou, B., & An, M. K, "Smartphone Forensic Challenges", International Journal of Computer Science and Security (IJCSS), vol.13(5), pp.183,2019.

[3] Feng, P., Li, Q., Zhang, P., & Chen, Z, "Private Data Acquisition Method Based on System-Level Data Migration and Volatile Memory Forensics for Android Applications", IEEE Access, vol.7, pp.16695-16703,2019.

[4] Binns, R., & Bietti, E, "Dissolving privacy, one merger at a time: Competition, data and third party tracking", Computer Law & Security Review, pp.105369,2019.

[5] Trisnasenjaya, H., & Riadi, I, "Forensic Analysis of Android-based WhatsApp Messenger Against Fraud Crime Using The National Institute of Standard and Technology Framework", International Journal of Cyber-Security and Digital Forensics, vol.8(1), pp.89-98,2019.

[6] Chang, M. S., & Yen, C. P, "Forensic Analysis of Social Networks Based on Instagram", International Journal of Network Security, vol.21(5), pp.850-860,2019.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

[7] Bhat, W. A., Jalal, M. F., Khan, S. S., Shah, F. F., & Wani, M. A, "Forensic analysis of Sync. com and Flip Drive cloud applications on Android platform", Forensic science international, vol.302, pp.109845,2019.
[8] AlSubaihin, A., Sarro, F., Black, S., Capra, L., & Harman, M, "App store effects on software engineering practices", IEEE Transactions on Software Engineering,2019.
[9] Talal, M., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Alsalem, M. A., Albahri, A. S., & Alaa, M, "Comprehensive review and analysis of anti-malware apps for smartphones", Telecommunication Systems, vol.72(2), pp.285-337,2019.
[10] Onyemaechi, B. C., Dehghantanha, A., & Choo, K. K, "Performance of android forensics data recovery tools", In Contemporary Digital Forensic Investigations of Cloud and Mobile Applications, pp. 91-110,2017.
[11] Al Mutawa, N., Baggili, I., & Marrington, A, "Forensic analysis of social networking applications on mobile devices", Digital Investigation, vol.9, pp. S24-S33,2012.
[12] Barmpatsalou, K., Damopoulos, D., Kambourakis, G., & Katos, V. , "A critical review of 7 years of Mobile Device Forensics", Digital Investigation, vol.10(4), pp.323-349,2013.
[13] Al Barghuthi, N.B. and Said, H., "Social networks IM forensics: Encryption analysis", Journal of Communications, vol.8(11), pp.708-15,2013.
[14] Zhang, X., Baggili, I., & Breitinger, F., "Breaking into the vault: Privacy, security and forensic analysis of Android vault applications", Computers & Security, Vol.70, pp.516-531,2017.
[15] Norouzizadeh Dezfouli, F., Dehghantanha, A., Eterovic-Soric, B., & Choo, K. K. R, "Investigating Social Networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms", Australian journal of forensic sciences, vol.48(4), pp.469-488,2016.
[16] Anglano, C, "Forensic analysis of WhatsApp Messenger on Android smartphones", Digital Investigation, vol.11(3), pp.201-213,2014.
[17] Moltisanti, M., Paratore, A., Battiato, S. and Saravo, L, "Image manipulation on Facebook for forensics evidence", In International Conference on Image Analysis and Processing, pp. 506-517. Springer, Cham,2015.
[18] Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A, "Mobile forensics: Advances, challenges, and research opportunities", IEEE Security & Privacy, vol.15(6), pp.42-51,2017.
[19] Deb, S. B. "Windows 8. x Facebook and Twitter Metro App Artifacts.",In IFIP International Conference on Digital Forensics, pp. 259-279. Springer, Cham,2016.
[20] Majeed, A., & Saleem, S, "Forensic analysis of social media apps in windows 10", NUST Journal of Engineering Sciences, vol.10(1), pp.37-45,2017.
[21] Yang, T.Y., Dehghantanha, A., Choo, K.K.R. and Muda, Z, "Windows instant messaging app forensics: Facebook and Skype as case studies", PloS one, vol.11(3),2019.
[22] Jones, G.M. and Winster, S.G, "Forensics analysis on smartphones using mobile forensics tools", International Journal of Computational Intelligence Research, vol.13(8), pp.1859-1869,2017.
[23] McDown, R. J., Varol, C., Carvajal, L., & Chen, L. "In-Depth Analysis of Computer Memory Acquisition Software for Forensic Purposes", Journal of forensic sciences, vol.61, pp. 110-116,2016.
[24] Ryu, J. H., Kim, N. Y., Kwon, B. W., Suk, S. K., Park, J. H., & Park, J. H, "Analysis of a Third-Party Application for Mobile Forensic Investigation", Journal of Information Processing Systems, vol.14(3),2018.
[25] Asim, M., Amjad, M. F., Iqbal, W., Afzal, H., Abbas, H., & Zhang, Y, "AndroKit: A toolkit for forensics analysis of web browsers on android platform", Future Generation Computer Systems, vol.94, pp.781-794,2019.
[26] Reddy, N, "Cloud Forensics", In Practical Cyber Forensics, Apress, Berkeley, CA, pp. 241-275,2019.
[27] Lin, F. Y., Huang, C. C., & Chang, P. Y, "A cloud-based forensics tracking scheme for online social network clients", Forensic science international, Vol.255, pp. 64-71,2015.
[28] Cloyd, T., Osborn, T., Ellingboe, B., Glisson, W. B., & Choo, K. K. R."Browser analysis of residual facebook data",In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications IEEE, pp. 1440-1445,2018.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495