Recursive Journal of Informatics
Vol. 2, No. 2, September 2024

p-ISSN 2963-5551 https://journal.unnes.ac.id/journals/index.php/rji e-ISSN 2986-6588

Development of Digital Forensic Framework for Anti-Forensic and Profiling Using Open Source Intelligence in Cyber Crime Investigation

Muhamad Faishol Hakim[1], Alamsyah[2]
[1,2]Informatics Engineering Study Program, Faculty of Mathematics and Natural Sciences,
Universitas Negeri Semarang, Indonesia

Abstract. Cybercrime is a crime that increases every year. The development of cyber crime occurs by utilizing mobile devices such as smartphones. So, it is necessary to have a scientific discipline that studies and handles cybercrime activities. Digital forensics is one of the disciplines that can be utilized in dealing with cyber crimes. One branch of digital forensic science is mobile forensics which studies forensic processes on mobile devices. However, in its development, cybercriminals also apply various techniques used to thwart the forensic investigation process. The technique used is called anti-forensics.

Purpose: It is necessary to have a process or framework that can be used as a reference in handling cybercrime cases in the forensic process. This research will modify the digital forensic investigation process. The stages of digital forensic investigations carried out consist of preparation, preservation, acquisition, examination, analysis, reporting, and presentation stages. The addition of the use of Open Source Intelligence (OSINT) and toolset centralization at the analysis stage is carried out to handle anti-forensics and add information from digital evidence that has been obtained in the previous stage.

Methods/Study design/approach: This research will modify the digital forensic investigation process. The stages of digital forensic investigations carried out consist of preparation, preservation, acquisition, examination, analysis, reporting, and presentation stages. The addition of the use of Open Source Intelligence (OSINT) and toolset centralization at the analysis stage is carried out to handle anti-forensics and add information from digital evidence that has been obtained in the previous stage. By testing the scenario data, the results are obtained in the form of processing additional information from the files obtained and information related to user names.

Result/Findings: The result is a digital forensic phase which concern on anti-forensic identification on media files and utilizing OSINT to perform crime suspect profiling based on the evidence collected in digital forensic investigation phase.

Novelty/Originality/Value: Found 3 new types of findings in the form of string data, one of which is a link, and 7 new types in the form of usernames which were not found in the use of digital forensic tools. From a total of 408 initial data and new findings with a total of 10 findings, the percentage of findings increased by 2.45%.

Keywords: Digital Forensic Framework, Open Source Intelligence, Anti Forensic, Mobile Forensic, Cyber Crime, Cyber Profiling.
Received Month 20xx / **Revised** Month 20xx / **Accepted** Month 20xx

INTRODUCTION

The onset of the disruption era has had a huge impact on human life, affecting all aspects of society. Now people depend on computer network services more than ever before. Based on the Indonesian Internet Service Providers Association (APJII) 2021-2022 (Q1) internet survey report [1], the penetration of internet users in Indonesia increased from 64.8% in 2018 to 77.02% of the total population of Indonesia. The more internet service users, the more information that can be obtained from the internet. The more information that is spread through the internet, the less privacy is owned. In addition, it also triggers the emergence of cybercrime. Cybercrime is defined as any crime committed using a computer or other means of communication that causes fear and anxiety in people or damages, harms, and destroys property [2]. The growth of cybercrime increases in line with technological developments.

The National Cyber and Crypto Agency (BSSN) and the Indonesian Honeypot Project (IHP), provide an information system related to cyber-attacks in Indonesia on the page https://honeynet.bssn.go.id/. Based on

[1]*Corresponding author.
Email addresses: faisholhakim@students.unnes.ac.id
DOI: 10.15294/rji.v8i1.25356

the 2021 Honeynet Project annual report by the National Cyber and Crypto Agency (2021), Indonesia ranks second internationally as the country with the highest source of cyber-attacks with a total of 32,091,240 attacks. Therefore, cybersecurity is an important sector to develop, especially through research in line with the industrial revolution.

Cyberattacks or digital crimes are nothing new. With the shift of crime to cyberspace, a new discipline called computer forensics is needed, to collect electronic evidence scientifically and technically, investigate and present the findings to law enforcement agencies to prove the crime [3]. Digital forensics itself is the application of computer science and technology for the benefit of legal proof (pro-justice) which in this case proves high-tech or computer crimes scientifically to be able to obtain digital evidence that can be used against offenders [4]. Conventional digital forensic practices imply the seizure and collection of everything that has the potential to become evidence [5]. The digital forensic data acquisition approach is carried out for thorough data retrieval to observe relevant and valid evidence to be used as evidence in a legal case issue [6]. In its development, the focus of studies on digital forensics is increasingly detailed.

The process in cybercrime investigation is also organised into several steps as a reference in the development of the investigation. Several frameworks in digital forensic investigation are applied depending on the specific case or objective to achieve the desired results by the investigator. Generally, frameworks are suggested for specific fields and are based on practitioners' experience and previous work. These frameworks or process models are essential to speed up the forensic digital investigation process [5]. Such as the CDFIPM model, which is a process model to deal with identified issues, such as harmonising and building on existing models [7]. Other models focus on specific areas and make modifications to focus on online social networks [5, 8].

However, in practice, digital evidence collection is not always done well. Cybercrime is also growing and can interfere with the collection of digital evidence. Attempts to thwart the process of analysing forensic digital evidence by complicating, or even making it unfinishable are called anti-forensics [9]. These actions are carried out by cybercriminals with a specific purpose and with certain techniques. Anti-forensic techniques can completely change the analysis results by providing false information to forensic experts. Data deletion, data hiding, steganography, encryption, erasure, data state restoration, and attacks on forensic tools are common techniques used in anti-forensics [10]. To ensure the achievement of the goal, some attackers combine several anti-forensic techniques, so that the attacker can escape the identification of existing evidence.

The impact of anti-forensics can reduce or even eliminate important information as evidence. This results in fewer data sources to analyse. Existing methods focus on specific frameworks or fields. It is necessary to collect data for profiling as a follow-up to the investigation process based on the evidence found. One way to gain more information is by utilising cyber intelligence. Cyber intelligence, which is knowledge generated through data and information about cyber threats and their perpetrators, is one of the tools explored for this purpose.

Open-Source Intelligence (OSINT) is one area of data collection [11]. OSINT consists of the collection, processing, and correlation of public information from open data sources such as mass media, social networks, forums and blogs, government public data, publications, or commercial data [12]. By utilising OSINT to collect data, it can help in the process of investigating cybercrime cases. The amount of data available from analysing forensic digital evidence suggests there is a wealth of information that can potentially be enhanced with open-source intelligence data to enable a better understanding of events or people, and greater decision-making opportunities [13].

This research intends to develop a digital forensic investigation process framework to deal with cybercrimes that utilise anti-forensics to erase traces and complicate the evidence collection process, as well as follow-up to profiling the attacker by utilising OSINT.

METHODS

In this study, anti-forensic investigations and the use of OSINT in mobile forensics will be carried out. The implementation of the mobile forensic investigation model in this study adapted the model process from [14]. Then carried out the implementation of anti-forensic investigations based on research [9]. Meanwhile, the use of OSINT in carrying out crime suspect profiling implements the writings of [15].

Case Scenario

The simulation data used in this study was obtained from the Huawei Y3II smartphone device. The scenario was prepared because the National Institute of Standards and Technology (NIST), a non-regulatory body within the Technology Administration section of the United States Department of Commerce, states that in order to conduct tests, all tools and devices must be listed. The simulation procedure is required in this study to mimic the behavior of the actual system in order to prove the problem formulation. Because it is impossible to investigate real-world scenarios, simulations are used. The data used in the investigation is collected from the device under investigation and can be seen in Figure 1.

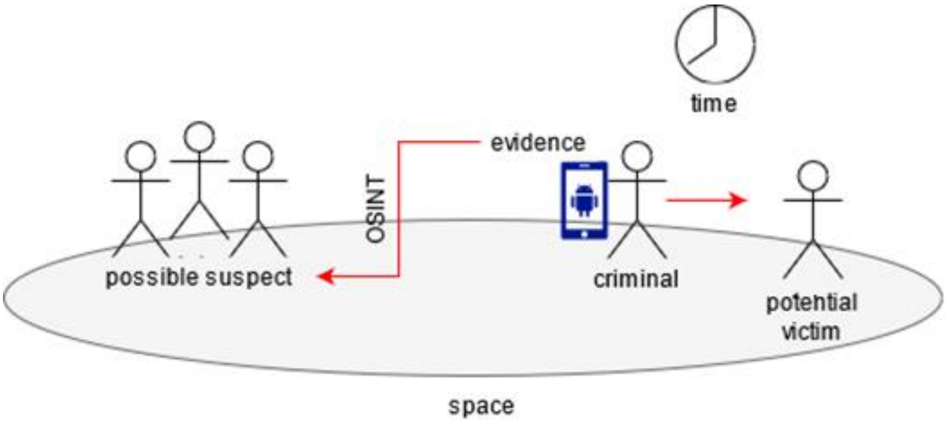


Figure 1. Case Scenario

According to research references from [16] the scenario that will be carried out in this stage is as follows:

1. A suspect is a cyber actor who has data from a data leak incident and attempts to sell and buy it.
2. Digital evidence in the form of a media carrying data obtained from the Suspect.
3. By saving the evidence in local storage, the media in question is discovered on a smartphone as the main evidence.
4. Anti-forensic techniques such as tampering, data masking, and data wiping on transmission media are used.
5. The smartphone is then purchased as the primary proof, which is subsequently analyzed.
6. An acquisition evidence analysis is performed to collect the appropriate digital evidence.
7. Use OSINT to investigate the information collected from the acquisition.
8. The following stage is suspect profiling of previous instances using OSINT information.

Digital Forensic Framework

It is proposed in this study to adjust the digital forensic investigation process to detect more deeply associated anti-forensic applications and to employ OSINT to further improve the investigative process in order to determine the profile of a person or organization. The set of tools for assisting with the digital forensic procedure is also included. Following the steps taken in this study, [17-19] conducted research:

1. Gather information about cybercrime cases including mobile forensics and the necessity for forensic analysis.
2. Identify the events that occurred in the form of cybercrime occurrences.
3. Plan ahead of time and assess what needs to be met during the investigative process, which may include the usage of additional instruments and gadgets.
4. Gather and keep evidence of crucial findings, as well as identify existing findings.
5. Acquiring digital evidence by imaging it, then duplicating image files as backup data and to maintain the credibility of the evidence.
6. Extracting the image file followed by an analysis of the digital evidence found. This stage is focused on finding out the incident and identifying whether there is use of anti-forensics. If indeed anti-forensic is found, then the process continues to identify what techniques were used to then be restored and analyzed again until no anti-forensic identification is identified.
7. The findings from the results of the analysis are then studied and continued with a more in-depth investigation by utilizing the metadata and information that has been obtained in previous processes to be traced using OSINT.

8. Then, if in the OSINT process important information is found related to the incident that occurred, especially related to the identity of a person or organization, then a profiling process is carried out to record this information. If no information is found that is considered important or related to the incident that occurred, the process continues at the reporting stage.
9. The results of this research will get output in the form of reports related to incidents that occurred and existing findings. It also includes explaining the process carried out and other requirements needed.

The digital forensic framework can be seen in Figure 2.

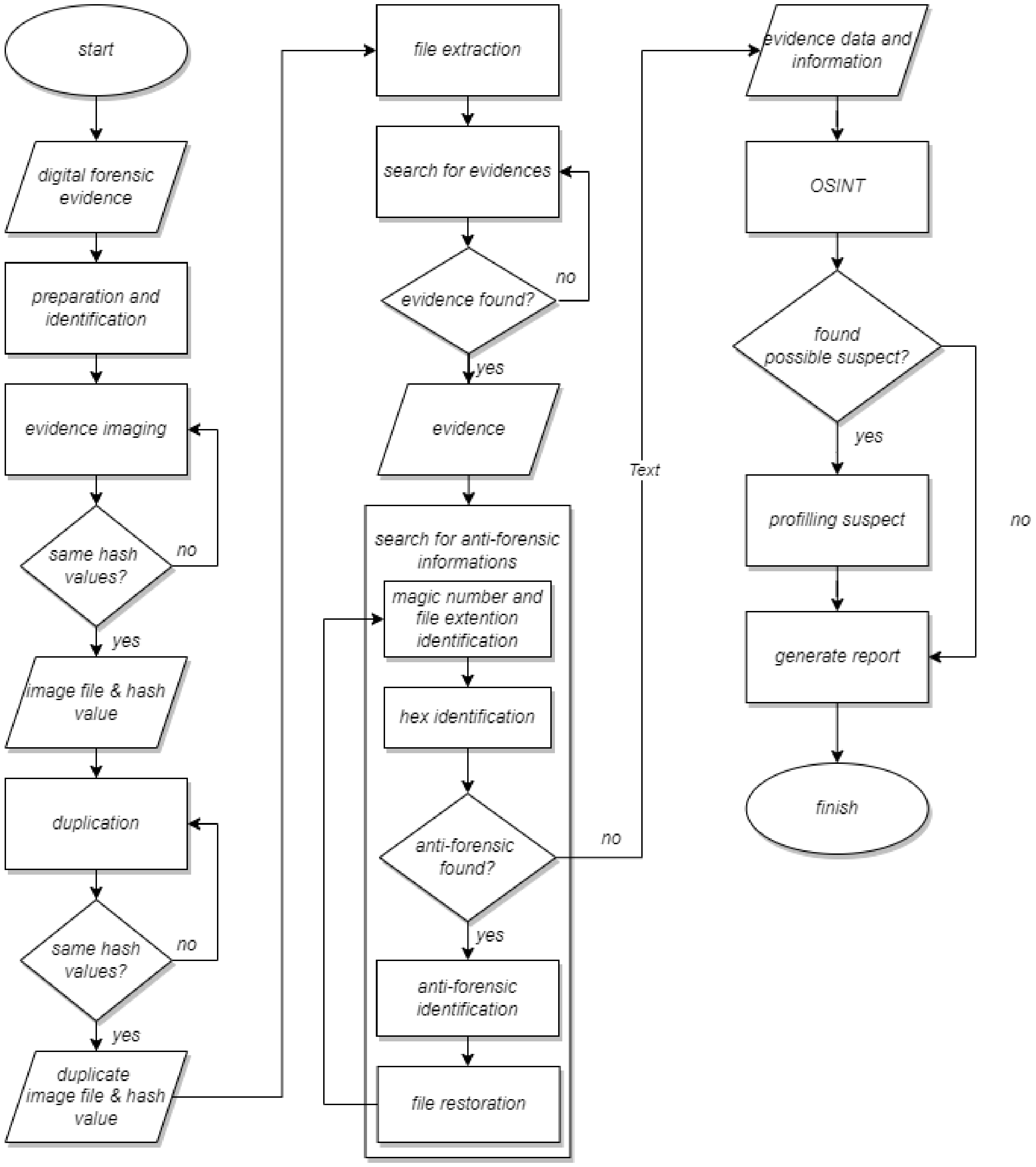


Figure 2. Digital Forensic Phase

Evaluation and Validation

The evaluation stage in this study was carried out by comparing the results of digital evidence and information that can be obtained from the process of analyzing digital evidence investigations. Apart from that, to guarantee the value of the findings of the existing evidence, a hash value comparison was also carried out from the initial data and after the investigation was carried out. The hash functions used are MD5 and SHA1 to ensure that there are no hash collisions [20].

RESULT AND DISCUSSION

In this chapter, several steps are taken to obtain the results of digital evidence acquisition from digital forensic investigations. The steps for obtaining digital evidence from digital investigations consist of seven stages, namely preparation, preservation, acquisition, examination, analysis, reporting, and presentation. The model framework to be carried out can be seen in Figure 3.

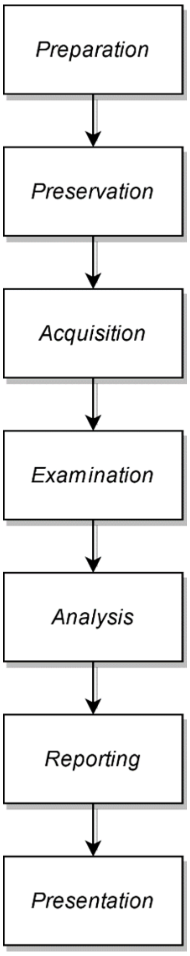


Figure 3. Digital Forensic Framework Phase

This is the first stage in the investigation. This stage is carried out to prepare related to the case that occurred. preparations are made by paying attention to the events and digital evidence obtained.

The evidence obtained in this case is a Huawei Y3II smartphone in active condition. Then identification is carried out in the form of where and how the evidence is stored, the specifications of the evidence, and the condition of the evidence. The software and hardware requirements used in this study are as follows:

1. Hardware:
   a. HP Pavillion 14-af118au laptop
   b. Micro USB cable
2. Software:
   c. Magnets AXIOM 4.10.0.23663
   d. Autopsy 4.19.3
   e. Steganalysis Tools (Steghide, Zsteg, Stegsnow, Stegsolve),
   f. Cryptanalysis tools (CyberChef).

Maintenance of evidence is carried out through network isolation using Faraday pockets and activation of airplane mode on evidence, so that no network or signals can affect or damage evidence. In doing so, this can help ensure the integrity of the evidence obtained and keep it safe and effectively used in research. Below shows an image of preservation with airplane mode in the document which can be seen in Figure 4 and the use of faraday bags.

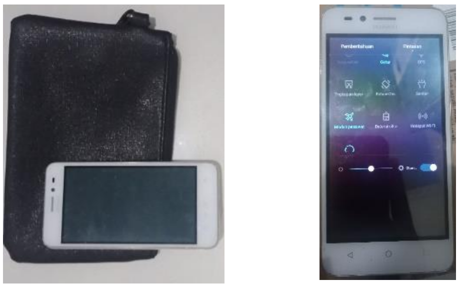
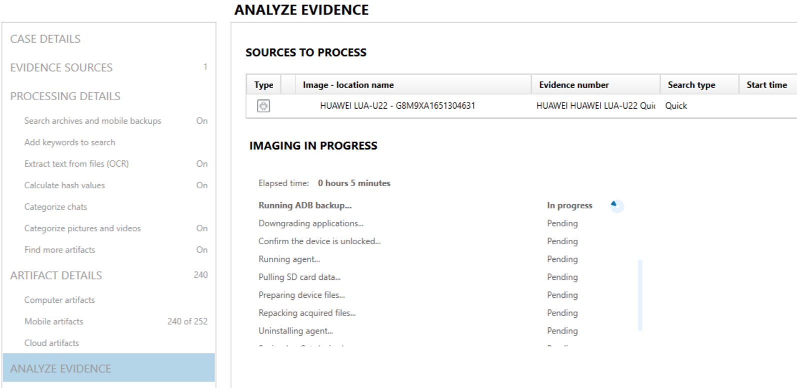


Figure 4. Preservation Using Flight Mode and Faraday Bag

The acquisition process is carried out using the Magnet Axiom with the quick imaging option. At this stage of the acquisition, duplication of evidence is also carried out and can be seen in figure 5.



ANALYZE EVIDENCE

CASE DETAILS
EVIDENCE SOURCES 1
PROCESSING DETAILS
Search archives and mobile backups On
Add keywords to search
Extract text from files (OCR) On
Calculate hash values On
Categorize chats
Categorize pictures and videos On
Find more artifacts On
ARTIFACT DETAILS 240
Computer artifacts
Mobile artifacts 240 of 252
Cloud artifacts
ANALYZE EVIDENCE

SOURCES TO PROCESS

Type	Image - location name	Evidence number	Search type	Start time
	HUAWEI LUA-U22 - G8M9XA1651304631	HUAWEI HUAWEI LUA-U22 Qui	Quick	

IMAGING IN PROGRESS

Elapsed time: 0 hours 5 minutes

```
Running ADB backup...            In progress
Downgrading applications...      Pending
Confirm the device is unlocked... Pending
Running agent...                 Pending
Pulling SD card data...          Pending
Preparing device files...        Pending
Repacking acquired files...      Pending
Uninstalling agent...            Pending
```

Figure 5. Analysis Using Magnet Axiom

This is done to avoid changes that occur to the original evidence during analysis and serves as a data backup, duplication results are hashed to maintain the authenticity of the evidence. The acquisition process lasted for 4 hours 43 minutes. At this stage there is a transformation of physical evidence into digital evidence which is presented in Table 1.

Table 1. Image Acquired from Evidence

Name	MD5 *checksum*	SHA1 *checksum*
HUAWEI HUAWEI LUA-U22 Quick Image	C718D9FA45CC357ACB3050A29A39F049	0F4486AA5B4E9D4E84FEA448084C7ADD5733C4F2

Digital evidence that has been obtained from the acquisition stage is then examined. At this stage, digital evidence extraction is carried out from the acquisition process to determine relevant data for further analysis at a later stage. The extraction process is carried out using an Autopsy tool. Obtained data that is considered encrypted in .jpeg format and also image data in .jpg format. with an encryption detected label for detailed data analysis results that are considered important and can be seen in Table 2.

Table 2. Evidence Acquired

Name	Tag	MD5 *Checksum*	SHA1 *Checksum*
WhatsApp Image 2021-02-22 at 02.03.14.jpeg	Encryption Detected	375dbd0ee50910c40031d5de3fdea978	1ad8cee5a57840da47d662cf8cadaf0680835b45
Name	Tag	MD5 *Checksum*	SHA1 *Checksum*
IMG_20220224_191552.jpg	Exif Metadata	ebdea671f62edd334b13f8d83b8a2083	09222ce9378f9c1c791a73c0f87a1d653333c0a8

The acquired data is then copied for use in the analysis stage processing. To verify the similarity of the evidence gathered before and after the extraction procedure is carried out using the Autopsy tool, the hash checksum value of the evidence obtained is employed. WhatsApp Image 2021-02-22 at 02.03.14.jpeg is one of the digital pieces of evidence files that Autopsy has identified as an encrypted file, but it is unable to perform any more investigation on it. Then, a file with the name IMG_20220224_191552.jpg has the Exif Metadata designation, indicating that it is an image file.

The analysis phase modifies the phase include adding to the analysis phase with case studies on digital evidence that is given anti-forensic treatment and adding processes before entering the reporting stage by increasing the scale of digital forensic investigations that utilize digital evidence that has been obtained at the analysis stage through searching for possible suspects or suspects who have links with perpetrators who directly touch digital evidence.

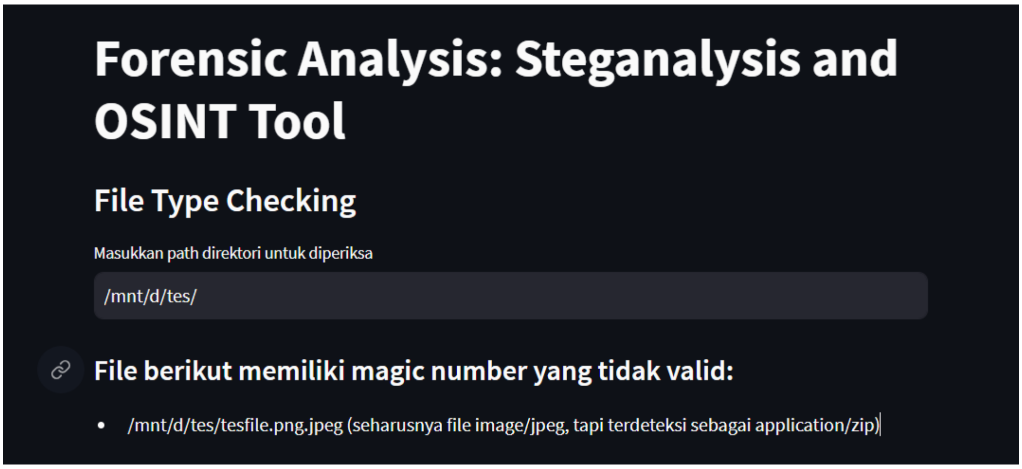
The search was carried out by utilizing open information sources, or OSINT and mapping was carried out obtained from public sources such as mass media and social media. The search process is also carried out by utilizing open-source tools such as Maltego and Sherlock. The results obtained from the addition of this investigative process also provide more results and can be used as a reference or additional information in the next stage to strengthen the evidence that has been obtained.

The difference in the results obtained became quite significant after using OSINT as an option in expanding digital forensic investigations. If we look back at the investigation process in general and adjust it to the investigative process being carried out. Here the table of common toolset and framework result in Table 3.

Table 3. Result Before Using Proposed Framework

No	Name	Data Type
1.	/IMG_20220224_191552.jpg	Gambar
2.	WhatsApp Ima2ge 2021-02-22 at 02.03.14.jpeg	Gambar (encrypted)
3.	kliwonzervalo@gmail.com	Email
4.	alinakor2202@gmail.com	Email
5.	janakovac@podjetje.com	Email

In the process of digital forensic investigations, the use of the same analytical tools as in the initial stages can produce two important types of data in the form of images. However, if you only rely on the same analytical tools, the investigation process is only able to identify the types of digital evidence data but is limited in its capabilities which are only limited to identifying these types of data. Figure 5 shows the Tools Developed in the Analysis Phase.



Forensic Analysis: Steganalysis and OSINT Tool

File Type Checking

Masukkan path direktori untuk diperiksa

/mnt/d/tes/

File berikut memiliki magic number yang tidak valid:

- /mnt/d/tes/tesfile.png.jpeg (seharusnya file image/jpeg, tapi terdeteksi sebagai application/zip)

Figure 6. Developed Tools in Analysis Phase

Therefore, even if it can mark digital evidence as encrypted or suspicious files, it will be constrained in taking further action. Next are the results obtained in the digital forensic investigation process with modifications and additions to some of the processes and show in Table 4.

Table 4. Information and Evidence Gathered Using Proposed Framework

No	Name	Data Type
1.	IMG_20220224_191552.jpg	Gambar
2.	WhatsApp Ima2ge 2021-02-22 at 02.03.14.jpeg	Gambar (encrypted)
3.	WhatsApp Ima2ge 2021-02-22 at 02.03.14.jpeg	Archive file
4.	kliwonzervalo@gmail.com	Email
5.	alinakor2202@gmail.com	Email
6.	janakovac@podjetje.com	Email
7.	cat cat.1.jpg cat.2.jpg cat.3.jpg cat.4.jpg cat.5.jpg … cat.151.jpg	Gambar
8.	dog.1.jpg dog.2.jpg dog.3.jpg dog.4.jpg dog.5.jpg … dog.202.jpg	Gambar
9.	cat.112.jpg	Unknown file
10.	https://pastebin.com/TwXmgSXS	Link string
11.	64;58;32;91;64encoded fGMxSCozRE47SXJIWEN+V2JKWnp0I1FZQE1eRjJsZmVRNTMvdiNqKkc2Y0tWdzdSfnEyMGw5RTZzN3dPWndnZSUhdi8rM0VZUjgvZzA3cmEqREo7SDMzakZOallBUCJkaXoqY3cjb1M4NytaOyslWUI4YzpmdkBNUzJ1SCFsI1JBZEsuY3YpU0E4c09yNn5kQjJ0MCE4SnAyNkIuNl0pZm9YV2NGd1BwaEo7SWs3I1JybEpiTSFYcD00Y1Jad35kd3olejt5fFhSOEpVK1tSYklYMy9Ga2lNYDZEbGZPKGZ1ZkxkJWtkcD9QbGN3NypmVzJPMGI3aUAjUGRLWXYkZW96b2Uva2lNOkw+SSFbN1hjMkQ6RzNwSC4zTXshQw==	Encoded string
12.	https://drive.google.com/drive/u/2/folders/1GBUaK291ueoPW0-yllh8g_wo_KUCyAAX	Link string
13.	Kliwonzervalo Son1x Son1x666 theninjaway1337 YourAnonS0u1 DarkArmyChannel UmRefugioNoUniverso inconscienteliterario	Username

Found a number of 3 new types of findings in the form of string data, one of which is a link and 7 new types in the form of usernames which are not found in the use of digital forensic tools. From a total of 408 initial data and new findings with a total of 10 findings, the percentage of findings increased by 2.45%. By using the investigative process and the toolset used, a number of results were obtained that were different from the investigative process used in the study [21]. The research carried out is in line with the research [21], the results obtained from the investigation of cybercrime cases carried out by utilizing the toolset used, obtained digital evidence in the form of files with image extensions but one of the pieces of evidence is indicated as an encrypted file. Investigations with the toolset used in [21] cannot perform descriptions and identification of encrypted files. Furthermore, there is an increase in the results of investigations obtained by adding tools to the process of analyzing digital evidence obtained, the toolset developed is specifically aimed at identifying media files such as images, text, and archive files. Besides being able to identify the associated password used in encrypted files, using OSINT as a combination in the system developed in the analysis process can also obtain better results in the form of profiling data from usernames obtained in digital evidence investigations and can be seen in Figure 7.

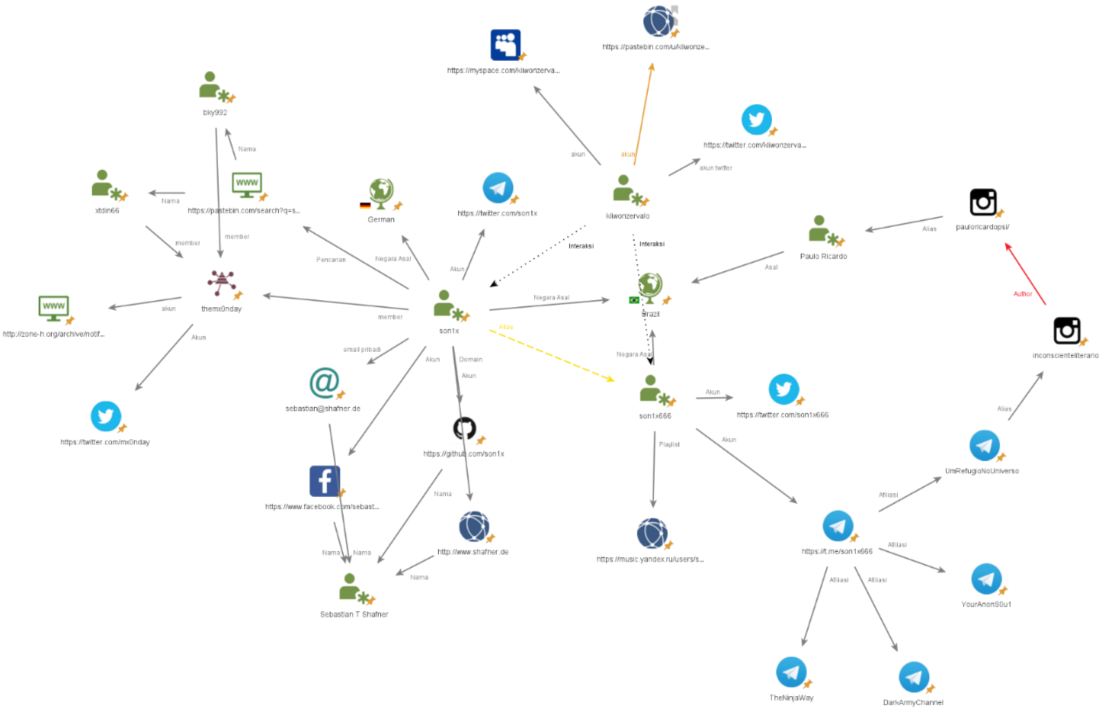


Figure 7. Profiling Result from Gathered Information

CONCLUSION

Based on the results of research and discussion related to anti-forensic analysis and investigation on mobile forensics with open-source intelligence as crime suspect profiling, the following conclusions can be drawn. The investigative process in mobile forensics in identifying anti-forensics consists of the stages of preparation, preservation, acquisition, examination, analysis, reporting, presentation. Anti-forensic identification and use of OSINT is carried out at the analysis stage with several toolsets used Utilization of OSINT at the analysis stage can expand information from data obtained in the previous process in the form of some new username information. From a total of 408 initial data and new findings with a total of 10 findings, the percentage of findings increased by 2.45%. In the future research, maximize the toolset used by adding other tools that can identify more types of digital evidence, not just media files and combine machine learning in the analysis and profiling process using OSINT to shorten the time dealing with large amounts of data sources with more false positives.

REFERENCES

[1] APJII. "Laporan survei internet APJII 2019 – 2020." Asosiasi Penyelenggara Jasa Internet Indonesia. https://apjii.or.id/survei (accessed 15 Agustus, 2023).

[2] W. A. Al-Khater, S. Al-Maadeed, A. A. Ahmed, A. S. Sadiq, and M. K. Khan, "Comprehensive review of cybercrime detection techniques," *IEEE Access*, vol. 8, pp. 137293-137311, 2020, doi: 10.1109/ACCESS.2020.3011259.

[3] M. Gul and E. Kugu, "A survey on anti-forensics techniques," *2017 International Artificial Intelligence and Data Processing Symposium (IDAP)*, pp. 1-6, 2017, doi: 10.1109/IDAP.2017.8090341.

[4] I. Riadi, A. Yudhana, and M. C. F. Putra, "Forensic tool comparison on instagram digital evidence based on android with the nist method," *Scientific Journal of Informatics*, vol. 5, no. 2, pp. 235-247, 2018, doi: 10.15294/sji.v5i2.16545.

[5] H. Arshad, E. Omlara, I. O. Abiodun, and A. Aminu, "A semi-automated forensic investigation model for online social networks," *Computers & Security*, vol. 97, p. 101946, 2020, doi: 10.1016/j.cose.2020.101946.

[6] K. Budiman, N. Zaatsiyah, U. Niswah, and F. M. N. Faizi, "Analysis of sexual harassment tweet sentiment on twitter in Indonesia using naïve Bayes method through national institute of standard and technology digital forensic acquisition approach," *Journal of Advances in Information Systems and Technology*, vol. 2, no. 2, pp. 21-30, 2020, doi: 10.15294/jaist.v2i2.44305.

[7] R. Montasari, "A comprehensive digital forensic investigation process model," *International Journal of Electronic Security and Digital Forensics,* vol. 8, no. 4, pp. 285-302, 2016, doi: 10.1504/IJESDF.2016.079430.

[8] Y.-J. Jang and J. Kwak, "Digital forensics investigation methodology applicable for social network services," *Multimedia Tools and Applications,* vol. 74, pp. 5029-5040, 2015, doi: 10.1007/s11042-014-2061-8.

[9] S. Rekhis and N. Boudriga, "A system for formal digital forensic investigation aware of anti-forensic attacks," *IEEE transactions on information forensics and security,* vol. 7, no. 2, pp. 635-650, 2011, doi: 10.1109/TIFS.2011.2176117.

[10] H. Riaz and M. A. Tahir, "Analysis of VMware virtual machine in forensics and anti-forensics paradigm," *6th International Symposium on Digital Forensic and Security (ISDFS),* pp. 1-6, 2018 2018, doi: 10.1109/ISDFS.2018.8355375.

[11] A. Magalhães and J. P. Magalhães, "Textractor: An OSINT tool to extract and analyse audio/video content," *Innovation, Engineering and Entrepreneurship,* vol. 505, pp. 3-9, 2019 2019, doi: 10.1007/978-3-319-91334-6_1.

[12] J. Pastor-Galindo, P. Nespoli, F. G. Mármol, and G. M. Pérez, "The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends," *IEEE Access,* vol. 8, pp. 10282-10304, 2020, doi: 10.1109/ACCESS.2020.2965257.

[13] D. Quick and K.-K. R. Choo, "Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+ OSINT): A timely and cohesive mix," *Future Generation Computer Systems,* vol. 78, pp. 558-567, 2018, doi: 10.1016/j.future.2016.12.032.

[14] A. Al-Dhaqm, S. Abd Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A review of mobile forensic investigation process models," *IEEE access,* vol. 8, pp. 173359-173375, 2020, doi: 10.1109/ACCESS.2020.3014615.

[15] S. Al-khateeb and N. Agarwal, "Social cyber forensics: leveraging open source information and social network analysis to advance cyber security informatics," *Computational and Mathematical Organization Theory,* vol. 26, no. 4, pp. 412-430, 2020, doi: 10.1007/s10588-019-09296-3.

[16] T. Tajuddin, A. Abd Manaf, N. F. Awang, S. R. M. Dawam, N. R. Ali, and R. Amat, "Crime Suspect Profiling (CSP) for forensic investigation on smartphone," *2019 4th International Conference and Workshops on Recent Advances and Innovations in Engineering (ICRAIE),* pp. 1-6, 2019 2019, doi: 10.1109/ICRAIE47735.2019.9037772.

[17] J. K. Alhassan, R. T. Oguntoye, S. Misra, A. Adewumi, R. Maskeliūnas, and R. Damaševičius, "Comparative evaluation of mobile forensic tools," *Proceedings of the International Conference on Information Technology & Systems (ICITS 2018),* pp. 105-114, 2018 2018, doi: 10.1007/978-3-319-73450-7_11.

[18] M. Riskiyadi, "Investigasi forensik terhadap bukti digital dalam mengungkap cybercrime," *Cyber Security dan Forensik Digital,* vol. 3, no. 2, pp. 12-21, 2020, doi: 10.14421/csecurity.2020.3.2.2144.

[19] S. Soltani and S. A. H. Seno, "A survey on digital evidence collection and analysis," *7th International Conference on Computer and Knowledge Engineering (ICCKE),* pp. 247-253, 2017 2017, doi: 10.1109/ICCKE.2017.8167885.

[20] A. P. Kuncoro, I. Riadi, and A. Luthfi, "Mobile forensics development of mobile banking application using static forensic," *International Journal of Computer Applications,* vol. 975, no. 1, 160, p. 8887, 2017.

[21] M. Goel and V. Kumar, "Layered framework for mobile forensics analysis," *Proceedings of 2nd international conference on advanced computing and software engineering (icacse),* 2019 2019, doi: 10.2139/ssrn.3351029.