Detection and Investigation Model for the Hard Disk Drive Attacks using FTK Imager

Ahmad Alshammari
Department of Computer Sciences-Faculty of Computing and Information Technology,
Northern Border University, Rafha, Kingdom of Saudi Arabia

***Abstract*—A computer hard disk drive (HDD) is a device that stores, organizes, and manages computer data. In general, it is used for system storage, in which the computer maintains its operating system and other programs. A hard disk drive can, however, be physically damaged as well as affected by software errors, data corruption, and viruses that are used by attackers to cause damage. This study aims to develop a detection and investigation model (DIM) for HDD to detect and investigate HDD attacks using the FTK Imager forensic tool. The design science method is adapted to develop and evaluate the DIM. The developed DIM consists of three main phases: detection, gathering, and analysis. In order to evaluate the capabilities of the developed DIM for HDD, a real scenario was used. According to the results, the DIM can detect and investigate the HDD easily using FTK Imager. Thus, organizations can use the developed DIM to detect, investigate, mitigate, or avoid HDD threats.**

Keywords*—HDD; cybercrimes; design science method; digital forensic tools; FTK imager

I. Introduction

Nowadays, cybercrime is becoming more prevalent, resulting in an adverse impact on the availability, confidentiality, and integrity of data stored on hard drives and in the cloud [1]. It is also notoriously known as one of the major threats for organization since they are obligated to spend fortune to protect their data from this. Companies must invest in sophisticated security systems, such as firewalls, anti-virus software, authentication, and encryption, to reduce their vulnerability to cybercrime [2]. In addition, organizations are equipping their employees with knowledge and training on cybersecurity best practices such as, enforcing the use of strong passwords and securing confidential data. Besides, organizations added a top notch security on their network to monitor against any malicious activity [3]. All these measures contribute to the reduction of cybercrime risks and the protection of data stored on hard drives and in the cloud.

HDDs are the most crucial component in a computer system [4], [5]. HDDs store both physical and logical data, which is the primary objective of an adversary. These devices are frequently used to store personal data such as photographs, music, documents, and applications stored on a computer [6]. Usually, the attackers aim for the HDDs to gain access to the data stored on them. By obtaining physical access to the system, they may be able to access the HDD data. In addition, they may attempt to extract data from the HDD using malicious software, such as spyware [7], [8].

Therefore, this study aims to develop a model for detecting and investigating HDD attacks using the FTK Imager software. For this purpose, the design science methodology is employed. The design science method is a research methodology that concentrates on the creation and evaluation of artefacts for the resolution of real-world issues. The developed detection and investigation model is comprised of three main phases: detection, collection, and analysis. Each phase of the investigation includes a series of activities designed to aid the investigator in detecting and investigating attacks on hard disc drives (HDDs).

Digital forensics software package FTK (Forensic Toolkit) is used to perform forensic analysis and digital investigations on computers and mobile devices [9]. It is used by law enforcement, the military, and business inspectors to examine computer activity. It can locate and analyse data associated with Internet activity, deleted files, emails, documents, and images, among other types of information. It includes data recovery, analysis, and reporting utilities. There are several contributions of this study, including improving HDD security by detecting and investigating potential threats before an incident occurs. It also enhances HDD's ability to identify and investigate potential threats more rapidly and the ability of organizations to respond rapidly and swiftly in the event of any possible attacks. Detection and investigation models can help companies educate themselves about potential threats.

The paper is organized as follows: Section II introduces the related works, and Section III introduces the methodology. Section IV introduces the results and discussion. Section V offers a conclusion and further work.

II. Related Work

Many forensic models, tools, strategies, processes, procedures, policies, models, and mechanisms have been proposed to assist with the detection and investigation of HDD attacks. These include data extraction, forensic file system analysis, low-level analysis, data recovery, and forensic imaging, among others. For example, a process model was proposed by the authors of [10] based on the following requirements: the model must be based on existing theory in physical crime investigations; the model must be practical and perform the same steps as the real study; the model should be technically generic and not limited to existing products and procedures; the model must be specific enough to further develop general technological requirements for each stage; the model should be abstract and applicable to law enforcement investigations, business investigations and incident response.

The authors of [11] proposed another (similar) event-based process model This model is also based on physical crime scene investigations and suggests that digital crime scene investigations be conducted as part of physical crime scene investigations. This paper focuses on the steps involved in digital crime scene investigation and determining the causes and effects of events in digital forensics.

The authors of [12] proposed a digital forensic investigation process known as an incident model, which includes the following steps: pre-incident preparation, incident detection, initial response, response strategy formulation, redundancy (system backup), investigation, security. remediation (shutdown and containment of suspect system), network monitoring, recovery (reset of suspect system to initial state), reporting and follow-up.

The authors of [13] proposed a goal-based hierarchical process model for digital forensics and also conducted a detailed comparison between the proposed process model and previous work in the field. Their proposed model has multiple layers, which is a novel approach.

The authors of [14] proposed a comprehensive cybercrime investigation model that is very detailed. The proposed model also includes a description of information flow between different stages.

A process model was proposed by the authors of [15] which includes the following steps: identification, collection, conservation, transportation, preservation, analysis, interpretation, assignment, reconstruction, presentation and destruction.

The authors of [16] defined the stages of the digital forensics process: gathering information and making observations, formulating a hypothesis to explain the observations, evaluating the hypothesis, drawing conclusions, and communicating the results.

The authors of [17] proposed a mutual database that includes the design science research method of forensic investigation processes. The four stages proposed of this process consist of, namely: 1) identification; 2) artefact assembly; 3) artefact analysis; and 4) documentation and delivery processes. This lets us align everyone's concepts and terms common database forensics processes.

The authors of [18] developed a coordinated database pre-search model based on three main categories (i.e., planning, preparation and pre-response, acquisition and preservation, analysis and reconstruction) In addition, the forensic database is designed to avoid confusion or ambiguity and to provide practitioners with a systematic approach to performing DBFI with a greater degree of certainty.

The authors of [19] developed a metamodel forensic database field. Then identified, extracted and proposed the municipality concept and concept definitions are aligned to propose a meta-model. They have applied the metamodeling process to ensure that it is a metamodel comprehensive and consistent.

The authors of [20] developed a unified model begin to treat and organize the mobile foreign domain using the meta-modelling method. The authors [21] proposed an integrated an incident response template to identify a database forensics field, respond to, mitigate, and recover from a potential database incident.

The authors in [5] proposed a new forensic method, a readiness system called drone forensics using design science method. The supported model consists of two phases: i) the active forensic phase and (ii) reactive forensics phase. The authors developed uniform forensics Forensic Database Field Template. The model is designed to be efficient and a comprehensive approach to forensic database investigation, addressing challenges in collection and analysis of digital evidence. The authors created a drone forensic metamodel. The developed meta-model ensured a uniform approach collect and organize evidence that allows the investigator to a to better understand the event.

The authors [22] developed the Internet of Things Metamodel of forensic investigation. The developed metamodel provided a detailed overview of the various stages of the investigation, from initial collection of evidence for potential identification and analysis problems. It is designed to be technology agnostic and scalable can be adapted to various scenarios. Additionally, several digital forensic works have been proposed to detect, and investigate the threats and risks of organizations.

III. Research Methodology

This study adapted the design science method to develop a detection and investigation model for HDD. The design science method is a research method that involves creating a solution to a problem, then analysing the effectiveness of the solution [23]. The process involves creating the solution, testing the solution, and refining the solution as needed. The design science method is particularly useful for developing systems or models such as the HDD detection and investigation model. Fig. 1 illustrates the development process for developing and validating DIM for HDD. The development process involves three stages:

Stage 1: Recognizing and selecting digital forensic models: This stage aims to identify and select appropriate digital forensic models from the literature for development purposes. It contains the following steps:

- Set recognized and selected criteria: To select the digital forensic models that are used in this study from the literature, the researcher looked at models that focused only on HDD, pen drive, RAM, and CD.
- Select the common Search Engines: For this study, five common search engines have been selected for searching and discovering digital forensics models: IEEE Explorer, Scopus, Web of Science, Springer, and Google Scholar.
- Assign a search protocol: The time and keywords were used for this study. The searching period is between 2015 and 2023, and the keywords are “Digital Forensic", "Hard Disk Drive Forensic", and "Pin Derived Forensic", "Memory Forensic".

- Filter the recognized and selected models: The results of the search yielded over 11,300 results from the search engines. These results were filtered to exclude results that were not related to the topic of HDD forensics. After the filtering process, the search yielded over 12 results that were relevant to the HDD forensics purely as shown in Table I.

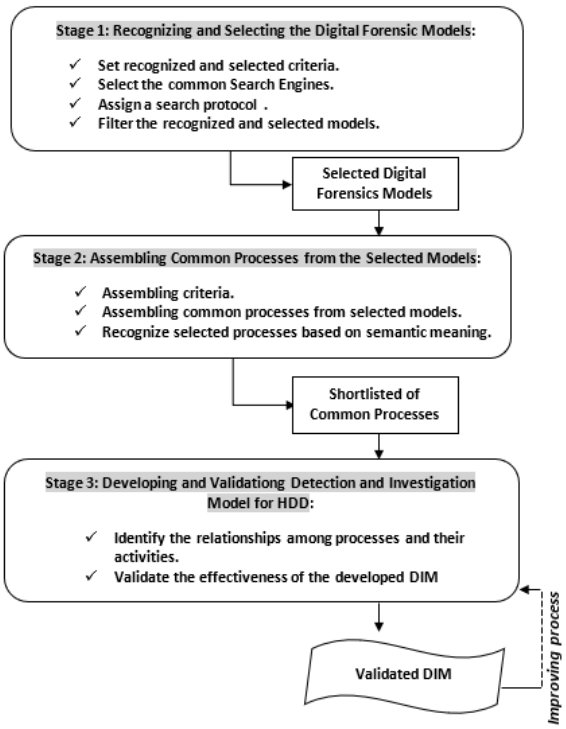

Fig. 1. Development process for developing and validating DIM for HDD.

TABLE I. SELECTED HDD FORENSIC MODELS

ID	Year	Title	Advantages
1	2018	Digital forensic analysis of hard disk for evidence collection [24]	In this study, authors have discussed the significance of digital forensic examination of file systems to recover removed data from hard disks.
2	2017	Towards subverting hard disk firmware boot kits [25]	It was demonstrated by the authors that firmware boot kits can be identified, and several options were offered for how even deep-seated firmware rootkits can be identified as well.
3	2015	The differences between SSD and HDD technology regarding forensic investigations [26]	The focus of this study was to enhance the storage space of the system by utilizing SSD, which is a much quicker and further consistent storage device than old HDD.
4	2022	Comparing HDD to SSD from a Digital Forensic Perspective [27]	From a digital forensic viewpoint, this study examined in depth the results obtained from forensics software on HDD and SSD to determine whether there is a difference between the two drives in terms of forensics.
5	2019	A Comparative Study of Analysis and Extraction of Digital Forensic Evidence from exhibits using Disk Forensic Tools [28]	The aim of this study was to provide a process for searching for evidence, the process may be a little simple or a little complicated. This would involve the location of a file saved on the device, or it could involve more complex processes that would involve hex sweeping or carving information in order to locate the necessary evidence in unallocated or slack memory.
6	2019	Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices. [29]	This study analysed roadmaps of computer forensic evaluation methods described in scientific files and proposed a laboratory protocol to retrieve digital evidence from hard drives. The authors proposed a six-step procedure to diagnose the case, present results, collect evidence, make copies of files, analyze data, and extract information.
7	2015	Hard disk failure and data recovery methods in computer forensic (Adli bilişimde hard disk arızaları ve arızalı disklerden veri kurtarma yöntemleri) [30]	The authors of this study explained how to retrieve data from a corrupted hard drive. A data improvement concept, data retrieval types, and the physical construct of modern HDD and their inner elements are reviewed first, followed by encountered failures.
8	2019	Data Sanitization Framework for Computer Hard Disk Drive: A Case Study in Malaysia [31]	In this study, the authors introduced a method for sanitizing data from computer hard drives. The proposed and tested a data sanitization process using commercially available tools. Several tests have been conducted at Cybersecurity Malaysia's accredited digital forensic lab.
9	2021	A Digital Forensics Approach for Lost Secondary Partition Analysis using Master Boot Record Structured Hard Disk Drives [32]	Using forensic tools, this study investigates the removal or fraud of partitions on generally employed DOS / Master Boot Record (MBR) designed HDDs.
10	2021	Data recovery in a case of fire-damaged Hard Disk Drives and Solid-State Drives [33]	This study describes how data can be recovered from HDD and strong public drives of different companies and models that have been damaged by fire.
11	2020	Automated support tool for forensics investigation on hard disk images [34]	A new system was designed as part of this study in order to assist criminal investigators in finding evidence on images of hard drives recovered from suspects' devices that could be used in conducting investigations. According to the authors, the content of the images on the disks was not encrypted, and therefore their focus was on multimedia content related to child abuse on the partition images.
12	2121	Forensic analysis and data recovery from water-submerged hard drives [35]	The study examined how long it will take for water to enter the hard drive once it has been submerged in water.

Stage 2: Assembling common processes from the selected models: the aim of this step is to collect the common

investigation processes from the 12 selected models. It involves three steps:

- *Assembling criteria*: The investigation processes should be gathered solely from the main text or figure of the model. The collection process has omitted the following items: abstracts, related works, introductions, methodologies, and conclusions.
- *Assembling common processes from selected models*: The common investigation processes have been gathered and filtered from the selected models using the criteria above.
- *Recognize selected processes based on semantic meaning*: In this phase, three common investigation processes for the DIM have been selected based on their semantic meaning: detection, collection, and analysis. The investigation procedure begins with the detection phase, which involves identifying any suspicious activity on the HDD. This involves inspecting the HDD's system logs and event logs, as well as analysing the drive for malicious or suspicious files. It will be your responsibility to collect and save files from your hard drive as part of the collection phase of the project.

Stage 3: Developing a Detection and Investigation Model for HDD: The aim of this stage is to develop the DIM for the HDD. It consists of the following two primary steps:

- *Identify the relationships among processes and their activities*: The procedure begins with the detection phase. It involves the identification of possible digital evidence. The accumulation and preservation of digital evidence is the next step. It comprises both the gathering of evidence and the verification of its authenticity. The assembling phase is the third phase. In this phase, digital evidence is examined and evaluated for its relevancy. Fig. 2 depicts the DIM developed for the HDD.

1) Detection phase: In this phase, there are three primary procedures: detection and investigation plans, detection and investigation tools, and investigation team identification. The detection and investigation plan includes the establishment of an organized plan outlining the steps required to detect any potential malicious activity on the hard disk drive (HDD). In contrast, the detection and investigation tools (which can be either software or hardware) concentrate on choosing the most appropriate tools for detecting any potential malicious activity on the HDD.

a) Identifying suspected HDD: The purpose of this step is to identify suspected hard drives. A tampered or suspicious activity indicator is included here. Investigation teams must determine the drive's origin and identify it with its serial number or other unique identifiers. Further investigations can then be initiated based on this information.

b) Verification: Following the identification of a suspected HDD, the investigative team will need to verify its legitimacy. To determine the integrity of the drive, tests may be conducted, or the data recorded on the drive may be examined using specialized forensic software. During this phase, the drive's authenticity and data integrity are determined.

c) Initial report: A preliminary report will be drafted by the investigation team after the verification procedure has been complete. It should include the results of their verification procedure as well as any evidence of tampering. If necessary, the organization (decision makers) can conduct a thorough forensic investigation or contact law enforcement based on this report.

2) Gathering phase: During the detection phase, a suspect HDD has been identified, and information is being collected from it. In the process of analysing suspicious hard drives, two primary procedures need to be followed: collecting and preserving all relevant data. FTK Imager is a forensic tool used to gather data from a suspected HDD that has been infected with malware. This data may include deleted files, fragmented data, and metadata. Preserving collected data requires ensuring that it can be analysed in the future. Several methods are available for achieving this goal. To preserve the data, copies of the data may be created, or images of the hard drive may be captured using forensic tools. To preventing data loss or corruption, this step must be performed as part of the analysis procedure.

3) Analysing phase: With FTK Imager, forensic data can be collected from infected HDDs. There may be deleted files, fragmented data, and metadata within this data. Data collection must be preserved so that it can be analysed in the future. There are several methods available for achieving this goal. Using forensic tools, images of the hard drive can be captured to preserve data, or copies of the data can be created. As part of the analysis process, this step must be performed to prevent data loss or corruption.

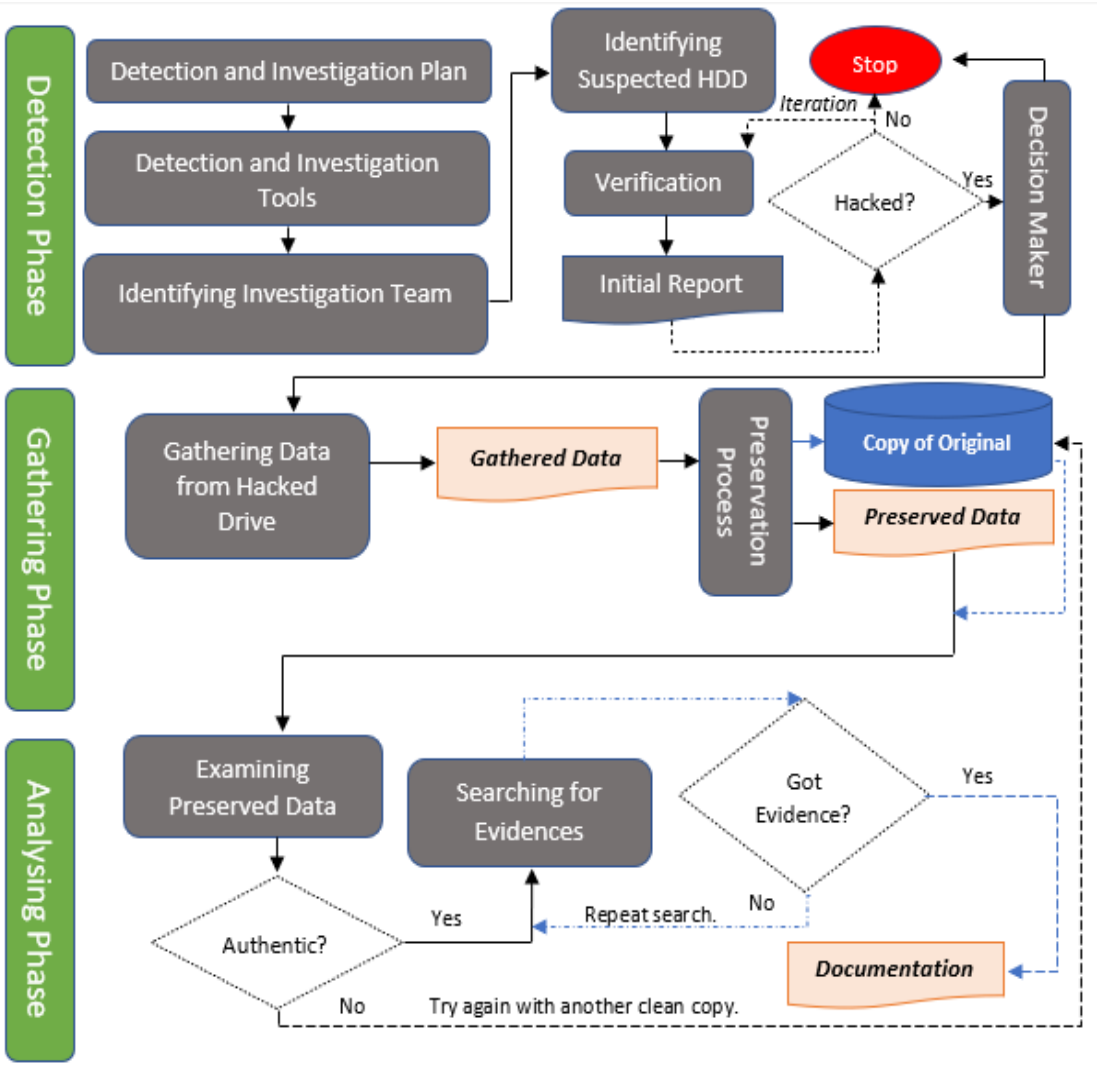

Fig. 2. Proposed detection and investigation model to detect and investigate HDD attacks.

- Validating the effectiveness of the developed DIM: This part evaluates the applicability of the devised DIM to actual HDD attack investigations. The forensic instruments FTK Imager and HashMyFiles are utilized for this purpose. The FTK Imager tool is used to capture and analyze the data, while the HashMyFiles utility is used to store the captured data. In order to accomplish this, the researcher employed the following scenario: "We received a complaint from a consumer named Ahmed. He reported that his flash drive was broken, and he cannot access it. Considering this, the following paragraphs describe how DIM will detect, acquire, analyse, and record data from the suspected pin drive.

1) Detection phase: To accomplish this task, the researcher of this paper prepared the tools FTK Imager and HashMyFiles. During the investigation, the investigative team conducted interviews with the victim to gather all the information necessary to verify the pen drive incident. It is essential that information such as the size of the pen drive, the types of files inside the pindrive, and the last time the pen drive was used is gathered during the interview. Consequently, the researcher discovered that the pen drive had been compromised because of this attack. A team of investigators would need to move to the acquisition stage of the investigation to accomplish this goal.

2) Gathering phase: A second phase of the investigation will be focused on the collection and preservation of pen drive data using the FTK Imager and HashMyFiles tools. As shown in Fig. 3 and 4, it shows how the investigation team can collect data from the suspected pen drive using FTK Imager. To ensure that the captured data is not harmed, it is recommended that it is copied to an external flash drive and then duplicated. The data that has been captured must be protected from alteration or always tampering with HashMyFiles tool. The purpose of HashMyFiles is to create hashed values for data collected from the user by using the HashMyFiles tool as shown in Fig. 5. In the next phase, the examination and analysis process will be explained in detail.

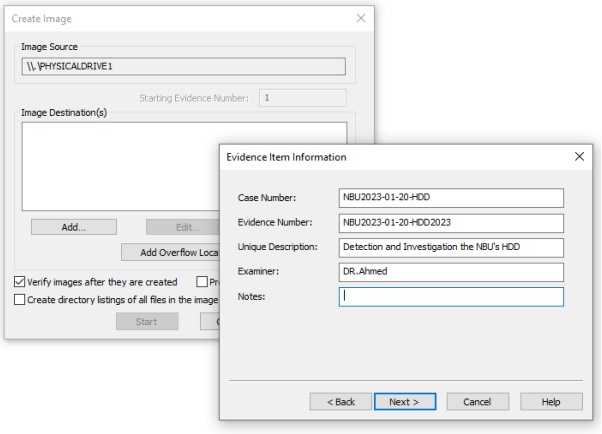

Fig. 3. Collect data using FTK imager.

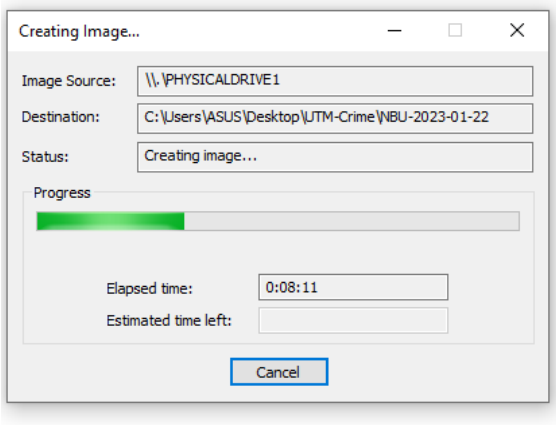

Fig. 4. Creating image from the suspected pen drive.

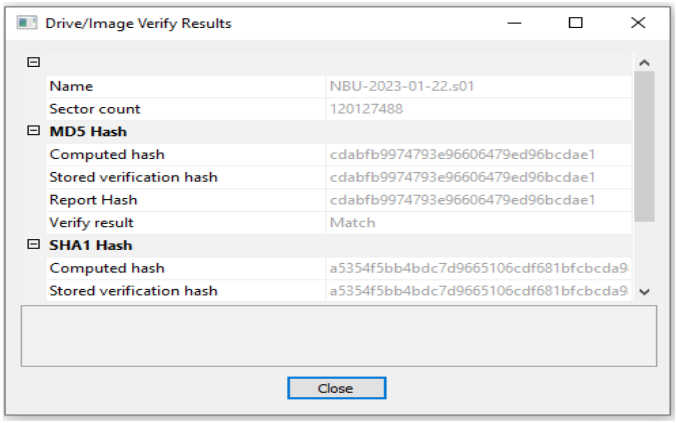

Fig. 5. Hashing collected data using HashMyFiles tool.

3) Analyzing phase: To verify the authenticity of the captured data before moving on to the analysis procedure, the authentication of the captured data needs to be verified using the FTK Imager tool to check whether it is consistent with the captured data. As a result, the hashed file has been verified as shown in Fig. 6. The researcher has confirmed that the authentication is correct, that the value is correct, and that no tampering has been done. This is why they can move forward with the next step of the investigation. By analyzing the captured information, malicious activities are identified because of analysis. After digging through the captured image, researcher found that the attacker had deleted information from the pen drive as shown in Fig. 7. The attacker was able to access the victim's computer remotely through a remote access program. After that, he used the "Delete file path" command to delete the files from the pen drive.

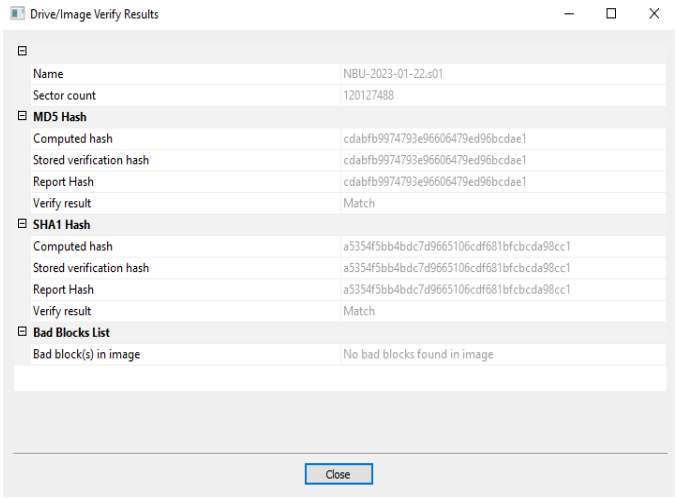

Fig. 6. Verifying hashed image using FTK Imager tool.

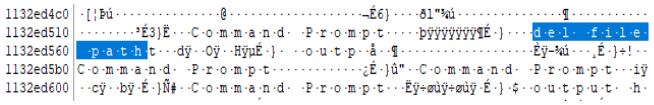

Fig. 7. Analyzing data using FTK Imager tool.

IV. Results and Discussion

In a nutshell, based on the results and discussion presented, this study proposed a detection and investigation model that aims to detect and investigate the occurrence of HDD attacks. This model is mainly comprised of three phases which are detection, capture, and analysis. Therefore, a set of forensic tools namely FTK Imager and HashMyFiles are utilized to accomplish these phases.

Initially, the detection phase aims to identify any evidence of HDD attacks. Therefore, the FTK Imager was utilized in this study to acquire any relevant data contained on the HDD, including the volume name, number of sectors, and sector size. This information is used for identifying any discrepancy that demonstrates the differences between predicted and actual outcomes. If discrepancies exist, it indicates that the HDD drive may have been tampered with. Secondly, the capture phase aims to capture any related evidence of the HDD attacks. Likewise, the FTK Imager and HashMyFiles are utilized for capturing and preserving this evidence that is significant for succeeding analysis phase. Thirdly, the analysis phase aims to analyse and examine the evidence of HDD attacks. During this phase, the FTK Imager is predominantly used to examine the evidence. Based on this analysis, the investigator will have information about the attack, including the type of attack, the method employed, and the suspect. In addition, it will facilitate the diagnosis of the attack's severity and the prevention of future attacks. For method evaluation, it is assumed that the

pen drive has been tampered with. In this case, there are several files that have been deleted and damaged. Therefore, the proposed DIM is applied to a compromised flash drive to demonstrate its capability to detect, capture, and analyze HDD attacks. The testing demonstrated that the proposed DIM is capable of precisely detecting deleted files and identifying the removal methods. Consequently, this demonstrated the effectiveness of the proposed DIM in terms of the identification and investigation of HDD attacks.

Based on the results of the evaluation, there are several advantages of the proposed DIM model that could be beneficial to organizations such that, it facilitates in the prevention, mitigation, and acceptance of variations of potential HDD attacks. Therefore, it provides organizations with the option to secure their environment by acknowledging their susceptibility to assaults and by identifying and mitigating them swiftly.

Comparing to the existing model, Table II displays the comparison of the proposed DIM with the existing models. Clearly, the proposed DIM covered whole existing HDD digital forensics models.

TABLE II. COMPARING THE PROPOSED DIM WITH THE EXISTING HDDS DIGITAL FORENSIC MODELS

ID	Year	Existing Model	Proposed DIM
1	2018	[24]	☑
2	2017	[25]	☑
3	2015	[26]	☑
4	2022	[27]	☑
5	2019	[28]	☑
6	2019	[29]	☑
7	2015	[30]	☑
8	2019	[31]	☑
9	2021	[32]	☑
10	2021	[33]	☑
11	2020	[34]	☑
12	2121	[35]	☑

V. CONCLUSION AND FUTURE WORK

A hard disk drive is a very important component of a computer system that stores the operating system and applications. It is essentially a non-volatile memory device that stores digital information in a permanent manner. Generally, attackers are trying to access the valuable information on the HDD with the intent of damaging or stealing it. In this study, a detection and investigation model for HDDs was proposed to detect and investigate the various types of HDD attacks. In the proposed model, there are three main phases, namely detection, gathering, and analysis. FTK Imager has been used in conjunction with the newly developed detection and investigation model to detect, preserve, and analyze HDD attacks. Results showed that the proposed detection and investigation model can detect and analyze HDD and pen drive attacks. It is recommended that the future work on this study should be focused on the real-life scenario of HDD attacks.

REFERENCES

[1] 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.

[2] O. Ameerbakhsh, F. M. Ghabban, I. M. Alfadli, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Digital Forensics Domain and Metamodeling Development Approaches," in 2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE), 2021, pp. 67–71.

[3] A. Al-Dhaqm et al., "Categorization and Organization of Database Forensic Investigation Processes," IEEE Access, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3000747.

[4] Y. Zhang, K. Shan, X. Li, H. Li, and S. Wang, "Research and Technologies for next-generation high-temperature data centers–State-of-the-arts and future perspectives," Renew. Sustain. Energy Rev., vol. 171, p. 112991, 2023.

[5] F. M. Alotaibi, A. Al-Dhaqm, and Y. D. Al-Otaibi, "A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field," Comput. Intell. Neurosci., vol. 2022, 2022.

[6] A. I. Taloba et al., "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare," Alexandria Eng. J., vol. 65, pp. 263–274, 2023.

[7] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, vol. 12, no. 6, p. 1333, 2023.

[8] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R. Kebande, and S. H. Othman, "Face validation of database forensic investigation metamodel," Infrastructures, vol. 6, no. 2, 2021, doi: 10.3390/infrastructures6020013.

[9] M. Yates, "Practical investigations of digital forensics tools for mobile devices," in 2010 information security curriculum development conference, 2010, pp. 156–162.

[10] B. Carrier and E. H. Spafford, "Getting physical with the digital investigation process," Int. J. Digit. Evid., vol. 2, no. 2, pp. 1–20, 2003.

[11] B. Carrier and E. Spafford, "An event-based digital forensic investigation framework," Digit. Investig., 2004.

[12] F. C. Freiling and B. Schwittay, "A common process model for incident response and computer forensics," IMF 2007 IT-Incident Manag. IT-Forensics, 2007.

[13] N. L. Beebe and J. G. Clark, "A hierarchical, objectives-based framework for the digital investigations process," Digit. Investig., vol. 2, no. 2, pp. 147–167, 2005.

[14] S. Ó. Ciardhuáin, "An extended model of cybercrime investigations," Int. J. Digit. Evid., vol. 3, no. 1, pp. 1–22, 2004.

[15] F. B. Cohen, "Fundamentals of Digital Forensic Evidence, Chapter in Handbook of Information and Communication Security," accessed all. net, vol. 4, p. 2011, 2011.

[16] E. Casey and C. W. Rose, "chapter" Forensic Analysis" in 'Handbook of Digital Forensics and Investigation,'" 2010.

[17] A. Al-Dhaqm et al., "CDBFIP: Common database forensic investigation processes for Internet of Things," IEEE Access, vol. 5, pp. 24401–24416, 2017.

[18] A. Al-Dhaqm et al., "Categorization and organization of database forensic investigation processes," IEEE Access, vol. 8, pp. 112846–112858, 2020.

[19] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a database forensic metamodel (DBFM)," PLoS One, vol. 12, no. 2, 2017, doi: 10.1371/journal.pone.0170793.

[20] A. Ali, S. Abd Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," PLoS One, vol. 12, no. 4, p. e0176223, 2017.

[21] A. Al-Dhaqm, S. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," IEEE Access, p. 1, 2020, doi: 10.1109/ACCESS.2020.3008696.

[22] M. Saleh et al., "A Metamodeling Approach for IoT Forensic Investigation," Electronics, vol. 12, no. 3, p. 524, 2023.

[23] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," MIS Q., pp. 75–105, 2004.

[24] B. B. Meshram and D. N. Patil, "Digital forensic analysis of hard disk for evidence collection," Int. J. Cyber-Security Digit. Forensics, vol. 7, no. 2, pp. 100–111, 2018.

[25] M. Gruhn, "Forensic limbo: Towards subverting hard disk firmware bootkits," Digit. Investig., vol. 23, pp. 138–150, 2017.

[26] F. Geier, "The differences between SSD and HDD technology regarding forensic investigations." 2015.

[27] M. Jazzar and M. Hamad, "Comparing HDD to SSD from a Digital Forensic Perspective," in Proceedings of International Conference on Intelligent Cyber-Physical Systems: ICPS 2021, 2022, pp. 169–181.

[28] K. Raychaudhuri, "A Comparative Study of Analysis and Extraction of Digital Forensic Evidences from exhibits using Disk Forensic Tools.," Int. J. Cyber-Security Digit. Forensics, vol. 8, no. 3, pp. 194–206, 2019.

[29] H. F. Villar-Vega, L. F. Perez-Lopez, and J. Moreno-Sanchez, "Computer forensic analysis protocols review focused on digital evidence recovery in hard disks devices," in Journal of Physics: Conference Series, 2019, vol. 1418, no. 1, p. 12008.

[30] Y. Z. Güllüce and R. Benzer, "Hard disk failure and data recovery methods in computer forensic Adli bilişimde hard disk arızaları ve arızalı disklerden veri kurtarma yöntemleri," J. Hum. Sci., vol. 12, no. 1, pp. 206–225, 2015.

[31] N. A. B. Yusof, S. N. H. B. S. Abdullah, M. F. E. bin Md Senan, and M. B. Sahri, "Data Sanitization Framework for Computer Hard Disk Drive: A Case Study in Malaysia," Int. J. Adv. Comput. Sci. Appl., vol. 10, no. 11, 2019.

[32] E. Akbal, Ö. F. YAKUT, S. Dogan, T. TUNCER, and F. Ertam, "A Digital Forensics Approach for Lost Secondary Partition Analysis using Master Boot Record Structured Hard Disk Drives," Sak. Univ. J. Comput. Inf. Sci., vol. 4, no. 3, pp. 326–346, 2021.

[33] D. Solodov and I. Solodov, "Data recovery in a case of fire-damaged Hard Disk Drives and Solid-State Drives," Forensic Sci. Int. Reports, vol. 3, p. 100199, 2021.

[34] J. M. N. Veloso, "Automated support tool for forensics investigation on hard disk images." NOVA University of Lisbon, 2020.

[35] A. Francois and A. Nisbet, "Forensic analysis and data recovery from water-submerged hard drives," Int. J. Electron. Secur. Digit. Forensics, vol. 13, no. 2, pp. 219–231, 2021.