IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 7 April 2023, accepted 23 April 2023, date of publication 26 April 2023, date of current version 4 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3270619

RESEARCH ARTICLE

A Novel Digital Forensic Framework for Data Breach Investigation

ARIF RAHMAN HAKIM[1], **(Member, IEEE), KALAMULLAH RAMLI**[1], **(Member, IEEE), TEDDY SURYA GUNAWAN**[2,3], **(Senior Member, IEEE), AND SUSILA WINDARTA**[1], **(Member, IEEE)**

[1]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Jawa Barat 16424, Indonesia
[2]Department of Electrical and Computer Engineering, Kulliyyah of Engineering, International Islamic University Malaysia, Kuala Lumpur 50728, Malaysia
[3]School of Electrical Engineering, Telkom University, Bandung 40257, Indonesia

Corresponding author: Kalamullah Ramli (kalamullah.ramli@ui.ac.id)

This work was supported in part by Universitas Indonesia through Hibah Publikasi Terindeks Internasional (PUTI) Kolaborasi Internasional (Q2) Scheme under Contract NKB-1339/UN2.RST/HKP.05.00/2022; and in part by the Indonesia Cyber Awareness and Resilience Center, Universitas Indonesia (IdCARE-UI), through the IT Forensics Enablement Workshop by the Japan International Cooperation Agency (JICA). The work of Arif Rahman Hakim was supported by Lembaga Pengelola Dana Pendidikan (LPDP), Ministry of Finance of the Republic of Indonesia.

ABSTRACT Data breaches are becoming an increasingly prevalent and global concern due to their massive impact. One of the primary challenges in investigating data breach incidents is the unavailability of a specific framework that acknowledges the characteristics of a data breach incident and provides clear steps on how the investigative framework can comprehensively answer what, who, when, where, why, and how (5WH) questions. This paper aims to develop a novel digital forensic investigation framework that can overcome these data breach investigation challenges. The proposed framework utilizes the data breach breakdown phases to analyze data breach incidents according to their characteristics. The main contribution of our work is a novel digital forensic framework for data breach investigation that enhances the 5WH analysis depth by utilizing evidence classification and artifact visualization based on data breach breakdown phases. Furthermore, we design the framework components to provide comprehensive analysis results that make it easier for investigators to summarize the answers to the 5WH questions. To validate the framework, we apply it to a case study of enterprise-level data breach incidents. Based on the case study analysis, the proposed investigation framework successfully provides all the answers to the 5WH questions. This comprehensive answering ability is the study's fundamental strength compared to other digital forensic investigation frameworks.

INDEX TERMS Data breach, digital forensics, framework, investigation.

I. INTRODUCTION

Data breaches are becoming an increasingly prevalent and global concern. Based on the Verizon Data Breach Investigation Report [1], 5,258 of 29,207 reported cyber incidents were confirmed data breaches. According to Flashpoint [2], there have been 1,980 cases of data breaches in various sectors during the first semester of 2022, an increase of 31.7% compared to the first semester of 2021. Accenture [3] also reports that the trend in data breaches has increased by 11% since 2018 and by 67% since 2014.

In addition, the massive impact of data breaches involves internal and external consequences for the organization [4]. Internal consequences affect the breached organization in terms of operations [5], [6], workforce [7], [8], [9], legal issues [10], [11], and finance [12], [13]; external consequences affect customers [14], [15], [16], competitors [17], [18], suppliers [19], [20], [21], and other stakeholders [22]. As an example of financial impacts, according to a report by IBM, global losses from data breach incidents increased from USD 3.86 billion in 2020 to USD 4.24 billion in 2021 [23]

The associate editor coordinating the review of this manuscript and approving it for publication was Diana Gratiela Berbecaru.

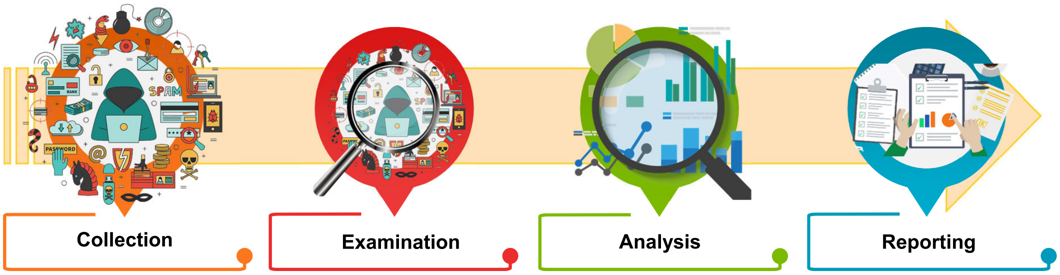


FIGURE 1. Sequential phases in digital forensic investigation procedures.

and USD 4.35 billion in 2022 [24]. This figure is predicted to continue to increase, as Cybersecurity Ventures [25] has stated that the impact of losses due to such incidents will reach USD 10.5 trillion by 2025.

Based on this massive impact, data breaches have become urgent and require a comprehensive solution regarding procedures, human resources, and technology [26]. Organizations must be supported by technological approaches to protect managed data, detect, analyze, and handle incidents, restore systems, and improve security controls so that similar incidents do not occur again. Furthermore, time is an essential factor in dealing with data breach incidents. Slow handling increases the likelihood of data breaches, the difficulty of data recovery, the impact on the victim organization's reputation, and the complexity of the investigation process [27].

Digital forensic investigation is vital in uncovering data breaches and finding essential facts related to the source and extent of incidents. The investigation process is highly dependent on the device type and environment used, which means that digital forensics has more than one branch because digital devices can include traditional computers, mobile devices, and network devices such as routers [28]. Furthermore, the continual emergence of new types of cybercrime necessitates adaptive investigation process models, new technology, and cutting-edge techniques to combat these incidents [29], [30]. The most significant objective of digital forensics is to gather evidence to respond to the 5Ws and How (5WH) questions: what occurred, who was involved, and when, where, why, and how an incident occurred.

Previous studies [31], [32], [33], [34] have proposed a digital forensic framework or process model to investigate incidents. However, they have some restrictions, such as failing to provide either a comprehensive scope of device types as sources of evidence on the organization's network architecture or a comprehensive analysis that explains the 5WH of the incident that occurred. In addition, they focus on the investigation of general cybercrime, cyberfraud, or cyberattacks rather than data breach investigations. It is essential to have a specific data breach investigation framework because the phases and objectives of data breach attacks are distinct. The distinctive characteristics of data breach incidents can be determined based on the last stage of the attack: the exfiltration of data from the victim's environment to the environment under the attacker's control. This distinguishes data breach incidents from other cyber incidents, such as website defacement, which alters the data integrity of a website's display system but does not involve data exfiltration. Similarly, denial-of-service attacks that target system availability do not aim at data exfiltration from within the system to a point outside the system under the attacker's control.

In general, digital forensic investigation (DFI) and digital forensic frameworks (DFF) can be applied to various types of cyber incidents. However, certain investigation models are designed for specific cases, such as online child abuse [35], cross-border crime [36], and financial transaction crime [37]. The novelty of the proposed framework that differentiates it from other DFI and DFF is its specificity to data breach incidents based on the data breach breakdown (DBB) phases. The DBB is a concept that characterizes the stages of data breach incidents. The availability of specific DFFs for data breach incidents is urgent, considering that effectiveness and efficiency are critical to minimizing the impact of a breach, and it is essential to use resources with the appropriate investigation framework. However, in the event of a data breach incident, the use of nonspecific DFI or DFF may result in inefficiencies.

We propose a novel digital forensic framework for data breach investigation by improving the framework proposed by Dimitriadis et al. [34]. Our proposed framework uses DBB phases as the reference for artifact categorization. The main contribution of our work is a novel digital forensic framework for data breach investigation that enhances the 5WH analysis depth by utilizing evidence classification, artifact visualization based on DBB phases, and findings mapping into each 5WH question. Therefore, it helps forensic investigators examine the preserved data; analyze the correlated artifacts, timeline, and attack flow; and map their results into 5WH answers. Furthermore, we present a case study to evaluate the performance of our proposed framework. The results indicate the effectiveness of our framework in that all 5WH questions have more straightforward answers as a result of the analysis.

This paper is organized into five sections. The second section begins with an explanation of the DFI and DBB phases and a summary of selected previous research on DFF. The third section describes the proposed framework and its components. The fourth section presents a case study

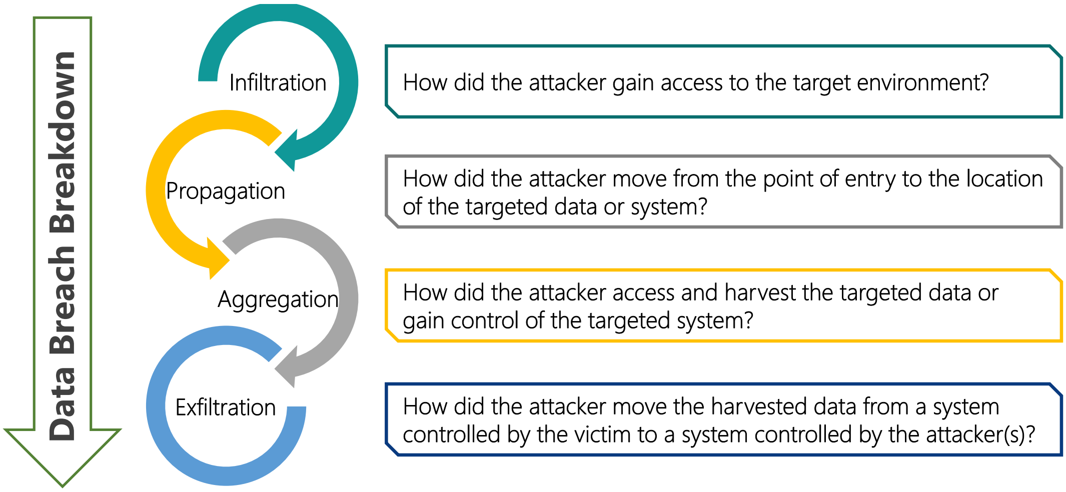

Data Breach Breakdown
Infiltration
Propagation
Aggregation
Exfiltration
How did the attacker gain access to the target environment?
How did the attacker move from the point of entry to the location of the targeted data or system?
How did the attacker access and harvest the targeted data or gain control of the targeted system?
How did the attacker move the harvested data from a system controlled by the victim to a system controlled by the attacker(s)?

FIGURE 2. Data breach breakdown phases.

demonstrating how our proposed framework illustrates a typical instance of data breaches resulting from spear phishing malware. In Section V, the conclusion is presented.

II. RELATED WORKS

The main purpose of this section is to define the DFI and DBB phases and summarize selected existing frameworks that focus on the examination and analysis phase of digital forensics.

A. DIGITAL FORENSIC INVESTIGATION

A DFI is an effort to investigate, examine, search for, and collect data, information, and other findings based on the stages of scientific procedures and special techniques used to obtain digital evidence that is admissible in court.

There are four phases of digital forensic procedures published by the National Institute of Standards and Technology (NIST) in Special Publication 800-86 of the Guide to Integrating Forensic Techniques into Incident Response, as follows [38]:

1) COLLECTION

The collection phase determines whether any potential data sources are relevant to the incident and then identifies and records those sources. Afterward, the information contained within these sources should be retrieved carefully to avoid compromising its integrity.

2) EXAMINATION

In the examination phase, forensic investigators examine the data collected from the collection phase and extract the data that are relevant to the incident while preserving their integrity.

3) ANALYSIS

The analysis phase involves analyzing the information extracted from the examination phase to answer the 5WH questions or determine that no or only a partial conclusion can be drawn.

4) REPORTING

The reporting phase is the process of preparing and presenting the investigation's procedure, methods, and tools, along with the results of the analysis phase.

Fig. 1 shows the intercorrelation of the steps in the DFI sequentially. In investigating a cybercrime or cyberattack, a forensic examiner tries to obtain artifacts from the observed incident. In digital forensics, an artifact is evidence used to support a response to a question, such as text or a resource reference.

B. DATA BREACH BREAKDOWN PHASES

A specific investigation into a data breach must provide a detailed explanation based on the breakdown concept of data breach incidents. This concept is often referred to as DBB [39], as depicted in Fig. 2. DBB is most applicable when data theft is the objective of the attack. However, an investigator typically faces a very complex situation. Therefore, the investigator should continue working logically throughout the investigation of each phase and stringing the phases together to tell the story of the breach.

Effectiveness and efficiency are essential to minimizing the impact of a breach, and it is of the utmost importance that resources are used with the appropriate investigation framework.

C. SELECTED EXISTING FRAMEWORKS

Up to this point, various DFFs are suitable for diverse investigations characterized by distinct details and phases. The authors in a previous survey [40] identified fifteen DFFs that most enterprises widely adopt. However, not all of these DFFs provide a detailed elaboration of the examination and analysis phases, which are crucial in the investigative process to uncover incidents. From the 15 DFFs, we selected CFFTPM,

TABLE 1. Selected framework benchmark and proposed solution.

Name	Contribution	Incident Type	Limitation	Proposed Solution
Digital FOrensics framework for Reviewing and Investigating cyberattacks (D4I) [34]	Enhances existing frameworks using artifact categorization based on the cyber kill chain (CKC) and proposes an instruction method for examination and analysis.	Cyberattack	This framework does not provide detailed explanations to obtain a complete analysis result that can answer all the 5WH questions of the incident.	The framework is designed so that each of the 5WH questions can be addressed by a phase in the framework.
Integrated Digital Forensics Process Model (IDFPM) [33]	Investigates the most prominent process models in digital forensics and proposes a new process model that overcomes problems in examination and analysis.	Cyberattack	This framework takes advantage of prior data and considers neither artifact types nor incident types.	The proposed framework is specifically for data breach incidents, with artifact analysis based on the characteristics and stages of the data breach incident.
Systematic Digital Forensic Investigation Model (SRDFIM) [32]	Proposes a new framework with eleven phases that help in evidence dynamics and event reconstruction and can ensure the integrity and admissibility of digital evidence.	Computer fraud and cybercrimes	This framework is technique-centric because it lacks a structured, step-by-step examination and analysis process.	The proposed framework is designed systematically according to digital forensics procedures [38] by ensuring that the framework structure has a phase that answers each 5WH question.
Cyber Forensic Field Triage Process Model (CFFTPM) [31]	Proposes a method for rapidly identifying, analyzing, and interpreting digital evidence by focusing on reducing the time required in an investigation.	Cybercrimes	The framework does not specify artifact categorization or provide a case study to show how it can be implemented.	In the proposed framework, the evidence sources are divided into three categories, hosts, network devices, and security devices, with the intent of obtaining potential artifacts in each phase of the DBB based on the device functions of the three categories.

SRDFIM, and IDFPM, as these three DFFs also focus on the examination and analysis phases. A new DFF called D4I has also emerged, which provides a detailed approach to both phases. Therefore, we included it in our selection, resulting in a total of four DFFs in our paper, namely, CFFTPM, SRDFIM, IDFPM, and D4I. In this subsection, we discuss these frameworks, especially their examination and analysis phases, which are the phases we focus on. We give their names, contributions, incident types, and limitations. Then, we propose a solution based on the limitations of each framework. In the next section, we take advantage of this proposed solution in our proposed framework. Table 1 summarizes the discussion in this subsection.

The CFFTPM [31] is concerned with the issue of time when conducting investigations; thus, the designed framework aims to provide an efficient examination and analysis process. The framework proposes six phases and suggests steps to take to obtain information from a Windows system. Although there appears to be an artifact classification method, it is not clearly defined or explained how to use this classification when investigating an incident within the framework. Based on this limitation, in our proposed framework, the evidence sources are divided into three categories, hosts, network devices, and security devices, to obtain potential artifacts in each DBB phase based on the device functions of the three categories.

The Systematic Digital Forensic Investigation Model (SRDFIM) investigates cybercrime and cyberfraud [32]. It takes advantage of the components of several frameworks that have been reviewed, and it focuses on the examination and analysis phase. The framework design consists of eleven phases, including the examination phase, which explores potential evidence as ASCII and non-ASCII data through search, filtering, recovery, and validation. The same process is also conducted on suspicious files, hidden directories, files with uncommon extensions, and mismatched metadata. The outputs of this process are then analyzed to establish correlations between the discovered artifacts and chronologically order the events to obtain a complete story of the incident. Its limitation is that its application is limited to computer fraud and cybercrimes [40]. In addition, the model is technique-centric without providing a structured and step-by-step method for conducting the examination and analysis phases [34]. We believe that such a process will be beneficial for forensic examiners to answer the 5WH questions comprehensively and support the investigation process. Despite the importance of the detailed technique in the framework, systematic and step-by-step processes are lacking. In the next section, our proposed framework is designed systematically according to digital forensics procedures by ensuring that the framework structure has a phase that answers each 5WH question.

The IDFPM [33] is a framework consisting of four steps for investigating cyberattacks. It suggests pattern-based evidence recognition to reduce the identification processing time. It takes advantage of a past incident dataset and uses it to locate determinate data based on hashes during the investigation. Considering the natural calculation of a hash function maps a bit string of arbitrary length to a fixed-length bit string. The bit string output of the hash function does not provide identification of the artifact type, whether it originates from a host, network device, or security device. Similarly, the incident type cannot be differentiated solely based on the hash value of the artifact. As a result, neither artifact types nor incident types are considered by this hash-based evidence recognition. In the analysis phase, the result of the previous step is compared to the recommended hypothesis to obtain the relevant data. From this point of view, we propose a framework specifically for data breach incidents, with artifact analysis based on the characteristics and stages of the incident.

The D4I is a framework that is intended to complement and strengthen existing digital forensic mechanisms instead of replacing them. Two pillars compose the D4I framework. The first obtains the proposed categorization artifacts and maps them to the CKC. The second is a sequential instruction procedure for the examination and analysis phase [34]. As a result, the chain of artifacts is shown as a graph, with each node representing an artifact from a different phase. The links represent their relationship in terms of correlation points, including timestamps, IP addresses, and processes. The CKC is used to identify cyberattacks. Therefore, according to its characteristics, a more suitable analysis pillar is required in specific cases, such as data breach incidents. For example, to answer the 5WH questions of a data breach incident, not all 7 phases of CKC are significantly related to the analysis results of 5WH, such as reconnaissance and weaponization. Running the D4I instruction method on these two phases is inefficient. This contrasts with the proposed framework based on DBB, which consists of only 4 phases that are appropriate for the characteristics of data breach incidents so that the executed analysis process becomes more efficient than D4I, which is based on the 7 phases of CKC.

III. PROPOSED FRAMEWORK

This section discusses the architecture of our proposed framework, with each component explained in detail. Based on Fig. 1, our framework focuses on the examination and analysis phases, where electronic evidence relevant to the incident is collected appropriately in the collection phase so that all preserved data from any devices that need to be examined and analyzed are available.

In the examination phase, we sort the assets from the network architecture as the sources of evidence into three categories, hosts, network devices, and security devices. Then, they are mapped to the DBB. Next, we examine the content of the preserved data based on each step in the DBB consecutively to obtain all the artifacts in each breakdown. The final step is to correlate all artifacts and visualize them as a chain of artifacts.

In the analysis phase, we conduct a timeline analysis to sort the sequence of artifacts based on their timestamps and an attack flow analysis to obtain the complete attack process. Finally, we analyze all the facts and findings and map them into the 5WH answers. The proposed framework is depicted in Fig. 3.

The proposed framework and D4I work with the same approach, as they both adopt a high-level digital forensic process defined by NIST. D4I has two main modules: artifact categorizations along with their mapping to CKC and a step-by-step instructing method. In comparison to D4I, the proposed framework offers three enhancements. First, based on the four phases of DBB, the proposed framework allows for a more precise analysis process according to the characteristics of a data breach incident, which is more efficient than the CKC-based analysis. Some phases in CKC, such as reconnaissance and weaponization, are not significantly related to the 5WH answers in the context of answering the questions concerning the breach incident being investigated. Therefore, executing the six-step instruction method on all seven CKC phases may be inefficient.

Second, while D4I focuses on artifacts that can be found in the Windows operating system, the proposed framework not only limits artifacts to those sourced from specific OSs but also includes logs from network applications and other tools. Third, in conducting content analysis, the step-by-step procedure in the proposed framework is not rigidly ordered based on the DBB phase sequence, as is the case with D4I, which follows the CKC phase order. In D4I, artifact examination is predetermined based on categorization for each CKC phase, thus limiting the potential artifacts from other sources. In contrast, the proposed framework starts its procedure based on trigger information or relevant findings from the previous analysis iterations. This allows for a more dynamic and comprehensive analysis process.

As shown in Fig. 3, the proposed data breach investigation framework comprises six components as follows:

A. EVIDENCE CATEGORIZATION

In this framework, evidence is categorized into three types, host (H), network device (ND), and security device (SD), based on the organization's network architecture. This categorization is intended to facilitate the subsequent process, especially content analysis and chain of artifacts (CoA). This categorization is used because data breach incidents generally involve these three types of evidence. Investigators often find it difficult to comprehensively uncover data breach incidents if they only analyze one type of device. Therefore, this categorization is particularly useful for investigators in interpreting the initial steps in the artifact search. By understanding the company's network architecture, device functions, and evidence source classification, investigators can more easily determine which node to focus on in content analysis when searching for artifacts. Each initial clue or information trigger about an event will be mapped to relevant hosts, network devices, and security devices. For example, in a case study, when a piece of trigger information is received as a malicious IP and domain, based on an understanding of the functions of each node in the network architecture, investigators can direct their search toward network devices such as DNS and security

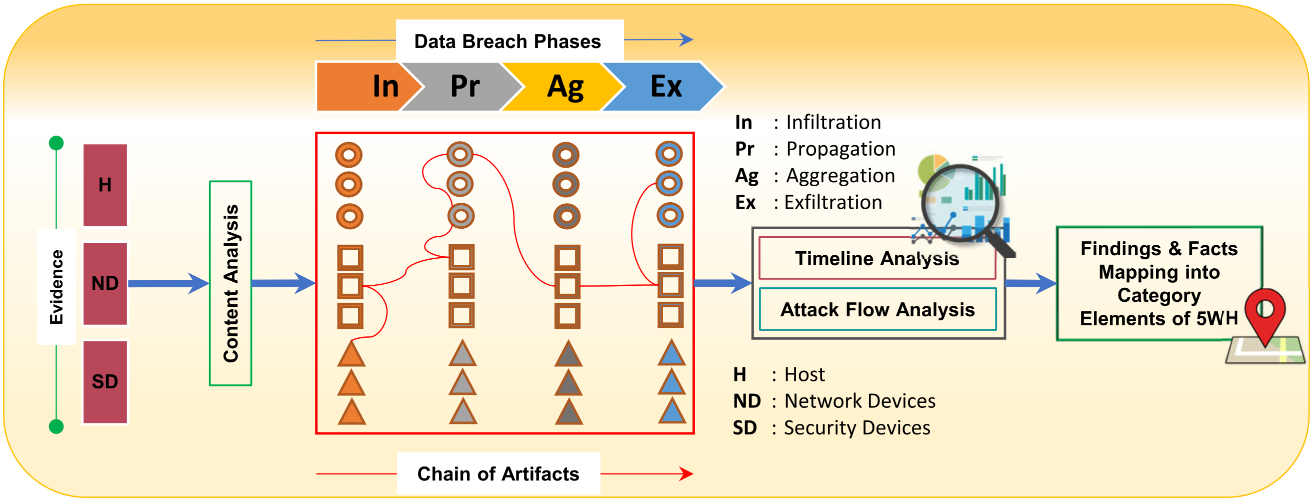


FIGURE 3. Proposed data breach investigation framework.

devices such as a proxy. They can then follow up on the search results from these two devices to obtain clues about the impacted host. Therefore, the evidence classification enables the potential artifact search to focus on being more targeted during the content analysis process. Furthermore, this categorization will be maintained when compiling the CoA and its visualization, making it easier for investigators to fully understand how incidents can occur.

B. CONTENT ANALYSIS

This step aims to extract all relevant data as artifacts from evidence obtained in the collection phase. In this step, we consider all trigger information about the incidents, including information on impacted or damaged systems from people within the organization; information that is publicly available about new vulnerabilities, exploits, or incidents at other organizations; and information from people outside the organization such as CERT/CSIRT and Interpol. This trigger information gives the investigator various hints regarding prioritizing evidence related to the information to be examined in advance. Furthermore, the content analysis process is carried out through a step-by-step procedure as follows:

1) Identify the source of evidence: Based on the trigger information, the investigator, considering the three artifact classification sources (H, ND, and SD), maps each event to potential evidence sources based on the device function and corporate network architecture.
2) Assess and extract relevant artifacts: Examining the collected data to identify and extract relevant artifacts may include filtering information records, searching relevant text or patterns, and comparing system characteristics to known baselines to identify various changes made to the system. The results obtained from this step can be utilized as trigger information for subsequent iterations of content analysis.
3) Map the artifacts to a DBB phase: Each relevant artifact found should be mapped into a single DBB phase. Investigators may map an artifact into one of the four DBB phases based on a thorough understanding of the characteristics of each DBB phase and the context of the artifact found in the preceding step.
4) Repeat: Repeat steps 1 through 3 by employing other trigger information or information obtained from step 2. Conduct this iteration until obtaining a complete set of artifacts for all four DBB phases, correlating between the phases, and demonstrating the occurrence of data exfiltration in its entirety.

C. CHAIN OF ARTIFACTS (CoA)

After obtaining each artifact from the content examination, investigators input it along with its timestamp in the CoA based on the DBB phase. Each discovered correlated artifact is then linked to the last artifact, either in the same, previous, or following DBB phase. This step is repeated until all artifacts discovered have been included in the CoA. In this paper, CoA is presented similarly to a four-dimensional array (Eq. 1):

$$\text{CoA}:[a, b, c],[d, e],\left[f, g, h^{x,y}\right],[i] \tag{1}$$

where a,b, and c are artifacts found in the infiltration phase; d and e are artifacts found in the propagation phase; f, g, and h are artifacts found in the aggregation phase; and i is an artifact found in the filtration phase. These components are split into different sets to facilitate artifact mapping within the same DBB phase and the correlation of artifacts between preceding and subsequent DBB phases. By grouping the artifacts found for each phase into one set, investigators can easily correlate these artifacts to create a sequence of the DBB phase framework, build an attack flow, and draw a complete conclusion about the incident.

TABLE 2. 5WH questions and answer mapping.

Questions	Answer	Step	Notes
What	Kind of data that has been breached	Content Examination	• Sensitive organization data • Personal data
Who	• External Actor • Internal Actor	• Content Examination • CoA • Attack Flow Analysis	• An external actor stole sensitive data • An internal employee stole sensitive data • Third-party service provider loss of sensitive data
When	Precise time or duration of the breach	• CoA • Timeline Analysis	Timeline table
Where	• In use • In transit • At rest	• Content Examination • CoA	The position of the sensitive data that were breached
Why	• Intentional • Unintentional	• Content Examination • CoA • Attack Flow Analysis	• Active attacks, including social engineering, hacking, or malware, cause the intentional breach • A system error, misuse, or misconfiguration causes an unintentional breach
How	Attack flow	• Content Examination • CoA • Attack Flow Analysis	The attack flow explains the adversary behavior sequences and helps investigators comprehend the incident's action order

Additionally, for artifact h, we use the superscripts x and y to distinguish two actions that were executed and investigated using the same artifact file. Superscripts are essential when a single artifact file contains two different events or actions. It helps to differentiate between the analysis of the first and second actions recorded in the same artifact file. For instance, when analyzing action x, which involves running thunderbird.exe on PC1 and refers to a prefetch file belonging to PC1, and action y, which involves running winword.exe on PC1 and refers to the same prefetch file, we use superscripts for the artifacts as PC1-Prefetch^{x,y} to distinguish between the two actions.

The CoA is written using a representation such as an array to facilitate artifact mapping within the same DBB phase and the artifact correlation mapping between preceding and subsequent DBB phases. As such, each mapping of artifacts into a DBB phase gradually contributes to the complete analytical findings of the investigation. In other words, using a 4-dimensional array is a viable method for representing the CoA within the context of a 4-phased data breach.

However, it is not the exclusive means for representing the data, particularly in implementing investigative tools. Other approaches exist that can provide a more intuitive visualization of CoA. For instance, CoA can be graphically synthesized in a graph where the nodes denote the artifacts of different phases in DBB, and the links indicate their correlation points. This graph illustrates the attack flow and the traces left behind. Another method is utilizing a linked list, wherein each node signifies an artifact and references other correlated nodes. Overall, while using a 4-dimensional array effectively represents the chain of artifacts in a 4-phase data breach, alternative methods are also available to facilitate CoA visualization. Further study is required to determine the time complexity of selecting a data representation method to achieve efficient implementation.

D. TIMELINE ANALYSIS

Along with the CoA, the timestamp of each correlated artifact is recorded in the previous step. In this step, the time sequence of the artifacts is used to obtain the storyline of the incident in chronological order. After obtaining the chronological sequence of the artifacts, the CoA visualization is updated by labeling the connecting lines (edges) between artifacts correlated with serial numbers according to chronological order. In this way, it is easier for investigators to determine the "when" of the incident investigation. This timeline presents each timestamp of the artifacts in the CoA in the same order as the corresponding artifacts.

E. ATTACK FLOW ANALYSIS

Based on the CoA updated from the timeline analysis, how incidents occur can be determined by analyzing the step-by-step attacks carried out by attackers on the system resulting in a data breach. Thus, the attack flow analysis results can answer the question "how" for incident investigation.

F. MAPPING FINDINGS AND FACTS INTO THE CATEGORY ELEMENTS OF 5WH

The final step of the analysis phase is to weave together the findings and facts obtained from the steps of this framework into answers to the 5WH questions of this data breach investigation. We propose mapping each answer to the 5WH questions from the investigations, as presented in Table 2.

IV. CASE STUDY

In this section, our proposed framework is applied to a case study of a data breach incident faced by a company. This case study is based on actual incidents that have been replicated in a laboratory environment with similar network architecture, asset profiles, and attack techniques. The attacker uses spear phishing and malware to access the victim's network. The attacker takes advantage of a compromised host to move laterally to the targeted system to steal sensitive data from the victim's file server as the final objective.

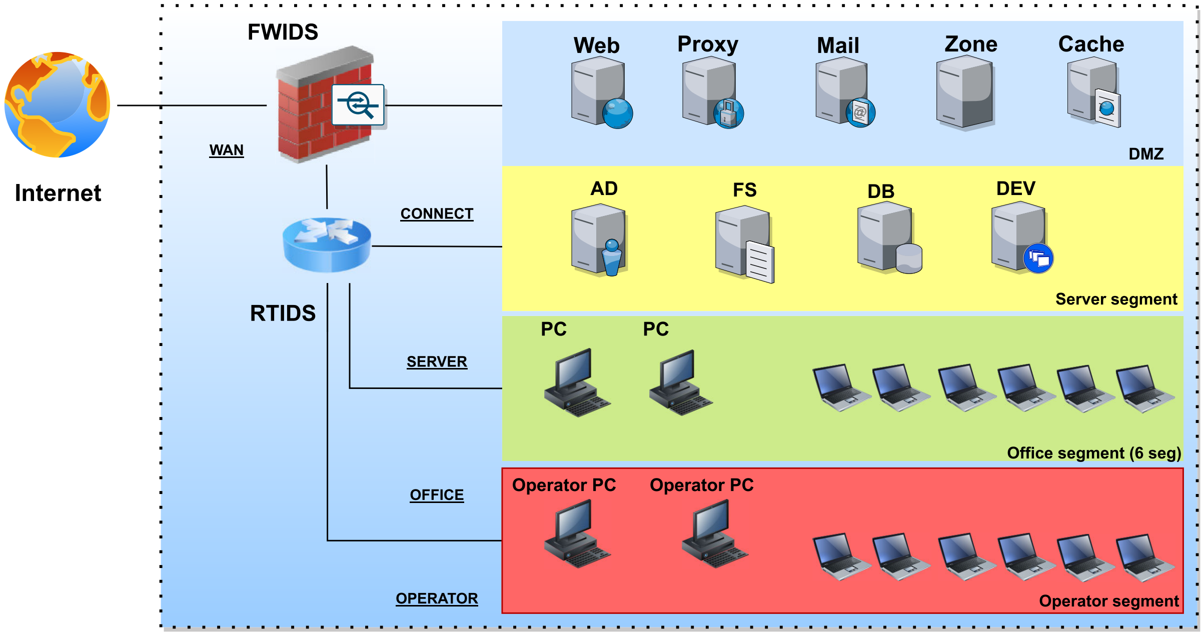


FIGURE 4. Company's network architecture.

A. SITUATION

The victim is a 300-employee food processing company with the network architecture shown in Fig. 4 with devices listed in Table 3. By understanding the network architecture, each device is classified based on its function to help investigators find a potential artifact from a relevant device. For instance, the DNS in the network architecture is considered a ND because it can resolve a domain name when a node in the network attempts to connect to that domain. When investigators are looking for clues for an event regarding whether there is a connection from a node in the network to a malicious domain, one of the relevant network devices to check is the DNS.

The investigation is triggered by information from National CERT. The security team has been contacted by National CERT, which has stated that several cyberattack campaigns were recently targeting unspecified companies in the country. National CERT has shared an indicator of compromise (IoC), including one malicious IP address and two malicious domains related to the campaigns. For anonymity, we write the malicious IP address as MIP-1 and the two malicious domains as MD-1 and MD-2. Using that information, the security team investigates the possibility that their company is also experiencing a cyberattack.

B. CONTENT ANALYSIS AND CHAIN OF ARTIFACTS

This step extracts all relevant artifacts from the devices collected in Table 3. We also use some trigger information from the National CERT information and the system users as hints to examine the evidence. Using these hints, each examination begins by determining which category of devices it relates to: hosts, network devices, or security devices. Understanding the device categorization and the specific function of each device in the network will make it easier to find devices that contain relevant artifacts.

TABLE 3. Company's evidence sources based on the network architecture.

Name	Description	Classification
WEB	Web server	Host
MAIL	Mail server	Host
AD	Active directory server	Host
FS	File server	Host
DB	Database server	Host
DEV	Development server	Host
PC1	User PC	Host
OPC1	Operator PC	Host
RTIDS	Router IDS	Network device
DNS	DNS	Network device
FWIDS	Firewall IDS	Security device
RTIDS	Router IDS	Security device
PROXY	Proxy server	Security device

In each examination, the investigators assign the artifacts found as part of a phase in the DBB and then compile the CoA. The examination results at each step, artifacts found, CoA compiled, and timeline are reassessed based on each phase of the DBB. We present a summary of the content examination, the CoA, and the timeline for the infiltration phase in Table 4, the propagation phase in Table 5, the aggregation phase in Table 6, and the exfiltration phase in Table 7. The following part of this subsection describes each stage this case study examination.

1) Given the external malicious IP address and domains mentioned in the IoC, the investigators examined the proxy server log for any connections from within the

TABLE 4. Summary of the content examination, CoA, and timeline for the infiltration phase.

Examination	Artifact	Chain of Artifacts (CoA)	Timeline
A record in the proxy server logs indicating that an IP address belonging to PC1 within the company sent a request to MD-2	PROXY-access.log	CoA: [PROXY-access.log], [-], [-], [-]	11/May/2021 07:50:45-09:36:34
A record discovered in the DNS query logs shows the name resolution of MD-2 in the same time range as the previous record discovered in the proxy server logs	DNS-queries	CoA: [PROXY-access.log, DNS-queries], [-], [-], [-]	5/11/21 7:50
From the prefetch files on PC1, the investigators found a record of file execution for thunderbird.exe as an email client	PC1-Prefetch^c	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^c], [AD-Security.evtx^{a,b}], [FS-Security.evtx], [-]	5/11/21 7:45
From the prefetch files on PC1, the investigators found a record of file execution for winword.exe	PC1-Prefetch^d	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^c,^{d}], [AD-Security.evtx^{a,b}], [FS-Security.evtx], [-]	5/11/21 7:48
From the prefetch files on PC1, the investigators found a record of file execution for MSHTA.exe	PC1-Prefetch^e	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}], [AD-Security.evtx^{a,b}], [FS-Security.evtx], [-]	5/11/21 7:50
The investigators found a record from the mail log showing that Alice's mail account received an email from an unknown mail account	MAIL-mail.log	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}], [FS-Security.evtx], [-]	5/11/21 7:31

company to the malicious domain and examined the DNS query logs to determine when the name resolution for the malicious domain occurred. The investigators discovered a record in the proxy server logs indicating that an IP address belonging to PC1 within the company sent a request to MD-2. A record discovered in the DNS query logs showed the name resolution of MD-2 in the same time range as the previous record discovered in the proxy server logs. We input these artifacts in the infiltration phase.

2) The investigation then moved on to PC1 as the MD-2 connection source. First, the investigation focused on the active directory (AD) account used to log in to PC1. An event was recorded as a standard login of user "Alice" in the AD Security Event Log. However, when PC1 and MD-2 were connected, another record showed a successful login using an administrator account. This login was a suspicious event because PC1 is a device that Alice should use only as a user, not an administrator. A record also showed that the administrator created a new account called "sidious," an unknown name or one that does not appear on the company employee list. We input these artifacts in the propagation phase.
3) The investigators then searched the FS's security event log for any records relating to "sidious." They discovered a successful FS login using the "sidious" account. We input this artifact in the aggregation phase.
4) Alice, the user of PC1, said that she received a suspicious email and executed an attachment file. Based on this clue, the investigator proceeded to check PC1 and determine whether any PCs or servers had been attacked via PC1. From the prefetch files on PC1, the investigators found three records of file execution: thunderbird.exe as an email client, winword.exe, and MSHTA.exe, which were suspicious. The investigators also found a Word-format file name "for_your_benefit.doc" as an email attachment opened just before mshta.exe was executed. We input these artifacts in the infiltration phase.
5) The investigation continued on the mail server to find related logs supporting Alice's information. The investigators found a record from the mail log showing that Alice's mail account received an email from an unknown mail account. We input this artifact in the infiltration phase.
6) From the Sysmon event log on PC1, the investigators found a suspicious command execution after mshta.exe was executed. The attacker executed various commands in the penetrated network to investigate whether this environment could be exploited. There is a log that shows the execution of "mz.exe" as a trace of an exploitation of the "zerologon" vulnerability (CVE-2020-1472), using Mimikatz to gain administrator privileges in the domain. Using this exploit, the attacker changed the password of the administrator account to NULL, used the administrator account to create a "sidious" account, and added "sidious" to the "Domain Admins" group. The attacker also used Mimikatz to create a "Golden Ticket" and ran a pass-the-ticket attack using the created Golden Ticket.
7) Further investigation of the Sysmon event log on PC1 showed suspicious lateral movement activity from PC1 to OPC1. OPC1 was remotely operated from PC1 using PsExec under the "sidious" account and accessed another malicious domain MD-1. From the registry hive files, the investigators found a suspicious autorun entry in Alice's NTUSER.dat that the attacker used as an autorun backdoor program.

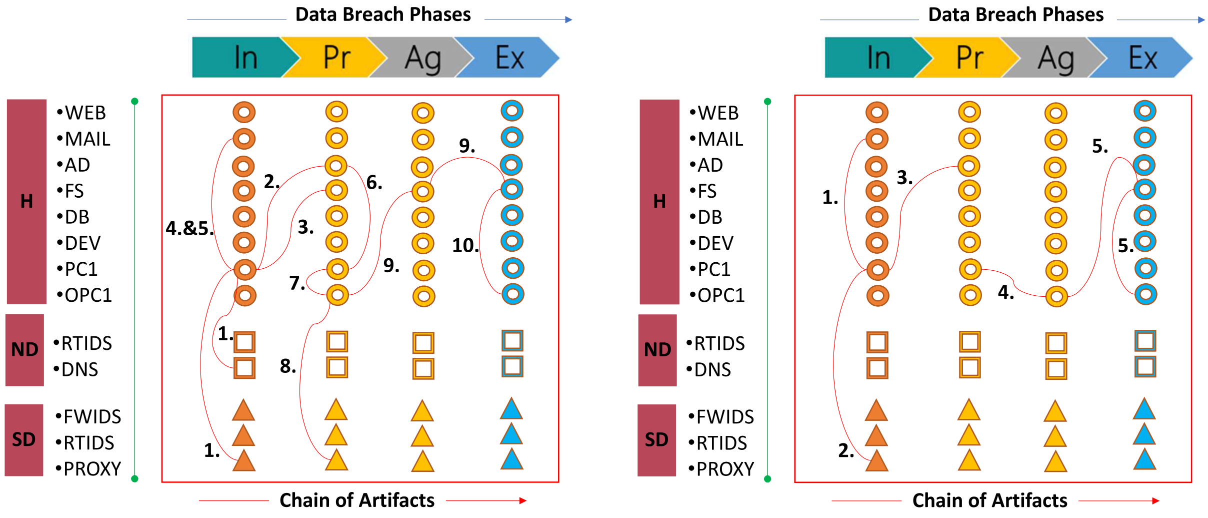
TABLE 5. Summary of the content examination, CoA, and timeline for the propagation phase.

Examination	Artifact	Chain of Artifacts (CoA)	Timeline
When PC1 and MD-2 were connected, a record showed a successful login using an administrator account.	AD-Security.evtx^{a}	CoA: [PROXY-access.log, DNS-queries], [AD-Security.evtx^{a}], [-], [-]	5/11/21 8:10
A record shows that the administrator created a new account called "sidious"	AD-Security.evtx^{b}	CoA: [PROXY-access.log, DNS-queries], [AD-Security.evtx^{a,b}], [-], [-]	5/11/21 8:10
There was a log that showed the execution of "mz.exe" as a trace of exploitation of "zerologon" vulnerability (CVE-2020-1472) using the Mimikatz to gain administrator privileges in the domain	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f}], [FS-Security.evtx], [-]	5/11/21 8:09
Using the Mimikatz exploit, the attacker changed the password of the administrator account to NULL	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{g}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g}], [FS-Security.evtx], [-]	5/11/21 8:09
The attacker used the administrator account to create "sidious" account	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{h}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h}], [FS-Security.evtx], [-]	5/11/21 8:10
The attacker added "sidious" to the "Domain Admins" group	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{i}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i}], [FS-Security.evtx], [-]	5/11/21 8:10
The attacker also used Mimikatz to create "Golden Ticket"	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{j}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j}], [FS-Security.evtx], [-]	5/11/21 8:20
After creating Golden Ticket, the attacker ran the pass-the-ticket attack	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{k}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k}], [FS-Security.evtx], [-]	5/11/21 8:20
The OPC1 was remotely operated from PC1 using PsExec under "sidious" account	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{l}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-WindowsSysmon%4Operation.evtx$^{f,g,h,i,j,k.l}$], [FS-Security.evtx], [-]	5/11/21 8:27
OPC1 accessed another malicious domain MD-1	PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{m}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx$^{f,g,h,i,j,k.l.m}$], [FS-Security.evtx], [-]	5/11/21 7:50
In the registry hive files, the investigators found a suspicious autorun entry in Alice's NTUSER.dat that the attacker used as an autorun backdoor program	PC1-Registry	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx$^{f,g,h,i,j,k.l.m}$, PC1-Registry], [FS-Security.evtx], [-]	5/11/21 8:19
The investigators verified a suspicious communication between OPC1 and MD-1, which was found in the proxy server logs	PROXY-access.log	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx$^{f,g,h,i,j,k.l.m}$, PC1-Registry, PROXY-access.log], [FS-Security.evtx], [-]	11/May/2021 08:27:41-09:29:05
The investigators found multiple EXE executions, such as PsExec, mshta and whoami	OPC1-Prefetch	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx$^{f,g,h,i,j,k.l.m}$, PC1-Registry, PROXY-access.log, OPC1-Prefetch], [FS-Security.evtx], [-]	5/11/21 8:27
From the OPC1 Sysmon, the investigators found a process creation event related to the MSHTA call	OPC1-Microsoft-Windows-Sysmon%4Operation.evtx	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx$^{f,g,h,i,j,k.l.m}$, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx], [-]	5/11/21 8:27

TABLE 6. Summary of the content examination, CoA, and timeline for the aggregation phase.

Examination	Artifact	Chain of Artifacts (CoA)	Timeline
Investigators discovered a successful FS login using a "sidious" account	FS-Security.evtx	CoA: [PROXY-access.log, DNS-queries], [AD-Security.evtx^{a,b}], [FS-Security.evtx], [-]	5/11/21 8:30
From OPC1 Sysmon event log, there was a suspicious activity that "sidious" attempted to mount the C drive of the FS server as the X drive of the OP1 using the net command	OPC1-Microsoft-Windows-Sysmon%4Operation.evtx	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [-]	5/11/21 8:29
The investigator found that OPC1 connected to FS via 445/TCP (Samba)	FS-Security.evtxo	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [ADSecurity.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o}], [-]	5/11/21 8:29
The investigator found that administrative privileges were assigned to "sidious"	FS-Security.evtx^{p}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p}], [-]	5/11/21 8:29
The investigator found that "sidious" successfully logged on	FS-Security.evtx^{q}	CoA:[PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q}], [-]	5/11/21 8:29
A record indicated that OP1 successfully mounted the FS server's C drive	FS-Security.evtx^{r}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q,r}], [-]	5/11/21 8:29

8) The next part of the investigation observed OPC1 and determined whether any PCs or servers had been attacked via OPC1. First, the investigators verified suspicious communication between OPC1 and MD-1, which was found in the proxy server logs. The communication lasted two minutes. Then, the investigators checked the OPC1 prefetch file to trace any suspicious file execution. The investigators found multiple EXE executions, such as PsExec, mshta and whoami. In addition, there were some typical Windows commands, SD.exe and RA.exe, which were located in the %TEMP% directory of "sidious". From the OPC1 Sysmon, the investigators found a process creation event related to the MSHTA call.
9) In the OPC1 Sysmon event log, there was a suspicious activity: "sidious" attempted to mount the C drive of the FS server as the X drive of OP1 using the net command. Further investigation of the FS security event log revealed that OPC1 connected to the FS via 445/TCP (Samba). Administrative privileges were assigned to "sidious", "sidious" successfully logged on, and OP1 successfully mounted the FS server's C drive. We input these findings in the exfiltration phase.



(a) Initial chain of artifacts from the case study.

(b) Updated version of the chain of artifacts.

FIGURE 5. Chain of artifacts of the case study.

10) Until step 9, the attacker was free to connect to the files on the FS server. The OPC1 Sysmon log showed that the attacker used the dir command to view the contents of the shared folder and its subfolders. Additionally, the attacker created some files using the certutil command in the %TEMP% folder, compressed all files in x:\share\ to “tmp.rar”, then deleted all files in %TEMP%\tmp using sd.exe. Here, the attacker successfully exfiltrated data from the FS drive to OPC1 and deleted the attack traces. We input the findings (Eq. 2) in the exfiltration phase.

CoA: [PROXY-access.log, DNS-queries,
PC1-Prefetch^{c,d,e}, MAIL-mail.log],
[AD-Security.evtx^{a,b}, PC1-Microsoft-Windows,
-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}
PC1-Registry,PROXY-access.log,OPC1-Prefetch,
OPC1-Microsoft-Windows-Sysmon%4Operation.evtx]
[FS-Security.evtx, OPC1-Microsoft-Windows
-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q,r}]
[OPC1-Microsoft-Windows
-Sysmon%4Operation.evtx^{s,t,u}] (2)

C. TIMELINE AND ATTACK FLOW ANALYSIS

Based on the content analysis and the CoA in the previous subsection, we obtained the incident’s timeline by sorting the artifacts’ timestamps from Tables 4, 5, 6, and 7. From the timeline table, we can identify the precise time or duration of the data breach. Here, the data exfiltration started on 11/05/2021 08:30:00 when “sidious” mounted the C drive of the FS server as the X drive of OP1 using the net use command and finished on 11/05/2021 08:39:27 when ra.exe (WinRAR) was executed to compress the x:\share folder and then create tmp.rar and exfiltrate it to the attacker.

To obtain the attack flow, we analyzed the step-by-step attacks carried out by the attacker in the system, resulting in the data breach. After obtaining the CoA as illustrated in Fig. 5(a), we simplify the steps according to the data breach breakdown phase to obtain the updated CoA, as presented in Fig. 5(b). To update the CoA, investigators reviewed all artifacts that were mapped at each DBB phase.

The review was carried out to justify the artifacts that most determined the attack stages that occurred in each DBB phase. In conducting this justification, investigators must have a strong understanding of the attacker’s perspective at each DBB phase. For instance, the infiltration phase, as explained in the previous section, is a phase that demonstrates how the attacker gains access to the system environment by exploiting an entry point. Therefore, reviewing artifacts for this attack flow should determine which host is the entry point and how the attacker gained access to that entry point. Based on Table 4, PC1 is the entry point where the attack stage occurred. Furthermore, based on the logs in Table 4 in chronological order, the attacker gained access to PC1 by sending an email containing malware, which then infected PC1, causing it to send a request packet to MD-2.

This process is at the core of the infiltration phase, so in Figure 5(b), the CoA for the infiltration phase consists of PC1, the mail server, and the proxy. Similarly, a review and justification process is carried out for the propagation, aggregation, and filtration phases to obtain an updated version of the CoA in Figure 5(b). Based on the updated CoA and timeline table, we obtained the attack flow as follows:

1) The attacker sent a targeted email to Alice. This email was sent from user[at]sv.test and had the subject IMPORTANT NOTICE!
2) Alice opened the attached file with the filename for_your_benefit.doc, and then her PC (PC1) was infected with RAT malware, which established a

TABLE 7. Summary of the content examination, chain of artifacts, and timeline for the exfiltration phase.

Examination	Artifact	Chain of Artifacts (CoA)	Timeline
The OPC1 Sysmon log showed that the attacker used the dir command to view the contents of the shared folder and its subfolders	OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{s}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q,r}], [OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{s}]	5/11/21 8:30
The attacker created some files using the certutil command in %TEMP% folder	OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{t}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtxa,b, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q,r}], [OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{s,t}]	5/11/21 8:38
The attacker compressed all files in x:\share\ to "tmp.rar", then deleted all files in %TEMP%\tmp using sd.exe"	OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{u}	CoA: [PROXY-access.log, DNS-queries, PC1-Prefetch^{c,d,e}, MAIL-mail.log], [AD-Security.evtx^{a,b}, PC1-Microsoft-Windows-Sysmon%4Operation.evtx^{f,g,h,i,j,k,l,m}, PC1-Registry, PROXY-access.log, OPC1-Prefetch, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx], [FS-Security.evtx, OPC1-Microsoft-Windows-Sysmon%4Operation.evtx, FS-Security.evtx^{o,p,q,r}], [OPC1-Microsoft-Windows-Sysmon%4Operation.evtx^{s,t,u}]	5/11/21 8:38

TABLE 8. 5WH questions and answers for the case study.

Questions	Answer Hints	Case Study Answer
What	Kind of data that has been breached	Files on the C drive of the file server (FS)
Who	• External actor • Internal actor • Partner	External actor
When	Precise time or duration of the breach	11/05/2021 08:30-08:39 (UTC)
Where	• In use • In transit • At rest	Data at rest on the FS
Why	• Intentional • Unintentional	Intentional breach using spear phishing and RAT malware.
How	Attack flow	a) The attacker sent a targeted email to Alice b) The attacker exploited the Zerologon vulnerability of the AD to gain domain administrative privileges c) The attacker conducted a lateral movement from PC1 to OP1 d) The attacker exfiltrated the FS server files, compressed them, and transferred them outside.

connection to the malicious domain (MD-2), and the attacker began to control PC1 remotely.

3) The attacker exploited the zerologon vulnerability of the AD to gain domain administrative privileges.
4) The attacker conducted a lateral movement by creating an unauthorized user account ‘‘sidious’’ and adding it to the ‘‘Domain Admins’’ group. Then, the attacker set up a registry backdoor on PC1 for permanent compromise and expanded control from PC1 to OP1 using the ‘‘sidious’’ account.
5) Finally, the attacker exfiltrated the FS server files from OP1, compressed them, and transferred them outside.

From the attack flow above, it can be seen how these case study incidents can occur by analyzing the step-by-step attacks carried out by attackers in the system, resulting in a data breach. Thus, the attack flow analysis results can answer the question ‘‘How’’ for incident investigation in the next step.

D. MAPPING FINDINGS AND FACTS INTO 5WH QUESTIONS

The final step of this case study is to answer this data breach incident investigation’s 5WH questions using the mapping provided in Table 2. By carrying out all the steps in the proposed framework, we obtain complete answers to the 5WH questions. Table 8 summarizes the complete answers to the 5WH questions from the case study investigations.

The above case study shows that our framework makes it easier to investigate an incident by using DBB as the main pillar. Furthermore, our 5WH mapping assists investigators in obtaining complete answers to the investigation questions. This characteristic is the main strength of our framework compared to other frameworks. Table 9 depicts the benchmarking of our proposed framework and other frameworks based on six characteristics. It can be seen that the entire framework provides a detailed description of the examination and analysis phases. Some of them also provide case studies,

TABLE 9. Characteristic benchmark of selected digital forensic frameworks.

Framework	Characteristics					
	Data breach characteristics	5WH phase and mapping	Evidence categorization	Detailed Examination and Analysis	Provides a case study	Gives the results of each case study step
Digital FOrensics framework for Reviewing and Investigating cyberattacks (D4I) [34]	×	×	√	√	√	×
The Integrated Digital Forensics Process Model (IDFPM) [33]	×	×	×	√	×	×
The Systematic Digital Forensic Investigation Model (SRDFIM) [32]	×	×	√	√	×	×
Cyber Forensic Field Triage Process Model (CFFTPM) [31]	×	×	×	√	√	×
Proposed Framework	√	√	√	√	√	√

showing that the designed framework is applicable. In contrast to others, our framework has a fundamental strength as a DBB-based design that has been proven to be compatible with data breach characteristics. Another major strength is that the investigation results focus more on answering the 5WH questions completely.

V. CONCLUSION

The main goal of the current study was to develop a new specific framework for data breach forensic investigations that can provide comprehensive answers to the 5WH questions of the investigation. The proposed framework is based on DBB, allowing it to analyze incidents for data breaches specifically. In addition, the proposed framework can provide answers to the 5WH questions based on the proposed mapping answers, which makes it easier to summarize the investigation's findings. This complete answer is the fundamental strength of the study compared to other studies in DFI. In addition, this study provides examples of how our proposed framework is applied in real-world data breach incident cases. Future research can explore how the proposed framework can be combined with classifications based on machine learning to provide predictive answers to questions such as "who", "where", and "why". In addition, future research can investigate the examined data's efficacy to obtain potential artifacts with reduced processing time. This can be achieved by developing a data reduction model for triage processes based on the specific characteristics of each of the three evidence classifications in the proposed framework.

ACKNOWLEDGMENT

This publication is supported by the Hibah Publikasi Terindeks Internasional (PUTI) Kolaborasi Internasional (Q2) Scheme, Universitas Indonesia, under Contract NKB-1339/UN2.RST/HKP.05.00/2022. The work of Arif Rahman Hakim was supported by the Lembaga Pengelola Dana Pendidikan (LPDP), Ministry of Finance of the Republic of Indonesia. The case study used in this work was provided by the Indonesia Cyber Awareness and Resilience Center, Universitas Indonesia (IdCARE-UI) through the IT Forensics Enablement Workshop supported by the Japan International Cooperation Agency (JICA).

REFERENCES

[1] S. Widup, A. Pinto, D. Hylender, G. Bassett, and P. Langlois, "DBIR 2021 data breach investigation report," Verizon Bus., New York, NY, USA, Tech. Rep. 2021DBIR, 2021.

[2] Flashpoint. (2022). *The State of Data Breach Intelligence: 2022 Midyear Edition | Flashpoint*. [Online]. Available: https://flashpoint.io/resources/report/state-of-data-breach-intelligence-2022-midyear/

[3] Accenture. (2022). *Elevating the Cybersecurity Discussion: Why CEOs Need to Get More Involved in Securing the Business*. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/custom/us-en/invest-cyber-resilience/pdf/Accenture-Elevating-the-Cybersecurity-Discussion.pdf#zoom=40

[4] F. Schlackl, N. Link, and H. Hoehle, "Antecedents and consequences of data breaches: A systematic review," *Inf. Manag.*, vol. 59, no. 4, Jun. 2022, Art. no. 103638. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0378720622000507

[5] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *J. Cybersecurity*, vol. 4, no. 1, Jan. 2018, Art. no. tyy006.

[6] P. Choong, E. Hutton, P. S. Richardson, and V. Rinaldo, "Protecting a brand: Evaluating the cost of a security breach from a marketer's perspective," *Amer. J. Manag.*, vol. 11, no. 1, pp. 59–67, 2017.

[7] P. Wang, H. D'Cruze, and D. Wood, "Economic costs and impacts of business data breaches," *Issues Inf. Syst.*, vol. 20, pp. 162–171, Apr. 2019.

[8] R. D. Banker and C. Feng, "The impact of information security breach incidents on CIO turnover," *J. Inf. Syst.*, vol. 33, no. 3, pp. 309–329, Sep. 2019. [Online]. Available: https://meridian.allenpress.com/jis/article-abstract/33/3/309/428598

[9] Y. Roumani, "Detection time of data breaches," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102508.

[10] Z. Song, G. A. Wang, and W. Fan, "Firm actions toward data breach incidents and firm equity value: An empirical study," in *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, 2017, pp. 4957–4966. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85103435589&partnerID=40&md5=3efc731ab7268f998a0b2359d072127a

[11] D. Kolevski, K. Michael, R. Abbas, and M. Freeman, "Cloud data breach disclosures: The consumer and their personally identifiable information (PII)?" in *Proc. IEEE Conf. Norbert Wiener 21st Century (CW)*. Wollongong, NSW, Australia: Institute of Electrical and Electronics Engineers, Jul. 2021, pp. 1–9. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85115985431&doi=10.1109%2F21CW48944.2021.953257&partnerID=40&md5=d4fc5cf596b5e59afba09bf41c937a2b

[12] M. Meisner, "Financial consequences of cyber attacks leading to data breaches in healthcare sector," *Copernican J. Finance Accounting*, vol. 6, no. 3, p. 63, Mar. 2018. [Online]. Available: https://apcz.umk.pl/czasopisma/index.php/CJFA/article/view/CJFA.2017.017

[13] D. D. Malliouris and A. Simpson, "Underlying and consequential costs of cyber security breaches: Changes in systematic risk," in *Proc. Workshop Econ. Inf. Secur.*, 2020, pp. 1–59.

[14] S. Muzatko and G. Bansal, "Consumer skepticism as it relates to E commerce data breaches and company efforts to enhance trust," in *Proc. MWAIS*, 2020, pp. 1–5.

[15] J. K. Pool, S. Akhlaghpour, F. Fatehi, and A. Burton-Jones, "Causes and impacts of personal health information (PHI) breaches: A scoping review and thematic analysis," in *Proc. 23rd Pacific Asia Conf. Inf. Syst.*, D. Xu, J. Jiang, and H. W. Kim, Eds. 2019, pp. 71–85. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85089221816&partnerID=40&md5=e8674dc1c5b735083c3a4248a50de2af

[16] Z. Aivazpour, R. Valecha, and R. Chakraborty, "The impact of data breach severity on post-breach online shopping intention," in *Proc. 39th Int. Conf. Inf. Syst.*, 2018, pp. 481–489. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85062490775&partnerID=40&md5=1133e04ed4d0187568e33b091665fcbb

[17] K. D. Martin, A. Borah, and R. W. Palmatier, "Data privacy: Effects on customer and firm performance," *J. Marketing*, vol. 81, no. 1, pp. 36–58, 2017. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1509/jm.15.0497

[18] S. Kashmiri, C. D. Nicol, and L. Hsu, "Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of IT, marketing, and CSR," *J. Acad. Marketing Sci.*, vol. 45, no. 2, pp. 208–228, Mar. 2017. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84973667602&doi=10.1007%2Fs11747-016-0486-5&partnerID=40&md5=e9ac76a50988cbac0ac5dd70b6c7f20d

[19] O. Durowoju, H. K. Chan, and X. Wang, "Investigation of the effect of e-platform information security breaches: A small and medium enterprise supply chain perspective," *IEEE Trans. Eng. Manag.*, vol. 69, no. 6, pp. 3694–3709, Dec. 2022.

[20] J. Haislip, K. Kolev, R. Pinsker, and T. Steffen, "The economic cost of cybersecurity breaches: A broad-based analysis," in *Proc. Workshop Econ. Inf. Secur. (WEIS)*, 2019, pp. 1–37.

[21] Z. He, J. HuangFu, M. J. Kohlbeck, and L. Wang, "The impact of customer's reported cybersecurity breaches on key supplier's relationship-specific investments and relationship duration," Feb. 2020. [Online]. Available: https://ssrn.com/abstract=3544245

[22] H. N. Chua, J. S. Teh, and A. Herbland, "Identifying the effect of data breach publicity on information security awareness using hierarchical regression," *IEEE Access*, vol. 9, pp. 121759–121770, 2021.

[23] IBM Corporation. (2021). *Cost of a Data Breach Report 2021*. [Online]. Available: https://www.ibm.com/security/data-breach

[24] *IBM Security's Cost of a Data Breach Report 2022*, IBM Corp., New York, NY, USA, 2022.

[25] S. Morgan. (2020). *Cybercrime to Cost the World $ 10.5 Trillion Annually by 2025*. [Online]. Available: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[26] S. Furnell, H. Heyburn, A. Whitehead, and J. N. Shah, "Understanding the full cost of cyber security breaches," *Comput. Fraud Secur.*, vol. 2020, no. 12, pp. 6–12, 2020, doi: 10.1016/S1361-3723(20)30127-5.

[27] G. Say and G. Vasudeva, "Learning from digital failures? The effectiveness of firms' divestiture and management turnover responses to data breaches," *Strategy Sci.*, vol. 5, no. 2, pp. 117–142, Jun. 2020.

[28] M. Khanafseh, M. Qatawneh, and W. Almobaideen, "A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 8, pp. 610–629, 2019.

[29] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial Revolution 4.0," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102237.

[30] R. E. Overill and J. Collie, "Quantitative evaluation of the results of digital forensic investigations: A review of progress," *Forensic Sci. Res.*, vol. 6, no. 1, pp. 13–18, Jan. 2021.

[31] M. Rogers, J. Goldman, R. Mislan, T. Wedge, and S. Debrota, "Computer forensics field triage process model," *J. Digit. Forensics, Secur. Law*, vol. 1, no. 2, pp. 1–21, 2006. [Online]. Available: https://commons.erau.edu/jdfsl/vol1/iss2/2

[32] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *Int. J. Comput. Sci. Secur. (IJCSS)*, vol. 5, no. 1, pp. 118–131, 2011. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8647&rep=rep1&type=pdf

[33] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Comput. Secur.*, vol. 38, pp. 103–115, Oct. 2013, doi: 10.1016/j.cose.2013.05.001.

[34] A. Dimitriadis, N. Ivezic, B. Kulvatunyou, and I. Mavridis, "D4I—Digital forensics framework for reviewing and investigating cyber attacks," *Array*, vol. 5, Mar. 2020, Art. no. 100015, doi: 10.1016/j.array.2019.100015.

[35] K. V. Acar, "Osint by crowdsourcing: A theoretical model for online child abuse investigations," *Int. J. Cyber Criminology*, vol. 12, no. 1, pp. 206–229, 2018.

[36] F. Casino, C. Pina, P. López-Aguilar, E. Batista, A. Solanas, and C. Patsakis, "SoK: Cross-border criminal investigations and digital evidence," *J. Cybersecurity*, vol. 8, no. 1, pp. 1–18, Jan. 2022. [Online]. Available: https://academic.oup.com/cybersecurity/article/8/1/tyac014/6909060

[37] L. Zarpala and F. Casino, "A blockchain-based forensic model for financial crime investigation: The embezzlement scenario," *Digit. Finance*, vol. 3, nos. 3–4, pp. 301–332, Dec. 2021. [Online]. Available: https://link.springer.com/article/10.1007/s42521-021-00035-5

[38] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-86, 2006.

[39] K. Fowler, *Data Breach Preparation and Response: Breaches are Certain, Impact is Not*. MA, USA: Elsevier, 2016.

[40] S. S. Mir, U. Shoaib, and M. S. Sarfraz, "Analysis of digital forensic investigation models," *Int. J. Comput. Sci. Inform. Secur.*, vol. 14, no. 11, pp. 292–301, 2016. [Online]. Available: https://sites.google.com/site/ijcsis/%0Ahttp://search.proquest.com.library.capella.edu/central/docview/1879098656/fulltextPDF/B41FDAC8A6604004PQ/4?accountid=27965

ARIF RAHMAN HAKIM (Member, IEEE) received the bachelor's degree in cryptography from the National Crypto Institute, Bogor, Indonesia, in 2008, and the master's degree in communication and information systems from the School of Electronics and Information Engineering, Beihang University, Beijing, China, in 2016. He is currently pursuing the Ph.D. degree in electrical engineering with the Faculty of Engineering, Universitas Indonesia, Depok, Indonesia. Since 2017, he has been a Lecturer with the National Cyber and Crypto Polytechnic, Indonesia. His research interests include cybersecurity, digital forensics, and cryptography.

KALAMULLAH RAMLI (Member, IEEE) received the master's degree in telecommunication engineering from the University of Wollongong, Wollongong, NSW, Australia, in 1997, and the Ph.D. degree in computer networks from Universität Duisburg-Essen (UDE), Germany, in 2003. Since 1994, he has been a Lecturer with Universitas Indonesia (UI), where he has been a Professor of computer engineering, since 2009. He currently teaches advanced communication networks, embedded systems, object-oriented programming, and engineering and entrepreneurship. He is a prolific author, with more than 125 journals and conference papers. He has published eight books and book chapters. His research interests include embedded systems, information and data security, computers and communication, and biomedical engineering.

TEDDY SURYA GUNAWAN (Senior Member, IEEE) received the B.Eng. degree (cum laude) in electrical engineering from Institut Teknologi Bandung (ITB), Indonesia, in 1998, the M.Eng. degree from the School of Computer Engineering, Nanyang Technological University, Singapore, in 2001, and the Ph.D. degree from the School of Electrical Engineering and Telecommunications, University of New South Wales (UNSW), Australia, in 2007. He was a Visiting Research Fellow with UNSW, from 2010 to 2021. He is currently an Adjunct Professor with Telkom University. He has been a Professor (since 2019) and the Head of Department (2015–2016) with the Department of Electrical and Computer Engineering, International Islamic University Malaysia. From 2017 to 2018, he was the Head of the Program Accreditation and Quality Assurance for the Faculty of Engineering, International Islamic University Malaysia. His research interests include speech and audio processing, biomedical signal processing and instrumentation, image and video processing, and parallel computing. He received the Best Researcher Award from IIUM, in 2018. He was the Chairperson of the IEEE Instrumentation and Measurement Society Malaysia Section, in 2013, 2014, 2020, and 2021. He has been a Chartered Engineer with IET, U.K., since 2016; an Insinyur Profesional Utama with PII, Indonesia, since 2021; a registered ASEAN engineer, since 2018; and an ASEAN Chartered Professional Engineer, since 2020.

SUSILA WINDARTA (Member, IEEE) received the degree in cryptography from the National Crypto Academy, Bogor, Indonesia, the bachelor's degree in information systems from Gunadarma University, Indonesia, and the master's degree in mathematics from the Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Depok, Indonesia, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering, Faculty of Engineering. Since 2013, he has been a Lecturer with the Department of Cyber-Security Engineering, National Cyber and Crypto Polytechnic, Indonesia. His research interests include cryptography and information security related topics, especially cryptographic hash functions and security protocols.