International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 11, No.1 (Mar-2022)

http://dx.doi.org/10.12785/ijcds/110186

Digital Forensics Investigation Procedures of Smart Grid Environment

Haris Iskandar Mohd Abdullah[1], Zul-Azri Ibrahim[2, 4], Fiza Abdul Rahim[3, 4], Hafizuddin Shahril Fadzil[1], Saiful Amin Sharul Nizam[1] and Muhammad Zulhusni Mustaffa[1]

[1]*UNITEN RD Sdn. Bhd., Kajang, Selangor, Malaysia*
[2]*College of Computing and Informatics, Universiti Tenaga Nasional, Kajang, Selangor, Malaysia*
[3]*Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia*
[4]*Institute of Informatics and Computing Energy, Universiti Tenaga Nasional, Kajang, Selangor, Malaysia*

Received 27 May. 2021, Revised 7 Jan. 2022, Accepted 9 Mar. 2022, Published 31 Mar. 2022

Abstract: Smart grids have been widely used around the world. The security of this system is debatable among the researchers because this area requires an improvement in order to reassure the grid is secured from cyberattacks. However, many malware were found attacking the smart grid systems such as Stuxnet, Flames, Triton, etc. Some of them are designed to avoid being tracked by a forensic investigator. The perpetrators used the fragility of digital evidence as an advantage to launch an attack on the smart grid without leaving traces. Technology development gives challenges to digital forensic procedures because the data volume is much higher. Thus, the digital forensic procedure needs to be redesigned, modified, and improved to capture traces and handle digital evidence. This paper aims to propose a digital forensic procedure to guide investigators to perform the digital forensic investigation, especially in a smart grid environment. This paper has discussed several suitable tools and techniques in digital forensic investigation to solve the problem or the challenges. This study discussed two cyberattacks examples and simulated the attack using a testbed to guide forensic investigators based on the proposed digital forensic procedure. Examples of cyberattacks are Distributed Denial of Service and False Data Injection attacks. This paper presented an appropriate methodology and relevant forensic tools to ensure the evidence's integrity during collection and analysis as legal evidence in court.

Keywords: Forensic, Process, Framework, Network Forensic, Live Digital Forensic, Dead Digital Forensic, Cyber-Physical System

1. Introduction and Overview

A smart grid is an infrastructure that consists of stations, substations, transmission lines, and transformers that are designed to deliver a certain area or a nation's power supply. Most smart grids use a system called Industrial Control Systems (ICS), which are the underlying monitoring and control components of critical infrastructures. Smart grid equipped with Advanced Metering Infrastructure (AMI), a system that consists of high technology hardware and software that enables data measurement intermittently and remote communication continuously [1].

Numerous real cases of cyberattacks have been reported attacking ICS around the world within the last ten years. The ICS cyber-attack threats believed to be started in 2010 when Stuxnet was discovered attacking a nuclear plant in Iran. Huge numbers of centrifuges are affected by this malware [2]. Duqu, believed as Stuxnet's cousin, found in 2011 that designed to collect information for cyber espionage [3]. The following year, Flame was found designed to perform the complex cryptanalytic attack [4]. Many other attacks were also detected in ICS, such as Gauss, Havex, Shamoon, etc. [5]. Eventually, the demand for digital forensics grows, and the need for a specific digital forensic procedure is required as the forensic process varies greatly from one environment to another.

Digital forensics plays an important role in modern-day cybercrime because the technology development emerges in a cyberattack, including the high technology environment such as the ICS. Some challenges related to the digital forensic procedure have been found and deliberately discussed among researchers. The first problem encountered is the lack of standard techniques to be used as a guideline to examine and analyze the data considering that the volume of data and type of digital sources are increasing [6]. In current years, technologies have evolved dramatically, and devices are growing in numbers. Existing procedures need to be improved parallel with the technology development in order to be able to investigate modern malware attacks.

E-mail address: haris.iskandar@uniten.edu.my, zulazri@uniten.edu.my, fiza.abdulrahim@utm.my, hafizuddin.shahril@uniten.edu.my, saiful.amin@uniten.edu.my, zulhusni@uniten.edu.my

The second problem is the increasing volumes of data, giving investigators a hard time in collecting evidence. This problem leads to the accumulation of digital forensic backlog commonly encountered by law enforcement [7]. A backlog is an event of uncompleted investigation work that requires a larger strategic plan. The third problem is the anti-forensic technique used to avoid evidence being captured [6]. One of the methods is to encrypt the data with a password. Multiple unsuccessful password attempts lead to all data being wiped out automatically [8]. An attacker has a chance to avoid evidence being tracked by implementing an anti-forensic technique.

Numerous other challenges occur when dealing with digital forensic investigation, as highlighted by Raghavan [9]. Raghavan lists five major challenges that came from complexity, diversity, consistency and correlation, quantity or volume, and unified time-lining problem. Therefore, it is necessary to revise existing procedures or design more procedures for the specific environment of digital forensic investigation. This study aims to review existing digital forensic investigation procedures and propose a digital forensics procedure for a smart grid environment.

2. Background

Several existing digital forensics frameworks are reviewed and analyzed, focusing on digital forensic investigation. Table 1 shows a list of frameworks proposed by previous researchers designed for digital forensic investigation.

Table **1**. Frameworks Proposed by Previous Researchers

Phase ID	Source	Framework Name	Environment
F01	[10]	Generic Computer Forensic Investigation Model	Computer
F02	[11]	Seamus Cybercrime Investigations Model	Cyber
F03	[12]	Seizure and Handling Evidence Process Model	Digital
F04	[13]	Digital Forensic Model Based on Malaysian Investigation Process	Technologies
F05	[14]	Systematic Digital Forensic Investigation Model	Wireless devices
F06	[15]	Digital Forensic Investigations using Internet of Things	Internet of Things
F07	[16]	Framework for Reliable Experimental Design	Digital data
F08	[17]	Cloud Computing Forensic Analysis Model	Log
F09	[18]	Digital Forensics Process for Computer Forensic	Digital Evidence
F10	[19]	Particle Deep Framework	Network

There are common processes, activities, or tasks highlighted in each phase of the existing frameworks. Table 2 shows phases proposed in frameworks designed by previous researchers.

Table **2**. Phases Mentioned in Proposed Frameworks

ID	Phases
F01	Pre-Process, Acquisition & Preservation, Analysis, Presentation, and Post-Process
F02	Awareness, Authorization, Planning, Notification, Search/Identify, Collection, Transport, Storage, Examination, Hypothesis, Presentation, Proof/Defense, and Dissemination.
F03	Identification/Preparation, Search and Seizure, Preservation, Examination, Analysis, and Reporting.
F04	Planning, Identification, Reconnaissance, Analysis, Result, Proof & Defense, Archive Storage, and Documentation.
F05	Preparation, Securing the Scene, Survey & Recognition, Documentation of Scene, Communication of Scene, Communication Shielding, Evidence Collection, Preservation, Examination, Analysis, Presentation, and Result.
F06	Preparation for Investigation, Protecting Evidence, Evidence Acquisition, Analysis of Evidence, Accelerating the Investigations, and Result Dissemination.
F07	Plan, Implement, Evaluate, Repeat Process, Analyze, and Confirm.
F08	Acquisition and Integration, Pre-processing, Correlation, Sequencing, and Analysis and Reporting.
F09	Identification, Acquisition, Preservation, Examination, and Presentation.
F10	Collection, Preservation, Examination and Analysis, and Presentation.

All the phases found in the ten frameworks are identified to find out which steps are identical and important that are needed in the framework of a digital forensic investigation. Table 3 shows each phase in the framework is classified as Phase ID, while Framework ID is used to justify which framework use the phase.

Table **3**. List of Phases in Proposed Frameworks

Phase ID	Name of phases	Framework ID
P01	Accelerating investigation	F06
P02	Acquisition	F01, F06, F08, F09
P03	Analysis	F01, F03, F04, F05, F06, F07, F08, F010

P04	Archive Storage	F04
P05	Authorization	F02
P06	Awareness	F02
P07	Collection	F02, F010
P08	Communication Shielding	F05
P09	Confirm	F07
P10	Correlation	F08
P11	Dissemination	F02, F06
P12	Documentation	F03, F05
P13	Evaluate	F07
P14	Evidence Collection	F05
P15	Examination	F02, F03, F05, F09, F010
P16	Hypothesis	F02
P17	Identification	F03, F04, F09
P18	Implement	F07
P19	Integration	F08
P20	Notification	F02
P21	Planning	F02, F04, F07
P22	Post-Process	F01
P23	Preparation	F03, F05, F06
P24	Pre-Process	F01
P25	Preprocessing	F08
P26	Presentation	F01, F02, F05, F09, F10
P27	Preservation	F01, F03, F05, F09, F10
P28	Proof/Defense	F02, F04
P29	Protecting evidence	F06
P30	Reconnaissance	F04
P31	Repeat	F07
P32	Reporting	F03, F08
P33	Result	F04, F05
P34	Search & Seizure	F03
P35	Search/identify	F02
P36	Securing scene	F05
P37	Sequencing	F08
P38	Storage	F02
P39	Survey & recognition	F05
P40	Transport	F02

Each description for all phases is observed to identify common activities performed in the identified phase. After detailed observation, seven phases are specified as a guideline to assist investigators in conducting a smart grid digital forensic investigation framework. As listed in Table 3, the 40 phases are then grouped into seven phases based on the similarity of phase description. The seven phases are shown in Table 4.

Table **4**. Proposed Phases Grouped into Seven Phases

Phase	**Phase ID**
Preparation	P05, P06, P21, P23, P24
Identification	P13, P17, P20, P30, P39
Collection	P02, P07, P08, P14, P19, P25, P34, P35, P36
Preservation	P12, P27, P29, P38, P40
Analysis	P01, P03, P10, P15, P16, P18, P31, P37
Proof/Defense	P09, P26, P28, P32, P33
Dissemination	P04, P11, P22

The phases outlined in Table 5 were then reevaluated to identify activities that could be carried out in parallel. The three phases, namely Identification, Collection and Preservation, are integrated into one phase called Collection. The last two phases, called Proof/Defense and Dissemination are grouped under a phase named Presentation in the framework.

Table **5**. Proposed Phases in Reviewed Frameworks

Phase	**Framework ID**
Preparation	F1, F2, F3, F4, F5, F6, F7
Identification	F2, F3, F4, F5, F7, F9,
Collection	F1, F2, F3, F4, F5, F6, F7, F8, F9, F10
Preservation	F2, F3, F5, F6, F9, F10
Analysis	F1, F2, F3, F4, F5, F6, F7, F8, F9, F10
Proof/Defense	F1, F2, F3, F4, F5, F7, F8, F9, F10
Dissemination	F1, F2, F4, F5, F6,

Since each phase depends on its respective procedures, tasks, and subtasks, Figure 1 features reversible phases indicating that new information can be obtained in previous phases before finalizing the findings.

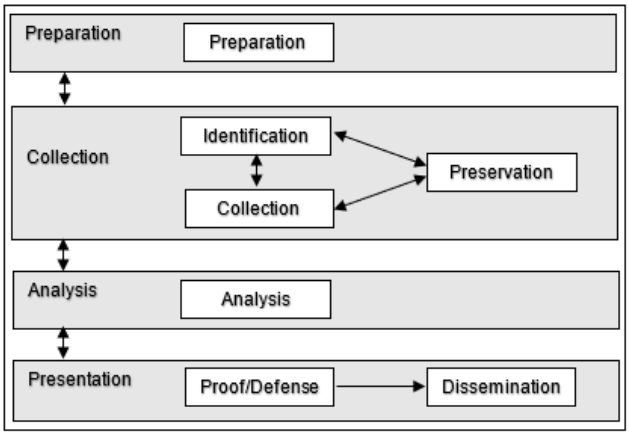

Figure 1. Integrated Phases of Digital Forensic Investigation

3. Related Work

In this section, the key activities of digital forensics investigations in a smart grid environment are explored in four major phases, as shown in Figure 2.

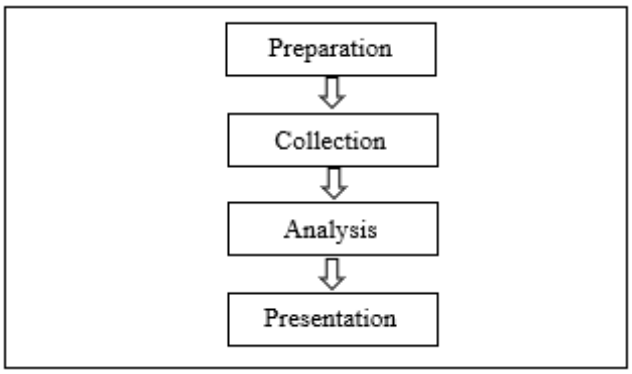

Figure 2. Major Phases in Digital Forensic Investigation

A. Smart Grid Digital Forensic Investigation Procedure

1) Preparation Phase

The first phase to investigate cyberattacks is to perform preparation in order to avoid unreadiness in an investigation of the crime. Proper preparation is essential, especially when it comes to investigating cyberattacks because the evidence is volatile and requires special skills and equipment. Before investigators perform an investigation, they need a thorough preparation regarding the crime. The forensic team must perform the preparation phase before launching the investigation at the crime scene. The forensic investigation framework was developed to guide investigators in handling data and preserving the integrity of the evidence to be presented in court. Digital data is volatile, thus requiring strategies and planning to launch the investigation. The activities in the preparation phase are summarized in Table 6.

Table 6. Preparation Phase Procedures

No.	Activity	References
1	Conduct briefing and brainstorming sessions with forensic team members.	[20]
2	Obtain authorization to conduct an investigation.	
3	Prepare a document to conduct an investigation.	
4	Prepare equipment to conduct an investigation.	
5	Interview experts to gain more information regarding the crime.	
6	Sketch the information in a journal for recreating or conveying details of the scene.	

After the investigator receives an order from a client to investigate a cyberattack, the first activity is to gather the forensic team and expose every information related to the crime. Item to be discussed during preliminary information gathering are built from what, who, where, when, and how. The team must brief the purpose of the investigation and explain the committed offence to build strategies to conduct the investigation.

The second activity is to obtain approval from the authority to perform the investigation. The authorization allows the investigator to seize the device to prevent the data from being tampered with, modified, or changed. In order to seize, investigators require authorization to conduct the investigation. Without the consent of the court, the evidence is unable to maintain the chain of custody. Eventually, the evidence will be inadmissible in court if authorization is not obtained in the preparation phase.

The third step of the preparation phase recommends that the investigators prepare the documents used in the investigation. Examples of documents are Investigation Diary or Journal, Seizure List, Chain of Custody Form, etc. [20]. Thus, investigators should prepare those documents to avoid untidy work of investigation.

Digital forensic investigation requires appropriate tools and equipment. Thus, it is important to prepare everything before performing an investigation. The list of equipment specifically for the smart grid would be a camera, labeling tools, imaging tool, analysis tool, storage media, Wireshark, etc.

After the information is briefed, the team should identify experts or technical persons to be interviewed to obtain more detailed information related to the crime scene. Without this information, the investigator may take a long time to investigate since the network communication and smart grid components are relatively complex. The suggested information to be gathered is the purpose of evidence, users of evidence, type of internet access, offsite storage, and etc. Then, the forensic team must document all information obtained in this phase to recreate or convey the scene's details. From that information, the team will be able to prepare plans and strategies to conduct the investigation. A thorough plan is required because smart grid forensic investigation deals with handling volatile data. The preservation planning also should be prepared in order to ensure the integrity of the evidence obtained later.

2) Collection Phase

In the Collection phase, the team acquires evidence from all possible sources. All data relating to the incident is identified, labeled, recorded, and collected while preserving its integrity. During evidence collection, it is necessary to use a preservation technique to preserve the integrity of evidence. Preservation is the main objective of reviewing digital forensic investigation procedures. When investigators fail to understand digital evidence authentication effectively, it may lead to adverse outcomes in the presentation before courts [21]. In this phase, the Chain of Custody process is initiated. The activities in the Collection phase are detailed in Table 4 and Table 5.

To collect evidence, investigators must ensure the scene is secured. If possible and necessary, the communication

must be blocked to avoid data contamination. It is also important to photograph the crime scene and devices for future reconstruction. Then, the investigator needs to identify affected components and check whether they are running or turned off. Ensure every cable was properly connected or disconnected and photograph every connected and disconnected component. From here, investigators would be able to identify which method can be used to conduct the investigation, whether it is live forensic or dead forensic. These two types of forensic require different techniques and procedures. Thus, this paper divided the collection of digital evidence into two types of forensic investigations.

a) Acquiring Live Digital Evidence

Acquiring live data is important to obtain vital information regarding the source of an attack. Live data is very fragile because any movement or activity may lead to the data being tampered. This paper proposes forensic procedures to collect evidence to ensure the integrity of evidence in the live digital forensic, as shown in Table 7.

Table **7**. Collection Phase Procedures in Smart Grid Live Forensic Investigation

No.	Activity	References
1	Photograph and label connected components.	[20]
2	Capture memory usage.	[22]
3	Collect CPU and TTL.	[22], [23]
4	Collect pagefile in the memory dump.	[22]
5	Perform network sniffing to capture network traffic.	[24]
6	Validate the data by calculating the hash value using MD5.	[25]
7	Label and photograph obtained evidence.	[20]

It is important to label connected cables and components with the devices. To prevent the devices from being turned off, ensure the power cable is properly connected. A lot of data can be collected from Random Access Memory (RAM) which will be lost if the device is dead. Thus, collecting RAM data is crucial to be performed as soon as possible to prevent the risk of data loss.

Some information contained in RAM that can be used as digital evidence are running processes, open files, network traffic information, etc. The investigators may capture a list of open network connections, the ARP table, the routing table, and interface configuration [22]. FTK Imager, Magnet RAM Capture, and Dumpit are some of the tools to capture the memory in RAM [26]. CPU and TTL usage are some of the attributes to detect anomalies in the live forensic investigation for cyberattack. Thus, collecting those evidence is crucial in the investigation of cyberattack in a smart grid environment.

Pagefile is a reserved portion of a hard disk that is used as an extension of RAM for data in RAM that hasn't been used recently. Therefore, collecting pagefile in a memory dump might contain evidence of the crime. Pagefile mostly can be obtained from hard disk. Many tools are available to collect pagefiles, such as X-Ways forensic, FTK imager, and DiskExplorer [27]. Due to the cyberattack can manipulate communication between components in the smart grid environment, investigators should perform network sniffing to capture network traffic. Some of the tools to capture network traffic are Ethereal, WinPcap, AirPcap, Tcpdump, Taps, SPAN, NetIntercept, Xplico, etc. [28], [29], and the popular one is Wireshark. By collecting traffic flow, it is possible to discover evidence regarding the attack source.

After crucial data is collected, the investigator needs to validate the data using MD5 or SHA to ensure the integrity of the evidence. Tools designed to calculate hash value are IgorWare Hasher, HashCheck, Nirsoft HashMyFiles, and etc. Lastly, photograph and sketch information related to the investigation should be obtained. The evidence's integrity can be verified and forensic analysis can be automated using Sleuthkit and md5sum [25].

b) Acquiring Dead Digital Evidence

When a system is powered off, collecting information from RAM is not applicable. The data may be stored in storage media. Some storage media that may consist of stored data are hard disk, floppy disk, CD, DVD, etc. The activities in acquiring dead data are detailed in Table 8.

Table **8**. Collection Phase Procedures in Smart Grid Dead Forensic Investigation

No.	Activity	References
1	Photograph and sketch crime scene.	[20]
2	Check affected components.	Proposed activity
3	Label connected cables and components.	[20]
4	Seize storage media or devices.	[30]
5	Record date and time in BIOS.	[31]
6	Connect drives to a write blocker to prevent OS from accidentally writing to the hard drive.	[32]
7	Perform data imaging to collect data from a hard disk while preserving the integrity of evidence.	[25]
8	Calculate the hash value to verify the integrity of the evidence.	[25]
9	Label and photograph obtained evidence.	[20]

Firstly, the investigators should photograph and sketch the crime scene and document all in a specific form to maintain the chain of custody. Next, the investigators must ensure that the system is completely turned off before conducting dead forensic because a turned-on system may consist of live digital data. Label all connected cables and components into the affected components to preserve the integrity of the evidence. If the system is completely turned off, investigators must remove the storage media from the

devices to acquire static data. The captured hardware needs to be labeled with unique identifiers such as brand, serial number, and etc. The investigator needs to record the exact date and time in the BIOS to determine when the attack occurred. This note is necessary to allow the investigator to compare time with reliable time sources and identify any differences.

Before collecting the data from storage media, it should be connected with a write blocker to prevent modification of the evidence or data from being tampered with. After being connected with a write blocker, the data need to be duplicated to preserve the originality of the data. A write-blocker device is used in this phase before collecting data from a hard disk to preserve the integrity of the file meta-data, such as timestamps [33]. Thus, the investigator needs to perform data imaging to collect data. It is recommended that evidence duplication be performed for every storage medium consisting of digital data using Logical Backup or Bit Stream Imaging [30]. Forensic software and hardware tools, namely Fundl and RegCon can be used for memory dumping and sorting evidence for analysis [34]. Next, the data need to be validated by calculating the hash value. Similar to the live digital forensic, the investigator may calculate the hash value using MD5 or SHA.

3) Analysis Phase

In the analysis phase, the investigation team performs an analysis of data collected during the previous phase. There are many techniques and justifiable methods to derive useful information for digital forensic investigation. The activities in the analysis phase are detailed in Table 9.

Table **9**. Analysis Phase Procedures in Smart Grid Forensic Investigation

No.	Activity	References
1	Perform data mining to sort and analyze seemingly unrelated entities within datasets.	[35]
2	Perform data classification to categorize data in order of level of effectiveness and efficiency.	[36]
3	Reduce the volume of data required to be analyzed using data reduction techniques.	[37]
4	Parse PCAP files and extract individual packets.	[38]
5	Divide packets at different low-level protocols.	
6	Collect TCP packets into streams.	
7	Divide streams with higher-level protocol dissectors	
8	Determine changes in the network and monitor timestamp.	[39]
9	Reconstruct the attack scenario and attribution to the source of attack based on the analysis.	

Due to the smart grid generating a large amount of database and containing huge data, investigators may perform data mining, data classification, and data reduction. Data mining is used to sort and analyze seemingly related entities within the dataset. Three steps involved in data mining are exploration, pattern identification, and deployment [40]. Next, the investigator may categorize data in order of level of effectiveness and efficiency. Some of the techniques the classify data are ID3, C4.5 Bayesian Network, K-Nearest Neighbor, SVM, and etc. [41]. Then, the investigator may perform data reduction to reduce the size of storing evidence. Several data reduction methods are available to be used, such as Features Reduction, Principal Component Analysis, Entropy Measure, Values Reduction, and Cases Reduction [37].

Wireshark, snort, and tcpdump are among popular tools to process PCAP files for analyzing network traffic. Cohen (2008) proposed the PyFlag method to analyze data in network forensic. The proposed method divides network traffic by parsing the PCAP files and files and extracting individual packets. Then, the packets are divided at different low-level protocols, such as Ethernet, IP, TCP, or UDP. The TCP packets are then collected into streams using a TCP stream reassembler. Next, the streams are divided with a higher-level protocol such as HTTP, IRC, MSN Chat, etc.

Rizal et al. (2018) proposed an analysis method using Wireshark, where the logs are examined to determine network changes and view timestamps. The analysis is performed on any part of the frame representing an attack packet flooding of IP address. Then, attack packets contained in the log file will be collected using the statistics module endpoint.

4) Presentation Phase

In the Presentation phase, the finding will be presented in court to justify the evidence. This phase involves proving a perpetrator of the cyber-attack or defense a victim from being sentenced to guilty based on the presentation of the result before jurisdiction. The procedures in the presentation phase are shown in Table 10.

Table **10**. Presentation Phase Procedures in Smart Grid Forensic Investigation

No.	Activity	References
1	Write a forensic workflow. Indicate the use of tools and methods	[42]
2	Classify all evidence in the investigation	
3	Prepare interactive cross-examination.	
4	Present the findings to management	
5	Disseminate the finding for future references	[11]

In this final phase, all activities, equipment, and methods are recorded to be presented to the management or court. The forensic workflow must be written by professional forensic staff. Then, investigators need to classify the ev-

idence to be presented, such as the type of tools used to launch an attack, professional personnel certification of digital evidence, etc. [42]. Next, the investigator can prepare interactive cross-examination to meet the need of management or court. Lastly, all the documents, workflow, data, evidence, and findings are presented to the management.

For future work, investigators disseminate the finding for other cases that may be related. Thus, the document must also include a recommendation. The disseminated document must also include a recommendation for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process. The investigation result is not destroyed but is to be stored for future references.

B. Smart Grid Digital Forensic Investigation Flowchart

Based on the proposed framework (Figure 2), this paper has developed a flowchart, which translates each phase and activity as shown in Figure 3. This flowchart aims to assist the forensic team, especially the first responder and forensic analyst. The first responder may use the flowchart as a reference when conducting on-scene investigations. At the same time, the forensic analyst may review the first responder's activities and indicate analytical activities to be carried out next.

4. Forensics Investigation On CyberAttack Scenario

This section discussed the examples of a cyberattack on AMI and applied the procedure proposed in this study to conduct a forensic investigation on Distributed Denial of Service (DDoS) and False Data Injection (FDI). This paper applied the procedure for each cyberattack to emphasize different techniques applicable depending on the type of attack.

A. Distributed Denial of Service

DDoS is an attack that attacks the network resource to prevent legitimate users from accessing the affected system [43]. An attacker may use two methods to launch DDoS, sending malformed packets to confuse or disrupt legitimate users by exhausting the resources [44]; thus, it is called an attack that violates availability.

This study simulates the DDoS attack using four Raspberry Pi's, switch, and Virtual Machine. Raspberry Pi's act as smart meters, and Virtual Machine operates as Data Collector and Meter Data Management System (MDMS). The topology of these components is shown in Figure 4. The Blue arrow shows normal communication between the smart meter and data collector, while the red arrow shows a communication under attack by four smart meters. Smart Meter A act as a normal user, while Smart Meter B, C, and D act as the attackers. Smart Meter B, C and D launch DDoS attacks to data collector so that Smart Meter A cannot send data to the data collector.

Network forensic live investigation is used when the cyber attack event occurs over a network connection, mostly ingresses and egress traffic from one device to another. Investigators need to prepare network forensic tools such as network sniffers to investigate DDoS attacks because this kind of attack is related to network forensics. Identification of DoS attacks is principally founded on network data analysis, for example, connection requests, packet headers, etc. [45].

Begin with acquiring data from a network connection. The evidence may contain multiple sources of data. The major one is the information maintained by network nodes [46]. In this study, we collect data received in MDMS to detect the attack. The artifacts collected from the dataset are log files, data files, data caches, transaction logs, widows log events, etc. [47]. Log Activity was key digital proof in noting every activity in the Router [48]. The artifacts enable investigators to identify notable events and classify action patterns. For DDoS investigation, we have to acquire real-time data such as CPU, memory performance, and ping reply as evidence from the DDoS attacks.

Collected data are analyzed to produce significant evidence using several available appropriate tools. The techniques vary on the type of collected data. For instance, this study compares the readings during DDoS attacks with readings during normal traffic flow. If the network bandwidth value is less than normal, CPU and memory performance is high, and ping reply often indicates that the device is under attack. After analyzing the data, this study constructs the attack scenario to obtain a correlation of the evidence with the crime event. This investigation shows that data collectors are unable to receive data consumption from smart meters due to DDoS attacks.

Investigators need to design a graph to show the attack on smart grid components based on the analysis. All activities are documented in legal forms to maintain the chain of custody. The result and documents are presented before the court to classify the case. This includes equipment and tools used while performing the investigation. Lastly, the case is stored and disseminated for other relevant investigations.

B. False Data Injection

FDI attack affects packets' data integrity by modifying their payloads [49]. According to [50], FDI attacks could bypass the SCADA system. In a smart grid, the DoS attack can disable the connection between the smart meter and the data collector, while the FDI attacks can change the smart meter reading to be collected by the server. Thus, this attack can be called an attack that violates integrity.

This paper has developed a testbed that consists of four main hardware components to simulate an FDI attack, as shown in Figure 5. Smart Meter A sends normal data to the data collector. Smart Meter B acts as an attacker to modify smart meter A's data and send it back to the data collector. Data Collector received false readings from Smart Meter B. The red arrows show two-way communications between Smart Meters and Data Collector, where the attacker sniffs network traffic and identifies the potentially vulnerable

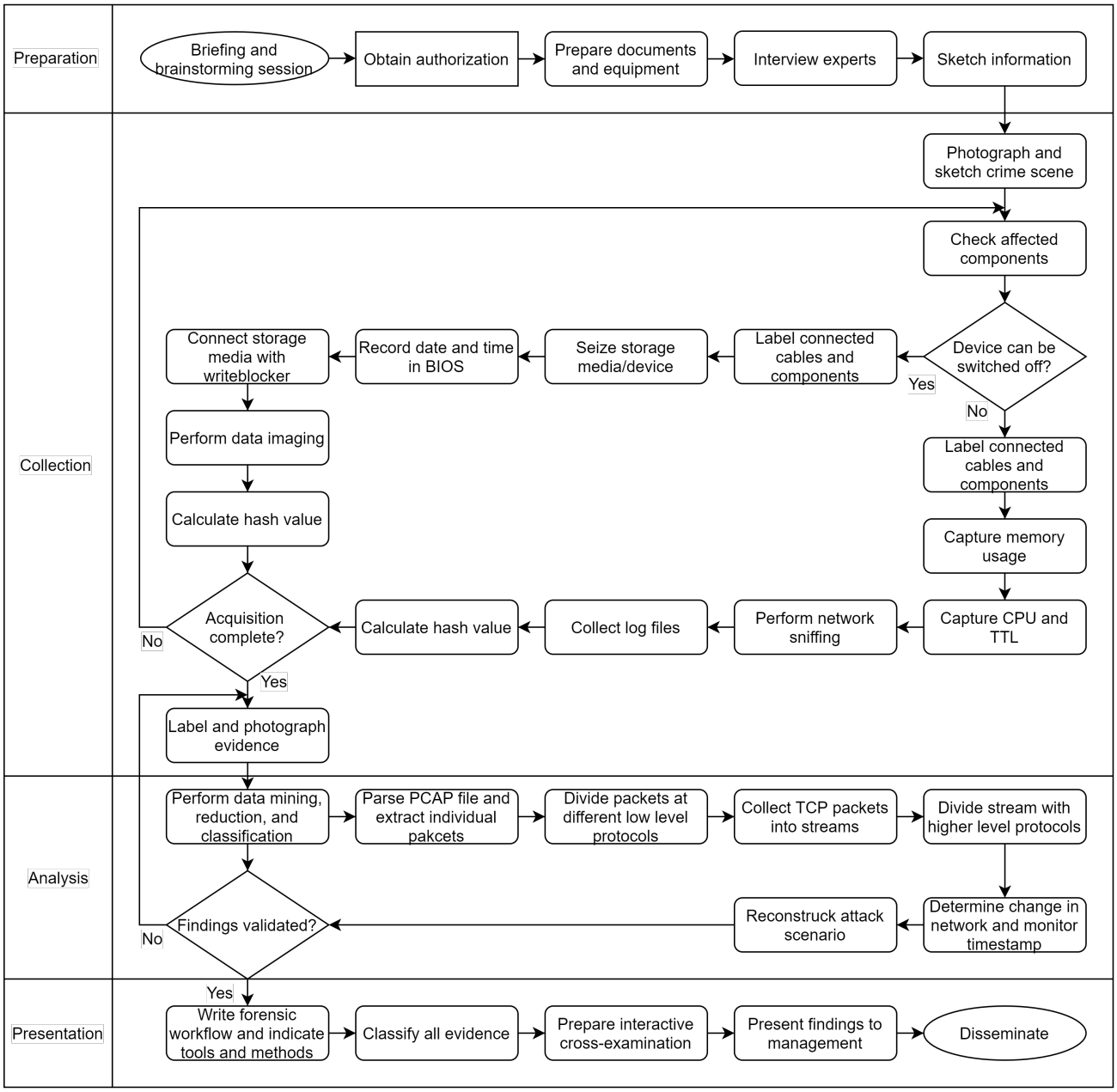

Figure 3. Smart Grid Digital Forensic Investigation Flow Chart

IP address. Then, the attacker spoofs the network traffic between Smart Meter A to Data Collector and proceeds with FDI attack.

FDIA can be a subtler attack than DoS [51] because it is difficult to detect. Thus, forensic investigator must prepare a subtle approach to detect the attack. This paper proposes these attributes to investigate FDI attack as shown in Table 11. These attributes may be found in the PCAP file collected from the packet sniffer. This study also gathers ARP cache from data collectors and smart meters.

Using SQL database, it can view and display artifacts of user data, device name, last accessed, last login, created by, etc. [52]. The attributes are monitored in order to analyze the data in the FDI attack. The attributes are then compared between normal traffic and under attack traffic. If the attributes are different, it indicates the probability that an attack has occurred between the smart meter communication and the data collector. After collection and analysis activi-

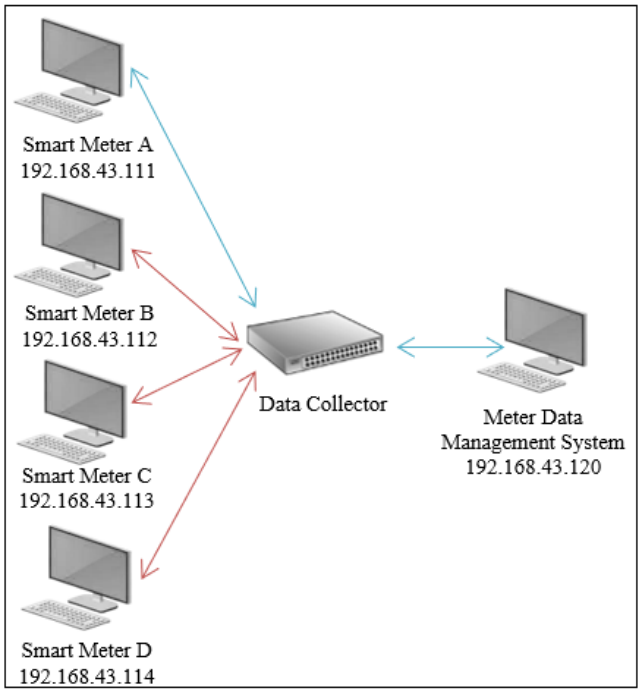

Figure 4. Distributed Denial of Service Attack Testbed Topology

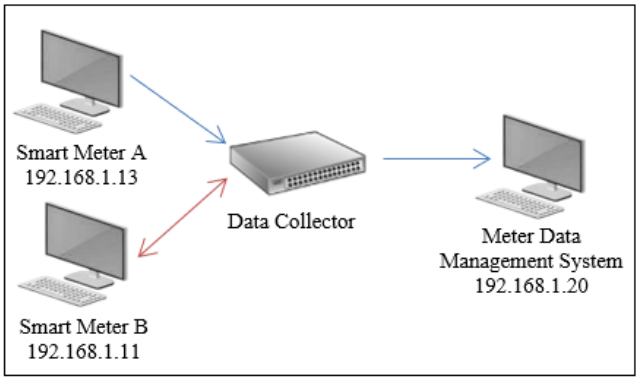

Figure 5. False Data Injection Attack Testbed Topology

ties are completed, this study constructs an attack scenario based on comparing attributes in Table 11 to propose the result in court.

Table 11. Attributes to detect FDI attack

Attributes	Description
SrcIp	Source IP address
SrcPort	Source port address
DstIp	Destination IP address
DstPort	Destination port address
SrcMac	Source MAC address
DstMac	Destination MAC address
TTL	Time to live of the packets
ARPReq	ARP request traffic
ARPRep	ARP reply traffic
TimeDelay	Time delay for the client to receive a reply from the server

Like every forensic investigation, all activity and workflow should be documented to maintain the chain of custody while conducting the investigation. Those documents and the result of the analysis are presented before law enforcement for verification of the case. The last step is to store the document related to the case and disseminate it for further related investigation.

5. Conclusion And Future Works

The world is facing tremendous growth in technology development. The know-how in IT enables more hazardous malware capable of attacking high technology systems, including the ICS. In order for cyberattacks to be investigated, specific guidance or procedure is needed. The procedures can preserve the integrity of the evidence and make it presentable in court. Four phases framework presented in this study can serve as a basis for investigators to perform digital forensic investigations in a smart grid environment. Given that this proposed procedure is the result of a variety of established procedures, the study intends to validate the proposed procedures in a larger-scale simulated environment, which could then be the baseline for other investigations. An effective collection and analysis tool will be proposed to improve the effectiveness of the procedure.

6. Acknowledgement

This study was funded by Tenaga Nasional Berhad Seed Fund (U-TD-RD-19-25) in collaboration with TNB Asset Management Department. We would like to thank UNITEN R&D Sdn. Bhd. for fund management.

References

[1] J. F. Martins, A. G. Pronto, V. Delgado-Gomes, and M. Sanduleac, "Smart Meters and Advanced Metering Infrastructure," *Pathways to a Smarter Power System*, no. October 2017, pp. 89–114, 2019.

[2] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[3] B. Bencsáth, G. Pék, L. Buttyán, and M. Félegyházi, "The cousins of Stuxnet: Duqu, Flame, and Gauss," *Future Internet*, vol. 4, no. 4, pp. 971–1003, 2012.

[4] N. Virvilis and D. Gritzalis, "The big four - What we did wrong in advanced persistent threat detection?" *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 248–254, 2013.

[5] K. E. Hemsley and D. R. E. Fisher, "History of Industrial Control System Cyber Incidents," *INL/CON-18-44411-Revision-2*, no. December, pp. 1–37, 2018. [Online]. Available: https://www.osti.gov/servlets/purl/1505628

[6] D. Lillis, B. Becker, T. O'Sullivan, and M. Scanlon, "Current Challenges and Future Research Areas for Digital Forensic Investigation," 2016. [Online]. Available: http://arxiv.org/abs/1604.03850

[7] X. Du, N. A. Le-Khac, and M. Scanlon, "Evaluation of digital forensic process models with respect to digital forensics as a service," *European Conference on Information Warfare and Security, ECCWS*, pp. 573–581, 2017.

[8] K. Conlan, I. Baggili, and F. Breitinger, "Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy," *DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference*, vol. 18, no. December 2015, pp. S66–S75, 2016.

[9] S. Raghavan, "Digital forensic research: current state of the art," *CSI Transactions on ICT*, vol. 1, no. 1, pp. 91–114, 2013.

[10] Y. Yunus, I. Roslan, and H. Zainuddin, "Common Phases of Computer Forensics Investigation Models," *International Journal of Computer Science & Information Technology (IJCSIT)*, vol. 3, no. 3, pp. 17–31, 2011.

[11] S. Ó. Ciardhuáin, "An Extended Model of Cybercrime Investigations - A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf," *Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004. [Online]. Available: https://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf

[12] J. T. Ami-Narh and P. A. Williams, "Digital forensics and the legal system: A dilemma of our times," *Proceedings of the 6th Australian Digital Forensics Conference*, pp. 30–40, 2008.

[13] S. Perumal, "Digital Forensic Model Based On Malaysian Investigation Process," *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 8, pp. 38–44, 2009.

[14] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *International Journal of Computer Science and Security (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

[15] K. Dhar and Y. Pingle, "Digital Forensic Investigations (DFI) using Internet of Things (IoT)," *Institute of Electrical and Electronics Engineers*, pp. 1443–1447, 2016.

[16] G. Horsman, "Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics," *Computers and Security*, vol. 73, pp. 294–306, 2018. [Online]. Available: https://doi.org/10.1016/j.cose.2017.11.009

[17] M. N. Ahmed Khan and S. W. Ullah, "A log aggregation forensic analysis framework for cloud computing environments," *Computer Fraud and Security*, vol. 2017, no. 7, pp. 11–16, 2017. [Online]. Available: http://dx.doi.org/10.1016/S1361-3723(17)30060-X

[18] 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," *Journal of Physics: Conference Series*, vol. 1418, no. 1, 2019.

[19] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020. [Online]. Available: https://doi.org/10.1016/j.future.2020.03.042

[20] S. Khadijah, T. Mohd, Z. Adil, and B. Talib, "Standard Operating Procedure of Digital Evidence Collection," no. July, 2013. [Online]. Available: http://www.cybercsi.my/download/SOPOFDIGITALEVIDENCECOLLECTION.pdf

[21] G. D. Rodríguez Rafael and F. Molina Granja, "The preservation of digital evidence and its admissibility in the court," *International Journal of Electronic Security and Digital Forensics*, vol. 9, no. 1, p. 1, 2017.

[22] D. Defreez and J. Mccoy, "The Process of Acquiring Live Systems Grant funding from Southern Oregon University Abstract," pp. 1–7, 2009.

[23] B. Cusack and R. Lutui, "Including network routers in forensic investigation," *Proceedings of the 11th Australian Digital Forensics Conference, ADF 2013*, pp. 59–70, 2014.

[24] A. Goudbeek, K. K. R. Choo, and N. A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 1446–1451, 2018.

[25] M. Hirwani, Y. Pan, B. Stackpole, and D. Johnson, "Forensic Acquisition and Analysis of VMware Virtual Hard Disks," no. July, pp. 255–259, 2012. [Online]. Available: http://scholarworks.rit.edu/other/297

[26] D. C. Prakoso, I. Riadi, and Y. Prayudi, "Detection of Metasploit Attacks Using RAM Forensic on Proprietary Operating Systems," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, no. May, pp. 155–160, 2020.

[27] S. Rahman and M. N. A. Khan, "Review of Live Forensic Analysis Techniques," *International Journal of Hybrid Information Technology*, vol. 8, no. 2, pp. 379–388, 2015.

[28] P. Kaur, A. Bijalwan, R. C. Joshi, and A. Awasthi, "Network forensic process model and framework: An alternative scenario," *Advances in Intelligent Systems and Computing*, vol. 624, no. January, pp. 493–502, 2018.

[29] P. Stephens, *Network forensics*, 2016.

[30] H. S. Dubey and S. K. Papola, "Standard Operating Procedure for Collection of Digital Evidences and Cyber Investigation Techniques," 2019.

[31] L. Y. Yiing and Z. Mahamod, "The Effectiveness of Kahoot on Primary School Pupils' Achievement in Learning Malay Language Vocabulary," *Jurnal Dunia Pendidikan*, vol. 3, no. 1, pp. 90–101, 2021. [Online]. Available: http://myjms.mohe.gov.my/index.php/jdpd/article/view/12559/6279

[32] INTERPOL Global Complex for Innovation, "Global Guidelines for Digital Forensics Laboratories," *INTERPOL Global Complex for Innovation*, no. May, pp. 1–80, 2019. [Online]. Available: https://www.interpol.int/content/download/13501/file/INTERPOL{_}DFL{_}GlobalGuidelinesDigitalForensicsLaboratory.pdf

[33] M. Kolhe and P. Ahirao, "Live Vs Dead Computer Forensic Image Acquisition," *International Journal of Computer Science and Information Technologies*, vol. 8, no. 3, pp. 455–457, 2017.

[34] M. Rafique and M. N. A. Khan, "Exploring Static and Live Digital Forensics: Methods, Practices and Tools," *International Journal of Scientific & Engineering Research*, vol. 4, no. 10, pp. 1048–1056,

2013. [Online]. Available: http://www.ijser.org/researchpaper{%}5CExploring-Static-and-Live-Digital-Forensic-Methods-Practices-and-Tools.pdf

[35] A. Venčkauskas, J. Toldinas, Š. Grigaliūnas, R. Damaševičius, and V. Jusas, "Suitability of the digital forensic tools for investigation of cyber crime in the Internet of Things and Services," *Proceedings of The 3rd International Virtual Research Conference In Technical Disciplines*, vol. 3, pp. 86–97, 2015.

[36] R.-M. Ştefan, "A Comparison of Data Classification Methods," *Procedia Economics and Finance*, vol. 3, no. 12, pp. 420–425, 2012.

[37] D. Quick and K. K. R. Choo, "Big forensic data reduction: digital forensic images and electronic evidence," *Cluster Computing*, vol. 19, no. 2, pp. 723–740, 2016.

[38] M. I. Cohen, "PyFlag - An advanced network forensic framework," *Digital Investigation*, vol. 5, no. SUPPL., pp. 112–120, 2008.

[39] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 382–390, 2018.

[40] B. M. Ramageri, "Data Mining Techniques and Applications," *Indian Journal of Computer Science and Engineering*, vol. 1, no. 4, pp. 301–305, 2010.

[41] A. Soofi and A. Awan, "Classification Techniques in Machine Learning: Applications and Issues," *Journal of Basic & Applied Sciences*, vol. 13, no. August, pp. 459–465, 2017.

[42] I. L. Lin, Y. S. Yen, and A. Chang, "A study on digital forensics standard operation procedure for wireless cybercrime," *Proceedings - 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011*, pp. 543–548, 2011.

[43] H. Harshita, "Detection and Prevention of ICMP Flood DDOS Attack," *International Journal of New Technology and Research*, vol. 3, no. 3, p. 263333, 2017.

[44] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks," *IEEE Communications Surveys and Tutorials*, vol. 15, no. 4, pp. 2046–2069, 2013.

[45] A. Califano, E. Dincelli, and S. Goel, "Using Features of Cloud Computing to Defend Smart Grid against DDoS Attacks," *10th Annual Symposium on Information Assurance (ASIA15)*, no. June, p. 44, 2015.

[46] V. Timcenko and M. Stojanovic, "Application of Forensic Analysis for Intrusion Detection against DDoS Attacks in Mobile Ad Hoc Networks," *Latest Trends in Information Technology, Wseas LLC*, pp. 301–310, 2012.

[47] A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Ali, F. A. Ghaleb, A. S. Rosman, and N. Marni, "Database forensic investigation process models: A review," *IEEE Access*, vol. 8, pp. 48 477–48 490, 2020.

[48] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *International Journal of Computer Applications*, vol. 180, no. 35, pp. 23–30, 2018.

[49] Y. Mo and B. Sinopoli, "False Data Injection Attacks in Cyber Physical Systems," *First Workshop on Secure Control Systems*, 2010.

[50] L. Xie, Y. Mo, and B. Sinopoli, "False Data Injection Attacks in Electricity Markets," pp. 226–231, 2010.

[51] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," *Proceedings of the IEEE Conference on Decision and Control*, no. January, pp. 5967–5972, 2010.

[52] S. N. Kane, A. Mishra, and A. K. Dutta, "Preface: International Conference on Recent Trends in Physics (ICRTP 2016)," *Journal of Physics: Conference Series*, vol. 755, no. 1, 2016.

Haris Iskandar Bin Mohd Abdullah Haris Iskandar Bin Mohd Abdullah holds Master in Business Administration, Universiti Malaysia Sabah, 2018; and Bachelor Degree in Islamic Finance, Universiti Malaysia Sabah, 2017. He is a research engineer at UNITEN R&D SDN BHD. He wrote an article titled Smart Grid Digital Forensic Investigation Framework in year 2020. His research interests in Cyber Security, Businesses, and Internet of Things.

Ts. Zul-Azri Bin Ibrahim holds Master of Science in Information Technology, Universiti Teknologi MARA, 2009; and Bachelor of Information Technology (Computer Networking), Universiti Utara Malaysia, 2002. He is a lecturer since 2009 and currently a lecturer at Universiti Tenaga Nasional. His research interests in Cyber Security, Advanced Metering Infrastructure, Digital Forensics, and Threat Intelligence.

Dr. Fiza Binti Abdul Rahim holds Doctor of Philosophy, Universiti Teknologi Malaysia, 2016; Master of Computer Science (Information Security), Universiti Teknologi Malaysia, 2009; and Bachelor of Computer Science, Management and Science University (MSU), 2005. She is a lecturer since 2012 and currently a senior lecturer at Universiti Teknologi Malaysia. Her research interests in Cyber Security, Advanced Metering Infrastructure, Cryptography, Digital Forensics, Information Privacy, and Machine Learning Algorithm.

Hafizuddin Bin Shahril Fadzli holds Bachelor's Degree in Computer Science major in Cyber Security, Universiti Tenaga National, 2021, and Diploma in Computer Science, Universiti Tenaga National, 2018. He is a research assistant at UNITEN R&D SDN BHD. He assisted in writing an article titled "Analysis on Digital Evidence for Tracing FDIA on IoT Environment" in the year 2020. His research focuses on Cyber Security, the Internet of Things, and smart grids.

Saiful Amin Bin Sharul Nizam holds Bachelor in Computer Science (Cyber Security), Universiti Tenaga Nasional, 2021; and Diploma in Computer Science, Universiti Tenaga Nasional, 2018. He is a research engineer at UNITEN R&D SDN BHD. He wrote an article titled Analysis on Digital Evidence for Tracing FDIA on IoT Environment in year 2020. His research interests are in Cyber Security, Information Security, and Digital Forensic.

Muhammad Zulhusni Bin Mustaffa holds Bachelor of Science in Computer Science Majoring in Network Computing, Universiti Malaysia Sarawak, 2020. He is a system engineer at AIRSTAR (M) SDN BHD. He is one of the author for an article titled Smart Grid Digital Forensic Investigation Framework in year 2020. His research interests in Cyber Security, Software-Defined Networking, Internet of Things, and Blockchain Technology.