International Journal of Scientific Engineering and Science
Volume 4, Issue 9, pp. 36-40, 2020. ISSN (Online): 2456-7361

Digital Forensic Process in Fraud Investigation: A Case Study on Email Analysis

Wishnu Agung Baroto[1,2], Ardhianto Hari Prasetyo[1]
[1]Directorate General of Taxes
[2]digital-forensic.id

***Abstract*—** *Email as part of a human interaction becomes important because it changes the way people transmit their data and information. However, the use of email can be positive or negative depends on the user. Fraudster may use the advanced technology to helps them conduct fraud. In fraud investigation, an investigator should gather all available evidence to support their task. Investigator should look for direct evidence comprehend investigation. Therefore, email plays a significant part of the investigation because it is a communication between employees or companies. This paper use Design Science Research Methodology to examines digital forensic on email fraud investigation. Using an email body and content, this research performs digital forensic process in an investigation. The result shows that digital forensics help investigator to analyze an email and maintain the integrity of the entire investigation process.*

***Keywords*—** *Email;fraud investigation;digital forensic;autopsy;imager*.

I. INTRODUCTION

Internet and other information technology tools have become a crucial element in people's activities—for example, e-commerce and digital currency can ease human life for commerce, especially during the Covid-19 pandemic. However, the technology has two sides of a coin. First, it provides easiness, but on the other side, it facilitates fraudsters to conduct almost every type of fraud. Financial fraud, asset misappropriation, tax fraud, and data fraud are the most common fraud using ICT. Therefore, fraud examiner or fraud investigator must gather all available and related evidence to fight against the fraudsters. Because information technology produces digital or electronic data, thus investigators should understand and capable of obtaining and analyzing digital data as evidence besides common physical evidence.

Data has moved from static data to dynamic data and from stack to flow. The flow and the dynamic of data also create an exponential data increase and thus creates a new term called Big Data. The term "big data" describes not only related to the amount of digital data produced, but also describes the variety of data, the velocity of data, and the veracity of data, as typical abbreviated as 4V's (Volume, Variety, Velocity, and Veracity). It has recently moved to 5V's by considering Value as the last V. This growth of data is mostly in the form of unstructured data with no structured pre-defined data model or schema. Examples of this data are email messages, audio files, video files, pdf reports, and other digital information.

Email is one of the primary communication tools in this internet era. It is quite common that fraudsters use email to commit fraud or to collaborate with their co-inspirators. Therefore, investigators should not deny an email as one of the pieces of evidence in a fraud investigation. However, as one email may comprise thousands of mail data and contacts, the investigator should utilize tools to process the email's contents. Moreover, the metadata of email also beneficial to be investigated because it can comprehend the investigation, incredibly to search for direct evidence, and to find intention or *mens rea* of the fraudster.

This paper elaborates on the investigation of email using a digital forensic framework. The research examines the process of email investigation by extracting the email, indexing the body of email, and combining digital forensic framework on fraud investigations. The objectives of this research are:

1. As proof of the concept that digital forensic beneficial on fraud investigation.
2. Test a digital forensic tool used to conduct digital forensic analysis.
3. All the processes are forensically sound manner as a requirement of digital evidence in a trial.

II. LITERATURE REVIEW

1. Fraud Investigation
   In an organization, fraud examination is carried out for various objectives as follows[1]: identifying improper conduct, identifying the persons responsible, stopping fraud, sending a message that fraud will not be tolerated, determine the extent of potential losses, facilitate the recovery, prevent future losses, mitigate other consequences, and strengthen internal control.
   The role of fraud examiner in an investigation is mostly divided into four activities: obtaining evidence, reporting, testifying, and assisting in fraud detection and prevention.
   a. Obtaining evidence
      The value of a fraud examination stands on the credibility of the evidence obtained. Evidence of fraud generally takes the form of documents or statements by witnesses; therefore, fraud examiners must know how to obtain documentary evidence and witness statements legally and adequately.
   b. Reporting
      Once the evidence has been obtained and analyzed, and findings have been drawn from it, the fraud examiner must report the results to the designated individuals (e.g., management, the board, or the audit committee). A fraud examination report is a narration

of the fraud examiner's specific activities, findings, and, if appropriate, recommendations.

c. Testifying
Often, fraud examiners are called upon to provide testimony and report their findings at a deposition, trial, or other legal proceedings. When providing testimony, fraud examiners must be truthful. They should also communicate clearly and succinctly.

d. Assisting in fraud detection and prevention
Fraud examiners are not responsible for preventing fraud; such responsibilities belong to management or other appropriate authority. Nevertheless, fraud examiners are expected to actively pursue and recommend appropriate policies and procedures to prevent fraud.

An investigator might utilize digital forensics tools to recover and investigate material discovered in a digital device to support the investigation.

2. Digital Forensic
Digital forensics is a branch of forensic science discipline where scientific principles, methodologies, and techniques are used in the investigation [6]. Data in digital forensic is divided into two categories: the volatile and nonvolatile data. Each of the categories has a different method in managing the digital evidence. Digital forensic usually initialize after an incident occurs. First, the Digital forensic examiner assesses the information system and other preparation, and then acquire or collect and preserve digital evidence.
Moreover, a digital forensic examiner then conducts an examination, analysis, and presentation of the investigation's results and findings. From 1995 until 2011, at least 21 proposed frameworks in digital forensic procedures have been issued by many scholars [4]. However, the most general steps are preparation, identification, collection, preservation, examination, analysis, and presentation [6].
   a. Preparation includes actions to guarantee equipment and personnel are organized.
   b. Identification contains detection of an incident.
   c. The collection covers any evidence acquisition using standardized techniques.
   d. Preservation creates proper evidence collection and the chain of custody.
   e. The examination evaluates digital evidence volumes, protected files, registry analysis.
   f. The analysis examines the content and context of digital evidence, determine relevancy, link, and analysis of the root cause of the incident.
   g. The presentation comprehends the reports for documentation of all processes.

According to the literature, there are four general principles as a useful practice guide for digital evidence [2].
   a. No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
   The first principle is related to data integrity.

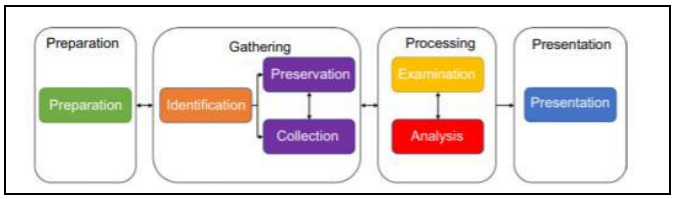

Figure 1: Digital Forensic Framework [6]

   b. In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
   This procedure is associated to the competency of digital forensic investigator.
   c. An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
   The process is related to the audit trail or chain of custody.
   d. The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.
   This process is linked to the responsibility of the investigator.

III. METHODOLOGY

This research utilizes Design Science Research Methodology as a method suggested in Information Science and Computer Science research [3]. The process of DSR are as follows:

1. Identify problem and motivation
Define the research problem and justify the value of a solution. This is the stage to show importance of the research.
2. Define objectives
In addition to general objectives such as feasibility and performance. This includes a specific criterion of a solution.
3. Design & development
Create constructs, models, or methods in which a research contribution is embedded.
4. Demonstration
Prove that the artifact works by solving one or more instances of the problem.
5. Evaluation
Observe and measure the artifact supports a solution to the problem.
6. Communication
Communicate the problem, its solution, and the utility, novelty, and effectiveness of the solution to researchers and other relevant audiences.

International Journal of Scientific Engineering and Science
Volume 4, Issue 9, pp. 36-40, 2020. ISSN (Online): 2456-7361

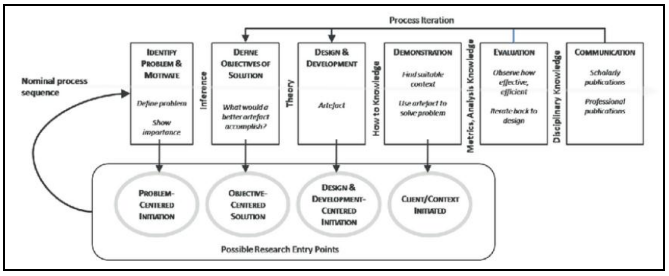

Figure 2: Design Science Research Methodology [5]

IV. Results and Discussion

The process of this research is conducted into six interrelated stages as required by the Design Science Research Methodology: identify problem and motivation, define objectives, design and development, demonstration, evaluation, and communication.

1. Identify problem and motivation.
   The problem of this research is mentioned in the introduction of this paper, which mainly focused on the use of digital forensic to support fraud investigations. This problem arises due to the fast growth of information technology.
2. The objectives are:
   a. As proof of the concept that digital forensic and network analysis beneficial on fraud investigation.
   b. Test the tools for conducting digital forensic.
   c. All the processes are forensically sound manner as a requirement of digital evidence in a trial.
3. Design & development
   This stage is one of the most essential in the whole research process. Based on the literature review, the process of email analysis and network analysis are as follows:
   a. Preparation
      First, the preparation process consists of an analysis whether the fraudster uses email as a means of communication. The manual internet history analysis or use a tool-based analysis can assist investigator to find digital footprints of email in the internet history. In this paper, we utilize the internet history browser as part of DART (Digital Advanced Response Toolkit) to support the process. Therefore, we also prepare some other tools for further process as the following:

Table 1: Tools Used in the Process of Digital Forensic

No.	Tools	Use
1	Outlook 365	To process email from web-based email to client-based email and export the metadata of email.
2	FTK Imager 4.3.1	To create an image file of the backup email file to maintain its integrity.
3	Autopsy 4.15.0	To analyze metadata and content of an email, indexing, and keyword searching.

   b. Gathering
      1) Importation
         This is an additional process in the digital forensic framework to accommodate the network analysis process. This process covers an email client's installation consisting of an email login (username and password) in Outlook, setting the IMAP, and then synchronizing the web-based email and email client in the Send/Receive menu.
      2) Collection
         After all the content of the email synchronize, then find the backup file (.ost or .pst) in the root of the Outlook folder. Generally, it is stored in: C:\Users\$USER$\AppData\Local\Microsoft\Outlook
      3) Preservation
         Using FTK Imager, the process of imaging the evidence and documenting the result of the image.

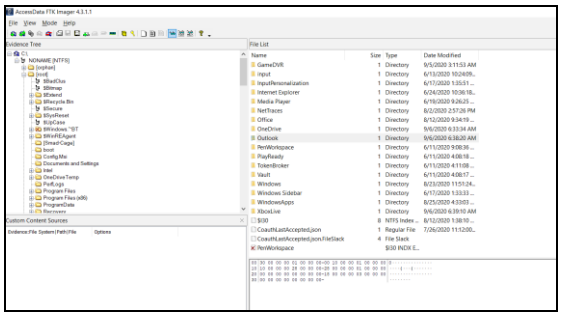
Figure 3: AccessData FTK Imager Process (author)

Furthermore, using Content of Folder feature to image only designated data then image the evidence.

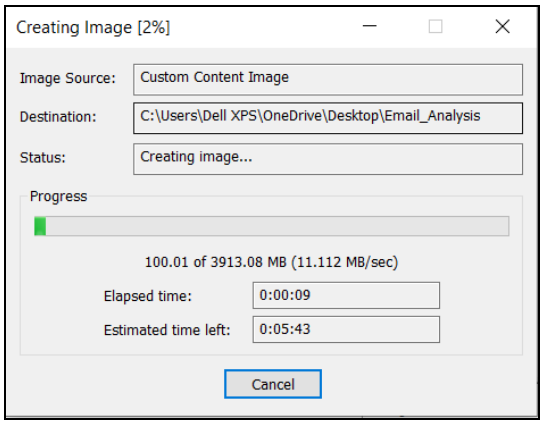

Figure 4: AccessData FTK Imager Process (author)

The result of this process is at least two files: one is the image of the evidence, and the other one is the manifest of the image, which includes the MD5 and SHA1 as a digital fingerprint of the evidence. This digital fingerprint should be documented and maintained as legal evidence in the court or other disputes.

International Journal of Scientific Engineering and Science
Volume 4, Issue 9, pp. 36-40, 2020. ISSN (Online): 2456-7361

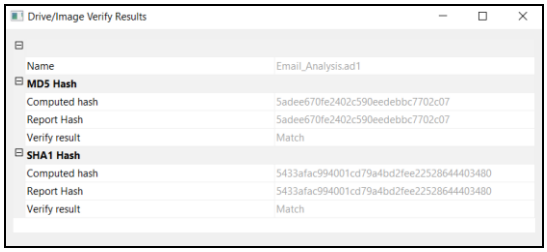

Figure 5: Digital Fingerprint in FTK Imager (author)

c. Processing

The next phase of digital forensic analysis is examining and analyzing the evidence. First, the evidence should be copied, and the investigator works on a copy of the evidence. To support the process, Autopsy Digital Forensic can be used as a tool for processing.

1) Examination

To process the evidence, first, we must create a new case. In this paper, the Suspect Case is the name of the case. Then, the investigator must conduct the following steps:

a) Add the evidence

b) Run ingest module

This is the step to configure several evidence processing. The most common process for email investigation is:

- Email parser
  This module detects and parsers file .mbox and .pst or.ost files and populates email artifacts.
- Keyword search
  Performs file indexing and periodic search using keywords and regular expressions in lists.
- Embedded file extractor
  Extracts embedded files, schedules for ingestion, and populates directory tree.
- File type identification
  Matches file types based on binary signatures.
- Extension Mismatch detector
  Flags files that have a non-standard extension based on their file type.
- Encryption detection
  Detect encrypted files with specified minimum entropy.

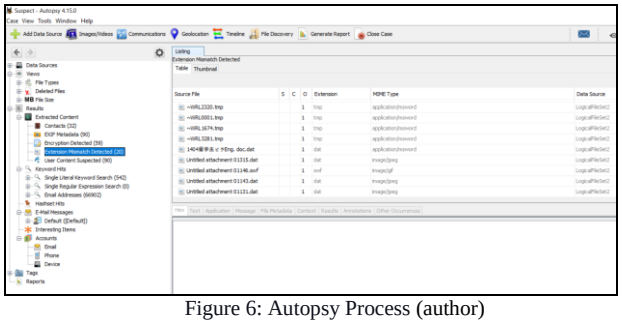
Figure 6: Autopsy Process (author)

d. Analysis

Analyzing the evidence depends on the purpose of the investigation. For example, the most common tax fraud investigation cases are fraudulent tax invoices or usually called as *faktur pajak yang tidak berdasarkan transaksi yang sebenarnya* (tax invoices that are not based on actual transactions). Therefore, a keyword search of "faktur pajak" will be necessary to be performed. The result shows that several hits in the "faktur pajak" word search, which support investigators for further examination.

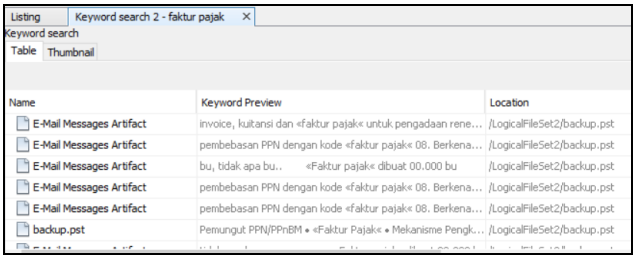

Figure 7: Keyword Search in Autopsy (author)

d. Presentation

The last phase is to present the result, which consists of reporting or creates a standard report of a comprehensive examination. The Autopsy provide a standardized report that can be performed in the reports tab to assist the investigator in creating a report, communicating, or disseminating the investigation results.

7. Demonstration
   All the process above includes a demonstration of the process.
8. Evaluation and Communication
   These parts are reflected in the conclusion and discussion of this paper.

V. CONCLUSION

This research uses the Design Science Research Methodology to determine the process of digital forensic in the email fraud investigation. Based on the research process and demonstration, we can conclude that:

1. Emails become essential as a means of communication.
2. The investigator is able to gather data in emails and maintain the integrity of data.
3. The email body can be extracted for further analysis (keyword search) and more advanced analysis, such as sensitivity analysis.

The digital forensic framework in email investigation should be expanded to network analysis to comprehends the investigation. This is necessary to find a connection between all involved parties in the email communication. For further research, the network analysis should be conducted to support the investigation.

REFERENCES

[1] Association of Certified Examiners, Fraud Examiners Manual, 2019.

[2] Baroto, Wishnu Agung and Darajat, Firman, Digital Forensic Readiness for Micro, Small, and Medium Enterprise in Indonesia, International Journal of Management and Applied Science, 2020
[3] Hevner R., A., Salvator T., Jinsoo Park, & Sudha Ram. (2004). Design Science in Information Science.
[4] Oettinger, William., Learn Computer Forensics, Packt., 2020.
[5] Peffers, Ken, Tuunanen, Tuure, Rothenberger, Marcus A., and Chatterjee, Samir, A Design Science Research Methodology for Information Systems Research, Journal of Management Information Systems, Volume 24 Issue 3, Winter 2007.
[6] Sachowski, Implementing digital forensic readiness from reactive to proactive process, Elsevier, 2016.