International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(3): 294-304
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation

[1]Subektiningsih, [2]Yudi Prayudi, [3]Imam Riadi

[1,] Department of Informatics Engineering, Universitas Amikom, Indonesia

[2]Departement of Informatics Engineering, Universitas Islam Indonesia, Indonesia

[3]Department of Information System, Universitas Ahmad Dahlan, Indonesia

E-mail: [1]neng.bekty@gmail.com, [2]prayudi@uii.ac.id, [3] imam.riadi@is.uad.ac.id

ABSTRACT

Digital forensic investigations must have references and procedures, and so many digital forensic models are developed according to different needs and focus. The average model focuses on the Phases of investigation, but has not yet explained the mechanism of the digital forensic process. This makes the interaction between digital forensic components cannot be exposed, but these components are very complex, i.e. actors, evidence, and processes in digital forensics activities all related to documentation in accordance with the chain of custody rules. The solution offered for this problem is the development of the Digital Forensic Workflow Model (DFWM) using the Business Process Model and Notation (BPMN) approach as a standard notation for describing semantic processes with Design Science Research Methodology. The use of Design Science Research is appropriate because it wants to generate a new artifact, which is an integrated digital forensic workflow model. DFWM makes the digital forensic investigation process more structured and exposes the accuracy of actors who must engage in digital forensic activity in accordance with systematic workflow sequences. DFWM performed system validation process and validation using acceptance questionnaires by law enforcers, Experts, and Digital Forensics Analysts, so DFWM can be applied in real digital forensic practice.

KEYWORDS

Digital Forensic, Investigation Model, workflow model, BPMN, Design Science Research.

1 INTRODUCTION

The general forensic goal proposed by [1] is to gain an understanding of an incident by finding and analyzing the facts related to the incident. Forensic techniques must be adapted to the incidents. As proposed by [2] in analyzing cerebral ransomware can use Network Forensic-Behavioral-Based. While, according to [2] the incompatibility of forensic tools with device technology (for example, mobile technology) is one of the challenges in the investigation. Execute the process of digital forensic investigation is necessary to observe the incidents that occurred, the reasons that caused it, how the incident related to the evidence found, and where evidence was found [3]. According to [4] in [5] states that digital forensics is a scientific method to support the process of identification, preservation, collection, validation, analysis, interpretation, documentation, presentation of digital evidence. In completing all these processes, the model is needed as a reference. Many researchers have made comparisons of various digital forensic models. One by [6] conducted a survey of the digital forensic investigation phase model by comparing four models, namely Computer Forensic Investigative Process, DFRWS Investigative Model, Abstract Digital Forensics Model, and Integrated Digital Investigation Process.

The digital forensics model has a different focus and phase with a slightly informal and intuitive approach [6]. According to [7] states that any researcher or organization can develop the appropriate digital forensic model. The business model becomes one of the approaches that can be used to develop digital forensic models. The business model is a conceptual form that can be used to illustrate the activities that occur and capture the value in them [8].

The study of centralized digital evidence storage systems ever performed by [9] is known as Digital Evidence Cabinets (DEC). The research was developed into Digital Forensics Business Model by [7] based on mechanisms that occur between people and digital evidence, evidence storage and chain of custody, and frameworks in the form of exploration, analysis, presentation. The use of this business model is chosen because it can explain the interactions that occur between people with various digital forensic processes that occur, but cannot explain the activities

that occur because of the interaction between the components in the business model.

The research in this paper focuses on developing digital forensic workflows. According to the Workflow Management Coalition's Dictionary in [10] states that workflows are the automation of an existing business process in whole or in part, as long as documents, information or tasks have been passed by a participant to other participants for action, based on a set of rules or procedures. Workflow perspective, participants can be people, applications, machines, or other processes or workflow engines.

Digital forensic workflows are complex, therefore workflow modeling is needed to facilitate understanding of interactions, phases, and processes undertaken in digital forensic investigations. Many models and frameworks have been developed by a number of researchers over the years but have not fully translated the processes and interactions that occur in digital forensic investigations. Existing models focus more on efforts to provide guiding steps in conducting forensic activities. Therefore, it is necessary to have another alternative to understand the interaction, phases, and various processes conducted in digital forensic investigation through workflow model approach using science research methodology design by [11].

2 RELATED WORKS

Research on the business model for digital forensics ever performed by [9] offers a chain of custody handling solution based on the business model. Chain of custody in the form of procedures to perform documentation of evidence in accordance with the timeliness in the settlement of cases. The developed model is known as Digital Evidence Cabinets (DEC), which consists of three components, namely digital evidence management, digital evidence bags with tags, and access control. This concept explains that digital evidence is not stored inside the investigator's computer, but is stored in a storage system. Digital evidence is inserted in the "evidence bags" to be kept and maintained by an officer of the evidences of evidence. The officer has the right to open and provide access to the investigator in charge of a case. This is an access control mechanism to maintain the role of individual officers. DEC is expected to maintain and enhance the integrity and credibility of digital evidence. However, in practice the handling of digital evidence is more difficult than physical evidence.

Handling of digital evidence must have the same procedures as handling physical evidence, therefore the DEC is proposed for handling the chain of custody digital evidence. [7] developed DEC into the Digital Forensics Business Model based on the mechanisms that occurred during the investigation process. The model consists of three parts, namely the handling of digital evidence relating to the person or actor, the storage and documentation (chain of custody) for access to digital evidence, and parts for major activities of digital forensics, which are; exploration, analysis, and presentation of findings. There is a connection between people, digital evidence, and the processes that occur. The use of the business model is due to the diverse interpretation of digital forensic activities in the field and the activities of handling digital evidence by considering the interaction of all the objects involved [7].

Research on the next forensic model is an Analytical Crime Scene Procedure Model (ASCPM) by [12]. A proposed analytical procedure for digital forensic investigation at the crime scene and can be used as a general guide for practitioners. This model describes a phase-based procedure for identifying a crime scene. ASCPM consists of managerial activities, crime scene examination, system assurance, evidence search, evidence acquisition, hypothesis and validation, organization of potential evidence, physical management of evidence, system-service restoration, provide chain of custody. From these phases can be seen the focus of ASCPM in the form of crime scene procedure in digital evidence management.

Subsequent research was carried out by [13] who developed the Integrated Digital Forensic Process Model (IDFPM) based on the processes and terminology during forensic investigations generally accepted by the digital forensics community. This model was developed to help investigators follow a uniform approach to digital forensic investigation. Modeling uses sequential logic notation to identify similarities and differences in task sequences when conducting digital forensic investigations. The IDFPM model consists of five processes, namely documentation, preparation, incident, incident response, digital forensic investigation. This model also explains the chain of custody of incidents that then the first responder must be able to secure potential evidence. The final process of this model consists of data collection, data verification, examination, reconstruction of incidents, communicating digital evidence found to interested parties, testing investigation results, re-examination or review sub-process, report presentation, incident, decision, and final is the phase of dissemination or return of evidence to the rightful owner.

This sequential logic method has also been used to build the Integrated Digital Forensic Investigation Framework (IDFIF) by [14]. This model is divided into four main phases, namely pre-process, proactive, reactive, and post-process. pre-process is the beginning phase. Proactive consists of several sub-

phases. The first phase is the proactive collection which is a quick action to collect the evidence at the scene of the case and the second phase is crime scene investigation followed by proactive preservation, proactive analysis, preliminary report, securing the scene, detection of incident. The third phase is reactive, a traditional phase of investigation involving six sub-phases; identification, chain of custody processing, collection and acquisition, preservation, examination, analysis, presentation. The fourth phase is the post-process which is the closing phase of the investigation including; conclusion, reconstruction, and dissemination.

3 BASIC THEORY

3.1 Business Process Model and Notation

The business model describes the architecture of value creation, delivery, and the mechanism of work performed [15]. In the business model also contains business processes that can be determined with BPMN. This Business Process Model and Notation (BPMN) provides graphical notation that can be used to define business processes in Business Process Diagrams. Provides a standard notation easily understood by business users capable of representing complex semantic processes [16]. BPMN first release in 2004 by Business Process Management Institute (BPMI) with the specification that is able to provide notation easily understood by business users. Creating the initial concept of a process as a business analysis, the application of technology from the process, to the ease for the person managing and observing the process [17].

BPMN provides a way to communicate business processes for management personnel, business analytics and developers, making it easy to define and analyze general and personal business processes. This BPMN helps ensure that XML documents (extensible markup language) designed for business process implementation can be visualized with common notation. The BPMN diagram is assembled from a small set of core elements, making it easy for both technical and non-technical observers to understand the processes involved. There are 3 main categories of elements of BPMN, namely; flow objects, connecting objects, swim lanes. Elements of flow objects are denoted by geometric images (circles, rectangles, diamonds). Flow objects show certain incidents and activities. Connecting objects are used to connect between elements of flow objects. These connecting objects can be solid lines, dashed lines, and dashed lines that contain an arrow to indicate the direction of the process. The next element is a swim lanes denoted by a straight line that extends in a rectangle. Swim lanes serves to regulate flow objects in diverse categories that have similar functions [18]. BPMN is designed for modeling business processes and creating end-to-end business processes.

According to [19] Sub-model BPMN used as a modeling form there are 3 types, namely:

1. Orchestration, which consists of three types, namely Private non-executable, Private executable, and Public Process. The Public Process Sub-Model is used to describe interactions to and from participant or processes that occur which can be modeled separately or in a collaborative form to indicate the direction of message flow.
2. Choreography, describes the interaction of a set of exchanges of messages or more consisting of two or more participants.
3. Collaboration, describes the interaction between two or more business entities consisting of two pools or more representing participants. Pools or objects in the collaboration are connected to the message stream to indicate the exchange of messages that occur. Collaboration may contain a combination of pools, processes, or choreography.

Business Process Model and Notation is not intended to build a data model, but to show the flow of messages, data, and associations of activity data artifacts [17].

3.2 Design Science Research

The Design Science Research paradigm (DSR) is a dominant paradigm in IS disciplines [20]. One reason for the dominance of this paradigm is the growing interest in IS research as design research [11]. Design as a research involves the idea of undertaking innovative designs that generate knowledge contributions. The form of such knowledge is constructions, models, methods, and instantiations [21] quoted by [22].

The results of the design research will include additions or extensions to the original theory and methods undertaken during the research, new artifacts; namely product design and process. Design research should contribute knowledge, not just a routine design based on the application of the process. The design study has seven guidelines, namely; design as artifacts, problem relevance, evaluation design, research contributions, research firmness, design as process tracking, and research communications [22]. DSR was used as a paradigm in this study because it wanted to produce a digital forensic workflow model, namely in the form of Design Science Research Methodology by [11].

4 METHODOLOGY

An explanation of the Design Science Research Methodology (DSRM) by [11] shown in figure 1.1.

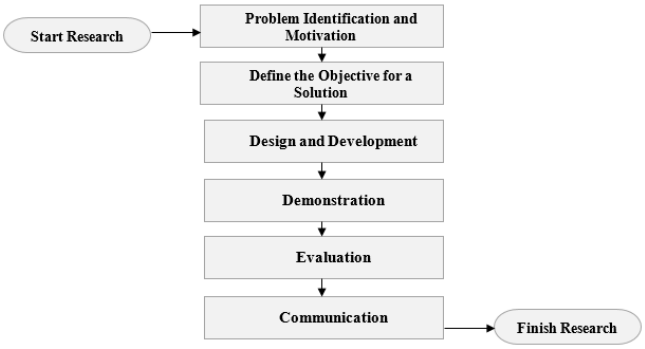

Figure 1. Phases of DSRM

Explanation of Design Science Research Methodology consisting of six stages are as follows:

1. Problem identification and motivation. Identify the problems and reasons to be investigated. This issue should be elaborated in detail in order to determine the correct solution.
2. Define the objective for a solution. Determine the objective to obtain the solution of the problems that have been described in the first stage.
3. Design and development. The third stage is to create new artefacts. These artefacts can be models, methods, or instantiations. Conceptually, a design research artefact can be either designed objects and research contributions embedded in the design. This stage is the determination of the desired artefact functionality and the architecture of the artefact.
4. Demonstration. It is the use of artefacts to solve one or more examples of problems. These stages may be simulations, case studies, or other suitable activities requiring effective knowledge resources in the use of such artefacts.
5. Evaluation. It is the stage of observing and measuring how well these artefacts can support a solution to an existing problem. This activity also compares the solution objectives for actual observations of demonstrations of the use of artefacts.
6. Communication. Communicating usability and novelty, firmness of artefacts, and effectiveness of artefacts generated on relevant researchers and imaginaries to be professionally practiced. This communication can be done with the publication of the research results.

This research uses BPMN (Business Process Model and Notation) approach as its business model and uses Design Science Research Methodology paradigm as the stages of research activity. BPMN is designed for business process modeling [17] that can be tailored to the needs of any agency or organization. The notation used in BPMN resembles a flowchart, but both are different. The use of flowcharts has not been able to explain the mechanisms that occur between each component involved in a process. Use of BPMN can be used to describe the mechanisms and components involved in the workflow or processes that occur. According to [8] the use of BPMN in digital forensic modeling with sub-model orchestration and collaboration can illustrate the interactions that occur from and to the digital forensic process and can explain the relationship of actors with digital forensic activities performed. Using BPMN can also perform element validation and process validation.

The process of modeling and validation of the Digital Forensic Workflow Model with BPMN is done using Bizagi Modeler. The first stage is to create a digital forensic workflow model which is continued by validating the use of notation, data flow or message, and process flow. The next stage performs a process validation which is one of a series of simulations available in Bizagi Modeler. A series of stages in the Bizagi Modeler simulation, among others; process validation, time analysis, resource analysis, calendar analysis. Whereas, in DFWM testing it only uses a process validation phase that aims to ensure the accuracy of the process flow that is modelled. The next test compares DFWM with a practical digital forensic workflow to know how much the similarity or difference is. In general, the limitations and assumptions constructed in this study is a model of this digital forensics workflow covering the stage of investigation and investigation of a case and does not prosecution, judgment, and court.

5 RESULT AND ANALYSIS

5.1 Problem Identification and Motivation

This first stage aims to identify problems in the form of many digital forensic models and frameworks that have been developed by various researchers, but more focused on the guide to carry out forensic activities but have not explained the interactions that occur between the interconnected components, namely; person, evidence obtained, evidence handling, Investigation phase and forensic process undertaken. The process here is a forensic activity undertaken during the investigation phase. The BPMN approach uses the DSRM to describe the interaction in a structured and systematic workflow model.

5.2 Define the Objective for a Solution

The next step is to identify the various related components, i.e. the personnel or actor, evidence, and the phase performed in the digital forensics workflow. The first component identified is the

actor/personnel/human resources associated with digital forensics. The corresponding actors or personnel at each phase of digital forensics is different. Researchers have different perspectives in defining actors or personnel involved in digital forensic processes. The description of the actor/person/ personnel/who runs this digital forensic process is done by [1], [7], [12], [23]. The previous researcher described the identification of the actor to obtain the equation of the actor type that has direct interaction with a process of digital forensics. Representation of the actor to be used to create the DFMW model showed in Table 1.

Table 1. Results of Identification of Actors/Personnel in Digital Forensic Activities.

No.	Actor	Explanation
1.	First Responder	They are responsible for protecting, integrating, and preserving evidence obtained from the scene. This First Responder may be law enforcement, a network administrator, police officer, or even an investigator [24];
2.	Investigators, Digital Investigator, Forensic Investigator	They are in charge of doing an investigation at the scene, Assisting the First Responder, analyzing the evidence obtained. Instead, investigators may also act as first responder or analyst [23] in [9];
3.	Police officer	They are in charge of managing the storage of physical, digital evidence;
4.	Professionals IT	An organization, private company, or person who can perform digital forensic activities. Law enforcement authorities can ask assistance from this private agency if they need it. Can also act as an expert witness.

The next component is evidence. The evidence of digital forensic process consists of electronic evidence (physical evidence) and digital evidence. These two pieces of evidence have different characteristics. Electronic evidence is easier to recognize. Whereas, digital evidence cannot be directly recognized visually. This digital evidence is the result of imaging [25] or extraction of electronic evidence, network capture results or network tracking. In addition, multimedia evidence in the form of images, sounds and videos are part of the digital evidence. Digital evidence is very fragile and can be influenced by many things, one of them is the person or actor involved for digital evidence. This digital evidence will be saved and documented suitable with applicable law and procedure in order to be used in the court as a crime evidence. Handling of digital evidence can use the International Standard Operating Procedure (SOP) from [26], [27]. This SOP contains the basic principles of digital forensics that must be performed by persons/personnel/actors who perform digital forensic processes

The process of documenting and maintaining evidence is the definition of the chain of custody. This process uses forms in the traditional form, i.e. using paper for physical evidence. Meanwhile, for digital evidence using electronic forms. This chain of custody form contains some of pieces' information's such as a name of the investigator, an explanation of the evidence obtained, even the hash value of the evidence [3]. The storage of digital evidence for this DFWM model applies the concept of Digital Evidence Cabinets (DEC) by [11] based on evidence handling the evidence-handling procedure existing in Indonesian jurisdiction, PERKAP No. 10/2010. Model Digital Proof Cabinet (DEC) is able to manage digital evidence using access control. According to [28] access control in DEC can implement appropriate rule policies not only not just applying simple authentication and authorization methods.

The next component is a phase in the digital forensic investigation, an explanation of this general phase of digital forensics was put forward by [2] which consists of four phases, namely Collection, Examination, Analysis, Reporting. The purpose of this digital forensics activity is to transform the media into evidence that can be used to help to solve a case or incident.

5.3 Design and Development

This stage begins by extracting the four digital forensic models developed by [7], [12]–[14] to obtain the phase and process of digital forensic activity that suits the needs of DFWM development. The Digital Forensics Business Model by [6] is the basic model of DFWM development to identify the interactions of various components, people, evidence and processes in digital forensics. Every process of digital forensic model extracted into suitable phases. That phases identified in accordance with the interaction as follow:

1. A↔E, Interaction between person involved in the investigation, namely Actor (A) with existing evidence, named with Evidence (E);
2. E↔D, Interaction between evidence obtained, i.e. Evidence (E) with the handling and recording of evidence, that is Documentation (D);

3. A↔P, Interaction between Actor (A) and the process is done to perform the digital forensic activity, that is Process (P);
4. E↔P, Interaction between Evidence (E) with Process (P);
5. N, mean None, which indicates no interaction between the actor, the evidence, or the process that occurred.

Design and development results in the form of Digital Forensic Workflow Model (DFWM) can be seen in Figure 2.

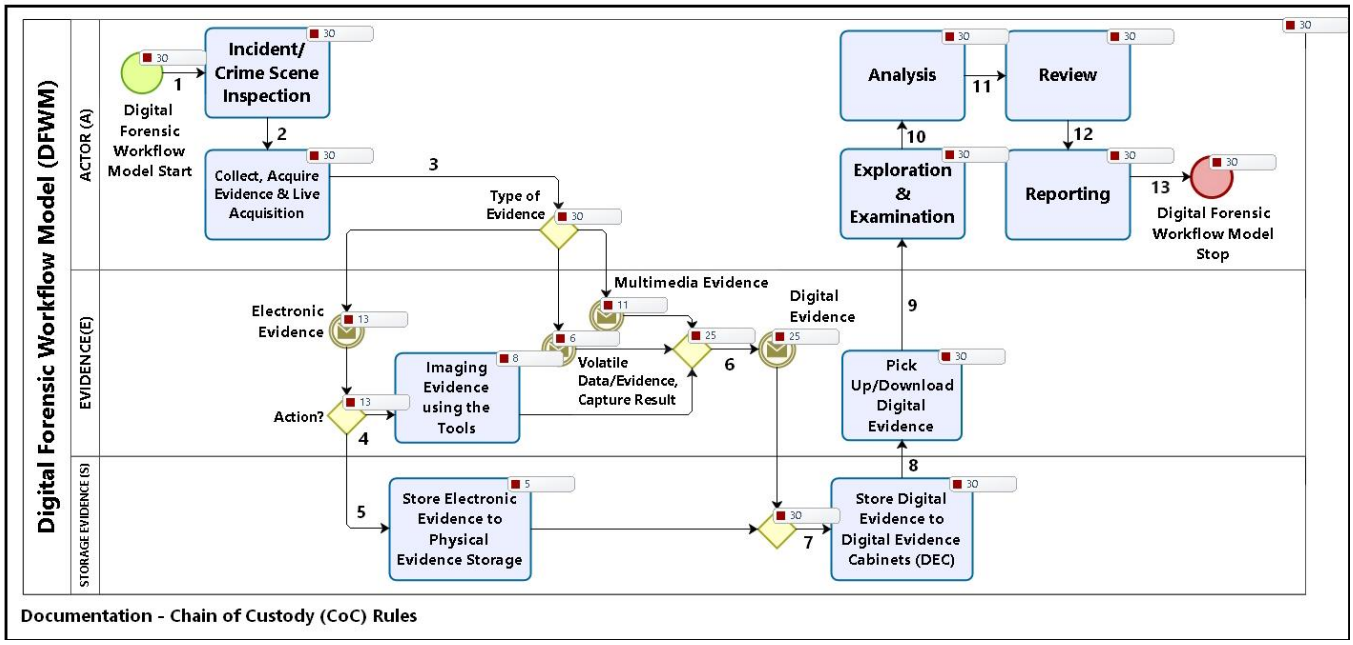

Figure 2. Digital Forensic Workflow Model (DFWM).

Explanation Digital forensics activity based on the workflow modeled in Figure 2 as follows:

1. Conduct a physical investigation of the crime scene after the preparation process for the investigation of case and crimes;
2. Collect potential evidence obtained at the scene and perform a live acquisition if necessary;
3. Categorize evidence obtained into electronic evidence, multimedia evidence, and evidence of results from live acquisition (network capture or volatile data);
4. Imaging for electronic evidence using tools in the form of hardware or software;
5. Storing electronic evidence to the storage of physical evidence that its security and access control is governed by the Physical Evidence Storage Officer;
6. Obtain digital evidence that is the result of imaging of electronic evidence, in the form of multimedia evidence and evidence of the results of network traffic capture or volatile data;
7. Storing digital evidence into DEC with access control by DEC Officers;
8. Digital evidence may be downloaded for the purpose of investigating a case or crime;
9. The actor downloaded digital evidence from DEC to explore and probe potential evidence relating to the event being investigated;
10. The actor analyzes the data obtained for processing into useful information for completion and verification;
11. Review the information obtained or the results of the investigation of the formulated hypothesis. The purpose of this phase is to ensure that the information obtained is relevant to the case
12. The final phase in a series of digital forensics workflows is reporting. This report is manifested in a document containing data, evidence findings, information obtained from a case/crime, and may also contain various other supporting documents. This report document can also be used for future case resolution references. Delivering the findings in court is also included at this phase if necessary;
13. Digital forensic investigation workflow is completed.

Based on the digital forensic activities described in Table 2 and Interactions shown by Actor (A), Evidence (E), and Evidence Storage (S) in Figure 2, the following six phases of the digital investigation process are:

1. Incident/Crime Scene Investigation (W1)

Physical investigation of the crime scene is the first activity in the digital forensics workflow. The investigation is carried out after completing all administrative requirements and preparing the necessary equipment. The physical investigation activity begins by securing and documenting the crime scene and possible evidence. The W1 phase also conducts a survey of the crime scene and conducts interviews. This interview activity is performed by the system administrator, the person at the crime scene, and possible resources. The next activity is to conduct a digital crime scene investigation, for the investigation that cannot be separated between the physical crime scene and digital crime scene, then the investigation can be done simultaneously [12]. In conducting an investigation of the crime scene, a forensic triage process can be done to obtain important information at the scene that can be used to support a digital forensic investigation as a whole [29]. The next activity is to determine the appropriate approach to complete the incident under investigation. The choice of approach is adapted to the incidents occurring or the similarity of cases that have been resolved in the past. Subsequent activities include restrictions on communication against electronic devices in the crime scene which aims to maintain the integrity of evidence and keep evidence in order not to change.

2. Collection and Acquisition (W2)

The W2 phase begins by finding the trigger of the incident and looking for potential evidence at the scene of the case. All potential evidence obtained is identified and collected according to the appropriate category. These categories include electronic evidence, multimedia evidence, and volatile data/network traces from the live acquisition process. A live acquisition is one method of gathering evidence when a suspected computer can be used as electronic evidence cannot be turned off for static acquisition. This direct acquisition process cannot be repeated because the data can continuously increase and change from the operating system factor of the suspected computer. In making this direct acquisition data is possible to change because it is not protected by the write protect [30].

All evidence must be kept authentic by evaluating and maintaining the integrity of the evidence. The next activity is to perform reduction and compression potential to facilitate the examination and analysis phase. All evidence obtained is recorded, labeled, documented and included in the evidence bags. Confiscation of evidence may be made where necessary. All the evidence obtained was transferred to the laboratory for examination and analysis. This activity should be accompanied by a list of inventory of evidence to ensure completeness of the submitted evidence. Electronic evidence obtained should be duplicate or imaging using digital forensic tools to maintain the authenticity of the evidence. Imaging results are performed by using the hashing method to ensure that the imaging result is a representation of the original evidence [13]. The next process is to request the right of access to the officer to store electronic evidence to the place of physical evidence. Imaging results are also stored in DEC, so investigators, analysts, IT professionals/Experts can download digital evidence for review and analysis.

3. Exploration and Examination (W3)

Exploration, examination, and analysis may be performed by the investigator, analyst, or private agency appointed to assist in the investigation. The first process of W3 is to examine the possibility of applying anti-forensics to the evidence obtained. Digital evidence is extracted to scan headers and footers of possible data. The data obtained are then narrowed, grouped and compared to obtain information relevant to the incidents investigated. The last activity of this phase is to prepare the hypothesis of the results of the investigation.

4. Analysis (W4)

The W4 phase begins by linking the findings with people and incidents to find the cause. The findings data were evaluated to confirm the correctness of the hypotheses. The process is continued by interpreting the findings data to prove the incident or the crime to be continued by reconstructing the incident. All findings data obtained are communicated to interested parties or related parties.

5. Review (W5)

The W5 phase begins with a review of the hypotheses and findings data obtained for improvement and addition of information. Subsequent activities in the form of reporting phase based on incidents, data findings, and hypotheses that have been tested.

6. Reporting (W6)

The W6 phase is to summarize the findings during the investigation to obtain information useful in case settlement. The next process is to process a report document. The report should be accompanied by a description of the incident, evidence obtained, findings data, relevant information, and various supporting documents in the investigation. The report document is made in triplicate. Two report documents for the prosecutor's office and one report document to be archived. Archiving aims as a future reference source for solving similar cases. Presentation of the findings in the trial conducted by the Expert is also included in phase W6.

5.4 Demonstration

The demonstration stage is done to see how valid DFWM is generated. This stage consists of two steps, namely to validate the BPMN elements used to build DFWM and validate the process to see the effectiveness of the process in digital forensic activities. Both ways are done using Bizagi Modeler tools, the same tools to build DFWM. This BPMN element validation aims to ensure accuracy in the use of elements according to BPMN rules. Error using elements will result in no process validation. Therefore, it is necessary to change the appropriate elements. In DFWM this is done validation of elements that can be known from the notification system validation element Bizagi Modeler in the form of "diagrams validated without error, warning or information messages". Therefore, the next demonstration step is to validate the DFWM process.

Validation of the DFWM process begins by determining the number of repetition scenarios for the process of forensic activity performed. The value of process repetition suggested by [31] is 30 repetitions. It aims to ensure that the process is repeated stable. In addition to determining the number of repetitions, it should also specify the probability scenario of the existing process flow branches, namely the "type of evidence" and "action?" Sections in the resulting DFWM artifact. Next, run the process validation system from Bizagi Modeler. The result of demonstration process or system testing from DFWM is successful, this can be seen in Figure 2 which shows the value of the validation process. This is indicated by the “start” input value and the DFWM "end" output value shows the same process repetition value, which is 30. This means that all processes are systematically and structured. Because if there is an error in the flow of the process, it will cause one of the processes performed cannot be resolved or experiencing recurrence constantly. This will make the output values and input values unbalanced or equal.

The success of the process validation is also shown in each activity value that is present in the DFWM. The first digital forensic investigation activity of "Incident/Crime Scene Inspection" also shows a value of 30, corresponding to the input value of the process repetition. The same values are also shown for the second activity, "Collect, Acquire Evidence & Live Acquisition". Meanwhile, in the "Type of Evidence" experienced a breakdown of values because there is a branching process performed. The input value for the process return of Type of Evidence is 30, then the value is splitting into three parts according to the specified probability value, i.e. multimedia evidence of 33%, electronic evidence 34%, and volatile data/evidence, capture Result by 33%. Thus, the value of the process return for "Multimedia Evidence" is 11, the value for "Electronic Evidence" is 13, and the value for "Volatile Data/Evidence, Capture Result" is 6. The value of these three types of pieces of evidence if summed will result in the same value of the Type of Evidence value, 30 (11 + 13 + 6).

The electronic evidence value section will also be splitting for two different activities, namely "Imaging Evidence using the Tools" of 8 and the "Store Electronic Evidence to Physical Evidence Storage" activity of 5. Both of these values are summed to be equal to the value of Electronic Evidence of 12 (8 + 5). Furthermore, the value portion of the Imaging Evidence using the Tools activity, the evidence type of Multimedia Evidence, and Volatile Data/Evidence, Capture Result will be passed to the value of input for "Digital Evidence", which is 25 (8 + 11 + 6). The value of process return from Digital Evidence and Store Electronic Evidence to Physical Evidence Storage activities will be continued as an input value for "Store Digital Evidence to Digital Evidence Cabinets" activity, which is 30 (25 + 5). This value will continue as the value of the process repetition input for "Pick Up/Download Digital Evidence". The next digital forensic workflow is a "Exploration and Examination" activity, followed by "Analysis", then "Review", to get to the "Reporting" with a process repetition value of 30. This value of 30 becomes the input and output value of the process loop for each activity. Until finally the digital forensics workflow is finished with a value of 30 as well.

The successful testing of this DFWM process will be evaluated by submitting questionnaires to law enforcement and IT/Expert/Digital Forensic Analyst professionals on DFWM implementation to the practice of digital forensic activities for cases or incident that have been completed. List of questions asked include:

1. Does DFWM comply with the workforce of digital forensic investigation that is practiced or according to work experience that has been done by Respondents?
2. Does DFWM fit into the digital forensic investigation workflow that should be done to deal with the real case?
3. Is there a phase in DFWM that is not in actual digital forensic investigation practice?
4. Is DFWM eligible to be applied for digital forensic investigation in actual practice?
5. Will the respondents apply DFWM as a reference for digital forensic investigation?
6. Provide a DFWM conformity rating with a digital forensic investigation workflow in actual practice?

Question in form of acceptance questionnaire. Respondents provide answers in the form of "Agree" or "Disagree" with the appropriate reasons included.

5.5 Evaluation

The next step is an evaluation that aims to measure how well DFWM can support solutions to related problems, i.e. to translate the processes undertaken in digital forensic investigations into a more structured way by considering personnel performing forensic activities, workflow sequences, and the handling of evidence and crime scenes. This stage is done by filing a DFWM acceptance questionnaire to six respondents consisting of three Police Officers, one Prosecutor's Office Personnel, and two Professional IT/Experts/Digital Forensic Analyst. The selection of respondents is based on expertise and professions directly related to digital forensic practice. The purpose of the filing of this admissions questionnaire is to determine the degree of conformity of DFWM with digital forensic practice. The six respondents gave different results. For the results of the questionnaire is in Figure 3.

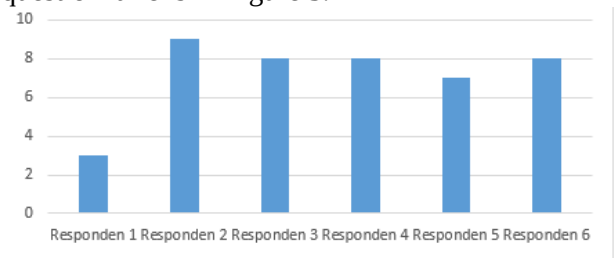

Figure 3. The value of the suitability DFWM

The average value of the six respondents' assessment of DFWM conformity with the practice of digital forensic workflow in case or incident inquiry based on the acceptance questionnaire is 7. 2. This indicates that DFWM is in conformity with the practice of digital forensic activities and DFWM is reasonably feasible to apply as a workflow guide. According to the results of the acceptance questionnaire, the DFWM compliance level with this digital forensic practice is influenced by the condition of the organization or agency, the readiness of human resources, infrastructure, forensic equipment, the type of incidents or cases handled, and the crime scene conditions.

5.6 Communication

This phase of DSRM ends with publication of research results to the International Journal of Cyber-Security and Digital Forensic (IJCSDF) to be communicated to readers, professionals in digital forensics, and researchers to update artefacts, the Digital Forensic Workflow Model (DFWM).

6 DISCUSSION

Based on the results of the workflow model in Figure 2 and a brief description of the explanation of digital forensic activity in Table 2 above the Digital Forensic Design Workforce Development (DFWM) uses the Design Research paradigm with the Business Process Model and Notation (BPMN) approach. The Design Science Research paradigm was chosen because the research was more solution-oriented rather than problem-oriented [32]. Digital forensic models developed by many researchers are more focused on the phases that need to be done in carrying out forensic activities. However, DFWM seeks to explain the processes that occur from each phase of digital forensics and its association with the various components involved in the forensic activity. In any digital forensic investigation, it will involve components in the form of actors/personnel/human resources performing activities, crime scene handling, and management of evidence obtained. Thus, DFWM can be used to explain the interconnections and interactions that occur between these components. In addition, Design Science Research is an appropriate discipline to produce artifacts, which can be either model, method, or instantiation [11]. Furthermore, [11] develops Design Science Research Methodology (DSRM) as a research framework or procedure based on the principles of Design Science Research. Therefore, selected DSRM to produce Digital Forensic Workflow Model. This DFWM is a model that explains a structured and systematic forensic digital workflow with a business model approach. In addition, DSRM provides emphasis on the creation and improvement of artifacts, evaluation, and solutions to a problem [32]. Thus, the creation of DFWM is not just a concept but can be evaluated and offer solutions.

The DSRM provides sequential steps to develop DFWM, so that appropriate extraction of digital forensic activity can be obtained based on identified problems and solutions. When forensic activity is successfully deployed, DSRM provides guidance for the basic design and development of new artifacts of the DFWM. In fact, DSRM provides a very flexible advantage in running the demonstration phase. This demonstration stage, in addition to simulations, case studies, and evidence, can also be done with other customized activities [11]. It is a little difficult to demonstrate from a workflow model that explains digital forensics activities. Therefore, demonstration steps using system testing using Bizagi Modeler software or tools. Because demonstrations can be tangible resources of effective knowledge about the use of artefacts [11]. DSRM also presents an evaluation phase to measure how well DFWM can be applied to support the solution of multiple frameworks or digital forensic forecasting models. Updates from DFWM are made easier with the communication offered by DSRM. However, DSRM may contain unnecessary elements in some design

contexts in practice or even too general to support the design of a person [11].

Digital Forensic Workflow Model that is produced using DSRM is expected to support Standard Operational Procedure (SOP) of an organization in conducting an investigation of incidents or cases related to computer crime, cyber-crime, and computer related crime. This is because DFWM provides a structured digital forensic investigation model that explains the needs of required personnel/actors/human resources, the various types of evidence, the handling and recording of evidence, how to handle crime scenes, and the process of any forensic activity that must be done systematically. DFWM can describe the interactions that occur between each of the related components, so the need to be met in digital forensic investigation becomes clearer and easier to understand. The convenience can make the settlement of a case or an incident more effective because the links between people, evidence, and processes become clearer. Thus, DFWM presents not only the process of forensic activity but also the critical personnel and management needs of evidence. Because the evidence must be kept authenticity, validity, chain of custody [33]. The evidence must also meet the five main characteristics, namely Admissible, Authentic, Complete, Reliable, Believable [34]. Because the evidence must be maintained for integrity to ensure that the information contained therein does not change from the first discovered, to the forensic process, to use in the court [35]. It is expected that DFWM can serve as an integrated workflow guide as it explains the interactions between actors conducting forensic activities, possible evidences, and digital evidence cabinets as well as physical evidence by following the chain of custody and documenting rules.

DFWM can be applied in organizations, companies, and private agencies as a workflow guide in conducting digital investigations. This is evidenced by three respondents out of a total of six respondents willing to implement DFWM in their institutions or organizations. Two respondents are willing to implement DFWM as a guide for digital forensic investigation workflow that is firstly tailored to the internal administration and applicable SOPs. DFWM has successfully accommodated aspects of digital forensics required. Furthermore, one respondent is willing to make DFWM as the basic reference for SOP Digital Forensic Analysis Team (DFAT) for handling chain of custody. For further verification should DFWM be applied to solve cases or incidents directly. Because in Design Science Research a design and evidence of the usefulness of the artifact is the main component [11].

7 CONCLUSION AND FUTURE WORKS

The choice of DSRM is precisely, because it produces a solution of a problem in the form of a new artifact, the Digital Forensic Workflow Model (DFWM) that can explain the complexity of components present in the forensic digital investigation phase, in the form of evidence, evidence storage, chain of custody, and process forensic activity in a structured and systematic way. Through DFWM can be known accuracy in the placement of appropriate personnel/actors in conducting digital forensic workflow in the order of processes to be done, thereby increasing the effectiveness in the settlement of cases or events. The interaction of these components in digital forensics can be understood easily because DFWM is developed using the BPMN approach which is also tested.

The first test of the system using Bizagi Modeler which aims to ensure that the flow of processes operate in accordance with BPMN rules. The second test uses a model acceptance questionnaire that aims to determine the degree of conformity of DFWM with the practice of digital forensic investigation by private agencies, organizations or agencies. The results of the questionnaire stated that DFWM as a whole can be applied in the practice of digital forensic investigation because it got a pretty good average score of six respondents. However, in the application of DFWM is influenced by two main factors, namely the condition of the organization and the condition of the case. Organizational conditions are influenced by the availability of human resources, laboratory infrastructure, and the availability of forensic tools. Meanwhile, case condition is influenced by case specification, crime scene condition, sequence of investigation process done. DFWM is expected to be a solution for enhancing the more structured and integrated forensic investigation process within the organization by making adjustments to the internal SOP of the organization.

The contributions of this DFWM can serve as a guide for activities within the digital inquiry workflow. The use of BPMN's approach also proves that the business model can not only explain the business processes of an enterprise, but can also be used to explain the process of digital inquiry with related components. DFWM in future research can be developed with workflow schemes when law enforcement agencies or institutions want external help. Because in DFWM law enforcement agencies, institutions, and private agencies (external parties) are assumed to be in the same condition, that is, the part of the Actor/Personnel. It would be better if the condition is divided into Internal Actor and External Actor.

REFERENCES

[1] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to integrating forensic techniques into incident response," *NIST Spec. Publ.*, no. August, pp. 800–886, 2006.

[2] A. Kurniawan and I. Riadi, "Detection and Analysis Cerber Ransomware Using Network Forensics Behavior Based," *Int. J. Netw. Secur.*, vol. 20, no. 5, pp. 1–8, 2018.

[3] I. Riadi, J. Eko Istiyanto, and A. Ashari, "Log Analysis Techniques using Clustering in Network Forensics," *IJCSIS) Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 7, 2012.

[4] G. Shrivastava, K. Sharma, and and A. Dwivedi, "Forensic Computing Models: Technical Overview," *ISI Thompson Conf.*, 2012.

[5] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," *J. Adv. Comput. Networks*, vol. 3, no. 1, pp. 82–86, 2015.

[6] P. S. Patil and P. A. S. Kapse, "Survey on Different Phases of Digital Forensics Investigation Models," pp. 1529–1534, 2015.

[7] Y. Prayudi, A. Ashari, and T. K. Priyambodo, "A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia," *I.J. Comput. Netw. Inf. Secur.*, vol. 11, no. October, pp. 1–8, 2015.

[8] Subektiningsih and Y. Prayudi, "BPMN Implementation to Build Digital Forensics Business Model," in *SENTIKA*, 2017, pp. 289–298.

[9] Y. Prayudi and A. Ashari, "Digital Evidence Cabinets : A Proposed Framework for Handling Digital Chain of Custody," vol. 107, no. 9, pp. 30–36, 2014.

[10] R. Broer Bahaweres, V. A, and Wahyudianto, "Development of Workflow System Document Submission Procedure Proposal Procedure With Alfresco Enterprise Content Management (ECM), Case Study: Informatics Engineering Program UIN Jakarta," *Semin. Nas. Teknol. Inf. Komun. Terap.*, vol. 2012, no. Semantik, pp. 356–363, 2012.

[11] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," *J. Manag. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, 2008.

[12] H. Ibrahim, H. G. Yavuzcan, and M. Ozel, "Digital forensics : An Analytical Crime Scene Procedure Model (ACSPM)," *Forensic Sci. Int.*, vol. 233, no. 1–3, pp. 244–256, 2013.

[13] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Comput. Secur.*, vol. 38, pp. 103–115, 2013.

[14] Y. D. Rahayu and Y. Prayudi, "Building Integrated Digital Forensics Investigation Frameworks (IDFIF) Using the Sequential Logic Method," *Semin. Nas. SENTIKA*, vol. 2014, no. Sentika, 2014.

[15] D. J. Teece, "Business models, business strategy and innovation," *Long Range Plann.*, vol. 43, no. 2–3, pp. 172–194, 2010.

[16] Object Management Group, "Business Process Model and Notation," 2016. [Online]. Available: www.omg.org/bpmn. [Accessed: 30-May-2017].

[17] M. Von Rosing, S. White, F. Cummins, and H. De Man, *Business Process Model and Notation-BPMN*. Elsevier Inc., 2015.

[18] Bizagi, "BPMN by Example-Bizagi Suite," *resouces.bizagi.com*. p. 25, 2014.

[19] M. Von Rosing, H. Von Scheel, and A. W. Scheer, *The Complete Business Process Handbook: Body of Knowledge from Process Modeling to BPM*, vol. 1. 2014.

[20] S. Gregor and A. R. Hevner, "Positioning and presenting design science research for maximum impact," *MIS Q.*, vol. 37, no. 2, pp. 337–355, 2013.

[21] S. T. March and G. F. Smith, "Design and natural science research on information technology," vol. 15, pp. 251–266, 1995.

[22] P. Antonelli, R. Mathew, A. Hevner, S. Chatterjee, and I. Series, "Design Science Research in Information Systems," pp. 9–23, 2010.

[23] J. Ćosić and Z. Ćosić, "Chain of Custody and Life Cycle of Digital Evidence," *Comput. Technol. Appl.*, vol. 3, no. 2012, pp. 126–129, 2012.

[24] Ec-Council, "Module 05 First Responder Procedures." 2012.

[25] P. Kepala, P. Laboratorium, B. Reserse, and K. Polri, *Standar Operasional Prosedur Pemeriksaan dan Analisa Digital Forensik*. Indonesia, 2014, p. 132.

[26] Williams Janet, "ACPO Good Practice Guide for Digital Evidence," *Ref. Mater. [Internet]*, no. March, pp. 1–43, 2012.

[27] D. J. Daniels and S. V Hart, "Forensic Examination of Digital Evidence : A Guide for Law Enforcement," *U.S. Dep. Justice Off. Justice Programs Natl. Inst. Justice Spec.*, vol. 44, no. 2, pp. 634–111, 2004.

[28] M. F. Panende, Y. Prayudi, and I.Riadi, "Comparison of Attribute Based Access Control (ABAC) Model and Rule Based Access (RBAC) to Digital Evidence Storage (DES)," *Int. J. Cyber-Security Digit. Forensics*, vol. 7, no. 3, pp. 275-282, 2018.

[29] A. Iswardani and I. Riadi, "Denial of service log analysis using density k-means method," *J. Theor. Appl. Inf. Technol.*, vol. 83, no. 2, p. 2, 2016.

[30] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*, 5th ed. Boston, Massachusetts, United States: Cengage Learning, 2014.

[31] Bizagi, "Process Validation," 2017. [Online]. Available: http://help.bizagi.com/process-modeler/en/index.html?system_requirements.htm. [Accessed: 01-Jan-2017].

[32] P. R. Lutui, "Digital Forensic Process Model for Mobile Business Devices : Smart Technologies," Auckland University of Technology, 2015.

[33] J. Sammons, "Digital Forensics," *Introd. to Inf. Secur.*, pp. 275–302, 2014.

[34] J. Richter, N. Kuntze, and C. Rudolph, "Securing digital evidence," *5th Int. Work. Syst. Approaches to Digit. Forensic Eng. SADFE 2010*, no. September, pp. 119–130, 2010.

[35] Y. Prayudi, A. Luthfi, and A. M. R. Pratama, "Approach of Ontology Model To Represent Body of Knowledge Digital Chain of Custody," *Cybermatika ITB*, vol. 2, no. 2, pp. 36–43, 2014.