ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE EVALUATION OF COMPLIENCE LEVEL OF COMPUTER AND MOBILE FORENSIC WITH ACPO IN HELPING SPECIAL AUDIT DISCLAIM FRAUD

[1]LELYA NOVITA KUSUMAWATI, [2]FERGYANTO E GUNAWAN

[1]BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Information System Management Department, Jakarta, Indonesia

[2]BINUS Graduate Program – Master of Industrial Engineering, Bina Nusantara University, Industrial Engineering Department, Jakarta, Indonesia

E-mail: [1]lelya.kusumawati001@binus.ac.id, [2]fgunawan@binus.edu

ABSTRACT

The threat on information system security in public service companies is a dangerous thing that often occur. For example, the electricity company in Indonesia, PT PLN, sees the high threat especially is fraud that involving information systems. The company, from 2015 to 2018, found many cases of fraud using information systems. PT PLN established an audit team to collect fraud's digital evidence by implementing computer and mobile forensic that referring to the guidelines of the Association of Chief Police Officers (ACPO). The purpose of this study is to measure the comlience level of the audits that have been carried out with the ACPO guidelines. Forensic digital examination and analysis procedures must follow and refer to the basic principles or guidelines (guidelines) internationally, such as the Good Practice Guide issued by the Association of Chief Police Officers (ACPO) so that the examination output in the form of digital findings can be accepted as legal evidence at the trial. The study involves 113 digital evidence from the implementation of computers and mobile forensics at PT PLN. Surveys that refer to ACPO are used to measure complience level in handling 113 evidence with ACPO. The results showed that the average of complience has only reached 51%. In more detail, the proportion of evidence (in %) and the level of ACPO's complience (in brackets and in %) are: 37 (57), 21 (48), 20 (52), 19 (43), and 2 (24).

Keywords: *Fraud, Computer Forensic, Mobile Forensic, Association of Chief Police Officer, Digital evidence*

1. INTRODUCTION

Threats to the security of the information systems of public service companies are dangerous things that often occur. For example, PT Perusahaan Listrik Negara (PT PLN) is one of the utility companies in Indonesia, an electricity company. As a large-scale company, PT PLN with a number of permanent employees as many as 50,000 people and the number of temporary employees as many as 60,000 people have a high level of threat to information security systems, including fraud involving information systems. Fraud is constitutes any illegal act in the form of concealment, or misuse of trust. Such actions are not limited to threats or violations in the form of physical strength, but fraud can be carried out by parties and organizations to obtain money, assets or services used to avoid payment or loss of services or to obtain benefits both personally and business [1].

There are frauds that using information systems that have been successfully disclosed by Internal Control Unit (SPI). In 2016, information system security violations were discovered by a former temporary employee in an area in Jakarta which resulted in a loss of Rp2 billion. In addition, in 2017, an employee downloaded confidential data from the SAP application and distributes it using e-mail and whatsapp. Finally, in 2018, there was an alleged manipulation of billing data by an employee.

Based on the cases of crimes that have occurred, PT PLN established an Internal Control Unit (SPI) [2] to supervise business processes and handle fraud cases through the Special Audit section with computer forensic [3] and mobile forensic. SPI also needs to gather evidence, often in digital form, which can be legal evidence that can be used by courts. For this reason, SPI adopts and applies the basic digital forensic principles issued by the Association of Chief Police Officers (ACPO).

Mobile Forensics is the science or expertise in processing and managing digital evidence originating from mobile devices, mobile phones, tablets, and various other types of variants using an accountable method. In principle, mobile forensics has similar methods with existing digital forensics. It can even be said that mobile forensic is a part of digital forensic, only the target of digital evidence usually found on desktop or laptop computers is transferred to cellular telephone devices or mobile devices [4].

Digital forensics can be interpreted as the collection and analysis of data from various computer resources which include computer systems, computer networks, communication lines, and various storage media that are suitable to be submitted in court hearings [5].

Digital evidence are any electronic information that is made, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, which can be seen, displayed and / or heard through a computer or electronic system. Including but not limited in writing, sound, images, maps, designs, photos, letters, signs, numbers, access codes, symbols or perforations that have meaning or can be understood by people who are able to understand it [6].

Digital evidence is valuable evidence and must be treated in the same way as traditional forensic evidence. Methods of handling electronic evidence may seem complicated and expensive but based on existing experience, if handled with the right procedures, digital evidence can provide interesting and efficient evidence

ACPO is a government institution in the field of law enforcement that has clear basic digital forensic principles. ACPO is an association of police chiefs in England, Wales, and Northern Ireland. Over the years, ACPO has developed guidelines for implementing law enforcement such as the 'ACPO Good Practice Guide for Digital Evidence' to guide law enforcement and all who assist in the investigation of cyber security crime incidents and cases.

The principles of Digital Forensic by ACPO [7] are: principle number one, 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. Principles number two, in n 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. Principle number three, 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. Principle number four, the person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to

Rahman & N. A. Khan (2016) stated that computer crime through the Internet is currently increasing and digital forensics has an important role to play in reducing rampant and uncontrolled crime [8]. Forensic investigation is used to find digital evidence using a variety of different tools which are complex and difficult processes. Digital evidence can be in the form of fragment images taken from various storage devices such as history browsing, email and files, can also be found from files that have been deleted. The technique of processing digital evidence has four steps: system preparation, image acquisition, image / snapshot comparison and report generation.

Furthermore, Alanazi, Jones, and Menon (2018) states that in Saudi Arabia a judge can receive digital evidence based on the judge's knowledge level of digital equipment [9]. Digital evidence can be accepted in court as a supporter of recognition and not as strong evidence. Regulations in Saudi Arabia define a computer as any digital device that can be repaired or moved that contains a data processing system, storage, connection between crime and suspect.

The ultimate goal of using digital evidence is to show that there is a crime or not, so it takes several steps to process digital evidence. The first step is confiscating evidence from certain crimes, second by trying to describe the mode of crime related to criminals and victims, the third stage is involving digital forensic experts who understand digital forensic procedures and can use their expertise in connecting suspects to the crime scene, and the last stage is preparing an answer about the crime committed, how it happened, what happened, when and by whom.

In addition to the ACPO standard, digital forensic implementation methods were also proposed by Román, Mora, Vicuña, & Orozco (2016), state the phase of computer forensics implementation: identification, preservation, analysis, and Presentation [10] and Umar, Riadi, and Zamroni, (2018) [11] state the phase of computer forensics implementation: collection, examination, analysis, and reporting. The discussion of the stages, advantages, and disadvantages of each method is given in Table 1.

Table 1. Comparison of Stages, Advantages, and Disadvantages of Digital Forensic Methods

Reference: Román, Mora, Vicuña, and Orozco (2016)	
Methodology	**Advantages/Disadvantages**
Phase of computer forensics implementation: a. Identification b. Preservation c. Analysis d. Presentation	**Advantages:** Provide guidance in implementing computer forensics starting from how to identify digital evidence, how to secure, analysis and provide information on how to handle evidence by investigators to the authorities. Each stage has been explained more detailed in steps that can be applied. **Disadvantages:** There are no planning stages that must be carried out by the investigator before go to the crime scene.
Reference: Umar, Riadi, & Zamroni (2018)	
Methodology	**Advantages/ Disadvantages**
Phase of computer forensics implementation: a. Collection b. Examination c. Analysis d. Reporting	**Advantages:** Provide guidance in implementing computer forensics starting from how to obtaining evidence, examining, analyzing and making reports on how the investigator handles the evidence. **Disadvantages:** There are no planning stages that must be carried out by the investigator before coming to the crime scene and how to provide information about handling evidence by the investigator to the authorities
Reference: ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence (2012)	
Methodology	**Advantages/ Disadvantages**
Phase of computer forensics implementation: a. Handling at crime scene (preparation, preserving, collecting, confirming, identifying) b. Handling in laboratory (administration, investigation, analyzing, recording) c. Handling reports (reports, packaging and sealing, administration of submission of reports) d. Presenting	**Advantages:** Providing guidance in implementing computer forensics starting fro how to handling at the crime scene, handling in the laboratory, handling reports and providing information on how to handle evidence by investigator to authorities. Each stage has been completed with more detailed steps and an explanation of how it should be done, so investigator can follow the steps set by ACPO in handling digital evidence. **Disadvantages:** The stages of handling evidence become more detailed when compared to other methods.

From the explanation in Table 1, the issue regarding handling digital evidence of crime is important. This study aims to measure the complience level between computer and mobile forensic based on ACPO standards and implementation by SPI.

2. METHOD

2.1 The Stages of Implementing Digital Forensic Based on ACPO

The analysis phase will be compared ACPO standards with the results of data obtained from the research methods, so we can measure the digital forensic implementation with ACPO standards.

The stages of implementing digital forensic based on ACPO are handling at crime scene, handling at labolatory, handling reports and presenting .

Handling at crime scene consists of five stages, the first stage is preparation (investigator must prepare a warrant, camera digital, stationery, label and triage tools that will used if digital evidence is found on/live at the scene). The seconds stage is preserving that contains activities to maintain and secure data by investigators to ensure that the evidence collected does not change. The third stage is collecting. It is an activity to collect data that is relevant to the investigation process in order to find evidence in accordance with the case. The fourth stage is confirming. It is an activity to determine data relating to the case being handled. The last stage is identifying, it is an activity to recognize data and ensure that the data found is original data in accordance with the crime scene, investigators have to checking digital evidence signature using hashing technique.

Handling at labolatory consists of four stages. The first stage is administration. At this stage digital evidence brought from the crime scene is received by the administrative registrar. Data must be recorded including the name of the institution / unit who sending digital evidence, sender's identity, date, number of items, technical specifications such as brand, type, serial number, International Mobile Equipment Identity (IMEI) etc. Checking digital signature of digital evidence received to ensure the evidence received is in accordance with what was taken at the crime scene. The second stage is investigation. Image files from digital evidence are examined using trusted digital forensic software to get a complete picture of the case being handled. The third stage is analyzing. At this stage, the data that have been obtained at the investigation stage will be examined in more detail and comprehensively using forensic analysis software to prove what crime is committed and to analyze whether there is a connection between the suspect and the crime. The last stage is recording data from the results that have been found at the analysis stage so data can be ensured of authenticity and can be reconstructed if needed.

Handling reports consists of four stages. The first stage is report, after obtaining digital evidence from the process of examining analysis data in accordance with the rules of investigation, then the digital evidence data is entered into the report, the report format can be made by provisions of the institution. The second stages is packaging and sealing. After the evidence has been analyzed, the evidence must be wrapped and sealed to be returned to the institution / unit that sent the evidence. The last stage is report submission administration. The reports of the results of inspection of evidence by forensics are returned to the institution / unit that sent the evidence.

In the presenting stage, if needed, digital forensic investigators will provide information to the authorities or the court in accordance with their expertise in conducting forensics on digital evidence so founded data can be used to assist the investigation process to find the suspect.

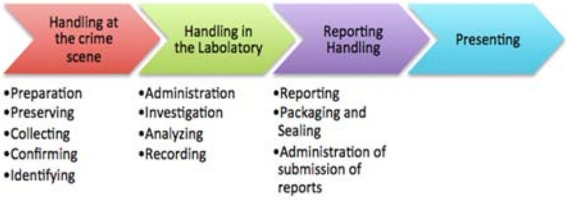

Figure 1. The Stages of Digital Forensic Implementation

2.2 Data Population

The data used in this study are digital forensic evidence collected by SPI during 2015-2018. In that period, there were six cases with a total of 113 evidences consist of 60 in the form of computers and 53 in the form of mobile phones. More detailed information about the evidence used is shown in Table 2.

Complience level of handling digital evidence with ACPO standards is evaluated using the questionnaire shown in Table 3. The study is carried out for all handling processes from the initial preparation stage at the crime scene, then handling procedures in the laboratory, to the procedure for handling reports.

Table 2. List of crime cases, locations of the incidents, and the number and form of digital evidence collected by SPI during 2015-2018

Year	Crime Cases	Location	Number of evidence	
			Computer	HP
2015	Manipulation of procurement (goods and services).	Batam	2	0
2016	Transaction engineering in the Customer Relationship Management (CRM) application.	Unit AP Jakarta	15	0
		Unit Jakarta	8	0
2017	Distribution of corporate secret data.	Purwakarta	3	3
		Sumbawa	3	3
		Lhoksumawe	2	2
		Palu	3	3
		Bandung	4	4
		Banten, Garut	5	5
		Lampung	3	3
		Medan	3	3
		Jogja	2	2
2018	Data billing manipulation	Semarang	3	3
	Manipulation of procurement (goods and services).	South Sumatera	4	4
	Wistle blower	Belawan, Medan	0	18
Total			60	53

Table 3. The List of questions to measure the complience level of handling evidence with ACPO standard

No	Statement	Do	
		Yes	No
Procedure of handling at crime scene			
Preparation			
1	The assignment letter has been completed with a statement that it may carry out searches and confiscation of evidence.		
2	Investigator prepares a digital camera to document the crime scene.		
3	Investigator prepares writing equipment to record technical specifications of the computer and information from witnesses.		
4	Investigator prepares measuring scales, labels used to mark electronic evidence that found at the crime scene.		
5	Investigator prepares the receipt form for evidence.		
6	Investigator prepares triage tools.		
7	Preserving		
8	Collecting		
9	Confirming		
10	Identifying		
Procedure of handling at labolatory			
Administration			
11	The labolatory's staff records the name of the agency / unit that sending digital evidence.		

12	The labolatory's staff records complete identity of digital evidence sender.		
13	The labolatory's staff records the date of receipt.		
14	The labolatory's staff records the amount of digital evidence received, technical specifications such as brand, type, serial number, IMEI etc.		
15	The labolatory's staff checking digital signatures of digital evidence.		
16	Investigation		
17	Analyzing		
18	Recording		
Procedure of handling reports			
19	Report		
20	Packaging and sealing		
21	Administration of submission of reports		

In addition, this observation is also done by collecting related documents. The examples of these documents can be in the form of policy documents, system documentation, and documentation relating to the application of computers and mobile forensics, so that information is obtained about the current implementation of the company.

Interview is performed with SPI Management as stakeholders of the application of computers and mobile forensic in disclosure of fraud to find out policies, and current achievements and expectations for development. In addition, interviews are conducted with implementers, facilities and infrastructure to implementation current implementation of computers and mobile forensic.

3. RESULT AND DISCUSSION

3.1. Current Computer Forensic And Mobile Implementtaion Identification

Identification of current computer and mobile forensic implementation is carried out by observation. The stages of this observation are conducted to find out directly the implementation of an activity in the company, especially how implementtaion of computers and mobile forensics. Observations were made as long as the author handled the implementation of computers and mobile forensics, for approximately two years.

The computer and mobile forensic implementation begins with the issuance of a special audit assignment letter and the investigation team will prepare triage tools that will be used to acquire evidence and analysis at the crime scene. After tool preparation is complete, the team will immediately go to the location or scene where digital evidence is exist and ends with making special audit report.

The current computer and mobile forensic implementation can be described Figure 2.

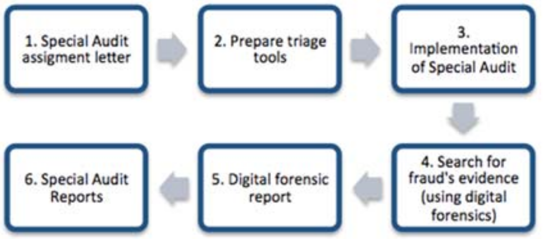
1. Special Audit assigment letter
2. Prepare triage tools
3. Implementation of Special Audit
4. Search for fraud's evidence (using digital forensics)
5. Digital forensic report
6. Special Audit Reports

Figure 2. Current Computer and Mobile Forensic Implementation

The first stage of implementation of computer and mobile forensic is the issuance of a special audit assignment letter. Forensic investigators are members of the Special Audit Team, and are responsible for acquiring and analyzing digital evidence. The second stage is the forensic investigators prepare triage tools, showed in Table 4.

Table 4. Triage Tools

No	Tool
1.	Laptop for forensic, contains software for acquisition and analysis (EnCase, Oxygen and Cellebrite)
2.	Tableu TD3 / TX1
3.	Screwdriver set toolkit
4.	Cellebrite cablekit
5.	The Letter of Borrowing Evidence
6.	Hardisk storage
7.	External Hardisk
8.	Stationery
9.	Dongle Encase

10.	Dongle Cellebrite
11.	Dongle Oxygen
12.	Camera UFED is use to open the lock password on the cellphone.
13.	Tableu bag

Considering that PT PLN does not have a forensic laboratory, the acquisition of evidence must be done directly at the scene. The third stage is implementation of a special audit to the crime scene, the investigator team together with special audit team members come to the scene and bring the triage tools. The fourth stage is search for fraud's evidence. Forensic investigators borrow a HP or laptop or PC that used by suspected, and then forensic investigators carry out computer and mobile forensic directly at the scene using triage tools that have been prepared. Forensic investigators acquisition digital evidence using Tableu TD3 (Figure 3) or Table TX 1 (Figure 4) to make image file

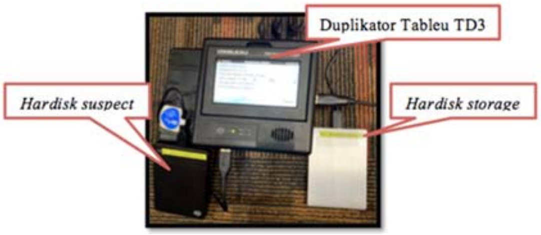

Figure 3. Acqusition digital Evidence Using Tableu TD3

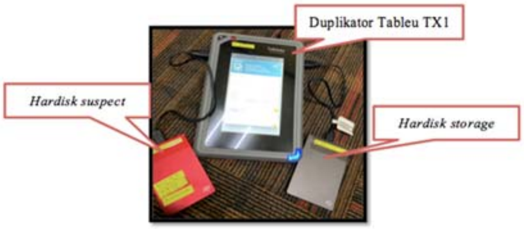

Figure 4. Acqusition digital Evidence Using Tableu TX1

After data acquisition is completed, forensic investigators conduct data analysis that has been obtained and search for fraud's evidence. Analysis data using software Encase (computer forensic, Figure 5) / Cellebrite or Oxygen (mobile forensic, Figure 6, Figure 7). Digital forensic reports are made by forensic investigators based on data obtained from electronic evidence attached to special audit report. Analysis data from electronic evidence is adjusted to the allegations or cases being handled. The final stage of the special audit assignment is making special audit report.

Figure 5. Software Encase

Figure 6. Software Cellebrite

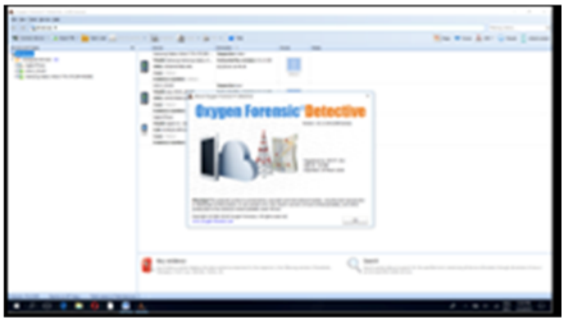

Figure 7. Software Oxygen

3.2. Data Processing

3.2.1. Questsionnaire

To answer the research question, the authors develop a questionnaire refering to the ACPO standard. Questionnaire is made by grouping questions at the stages of handling procedures at the crime scene, laboratory handling procedures, and procedure of reports making, refer to Table 3.

3.2.1. Respondents Profile

The amount of respondents is 113 evidence from six cases that have been handled using computer and mobile forensic from 2015 to 2018. The distribution of the number of cases across the duration is presented in Figure 8.

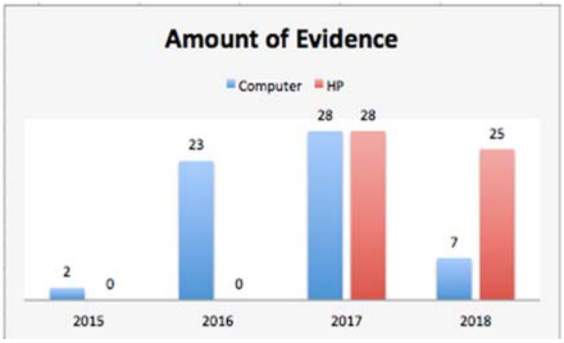

Figure 8. The Number of The Collected Evidence During The Duration of 2015-2018

3.2.3. Validity and Reliability Test

Firstly, we evaluate the validity of the questions used to study the 113 digital evidence. Each question in questionnaire is indicated by a significance level with a correlation value of 5% or 0.05. If the correlation value or r count ≥ r table means there is a correlation and valid. The result of the validity tests are presented in Table 5.

From the results of testing the validity, 21 questions from the questionnaire have a positive r value where r count> r table, so the questions are valid.

Reliability test of questionnaire data can be trusted or reliable by using the Split Half technique, which is by grouping the values of odd questions and the value of even questions. Each group has a total value then correlates the total odd values and the total even values using MS. Excel and the same formula with the validity test using CORREL (Array 1, Array 2). The instrument criteria have a high level of reliability if the coefficient value obtained is ≥ 0.60.

From the calculation using the Split Half technique, the correlation value or r count is 0.5596. Then the test results are included in the Spearman Brown formula:

$$
\begin{aligned}
R &= 2r / (1 + r) \\
&= (2 \text{ x } 0.5596) / (1 + 0.5596) \\
&= 1.1192 / 1.5596 \\
&= 0.7176
\end{aligned}
$$

The calculation provides value of R = 0.7176. It can be concluded that the instrument of the questionnaire has good reliability, because the value of R> 0.60, and then value of R> value of r table so the results of the questionnaire can be declared reliable

Table 5. Validity Test Result

Correlation between questions and total	Correlation Value (r)	r table value (n = 113, a = 5%)	Information	Conclusion
Question 1	0.3438	0.1555	r positif, r hitung > r tabel	valid
Question 2	0.4129			
Question 3	0.2735			
Question 4	0.4518			
Question 5	0.4675			
Question 6	0.2559			
Question 7	0.3568			
Question 8	0.4391			
Question 9	0.3636			
Question 10	0.3778			
Question 11	0.3978			
Question 12	0.2215			
Question 13	0.3696			
Question 14	0.3696			
Question 15	0.4018			
Question 16	0.3781			
Question 17	0.2999			
Question 18	0.3730			

Question 19	0.2031			
Question 20	0.4085			
Question 21	0.2450			

3.2.4. Analysis of Questionnaire Results

Questionnaires are used to test the 113 digital evidence from computer and mobile forensic. The evidence consist of 60 computers and 53 HP. The results from questionnaire calculation showed in Figure 5.

Figure 9 shows the complience level amount of evidence with ACPO, in detail are 2 evidence showing complience level of 24%, 22 evidence showing complience level of 43%, 24 evidence showing complience level of 48%, 23 evidence showing complience level of 52% and most 42 evidence showing complience level of 57%.

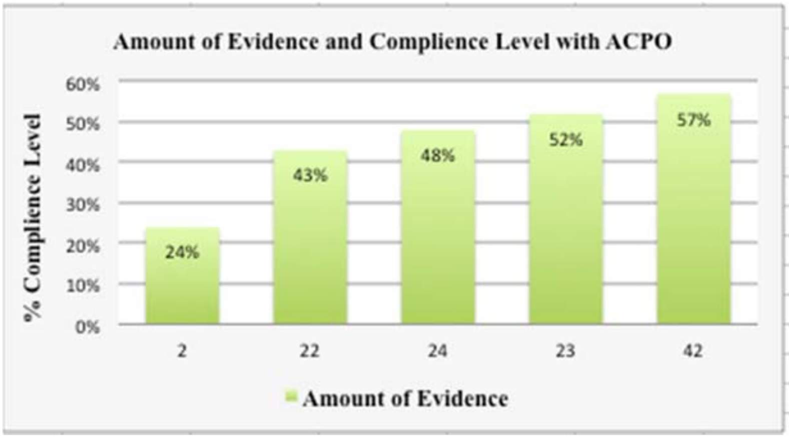

Figure 9. The numbers of evidence and their complience with ACPO standard

4. CONCLUSION

From the results of this study, it can be concluded that processing data from 113 evidences (60 computers and 53 HP), the results showed that 2 pieces of evidence showed a conformity of 24%, 22 pieces of evidence showed a conformity of 43%, 24 pieces of evidence showed conformity of 48%, 23 pieces of evidence shows a conformity of 52% and the most is 42 pieces of evidence showing conformity of 57%. The average of complience level with ACPO had only reached 51%.

We concluded that the implementation of computer and mobile forensic can reasonably meet the requirement of ACPO. The following suggestions are for PT PLN to make a standard procedure to implementation computers and mobile forensics and PT PLN makes a program for increase competency of human resource / forensic investigator by computer and mobile forensic certification.

REFRENCES:

[1] Auditors, T. I. of I. (2012). Standar Internasional Praktik Profesional Audit Internal. The Institute of Internal Auditors.

[2] PLN P.T. (2015). Satuan Pengawasan Intern. Standar Prosedur Audit Khusus, 135.

[3] Farjamfar, A., Abdullah, M. T., Mahmod, R., & Udzir, N. I. (2014). A review on mobile device's digital forensic process models. Research Journal of Applied Sciences, Engineering and Technology, 8(3), 358–366. https://doi.org/10.19026/rjaset.8.981.

[4] Manendra Sai, D., G K Prasad, N. R., & Dekka, S. (2015). The Forensic Process Analysis of Mobile Device. International Journal of Computer Science and Information Technologies, 6(5), 4847–4850.

[5] Meiyanti, R., & Ismaniah. (2015). Perkembangan Digital Forensik. Junal Kajian Ilmial UBJ, 15(September 2015), 1–7.

[6] Nuh Al-Azhar, M. (2012). Digital Forensics Practical Guidelines for Computer Investigation. Salemba Infotek.

[7] ACPO Good Practice Guide ACPO Good Practice Guide for Digital Evidence for Digital Evidence. (2012).

[8] Rahman, S., & N. A. Khan, M. (2016). Digital Forensics through Application Behavior Analysis. International Journal of Modern Education and Computer Science, 8(6), 50–56. https://doi.org/10.5815/ijmecs.2016.06.07

[9] Alanazi, F., Jones, A., & Menon, C. (2018). Sharia Law and Digital Forensics in Saudi Arabia. The Journal of Digital Forensics, Security and Law, 13(3), 5–19.

[10] Román, R. F. M., Mora, N. M. L., Vicuña, J. P. N., & Orozco, J. I. P. (2016). Digital forensics tools. International Journal of Applied Engineering Research, 11(19), 9754–9762.

[11] Umar, R., Riadi, I., & Zamroni, G. M. (2018). Mobile Forensic Tools Evaluation for Digital Crime Investigation. International Journal on Advance Science Engineering Information Technology, 8(3), 949–955.