Analysis of Smartphone Users Awareness Activities Cybercrime

Abdul Kohar
Islamic University of Indonesia
Jl. Kaliurang KM 14,5
Yogyakarta, 55584

Imam Riadi
Ahmad Dahlan University
Jl. Prof. Dr. Soepomo,
Yogyakarta, 55164

Ahmad Lutfi
Islamic University of Indonesia
Jl. Kaliurang KM 14,5
Yogyakarta, 55584

ABSTRACT
Cybercrime on smartphone users increasing every year. Unfortunately, the crime rate is not matched with user awareness about security in cybercrime activity so that similar crimes often occur back on the user's smartphone. Based on the literature study and review of related research beforehand. The main component of the research can not be separated from some things, such as user characteristics, awareness of smartphone users against cybercrime activity and the type of data that the target of the attack.

This study is one of the solutions to measure the awareness of smartphone users against cybercrime activity and to produce research schemes that have better value. With the research is expected to overcome the problem of cybercrime is happening on smartphone users which caused a lack of awareness of smartphone users against cybercrime activity.

Keywords
Digital Forensics, Smartphone, Security, Cybercrime

1. INTRODUCTION
The development of communication technology has been very rapidly penetrated into all layers, so in some aspects have changed the pattern of community life. Results of development of communication technology is the emergence of the smartphone, which is a very smart thing to use a variety of ways by the users. Smartphone equipped with a wide range of applications for the purposes of chat, email, phone, social media, and other applications [1].

In 2014, the number of Internet users, or Internet users in Indonesia is estimated to reach 71 million users. Of that amount, 41 million of whom access via smartphone and 70 million of them accessing social media such as Facebook, Twitter, Path, Instagram, LinkedIn, Google+. In addition, four out of ten people said user of social networking sites have or know of an attack on the social networking site. The data also shows, one in six people admitted they never compromised accounts, another 10% said never fooled by fraud techniques on the Internet or mengclick links that appear on their social networking site pages [2].

Indonesian Computer Emergency Response Team (IDCERT) said in 2013 in less than 24 hours of action cybercrime has increased two-fold from 30 535 at 11 June to 71,000 on June 12, where at least there are about 6 thousand IP addresses that allegedly affiliated Indonesia with a particular application so that it can result in a variety of things (information leakage, data theft, etc.) [3].

An estimated 556 million people each year become victims of Internet crimes, in addition to the estimated loss reached 21 billion dollars in result by malware, viruses, spam, hacking and fraud or theft [4].

The results of various research above, it appears that the crime at smartphone users is increasing. Unfortunately, awareness of users of smartphones on network security in cybercrime activities is still lacking, so that similar crimes often occur back on the user's smartphone. With no finding of previous studies regarding awareness of smartphone users against cybercrime activities, so this research is very important and useful for a variety of institutions and individuals.

2. LITERATURE REVIEW
2.1 Digital Forensics
Digital forensics/computer forensics is a derivative disciplines of computer security that discusses the findings of digital evidence after an event occurs. Computer forensics activity itself is a process to identify, preserve, analyze, and use digital evidence under applicable law. Digital forensics is the application of science and computer technology to carry out the examination and analysis of electronic evidence and digital evidence in view of its association with crime [5].

According to the EC Council [6], digital forensics is a series of models of techniques and procedures to obtain evidence of computer equipment, various storage media and digital media that can be presented in court with a format that can be understood and have meaning. Sedabgkan according to [7]. Digital forensics is the application of science and computer technology to carry out the examination and analysis of electronic evidence and digital evidence in view of its association with crime.

2.2 Cybercrime
Cybercrime is against the law that utilize computer technology based on the sophistication of Internet technology development. Where the Internet is a network of computers connected to each other through communication media. Cybercrime (cybercrime) is a term that refers to criminal activity with a computer or computer network into a tool, target or scene of the crime. Including into cybercrimes include online auction fraud, check forgery, credit card fraud/carding, confidence fraud, identity fraud, child pornography, etc. [8].

According to Petrus Reinhard Golose, the quotation Putra and Evan [9]. the types of cybercrime can be described as follows.

a. Entering network/computer system illegally, without permission or without the knowledge of the owner of the network / system.

b. Transmits data or disseminate information about something that is untrue, unethical, and may violate the law or disturbing public order.

c. Falsifying the data contained in the network as well as action to enter data that can benefit the perpetrator or

another person unlawfully.

d. Create a disturbance, destruction or the destruction of the data, a computer program or computer networks connected to the Internet.

e. Infringement of intellectual property rights of any party.

f. Misuse or dissemination of personal information of a person that which can have adverse effects on the person, both material and immaterial.

g. Destruction of the security system of a computer system and is usually done with the intent to commit theft of data or anarchy.

h. Using someone else's credit card without the knowledge or consent so that the person can harm both material and non-material.

i. Changing the site pages/websites other party.

j. Stealing information regarding the identity of visitors to a site.

k. Transmission of information via e-mail in which the information is unwanted by the recipient.

l. Spread malware.

Disseminate information to child pornography (child pornography).

3. RESEARCH METHODOLOGY

3.1 Components Research

Based on the literature study and a review of previous studies. The main criteria in the research component as in figure 3.1:

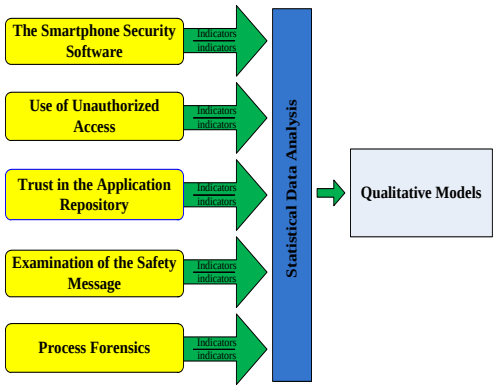

Figure 3.1 Qualitative Models

Furthermore, each component in the breakdown into a number of indicators that provide information/more complete picture of the criteria/main components. The indicator detail each component are as follows:

1. The Smartphone Security Software

The indicator smartphone security software components, namely:

a. IT skills

b. the use of smartphone applications

c. Using sossial media applications on smartphones

d. Log management assurance from each of the data, maintenance, and management

e. Storage of personal information on a smartphone

f. Using a combination of a good password on the smartphone

g. Doing policies and procedures in using any application users

h. Conduct a review of each stream data stored in smartphones

i. Knowledge of the smartphone and the smartphone malware secsoft

j. Periodic renewal application

2. Use of Unauthorized Access

The use of the component indicators unauthorized access:

a. Use of unauthorized remote access

b. Conduct a review of the impact of unauthorized access

c. Doing use of access policies and procedures

3. Trust in the Application Repository

The components of the confidence indicator in the application repository that is:

a. Using the data application repository on the smartphone

b. Malware review of the index in the application repository

4. Examination of the Safety Message

As an indicator component that checks the security message:

a. Doing policies and procedures on the use of security messages

b. Examining the security message to the physical security controls.

5. Process Forensics

The forensic process component indicators:

a. Forensic IT skills

b. Understanding of digital forensic evidence

c. Mechanism of action of digital forensics expert

d. The identification process of digital forensics expert

e. Data stored in the SIM card, memory, SD Card and service providers

f. Data storage of contacts, sms, galleries, email, recording/video and password

g. Using encryption applications

3.2 Method of Collecting Data

3.2.1 Design Research

The study design was made in several steps as in Figure 3.2:

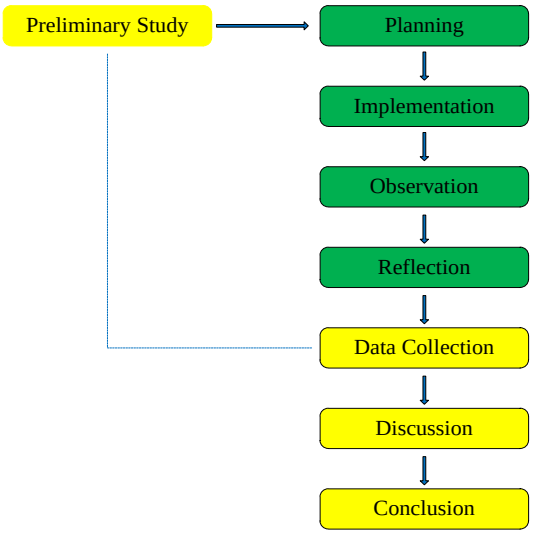

Figure 3.2 Draft Grooves Research

Based on the above study design as shown in Figure 3.2 can be focused on the points of which:

1. Preliminary Study: some material finding stage of the topics discussed in the study.
2. Planning: In the planning phase, direct observation state of the research sites. After that, identify problems that occur and develop hypotheses action.
3. Implementation: During the implementation phase to measure the awareness of smartphone users against cybercrime activities using tools orinstruments to use E-survey research tailored to the formulation of research.
4. Observation: During the process of implementation of the action takes place, observing everything that happens during the execution of the action takes place.
5. Reflection: Reflection serve as an evaluation as well as to establish the conclusions of this study.
6. Data Collection: Data collection is done to obtain the information needed in order to achieve the research objectives of the preliminary study.
7. Discussion: Perform the test results of statistical data collection by t test using SPSS.
8. Conclusion: Summing up the results of the discussion or the results of research conducted.

3.2.2 Research Instruments

The research instrument is a tool that can be used to collect research data, and is also called the research techniques. The types of instruments used in the study as follows:

1. Survey Applications / E-Survey

E-survey is a data collection framework is extremely versatile and tools to help plan the event, send surveys or gather information easily in an efficient manner in order to facilitate access to electronic data.

2. SPSS

SPSS was used to analyze the data obtained from the research. SPSS is a statistical computer program that serves to assist in processing statistical data accurately and quickly, and produce a variety of desired output.

3.2.3 Draft Scenario Testing

Stages will be done in testing the results of this study are shown in Figure 3.3:

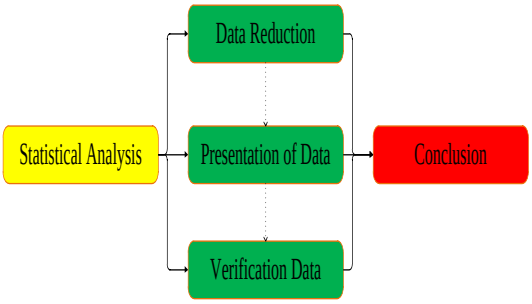

Figure 3.3 Draft grooves Testing Results

Based on the above test design as shown in Figure 3.3 can be focused on the points of which:

1. Statistical Analysis: testing data by statistical t test using SPSS.
2. Data Reduction: The process of selecting activities, focus and simplify all the data have been obtained, starting from the beginning of data collection to the preparation of research reports.
3. Presentation of Data: Presentation of data is done by simply compiling data into tables and named qualitative. Thus providing the possibility of drawing conclusions.
4. Verification Data: Process appearance essence of a dish that has been organized in the form of a sentence or statement clear and concise information.
5. Conclusion: As a result of review test results.

The plan to analyze the data generated by observational analysis techniques rating recording. Rating recording is used to evaluate whether there is a correlation between the results of the questionnaire survey with the results of monitoring observations on smartphone users use applications Bloove or Bloove agent. Process monitoring with observation technique recording techniques rating for smartphone users in show in Figure 3.4:

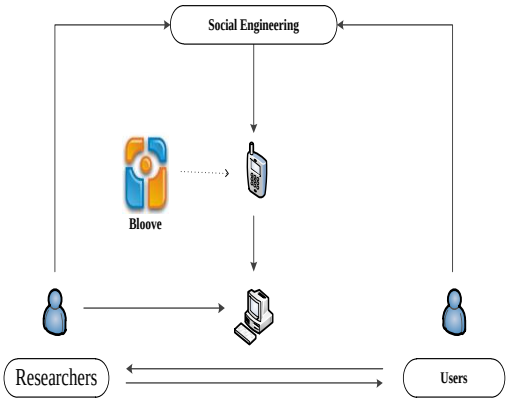

Figure 3.4 Rating Observation Techniques Recording

Based on the monitoring process of smartphone users in the top as shown in Figure 3.4 can be focused on points such as:

1. Researchers: Someone who does the monitoring of the user's smartphone or target.
2. Social engineering: techniques used to approximate the user or the target so that it can grow on a smartphone application for monitoring users or target.
3. Bloove: Applications are planted or installed on a user's smartphone or target.
4. Computer: as a tool to monitor the user's smartphone or target the object of research.
5. Smartphone: the object or target penelitaian.
6. Users / user: A person who becomes the target of monitoring.

As for the draft to analyze the ontology or forensic process in this research is the show in figure 3.4:

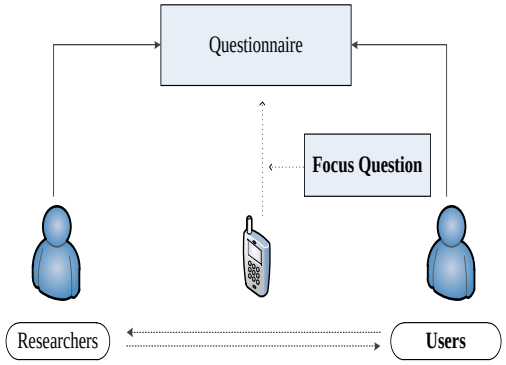

Figure 3.4 Draft grooves Forensic Process

Based on the above draft forensic process as shown in Figure 3.4 can be focused on the points of which:

1. Researchers: Someone who searches the research data.
2. Questionnaire: as a tool to obtain data.
3. Smartphone: a theme discussion in the questionnaire.
4. Users: A person who becomes the respondents in the study.

3.3 Statistical Data Analysis

3.3.1 Research Design

Implementation of this study followed the research phase diagram refers to modifications listed Kemmis and Mc Taggart [10]. Carried out in several stages, namely 1) planning, 2) Implementation, 3) observation, and 4) Reflection.

3.3.2 Data Measurement Techniques

Data collected through observation techniques performed during research activities. Implementation of observation to the subject of research done by filling out a questionnaire observations that have been prepared.The type of data that can be gained from this research, ie qualitative data.

Qualitative data analysis in this study is done after data collection. The stages of qualitative data analysis activities by Miles and Huberman [11]. adalah: a) data reduction, b) present the data, and 3) Verification of data / inference.

a. Data Reduction

Data reduction is the process of selecting, simplifying all the data have been obtained, starting from the initial focus, and data collection to the preparation of research reports.

b. Presentation of Data

Presentation of data is done by simply compiling data into tables and named qualitative. Thus providing the possibility of drawing conclusions.

c. Verification/inference

Inference is the process of appearance of the essence, of the dish which has been organized in the form of a sentence or statement clear and concise information.

3.3.3 Data Analysis Techniques

Data analysis techniques will be performed calculations through t test. The research hypothesis:

1. Calculate correlation, using the formula Pearson Product Moment:

$$r_{xy} = \frac{n.(\sum XY) - (\sum X)(\sum Y)}{\sqrt{\{n.\sum X^2 - (\sum X)^2\}\{n.\sum Y^2 - \sum Y)^2}}$$

Information:

r_{xy} : Correlation Coefficient

N : Number of respondents

Y : Total score of all items

X : Total score for each item

2. Test the significance of the correlation obtained by using t-test, ie by the formula:

$$t_{hitung} = \frac{r\sqrt{n-2}}{\sqrt{1-r^2}}$$

If $t_{arithmetic} > t_{table}$, the measuring instrument or instruments used in this research is valid

If $t_{arithmetic} > t_{table}$, then the measuring instrument or instruments used in this research is not valid.

Testing instrument by using SPSS application.

3. Giving interpretation using assessment guidelines as proposed by [12], is shown as follows:

81 % - 100 % : very good

71% - 80 % : good

66 % - 70 % : pretty

0 % - 60 % : less

0% : very less

3.4 Rating Observation Techniques Recording

The plan to analyze the data generated by observational analysis techniques rating recording. Rating recording is done after getting the results of the data analysis of the survey questionnaire that aims to evaluate whether there is a correlation between the results of the questionnaire survey with the results of the monitoring on a smartphone device users use applications Bloove or Bloove agent. Steps rating observation techniques to obtain monitoring data recording device smartphone users conducted in the following manner:

1. Social engineering, ie to approach the smartphone user or target so that it can grow or install a monitoring application for smartphone users or target. Smartphone or target users who already installed the application will be the object of a study to determine awareness of smartphone users against cybercrime activity.
2. Analysis of the results of monitoring, namely data analysis techniques in getting the results of the monitoring on a smartphone device users or target so as to produce the output characteristics and awareness of smartphone users against cybercrime activity. The title (Helvetica 18-point bold), authors' names (Helvetica 12-point) and affiliations (Helvetica 10-point) run across the full width of the page – one column wide. We also recommend e-mail address (Helvetica 12-point). See the top of this page for three addresses. If only one address is needed, center all address text. For two addresses, use two centered tabs, and so on. For three authors, you may have to improvise.

3.5 Forensic Verification Methods Related Activities

According to Hopkins in Iskandar [11], form validation study was carried out in the following manner:

1. Triangulation, which did check the accuracy of data and information to confirm to the user that is directly involved in the action.
2. Membercheck, which checks the data correctness and validity of research findings by confirming the source of the data.
3. Audit Trail, which checks correctness interim research results and the procedures and methods of data collection complete with evidence of the findings in the study.
4. Expert opinion, which checks the data against the validity of research findings to professional experts in the areas of materials research study.

4. RESULTS AND DISCUSSION

4.1 Research Result

Of the various review and revision of various studies. concluded that penelitisn components can not be separated from several things, among others:

1. The smartphone security software
2. Use of unauthorized access
3. Trust in the application repository
4. Examination of the safety message
5. Process forensics

Then, with the formation of the components and indicators of each component, can be used to determine the awareness of smartphone users against cybercrime activities.

4.2 Application of Data Analysis Test-T

This research was conducted on students in Cirebon region consisting of various majors with 61 respondents. Before melakukak data analysis needs to be conducted to determine the sample of the entire population or research respondents. According [12], the sample is part of the number and characteristics possessed by this population. When large populations, and researchers may not learn all that there is in the population, for example, because of limited funds, manpower and time, the researchers can use the sample drawn from the population. Sample withdrawal technique often referred to as the sampling technique. Sampling is the process of determining the sample to be used in research. In his book, Arikunto said that "if the population numbers less than 100, it would be better if taken as a whole, and this research is also called the study population, if the population of more than 100, it can be 10-15% or 20-25% or more ". Data were collected on July 05 - August 5, 2015.

4.3 Data Analysis

Basing on the research component can be calculated based on each component, can also be calculated as a whole/in person of all the component. The details can Adapaun in Table 4.1:

Table 4.1 Component Index Research

No	Component	Description				
		A	B	C	D	E
1	smartphone security software	80	328	175	31	0
2	of unauthorized access	3	64	78	26	0
3	st in the application repository	5	54	47	14	0
4	mination of the safety message	13	55	46	8	0
5	cess forensics	29	184	153	43	0

Based on table 4.1 above, for smartphone security software components from 61 respondents obtained very good (A) 80, both (B) 328, just 175, less (D) 31 and very less (E) 0. So that the security software smartphone smartphone users are aware of cybercrime activity. Furthermore, the index is obtained for the use of component usage unauthorized access of 61 respondents obtained very good (A) 3, both (B) 64, just 78, less (D) 26 and very less (E) 0. So that the use of access Unauthorized smartphone users are aware of cybercrime activity. Then obtained an index of confidence in the application repository component of 61 respondents obtained very good (A) 5, both (B) 54, just 47, less (D) 14 and very less (E) 0. So that trust in the application repository conscious smartphone users will cybercrime activity.

Based on the examination of the examination component index's security messages of 61 respondents obtained very good (A) 13, both (B) 55, just 46, less (D) 8 and very less (E) 0. So that checks the message's security smartphone users are aware of the activity cybercrime. Furthermore, the index for forensic process component of 61 respondents obtained very good (A) 29, both (B) 184, just 153, less (D) 43 and very less (E) 0. So that process forensic smartphone users are aware of cybercrime activity ,

Based on the overall research component of 61 respondents obtained very good (A) 130, both (B) 685, just 510, less (D) 122 and very less (E) 0. So overall smartphone users are aware of cybercrime activity.

4.4 Discussion

Discussion indexes on each of the components, the highest index score of the answer lies in either (B) of 685. This shows smartphone users are aware of the ativitascybrcrime. But

there who score less answer (D) with a value of 122, because there are still users who do not care or do not understand cybercrime activity.

In addition to some of the components, it appears there are some respondents expressed less (D), this shows the uneven dissemination and understanding of smartphone users against cybercrime activity.

5. CONCLUSIONS AND SUGGESTIONS

5.1 Conclusion

From various literature, review some of the research, application, discussion and analysis can be concluded several things, among others:

a. Based on the results of the components used in the research in the study of consciousness analysis smartphone users against cybercrime aktivititas overall characteristics of smartphone users are aware of cybercrime activity, although still lacking.

b. Awareness of smartphone users against cybercrime activity of students in the Cirebon. Results of the survey questionnaire and observation techniques rating recording using SPSS research instruments and applications or tools Bloove overall research component of the overall score of the answer and score assessment that smartphone users are aware of cybercrime activity, although there is still no significant assessment scores.

5.2 Suggestion

For their next study, can be supplemented and corrected, among others:

a. Research can be used in other aspects, not on the aspects of mobile smartphone users only.

b. In the research could be used more samples, both in the field as well as several different areas.

c. To get thenextvalid researchstudiesmay usedifferentquestionnaires.

d. Techniquesanswersscoreintervaljudgment can be madein order to getratingsthatare more relevant tothe real situation.

6. REFERENCES

[1] Raharjo, P., Utami, E. T. (2012). *Aplikasi Penerima Radio Streaming Online Pada Smartphone Berbasis Java.* Politeknik Negri Semarang. Semarang.

[2] Widodo, T.,Prayudi, Y. (2013). *Model Digital Forensic Readiness Index (Difri) Untuk Mengukur Tigkat Kesiapan Institusi.* Magister Teknik Informatika Universitas Islam Indonesia (UII). Yogyakarta.

[3] Alkazamy, Ahmad Khalil. (2011). Statistik Internet Abuse Indonesia 2011:Laporan Smester-1 Tahun 2011, edisi 1.

[4] Nortton.(2012). 2012 Norton cybercrimeReport, 12 Januari *Tahun 2012*, edisi 4.

[5] Asrizal. (2012). *Digital Forensik.* Magister Teknik Informatika Universitas Sumatera Utara.

[6] ECCouncil. (2008). CHFI v4 Module 01 Computer Forensics in Todays World.

[7] Al-Azhar, M. N. (2012). Digital Forensik Panduan Praktis Investigasi Komputer (Edisi Pert.). Salemba Infotek. Jakarta

[8] Suseno, S. (2014). *Cybercrime dan Keberlakuan Hukum Pidana Nasional*. :Universitas Padjadjaran. Bandung.

[9] Aldyputra, Martinus Evan. (2012). Pengaturan Penyebaran Informasi yang Memiliki Muatan Penghinaandan/Pencemaran Nama baik dalam Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaks iElektronik (Tinjauan Yuridis Terhadap Pasal 27 ayat (3) Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, LN No. 58 Tahun 2008, TLN No. 4843), Universitas Indonesia. Depok.

[10] Hari, Gunansyah.d. (2010). *Penerapan Model Value Clarification Technique*. Unesa. Surabaya

[11] Nasia (2014). Pengembangan Instrumen dan Bahan Ajar untu k Meningkatkan Komunikasi, Penalarandan Koneksi Matematis dalam Konsep Integral. Unisba. Bandung.

[12] Sugiyono. (2011). *Metode Penelitian Kuantitatif, kualitatif dan R & D*. Alfabeta. Bandung.