Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

ANALYSIS ON PREDICTING CYBERTERRORISM USING AHP (*ANALYTICAL HIERARCHY PROCESS*) METHOD

[1] LUTHFI FEBRIANSYAH, [2] IMAM RIADI
[2]

[1] Department of Informatics , Universitas Islam Indonesia, Yogyakarta, INDONESIA

[3] Department of Information System, Universitas Ahmad Dahlan,Yogyakarta, INDONESIA

[4] E-mail: [1]15917112@students.uii.ac.id, [2]imam.riadi@is.uad.ac.id

ABSTRACT

This research aims to develop the steps used in mobile forensic based on the previous cases by using EWS (Early Warning System) to gather useful information about radical beliefs which will be transfered into intelligence product. The process of this research began by making a case simulation, which contains illustrations of the case that had happened and had been followed up by the Police. Furthermore, the afformentioned case featured some evidences and one of them is digital evidence which can be used to gain more information from the followed up case so that information could be used to monitor the connection between similar cases.The analytical method used is AHP (Analytical Hierarchy Process) which is a method used to analyze the suspect's acquired Smartphone to search some contacts from the Whatsapp Messenger using these criteria: frequent or high intensity with the suspect, contact, or individual or group that had not yet inputted to the ISIS symphatizer list or the list of radical groups (database), the existence of documents or information which lead to ISIS movement or radical groups that lean towards terrorism. The result obtained from this research is that Early Warning System, in predicting Cyberterrorism, could use AHP (Analytical Hierarchy Process) method by doing these steps: determining criteria, weighing which is adjusted to its importance, deciding on alternatives to get new targets from on-going case and also based on analysis results and tests.

Keywords: *Cyberterrorism, AHP, Digital Evidence, case simulation.*

1. INTRODUCTION

Daerah Istimewa Yogyakarta is a region which is known by many names, for examples: The City of Culture, The City of History, The City of Students, and The City of Tourism. As a result, Daerah Istimewa Yogyakarta has plural society which characteristic consisted of various tribes, religions, languages, cultures and traditions. The diversity (in social interaction between people) in daily lives often produced sparks which has potential in creating disturbance. This matter need to be regulated properly by the whole apparatus of government in Daerah Istimewa Yogyakarta so all arising problems could be well detected and anticipated,. In the last 3 years, cases of violence in Daerah Istimewa Yogyakarta increased, such as thuggery, the destruction of the tomb that became the cultural heritage and cases of religious intolerance. Especially in cases of religious intolerance in Daerah Istimewa Yogyakarta, due to the existence of communities of certain religious organizations with radical beliefs which actions always apply fanatical ideologies that are later manifested in radical actions ranging from conducting sweeping or even their disagreement of other religious followers carrying out religious prayer.

The phenomenon ISIS ideology all over the world is extraordinary and it is feared that this ISIS ideology expanding in Daerah Istimewa Yogyakarta, so it is of utmost importance to prepare anticipatory steps towards these radical groups by early detection using *mobile forensic*, to learn the technologies used and the steps of utilizing *mobile forensic* to obtain information which is beneficial for the Police, especially the intelligent force in early detection and giving out early warning, or anticipating the movements of the radical groups.

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

2. LITERATURE REVIEW

2.1. Digital Forensic

2.1. 1. Definition

Handling a case which is connected with information technology usage often needs forensic. Forensic is an activity to investigate and determine facts which is related with criminal cases and other legal problems. Digital forensic is part of forensic science which covers the discovery and investigation of materials (data) that can be found on digital devices (computer, handphone, tablet, PDA, net-working devices, storage, etc.). Digital forensic could be divided further into forensic which is related to computer, (host, server), network, applications (including database), and devices (digital devices). (Raharjo, 2013)

According to Budhisantoso, "digital forensik adalah kombinasi disiplin ilmu hukum dan pengetahuan komputer dalam mengumpulkan dan menganalisa data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan sehingga dapat dibawa sebagai barang bukti di dalam penegakan hukum." (Asrizal, 2015)

2.2.2. The Function of Forensic Computing

In line with its definition, Forensic Computing principally has one main purpose (Indrajit, 2011), which is:

a. To help recover data, to analyze, and to present digital–based or electronic material/entity in such way that it is admissible as legal evidence on court.
b. To help the identification process of evidence in a relatively quick time, in order to estimate the potential of the impact caused by the malicious behavior which had been done by the criminal towards his/her victim, and also to reveal the reason and motivation of the behavior while searching for the parties related to the unsavory behavior, whether directly or indirectly. As for the activity of forensic computing, it is usually done in two main contexts: First is context related to the collection and preserving the data containing all the detailed record about the routine activity which is done by certain organizations or companies which involves information technology and communication. Second is data collection which is specifically intended for context where there is a technology-based crime.

2.2. Mobile Forensic

Mobile phone Forensic is a study to recover *digital evidence* where the *mobile phone* is in a *Forensically Sound* state (a state where if the phone is turned off it stays turned off, while if it is turned on it stays turned on) upon acquisition in accordance to the handling procedure. *Mobile Foresic* nowadays is growing rapidly along the development of mobile phone among the masses.

Mobile phone Forensic Analysis involves *mobile forensic examiner*, whether manually or automatically. *Auto extraction* is used when the device is compatible with a *software* and *manual extraction* when the device is incompatible (Kevin Curran, 2010).

Mobile phone usage in criminal acts is recognized in recent years, while mobile phone forensic is a relatively new scientific study which began around 2000. Mobile phone development (especially *smartphone*) in consumer market resulted in the increase of demands for mobile phone forensic, which cannot all be fulfilled by *Digital Forensic* field.

Investigation process is usually focused on simple data such as call log, and communication such as email or SMS, and also deleted data from the *mobile device*'s storage media. *Mobile devices* are also usually used to find information about location, by using GPS or locator tools or through *cell site logs*, which track the devices that enter its range.

Information collected from mobile device can be useful in various legal problems, administration, and investigation such as:

a. Intellectual property theft
b. Online scam
c. Economic abuse
d. Divorce and Family Law
e. Geo-Location Controversy
f. Evidence of Crime (Fajar, 2014).

Nowadays, *social networking* trend through social media has led habit and lifestyle change in socializing. For examples among others are Facebook, Twitter, Path, etc, with Facebook as the *leader*. It is proven by Facebook's numerous active user to date and will continue to increase daily. Official release of *newsroom facebook* states that 1.01 billion of *users* are active every day and 894 milion are active via mobile phone, based on September 2015 data. Meanwhile, quoted from *consumer.org* article which is released on 2011 states that 5 million Facebook accounts had experienced harassment and 9.5 million Facebook users are using fake identity. These statistical numbers from Facebook are

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

enough to illustrate the number of users and the size of social media potential to be involved in all kinds of humanly activities, whether positive or negative, and it is not impossible to include activities which are going against the law.

Those data and facts then require an investigative procedure to help uncovers a crime case as a response when the activity of one of the Facebook accounts had touch the realm of law, whether it is faking/thievery of personal identity, scamming, kidnapping, defamation, homicide, and there are still much potential that could be a new modus operandi in a crime. Facebook is a digital realm and involves computer technology in it so obviously the investigation done is using *digital forensics* technique. (for-i.blogspot.co.id, 2016).

2.3. The Impact of Social Media

Reading news on the internet, not only practical, but there are also a lot of sources and always *up to date*. But oftentimes I was confused by the contrasting news between different medias, where one media giving the impression of attacking, while other media is instead defending. No small amount of readers which are then provoked by the news "which veracity and sources are not proved yet". As a prove, we could see in the comment section where blasphemy run rampants instead of constructive criticism/opinion. Comments that contain blasphemy, swearing, or even animals are on the roll call there. Often I could not read it due to pity. (Hanifa, 2013)

Media propaganda to ignite a war now can be taken over by social media or social network. The question is, why social media is so powerful in spreading its messages? First, people are in euphoria towards social media. It is loved by international community. There is no citizen which is not influenced by social media. Even all print media and electronic media nowadays had to utilize that social media to spread their messages. No matter where, people make use of social media. It is proof on how great the impact of social media's influence. Even Indonesia is occupying the 4th rank in world's Facebook usage (43 million users) after America, India, and Brazil. Second, social media is capable of sharing a message in a revolutionary way. The message spreads on social media is so powerful that it could influence people's behavior and attitude. For example is the Egypt Revolution (2011) where Hosni Mobarak was overthrown due to social media. In relation with social media, Egypt Revolution starts from the inisiative of Whael Gonim which created a FB account *'We are all Khaled Said'* on July, 2010. That account then attracted large number of people, especially people who oppose the government. That account was made by Ghonim as a form of sympathy towards Khaled Said who become the torture victim of Egypt's members of police force in an internet caffee in Alexandria. In the end, the case become communication media of an anti-government group in conducting a demonstrative movement (Lutvia, 2011). After account '*We are all Khaled Said'*, Ghanim's supporters then create another Facebook account. One of those accounts is '*6th of April Youth Movement*' which is also used as anti-government movement. Not only FB, Twitter is also used. Through Twitter, the demonstrators communicate with each other and offer information regarding the development of Egypt demonstration. Third, people's belief in social media exceeds reality. This can be seen because of people's strong belief in social media, even though it may differ in reality. The analogy could be like this, there is a possibility where someone who is addicted to watch a ghost show in the TV would be afraid to go outside during the night due to his perception of being surrounded by many ghosts even though the reality is not how it was portrayed by the television. It is why social media also had planted a belief which transcends the reality (Nurudin, 2012).

2.4. Analitycal Hierarchy Process (AHP)

AHP is a decision support system which is developed by Thomas L Saaty. This decision support system will decompose multi-factorial or multiple-criteria problems which are very complex into a hierarchy, according to Saaty (1993), hierarchy is defined as a representation of a complex problem in a multi-level structure where first level is goal, which is followed by factor level, criteria, sub-criteria, and so on to the bottom until the last level of alternative. With hierarchy, a complex problem could be unraveled into groups which then arranged into some form of hierarchy so the problem will seem more structured and systematic.

AHP is often used as a problem solving method in comparison with other methods due to these reasons:

1. Hierarchical structure, as a consequence of the chosen criteria, to the inner most sub-criteria.
2. Consider the validity into the inconsistency tolerance limit as various criteria and alternatives chosen by the decision maker.

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

3. Calculate the durability of sensitivity analysis output of the decision maker (Syaifullah, 2010).

Steps done in supporting AHP decision maker are as follow:

a. To define the problem and determine the desired solution.
b. To create a hierarchical structure which is started with the general goal, followed by chosen criteria and alternatives (Eko Darmanto, 2014). As Figure 1 has shown:

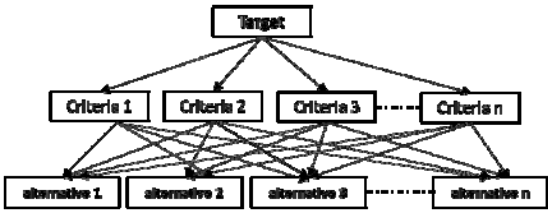

Figure 1. AHP Steps Structure

3. RESEARCH METODOLOGY

Analytical method used is AHP (*Analytical Hierarchy Process*). That is giving weight to the contacts connected with the suspect using criteria below:

- Frequent or high communication intensity towards the suspect

- Contact or the individual or the group has yet to be inputted into the ISIS Sympathizer List or Radical Groups List (database)

- The existance of documents or information which lead towards ISIS movement or Radical Groups that lean towards Terrorism.

Detail metodology are from Case Simulation, Digital Evidence, Investigation Digital Evidence etc. Illustration research can be seen at Figure 2:

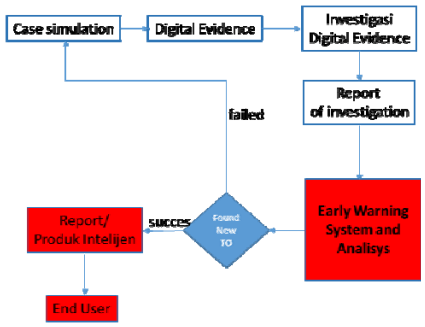

Figure 2. Illustration of the research steps

3.1. *Case Simulation* is illustration of the case that had happened and had been followed up by the police. Furthermore, the afformentioned case featured some evidences and one of them is *digital evidence* which can be used to gain more information from the followed up case so that information could be used to monitor the connection between similar cases.

3.2. This *Digital Evidence* is acquired from case simulation which had been followed up by the police. While the steps after obtaining the *digital evidence* are as follow:

a. *Identification Digital Evidence*, which is identificating any digital evidence that could be investigated in order to gain new information.
b. *Preparing tools*, which is preparing the tools that could investigate the *digital evidence* compatibly.
c. *Storage of digital evidence*, which is preserving the *digital evidence* in order to guarantee the safety and authenticity of the *digital evidence* (Asrizal, 2012). As for the view of the steps after the acquisition of the *digital evidence* can be seen at Figure 3:

Figure 3. Digital evidence identification steps

3.3. *Investigation Digital Evidence*
This step is doint the extraction/imaging process from the digital evidence which expectantly will show or discover new target whose development could be monitored (Yunus Yussof, 2011).

3.4. *Report of Investigation*

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

This step is the result of step 3 in the form of documents so the investigator can do the research on the target/mark and can do the inputting to the Early Warning System. (Ben Martini, 2012)

3.5. *Early Warning System and Analisys Early Warning System (EWS)* are a way in detecting, monitoring and analyze the seeds of conflict as early as possible

From the result of inputting data into EWS, so in this step is to show the data in the form of graphic, numbers, and percentage from the suspect's social media towards the other associates. It is expected that a new target whose development could be monitored can be found, in this case is the spreading of radical belief. (Karnaji, 2013).

Analytical method used is AHP (*Analytical Hierarchy Process*). That is giving weight to the contacts connected with the suspect using criteria below:

- Frequent or high communication intensity towards the suspect
- Contact the individual or the group has yet to be inputted into the ISIS Sympathizer List or Radical Groups List (database)

The existance of documents or information which lead towards ISIS movement or Radical Groups that lean towards Terrorism as can be seen from Figure 4:

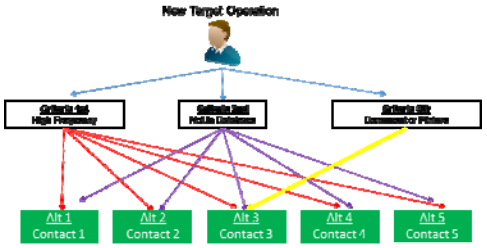

Figure 4. Analysis with AHP Flow Chart

Explanation :

Alt 1 : Alternative 1
Alt 2 : Alternative 2
Alt 3 : Alternative 3
Alt 4 : Alternative 4
Alt 5 : Alternative 5

3.6. *Found New TO*

From the acquisition of the suspect's Smartphone, it is gathered that some contacts are often in touch with the suspect with criteria as follow:

- Frequent or high communication intensity towards the suspect
- Contact the individual or the group has yet to be inputted into the ISIS Sympathizer List or Radical Groups List (database)
- The existance of documents or information which lead towards ISIS movement or Radical Groups that lean towards Terrorism.

Using AHP method, weighing and ranking from the contact's alternatives will be done

3.7. *Report*/ Intelligence product

This step is the creating of a report which will illustrate the EWS analytical result to the level of determining new targets, in this case the report meant in intelligence world is Information Report or Specialized Report which is addressed to Direktur Intelijen Keamanan Polda and forwarded to Kapolda DIY as *end user* and can be seen from the Figure 5 (Kabaintelkam, 2014):

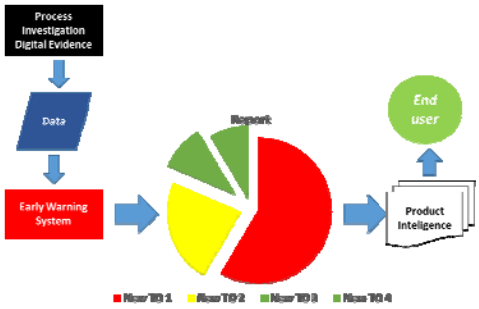

Figure 5. Early Warning System flow

4. RESULT AND DISCUSSION

4.1. Case Simulation

On Tuesday afternoon, August 16, 2017 at Dusun Jeruk, Desa Kepek, Kecamatan Wonosari Gunungkidul Yogyakarta, Roni Suroto (RS) 33 years old, Muslim, was apprehended for being suspected to be a member of terrorist group. From the shakedown on RS' house, some evidences are secured, such as:

a. 1 Samsung Galaxy E7 Smartphone
b. Money at the amount of Rp. 240.000,-
c. ID Card of the suspect with RS initials and domiciled at Tegal, Central Java

Illustration pre-incident as in the Figure 6 :

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

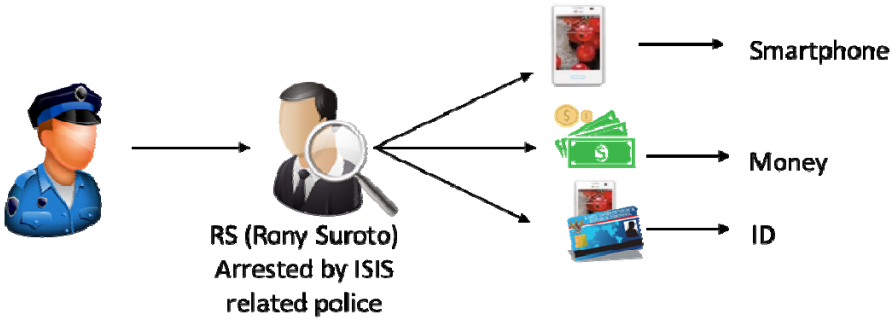

Figure 6. Illustration pre-incident

The arrest was done by Densus 88 Anti Teror Polri helped by Sat Reskrim Polres Gunungkidul and some members of Satbrimobda DIY. Other than RS, his wife and his three children and 1 child from his elder sibling are also taken into custody. Evidences secured during the search are preserved at Ditreskrimum Polda DIY for further investigation. Ditintelkam Polda DIY borrows and uses those evidences to catch other targets, by sending official note towards Direktur Reskrimum Polda DIY numbered: B/ ND-1256/VIII/2017/Ditintelkam on August 18, 2017, which later on an investigation will be done by Sie Inteltek Ditintelkam Polda DIY, just like Figure 7 :

Incident

Figure 7. Illustration Incident

Picture The process of borrowing and using evidences to Ditintelkam Polda DIY through Ditreskrimum which was found by Densus 88 AT at the search location

After the investigation which was done by Sie Inteltek Ditintelkam Polda DIY is finished, the discovered result can be seen on Figure 8:

Past Incident

Figure 8. The result of Sie Inteltek Ditintelkam Polda DIY investigation

4.2. Digital Evidence

a. Identification Digital Evidence

Sie Inteltek Police Department of Yogyakarta had investigated the evidences found at the house of the suspected member of terrorist group, RS. From the identification process on those evidences, the gathered information is as shown in Figure 9. and Figure 10:

- Merk : Samsung Galaxy E7
- IMEI 1 : [redacted]060961777 / 01
- IMEI 2 : [redacted]060961775 / 01

For found this IMEI, can be dial *#06#. Function of IMEI is identify smartphone, because number in IMEI always different from other smartphone.

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

Figure 9. IMEI from the suspect's Samsung E7 Smartphone

From imei information, this is information about smartphone the suspect.

Figure 10. The information is based on the imei of the suspect's evidences Samsung E7 Smartphone

b. Preparing Tools

Before doing the investigation process, the researcher prepared some tools starting from Digital Evidence identification to the EWS (*Early Warning System*) analysis stage, such as:

A. Software

1) Info IMEI online : http://www.imei.info
2) Oxygen Forensic
3) Andriller
4) Sqlite Browser
5) Odin3-v3.10.6
6) Notepad ++
7) Php Myadmin / Sql Database

B. Hardware

1) Laptop Lenovo G40
2) Data Cable
3) OTG
4) Eksternal HD

c. Storage of Digital Evidence

Preservation of the investigation is done on Eksternal Hardisk Sie Inteltek in Police Department Yogyakarta

4.3. Investigation Digital Evidence

- **Rooting Process**

In this research, rooting process done on the suspect's Samsung E7 Smartphone is using **Odin3-v3.10.6** which is compatible with the suspect's Smartphone, because this smartphone used Android for OS (*Operating System*) and for rooting proccess can be used notebook or PC . Like in Figure 11 and Figure 12 for interface **Odin3-v3.10.6**.

Figure 11. Rooting process preparation using Laptop or PC

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

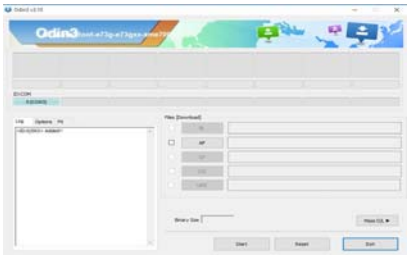

Figure 12. Rooting process using Odin V3

- **Acquisition**

a) Andriller

Andriller is forensics tools for smartphone that has features such as: sound forensics, database, pattern lock, Pin and password. View of andriller tools and the acquisition process using andriller . Like in Figure 13 and procces acquisition in Figure 14:

Figure 13. The View of Andriller V2.5.2.0 tools

Figure 14. Acquisition process with andriller tools

Oxygen Forensic

Oxygen Forensic is forensics software to extract and analyze mobile device data, smartphone, and tablet.

Oxygen Forensic is using proprietary protocol which allows much more data extraction, but still within the steps of standard forensics and without changing the content of the analyzed device. This software had been used by law enforcement and governmental institute, private and other digital forensics specialist. Here are the features that could be extracted using oxygen forensic and can be seen on the Table 1.

- Common device information
- Contacts with the information and photos
- Call Registry
- Organizer Data (meetings, appointments, memos, etc)
- SMS/MMS
- Photo, video, audio file and voice recorder
- Map when using the camera
- Wifi connection with the password
- Device logs
- Data file stored in the device
- And other features of oxygen forensic are:

Table 1. Oxygen Forensic Features

Capabilities	Oxygen Forensic® Extractor
Live device acquisition	Yes
Android devices rooting	Yes
Device backups import	Yes
Android and iOS images import	Yes
Saving data to OFB backup	Yes
Device data reports	Yes(PDF, RTF, XLS, HTML, XML. CSV, TSV, etc.)
Price (Final offer depends on the number of hardware pieces where Oxygen Forensic® Extractor will be activated)	**Request Quote** (20 activations)
	Request Quote (1 activation)

Journal of Theoretical and Applied Information Technology
30th November 2018. Vol.96. No 22

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

Below are the views of the acquisition process on the suspect's smartphone using oxygen forensics, like in Figure 15:

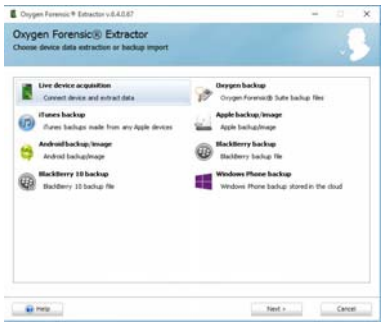

Figure 15. Acquisition process of the suspect's smartphone using oxygen forensics tools

Below are the views of *Physical dump Oxygen Forensic* process on the suspect's smartphone, we can choose the one that is most suitable android, apple or Blackberry, like in Figure 16

Figure 16. Physical dump Oxygen Forensic process on the suspect's smartphone

Below are the views of *Finishing Process physical dump Oxygen Forensic* on the suspect's smartphone, like in Figure 17

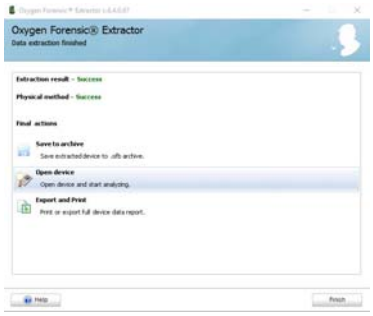

Figure 17. Finishing Process physical dump Oxygen Forensic on the suspect's smartphone

Below are the views of *Result of Acquisition with Oxygen Forensic* on the suspect's smartphone, like in Figure 18

Figure 18. Result of Acquisition with Oxygen Forensic on the suspect's smartphone

4.4. Report of Investigation

From the acquisition process using andriller and Oxygen Forensic tools, information from Whatsapp Messanger that are found are as follow:

a. Contact with high frequency can be seen on the Table 2:

Table 2. Contact with high frequency that communicate with the suspect

NO	NUMBER OF CONTACT	FREQ	ALT
1	+62856014XXXXX	21	ALT 1
2	+62851014XXXXX	6	ALT 2
3	+62812295XXXXX	9	ALT 3
4	+62821367XXXXX	64	ALT 4
5	+62895344XXXXX	10	ALT 5

From those contacts, below is the capture of conversation via Whatsapp Messanger that can be seen on Figure 19:

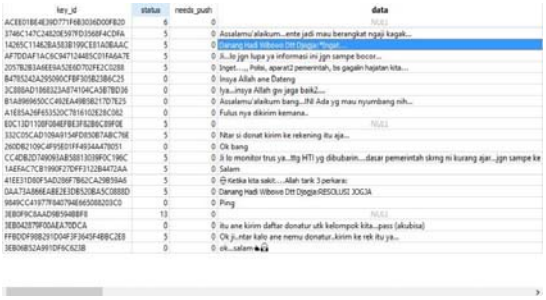

Figure 19. capture of the suspect's conversation via Whatsapp Messanger

b. Suspicious document or picture like table 3 below:

This table explain where contact-contact in suspect smartphone ever sent documen or image to realated this case.

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

Table 3. Contact with high frequency that communicate with the suspect

NO	NUMBER OF CONTACT	DOC/ PICTURE	INFO
1	+62856014XXXXX	0	*.xls and *.JPG extention
2	+62851014XXXXX	0	
3	+62812295XXXXX	2	
4	+62821367XXXXX	0	
5	+62895344XXXXX	0	

c. Existance in database

- **Discovered document**
  In Result of Acquisition, found document or picture like Figure 20 and Figure 21:

Figure 20. capture of documents found on the suspect's smartphone

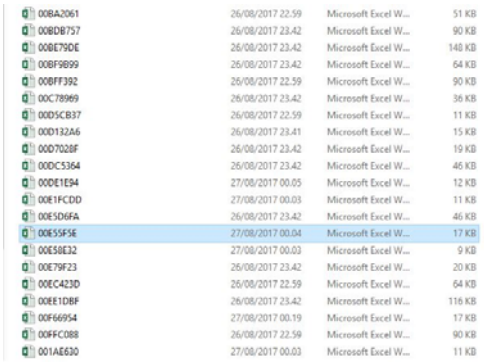

Figure 21. capture of documents found on the suspect's smartphone

We found in investigation a suspicious and protected document like Figure 22:

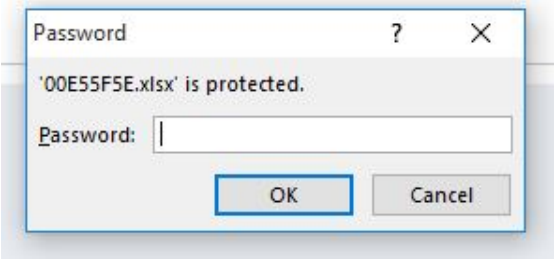

Figure 22. capture of a suspicious and protected document

And result after open protected, found list document like Figure 23:

Figure 23. capture of a document where it listed some donors who are sending fund

4.5. Early Warning System

Early Warning System is an application to map individuals or groups with radical belief which lean towards terrorism. This application contains a database of individuals or groups which had been detected by the police as ISIS sympathizer or had a connection with someone that had become the operational target of the police, here are the view of the *Early Warning System Cyberterrorism* application's *login* page and distributed location of the suspected alternative contacts throughout Indonesia, as in the Figure 24.

Figure 24. capture of EWS login page

Interface or main page for EWS System, like Figure 25 below:

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

Figure 25. Capture of EWS main page

- **EWS Analysis**

From the data above, the researcher determined some criteria as follow:

a. Document criteria which are contacts who send documents whether in the form of doc, xls, pdf or jpeg.
b. Database criteria which are contacts who is not yet within the database of ISIS sympathizer or radical believers whether groups or an individual at Mabes Polri.
c. Frequency criteria which are contacts who has high frequency of communication with the suspect, RS

It is possible to rank the priority of each criterian and alternatives based on pairwise comparison matrixes by using **Eigenvector** concept (Saaty, 1980). As the Table 3 has shown:

Table 3. Eigenvector concept about the criterion comparison

Intensity of Importance	Definition
1	Equal Importance
3	Moderate Importance
5	Strong Importance
7	Very Strong Importance
9	Extreme Importance
2, 4, 6, 8	For compromises between the above
Reciprocals of above	In comparing elements i and j - if i is 3 compared to j - then j is 1/3 compared to i
Rationals	Force consistency Measured values available

Based on the **Eigenvector** concept, the researcher assigns the comparison of the determined criteria, and that Document is of utmost importance, then the existence within the database, and lastly the Frequency of the conversation, as can be seen from the table 4 :

Table 4. Weighing the criteria

NO	CRITERIA	WEIGHT	IMPORTANCE
1	Document	9	Absolute Importance
2	Database	5	Very Important
3	Frequency	3	Important

From the analysis result using AHP as the calculation below

$$\begin{pmatrix} 0{,}190909091 & 0 & 0 \\ 0{,}054545455 & 0 & 0 \\ 0{,}081818182 & 0 & 1 \\ 0{,}581818182 & 0 & 0 \\ 0{,}090909091 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0{,}176470588 \\ 0{,}294117647 \\ 0{,}529411765 \end{pmatrix} = \begin{pmatrix} 0{,}03368984 \\ 0{,}009625668 \\ 0{,}543850267 \\ 0{,}102673797 \\ 0{,}016042781 \end{pmatrix}$$

Then information can be obtained, that ALT 3 gained 1 priority to be further investigated or monitored, just like the Table 5:

Table 5. Result of AHP

NO	ALTERNATIVE	VALUE	RANK
1	ALTERNATIVE 1	0,00336984	3
2	ALTERNATIVE 2	0,009625668	5
3	ALTERNATIVE 3	0,543850267	1
4	ALTERNATIVE 4	0,1026773797	2
5	ALTERNATIVE 5	0,016042781	4

4.6. Report Intelligence Product

This stage is where the making of an intelligence product which illustrated the EWS analysis result to the level of determining new targets is done. The report, in this case, is Specialized Information addressed to Kapolda DIY as an *end user* to be followed up by the other function of the police or the inter-sectoral.

5. CONCLUSION FUTURE WORK

5.1 Conclusion

From the research result of Analysis on Predicting Cyberterorism using the AHP (*Analytical Hierarchy Process*) Method, it can be

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

concluded, Early Warning System can be used to gain new target from on-going case using AHP (*Analytical Hierarchy Process*) method through these steps: determining criteria, weighing which is adjusted to its importance, deciding on alternatives and Based on the test result and analysis on the previous chapter, it is gathered that alternative 3 is the main priority and the new target which is poured into the intelligence product (specialized information).

5.2 Future Work

For the police to increase the IT skill and improving the facilities to ease the work on site in doing prevention or even discovering terrorism act in Indonesia and a good synergy between the function of the police especially in handling Cyberterorrism case, for example the function of Binmas (People's Guidance), Reserse, Densus 88 and Intelligence Function and also people's active support. For Academic Nowadays, terrorism cases are intensively handled by the police. In dealing with before or after the incident, it often used the help of IT, and for that reason the researcher suggests that digital forensics could take a role in handling terrorism or cyberterorism, whether before or after the incident, in an attempt to prevent terrorism and having a good cooperation between the academic and the police side in balancing and developing digital forensics together so there would not be any difference between the theoretical knowledge with the task done during a field operation.

The future researchers the need for Mobile Forensics investigation standard that is combined with Decision Support System in commencing monitoring or developing terrorism cases so future researchers could process the data and gain better and more accurate information.

REFERENCES:

[1] A. Rokhmad, "Islamic Radicalism and Deradicalization Radical Efforts," *Walisongo*, vol. 20, no. 1, pp. 79–114, 2012.

[2] H. Prunckun, "Handbook of Scientific Methods of Inquiry for Intelligence Analysis," no. 2010, p. 249, 2010.

[3] F. Sulianta, "Computer Forensics," 2008.

[4] B. Martini, Q. Do, and K.-K. R. Choo, "Conceptual evidence collection and analysis methodology for Android devices," *Cloud Secur. Ecosyst.*, pp. 285–307, 2015.

[5] K. Curran, A. Robinson, S. Peacocke, and S. Cassidy, "Mobile Phone Forensic Analysis," vol. 2, no. 2, 2010.

[6] M. Agarwal and M. Gupta, "Systematic digital forensic investigation model," … *J. Comput.* …, no. 5, pp. 118– 131, 2011.

[7] L. Usman, Y. Prayudi, and I. Riadi, "Ransomware analysis based on the surface, runtime and static code method," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 11, pp. 2426–2433, 2017.

[8] O. Osho and S. O. Ohida, "Comparative Evaluation of Mobile Forensic Tools," *I.J. Inf. Technol. Comput. Sci. Inf. Technol. Comput. Sci.*, vol. 1, no. 1, pp. 74–83, 2016.

[9] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *Int. J. Comput. Sci. Inf. Technol.*, vol. 3, no. 3, pp. 17–31, 2011.

[10] A. Y. Aljawiy and A. Muklason, "Social Network And User Impact," *Sist. Inf.*, 2014.

[11] D. P. Lestari, " Negative and Positive Impact of Social Network."

[12] Hariani and I. Riadi, "Detection Of Cyberbullying On Social Media Using Data Mining Techniques," *Int. J. Comput. Sci. Inf. Secur.*, vol. 15, no. 3, pp. 244–250, 2017.

[13] N. S. Eko Darmanto, Noor Latifah, "Aplicated Method of AHP (Analythic Hierarchy Process) to Determine Sugar Quality," *J. SIMETRIS*, vol. 5, no. 1, pp. 75–82, 2014.

[14] A. Kurniawan, I. Riadi, and A. Luthfi, "Forensic analysis and prevent of cross site scripting in single victim attack using open web application security project (OWASP) framework," *J. Theor. Appl. Inf. Technol.*, vol. 95, no. 6, pp. 1363–1371, 2017.

[15] C. Beggs and M. Warren, "Safeguarding Australia from Cyber-terrorism : A

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

Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption," 2009.

[16] I. Riadi, J. Eko, A. Ashari, and S. -, "Internet Forensics Framework Based-on Clustering," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 12, pp. 115–123, 2013.

[17] K. Vlachopoulos, E. Magkos, and V. Chrissikopoulos, "A Model for Hybrid Evidence Investigation," *Int. J. Digit. Crime Forensics*, vol. 4, no. 4, pp. 47–62, 2012.

[18] V. L. L. Thing, K. Y. Ng, and E. C. Chang, "Live memory forensics of mobile phones," *Digit. Investig.*, vol. 7, no. SUPPL., 2010.

[19] K. Kepolisian and N. Republik, "No Title," 2010.

[20] T. L. Saaty, T. Analytic, H. Process, and T. L. Saaty, "The Analytic Hierarchy Process," *Education*, pp. 1–11, 1980.