Forensic SIM Card Cloning Using Authentication Algorithm

By Imam Riadi

Forensic SIM Card Cloning Using Authentication Algorithm

Nuril Anwar[1], Imam Riadi[2], Ahmad Luthfi[1]

(Corresponding author: Nuril Anwar)

Islamic University of Indonesia[1]
Jl. Kaliurang KM 14,5 Yogyakarta 55584
Ahmad Dahlan University[2]
Jl. Prof. Dr. Soepomo, S.H. Janturan Yogyakarta 55164, Indonesia
Email: anwar_nuril@yahoo.co.id

(Received Sept. 20, 2015; revised and accepted Jan. 11, 2016)

Abstract

Crime in the telecommunications sector increasingly, especially in the mobile security system found several security flaws of data outside of the network. Clone SIM card is a major problem in the SIM card device. Research cloning SIM card can be presented in the form of analysis algorithms A3 SRES, and A8 RAND to get Ki AUC for the investigation process digital forensic cloning SIM card, testing scheme SIM card cloning used parameter "Due Under Test" (DUT) and "Trial and Error" with the following phases ; identification, preservation, collection, examination, anally and presentation. Conclusion SIM card cloning and analysis in the form of percentage of success then conducted a forensic investigation to cloning SIM card with the matching algorithm A8 (RAND) contained in each SIM card which produces authentication Ki as contained in the investigation file structure SIM card. Memory capacity has advantages and disadvantages, which is 32kb SIM card Ki produced a success rate of 100% success, 64kb SIM card cloning success rate of 25% to 50%. Research cloning SIM card with forensic investigations have been successfully cloned.

Keywords: Authentication, Cloning, Forensic, RAND, SIM card

1 Introduction

This SIM card storing information relating to the network that is used for authentication and user identification. The most important data is the number of identity card (ICCID Integrated Circuit Card ID), the number of international users (IMSI, International Mobile Subscriber Identity), a key authentication (Ki, Authentication Key), area code (LAI, Local Area Identity), and number emergency call operator. SIM card also store numbers for the SMS service center (SMSC, Short Message Service Center), service provider name (SPN Service Provider Name). When the SIM card is oriented as a smart card, it opens the possibility of security that resonate far beyond the world that is mobile [7]. SIM card containing electronic components as well as consist of various sizes as shown in Figure 1.

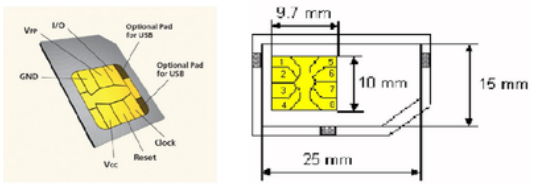

Fig. 1 Model SIM card [12]

(Ki, Authentication Key), a GSM SIM card using cryptography to reduce fraud against the confidentiality of the user. Before it is released to customers SIM card programmed in advance for the purposes to authentication.

Being required to read a special computer algorithm that runs internally on SIM card. KI copy is also stored by the network operator in the Authentication Center (AuC).

SIM card produced on the basis of algorithms COMP128v1, SIM card used now mostly still use in the development of algorithms COMP128v1. COMP128v1 algorithm contained in the coding system which consists of a SIM card GSM algorithms A3 and A8. A3 authentication algorithm is an algorithm in the GSM security model. A3 function is to generate response better known as the SRES in response to the random challenge known as the Random Number Generator (RAND) in other words SRES and RAND are algorithms that are on the network or provide on the network. while the A8 algorithm is an algorithm that serves to generate a session key, Kc or KI in SIM card, by looking at the random challenge, RAND received from the MSC and the secret key Ki contained in the SIM card [13].

COM128v1 has the major advantage that there are two systems of encoding or algorithms A3 and A8, A3 refers to the security of the network is being A8 refers to the security SIM card but on the other hand there is a shortage caused by the algorithm A8 which includes encryption security in the form of Authentication Key (KI) contained in SIM card.

SIM cards are available in various data capacities, from 8 kb to 128 kb however, from various SIM card memory capacity existing generation SIM card 32kb, 64kb and 128kb more in the market. Related SIM card memory usage associated with it play a role in determining the success of cloning SIM card it self more memory contained on the original SIM card then the longer the process of crack Ki A8 algorithm on SIM card.

Problems that arise from the above background related to the presence A8 algorithm embedded in every SIM card used by telecommunication users allowing copying, or cloning SIM card harm either side of the privacy and security of mobile telephone users. The goal of research cloning SIM card this is to give a warning to the security of users and provide dedicated SIM card to handling criminal investigations cloning SIM card along with its misuse of data.

SIM card include Subscriber Authentication Based on IMSI (Stored on SIM) and Random Number Generator/RAND (Provided by Network), it will be investigated further about SIM card cloning authentication by matching the customer's network login response to the mobile service network. Random Number Generator (RAND) contains an algorithm A3 (Provide by Network) so that in the process of cloning SIM card RAND participate in the process of matching algorithms contained on SIM card A8 to A3 algorithms contained on linked network authentication user data.

2 Literature Review

Related research studying the possibility of using the SIM card cloning subscriber identity module (SIM), Universal Mobile Telecommunications System. It also explores how the mobile system can find the SIM card cloning as soon as possible and how to reduce the possibility of using cloning a SIM card in the mobile network. Illegal mobile station is attached to a mobile network can be detected by the location in Area Update, update the location of the area periodically, and by calling out is removed from the original phone. Analytic model was developed to investigate the effects of location area updates and outgoing calls issued by the original phone on illegal cell phone use. Mobility management, such as registration, cancellation, and entry and exit procedures for legal and illegal users will be investigated and analyzed. Analytical models to determine the effect of the arrival of outgoing calls, and regional location of the residence time on detected illegal users have been presented. This study sought to improve the security of communication by avoiding deception of phone cloning by proposing solutions to accelerate the detection of SIM card cloning [8].

Mobile computing and mobile commerce are the most popular now days because of the services offered for mobility. Mobile computing has become a reality today than the wireless market. Mobile is rapidly increasing. Quality and speed available in the mobile environment must be in accordance with the fixed network if network convergence of fixed and mobile wireless communication occurs in the rea sense. The challenge for mobile network located within a very large footprint providing mobile service with high speed and security. Online transactions using mobile devices must ensure high security for user credentials and possibly to abuse. M-Commerce is the electronic trading is done by using a mobile device. Since a user's credentials to be kept secret, a high level of security must be ensured [9].

Exploration of digital evidence on SIM card scheme case of SIM card cloning in this case to find out more about the characteristics of the data and the digital evidence to the SIM card, imaging techniques, collecting and analyzing data, as well as exploration SIM card and investigative efforts SIM card in general [10].

Studies and Comparative Security GSM and CDMA GSM security system based on the exchange of data between the HLR (Home Location Register) with the SIM card in the MS (Mobile Station) RAND, MSC to the BTS and then MS. Ki and Kc is used to encrypt messages between base stations with MS. RAND, SRES Authentication in GSM is using A3 algorithm with a key Ki with the method Challenge and Response. Authentication using unique challenge procedure [4].

Analysis clone SIM card on IM3 smart and use Elliptic Curve Cryptosystem, this research cloning SIM card and

cryptographic methods to analyze the combination of ECC (Elliptic Curve Cryptography) algorithms A3, A5 and A8 to get quality better security. It was found that the method can only be combined with the ECC algorithms A3 and A8 as well as the ECC method was not effective when combined with the algorithm A5 is due to differences between the two systems and procedures [5].

Forensic Software Tools for Cell Phone Subscriber Identity Module forensic specialists in making appropriate and inspection data. For the Global System for Mobile Communications (GSM), This paper gives an overview of the state of forensic software for SIM card. Forensic examination tool translating the data into a format and structure that can be understood by the examiner in identifying and recovering digital evidence with advantages and disadvantages [13].

Forensics and the GSM mobile telephone system Senior Investigator, this paper briefly describes the basics of the GSM system. The items of evidence that can be obtained from the Mobile Equipment, SIM and explored the core network to develop better forensic procedures. GSM SIM card conclusion that imitation is indeed possible for anyone who could. Forensic analysis methods are still physical contact with a mobile phone to access the stored information [13].

Validating Tools for Cell Phone Forensics This paper presents preliminary research in creating a basis for testing forensic tools and observed that some phones with information stored in the subscriber identity in the SIM card exactly in store logs on a T-Mobile SIM card standard SIM standard T-Mobile locked, it is still possible changes and modifications related to data protection [2].

Analysis SIM card Cloning With Algorithm Random Number Generator. This study discusses cloning SIM card along with stages ranging from crack SIM card cloning testing stage along with further analyze the effects of cloning media are bought and sold freely. Conclusions of research in the form of analysis SIM card after cloned and a series of early stage research and will be further examined for forensic investigation SIM card cloning research [1].

In this study focused on cloning SIM card forensic authentication algorithm using a random number generator (RAND). Forensic investigations against cloning and SIM card original with matching algorithms A3 and A8 to get Authentication Key (KI) in SIM card. Results are expected to be a description of the process of forensic investigation related to cloning SIM card authentication and authentication algorithm analysis Random Number Generator (RAND).

3 Research Methods

The subjects of this research is focused on authentication SIM card to stage cloning for further development of forensic investigation with SIM card cloning as evidence. The process of investigation will be conducted at the Laboratory of IT Centrum Islamic University of Indonesia, which is part of the Center for the Study of Digital Forensics. Related research methods to analyze forensic SIM card based on the theory that the focus of research in accordance with the facts related field evidence handling cloning SIM card for further analysis to prove that the hypotheses raised in accordance with the criteria. The final stage of the analysis of the study will be presented influence cloning SIM card, SIM card log cloning based clones with original SIM card log. Analysis of the research include:

- Attack and scenario testing;
- Design and cloning SIM card forensic proposal;
- Testing cloning SIM card;
- RAND Authentication;
- Forensic Analysis SIM card cloning.

3.1 Attack and Scenario Testing

Scenario testing is emphasized in the process of cloning of SIM card cloning it self include the success of the process generate authentication key (Ki) RAND A8 towards SIM card original and then tested the response A3 SRES to the network when SIM card cloning direct contact with SIM card original while attack scenarios attack inflicted post SIM card cloned in the form of attacks or duplication of such communication access short messages (SMS), call and access the data from SIM card cloning as if there is the same number as the original SIM card further here in after known effects [11]. Flowchart SIM card cloning attack shown in Figure 2.

3.2 Design and Cloning SIM Card Forensic Proposal

Based on forensic proposal SIM card cloning in Figure 3 above it can be concluded that the design refers to the RAND topic as the subject of research with the authentication key Ki as a sub topic of research.

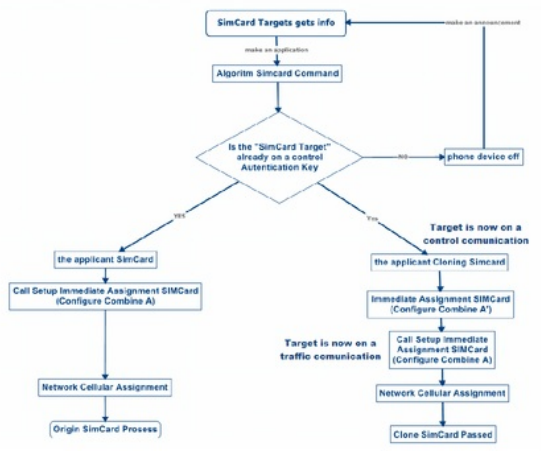

Fig. 2 Flowchart Attack SIM card Cloning

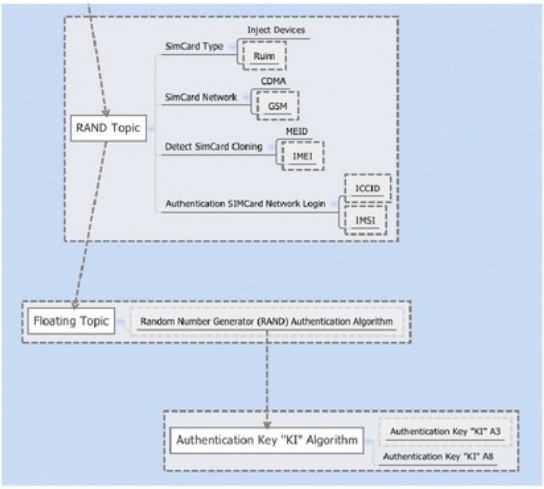

Fig. 3 Forensic Proposal SIM card Cloning

3.3 Testing Cloning SIM card

Authentication Cloning SIM card in scenario testing refers to authentication key (Referred to as Ki SIM card GSM), which consists of IMSI and ESN number, the test trial-and-error, giving input different SIM card and observe responses of both SIM card both include:

- Response to post providers network SIM card cloned;
- Accumulate between RAND and the authentication response SRES;
- The possibility of modifying the RAND algorithm or simply distribute authentication Ki to the media cloning;
- The effect of traffic from mobile users to the base station SIM card has been cloned to the original SIM card.

3.4 RAND Authentication

Another important aspect is the strength of the GSM authentication algorithm SIM card or often called A3. In principle, A3 owned by certain mobile operators, but the use of inter-operator algorithms tend to be the same. The statement further from the two algorithms in comparison RAND and SRES Authentication based on GSM security. If Ki can be extracted from the SIM, the user will be able to make a duplicate driver's license. Algorithms A3 and A8 determine the input (RAND and Ki) and output (SRES and Kc) of each algorithm [6].

3.5 Forensic Analysis SIM card Cloning

SIM card is a smart card, which contains a processor and non-volatile memory. In GSM, a SIM card which is used as a data storage device customers. The sole purpose of this procedure is to apply the mechanism of access and security features. The SIM card can be accessed by mounting the card the reader with the smart card reader whereas the standard required to access the software as a card reader or access SIM card. SIM card consisting of structures containing binary data file. Best forensic procedures will overview the entire contents is to download the entire SIM memory and compute the hash value memory is often called the acquisition of evidence, were to do this it takes forensic tools to access the file [3].

4 Results and Discussion

4.1 Analysis SIM Card Cloning

Ability SIM card cloner counter market is extremely diverse and has the advantage of each other, but from a variety of power applications has generated Ki cover or scan generated different. The percentage success rate of cloning SIM card consists of variables including mobile operators, generation, application cloner and SIM card memory capacity can be presented in Table. 1

Table 1: The success percentage cloning SIM card

No	Provider Name	Gen.1st	Gen.2nd	Gen.3th
		Before 2011	2011 2014	2015 - Now
1.	Telkomsel	100%	100%	100%
2.	Indosat	100%	50%	0%
3.	XL	100%	25%	0%
4.	3	-	25%	-
Memory		32kb	64kb	128kb
Signal Coverage		1G	2G/3G	3G/4G

Inter-generation SIM card obtained from the sample between the users SIM card to register early for the network is divided into classifications include:

- 1st Generation = Before the year 2011;
- 2nd Generation = Between the years 2011-2014;
- 3rd Generation = After 2015 Now.

Based on the list of tables SIM card along with the providers and the application of cloning that accompanies it can be concluded while that object and focus SIM card cloning taken SIM card with a provider "Telkomsel" on the grounds of the generation SIM card most still use generation 1st and all 2nd which allows cloning SIM card with generated relatively short time compared to other providers, assuming the less memory is embedded in the SIM card allows the crack / authentication generated key that is relatively short. Powered by multiple applications SIM card cloner after test-generated Ki that SIM card with mobile operators "Telkomsel" assessed tend to be quicker to obtain the crack of authentication key Ki.

Here is a comparison between algorithms which emphasized the role of RAND and SRES algorithms, the algorithms are interconnections where A8 RAND in contact with A3 AUC SIM card Network so as to obtain the process flow as shown in Figure 4.

Formation of cloning SIM card to put the results of the algorithm generated Ki A8 of the original to be copied to the device subsequent cloning SIM card write with certain specifications that can serve the same cloning SIM card when making contact with the communications network. From the figure above it can be stated that Ki1, A31 and A81 are similar to variable SIM card original, then the cloning process is forwarded to the mobile station network or SRES Authentication act as authentication of customer data provider, if the data contained on the device SIM card (Ki and Random Number Generator) is considered matched with the central database will be given access to communications. Formation of cloning as shown in Figure. 5

Based on the formation and flow of the process of RAND and SRES can be concluded that the role of algorithms. RAND and SRES in this case is that the RAND as an algorithm of random formation of Ki authentication key and play a role in the authentication process of post SIM card performed the cloning was the role of algorithms SRES as challenge response to a

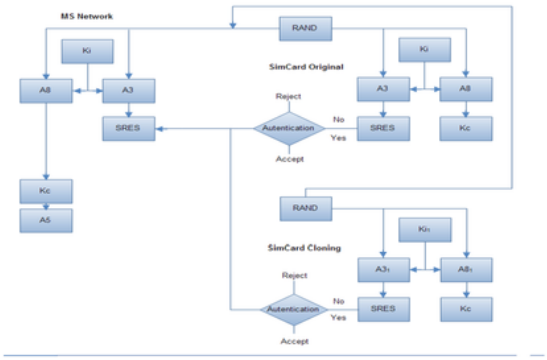

Fig. 4 RAND and SRES Cloning

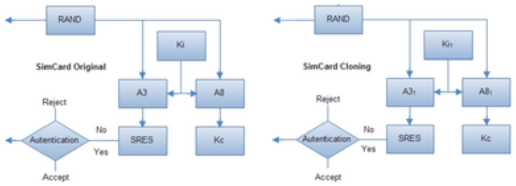

Fig. 5 Formation of Cloning

4.2 Forensic SIM Card Cloning

The next stage after the SIM card cloning is analyzed by algorithms auentikasi random number generator will be studied further forensic investigations related to cloning SIM card that will be on the exploration of the data contained in the findings of SIM card. Stages forensic SIM card cloning refers to the table network of contacts and response when there is more than one SIM card have a common authentication key Ki. SRES algorithm in this case in particular for the benefit of forensic investigations can not be explored by the analysis device SIM card because the algorithms contained in the communication service provider (provide by the network).

Investigative Process for Digital Forensic Science (DFRWS) technical report further adapted to the handling of evidence obtained by cloning SIM card table refer investigations to stage SIM card handling device as shown in Table. 2.

Based on the stage table above is obtained stages more emphasis on research related to the investigation of evidence SIM card that stage of examination will be conducted data acquisition, investigations, from the exploration of evidence with stages examination described above, can then be obtained data findings can combined until eventually the data findings goods evidence can be presented in table form table classification as a test case as shown in Table. 3:

Results of comparative investigation of data can be argued that the acquisition of evidence in the form of analysis and its SIM card can be obtained using forensic software and the conclusion is valid in accordance with the original SIM card which is owned by the victim.

4.3 Discussion

The discussion on the SIM card cloning and analysis of variables that can affect the success rate of cloning and consists of

- Generation SIM card
  SIM card generational differences can affect the success rate in cloning SIM card actors, that the SIM card with 1st generation and 2nd generation was the one that lets done authentication crack or generated key.

- Memory SIM card
  The memory is pinned by the provider of the service provider to each provider based generation also affects

Table 2: SIM card Investigation Process Cloning

Indentification	Preservation	Collection	Examination	Analyst	Presentation
Identification of crime simcard	Processing cases simcard	Securing evidence simcard	Tracking the evidence simcard	Data comparative investigation	Documentation
Profile crime simcard	Chain of custody / chronological simcard cloning	Simcard investigative techniques	Validation of evidence simcard	Processing of finding evidence	Clarification investigator
Audit and analysis of case	Time management investigation		Filtering evidence		Statements, advice and action
	Processing cases simcard		Matching evidence		Simcard data interpretation
			The discovery of hidden data		

Table. 3 Test Case Result (Forensics Tools)

Testing Test	Scenario Expected	Results Testing	Results	Conclusion
Simcard acquisition and analysis	Scan device simcard cloning (Ki generate)	Exploration & repport	Magic SIM 16 in 1 SMSP : 62811000000 ICCID : 8962101xxxxxxx IMSI : 0859010 xxxxxxxx Ki : 9A1154814652D3 2339360947A69986C4	Ki and his identity was found identical simcard
Forensics investigation	HLR Lookup	(Digital Evidence) Simcard Cloning	Shlrlookup : 08529260xx Operator : Service providers (Telkomsel)-KartuHalo/Simpati/ KartuAs HLR : Yogyakarta/Indonesia	Found home local registers in accordance with the original simcard
	Acquisition Evidence		MD5 Checksum : BA0A76666C8F1375E8D87BBAC21E A9F9 SHA1 Checksum : 87D74A0F18C2E9430AC9473D62A410 6547878B1E	The acquisition process extraction file evidence
	File Structure Evidence		Slot : 1.f f f f f f f f f 9A1154814652D3233936 0947A6999986C4 f f f f f f f f f f f f	Akey findings on clone sim slot

related literacy cloning application, the greater the SIM card memory ranging from 32kb, 64kb to 128kb latter will affect the reading process and Ki crack at the target SIM card cloning.

The next stage after that SIM card analysis of forensic investigation phase to the final destination in the form of a series of stages evidence handling cloning SIM card along with the findings contained or hidden in

order to represent data. Based on the research include analysis of forensic SIM card cloning and cloning it can get the gist of related research SIM card. That the motives that made the perpetrator in committing of crimes targeting SIM card cloning is copying the data on devices SIM card in the form of results generated authentication key (Ki) henceforth be copied to media SIM card cloner that can be acquired or traded on the market freely and where actors can clone SIM card then can certainly add to the long list of motives of crime, especially mobile phone, while the results of forensic investigation SIM card cloning to explore the evidence can be found the file structure of a SIM card cloning containing partially identical data such as authentication key (Ki) obtained during generates a random number on the device SIM card along with data cloning victims. From the discussion above may be obtained several sub discussion include:

- Research Focus
  Forensics SIM card along with analysis is the focus of this study refers to the SIM card cloning scheme further testing scenario SIM card combine against cloning according to research methods. Based on the scenario and the process can be obtained SIM card cloning research focus as in Figure. 6

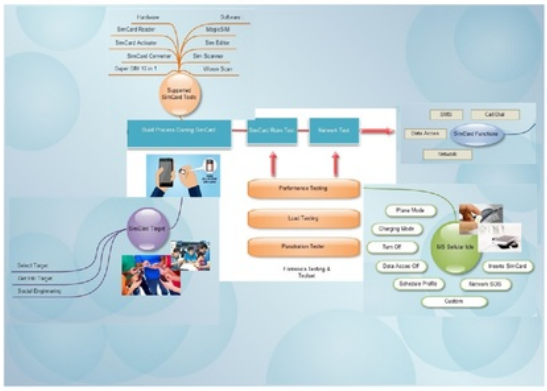

Fig 6: Focus SIM card Research Cloning

- Resume Research
  Based on the results and discussion of research related to the presence of SIM card and has been analyzed along with the working principles of cloning on SIM card subsequently conducted the investigation based on the stage of the investigation SIM card cloning which is emphasized in the process of examination of evidence SIM card to obtain detailed findings of digital evidence from the SIM card, then the results can be obtained and verification as in Table 4:

The next stage after that SIM card analysis of forensic investigation phase to the final destination in the form of a series of stages evidence handling cloning SIM card along with the findings contained or hidden in order to represent data.

The results of forensic investigation SIM card cloning to explore the evidence can be found of the file structure that contains a SIM card cloning partially identical data such as authentication key (Ki) obtained during a random number generated on the device along with the SIM card data cloning victims. The file structure attached to both SIM card original or cloning has similar characteristics but in the interests of the investigation needed further examination to be able to distinguish the characteristics of the file system of each SIM card. Classification of the file structure along with the sub file system can be seen in Figure. 7

The file structure that consists of a:

- Master File (MF),
- Directory File (DF) and
- Elementary File (EF),

Each component sub-system has file different capacity. In the interest of forensic investigations related evidence cloning SIM card will be differentiated based hierarchical file system for combined and match against the original SIM card. SIM card with each provider both 1st generation, 2nd and 3rd with different memory capacity when done scanning the file system will obtain the same file hierarchy. Comparison between the original SIM card and SIM card cloning discovered that differentiate file system that is contained in the file system:

- Elementary file (EF)

Table 4: Resume SIM card Research Cloning

Testing Test	Scenario Expected	Results Testing	Results	Conclusion
SIM card Acquisition and Analysis	SimCard Origin Telkomsel/AS	Synonymous with genuine SIM card (RAND, Ki)	Sim Number 085292608008 ICCID 89621019924260800080F IMSI 085901012924060880 Ki(A) Origin 9A1154814652D32339360947A69986C4 Ki(A') MagisSim 16 in 1 9A1154814652D32339360947A69986C4	Valid
	Scan device SIM card cloning (Ki generate)	Exploration & Report (Digital Evidenc) SIM card Cloning	Magic SIM 16 in 1 SMSP: 62811000000 ICCID: 8962101xxxxxxxxx IMSI: 0859010 xxxxxxxxxx Ki: 9A1154814652D32339360947A69986C4	Valid
	HLR Lookup		$hlrlookup: 08529260xxxx Operator: Service providers (Telkomsel) - KartuHalo/Simpati/ KartuAs, HLR: Yogyakarta/Indonesia	Valid
	Acquisition Evidence			Valid
			MD5 Checksum: BA0A76666C8F1375-E8D87BBAC21EA9F9	Valid
	File Structure Evidence		SHA1 Checksum: 87D74A0F18C2E943 0AC9473D62A41065 47878B1E Slot: 1.ffffffff9A1154814 652D32339360947 A69986C4ffffffff 2.Last Dial Number +6221500046 3.Phone Book Copy 0163827648 4.Pesan Text: Status: Read From: +6285105870607	Valid Valid Valid Valid

– Elementary File (EF_Ki)

Elementary file (EF) with sub-system Elementary File (EF_Ki), with a storage slot containing EF_Ki Ki according to media cloning SIM card capability.

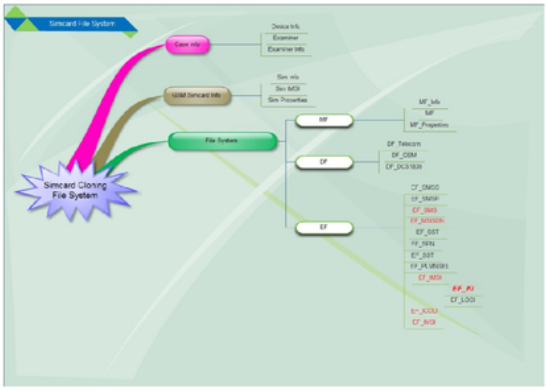

Fig. 7 File System SIM card

5 Conclusion

The process of matching algorithm or Random Generator / RAND against SIM card cloning in this research is to produce a RAND algorithm called A8 or SIM card cloning Ki to the media. Analysis SIM card cloning able to provide early warning for communications service, and can provide knowledge to the user (end user) in maintaining the security of mobile devices. SIM card generation in this case consists of generation 1st , 2nd , and 3rd respectively with memory capacity between 32kb, 64kb and 128kb. After Ki generated between generations conclude that the only SIM card with generation 1st, 2nd generation 32kb and 64kb able to perform the cloning and cloner applications that are sold freely in the latest. Newes generation SIM card with Ki can not be generated due to the limitation to read and scan Ki with larger memory , Random Number Generator (RAND) A8 and Sign Response (SRES) A3 participate in the process of forensic SIM card cloning. RAND to authenticate against Ki contained in SIM card while SRES act on network authentication network (mobile station). Both algorithms intertwined when it comes in contact SIM card to mobile networks. Forensic investigation SIM card cloning refers to the process table investigation published by the Digital Forensics Research Conference which emphasizes on the stage of the examination process. SIM card evidence of the exploration process of cloning can be concluded that matching or authentication algorithm A8-based Random Number Generator (RAND) is very helpful in the investigation related to the presence of cloning SIM card. The process of matching algorithm Random Number Generator (RAND) on cloning SIM card can be used as a step acquisition of evidence related to the SIM card cloning.

Contribution related forensic investigators SIM card cloning using a random number generator algorithm is to contribute to the analysis of SIM card cloning and its impact, further investigation and exploration forensic evidence SIM card cloning to be matched between a data SIM card cloning of the original SIM card.

6 Acknowledgments

This study was supported by the Laboratory of IT Centrum Indonesian Islamic University under Centre for the Study of Digital Forensics. The authors gratefully acknowledge the Reviewers for reviews their valuable comments.

References

[1] N. Anwar, I. Riadi, A. Luthfi, "Analysis SIM card Cloning With Algorithm Random Number Generator", *Jurnal Buana Informatika*, vol. 7, no. 2, pp. 143–150, April 2016.

[2] N. Bhadsavle, J. A. Wang, "Validating Tools for Cell Phone Forensics", in *Southeast Section Conference*, South Marietta Parkway: ASEE Southern Polytechnic State University, 2009.

[3] G. Palmer, "A Road Map for Digital Forensic Research", Technical Report DTR-T001-01, Digital Forensic Research Workshop (DFRWS 2001), Nov. 2001.

[4] M. F. Fauzan, "Studies and Comparative Security GSM and CDMA", Informatics Engineering Program, Bandung Institute of Technology, 2013.

[5] C. Hayat, "Analysis of the Clone In IM3 SIM card Smart And Use Ellptic Curve Cryptosystem To Improve Network Security GSM", Depok, Indonesia: Department of Information Systems, University Gunadarma, 2004.

[6] M. Isomaki, "The relationship between GSM security paramenters and functions", Security in the Traditional Telecommunications Networks and in the Internet, Nov. 1999.
[7] W. Jansen, R. Ayers, "Forensic Software Tools For Cell Phone Subcriber Identity Modules", in *Procedings of the Conference on Digital Forensics, Security and Law*, pp. 93-106, 2006.
[8] M. A. Al-Fayoumi, F. Nidal, "Cloning SIM cards usability reduction in mobile networks", *Journal of Network and Systems Management*, vol. 22, no. 2, pp. 259–279, Apr. 2014.
[9] K. Prakash and Balachandra, "Security issues and challenges in mobile computing and M-commerce", *International Journal of Computer Science & Engineering Survey*, vol. 6, no. 2, pp. 29–45, Apr. 2015.
[10] Y. Prayudi, F. Rifandi, *Digital Evidence on SIMCard Exploration*, Digital Forensika Study Center, SESINDO FTI Islamic University of Indonesia, Dec. 2013.
[11] D. P. Tomcsanyi, "The big GSM write-up, how to capture, analyze and crack GSM", Oct. 13, 2013. (`https://domonkos.tomcsanyi.net/?p=418`)
[12] C. Velazco, *SIM Card Maker Gemalto Investigates Spy Agencies' Hack Attack*, May 2016. (`http://www.engadget.com/2015/02/20/gemalto-investigates-spy-hacks/`)
[13] S. M. Willassen, "Forensics and the GSM mobile telephone system", *International Journal of Digital Evidence Spring*, vol. 2, no. 1, pp. 1–7, 2003.

Nuril Anwar earned a BA from the Department of Informatics, University of Ahmad Dahlan (UAD) in 2012 and he is currently studying a Master of Computer Science with Digital Forensic interest of Megister Department of Information Engineering, Islamic University of Indonesia (UII). Email: `anwar_nuril@yahoo.co.id`.

Imam Riadi earned his Doctoral Program from the Department of Computer Science, University of Gadjah Mada (UGM) in 2014. Currently he is a lecturer at Ahmad Dahlan University (UAD) with interest in Network Engineering with concentration and interest in Internet Forensics. Email: `imam.riadi@is.uad.ac.id`.

Ahmad Luthfi He has got a Master of Computer Science from the Department of Computer Science, University of Gadjah Mada (UGM) in 2005. Today, He is staff and lecturer at Islamic University of Indonesia (UII) with concentration and interest in Mobile Forensics. Email: `ahmad.luthfi@uii.ac.id`.

Forensic SIM Card Cloning Using Authentication Algorithm

ORIGINALITY REPORT

3%

SIMILARITY INDEX

PRIMARY SOURCES

1	jiuvalley.info Internet	60 words — 1%
2	eprints.manipal.edu Internet	38 words — 1%
3	www.acm.org Internet	23 words — < 1%
4	files.spogel.com Internet	11 words — < 1%
5	Singh, Ramesh, Preeti Bhargava, and Samta Kain. "Cell phone cloning : a perspective on GSM security", Ubiquity, 2007. Crossref	6 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		