Radio Cellular Forensics Analysis: Where is the Adversary?

Muhammad Dzakwan Falih, Student Member, IEEE, Gandeva Bayu Satrya, Member, IEEE
School of Applied Science, Telkom University, Republic of Indonesia
dzakwan@ieee.org, *gbs@telkomuniversity.ac.id

Abstract—The evolution of mobile cellular communication has been growing rapidly from 1G to 4G. Unfortunately, with this technology comes an increasing risk of cellular cybercrime. This research proposed a novel methodology to reveal the cybercrime adversary’s location by using radio cellular forensics. Several tests were conducted to validate the proposed methodology. This research also presented the digital evidence in a forensically sound manner to support the forensics investigators. Finally, it is concluded that the proposed methodology can be used as a reference for investigators, analysts, and police in cybercrime cases.

Index Terms—Cellular forensics, cybercrime, adversary, digital evidence, location.

I. INTRODUCTION

Cellular network uses basic RF (Radio Frequency) transmission principles on its communication method [1]. The rapid evolution of cellular network from 1G to 4G is due to its user’s demand for better Quality of Service (QoS) as well as Quality of Experience (QoE). Mobile phone network consists of many radio ‘cells’, each of which covers a limited geographical area. Each cell is assigned a unique ‘Cell ID’, which is captured in the Call Detail Record (CDR) when calls are made. Cell site analysis attempts to provide evidence of where a mobile phone may have been located when certain significant calls were made.

The fastest growing field in the telecommunication industry is cellular technology. Day by day, the cellular network providers and vendors are upgrading their network coverage, network capacity, and network quality in order to fulfill requirements of users or mobile subscribers (MSs) [2]. On the other hand, the evolution of cellular network system also leads to the increasing numbers of cybercrime, cyberterrorism, and cyberwarfare. Some of the initiatives to tackle cybercrime that have been released by the Interpol [3] i.e. operational and investigative support, cyber intelligence and analysis, digital forensics, innovation and research, capacity building, and national cyber reviews.

This experiment used original records from actual cellular forensics, so the correlated number and personal data are blurred to protect the anonymity of the adversary. Fig. 1 illustrates the preliminary phase before going further into the investigation. Initially, the investigator does not know which cellular network operator and cell sector used by the adversary. In this illustration, each color represents one cellular network operator. This problem was opted to point the criminal investigation at the right direction and to prove or contradict the allegation. The contributions of this research are as follows:

- Proposing a novel methodology for supporting cellular radio forensics in finding the location of the adversary.
- Providing effective and accurate phases of investigation to be used in 2G, 3G, and 4G cellular network technology.
- Presenting guidance for investigator, analyst, and cyber-law enforcement that is acceptable in court.

Fig. 1. Finding user equipments within several operator networks

II. LITERATURE REVIEW

Hoy defined three reasons that are usually undertaken in radio forensics surveys [1]. First, to determine the set of cells that cover a certain location. Second, to ascertain the extent of serving coverage of a cell. Last, to determine the serving coverage of a set of cells on a given route. He stated that cell site analysis (or cell tower tracking) attempts to provide evidence of the location of a mobile phone when certain calls were made.

Proc. of the 2019 IEEE International Conference on Signal and Image Processing Applications (IEEE ICSIPA 2019), Malaysia, September 17-19, 2019
Minor’s research project resulted in the creation of a method for validating the accuracy of cellular carrier records and mitigating errors in forensic cell site analyst’s conclusions [4]. The process establishes a scientific foundation critical to satisfying key of Daubert requirements. This study determined the significance of validating the CDR evidences. Several specialty software tools imply to produce accurate analysis results, but none of the software tools currently perform the discovered evidence validation and analysis error mitigation methodology. This research concluded that none of the software tools can execute the validation of discovered evidence and analysis error mitigation methodology.

Zhuang et al. designed FBsleuth, an fake base station (FBS) crime forensics framework employing “radio frequency (RF) fingerprints”, i.e., the unique characteristics of the FBS transmitters embedded in the electromagnetic signals [5]. Essentially, such fingerprints were obtained from the imperfections in hardware manufacturing therefore it represents a consistent bond between an individual FBS device and its committed crime. The RF fingerprint were modeled from subtle variance of the modulation errors, instantaneous frequency, and phases of the RF signals. However, the experiments were limited on only using FBsleuth and scanning in RF with different working frequency points.

Dabrowski et al. evaluated the system that is detecting International Mobile Subscriber Identity (IMSI) catcher by using lab tests as well as field tests [6]. For the lab tests, they used an USRP1 based IMSI Catcher running OpenBTS 2.6 on identification mode. Therefore, they patched OpenBTS to download the IMEI and IMSI of certain smartphone and then reject the Location Update request - pushing the smartphone back into the genuine network. Because of their brief interaction with the smartphone, such IMSI Catchers are particularly hard to detect. Their experiments were concluded in a controlled environment so as to not interfere with outside smartphone. There were still many limitations on their research, e.g. static mobile network structure, no decoding the broadcast and control channels, showing only using Google Maps, etc.

### III. Cellular Forensics Methodology

#### A. System Model

Based on the author’s real experiment, system design of the radio cellular forensics is illustrated in Fig. 2. Assuming that the investigator does not know at all the position and operator used by the adversary except for the MS number. With the help and permission of the Police of Republic of Indonesia, the cellular radio forensics were legally carried out to pinpoint the real location of the adversary. Using cellular network communication protocol analysis can help in finding the exact position of the adversary e.g. Broadcast Control Channel (BCCH), Paging Control Channel (PCCH), Common Control Channel (CCCH), and Dedicated Control Channel (DCCH). The equipment used by the investigator in this research were Laptop with Ubuntu 16.04 OS, Nexus 5 smartphone, Signaling Collection and Analysis Tool (SCAT), CellMapper, NetMonitor Cell Signal Logging v1.53, Google Maps, and Wireshark v2.6.7.

#### B. Proposed Methodology

With the respect to previous researchers [7]–[9], a novel methodology for cellular forensics is proposed. The methodology consists of two parts which are passive mode and active mode. This research only focuses on passive mode, while the active mode is currently in development process for further work. The processes that have been made for cellular forensics analysis encompasses five phases as depicted in Fig. 3.
1) Preparation: The investigator should ensure that the preparation phase includes considerations for any organization’s specific requirements related to retaining, extracting, or maintaining evidence and the necessary warrants for search and seizure. Looking up the MS integrated services digital network Number (MSISDN) is the important factor in preparation phase. MSISDN is a series of numbers uniquely identifying a subscription in a global system mobile (GSM) or universal mobile telecommunications service (UMTS) or long-term evolution (LTE) mobile networks [10].

2) Plotting and survey: By using location-based services (LBS), the investigator could recognize the device’s geographical location. The investigator should make sure the tools used in plotting and survey are in such a manner to be acceptable in court [11]. For more convincing digital evidences, the investigator needs to scan and tap into the adversary’s channel to reveal the accurate location of the adversary.

3) Scanning and tapping: For a successful radio forensics, an understanding of 2G/3G/4G cellular network systems is essential. In this process, the investigator must be able to know the base station or node-b parameters. Accurate and efficient scanning and tapping have become vital requirements in radio forensics. From the best of authors’ knowledge, doing the scanning and tapping at night is preferable to increase the probability of finding the cell_id of the adversary due to uncrowded network.

4) Analysis: In the analysis phase, the investigator can connect the clues and draw a complete picture from plotting, scanning, and tapping phases. Proper analysis along with knowledge about telecommunication protocol are written as analysis result list. The analysis result list describes all the meaningful information that answers who, what, when, where, how, and other questions.

5) Presentation: The observation results deduced from analysis processes must be organized into an actual report for the court room or expert witnesses. The actual report must be qualified and credible in the court of cyberlaw. Reporting is also important because the entire cellular forensic phases is only worth as much as the information’s investigator convey to the cyberlaw.

IV. RESULTS AND DISCUSSION

Based on the proposed methodology, the scenario conducted in this research is illustrated in Fig. 2. Below are the results and discussion for each phase.

A. Experiment Results

1) Preparation: The main requirement is to connect to a cellular network using a SIM card. Everyone connected to the cellular network has at least one SIM card, as the identity and authentication used to connect to the operator network. In the operator’s side, IMSI is used as a login account for the user, which is stored in the Authentication Center (AuC). In terms of mobile communication network, user’s data is stored in the home location register (HLR) or visitor location register (VLR).

In obtaining MSISDN data as shown in Fig. 4, the investigator utilized assistance from the Indonesian National Police specifically the cybercrime section. With respect to the cyberlaw, these digital evidences were presented to help identifying adversary in a cybercrime or in this case. Before conducting an investigation, the MSISDN number of the adversary must be known first. In this research’s real scenario, the information of the MSISDN was acquired from the Police and the MSISDN number 6281938227366 is the target.

2) Plotting and survey: However, the MSISDN number from the HLR/VLR database is not enough to find the adversary because of low accuracy of the location obtained. It was found that the actual location could be far away from the position checked on the HLR/VLR. Hence, further analysis is needed to ensure a valid user position as can be seen in Fig. 5, 6, and 7.
3) Scanning and tapping: The data needed from telecommunications operator is a map of the base station of said operator. In this research, data can be found from open sources such as Net Monitor (Fig. 8) and CellMapper. Some information that can be obtained from this phase are MNC (operator code), LAC (location area code), network type (2G, 3G, 4G), protocols (Fig. 9), and cell coordinate.

4) Analysis: By using Table I, cell_id target and BTS (or node-B) were analyzed. If the MS was still connected to cellular network (in this case is WCDMA networks), then the investigator can identify and analyze the protocol from paging request which can be correlated with the adversary’s IMSI. Hence, based on Table 1, the location of the adversary can be diminished to 550m area. The data and formula adopted to get these details, i.e., time propagation (TP) or time advance (TA) referred to [12].

5) Presentation: Each digital evidence that has been analyzed was then finalized to be more acceptable in court. This research was conducted by using three cellular network technologies which were the 2G, 3G, and 4G cellular networks with unique digital evidences. Furthermore, the report for summary of findings are shown in Appendix A.

B. Discussion

To ensure that the proposed methodology can be implemented in 2G, 3G, and 4G cellular networks, each phase was repeated from the beginning to the end to all of those cellular networks. In each 2G, 3G, and 4G cellular networks, each phase from the preparation to the plotting and survey produced almost the same result. However, the scanning and validation phase showed a different output: GSMTAP was found in 2G network, RRC was found in 3G network, and LTE-RRC was found in 4G network. While for analysis phase, the information and formula used were derived from Table I.

V. Conclusion

Based on the experiment in 2G, 3G, and 4G cellular network systems, it has proven that the proposed methodology works in every cellular network. This research also showed the digital evidences sequentially and in acceptable manner on the cybercrime court. The novel methodology can also be adapted by investigator, analyst, and others organization which has a cybercrime department for investigating cybercrime cases in finding the exact location of the adversary. Furthermore, the extension of this research is still in development phase which will propose a methodology for the cellular forensics in active mode instead of passive mode.
ACKNOWLEDGMENT

This research was supported by Reverse Manggo RG, School of Applied Science, Telkom University. The authors also wish to thank the person who does not want to be named for their technical support and provision in this research.

REFERENCES

APPENDIX A
SUMMARY OF FINDINGS

This adversary was suspected of being engaged in cybercrime and cyberterrorism. The aid of radio cellular forensics along with legal authorities was employed by "GBS & MDF Inc." in the investigation in order to exonerate or convict the accused (adversary). Based on the proposed methodology, the investigation was executed while the adversary is doing the paging and calling at his/her area.

To conduct an effective and efficient investigation, tools utilized in this research were a Laptop with Ubuntu 16.04 OS, Nexus 5 smartphone, Signaling Collection and Analysis Tool (SCAT), CellMapper, NetMonitor Cell Signal Logging v1.53, Google Maps, and Wireshark v2.6.7 to survey and detect the adversary’s location.

Based on the authors’ knowledge of radio cellular forensics, the example of summary of finding is shown in Table II.

### TABLE II
REPORT OF RADIO CELLULAR ANALYSIS

<table>
<thead>
<tr>
<th>TAG#</th>
<th>PROTOCOL</th>
<th>INFORMATION</th>
<th>LENGTH (bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>GSMTAP</td>
<td>GSM CCCH - System Information Type 3</td>
<td>93</td>
</tr>
<tr>
<td>02</td>
<td>GSMTAP</td>
<td>GSM CCCH - Immediate Assignment</td>
<td>93</td>
</tr>
<tr>
<td>03</td>
<td>RRC</td>
<td>cellUpdateConfirm</td>
<td>229</td>
</tr>
<tr>
<td>04</td>
<td>GSMTAP</td>
<td>GSM A-I/F DTAP - Location Updating Request</td>
<td>90</td>
</tr>
<tr>
<td>05</td>
<td>GSMTAP</td>
<td>GSM A-I/F DTAP - Identity Response</td>
<td>81</td>
</tr>
<tr>
<td>06</td>
<td>LTE RRC DL_DCCH</td>
<td>rrcConnectionRelease</td>
<td>1253</td>
</tr>
<tr>
<td>07</td>
<td>LTE RRC PCCH</td>
<td>Paging Record</td>
<td>77</td>
</tr>
<tr>
<td>08</td>
<td>NAS-EPS</td>
<td>Tracking Area update accept</td>
<td>107</td>
</tr>
</tbody>
</table>

1. Status: Closed.
2. Summary of findings:

<table>
<thead>
<tr>
<th>NET. TYPE</th>
<th>PROTOCOLS</th>
<th>GEO. LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2G (GPRS)</td>
<td>GSMTAP</td>
<td>LAC, CI, TA</td>
</tr>
<tr>
<td>3G (WCDMA)</td>
<td>RRC</td>
<td>CI</td>
</tr>
<tr>
<td>4G (LTE)</td>
<td>LTE RRC DI_DCCH</td>
<td>LAC, RAC, CI</td>
</tr>
<tr>
<td></td>
<td>LTE RRC PCCH</td>
<td>s-TMSI</td>
</tr>
<tr>
<td></td>
<td>NAS-EPS</td>
<td>TAC, LAI</td>
</tr>
</tbody>
</table>

3. Items Analyzed:

MDF
Radio Forensics Examiner

Released by GBS
Place, March 15th, 2019