Extended Generic Process Model For Analysis MITM Attack Based On Evil Twin

MS Ahmad¹, Lutfi², SD Abdullah³
¹Department of Informatics, Faculty of Engineering, Universitas Khairun, Indonesia
*Corresponding author: msabri@unkhair.ac.id, sarkin.luthfi@unkhair.ac.id,
saiful.abdullah@unkhair.ac.id

Abstract. The high of criminal level related to the field of networking, is a threat that is quite dangerous MITM. The perpetrators of this attack use a fake AP (access point) with different gateway settings that are legitimate AP, so this type of attack becomes quite difficult to detect. This is due to the lack of standard operating procedures (SOP) in handling this case. This research was conducted with the aim of making a forensic model based on the analysis stages in the Evil Twin based MITM case using the user side based live forensic method. The results of the forensic investigation in the study resulted in an investigative model of ENFGP (Extended NFGP) which was divided into 10 stages and consisted of 30 completion steps, obtained through the process of testing and implementation methods in the MITM based Evil Twin attack and further testing based on several previous forensic models.

Keyword: Evil Twin, forensic, Live, MITM.

1. Introduction

The internet on the Wifi network is much in demand by the public as a means to carry out various activities such as business, buying and selling transactions, payment activities and various other things, but unwittingly this can invite unexpected danger, in fact there have been many cases of data theft through Wifi networks, on the other hand The handling of crimes involving wireless technology, [1] especially MITM attacks with wireless technology is still very minimal for now, due to the lack of available human resources, and the lack of (SOP) standard operational procedures in handling in the forensic field, resulting in increasingly increasing cybercrime-based crime, especially in the case of MITM Based Evil Twin, fake AP made deliberately to outwit the users, with the same name (SSID) (service set identification) is almost no different from legitimate AP or legitimate AP [2],[3],[4].

This is what causes many wireless network users to be fooled into the trap of the perpetrator, then the perpetrator can freely carry out sniffing, phishing, and other illegal activities using the Man In The Middle Attack technique [5].There are two types of attacks on the Evil Twin, the first is the Evil Twin configured using IP getaway which is likened to the AP router by the perpetrator, while the second Evil Twin AP is configured using a different getaway from the AP router. In this case the discussion will lead to the second type of attack, where the Evil Twin configures a different IP getaway with the AP router, so that the perpetrator cannot be reached by administrator supervision, in analyzing and detecting attacks, another method is needed that can handle this type of attack, namely by using a wired or user-based approach, so that it can assist investigators in conducting investigations.

Some IT practitioners have previously conducted research related to handling Evil Twin attacks using various methods, such as [2],[6],[7] discussing how to detect mobile-based Evil Twin attacks, [8],[9] and [10] Discusses how to detect Evil Twin attacks using the statically detection method,[7] Discussing how to detect Evil Twin attacks using the TCP / IP protocol, but unfortunately the handling of Evil Twin attacks carried out is only detecting and carrying out attack mitigation steps, without further action relating to forensics, because of this reason in this study will discuss how to do Forensic investigation in the MITM Based Evil Twin attack case, by applying several forensic methods such as the live forensic method, namely a process of collecting data on an ongoing system, according to [11] forensic data collected through the current system can provide evidence that cannot be obtained from static disk image. then the results of the study will be made an effective flow chart development based on the framework [12] (NFGP) network forensic general process and several other phases.
2. Methods

2.1 Case Simulation
The simulation is a trial activity of Evil Twin attacks carried out in the hotspot area of the technology faculty of the Indonesian Islamic university-industry (Fti UII) [13], in this case, the perpetrators of the Evil Twin attack made a different getaway setting with IP getaway from the Fti UII router, so the investigation process was not can be done by the administrator or router side, therefore in conducting the identification process it takes a wired or user-based approach that is implemented with the live forensic method to analyze data from the running system, as seen in Figure 2.1 which shows how the pattern of MITM based Evil attacks Twin, where the perpetrator tries to make a fake AP, and after the victim is connected, the perpetrator can easily do sniffing to find important information belonging to the victim, on the other hand, the investigator who accidentally enters the victim's network, tries to do sniffing between the perpetrator's communication and other victims.

2.3 Forensic Investigation
The method used in this case is live forensics where the data are taken is more live or direct [5], besides that it is also used as user side approach, where the analysis process is done from the user/client field, in this case, the
researcher intentionally enters into network coverage of the evil twin attack based mitm itself, and from the results of the research can be drawn several methods that have been carried out.

- Process scanning identification of evil twin attacks. Performed using the chellam application.
- Analyze network scanning further using helpful tools such as chellam, acrylic-wifi.
- After being identified as an evil twin attack, it will enter intentionally into the evil twin network.
- Process network packet capture traffic using Wireshark tools and network miners.
- After getting traffic capture results, further analysis is carried out to find information that can be obtained by evidence.

### 2.4 Analysis

It is a final process in analyzing identification evil twin AP and p.cap files from the previous capture, with the aim of finding data that can support the investigation process. In this study, several filtering methods will be used which have been provided by the Wireshark application or tcpdump. To facilitate the process of forensic identification

### 2.5 The stage of making (ENFGP) extender network framework is a generic process

Network forensic generic process model (NFGP) is a forensic model or framework designed to handle cases related to networking [6]. NFGP itself consists of several stages as seen in Figure 2.3 starting with stages of preparation or commonly referred to as the initial stages of preparation, the detection stage or the stage of detecting an attack, the incident responds or what initial response when the attack occurs. Then the collection stage or the stage of collecting data related to evidence, preservation, examination, analysis, investigation, and the last stages are presentations is a final stage of the case evaluation results to proceed to the report making stage.

![Network forensic generic process model](image)

**Figure 2.1** Network forensic generic process model

The making of an investigative framework is based on the stages passed from the previous forensic analysis process to find evidence, then developed based on the model (NFGP) generic forensic network process as seen in Figure 2.3 [6]. NFGP is a model of a forensic investigation made to handle cases related to networking, the NFGP model consists of 9 stages of forensic analysis, namely.

- a. Preparation: is the initial stage of the investigation that discusses how to prepare in the investigation analysis process.
- b. Detection: is a process of finding threats of attacks or illegal activity that occurs on a network network
- c. The collection is the stage of gathering information related to threats and information that can be analyzed to be used as evidence.
- d. Preservation: is the stage of maintaining or securing information or data collected to maintain the authenticity of evidence
- e. Acquisitions: is the stage of checking the authenticity of information collected through the inspection phase.
- f. Analysis: is the process of analyzing information and data found on a computer network to find evidence. Investigation: is the final stage of investigation in which forensic methods are carried out to find evidence that is carried out after the analysis process.
g. Reporting: is the final process, which is the compilation of reports from the results of evidence information found from several previous stages of analysis.

The process of making a forensic model, in this case, is based on the evaluation results of the lack of the NFGP model in resolving the case of the MITM based Evil Twin attack, and from the evaluation results found several advantages and disadvantages in the forensic model.

a. The advantages of the NFGP model are based on the functions and stages of the forensic investigation.
   - There are many systematic and regular stages especially in handling networking related cases.
   - Is a model developed from several previous investigation modules
   - The investigation stage also consists of possessing detection and incident to respond.

b. The shortcomings of the NFGP model in handling the MITM Based Evil Twin case are:
   - Basically, the MITM Based Evil Twin case is two types of attacks which are combined into one, namely attacks on computer networks that use fake AP media as the next launcher combined with Man In The Middle Attack technique where an attack attempts to utilize network traffic to do sniffing, spoofing, etc., so that it takes two stages of detection in conducting the investigation process, while in the NFGP module only has one detection stage.
   - The process of data collection stages must be carried out twice to determine the type of Evil Twin attack then proceed to the stage of detection and collection of MITM attacks.
   - The analysis process is combined with the investigation process to facilitate the stages of case resolution

3. Result and Discussion

3.1. The process of making a Model Forensic Extended NFGP

The validation of the NFGP model for the previous Evil Twin Based MITM case, found some shortcomings in the process of disclosing cases, among others, the process of detections and collection is only done once, but in the detections and data collection process in the case of Evil Twin based MITM, two the detection and collection stages, this is because this case is a type of attack method that is combined into one attack method.

The following is a table of the process of proposing the ENFGP forensic model framework which was implemented from the shortcomings of the NFGP model framework. From the evaluation results, 10 forensic stages are proposed, for more details can be seen in Table 3.1.

| Collectio  ns | Approach Strategy | Detection MITM | Collection MITM | Preservations | Acquisitions | Analysis and investigation | Reporting |
|-------------|-------------------|----------------|-----------------|---------------|--------------|----------------------------|-----------|
| collection  | x                  | x              | x               | Preservations | Examinations | x                          | Reporting |

Figure 3.1 Chart of the Extended Flow of NFGP for MITM Based Evil Twin
The process of making an ENFGP model is generated from the evaluation of the shortcomings of the NFGP model in handling the MITM Based Evil Twin case, and from the evaluation results an Extended NFGP (NFGP) flow chart / forensic model can be seen in Figure 3.1.

The stages of testing are carried out based on several forensic models from previous studies, and data from the description of the forensic model are taken from several reviews of previous forensic model development papers such as [14] by applying the elimination method, in developing NFGP models. The elimination stage is carried out by eliminating the stages from the steps that have been previously existing [15], to be used further as a reference for developing the framework.

Testing the framework in this study will be made a test table based on the forensic model of previous research which will then be applied with the elimination similar state method as shown in Table 3.2, where the elimination stage is carried out by identifying all phases from the previous model and then finding descriptions stages that are not the same will be deleted / combined and if the process of elimination there are stages that have the same description then, will be maintained.

**Table.3.2 Previous Testing of Forensic Models**

| No id | Years | Models name |
|-------|-------|-------------|
| M1    | 1995  | Computer Forensic investigation Process |
| M2    | 2001  | DWRWS investigative model |
| M3    | 2002  | Abstract digital forensic model |
| M4    | 2003  | End to End Digital investigation |
| M5    | 2004  | Enhance Digital investigation process |
| M6    | 2004  | extended model of cybercrime investigations |
| M7    | 2004  | A Hierarchical, Objective-based Framework for the digital investigations |
| M8    | 2006  | framework for a digital forensic investigations |
| M9    | 2007  | Dual Data Analysis Process |
| M10   | 2009  | Digital forensic model based on malaysian investigation process |
| M11   | 2010  | Network forensic generic process model |

**Table.3. 3 ENFGP Testing**

| No  | Extended NFGP Generic Phase | Available phase | No Phase |
|-----|------------------------------|-----------------|---------|
| 1   | Prepration                   | M3,M7,M9,M10    | 1,2,1,3 |
| 2   | detection evil twin          | M15             | 4,5,6   |
| 3   | Collections                  | M2,M3,M4,M6,M7,M11 | 7,8,9 |
| 4   | Approach Strategy            | M5              | 10      |
| 5   | Detection MITM               | M15             | 11,12,13 |
| 6   | Collection MITM              | M2,M3,M4,M6,M7,M15 | 14,15,16 |
| 7   | Preservations                | M2,M4,M15       | 17      |
| 8   | Acquisitions                 | M9              | 18,19,20,18,21,22 |
| 9   | Analysis and investigation   | M2,M1,M11       | 23,24,25,26,23,27,28,29 |
| 10  | Reporting                    | M3,M4,M6,M7,M8,M11 | 30      |

The next process of testing is based on the implementation of the case from MITM based Evil Twin, which was carried out in this study, for more details can be seen in Table.3.3 in the appendix.
Figure 3.3 is the process of Extended NFGP forensic investigation implemented from the MITM based Evil Twin case. Model development is based on the testing process using previous models. The stages in the model which are marked in blue are the general stages found in the NFGP model, while the stages marked with yellow are the stages proposed from this study, namely the Approach Strategy, MITM detection, MITM collection and analysis, and investigation stages.

The magic results from testing the Extended NFGP development model obtained 10 stages of analysis and 30 steps of the investigation, which were obtained through stages developed based on the methodology implemented from several previous forensic models, as shown in Table 3.2 and Table 3.3.

The implementation of the Extended NFGP flow chart process can be run under conditions such as the following:

a. Identifying attacks by Evil Twin AP / Rogue AP.

b. Connecting to fake AP to do the sniffing process.

If the above conditions are not met, modifications can be made to certain parts. The possible part of the modification process is the acquisition and analysis parts, which can be modified according to the needs of the investigation process.

4. Conclusions and Recommendations

4.1 Conclusions

Based on the results obtained in the process of implementing the results and discussion, then, in the study of digital forensic studies and analysis in developing the framework of forensic investigations in the case of MITM Based Evil Twin attacks, some conclusions can be drawn, namely:

-
previous study [14],[12],[16], and [17] Making an investigative framework (Pilli et al. 2010) consisting of 9 steps, it was known that it was still not effective in dealing with the case of the evil twin attack, because of that a development model was built to deal with the case of the evil twin attack.

[15],[18],[19] carried out a model development based on several previous frameworks, but the framework was tested after, still not effective in dealing with cases of evil twin attacks.

The process of developing the investigation framework is carried out through testing the framework of several previous forensic models of research. The results of the forensic investigation analysis produce an ENFGP investigation model (Extendend NFGP) which is divided into 10 stages and consists of 30 completion steps, which are obtained through the process of testing and implementation methods in the case of MITM Based Evil Twin attacks and further testing based on several previous forensic model.

4.2 Recommendations

Further research is expected to be able to implement the approaches both user side and server side, due to the limited analysis of the search for evidence carried out in the forensic investigation process in the MITM Based Evil Twin case.[20]

Further research is expected to be able to follow the development of the attack method carried out by the development of MITM Based Evil Twin. It is used to develop a framework for further forensic investigation.

Reference

[1] V. Kumar, S. Chakraborty, F. A. Barbhuiya, and S. Nandi, “Detection of stealth Man-in-the-Middle attack in wireless LAN,” Proc. 2012 2nd IEEE Int. Conf. Parallel, Distrib. Grid Comput. PDGC 2012, pp. 290–295, 2012.

[2] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, “Hacker’s toolbox: Detecting software-based 802.11 evil twin access points,” 2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015, pp. 225–232, 2015.

[3] S. B. Vanjale and M. T. Scholar, “Wireless LAN Intrusion Detection and Prevention System for Malicious Access Point,” pp. 2–5.

[4] V. V Nanavare, “Robust and Effective Evil Twin Access Point,” pp. 9074–9084, 2016.

[5] H. Mustafa and W. Xu, (“ETAD: Detecting evil twin access point attacks in wireless hotspots,” 2014 IEEE Conf. Commun. Netw. Secur. CNS 2014, pp. 238–246, 2014.

[6] K. Bauer, H. Gonzales, and D. Mccoy, “[OLD] See Practical defences against Evil Twins -- Mitigating Evil Twin Attacks in 802.11,” pp. 513–516, 2008.

[7] O. Nakhila, E. Dondyk, M. F. A. Barbhuiya, and C. Zou, “User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols,” 2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015, pp. 239–244, 2015.

[8] C. Yang, Y. M. Song, and G. F. Gu, “Active User-Side Evil Twin Access Point Detection Using Statistical Techniques,” IEEE Trans. Inf. Forensics Secur., vol. 7, no. 5, pp. 1638–1651, 2012.

[9] H. Gonzales, K. Bauer, J. Lindqvist, D. McCoy, and D. Sicker, “Practical defenses for evil twin attacks in 802.11,” GLOBECOM - IEEE Glob. Telecommun. Conf., 2010.

[10] T. M. Le, R. P. Liu, and M. Hedley, “Rogue access point detection and localization,” 2012 IEEE 23rd Int. Symp. Pers. Indoor Mob. Radio Commun. - , pp. 2489–2493, 2012.

[11] F. Adelstein, “Diagnosing your system without killing it first,” Communications of the ACM, vol. 49, no. 2, pp. 63–66, 2006.

[12] E. S. Pilli, R. C. Joshi, and R. Niyogi, “A Generic Framework for Network Forensics,” Int. J. Comput. Appl., vol. 1, no. 11, pp. 1–6, 2010.

[13] M. S. Ahmad, I. Riadi, and Y. Prayudi, “Investigasi Live Forensik Dari Sisi Pengguna Untuk Menganalisa Serangan Man in the Middle Attack Berbasis Evil Twin,” Ilk. J. Ilm., vol. 9, no. 1, p. 1, 2017.

[14] E. S. Pilli, R. C. Joshi, and R. Niyogi, “Network forensic frameworks: Survey and research challenges,” Digit. Investit., vol. 7, no. 1–2, pp. 14–27, 2010.

[15] 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.
[16] S. Ó. Ciardhuáin, “An Extended Model of Cybercrime Investigations - A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf,” vol. 3, no. 1, pp. 1–22, 2004.
[17] Y. N. Kunang et al., “Analisis Forensik Database SQL Server dan Mysql,” no. 12, 2013.
[18] I. O. Ademu, C. O. Imafidon, and D. S. Preston, “A New Approach of Digital Forensic Model for Digital Forensic Investigation,” Int. J. Adv. Comput. Sci. Appl., vol. 2, no. 12, pp. 175–178, 2011.
[19] F. C. Freiling and B. Schwittay, “A Common Process Model for Incident Response and Computer Forensics,” Inf, vol. 7, no. 2007, pp. 19–40, 2007.
[20] F. Cohen, “Two models of digital forensic examination,” 4th Int. Work. Syst. Approaches to Digit. Forensic Eng. SADFE 2009, vol. 1, no. 3, pp. 42–53, 2009.