Sri Lankan Journal of Technology
Research

SLJoT
2020 (01 & 02) 65-68
ISSN 2773-6970

A Protocol for De-anonymising Fake E-Mail Accounts in Identifying Criminals in Sri Lanka

Kasun De Zoysa

University of Colombo School of Computing
menaka@crop.ruh.ac.lk

Received: 05-11-2020 * Accepted: 11-02-2021 * Published Online: 30-03-2021

***Abstract*—**The e-mail users anonymously engaged to harass others, who are against them. Therefore, de-anonymizing e-mail accounts are very important and necessary to identify the real person behind them. It helps legitimate account users to bring them before the court for necessary actions. Once the law enforcement has enough evidence against a person, they can lay criminal charges and a judge decides if the accused should be released or remanded. Therefore, this research focuses on "de-anonymizing protocol for e-mail accounts" to identify the real identity of them. The de-anonymizing protocol is a detection and investigation of the real user behind an anonymous e-mail address. The detection system of the de-anonymizing protocol can be modified and changed according to the nature of the crime. The proposed investigation methodology can be applied for any e-mail service provider.

***Keywords*—**digital forensic, de-anonymizing, fake e-mails accounts, computer crime, digital evidence

I. Introduction

The evolution of web-based free e-mail network applications has made the world a much smaller place than it used to be. A number of e-mail services and applications aiding social interaction competing with each other to be the most effective and popular social networking tool. Despite the benefits of web-based e-mail systems and social networking tools, it has become a challenging task to identify outlaws hiding behind anonymous/forged identities (Agarwal Pandey, 2019).

Most of the online e-mail service providers have not taken basic information security requirements such as confidentiality, integrity, authentication, and non-repudiation concepts into consideration resulting in identity theft or creating virtual identities. This in-turn provides users with the criminal instinct to make use of such e-mail accounts to carry out their unlawful activities (Agarwal Pandey, 2019), (Acar et al., 2014), (Fu et al., 2020).

There are several kinds of research discussing the possibility of extracting evidence from e-mail services and social media networks (Tripathy, 2019). However, with the controls in place to protect the user accounts, the amount of data that can be extracted is limited (Zhongzhao et al., 2019). Identifying real people behind e-mail accounts is a problem that people still looking for a solution (Lappin et al., 2019), (Shao et al., 2019), (Qasem et al., 2016). Identifying the relationship between avatars from online e-mail services and social media networks does not reveal the real identity of a person who may be involved in an act of crime (Ji et al., 2014). Thereby, we have introduced a simple investigation protocol to assist law enforcement in finding verifiable digital evidence about fake e-mail accounts to find real people behind any criminal activities.

II. Methodology

A. Online E-mail Services

A considerable number of user accounts created on online e-mail services are fake accounts (Qasem et al., 2016). Creating a fake account in an online e-mail system is a simple task. Most of the fake accounts are set-up by criminals in relationships seeking to destroy the reputation of their ex-partner or harass the people. Law enforcement agencies often receive a complaint from people who find themselves or their relatives in this situation.

A victim can report such imposters' e-mail addresses to the corresponding service providers using their reporting form. However, it takes a considerable amount of time for the e-mail services provider to review the complaint and disable it (Gao et al., 2010). Moreover, law enforcement may not go through the hassle of contacting online e-mail service providers to track down the imposter unless the matter is very serious. In addition to that, most of the online e-mail service providers will never disclose more details about the fake accounts such as when it was created and from which IP addresses it was operated.

If law enforcement can obtain the public IP address of a fake e-mail in which it was operated, they can get a court order for the Internet Service provider (ISP) to reveal the information and billing address of the person involved. In case of the fake user had used a proxy server to hide real-IP, it would be very

difficult to track down the public IP address. Thus, a simple de-anonymizing protocol for online e-mail services to identifying criminals is an essential task.

B. De-anonymising Protocol

We have designed and implemented a simple de-anonymizing protocol and nab the culprit associates with criminal cases in Sri Lanka in the last three (3) years. This simple protocol operates in three (3) phases as follows:
1. Trust building phase,
2. Evidence collecting phase and
3. Legal phase. .

C. Trust Building Phase

An investigator performs the following actions in trust building phase:

The investigator should collect as much information about the fake e-mail account and the victim to find out the most trusted e-mail account of the criminal. For an example, a criminal wants to destroy the reputation of his/her ex-partner, he might send a couple of harassment e-mails copying to different people. If most of these harassment e-mails are copied to a single person, then that e-mail account may be the most trusted e-mail address of the criminal.

If such an e-mail address cannot be identified, the investigator should become a trusted friend of the criminal by using a fake e-mail address. The investigator can prepare a running incident as news, gossip, or an interesting article that should attract the criminal to build such a relationship. If that criminal interests woman, the investigator should be compatible with the interest. If the relationship-building process gets successful, the fake e-mail address of the investigator may become a trusted e-mail address of the criminal.

D. Evidence Collecting Phase

In the evidence collecting phase, an investigator performs the following actions:

The evidence collecting web server need to be deployed as the first action of this phase. Most of the cases apache web servers were deployed in a cloud service provider to meet this requirement.

```php
<body>
<?php
header("Location:http://maps.google.co.uk/maps?q=6.024123,80.217378");
die();
?>
</body>
```

Fig. 1. PHP Code to Redirect a User to Google Map (map.php)

As the second action, a simple web page that redirects its connections to the other web site should be created and deployed. As an example, the following PHP page called map.php (Fig. 1) was deployed at the webserver. It automatically redirects its users to the Google Map server and displays the given coordinates.

As the third action, the e-mail should be composed which includes the link to the above web page. Such a sample phishing e-mail is given below (Fig. 2).

Fig. 2. A Sample Phishing Email

In order to send this e-mail, the investigator should use the trusted e-mail address identified or built in the first phase. If the investigator has built a good relationship with the criminal by using a fake e-mail address, the probability of clicking a link on this e-mail is very high. All of the criminals have clicked the link in all the cases after succeeding the trust building phase .

In the above phishing e-mail, when the criminal clicks the link a given coordinate of a google map was displayed as shown in Fig. 3. In this sample case, we have displayed a location in down south of Sri Lanka by assuming the criminal is from the same are .

After the link was clicked, the web page was loaded from our web server and the browser was redirected to the landing page. Thus, the criminal may not detect the phishing attack and the public IP address of the criminal and time of access is automatically recorded by the evidence collecting web servers .

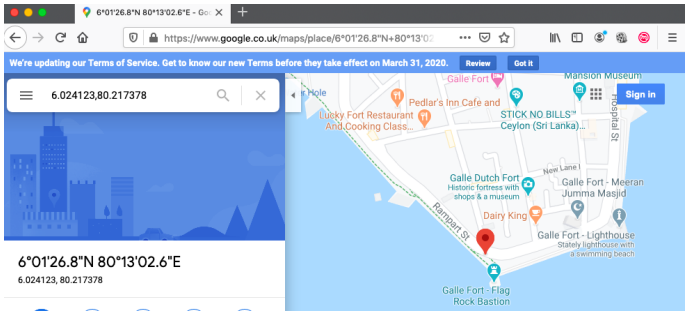

Fig. 3. A Sample Landing Page

The recorded information can be obtained from the access log of the web server by giving the two simple unix command

cat and grep. A sample outputs of such command execution is shown in the Fig. 4 .

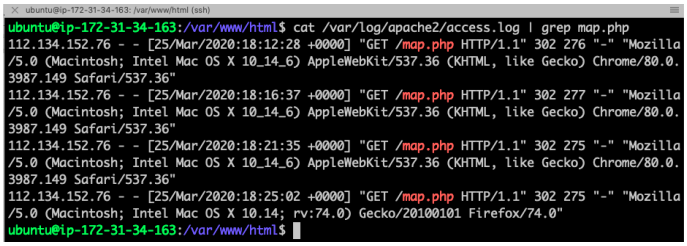

Fig. 4. Obtaining the Public IP Address

The Fig. 5 summarises the entire process of the evidence collecting phase. The e-mail content and redirection web site should be decided based on the case and the relationship which you have built with the criminal .

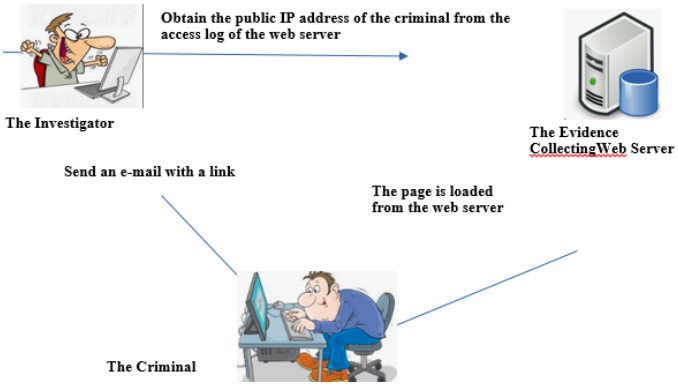

Fig. 5. The Evidence Collecting Phase

If the first attempt fails, the investigator should repeat the phase one send a different e-mail from a different trusted e-mail address until it works. When it works the public IP address of the criminal gets recoded at the evidence collecting web server. Then the online tools such as www.ip2location.com can be used to collect more information on the IP address. The collected information from such tools is Internet Service Provider (ISP) name, area-code, postal-code, country and map of the area as shown in the Fig. 6 .

E. Legal Phase

In the legal phase, an investigator performs the following actions:

The actions in this phase are depend on the legislations of the country. In Sri Lanka, the court order should be obtained from the court by submitting the collected ISP details of the criminal as the first action .

Then the investigator should submit the collected IP and the time of access to the ISP to obtain the subscriber detail.

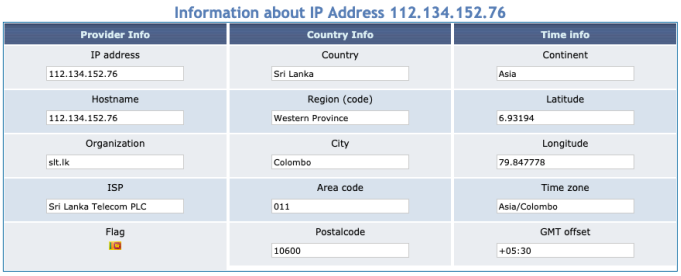

Fig. 6. Information about Public IP Address

If the subscriber is an individual, he/she may be the criminal. Otherwise, the investigator should contact the subscriber organization and find it out an individual who uses the computer at the given time .

With these actions, the investigator has successfully nabbed the culprit. As the final action, the suspect should be produced to the court with seizing equipment. The extracts of the case should be sent to the Hon. Attorney General Department for indicting to the suspect. With that action, the protocol for de-anonymizing the fake e-mail account is completed .

III. Evaluation

As described, this protocol has three phases and Fig. 7 shows the state transamination diagram of these three phases.

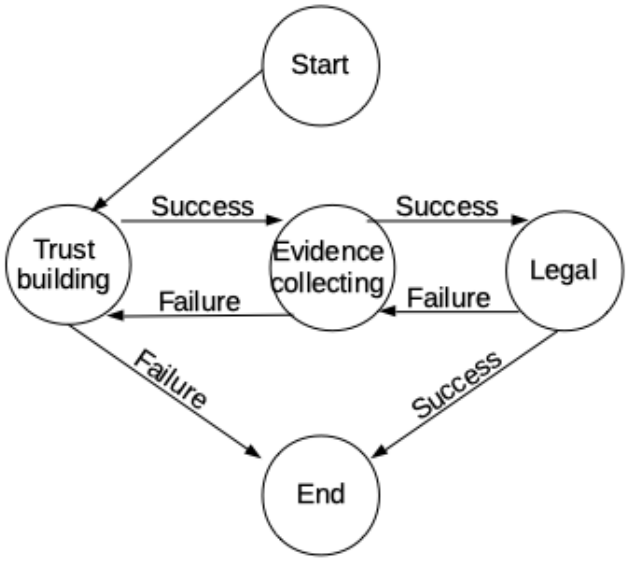

Fig. 7. State Transition Diagram of the Protocol

The protocol was evaluated based on the real investigation, and the following section describes such sample case.

A. A Sample Case

Evaluation of the protocol has conducted by applying it to several real investigation cases in the last three (3) years. An example of such a real case is described below .

A foreign student has visited Sri Lanka for higher studies. While he was studying, he has collected personal information of the reputed national in his country through social media. After that few fake e-mail accounts were created as foreign modellers who could use the native language and build a relationship with the victim. After a couple of fake e-mails, the student has brought the victim to video chat and run a nude video at the live chat. Then the victim had shown his naked body and it was recorded by the student. By showing the recorded naked video the student had demanded ransom by giving a deadline. The victim has deposited ransom into two bank accounts of his country and noticed that all money has withdrawn from Sri Lanka. The victim came to Sri Lanka and logged a complaint. The investigation was initiated, and the above-mentioned protocol was executed. After a few weeks, the investigators successfully traced the suspect.

B. Results

As shown in the following Fig., sixty one(61) investigations were conducted in various organizations in last three years. Among these investigations, eighteen (18) required the e-mail de-anonymization. Thus 30% of the cases reported to us require the support of this protocol.

	2018	2019	2020	Total	%
Fake E-Mail	5	7	6	18	29.51%
The other	12	13	18	43	70.49%
Total	17	20	24	61	

Fig. 8. The Number of Cases Reported

The trust building phase is the most important phase of this protocol. It always depends on the social engineering ability of the investigator. As shown in following Fig., the success rate of this phase is around 72%. If that phase succeeded, the success rates of the other two phases are 100%.

	2018		2019		2020		Total		%	
	Success	Failure	Success	Failure	Success	Failure	Success	Failure	Success	Failure
Trust building phase	4	1	5	2	4	2	13	5	72.22%	27.78%
Evidence collecting phase	4	0	5	0	4	0	13	0	100.00%	0.00%
Legal phase	4	0	5	0	4	0	13	0	100.00%	0.00%

Fig. 9. The break down of the success and failure rates

Thus, this simple de-anonymizing protocol had used to trace e-mail address of thirteen (13) criminals in the last three (3) years. Due to the privacy and legal obligations, information about these investigations is not described in this paper. According to the outcomes of these investigations we can claim that overall success rate of this protocol is 72%. It gives the necessary level of accessibility to the required information without the help of online e-mail service providers .

IV. Conclusion

This protocol was used to solve thirteen (13) real investigations out of 18 fake e-mail related cases reported to us in the last three (3) years in Sri Lanka. Thus this protocol is very successful in tracking criminals who use fake e-mail accounts to collect ransoms. It also helps to identify the criminals behind the cyber harassments and deformations. This protocol has given control towards mitigating the issues which are facing by law enforcement in developing countries such as Sri Lanka. Although the success rate of this protocol is 72%, it always depends on the social engineering capabilities of an investigator.

References

Agarwal D. Pandey A. (2019), Determining Fake Accounts on Facebook, International Journal of Management, Technology And Engineering, Volume IX, Issue IV, pages 1065-1069

Acar G, Eubank C., Englehardt S., Juarez M., Narayanan A., Diaz C. (2014), The web never forgets: Persistent tracking mechanisms in the wild, Proceedings of ACM CCS, pages 674–689

Fu L. , Zhang J., Wang S., Wu X., Wang X. Chen G. (2020), De-Anonymizing Social Networks With Overlapping Community Structure, IEEE/ACM Transactions on Networking, vol. 28, no. 1, pages. 360-375.

Tripathy B.K. (2019), De-Anonymization Techniques for Social Networks, Social Network Analytics, Computational Research Methods and Techniques, pages 71-85.

Zhongzhao H., Luoyi F., Xiaoying G. (2019), De-anonymize Social Network Under Partial Overlap, Proceedings of the ACM Turing Celebration Conference, Article No. 16, pages 1–5, https://doi.org/10.1145/3321408.3321577

Lappin J., Jackson T., Matthews G. Onojeharho E. (2019), The Defensible Deletion of Government Email, Management Journal, ISSN: 0956-5698.

Shao Y., Liu J., Shi S. et al (2019), Fast De-anonymization of Social Networks with Structural Information, Data Science and Engineering, pages 76–92, https://doi.org/10.1007/s41019-019-0086-8

Qasem Z., Jansen M., Hecking T. et al. (2016), Detection of Strong Attractors in Social Media Networks. Computational Social Networks 3, Article No 11, https://doi.org/10.1186/s40649-016-0036-9

Gao H., Hu J., Wilson C., Li Z., Chen Y., Zhao B. Y. (2010). Detecting and Characterizing Social Spam Campaigns. In IMC.

Ji S., Li W., Srivatsa M., He J. S. Beyah R. (2014), Structure based data de- anonymization of social networks and mobility traces, Information Security, Springer, pages 237–254.