International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Forensics using feedback approach and call logs

Sumita[1]

[1]*Student of M.Tech, Dept. of Information Science and Engineering, PESIT, Bengaluru, India*

Abstract - *The proposed tool aims to help the cyber forensics team who use Autopsy software to investigate digital data. It helps investigators to preserve their efforts, process, and experiences of investigation in the investigation reports. It lets investigators to write their feedback and append it along with the report of case. This set of feedback comments can later be utilized by other investigators as a knowledge source in solving similar cases, or as training materials for fresher investigators. The tool provides a search engine to help investigators search for existing case reports based on keywords.*

Another module of the tool helps investigators to perform phone calls analysis on the call log history provided by mobile network operators. Call log analysis is a great source of clues to help solve the cases.

Key Words: Autopsy; Digital Forensics; Feedback; Call log analysis; Search Engine

1. INTRODUCTION

In the cyber forensic world, the investigators use various software tools to perform investigation such as EnCase, FTK, Wireshark, Sleuthkit, Autopsy, etc. Autopsy is one of those popular useful tools, that helps investigators perform various analysis on the data found on the criminal's computer, hard drives, etc.

Though the Autopsy's investigation report includes various interesting facts of the case, there's no way to store the investigation process and the experience of the investigator in solving the case.

Autopsy doesn't have a feature to perform analysis of the call logs provided by the mobile network service providers. The call log history can prove to be a great source of clues in solving many cases.

2. MOTIVATION, NEED FOR THE NEW TOOL

2.1 Learning curve involved with new Tool

In the real world digital forensics there are many popular forensic tools employed to investigate the ceased computing devices. All tools come with their own level of complexities. The investigator must learn and understand the user guide/documentation to familiarize him with the tool. The investigator can practice sample exercises to gain hands on experience on the tool. However, few cases require a good amount of careful steps to be performed to analyze complex details from the device. These steps are learned by the investigator by putting time and effort to learn the tool.

2.2 KT from experienced investigators

When a new investigator gets to investigate the case, he may need to seek the guidance of the senior investigators who have solved the similar cases. The guidance of the senior investigators proves to be the valuable source of knowledge to the fresh investigator. However, it may not be feasible to seek in-person guidance. The senior investigator can maintain a library of physical notes where he writes his experience in solving the cases. Such notes act as a very valuable knowledge-base for the other investigators in solving similar cases.

The cost of training the new investigator is expected to go high when an in person training need to be given. In fact, in many cases, the tips and tricks applied to solve complex cases would prove to be invaluable for other investigators needing help in solving the new complex cases.

2.3 Autopsy doesn't support phone call log analysis

In the recent few years, mobile forensics has become the key contributor in solving many cases. As almost everybody uses the mobile phone, it's a very effective effort to see the activities of call logs of the suspects to get the potential clue on the crime. Call logs come from two different sources. One is from the suspect's mobile phone itself, and the other is from the logs maintained at the telecom operators or mobile network service providers.

Though the call logs in the seized suspect's mobile phone may reveal vital details, it may not be dependable as the call logs might be deleted by the phone user. However, the call logs maintained at the telecom operators is very much dependable. As per the law, all telecom operators need to maintain automated call logs of each of their customers. This mechanism is automated with the help of the software at telecom operator's premises. The software uses call details to generate bills to customers, to keep records and produce it when demanded legally by the law agencies or government.

This work is the effort to store the investigation feedback given by the investigator performing the analysis on the data source for the case. Autopsy tool is leveraged by the investigator to dig deeper into the data source, get

interesting facts out of it. The investigation feedback describes the various best practices, steps applied by the investigator in successfully solving the case.

The cyber forensic process involves many phases throughout the investigation. Cyber Forensic is the application of investigation and analysis techniques. The process involves gathering, storing, analyzing, and reporting evidence. The information gathered is from the computers used to commit the crime. Along with that, hard disk drives, CDs, and other ceased storage devices.

The evidences gathered from the ceased devices will then be analyzed by using one of the various software tools. The analysis report can contain the summary of the crime, evidences of the crime activities, and the pictorial representation. The report will then be used as the evidence against the criminals in the court of law. The computer forensics' goal is to perform the structured investigation by maintaining a documented chain of evidence. The evidences then helps to find out exactly what happened on a computing device that was used to commit the crime and who was responsible for that.

On every call made by the phone user, the billing software at telecom operator will store the details of the call such as caller and callee's mobile number, their mobile's IMEI numbers, the tower details within which both are talking, date and time of the call started, duration of the call, etc. These details are used by the telecom operator to perform billing on each call, and to keep track of the customer's network usage. Autopsy has a built-in feature to perform analysis on the android phone. To utilize this feature, the physical mobile phone ceased from the suspects should be available and connected to the computer that's performing analysis. However, it's also possible that the mobile phone user might have deliberately deleted the call logs before getting the device ceased. Thus, this approach is not dependable.

The law agency or government can request the telecom operator to get the detailed call log records of the suspected person. This request should be legal and a legal order has to be obtained from the higher officials has to be obtained. Unless which, the telecom operators reserve the right to deny disclosure of call logs of their customers. The call logs are the private records of the customer's activities and the telecom operators are maintained to keep the confidentiality of those records with the exception of disclosing to law agencies on government as per the law.

The call logs obtained from the telecom operators would be either in the database format or MS-Excel file formats. This data can be very huge and manual investigation on these data can be very time consuming effort for investigators. As the legal cases should be solved in a timely manner, it's important for the investigation agencies to make use of a software that helps the investigator to perform analysis quickly and accurately.

Autopsy doesn't support performing analysis on the phone call logs given by the mobile network service providers. And thus, it's required to develop a tool that exclusively performs the call log analysis.

Autopsy is intuitive software which is very easy to install out of the box. Autopsy's plug-in architecture allows the out of the box modules seamlessly, and other plug-in modules can be availed from third party developers. Any third party developer can write a new module on top of Autopsy and can distribute as a plugins for others to install inside autopsy's plugin collection, and start using it. This helps the entire digital forensics community to help each other and grow the innovation in the Digital forensic world.

Autopsy has the feature that lets the investigator to generate the report on the analysis performed on the data source of the case. Interesting facts are intelligently picked by the Autopsy and are properly formatted to further display in the report.

Autopsy supports various report formats including Excel, CSV, HTML, Text, Google Earth / KML, STIX, TSK body file. Out of all these supported formats, Excel and HTML formats reports are most widely used and helpful. Such formats can further be converted into PDF files using other PDF convertor software.

The analysis result is stored in what is called the Blackboard Artifacts table in the Autopsy. Interesting details of the analysis are tagged for future reference. The tags help investigator quickly focus on the interesting details out of many other details.

While the investigator tries to generate the report, the report generation wizard has multiple options to choose from. Options such as report format (Excel, CSV, HTML) and in the next screen investigator can choose which tags need to be part of the report.

3. PROPOSED MODULE IN THE AUTOPSY TOOL

The proposed module aims to solve the problems in the existing system Autopsy. It helps the investigator to preserve the investigation feedback, experience and comments along with the Autopsy case reports. The system will provide a new Autopsy plugin that lets investigator to enter this feedback on the case. This plugin is merged in the Autopsy's Report module.

3.1 Autopsy plugin to preserve investigator's feedback

The proposed system adds a new plugin into the Autopsy tool. The plugin works with the Report Generation feature of the Autopsy. It lets the investigator to write his valuable experience, feedback, tips and tricks applied in solving the current case. This feedback text will be stored along with the HTML reports generated by the Autopsy. This way, the Forensic agency will timely build a good resource of investigation experience from the investigators.

3.2 Search Engine to search for keywords in saved case reports

- The feature further extends the investigator's ability to search all the feedback of the case reports. As the feedback is merged with the reports, the feedback goes along with the case reports. Ideally, all the case reports are managed or stored in a central repository to keep back and share with other investigator when required.
- Leveraged the popular search engine "Solr" to achieve crawling and searching tasks.
- The module provides a search web page with the search text box. New investigators can type in the keywords to be searched in the entire reports repository. The module contacts the Solr search engine to get the search results on the given input keywords.
- The search results include the path of the case reports files that contain the keywords.

3.3 Call log analyzer

- The proposed system aims at building a new software tool to help ease the filtering requirement. It filters the call log records on various input criteria to ease investigation.
- The system expects that the CDR database has already been obtained from the network service provider. The call log analyzer tool proves to be very useful in police investigation, crime department's investigation. By just knowing the suspect's mobile number, all his contacts, activities of pre and post crime commitment can be easily tracked. The CDR database typically will be in a Excel file or any RDBMS. The proposed system is built to read both the formats. All the input criteria fields are optional to be specified. User can select any combination of criteria al or no combination at all. The filter results will filter the call log records based on the criteria selected.
- The flexibility of the criteria is so beneficiary that a date range criteria will filter all the call log which were made within given date range. The tower id based filter gives very potential filtered logs of call which are made using given tower id. The call log analyzer tool proves to be very useful in police investigation, crime department's investigation. By just knowing the suspect's mobile number, all his contacts, activities of pre and post crime commitment can be easily tracked.

4. DIAGRAMS

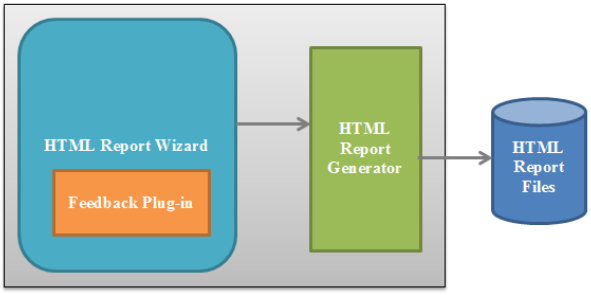

Fig -1: Feedback plugin on Autopsy's architecture

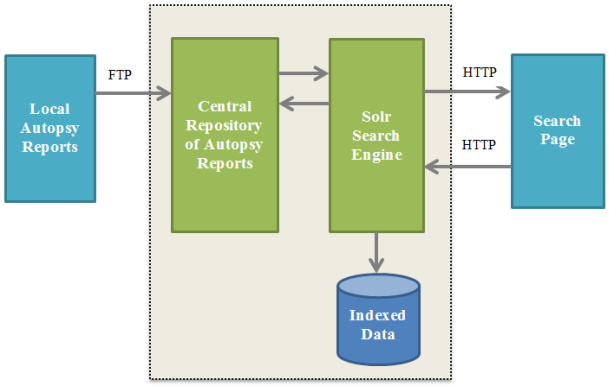

Fig -2: Architecture of Reports History and Search Page

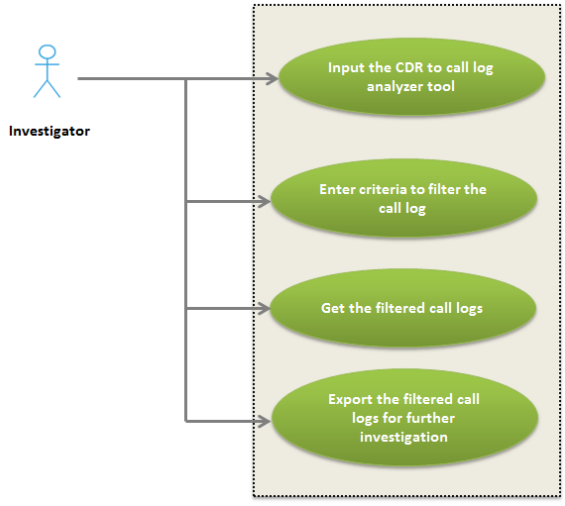

Fig -3: Use case of a call log analysis process

Serial_No	Caller Number	Callee Number	Call Date	Call Time	Duration	First Cell Id	Last Cell Id	Call Type	Caller IMEI	Callee IMEI
1	09780978726	09623282673	20-MAR-2016	09:44:16	4	404864000000583	404864000000583	Call	358502020718140	404864416416277
2	09780978726	09620823571	20-MAR-2016	09:44:39	4	404864000000583	404864000000583	Call	358502020718140	404864416416277
3	09780978726	09620823571	20-MAR-2016	09:45:14	4	404864000000583	404864000000583	Call	358502020742270	404864416416277
4	08277673950	09623282673	20-MAR-2016	14:10:18	1	404864000000583	404864000000583	SMS	358502020718140	404864416416277
5	08277673950	09620823571	20-MAR-2016	14:53:01	1	404864000000583	404864000000583	SMS	358502020718140	404864416416277
6	09780978726	09623282673	20-MAR-2016	19:06:47	110	404864000000583	404864000000583	Call	358502020742270	404864418761724
7	08277673950	09834652343	20-MAR-2016	20:49:50	540	404864000000583	404864000000583	Call	358502020718140	404864416416277
8	09686023532	8736882353	21-MAR-2016	17:33:53	224	404864000000781	404864000061471	Call	404864418761724	404864416416277
9	09119069919	8736882353	22-MAR-2016	13:17:01	26	404864000061471	404864000061471	Call	358502020718140	404864416416277
10	0353637383839	7888361242	22-MAR-2016	14:57:54	1	404864000000591	404864000000591	SMS	358502020718140	404864416416277

Fig -4: Sample of call log provided by telecom operator

4. CONCLUSION

The repository of written investigation experience feedback proves to be a great resource of knowledge that helps both fresh and experienced investigators to refer to learn the tips and tricks, applied in performing digital forensics. This repository with search engine capabilities is easier to search for reports on the given keywords. The phone call log analyzer module proves to be very helpful in solving many cases by getting phone call logs of the suspects from mobile network service providers and performing analysis on the log gives all the connections and activities of the suspects

REFERENCES

[1] http://www.sleuthkit.org/autopsy/
[2] https://github.com/sleuthkit/sleuthkit
[3] https://github.com/sleuthkit/autopsy
[4] http://www.basistech.com/blog/
[5] http://stackoverflow.com/
[6] https://code.msdn.microsoft.com/101-LINQ-Samples-3fb9811b
[7] https://msdn.microsoft.com/app-development-msdn#desktop