Annual ADFSL Conference on Digital Forensics, Security and Law

2018
Proceedings

May 17th, 2:45 PM - 3:20 PM

Non-Use of a Mobile Phone During Conducting Crime Can Also Be Evidential

Vinod Polpaya Bhattathiripad Ph D
GJ Software Forensics, vinodpolpaya@gmail.com

NON-USE OF A MOBILE PHONE DURING CONDUCTING CRIME CAN ALSO BE EVIDENTIAL

Vinod Polpaya Bhattathiripad, Ph. D.
Cyber Forensic Consultant
GJ Software Forensics
Kozhikode - 673004, Kerala, India
vinodpolpaya@gmail.com

ABSTRACT

Cyber-clever criminals who are aware of the consequence of using mobile phones during conducting crimes often stay away from their phones while involved in crimes. Some of them even change their handset and SIM card, subsequently. This article looks into how intentional disassociation (and even unintentional non-use) of mobile phone in non-cybercrimes, can become evidential clues of the perpetrators' involvement in criminal acts. With the help of a recent judicial episode, this article reveals how extremely careful and masterful handling of extensive and voluminous CDRs and tower dumps by a cyber-savvy investigating official can unearth evidential clues to locate the perpetrator, even when the perpetrator stayed away from his or her mobile phone while committing the crime. This is not a typical case study article, but an article to report a rare, live episode in cyber forensics which can be procedurally highly informative for cyber investigators and related researchers worldwide.

Keywords: CDR, Call Details Records, Cyber investigation, Crime investigation, tower dump, Police, Kerala Police

1. INTRODUCTION

In today's world, dominated by the magical device of omnipresent mobile phones, criminals conducting traditional, non-cybercrimes often tend to use mobile phones while committing crimes. As a knock-on effect of their phone use, they often leave behind different types of "footprints" in the form of data in the cyber space.

Accordingly, modern, clever, and dedicated investigators of non-cybercrimes often search through the cyber space too for the presence of such "footprints" and use them as instruments to track criminals or even as potential evidence.

No wonder then that cyber-clever criminals who are aware of the potential danger of using mobile phones during conducting crimes stay away from their phones while involved in crimes and even change their handset and SIM card, subsequently. By doing so, they attempt to ensure that they do not leave any cyber evidence of their presence in the crime scene or their criminal act and/or of their physical movement as part of the crime. Needless to say, such a cyber-savvy precaution by any criminal will normally make his or her phone tracks remain 'invisible' or untraceable to the police, and hence will drastically reduce the criminal's chance of being suspected, especially when there

is absence of human witness and other physical evidence.

Such a crime scenario will surely make the job of the cyber investigation expert difficult and will demand the use of non-conventional approaches in cyber forensics in order to identify, trace, and locate the criminal. Hence, cyber investigation experts worldwide need to be made aware of the possible non-conventional approaches to intelligently handle such difficult situations.

With such an objective, this article documents a non-conventional way adopted by an intelligent cyber investigation expert of the Kerala Police in order to identify, trace and locate a clever rapist-cum-murderer who had conducted the crime without leaving any direct, explicit, physical as well as cyber trace.

2. A CRIMINAL EPISODE AND ITS CYBER (NON)CONNECTION

Ironically, intentional disassociation and even unintentional non-use of mobile phone does not necessarily exempt or exonerate the owner of a phone. Indeed, the absence or non-use of a phone can itself lead on to evidential clues of his or her involvement in criminal acts. Extremely careful and masterful handling of extensive and voluminous telecom records by the investigating team can unearth evidential clues even in such situations. Thus, acts of omission can paradoxically lead on to evidence of commission in cyber forensics.

Such an extremely careful evaluation is not new in research. Various related theoretical studies have already revealed that careful evaluation of large telecom call graphs (with rich temporal and geographical labels on their edges), generated from massive telecom data, can successfully provide crucial information on various hidden call patterns in the telecom networks (Pundit et al, 2008, Phadke et al, 2013).

In an actual real-life criminal incident, a clever rapist-cum-murderer was recently successfully traced by the clever handling of massive 8.4 million tower dump data and also by unearthing hidden call patterns from this massive data by a local police team. This perpetrator, who was a migrant labourer with no past criminal history and working in south-western India, had stopped using his mobile phone long before conducting the crime and had even changed his handset twice and SIM card once, after the criminal act. In addition, he had made sure that his telephone was only minimally used during his travel of about 2500 miles across the country after conducting the crime and then again was never used during the subsequent travel of about 2000 miles, both within 40 days of committing the crime.

The role and significance of the cyber evidence against the criminal was later crucially justified and vindicated since the criminal's involvement in the crime was later unequivocally established through a DNA match and the trial court even gave him the death sentence. Section 169 (titled "Call Data Records," pages 208 to 241) of the 410-page judgment narrates the way the police cyber expert innovatively used the information relating to the mobile calls in order to trace, locate, and catch the perpetrator.

Generally, prima facie absence of telephone evidence in such cases persuades the investigating police team not to pursue the cyber part any more. Even so, an apparent lack of telephone evidence may not really be a lack of evidence and a very dedicated and clever cyber-savvy police officer can still derive intelligent facts by thoroughly investigating the details and the background of the perceived absence of telephone evidence. Occasionally, such an investigation can be extremely complex

and complicated, but for a well-motivated cyber expert, that itself can be a provocative push for more intense and often challengingly strange findings. A reasonably detailed account of the approach, procedures and methods used by the cyber-savvy police officer in the case mentioned above appears to be very relevant for an insight into the cyber modus-operandi for such cases.

3. THE RECENT INDIAN STORY OF SUCCESSFUL CYBER-TRACING OF A RAPIST-MURDERER

On 28th of April 2016, a 30-year-old woman (whose name is not disclosed here as also preferred in the judgment) was found brutally assaulted and dead at her home on the outskirts of the town of Perumbavoor in the Ernakulam district of the state of Kerala in South India.

The police team, which first arrived at the crime spot, found that most parts of the dead body, especially the genitals, were brutally damaged, with bloodstains all over the body, that her intestines were pulled out and that the dress on the dead body was soaked with blood. Subsequently, the police registered a criminal case (Case, 2016) and sent the body for postmortem after completing the initial formalities.

In a couple of days, the crime incident received national importance and wide public attention through the media, for various reasons. Firstly, the murdered woman was an undergraduate student of law in the prestigious Government Law College nearby. Secondly, she belonged to a financially-challenged family who were housed in a temporary hut on the government-owned land nearby the Periyarvally irrigation canal. She was staying with her mother, a casual labourer as her father had abandoned the family when she was a child. Thirdly, she belonged to a traditionally under-privileged Indian ethnic community which officially falls in the special protective category namely "Scheduled Castes and Scheduled Tribes." All these heightened and intensified the police attention on the investigation and the search for the culprit(s).

Based on the postmortem report (postmortem, 2016), the preliminary and traditional police investigation did unearth enough evidence to establish rape and murder, but there was not enough evidence to identify and locate the perpetrator(s).

The biological forensics experts soon found that the DNA of one of the bloodstains found on the body did not actually match with the victim's DNA (RGCB, 2016) and so, suggested that the perpetrator(s) too may have been injured and bled during the crime. Accordingly, the police re-oriented their course of action to locate the person with this DNA.

However, locating the person with this DNA in this thickly populated state was not an easy task. The population of this tiny south-western Indian state (which is not much larger than Maryland in the USA) is 34 million (which is almost the same as that of big California) (Census, 2011). In addition, the crime spot, which is very close to the thickly populated Perumbavoor town, was multi-ethnic, housing several thousands of migrant laborers of diverse Indian communities too.

All these complex, demographic difficulties induced the police to incorporate a few necessary scientific cyber procedures also into their investigation tactics in order to locate the criminal in the strong belief that the criminal may have used a mobile phone during the crime. This belief was scientifically backed-up by the fact that this tiny state had already achieved a mobile phone density of 110% of the population (TRAI, 2017).

Accordingly, from the various telecom companies operating in the area of crime, the police collected around a huge mass of over 1 million mobile tower dump data (or the metadata of each communicational activity relating to mobile phone of all those present under the various mobile towers installed around the crime spot) generated during the two hours before and the two hours after the crime. Further, they scientifically analyzed this tower dump data (obtained in the Microsoft Excel format) with the objective of creating a list of suspects. However, after systematically sieving out and removing all "normal" and "innocent" data from this tower dump, they failed to locate any suspicious number or any suspicious IMEI (International Mobile Equipment Identity) code in it. Thus, it became almost evident to the police that the suspect had not used a mobile phone in connection with the crime and that their investigation using telecom records would not deliver any more fruitful results.

Strong media publicity (TNIE, 2016) and active public attention made the authorities decide to take on a more rigorous cyber investigation policy, and so the investigation team was further strengthened by a police officer who, although not qualified in computer science, had enjoyed a successful track record with his intuitive (as against, trained) skills to analyze around massive 2-3 million telephone call-related details to locate criminals in several sensitive cases, ranging from political murder to anti-national activities. The team thus definitely achieved greater cyber-savvy and fortification and the modus operandi of the newly joined expert is the basis of the 'something from nothing' cyber evidence focused herein.

This police officer chose to begin his duty with the CDR (Call Details Records for the past one year, obtained in the Microsoft Excel format) of the mobile number of the victim. By using the pivot table facility of the Microsoft Excel, he ranked all the contacts found in it according to the total time the victim had spent with each of them over phone during the past one year. The objective of such a ranking was to find if the victim had any telephonic contacts with anyone enjoying past criminal history and an immoral life style (measured along the standards often followed by the well-knit, orthodox society of this southern-Indian state of Kerala with 100% literacy and close to 110% mobile phone density). With this rank-list, the field squad of the police investigation team proved that no one in the rank-list had any criminal-past, that the victim's past life was quite normal and that the perpetrator(s) could very unlikely to be one from among those telephonically communicated with the victim during the past one year.

In addition, this police officer logically collected and analyzed a gigantic load of 8.4 million tower dump data (also obtained in the Microsoft Excel format). This data came from the around 15 mobile phone towers installed 5-6 miles around the crime spot and covering the preceding 48 hours and the succeeding 24 hours of the incident. The data scientifically established that the chance for the criminal to have used a mobile phone in connection with the crime was very remote.

Proceeding further, the officer used these same 8.4 million tower dump data to list out (and also to rank them based on their non-use) all the mobile phones which were suspiciously silent for hours together before the crime had happened. In this rank list (which was also prepared using the pivot table facility of the Microsoft Excel), he zeroed-in on a particular mobile number which was not in use since 1:05AM on 27th April 2016, 40 hours before the crime had happened. The SIM card relating to the number was traced then to its owner, S. K. Saharul, a migrant labourer who lived in the locality of the crime. However, according to the

police records, neither the mobile number nor its owner had any past criminal history, and so there was no reason for the police to suspect him. Even so, for a total confirmatory exclusion of this number from the crime, the police officer obtained the CDR of this SIM card from the telephone service provider and analyzed it. He found that there were absolutely no incoming and outgoing calls and no text messages during the 40 hours before the crime. Surprisingly, there was no record of even messages that should have been routinely there. This absence of messages that should have been routinely and unavoidably there, no matter what, raised his suspicion as it suggested the owner's intentional dissociation of the phone from communicational traffic (as against an unintentional, natural silence of the phone).

Delving further, he noted in the CDR that this telephone number (that means, the SIM card) was again made operational four hours after the incident (that means, after remaining non-operational for 44 hours) when it was under a mobile phone tower installed at the nearby Perumbavoor town. However, the mobile handset used before the crime was certainly different from the mobile handset used after the crime as indicated by the difference in the IMEI codes found in the meta-details of the calls in the CDR.

Also, from the CDR, it was noted that not only was the handset different, but the locations too were totally different. In addition, it was noteworthy that the subsequent mobile phone activities showed locational connections with a stretch of railway stations wide apart across the country. The final activity from this number was an outgoing call made on 2nd May 2016, four days after the incident, from Dumdumiya, a remote village in the state of Assam which is as far as 2500 miles away from the crime spot. After this final activity, the SIM card was suspected to have been dissociated from communicational traffic again as there were no records of delivery of even messages that should have been routinely and unavoidably there.

Altogether, in the above process intended to totally exclude this number from crime, the police ironically found that there were quite a few suggestive factors for its involvement in the crime. Firstly, the mobile phone was inactive 40 hours before the crime and then, until 4 hours after the crime. Secondly, there was evidence of a sudden change of handset. Thirdly, it appeared that the phone has been moving by rail thousands of miles across the country immediately after the crime had happened. Fourthly, during most of this time there were periods of long non-use of the phone (and this history and pattern of non-use during this short period did not tally with the history and pattern of non-use of the phone during the previous one year). Finally, the final instance of the use of the phone was located to be in the owner's native land after which, even messages that should have been routinely and unavoidably there were also seen to have been undelivered. All these strongly suggested an effort to disconnect or dissociate oneself from the phone and to suddenly move away across the country with an attempt to be minimally communicating using the phone. So, the owner of the number, S. K. Saharul became a suspect in this case.

Further, the whole forensic task became more complex when it came out that the Saharul had in fact never left the place, and was still about and around, but had preferred not to entertain any family relationship or friendship with anyone in the CDR of his number. Upon interrogation, Saharul revealed to the police that it was not he, but his friend, by the name 'Ameer-ul Islam' who had been actually and illegally using the SIM card for that long. The police had no reason to disbelieve Saharul's revelation because Ameer-ul Islam (who belonged to Saharul's home state), was also a migrant labourer staying in the town near the

crime spot. Moreover, the frequent contacts (obtained from the CDR of the SIM card) consisted of Ameer-ul-Islam's wife, father, brother and a few other kith and kin and did not include any of Saharul's kith or kin.

Assuming the possibility that Saharul can be discounted but Ameer-ul Islam can be listed as a suspect, the police then physically conducted a raid at the temporary home of Ameer-ul Islam nearby the crime spot and found that he had left home a few hours after the crime had happened and that he did not leave behind any kind of biological traces at his temporary home to obtain his DNA information. Thus, at that stage, Ameer-ul Islam had remained a potential suspect-at-large with absolutely no helpful evidence to confirm his involvement in the crime. Yet, the police proceeded with their plan to trace, locate, and then interrogate him.

More confirming cyber facts emerged while interrogating the friends and relatives staying with Ameer-ul Islam. The police learned that he was seen engaged in an argumentative telephone call with his wife after which he had broken his mobile handset by throwing it against the wall sometime just past midnight on 27th April 2016 (which was about 40 hours before the crime had happened). It was further revealed that Ameer-ul Islam was away from home during the subsequent 2 days (including the day on which the crime had happened) but had returned home in the evening with a sudden plan to leave for his hometown, 2500 miles away (such a sudden, non-preplanned trip home was uncommon in this well-knit, communally orthodox group of migrant labourers). In addition, one of his fellow residents (who was his father's brother's son and also a migrant labourer) revealed to the police that he had handed over a new mobile handset to Ameer-ul Islam as a gift to be handed over to his mother in his hometown near Dumdumiya in Assam, and that he had later heard from his mother that Ameer-ul Islam had indeed promptly delivered it to her. All these crucial pieces of information (including the IMEI of the gifted handset) and also the pieces of related information subsequently collected from the home town of Ameer-ul Islam (with the help of the Assam Police) were actually corroborating with the predictions of the cyber police officer. However, unlike he assumed, the absence of mobile phone evidence was not due to the perpetrator's intentional attempt to disassociate his phone from the crime but was because his mobile handset was actually dysfunctional since 1:05 AM, 40 hours before the crime had happened.

Anyway, with the motivation gained by the perfect corroboration of his cyber-predictions, the police officer proceeded further to put the mobile numbers of Ameer-ul Islam and his nearest kith and kin under surveillance and then waited for Ameer-ul Islam to further call them either using his original SIM card (after loading it in a new mobile handset) or using another SIM card in a new handset. Also, at regular intervals, the officer kept on sending text messages to the mobile number of Ameer-ul Islam with the hope that at least one of these messages will be delivered as and when his SIM card became functional and that the metadata of such a delivery can remain evidential to locate him. Just as the officer expected, on 6th June 2016, the 40th day of the crime, a message sent to his mobile was found promptly delivered onto his mobile which was an indication to the police that the original SIM card of Ameer-ul Islam had become once again active after a gap of 40 days. From the IMEI code contained in the meta-details of the delivery of this message, the police noted that he was using a new mobile handset. Moreover, the tower location in the meta-details suggested that he was then at Kanchipuram which is a place in the south-eastern Indian state of Tamilnadu, about 2000 miles south of his home town and about 400

miles east of the crime spot. This telecom information was decisive for the investigating team and they soon sent their field squad to Kanchipuuram with a plan to conduct a combing operation there to locate him. But, by the time the team reached Kanchipuram, the original SIM card of Ameer-ul Islam was once again found non-functional as there were no specific traces of his further movements.

In addition to this decisive, crucial information, the police cyber expert soon noted that Ameer-ul Islam's kith and kin had already started receiving calls from Kanchipuram from a new SIM card. This new SIM card was then traced to its owner, Udayakumar, who, ironically, was found totally unrelated to Ameer-ul Islam's family members. However, upon interrogation, Udayakumar revealed to the police field squad that, through his friend, he had recently sold his SIM card illegally to Ameer-ul Islam. With his and his friend's help, the police soon successfully located Ameer-ul Islam in Kanchipuram and took him into custody on the 59th day of the crime incident.

They then forcibly took his blood sample and sent it for DNA matching. A successful cross-match of his DNA (with the DNA obtained from the bloodstains found on the dead body and also on the cloths nearby) proved (RGSB, 2016) that he was present at the crime spot and had shed blood there and so could have had a part in the crime.

This confirmation marked the end of the successful searching of the police cyber expert along the cyber space for the person carrying the particular DNA.

Later, the trial court finally found him guilty of both rape and murder and awarded him the capital punishment of death sentence, subject to the confirmation of the High Court of Kerala (Judgment, 2017).

4. REASONS FOR REPORTING THIS CASE

Such a successful, scientific, and non-conventional investigation by the Kerala Police using cyber forensics in order to locate, trace, and eventually convict such a perpetrator deserves international attention, for various reasons.

Firstly, this case was a traditional rape and murder with no human witness and also with no helpful clues found in the CDR of the victim's mobile number. There were no clues in the ±2-hour tower dump generated during the crime either. Generally, absence of telephone evidence in such cases persuades the police not to pursue the telecom call lists any more. But, in this case, by assuming that apparent lack of telephone evidence may not really be a lack of evidence, the police officer had expanded his investigation by collecting more telecom records generated days before and after the crime had happened and apparently derived intelligent facts from it, innovatively.

Secondly, the temporarily inactive SIM card found belonged to one among the hundred thousand generally active SIM cards found in the thickly populated area around the crime scene where the SIM card density was more than 100% of the population. Identifying such an active SIM card with such an hours-long inactivity history from a gigantic 8.4 million call records demanded absolute cyber forensic brilliance, supreme cleverness and sheer dedicated persistence from the part of the police officer who was equipped only with a laptop and Microsoft Excel. He approached and carried out his task by using the various innovative alternatives in a systematic manner. His successful identification of this SIM card turned out to be a crucial milestone in the success of the investigation of this crime, and undoubtedly provides an interesting precedent in clever forensic procedure.

Thirdly, in a densely populated country (with population close to 1.3 billion, more than four times that of the US and the second largest in the world) and with an area close to only 1.3 million square miles (only slightly more than one-third of that of the US), and with an ethno-cultural, linguistic, and communicative diversity more than found in any nation in the world (Census, 2011), tracing the movement of this already identified SIM card also demanded absolute cyber inventiveness and innovation on the part of this police officer especially when the SIM user, a migrant labourer, had changed his handset twice and this SIM card once, and had travelled almost 4500 miles during the following 40 days of the crime with an absolute minimal use of his SIM card.

Cyber investigation experts and related researchers worldwide are expected to be made aware of such possible non-conventional approaches to intelligently handle such difficult and unfavorable forensic situations.

5. CONCLUSION

To sum up, modern crime investigation depends heavily on digital evidence which is something that is automatically created during use or abuse of digital equipment while conducting crimes. Digital evidence, if properly backed by scientific methods, often helps investigation agencies to unequivocally establish not just abuses of digital equipment but also solve various other traditional crimes in which digital equipment is involved. Not only presence of the information generated by such digital gadgets but also the absence of the mandatory information generated by such digital gadgets can remain evidential If analyzed cleverly and inferred brilliantly, the apparent absence need not be an unhelpful negative forensic phenomenon, but can lead on to positive evidential clues, as revealed by the live, actual and rare cyber forensic instance, mentioned above.

REFERENCES

Case. (2016), crime number 909/2016, The Kuruppampady police station of the Kerala police, India

Census. (2011). http://censusindia.gov.in

Phadke, C., Mendiratta, V., Uzunalioglu, H. Doran, D. (2013). Prediction of Subscriber Churn Using Social Network Analysis, Bell Labs Technical Journal. 17. 63-75. 10.1002/bltj.21575.

Judgment. (2017). Sessions case number 662/2016, Court of Session/Special Judge for Scheduled Castes and Scheduled Tribes, Ernakulam Division, Kerala State, India

Pundit, V. Modani, N., Mukherjea, S., Nanavati, A. A., Roy, S., Agarwal, A. (2008). Extracting dense communities from telecom call graphs, 3rd IEEE International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE 2008

Postmortem. (2016). Postmortem report 298/16 of T. D. Medical College, Alapuzha, Kerala State, India

RGCB. (2016). The two letters dated 18 May 2016 and 14 June 2016 with the reference number RFDF file No.742/16, Rajiv Gandhi Centre for Biotechnology, Thiruvananthapuram, Kerala state, India

TNIE. (2016). "Whodunnit? Probe leads nowhere", Page 1, 5 May, 2016, The New Indian Express, Kochi Edition

TRAI. (2017). The press release numbered 03/2017 dated 9 January, 2017, of the Telecom Regulatory Authority of India, available at http://www.trai.gov.in/sites/default/files/Telecom%20Sub_Eng_pr.03_09-01-2017_0.pdf and accessed on 4 January, 2018

