Grenze International Journal of Engineering and Technology, June Issue

Mechanism to Handle Mobile Devices in Cyber Security Investigations

Abhishek Kumar[1], Kishore Kumar Senapati[2] and K.Sridhar Patnaik[3]
[1-3]Computer Science & Engineering Department, Birla Institute of Technology Mesra
Ranchi. India
Email: abhishek.luck@gmail.com, kksenapati@bitmesra.ac.in, kspatnaik@bitmesra.ac.in

***Abstract*—Smartphones play an extensive position withinside most company investigations into cyber intrusions. Investigations from the Law Enforcement additionally contain cellular gadgets sporting crucial proof that could assist carry the case to its logical conclusion. Smartphones are utilized in several crook justice contexts. The company presents mobile telephones to lots of its personnel as a part of their task duties, and the BOYD (carry your very own tool) idea is broadly adopted, permitting customers to get admission to workplace applications (like Outlook, Skype, etc.) the usage of their very own transportable gadgets. Based on forensic proof from research starting from conventional crimes (homicide, robbery, kidnapping, etc.) to technological crimes like cybersecurity incidents on company-huge cellular facilities, unlawful get admission to or exchanges, or facts theft, the cybercrime inquiry unit can be required to capture the cellular gadgets and ship them to FLS for added analysis. The chain of custody high-quality practices for securing mobile telephones, iPads, company cellular telephones, and BYOD gadgets in a manner that protects the integrity of the proof and is consequently suited in courtroom docket are in short defined on this paper. This paper's chain of custody technique was created especially for cellular platforms which require specific application of mind and use of tools in the reconstruction of the scene of crime as well as management of the evidence due to the variety of operating systems and nature of dynamic evidence which mobile devices have. The necessities of the commercial enterprise and regulation enforcement agencies that might use the record for normal cellular tool investigations in India have been taken into consideration while it was being developed. This paper has been written retaining in view the necessities of each enterprise in addition to the Law Enforcement Agencies to apply it for his or her everyday cybersecurity investigations concerning cellular gadgets.**

***Index Terms*— Chain of Custody, Digital Forensics, Investigations, BOYD, mobile devices, cybersecurity.**

I. INTRODUCTION

The chain of custody of mobile devices (with internet enabled phones and tablets) is one of the many important areas of the overall mobile forensics' investigation process after mobile device seizure and involves data extraction, analysis, and reporting. On the other hand, seizing a mobile device or group of mobile devices entails keeping safe control of them while avoiding tampering with or changing the information on them or any removable media (like a SIM card, memory card, etc.). The integrity of the entire investigation may be

Grenze ID: 01.GIJET.9.2.76_1

questioned if the evidence is not kept secure.
Chain of custody, according to [1] is a procedure for recording evidence in the sequence of events. In order to ensure that the evidence can be used in court, the chain of custody is a crucial step in the investigative process. [2]. The chain of custody can occasionally be a drawn-out procedure, but it is necessary if the evidence is to be used in court. The evidence has a clear chain of custody because it identifies who had it, where it was when it was discovered and taken (at the crime scene or from a person), and when it was delivered to the lab for analysis. The issue of the chain of custody has grown significantly in importance in current investigations because of the sensitive information that is present in digital evidence and the fact that it affects both the integrity of the digital evidence and future legal processes. The following are the contributions made:

- A new form is designed for the chain of custody during the seizure of a mobile device in cases of cybercrimes or cyber breach [5] [7] involving a corporate mobile device or a bring your own device in a corporate setup.
- Identified the gap in the existing work and enhanced and practical understanding is provided for cases involving seizure of a mobile device.

II. Discussion

One of the most unsettling developments is how quickly mobile device-related cybercrime is spreading. "Last year was the first year when revenues from cybercrime were bigger than earnings from the sale of illegal narcotics, and that was, I believe, over $105 billion," declared Valerie McNiven, a U.S. Treasury Advisor. " She continued by saying, "The pace of cybercrime makes it impossible for law enforcement to keep up." Now that experts have figured out how to take advantage of the potential windfalls, it seems clear that the problem will only get worse in the coming years. There has been a lot of debate recently about how organized crime and cybercrime are intertwined. Such a combination portends bad things for the near future. There is little chance of limiting and neutralizing the danger by conventional means of traditional computer forensics, because the majority of criminal organizations are based in Eastern Europe, Russia, and Asia, where laws and enforcement are weak and technological advancements in computer forensics are not yet up to date. Phil Williams, a visiting scientist at CERT, provided a short summary of the problem. "Crime may be committed using the Internet as both a conduit and a target, and it makes it possible to profit greatly while taking very little risk." It is tough to ask more of organized crime.

III. Existing Approach

Most of the time, desktop and laptop computers are involved in the current chain of custody and seizure of electronic evidence. Mobile devices, on the other hand, necessitate a modified and more focused chain of custody strategy due to the dynamic nature of the data and the preservation of evidence. Even though [3] lists the many problems computer forensics investigators face when trying to get data from mobile devices to use in criminal investigations, it doesn't offer any solutions to the problems with the chain of custody in crimes involving mobile devices.
David Bennett [3] carried out a study in which several types of mobile devices with huge storage capacities are covered, along with the difficulties faced by forensics specialists in extracting data from the devices for use in criminal investigations. The article talks about several forensics' technologies, legal problems that a forensics expert might run into when trying to get information from a mobile device (like the Fourth Amendment), and problems with the chain of custody.
Murthy et al. [5] concluded that the integrity and correct sequence of evidence must be maintained to ensure that evidence is admissible in court.
In 2022, Keshav Kaushik wrote a book [6] about the methods and tools used in mobile forensics. This chapter of the book also discusses how to manage digital evidence while upholding the chain of custody.
Dirk Pawlaszczyk [7] has mentioned the FORMOBILE project that aims to map the continuum of custody from crime scene first response teams to courtroom evidence in a standardized way. This project will be used as an example for this article.
Fahdiaz Alief, Linda Roselina, Yohan Suryanto, and Tofan Hermawan [8] conducted a study discussing the unsend functionality of social media messages in relation to cell phone forensics. It helps Indonesian forensic scientists or law enforcement officers to obtain digital evidence for cybercrime issues such as: B. Hoaxes, cyberbullying, illegal trading, online protection, or other crimes committed on social media. The investigation uses MOBLE edit and the Universal Forensic Extraction Device (UFED) to collect digital evidence.

June Tanner and April Tanner [9] suggest, in their study, using chain of custody reports to track and record changes in the ownership or possession of evidence. Timelines have been proven to be useful visualization tools for organizing and showing information, even when textual reports are the norm.

IV. Proposed Approach

A new chain of custody mechanism and its related areas are proposed in a flow chart depicted in Figure 1, where the step-by-step chain of custody in mobile devices, which is a practical approach to mobile device seizure, is provided. This paper's chain of custody technique is created especially for cellular platforms which require specific application of mind and use of tools in the reconstruction of the scene of crime as well as management of the evidence due to the variety of operating systems and nature of dynamic evidence which mobile devices have.

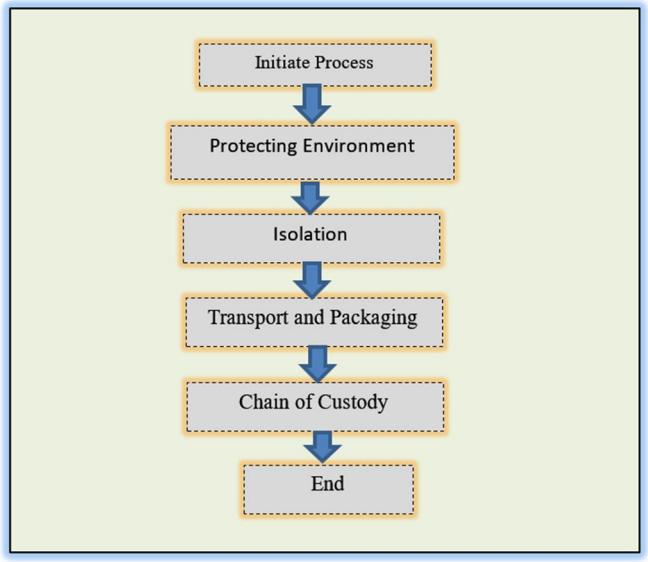

Figure 1. Chain of Custody Process

V. Scene of Crime - Securing the Environment

When evidence is brought into court as an exhibit, a record of the chain of evidence must be kept and shown. Otherwise, the evidence might not be allowed to be used in court, raising major concerns about its reliability and the way it was examined. To prove that no one else could have obtained or had that evidence without authority, the chain of custody must record every transfer from one person to another from the moment the evidence is gathered. The number of transfers is unrestricted, but it is important to maintain it as low as possible. Considering this, here are some general guidelines for keeping the devices and their surroundings safe so that a good chain of custody record can be made when mobile devices are involved.

1. To ensure that they are not overlooked during the seizure, it is crucial to comprehend mobile devices and the numerous pieces of equipment they are connected to.
2. Other major seizure triggers include ports, adapters, memory cards, UICCs (Universal Integrated Circuit Cards), WIFI modems, routers, and PCs to which mobile devices have trusted connections. Attempts to confiscate these should be made as advised by the legal team.
3. When accessing a mobile device, personal computers may be quite helpful provided they have a good working connection with the device. Thanks to a pairing process specifically initiated by Apple, some programs can use the existing pairing record file while accessing the mobile device when it is still locked.
4. In addition to smartphones and other devices, attempts may be made to record security codes, passwords, or access gestures. For example, you can set different passwords for unlocking your mobile device and accessing internal storage.

5 If the accused is informed to use the phone on their own, extreme caution should be exercised. A master reset code allows you to fully restore factory settings on various mobile devices. Additionally, a master reset can be initiated remotely. Therefore, great care and network isolation are required in such cases to prevent evidence from being tampered with or deleted.
6 Before sending a mobile device to a forensic investigation team, storage components (such as removable memory cards) should be removed from the device.
7 Investigators may need to use other connected devices during a seizure. B. Internet of Things (IoT) devices.

VI. Scene of crime - Isolation of devices

Because a mobile device is such a fluid system, it is important to keep it from being connected to too many places in case of an emergency. Many modifications to the data and evidence within are made just by turning on the device. The effectiveness of the chain of custody is greatly influenced by how well the mobile device is isolated before and following its capture.
Users of many cell gadgets can lock or wipe their tool from afar via means of sending a command (like a textual content message) to the cell tool whilst it's miles away and linked to a cell community or the Internet. Also, getting a name or textual content message may alter the data inside the phone, hence compromising its integrity. Any records that are dispatched out, which includes a GPS location, can also be inaccurate. If the mobile device is attached to some other tool with synchronization abilities, the proof saved at the phone can be extensively altered.
Therefore, it is advised to adhere to isolation best practices.

1. Keep everyone who was not engaged in the event away from the mobile device.
2. If the mobile device is linked to a computer, disconnect it from the computer to stop any data synchronization or transmission.
3. It is preferable, if at all feasible, to additionally record the memory of the computer to which it was attached.
4. There are three different ways to remove the phone's radio networks (Cellular network, Bluetooth, and Wi-Fi) from it:
    a. Activating flight mode on a phone
    b. Turning it off
    c. putting the phone inside a Faraday bag or other radio isolation device

PS: Each of the three approaches has its drawbacks, so it is a good idea to stay in touch with your forensic team while managing a mobile investigation.

5. Don't remove mobile device's media card, UICC, or other mobile accessories. Removing media or memory is only permitted in cases where the mobile device is broken.

VII. The Next Step - Wrapping and Transport

Once the mobile device has been separated from the various touchpoints (FSLs), it must be sealed, tagged, and handed over to the forensic analysis team at the forensic laboratory. Please note -

1. Before the mobile device is packed for transit, it's crucial to make sure that it is accurately documented, tagged, labeled, photographed, or videotaped.
2. Wrap the phone in an antistatic cloth. Digital evidence can be contained in antistatic containers, cardboard cartons, paper bags, and envelopes. Plastic shouldn't be used since it might create static electricity and allow condensation and moisture to form, which could taint or destroy the evidence.
3. All containers used to pack and store smartphones and their accessories must have legible labels.
4. The gadget should be packaged so that it doesn't get rotated, damaged, or otherwise distorted.
5. Persons responsible for transportation must advise that radio transmitters, speaker magnets, and magnetic emergency lights must be kept away from mobile devices.

VIII. Chain of Custody form

The CoC form below has been created specifically for the purpose of confiscation and transportation of mobile devices. [10].

About the case	
Chief IO:	
CASE #:	
Crime place:	
Smartphone details	
IMEI No.	
Type and Model:	
ICCID No.	
MSISDN No.	
Micro SD?	(TRUE / FALSE)
If TRUE	Micro SD details:
	MB/GB/TB:
	Serial No:
Smartphone connected to cloud storage	(TRUE / FALSE)
If True	Storage details
	Login details
	passcode:
Smartphone in Sync with accused laptop?	(TRUE / FALSE)
If TRUE	Laptop serial number:
	Laptop model:
Chain of custody	

Date	Who received it:	Sign	Remarks

IX. Conclusion

Mobile devices are now ubiquitous in the lives of more than 900 million population of India. Smartphones are rapidly making inroads and with its abilities to store and process a lot of data, investigation of mobile phones are now carrying an important role in the overall investigation ecosystem both within the LEAs and the Industry. A

proper mechanism hence is utterly important in handling a mobile device during such cybersecurity investigations. The paper has discussed a few mechanisms including a chain of custody of handling mobile devices in such investigations.

REFERENCES

[1] G. Giova, “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 1–9, 2011.

[2] J. Ćosić, Z. Ćosić, M. Bača, J. Cosic, G. Cosic, and M. Baca, “An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence,” JIOS, vol. 35, no. 1, pp. 1–13, 2011.

[3] David Bennett, “The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations”, Information Security Journal: A Global Perspective, 21:3, 159-168, DOI: 10.1080/19393555.2011.654317

[4] Tino Feri Efendi, “The Management of Physical Evidence and Chain of Custody (CoC) in Digital Forensic Laboratory Storage”, International Journal of Seocology (Science, Education, Economics, Psychology and Technology)

[5] Shetty, Anoop A., and K. Venkatesh Murthy. "Standardization of investigative process in invasive and destructive techniques of mobile forensics in India." Security Journal (2021): 1-15.

[6] Kaushik, Keshav. "Investigation on Mobile Forensics Tools to Decode Cyber Crime." Security Analytics. Chapman and Hall/CRC, 2022. 45-56.

[7] Pawlaszczyk, Dirk. "Mobile forensics–the end of a golden age." J Forensic Sci & Criminal Inves 15 (2022): 1-4.

[8] Hermawan, Tofan, et al. "Android forensic tools analysis for unsend chat on social media." 2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI). IEEE, 2020.

[9] Tanner, April, and Jason Bruno. "Timely: A chain of custody data visualizer." 2019 SoutheastCon. IEEE, 2019.

[10] Shashank Anand, IPS, & Abhishek Kumar Sardar Vallabhbhai Patel National Police Academy Journal Vol. LXX, No. 1, 1-7

[11] G. Giova, “Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems,” Int. J. Comput. Sci. Netw. Secur., vol. 11, no. 1, pp. 1–9, 2011.

[12] J. Ćosić, Z. Ćosić, M. Bača, J. Cosic, G. Cosic, and M. Baca, “An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence,” JIOS, vol. 35, no. 1, pp. 1–13, 2011.

[13] David Bennett, “The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations”, Information Security Journal: A Global Perspective, 21:3, 159-168, DOI: 10.1080/19393555.2011.654317

[14] Somaya Adwan , Fahad Salamah “A Manual Mobile phone forensic approach towards the analysis of WhatsApp Seven-Minute Delete Feature”

[15] https://articles.forensicfocus.com/2011/08/22/the-challenges-facing-computer-forensics-investigators-in-obtaining-information-from-mobile-devices-for-use-in-criminal-investigations/

[16] Žaklina Spalevi, Željko Bjelajac, Marko Cari, ‘The Importance And The Role Of Forensics Of Mobile’. FACTA UNIVERSITATIS, Ser: Elec. Energ. Published by the University of Niš, Serbia. Vol. 25, No 2, August 2012, pp. 121-136.

[17] S Kumar Reddy Mallidi & Parimala Palli. “A Comprehensive Analysis of Smartphone Forensics & Data Acquisitions”. International Journal of Advanced Research in Computer Science and Software Engineering

[18] Schrittwieser, Peter Fruehwirt, Peter Kieseberg, Edgar Weippl. “Security and Privacy of Smartphone Messaging Applications”, Robin Mueller, Sebastian 2014 978-1-4503-3001-5/14/125.

[19] Tino Feri Efendi, “The Management of Physical Evidence and Chain of Custody (CoC) in Digital Forensic Laboratory Storage”, International Journal of Seocology (Science, Education, Economics, Psychology and Technology)

[20] J. A. Kramer, "DroidSpotter: A Forensic Tool for Android Location Data Collection and Analysis," Digital Repository,Ames, IA 50011, United States, 2013.

[21] "The Volatility Foundation," The Volatility Foundation, [Online]. Available: http://www.volatilityfoundation.org/. [Accessed 13 November 2022].