Forensic Data Extraction from UVC Camera-embedded Spy Devices: A Case Study

Prakhar Prasoon, Gouri R. Uplenchwar, P N Ramakrishnan, M Krishna
Central Forensic Science Laboratory, Directorate of Forensic Science Services, Hyderabad, Telangana, India

Corresponding Authors: Prakhar Prasoon, Gouri R. Uplenchwar

***Abstract*— The present paper presents an interesting case study of spy cameras, exploring their ethical and legal implications. The case study examines a 'm MHB Keychain Spy Camera' and its memory card to determine the presence of an accused individual in recorded video clips. Using versatile forensic tools like Cellebrite UFED Touch 2 and Encase, data extraction and analysis were conducted, recovering seven incriminating video clips and numerous images. Discrepancies in image counts between tools were observed. This comprehensive approach underscored the importance of employing diverse forensic methodologies for extracting, interpreting, and finalizing digital evidence report. It highlights the challenges posed by hidden surveillance devices, emphasizing the significance of legal and ethical considerations of their use in vital installation and breach of national security.**

***Keywords*—UVC Camera Device, UFED Touch 2, Encase, Spy Camera**

I. INTRODUCTION

A spy camera, also known as a covert or hidden camera, is a device employed to capture images or videos of subjects, frequently individuals, without their awareness. These cameras are often concealed from the subjects' view, either by being camouflaged as other objects or by remaining entirely unseen. Such covert cameras are commonly utilized as a means of surveillance [1].

In the realm of surveillance, the term "hidden camera" denotes recording subjects without their knowledge or consent, while "spy camera" implies that subjects would object to being recorded if aware of its presence [4]. Conversely, "security camera" refers to visible cameras or those accompanied by notices, ensuring subjects are aware of being filmed.

Hidden cameras find diverse applications including property security, personal monitoring, photography, and entertainment, although their usage extends to espionage or surveillance by law enforcement, intelligence agencies, corporations, and various entities. Unfortunately, they are also employed for illicit activities such as criminal reconnaissance, stalking, or voyeurism [1].

The utilization of hidden cameras poses significant challenges to personal privacy rights. These covert devices often raise ethical concerns as they capture footage without individuals' knowledge or consent, potentially intruding upon private spaces or sensitive situations. Legal considerations surrounding their use vary considerably based on jurisdiction, encompassing laws related to surveillance, privacy, and consent. In many regions, the legality of hidden camera uses hinges on factors such as the location of recording, the expectation of privacy in that particular space, and the purpose for which the recordings are being made. Consequently, navigating the legal landscape around hidden cameras involves a complex interplay of local laws, regulations, and ethical considerations [4].

Many spy cameras leverage USB Video Class (UVC) Cameras for their exceptional bandwidth, reliability, and seamless integration. These cameras feature prominently across various applications, including biometric and access control systems, robotic vision, medical imaging, surveillance drones, augmented reality, and numerous other fields. UVC cameras operate as USB-powered devices with built-in standard video streaming capabilities, facilitating smooth connectivity with host machines [3]. These cameras are characterized by standard and class-specific descriptors, which are data structures employed to outline the capabilities of a USB device. The comprehensive set of class-specific video control (VC) unit/terminal descriptors provides a complete description of the video function to the host [6].

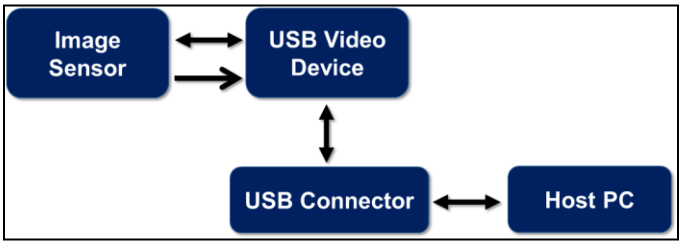


Figure 1: Block diagram of USB video class application

In the laboratory, a case involving a suspected 'm MHB Keychain Spy Camera' shown in Figure-2 was received for examination. The forensic examination entails analyzing a spy device, a memory card, and a photograph of the suspect to determine if the individual was present in the video clips recorded by that particular spy camera. The memory card was subjected to Physical Extraction using Cellebrite Universal Forensic Extraction Device (UFED) Touch 2 Device Version 7.60.0.222 which created UFED Dump file which was further parsed using Cellebrite Physical Analyzer Version 7.62.0.59. Also, it has been imaged and examined using Encase Version 6.19 as 'E01' image.

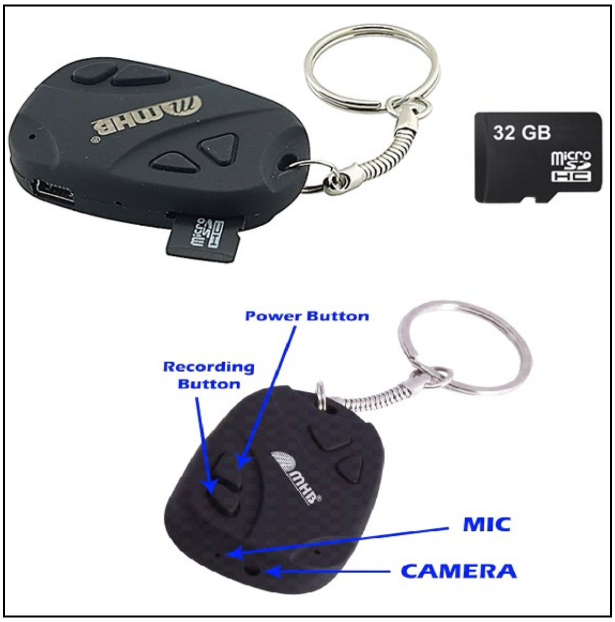


Figure 2: MHB Keychain Spy Camera with micro-SD Memory Card 32 GB

II. MATERIALS AND METHODOLOGY

Upon its connection to the FRED Forensic Workstation, the initial step involved evaluating its functionality. The spy camera, identified as General-UVC during this process, exhibited a blinking indicator that served as confirmation of its operational status, thereby validating the functionality of the device. The analysis commenced by utilizing the specialized hardware Cellebrite Universal Forensic Extraction Device (UFED) Touch 2 Device Version 7.60.0.222 shown in Figure 3, specifically designed for data extraction from diverse digital devices, including memory cards. This tool established a connection with the memory card, initiating a comprehensive physical extraction process. This process aimed to capture both visible and deleted data, generating a UFED dump file—a complete, unaltered copy of the memory card's content in a raw format. The steps involved in extraction of the data from the memory card has been shown in Figure 4.

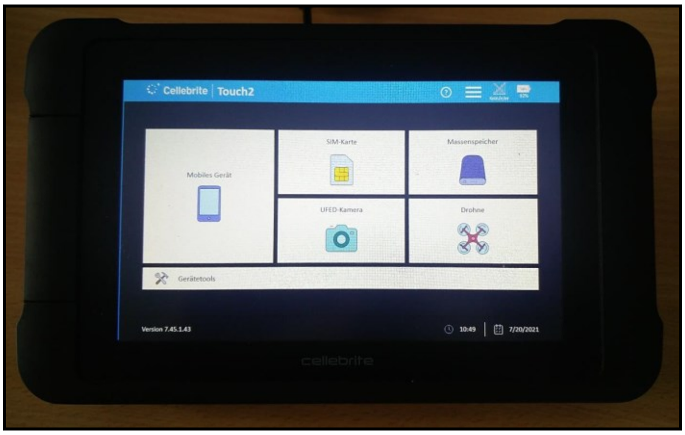


Figure 3: Cellebrite UFED Touch 2 Device

Initially, the memory card underwent connection to the UFED Touch 2 via the Cellebrite Memory Card Reader (set to Write Blocked mode) shown in Figure 5, where the Mass Storage option was activated. Subsequently, the 'Mass storage device' was specifically chosen, followed by the selection of the Physical method within the extraction type, opting for the Method 1 mode. Lastly, the destination hard drive was connected, and the extraction location interface involved the selection of the 'Removable Drive' option.

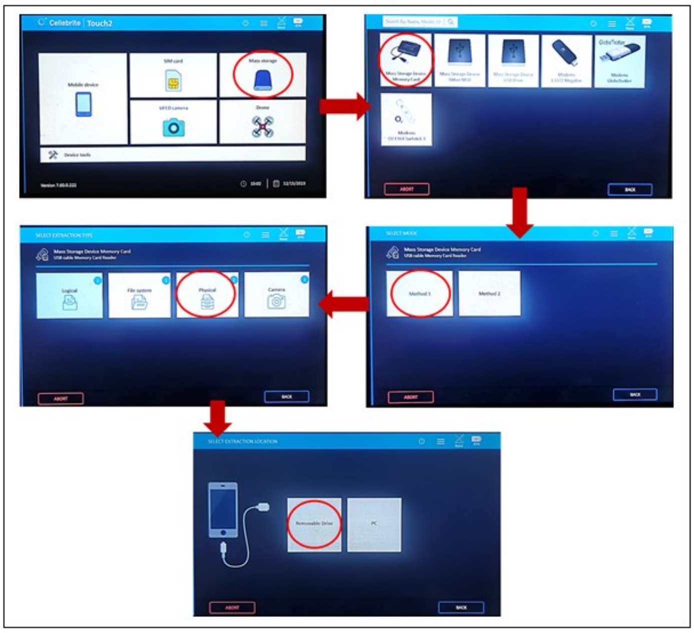


Figure 4: Steps involved in the extraction of data from Memory Card

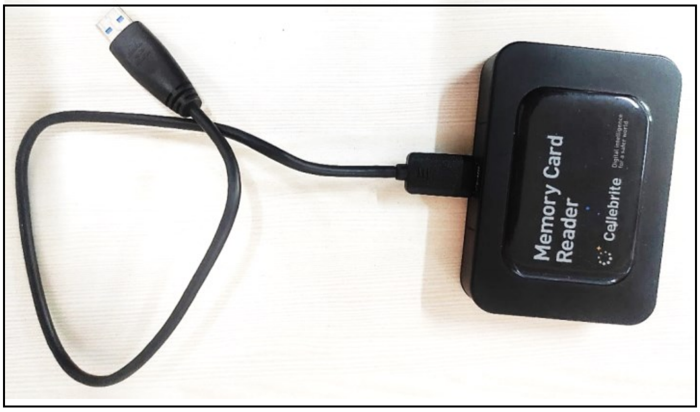
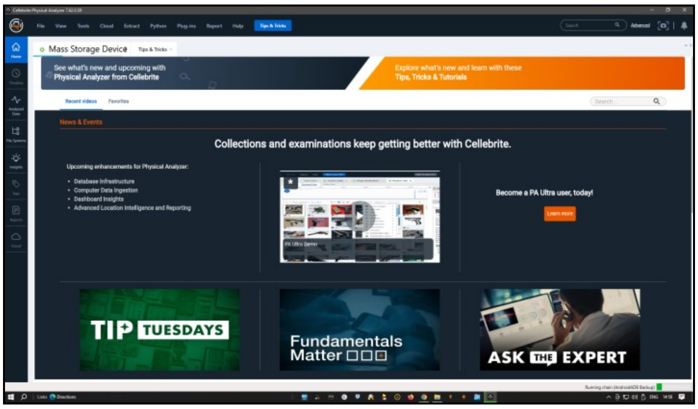


Figure 5: Cellebrite Memory Card Reader

Subsequently, the data obtained in the UFED dump file having '.ufdx extension' underwent analysis using the Cellebrite Physical Analyzer Version 7.62.0.59 shown in Figure 6. This software facilitated the interpretation and organization of the extracted data. Through parsing and structuring, it transformed the complex raw data into a comprehensible format, enabling systematic examination and identification of relevant evidence by forensic examiners [5].



See what's new and upcoming with Physical Analyzer from Cellebrite

Explore what's new and learn with these Tips, Tricks & Tutorials

Collections and examinations keep getting better with Cellebrite.

Upcoming enhancements for Physical Analyzer:

- Database Infrastructure
- Computer Data Ingestion
- Dashboard Insights
- Advanced Location Intelligence and Reporting

Become a PA Ultra user, today!

Figure 6 Parsing of .ufdx file using Cellebrite Physical Analyzer v 7.62

Moreover, the memory card which was imaged and same was analaysed using Encase Version 6.19 in '.E01' format. Extracted data accessible from the memory card has been retrieved along with their MAC properties [2].

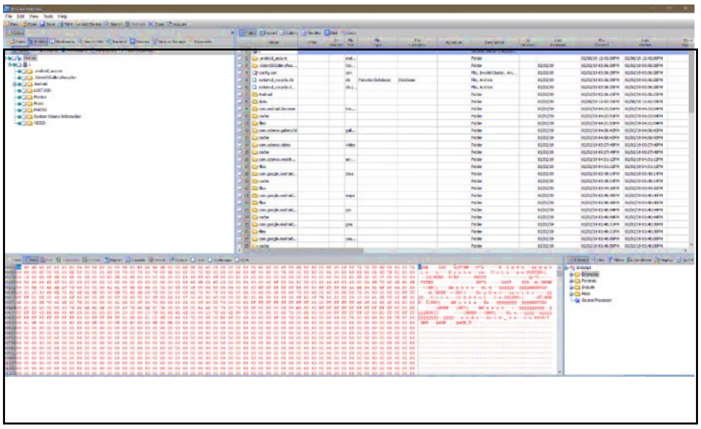


Figure 7 Analysing imaged data using Encase Software

This cardinal standard methodological approach involving specialized hardware and advanced software tools ensured a systematic and detailed process for extracting, analysing, and interpreting digital data from memory cards, supporting forensic analysis and legal validations.

III. RESULTS AND DISCUSSION

After the forensic examination and analysis of the suspected 'm MHB Keychain Spy Camera', utilizing tools like Cellebrite UFED Touch 2 and Encase, significant digital data was recovered from the memory card. After analyzing it with Cellebrite Physical Analyzer Version 7.62.0.9, seven video clips and 7,529 images were recovered. Subsequently, when the same memory card was imaged with Encase Version 6.19, the same seven video clips were retrieved, but the number of images retrieved was less, a discrepancy in the number of images was noted in comparison to UFED Physical Analyzer. This variation in the quantity of images emphasizes the significance of using diverse forensic techniques to ensure thorough data retrieval. It also brings attention to the possible differences in outcomes between various forensic tools during the analysis of digital evidence. Further file property studies like file extension, Hex codes, codecs, metadata and other pixel properties are required, particularly concerning the involvement of the accused individual in the video recordings.

IV. CONCLUSION

The examination and analysis involving the ‘m MHB Keychain Spy Camera' and its associated memory card utilized comprehensive forensic methodologies. The extraction and analysis conducted through tools like Cellebrite UFED Touch 2 and Encase resulted in the recovery of crucial digital content, comprising seven video clips and a significant number of images. Notably, discrepancies in image counts between the tools were observed, emphasizing the importance of employing multiple forensic techniques for comprehensive data retrieval and analysis in such cases. This case study underscores the critical role of forensic procedures in uncovering digital evidence, albeit needing further expert scrutiny, especially concerning the presence of the accused individual in the recorded video clips. However, the conclusions drawn from the retrieved data, including the presence of the suspect in the video clips recorded by the spy camera, would require further study and analysis by forensic experts and legal authorities including the codecs and metadata of the images and the videos for the authentication generated by such UVC-Cameras can scientifically strengthen the authentication and veracity.

LIST OF ABBREVIATIONS

UVC	USB Video Class
UFED	Universal Forensic Extraction Device

ACKNOWLEDGMENT

The authors are thankful to Shri Sujay Saha, Director, CFSL Hyderabad for constant encouragement and support for carrying out R&D activities. Also, the authors wish to thank the senior scientists of Digital Forensics Division, CFSL Hyderabad for the technical know-how and support during the critical stage of interpretation and finalizing the paper.

REFERENCES

[1] Herodotou, S., & Hao, F. (2023). Spying on the Spy: Security Analysis of Hidden Cameras. 1–19. http://arxiv.org/abs/2306.00610

[2] Javed, A. R., Ahmed, W., Alazab, M., Jalil, Z., Kifayat, K., & Gadekallu, T. R. (2022). A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. IEEE Access, 10, 11065–11089. https://doi.org/10.1109/ACCESS.2022.3142508

[3] Krejcar, O. (2013). Motion detection using a USB camera. INES 2013 - IEEE 17th International Conference on Intelligent Engineering Systems, Proceedings, 281–286. https://doi.org/10.1109/INES.2013.6632827

[4] Liu, T., Liu, Z., Huang, J., Tan, R., & Tan, Z. (2018). Detecting wireless spy cameras via stimulating and probing. MobiSys 2018 - Proceedings of the 16th ACM International Conference on Mobile Systems, Applications, and Services, 243–255. https://doi.org/10.1145/3210240.3210332

[5] Shukla, R. K., Agrawal, J., Sharma, S., & Tomer, G. S. (2019). Data, Engineering and Applications: Volume 2. In Data, Engineering and Applications: Volume 2 (Vol. 2). Springer Singapore. https://doi.org/10.1007/978-981-13-6351-1

[6] Wlodek, J., & Gofron, K. J. (n.d.). ADUVC - AN EPICS AREADETECTOR DRIVER FOR USB VIDEO CLASS DEVICES also at Stony Brook University , Stony Brook , USA. https://doi.org/10.18429/JACoW-ICALEPCS2019-WEPHA174