Journal of Forensic Sciences And Criminal Investigation ISSN: 2476-1311



DOI: 10.19080/JFSCI.2024.18.555983



J Forensic Sci & Criminal Inves Copyright © All rights are reserved by Prakhar Prasoon

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



Prakhar Prasoon*, Gouri R Uplenchwar*, Ramakrishnan PN and Krishna M

Central Forensic Science Laboratory, Directorate of Forensic Science Services, India

Submission: January 04, 2024; Published: February 27, 2024

*Corresponding author: Prakhar Prasoon, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India, Ramanthapur, Hyderabad, Telangana, India, Email: prakhar.prasoon01@gmail.com

Gouri R Uplenchwar, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India, Ramanthapur, Hyderabad, Telangana, India, Email: gouriru312000@gmail.com

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 device; UFED Touch 2; Encase; Spy camera

Abbreviations: UVC: USB Video Class; UFED: Universal Forensic Extraction Device

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. 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.

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 [2].

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 classspecific descriptors, which are data structures employed to outline the capabilities of a USB device. The comprehensive set of classspecific video control (VC) unit/terminal descriptors provides a complete description of the video function to the host [4]. Keychain Spy Camera' shown in Figures 1 & 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.

In the laboratory, a case involving a suspected 'm MHB





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, 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 3 [5] Figure 4.



003 How to cite this article: Prakhar Prasoon, Gouri R Uplenchwar, Ramakrishnan PN, Krishna M. Forensic Data Extraction from UVC Camera-Embedded Spy Devices: A Case Study. J Forensic Sci & Criminal Inves. 2024; 18(2): 555983. DOI: 10.19080/JFSCI.2024.18.555983



file Life Year Task Ting												
Des gibe gibe give Grantes Riters Bitres Xite Base												
Low William and the second states and	XEX	a gloon Han	Sinks 0	04 00								
Con Star Under Carten Chess Con Substant Phen	1.0	-	1.0	1. 1.			200.0	Dereta	1.8.1.1.1	int Pe	14	
The Orbitan Stream (Taken Latherts	-			Sear 14	C. P. L	Longer .		In su have here	ware to	rest Overs		-
at /s form	2.3	O attail store		and .				100		10112-007	DEDOGRA	
9408-	1.5	Co Coloritative		Ġ.,				Na	101019	101019-003-087	CODD30N	
- Carlos and a constant of the second	24	2 ofter		-				R. INSTARLAS.	101019	101010-00307	GUNDARY.	
- DisOlideylesple	2.4	Control (solution C			Parcle Deblers	Dollar		8,804	NAME OF TAXABLE	KAUP IS A OF	SUCCESSION OF	
De la sete	21	anterd, souled.		41.				8,804	NAME OF TAXABLE	STATISTICS.	STORAGE ST	
a Co Rein	21	Change of the second						Nik	1000	STATISTICS.	SALTHER ADD	
- 00 Ref.	21	C de						Nie	1000	10010-0010	ADDITION OF A DISCOUNT	
+ 70 MOD	2.4	Constationer		he.,				Nie	adada	0,0,0,0,0,0,0,0,0	approxime.	
-	25	Conte						Nie	100	100/04/04/02/04	ERCHARDER.	
-+7 <u>0</u> ED	28	01						NH	8(0)9	REAL PROPERTY	ERCHARDER.	
	2.8	Conciles pletti		p .		-	-	7478	60079	101039 H-31-674	EXCHARGE	
	20	Quarter Quarte	_			_	-	Terme .	10/0/9	10009143404	EESHRAM	
	28	0.01.000.400					-	N/W	101019	101034007-074	END-ROADA	
		U ON					-	NIN	1000	101010-001-014	000000494	
		Containings.		×			-	NOV	1000	101019-040129	ENCOMPLET.	
	140			-				100	1000	COLUMN STATE	COLUMN STATE	
	152	Date:		-				No.	1000	COLUMN TWO IS NOT	COLUMN ALON	
	110	24						-	-	COLUMN TWO IS NOT	COLUMN IN STREET	
		Description		-				No.	and the local division of the local division	122004-07	STATISTICS.	
	1.1	04		-				Nie	shite	skine er	although a	
		Omental and a					-	Nite	suburbs	100310-0-07	ERCHARMENT	
	2.5	Quele						Nie	10/10/19	100040404	680904H	
	28	Comprohented.		10				NR	10/079	1000940-009	SIGNER AND READER	
	28	0.4						NO	101079	000910-009	REPORTE	
	27	Comprehensed.		×				NOT	10/0/9	000000000	GORDADAN	
	2.2	Contra Co	_		_			NIK	101019	000004099	DOPD49N	
	4							100.000	1 10 10 10	1. A		
			40 ME ME ME ME 1 40 ME ME ME ME 1 40 ME ME ME ME ME 1 34 ME ME ME ME ME ME 1 44 ME ME ME ME ME ME 1 42 ME ME ME ME ME ME	NO GA NO NO NO NO			an Love	A LAN	11 4111 12 4100 13 4100 10 4100 10 4100	A Contraction of the contraction		
						10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10 10		i di seco i di seco i di di di di seco di	1100 - 110 1000 - 110 1000 - 110 1000 - 110	-		
	N N			X0 X1 44 X0 X2 44	Image Image <th< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>							

How to cite this article: Prakhar Prasoon, Gouri R Uplenchwar, Ramakrishnan PN, Krishna M. Forensic Data Extraction from UVC Camera-Embedded Spy Devices: A Case Study. J Forensic Sci & Criminal Inves. 2024; 18(2): 555983. DOI: 10.19080/JFSCI.2024.18.555983

004

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 4, 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. Subsequently, the data obtained in the UFED dump file having 'ufdx extension' underwent analysis using the Cellebrite Physical Analyzer Version 7.62.0.59. 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]. 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 [6].

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.

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.

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.

Conflict of Interests

The authors declare that they have no competing interests.

Acknowledgement

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 DFD, CFSL Hyderabad for the technical know-how and support during the critical stage of interpretation and finalizing the paper.

References

- Herodotou S, Hao F (2023) Spying on the Spy: Security Analysis of Hidden Cameras. Arxiv, Cornell University, 1-19.
- 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.
- Krejcar O (2013) Motion detection using a USB camera. INES 2013

 IEEE 17th International Conference on Intelligent Engineering Systems, Proceedings 281-286.
- Wlodek J, Gofron KJ (n.d.). ADUVC AN EPICS AREADETECTOR DRIV-ER FOR USB VIDEO CLASS DEVICES also at Stony Brook University , Stony Brook , USA.
- Shukla RK, Agrawal J, Sharma S, Tomer GS (2019) Data, Engineering and Applications: Volume 2. In: Data, Engineering and Applications. Springer Singapore.
- Javed AR, Ahmed W, Alazab M, Jalil Z, Kifayat K, et al. (2022) A Comprehensive Survey on Computer Forensics: State-of-the-Art, Tools, Techniques, Challenges, and Future Directions. IEEE Access 10: 11065-11089.



This work is licensed under Creative Commons Attribution 4.0 License DOI: 10.19080/JFSCI.2024.18.555983

Your next submission with Juniper Publishers will reach you the below assets

- Quality Editorial service
- Swift Peer Review
- Reprints availability
- E-prints Service
- Manuscript Podcast for convenient understanding
- Global attainment for your research
- Manuscript accessibility in different formats (Pdf, E-pub, Full Text, Audio)
- Unceasing customer service

Track the below URL for one-step submission https://juniperpublishers.com/online-submission.php