U.S. Secret Service
Cleveland Field Office
Digital Evidence
Forensic Lab

Digital Forensic Exam Report

Examiner: Special Agent Michael Braun
Case Number: 203-866-51642
Phone: 216-750-2058
Email: michael.a.braun@usss.dhs.gov

Report Date: 02/02/2024
Requestor: Detective Matthew Mysliwiec, Cuyahoga County Sheriff's Office

Synopsis of Investigation:

On January 22, 2024 Detective Matthew Mysliwiec Cuyahoga County Sheriff's Office (CCSO), requested the assistance of the U.S. Secret Service (USSS), Cleveland Field Office's Digital Evidence Forensic Lab (DEFL) to image and process multiple pieces of digital evidence pursuant to a State Search Warrant, signed on January 19, 2024. These items correspond with CCSO case number 2024-002456 and USSS case number 203-866-51642.

On 01/22/2024, the DEFL received the below listed items for processing.

Items Examined:

On 01/22/2024, the lab received the following pieces of electronic media for forensic processing:

Item 9: Lenovo Yoga 2 Pro Laptop SN: [redacted]
Item 10-1: Lenovo ThinkPad X1 Carbon Laptop SN: [redacted]
Item 10-2: SanDisk Extreme Pro MicroSD Card SN: [redacted]
Item 10-3: Generic USB Drive – Dodd Camera branded
Item 10-4: Generic USB Drive – Black
Item 18: Google Pixel 6a Cell Phone SN: [redacted]

Details of Examination:

On or about 01/22/2024, the DEFL began processing the above digital media.

The forensic computer examination is designed to provide information on what data is present on the subject media. The forensic computer examination consists of making an exact copy of subject media and placing original media in evidence. It is the copy, also called the image, which is examined with forensic software which prevents adding, removing, or altering the original files.

All items were forensically imaged as described below and the results have been provided to the case agent.

Specific Findings and Facts:

Item 9 – Lenovo Yoga 2 Pro Laptop:

On 01/22/2024, I began processing this device. The drive was removed from the laptop and imaged using my Tableau TX1 imager, version 22.3.0. The drive contained the following identifiers:

Forensic Report

Make: SAMSUNG
Model: MZMTE256HMHP-000L1
Capacity: 256 GB
Acquisition MD5 Hash: 3440ba2011c2d0c6d7f9a3f5e3cd57b7

This image was then processed using Axiom (Ver. 7.8.0.38310.) A portable case was generated by the tool and provided to the requester for further analysis.

Item 10-1: Lenovo ThinkPad X1 Carbon Laptop:

On 01/31/2024, I began processing this device. This drive had BitLocker encryption running on the data partition, however the key was stored clear (unencrypted.) This allows my forensic tools to decrypt the partition without entering the BitLocker key. The drive was removed from the laptop, connected to my forensic workstation through a Tableau T7u write-blocker and imaged with FEX Imager (Ver.2.2.0(263).) The drive contained the following identifiers:

Make: Western Digital
Model: NVMe WDC PC SN730 SDB
Serial Number: [redacted]
Capacity: 256 GB
Acquisition SHA256 Hash: 01a2f48b9d56b3aa9a326ade12fc7b5003f060cc484a7b861476e08d5d732ec5

This image was then processed using Axiom (Ver. 7.8.0.38310.) A portable case was generated by the tool and provided to the requester for further analysis.

Item 10-2: SanDisk Extreme Pro MicroSD Card:

On 01/22/2024, I began processing this device. The microSD card was connected to my forensic workstation using a write-blocked Digital Intelligence card reader. An image of the device was taken using FTK Imager (Ver. 4.5.0.3.) The card contained the following identifiers:

Make: SanDisk
Model: Extreme Pro microSD
Serial Number: [redacted]
Capacity: 256 GB
Acquisition MD5 Hash: 22057983366285362e4900ccda4bc8

The image was processed using Axiom (Ver. 7.8.0.38310.) A portable case was generated by the tool and provided to the requester for further analysis.

Item 10-3: Generic USB Drive – Dodd Camera branded:

On 01/22/2024, this device was imaged using my forensic workstation and a Tableau T8u USB write blocker. The drive contained the following identifiers:

Make: Generic
Model: Specific STORAGE DEVICE USB Device
Serial Number: [redacted]
Acquisition MD5 Hash: e5c101abee59e64d4030f97d56810a35

The image was processed using Axiom (Ver. 7.8.0.38310.) A portable case was generated by the tool and provided to the requester for further analysis.

Item 10-4: Generic USB Drive – Black

On 01/22/2024, this device was imaged using my forensic workstation and a Tableau T8u USB write blocker. The drive contained the following identifiers:

Make: Generic
Model: General UDisk USB Device

Forensic Report

Serial Number: [redacted]
Acquisition MD5 Hash: 49ca8675ad5fb9152e75ed3353425cfc

The image was processed using Axiom (Ver. 7.8.0.38310). A portable case was generated by the tool and provided to the requester for further analysis.

Item 18: Google Pixel 6a Cell Phone SN: [redacted]

On 01/23/2024, I began processing this device. Using Grayshift GrayKey (Ver. 3.31.0b1) the passcode was recovered, the device was unlocked, and a full file extraction was performed. The mobile device contained the following identifiers:

Make: Google
Model: Pixel 6a
Serial Number: [redacted]
Capacity: 128 GB
Recovered Passcode: 8969
Acquisition SHA256 Hash: b786dffbc39113c232190cb39fc650f8b6a357a0acf3afe2692f553f718c4896

The image was processed using Cellebrite Physical Analyzer (Ver. 8.8.100.46). A Reader Report was generated by the tool and provided to the requester for further analysis

SPECIAL NOTICE FOR STATE AND LOCAL AUTHORITIES:

In the event that the examiner is requested to testify, a letter will need to be sent for my deposition/testimony to:

USSS
Office of Chief Counsel
Communications Center
245 Murray Lane, SW, Building T-5
Washington, DC 20223

This letter needs to follow Federal Law: Title 6, Chapter I, Part 5, Subpart C – Disclosure of Information in Litigation. The letter needs to address the scope and type of testimony the Examiner will be required to provide. After consulting with the examiner concerning the testimony our Legal Department will issue a "Touhy" letter authorizing the examiners deposition and/or testimony and limit the scope based on your request outlined in this letter. For any questions, please contact our Office of Chief Counsel at (202) 406-5771.

Conclusion:

The Cleveland Cyber Fraud Task Force (CFTF) Digital Evidence Forensic Laboratory (DEFL) had the opportunity to assist your agency in the furtherance of your criminal investigation. Please note that the CFTF DEFL forensic examiners did not perform any analysis on the data returned to you. We extracted as much available information as possible from the electronic device(s) that your office sent using the tools and methods available at the time of submission.

Requests for further examination may be directed to SA Michael Braun, telephone 216-750-2058, or email michael.a.braun@usss.dhs.gov.

Submitted by:

Michael Braun
Special Agent
U.S. Secret Service
Cleveland Field Office