TRIPLE R

Examination Report

CASE #: 001-2022

Examiner: Zachary Rousseau

# Table of Contents

Contents

[Table of Contents 1](#_Toc496005748)

[Summation 2](#_Toc496005749)

[Disclaimer 2](#_Toc496005750)

[Background 2](#_Toc496005750)

[Summary of Findings 2](#_Toc496005751)

Acquisition and [Data Analysis Tools 2](#_Toc496005752)

Acquisition  [3](#_Toc496005754)

Data Analysis and [Tools Used 3](#_Toc496005755)

[Analysis 3](#_Toc496005756)

[Item Description 3](#_Toc496005757)

[File Structure and Root contents 3](#_Toc496005758)

[Document Files 5](#_Toc496005759)

[Image Files 6](#_Toc496005760)

[Text Files 7](#_Toc496005761)

[Image Files 8](#_Toc496005762)

[Deleted Image Files 10](#_Toc496005763)

[Zip Archive 13](#_Toc496005764)

[Executable File 8](#_Toc496005762)

[Recommendations 13](#_Toc496005765)

# Summation

## Disclaimer

This document contains classified information solely for the use of ACME Inc and should not be circulated without prior written consent. If you are not the intended recipient, you may not disclose or use the information in this document in any way.

## Background

Triple R received a request from ACME Inc. to conduct a digital forensic examination. On 2 June 2019, IT Specialist, Kevin Smith, observed a USB thumbdrive marked classified in the conference room. Since the thumbdrive is an unclassified area, this was noted as a security violation and Mr. Smith took the drive over to Security. At 12:30pm on the same day, Security Officer Charles Edwards collected the drive for examination. Officer Edwards imaged the drive using FTK Imager version 3.4.3.3 and store the drive in an evidence locker.

ACME Inc. has requested Triple R to examine a separate thumbdrive containing the E01 image of the original classified drive for the following:

* Determine if files exist on the device (including deleted data)
* Determine the logical folder structure and file system
* Identify classified material
* Attempt to attribute any found data to specific person’s
* Provide recommendations for future investigative steps.

## Summary of Findings

The examination determined that the flash drive contained data including classified data. The following data was identified:

* An NTFS [[1]](#footnote-1)file system was found on the drive that contained (15) images, (3) documents, (1) executable and (1) zip archive[[2]](#footnote-2).
* Of the files found (6) images were deleted
* Of the files found (5) files contained classified information, 4 of which were deleted.
* The zip archive contained (2) additional files, both containing classified information.
* Of the files found 2 files reference John Milburn, 1 file references John and 1 File references C. Miller
* Of the files found (2) files were encrypted
* (2) files reference getting paid in exchange for documents

It is recommended that John Milburn and C. Miller be interviewed to determine their involvement with the content of the thumbdrive.

# Acquisition and Data Analysis Tools

## Acquisition

On 11 October 2022, Examiner Rousseau received a Generic Flash Disk USB Device s/n 06524F76 from Officer Charles Edwards. The thumbdrive contains an E01[[3]](#footnote-3) image created using FTK Imager 3.4.3.3 of the original classified drive discovered by Kevin Smith. The log indicates that the image was created by Officer Edwards on 2 June 2019. Utilizing QuickHash v3.3.1, the image file was verified to match the hash values contained in the log.

Acquisition and verification hashes[[4]](#footnote-4):

MD5[[5]](#footnote-5): b3f8ae848357877fed3846e2029ac170

SHA1[[6]](#footnote-6): 107480a13f75c5504b354365d9528e0c4f98400d

## Data Analysis Tools Used

For this examination the following tools were used, previously validated by Triple R:

* QuickHash v3.3.1
* Autopsy v4.19.3

# Analysis

## File Structure and Root contents

The image below displays the logical structure of the imaged drive, indicating the instance of 3 partitions including an NTFS volume, labeled “vol2”

A picture containing text

Description automatically generated

The root directory of the NTFS volume contained 2 directories, 8 images of which 3 were deleted, 1 executable, 2 documents, and 1 zip file.

### Document Files

Milburn Resume 2019.docx

MD5: a83addabf4f08e8b27aa2d2c24a37cab

|  |  |
| --- | --- |
| SHA256[[7]](#footnote-7): | 25a9a943cb811d12e13d847fdefbc273913478ac6b7e49cb9f4a342352911aa9 |

The file Milburn Resume.docx contained personal information to ACME Inc. employee, John Milburn. The file contained information regarding Mr. Milburn including his address, phone number, previous work experience, education, and skills

Graphical user interface, text, application, email

Description automatically generated

New Plan.docx

|  |  |
| --- | --- |
| MD5: | 7a2d32b864446b417d4cdb7f959b7c60 |

|  |  |
| --- | --- |
| SHA256: | c9e985f35a17be89437ecb7fc8f13a3f8f2d719328662af06f5387b4b2b782a1 |

The file New Plan.docx was an encrypted file on the thumbdrive. It was able to be read with the password discovered in [Funny.jpg](#_Image_Files). The file contained a classified image of a Software Development plan.

# Graphical user interface, application, table Description automatically generated

Blue Prints.pdf

MD5: 7a2d32b864446b417d4cdb7f959b7c60

SHA256: c9e985f35a17be89437ecb7fc8f13a3f8f2d719328662af06f5387b4b2b782a1

The file Blue Prints.pdf is a classified document containing a blueprint of 33 Richdale Avenue, Cambridge, Massachusetts. The file extension, .pdf, does not match the file signature, image/gif.

Diagram, engineering drawing

Description automatically generated

### Image Files

Email.jpg

MD5: db87eb47161ca8e0d53261f991806c27

SHA256: 4f1e25dddbf99d7e9fb558bf35a4dfacaf5948cb9f093d3f57d23149b4f2e48f

The image Email.jpg contained an email from [c.Miller@acme.com](mailto:c.Miller@acme.com) to “John.” It is titled “Hawaii” and states once “John” is on the ground to send a text to 202-555-0142 to discuss payment for “the documents.” The email is signed by “CM.”

Graphical user interface, text, application, email

Description automatically generated

Funny.jpg

MD5: 6c75ba4419f76ffaa570ce72d2acaa41

SHA256: fcc960e281600a8b9bc0aa3baf81b9febb9e24ad2404fdae5dd792a8d49d1b6a

The image Funny.jpg contained the keyword possessing a password: “B1gM0ney”.

A person in a suit

Description automatically generated with medium confidence

Trip Information.jpg

MD5: 1794cd81fcb260c3f088c9e2c8bc9fb5

SHA256: 256599a798ec58674434af2bc74639db4b15c934d31aeef90e79e9dbf3281924

The image Trip Information.jpg contained a flight confirmation for John Milburn issued 19 January 2019. The flight was booked from Ronald Reagan Washing National Airport in Arlington, Virginia to Daniel K. Inouye International Airport in Honolulu, Hawaii.

Graphical user interface, text, application, email

Description automatically generated

Meet me here after we all get paid.jpg

MD5: 14afec88719d88265e551926f00f70ba

SHA256: 3c023dd15f8d0da5d2c90fa73d8795ab997fa09cb507ae314f6655e61c2cd2d5

The image Meet me here after we all get paid.jpg depicts a flower. The Microsoft metadata indicates that it was taken by a Samsung SM-G950U. The GPS Coordinates in decimal degrees is Latitude 32.291 and Longitude -64.765 at an elevation of 16.318 ft above sea level. The coordinates point to Camden, Bermuda.



Software Dev Plan 1.png

MD5: 5aaef35feb6fec96c62fc9bf6089683b

SHA256: 688ea94832edb992f7df1aa15ecc03a7cb5524a1524d5ce8777d39178ea72466

The image Software Dev Plan 1.png is a classified image. It depicts a software Development plane from quarter 3 2011 until quarter 3 2013.

Application

Description automatically generated with medium confidence

### Deleted Image Files

F0000000.jpg

MD5: b821e8dc3d71e1964959057ba7272adb

SHA256: e8307bf5782634d3c767ae41c08d88c6caf7aff139127ef9d1e42b94f53f21b9

The deleted image F0000000.jpg contains classified information. It depicts the Network Diagram [[8]](#footnote-8)of the Telecommunications Network Architecture.

Diagram

Description automatically generated

F0000824.png

MD5: 5692c64d299cff65e257c95a58e8e350

SHA256: 6685b6a909c6f5ceb09961b08457f35dcdb14aa6a69ce46129114c0920d1942

The deleted image f0000824.png contains classified information. It depicts financial statements including historical records from 2012 to 2016 and forecast period from 2017 to 2021

Table

Description automatically generated with medium confidence

F0001408.png

MD5: d3ad53debe9d38c575360371c8a931e4

SHA256: f98db10ae3d5bc47f5d7f450fb2e2d5d63dd9444a9f037e2e0ef3dd1e702361e

The deleted image f0001408.png contains classified information. It depicts a large aircraft.

A picture containing text, outdoor

Description automatically generated

### Zip Archive

Transfer.zip

MD5: 5a391af27550b1188b0ae50bcf22ea46

SHA256: 80c04429b56881a14611eef1a5c1707a592e10d73beca3f17ecbdad9f19a8168

The contents of Transfer.zip contains two files Future Aircraft.png and Network Map.png. The hashes and contents of these files match that of two deleted files found on the drive. Network Map.pdf was only able to be viewed when the file extension was changed to .png. Future Aircraft.png is a duplicate of f0001408.png and Network Map.pdf is a duplicate of f0000000.pdf.

Future Aircraft.png

MD5: d3ad53debe9d38c575360371c8a931e4

SHA-256: f98db10ae3d5bc47f5d7f450fb2e2d5d63dd9444a9f037e2e0ef3dd1e702361e

A picture containing text, outdoor

Description automatically generated

Network Map.pdf

MD5: b821e8dc3d71e1964959057ba7272adb

SHA256: e8307bf5782634d3c767ae41c08d88c6caf7aff139127ef9d1e42b94f53f21b9

A picture containing text, sky, map

Description automatically generated

### Executable File

Click Me.exe

MD5: 6c2f8f93764f7023d92974a916389a36

SHA256: 861966a21e80d0336c31bee66ebea6bd5709ca918194a4493b7dd1223d716d89a

Click Me.exe is located in the root directory of “vol2.” Analysis shows that it is a Ransomware virus[[9]](#footnote-9) and all files on connected devices will be locked upon execution. Indicates that all files will be exfilled to the IP address[[10]](#footnote-10) 80.92.160.32.



# Recommendations

Triple R recommends the following actions that could help further the investigation:

* Interview John Milburn to discuss the content found on the thumbdrive and his knowledge regarding the classified information contained on the drive and the plans to sell the information
* Identify and Interview C. Miller to determine his involvement with the data and correspondence with Mr. Milburn
* Conduct malware analysis to determine the source and any known characteristic of the ransomware virus found.
* Notify law enforcement of the malware found on the thumbdrive
* Personal documents belonging to John Milburn indicates that he may be the owner of the thumbdrive
* It is reasonable to state that the owner of the thumbdrive may have been aware of the allocated classified information located on the thumbdrive
* While there is evidence indicating that Mr. Milburn may have knowingly been in possession of classified within an unclassified area. There is not enough information to definitively indict Mr. Milburn. Further investigation is required.

1. NTFS is an acronym that stands for New Technology File System. It was first released by Microsoft in 1993 along with Windows NT 3.1 and has been the primary file system used by Microsoft Since [↑](#footnote-ref-1)
2. ZIP is an archive file format that can compress multiple files and directories without loss [↑](#footnote-ref-2)
3. An E01 image is a forensic image containing a direct bit-for-bit copy including additional data within the forensic image format. [↑](#footnote-ref-3)
4. A digital fingerprint generated using a one-way cryptographic algorithm [↑](#footnote-ref-4)
5. MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value [↑](#footnote-ref-5)
6. SHA-1 is an acronym that stands for Secure Hash Algorithm 1. It produces a 160-bit hash value [↑](#footnote-ref-6)
7. An Acronym for Secure Hashing Algorithm 256. Produces a 256-bit hash value. [↑](#footnote-ref-7)
8. A Network Diagram is a visual representation of a telecommunications networks. It displays devices that make up a network and how they are connected including routers, firewalls, computers, etc. [↑](#footnote-ref-8)
9. Ransomware is a type of malware blocking data from being used unless a ransom is paid. [↑](#footnote-ref-9)
10. An IP address is a unique number indicating a device on the local network or across the internet [↑](#footnote-ref-10)