Digital Forensics Company LLC

DIGITAL FORENSIC ACTIVITY REPORT

Case Title: Forensic Report #1 CMIT 424 Spring 2020	**Case Number:** PAGS01
Digital Forensics Company, LLC Address: 123 Forensics Street, Denver, CO 80135	**Report Date:** February 15, 2020
Examiner: Dmitry Landy #891920	**Examiner Signature:** Dmitry Landy

Report Subject
Digital Evidence Report – Verbatim USB Drive, black, 2.0GB, Serial #23097JR2. Marked as USB02_032816_4-2".

BACKGROUND

On December 12, 2019, James Randell (Practical Applied Gaming Solutions, Inc (PAGS) president and owner) requested an investigation to be conducted to determine the unexpected resignation of George Dean (PAGS Assistant Chief Security Officer). Norbert Singh (Human Resources Officer) had reported that Mr. Dean left a voicemail tendering his resignation effective immediately. An investigation of Mr. Dean's office was performed. During the investigation, a USB drive was recovered for further examination in order to determine why Mr. Dean left suddenly and what he was doing prior to his resignation.

TABLE OF CONTENTS

LEGAL AUTHORITY

James Randell, the owner and president of Practical Applied Gaming Solutions, Inc, provided legal consent to Digital Forensics Company LLC to assist in the investigation for case 0001.

ASSESSMENT OF PREVIOUS INVESTIGATION

Due to the abrupt resignation of Mr. Dean, Mr. Singh reported it to his supervisor Ms. Betty Mayne (Chief Security Officer). Ms. Mayne opened Mr. Dean's office, per Mr. Singh's request, to find an unusually organized office. Additionally, the company laptop and workstation were both missing. Mr. Randell requested a further investigation of this.

The workstation, along with two other company computers, was taken to the IT Service Center that week to be wiped and reimaged due to a rootkit. They were expected back the following Friday by 10:00 AM. Ms. Mayne requested all work on the computers to stop immediately and be returned. The company-issued laptop was used by Mr. Dean as a temporary replacement for the workstation. Although the laptop was not found in the office, an empty laptop case was. It contained a single 2GB USB drive, which was discovered by Mr. Singh and Ms.Mayne. Initial examination of the USB contents revealed files relating to Mr.Dean's duties as Assistant Chief Security Officer and nothing inappropriate.

The initial findings were both inaccurate and invalid as the data recovered did contain inappropriate content. This inappropriate content was found after conducting file carving in order to discover additional files in the unallocated space of the drive. The partitioned drive did not contain any inappropriate material.

INITIAL PROCESSING

On August 21, 2016, Digital Forensics Company LLC processed the submitted USB drive " USB02_032816_4-2". The processing included inspection, photography, anti-virus (AV) scan, and the forensic imaging of the USB drive. The forensic imaging of the digital media created forensic evidence files for use in subsequent forensic examination of the digital media. Methods were forensically sound and verifiable

During an AV scan, USB02_032816_4-2 was identified as containing 0 infected files.

Acquisition MD5 hash: bc1bedd931cacfd5bc4004ec9ef2fb3e
Verification MD5 hash: bc1bedd931cacfd5bc4004ec9ef2fb3e

See ADDENDUM A "Evidence Photos" and ADDENDUM B, "Steps Taken" for more information.

PRELIMINARY FINDINGS

The digital analysis of the contents of the USB drive resulted in 70 out of 216 files forensically interesting (the majority being duplicates). The drive contained a single partition with the rest being unallocated space. The total capacity of the drive was reported by WinHex to be 496MB when it was a

2GB drive. Partition 1 (the only partition) used the FAT16 file system, had volume name PAGS01 and had 495 MB of space with 95% of it unused. There was a total of 511KB of unused or inter-partition space. File carving was performed using WinHex to reveal and an additional 149 files. These files were further analyzed using EnCase.

Please see "Detailed Findings" below for more information.

DETAILED FINDINGS / ANALYSIS

After acquiring the forensic copy (PAGS01_06132014.E01) of PAGS01_06132014, FTK Imager was used to convert that file into a raw data file. The post-processing hash was used to confirm that no changes to the file were made. WinHex was used to the raw data file to review the data's logical structure. The following provides the structure and additional description of the drive:

1. Total capacity: 496 MB
2. Partitioning style: MBR
3. Unpartitionable space: 960 Sectors
4. Partition 1
    a. Sectors 62 - 1,013,823
    b. Partition table: Sector 0
    c. File system: FAT16
    d. Name: PAGS01
    e. Total capacity: 495 MB
    f. Free clusters: 95% free
    g. Volume label date: 06/13/2014 21:37:36
5. Unused inter-partition space:
    a. Sectors 0 - 61 (31.0 KB)
    b. Sectors 1,013,824 - 1,014,783 (480 KB)
    c. Total space= 511 KB

Analyzing the structure revealed that only 496 MB was recognized by the drive when it should be 2GB. To further analyze this, WinHex performed file carving on the raw data file which revealed an additional 149 files. The images were screened for any child pornography (none were found) and then exported to be analyzed by EnCase.

After analyzing the processed forensic files, a list of all the files was exported to a spreadsheet to be further analyzed and sorted. All forensically interesting files remained in the spreadsheet while the rest were discarded. This new spreadsheet (FR1_Inventory_Landy.xlsx) has comments and other additional information about the forensically interesting files.

CONCLUSIONS

The analysis of the USB drive left in the laptop case was not able to reveal anything about the following questions:

1. What was George Dean up to before he resigned?
2. Why did he resign so suddenly?

Although there were an additional 149 file recovered through file carving, only 1 of those files was inappropriate (adult pornography). 68 other files were duplicates based on their MD5 hash. However, no files were able to provide insight as to why George Dean was doing prior to leaving, nor why he left so suddenly.

Further investigation and analysis is recommended to confirm these findings and conclusions and may be the subject of future digital forensic reports.

SOFTWARE UTILIZED

Collecting the evidence involved the following software

SOFTWARE	HOW USED
Samuri Paladin	Created forensically sterile media to be used for imaging operation as the target media.
FTK Imager 2.6.0.49	Create a forensic copy of the USB drive onto the target media (PAGS01_06132014.E01). Create a raw data file of PAGS01_06132014.E01 to be to be analyzed in WinHex
WinHex 18.8	Analyze raw data file to review the file structure and perform brief low-level analysis of partition
EnCase 8.09.00.192	Analyzed forensic image file and its contents. Exported evidence item inventory to a spreadsheet.

HARDWARE UTILIZED

Collecting the evidence involved the following hardware.

HARDWARE	HOW USED
Verbatim USB Drive Serial #23097JR2 (USB02_032816_4-2)	The recovered USB Drive of Mr. Dean
LEXAR JUMPDRIVE USB Device Serial #8KRZ24B (PAGS01_06132014)	Target USB Drive to store the forensic copy.

DIGITAL MEDIA PROCESSED

The following digital media was submitted and processed.

PHOTOGRAPH OF DIGITAL MEDIA& IMAGING PROCESS	DESCRIPTION OF ITEMS SUBMITTED
See ADDENDUM A	Include serial numbers and how marked as evidence.

DISPOSITION OF EVIDENCE

USB Drive marked as "USB02_032816_4-2" and assigned inventory #1 is currently secured in the evidence locker at Digital Forensics Company LCC building.

Note that each piece of evidence in this case has been secured and filed with its own individual chain of custody form.

GLOSSARY

Data Carving– A process involving the examination of media for content relating to multiple types of empty space (i.e. slack space, unused space, unallocated space).

Deleted Files–Files that may have been deleted by the computer user or operating system. Normally deleted files are not removed from the hard drive. The deletion process only alters a directory entry in most cases. This leaves deleted files accessible to forensic examinations.

Digital Evidence– Information stored or transmitted in binary form that may be relied upon in court.

File Slack – The space between the end of the file data and the end of the cluster. File slack may contain data from previous files that has been previously overwritten.

Forensic Image – A bit stream copy of the available data. The result may be encapsulated in a proprietary format (e01, ad1, etc).

Forensic Copy – The data from the source (original) media is copied "bit by bit" and written to other media in the same bit-by-bit order that it was obtained.

Forensic Evidence File – Consist of one or more files that contain the data from the source media that can be restored to other media in such a manner that the "bit by bit" order on the source drive is the same as the restored drive. The file may contain "additional" data written by the backup software. The additional data is program overhead.

Hash–Numerical values, generated by various hashing functions, used to substantiate the integrity of digital evidence and/or for inclusion / exclusion comparisons against known value sets.

Message Digest 5 (MD5) Hash–A 128-bit value that uniquely describes the contents of a file. This is a standard hash value used in digital forensics.

New Technology File System–NTFS (NT file system; sometimes New Technology File System) is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk. NTFS is the Windows NT equivalent of the Windows 95 file allocation table (FAT) and the OS/2 High Performance File System (HPFS).

Removable Media– Items (e.g., floppy disks, CDs, DVDs, USB Drives, tape) that store data and can be easily removed.

Unallocated Space – also called free space, is defined as the unused portion of the hard drive.

Universal Time Coordinated– UTC / GMT is the basis for local times worldwide. Other names include Universal Time Coordinated / Universal Coordinated Time. UTC is the successor to Greenwich Mean Time (GMT).

ADDENDUM A

The following details the forensic image processing.

Digital Forensics Examiner (DFE) created forensic evidence files of Verbatim USB Drive, black, 2.0GB, Serial #23097JR2. The pre-processing hash results are presented below:

MD5 checksum: bc1bedd931cacfd5bc4004ec9ef2fb3e
SHA1 checksum: 217eb21b8e9f4e363824df43204f0f3b75025fd1

The forensic processing subsequently created 1 file.

Forensic Evidence Files Created: PAGS01_06132014.E01

The forensic imaging process involved a post-processing hash verification of the contents of the evidence file compared with the pre-processing hash. The hash analysis is presented below.

MD5 checksum: bc1bedd931cacfd5bc4004ec9ef2fb3e : verified
SHA1 checksum: 217eb21b8e9f4e363824df43204f0f3b75025fd1 : verified

The forensic imaging process successfully created a forensically sound and verifiable bit stream copy of the hard drive in the form of forensic evidence files.

ADDENDUM B

Steps Taken:

1. PI Smith, #351 released the USB Drive "USB02_032816_4-2" to Digital Forensic Examiner (DFE) Dmitry Landy #891920 on 08/21/16 for digital forensics processing.
2. DFE acquired a pre-processing hash of USB02_032816_4-2.
3. Initial processing included inspection, photography, anti-virus (AV) scan of USB02_032816_4-2.
4. DFE created forensically sterile media PAGS01_06132014 (LEXAR JUMPDRIVE USB Device Serial #8KRZ24B) by using Sumuri Paladin and then verified by using the DCFLDD command.
5. DFE created a forensic copy of USB02_032816_4-2 onto PAGS01_06132014 and confirmed the hash of the forensic copy matched the pre-processing hash.
6. DFE released USB02_032816_4-2 to evidence custodian Jane Smith on 08/22/16 to be secured in the evidence locker.
7. Forensic imaging of PAGS01_06132014 was conducted by the DFE using FTK Imager to create forensic evidence file PAGS01_06132014.E01. After the imaging process, the hash of the forensic image and its contents to the pre-processing hash were compared. It was confirmed both hash values matched.
8. DFE used FTK Imager to convert PAGS01_06132014.E01 to a raw data file (FR1_.001)for WinHex to analyze it.
9. After the conversion, the post-processing hash was confirmed to have matched the pre-processing hash.
10. Using WinHex, FR1_.001 was opened to review the partition structure
11. A scan for lost partitions found nothing.
12. A brief low-level analysis of partition was conducted and found that only 496 MB of 2GB was used.
13. After analyzing the file structure and its additional details, it was WinHex performed file carving on FR1_.001 which resulted in 150 found files.
14. The files were screened for any child pornography (none were found) in preparation for exporting the files for review by EnCase.
15. The carved files were exported to be later reviewed by EnCase. A list of the files was also exported to be reviewed.
16. EnCase was used to analyze the forensic file (PAGS01_06132014.E01) as well as the carved files recovered from using WinHex.
17. A forensic file was created from the exported files (FR1ExportFiles.L01)
18. The new forensic file was added as evidence to the case and the original export files were removed. Both files were processed
19. The graphical files were analyzed and revealed 1 Adult pornographic image.
20. Additional analysis of the files did not reveal anything of interest.
21. Evidence items were exported into a spreadsheet FR1_Inventory_Landy.xlsx and sorted for forensically interesting items.