ID Forensic

Where Investigative, Digital and
Forensics Meet

CONFIDENTIAL CASE REPORT

AUTHORIZED EYES ONLY

This document contains sensitive and confidential information pertinent to a forensic investigation. Proceeding implies that you are authorized to do so and agree to keep confidential all information contained herein.

TABLE OF CONTENTS

Case: **2016-0001**
Client: **PI Sam Slade**
Re: **Klaus von Kloptstadt**

Summation

I. INTRODUCTION

On May 19, 2016, a request was received to investigate the contents within a removable USB storage device that was recovered by Private Investigator Sam Slade from Sam Goodwin's computer [1].The objective of the investigation was to examine the USB drive's contents and to find whatever evidence was on the drive, and the results would be given to PI Slade. A completed documentation of chain of custody (separate document) was received.

II. HANDLING AND IMAGING OF ORIGINAL USB STORAGE DEVICE ANDFINDINGS

The removable USB storage device recovered by PI Slade was an unmarked D6DEAD30 126 MB USB drive[2]. Both the posterior and anterior sides were unmarked. The USB drive was examined for physical damage and none was detected. The device's outer structure consisted of a metallic unscratched covering with no retractable slides. The device could be connected to a standard USB port within a laptop or desktop computer. Connection of the device to a laptop or desktop computer could be done by pointing the posterior of the device downward. The USB storage device was labeled with the examiner's initials and date acquired.

The USB storage device was hashed using our licensed version of Raptor Linux. Within Raptor Linux, the media is not automatically mounted during the verification process or creation of a forensic image which also contributes to no alteration of data. The original drive (unmarked D6DEAD30 126MB) was hashed. A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The two hashes produced were an MD5 and a Sha1 hash. The MD5 message-digest algorithm is a widely

[1] Reference Appendix B, Exhibit 1
[2] Reference Appendix B, Exhibit 2

used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. In cryptography, SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States NIST. SHA-1 produces a 160-bit (20-byte) hash value known as a message digest. The original USB storage device was cloned to a USB storage device with a similar storage space of 128 MB known as C873A155 126MB (/dev/sdd). The USB storage device C873A155 126MB (/dev/sdd) became the “working” device. This device was then imaged to Partition 1 of Physical device ATA Hitachi HTS547564A9E384 J2130053GUM7drive of the laptop that was used during the examination. Below is the hash of the original USB storage device before and after cloning and the USB device C873A155 126MB (/dev/sdd) that the original USB was cloned to. The table below also depicts the hash verification of the Partition 1 of Physical device ATA Hitachi HTS54756A9E384 J2130053GUM7 drive of which the USB device C873A155 126MB (/dev/sdd) was imaged to. The Generic Flash Disk C873A155 126MB (/dev/sdd) was forensically sterilized before cloning occurred. The sterilization report can be found in next subsection of this report. The name of the image was PE6-2.001. It was imaged as a raw dd image. A raw dd image is a bit-for-bit copy of the RAW data of either the disk or the volume, without any additions or deletions.

Hash value verification of Original USB Storage Device Generic Flash Disk D6DEAD30 126 MB(/dev/sdc)	Hash value verification of Original USB Storage Device (After Cloning to Generic Flash C873A155 126MB (/dev/sdc)	Hash value verification of the Generic Flash Disk C873A155 126MB (/dev/sdb) (After Cloning from the Original USB Generic Flash Disk D6DEAD30 126 MB(/dev/sdc)	Hash value verification of the Partition 1 of Physical ATA Hitachi HTS547564A9E384 J2130053GUM7EA63(After Imaging from the Generic Flash Disk C873A155 126MB (/dev/sdc)	Hash value verification of the Generic Flash Disk C873A155 126MB (/dev/sdb) (After Imaging to Partition 1 of Physical ATA Hitachi HTS547564A9E384 J2130053GUM7EA63)
Hash value verification started at 20160519 17:45:21: Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Completed verification process at 20160519 17:45:32	Hash value verification started at 20160519 18:48:50: Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Completed verification process at 20160519 18:49:02	Hash value verification started at 20160519 19:58:46: Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Completed verification process at 20160519 19:58:58	Hash value calculated during initial creation: 0-126877696: e8752d9457ee160c70a76f246b82884e 0-126877696: 0f33db90f5edc1672dac8b4470295b65b2ace0fe Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Hash values for verification started at 20160519	Hash value verification started at 20160519 20:23:45: Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Completed verification process at 20160519 20:23:56

			19:58:46: Completed verification process at 20160519 20:06:33 Total (md5): e8752d9457ee160c70a76f246b82884e Total (sha1): 0f33db90f5edc1672dac8b4470295b65b2ace0fe Completed verification process at 20160519 20:06:41	

Table 1:Before and After MD-5 and SHA-1 Hashes of the Original USB Generic Flash Disk D6DEAD30, C873A155 USB Drive, and Partition 1 of Physical ATA Hitachi HTS547564A9E384 J2130053GUM7EA63 after Cloning and Imaging Processes

All of the hashes matched which meant that the data was not altered during cloning and the clone was identical to the original. The original USB Generic Flash Disk D6DEAD30 was removed from the examination and logged in the Chain of Custody form and stored in the locker.

IMAGE PE6-2.001

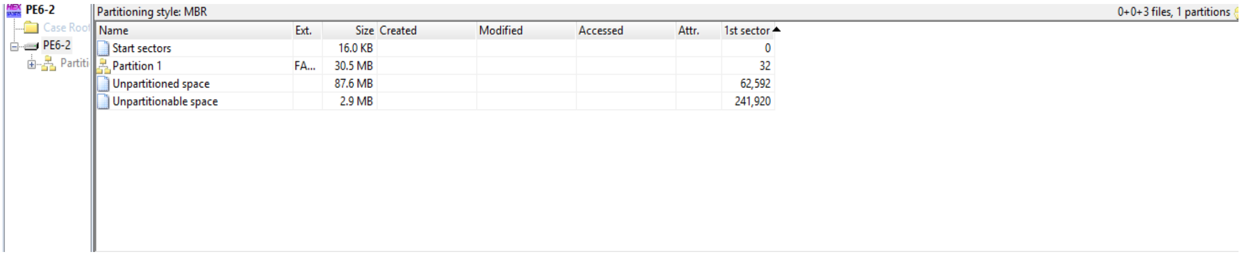
a. Methods

The raw dd image PE6-2.001 was stored in a folder within Partition 1 of Physical device ATA Hitachi HTS547564A9E384 J2130053GUM7EA63. Our licensed version of Winhex was opened and a new case was created. The case title/number was named PE6-2. The image PE6-2.001 was added to file. The total capacity was 121 MB.

b. Results

Directory View:

In the directory view of image PE6-2, it lists the Start sectors, Partition 1, Unpartitioned Space, and Unpartitionable space along with its extension, size, date created, date modified, date accessed, attr., and 1st sector. The directory view of the image file PE6-2 is pictured below.



Partitioning style: MBR

0+0+3 files, 1 partitions

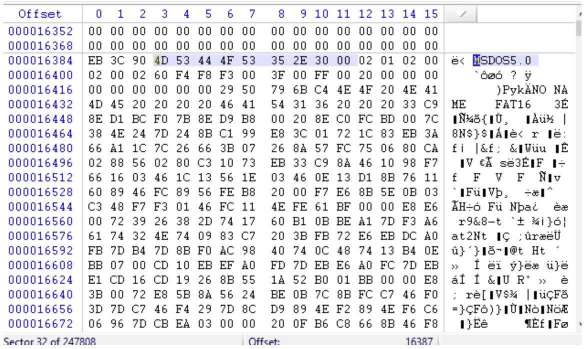
Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
Start sectors		16.0 KB					0
Partition 1	FA...	30.5 MB					32
Unpartitioned space		87.6 MB					62,592
Unpartitionable space		2.9 MB					241,920

Figure 1. Directory view of Image File PE6-2

The following subsections present the results of Partition 1.

Partition 1

Parition 1 was located on sector 32. It was 30.5 MB in size with a FAT16 file system. A FAT16 file system is the original file system used in DOS and Windows 3.x. Therefore, it can be concluded that the operating system was MSDOS 5.0. This can be verified by the screenshot of the Hex view of Partition 1 within Winhex.



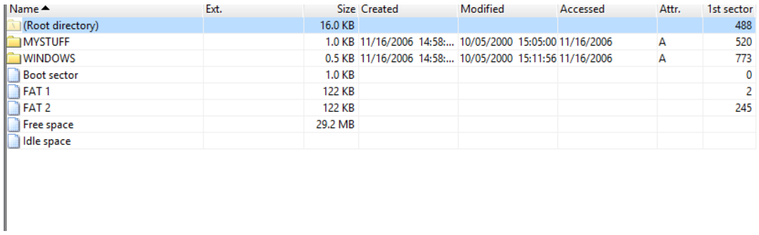
```
  Offset     0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15
000016352   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000016368   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000016384   EB 3C 90 4D 53 44 4F 53  35 2E 30 00 02 01 02 00   ë< MSDOS5.0
000016400   02 00 02 60 F4 F8 F3 00  3F 00 FF 00 20 00 00 00     `ôøó ? ÿ
000016416   00 00 00 00 00 00 29 50  79 6B C4 4E 4F 20 4E 41         )PykÄNO NA
000016432   4D 45 20 20 20 20 46 41  54 31 36 20 20 20 33 C9   ME    FAT16   3É
000016448   8E D1 BC F0 7B 8E D9 B8  00 20 8E C0 FC BD 00 7C   Ñ¼ð{Ù¸  Àü½ |
000016464   38 4E 24 7D 24 8B C1 99  E8 3C 01 72 1C 83 EB 3A   8N$}$Áè< r ë:
000016480   66 A1 1C 7C 26 66 3B 07  26 8A 57 FC 75 06 80 CA   f¡ |&f; &Wüu Ê
000016496   02 88 56 02 80 C3 10 73  EB 33 C9 8A 46 10 98 F7    V €Ã së3ÉF ÷
000016512   66 16 03 46 1C 13 56 1E  03 46 0E 13 D1 8B 76 11   f  F  V  F  Ñv
000016528   60 89 46 FC 89 56 FE B8  20 00 F7 E6 8B 5E 0B 03   `FüVþ¸  ÷æ^
000016544   C3 48 F7 F3 01 46 FC 11  4E FE 61 BF 00 00 E8 E6   ÃH÷ó Fü Nþa¿  èæ
000016560   00 72 39 26 38 2D 74 17  60 B1 0B BE A1 7D F3 A6    r9&8-t `± ¾¡}ó¦
000016576   61 74 32 4E 74 09 83 C7  20 3B FB 72 E6 EB DC A0   at2Nt Ç ;ûræëÜ
000016592   FB 7D B4 7D 8B F0 AC 98  40 74 0C 48 74 13 B4 0E   û}´}ð¬@t Ht ´
000016608   BB 07 00 CD 10 EB EF A0  FD 7D EB E6 A0 FC 7D EB   »  Í ëï ý}ëæ ü}ë
000016624   E1 CD 16 CD 19 26 8B 55  1A 52 B0 01 BB 00 00 E8   áÍ Í &U R° »  è
000016640   3B 00 72 E8 5B 8A 56 24  BE 0B 7C 8B FC C7 46 F0   ; rè[V$¾ |üÇFð
000016656   3D 7D C7 46 F4 29 7D 8C  D9 89 4E F2 89 4E F6 C6   =}ÇFô)}ÙNòNöÆ
000016672   06 96 7D CB EA 03 00 00  20 0F B6 C8 66 8B 46 F8    }Ëê     ¶ÈfFø
Sector 32 of 247808                 Offset:              16387
```

Figure 2. HEX view of MSDOS5.0

Located within Partition 1 was a Root directory with no files with a 16.0 KB size located on 488 of the 1st sector. The media contained two sub-directories which were MYSTUFF and WINDOWS. A user created the subdirectory. Subdirectories are created to help organize files on the disks. When one creates directories, he is developing a category and classification scheme. This allows one to quickly locate files and to manage the numerous files and programs that one creates and collects.

Subdirectories are also created to defeat the limitation the operating system places on the number of files that can be in the root directory. By creating subdirectories, the files on a disk are only constrained by the disk space itself.

The following is the directory view of Partition 1.

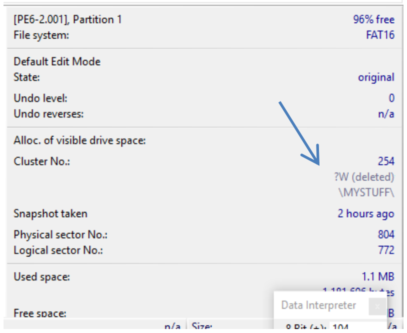


Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16.0 KB					488
MYSTUFF		1.0 KB	11/16/2006 14:58:...	10/05/2000 15:05:00	11/16/2006	A	520
WINDOWS		0.5 KB	11/16/2006 14:58:...	10/05/2000 15:11:56	11/16/2006	A	773
Boot sector		1.0 KB					0
FAT 1		122 KB					2
FAT 2		122 KB					245
Free space		29.2 MB					
Idle space							

Figure 3. Directory view of Partition 1 of Image PE6-2.001

With the empty root directory and the existing files, it can be concluded that the media was not formatted by the user. Although the media was not formatted, the files were deleted. When a file is deleted, the following occurs: files that were previously erased are noted with a "σ" symbol known as the Greek letter for sigma. In order to recover this file, the first character of the directory is changed to a valid character. In this instance, a valid character "-" would be placed in front of the file name. The cluster would be allocated to the file and the data is untouched. Below shows a screenshot of a deleted file within Partition 1 that further verifies that the files were deleted.

.



[PE6-2.001], Partition 1	96% free
File system:	FAT16
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Alloc. of visible drive space:	
Cluster No.:	254 ?W (deleted) \MYSTUFF\
Snapshot taken	2 hours ago
Physical sector No.:	804
Logical sector No.:	772
Used space:	1.1 MB
Free space:	

Figure 4. Winhex Reference of File Deletion

The following two sections describe the results of the two subdirectories MYSTUFF and WINDOWS.

a. MYSTUFF
Subdirectory MYSTUFF was size 1.0 KB, and it was located on sector 520 of the 1st sector. It was created on 11/16/2006 at 14:58:26.4. The subdirectory had nine deleted files with eight being child pornography jpg files. All files are listed below in Table 1 along with their extension, size, date created, date modified, date accessed, attributes, sector location and image.