CASE STUDY 1 03-01-2018

AKASH MUKHERJEE
COMPUTER AND NETWORK FORENSICS
UNIVERSITY OF SOUTHERN CALIFORNIA

Table of Contents

I. EXECUTIVE SUMMARY

Mr. Thomas Trojan convicted his roommate Mr. Richardson Bruin of possessing contraband material on his computer. Mr. Trojan reported to the IT staff that he saw possible child pornography on Mr. Brian's computer while he was seated in his computer. Based on the credibility of Mr. Trojan, Mr. Bruin's computer has been confiscated. A digital image of the entire drive has been created and shared with the Digital Forensics investigators for validating the authenticity of Mr. Trojan's claim. An EnCase image of the drive was shared with investigators. The investigator is tasked with verifying the existence of any contraband materials on the hard disk as well as possible distribution of the same content.

Investigation confirmed existence of contraband material on the disk image file. No files were found on the available drives of the disk, but investigation successfully revealed existence of one deleted partition. The suspected contraband materials existed in the deleted partition. However, those files had their extensions renamed to hide their existence. Utilizing advanced features of forensic tools, the files were identified with their original extensions. Subsequently, the entire drive was examined for child pornography and evidence of existence was obtained. Distribution of the contraband material could not be verified. However, an external drive connection was revealed. Initial instruction included confiscation of additional drives besides the main hard disk. Investigating the additional drives might disclose more information regarding distribution of child pornography.

II. COMPUTER EVIDENCE ANALYZED

The details of the image file which was shared on Dropbox are given below:

	https://www.dropbox.com/s/3qk6hooujcaybhu/INF%20528%20Case%201.E01
Shared on	Feb 25, 2018 9:30 AM PST
Shared by	Mr. Joseph Greenfield
File name	INF 528 Case 1.E01
MD5	b144a2d5ea39fe575638485bd8c94b7b
SHA1	44944880aca09ab160c0b4cdb1468d41f6c1faff

III. ANALYSIS RESULTS

The aforementioned disk image file has been analyzed to fetch these basic system information:

- **Operating System:** Windows 7 Professional English
- **Drive Information:** Operating System stored in C drive
- **Username:** Richard

Operating system was installed on C drive. This drive was examined for possessing any contraband child pornography material. A wide array of forensic tools has been used for this investigation, chief among them being EnCase and Forensic Explorer. There was no indication of existence of child pornography in this part of the drive. However, a deleted partition was identifed.

a) Partition Recovery

Analyzing the data stored on byte offset 446 to 509 of Master Boot Record (MBR), the partition table was generated using EnCase bookmark feature. This indicated possibility of a deleted memory. EnCase Case Processor EnScript was used to scan for any deleted partition or consecutive memory area. An indication of existence of a deleted FAT32 partition was discovered at sector offset 125,827,072. Upon using EnCase 'Add Partition' feature, a deleted FAT32 D drive was recovered.

b) Possession of Contraband Material Analysis:

After recovering the deleted D drive on the image file, 'Backup' folder was found, which was confirmed to contain 7 contraband materials. It was learnt by analyzing this deleted folder that files under this folder had modified extension, resulting in failure of rendering the data. For example, if an image file has a modified extension as .pdf, operating system will try to open it with a PDF reader software which will generate error message stating corrupted data. With EnCase File Signature Analysis, it was identified from these file headers that they are JPEG image files. After displaying these files as image in EnCase, it was confirmed to be child pornography.

Details of identified contraband materials are tabulated below:

Name	File Extension	Last Accessed	File Created	Last Written	Full Path	Hash Value
Expense Reports 2013.docx	Docx	10/13/15	10/13/15 11:54:58AM	10/13/15 11:54:58AM	\D\Backup\Expense Reports 2013.docx	9ea4f6b0300544f4420881c1ba9531c8
Expense Reports 2014.docx	Docx	10/13/15	10/13/15 11:55:16AM	10/13/15 11:55:16AM	\D\Backup\Expense Reports 2014.docx	07d644aa001caeaaf3c47644af8ae050
Expenses 2013.xls	Xls	10/13/15	10/13/15 11:55:08AM	10/13/15 11:55:08AM	\D\Backup\Expenses 2013.xls	e314b6ce5073434d3484b1c5ef06c7ea
Expenses 2014.xls	Xls	10/13/15	10/13/15 11:55:30AM	10/13/15 11:55:30AM	\D\Backup\Expenses 2014.xls	
Resume.doc	Doc	10/13/15	10/13/15 11:56:08AM	10/13/15 11:56:08AM	\D\Backup\Resume.doc	c062ff78f2ffb9474178e9d0e65b387a
Tax Return 2013.pdf	Pdf	10/13/15	10/13/15 11:55:40AM	10/13/15 11:55:40AM	\D\Backup\Tax Return 2013.pdf	f186a2ef547d5cf6b2efd3503f032831
Tax Return 2014.pdf	Pdf	10/13/15	10/13/15 11:55:52AM	10/13/15 11:55:52AM	\D\Backup\Tax Return 2014.pdf	378ef54bda36876e0df38498c0742dea
$RTMAUEG.docx	Docx	10/13/15	10/13/15 11:54:58AM	10/13/15 11:54:58AM	\D\$RECYCLE.BIN\$RTMAUEG.docx	
$RL6TJRN.docx	Docx	10/13/15	10/13/15 11:55:16AM	10/13/15 11:55:16AM	\D\$RECYCLE.BIN\$RL6TJRN.docx	
$RHUHXRP.XLS	Xls	10/13/15	10/13/15 11:55:30AM	10/13/15 11:55:30AM	\D\$RECYCLE.BIN\$RHUHXRP.XLS	5780a977548c2380c8190673022a6eb2
_RQETMTR.XLS	Xls	10/13/15	10/13/15 11:55:08AM	10/13/15 11:55:08AM	\D\$RECYCLE.BIN_RQETMTR.XLS	
$RH8KVUG.DAT	Dat	10/13/15	10/13/15 11:56:38AM	10/13/15 11:56:38AM	\D\$RECYCLE.BIN\$RH8KVUG.DAT	f11feab14d85c2ac0b01015ba406d0d0
$R3V984Y.DAT	Dat	10/13/15	10/13/15 11:55:22AM	10/13/15 11:55:22AM	\D\$RECYCLE.BIN\$R3V984Y.DAT	83efd9566e8a68b5dd45c410f9ebd3c6

c) Distribution of Contraband Material Analysis

Child pornography can be distributed in many ways. Investigation of internet history, print spool, email from windows and registry analysis yielded no evidence of distribution. Connection of USB drive to the computer was found via registry file analysis. However, there was no evidence of transferring any contraband material through the USB drive.

IV. INVESTIGATIVE LEADS

Windows registry files indicated that an external storage device had been connected to the machine. However, with the current resources, it is uncertain whether child pornography was distributed through it. It has been mentioned that along with the hard disk of Mr. Bruin's computer, other removable media were also confiscated. So, further investigation of the portable drives can be helpful for revealing more information about distribution of child pornography.

V. CONCLUSIONS

Image of Mr. Bruin's computer has been investigated to identify evidence of possession and distribution of child pornography. The image was analyzed for any stored contraband material and user activities utilizing windows system files.

Possession of child pornography has been established by this investigation. Files related to contraband materials had been edited to change their extension and the drive holding those files had been deleted to avoid detection. However, evidence for distribution of those contents were not found.

VI. RECOMMENDATIONS

Possession of contraband material in Mr. Bruins laptop has been established. This should be reported to Law and Enforcement for further legal action on Mr. Bruin's possession of child pornography.

VII. REFERENCES

[1] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/486289/2015_12_15_FSR-C-214_Cell_site_consultation_draft.pdf

[2] Criminal Practice Directions (2015). Accessed 07/12/15 from: https://www.judiciary.gov.uk/publications/criminal-practice-directions-2015/.

[3] Criminal Procedure Rules (2015). Published by the Ministry of Justice on behalf of the Criminal Procedure Rule Committee. Accessed 07/12/15 from: http://www.legislation.gov.uk/uksi/2015/1490/contents/made.

[4] http://www.forensicfocus.com/forensic-analysis-windows-registry

[5] https://www.easeus.com/ad/partition-recovery.htm?gclid=EAIaIQobChMI_OXI8pzK2QIVhWx-Ch2iGwbOEAAYASAAEgLu8fD_BwE

[6] File Signatures. (n.d.). Retrieved March 10, 2016, from http://www.garykessler.net/library/file_sigs.html

[7] Miller, P. (n.d.). How (and Why) to Partition Your Hard Drive. Retrieved March 10, 2016, from http://www.pcworld.com/article/185941/how_and_why_to_partition_your_hard_drive.html

[8] Rouse, M. (2005, April). What is Master Boot Record (MBR)? - Definition from WhatIs.com. Retrieved March 09, 2016, from http://whatis.techtarget.com/definition/Master-Boot-Record-MBR

[9] Rouse, M. (2005, September). What is CD-ROM? - Definition from WhatIs.com. Retrieved March 09, 2016, from http://whatis.techtarget.com/definition/CD-ROM

VIII. GLOSSARY

Byte	Collection of 8 binary digits (0s/1s).
CD/DVD ROM	Hardware storage devices used for Read/Write data.
DISK	Storage device used for Read/Write.
Encase	Digital Forensic investigation tool from Guidance Software.
Encase Image File format	Copy of a hard disk copied bit by bit in purpose of use it for forensic investigations. Aside EnCase, major forensic tools support this image format.
Extensions	Identifiers for a particular file to render using proper application.
Hard disk	Storage device used for Read/Write.
Hash	Digital fingerprint used to verify integrity of a file.
Image file	Copy of a hard disk copied bit by bit in purpose of use it for forensic investigations.
JFIF/EXIF	File signature for jpg (image) file.
MBR	First sector on disk, that contains information about partition and boot sequence of a computer.
MD5	Message Digest algorithm to verify integrity of a file. Generates 128 bits unique fingerprint.
OFFSET	Relative address from a base. In this case, base is 0.
Operating System	Central manager to all resources to a computer.
Partition	Sub portion of a physical drive in groups.
SHA1	Algorithm to verify integrity of a file. Generates 160 bits unique fingerprint.
USB	Standard used for sharing digital content across machines.