Texas Tech University
Computer Science Department
CS5332 – Digital Forensics
Spring 2018, Assignment 2
Due Date: TBA

Replicate the following data leakage case:

https://www.cfreds.nist.gov/data_leakage_case/data-leakage-case.html

The analysis report is also given in the end of the link. You just need to replicate them using tools and commands. For your reference, the description is also copied and pasted in the end of this document.

For a quick tutorial on using the Sleuth Kit disk analyzer tool, you may review the following links:

https://diuf.unifr.ch/drupal/tns/sites/diuf.unifr.ch.drupal.tns/files/cmarko-tskintro.pdf

http://booksite.elsevier.com/samplechapters/9781597495868/Chapter_3.pdf

Deliverable:

Similar report given in the link along with some snapshots.

The description given in the link:

Data Leakage Case

The purpose of this work is to learn various types of data leakage, and practice its investigation techniques.

Scenario Overview

‘Iaman Informant’ was working as a manager of the technology development division at a famous international company OOO that developed state-of-the-art technologies and gadgets.

One day, at a place which ‘Mr. Informant’ visited on business, he received an offer from ‘Spy Conspirator’ to leak of sensitive information related to the newest technology. Actually, ‘Mr. Conspirator’ was an employee of a rival company, and ‘Mr. Informant’ decided to accept the offer for large amounts of money, and began establishing a detailed leakage plan.

‘Mr. Informant’ made a deliberate effort to hide the leakage plan. He discussed it with ‘Mr. Conspirator’ using an e-mail service like a business relationship. He also sent samples of confidential information though personal cloud storage.

After receiving the sample data, ‘Mr. Conspirator’ asked for the direct delivery of storage devices that stored the remaining (large amounts of) data. Eventually, ‘Mr. Informant’ tried to take his storage devices away, but he and his devices were detected at the security checkpoint of the company. And he was suspected of leaking the company data.

At the security checkpoint, although his devices (a USB memory stick and a CD) were briefly checked (protected with portable write blockers), there was no evidence of any leakage. And then, they were immediately transferred to the digital forensics laboratory for further analysis.

The information security policies in the company include the following:

1. Confidential electronic files should be stored and kept in the authorized external storage devices and the secured network drives.
2. Confidential paper documents and electronic files can be accessed only within the allowed time range from 10:00 AM to 16:00 PM with the appropriate permissions.
3. Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.
4. All employees are required to pass through the ‘Security Checkpoint’ system.
5. All storage devices such as HDD, SSD, USB memory stick, and CD/DVD are forbidden under the ‘Security Checkpoint’ rules.

In addition, although the company managed separate internal and external networks and used DRM (Digital Rights Management) / DLP (Data Loss Prevention) solutions for their information security, ‘Mr. Informant’ had sufficient authority to bypass them. He was also very interested in IT (Information Technology), and had a slight knowledge of digital forensics.

In this scenario, find any evidence of the data leakage, and any data that might have been generated from the suspect's electronic devices.

Target Systems and Devices

Target	Detailed Information	
Personal Computer (PC)	Type	Virtual System
	CPU	1 Processer (2 Core)
	RAM	2,048 MB
	HDD Size	20 GB
	File System	NTFS
	IP Address	10.11.11.129
	Operating System	Microsoft Windows 7 Ultimate (SP1)
Removable Media #1 (RM#1)*	Type	USB removable storage device
	Serial No.	4C530012450531101593
	Size	4 GB
	File System	exFAT
Removable Media #2 (RM#2)	Type	USB removable storage device
	Serial No.	4C530012550531106501
	Size	4 GB
	File System	FAT32
Removable Media #3 (RM#3)	Type	CD-R
	Size	700 MB
	File System	UDF

* Authorized USB memory stick for managing confidential electronic files of the company.

Acquired Data Information

Personal Computer (PC) – 'DD' Image

Download Links	pc.7z.001, pc.7z.002, pc.7z.003 (total 5.05 GB compressed by 7zip) - hash
Imaging S/W	FTK Imager 3.4.0.1
Image Format	converted from VMDK

Personal Computer (PC) – 'EnCase' Image

Download Links	pc.E01, pc.E02, pc.E03, pc.E04 (total 7.28 GB compressed by EnCase) - hash
Imaging S/W	EnCase Imager 7.10.00.103
Image Format	E01 (Expert Witness Compression Format) converted from VMDK

Removable Media #2 (RM#2) – 'DD' Image

Download Links rm#2.7z (total 219 MB compressed by 7zip) - hash

Imaging S/W	FTK Imager 3.3.0.5 (write-blocked by Tableau USB Bridge T8-R2)
Image Format	DD

Removable Media #2 (RM#2) – 'EnCase' Image

Download Links	rm#2.E01 (total 243 MB compressed by EnCase) - hash
Imaging S/W	EnCase Imager 7.09.00.111 (write-blocked by Tableau USB Bridge T8-R2)
Image Format	E01 (Expert Witness Compression Format)

Removable Media #3 (RM#3) – 'Raw / CUE' Image

Download Links rm#3-type1.7z (total 92.8 MB compressed by 7zip) - hash

Imaging S/W	FTK Imager 3.3.0.5
Image Format	RAW ISO / CUE (sometimes BIN / CUE)*

* The RAW ISO file is a raw sector-by-sector binary copy of tracks in the original disk, and the CUE file is a plain-text file which stores the information of disk and tracks.

Removable Media #3 (RM#3) – 'DD' Image

Download Links rm#3-type2.7z (total 78.6 MB compressed by 7zip) - hash

Imaging S/W	FTK Imager 3.3.0.5 + bchunk (http://he.fi/bchunk)
Image Format	DD converted from 'RAW ISO + CUE'

Removable Media #3 (RM#3) – 'EnCase' Image

Download Links rm#3-type3.E01 (total 90.2 MB compressed by EnCase) - hash

Imaging S/W	EnCase Imager 7.09.00.111
Image Format	E01 (Expert Witness Compression Format)

Additional Data Information

Seed Files

Download Links	seed-files.7z (total 150 MB compressed by 7zip) - hash
File Information	- Seed files stored in RM#1 and a shared network drive - Base files for creating seed files were randomly selected from Govdocs1 - The first page of each seed file was manually added - Seed file list and hash values

Digital Forensic Practice Points

The followings are the summary of detailed practice points related to above images.

Practice Point	Description
Understanding Types of Data Leakage	- Storage devices > HDD (Hard DiskDrive), SSD (Solid State Drive) > USB flash drive, Flash memory cards > CD/DVD (with Optical Disk Drive) - Network Transmission > File sharing, Remote Desktop Connection > E-mail, SNS (Social Network Service) > Cloud services, Messenger
Windows Forensics	- Windows event logs - Opened files and directories - Application (executable) usage history - CD/DVD burning records - External devices attached to PC - Network drive connection traces - System Caches - Windows Search databases - Volume Shadow Copy
File System Forensics	- FAT, NTFS, UDF - Metadata (NTFS MFT, FAT Directory entry) - Timestamps - Transaction logs (NTFS)
Web Browser Forensics	- History, Cache, Cookie - Internet usage history (URLs, Search Keywords…)
E-mail Forensics	- MS Outlook file examination - E-mails and attachments
Database Forensics	- MS Extensible Storage Engine (ESE) Database - SQLite Database
Deleted Data Recovery	- Metadata based recovery

	- Signature & Content based recovery (aka Carving) - Recycle Bin of Windows - Unused area examination
User Behavior Analysis	- Constructing a forensic timeline of events - Visualizing the timeline

Questions

1. What are the hash values (MD5 & SHA-1) of all images?
   Does the acquisition and verification hash value match?
2. Identify the partition information of PC image.
3. Explain installed OS information in detail.
   (OS name, install date, registered owner…)
4. What is the timezone setting?
5. What is the computer name?
6. List all accounts in OS except the system accounts: *Administrator, Guest, systemprofile, LocalService, NetworkService*. (Account name, login count, last logon date…)
7. Who was the last user to logon into PC?
8. When was the last recorded shutdown date/time?
9. Explain the information of network interface(s) with an IP address assigned by DHCP.
10. What applications were installed by the suspect after installing OS?
11. List application execution logs.
    (Executable path, execution time, execution count...)
12. List all traces about the system on/off and the user logon/logoff.
    (It should be considered only during a time range between 09:00 and 18:00 in the timezone from Question 4.)
13. What web browsers were used?
14. Identify directory/file paths related to the web browser history.
15. What websites were the suspect accessing? (Timestamp, URL...)
16. List all search keywords using web browsers. (Timestamp, URL, keyword...)
17. List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword)
18. What application was used for e-mail communication?
19. Where is the e-mail file located?
20. What was the e-mail account used by the suspect?
21. List all e-mails of the suspect. If possible, identify deleted e-mails.
    (You can identify the following items: *Timestamp, From, To, Subject, Body, and Attachment*)
    [Hint: just examine the OST file only.]
22. List external storage devices attached to PC.
23. Identify all traces related to ‘renaming’ of files in Windows Desktop.
    (It should be considered only during a date range between 2015-03-23 and 2015-

03-24.)
[Hint: the parent directories of renamed files were deleted and their MFT entries were also overwritten. Therefore, you may not be able to find their full paths.]

24. What is the IP address of company's shared network drive?
25. List all directories that were traversed in 'RM#2'.
26. List all files that were opened in 'RM#2'.
27. List all directories that were traversed in the company's network drive.
28. List all files that were opened in the company's network drive.
29. Find traces related to cloud services on PC.
    (Service name, log files...)
30. What files were deleted from Google Drive?
    Find the filename and modified timestamp of the file.
    [Hint: Find a transaction log file of Google Drive.]
31. Identify account information for synchronizing Google Drive.
32. What a method (or software) was used for burning CD-R?
33. When did the suspect burn CD-R?
    [Hint: It may be one or more times.]
34. What files were copied from PC to CD-R?
    [Hint: Just use PC image only. You can examine transaction logs of the file system for this task.]
35. What files were opened from CD-R?
36. Identify all timestamps related to a resignation file in Windows Desktop.
    [Hint: the resignation file is a DOCX file in NTFS file system.]
37. How and when did the suspect print a resignation file?
38. Where are 'Thumbcache' files located?
39. Identify traces related to confidential files stored in Thumbcache.
    (Include '256' only)
40. Where are Sticky Note files located?
41. Identify notes stored in the Sticky Note file.
42. Was the 'Windows Search and Indexing' function enabled? How can you identify it?
    If it was enabled, what is a file path of the 'Windows Search' index database?
43. What kinds of data were stored in Windows Search database?
44. Find traces of Internet Explorer usage stored in Windows Search database.
    (It should be considered only during a date range between 2015-03-22 and 2015-03-23.)
45. List the e-mail communication stored in Windows Search database.
    (It should be considered only during a date range between 2015-03-23 and 2015-03-24.)
46. List files and directories related to Windows Desktop stored in Windows Search database.
    (Windows Desktop directory: \Users\informant\Desktop\)
47. Where are Volume Shadow Copies stored? When were they created?
48. Find traces related to Google Drive service in Volume Shadow Copy.
    What are the differences between the current system image (of Question 29 ~ 31) and its VSC?

49. What files were deleted from Google Drive?
    Find deleted records of *cloud_entry* table inside *snapshot.db* from VSC.
    (Just examine the SQLite database only. Let us suppose that a text based log file was wiped.)
    [Hint: DDL of *cloud_entry* table is as follows.]

    CREATE TABLE *cloud_entry*
    (doc_id **TEXT**, filename **TEXT**, modified **INTEGER**, created **INTEGER**, acl_role **INTEGER**, doc_type **INTEGER**, removed **INTEGER**, size **INTEGER**, checksum **TEXT**, shared **INTEGER**, resource_type **TEXT**, PRIMARY KEY (doc_id));
50. Why can't we find Outlook's e-mail data in Volume Shadow Copy?
51. Examine 'Recycle Bin' data in PC.
52. What actions were performed for anti-forensics on PC at the last day '2015-03-25'?
53. Recover deleted files from USB drive 'RM#2'.
54. What actions were performed for anti-forensics on USB drive 'RM#2'?
    [Hint: this can be inferred from the results of Question 53.]
55. What files were copied from PC to USB drive 'RM#2'?
56. Recover hidden files from the CD-R 'RM#3'.
    How to determine proper filenames of the original files prior to renaming tasks?
57. What actions were performed for anti-forensics on CD-R 'RM#3'?
58. Create a detailed timeline of data leakage processes.
59. List and explain methodologies of data leakage performed by the suspect.
60. Create a visual diagram for a summary of results.

Answers

Look at the answers (PDF, MS-Word).
