INSTITUTO SUPERIOR TÉCNICO

DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

FORENSICS CYBER-SECURITY

MEIC, METI

Lab Assignment III

The Case of Mr. Informant

2017/2018

{danielporto, nuno.m.santos}@tecnico.ulisboa.pt

Introduction

The purpose of this task is to learn various types of data leakage and practice its investigation techniques using a simulated scenario. As part of this exercise, we provide digital evidence files which will be analyzed using forensic tools for Windows. For this reason, you will need to either setup a Windows virtual machine or use your own Windows computer as forensics platform. To set up a Windows forensics VM, follow the instructions provided in the Microsoft developer's web site[1]. In that VM, you will also need to install additional forensic tools for Windows, which will allow you, e.g., to examine the registry.

Scenario overview

Mr. 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 Mr. Spy Conspirator to leak 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:

(a) Confidential electronic files should be stored and kept in the authorized external storage devices and the secured network drives.

(b) 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.

(c) Non-authorized electronic devices such as laptops, portable storages, and smart devices cannot be carried onto the company.

(d) All employees are required to pass through the Security Checkpoint system.

(e) 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. The table below lists the details of the target systems and devices. Some collected media were formatted with exFAT and UDF file systems. You can find more information about these file systems on the Web.

[1] `https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/`

Target	Detailed Information	
Personal Computer (PC)	Type	Virtual System
	CPU	1 Processor (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. The images presented next were collected for digital investigation. You can download them from: `https://goo.gl/ofDL8c`.

Image	Details	
Personal Computer (PC)	Files	pc.dd.7z.00? (3 files, total 5.1 GB compressed by p7zip)
DD Image	Imaging S/W	FTK Imager 3.4.0.1
	Image Format	converted from VMDK
Removable Media #2 (RM#2)	Files	rm#2.dd.7z (total 220 MB compressed by p7zip)
DD Image	Imaging S/W	FTK Imager 3.3.0.5 (write-blocked by Tableau USB Bridge T8-R2)
	Image Format	DD
Removable Media #3 (RM#3)	Files	rm#3.dd.7z (total 79 MB compressed by p7zip)
DD Image	Imaging S/W	FTK Imager 3.3.0.5 + bchunk (`http://he.fi/bchunk`)
	Image Format	DD converted from 'RAW ISO + CUE'

Forensic tools. Unfortunately, some of the best forensic tools for Windows are not freely available. However, you can obtain a trial version of some of them from the Internet. Make sure that among the tools you installed into your Windows forensic station, you have installed at least, Autopsy, OSFMount, and OSForensics. You can download some auxiliary forensic tools from the same URL as the forensic artifacts'. These tools are bundled into the archive file `csf1718-lab3-tools.tgz`.

Questions

Answering the following questions will help you solve this case. These questions have several difficulty levels and demand specific background knowledge. We recommend you to start by answering the

File name	SHA1
pc.dd.7z.001	F07632FAA66A47088DEB07BDB45CC568E4BF650B
pc.dd.7z.002	5DEE46ABF6FA833268E5AE199A13854CCF42689B
pc.dd.7z.003	1687686F819092E05047F195F102D8FA0C38ED66
rm#2.dd.7z	DDFE97AA3D8D0B33CC6092123090A8154945F38E
rm#3.dd.7z	AE26235F6FB5EDDFFB670DD060EF109EDA91EB8F

questions of level L1. Then move on to questions L2 and finally L3. Use the tools that we recommend above and search for any other material that can help you in this task (e.g., slides from the theory classes, material available online, etc.). Feel free to install additional tools if you find that the recommended ones are not sufficient to obtain all the information you need from the evidence files.

1. (L1) What are the hash values (MD5) of all images? Does the acquisition and verification hash value match?
2. (L1) Identify the partition information of PC image. [Hint: use Autopsy.]
3. (L1) Explain installed OS information in detail. (OS name, install date, registered owner...) [Hint: mount the PC image with OSFMount, and inspect the Registry using OSForensics.]
4. (L1) What is the timezone setting? [Hint: inspect the Registry.]
5. (L1) What is the computer name?
6. (L1) List all accounts in OS except the system accounts: *Administrator*, *Guest*, *systemprofile*, *LocalService*, *NetworkService*. (Account name, login count, last logon date...)
7. (L1) Who was the last user to logon into the PC?
8. (L1) When was the last recorded shutdown date/time?
9. (L1) Obtain information of network interface(s) with an IP address assigned by DHCP. [Hint: inspect the Registry.]
10. (L1) What applications were installed by the suspect after installing the OS?
11. (L1) List application execution logs. (Executable path, execution time, execution count...) [Hint: inspect the UserAssis from the Registry, and the Windows Prefetch folder.]
12. (L1) 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.) [Hit: read the Windows Event Log using the event viewer of the ProDiscover tool.]
13. (L2) What web browsers were used?
14. (L2) Identify directory/file paths related to the web browser history. [Hint: for all relevant browsers identify the directories where are stored the browsing history, cache, and cookies.]
15. (L2) What websites were the suspect accessing? (Timestamp, URL...) [Hint: inspect the content of the relevant directories found from the previous question.]
16. (L2) List all search keywords using web browsers. (Timestamp, URL, keyword...) [Hint: inspect the web browser logs.]
17. (L1) List all user keywords at the search bar in Windows Explorer. (Timestamp, Keyword) [Hint: inspect the Registry.]
18. (L1) What application was used for e-mail communication? [Hint: check the Registry.]

19. (L2) Where is the e-mail file located?

20. (L2) What was the e-mail account used by the suspect?

21. (L2) 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. (L1) List external storage devices attached to PC.

23. (L3) 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. Possible sources: NTFS journal file analysis ($UsnJrnl), \$Extend\UsnJrnl-$J + $MFT for identifying full paths of files. You can consider the Registry ShellBags for further information and the Windows Search database, which is used in Question 46.]

24. (L1) What is the IP address of company's shared network drive? [Hint: check the Registry.]

25. (L3) List all directories that were traversed in 'RM#2'. [Hint: make use of the information about external storage devices attached to PC in Question 22. Inspect the ShellBag.]

26. (L3) List all files that were opened in 'RM#2'. [Hint: use information from Question 2, and inspect the JumpList and the ShellBag.]

27. (L3) List all directories that were traversed in the company's network drive. [Hint: inspect the JumpList, the ShellBag, and LNK files recently opened mentioned in the Registry.]

28. (L3) List all files that were opened in the company's network drive. [Hint: same as previous question.]

29. (L1) Find traces related to cloud services on PC. (Service name, log files...) [Hint: find evidence in Google Drive's installation directory and Registry: Configuration, Uninstall Information, Autoruns, UserAssist, Classes...]

30. (L3) 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. (L3) Identify account information for synchronizing Google Drive.

32. (L2) What a method (or software) was used for burning CD-R? [Hint: check if third-party software or default CD/DVD features were used. Learn the two burning types supported by Windows. Inspect the Windows Event Log, the Registry, and the NTFS journal file for more clues.]

33. (L3) When did the suspect burn CD-R? [Hint: it may be one or more times.]

34. (L3) 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. (L2) What files were opened from CD-R? [Hint: study the JumpList and LNK files.]

36. (L1) Identify all timestamps related to a resignation file in Windows Desktop. [Hint: the resignation file is a DOCX file in NTFS file system. Check the attributes of the corresponding NTFS MFT Entry.]

37. (L1) How and when did the suspect print a resignation file? [Hint: look up for installed printers in the system.]

38. (L1) Where are 'Thumbcache' files located?

39. (L1) Identify traces related to confidential files stored in Thumbcache. (Include '256' only) [Hint: open the thumbcache files found previously.]

40. (L1) Where are Sticky Note files located? [Hint: learn about Sticky Note files on the Web.]
41. (L1) Identify notes stored in the Sticky Note file.
42. (L2) 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? [Hint: check the Registry.]
43. (L2) What kinds of data were stored in Windows Search database? [Hint: open the Windows Search database using a tool that reads .edb files.]
44. (L2) 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. (L2) 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. (L2) List files and directories related to Windows Desktop stored in Windows Search database. (Windows Desktop directory: \Users\informant\Desktop\)
47. (L3) Where are Volume Shadow Copies stored? When were they created? [Hint: find a meaningful directory in the root directory.]
48. (L3) 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. (L3) 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. (L3) Why can't we find Outlook's e-mail data in Volume Shadow Copy? [Hint: find more information about Volume Shadow Copy online.]
51. (L1) Examine 'Recycle Bin' data in the PC. [Hint: deleted files from an emptied Recycle Bin might be recovered by metadata-based data recovery.]
52. (L3) What actions were performed for anti-forensics on PC at the last day '2015-03-25'? [Hint: combine information from most of the previous questions.]
53. (L1) Recover deleted files from USB drive 'RM#2'. [Hint: use a file carving tool.]
54. (L1) What actions were performed for anti-forensics on USB drive 'RM#2'? [Hint: this can be inferred from the results of Question 53.]
55. (L3) What files were copied from PC to USB drive 'RM#2'? [Hint: this can be inferred from the results of deleted data recovery in Question 53 and from the results of traversed files/directories in Question 25 and 26.]
56. (L2) Recover hidden files from the CD-R 'RM#3'. How to determine proper filenames of the original files prior to renaming tasks? [Hint: use file carving and metadata based data recovery tools.]
57. (L2) What actions were performed for anti-forensics on CD-R 'RM#3'? [Hint: this can be inferred from CD-R image examination.]
58. (L3) Create a detailed timeline of data leakage processes.
59. (L3) List and explain methodologies of data leakage performed by the suspect.
60. (L3) Create a visual diagram for a summary of results.

Deliverables

Write a forensic report that describes your findings. This report can consist exclusively in your (detailed and justified) answers to the questions posed in the previous section. The deadline for this work is November 24^{th}. Until then, you must upload to Fenix a compressed zip file containing your report alone.

Good luck!