Activity: Computer Forensics

Instructors : Kunwadee Sripanidkulchai, Ph.D.

Overview

In this activity, we will practice our forensics analysis skills. There are 2 parts to this activity: (1) File Carving and (2) Investigation. This activity is best done on Windows machines.

Part I. File Carving

We will use autopsy to analyze file system images. Autopsy may be installed on non-Windows machines, but requires configuring the right dependencies. In the past, I have had trouble getting it to work on my Mac. Try this at your own risk as it is not guaranteed to work. It is easier to install the Windows version on a Windows VM on your Mac/Linux notebook.

Download autopsy from https://www.sleuthkit.org/autopsy/download.php or https://drive.google.com/drive/folders/13l4w5CDAbCbpUXvr_tkY3OQNPd58-LP8?usp=sharing. Follow the instructions on the web page to install this on your notebook. Do this ahead-of-time because the installation file is large (1+ GB) .

Autopsy analyzes disk images, local drives, or a folder of local files. It has the following features:
Multi-User Cases, Timeline Analysis, Keyword Search, Web Artifacts, Registry Analysis, LNK File Analysis, Email Analysis, EXIF, File Type Sorting, Media Playback, Thumbnail viewer, Robust File System Analysis, Hash Set Filtering, Tags, Unicode Strings Extraction, File Type Detection, Interesting Files Module, Android Support. Read the documentation at
https://www.sleuthkit.org/autopsy/docs/user-docs/latest/

You are given a test disk of a FAT32 file system here https://goo.gl/eL7kgP. The file name is forensics-p2.dd.

Your goal is to test data carving capabilities of autopsy to extract various files out from the image. Load the image, and run the ingest modules (under Tools).

The image contains several allocated and deleted files and the header of one JPEG file was modified (to show the importance of ignoring corrupted files). The FAT boot sector has been corrupted so that the image cannot be mounted and therefore data carving methods must be used to extract the files.

Use autopsy to explore what files you can recover. There are a total of 14 files in this image. Find as many as you can answer the questions.

1. Look at the data on the file system (Click on Data Sources and look at the hex values on the right). The file system has no files, but why are we able to find items on the disk image? Explain why the file system has no files but there are items that can be found on the disk image.
2. How many objects can you find?
3. List all the objects here and report on whether or not the content is accessible or damaged/corrupted. Also note which files were actually already deleted.
4. Think securely: If we want to delete files on a magnetic hard disk and not have them be recovered by any tool, what do we need to do? And how much time do you think you need to wipe a 1TB magnetic hard disk?
5. Will file carving be able to recover deleted files on an SSD? Why or why not?

Part II. Investigation

Again, we will use autopsy to explore a more realistic scenario.

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 visited by 'Mr. Informant' for business, he received an offer from '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 through 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:

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

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.

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

All employees are required to pass through the 'Security Checkpoint' system.

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.

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

There are many steps to work on, and the most revealing one will be to work with the PC disk. But due to limited time and storage, we will focus on examining the removable media #2 (https://goo.gl/EptMH3) and #3 (https://goo.gl/73hKgN).

Answer these questions:

1. List all directories that were traversed in ‘RM#2’.
2. List all files that were opened in 'RM#2’.

3. Recover deleted files from USB drive 'RM#2'. What files were you able to recover?
4. What actions were performed for anti-forensics on USB drive 'RM#2'? [Hint: this can be inferred from the results of the above question]

Examine media #3.

5. Recover hidden files from the CD-R 'RM#3'. What files were you able to recover?
6. What actions were performed for anti-forensics on CD-R 'RM#3'?