Group “½ of 5”

The Rupert Case

GROUP 5.8 ASSIGNMENT

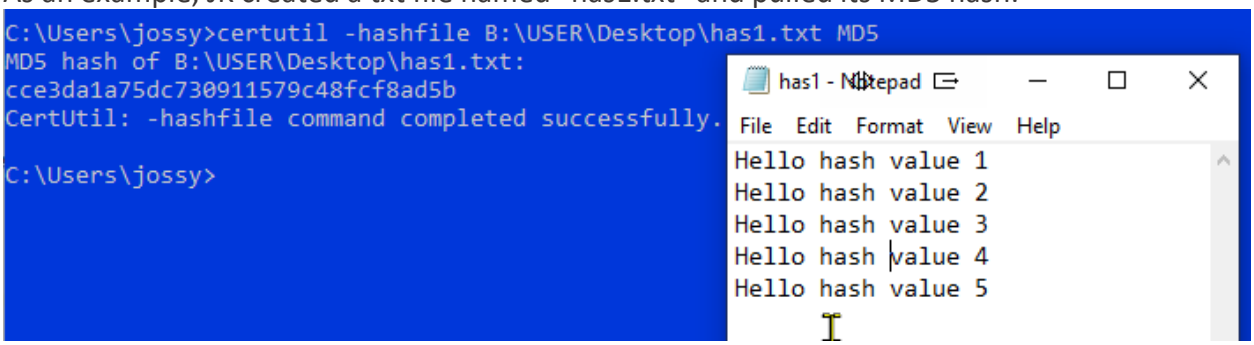
ANNA LIZA SMITH, IIRAI COSTNER, JOSE KRASNIANSKY

1. Why is it important to take note of the hash value of the drive image? What function does it serve?

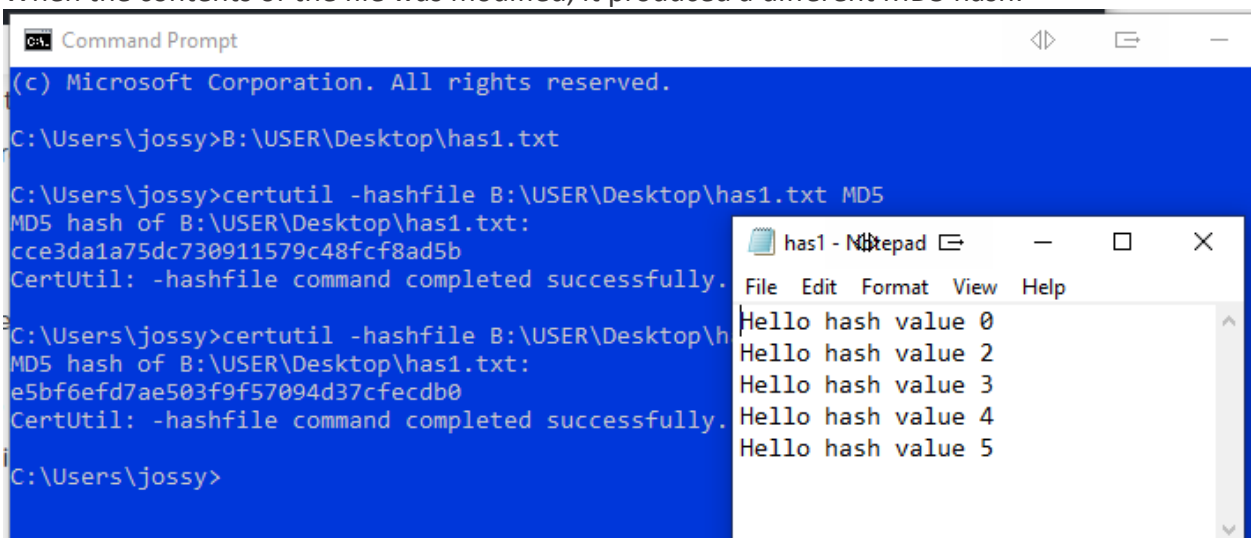
Taking note of the hash value of the drive image is crucial for ensuring the integrity of data, maintaining its admissibility in court, and enabling traceability and accountability in the forensic analysis.

It serves as a digital fingerprint (like a single letter in a document) by generating a unique fixed-size value for the given input data. Any changes to the input data will result in a different hash. The function of this digital fingerprint is to ensure the integrity and authenticity of the data, confirming a copy or clone of the image is identical to the original, without any changes or tampering.

As an example, JK created a txt file named "has1.txt" and pulled its MD5 hash:



When the contents of the file was modified, it produced a different MD5 hash:



For this Rupert Case group assignment, we've noted the different hashes below, along with a screenshot for MD5:

```
┌──(root㉿kali)-[/home/kali]
└─# dcfldd if=/media/cdrom0/ hash=md5 of=/home/kali/Downloads/rubert-usb.iso bs=512
dcfldd:/media/cdrom0/: Is a directory

Total (md5): d41d8cd98f00b204e9800998ecf8427e

0+0 records in
0+0 records out
```

MD5:fb3e88027e8fce90a2287b9ec4f2647e
SHA1:59af595ffb5367efc9a45c5a0194629f5ab9944c
RIPEMD160:de2f940f8af63faefcda9e06195966ec4c108f9d
CR32:e0a45e70

2. What kinds of important metadata are usually collected in a disk image such as this one? How can this metadata shape your investigation?

Metadata refers to the data that describes the attributes of a file or document. It can be found in many types of files on a hard drive, such as images, documents, videos, and audio recordings. By examining the metadata, we can often obtain important information about the file, including when it was created, who created it, and what software was used to create it.

For example, in a picture, we can find metadata that tells us where and when the picture was taken, what type of camera was used, and who owns the device that took the picture. Similarly, in a document, we can find metadata that tells us who created the document, when it was last edited, and what software was used to create it.

Commonly used computer metadata collected in a disk image includes:

a. **File System Metadata**: File attributes can indicate if a file is hidden, read-only, compressed, or modified. Timestamps can provide information on when files were created, modified, or accessed. File size information can help identify potentially suspicious files that are significantly larger or smaller than expected. File system metadata, such as the file allocation (FAT) or master file table (MFT), can provide information about the file system structure and can help identify deleted files or hidden data.
b. **Deleted Files Metadata**: When a file is deleted from a USB drive, it is not immediately removed from the device. Instead, the file system removes the reference to the file from the file allocation table, making the file inaccessible to the user. However, the file content remains on the device until it is overwritten

by new data. Metadata about deleted files can provide valuable information about the data that was once present on the device.

c. **User Account Information**: This metadata can include usernames, passwords, and other account-related information that can be used to identify who accessed the USB drive and when.
d. **System Metadata**: This includes system-level information such as the hardware configuration of the USB device, the operating system version, and other system settings that can provide additional context to an investigation.

The metadata collected from a USB drive image can shape an investigation by providing valuable insights and assist in piecing together the events leading up to a particular incident. Forensic investigators can glean information from the data on a disk image and identify potentially relevant files and directories. They can recover deleted data or identify data that has been hidden or tampered with.

3. When it comes to keeping this disk image secure, what sort of preservation techniques would you recommend?

Here are some preservation techniques that we would recommend:

a. **Write-Protect the Original Device:** Write protection prevents accidental or intentional modifications and can be achieved through various means, such as setting the file attribute to read-only or using write-blockers.
b. **Store the Image in a Secure Location**: Storage should be on a secure, write-protected device in a controlled environment to prevent physical damage, and only authorized individuals should have access.
c. **Verify the Integrity of the Image**: Before storing the disk image, its integrity should be verified using a hash function such as SHA-256 or MD5. This hash value should be recorded and stored separately from the disk image itself to ensure its authenticity.
d. **Use Encryption**: Using encryption protects the confidentiality of the data by ensuring only an authorized individual can access it. If the disk image contains sensitive information, it should be encrypted to prevent unauthorized access. Full-disk encryption or file-level encryption can be used to protect the data on the disk image.
e. **Backup**: Backup is always recommended to ensure evidence remains secure and intact in case of unforeseen events, such as data corruption or loss. Regular backups of the disk image should be created and stored in multiple locations to ensure the preservation of evidence in case of data loss or corruption. These backups should also be encrypted and stored securely.
f. **Document the Preservation Process**: Documentation and its chain of custody ensures admissibility of the evidence in court and should include details such as

who created the disk image, when, and who has access. The preservation process should be thoroughly documented to ensure that it can be reproduced and verified in the future. This documentation should include details such as the date and time of the preservation, the tools and methods used, and the personnel involved in the process.

4. How will using this tool help you in your case against Rupert?

Autopsy is an open-source digital forensic tool that allows forensic analysts to analyze images and file systems and investigate digital evidence in a user-friendly interface, using advanced tools for data recovery, search, and indexing of files and metadata. Using file analysis, it can identify suspicious or incriminating data by analyzing various file types and metadata information. This can help investigators identify files Rupert accessed or modified shortly before or after the alleged theft occurred.

5. From Autopsy, you could see the file names in the DT Watch folder. Many of them are identical to the sensitive files on the research and development server that was breached, including the smartwatch_schematic3.png file that the host-based intrusion detection system (HIDS) detected was being copied to a remote host. You could also view these files and verify that they contain sensitive information—including the smartwatch schematic and other smartwatch-related content. These are all files that Rupert does not have authorization to view, much less copy off the server. Considering all of your work so far, how confident are you of Rupert's involvement in the incident? Justify your position with evidence.

The next page shows a list of files found in the USB that may serve as evidence to confirm Rupert's involvement in the incident:

File	MD5 Hash	Created Time	File Path
WATCH_PI.JPG	5f53e931167475bdefbd4df4605808fd	2/20/2015 1:10	/DT_WATCH/WATCH_PI.JPG
SCHEMATI.JPG	3645ee25b8bd60437ab7cb3f9fdd888a	2/20/2015 1:10	/DT_WATCH/SCHEMATI.JPG
WATCH2.JPG	4de8e4053750cc2bd4e845e5eb391301	2/20/2015 1:11	/DT_WATCH/WATCH2.JPG
SCHEMA.JPG	d0fa52407d1e4fd13ee4eeb7343b6a97	2/20/2015 1:11	/DT_WATCH/SCHEMA.JPG
MANUFACT.JPG	7d27927642efba1755633fa5eeddf773	2/20/2015 1:12	/DT_WATCH/MANUFACT.JPG
CONCEPT.JPG	607f28f94a6809b63e371846185592c8	2/20/2015 1:12	/DT_WATCH/CONCEPT.JPG
WEARABLE.DOC	737963878de6909b4dd10438bba6c6d0	2/20/2015 1:13	/DT_WATCH/WEARABLE.DOC
SMARTWAT.PNG	a8667d58f4a698dfc437e5bac4ef83d7	2/20/2015 1:15	/DT_WATCH/SMARTWAT.PNG
CAPABILI.JPG	62b464c57b5668495b50dec5502484a2	2/20/2015 1:15	/DT_WATCH/CAPABILI.JPG
IMAGE3.JPG	a0bbfb3ee870546eea2cfeee0b6eb081	2/20/2015 1:18	/DT_WATCH/IMAGE3.JPG
PROTOTYP.JPG	883912f8f60943fdb610cf3760360985	2/20/2015 1:18	/DT_WATCH/PROTOTYP.JPG
BUDGET.XLS	8f246ea7378f044a9538d950031a9b3a	2/20/2015 20:23	/DT_WATCH/BUDGET.XLS
CASH_FLO.EXE	0a0794b05d0f71a9c4e61156f5a6762d	2/20/2015 20:24	/DT_WATCH/CASH_FLO.EXE
FUN_STUF.DOC	9b83afd7576d5901aa349871b97a296c	2/20/2015 20:26	/FUN_STUF.DOC
MY_CONTR.DOC	6c31658ad9bc76ac99b17a3cf1e50fc8	2/23/2015 22:36	/MY_CONTR.DOC
image2.jpeg	cbc3ba1ec530e65754d12c2e5fb5acac	-	/DT_WATCH/WEARABLE.DOC/image2.jpeg
image4.jpeg	b46cc450e5beabcc9cfe27e209439db8	-	/DT_WATCH/WEARABLE.DOC/image4.jpeg
image5.jpeg	2b0ebd288048dd5eeceda6afd33ceecd	-	/DT_WATCH/WEARABLE.DOC/image5.jpeg
image6.jpeg	d1919b352c77f56c23fb134a3a0e5c0e	-	/DT_WATCH/WEARABLE.DOC/image6.jpeg

Based on this evidence, including the fact that the sensitive files from the research and development server were found in the DT_Watch folder, it appears highly likely that Rupert was involved in the incident of stealing sensitive information. The following evidence supports this position:

- **File names**: Autopsy revealed that many of the file names in the DT_Watch folder on Rupert's USB drive were identical to the sensitive files on the research and development server that was breached. This suggests that Rupert had access to the sensitive files on the server and deliberately copied them to his USB drive.
- **HIDS alert**: The host-based intrusion detection system (HIDS) detected that the smartwatch_schematic3.png file was being copied to a remote host. This file was found on Rupert's USB drive, further suggesting that he was involved in the incident.
- **File contents**: Upon viewing the files in the DT_Watch folder, it was confirmed that they contained sensitive information, including the smartwatch schematic and other smartwatch-related content. Rupert does not have authorization to view or copy these files, providing further evidence of his involvement in the incident. This may suggest Rupert obtained privileged access to the DT_Watch folder which means he possibly had some access to the research and dev server.

Overall, the evidence gathered from Autopsy and the HIDS alert strongly suggest that Rupert was involved in the incident of stealing sensitive information from the research and development server. The file names, contents, and HIDS alert all point to Rupert as the culprit.

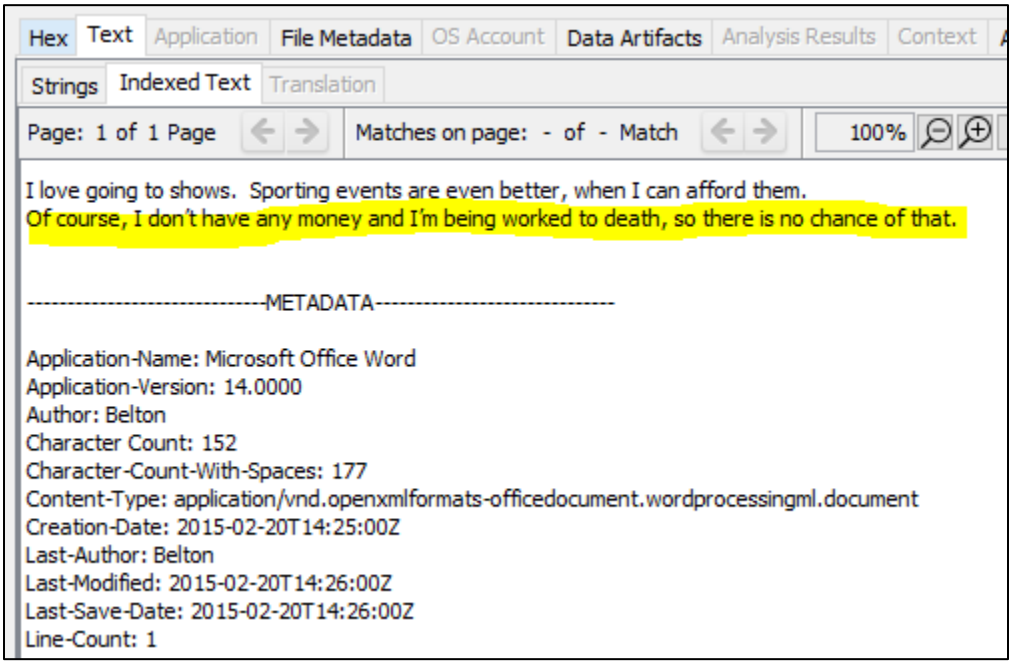
6. The team is looking to establish a motive. They've interviewed some of Rupert's coworkers, some of whom reveal that Rupert appeared frustrated

with his job. He believed that he was underpaid and treated poorly by his bosses. They claim that only a few days ago, Rupert mentioned that he was offered a job by a competitor. Given the nature of the evidence you've analyzed, what would you suggest Rupert's intentions were?

Based on the evidence analyzed, it is possible to suggest that Rupert's intentions were to steal sensitive information from the research and development server and potentially sell it to a competitor. The following points support this suggestion:

- **Copying sensitive files:** Autopsy revealed that Rupert had copied sensitive files from the research and development server onto his USB drive. This suggests that he intended to take the information with him. Also note the creation date/time of the files in the USB. All of these sensitive company files transferred to his USB drive on 2/20/2015 was done in under 10 minutes.

- **File names and contents:** The sensitive files that Rupert copied were related to smartwatch technology. Given that he was frustrated with his job and believed that he was underpaid, it is possible that he intended to sell this information to a competitor for financial gain. A notable file could be the Word document, FUN_STUF.DOC, confirms Rupert's frustrations with his job:



- **Offer from a competitor:** Rupert's coworkers reported that he had mentioned being offered a job by a competitor just a few days before the incident. This

raises the possibility that he intended to use the stolen information to impress his potential new employer or to secure a higher salary or better job offer. On 2/23/2015, 3 days after the transfer of sensitive files to his USB drive, a Word document titled MY_CONTR.DOC was added:

Rupert

INVOICE

INVOICE #3
DATE: 5/1/2013

TO:
Develetech
Greene City, RL
555-555-5555

FOR:
Consulting

DESCRIPTION	HOURS	RATE	AMOUNT
Consulting	40	$15/hr	$600
		TOTAL	$600

Make all checks payable to Rupert

This may or may not be noteworthy, but it appears to be a contract dated back in 2013, which may suggest Rupert having had done this for a while, or it may not mean anything related to this case. Overall, while it is impossible to know for certain what Rupert's intentions were without further evidence, the combination of his frustration with his job, the nature of the stolen information, and the offer from a competitor suggest that his intentions may have been to steal the information for financial gain or to use it to secure a better job offer.