



University of Dhaka
Dept. of Computer Science and Engineering
Professional Masters in Information and Cyber
Security (PMICS) Program

CSE 808 - Information Infrastructure Protection

Practical Demonstration of CIA

Lab Class 2 – Manual

Conducted by: Md. Shakhawat Hossain Robin

INTEGRITY

Integrity of CIA Triad

Data Integrity and its Importance

Data integrity refers to the accuracy, consistency, and reliability of data over its entire lifecycle. It ensures that data remains unchanged and uncorrupted, maintaining its integrity and trustworthiness. Data integrity is crucial for various reasons:

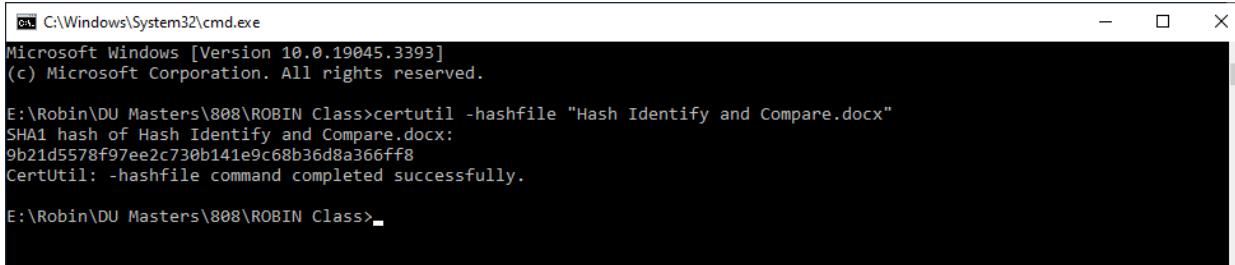
- **Security:** Detects unauthorized modifications or tampering of files, which could be indicators of malicious activity, such as malware infections, unauthorized access, or data breaches. File integrity checking helps detect and mitigate security threats by identifying unauthorized changes to files.
- **Compliance:** Many industries and organizations are required to comply with regulations and standards that mandate file integrity checking as part of their security and compliance requirements. Examples include the Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and Sarbanes-Oxley Act (SOX).
- **Prevention of Data Loss:** Identifies file corruption or errors that could lead to data loss or system instability. By detecting and correcting file integrity issues proactively, organizations can prevent data loss and minimize downtime.
- **Forensic Analysis:** Helps with forensic analysis and investigation by providing a reliable baseline of files and their integrity status. This is essential for determining the scope and impact of security incidents, as well as identifying the root cause of data breaches or system compromises.
- **Trust and Reliability:** Builds trust and confidence in data and systems by ensuring the integrity and authenticity of files. This is particularly important in environments where data accuracy and reliability are critical, such as in e-commerce, online banking, and healthcare.

Checking the integrity of a file using CMD.exe

View default hash algorithm

To see the default hash value in CMD execute the below command. This command provide the SHA1 hash value.

Command: Certutil -hashfile "filename"



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3393]
(c) Microsoft Corporation. All rights reserved.

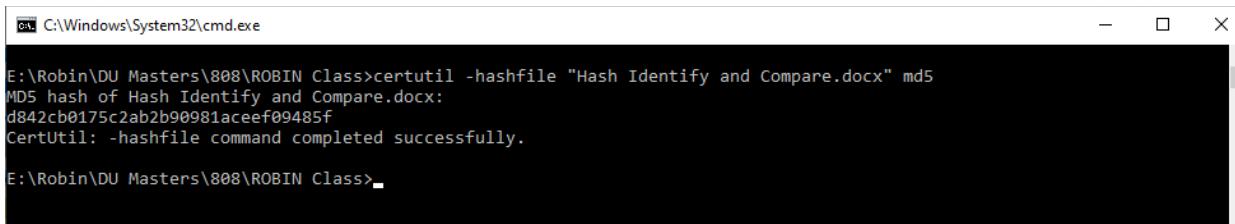
E:\Robin\DU Masters\808\ROBIN Class>certutil -hashfile "Hash Identify and Compare.docx"
SHA1 hash of Hash Identify and Compare.docx:
9b21d5578f97ee2c730b141e9c68b36d8a366ff8
CertUtil: -hashfile command completed successfully.

E:\Robin\DU Masters\808\ROBIN Class>
```

View specific types of hash algorithm

To see the specific types of hash value in CMD execute the below command.

Command: Certutil -hashfile "filename" md5



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.3393]
(c) Microsoft Corporation. All rights reserved.

E:\Robin\DU Masters\808\ROBIN Class>certutil -hashfile "Hash Identify and Compare.docx" md5
MD5 hash of Hash Identify and Compare.docx:
d842cb0175c2ab2b90981aceef09485f
CertUtil: -hashfile command completed successfully.

E:\Robin\DU Masters\808\ROBIN Class>
```

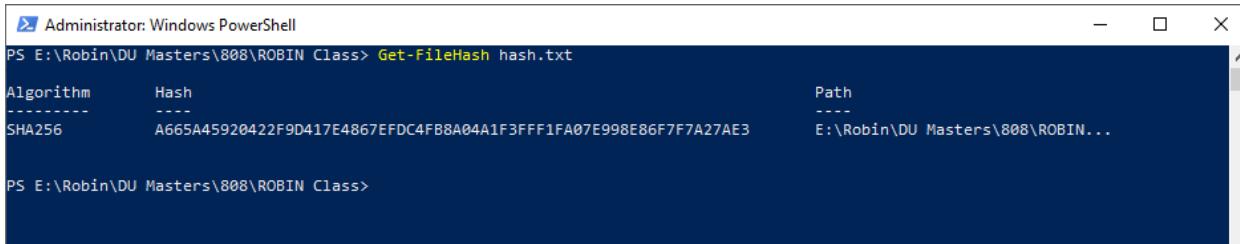
N: B: Instead of md5 we can use sha1, sha256, and any other hash algorithm.

Checking the integrity of a file using Powershell.exe

View default hash algorithm

To see the default hash value in powershell execute the below command. This command provide the SHA256 hash value as a powershell default value.

Command: Get-FileHash "filename"

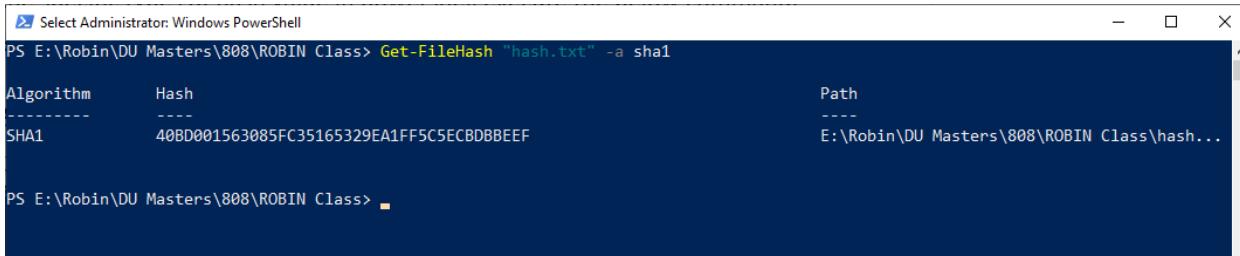


```
Administrator: Windows PowerShell
PS E:\Robin\DU Masters\808\ROBIN Class> Get-FileHash hash.txt
Algorithm      Hash                               Path
----          ----
SHA256        A665A45920422F9D417E4867EFDC4FB8A04A1F3FFF1FA07E998E86F7F7A27AE3  E:\Robin\DU Masters\808\ROBIN...
```

View specific types of hash algorithm

To see the specific types of hash value in powershell execute the below command.

Command: Get-FileHash "filename" -a SHA256



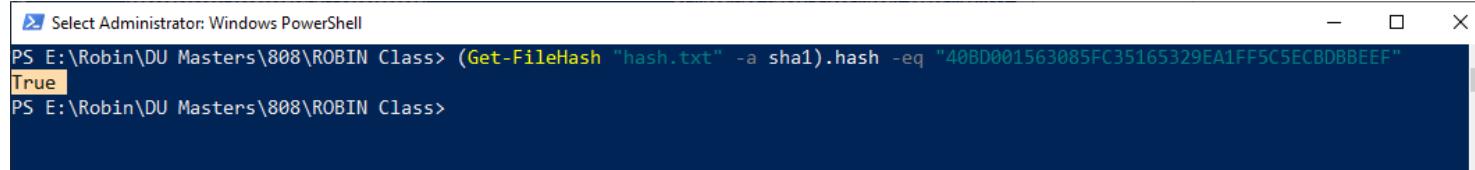
```
Select Administrator: Windows PowerShell
PS E:\Robin\DU Masters\808\ROBIN Class> Get-FileHash "hash.txt" -a sha1
Algorithm      Hash                               Path
----          ----
SHA1          40BD001563085FC35165329EA1FF5C5ECBDBBEF  E:\Robin\DU Masters\808\ROBIN Class\hash...
```

Here, -a : used for algorithm (e.g. sha256, sha512, etc.)

Compare file with hash value

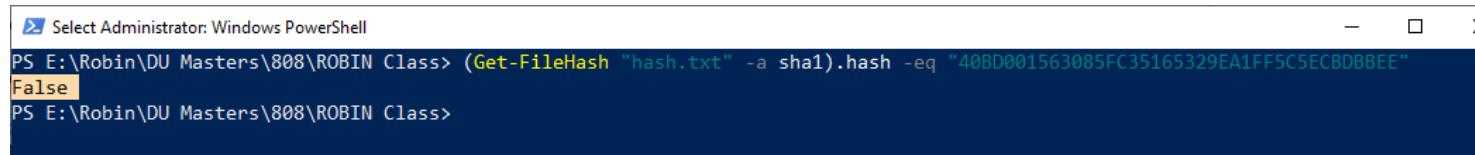
To compare a file with the provided or previously stored hash value in powershell execute the below command.

Command: `(Get-FileHash "hash.txt" -a sha1).hash -eq "hash_of_the_file"`



```
PS E:\Robin\DU Masters\808\ROBIN Class> (Get-FileHash "hash.txt" -a sha1).hash -eq "40BD001563085FC35165329EA1FF5C5ECBDBBEEF"
True
PS E:\Robin\DU Masters\808\ROBIN Class>
```

If the result found as True, it means the given hash value and the file hash are matched.



```
PS E:\Robin\DU Masters\808\ROBIN Class> (Get-FileHash "hash.txt" -a sha1).hash -eq "40BD001563085FC35165329EA1FF5C5ECBDBBEEF"
False
PS E:\Robin\DU Masters\808\ROBIN Class>
```

On the other hand, if the result is False, it means the given hash value and the file hash didn't matched.

Hash-identifier in Kali Linux

This tool is used to identify the types of a hash value. Basically it's a kali linux tools, but we can use this in different operating system by the help of python.

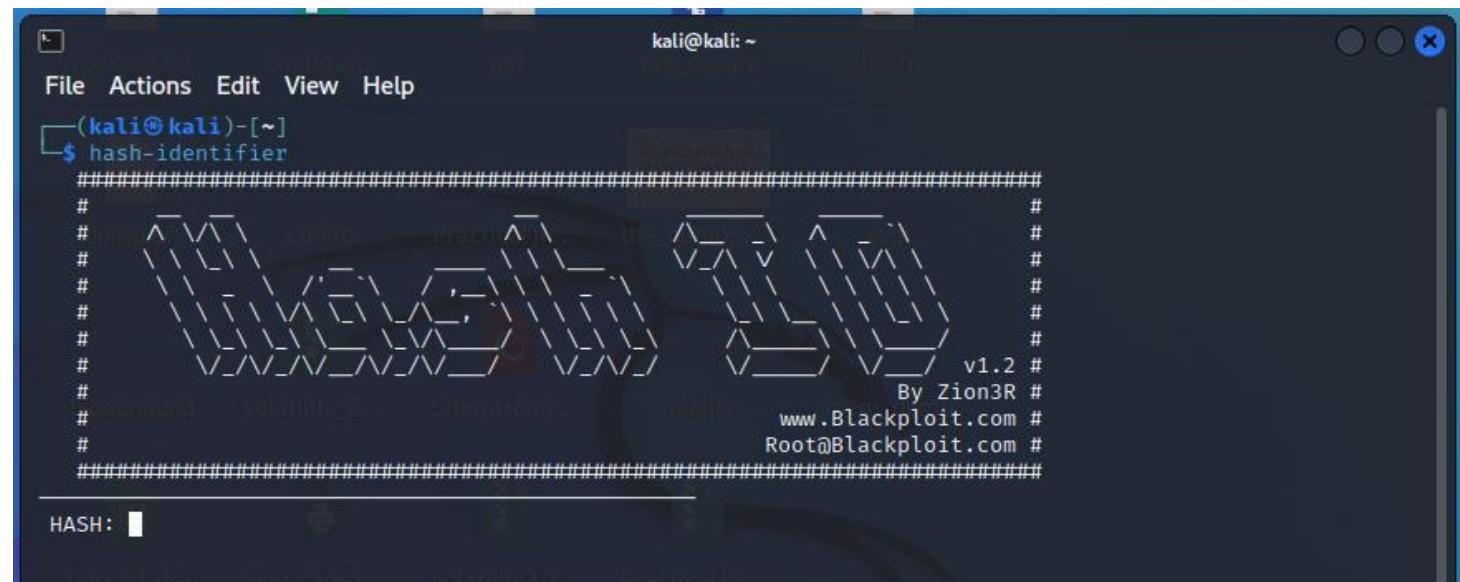
By default its keeps installed in kali linux, but somehow if the tools is missing follow the below command to install it.

To install hash-identifier

Command: sudo apt install hash-identifier

Step 1: Open terminal

Command: hash-identifier



Step 2: type or paste the hash file you want to identify and hit enter

File hash identify

➤ md5sum:

- md5sum is a simple command-line utility that calculates the MD5 hash value of files.
- It takes one or more filenames as arguments and computes the MD5 hash value for each file.
- The output consists of the MD5 hash value followed by the filename.
- Example: md5sum file.txt

```
Spiderroot
└─(root💀kali㉿kali)-[/home/kali/Desktop/pmics/encoding]
  └─# md5sum private.key
    30b6f526f4b197c96ff94b26fb14375f  private.key
```

➤ md5deep:

- md5deep is a more advanced tool that can recursively compute MD5 hash values for files in a directory tree.
- It is designed for forensic and security purposes, allowing you to verify the integrity of files in a directory and its subdirectories.
- md5deep can handle multiple files and directories as arguments and provides detailed output, including the MD5 hash value, filename, and relative path.
- It can also generate hash values in different formats and compare hash values against a list of known hashes (hash sets).
- Example: md5deep -r directory

```
Spiderroot
└─(root💀kali㉿kali)-[/home/kali/Desktop/pmics]
  └─# md5deep -r encoding
    72ce4d093f8257bd9c67b278271cc62d  /home/kali/Desktop/pmics/encoding/public.key
    30b6f526f4b197c96ff94b26fb14375f  /home/kali/Desktop/pmics/encoding/private.key
```

Thank you