Name: Harsh Mishra
Roll no: 64
Batch: T21

Aim : To explore hashdeep tool in kali linux for generating, matching and auditing hash of files.

Theory :

Hashdeep on Ubuntu is utilized for file integrity verification and forensic analysis. Here's a theoretical overview of its purpose and functionality:

Overview of Hashdeep

1. **Purpose:**
    - Hashdeep is designed to calculate and verify file hashes, ensuring data integrity and authenticity. It can help detect unauthorized changes to files, which is crucial for security audits and forensic investigations.
2. **Supported Hash Algorithms:**
    - Hashdeep supports multiple hashing algorithms:
        - MD5
        - SHA-1
        - SHA-256
        - Tiger
3. **Features:**
    - **Recursive Checking:** Hashdeep can scan directories and their subdirectories for file integrity checks.
    - **Hash Comparisons:** It allows comparing computed hashes against known good hash values stored in a file.
    - **Output Formats:** It can produce various output formats for logs and reports, which is useful for record-keeping and analysis.

Use Cases

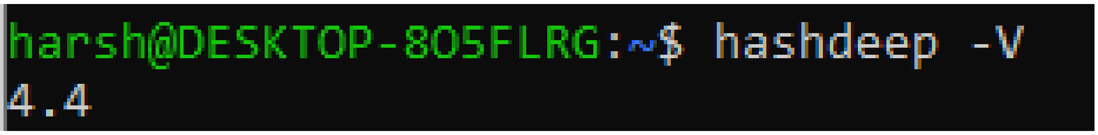
1. **File Integrity Monitoring:**
    - Regularly compute and store hashes of important files to detect unauthorized modifications.

Name: Harsh Mishra
Roll no: 64
Batch: T21

2. **Forensic Investigations:**
   - Verify the integrity of digital evidence by comparing file hashes against known values.
3. **Data Backup Verification:**
   - Ensure that backups have not been corrupted by comparing current file hashes against the original hashes.

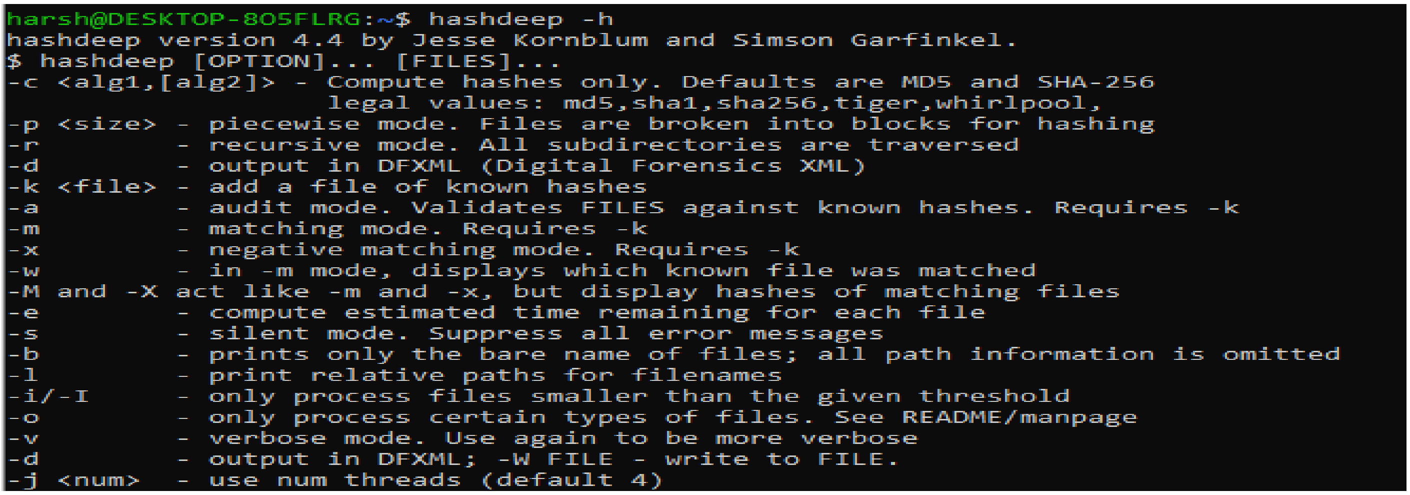
Output:

1.



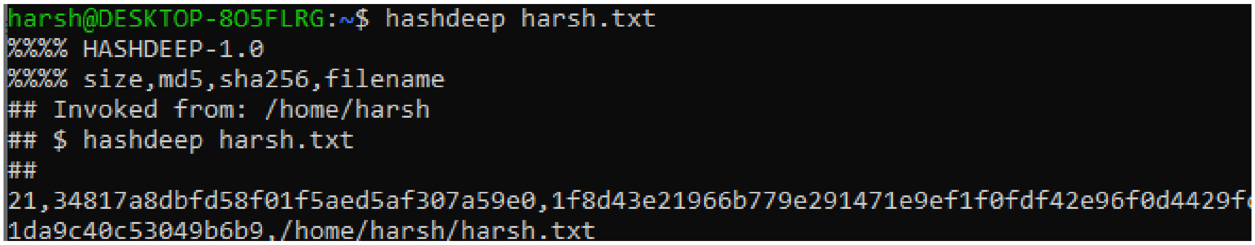
```
harsh@DESKTOP-805FLRG:~$ hashdeep -V
4.4
```

2.



```
harsh@DESKTOP-805FLRG:~$ hashdeep -h
hashdeep version 4.4 by Jesse Kornblum and Simson Garfinkel.
$ hashdeep [OPTION]... [FILES]...
-c <alg1,[alg2]> - Compute hashes only. Defaults are MD5 and SHA-256
                   legal values: md5,sha1,sha256,tiger,whirlpool,
-p <size> - piecewise mode. Files are broken into blocks for hashing
-r        - recursive mode. All subdirectories are traversed
-d        - output in DFXML (Digital Forensics XML)
-k <file> - add a file of known hashes
-a        - audit mode. Validates FILES against known hashes. Requires -k
-m        - matching mode. Requires -k
-x        - negative matching mode. Requires -k
-w        - in -m mode, displays which known file was matched
-M and -X act like -m and -x, but display hashes of matching files
-e        - compute estimated time remaining for each file
-s        - silent mode. Suppress all error messages
-b        - prints only the bare name of files; all path information is omitted
-l        - print relative paths for filenames
-i/-I     - only process files smaller than the given threshold
-o        - only process certain types of files. See README/manpage
-v        - verbose mode. Use again to be more verbose
-d        - output in DFXML; -W FILE - write to FILE.
-j <num>  - use num threads (default 4)
```

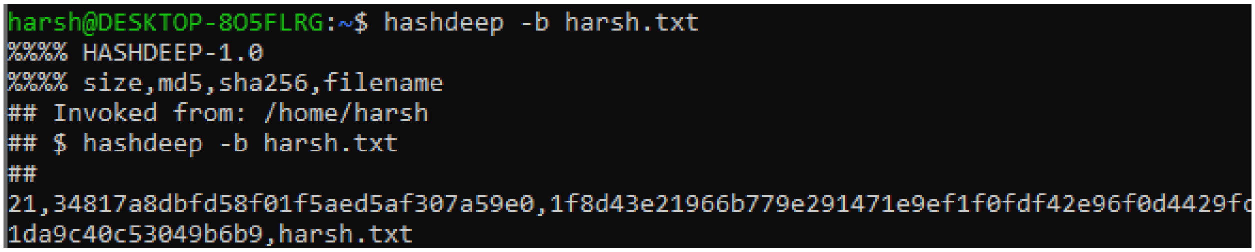
3.



```
harsh@DESKTOP-805FLRG:~$ hashdeep harsh.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/harsh
## $ hashdeep harsh.txt
##
21,34817a8dbfd58f01f5aed5af307a59e0,1f8d43e21966b779e291471e9ef1f0fdf42e96f0d4429f
1da9c40c53049b6b9,/home/harsh/harsh.txt
```

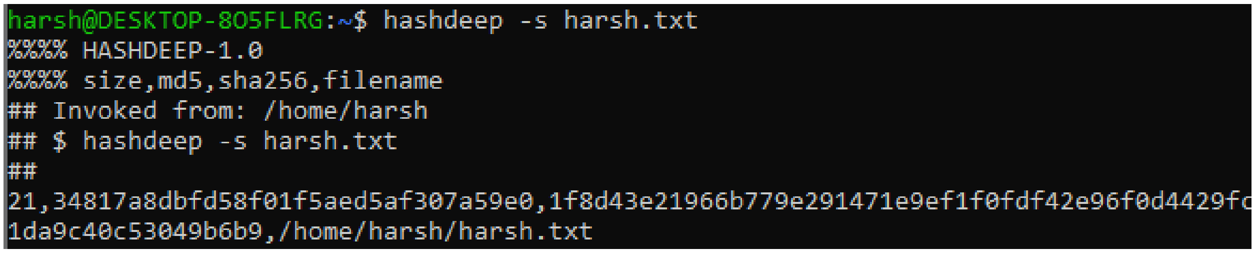
Name: Harsh Mishra
Roll no: 64
Batch: T21

4.



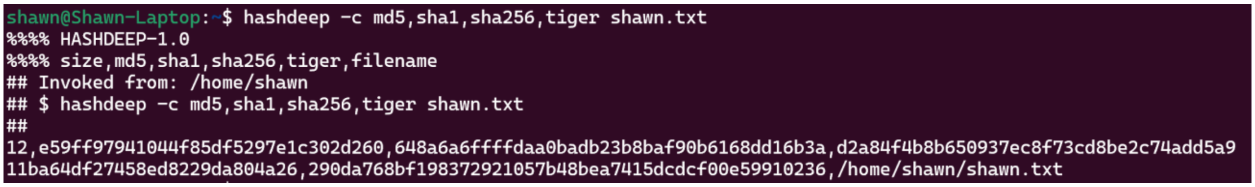
```
harsh@DESKTOP-8O5FLRG:~$ hashdeep -b harsh.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/harsh
## $ hashdeep -b harsh.txt
##
21,34817a8dbfd58f01f5aed5af307a59e0,1f8d43e21966b779e291471e9ef1f0fdf42e96f0d4429fc
1da9c40c53049b6b9,harsh.txt
```

5.



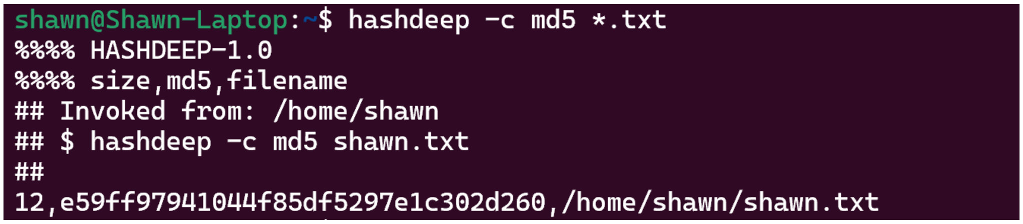
```
harsh@DESKTOP-8O5FLRG:~$ hashdeep -s harsh.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/harsh
## $ hashdeep -s harsh.txt
##
21,34817a8dbfd58f01f5aed5af307a59e0,1f8d43e21966b779e291471e9ef1f0fdf42e96f0d4429fc
1da9c40c53049b6b9,/home/harsh/harsh.txt
```

6.



```
shawn@Shawn-Laptop:~$ hashdeep -c md5,sha1,sha256,tiger shawn.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/shawn
## $ hashdeep -c md5,sha1,sha256,tiger shawn.txt
##
12,e59ff97941044f85df5297e1c302d260,648a6a6ffffdaa0badb23b8baf90b6168dd16b3a,d2a84f4b8b650937ec8f73cd8be2c74add5a9
11ba64df27458ed8229da804a26,290da768bf198372921057b48bea7415dcdcf00e59910236,/home/shawn/shawn.txt
```

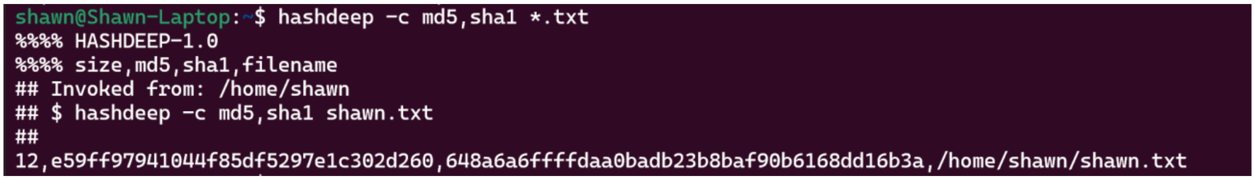
7.



```
shawn@Shawn-Laptop:~$ hashdeep -c md5 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/shawn
## $ hashdeep -c md5 shawn.txt
##
12,e59ff97941044f85df5297e1c302d260,/home/shawn/shawn.txt
```

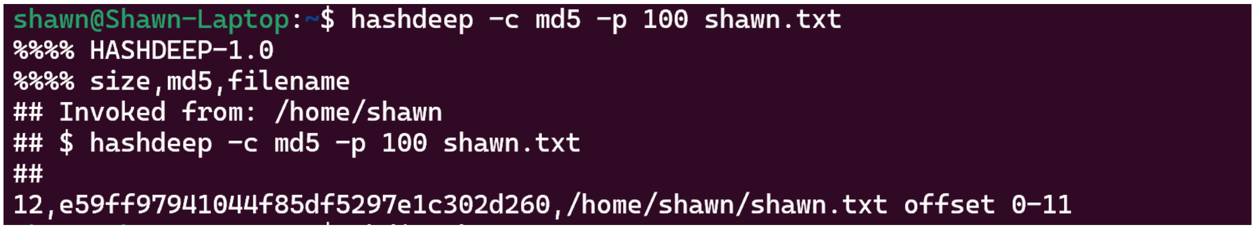
8.

Name: Harsh Mishra
Roll no: 64
Batch: T21



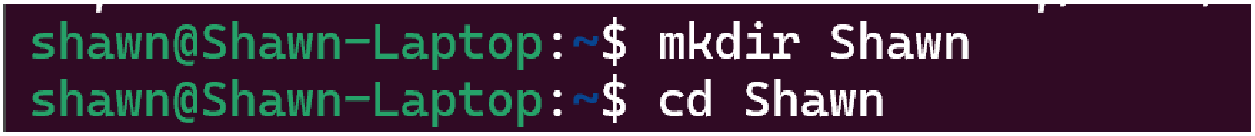
```
shawn@Shawn-Laptop:~$ hashdeep -c md5,sha1 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: /home/shawn
## $ hashdeep -c md5,sha1 shawn.txt
##
12,e59ff97941044f85df5297e1c302d260,648a6a6ffffdaa0badb23b8baf90b6168dd16b3a,/home/shawn/shawn.txt
```

9.

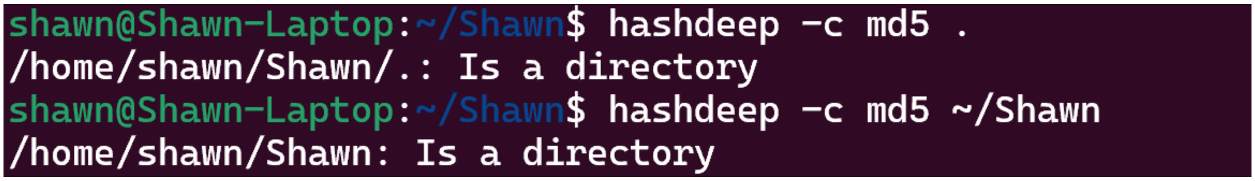


```
shawn@Shawn-Laptop:~$ hashdeep -c md5 -p 100 shawn.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/shawn
## $ hashdeep -c md5 -p 100 shawn.txt
##
12,e59ff97941044f85df5297e1c302d260,/home/shawn/shawn.txt offset 0-11
```

10.



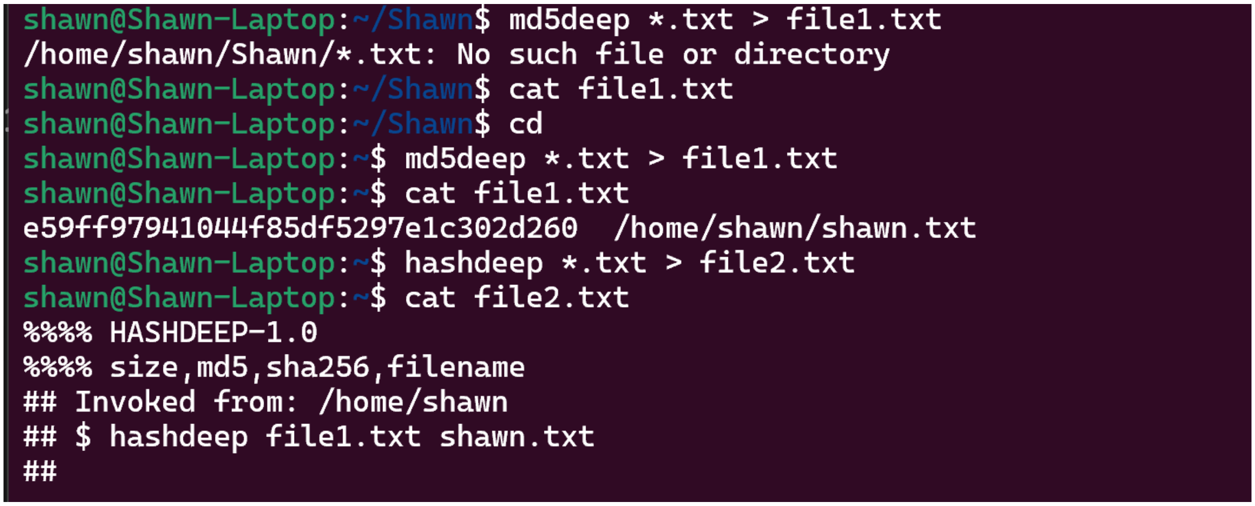
```
shawn@Shawn-Laptop:~$ mkdir Shawn
shawn@Shawn-Laptop:~$ cd Shawn
```



```
shawn@Shawn-Laptop:~/Shawn$ hashdeep -c md5 .
/home/shawn/Shawn/.: Is a directory
shawn@Shawn-Laptop:~/Shawn$ hashdeep -c md5 ~/Shawn
/home/shawn/Shawn: Is a directory
```

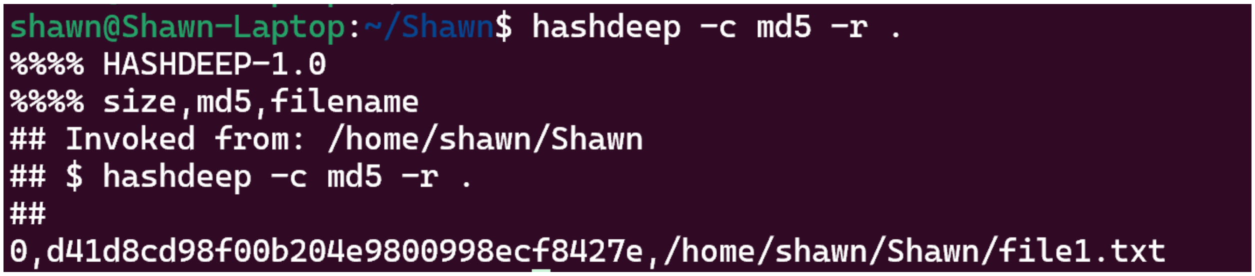
Name: Harsh Mishra
Roll no: 64
Batch: T21

11.



```
shawn@Shawn-Laptop:~/Shawn$ md5deep *.txt > file1.txt
/home/shawn/Shawn/*.txt: No such file or directory
shawn@Shawn-Laptop:~/Shawn$ cat file1.txt
shawn@Shawn-Laptop:~/Shawn$ cd
shawn@Shawn-Laptop:~$ md5deep *.txt > file1.txt
shawn@Shawn-Laptop:~$ cat file1.txt
e59ff97941044f85df5297e1c302d260  /home/shawn/shawn.txt
shawn@Shawn-Laptop:~$ hashdeep *.txt > file2.txt
shawn@Shawn-Laptop:~$ cat file2.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/shawn
## $ hashdeep file1.txt shawn.txt
##
```

12.



```
shawn@Shawn-Laptop:~/Shawn$ hashdeep -c md5 -r .
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/shawn/Shawn
## $ hashdeep -c md5 -r .
##
0,d41d8cd98f00b204e9800998ecf8427e,/home/shawn/Shawn/file1.txt
```

Conclusion: Demonstrated key management, distribution and user authentication (LO2 is achieved).