Roll no. : 53
Name: Shreya Kamath
Date: 17th August, 2023.

LAB ASSIGNMENT NO. 5

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

LAB OUTCOME ATTAINED:

LO 2: Demonstrate Key management, distribution and user authentication.

THEORY:

Hashing serves the crucial purpose of ensuring data integrity, security, and efficient data retrieval. It's used in various applications like password storage, digital signatures, data verification, and more. Hashing generates a fixed-size output (hash value) from an input (data), making it efficient for comparing large datasets and detecting changes.

Different Hashing Algorithms:
1. MD5 (Message Digest Algorithm 5)
2. SHA-1 (Secure Hash Algorithm 1)
3. SHA-256 (Secure Hash Algorithm 256)
4. SHA-512 (Secure Hash Algorithm 512)
5. SHA-3 (Secure Hash Algorithm 3)
6. Whirlpool

Hashdeep is a command-line tool in Kali Linux used for computing and verifying file hash values, such as MD5, SHA-1, SHA-256, etc. It calculates hashes for files and directories and can create hash databases for later comparison. Hashdeep supports recursive hashing, making it useful for validating file integrity over time. It's commonly used for digital forensics, data verification, and ensuring file authenticity in security assessments.

1. Check Hashdeep Version: `hashdeep -V`
2. Display Help: `hashdeep -h` or `hashdeep -hh`
3. Manual Page: `man hashdeep`
4. Manual Page for Specific Algorithm: `man md5deep`
5. Hash a File: `hashdeep filename`
6. Hash with Hidden Paths: `hashdeep -b filename`
7. Suppress Errors: `hashdeep -s filename`
8. Multiple Hash Algorithms: `hashdeep -c md5,sha1,sha256,tiger filename`
9. Hash Multiple Files (MD5): `hashdeep -c md5 *.txt`
10. Hash Multiple Files (MD5 & SHA-1): `hashdeep -c md5,sha1 *.txt`
11. Hashing Block of Files: `hashdeep -c md5 -p 100 example.txt`
12. Recursive Hashing: `hashdeep -c md5 -r /home/user/myfiles`
13. Redirect Output: `md5deep *.txt > hashset.txt`
14. Matching Mode Output: `md5deep -m hashset.txt *`
15. Suppress System Messages: `md5deep -s -m hashset.txt *`
16. Display Negatively Matching Files: `md5deep -s -x hashset.txt *`

Forensic auditing can be done using hashdeep tool which means a check to determine if any files in the system are changed due to malware or any normal system operation like update patching.

Roll no. : 53
Name: Shreya Kamath
Date: 17th August, 2023.

17. Create Hashset and Audit:
  - Create Hashset: `hashdeep -c md5,sha1,sha256 -r /home/user/myfiles > hashset1.txt`
  - Audit Files: `hashdeep -a -r -k hashset1.txt /home/user/myfiles`

18. Audit with New File (Fails):
  - Create New File: `touch /home/user/myfiles/newfile.txt`
  - Audit Again: `hashdeep -a -r -k hashset1.txt /home/user/myfiles`

19. Check Failed Points (Verbose):
  - Audit with Verbose: `hashdeep -v -a -r -k hashset1.txt /home/user/myfiles`

20. Audit After Moving File:
  - Move File: `mv /home/user/myfiles/example.txt /tmp`
  - Audit Again: `hashdeep -v -a -r -k hashset1.txt /home/user/myfiles`

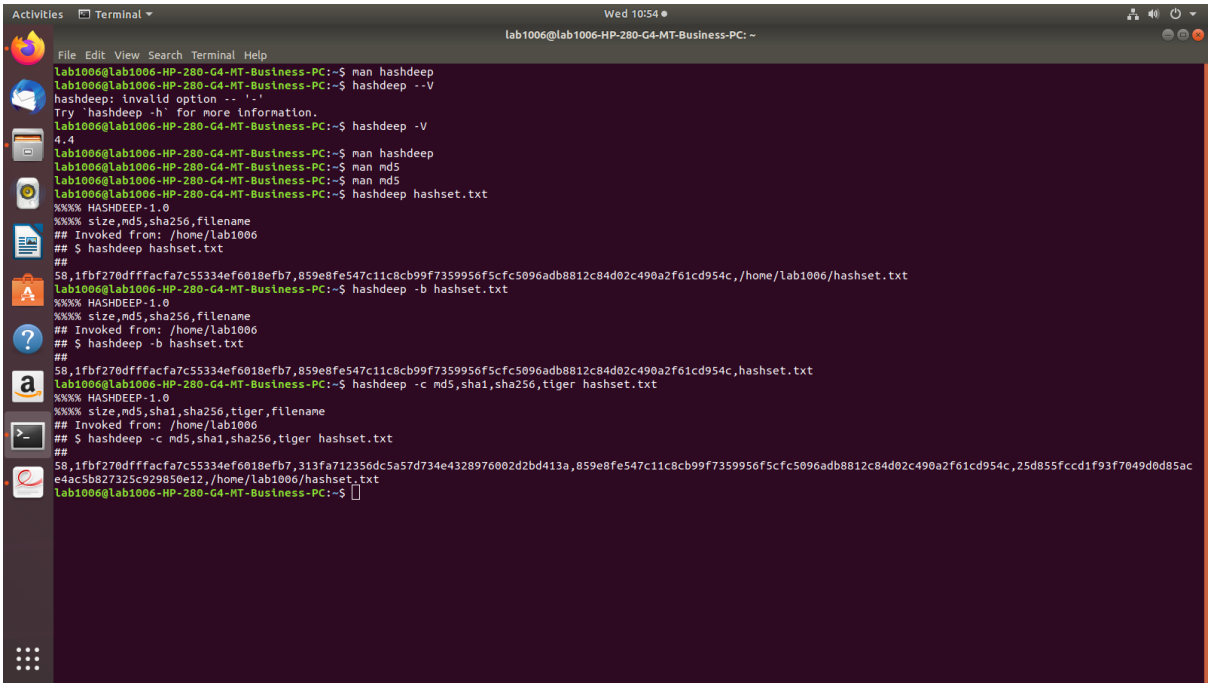
21. Audit After Renaming File:
  - Rename File: `mv /home/user/myfiles/shreya.txt /home/user/myfiles/backup.txt`
  - Audit Again: `hashdeep -v -a -r -k hashset1.txt /home/user/myfiles`

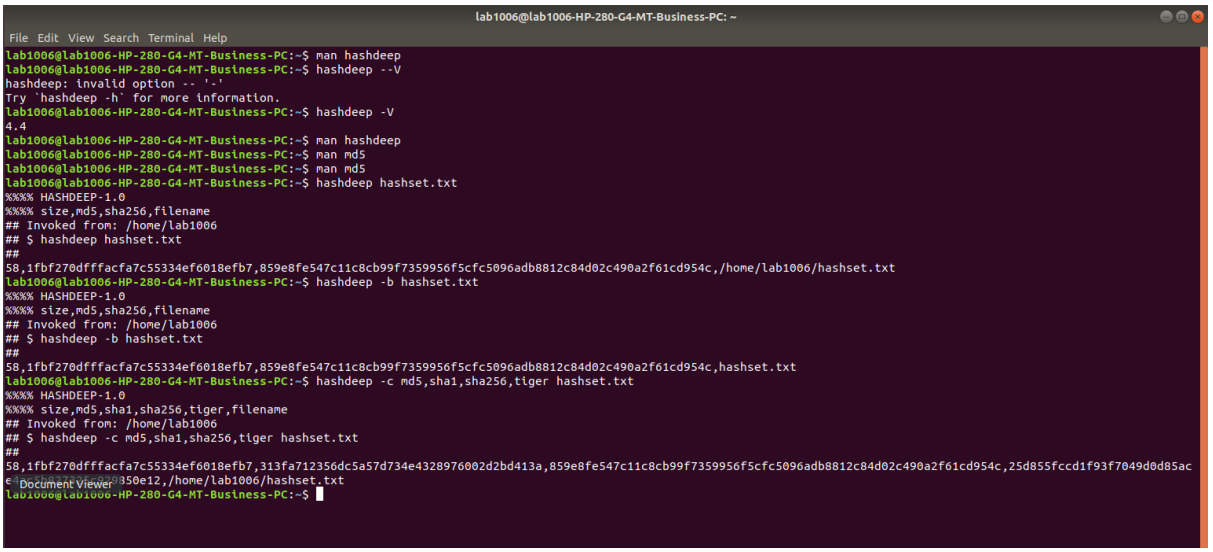
22. Verbose Audit Output:
  - More Verbose: `hashdeep -vv -a -r -k hashset1.txt /home/user/myfiles`
  - Very Verbose: `hashdeep -vvv -a -r -k hashset1.txt /home/user/myfiles`

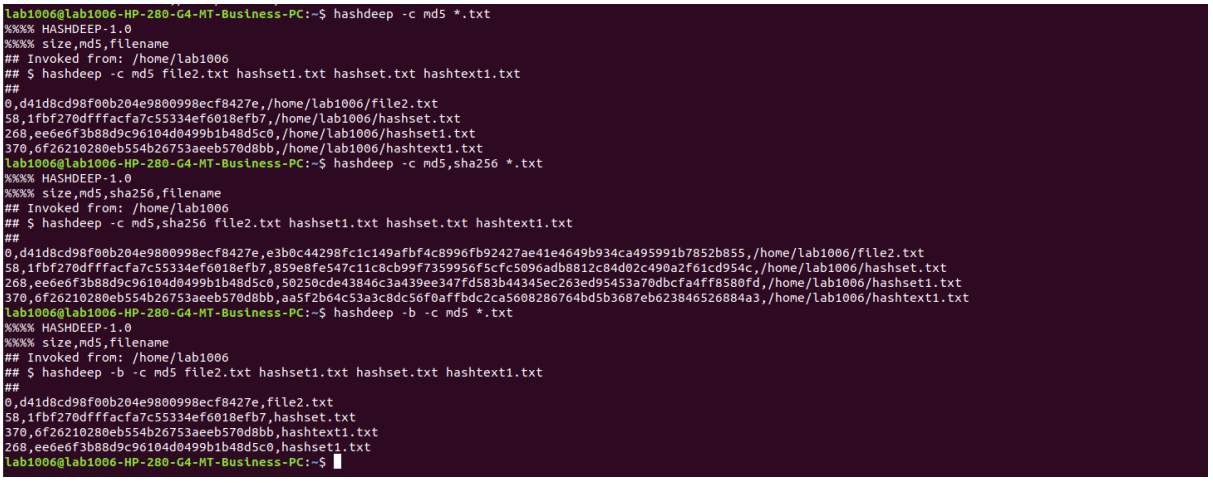
Note: Replace the paths and filenames with actual directory and file names as needed.

OUTPUT:

Roll no. : 53
Name: Shreya Kamath
Date: 17th August, 2023.







Roll no. : 53
Name: Shreya Kamath
Date: 17th August, 2023.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 hashset1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 100 hashset1.txt
##
100,52c24a1f83621f9e5be6114f45b1581f,/home/lab1006/hashset1.txt offset 0-99
100,27ea0f4cfb65783f4a79db493f28914b,/home/lab1006/hashset1.txt offset 100-199
68,c789c84006c3f1b15ce33b8e50c83001,/home/lab1006/hashset1.txt offset 200-267
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 20 hashset.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 -p 20 hashset.txt
##
20,f9892b0092d2fc81fa7b50d6ad6f85a2,/home/lab1006/hashset.txt offset 0-19
20,47578064338e85b10b8f53aa72a62e89,/home/lab1006/hashset.txt offset 20-39
18,007605755622844bc154e50b240f6e20,/home/lab1006/hashset.txt offset 40-57
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$  hashdeep c md5 -r /home/lab1006/T13-53-CNS
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -r c md5 /home/lab1006/T13-53-CNS
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/T13-53-CNS/1/file2.txt
370,6f26210280eb554b26753aeeb570d8bb,aa5f2b64c53a3c8dc56f0affbdc2ca5608286764bd5b3687eb623846526884a3,/home/lab1006/T13-53-CNS/2/hashtext1.txt
58,1fbf270dfffacfa7c55334ef6018efb7,859e8fe547c11c8cb99f7359956f5cfc5096adb8812c84d02c490a2f61cd954c,/home/lab1006/T13-53-CNS/1/hashset.txt
268,ee6e6f3b88d9c96104d0499b1b48d5c0,50250cde43846c3a439ee347fd583b44345ec263ed95453a70dbcfa4ff8580fd,/home/lab1006/T13-53-CNS/2/hashset1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/T13-53-CNS/1
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -r c md5 /home/lab1006/T13-53-CNS/1
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/T13-53-CNS/1/file2.txt
58,1fbf270dfffacfa7c55334ef6018efb7,859e8fe547c11c8cb99f7359956f5cfc5096adb8812c84d02c490a2f61cd954c,/home/lab1006/T13-53-CNS/1/hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/T13-53-CNS/2
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -r c md5 /home/lab1006/T13-53-CNS/2
##
370,6f26210280eb554b26753aeeb570d8bb,aa5f2b64c53a3c8dc56f0affbdc2ca5608286764bd5b3687eb623846526884a3,/home/lab1006/T13-53-CNS/2/hashtext1.txt
268,ee6e6f3b88d9c96104d0499b1b48d5c0,50250cde43846c3a439ee347fd583b44345ec263ed95453a70dbcfa4ff8580fd,/home/lab1006/T13-53-CNS/2/hashset1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/T13-53-CNS
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -r c md5 /home/lab1006/T13-53-CNS
##
58,1fbf270dfffacfa7c55334ef6018efb7,859e8fe547c11c8cb99f7359956f5cfc5096adb8812c84d02c490a2f61cd954c,/home/lab1006/T13-53-CNS/1/hashset.txt
268,ee6e6f3b88d9c96104d0499b1b48d5c0,50250cde43846c3a439ee347fd583b44345ec263ed95453a70dbcfa4ff8580fd,/home/lab1006/T13-53-CNS/2/hashset1.txt
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/T13-53-CNS/1/file2.txt
370,6f26210280eb554b26753aeeb570d8bb,aa5f2b64c53a3c8dc56f0affbdc2ca5608286764bd5b3687eb623846526884a3,/home/lab1006/T13-53-CNS/2/hashtext1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep *.txt>hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset4.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/hashoutput.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset4.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/hashoutput.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep *.txt>hashset5.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat hashset5.txt
9ed2bf26a0e00346cc78b1070d102897  /home/lab1006/hashset4.txt
ed5d34c74e59d16bd6d5b3683db655c3  /home/lab1006/file2.txt
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/hashoutput.txt
ee6e6f3b88d9c96104d0499b1b48d5c0  /home/lab1006/hashset1.txt
6f26210280eb554b26753aeeb570d8bb  /home/lab1006/hashtext1.txt
1fbf270dfffacfa7c55334ef6018efb7  /home/lab1006/hashset.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

Roll no. : 53
Name: Shreya Kamath
Date: 17th August, 2023.

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m hashset5.txt *
/home/lab1006/Desktop: Is a directory
/home/lab1006/Documents: Is a directory
/home/lab1006/Downloads: Is a directory
/home/lab1006/file2.txt
/home/lab1006/hashset1.txt
/home/lab1006/hashoutput.txt
/home/lab1006/mojo: Is a directory
/home/lab1006/Music: Is a directory
/home/lab1006/hashtext1.txt
/home/lab1006/hashset.txt
/home/lab1006/Pictures: Is a directory
/home/lab1006/hashset4.txt
/home/lab1006/Public: Is a directory
/home/lab1006/T13-53-CNS: Is a directory
/home/lab1006/Templates: Is a directory
/home/lab1006/Videos: Is a directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -m -s hashset5.txt *
md5deep: -s: No such file or directory
md5deep: Unable to load any matching files.
Try `md5deep -h` for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5 -s -m hashset5.txt *

Command 'md5' not found, did you mean:

  command 'mdl' from snap mdl (0.11.0)
  command 'cd5' from deb cd5
  command 'mdu' from deb mtools
  command 'mdp' from deb mdp

See 'snap info <snapname>' for additional versions.

lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -m hashset5.txt *
/home/lab1006/file2.txt
/home/lab1006/hashoutput.txt
/home/lab1006/hashset.txt
/home/lab1006/hashset4.txt
/home/lab1006/hashtext1.txt
/home/lab1006/hashset1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ md5deep -s -x newhashset.txt *
/home/lab1006/file3inverse
/home/lab1006/newhashset.txt
/home/lab1006/examples.desktop
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$
```

CONCLUSION:

Hence, I have successfully conducted an extensive exploration of forensic auditing tools, particularly Hashdeep. Through these activities, I've gained a deeper understanding of the significance of maintaining data integrity and the role Hashdeep plays in ensuring the authenticity and unaltered state of files, thus reinforcing my comprehension of forensic analysis and its relevance in preserving data reliability.