Roll No: 09
Name: Shreya Bagade
Date: 11/08/2023

LAB ASSIGNMENT NO:05

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

Lab Outcome Attained: Demonstrate Key management, distribution and user authentication.

Theory:

What is the need of hashing? List different hashing algorithms.

Hashing serves several important purposes in computer science and information security:

1. Data Integrity: Hashing is used to verify the integrity of data. By generating a hash value (digest) of the original data, any changes to the data will result in a different hash value. This makes it useful for ensuring that data has not been tampered with during storage or transmission.

2. Password Storage: Hashing is commonly used for storing passwords securely. Instead of storing actual passwords, systems store the hash of the password. When a user logs in, their entered password is hashed and compared to the stored hash, providing security even if the stored hashes are compromised.

3. Digital Signatures: Hashing is a crucial component of digital signatures. A hash of a message is signed with a private key to create a digital signature. Recipients can then verify the signature using the corresponding public key and compare the hash of the received message with the hash in the signature to ensure the message's authenticity and integrity.

4. Efficient Data Retrieval: Hashing is used in data structures like hash tables to quickly retrieve information based on a key. This provides efficient data retrieval in cases where a large amount of data needs to be stored and accessed.

5. Data Comparison: Hashing is useful for comparing large datasets. Instead of comparing the entire datasets, you can compare their hash values to quickly determine if they are the same or different.

6. Cryptography: Hash functions are used in cryptographic protocols for tasks such as generating unique identifiers (e.g., UUIDs), deriving keys, and creating message authentication codes.

7. Distributed Systems: Hashing is employed to distribute data evenly across multiple servers in distributed systems, aiding load balancing and fault tolerance.

Different hashing algorithms exist, each with its own properties, strengths, and weaknesses. Here are some commonly used hashing algorithms:

1. MD5 (Message Digest Algorithm 5): Once widely used, MD5 is now considered insecure due to vulnerabilities that allow collision attacks.

2. SHA-1 (Secure Hash Algorithm 1): Similar to MD5, SHA-1 is now considered weak and unsuitable for secure applications due to vulnerabilities.

3. SHA-256 (Secure Hash Algorithm 256): A part of the SHA-2 family, SHA-256 is widely used for data integrity and security. It produces a 256-bit hash value.

4. SHA-3 (Secure Hash Algorithm 3): A recent addition to the family of secure hash algorithms, designed to provide increased security and resistance to attacks.

5. bcrypt: A hash function specifically designed for securely hashing passwords, using a work factor that can be increased over time to counteract increasing computational power.

6. Argon2: A modern and memory-hard password hashing algorithm designed to resist attacks like brute force and GPU cracking.

7. Whirlpool: A cryptographic hash function that offers a larger bit size and is considered secure for various applications.

8. RIPEMD (RACE Integrity Primitives Evaluation Message Digest): A family of hash functions offering different bit sizes, designed as an alternative to the MD5 and SHA-1.

9. BLAKE2: A high-speed cryptographic hash function that is an improvement over its predecessor, BLAKE.

Write the commands used for generating hash values, matching them with stored hash values and auditing using hashdeep tool.

`hashdeep` is a command-line tool that is used for generating hash values, matching them with stored hash values, and performing audits to verify the integrity of files and directories. It's a useful tool for ensuring data integrity and conducting forensics investigations. Here are some common commands and their purposes using the `hashdeep` tool:

1. Generating Hash Values:

To generate hash values for files and directories, you can use the following command:

```
hashdeep -r -c SHA256 -l -vvv /path/to/directory > hash.txt
```

- `-r`: Recursively process directories.
- `-c`: Specify the hash algorithm (`SHA256` in this example).
- `-l`: Display file path for each hash entry.
- `-vvv`: Increase verbosity level.
- `/path/to/directory`: The directory you want to generate hash values for.
- `hash.txt`: Output file where hash values will be stored.

2. Matching Hash Values:

To match generated hash values with stored hash values and check for any discrepancies, use:

```
 hashdeep -r -k hash.txt /path/to/directory
```

- `-r`: Recursively process directories.
- `-k`: Use a known hash values file (previously generated using `hashdeep`).
- `hash.txt`: The file containing the stored hash values.
- `/path/to/directory`: The directory to be audited against the stored hash values.

3. Auditing and Verifying:

To perform an audit and verify the integrity of files against stored hash values, use:

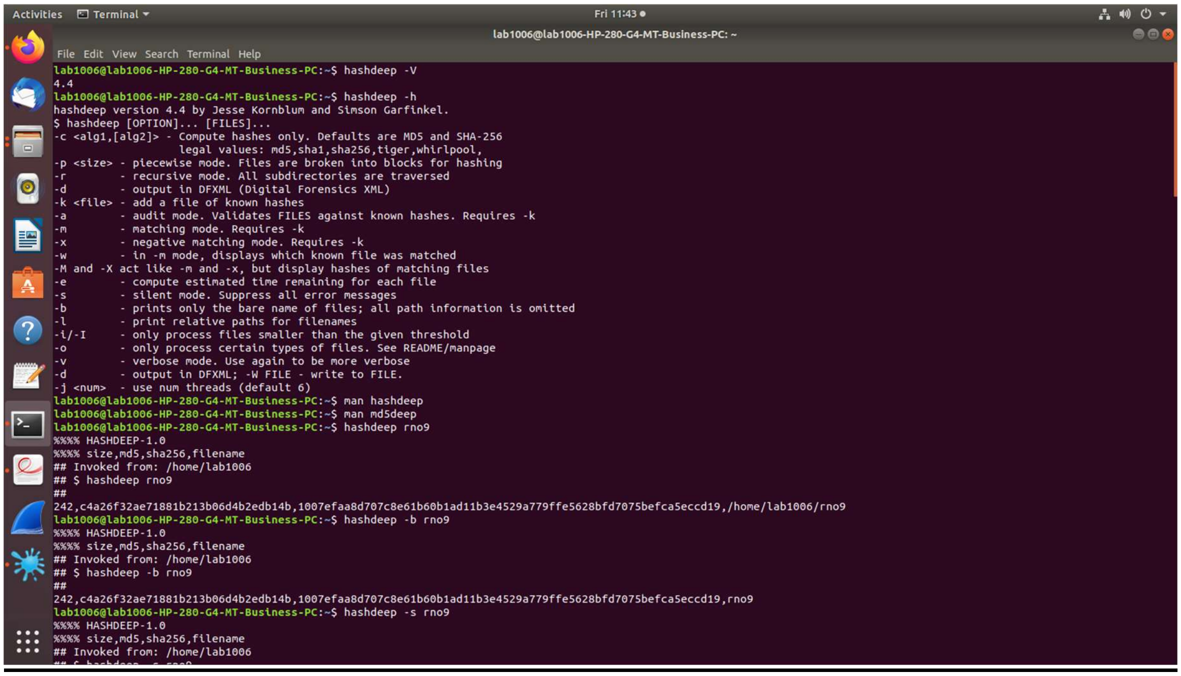
```
hashdeep -r -k -a -v -v hash.txt /path/to/directory
```

- `-r`: Recursively process directories.
- `-k`: Use a known hash values file.
- `-a`: Perform an audit to verify files.
- `-v -v`: Increase verbosity level.
- `hash.txt`: The file containing the stored hash values.
- `/path/to/directory`: The directory to be audited.

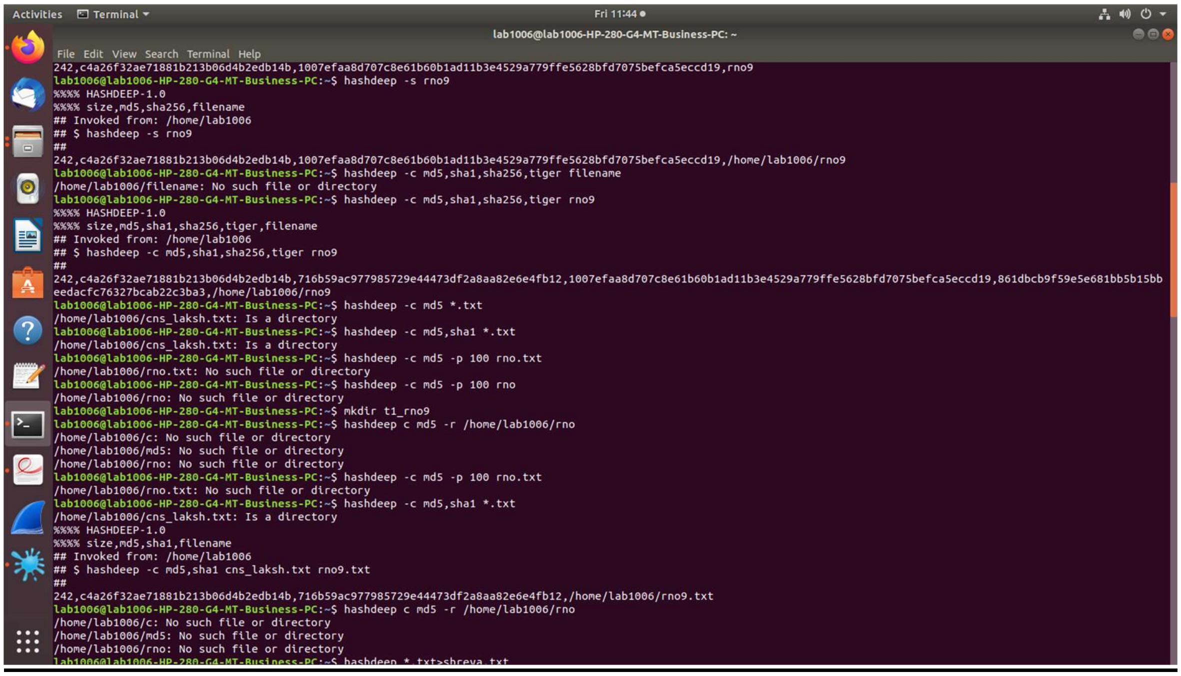
`hashdeep` supports multiple hash algorithms like SHA-1, SHA-256, MD5, etc. You can replace the `-c` option with the desired hash algorithm and adjust the other options as needed. It's important to keep the generated hash values and the tool itself in a secure location to prevent tampering.

Roll No: 09
Name: Shreya Bagade
Date: 11/08/2023

Output Screenshots:

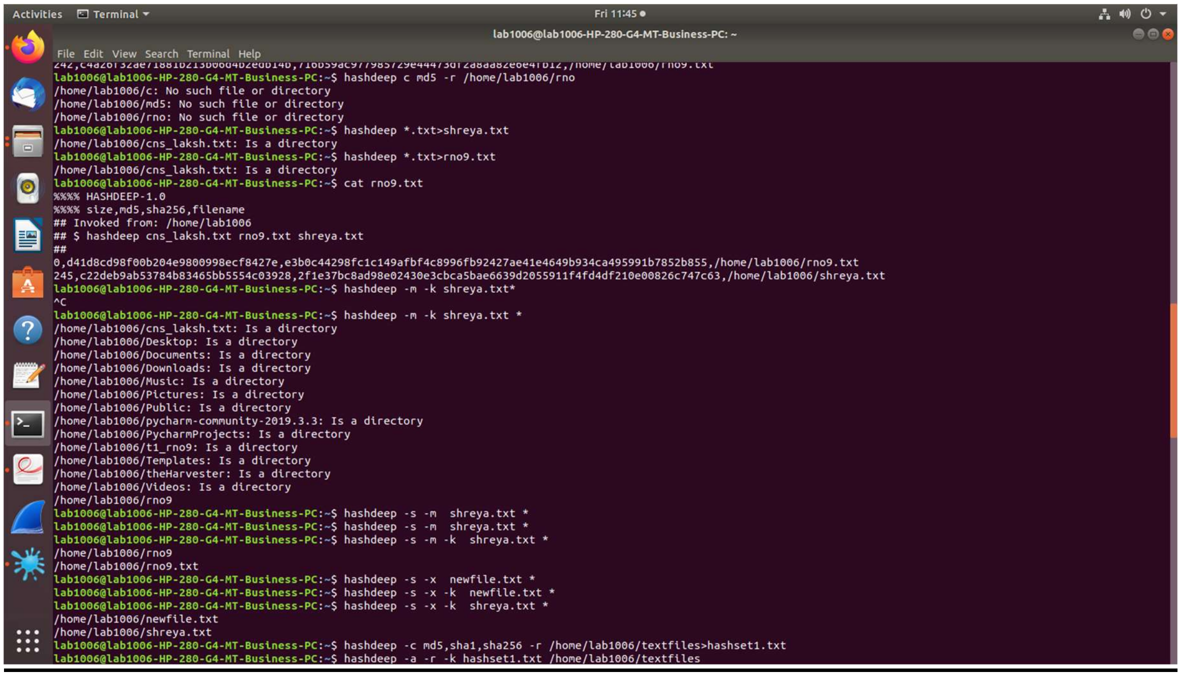

Activities
Terminal
Fri 11:43
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -V
4.4
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 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 6)
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man hashdeep
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ man md5deep
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep rno9
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep rno9
##
242,c4a26f32ae71881b213b06d4b2edb14b,1007efaa8d707c8e61b60b1ad11b3e4529a779ffe5628bfd7075befca5eccd19,/home/lab1006/rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -b rno9
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -b rno9
##
242,c4a26f32ae71881b213b06d4b2edb14b,1007efaa8d707c8e61b60b1ad11b3e4529a779ffe5628bfd7075befca5eccd19,rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s rno9
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s rno9
```

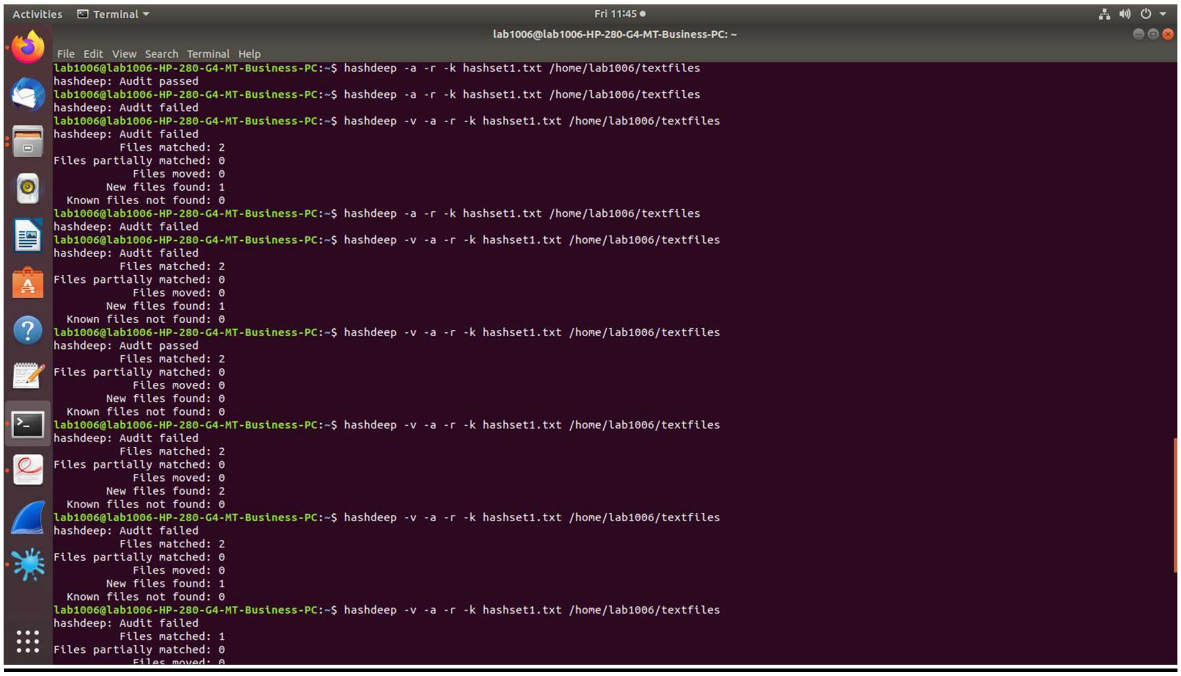

Activities
Terminal
Fri 11:44
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
242,c4a26f32ae71881b213b06d4b2edb14b,1007efaa8d707c8e61b60b1ad11b3e4529a779ffe5628bfd7075befca5eccd19,rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s rno9
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s rno9
##
242,c4a26f32ae71881b213b06d4b2edb14b,1007efaa8d707c8e61b60b1ad11b3e4529a779ffe5628bfd7075befca5eccd19,/home/lab1006/rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger filename
/home/lab1006/filename: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger rno9
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256,tiger rno9
##
242,c4a26f32ae71881b213b06d4b2edb14b,716b59ac977985729e44473df2a8aa82e6e4fb12,1007efaa8d707c8e61b60b1ad11b3e4529a779ffe5628bfd7075befca5eccd19,861dbcb9f59e5e681bb5b15bb
eedacfc76327bcab22c3ba3,/home/lab1006/rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 *.txt
/home/lab1006/cns_laksh.txt: Is a directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1 *.txt
/home/lab1006/cns_laksh.txt: Is a directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 rno.txt
/home/lab1006/rno.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 rno
/home/lab1006/rno: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ mkdir t1_rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/rno
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
/home/lab1006/rno: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 -p 100 rno.txt
/home/lab1006/rno.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1 *.txt
/home/lab1006/cns_laksh.txt: Is a directory
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1 cns_laksh.txt rno9.txt
##
242,c4a26f32ae71881b213b06d4b2edb14b,716b59ac977985729e44473df2a8aa82e6e4fb12,/home/lab1006/rno9.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/rno
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
/home/lab1006/rno: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep *.txt>shreya.txt
```

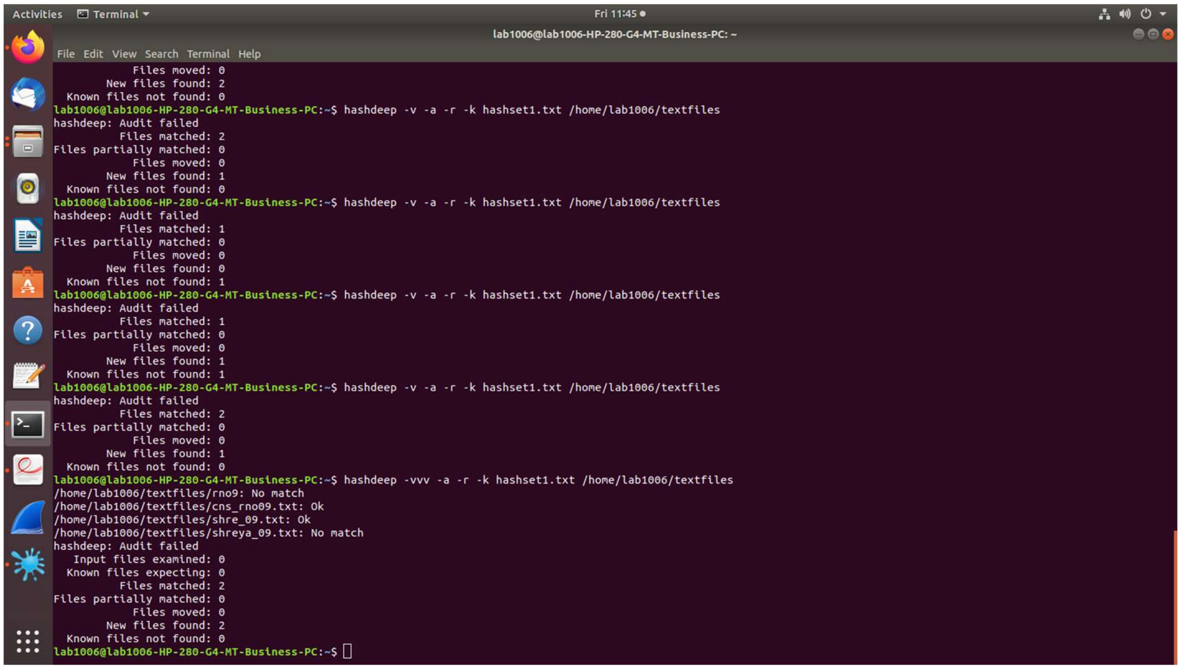
Roll No: 09
Name: Shreya Bagade
Date: 11/08/2023


Activities
Terminal
Fri 11:45
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
242,c4a26f32ae71881b213b06d4b2edb14b,716b59ac977985729e44473df2a8da82e6e41b12,/home/lab1006/rno9.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/rno
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
/home/lab1006/rno: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep *.txt>shreya.txt
/home/lab1006/cns_laksh.txt: Is a directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep *.txt>rno9.txt
/home/lab1006/cns_laksh.txt: Is a directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ cat rno9.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep cns_laksh.txt rno9.txt shreya.txt
##
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/rno9.txt
245,c22deb9ab53784b83465bb5554c03928,2f1e37bc8ad98e02430e3cbca5bae6639d2055911f4fd4df210e00826c747c63,/home/lab1006/shreya.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -m -k shreya.txt*
^C
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -m -k shreya.txt *
/home/lab1006/cns_laksh.txt: Is a directory
/home/lab1006/Desktop: Is a directory
/home/lab1006/Documents: Is a directory
/home/lab1006/Downloads: Is a directory
/home/lab1006/Music: Is a directory
/home/lab1006/Pictures: Is a directory
/home/lab1006/Public: Is a directory
/home/lab1006/pycharm-community-2019.3.3: Is a directory
/home/lab1006/PycharmProjects: Is a directory
/home/lab1006/t1_rno9: Is a directory
/home/lab1006/Templates: Is a directory
/home/lab1006/theHarvester: Is a directory
/home/lab1006/Videos: Is a directory
/home/lab1006/rno9
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -m  shreya.txt *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -m  shreya.txt *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -m -k  shreya.txt *
/home/lab1006/rno9
/home/lab1006/rno9.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -x  newfile.txt *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -x -k  newfile.txt *
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s -x -k  shreya.txt *
/home/lab1006/newfile.txt
/home/lab1006/shreya.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256 -r /home/lab1006/textfiles>hashset1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -a -r -k hashset1.txt /home/lab1006/textfiles
```


Activities
Terminal
Fri 11:45
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit passed
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit passed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 0
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 2
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 1
Files partially matched: 0
            Files moved: 0
```


Activities
Terminal
Fri 11:45
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
           Files moved: 0
       New files found: 2
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 1
Files partially matched: 0
            Files moved: 0
        New files found: 0
  Known files not found: 1
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 1
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 1
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -v -a -r -k hashset1.txt /home/lab1006/textfiles
hashdeep: Audit failed
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 1
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -vvv -a -r -k hashset1.txt /home/lab1006/textfiles
/home/lab1006/textfiles/rno9: No match
/home/lab1006/textfiles/cns_rno09.txt: Ok
/home/lab1006/textfiles/shre_09.txt: Ok
/home/lab1006/textfiles/shreya_09.txt: No match
hashdeep: Audit failed
   Input files examined: 0
  Known files expecting: 0
          Files matched: 2
Files partially matched: 0
            Files moved: 0
        New files found: 2
  Known files not found: 0
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ 
```

<u>Conclusion:</u> This experiment involved the exploration of the hashdeep tool in Kali Linux for generating, matching, and auditing file hashes has provided valuable insights into maintaining data integrity and security. Through this tool, we have gained the ability to generate hash values for files and directories, which act as unique fingerprints, ensuring the integrity of data throughout storage and transmission.