Name – Divya Shah
Roll No – 115

ASSIGNMENT NO – 5

Aim: Hashing n auditing using Hashdeep tool in Kali Linux

Lab Outcome:

LO3: Explore the different network reconnaissance tools to gather information about networks.

Theory:

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

Data Integrity: Hashing is used to ensure the integrity of data. When data is hashed, a fixed-length hash value is generated. If the data changes even slightly, the hash value will change significantly, making it easy to detect tampering.

Data Retrieval: Hashing is used in data structures like hash tables, which allow for efficient data retrieval. Hash functions convert data into an index in an array, making data lookup faster compared to linear search.

Password Storage: Hashing is crucial for securely storing passwords. Instead of storing actual passwords, systems store their hash values. This way, even if the database is compromised, attackers won't immediately gain access to the actual passwords.

Cryptographic Applications: Hashing is a foundational element in cryptography. It's used in various cryptographic algorithms and protocols for ensuring data integrity, creating digital signatures, and more.

Digital Signatures: Hashing is used to create digital signatures, ensuring the authenticity and integrity of digital documents.

Different hashing algorithms exist to serve different purposes. Here are some commonly used hashing algorithms:

1. MD5 (Message Digest Algorithm 5): A widely used hash function that produces a 128bit hash value. However, it is considered weak due to vulnerabilities that allow collision attacks.
2. SHA-1 (Secure Hash Algorithm 1): Initially designed for security, SHA-1 has become obsolete due to vulnerabilities. It produces a 160-bit hash value.
3. SHA-256 (Secure Hash Algorithm 256): A member of the SHA-2 family, it produces a 256-bit hash value. It is widely used for cryptographic applications and is considered secure.

4. SHA-3 (Secure Hash Algorithm 3): Part of the Keccak family, SHA-3 offers a different approach to hashing compared to SHA-2. It is designed to be resistant to certain types of attacks.
5. bcrypt: A password hashing function that uses a variant of the Blowfish encryption algorithm. It's designed to be slow and computationally intensive, making it difficult for attackers to perform brute-force attacks on passwords.
6. Argon2: A modern and memory-hard password hashing function designed to resist various attacks, including GPU and ASIC-based attacks. It won the Password Hashing Competition (PHC) in 2015.

Hashdeep is a command-line tool used for generating hash values, matching them with stored hash values, and auditing files for integrity. It is particularly useful for verifying data integrity, performing audits, and ensuring that files have not been tampered with. Here are some commands commonly used with the `hashdeep` tool:

1. Generate Hash Values:

To generate hash values for a single file:

```
hashdeep -c sha256 filename
```

To generate hash values for multiple files:

```
hashdeep -c sha256 file1 file2 file3
```

To generate hash values for all files in a directory:

```
hashdeep -r -c sha256 directory/ 2.
```

Match Hash Values:

To match hash values against a known hash value:

```
hashdeep -c sha256 -m known_hashes.txt
```

`known_hashes.txt` is a text file containing the known hash values and corresponding filenames.

3. Audit Files:

To audit files in a directory against hash values:

```
hashdeep -r -c sha256 -a -k known_hashes.txt directory/
```

This command will audit the files in the specified directory against the hash values in

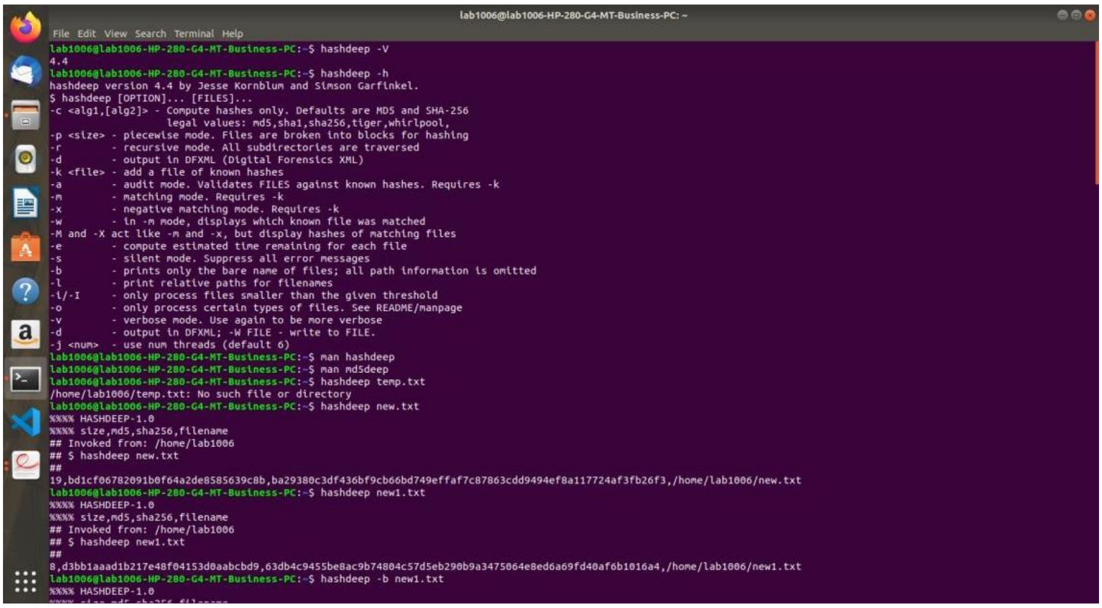
the `known_hashes.txt` file. 4. Generating Hash Values for Auditing:

To generate hash values and save them for later auditing:

```
hashdeep -r -c sha256 -k -l -o output_hashes.txt directory/
```

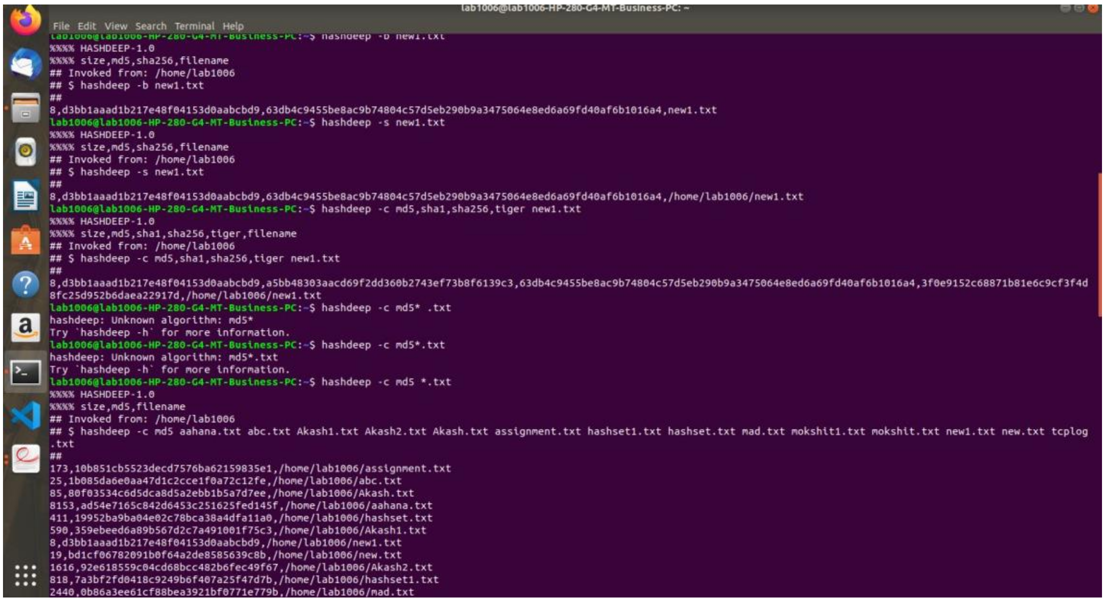
This command generates hash values for auditing purposes and saves them to the `output_hashes.txt` file.

Output:



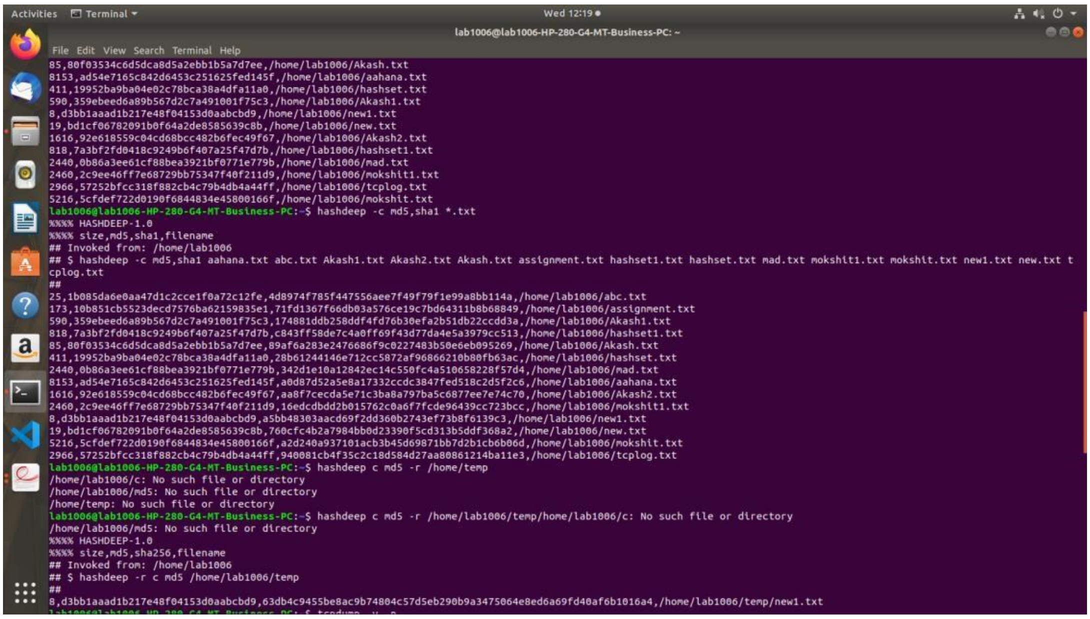
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
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 temp.txt
/home/lab1006/temp.txt: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep new.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep new.txt
##
19,bd1cf06782091b0f64a2de8585639c8b,ba29380c3df436bf9cb66bd749effaf7c87863cdd9494ef8a117724af3fb26f3,/home/lab1006/new.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep new1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep new1.txt
##
8,d3bb1aaad1b217e48f04153d0aabcbd9,63db4c9455be8ac9b74804c57d5eb290b9a3475064e8ed6a69fd40af6b1016a4,/home/lab1006/new1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -b new1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
```

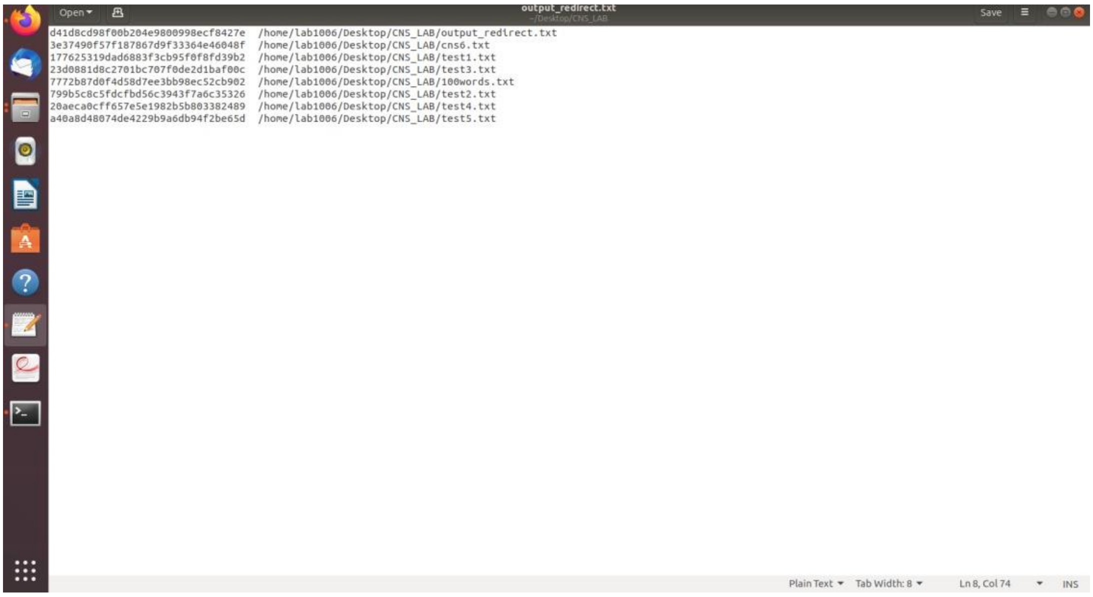


lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -b new1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -b new1.txt
##
8,d3bb1aaad1b217e48f04153d0aabcbd9,63db4c9455be8ac9b74804c57d5eb290b9a3475064e8ed6a69fd40af6b1016a4,new1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -s new1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: /home/lab1006
## $ hashdeep -s new1.txt
##
8,d3bb1aaad1b217e48f04153d0aabcbd9,63db4c9455be8ac9b74804c57d5eb290b9a3475064e8ed6a69fd40af6b1016a4,/home/lab1006/new1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1,sha256,tiger new1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1,sha256,tiger new1.txt
##
8,d3bb1aaad1b217e48f04153d0aabcbd9,a5bb48303aacd69f2dd360b2743ef73b8f6139c3,63db4c9455be8ac9b74804c57d5eb290b9a3475064e8ed6a69fd40af6b1016a4,3f0e9152c68871b81e6c9cf3f4d
8fc25d952b6daea22917d,/home/lab1006/new1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5* .txt
hashdeep: Unknown algorithm: md5*
Try `hashdeep -h` for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5*.txt
hashdeep: Unknown algorithm: md5*.txt
Try `hashdeep -h` for more information.
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5 aahana.txt abc.txt Akash1.txt Akash2.txt Akash.txt assignment.txt hashset1.txt hashset.txt mad.txt mokshit1.txt mokshit.txt new1.txt new.txt tcplog
.txt
##
173,10b851cb5523decd7576ba62159835e1,/home/lab1006/assignment.txt
25,1b085da6e0aa47d1c2cce1f0a72c12fe,/home/lab1006/abc.txt
85,80f03534c6d5dca8d5a2ebb1b5a7d7ee,/home/lab1006/Akash.txt
8153,ad54e7165c842d6453c251625fed145f,/home/lab1006/aahana.txt
411,19952ba9ba04e02c78bca38a4dfa11a0,/home/lab1006/hashset.txt
590,359ebeed6a89b567d2c7a491001f75c3,/home/lab1006/Akash1.txt
8,d3bb1aaad1b217e48f04153d0aabcbd9,/home/lab1006/new1.txt
19,bd1cf06782091b0f64a2de8585639c8b,/home/lab1006/new.txt
1616,92e618559c04cd68bcc482b6fec49f67,/home/lab1006/Akash2.txt
818,7a3bf2fd0418c9249b6f407a25f47d7b,/home/lab1006/hashset1.txt
2440,0b86a3ee61cf88bea3921bf0771e779b,/home/lab1006/mad.txt
```

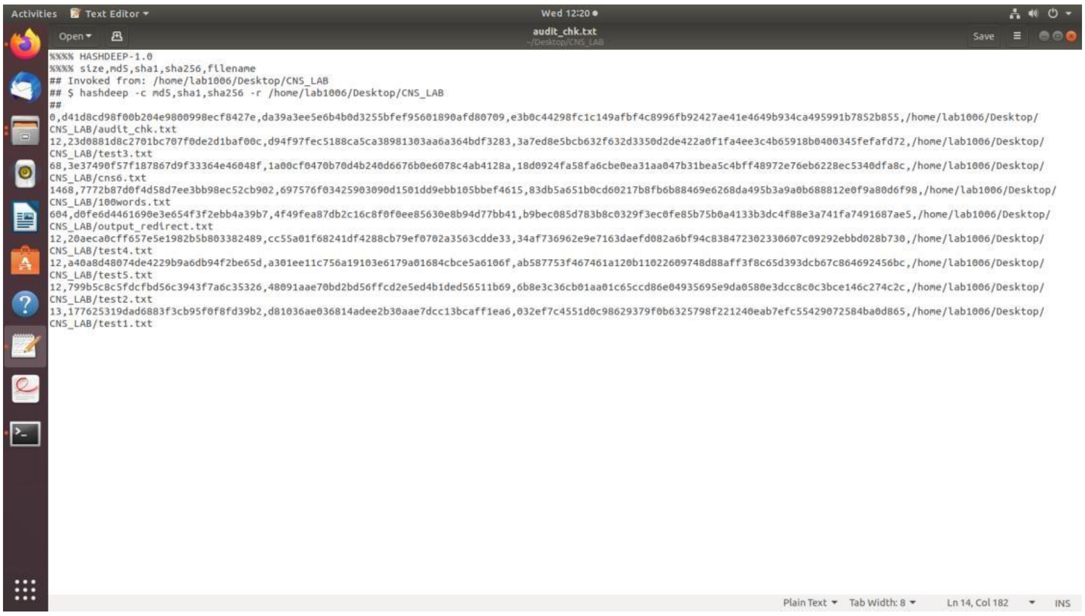

Activities
Terminal
Wed 12:19
lab1006@lab1006-HP-280-G4-MT-Business-PC: ~
File Edit View Search Terminal Help

```
85,80f03534c6d5dca8d5a2ebb1b5a7d7ee,/home/lab1006/Akash.txt
8153,ad54e7165c842d6453c251625fed145f,/home/lab1006/aahana.txt
411,19952ba9ba04e02c78bca38a4dfa11a0,/home/lab1006/hashset.txt
590,359ebeed6a89b567d2c7a491001f75c3,/home/lab1006/Akash1.txt
8,d3bb1aaad1b217e48f04153d0aabcbd9,/home/lab1006/new1.txt
19,bd1cf06782091b0f64a2de8585639c8b,/home/lab1006/new.txt
1616,92e618559c04cd68bcc482b6fec49f67,/home/lab1006/Akash2.txt
818,7a3bf2fd0418c9249b6f407a25f47d7b,/home/lab1006/hashset1.txt
2440,0b86a3ee61cf88bea3921bf0771e779b,/home/lab1006/mad.txt
2460,2c9ee46ff7e68729bb75347f40f211d9,/home/lab1006/mokshit1.txt
2966,57252bfcc318f882cb4c79b4db4a44ff,/home/lab1006/tcplog.txt
5216,5cfdef722d0190f6844834e45800166f,/home/lab1006/mokshit.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep -c md5,sha1 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: /home/lab1006
## $ hashdeep -c md5,sha1 aahana.txt abc.txt Akash1.txt Akash2.txt Akash.txt assignment.txt hashset1.txt hashset.txt mad.txt mokshit1.txt mokshit.txt new1.txt new.txt t
cplog.txt
##
25,1b085da6e0aa47d1c2cce1f0a72c12fe,4d8974f785f447556aee7f49f79f1e99a8bb114a,/home/lab1006/abc.txt
173,10b851cb5523decd7576ba62159835e1,71fd1367f66db03a576ce19c7bd64311b8b68849,/home/lab1006/assignment.txt
590,359ebeed6a89b567d2c7a491001f75c3,174881ddb258ddf4fd76b30efa2b51db22ccdd3a,/home/lab1006/Akash1.txt
818,7a3bf2fd0418c9249b6f407a25f47d7b,c843ff58de7c4a0ff69f43d77da4e5a3979cc513,/home/lab1006/hashset1.txt
85,80f03534c6d5dca8d5a2ebb1b5a7d7ee,89af6a283e2476686f9c0227483b50e6eb095269,/home/lab1006/Akash.txt
411,19952ba9ba04e02c78bca38a4dfa11a0,28b61244146e712cc5872af96866210b80fb63ac,/home/lab1006/hashset.txt
2440,0b86a3ee61cf88bea3921bf0771e779b,342d1e10a12842ec14c550fc4a510658228f57d4,/home/lab1006/mad.txt
8153,ad54e7165c842d6453c251625fed145f,a0d87d52a5e8a17332ccdc3847fed518c2d5f2c6,/home/lab1006/aahana.txt
1616,92e618559c04cd68bcc482b6fec49f67,aa8f7cecda5e71c3ba8a797ba5c6877ee7e74c70,/home/lab1006/Akash2.txt
2460,2c9ee46ff7e68729bb75347f40f211d9,16edcdbdd2b015762c0a6f7fcde96439cc723bcc,/home/lab1006/mokshit1.txt
8,d3bb1aaad1b217e48f04153d0aabcbd9,a5bb48303aacd69f2dd360b2743ef73b8f6139c3,/home/lab1006/new1.txt
19,bd1cf06782091b0f64a2de8585639c8b,760cfc4b2a7984bb0d23390f5cd313b5ddf368a2,/home/lab1006/new.txt
5216,5cfdef722d0190f6844834e45800166f,a2d240a937101acb3b45d69871bb7d2b1cb6b06d,/home/lab1006/mokshit.txt
2966,57252bfcc318f882cb4c79b4db4a44ff,940081cb4f35c2c18d584d27aa80861214ba11e3,/home/lab1006/tcplog.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/temp
/home/lab1006/c: No such file or directory
/home/lab1006/md5: No such file or directory
/home/temp: No such file or directory
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ hashdeep c md5 -r /home/lab1006/temp/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/temp
##
8,d3bb1aaad1b217e48f04153d0aabcbd9,63db4c9455be8ac9b74804c57d5eb290b9a3475064e8ed6a69fd40af6b1016a4,/home/lab1006/temp/new1.txt
lab1006@lab1006-HP-280-G4-MT-Business-PC:~$ tcpdump -v -n
```

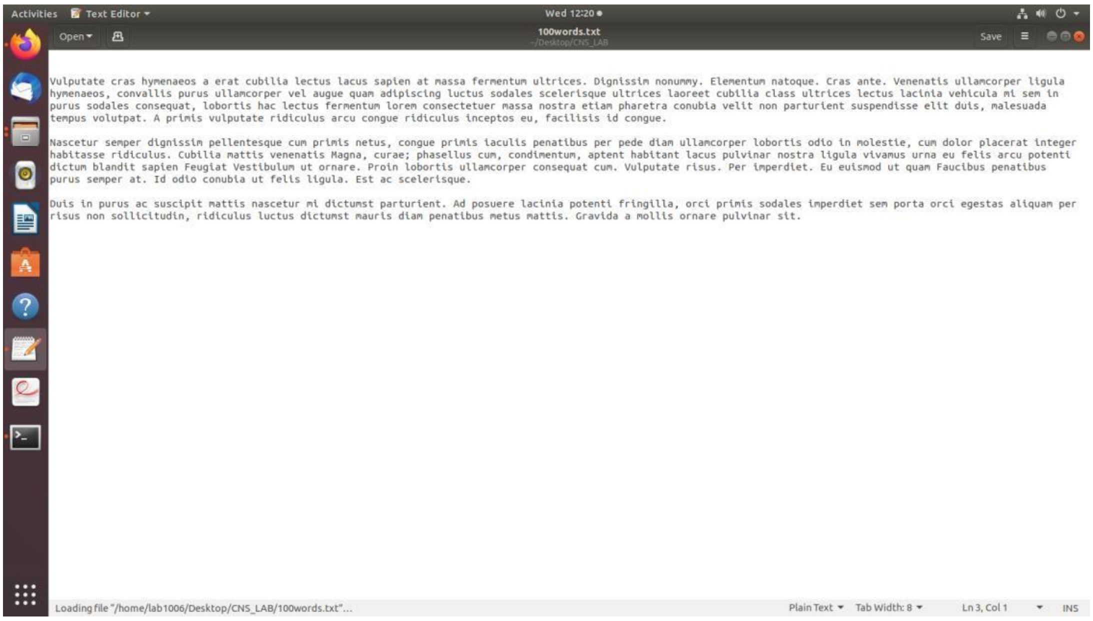


```
d41d8cd98f00b204e9800998ecf8427e  /home/lab1006/Desktop/CNS_LAB/output_redirect.txt
3e37490f57f187867d9f33364e46048f  /home/lab1006/Desktop/CNS_LAB/cns6.txt
177625319dad6883f3cb95f0f8fd39b2  /home/lab1006/Desktop/CNS_LAB/test1.txt
23d0881d8c2701bc707f0de2d1baf00c  /home/lab1006/Desktop/CNS_LAB/test3.txt
7772b87d0f4d58d7ee3bb98ec52cb902  /home/lab1006/Desktop/CNS_LAB/100words.txt
799b5c8c5fdcfbd56c3943f7a6c35326  /home/lab1006/Desktop/CNS_LAB/test2.txt
20aeca0cff657e5e1982b5b803382489  /home/lab1006/Desktop/CNS_LAB/test4.txt
a40a8d48074de4229b9a6db94f2be65d  /home/lab1006/Desktop/CNS_LAB/test5.txt
```

Name – Divya Shah
Roll No – 115

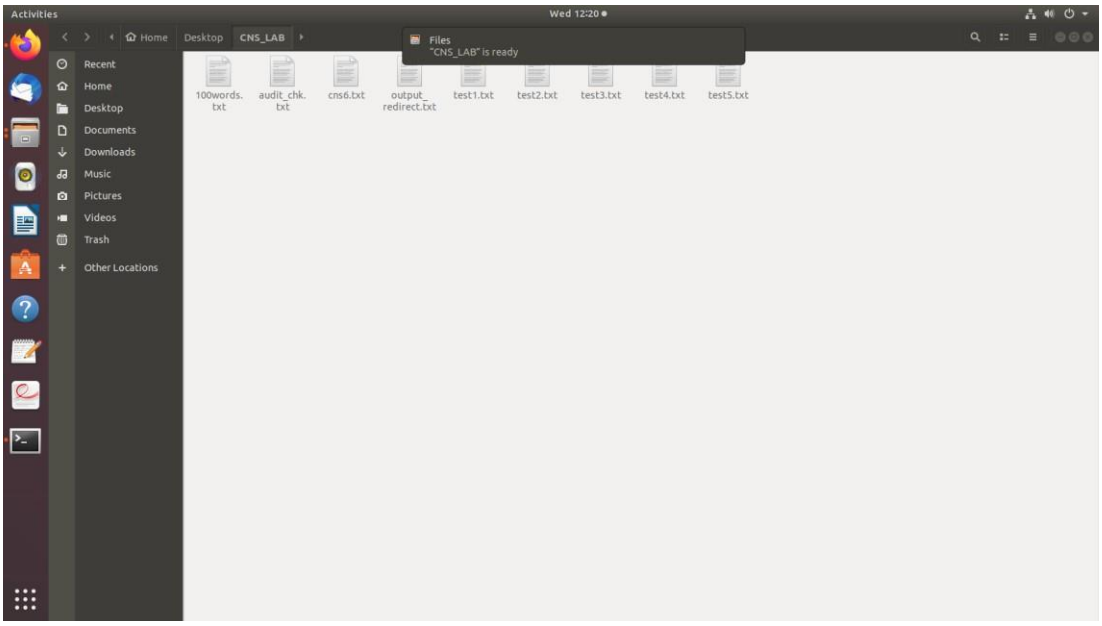


```
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,filename
## Invoked from: /home/lab1006/Desktop/CNS_LAB
## $ hashdeep -c md5,sha1,sha256 -r /home/lab1006/Desktop/CNS_LAB
##
0,d41d8cd98f00b204e9800998ecf8427e,da39a3ee5e6b4b0d3255bfef95601890afd80709,e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855,/home/lab1006/Desktop/
CNS_LAB/audit_chk.txt
12,23d0881d8c2701bc707f0de2d1baf00c,d94f97fec5188ca5ca38981303aa6a364bdf3283,3a7ed8e5bcb632f632d3350d2de422a0f1fa4ee3c4b65918b0400345fefafd72,/home/lab1006/Desktop/
CNS_LAB/test3.txt
68,3e37490f57f187867d9f33364e46048f,1a00cf0470b70d4b240d6676b0e6078c4ab4128a,18d0924fa58fa6cbe0ea31aa047b31bea5c4bff48972e76eb6228ec5340dfa8c,/home/lab1006/Desktop/
CNS_LAB/cns6.txt
1468,7772b87d0f4d58d7ee3bb98ec52cb902,697576f03425903090d1501dd9ebb105bbef4615,83db5a651b0cd60217b8fb6b88469e6268da495b3a9a0b688812e0f9a80d6f98,/home/lab1006/Desktop/
CNS_LAB/100words.txt
604,d0fe6d4461690e3e654f3f2ebb4a39b7,4f49fea87db2c16c8f0f0ee85630e8b94d77bb41,b9bec085d783b8c0329f3ec0fe85b75b0a4133b3dc4f88e3a741fa7491687ae5,/home/lab1006/Desktop/
CNS_LAB/output_redirect.txt
12,20aeca0cff657e5e1982b5b803382489,cc55a01f68241df4288cb79ef0702a3563cdde33,34af736962e9e7163daefd082a6bf94c838472302330607c09292ebbd028b730,/home/lab1006/Desktop/
CNS_LAB/test4.txt
12,a40a8d48074de4229b9a6db94f2be65d,a301ee11c756a19103e6179a01684cbce5a6106f,ab587753f467461a120b11022609748d88aff3f8c65d393dcb67c864692456bc,/home/lab1006/Desktop/
CNS_LAB/test5.txt
12,799b5c8c5fdcfbd56c3943f7a6c35326,48091aae70bd2bd56ffcd2e5ed4b1ded56511b69,6b8e3c36cb01aa01c65ccd86e04935695e9da0580e3dcc8c0c3bce146c274c2c,/home/lab1006/Desktop/
CNS_LAB/test2.txt
13,177625319dad6883f3cb95f0f8fd39b2,d81036ae036814adee2b30aae7dcc13bcaff1ea6,032ef7c4551d0c98629379f0b6325798f221240eab7efc55429072584ba0d865,/home/lab1006/Desktop/
CNS_LAB/test1.txt
```

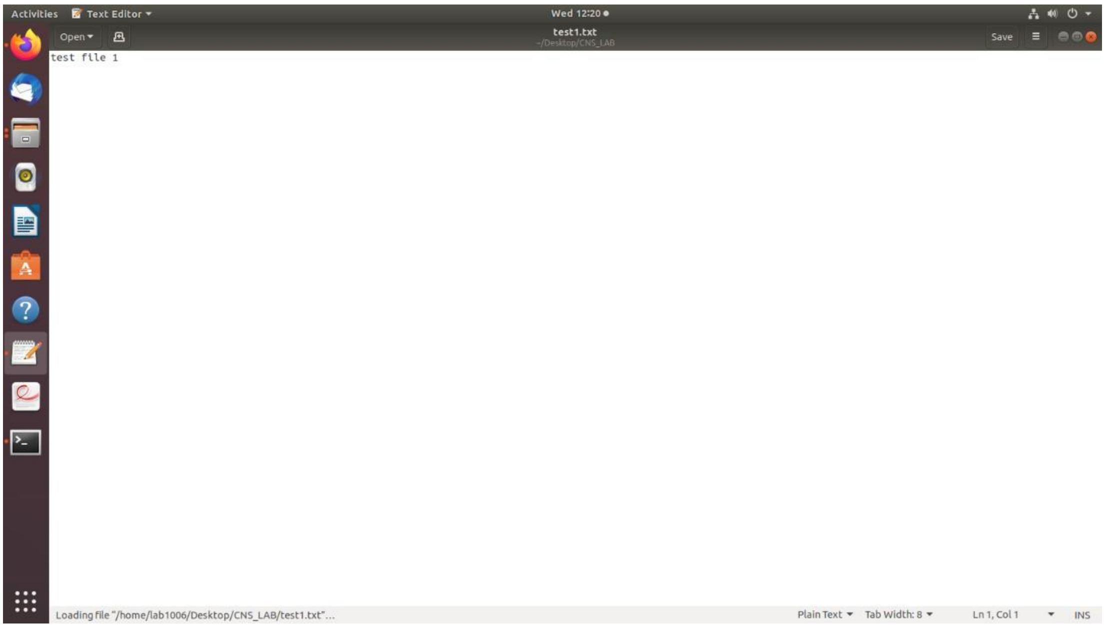


```
Vulputate cras hymenaeos a erat cubilia lectus lacus sapien at massa fermentum ultrices. Dignissim nonummy. Elementum natoque. Cras ante. Venenatis ullamcorper ligula
hymenaeos, convallis purus ullamcorper vel augue quam adipiscing luctus sodales scelerisque ultrices laoreet cubilia class ultrices lectus lacinia vehicula mi sem in
purus sodales consequat, lobortis hac lectus fermentum lorem consectetuer massa nostra etiam pharetra conubia velit non parturient suspendisse elit duis, malesuada
tempus volutpat. A primis vulputate ridiculus arcu congue ridiculus inceptos eu, facilisis id congue.

Nascetur semper dignissim pellentesque cum primis netus, congue primis iaculis penatibus per pede diam ullamcorper lobortis odio in molestie, cum dolor placerat integer
habitasse ridiculus. Cubilia mattis venenatis Magna, curae; phasellus cum, condimentum, aptent habitant lacus pulvinar nostra ligula vivamus urna eu felis arcu potenti
dictum blandit sapien Feugiat Vestibulum ut ornare. Proin lobortis ullamcorper consequat cum. Vulputate risus. Per imperdiet. Eu euismod ut quam Faucibus penatibus
purus semper at. Id odio conubia ut felis ligula. Est ac scelerisque.

Duis in purus ac suscipit mattis nascetur mi dictumst parturient. Ad posuere lacinia potenti fringilla, orci primis sodales imperdiet sem porta orci egestas aliquam per
risus non sollicitudin, ridiculus luctus dictumst mauris diam penatibus metus mattis. Gravida a mollis ornare pulvinar sit.
```

Loading file "/home/lab1006/Desktop/CNS_LAB/100words.txt"...



Files
"CNS_LAB" is ready



test1.txt
~/Desktop/CNS_LAB

```
test file 1
```

Loading file "/home/lab1006/Desktop/CNS_LAB/test1.txt"...

Conclusion:

In summary, leveraging hashing and auditing with the Hashdeep tool in Kali Linux is a powerful strategy for ensuring data integrity and security. Hashing safeguards against tampering by generating unique identifiers for files, while Hashdeep's auditing capabilities verify these identifiers and timestamps. Together, they offer a strong defense against unauthorized changes and provide essential tools for maintaining trustworthy data and bolstering cybersecurity measures.