Forensic Analysis Notes:

Case Information:

Case: Find the file with text “umkc436IsMyFavoriteClass” and provide the hash

Analyst: Julius Niyonzima

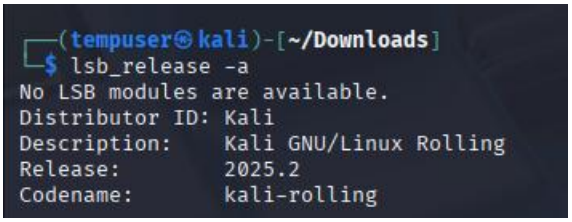
Professor: Dr. Chris Lamb

Email: jnbfg@umkc.edu

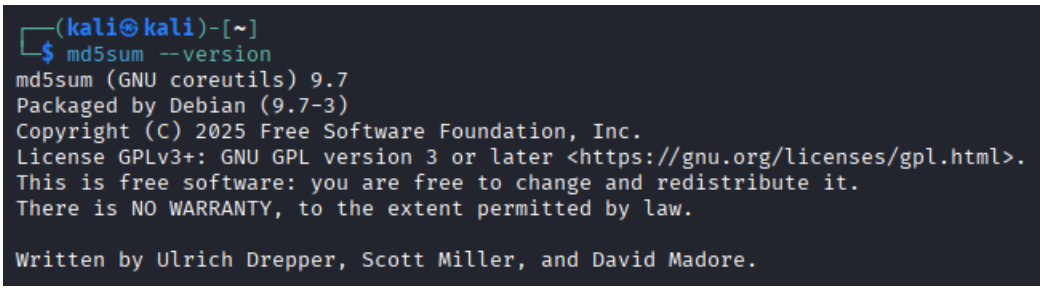
Id	Text	Hash(None)	Notes
1	umkc436IsMyFavoriteClass	Plain text	Suspected directory traversal

Tools and Environment

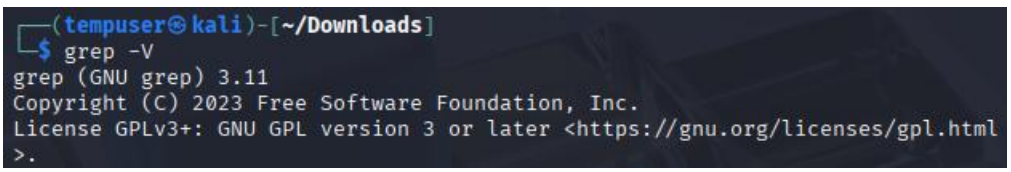
Kali Linux v2025.2



Md5sum v9.7 to hash the file



Grep v3.11 used as filter to search for a particular keyword



Locate v1.1.23 helps in searching for the word

```
┌──(kali㉿kali)-[~]
└─$ locate --version
plocate 1.1.23
Copyright 2020 Steinar H. Gunderson
License GPLv2+: GNU GPL version 2 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

Find v4.10.0 is used to search for utilities

```
┌──(kali㉿kali)-[~]
└─$ find -- version
find: ‘version’: No such file or directory

┌──(kali㉿kali)-[~]
└─$ find --version
find (GNU findutils) 4.10.0
Copyright (C) 2024 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Eric B. Decker, James Youngman, and Kevin Dalley.
Features enabled: D_TYPE O_NOFOLLOW(enabled) LEAF_OPTIMISATION FTS(FTS_CWDFD) CBO(level=1)
```

Analysis Steps :

Step 1: Verify if the file exists using the locate command

Command: locate umkc436IsMyFavoriteClass

```
┌──(kali㉿kali)-[~]
└─$ locate umkc436IsMyFavoriteClass
```

Result: Not found because locate is used to locate a file, not a text

Status: did not work

Step2: I used find to locate text within the home directory

Command : find /home -type f -name “umkc436IsMyFavoriteClass*.txt”

```
┌──(kali㉿kali)-[~]
└─$ find /home -type f -name "umkc436IsMyFavoriteClass*.txt"

┌──(kali㉿kali)-[~]
└─$
```

Result: Not a good example to find the text, because it is good at finding files, not text

Status: did not work

Step 3: used grep to search for a text with -r recursive to search for the text in the home directory and its subdirectories.

Command: grep -r “umkc436IsMyFavoriteClass” /home

Result: found the text in the these_are_not_the_droids_yer_looking_for.txt file

```
┌──(kali㉿kali)-[~]
└─$ grep  -r "umkc436IsMyFavoriteClass" /home
/home/kali/nested_test_data/so00o5ew/p11321to/w5xk7a1f/2fja8xce/jqij8rw3/edct8m75/f4fehn3v/aooalyby/zftjbqdp/these_are_not_the_droids_yer_looking_for.txt:um
kc436IsMyFavoriteClass
```

Status: Worked and found the text exists.

```
┌──(kali㉿kali)-[~]
└─$ sudo grep -r "umkc436IsMyFavoriteClass" /home

/home/kali/nested_test_data/so00o5ew/p11321to/w5xk7a1f/2fja8xce/jqij8rw3/edct8m75/f4fehn3v/aooalyby/zftjbqdp/these_are_not_the_droids_yer_looking_for.txt:um
kc436IsMyFavoriteClass
```

Step4: Used md5sum to hash the file

Command : md5sum these_are_not_droids_yer_looking_for.txt

Result: used md5sum to produce the hash of the filename

```
┌──(kali㉿kali)-[~]
└─$ md5sum /home/kali/nested_test_data/so00o5ew/p11321to/w5xk7a1f/2fja8xce/jqij8rw3/edct8m75/f4fehn3v/aooalyby/zftjbqdp/these_are_not_the_droids_yer_looking
_for.txt
d113d7e847fd04d53c58c1c41feec898  /home/kali/nested_test_data/so00o5ew/p11321to/w5xk7a1f/2fja8xce/jqij8rw3/edct8m75/f4fehn3v/aooalyby/zftjbqdp/these_are_not
_the_droids_yer_looking_for.txt
```

Status: worked, I was able to find the file and hash it. It produced the same hash when I copied to a different file and hashed the copied file

```
┌──(kali㉿kali)-[~/…/edct8m75/f4fehn3v/aooalyby/zftjbqdp]
└─$ ls
these_are_not_the_droids_yer_looking_for.txt

┌──(kali㉿kali)-[~/…/edct8m75/f4fehn3v/aooalyby/zftjbqdp]
└─$ md5sum these_are_not_the_droids_yer_looking_for.txt
d113d7e847fd04d53c58c1c41feec898  these_are_not_the_droids_yer_looking_for.txt
```

```
┌──(kali㉿kali)-[~]
└─$ md5sum androd.txt
d113d7e847fd04d53c58c1c41feec898  androd.txt

┌──(kali㉿kali)-[~]
└─$
```

Findings: The text was discovered in the filename located deep within the 10th subdirectory under the home directory. Standard commands such as locate and find were unable to identify the exact file, since they are more effective at searching for filenames rather than content. In contrast, grep proved to be more effective, successfully locating the file within the /zftjbqdp folder

Conclusion.

This demonstrates that **while locate** and **find** are valuable for indexing and navigating file paths, grep remains a more reliable tool when the objective is to uncover specific text strings within files or filenames, particularly in deeply nested directory structures.