Forensic Analysis Notes:

Case Information:

Case: Decode a text from assignment_hex.txt

Analyst: Julius Niyonzima

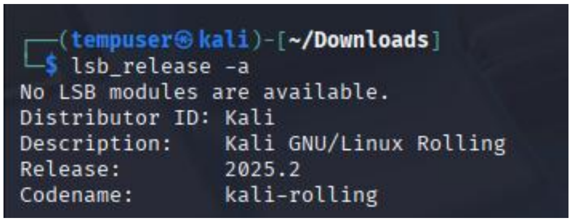
Professor: Dr. Chris Lamb

Email: jnbfg@umkc.edu

Id	File	Hash(None)	Notes
1	assignment_hex.txt	Contains ASCII text	Suspected obfuscation

Tools and Environment

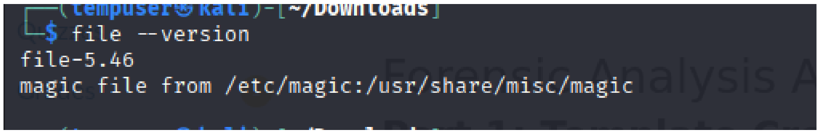
Kali Linux v2025.2



```
┌──(tempuser㉿kali)-[~/Downloads]
└─$ lsb_release -a
No LSB modules are available.
Distributor ID: Kali
Description:    Kali GNU/Linux Rolling
Release:        2025.2
Codename:       kali-rolling
```

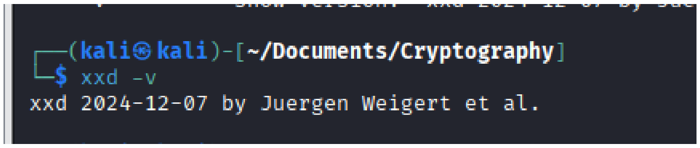
File to determine the type of file

File v5.46



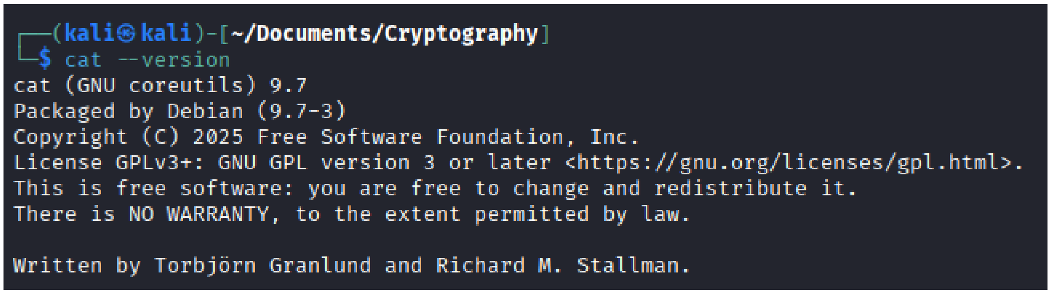
```
┌──(tempuser㉿kali)-[~/Downloads]
└─$ file --version
file-5.46
magic file from /etc/magic:/usr/share/misc/magic
```

xxd used to create an hex dump



```
    -v          show version: "xxd 2024-12-07 by Jue

┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ xxd -v
xxd 2024-12-07 by Juergen Weigert et al.
```

Cat v9.7 to read the text in the file



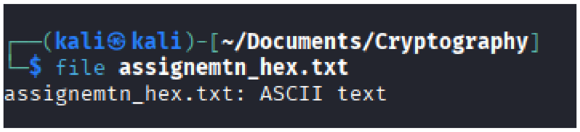
```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ cat --version
cat (GNU coreutils) 9.7
Packaged by Debian (9.7-3)
Copyright (C) 2025 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Torbjörn Granlund and Richard M. Stallman.
```

Analysis Steps :

Step1: Verified file type using the file command

Command: File assignment_hex.txt

Result: the file was confirmed to be ASCII text



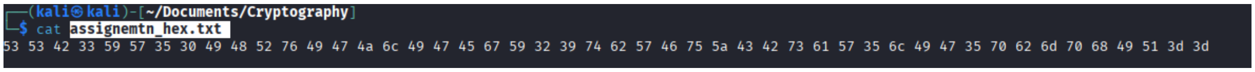
```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ file assignemtn_hex.txt
assignemtn_hex.txt: ASCII text
```

Status: Worked.

Step2: Read the file using cat

Command : cat assignemtn_hex.txt

Result: file is confirmed to contain hexadecimal data



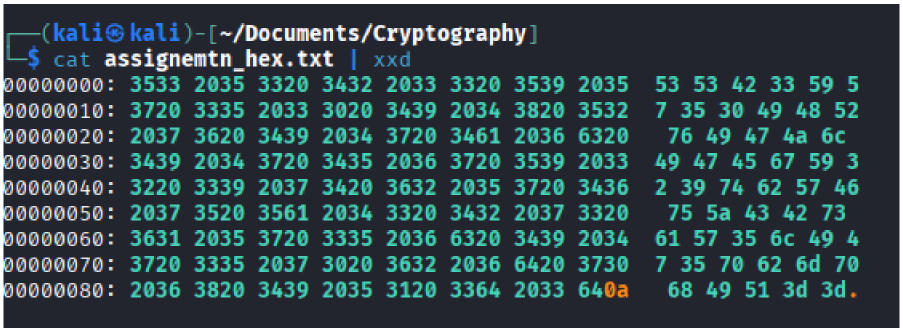
```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ cat assignemtn_hex.txt
53 53 42 33 59 57 35 30 49 48 52 76 49 47 4a 6c 49 47 45 67 59 32 39 74 62 57 46 75 5a 43 42 73 61 57 35 6c 49 47 35 70 62 6d 70 68 49 51 3d 3d
```

Status: it shows the data is hexadecimal

Step3: Convert the data into hex dump

Command : cat assignment_hex.txt | xxd

Result: Data is converted to hex dump



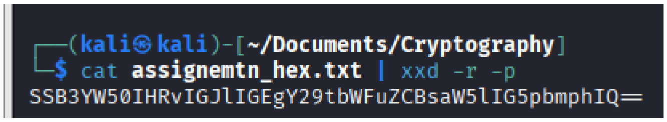
```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ cat assignemtn_hex.txt | xxd
00000000: 3533 2035 3320 3432 2033 3320 3539 2035  53 53 42 33 59 5
00000010: 3720 3335 2033 3020 3439 2034 3820 3532  7 35 30 49 48 52
00000020: 2037 3620 3439 2034 3720 3461 2036 6320   76 49 47 4a 6c
00000030: 3439 2034 3720 3435 2036 3720 3539 2033  49 47 45 67 59 3
00000040: 3220 3339 2037 3420 3632 2035 3720 3436  2 39 74 62 57 46
00000050: 2037 3520 3561 2034 3320 3432 2037 3320   75 5a 43 42 73
00000060: 3631 2035 3720 3335 2036 6320 3439 2034  61 57 35 6c 49 4
00000070: 3720 3335 2037 3020 3632 2036 6420 3730  7 35 70 62 6d 70
00000080: 2036 3820 3439 2035 3120 3364 2033 640a   68 49 51 3d 3d.
```

Status: works

Step 4: Converting the hex dump to readable text

Command: cat assignment_hex.txt | xxd -r -p

Result: It produced a Base64-formatted text.



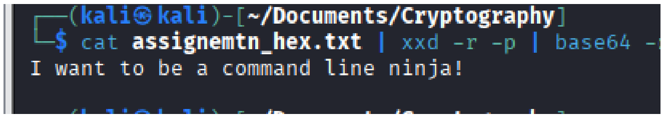
```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ cat assignemtn_hex.txt | xxd -r -p
SSB3YW50IHRvIGJlIGEgY29tbWFuZCBsaW5lIG5pbmphIQ==
```

Status: Did not produce the plain text

Step 5: Output the base64-formatted text into base64 command and decode it with -d

Command: cat assignment_hex.txt | xxd -r -p | base64 -d

Result: produced plain text



```
┌──(kali㉿kali)-[~/Documents/Cryptography]
└─$ cat assignemtn_hex.txt | xxd -r -p | base64 -
I want to be a command line ninja!
```

Status: Works

Findings:

The file assignment_hex.txt was analyzed using standard Kali Linux tools.

The file was read using cat, and it was found to be hex-encoded data.

Using xxd -r -p, the text was converted back to ASCII text, but was later found to be base-64.

Used base-64 -d to decode the text, and a text was revealed

Conclusion:

The assignemtn_hex.text was obfuscated with hexadecimal and base64 to conceal the text. Upon decoding, the text appeared to be a short message.