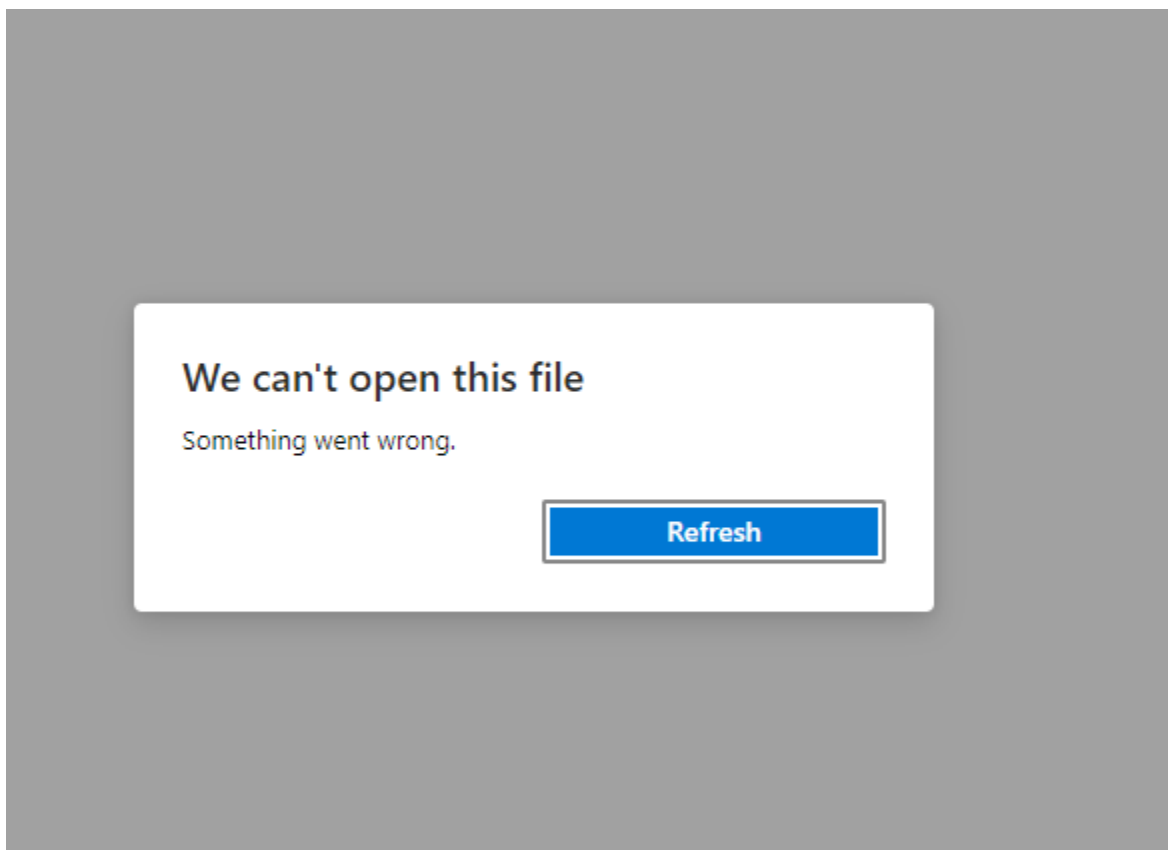


Homework #5 RE

Honor Pledge: I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

1.

This pdf, from just downloading it, cannot be opened. The following is the error that is given.



To find more information on the file, I can run 'file supersecret.pdf' in the terminal

```
(kali㉿kali)-[~/Downloads]
└─$ file supersecret.pdf
supersecret.pdf: ISO Media, MP4 Base Media v
1 [ISO 14496-12:2003]
```

This shows that the file is a ISO Media, MP4 Base file, so it is a video file

I discovered what the file actually is, but I told the file "Never going to give you up".

2.

The flag is “CMSC388u{You_Found_M3_IOL}”

I first downloaded the file from http://supersecure.store:7070/cmssc388u_midterm_answers

Then ran “strings cmssc388u_midterm_answers” in the terminal

```
(kali@kali)-[~/Downloads]
$ strings cmssc388u_midterm_answers
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
printf
__cxa_finalize
__libc_start_main
GLIBC_2.7
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
u+UH
[]A\A]A^A_
Press 1 for answer key, 2 for exam.
→CMSC388u{You_Found_M3_IOL}←
Press 3 for 1, 1 for 2, 5 to waste your time
:*3$
GCC: (Ubuntu 9.3.0-17ubuntu1~20.04) 9.3.0
crtstuff.c
deregister_tm_clones
__do_global_ctors_aux
completed.8060
```

The flag has been circled.

3.1

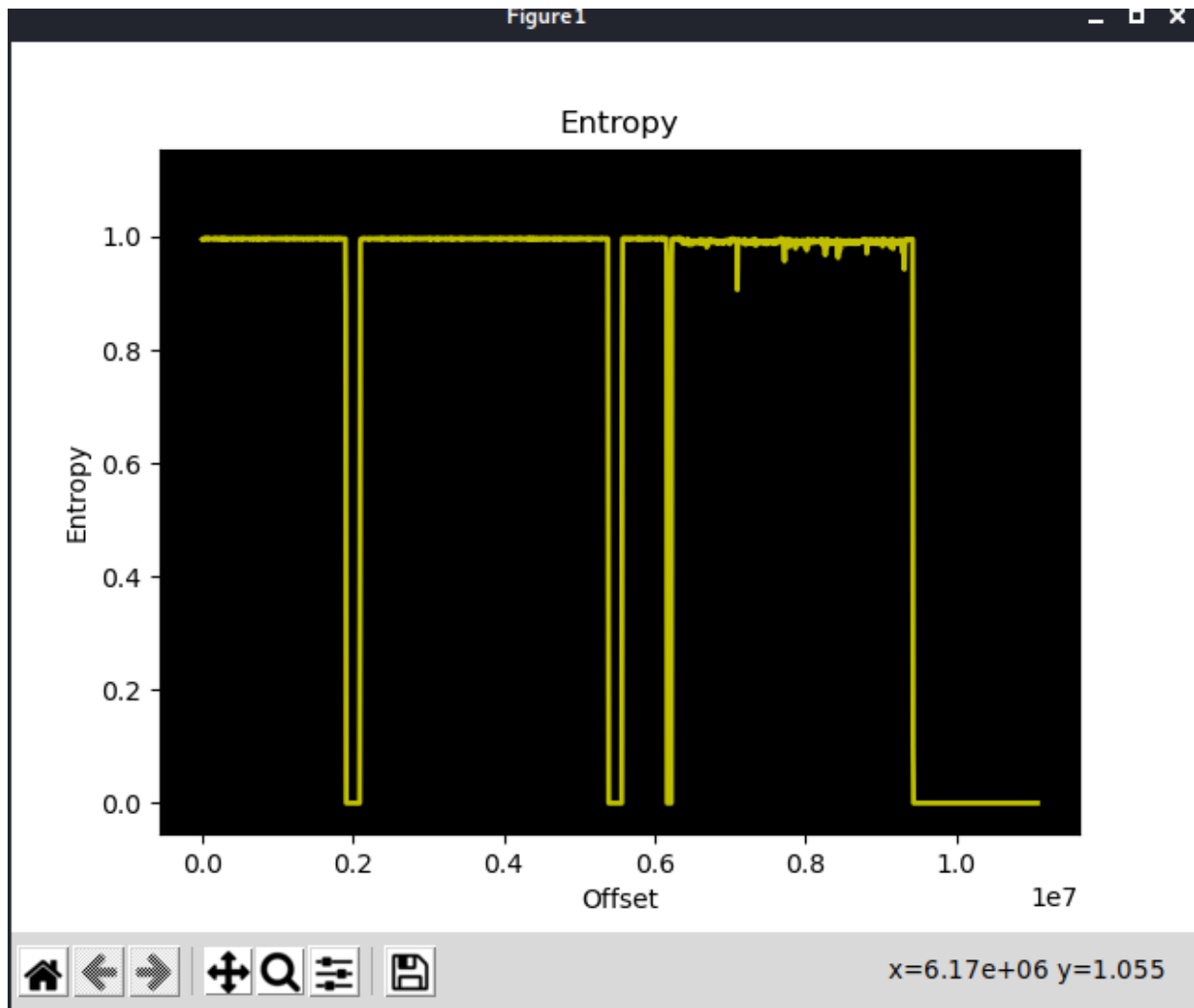
The output of the command ‘file mystery_firmware.bin’

```
(kali@kali)-[~/Downloads]
$ file mystery_firmware.bin
mystery_firmware.bin: u-boot legacy uImage, jz_fw, Linux/MIPS, Firmware Image (Not compressed),
11075584 bytes, Mon Nov 16 07:26:44 2020, Load Address: 0x00000000, Entry Point: 0x00000000, H
eader CRC: 0x0397CD15, Data CRC: 0xDB5930A7
```

As you can see, it appears that this file is some sort of Linux/MIPS Firmware Image ie you could run code on it and it may even be a mini OS???

3.2

Running ‘binwalk -E myster_firmware.bin’:



DECIMAL	HEXADECIMAL	ENTROPY
0	0x0	Rising entropy edge (0.995367)
1908736	0x1D2000	Falling entropy edge (0.000000)
2097152	0x200000	Rising entropy edge (0.991855)
5384192	0x522800	Falling entropy edge (0.585710)
5574656	0x551000	Rising entropy edge (0.996314)
6164480	0x5E1000	Falling entropy edge (0.000000)
6225920	0x5F0000	Rising entropy edge (0.955090)
7102464	0x6C6000	Rising entropy edge (0.992726)
9316352	0x8E2800	Rising entropy edge (0.982819)
9426944	0x8FD800	Falling entropy edge (0.099588)

The entropy file is the randomness of information associated with a file. It is often used to determine if a file is compressed or encrypted. Files that have these characteristics have a high entropy. [source](#)

3.3

Running 'binwalk myster_firmware.bin'

```
(kali@kali)-[~/Downloads]
$ binwalk myster_firmware.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes, header CRC: 0x397CD15, created: 2020-11-16 07:26:44, image size: 11075584 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xDB5930A7, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64	0x40	uImage header, header size: 64 bytes, header CRC: 0x6F5948F4, created: 2020-05-26 05:03:55, image size: 1907357 bytes, Data Address: 0x80010000, Entry Point: 0x80421870, data CRC: 0xD8FCDDFA, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux-3.10.14"
128	0x80	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: -1 bytes
2097216	0x200040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3289920 bytes, 414 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:39
5570624	0x550040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 593566 bytes, 13 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:40
6225984	0x5F0040	JFFS2 filesystem, little endian

This was hard to read, so I copied it and placed it into a text file

```
*Untitled - Notepad
File Edit Format View Help
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes, header CRC: 0x397CD15, created: 2020-11-16 07:26:44, image size: 11075584 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xDB5930A7, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64	0x40	uImage header, header size: 64 bytes, header CRC: 0x6F5948F4, created: 2020-05-26 05:03:55, image size: 1907357 bytes, Data Address: 0x80010000, Entry Point: 0x80421870, data CRC: 0xD8FCDDFA, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux-3.10.14"
128	0x80	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: -1 bytes
2097216	0x200040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3289920 bytes, 414 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:39
5570624	0x550040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 593566 bytes, 13 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:40
6225984	0x5F0040	JFFS2 filesystem, little endian

It appears that there are 6 files present inside of this file.

3.4.1

Ran the command 'binwalk --extract myster_firmware.bin'

```
(kali@kali) - [~/Downloads]
$ binwalk --extract mystery_firmware.bin
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes, header CRC: 0x397CD15, created: 2020-11-16 07:26:44, image size: 11075584 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xDB5930A7, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64	0x40	uImage header, header size: 64 bytes, header CRC: 0x6F5948F4, created: 2020-05-26 05:03:55, image size: 1907357 bytes, Data Address: 0x80010000, Entry Point: 0x80421870, data CRC: 0xD8FCDDFA, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux-3.10.14"
128	0x80	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: -1 bytes
2097216	0x200040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3289920 bytes, 414 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:39
5570624	0x550040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 593566 bytes, 13 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:40
WARNING: Extractor.execute failed to run external extractor 'jefferson -d 'jffs2-root' '%e': [Errno 2] No such file or directory: 'jefferson', 'jefferson -d 'jffs2-root' '%e' might not be installed correctly		
6225984	0x5F0040	JFFS2 filesystem, little endian

Cleaned up output:

```
*Untitled - Notepad
File Edit Format View Help
```

DECIMAL	HEXADECIMAL	DESCRIPTION
0	0x0	uImage header, header size: 64 bytes, header CRC: 0x397CD15, created: 2020-11-16 07:26:44, image size: 11075584 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0xDB5930A7, OS: Linux, CPU: MIPS, image type: Firmware Image, compression type: none, image name: "jz_fw"
64	0x40	uImage header, header size: 64 bytes, header CRC: 0x6F5948F4, created: 2020-05-26 05:03:55, image size: 1907357 bytes, Data Address: 0x80010000, Entry Point: 0x80421870, data CRC: 0xD8FCDDFA, OS: Linux, CPU: MIPS, image type: OS Kernel Image, compression type: lzma, image name: "Linux-3.10.14"
128	0x80	LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: -1 bytes
2097216	0x200040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 3289920 bytes, 414 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:39
5570624	0x550040	Squashfs filesystem, little endian, version 4.0, compression:xz, size: 593566 bytes, 13 inodes, blocksize: 131072 bytes, created: 2020-11-16 07:26:40
WARNING: Extractor.execute failed to run external extractor 'jefferson -d 'jffs2-root' '%e': [Errno 2] No such file or directory: 'jefferson', 'jefferson -d 'jffs2-root' '%e' might not be installed correctly		
6225984	0x5F0040	JFFS2 filesystem, little endian

After running this, i did 'ls' and it showed:

```
(kali@kali) - [~/Downloads]
$ ls
cmsc388u_midterm_answers  mystery_firmware.bin  supersecret.pdf
Image.lzma                _mystery_firmware.bin.extracted  uImage
```

I then cd into `_mystery_firmware.bin.extracted` and here are the contents

```
(kali㉿kali)-[~/Downloads]
$ cd _mystery_firmware.bin.extracted

(kali㉿kali)-[~/Downloads/_mystery_firmware.bin.extracted]
$ ls
200040.squashfs  550040.squashfs  5F0040.jffs2  80  80.7z  squashfs-root  squashfs-root-0
```

There is little of interest in 'squashfs-root-0'

```
(kali㉿kali)-[~/Downloads/_mystery_firmware.bin.extracted]
$ cd squashfs-root-0

(kali㉿kali)-[~/Downloads/_mystery_firmware.bin.extracted/squashfs-root-0]
$ ls
audio.ko      sample_motor.ko  sample_speakerctl.ko  sinfo.ko
exfat.ko      sample_pwm_core.ko  sensor_jxf22.ko      tx-isp.ko
rtl8189ftv.ko  sample_pwm_hal.ko  sensor_jxf23.ko      usb-akubelli.ko
```

However, in 'squashfs-root' we see that there appears to be something with a similar architecture to an OS.

```
(kali㉿kali)-[~/Downloads/_mystery_firmware.bin.extracted/squashfs-root-0]
$ cd ../squashfs-root

(kali㉿kali)-[~/Downloads/_mystery_firmware.bin.extracted/squashfs-root]
$ ls
backupa  backupk  configs  driver  lib      media  opt    proc  run  sys  thirdlib  usr
backupd  bin      dev      etc     linuxrc  mnt    params  root  sbin  system  tmp      var
```

Therefore, the root file system is located at `_myster_firmware.bin.extracted/squashfs-root`

3.4.2

First, I run `'cd /usr/bin/etc/'`. Then I run `'cat passwd'` with the points of interest being the lines

```
root:x:0:0:root:/root:/usr/bin/zsh
kali:x:1000:1000:Kali,,,:/home/kali:/usr/bin/zsh
```

and `'sudo cat shadow'` with the points of interest being the lines

```
root!!:18583:0:99999:7:::
```

```
kali:$6$jmPOPFIq42CdprqE$E0Yan4GtRMjGWULws2eGsjkdo2igDmFI4Bmg2T9c8gOFiVkyO/eE.0ztZX8mjAb6aJO1wmShGxePBJNfzyUTH.:18583:0:99999:7:::
```

The password hasf for the device was located at the path
_myster_firmware.bin.extracted/squashfs-root/etc/shadow.

The password hash is:

\$6\$jmPOPFIq42CdprqE\$E0Yan4GtRMjGWULws2eGsjkdo2igDmFI4Bmg2T9c8gOFiVkyO/eE.0ztZX8mjAb6aJO1wmShGxePBJNfzyUTH.