Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52

[1]Submit your document as firstname_ INFO 37721.Assignment3

Change the footer of the document as your name and student ID.

Introduction to the Assignment

You are asked to execute three tasks and reflect on questions.

Task 1: Calculation and comparing hashes of the files.

Task 2: To detect NTFS stream data

Task 3: To display contents in Steganography

Pre-requisites of the assignment

The pre-requisites (recommended system requirement) for this assignment are:

- VMware Fusion or Workstation (It must be registered; trials will not work)
- Windows 10 Virtual Machine
- Resources(files) provided in Slate

Task 1: Calculation and comparing hashes of the files [26 Marks]

A txt file is very simple and doesn't contain any header detail aside from the content of the text file. However, most files have a lot more information and details baked in.

a) **[3 Marks]** In your resources for this assignment, you will find two rich text format files- file1.rtf and file3.rtf. The file has a lot more features than a simple txt file and since that's the case, more information is contained within it. **List the three differences between .txt and .rtf file.**

The 3 differences between .txt and .rtf file is Hex Signature, Images like png and jpg can be embedded(Saved in)(ref https://www.quora.com/What-is-the-difference-between-TXT-and-RTF-files) in .rtf file compared to .txt, Font information(Calibri) is provided in .rtf files compared to .txt files.

b) **[3 Marks]** Open file1.rtf in WinHex and answer the following questions:

Assignment 3: Working with Windows, CLI Systems and Steganography

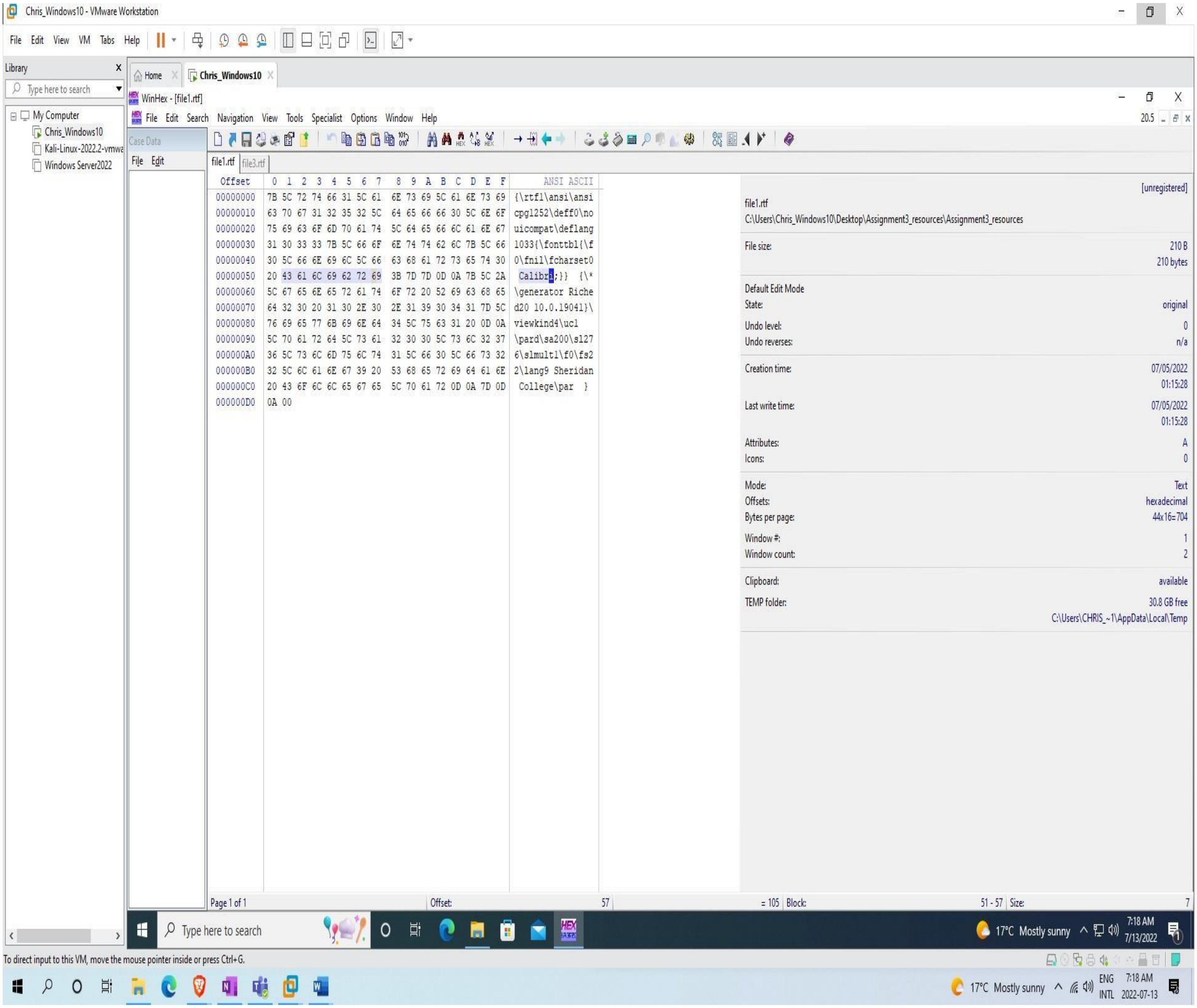
Total Marks: 52

i. Mention the font of the content. ______**Calibri**___________________ ii. What's the hex value of captured font. _____**43 61 6C 69 62 72 69**____________________ iii. Attach the screenshot highlighting the font captured.

[1]

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52



```
 Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010  63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020  75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030  31 30 33 33 7B 5C 66 6F  6E 74 74 62 6C 7B 5C 66  1033{\fonttbl{\f
00000040  30 5C 66 6E 69 6C 5C 66  63 68 61 72 73 65 74 30  0\fnil\fcharset0
00000050  20 43 61 6C 69 62 72 69  3B 7D 7D 0D 0A 7B 5C 2A   Calibri;}}  {\*
00000060  5C 67 65 6E 65 72 61 74  6F 72 20 52 69 63 68 65  \generator Riche
00000070  64 32 30 20 31 30 2E 30  2E 31 39 30 34 31 7D 5C  d20 10.0.19041}\
00000080  76 69 65 77 6B 69 6E 64  34 5C 75 63 31 20 0D 0A  viewkind4\uc1
00000090  5C 70 61 72 64 5C 73 61  32 30 30 5C 73 6C 32 37  \pard\sa200\sl27
000000A0  36 5C 73 6C 6D 75 6C 74  31 5C 66 30 5C 66 73 32  6\slmult1\f0\fs2
000000B0  32 5C 6C 61 6E 67 39 20  53 68 65 72 69 64 61 6E  2\lang9 Sheridan
000000C0  20 43 6F 6C 6C 65 67 65  5C 70 61 72 0D 0A 7D 0D   College\par  }
000000D0  0A 00
```

[unregistered]

file1.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size: 210 B
210 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 07/05/2022 01:15:28

Last write time: 07/05/2022 01:15:28

Attributes: A
Icons: 0

Mode: Text
Offsets: hexadecimal
Bytes per page: 44x16=704

Window #: 1
Window count: 2

Clipboard: available

TEMP folder: 30.8 GB free
C:\Users\CHRIS_~1\AppData\Local\Temp

Page 1 of 1 | Offset: 57 | = 105 | Block: 51 - 57 | Size: 7

Assignment 3: Working with Windows, CLI Systems and Steganography

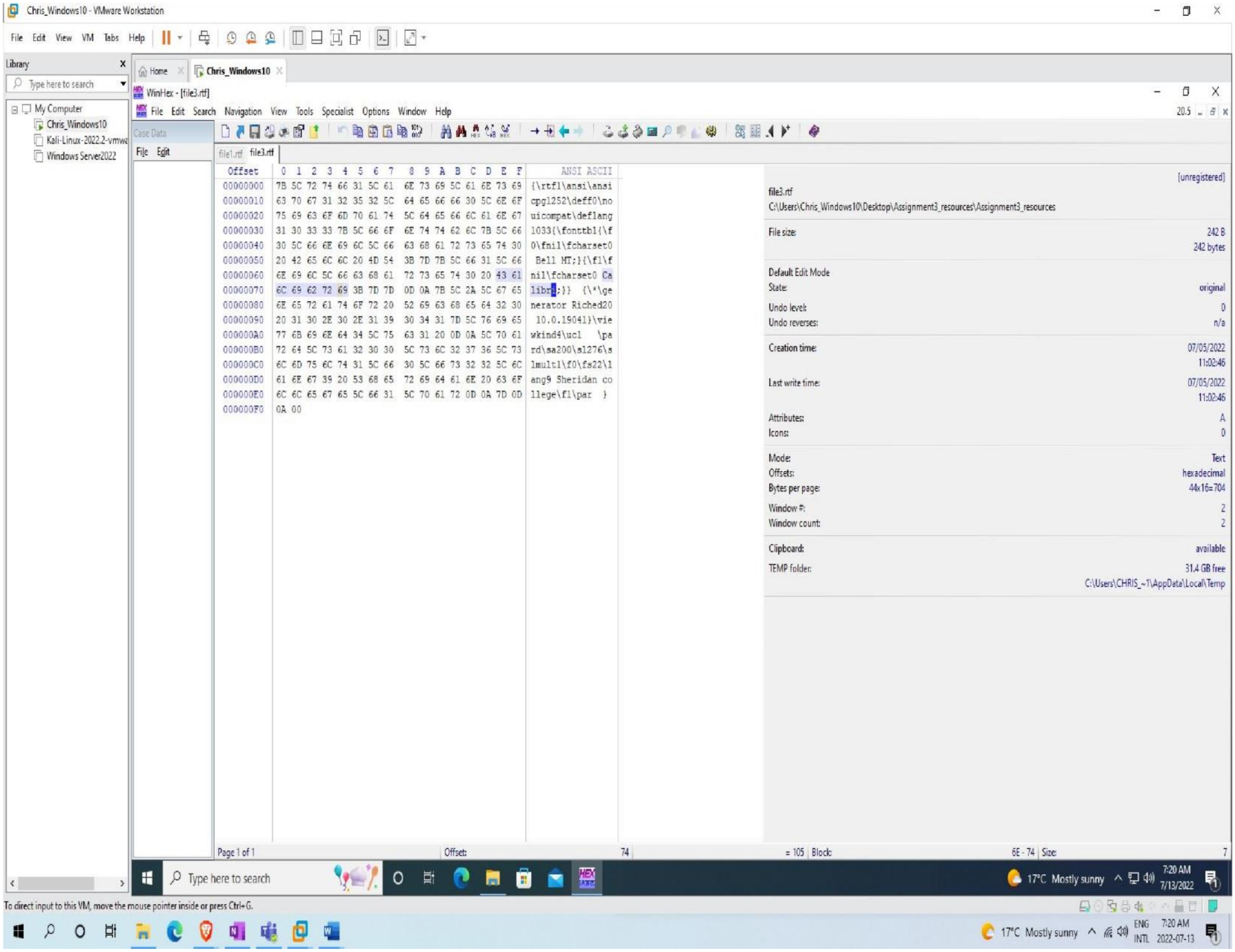
Total Marks: 52

c) **[3 Marks]** Open file3.rtf in WinHex and answer the following questions:

i. Mention the font of the content. _____**Calibri**____________________

ii. What's the hex value of captured font. __**43 61 6C 69 62 72 69** ______________________

iii. Attach the screenshot highlighting the font captured.



WinHex - [file3.rtf]

```
Offset     0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010  63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020  75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030  31 30 33 33 7B 5C 66 6F  6E 74 74 62 6C 7B 5C 66  1033{\fonttbl{\f
00000040  30 5C 66 6E 69 6C 5C 66  63 68 61 72 73 65 74 30  0\fnil\fcharset0
00000050  20 42 65 6C 6C 20 4D 54  3B 7D 7B 5C 66 31 5C 66   Bell MT;}{\f1\f
00000060  6E 69 6C 5C 66 63 68 61  72 73 65 74 30 20 43 61  nil\fcharset0 Ca
00000070  6C 69 62 72 69 3B 7D 7D  0D 0A 7B 5C 2A 5C 67 65  libri;}}  {\*\ge
00000080  6E 65 72 61 74 6F 72 20  52 69 63 68 65 64 32 30  nerator Riched20
00000090  20 31 30 2E 30 2E 31 39  30 34 31 7D 5C 76 69 65   10.0.19041}\vie
000000A0  77 6B 69 6E 64 34 5C 75  63 31 20 0D 0A 5C 70 61  wkind4\uc1  \pa
000000B0  72 64 5C 73 61 32 30 30  5C 73 6C 32 37 36 5C 73  rd\sa200\sl276\s
000000C0  6C 6D 75 6C 74 31 5C 66  30 5C 66 73 32 32 5C 6C  lmult1\f0\fs22\l
000000D0  61 6E 67 39 20 53 68 65  72 69 64 61 6E 20 63 6F  ang9 Sheridan co
000000E0  6C 6C 65 67 65 5C 66 31  5C 70 61 72 0D 0A 7D 0D  llege\f1\par  }
000000F0  0A 00
```

[unregistered]

file3.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size:	242 B 242 bytes
Default Edit Mode	
State:	original
Undo level:	0
Undo reverses:	n/a
Creation time:	07/05/2022 11:02:46
Last write time:	07/05/2022 11:02:46
Attributes:	A
Icons:	0
Mode:	Text
Offsets:	hexadecimal
Bytes per page:	44x16=704
Window #:	2
Window count:	2
Clipboard:	available
TEMP folder:	31.4 GB free C:\Users\CHRIS_~1\AppData\Local\Temp

Page 1 of 1 | Offset: 74 | = 105 | Block: 6E - 74 | Size: 7

d) **[1 Mark]** Open the two files- file1.rtf and file3.rtf in WordPad. What are the contents of both files? ________________**SC**___________________________

e) **[1 Mark]** Compute the MD5 hash values of both the files. Both the files appear to be copies of each other. Do the hash values match? ___**No the hash values don't match**_________________

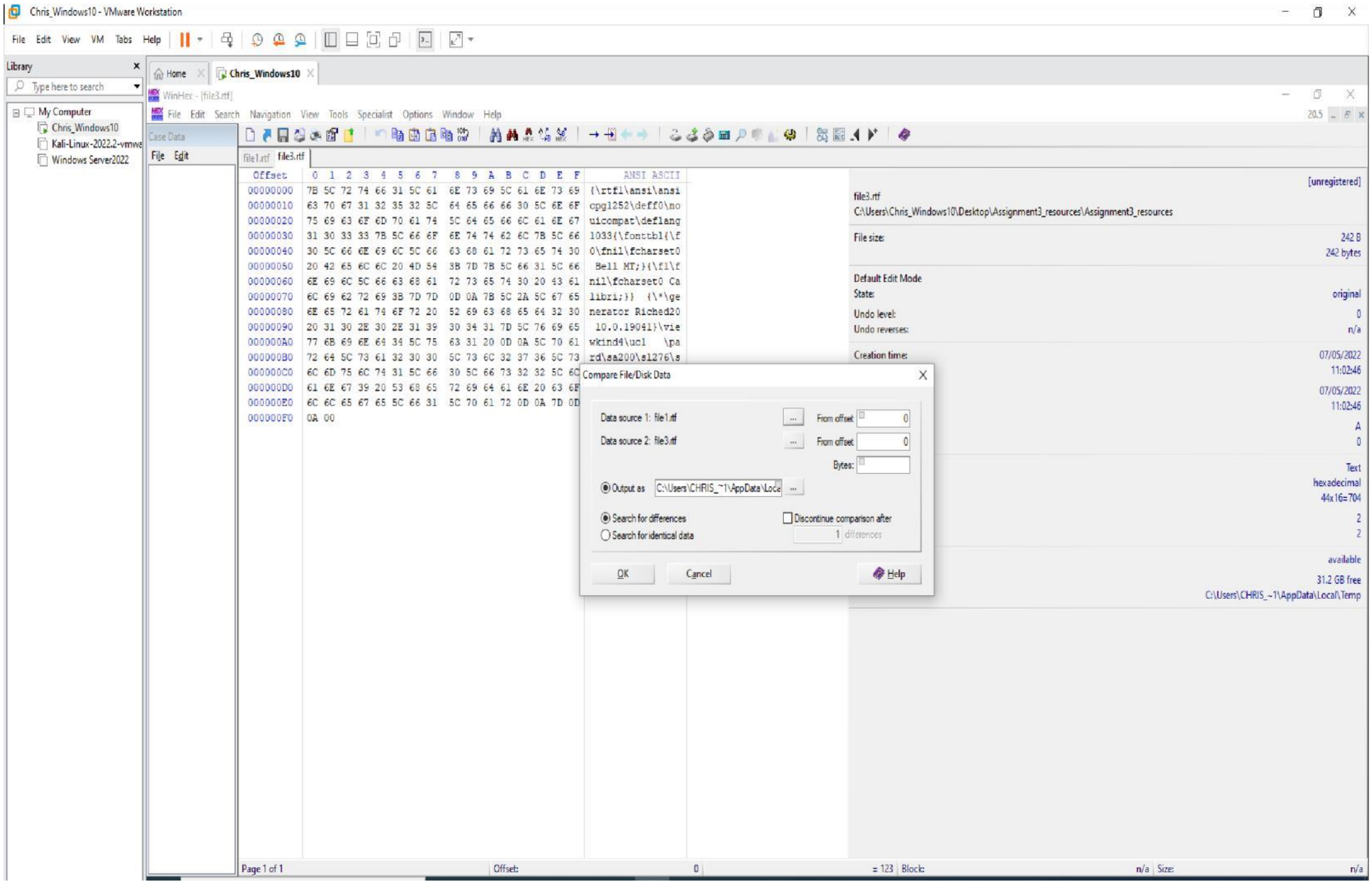
f) **[2 Marks]** are MD5 hashes of both files? **file1.rtf: ea5e0baf344e4ded369b4ce708d809e3 file3:rtf: 6de2e15ddd5df04dea743f651ddee635**

g) **[2 Marks]** Why or Why don't the hashes match?
The hashes don't match because file 1 and file 3 contents in ANSI ASCII are different in winhex. This means that if you have 2 separate files that are modified differently you will have different hash values.

h) **[2 Marks]** Use WinHex to look a bit deeper into these two files. Use the Tools/Compare data feature in WinHex to determine what's going on with these two files. Let your data source1 be file1.rtf and data source2 be file3.rtf. Save the output results as firstname_differences.txt in some folder. **Attach the screenshot of this activity.**

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52



Chris_Windows10 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
Chris_Windows10
Kali-Linux-2022.2-vmwa
Windows Server2022
Home
Chris_Windows10
WinHex - [file3.rtf]
File Edit Search Navigation View Tools Specialist Options Window Help
file1.rtf file3.rtf

```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000 7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010 63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020 75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030 31 30 33 33 7B 5C 66 6F  6E 74 74 62 6C 7B 5C 66  1033{\fonttbl{\f
00000040 30 5C 66 6E 69 6C 5C 66  63 68 61 72 73 65 74 30  0\fnil\fcharset0
00000050 20 42 65 6C 6C 20 4D 54  3B 7D 7B 5C 66 31 5C 66   Bell MT;}{\f1\f
00000060 6E 69 6C 5C 66 63 68 61  72 73 65 74 30 20 43 61  nil\fcharset0 Ca
00000070 6C 69 62 72 69 3B 7D 7D  0D 0A 7B 5C 2A 5C 67 65  libri;}}  {\*\ge
00000080 6E 65 72 61 74 6F 72 20  52 69 63 68 65 64 32 30  nerator Riched20
00000090 20 31 30 2E 30 2E 31 39  30 34 31 7D 5C 76 69 65   10.0.19041}\vie
000000A0 77 6B 69 6E 64 34 5C 75  63 31 20 0D 0A 5C 70 61  wkind4\uc1   \pa
000000B0 72 64 5C 73 61 32 30 30  5C 73 6C 32 37 36 5C 73  rd\sa200\sl276\s
000000C0 6C 6D 75 6C 74 31 5C 66  30 5C 66 73 32 32 5C 6C
000000D0 61 6E 67 39 20 53 68 65  72 69 64 61 6E 20 63 6F
000000E0 6C 6C 65 67 65 5C 66 31  5C 70 61 72 0D 0A 7D 0D
000000F0 0A 00
```

[unregistered]

file3.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size: 242 B
242 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 07/05/2022
11:02:46

07/05/2022
11:02:46

A
0

Text
hexadecimal
44x16=704

2
2

available

31.2 GB free
C:\Users\CHRIS_~1\AppData\Local\Temp

Compare File/Disk Data

Data source 1: file1.rtf ... From offset 0

Data source 2: file3.rtf ... From offset 0

Bytes:

● Output as C:\Users\CHRIS_~1\AppData\Loca ...

● Search for differences

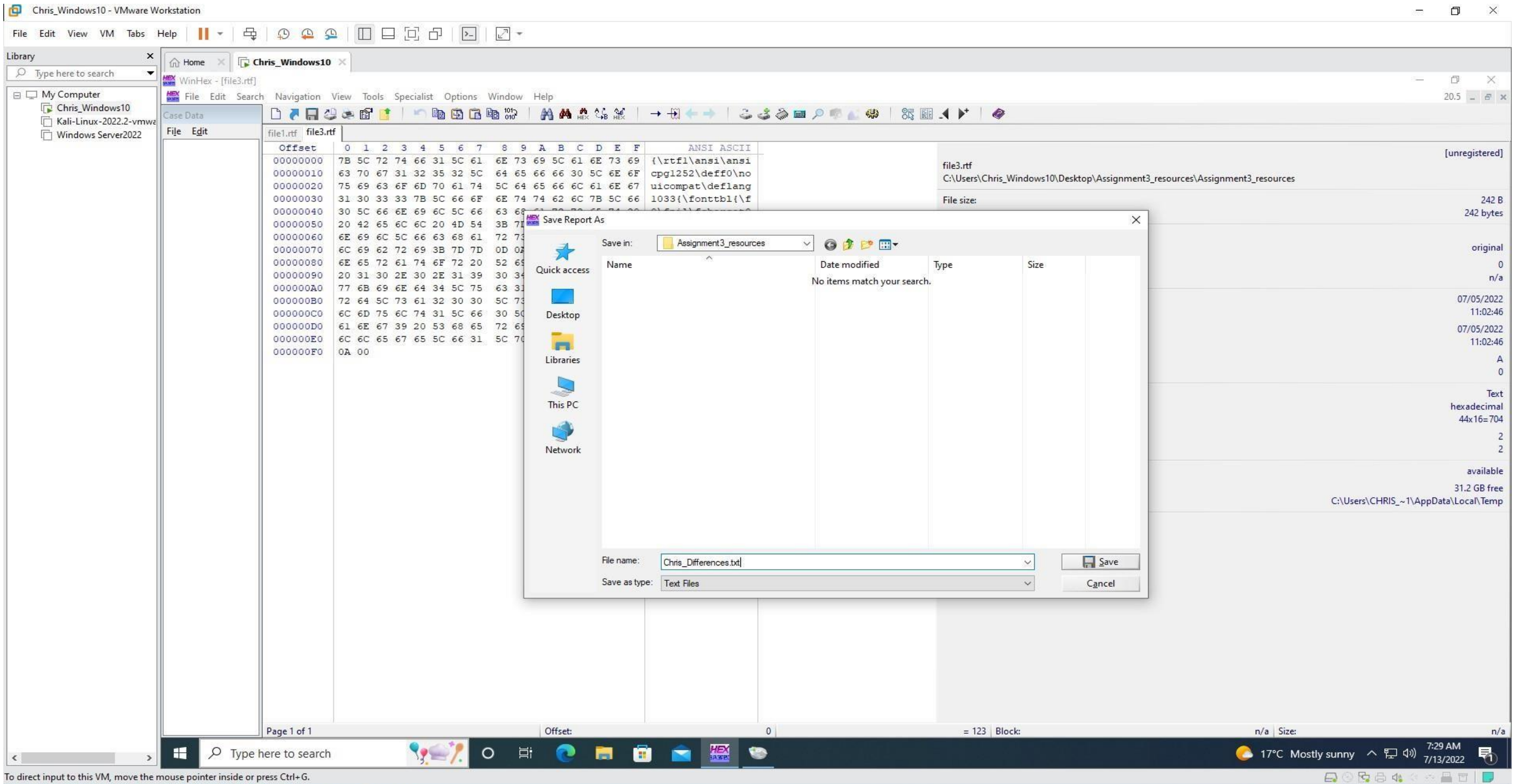
○ Search for identical data

□ Discontinue comparison after 1 differences

Page 1 of 1 Offset: 0 = 123 Block: n/a Size: n/a

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52



```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010  63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020  75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030  31 30 33 33 7B 5C 66 6F  6E 74 74 62 6C 7B 5C 66  1033{\fonttbl{\f
00000040  30 5C 66 6E 69 6C 5C 66  63 68
00000050  20 42 65 6C 6C 20 4D 54  3B 7D
00000060  6E 69 6C 5C 66 63 68 61  72 73
00000070  6C 69 62 72 69 3B 7D 7D  0D 0A
00000080  6E 65 72 61 74 6F 72 20  52 69
00000090  20 31 30 2E 30 2E 31 39  30 34
000000A0  77 6B 69 6E 64 34 5C 75  63 31
000000B0  72 64 5C 73 61 32 30 30  5C 73
000000C0  6C 6D 75 6C 74 31 5C 66  30 5C
000000D0  61 6E 67 39 20 53 68 65  72 69
000000E0  6C 6C 65 67 65 5C 66 31  5C 70
000000F0  0A 00
```

Save Report As

Save in: Assignment3_resources

Name	Date modified	Type	Size
	No items match your search.		

File name: Chris_Differences.txt

Save as type: Text Files

Save | Cancel

[unregistered]

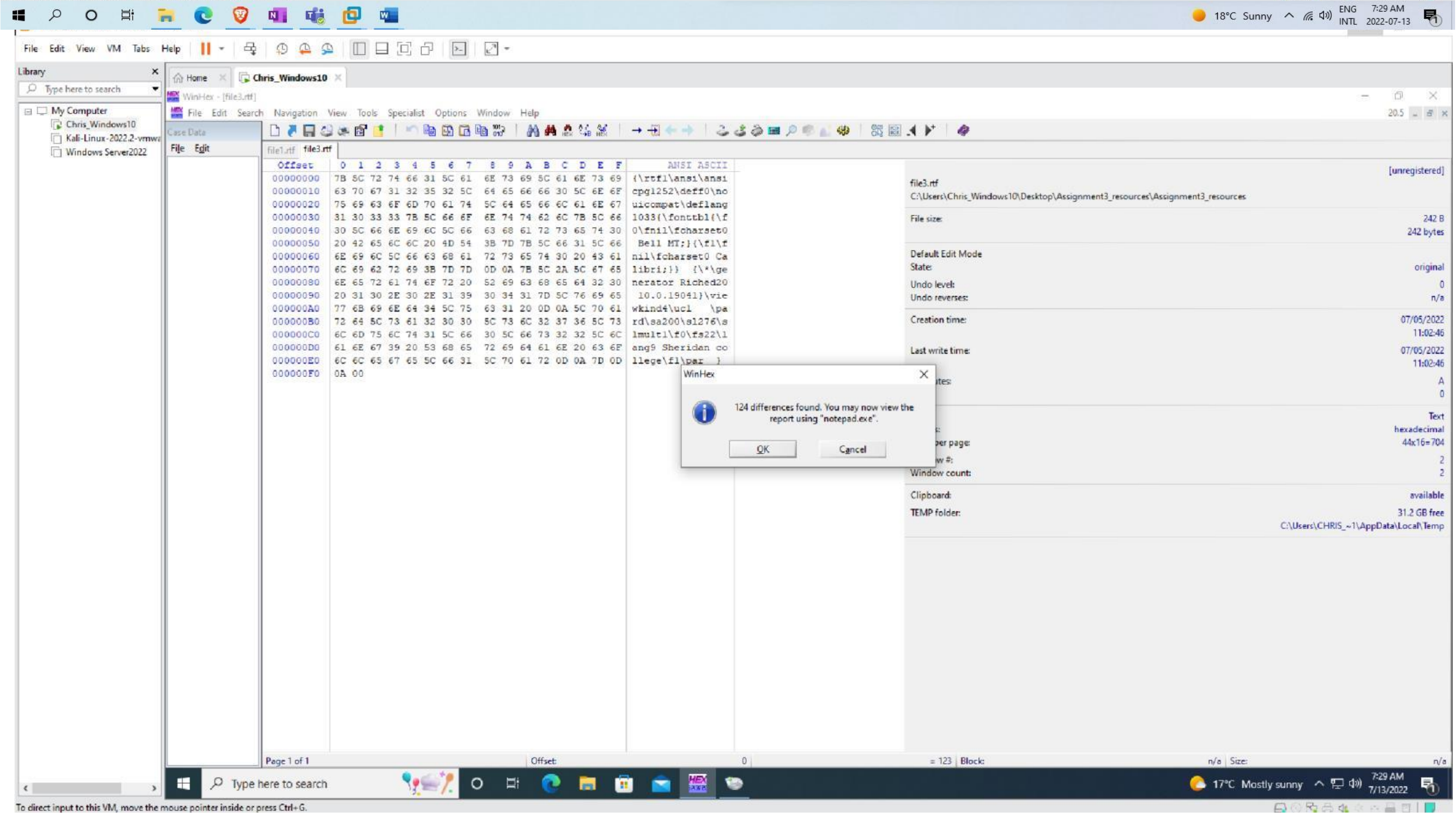
file3.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size: 242 B
242 bytes

original
0
n/a
07/05/2022
11:02:46
07/05/2022
11:02:46
A
0
Text
hexadecimal
44x16=704
2
2
available
31.2 GB free
C:\Users\CHRIS_~1\AppData\Local\Temp

= 123 Block: n/a Size: n/a

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



```
Offset    0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000  7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69  {\rtf1\ansi\ansi
00000010  63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F  cpg1252\deff0\no
00000020  75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67  uicompat\deflang
00000030  31 30 33 33 7B 5C 66 6F  6E 74 74 62 6C 7B 5C 66  1033{\fonttbl{\f
00000040  30 5C 66 6E 69 6C 5C 66  63 68 61 72 73 65 74 30  0\fnil\fcharset0
00000050  20 42 65 6C 6C 20 4D 54  3B 7D 7B 5C 66 31 5C 66   Bell MT;}{\f1\f
00000060  6E 69 6C 5C 66 63 68 61  72 73 65 74 30 20 43 61  nil\fcharset0 Ca
00000070  6C 69 62 72 69 3B 7D 7D  0D 0A 7B 5C 2A 5C 67 65  libri;}}  {\*\ge
00000080  6E 65 72 61 74 6F 72 20  52 69 63 68 65 64 32 30  nerator Riched20
00000090  20 31 30 2E 30 2E 31 39  30 34 31 7D 5C 76 69 65   10.0.19041}\vie
000000A0  77 6B 69 6E 64 34 5C 75  63 31 20 0D 0A 5C 70 61  wkind4\uc1   \pa
000000B0  72 64 5C 73 61 32 30 30  5C 73 6C 32 37 36 5C 73  rd\sa200\sl276\s
000000C0  6C 6D 75 6C 74 31 5C 66  30 5C 66 73 32 32 5C 6C  lmult1\f0\fs22\l
000000D0  61 6E 67 39 20 53 68 65  72 69 64 61 6E 20 63 6F  ang9 Sheridan co
000000E0  6C 6C 65 67 65 5C 66 31  5C 70 61 72 0D 0A 7D 0D  llege\f1\par  }
000000F0  0A 00
```

WinHex

124 differences found. You may now view the report using "notepad.exe".

OK | Cancel

[unregistered]

file3.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size: 242 B
242 bytes

Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a

Creation time: 07/05/2022
11:02:46

Last write time: 07/05/2022
11:02:46

...tes: A
0

Text
hexadecimal
...er page: 44x16=704
...w #: 2
Window count: 2

Clipboard: available
TEMP folder: 31.2 GB free
C:\Users\CHRIS_~1\AppData\Local\Temp

= 123 Block: n/a Size: n/a

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

i) **[4 Marks]** Something is strange on offset.

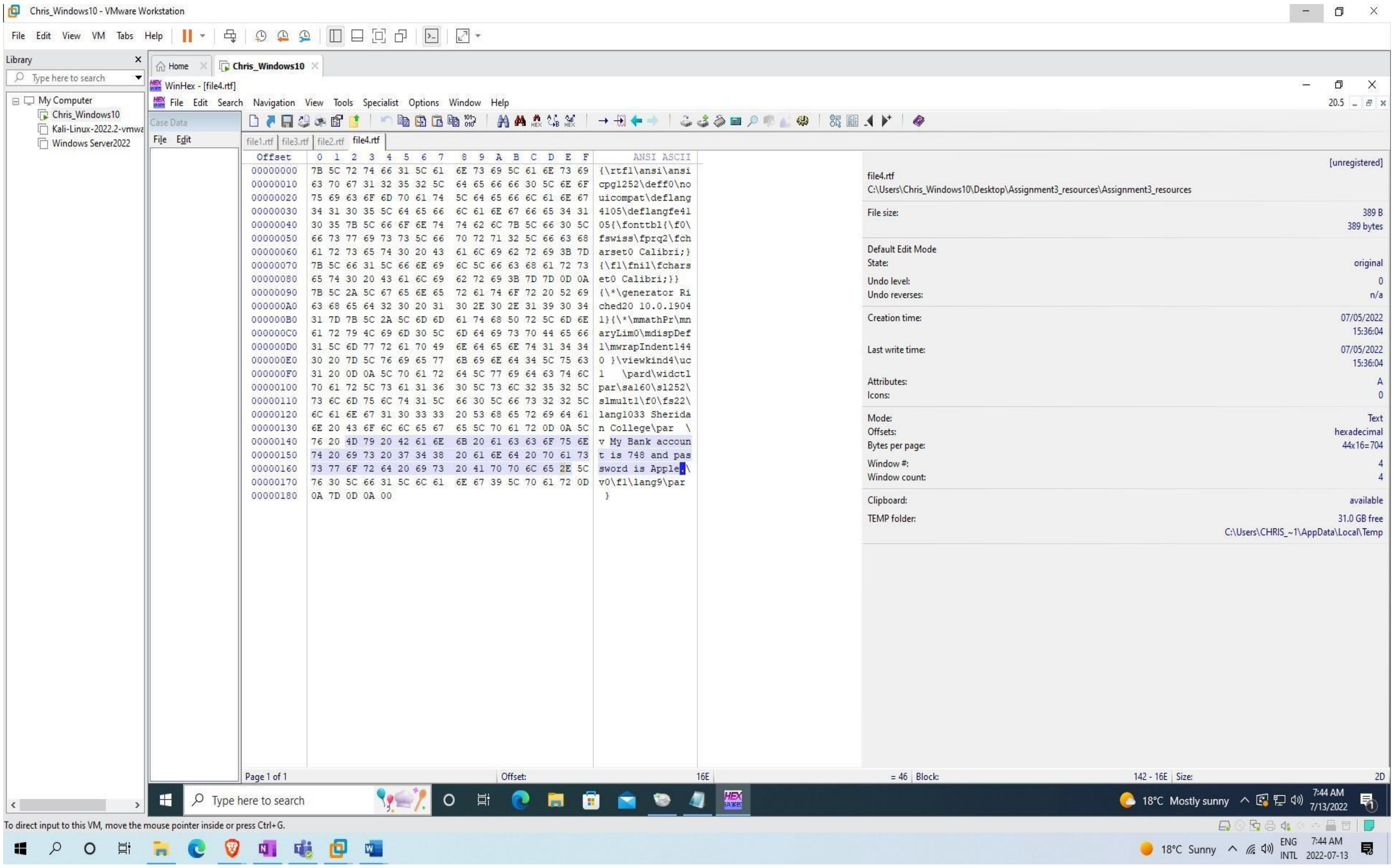
i. How much byte are different? ____**124 Bytes**_______ ii. How many differences you got (check the report)? _____**124**_________ iii. Submit the differences report you got with the submission

j) **[1Mark]** Open file4.rtf in wordpad. **What is the original content you see here? ______SC** ____________

k) **[2 Marks]** Looks like the contents is same as file1.rtf, file2.rtf and file3.rtf. However, this file is hiding a dark secret!! Open the file in WinHex to see a hidden message. What is the secret message you received? _______**My Bank account is 748 and password is Apple.**____. Attach the screenshot highlighting the secret message. This is a form a steganography, that is, hiding information or a message within another file.

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F    ANSI ASCII
00000000   7B 5C 72 74 66 31 5C 61  6E 73 69 5C 61 6E 73 69   {\rtf1\ansi\ansi
00000010   63 70 67 31 32 35 32 5C  64 65 66 66 30 5C 6E 6F   cpg1252\deff0\no
00000020   75 69 63 6F 6D 70 61 74  5C 64 65 66 6C 61 6E 67   uicompat\deflang
00000030   34 31 30 35 5C 64 65 66  6C 61 6E 67 66 65 34 31   4105\deflangfe41
00000040   30 35 7B 5C 66 6F 6E 74  74 62 6C 7B 5C 66 30 5C   05{\fonttbl{\f0\
00000050   66 73 77 69 73 73 5C 66  70 72 71 32 5C 66 63 68   fswiss\fprq2\fch
00000060   61 72 73 65 74 30 20 43  61 6C 69 62 72 69 3B 7D   arset0 Calibri;}
00000070   7B 5C 66 31 5C 66 6E 69  6C 5C 66 63 68 61 72 73   {\f1\fnil\fchars
00000080   65 74 30 20 43 61 6C 69  62 72 69 3B 7D 7D 0D 0A   et0 Calibri;}}
00000090   7B 5C 2A 5C 67 65 6E 65  72 61 74 6F 72 20 52 69   {\*\generator Ri
000000A0   63 68 65 64 32 30 20 31  30 2E 30 2E 31 39 30 34   ched20 10.0.1904
000000B0   31 7D 7B 5C 2A 5C 6D 6D  61 74 68 50 72 5C 6D 6E   1}{\*\mmathPr\mn
000000C0   61 72 79 4C 69 6D 30 5C  6D 64 69 73 70 44 65 66   aryLim0\mdispDef
000000D0   31 5C 6D 77 72 61 70 49  6E 64 65 6E 74 31 34 34   1\mwrapIndent144
000000E0   30 20 7D 5C 76 69 65 77  6B 69 6E 64 34 5C 75 63   0 }\viewkind4\uc
000000F0   31 20 0D 0A 5C 70 61 72  64 5C 77 69 64 63 74 6C   1   \pard\widctl
00000100   70 61 72 5C 73 61 31 36  30 5C 73 6C 32 35 32 5C   par\sa160\sl252\
00000110   73 6C 6D 75 6C 74 31 5C  66 30 5C 66 73 32 32 5C   slmult1\f0\fs22\
00000120   6C 61 6E 67 31 30 33 33  20 53 68 65 72 69 64 61   lang1033 Sherida
00000130   6E 20 43 6F 6C 6C 65 67  65 5C 70 61 72 0D 0A 5C   n College\par  \
00000140   76 20 4D 79 20 42 61 6E  6B 20 61 63 63 6F 75 6E   v My Bank accoun
00000150   74 20 69 73 20 37 34 38  20 61 6E 64 20 70 61 73   t is 748 and pas
00000160   73 77 6F 72 64 20 69 73  20 41 70 70 6C 65 2E 5C   sword is Apple.\
00000170   76 30 5C 66 31 5C 6C 61  6E 67 39 5C 70 61 72 0D   v0\f1\lang9\par
00000180   0A 7D 0D 0A 00                                       }
```

```
[unregistered]
file4.rtf
C:\Users\Chris_Windows10\Desktop\Assignment3_resources\Assignment3_resources

File size:                 389 B
                       389 bytes

Default Edit Mode
State:                  original
Undo level:                    0
Undo reverses:               n/a

Creation time:        07/05/2022
                        15:36:04

Last write time:      07/05/2022
                        15:36:04

Attributes:                    A
Icons:                         0

Mode:                       Text
Offsets:             hexadecimal
Bytes per page:       44x16=704
Window #:                      4
Window count:                  4

Clipboard:             available
TEMP folder:         31.0 GB free
C:\Users\CHRIS_~1\AppData\Local\Temp
```

```
Page 1 of 1    Offset:    16E    = 46  Block:    142 - 16E  Size:    2D
```

l) **[2 Marks]** Why would steganography be important to identify in digital forensics? Give an example to support your answer.

Steganography is important to identify specific text, and files that are hiding in an image. An example of this would be if someone is hiding a password inside of the image and you need the password to access an account, zip file, etc.

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52

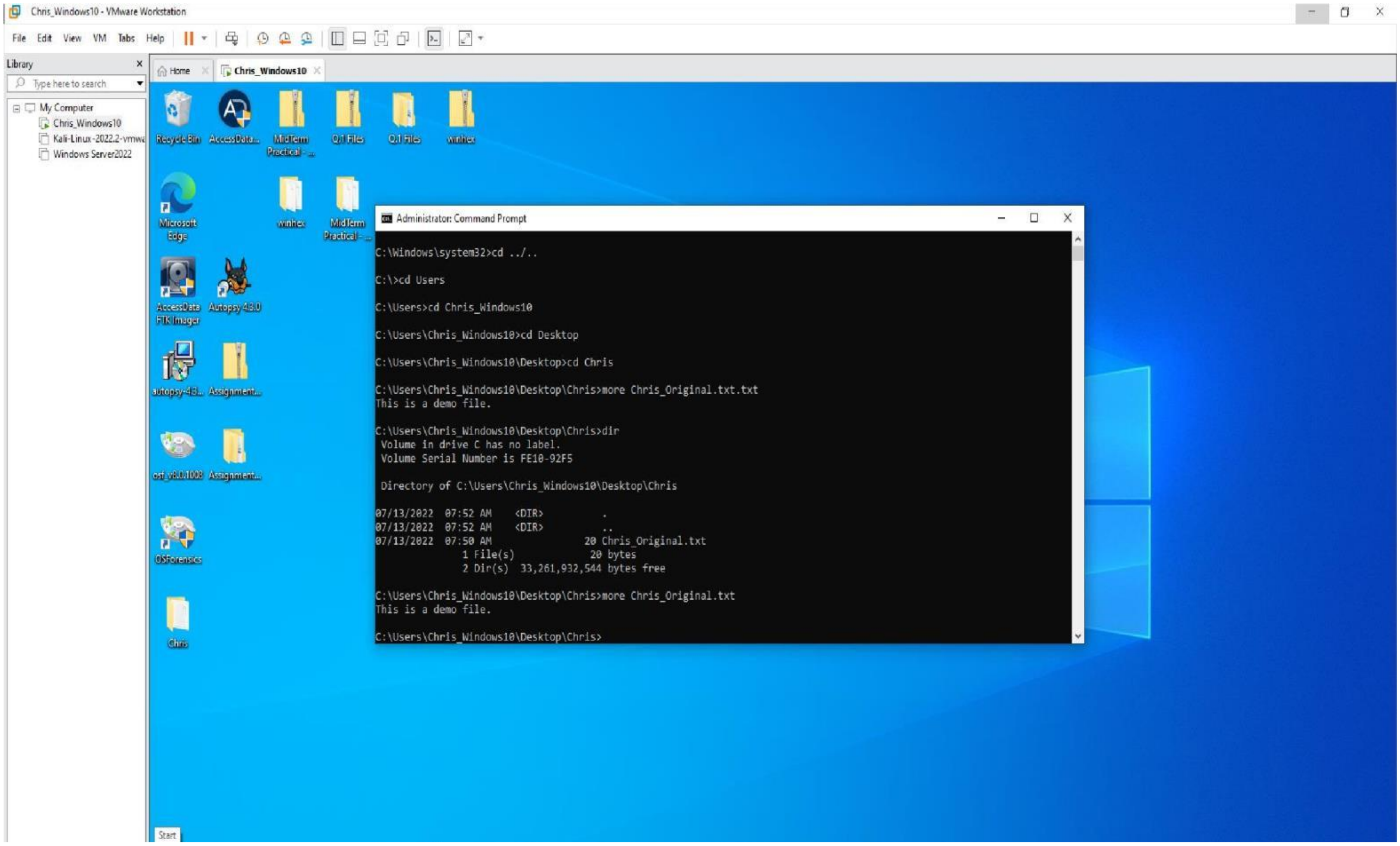
Task 2: To detect NTFS stream data [8 Marks]

a) Create a new directory as your firstname. Create a txt file in that directory as firstname_original.txt having content as – This is a demo file. Save and close.

b) Open a command prompt and run as administrator.

c) **[3 Marks]** From command prompt, display the content of firstname_original.txt file.

i. What is the command used? ________**more_Chris_original.txt**____________________ ii. Attach the screenshot displaying the contents of the file in command prompt.

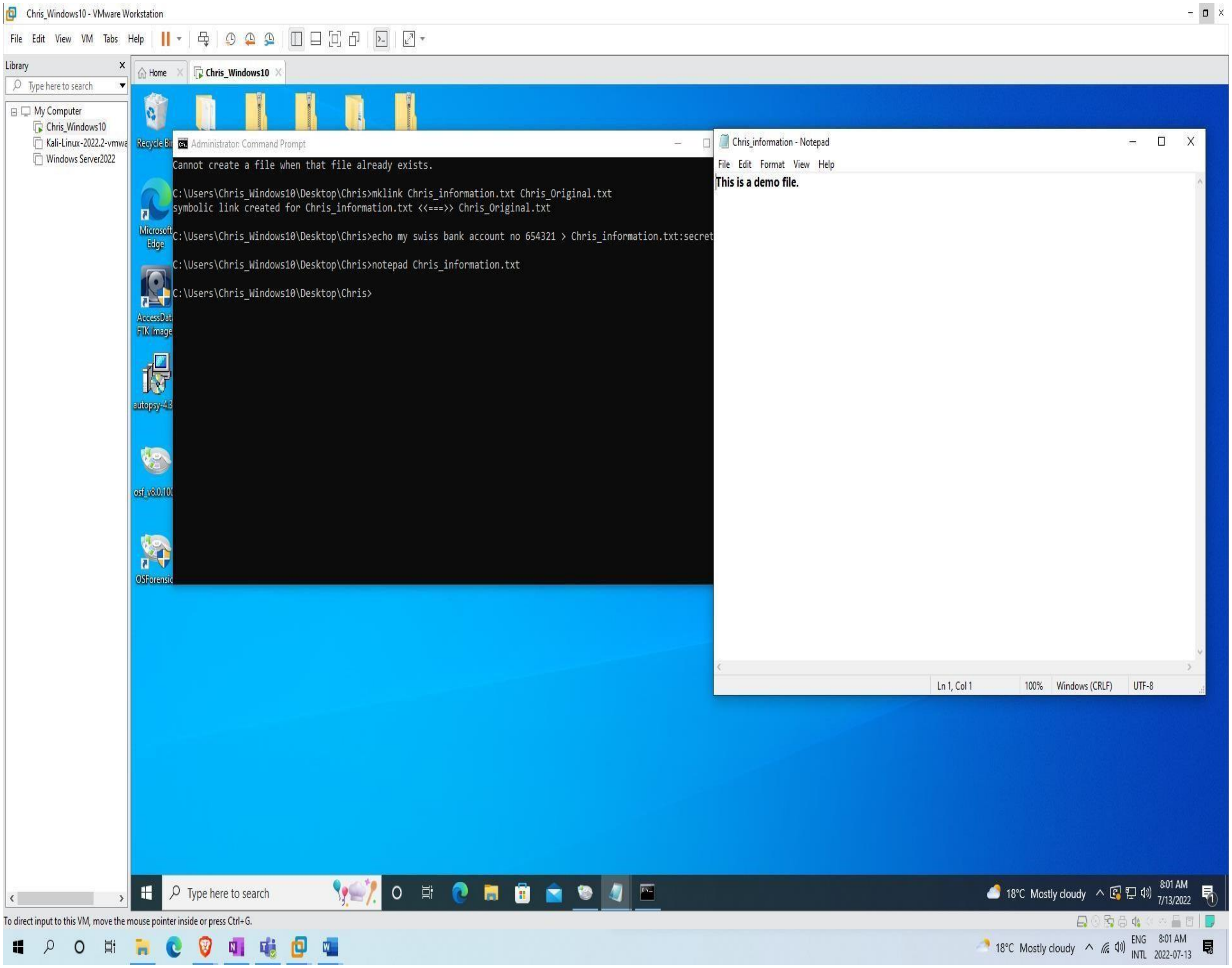


```
C:\Windows\system32>cd ../..

C:\>cd Users

C:\Users>cd Chris_Windows10

C:\Users\Chris_Windows10>cd Desktop

C:\Users\Chris_Windows10\Desktop>cd Chris

C:\Users\Chris_Windows10\Desktop\Chris>more Chris_Original.txt.txt
This is a demo file.

C:\Users\Chris_Windows10\Desktop\Chris>dir
 Volume in drive C has no label.
 Volume Serial Number is FE10-92F5

 Directory of C:\Users\Chris_Windows10\Desktop\Chris

07/13/2022  07:52 AM    <DIR>          .
07/13/2022  07:52 AM    <DIR>          ..
07/13/2022  07:50 AM                20 Chris_Original.txt
               1 File(s)             20 bytes
               2 Dir(s)  33,261,932,544 bytes free

C:\Users\Chris_Windows10\Desktop\Chris>more Chris_Original.txt
This is a demo file.

C:\Users\Chris_Windows10\Desktop\Chris>
```

d) **[1 Mark]** Create the reference (symbolic link) of this firstname_original.txt in firstname_information.txt file. What's the command used to create this symbolic link? ______**mklink___Chris_information.txt Chris_original.txt**____

e) Type the following command to save secret notes to a different text file - echo my swiss bank account no 654321 > firstname_information.txt:secret.txt

f) **[2 Marks]** Type the following command- notepad firstname_information.txt. What do you get as an output? Attach the screenshot.

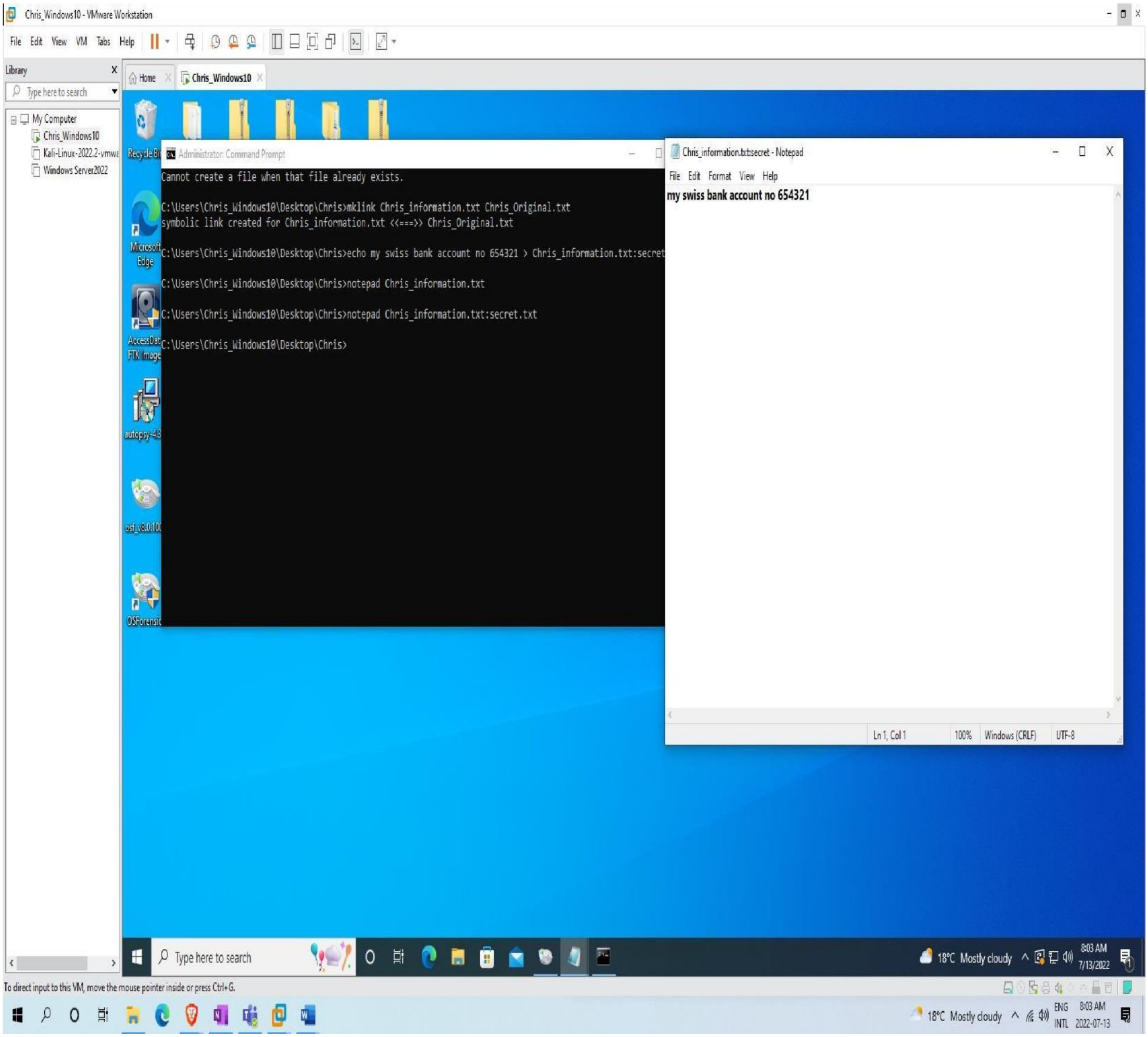


Chris_Windows10 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Chris_Windows10
Kali-Linux-2022.2-vmwa
Windows Server2022
Home
Chris_Windows10
Administrator: Command Prompt
Chris_information - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
Type here to search
18°C Mostly cloudy
8:01 AM
7/13/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
ENG
INTL
2022-07-13

```
Cannot create a file when that file already exists.

C:\Users\Chris_Windows10\Desktop\Chris>mklink Chris_information.txt Chris_Original.txt
symbolic link created for Chris_information.txt <<===>> Chris_Original.txt

C:\Users\Chris_Windows10\Desktop\Chris>echo my swiss bank account no 654321 > Chris_information.txt:secret

C:\Users\Chris_Windows10\Desktop\Chris>notepad Chris_information.txt

C:\Users\Chris_Windows10\Desktop\Chris>
```

This is a demo file.

g) [2 Marks] Try the following command to see the secret message: notepad firstname_information.txt:secret.txt. Attach your screenshot.


Chris_Windows10 - VMware Workstation
Library
My Computer
Chris_Windows10
Kali-Linux-2022.2-vmwa
Windows Server2022
Home
Chris_Windows10
Administrator: Command Prompt
Chris_information.txt:secret - Notepad
File Edit Format View Help
Ln 1, Col 1
100%
Windows (CRLF)
UTF-8
18°C Mostly cloudy
8:03 AM
7/13/2022
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Cannot create a file when that file already exists.

C:\Users\Chris_Windows10\Desktop\Chris>mklink Chris_information.txt Chris_Original.txt
symbolic link created for Chris_information.txt <<===>> Chris_Original.txt

C:\Users\Chris_Windows10\Desktop\Chris>echo my swiss bank account no 654321 > Chris_information.txt:secret

C:\Users\Chris_Windows10\Desktop\Chris>notepad Chris_information.txt

C:\Users\Chris_Windows10\Desktop\Chris>notepad Chris_information.txt:secret.txt

C:\Users\Chris_Windows10\Desktop\Chris>
```

my swiss bank account no 654321

Assignment 3: Working with Windows, CLI Systems and Steganography

Total Marks: 52

Task 3: To display contents in Steganography [18 Marks]

a) Download the ***steg.zip*** folder in your computer and unzip it on your desktop.

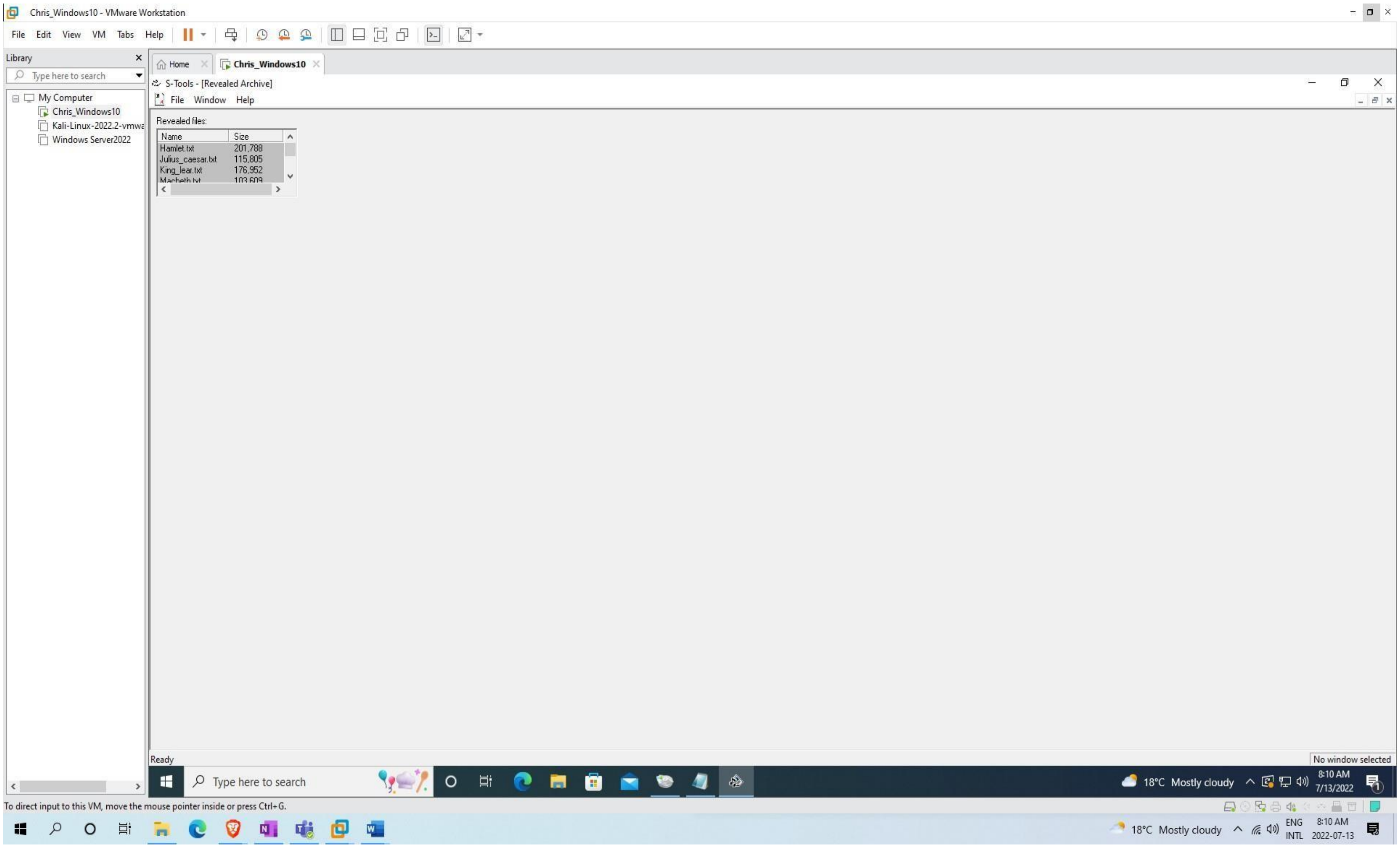
b) Start S-tools.exe by double clicking on the icon on the desktop. A window will appear. Drag the zebras.bmp file to the S-tools window.

c) Right click on the zebras pictures and select Reveal from the menu. Fill in the 3-character pass phrase 'abc' (without the quotes) in two places. Leave IDEA as the encryption algorithm. Click on OK.

d) **[8 Marks]** Wait until the Revealed Archive dialog box appears. This may take a minute or two.

i. Name the hidden files you found along with their sizes. **Hamlet.txt – 201,788, Julius_caesar.txt 115,805, King_lear.txt 176,952, Macbeth.txt 103,609, Merchant.txt 120,927, Notice.txt 15,810** ii.

Attach the screenshot too.



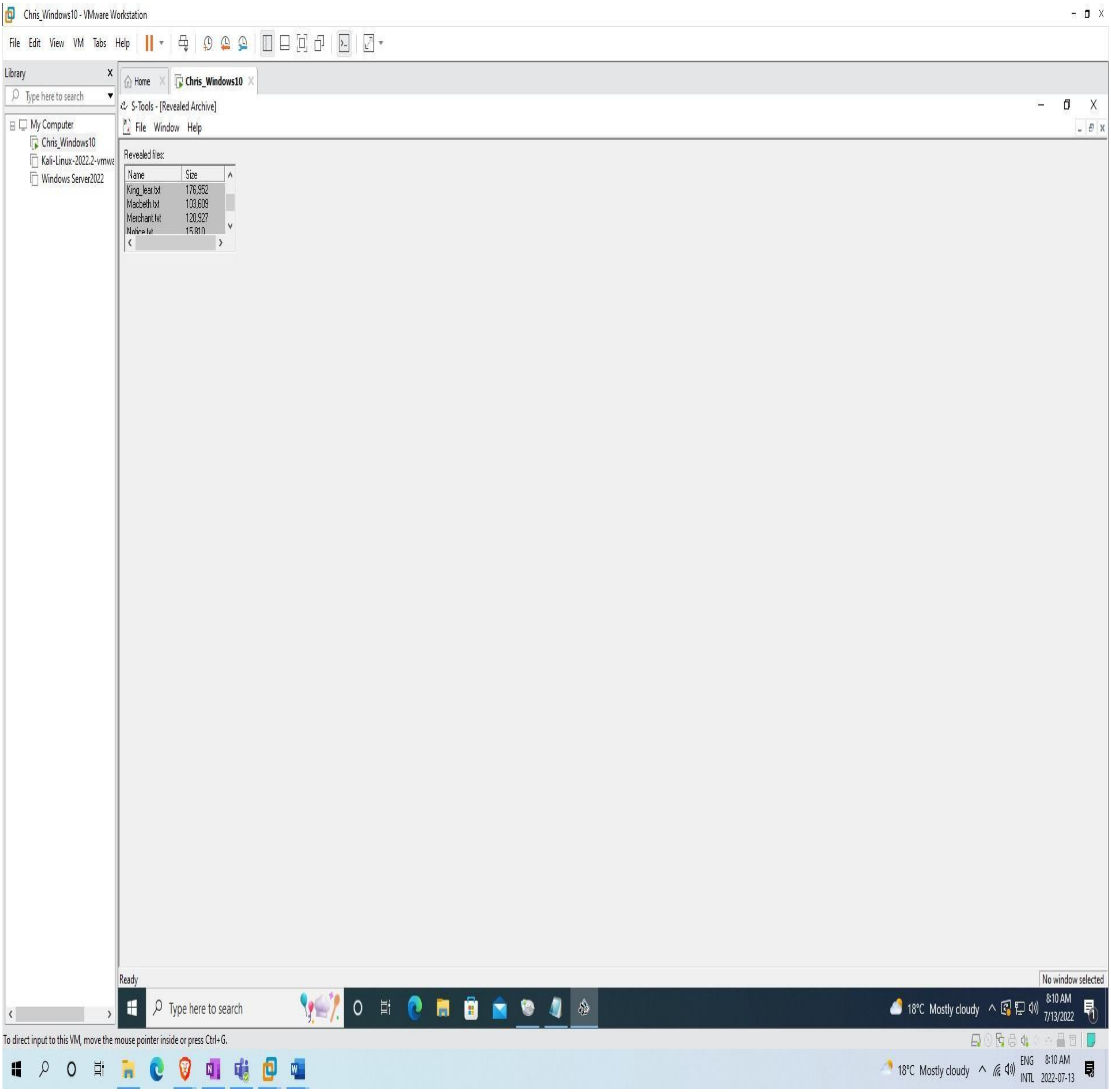
Revealed files:

Name	Size
Hamlet.txt	201,788
Julius_caesar.txt	115,805
King_lear.txt	176,952
Macbeth.txt	103,609

Ready

No window selected

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



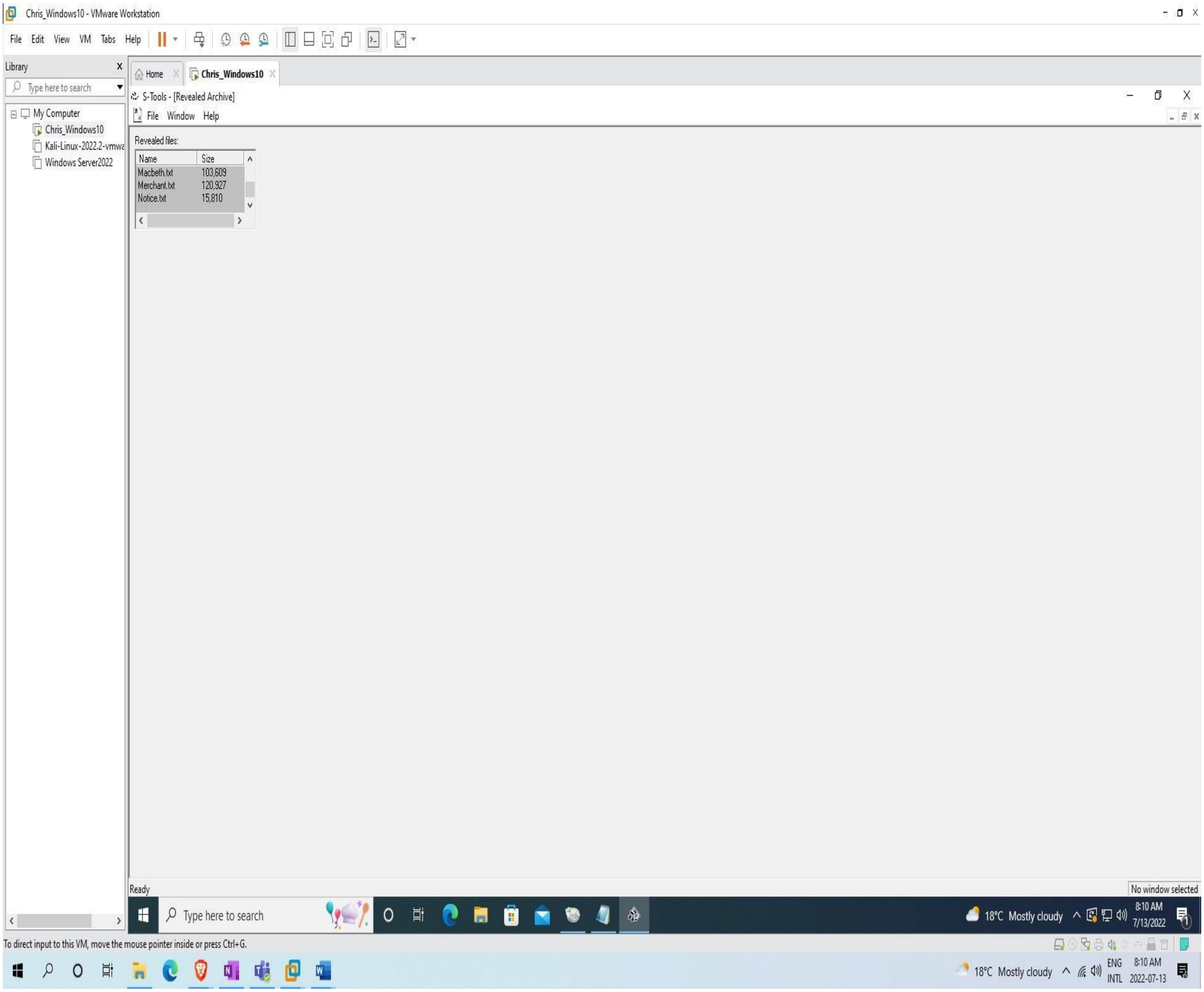
Revealed files:

Name	Size
King_lear.txt	176,952
Macbeth.txt	103,609
Merchant.txt	120,927
Notice.txt	15,810

Ready

No window selected

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Revealed files:

Name	Size
Macbeth.txt	103,609
Merchant.txt	120,927
Notice.txt	15,810

e) **[6 Marks]** Right click on any item and select Save As to save the file. Repeat for the other ones. These are the hidden files. Attach the hidden files with your submission.

f) **[4 Marks]** The file *original-zebras.bmp* is the file before the steganography was done. Compare the 'before' and 'after' images. How many differences were found? Attach the differences report with the submission. Name the report as firstname_stegno.txt

Things to Explore:

You are welcome to explore beyond the mandatory requirements if you wish.

General submission requirements

- Include an opening comment with your full name, date, and a short description.
- **Marks distribution (You are eligible to get complete marks if you satisfy the conditions of screenshots):**

  Task 1: 26 marks

  a) 03

  b) 03

  c) 03

  d) 01

  e) 01

  f) 02

  g) 02

  h) 02

  i) 04

  j) 01

  k) 02

  l) 02

  Task 2: 8 marks

Total Marks: 52

- **c) 03**
- **d) 01**
- **f) 02**
- **g) 02**

Task 3: 18 marks

- **d) 08**
- **e) 06**
- **f) 04**

- **Do not alter the sequence of steps of this document. Do not delete the words [Attach the screenshot] anywhere from the assignment. Keep the numbering same. Paste the screenshots wherever it's being asked. You should be not even submitting another student's screenshot- Academic Integrity alert.**
- **Your screenshots should have your virtual machine showing your name and date and time of the day the assignment was performed.**