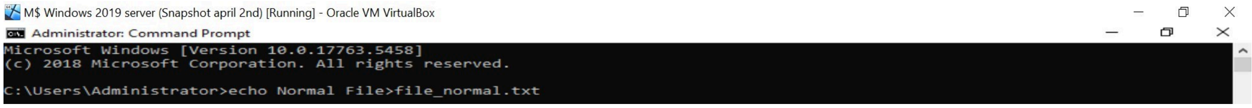
Name: Cristian Barreno

Incident Response Exercises - Second Group.

Exercise 1 - Alternate Data Streams.

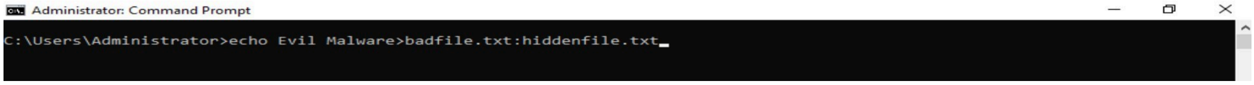
Task 1


M$ Windows 2019 server (Snapshot april 2nd) [Running] - Oracle VM VirtualBox
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.5458]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>echo Normal File>file_normal.txt
```

In the Windows command prompt I entered echo Normal File>file_normal.txt.
Echo is used to display messages
I redirected Normal File into file_normal.txt

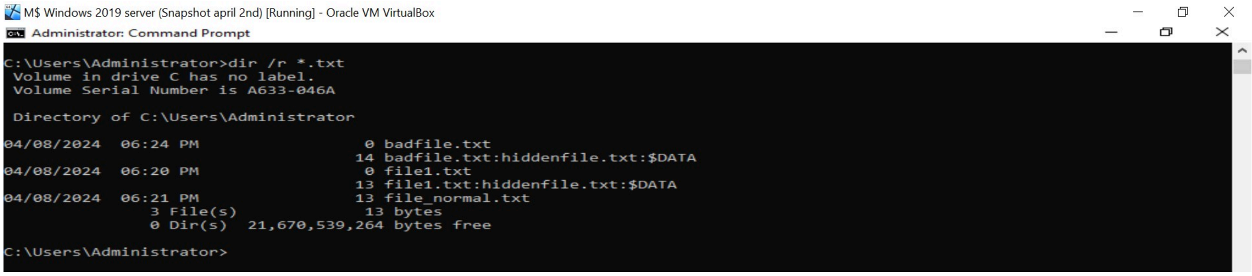
Task 2



```
C:\Users\Administrator>echo Evil Malware>badfile.txt:hiddenfile.txt_
```

In the Windows command prompt i entered echo Evil Malware>badfile.txt:hiddenfile.txt
Here i redirected Evil Malware into badfile.txt followed by colon, and followed by hiddenfile.txt which is the Alternate Data Stream

Task 3


M$ Windows 2019 server (Snapshot april 2nd) [Running] - Oracle VM VirtualBox
Administrator: Command Prompt

```
C:\Users\Administrator>dir /r *.txt
 Volume in drive C has no label.
 Volume Serial Number is A633-046A

 Directory of C:\Users\Administrator

04/08/2024  06:24 PM                    0 badfile.txt
                                       14 badfile.txt:hiddenfile.txt:$DATA
04/08/2024  06:20 PM                    0 file1.txt
                                       13 file1.txt:hiddenfile.txt:$DATA
04/08/2024  06:21 PM                   13 file_normal.txt
               3 File(s)               13 bytes
               0 Dir(s)  21,670,539,264 bytes free

C:\Users\Administrator>
```

In the screenshot above i entered dir /r *.txt

Dir is used to list the contents of a directory.
/r instructs the dir command to display alternated data streams for each file listed
.txt Here the wildcard (*) matches any sequence of characters , and .txt specifies the type of file.

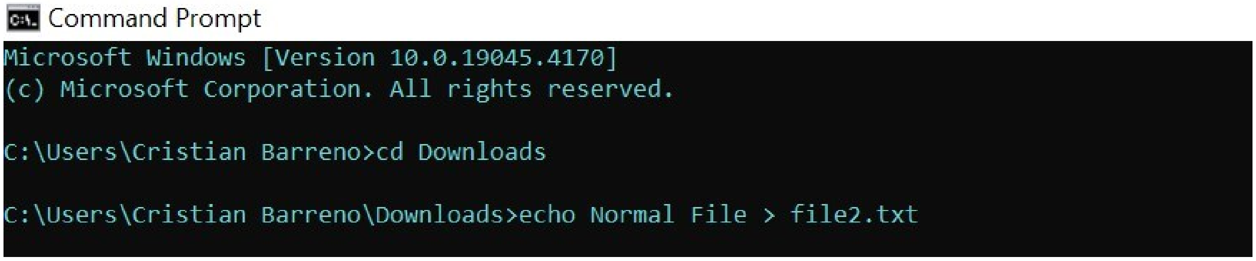
Task 4

What was the output of the dir command, what did that output mean?

It shows the .txt files that I created, and a copy of the created files with Alternate Data Streams.

Exercise 2
Alternate Data Streams – Things aren’t always as they seem

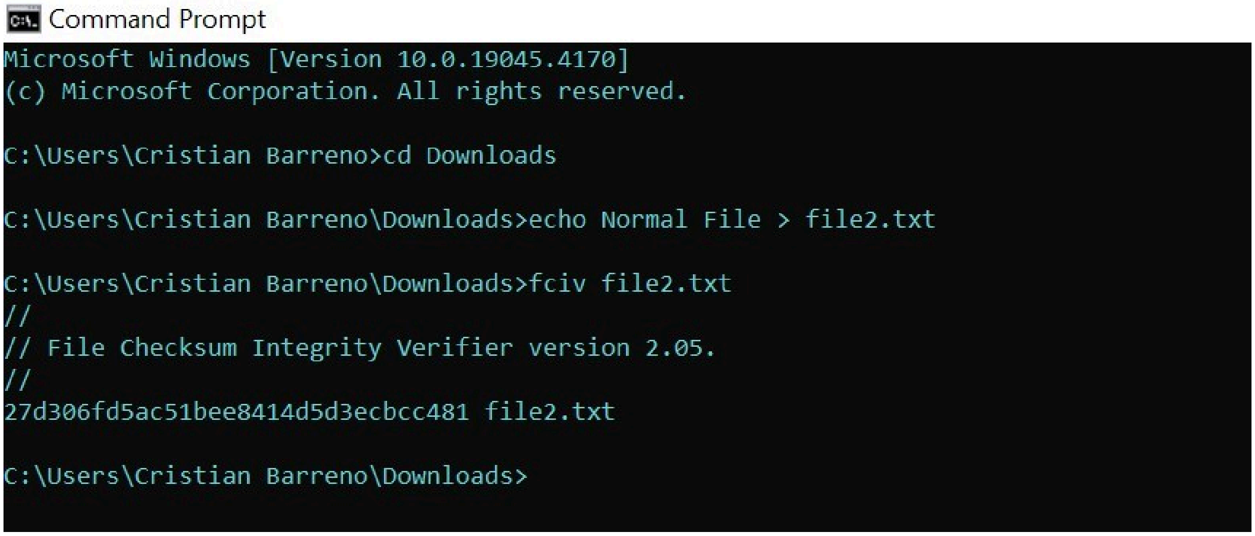
Task 1



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Cristian Barreno>cd Downloads

C:\Users\Cristian Barreno\Downloads>echo Normal File > file2.txt
```

I redirected echo Normal File to file2.txt

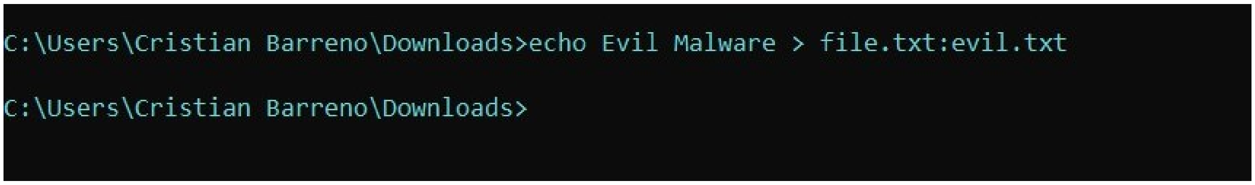
Task 2
Obtain a hash of file2.txt



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Cristian Barreno>cd Downloads

C:\Users\Cristian Barreno\Downloads>echo Normal File > file2.txt

C:\Users\Cristian Barreno\Downloads>fciv file2.txt
//
// File Checksum Integrity Verifier version 2.05.
//
27d306fd5ac51bee8414d5d3ecbcc481 file2.txt

C:\Users\Cristian Barreno\Downloads>
```

FCIV stands for File Checksum Integrity Verifier. Is a command line utility for making hashes of files. FCIV provided me with a hash of file2.txt

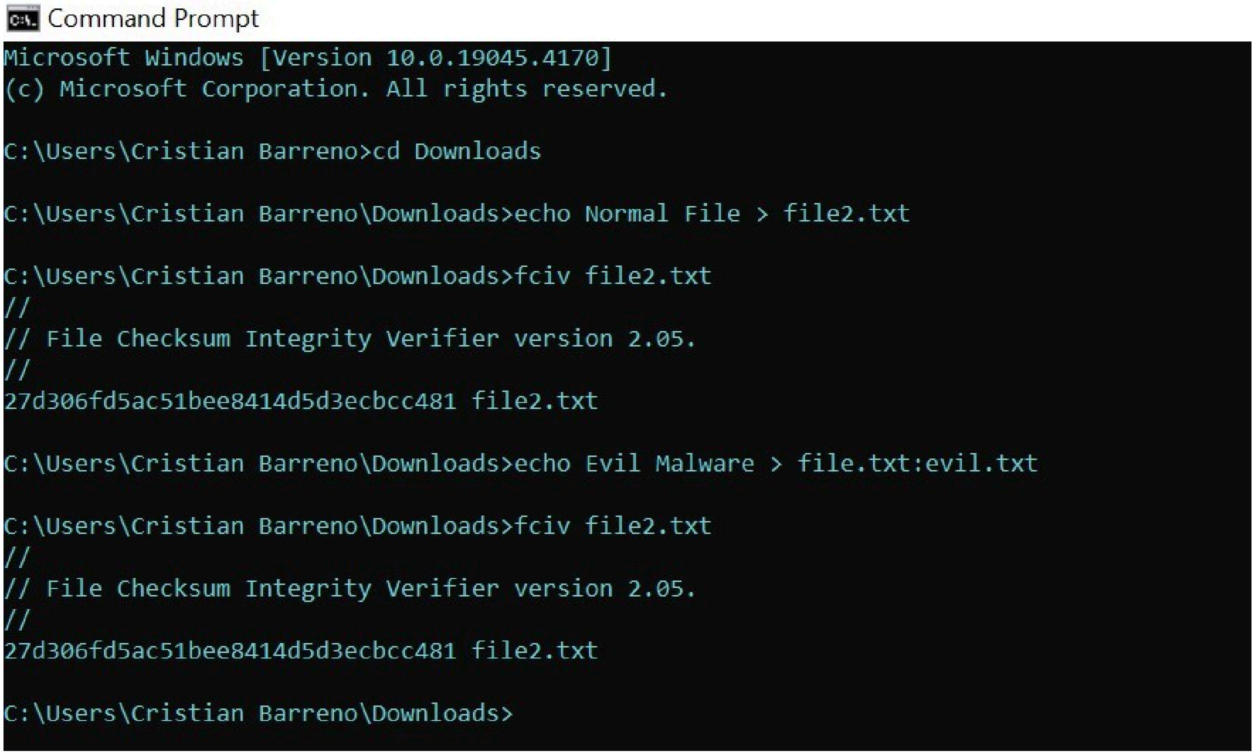
Task 3



```
C:\Users\Cristian Barreno\Downloads>echo Evil Malware > file.txt:evil.txt

C:\Users\Cristian Barreno\Downloads>
```

I added Evil Malware as an alternate data stream to file2.txt:evil.txt

Task 4



```
Microsoft Windows [Version 10.0.19045.4170]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Cristian Barreno>cd Downloads

C:\Users\Cristian Barreno\Downloads>echo Normal File > file2.txt

C:\Users\Cristian Barreno\Downloads>fciv file2.txt
//
// File Checksum Integrity Verifier version 2.05.
//
27d306fd5ac51bee8414d5d3ecbcc481 file2.txt

C:\Users\Cristian Barreno\Downloads>echo Evil Malware > file.txt:evil.txt

C:\Users\Cristian Barreno\Downloads>fciv file2.txt
//
// File Checksum Integrity Verifier version 2.05.
//
27d306fd5ac51bee8414d5d3ecbcc481 file2.txt

C:\Users\Cristian Barreno\Downloads>
```

We can see that the hash did not change because the hash is typically calculated only on the primary data stream of the file.