Exercise 7

28/09/2020

Comparing file structures using a Hex editor

a) Text editing tools such as Notepad, Wordpad, MS Word provide additional formatting information to text files. Create text files using these tools. Then use a Hex editor such as vim or WinHex to view these files. What similarities and differences do you notice? How can you tell what type of file you are looking at by what vim or WinHex shows in the Hex window?

Note: WinHex is a universal hexadecimal editor, particularly helpful in the realm of computer forensics. Download an evaluation copy of WinHex from https://www.x-ways.net/winhex/

WinHex is used to inspect and edit all kinds of files, recover deleted files or lost data from hard drives with corrupt file systems or from digital camera cards.

See https://en.wikipedia.org/wiki/Hex_editor for info about hex editors.

See https://en.wikipedia.org/wiki/Comparison_of_hex_editors for a comparison of Hex editor features.

b) NTFS hidden streams

NTFS streams allow us to store more than a single file under the same name. Create a folder dirtysecret. (If one already exists, remove all its contents.) In the dirtysecret folder we first create a file and then a stream.

```
c:\dirtysecret echo "This is a file" > file.txt
```

```
c:\dirtysecret echo "This is another file" > file.txt:hiddenstream.txt
```

Try now to find the second file using the DIR command. You cannot find it, but you can use it by employing tools such as Notepad:

```
c:\dirtysecret notepad file.txt:hiddenstream.txt
```

To discover an alternative data stream (ADS), we need to use tools such as Streams.exe from SysInternals

See https://docs.microsoft.com/en-us/sysinternals/downloads/streams

Getting rid of an ADS without destroying the original file is difficult. One can copy to a FAT file system, which would get rid of it or one can run the file through ftp. However, all of this becomes more tedious, if we associate an ADS to a directory. We can also connect the ADS to a file protected by Windows File Protection, which would make it nearly impossible to delete.

Read more about ADS at

https://en.wikipedia.org/wiki/NTFS#Alternate_data_streams_(ADS)

https://www.sciencedirect.com/topics/computer-science/alternate-data-stream

https://www.deepinstinct.com/2018/06/12/the-abuse-of-alternate-data-stream-hasnt-disappeared/

Include screenshots in your submission.