Logbook & Assignment Questions

Part A:

Provide a description of the function of the boot sector:

The function of the boot sector is to start the boot process in order to load an operating system, the boot sector exists on the hard drive where the operating system windows/Linux/Mac is installed. Once a computer is launched the bios looks for clues on how to boot up the OS, in doing so the first place the bios will check is the boot sector and each drive has one boot sector, the bios checks the boot sector and finds which drive holds the OS.

Provide a description of the function of the FAT:

A file allocation table aka FAT is a table that an operating system maintains on a hard disk that provides a map of the clusters which is the basic units of logical storage on a hard disk that a file has been stored in. The OS creates a FAT entry for the new file that records where each cluster is created and their order. When you read a file, the OS assembles the file from clusters and places it as an entire file where you want to read it.

Part B:

A. Image Name: Test-Image1-clean.dd.001

B. Hash Value:

MD5: cce9a0e19318ff056e45f98e876c40a2

SHA1: 5b0b07151e8c0a559c0fe2bb9253e6b392ad5c71

C. Storage Location: C:\Temp\Test-Image1-clean.dd

What is the FAT32 File System and why is it important for Pen Drives?

FAT32 is a disk format used to organise the files that are on a disk drive. The disk drive is sorted into different sections called sectors and a File Allocation table (FAT) is created at the beginning of the drive so that information in the file can bee found by the computer. 32 refers to the number of bits that the system uses to store these addresses. FAT32 is important for its usefulness, there's a good reason it's lasted so long and is still used in this modern decade. FAT32 is important due to its compatibility with a huge variety of devices such as smartphones, tablets, computers, digital cameras, gaming consoles, surveillance cameras, etc etc.

Part D:

A. Image Name: Test-Image-clean-with-textfile.dd.001

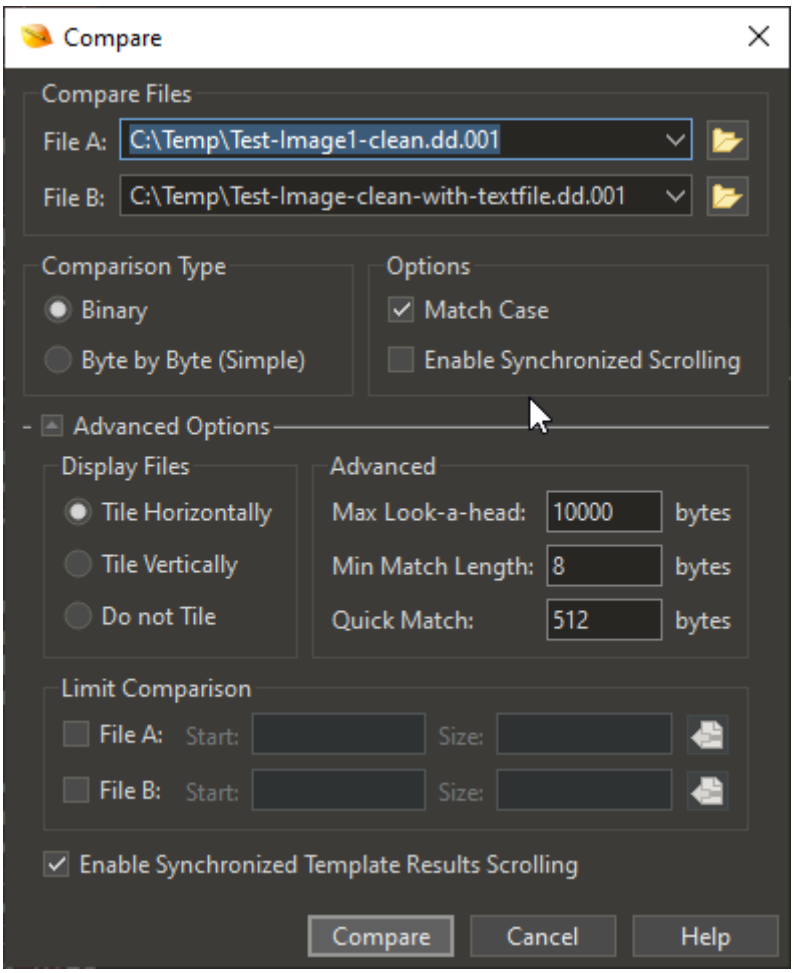
B. Hash Value:

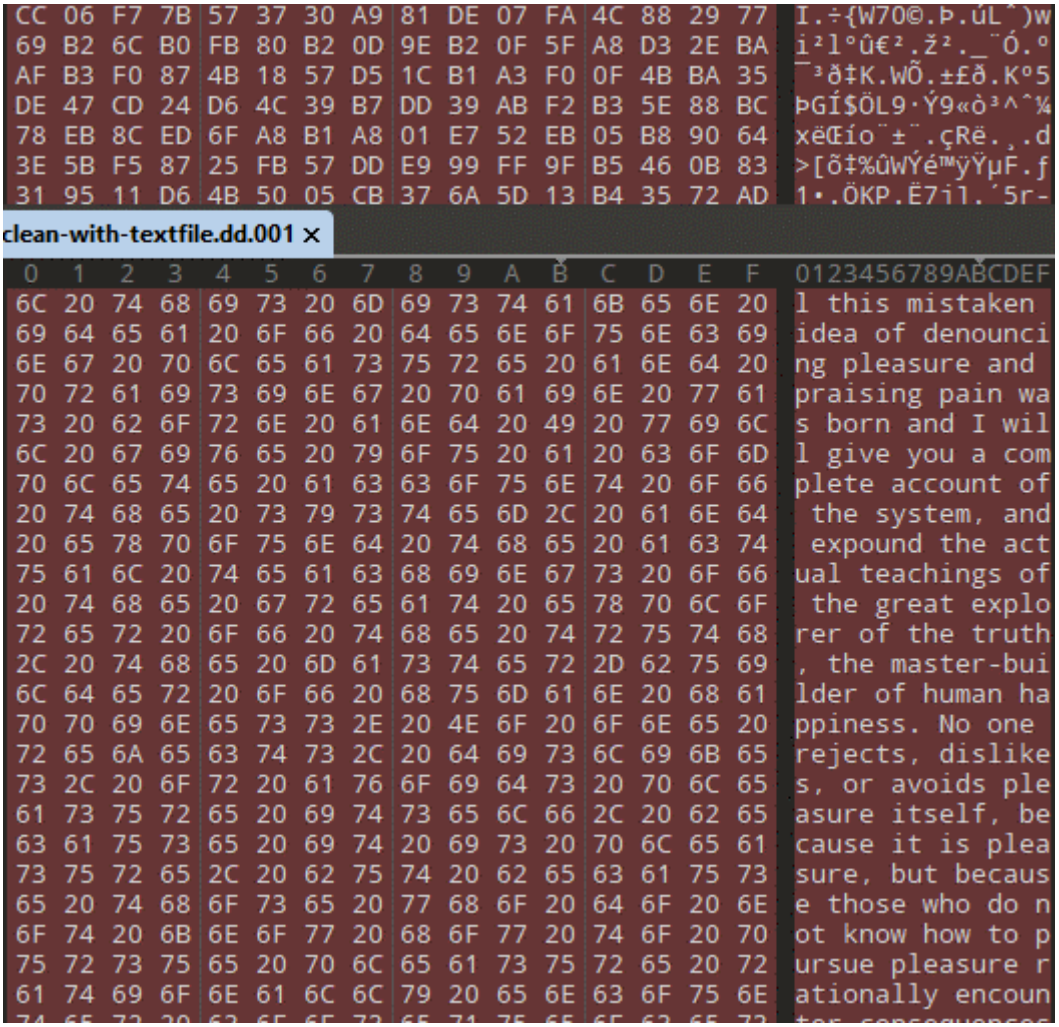
MD5: 7a000c950f55c0c3bb44a9214ede5bdb

SHA1: 5d39785548ff9aa7fe13438b70d8489da3e5bd07

C. Storage Location: C:\Temp\Test-Image-clean-with-textfile.dd.001

For my observation of the files and their comparison I don't feel like there's a major difference between the 2 cleaned disk images beside the fact that one has a text file embodied in it as I found and presented below.

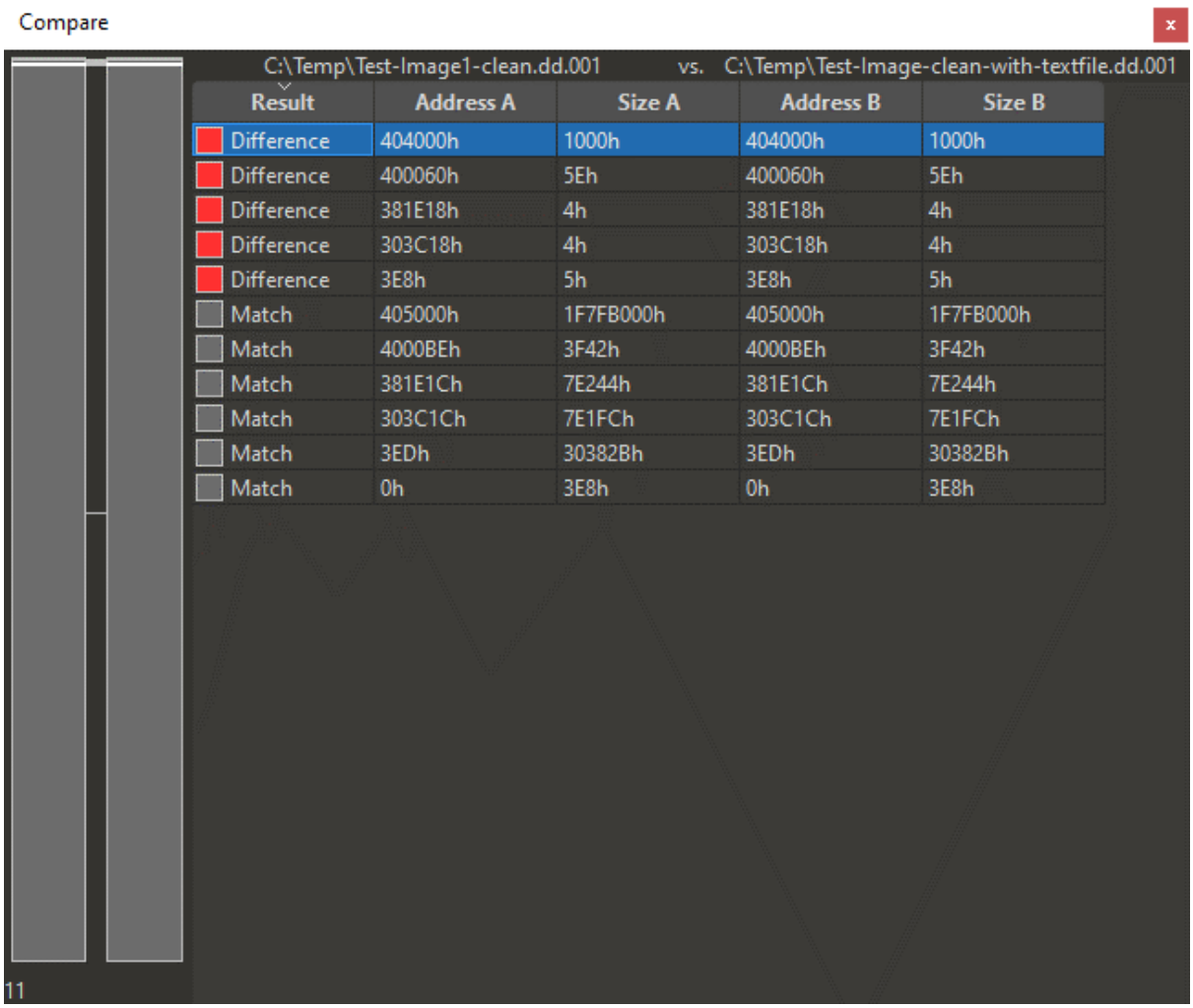




```
CC 06 F7 7B 57 37 30 A9 81 DE 07 FA 4C 88 29 77  Ì.÷{W70©.Þ.úLˆ)w
69 B2 6C B0 FB 80 B2 0D 9E B2 0F 5F A8 D3 2E BA  i²l°û€².ž².¨Ó.º
AF B3 F0 87 4B 18 57 D5 1C B1 A3 F0 0F 4B BA 35  ¯³ð‡K.WÕ.±£ð.Kº5
DE 47 CD 24 D6 4C 39 B7 DD 39 AB F2 B3 5E 88 BC  ÞGÍ$ÖL9·Ý9«ò³^ˆ¼
78 EB 8C ED 6F A8 B1 A8 01 E7 52 EB 05 B8 90 64  xëŒío¨±¨.çRë.¸.d
3E 5B F5 87 25 FB 57 DD E9 99 FF 9F B5 46 0B 83  >[õ‡%ûWÝé™ÿŸµF.ƒ
31 95 11 D6 4B 50 05 CB 37 6A 5D 13 B4 35 72 AD  1•.ÖKP.Ë7j].´5r-
```

clean-with-textfile.dd.001 ×

```
 0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
6C 20 74 68 69 73 20 6D 69 73 74 61 6B 65 6E 20  l this mistaken
69 64 65 61 20 6F 66 20 64 65 6E 6F 75 6E 63 69  idea of denounci
6E 67 20 70 6C 65 61 73 75 72 65 20 61 6E 64 20  ng pleasure and
70 72 61 69 73 69 6E 67 20 70 61 69 6E 20 77 61  praising pain wa
73 20 62 6F 72 6E 20 61 6E 64 20 49 20 77 69 6C  s born and I wil
6C 20 67 69 76 65 20 79 6F 75 20 61 20 63 6F 6D  l give you a com
70 6C 65 74 65 20 61 63 63 6F 75 6E 74 20 6F 66  plete account of
20 74 68 65 20 73 79 73 74 65 6D 2C 20 61 6E 64   the system, and
20 65 78 70 6F 75 6E 64 20 74 68 65 20 61 63 74   expound the act
75 61 6C 20 74 65 61 63 68 69 6E 67 73 20 6F 66  ual teachings of
20 74 68 65 20 67 72 65 61 74 20 65 78 70 6C 6F   the great explo
72 65 72 20 6F 66 20 74 68 65 20 74 72 75 74 68  rer of the truth
2C 20 74 68 65 20 6D 61 73 74 65 72 2D 62 75 69  , the master-bui
6C 64 65 72 20 6F 66 20 68 75 6D 61 6E 20 68 61  lder of human ha
70 70 69 6E 65 73 73 2E 20 4E 6F 20 6F 6E 65 20  ppiness. No one
72 65 6A 65 63 74 73 2C 20 64 69 73 6C 69 6B 65  rejects, dislike
73 2C 20 6F 72 20 61 76 6F 69 64 73 20 70 6C 65  s, or avoids ple
61 73 75 72 65 20 69 74 73 65 6C 66 2C 20 62 65  asure itself, be
63 61 75 73 65 20 69 74 20 69 73 20 70 6C 65 61  cause it is plea
73 75 72 65 2C 20 62 75 74 20 62 65 63 61 75 73  sure, but becaus
65 20 74 68 6F 73 65 20 77 68 6F 20 64 6F 20 6E  e those who do n
6F 74 20 6B 6E 6F 77 20 68 6F 77 20 74 6F 20 70  ot know how to p
75 72 73 75 65 20 70 6C 65 61 73 75 72 65 20 72  ursue pleasure r
61 74 69 6F 6E 61 6C 6C 79 20 65 6E 63 6F 75 6E  ationally encoun
```



Part E:

Open http://www.tavi.co.uk/phobos/fat.html and https://www.pjrc.com/tech/8051/ide/fat32.html and summarise what it says about the FAT:

The FAT file system is heavily based on the file map model in terms of its on-disk layout, it is a simple robust file system. There are 3 variants of the FAT file System, a 12-bit, 16 bit and 32-bit version.

Here's a basic layout:

Basic layout

All disks using the FAT file system are divided into several areas. The following table summarises the areas in the order that they appear on the disk, starting at block 0:

Area description	Area size
Boot block	1 block
File Allocation Table (may be multiple copies)	Depends on file system size
Disk root directory	Variable (selected when disk is formatted)
File data area	The rest of the disk

The FAT file system contains several important data areas which help to describe the rest of the file system, to understand how a disk is laid out, it is necessary to understand the boot block.

Here's a boot block chart:

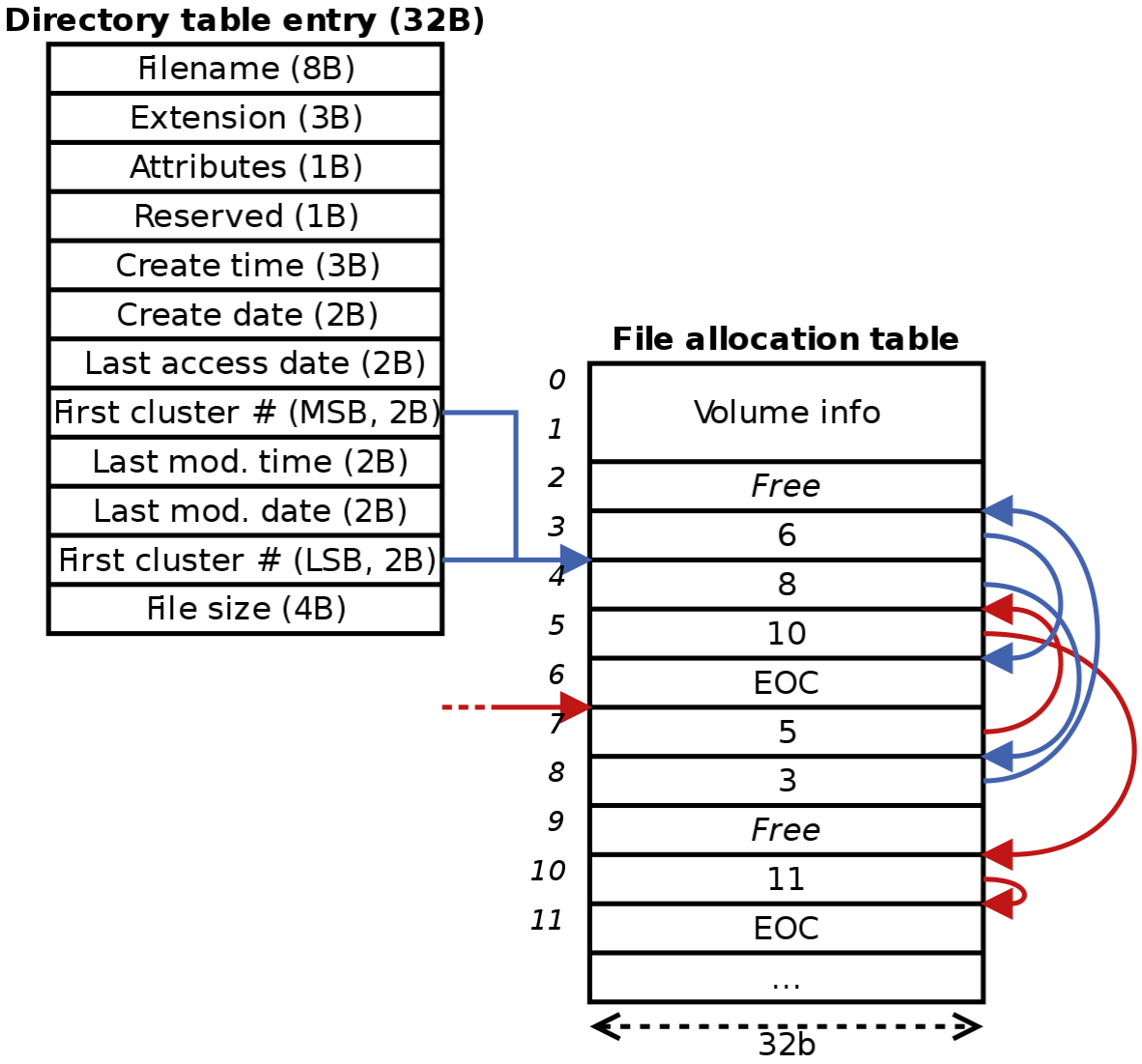
Offset from start	Length	Description
0x00	3 bytes	Part of the bootstrap program.
0x03	8 bytes	Optional manufacturer description.
0x0b	2 bytes	Number of bytes per block (almost always 512).
0x0d	1 byte	Number of blocks per allocation unit.
0x0e	2 bytes	Number of reserved blocks. This is the number of blocks on the disk that are not actually part of the file system; in most cases this is exactly 1, being the allowance for the boot block.
0x10	1 byte	Number of File Allocation Tables.
0x11	2 bytes	Number of root directory entries (including unused ones).
0x13	2 bytes	Total number of blocks in the entire disk. If the disk size is larger than 65535 blocks (and thus will not fit in these two bytes), this value is set to zero, and the true size is stored at offset 0x20.
0x15	1 byte	Media Descriptor. This is rarely used, but still exists. .
0x16	2 bytes	The number of blocks occupied by one copy of the File Allocation Table.
0x18	2 bytes	The number of blocks per track. This information is present primarily for the use of the bootstrap program, and need not concern us further here.
0x1a	2 bytes	The number of heads (disk surfaces). This information is present primarily for the use of the bootstrap program, and need not concern us further here.
0x1c	4 bytes	The number of *hidden blocks*. The use of this is largely historical, and it is nearly always set to 0; thus it can be ignored.
0x20	4 bytes	Total number of blocks in the entire disk (see also offset 0x13).
0x24	2 bytes	Physical drive number. This information is present primarily for the use of the bootstrap program, and need not concern us further here.
0x26	1 byte	Extended Boot Record Signature This information is present primarily for the use of the bootstrap program, and need not concern us further here.
0x27	4 bytes	Volume Serial Number. Unique number used for identification of a particular disk.
0x2b	11 bytes	Volume Label. This is a string of characters for human-readable identification of the disk (padded with spaces if shorter); it is selected when the disk is formatted.
0x36	8 bytes	File system identifier (padded at the end with spaces if shorter).
0x3e	0x1c0 bytes	The remainder of the bootstrap program.
0x1fe	2 bytes	Boot block 'signature' (0x55 followed by 0xaa).

The FAT occupies one or more blocks immediately following the boot block, part of its last block will remain unused, if there is a second FAT, this immediately follows the first block, but starting in a new block, this is repeated in any further FATS. On a hard drive there is usually only one FAT, a floppy disk can have several FATs. If a FAT is unreadable, files cannot be accessed, and another version/copy of the FAT must be used.

In the case of the 16-bit FAT file system, each entry in the FAT is two bytes in length (i.e. 16 bits). The disk data area is divided into clusters, which are the same thing as allocation units, but numbered differently (instead of being numbered from the start of the disk, they are numbered from the start of the disk data area). So, the cluster number is the allocation unit number, minus a constant value which is the size of the areas in between the start of the disk and the start of the data area.

There is only one entry in the FAT for every cluster aka data area block on the disk. Every N relates to a cluster N. Clusters 0 and 1 don't exist and those FAT entries are special. The Last cluster of a file has the value 0xffff in its FAT entry to indicate that there are no more clusters

FAT32 STRUCTURE PROVIDED BELOW



Part F:

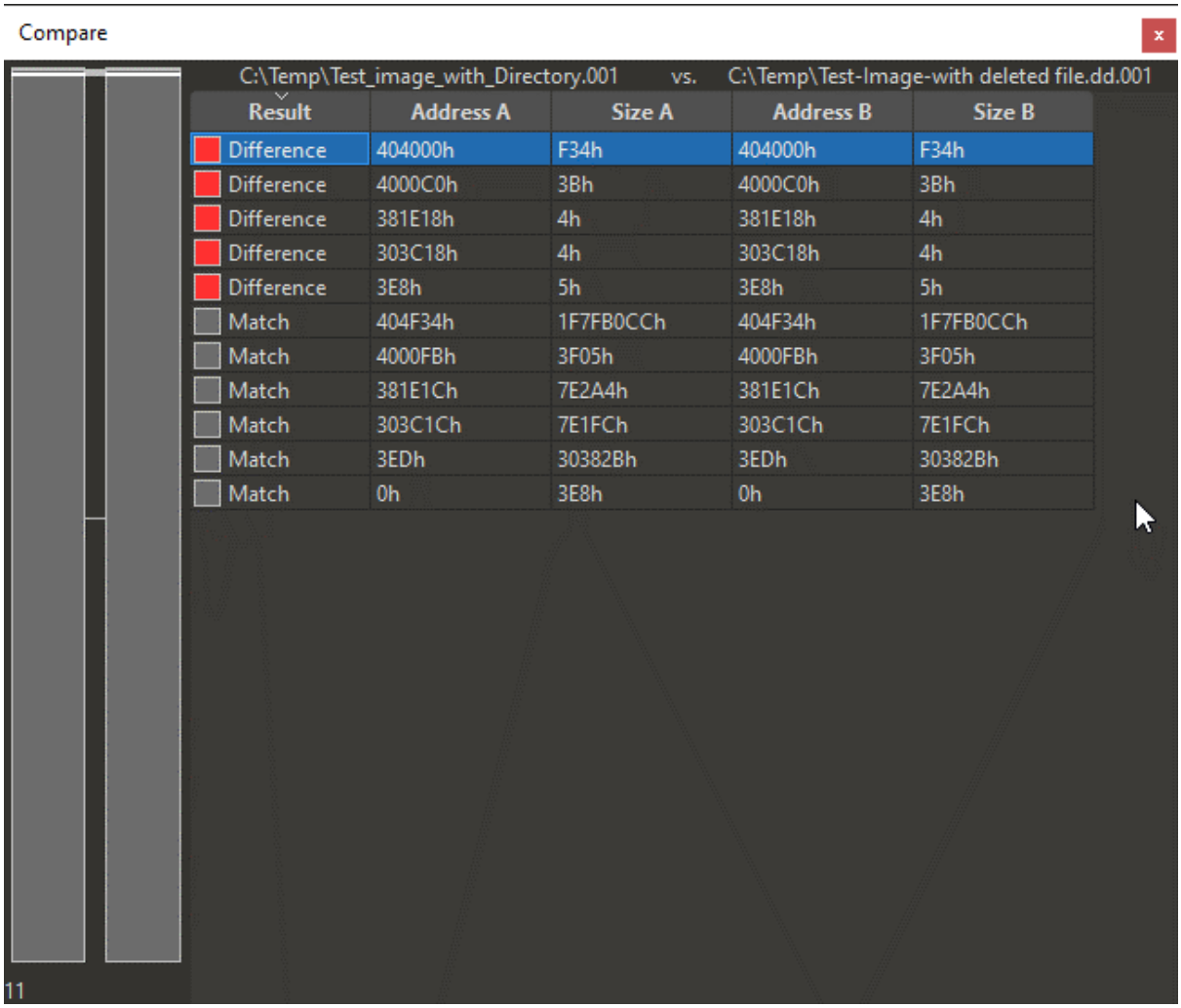
A. Image Name: Test-Image-with deleted file.dd.001

B. Hash Value:

MD5: ce2626a732d3457b860ed31bf5bedad0

SHA1: 21bfe0f40cde196c821973d2b025a201aabbe394

C. Storage Location: C:\TEMP\Test-Image-with deleted file.dd

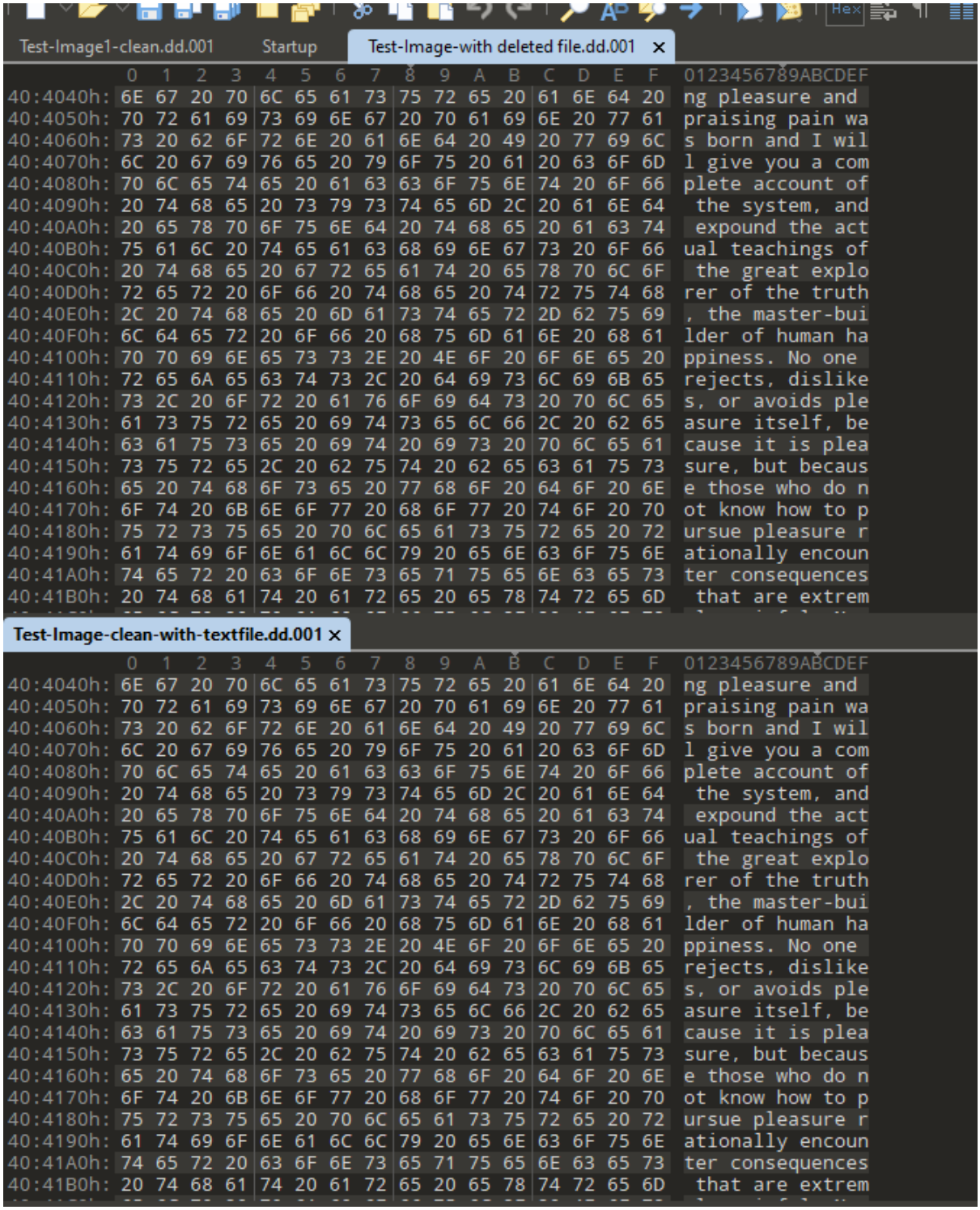


What happens when a file is deleted?

The MD5 sum has changed and is different to the original MD5 sum and the text remains from the deleted text file from the other image.

Can you still 'see' the text of the text file (are the contents of the text file still visible on the image?). Yes/no

Yes, the text of the text file is still visible on the image.


Test-Image1-clean.dd.001
Startup
Test-Image-with deleted file.dd.001
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
40:4040h: 6E 67 20 70 6C 65 61 73 75 72 65 20 61 6E 64 20 ng pleasure and
40:4050h: 70 72 61 69 73 69 6E 67 20 70 61 69 6E 20 77 61 praising pain wa
40:4060h: 73 20 62 6F 72 6E 20 61 6E 64 20 49 20 77 69 6C s born and I wil
40:4070h: 6C 20 67 69 76 65 20 79 6F 75 20 61 20 63 6F 6D l give you a com
40:4080h: 70 6C 65 74 65 20 61 63 63 6F 75 6E 74 20 6F 66 plete account of
40:4090h: 20 74 68 65 20 73 79 73 74 65 6D 2C 20 61 6E 64 the system, and
40:40A0h: 20 65 78 70 6F 75 6E 64 20 74 68 65 20 61 63 74 expound the act
40:40B0h: 75 61 6C 20 74 65 61 63 68 69 6E 67 73 20 6F 66 ual teachings of
40:40C0h: 20 74 68 65 20 67 72 65 61 74 20 65 78 70 6C 6F the great explo
40:40D0h: 72 65 72 20 6F 66 20 74 68 65 20 74 72 75 74 68 rer of the truth
40:40E0h: 2C 20 74 68 65 20 6D 61 73 74 65 72 2D 62 75 69 , the master-bui
40:40F0h: 6C 64 65 72 20 6F 66 20 68 75 6D 61 6E 20 68 61 lder of human ha
40:4100h: 70 70 69 6E 65 73 73 2E 20 4E 6F 20 6F 6E 65 20 ppiness. No one
40:4110h: 72 65 6A 65 63 74 73 2C 20 64 69 73 6C 69 6B 65 rejects, dislike
40:4120h: 73 2C 20 6F 72 20 61 76 6F 69 64 73 20 70 6C 65 s, or avoids ple
40:4130h: 61 73 75 72 65 20 69 74 73 65 6C 66 2C 20 62 65 asure itself, be
40:4140h: 63 61 75 73 65 20 69 74 20 69 73 20 70 6C 65 61 cause it is plea
40:4150h: 73 75 72 65 2C 20 62 75 74 20 62 65 63 61 75 73 sure, but becaus
40:4160h: 65 20 74 68 6F 73 65 20 77 68 6F 20 64 6F 20 6E e those who do n
40:4170h: 6F 74 20 6B 6E 6F 77 20 68 6F 77 20 74 6F 20 70 ot know how to p
40:4180h: 75 72 73 75 65 20 70 6C 65 61 73 75 72 65 20 72 ursue pleasure r
40:4190h: 61 74 69 6F 6E 61 6C 6C 79 20 65 6E 63 6F 75 6E ationally encoun
40:41A0h: 74 65 72 20 63 6F 6E 73 65 71 75 65 6E 63 65 73 ter consequences
40:41B0h: 20 74 68 61 74 20 61 72 65 20 65 78 74 72 65 6D that are extrem
Test-Image-clean-with-textfile.dd.001
0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
40:4040h: 6E 67 20 70 6C 65 61 73 75 72 65 20 61 6E 64 20 ng pleasure and
40:4050h: 70 72 61 69 73 69 6E 67 20 70 61 69 6E 20 77 61 praising pain wa
40:4060h: 73 20 62 6F 72 6E 20 61 6E 64 20 49 20 77 69 6C s born and I wil
40:4070h: 6C 20 67 69 76 65 20 79 6F 75 20 61 20 63 6F 6D l give you a com
40:4080h: 70 6C 65 74 65 20 61 63 63 6F 75 6E 74 20 6F 66 plete account of
40:4090h: 20 74 68 65 20 73 79 73 74 65 6D 2C 20 61 6E 64 the system, and
40:40A0h: 20 65 78 70 6F 75 6E 64 20 74 68 65 20 61 63 74 expound the act
40:40B0h: 75 61 6C 20 74 65 61 63 68 69 6E 67 73 20 6F 66 ual teachings of
40:40C0h: 20 74 68 65 20 67 72 65 61 74 20 65 78 70 6C 6F the great explo
40:40D0h: 72 65 72 20 6F 66 20 74 68 65 20 74 72 75 74 68 rer of the truth
40:40E0h: 2C 20 74 68 65 20 6D 61 73 74 65 72 2D 62 75 69 , the master-bui
40:40F0h: 6C 64 65 72 20 6F 66 20 68 75 6D 61 6E 20 68 61 lder of human ha
40:4100h: 70 70 69 6E 65 73 73 2E 20 4E 6F 20 6F 6E 65 20 ppiness. No one
40:4110h: 72 65 6A 65 63 74 73 2C 20 64 69 73 6C 69 6B 65 rejects, dislike
40:4120h: 73 2C 20 6F 72 20 61 76 6F 69 64 73 20 70 6C 65 s, or avoids ple
40:4130h: 61 73 75 72 65 20 69 74 73 65 6C 66 2C 20 62 65 asure itself, be
40:4140h: 63 61 75 73 65 20 69 74 20 69 73 20 70 6C 65 61 cause it is plea
40:4150h: 73 75 72 65 2C 20 62 75 74 20 62 65 63 61 75 73 sure, but becaus
40:4160h: 65 20 74 68 6F 73 65 20 77 68 6F 20 64 6F 20 6E e those who do n
40:4170h: 6F 74 20 6B 6E 6F 77 20 68 6F 77 20 74 6F 20 70 ot know how to p
40:4180h: 75 72 73 75 65 20 70 6C 65 61 73 75 72 65 20 72 ursue pleasure r
40:4190h: 61 74 69 6F 6E 61 6C 6C 79 20 65 6E 63 6F 75 6E ationally encoun
40:41A0h: 74 65 72 20 63 6F 6E 73 65 71 75 65 6E 63 65 73 ter consequences
40:41B0h: 20 74 68 61 74 20 61 72 65 20 65 78 74 72 65 6D that are extrem

Part G:

A. Image Name: Test_image_with_Directory.dd.001

B. Hash Value:

MD5: ce2626a732d3457b860ed31bf5bedad0

SHA1: 5dd27e771db73ad14dbb37af9f76189bb65137b4

C. Storage Location: C:\TEMP\Test_image_with_Directory.dd

Part 2:

A. Image Name: Test_image_with_Directory_Deleted.dd.001

B. Hash Value:

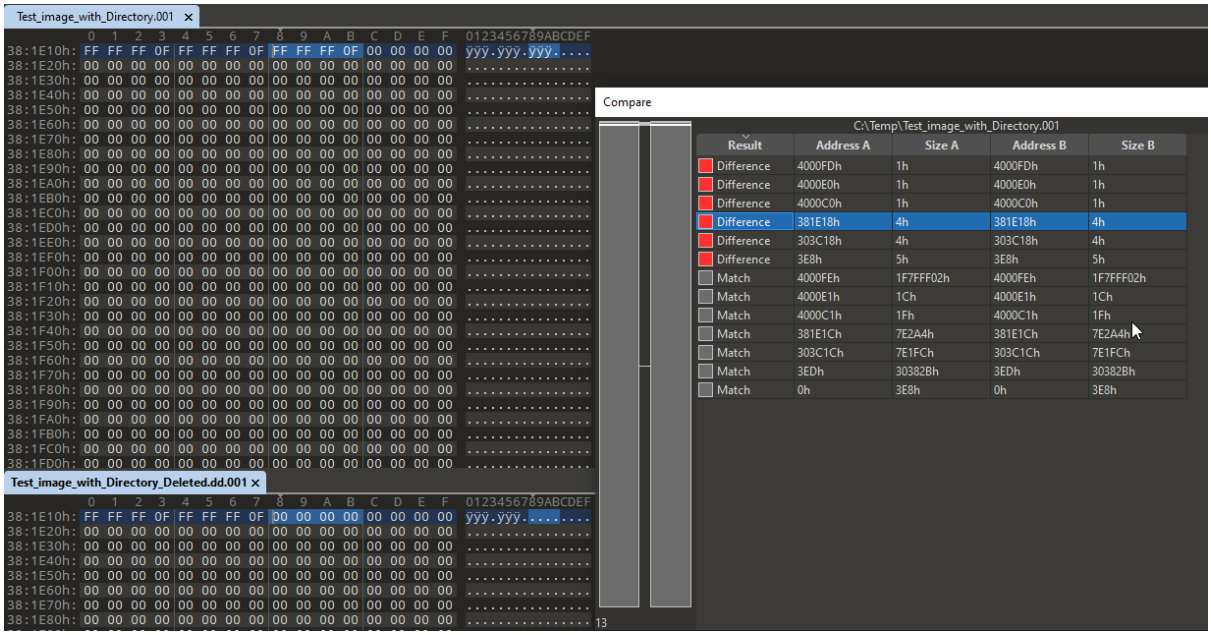
MD5: 735f984e95cda21c4f9c0b2085a86a69

SHA1: 7c724c88ba916a073b72e6ec81744fd8f18e7cd5

C. Storage Location: C:\TEMP\ Test_image_with_Directory_Deleted.dd

C:\Temp\Test_image_with_Directory.001

Result	Address A	Size A	Address B	Size B
Only in B			4000FDh	1h
Only in B			3FFFFCh	4h
Only in B			381DFCh	4h
Only in A	400FFFh	1h		
Only in A	381E08h	4h		
Only in A	303C18h	4h		
Difference	4000E0h	1h	4000E0h	1h
Difference	4000C0h	1h	4000C0h	1h
Difference	3E8h	5h	3E8h	5h
Match	401000h	1F7FF000h	401000h	1F7FF000h
Match	4000FDh	F02h	4000FEh	F02h
Match	4000E1h	1Ch	4000E1h	1Ch
Match	4000C1h	1Fh	4000C1h	1Fh
Match	400000h	C0h	400000h	C0h
Match	381E0Ch	7E1F4h	381E08h	7E1F4h
Match	381E00h	8h	381E00h	8h
Match	303C1Ch	7E1E4h	303C18h	7E1E4h
Match	3EDh	30382Bh	3EDh	30382Bh
Match	0h	3E8h	0h	3E8h



What happens when a Directory is deleted?

The folder/Directory isn't completely gone it just leaves an earmark of the space the file takes up on your usb as vacant.

Part H:

A. Image Name: Test_image_with_Saved_Word_File.dd.001

B. Hash Value:

MD5: 8705f844e712fd256f51dca6958c9284

SHA1: 4777199e8dde7d7ad0f19e3aa37cf0f0524aa4ed

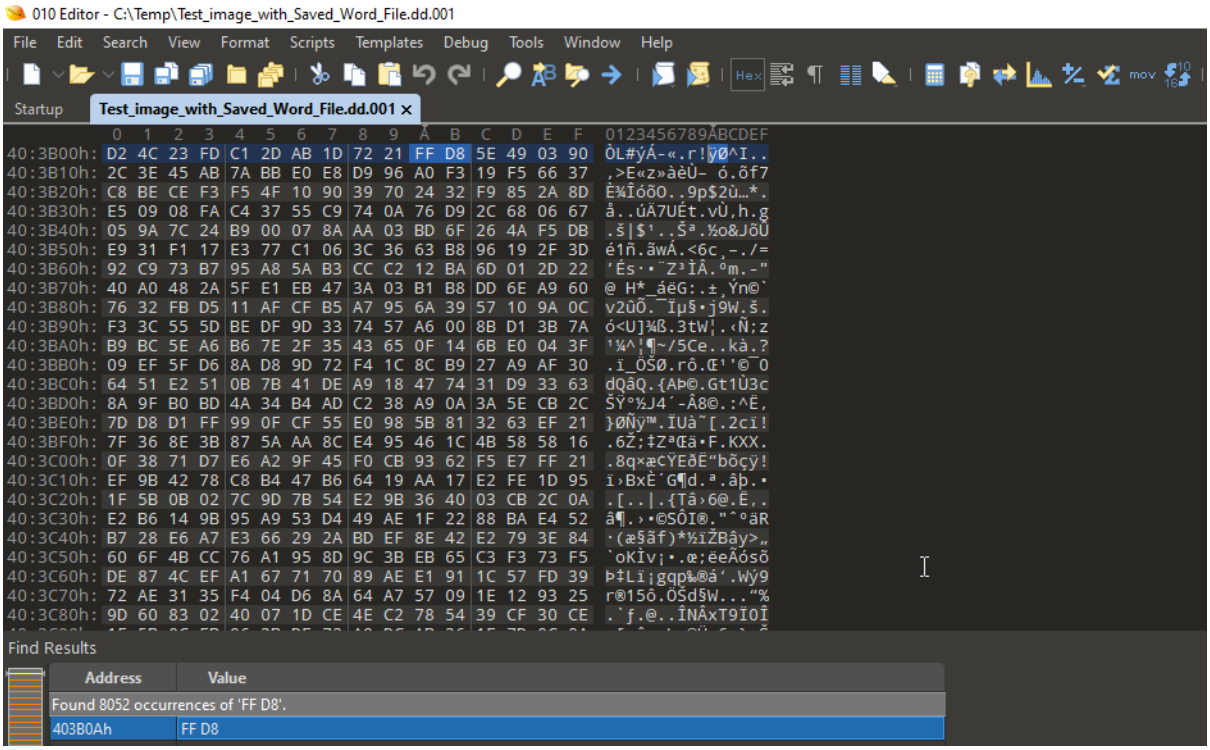
C. Storage Location: C:\TEMP\ Test_image_with_Saved_Word_File.dd

Find the start and end magic numbers associated with a jpeg file.

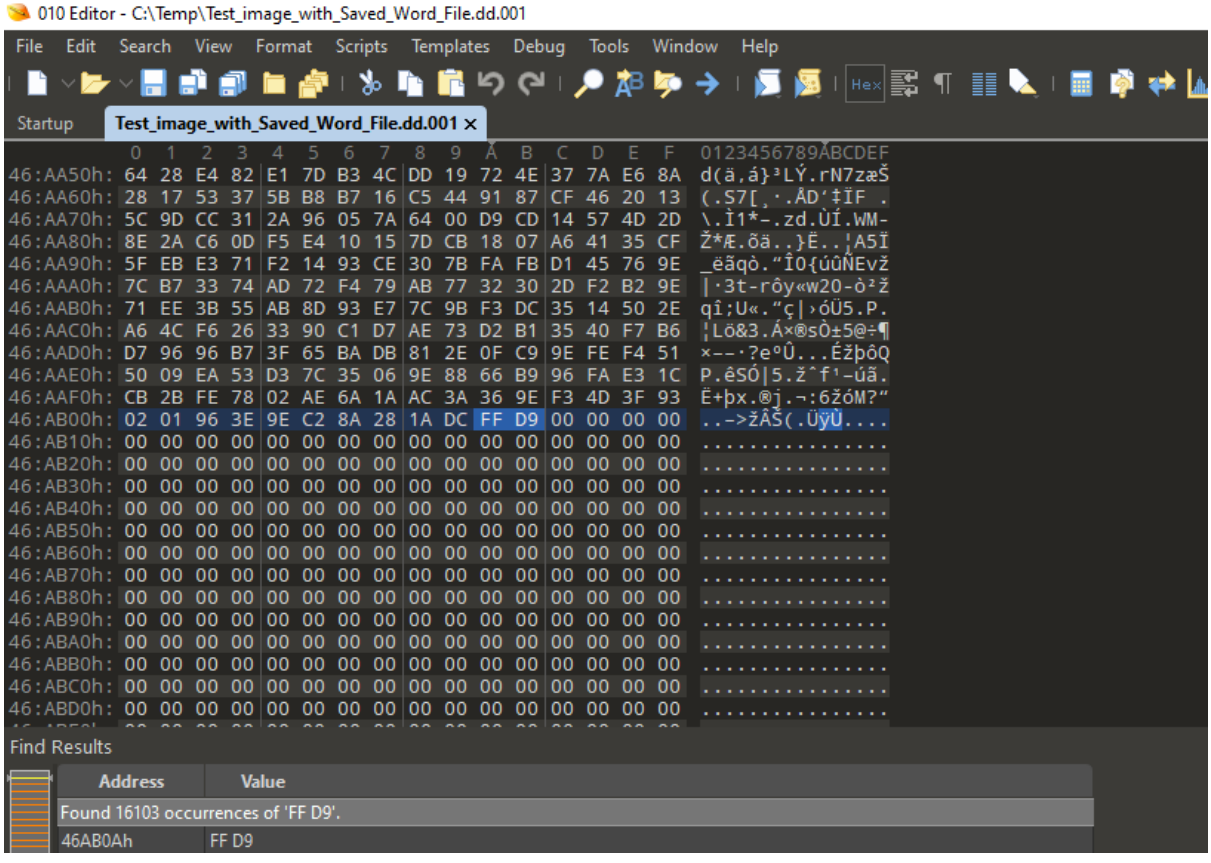
Start: FF D8

End: FF D9

Using the start magic number, find the beginning of the jpeg File



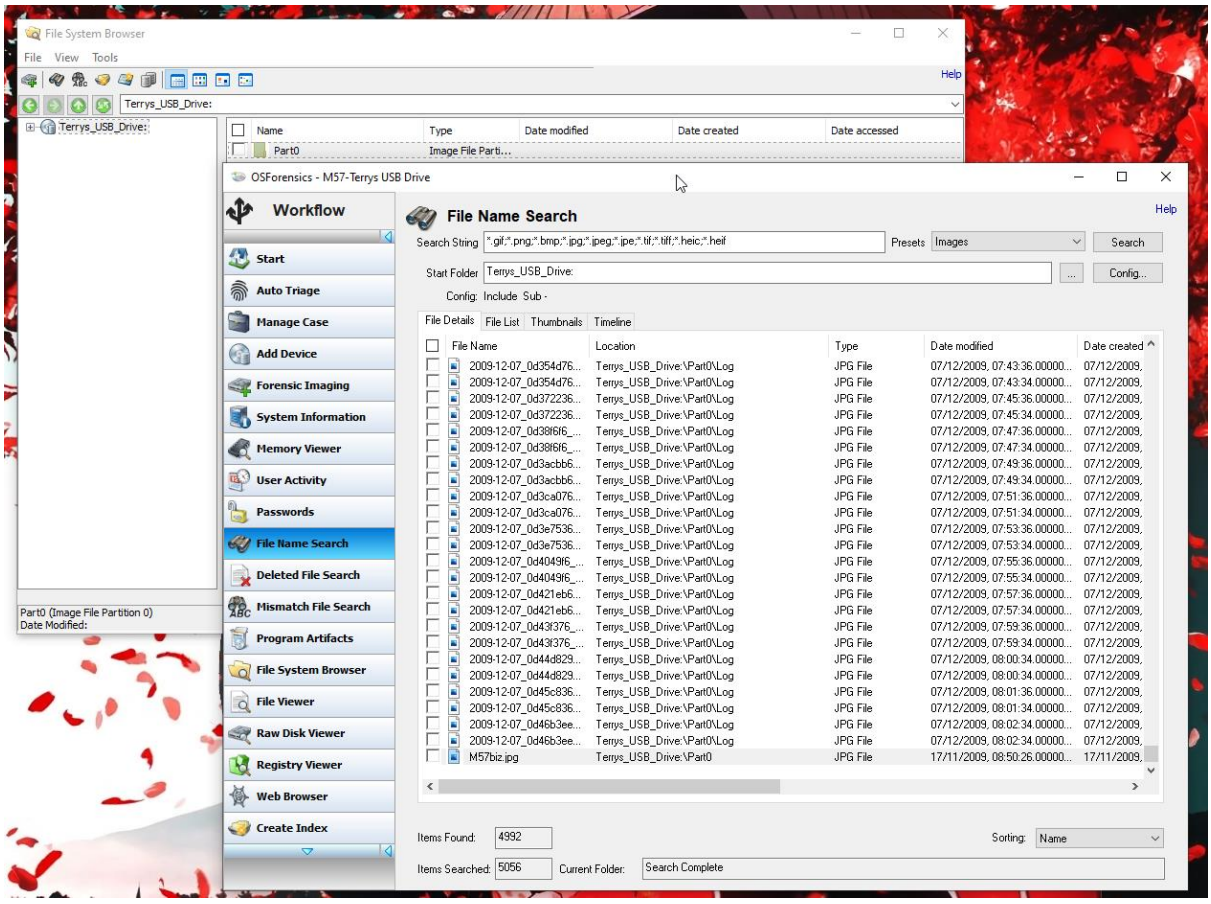
Using the End magic number, find the end of the jpeg image file.



What is the sector number and the memory offset to the start of the JPEG file? Log the information in the following table:

Starting Sector	Ending Sector	Observed data	Date and Time	Signature
403B0Ah	46AB0Ah		30/10/2021	Stephen Duffy
Starting Offset	Ending Offset		30/10/2021	Stephen Duffy
0xFFD8	0xFFD9		30/10/2021	Stephen Duffy

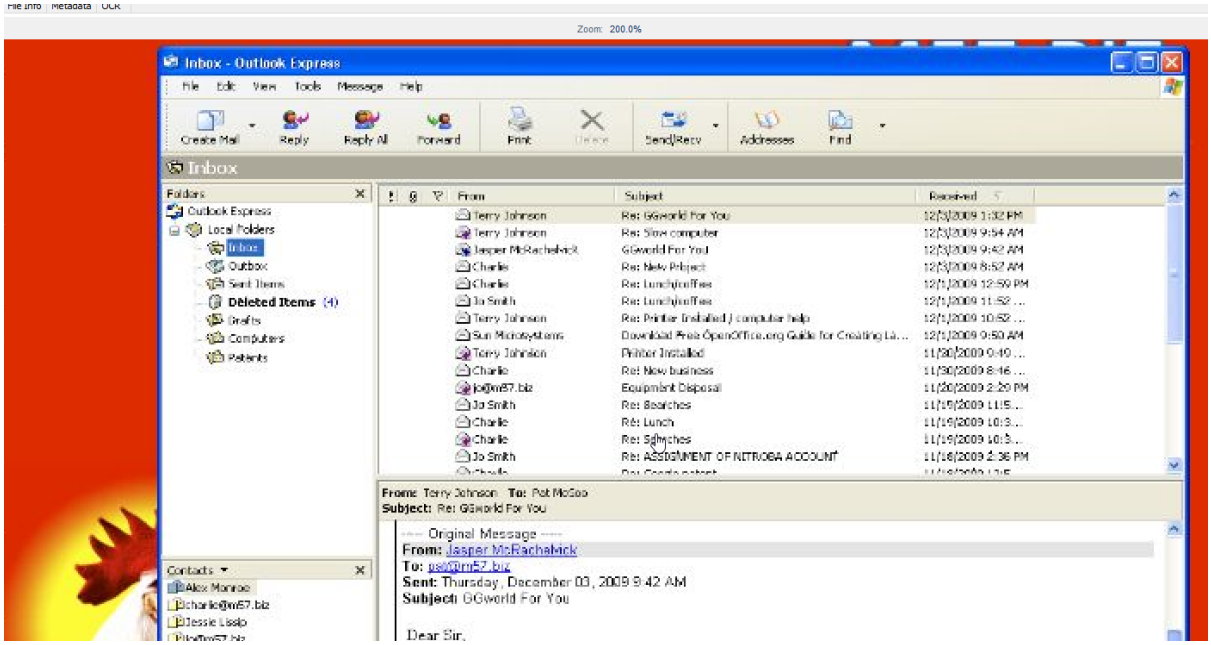
Part I:

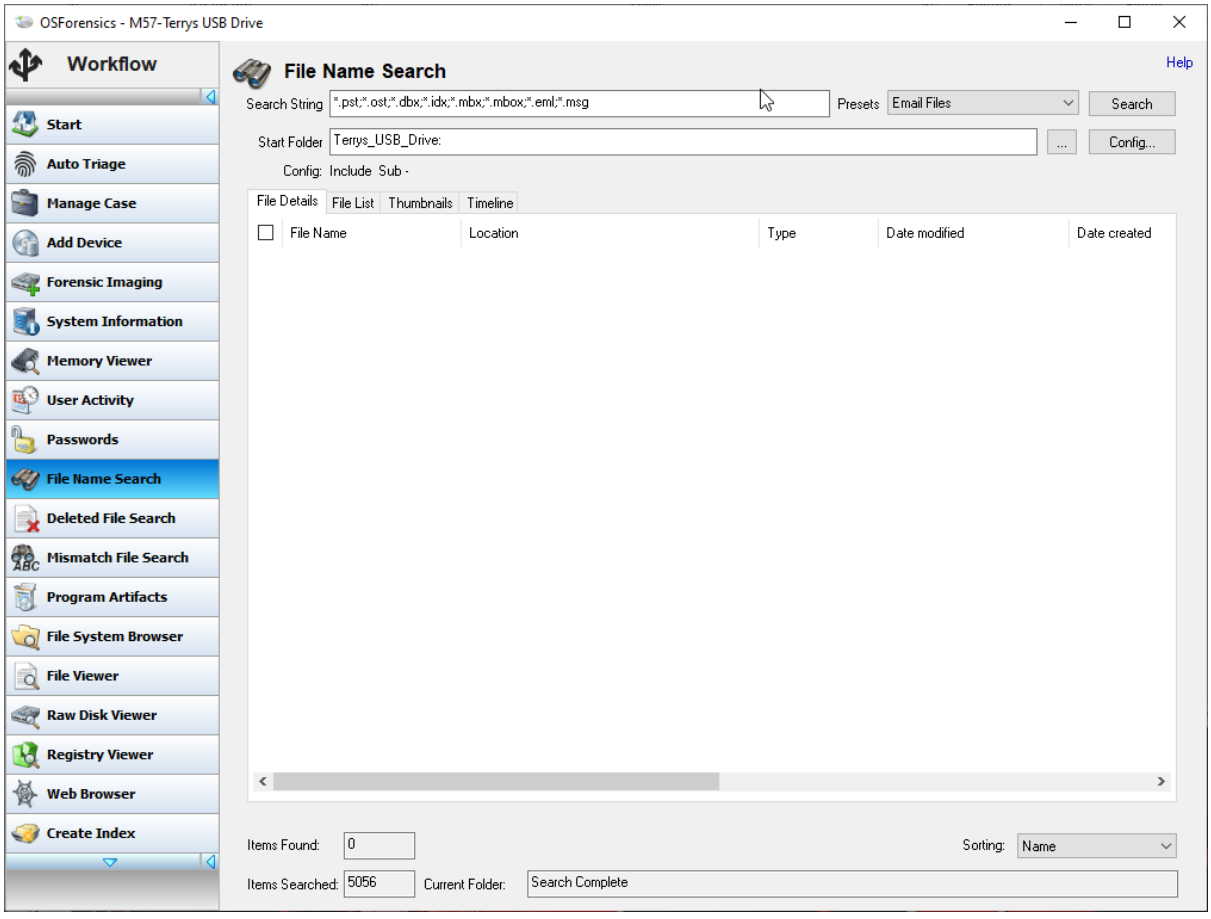


(Sorry if any of Terry's Evidence pictures are blurry they were all really bad quality for me)

Has Terry sent any emails? Document the emails.

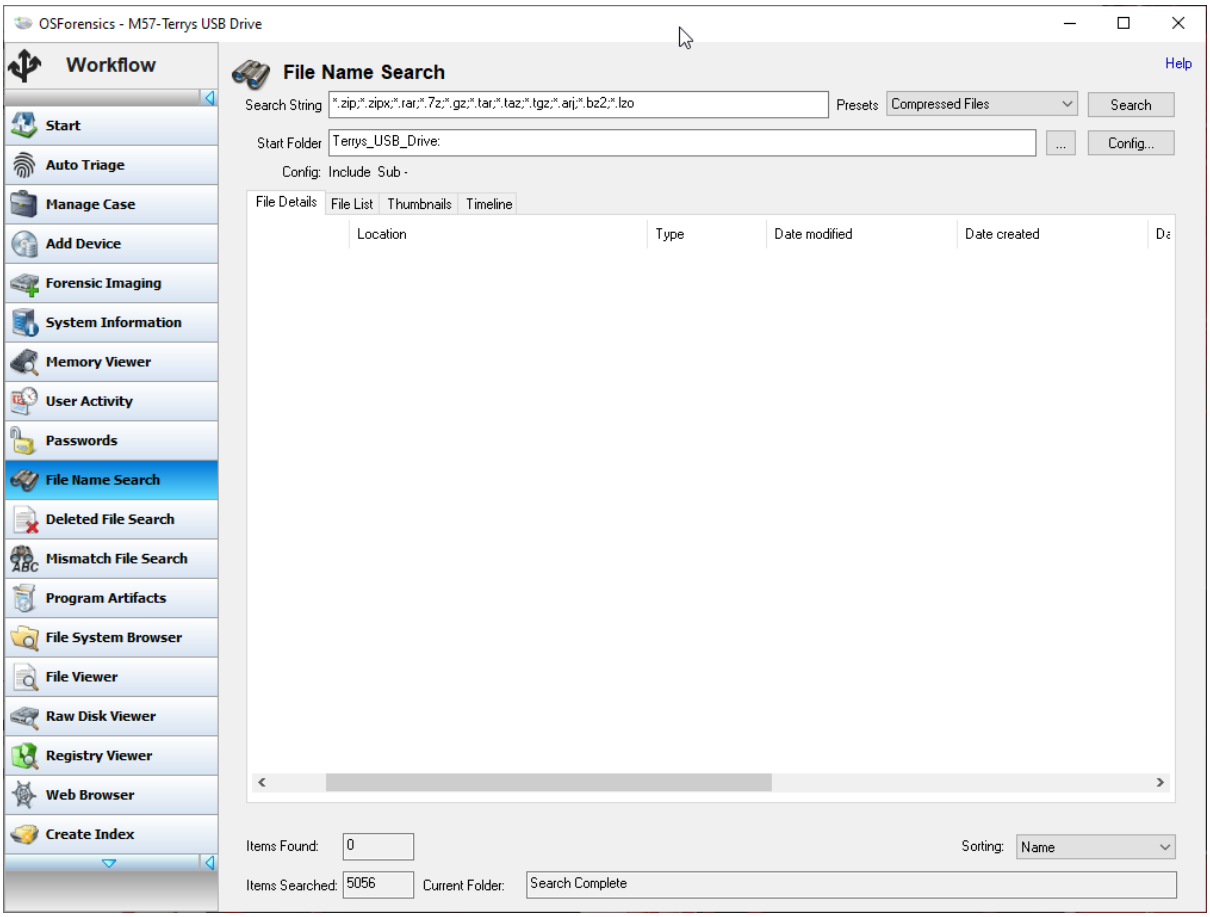
Terry has not sent any emails that we can find but there is images of him sending/receiving emails.





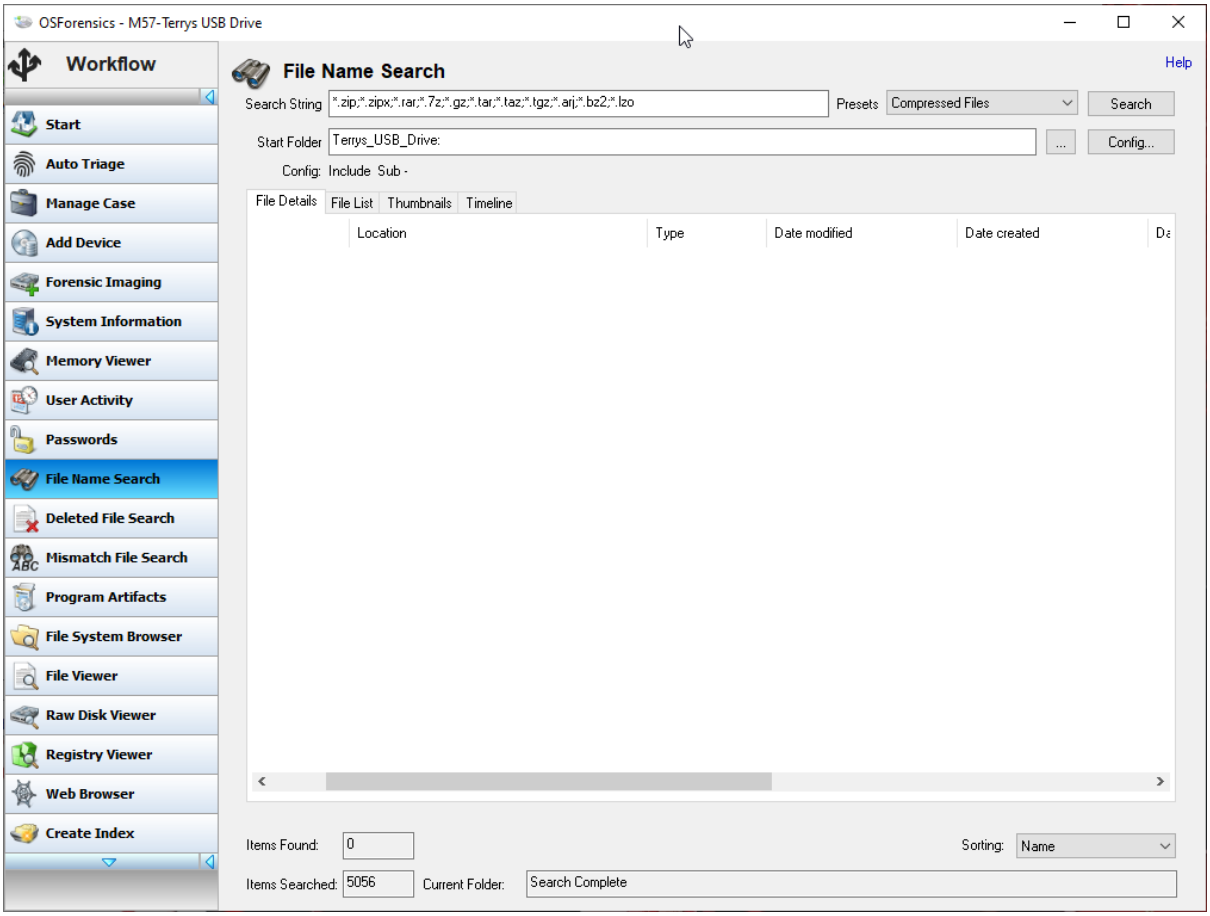
Has he been using zip files? Document the Zip files (file size, ownership, metadata)

He had not been using any Zip Files from what I have found

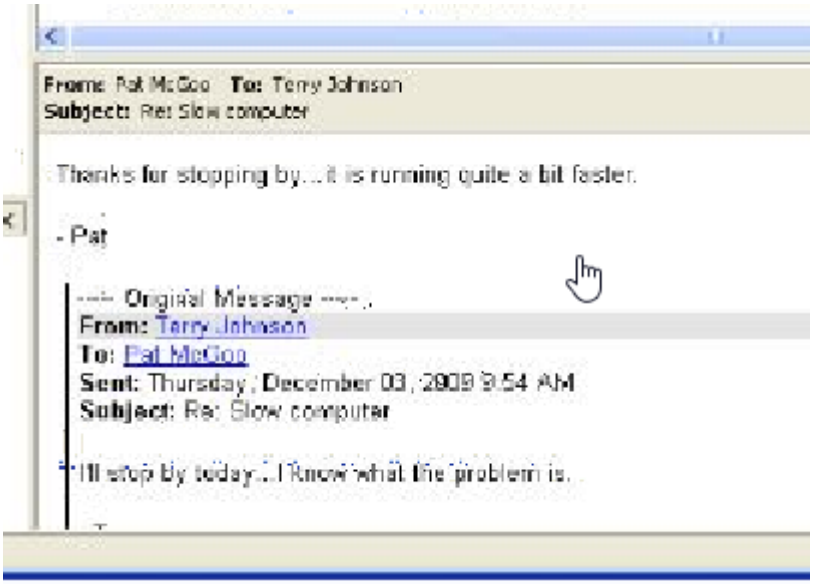


Are there any Office or Open Office documents? Document the evidence.

There was no office or open office documents on the evidence drive

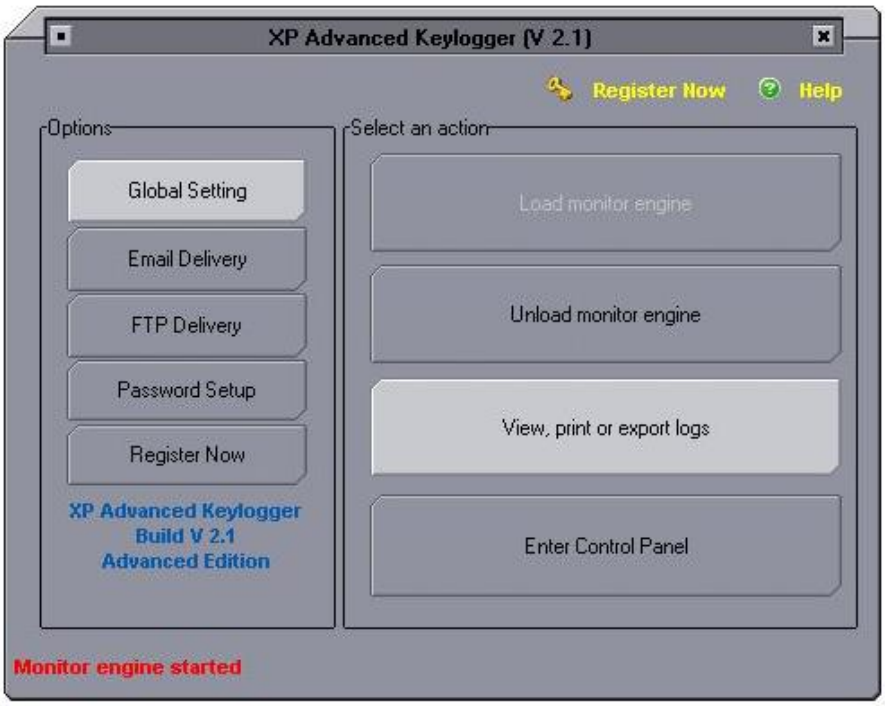


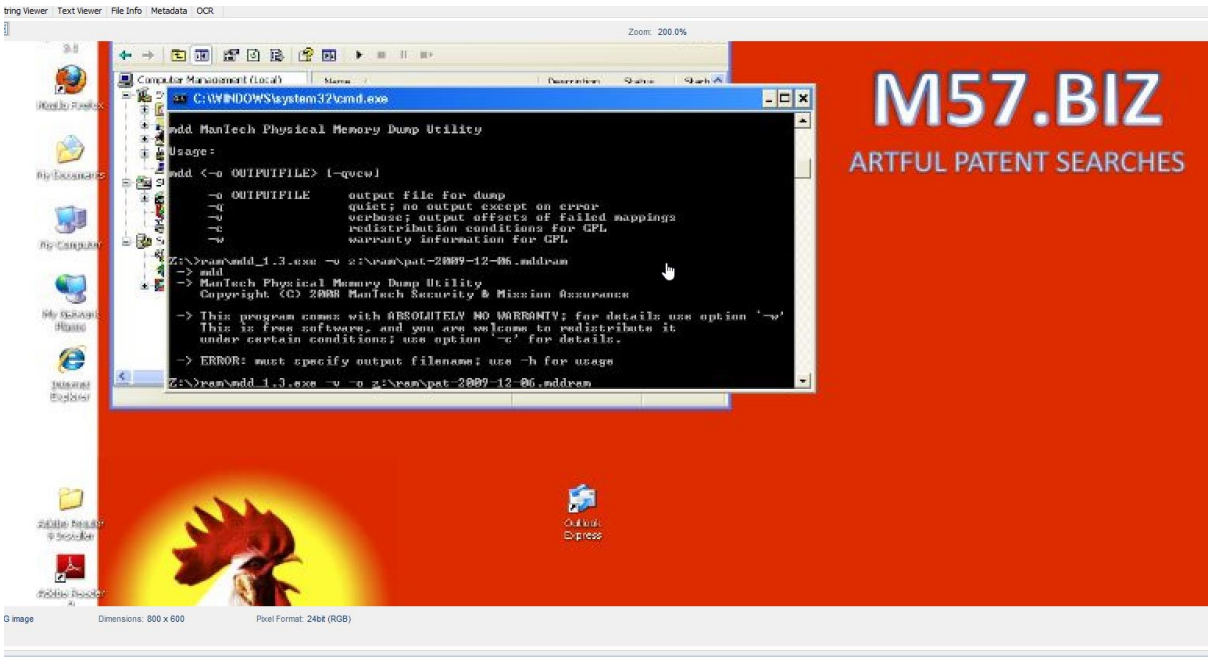
Are there any images that showing any illicit business? Document thoroughly.

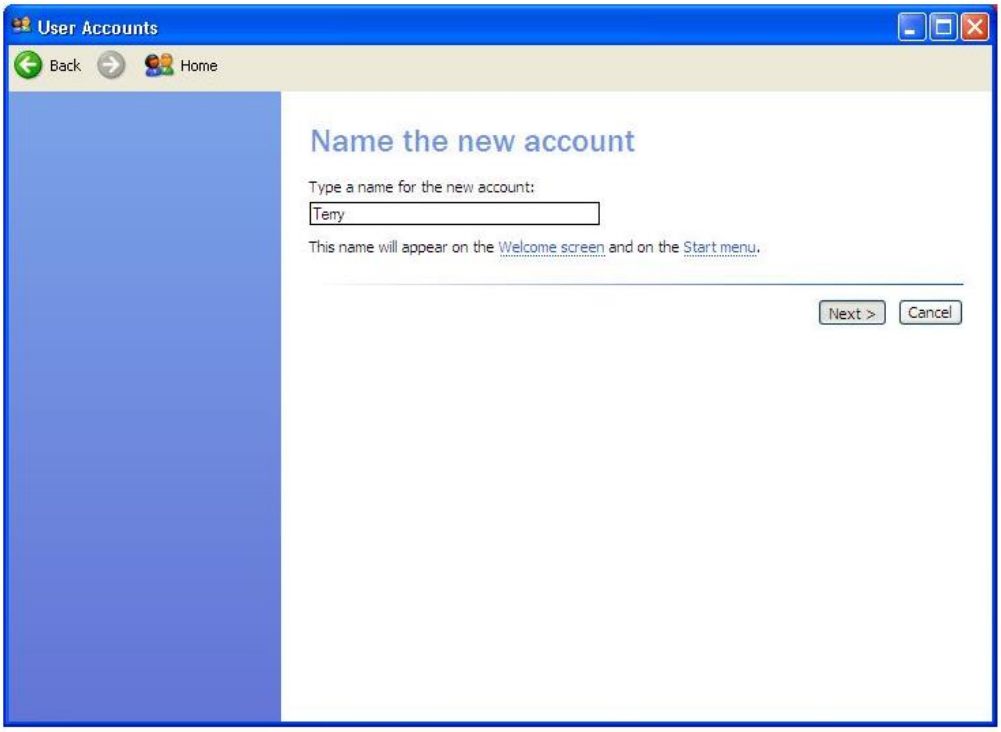


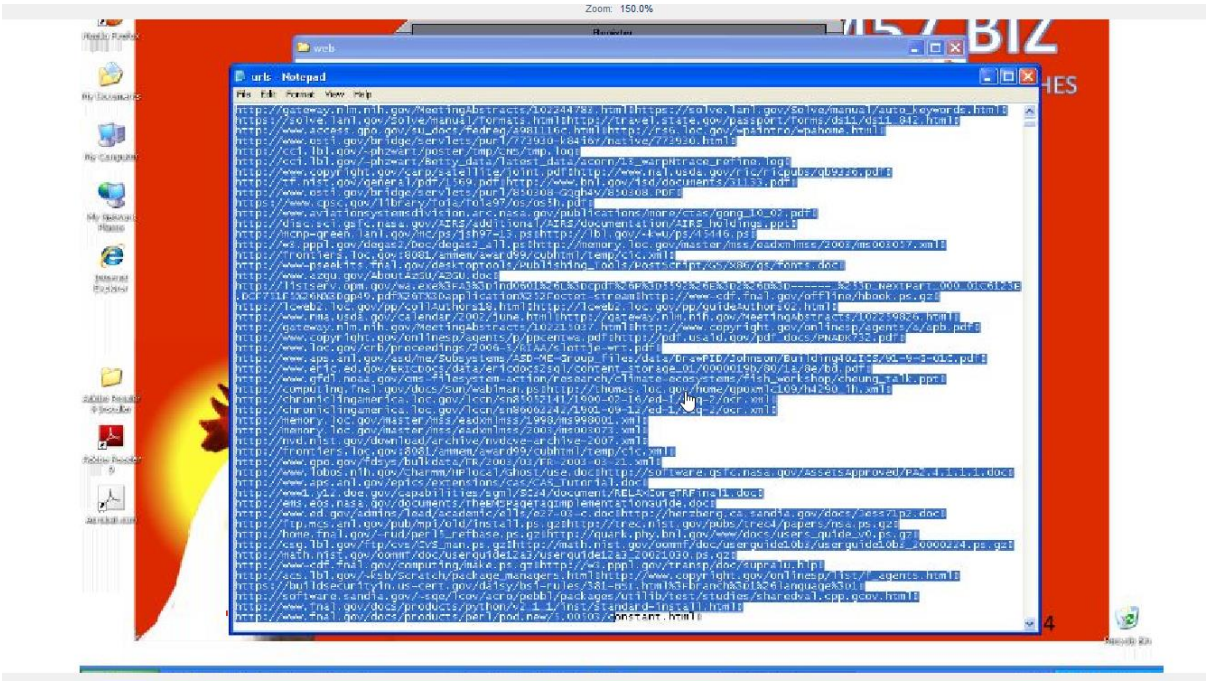
Using Keylogger:

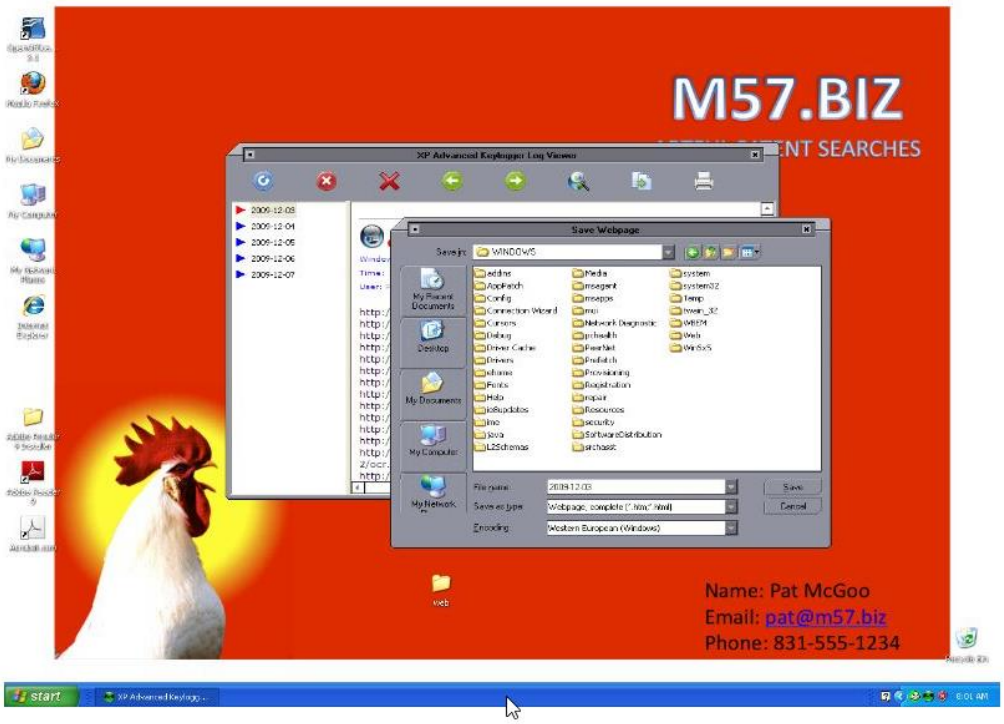

Register
Thank you for evaluating XP Advanced Keylogger!
XP Advanced Keylogger is not free. You can evaluate it before you buy it. The trial period is 5 days. It will no longer work after it is expired. To continue using it, you have to purchase it.
To purchase the program please click Purchase Online or click Continue Evaluation to access the trial version.
Registered users please click Enter Registration Code, then provide your registration and license information to activate the full version.
Unregistered - 5 days of trial period left.
Purchase Online
Enter Registration Code
Exit
Continue Evaluation
Express


XP Advanced Keylogger (V 2.1)
Register Now
Help
Options
Global Setting
Email Delivery
FTP Delivery
Password Setup
Register Now
XP Advanced Keylogger
Build V 2.1
Advanced Edition
Select an action
Load monitor engine
Unload monitor engine
View, print or export logs
Enter Control Panel
Monitor engine started


tring Viewer
Text Viewer
File Info
Metadata
OCR
Zoom: 200.0%
C:\WINDOWS\system32\cmd.exe
mdd ManTech Physical Memory Dump Utility
Usage:
mdd <-o OUTPUTFILE> [-qvcw]
-o OUTPUTFILE output file for dump
-q quiet; no output except on error
-v verbose; output offsets of failed mappings
-c redistribution conditions for GPL
-w warranty information for GPL
Z:\>ram\mdd_1.3.exe -v z:\ram\pat-2009-12-06.mddram
-> mdd
-> ManTech Physical Memory Dump Utility
Copyright (C) 2008 ManTech Security & Mission Assurance
-> This program comes with ABSOLUTELY NO WARRANTY; for details use option '-w'
This is free software, and you are welcome to redistribute it
under certain conditions; use option '-c' for details.
-> ERROR: must specify output filename; use -h for usage
Z:\>ram\mdd_1.3.exe -v -o z:\ram\pat-2009-12-06.mddram
M57.BIZ
ARTFUL PATENT SEARCHES
G image
Dimensions: 800 x 600
Pixel Format: 24bit (RGB)


User Accounts
Back
Home
Name the new account
Type a name for the new account:
Terry
This name will appear on the Welcome screen and on the Start menu.
Next >
Cancel


Zoom: 150.0%
urls - Notepad
File Edit Format View Help


M57.BIZ
XP Advanced Keylogger Log Viewer
Save Webpage
Name: Pat McGoo
Email: pat@m57.biz
Phone: 831-555-1234

Zoom: 56.7%

M57.BIZ

ARTFUL PATENT SEARCHES

Name: Pat McGoo
Email: pat@m57.biz
Phone: 831-555-1234