Mid-Term Exam

Due Sep 30 at 11:59pm **Points** 200 **Questions** 22 **Time Limit** None

Instructions

This exam covers the topics discussed in the first 6 sessions of the course. You may access your notes, course videos, course presentations, and the Internet during this exam. **The only restriction is that you may not work with others on this assignment**. The exam will be released on Wednesday 28 September and will be due by Friday 30 September before 11:59 pm. Please contact me on Discord if you have any questions while taking the exam.

The files you will need for the exam are located on Canvas under Files > Mid Term Files. You will need to unzip those files to use them.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	131 minutes	200 out of 200

Correct answers are hidden.

Score for this quiz: **200** out of 200
Submitted Sep 29 at 10:36am
This attempt took 131 minutes.

Question 1 **5 / 5 pts**

Which of the following is not a step in the digital forensics investigative process?

○ Identify

○ Examine

○ Preserve

○ Collect

○ Present

● Detect

Question 2 **5 / 5 pts**

Out of the items listed, what is the most volatile from an evidence collection perspective?

○ Swap Space

○ Network Topology

● Process Tables

○ Remote Logging

Question 3 **18 / 18 pts**

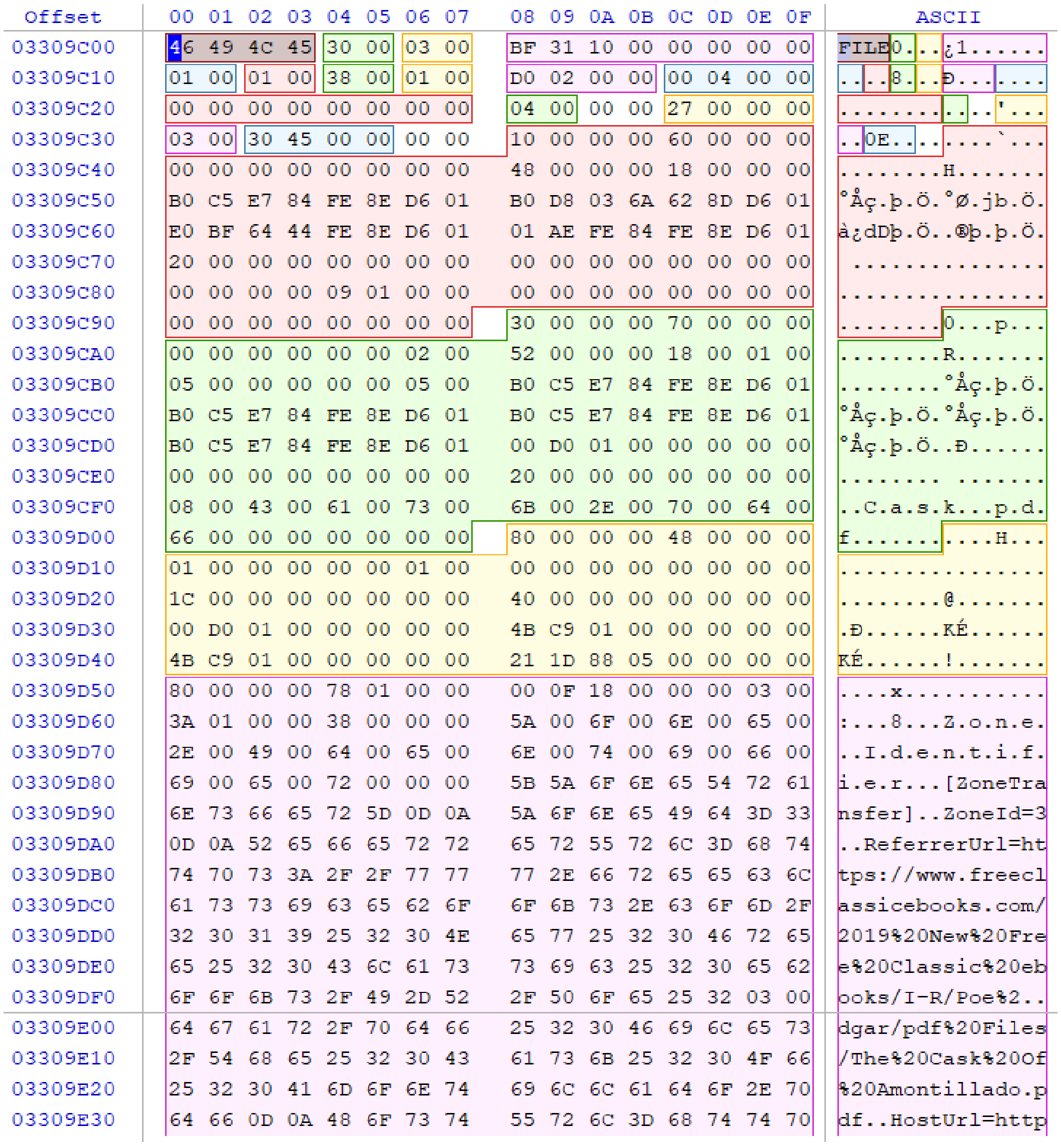
During a forensics analysis you are given a disk image named fat16.dd which contains a single FAT16 partition. Answer the following questions about the FAT16 partition.

How many bytes per sector are specified in the boot sector?	512
How many file allocation tables are contained in the partition?	2
How many sectors are contained within each file allocation table?	200
How many sectors are in the FAT16 partition?	204798
How many sectors per cluster are specified in the boot sector?	4
Counting from the start of the partition, what sector does the root directory start at?	404

Question 4

5 / 5 pts

Based on MFT entry shown below, specify the size of the file in bytes.



```
Offset     00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F        ASCII
03309C00   46 49 4C 45 30 00 03 00  BF 31 10 00 00 00 00 00   FILE0...¿1......
03309C10   01 00 01 00 38 00 01 00  D0 02 00 00 00 04 00 00   ....8...Ð.......
03309C20   00 00 00 00 00 00 00 00  04 00 00 00 27 00 00 00   ............'...
03309C30   03 00 30 45 00 00 00 00  10 00 00 00 60 00 00 00   ..0E........`...
03309C40   00 00 00 00 00 00 00 00  48 00 00 00 18 00 00 00   ........H.......
03309C50   B0 C5 E7 84 FE 8E D6 01  B0 D8 03 6A 62 8D D6 01   °Åç.þ.Ö.°Ø.jb.Ö.
03309C60   E0 BF 64 44 FE 8E D6 01  01 AE FE 84 FE 8E D6 01   à¿dDþ.Ö..®þ.þ.Ö.
03309C70   20 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    ...............
03309C80   00 00 00 00 09 01 00 00  00 00 00 00 00 00 00 00   ................
03309C90   00 00 00 00 00 00 00 00  30 00 00 00 70 00 00 00   ........0...p...
03309CA0   00 00 00 00 00 00 02 00  52 00 00 00 18 00 01 00   ........R.......
03309CB0   05 00 00 00 00 00 05 00  B0 C5 E7 84 FE 8E D6 01   ........°Åç.þ.Ö.
03309CC0   B0 C5 E7 84 FE 8E D6 01  B0 C5 E7 84 FE 8E D6 01   °Åç.þ.Ö.°Åç.þ.Ö.
03309CD0   B0 C5 E7 84 FE 8E D6 01  00 D0 01 00 00 00 00 00   °Åç.þ.Ö..Ð......
03309CE0   00 00 00 00 00 00 00 00  20 00 00 00 00 00 00 00   ........ .......
03309CF0   08 00 43 00 61 00 73 00  6B 00 2E 00 70 00 64 00   ..C.a.s.k...p.d.
03309D00   66 00 00 00 00 00 00 00  80 00 00 00 48 00 00 00   f...........H...
03309D10   01 00 00 00 00 00 01 00  00 00 00 00 00 00 00 00   ................
03309D20   1C 00 00 00 00 00 00 00  40 00 00 00 00 00 00 00   ........@.......
03309D30   00 D0 01 00 00 00 00 00  4B C9 01 00 00 00 00 00   .Ð......KÉ......
03309D40   4B C9 01 00 00 00 00 00  21 1D 88 05 00 00 00 00   KÉ......!.......
03309D50   80 00 00 00 78 01 00 00  00 0F 18 00 00 00 03 00   ....x...........
03309D60   3A 01 00 00 38 00 00 00  5A 00 6F 00 6E 00 65 00   :...8...Z.o.n.e.
03309D70   2E 00 49 00 64 00 65 00  6E 00 74 00 69 00 66 00   ..I.d.e.n.t.i.f.
03309D80   69 00 65 00 72 00 00 00  5B 5A 6F 6E 65 54 72 61   i.e.r...[ZoneTra
03309D90   6E 73 66 65 72 5D 0D 0A  5A 6F 6E 65 49 64 3D 33   nsfer]..ZoneId=3
03309DA0   0D 0A 52 65 66 65 72 72  65 72 55 72 6C 3D 68 74   ..ReferrerUrl=ht
03309DB0   74 70 73 3A 2F 2F 77 77  77 2E 66 72 65 65 63 6C   tps://www.freecl
03309DC0   61 73 73 69 63 65 62 6F  6F 6B 73 2E 63 6F 6D 2F   assicebooks.com/
03309DD0   32 30 31 39 25 32 30 4E  65 77 25 32 30 46 72 65   2019%20New%20Fre
03309DE0   65 25 32 30 43 6C 61 73  73 69 63 25 32 30 65 62   e%20Classic%20eb
03309DF0   6F 6F 6B 73 2F 49 2D 52  2F 50 6F 65 25 32 03 00   ooks/I-R/Poe%2..
03309E00   64 67 61 72 2F 70 64 66  25 32 30 46 69 6C 65 73   dgar/pdf%20Files
03309E10   2F 54 68 65 25 32 30 43  61 73 6B 25 32 30 4F 66   /The%20Cask%20Of
03309E20   25 32 30 41 6D 6F 6E 74  69 6C 6C 61 64 6F 2E 70   %20Amontillado.p
03309E30   64 66 0D 0A 48 6F 73 74  55 72 6C 3D 68 74 74 70   df..HostUrl=http
```

117067

Question 5

5 / 5 pts

What is the name of the security principle that "holds that the perpetrator of a crime will bring something into the crime scene and leave with something from it, and that both can be used as forensic evidence."

○ Cross Contamination Principle

● Locard’s Exchange Principle

○ Picards’s Exchange Principle

○ Evidence Exchange Principle

Question 6 **10 / 10 pts**

During a forensics analysis you are given a disk image named fat16.dd which contains a single FAT16 partition. What are the names of the deleted files listed in the root directory?

☐ Raven.pdf

☐ Range.png

☑ Yoda.jpeg

☑ Groot.jpg

□ Star.jpg

☑ Babu.jpg

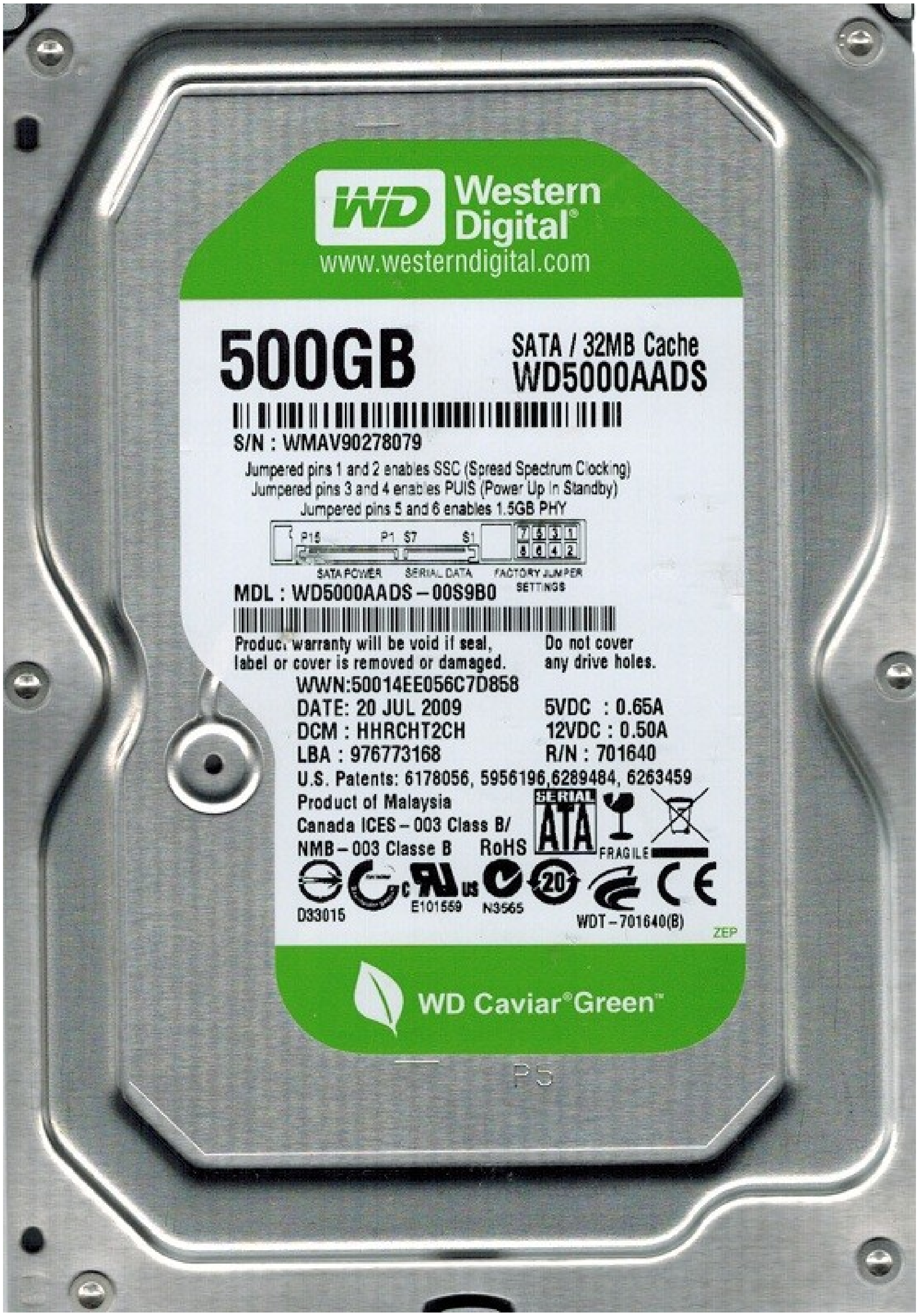
□ Ocean.avi

□ Data.txt

Question 7

5 / 5 pts

What are the total number of sectors contained within the hard drive shown below?


WD Western Digital®
www.westerndigital.com
500GB
SATA / 32MB Cache
WD5000AADS
S/N : WMAV90278079
Jumpered pins 1 and 2 enables SSC (Spread Spectrum Clocking)
Jumpered pins 3 and 4 enables PUIS (Power Up In Standby)
Jumpered pins 5 and 6 enables 1.5GB PHY
P15 P1 S7 S1
7 5 3 1
8 6 4 2
SATA POWER SERIAL DATA FACTORY JUMPER SETTINGS
MDL : WD5000AADS - 00S9B0
Product warranty will be void if seal, label or cover is removed or damaged.
Do not cover any drive holes.
WWN:50014EE056C7D858
DATE: 20 JUL 2009
DCM : HHRCHT2CH
LBA : 976773168
5VDC : 0.65A
12VDC : 0.50A
R/N : 701640
U.S. Patents: 6178056, 5956196,6289484, 6263459
Product of Malaysia
Canada ICES - 003 Class B/
NMB - 003 Classe B
RoHS
SERIAL ATA
FRAGILE
D33015
E101559
N3565
WDT - 701640(B)
ZEP
WD Caviar® Green™
P5

976773168

Question 8

5 / 5 pts

Which RFC specifies the best practices for digital evidence collection and storage?

3227

Question 9

15 / 15 pts

Provide 2 differences between the FAT16 and NTFS file system and explain which one provides a greater benefit during a forensics investigation.

Your Answer:

Overall, NTFS provides a wider range of capabilities than FAT16 does. For example, NTFS has compression, encryption, file permission, built-in security, and fault tolerance capabilities while FAT16 does not. Additionally, NTFS supports larger volume and file sizes than FAT16. From a forensics standpoint it is better to have more information about the data you are recovering and therefore NTFS is going to provide greater benefits that FAT16.

Question 10

5 / 5 pts

A forensic investigator determines that malicious code has been found on a system. Using the

NIST incident reporting method, what category should this attack be reported under?

● CAT 3

○ CAT 5

○ CAT 6

○ CAT 1

Question 11 **15 / 15 pts**

During a forensics analysis you are given a disk image named ntfs.dd which contains a single NTFS partition. Answer the following about the NTFS partition.

How many bytes per sector are specified in the Master Boot Record?	512 ∨
How many sectors are there in the NTFS partition?	204799 ∨
How many sectors per cluster are specified in the Master Boot Record?	8 ∨

What sector does the first MFT record start at?	32
Counting from the start of the partition, what sector does the first user generated MFT record start at?	160

Question 12

10 / 10 pts

Why are disk images and files hashed during a forensics investigation?

Your Answer:

By taking hashes before and after an investigation, we can know if any modifications were made to the evidence during the analysis. Modifications could mean that the evidence was tampered with or misused during the investigation. Therefore, hashes let us know if the integrity of the evidence has been maintained.

Question 13

12 / 12 pts

What is the maximum partition size for each of the following file systems?

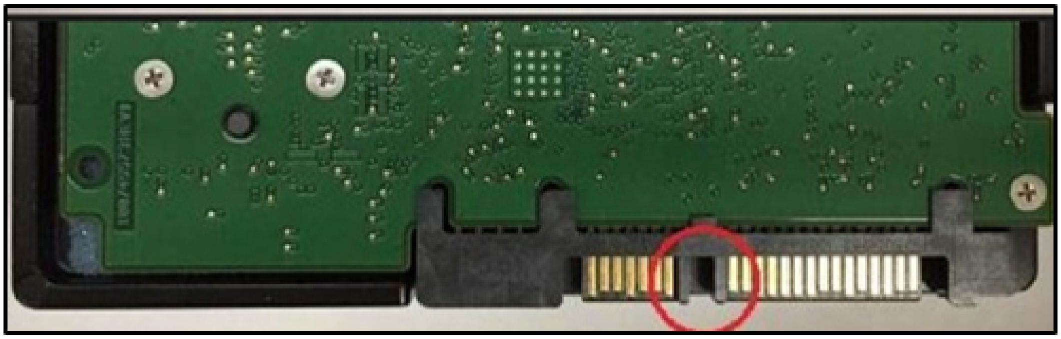
FAT16	2 GiB

FAT32	8 TiB
NTFS	256 TiB
FAT12	16 MiB

Question 14

5 / 5 pts

Which Solid State Drive interface is shown below?



○ Serial Attached Small Computer System Interface

● Serial Advanced Technology Attachment

○ Micro Secure Digital

○ Integrated Drive Electronics

Question 15

10 / 10 pts

What are the steps used during the digital forensics investigate process?

Your Answer:

There are six steps in the digital forensics investigative process: identify, preserve, collect, examine, analyze, and present. Identify generally refers to the detection/identification of a crime/issue that needs forensic investigation. Preserve is the act of preserving/securing the evidence for forensic analysis. Collect refers to collecting data off of the evidence and could even include recovery techniques. Examine is the process of finding data off of the evidence, especially hidden data. Analysis is the act of looking at what has been found from the evidence and building a timeline/narrative/understanding of the findings. Present refers to the end of the investigation when the findings are documented and presented.

Question 16 **15 / 15 pts**

During a forensics analysis you are given a disk image named ntfs.dd which contains a single NTFS partition. What are the names of the user generated files specified in the Master File Table?

□ Inventory.docx

□ Ocean.avi

☑ Jets.jpg

☑ Mystery.GIF

☑ Bear.avi

□ Data.dat

Question 17

11 / 11 pts

What are the layers of the file system abstraction model discussed in class?

Your Answer:

There are six layers in the file system abstraction model: disk, partition, file system, data unit, metadata, and file name. Disk refers to the physical storage device. Partition refers to the logical separations for a disk. The file system defines the partition file layout and metadata (each partition/volume has a file system). Data unit refers to the smallest addressable data. Metadata is the data about the data units. File name refers to the user space naming.

Question 18

5 / 5 pts

Which of the following is not a capability of the NTFS file system?

○ Self-Healing

○ Alternate Data Streams

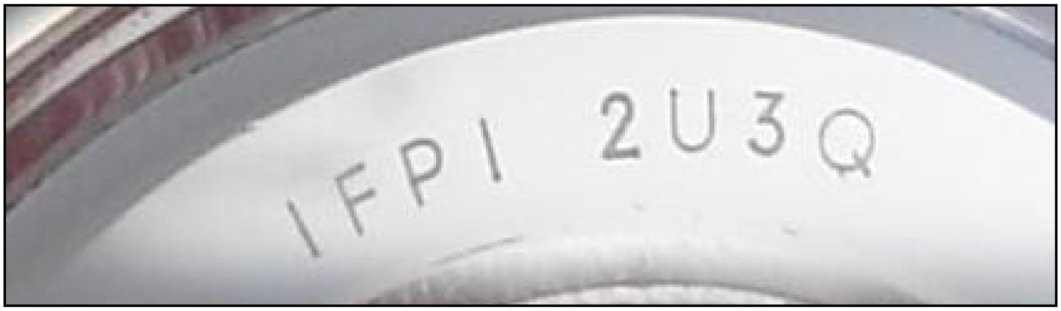
○ File Compression

● File Scripting

Question 19

5 / 5 pts

Your team has been provided with a wide variety of removal media to analyze and part of the analysis process is to determine where each device was produced. Where was the following CD manufactured?



○ Tilburg, Netherlands

● Olyphant, USA

○ Hofa, Germany

○ Buenos Aires, Argentina

Question 20

15 / 15 pts

Explain the importance of chain of custody during a forensics investigation.

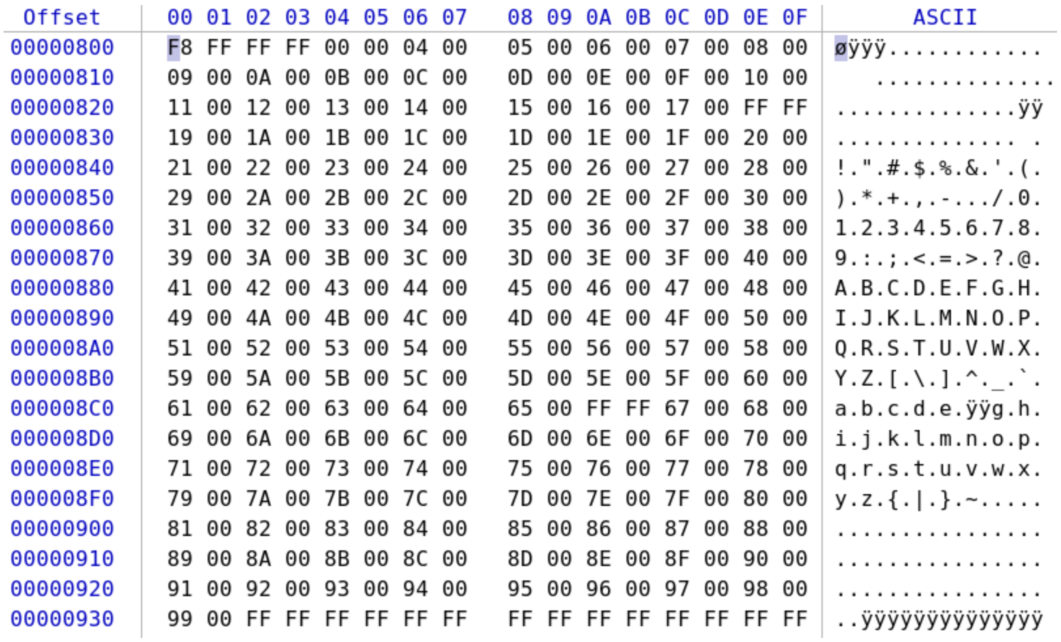
Your Answer:

Tracking the chain of custody for all pieces of evidence in an investigation is a critical part of ensuring the integrity of the evidence throughout the investigative process. It is important to make sure that all evidence is accounted for, secured, and not modified or misused during the investigation. If this is not done, then the evidence could become unusable, especially in the case of a criminal trial. Chain of custody helps us to do this and could include the following: documenting artifacts collected, identifying the collecting agent, segregating items in secured facilities, calculating artifact hashes, securely transporting evidence, and conducting proper hand-off evidence.

Question 21

4 / 4 pts

Based on the File Allocation Table shown below, how many files are stored on the partition?



```
Offset    00 01 02 03 04 05 06 07  08 09 0A 0B 0C 0D 0E 0F   ASCII
00000800  F8 FF FF FF 00 00 04 00  05 00 06 00 07 00 08 00   øÿÿÿ............
00000810  09 00 0A 00 0B 00 0C 00  0D 00 0E 00 0F 00 10 00      ..............
00000820  11 00 12 00 13 00 14 00  15 00 16 00 17 00 FF FF   ..............ÿÿ
00000830  19 00 1A 00 1B 00 1C 00  1D 00 1E 00 1F 00 20 00   .............. .
00000840  21 00 22 00 23 00 24 00  25 00 26 00 27 00 28 00   !.".#.$.%.&.'.(.
00000850  29 00 2A 00 2B 00 2C 00  2D 00 2E 00 2F 00 30 00   ).*.+.,.-.../.0.
00000860  31 00 32 00 33 00 34 00  35 00 36 00 37 00 38 00   1.2.3.4.5.6.7.8.
00000870  39 00 3A 00 3B 00 3C 00  3D 00 3E 00 3F 00 40 00   9.:.;.<.=.>.?.@.
00000880  41 00 42 00 43 00 44 00  45 00 46 00 47 00 48 00   A.B.C.D.E.F.G.H.
00000890  49 00 4A 00 4B 00 4C 00  4D 00 4E 00 4F 00 50 00   I.J.K.L.M.N.O.P.
000008A0  51 00 52 00 53 00 54 00  55 00 56 00 57 00 58 00   Q.R.S.T.U.V.W.X.
000008B0  59 00 5A 00 5B 00 5C 00  5D 00 5E 00 5F 00 60 00   Y.Z.[.\.].^._.`.
000008C0  61 00 62 00 63 00 64 00  65 00 FF FF 67 00 68 00   a.b.c.d.e.ÿÿg.h.
000008D0  69 00 6A 00 6B 00 6C 00  6D 00 6E 00 6F 00 70 00   i.j.k.l.m.n.o.p.
000008E0  71 00 72 00 73 00 74 00  75 00 76 00 77 00 78 00   q.r.s.t.u.v.w.x.
000008F0  79 00 7A 00 7B 00 7C 00  7D 00 7E 00 7F 00 80 00   y.z.{.|.}.~.....
00000900  81 00 82 00 83 00 84 00  85 00 86 00 87 00 88 00   ................
00000910  89 00 8A 00 8B 00 8C 00  8D 00 8E 00 8F 00 90 00   ................
00000920  91 00 92 00 93 00 94 00  95 00 96 00 97 00 98 00   ................
00000930  99 00 FF FF FF FF FF FF  FF FF FF FF FF FF FF FF   ..ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ
```

○ 8

○ 5

○ There are no files on the partition

○ 1

● 3

Question 22

15 / 15 pts

During a forensics analysis you are given a disk image named ntfs.dd which contains a single NTFS partition. What command would you use to recover the file named Jets.jpg in the Master File Table and what is the MD5 value of the resulting file?

Your Answer:

Command: dd if=ntfs.dd of=Jets.jpg bs=512 skip=106496 count=320

md5sum: fa726305fd2ee2eb2456be8b3e771ce4

Quiz Score: **200** out of 200