Anil Naraine

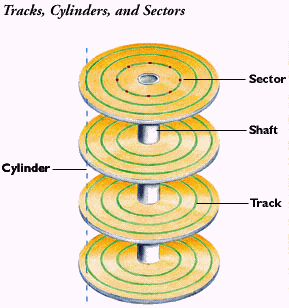
Assignment 1

Part I. Clearly define the following terms. Give an example and/or a diagram to

help in your explanation. [12 marks]

1. [4]Cylinder (Hard Disk Drive)

Hard disks contain one or more circular platters that are stacked on top of each other and spin at the same time.

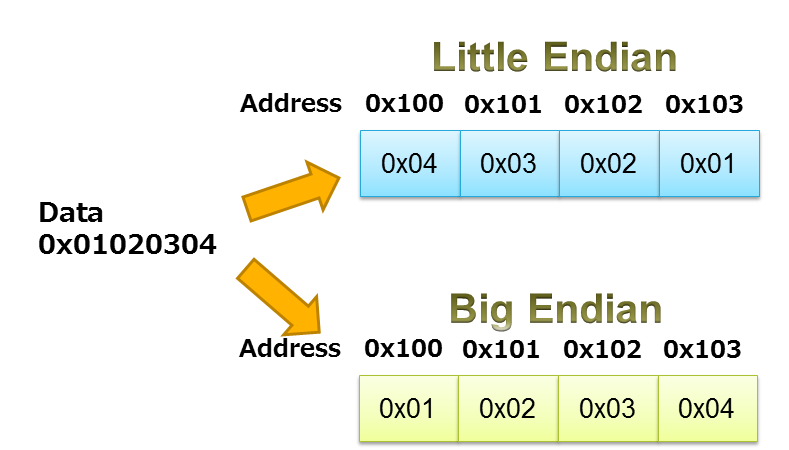


2. [4]Digital forensics

A branch of forensic science using various technologies to recover and investigate data and information used in a crime for an investigation.

3. [4]Endianness

Endianness is the ordering of individually addressable sub-units (for example, a byte is the smallest amount of space that is typically allocated to data.) within a longer data word stored.



Part II. True or False (no need to explain) [6 marks]

1. It is important to only look for digital evidence that supports your hypothesis

during an investigation. F

2. The main difference between FAT16 and FAT32 is that FAT16 is designed

for 16-bit CPU and FAT32 for 32-bit CPU. F

3. A Solid State Drive or SSD is faster than a mechanical Hard Disk Drive. T

4. Solid state hard drives (SSDs) come with any of the same interfaces as hard

disk drives, and SATA is a very common SSD interface. T

5. The number of hard disks on a computer system is equal to the number of disk

controllers. T

6. Digital forensics and data recovery refer to the same activities. F

Part III. Multiple-Choice Questions: Choose the answer that best applies.

[24 marks]

1) Which of the following type of USB connectors is Series B plug?

(a)

(b)

(c)

(d)

2) Why are SSDs superior to standard hard disk drive technology?

(a) Smaller

(b) Faster

(c) No moving parts

(d) All of the above

3) IDE hard disks can be configured as master or slave using

(a) Physical jumper on the disk

(b) BIOS setting

(c) Hard disk controller registers

(d) None of above

INFR 4690U IT Forensics

4) Which of the following is NOT metadata in file systems?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(a) FAT directory entries

(b) NTFS Master File Table (MFT) entries

(c) Ext3 inode structures

(d) None of the above

5) The octal numeral system (or oct for short) is the base \_\_\_\_\_\_\_ number

system.

(a) 2

(b) 8

(c) 10

(d) 16

6) In FAT, a 18KB file uses how many sectors (Assume that the size of a cluster

is 8 sectors.)

(a) 18

(b) 20

(c) 36

(d) 40

7) \_\_\_\_\_\_\_\_\_\_\_\_\_ is the most common source of digital evidence

(a) Hard disk

(b) USB flash drive

(c) CD Disc

(d) DVD Disc

8) What is the length of the hash generated by using SHA-1? \_\_\_\_\_\_\_\_\_\_\_\_\_

(a) 128 bits

(b) 160 bits

(c) 178 bits

(d) 256 bits

9) Which component is the "brains" of a computer system?

(a) RAM

(b) Hard Drive

(c) Central processing unit (CPU)

(d) Power supply unit (PSU)

10) What does the FS stand for in NTFS?

(a) File System

(b) File Systems

(c) Forensic System

(d) FAT Supplement

11) How many Gigabytes make one Terabyte?

(a) 210

(b) 220

(c) 230

(d) 240

12) In the Linux command line, what command would you type to navigate to a

sub-folder called "images"?

(a) cd .\images

(b) cd /images

(c) cd images

(d) goto images

13) Which command in TSK can be used for building and searching “good” and “bad”

hash databases?

(a) blkcat

(b) blkstat

(c) fsstat

(d) hfind

14) Fedora can be configured to access which of the following file systems?

(a) ext3

(b) FAT32

(c) NTFS

(d) All of the above

15) Slack space is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(a) the unused bytes in the last data unit for a file

(b) the unallocated space in a disk volume system

(c) the unused data units in a file system

(d) the unused data units listed as damaged

16) The following figure shows the status of 16 data units. If the Best fit strategy is

used by an OS to allocate data units, which unit will be chosen if three data

units are needed?

(a) 1, 2 and 5

(b) 5, 6 and 7

(c) 12, 14 and 16

(d) 7, 12 and 14

17) Suppose that the size of the File Allocation Table (FAT) in a FAT32 file system

is 32 sectors. What is the maximum number of data units can be represented?

(a) 512

(b) 1024

(c) 4096

(d) 8192

18) Data compression can occur in the level \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_?

(a) inside a file format

(b) an external application

(c) the file system

(d) All of the above

19) Which of the following algorithms are NOT cryptographic hash functions?

(a) SHA-1

(b) RIPEMD-160

(c) RSA

(d) MD5

20) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can be used to preserve the integrity of digital evidence

material.

(a) Message authentication

(b) Message digest

(c) Message confidentiality

(d) None of the above

21) Today's computers can support many different kinds of hard drives. What

kind of hard drive interface does this picture show?

(a) USB

(b) SCSI

(c) Parallel ATA

(d) Serial ATA

22) What does the acronym MBR represent?

(a) Master Broadcast Record

(b) Master Boot Record

(c) Mega Boot Record

(d) Multiple Boot Record

23) What is the maximum number of primary partitions supported by MBR?

(a) 1

(b) 4

(c) 32

(d) 512

24) To protect the data on a USB flash drive, you can \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(a) enable write protection for the USB disk drive

(b) hang it from your keychain using the drive's cap

(c) encrypt the data

(d) change the file attributes to Read-Only

Part IV. Fill in the appropriate word, phrase or value in the space provided [1 mark

each, 23 marks]

1. Convert the decimal number 37 to the following bases:

a) base 2: \_\_\_\_\_\_100101\_\_\_\_\_\_\_

b) base 7: \_\_\_\_\_52\_\_\_\_\_\_\_\_

c) base 8: \_\_\_\_45\_\_\_\_\_\_\_\_\_

d) base 9: \_\_\_\_41\_\_\_\_\_\_\_\_\_

2. Convert the following binary numbers to their hexadecimal and octal

equivalents.

0b1111011011\_\_\_3db\_\_\_\_\_\_\_ (Hexadecimal) and \_\_\_1733\_\_\_\_\_\_\_\_\_ (Octal)

0b1011010111\_\_\_\_2d7\_\_\_\_\_\_ (Hexadecimal) and \_\_\_\_1327\_\_\_\_\_\_\_\_ (Octal)

3. Two popular internal Advanced Technology Attachment (ATA) drive

interfaces are \_SATA\_\_\_\_\_\_\_\_\_ and \_\_\_\_PATA\_\_\_\_\_\_, where \_\_\_PATA\_\_\_\_\_\_ is a parallel

interface.

4. The three phases of a Digital Crime Scene Investigation is \_\_system preservation \_\_\_\_\_\_\_\_\_\_\_,

\_\_\_evidence searching\_\_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_event reconstruction\_\_\_\_\_\_\_\_\_\_\_\_.

5. Consider a disk that reported 16 heads per cylinder and 63 sectors per track. If

we had a CHS address of cylinder 2, head 2, and sector 8, the LBA address is

\_\_2149\_\_\_\_\_\_\_\_\_\_\_.

6. The PICL guidelines have been widely adopted by forensic investigators as well

as the legal authority on how to conduct digital crime scene investigations.

PICL stands for preservation\_\_\_\_\_\_\_\_\_\_, \_\_isolation\_\_\_\_\_\_\_\_\_\_, \_\_correlation\_\_\_\_\_\_\_\_\_, and

\_\_\_\_logging\_\_\_\_\_\_\_\_\_.

7. The size of a standard MFT Entry in NTFS is \_\_\_1024 bytes\_\_\_\_\_\_\_.

8. Data structures for tracks and sectors are created to a hard drive before it leaves

the hard disk manufacturers in a process called

\_\_\_\_\_\_low level\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ formatting.

9. The National Institute of Standards and Technology (NIST) maintains a library

which contains hashes of files that are found in operating systems and software

distributions. It is called \_\_national software reference library \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

10. If the following 3-byte value is stored in big--endian ordering, the actual value

is \_\_00 23 56\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Please note that each byte value

is in hexadecimal.

Address 70 71 72 73 74 75 76 77 78

00 12 56 23 00 76 45 70 18

3-byte value

Part V. Answer all of the following questions. [51 marks]

1. [3] A double-sided disk has parameters 512 bytes/sector, 28 sectors/track,

63 tracks/side. What is the capacity of the disk?

57344 bytes

2. [5] Briefly discuss why computer forensics is important to our society.

Digital forensics is important in today’s society because practically everything is digital. Without digital forensics it would be impossible to retrieve evidence to solve criminal cases. Outside of the legal system, digital forensics plays an important part in data recovery on a consumer and industrial level.

3. [5] What is hash function, and what can it be used for (You only need to describe

ONE usage scenario, particularly in digital forensics investigations)?

We can use hashes or file signature search. We can hash the suspects files to create a database then simply calculate the MD5 hash and compare it to a hash database to determine if they are good or bad.

4. [5] List five common types of computer crimes?

Fraud, piracy, identity theft, drug trafficking, harassment.

5. [5] Why should your evidence media be write-protected? How many types of

write protection are available? What are they?

It is important to preserve the evidence to ensure the data has not been changed to make it admissible in court. There are two types of write protection: hardware-based, and software-based.

6. [5]List five common analysis techniques for data content in a file system?

Data unit viewing, wiping techniques, consistency checks, data unit allocation status, logical file system-level searching.

7. [7]What is a File System? List 5 different file system.

A file system is a collection of data structures that allow an application to create, read, and write files. FAT, exFAT, NTFS, HFS ,and XFS are all examples of file systems.

8. [3] Use a Web search engine, such as Google, and search for job postings

specialized in the investigation of digital media. By going through the job

descriptions and skills requirements, identify and list any 3 key skills needed

for jobs in career fields of digital forensics investigations.

<https://jobs.scotiabank.com/job/Scarborough-Senior-Manager-Digital-Forensics-ON/356624417/?feedId=214217&utm_source=Indeed&utm_campaign=Scotiabank_Indeed&emid=3640>

Experience conducting senior level digital forensics examinations on Microsoft Windows operating systems using industry standards digital forensic tools (ex. EnCase, Cellebrite, others) and various security technologies (ex. endpoint protection, data loss prevention, security information and event management, and others).

Key technical expertise in subject areas including but are not limited to: information and cyber security, networking and routing, data management, data privacy laws and regulations

Working knowledge of protocols, technologies, and environments including but are not limited to: TCP/IP, SQL, Windows Server, Linux, Unix, IIS & STB client technologies

9. [3] Which certifications should be in your list of credentials if you decide to

pursue a career in digital forensics? Please list 3 certifications you think are

the most demanded (hottest) certifications in digital forensics.

Please note that you can browse through a list of profiles of digital forensics

professionals in LinkedIn and mine certifications they hold.

Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE), Certified Information Systems Security Professional (CISSP)

10. [10] Search for companies specializing in digital investigations (a.k.a. digital

forensics and computer forensics). Select one and write a one-page summary

about what it does including services offered and a brief explanation for them.

<https://www.digitalforensics.com/>

COMPUTER FORENSICS SERVICES

* Digital Investigation
* E-Discovery
* Forensic Analysis
* Expert Testimony
* Forensics Reporting

MOBILE DEVICES INVESTIGATIONS

* Calls, web, chats history
* Contacts, text messages
* GPS Data
* Deleted Data
* Photos & Videos