Chapter-03

Data Acquisition

Chapter Summary

- **Forensics data acquisitions are stored in three different formats: raw, proprietary, and AFF. Most proprietary formats and AFF store metadata about the acquired data in the image file.**
- **The four methods of acquiring data for forensics analysis are disk-to-image file, disk-to-disk copy, logical disk-to-disk or disk-to-data file, and sparse data copy of a folder or file.**
- **Lossless compression for forensics acquisitions doesn't alter the data when it's restored, unlike lossy compression.**
- **Lossless compression can compress up to 50% for most data. If data is already compressed on a drive, lossless compression might not save much more space.**
- **If there are time restrictions or too much data to acquire from large drives or RAID drives, a logical or sparse acquisition might be necessary. Consult with your lead attorney or supervisor first to let them know that collecting all the data might not be possible.**
- **You should have a contingency plan to ensure that you have a forensically sound acquisition and make two acquisitions if you have enough data storage. The first acquisition should be compressed, and the second should be uncompressed. If one acquisition becomes corrupt, the other one is available for analysis.**
- **Write-blocking devices or utilities must be used with GUI acquisition tools in both Windows and Linux. Practice with a test drive rather than suspect drive, and use a hashing tool on the test drive to verify that no data was altered.**
- **Always validate your acquisition with built-in tools from a forensics acquisition program, a hexadecimal editor with MD5 or SHA-1 hashing functions, or the Linux md5sum or sha1sum commands.**
- **A Linux Live CD, such as Ubuntu, openSUSE, Arch Linux, Fedora, or Slackware provides many useful tools for digital forensics acquisitions.**
- **The preferred Linux acquisition tool is dcfldd instead of dd because it was designed for forensics acquisition. The dcfldd tool is also available for Windows. Always validate the acquisition with the hashing features of dcfldd and md5sum or sha1sum.**
- **When using the Linux dd or dcfldd commands, remember that reversing the output field (of=) and input field (if=) of suspect and target drives could write data to the wrong drive, thus destroying your evidence. If available, you should always use a physical write-blocker device for acquisitions.**
- **To acquire RAID disks, you need to determine the type of RAID and which acquisition tool to use. With a firmware-hardware RAID, acquiring data directly from the RAID server might be necessary.**

Q.1) What's the main goal of a static acquisition?

Ans: In *digital forensics*, there are two main types of data acquisitions: **static acquisition** and **live acquisition**.

A **static acquisition** is the process of acquiring data from a storage device that is not actively running. The main goal of a static acquisition is to create a bit-for-bit copy of the original data without altering any of its contents. This allows investigators to preserve the integrity of the evidence and perform analysis on the acquired data without the risk of modifying or damaging the original source.

On the other hand, a **live acquisition** involves acquiring data from a storage device that is actively running. The main goal of a live acquisition is to capture volatile data, such as open files, running processes, and network connections, which may not be available in a static acquisition. Live acquisitions are often performed in situations where time is critical, such as during an ongoing investigation or when immediate access to the data is required.

Q.2) Name the three formats for digital forensics data acquisitions.

Ans: There are three common formats for digital forensics data acquisitions:

1. ***Raw format*:** The raw format is a binary image of the acquired data, preserving the exact content and structure of the original source. It does not include any built-in metadata and can be large in size. However, it is compatible with various forensic tools and can capture deleted or hidden data.
2. ***Advanced Forensic Format* (AFF):** The Advanced Forensic Format (AFF) is a flexible and extensible format that includes metadata and supports compression. It allows for efficient storage and analysis of acquired data.
3. ***Expert Witness Compression Format* (EWF):** The Expert Witness Compression Format (EWF) is a format that combines compression and encryption to create a secure and efficient way of storing acquired data. It is commonly used in forensic investigations.

Advantages of the raw format include its compatibility with various forensic tools and its ability to capture deleted or hidden data. However, it has *disadvantages* such as large file size and the lack of built-in verification mechanisms.

Proprietary format acquisition files often have features such as encryption, compression, or proprietary metadata that are specific to the tool or software used for the acquisition.

Q.3) What are two advantages and disadvantages of the raw format?

Ans: Raw Format • Makes it possible to write bit-stream data to files

• Advantages –

Fast data transfers – Can ignore minor data read errors on source drive

– Most computer forensics tools can read raw format • Disadvantages – Requires as much storage as original disk or data – Tools might not collect marginal (bad) sectors

Advantages of RAW Format in Cyber Forensics:

1. **Preservation of Original Data:** RAW format preserves the original data of digital evidence without any compression or modification. In cyber forensics, maintaining the integrity of digital evidence is crucial for investigations and legal proceedings. The unaltered nature of RAW files ensures that investigators have access to the most accurate representation of the data as it existed on the digital device.
2. **Enhanced Analysis and Recovery Options:** RAW format allows forensic investigators to analyze data at a lower level, including recovering deleted files, examining metadata, and detecting hidden or encrypted information. This level of granularity can be essential in uncovering digital artifacts and traces left by cybercriminals. It provides a more comprehensive view of the digital landscape, enabling investigators to uncover critical details that might be lost in compressed or processed formats.

Disadvantages of RAW Format in Cyber Forensics:

1. **Increased Storage Requirements:** RAW files tend to have larger sizes compared to compressed formats. Storing large volumes of RAW data from multiple investigations can demand substantial storage space. This can pose a challenge for forensic labs with limited

resources, requiring them to invest in scalable and secure storage solutions to manage the growing volume of digital evidence.

2. **Complexity in Processing and Analysis:** RAW files require specialized software and expertise for processing and analysis. Cyber forensic investigators must be proficient in using tools that can handle RAW data and extract relevant information effectively. The complexity of working with RAW files may lead to longer processing times and require a higher level of skill, potentially limiting the accessibility of these tools to less experienced forensic professionals.

Q.4) List two features common with proprietary format acquisition files.

Proprietary format acquisition files are specific to certain software. The two common features are limited compatibility and closely protected information

Computer Forensics a

Chapters 1-7

QUESTION	ANSWER
1. List two organizations mentioned in the chapter that provide computer forensics training.	1.(IACIS) International Association of Computer Investigation Specialist. 2. FLECT Federal Law Enforcement Training Center.
2. Computer forensics and data recovery refer to the same activities. True or False?	False
3. Police in the United States must use procedures that adhere to which of the following? a. the Third Amendment b. the Fourth Amendment c. the First Amendment d. none of the above	Fourth Amendment
4. The triad of computing security includes which of the following?	Vulnerability Assesment, Intrusion Response, and Investigations.
5. List three common types of digital crime.	Internet Pornagraphy, Espianage, Abuse of Internet Properties.
6. A corporate investigator must follow Fourth Amendment standards when conducting an investigation. True or False?	False as long as the company has a security Banner.
7. To what does the term “silver-platter doctrine” refer?	when a civillian or corporate investigative agent delivers evidence to a law enforcement agenttheir job is to minimize risk to the company
8. Policies can address rules for which of the following?	D. All of the above. (Refer to books Review Ques.)
9. List two items that should appear on an internal warning banner.	A.) Access to this system and Network are Restricted B.) Use of this System and Network is for Official use Only.

10. Warning banners are often easier to present in court than policy manuals are. True or False?	True. They are easier to present in a trial.
11. A corporate investigator is considered an agent of law enforcement. True or False?	False. Refer to page 18 in book
12. List two types of computer investigations typically conducted in the corporate environment.	E-mail Abuse and Internet Abuse.
13. What is professional conduct and why is it important?	Maintaining confidentiality, having moral ethics, standards of behavior. It is critical to maintaining your integrity and credibility.
14. You can lose your job for violating a company policy, even if you don't commit a crime. True or False?	True.
15. What is the purpose of maintaining a professional journal?	Can help remembering certain tasks or issues and what types of tools software or hardware you used for a particular problem.
16. iLook is maintained by _____.	ILook is an all-in-one computer forensics suite originally created by Elliot Spencer and currently maintained by the U.S. Department of Treasury Internal Revenue Service Criminal Investigation Division (IRS-CI) Electronic Crimes Program. It was made avail
17. The U.S. _____ maintains a manual on procedures to follow for search and seizure of computers.	IRS
18. Laws and procedures for PDAs are which of the following? a. well established b. still being debated c. on the law books d. none of the above	b.) Still being established.
19. Why should companies appoint an authorized requester for computer investigations?	To avoid conflicts and competions between departments and limits who is authorized to request an investigation. Authorized requster
What is the purpose of an Affidavit?	Its a sworn statement for a judge to get a warrent if you have found facts that support the evidence of a crime.
What are the neccesary componaents of a search warrant?	Exhibits (evidence) Notarized Verdict.
Chapt 2	chapt 2
1. What are some initial assessments you should make for a computing investigation?	A.) Talk to others involved in the case about the incident. B.) Has evidence already been seized by Law enforcement or security officers?
2. What are some ways to determine the resources needed for an investigation?	Identify the Risk; find out what OS to work with and which types of hardware or software and tools to use and security measures.
3. List three items that should be on an evidence custody form.	Case number, Investigating officer, Investigating Agency.

4. Why should you do a standard risk assessment to prepare for an investigation?	Identify the risks as in having a set amount of things that can or normally will happen who is the user what type of equipment
5. You should always prove the allegations made by the person who hired you. True or False?	False. Because other investigators or persons involved involved in the case might alter somethinfg in the evidence.
6. For digital evidence, an evidence bag is typically made of antistatic material. True or False?	True. refer to pg36
7. Who should have access to a secure container? a. only the primary investigator b. only the investigators in the group c. everyone on the floor d. only senior-level management	Only investigators in the group.
8. For employee termination cases, what types of investigations do you typically encounter?	Employee abuse of corporate assets,incidents that create a hostile enviroment, examples pornagraphy, inappropriate e-mails.
9. Why should your evidence media be write-protected?	If you just start windows without anaylizing a hard disk by writing data to the recycling bin it currupts the quality and integrity of eveidence
10. List three items that should be in your case report.	Resources needed such as tools hardware software example: deleted files email standard risk assesments
11. Why should you critique your case after it's finished?	Self evaluationfor growth and improved identity secessful decisions, how you could have improved.
12. What do you call a list of people who have had physical possession of the evidence?	Evidence of custody.
13. What two tasks is an acquisitions officer responsible for at a crime scene?	Documentations of items the investigating officers collected with computer to include list of storage media, i.e. removable disk photographs of equipments and windows before they are such down.
14. What are some reasons that an employee might leak information to the press?	Disgruntled employee, embarrass management power struggle between corporations premature release of info on new products
15. When might an interview turn into an interrogation?	An interrigation is trying to get a suspect to confess. An interview is getting info from a witness. Sometimes a witness in questioning might lose their credibility and turns into a suspect
16. What is the most important point to remember when assigned to work on an attorney-client privilege case?	When conducting an (ACP) atorney client priviledge you must keep all findings confidential.
17. What are the basic guidelines when working on an attorney-client privilege case?	1) memorandum 2) list of key words of interest to the investigation 3) compare hash values 4)bit stream imaging 4) documentation private legal
18. Data collected before an attorney issues a memorandum for an attorney-client privilege case is	False refer to pg. 20

protected under the confidential work product rule. True or False?	
chapter 3	chapter 3
1. An employer can be held liable for e-mail harassment. True or False?	True
2. Building a business case can involve which of the following?	d) all of the above refer to review ques
3. The ASCLD mandates the procedures established for a computer forensics lab. True or False?	False
4. The manager of a computer forensics lab is responsible for which of the following? (Choose all that apply.) a. necessary changes in lab procedures and software b. ensuring that staff members have sufficient training to do the job c. knowing the lab	all the answers refer to review sheet
5. To determine the types of operating systems needed in your lab, list two sources of information you could use.	Uniform Crime Report statistics for your area and a list of cases handled in your area or at your company
6. What items should your business plan include?	physical security items, such as evidence lockers; how many machines are needed; what OSs your lab commonly examines; why you need certain software; and how your lab will benefit the company (such as being able to quickly exonerate employees or discover w
7. List two popular certification systems for computer forensics.	IACIS, HTCN, EnCE refer to pg 76
8. The National Cybercrime Training Partnership is available only to law enforcement. True or False?	True
9. Why is physical security so critical for computer forensics labs?	to maintain the chain of custody and prevent data from being lost, corrupted, or stolen
10. If a visitor to your computer forensics lab is a personal friend, it's not necessary to have him or her sign the visitor's log. True or False?	False
11. What three items should you research before enlisting in a certification program?	requirements, cost, and acceptability in your chosen area of employment
12. Large computer forensics labs should have at least _____ exits.	two
13. Typically, a(n) _____ lab has a separate storage area or room for evidence.	regional
14. Computer forensics facilities always have windows. True or False?	False refer to pg 84

15. The chief custodian of evidence storage containers should keep several master keys. True or False	False refer to page 80,81
16. Putting out fires in a computer lab typically requires a _____ rated fire extinguisher.	B Refer to review sheets
17. A forensic workstation should always have a direct broadband connection to the Internet. True or False?	False refer to pg.84
18. Which organization provides good information on safe storage containers?	NISPOM refer to pg. 80,81
19. Which organization has guidelines on how to operate a computer forensics lab?	ASCLD refer to pg. 72
20. What name refers to labs constructed to shield EMR emissions?	TEMPEST refer to pg. 80
chapter 4	chapter 4
1. What is the primary goal of a static acquisition?	preservation of digital evidence
2. Name the three formats for computer forensics data acquisitions.	raw format, proprietary formats, and Advanced Forensic Format (AFF)
3. What are two advantages and disadvantages of the raw format?	Advantages: faster data transfer speeds, ignores minor data errors, and most forensic analysis tools can read it. Disadvantages: requires equal or greater target disk space, does not contain hash values in the raw file (metadata), might have to run a sepa
4. List two features common with proprietary format acquisition files.	Can compress or not compress the acquisition data; can segment acquisition output files into smaller volumes, allowing them to be archived to CD or DVD; case metadata can be added to the acquisition file, eliminating the need to keep track of any addition
5. Of all the proprietary formats, which one is the unofficial standard?	Expert Witness, used by Guidance Software EnCase
6. Name two commercial tools that can make a forensic sector-by-sector duplicate of a drive to a larger drive.	EnCase, SafeBack, and SnapCopy.
7. What does a logical acquisition collect for an investigation?	only specific files of interest to the case
8. What does a sparse acquisition collect for an investigation?	fragments of unallocated data in addition to the logical allocated data
9. What should you consider when determining which data acquisition method to use?	size of the source drive, whether the source drive be retained as evidence, how long the acquisition will take, and where the disk evidence is located

10. What is the advantage of using a tape backup system for forensic acquisitions of large data sets?	There is no limit to the size of data you can write to magnetic tape.
11. When is a standard data backup tool, such as Norton Ghost, used for a computing investigation?	when the suspect computer can't be taken offline for several hours but can be shut down long enough to switch disks with a Ghost backup, allowing the investigator to take the original disk and preserve it as digital evidence
12. Why is it a good practice to make two images of a suspect drive in a critical investigation?	to ensure at least one good copy of the forensically collected data in case of any failures
13. When you perform an acquisition at a remote location, what should you consider to prepare for this task?	determining whether there's sufficient electrical power and lighting and checking the temperature and humidity at the location
14. What is the disadvantage of using the Windows XP/Vista USB write-protection Registry method?	If the target drive is an external USB drive, the write-protect feature prevents data from being written to it.
15. With newer Linux kernel distributions, what happens if you connect a hot-swappable device, such a USB thumb drive, containing evidence?	Newer Linux distributions automatically mount the USB device, which could alter data on it.
16. In a Linux shell, the fdisk -1 command lists the suspect drive as /dev/hda1. Is the following dcfldd command correct? dcfldd if=image_file.img of=/dev/hda1	Wrong. This command reads the image_file.img file and writes it to the evidence drive's /dev/hda1 partition. The correct command is dcfldd if=/dev/hda1 of=image_file.img.
17. What is the most critical aspect of computer evidence?	validation
18. What is a hashing algorithm?	A program designed to create a binary or hexadecimal number that represents the uniqueness of a data set, file, or entire disk
19. Which hashing algorithm utilities can be run from a Linux shell prompt?	md5sum and sha1sum
20. In the Linux dcfldd command, which three options are used for validating data?	hash=, hashlog=, and vf=
21. What's the maximum file size when writing data to a FAT32 drive?	2 GB (a limitation of FAT file systems)
22. What are two concerns when acquiring data from a RAID server?	) amount of data storage needed. 2) the type of RAID server (0, 1, 5, etc.) 3) whether your acquisition tool can handle RAID acquisitions. 4) whether your analysis tool can handle RAID data 5) whether your analysis tool can split RAID data into separate d
23. R-Studio and DiskExplorer are used primarily for computer forensics. True or False?	False. They are designed as data recovery tools but are useful in rebuilding corrupt data when forensics tools fail.
24. With remote acquisitions, what problems should you be aware of?	d. All of the above refer to review sheet

25. How does ProDiscover Investigator encrypt the connection between the examiner's and suspect's computers?	ProDiscover provides 256-bit AES or Twofish encryption with GUID and encrypts the password on the suspect's workstation.
25. How does ProDiscover Investigator encrypt the connection between the examiner's and suspect's computers?	ProDiscover provides 256-bit AES or Twofish encryption with GUID and encrypts the password on the suspect's workstation.
26. What is the EnCase Enterprise remote access program?	ServLet
27. What is the ProDiscover remote access program?	PDServer
28. What is the Runtime Software utility used to acquire data over a network connection?	DiskExplorer for NTFS or DiskExplorer for FAT
29. HDHost is automatically encrypted when connected to another computer. True or False?	False look up pg
30. List the two types of connections in HDHost..	TCP/IP and serial RS232 port
31. Which computer forensics tools can connect to a suspect's remote computer and run surreptitiously?	EnCase Enterprise, ProDiscover Investigator, and ProDiscover Incident Response
32. EnCase, FTK, SMART, and iLook treat the image file as though it were the original disk. True or False?	True look up pg
33. When possible, you should make two copies of evidence. True or False?	True look up pg.
34. FTK Imager can acquire data in a drive's host protected area. True or False?	False look up pg.
1. Corporate investigations are typically easier than law enforcement investigations for which of the following reasons?	a. Most companies keep inventory databases of all hardware and software used.
2. In the United States, if a company publishes a policy stating that it reserves the right to inspect computing assets at will, a corporate investigator can conduct covert surveillance on an employee with little cause. True or False?	True look up pg.
3. If you discover a criminal act, such as murder or child pornography, while investigating a corporate policy abuse, the case becomes a criminal investigation and should be referred to law enforcement. True or False?	True look up pgs.
4. As a corporate investigator, you can become an agent of law enforcement when which of the following happens? (Choose all that apply.)	a. You begin to take orders from a police detective without a warrant or subpoena. b. Your internal investigation has concluded, and you have filed a criminal complaint and turned over the evidence to law enforcement.
5. The plain view doctrine in computer searches is well-established law. True or False?	False look up pgs.

6. If a suspect computer is located in an area that might have toxic chemicals, you must do which of the following? (Choose all that apply.)	a. Coordinate with the HAZMAT team. c. Assume the suspect computer is contaminated. Rfer to review sheets
7. What are the three rules for a forensic hash?	It can't be predicted, no two files can have the same hash value, and if the file changes, the hash value changes.
8. In forensic hashes, a collision occurs when _____.	two files have the same hash value
9. List three items that should be in an initial-response field kit.	REFER TO REVIEW PGS. Small computer toolkit, large-capacity drive, IDE ribbon cables, forensic boot media, laptop IDE 40-to-44 pin adapter, laptop or portable computer, FireWire or USB dual write-protect external bay, flashlight, digital camera or 35mm ca
10. When you arrive at the scene, why should you extract only those items you need to acquire evidence?	to minimize how much you have to keep track of at the scene
11. Computer peripherals or attachments can contain DNA evidence. True or False?	LOOK UP PGS
12. If a suspect computer is running Windows 2000, which of the following can you perform safely?	a. Browsing open applications refer to review sheets
13. Describe what should be videotaped or sketched at a computer crime scene.	Computers, cable connections, overview of scene—anything that might be of interest to the investigation
14. Which of the following techniques might be used in covert surveillance?	a. Keylogging b. Data sniffing refer to review sheets
15. Commingling evidence means what in a corporate setting?	sensitive corporate information being mixed with data collected as evidence
16. Identify two hashing algorithms commonly used for forensic purposes.	MD5 and SHA-1
17. Small companies rarely need investigators. True or False?	False look up pgs
18. If a company doesn't distribute a computing use policy stating an employer's right to inspect employees' computers freely, including e-mail and Web use, employees have an expectation of privacy. True or False?	True look up pgs
19. You have been called to the scene of a fatal car crash where a laptop computer is still running. What type of field kit should you take with you?	initial-response field kit
20. You should always answer questions from onlookers at a crime scene. True or False?	False
chapter 6	chapter 6

1. In DOS and Windows 9.x, Io.sys is the first file loaded after the ROM bootstrap loader finds the disk. True or	True look up pgs
2. Sectors typically contain how many bytes?	b. 512 refer to review sheet
3. What does CHS stand for?	cylinders, heads, sectors
4. Zoned bit recording is how manufacturers ensure that the outer tracks store as much data as possible. True or False?	False look up pages
5. Areal density refers to which of the following?	c. Number of bits per square inch of a disk platter refer to review sheet
6. Clusters in Windows always begin numbering at what number?	2
7. What is the ratio of sectors per cluster in a floppy disk?	a. 1:1 refer to review sheets
8. List three items stored in the FAT database.	file and directory names, starting cluster numbers, file attributes, and date and time stamps
9. Windows 2000 can be configured to access which of these file formats? (Choose all that apply.)	a. FAT12 b. FAT16 c. FAT32 d. NTFS
10. In FAT32, a 123 KB file uses how many sectors?	The answer is 246 sectors. 123 x 1024 bytes per KB = 125,952 total bytes in the file. 125,952 bytes / 512 sectors per cluster = 246 sectors
11. What is the space on a drive called when a file is deleted? (Choose all that apply.)	b. Unallocated space d. Free space refer to review sheets
12. List two features NTFS has that FAT does not.	Unicode characters, security, journaling
13. What does MFT stand for?	Master File Table
14. In NTFS, files smaller than 512 bytes are stored in the MFT. True or False?	True look up pages
15. RAM slack can contain passwords. True or False?	True look up pages
16. A virtual cluster consists of what kind of clusters?	chained clusters
17. The Windows Registry in Windows 9x consists of what two files?	System.dat and User.dat
18. HPFS is used on which OS?	OS/2
19. Device drivers contain what kind of information?	instructions for the OS on how to interface with hardware devices

20. Which of the following Windows XP files contains user-specific information?	b. Ntuser.dat refer to review pgs
21. Virtual machines have which of the following limitations when running on a host computer?	c. Virtual machines are limited to the host computer's peripheral configurations, such as mouse, keyboard, CD/DVD drives, and other devices. refer to review pgs
22. An image of a suspect drive can be loaded on a virtual machine. True or False?	True look up pgs
23. EFS can encrypt which of the following?	a. Files, folders, and volumes refer to review pgs.
24. To encrypt a FAT volume, which of the following utilities can you use?	c. PGP Whole Disk Encryption
25. What are the functions of a data run's field components in an MFT record?	Refer to review pg. Data runs have three components; the first declares how many bytes are required in the attribute field to store the number of bytes needed for the second and third components. The second component stores the number of clusters assigned
chapter 7	chapter 7
1. What are the five required functions for computer forensics tools?	acquisition, validation and discrimination, extraction, reconstruction, and reporting
2. A disk partition can be copied only with a command-line acquisition tool. True or False?	False
3. What two data-copying methods are used in software data acquisitions?	c. Logical and physical
4. During a remote acquisition of a suspect drive, RAM data is lost. True or False?	False
5. Hashing, filtering, and file header analysis make up which function of computer forensics tools?	a. Validation and discrimination
6. Sleuth Kit is used to access Autopsy's tools. True or False?	False (Autopsy is the front end to Sleuth Kit.)
7. When considering new forensics software tools, you should do which of the following?	c. Test and validate the software.
8. Of the six functions of computer forensics tools, what are the subfunctions of the Extraction function?	Data viewing, Keyword searching, Decompressing, Carving, Decrypting, and Bookmarking
9. Data can't be written to the disk with a command-line tool. True or False?	False look up pgs.
10. Hash values are used for which of the following purposes? (Choose all that apply.)	b. Filtering known good files from potentially suspicious data d. validating change.

11. What's the name of the NIST project established to collect all known hash values for commercial software and OS files?	National Software Reference Library (NSRL)
12. Many of the newer GUI tools use a lot of system resources. True or False?	True look up pgs.
13. Building a forensic workstation is more expensive than purchasing one. True or False?	False look up pgs
14. A live acquisition is considered an accepted forensics practice. True or False?	False look up pgs.
15. Which of the following is true of most drive-imaging tools? (Choose all that apply.)	b. They ensure that the original drive doesn't become corrupt and damage the digital evidence. c. They create a copy of the original drive. look up review sheet
16. The standards for testing forensics tools are based on which criteria?	c. ISO 17025 look up review sheet
17. Which of the following tools can examine files created by WinZip?	a. FTK look up review sheet
18. List four subfunctions of reconstructing drives.	disk-to-disk copy, image-to-disk copy, partition-to-partition copy, image-to-partition copy
19. When validating the results of a forensic analysis, you should do which of the following?	d. Do both a and b. refer to review sheet
20. NIST testing procedures are valid only for government agencies. True or False?	False look up pgs.

Created by: settleup22

Q.5) Of all the proprietary formats, which one is the unofficial standard?