CySA+

Cybersecurity Analyst

CCI
Post Office Box 9627
Mississippi State, MS 39762

CySA+

Part 3

Cyber Incident Response

Preparing the Incident Response Toolkit

Chapter 9

Outline

- Digital Forensics
- Forensic Investigation Suit
- Building Your Forensic Kit
- Quiz

Digital Forensics

- Digital Forensics
  - The process of analyzing collected data to determine if and how an incident happened
  - Answers the questions of what, where, when, and how
  - The questions of who and why are answered by the rest of the investigation process
- Each investigation should be guided by the three principles the National Institute of Justice has identified
  - Actions taken to secure and collect digital evidence should not affect the integrity of that evidence
  - The person examining digital evidence should be trained for that purpose
  - Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved and available for review

[1]

Digital Forensics

- **Phases of an investigation**
  - **Seizure**
    - **The process of controlling the crime scene and the state of possible evidence**
  - **Acquisition**
    - **The preservation of evidence in a legally acceptable manner**
  - **Analysis**
    - **In a controlled environment, analyze the evidence without tainting it**
  - **Reporting**
    - **A complete, accurate, and unbiased report**
- **Side Note:**
  - **Many organization combined seizure and acquisition into one phase**

[1]

Seizure

- Seizure
  - Goal is to ensure neither advisory nor investigator makes any changes to the evidence
  - Controlling the Crime Scene
    - Ensure the integrity of the evidence, whether physical or digital
    - Steps to protect the crime scene
      - Allow access to only authorized individuals
      - Ensure only trained and certified individuals are involved in technical tasks
      - Keep a log of the individuals at the crime scene
      - Document the last individuals to interact with the system
      - Ensure to document any contamination of the crime scene
        - » Contamination does not negate the procured evidence, but it does complicate the investigation

[1]

Seizure

- Do not power off a system unless required
  - If evidence is being destroyed on the system, then you must pull the plug to save what evidence you can
  - Many reasons to keep a machine running one being to collect the volatile memory
  - Memory Forensics
    - Digital forensics on the primary storage units of a system
    - Almost impossible for an advisory to hide tracks in running memory
    - An increasing number of malware lives in memory
  - Acquiring volatile memory
    - Requires imaging the machine while it is running
    - Imaging causes changes to the machine
    - Anything that causes changes to the machine must be documented

[1]

Seizure

- Document the Crime Scene
  - An important part of an investigation is documenting the entire physical environment
  - Take pictures from every angle around a device, such as
    - Computer monitor
      - If unlocked, might have running processes or desktop programs
    - Devices connected to the machine
      - E.g., thumb drive or external drive
    - Immediate surroundings
      - E.g., physical desktop or cables
    - Proximate surroundings
      - E.g., Room or cubicle
  - Take notes of the physical environment and every action taken to seize evidence

[1]

Seizure

- Unplug, tag, label, inventory
  - After documenting the crime scene, there should be no questions of what was where
  - Will need tools for removal and disassembly such as
    - Antistatic bands, pliers, and screwdrivers
  - Need appropriate inventory bags
    - E.g., antistatic bags and evidence bags
    - Weather might also be a factor ensure evidence is packaged so that it’s not damaged in transition

[1]

Seizure

- Chain of Custody
  - Documentation that shows the history of each stage of the process
    - how evidence was collected, transported, and preserved
  - Provides integrity of digital evidence, which is easily modified
- Chain of Custody Lifecycle
  - Begins with identification of evidence
  - Ends with the distraction, permanent archiving, or returning the evidence to the owner

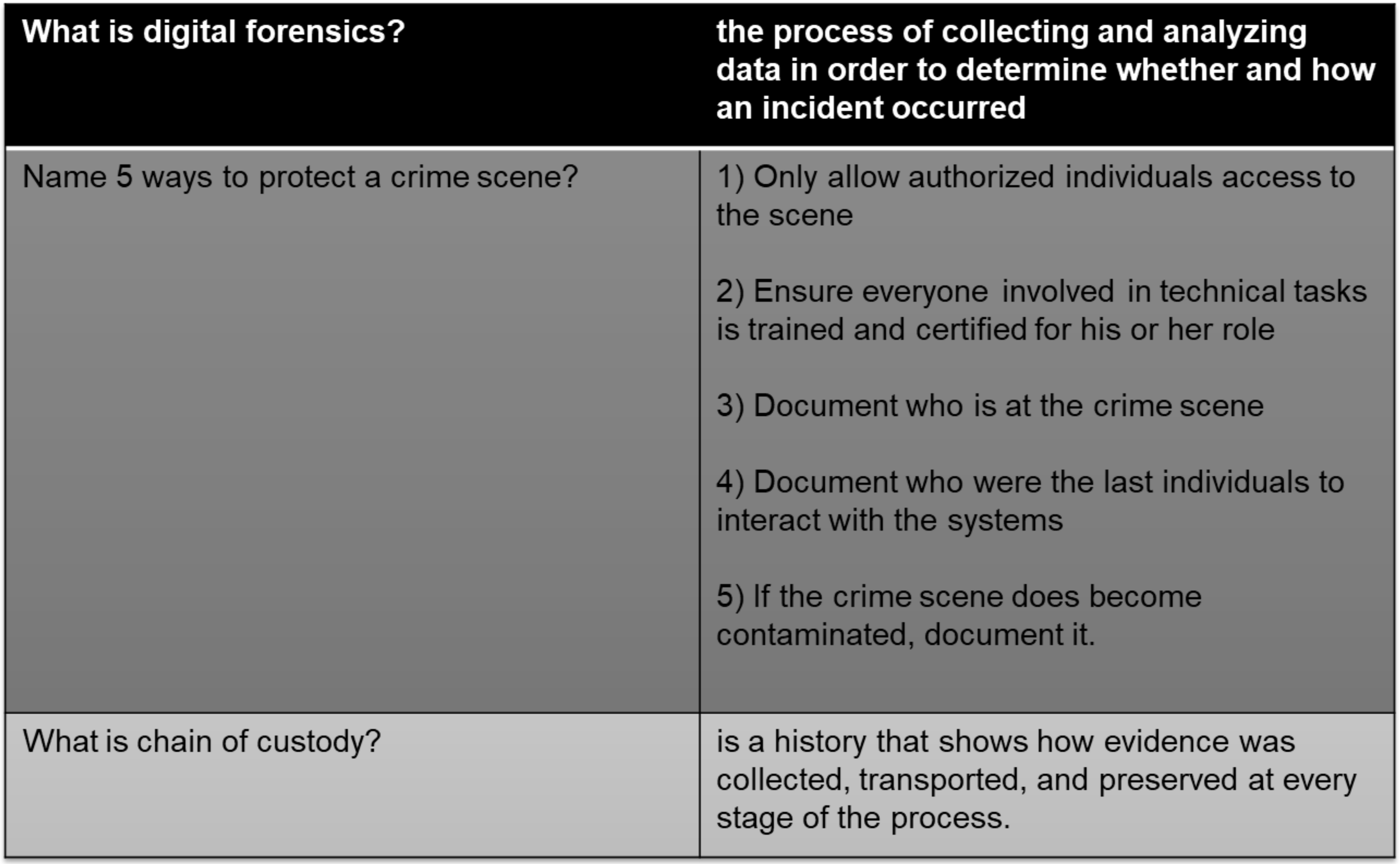
[1]

Interactive Exercise 1

What is digital forensics?	
Name 5 ways to protect a crime scene?	
What is chain of custody?	

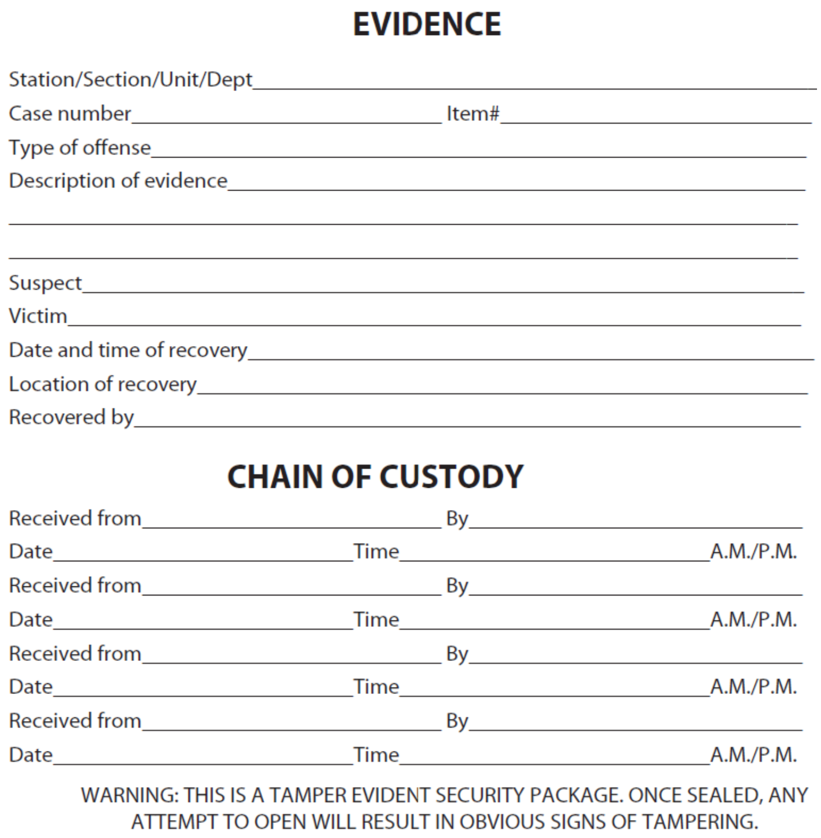
[1,2]

Interactive Example 1 Answers



What is digital forensics?	the process of collecting and analyzing data in order to determine whether and how an incident occurred
Name 5 ways to protect a crime scene?	1) Only allow authorized individuals access to the scene 2) Ensure everyone involved in technical tasks is trained and certified for his or her role 3) Document who is at the crime scene 4) Document who were the last individuals to interact with the systems 5) If the crime scene does become contaminated, document it.
What is chain of custody?	is a history that shows how evidence was collected, transported, and preserved at every stage of the process.

[1,2]



EVIDENCE

Station/Section/Unit/Dept________________________________

Case number__________________ Item#__________________

Type of offense________________________________

Description of evidence________________________________

____

____

Suspect________________________________

Victim________________________________

Date and time of recovery________________________________

Location of recovery________________________________

Recovered by________________________________

CHAIN OF CUSTODY

Received from__________________ By__________________

Date__________________Time__________________A.M./P.M.

Received from__________________ By__________________

Date__________________Time__________________A.M./P.M.

Received from__________________ By__________________

Date__________________Time__________________A.M./P.M.

Received from__________________ By__________________

Date__________________Time__________________A.M./P.M.

WARNING: THIS IS A TAMPER EVIDENT SECURITY PACKAGE. ONCE SEALED, ANY ATTEMPT TO OPEN WILL RESULT IN OBVIOUS SIGNS OF TAMPERING.

Chain Of Custody Ex

Above is an empty evidence container data form implements chain of custody.

[1]

Seizure

- Servers
  - Issues
    - Usually, can not be removed from the production environment
    - Have significantly more storage than a normal workstation
  - Live Forensics
    - Is conducting digital forensics on a device that remains operational during the investigation
    - Is useful if the server cannot be moved to an analysis room
- Mobile Devices
  - Mobile devices must be powered off or placed in a faraday bag to be disconnected from the network
  - Faraday Bag
    - Made of material that absorbs radio frequency (RF) energy and redistributes it
    - Prevents communication from outside devices

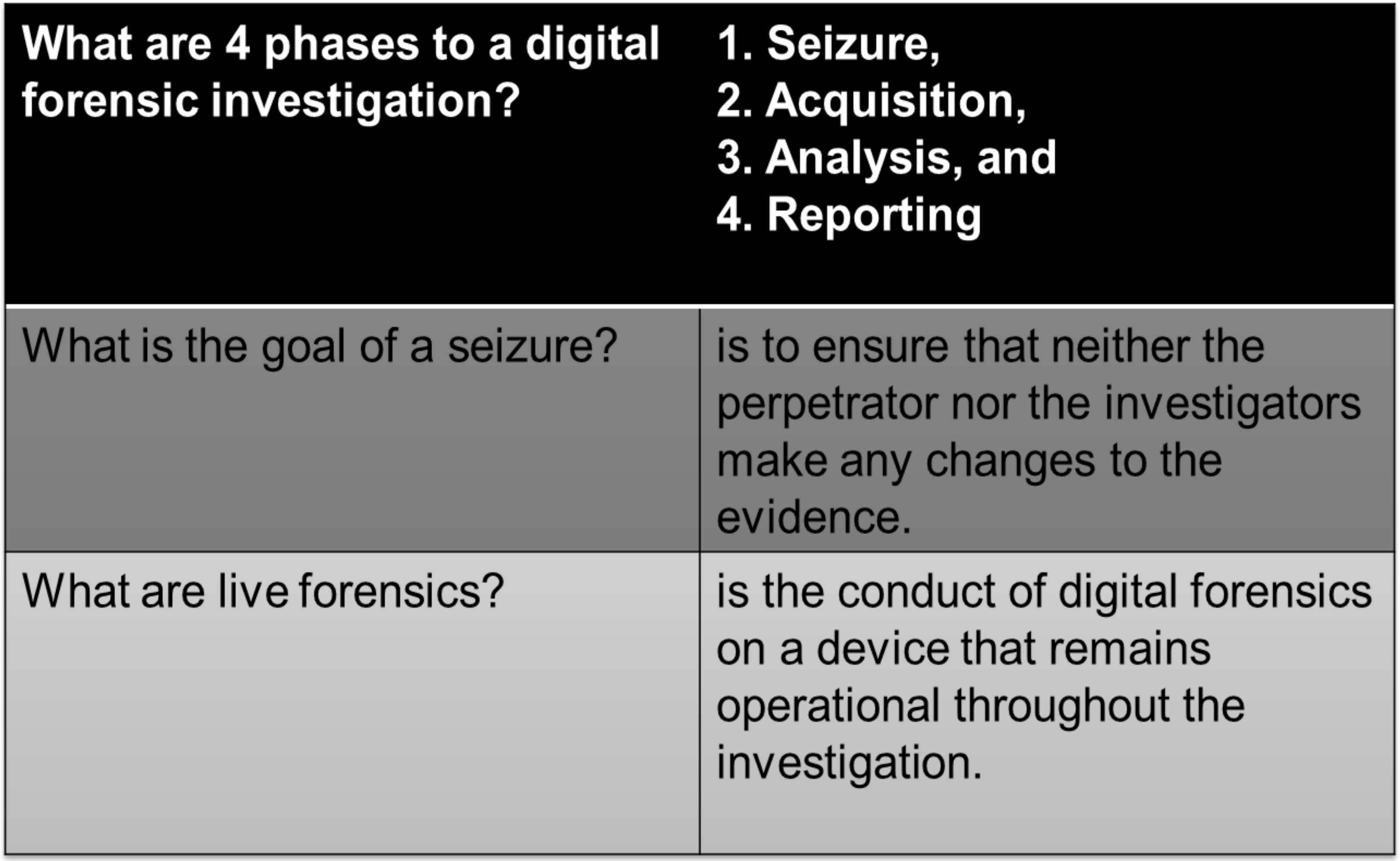
[1]

Interactive Exercise 2

What are 4 phases to a digital forensic investigation?	
What is the goal of a seizure?	
What are live forensics?	

[1,2]

Interactive Example 2 Answers



What are 4 phases to a digital forensic investigation?	1. Seizure, 2. Acquisition, 3. Analysis, and 4. Reporting
What is the goal of a seizure?	is to ensure that neither the perpetrator nor the investigators make any changes to the evidence.
What are live forensics?	is the conduct of digital forensics on a device that remains operational throughout the investigation.

[1,2]

Acquisition

- Forensic acquisition
  - Process of extracting digital content from seized devices and analyzing it
  - Also known as taking a forensic image
  - It is vital to make a copy of the original seized device and only perform analysis on the copy
    - Protects and preserves the original media
- Forensic Acquisition Best Practices
  - Prepare the destination media
    - When extracting digital content, it is important to store the content on a clean device
    - Securely wipe the media before storing digital evidence
  - Prevent changes to the original
    - Hardware write blockers will prevent evidence from being changed when extracting digital content

[1]

Acquisition

- Forensic Acquisition Best Practices
  - Hash the original evidence
    - Hash should be taken before and after extracting digital evidence to ensure the integrity of the copy
  - Copy the evidence
    - There are a variety of applications that can be used to copy digital content such as
      - dd a Linux utility
    - These type of applications perform complete binary copies
  - Verify the acquisition
    - Take a hash of the copy and compare it to the original hash to ensure the copy has not been modified
  - Safeguard the original evidence
    - Only perform analysis on the copy
    - Ensure the original is stored in a safe place and cannot be modified

[1]

Analysis

- **Analysis**
  - **Process of interpreting the digital content extracted and determining the significates of it to the case**
- **Types of Analysis include**
  - **Timeframe**
    - **Determining the timeline of what happened**
  - **Data hiding**
    - **Finding any intentionally concealed data**
  - **Application and file**
    - **Determining what applications accessed which files**
  - **Ownership and possession**
    - **Determining the users that accessed applications and files**

[1]

Analysis

- Most important forensic analyst tool is the timeline
  - Establishes a framework for comparing the system states at different points
- Timeline
  - An ordered list of actions taken on the system
- System actions
  - Read, Write, Modify, and Delete Operations
- Many investigators use a spreadsheet to keep track of their timelines
- List of timeline spreadsheet columns
  - Data and time
  - Time zone
  - Source
    - E.g., Windows Registry or Syslog
  - Item Name
    - E.g., Registry Key name or filename
  - Item location
    - E.g., full path
  - Description

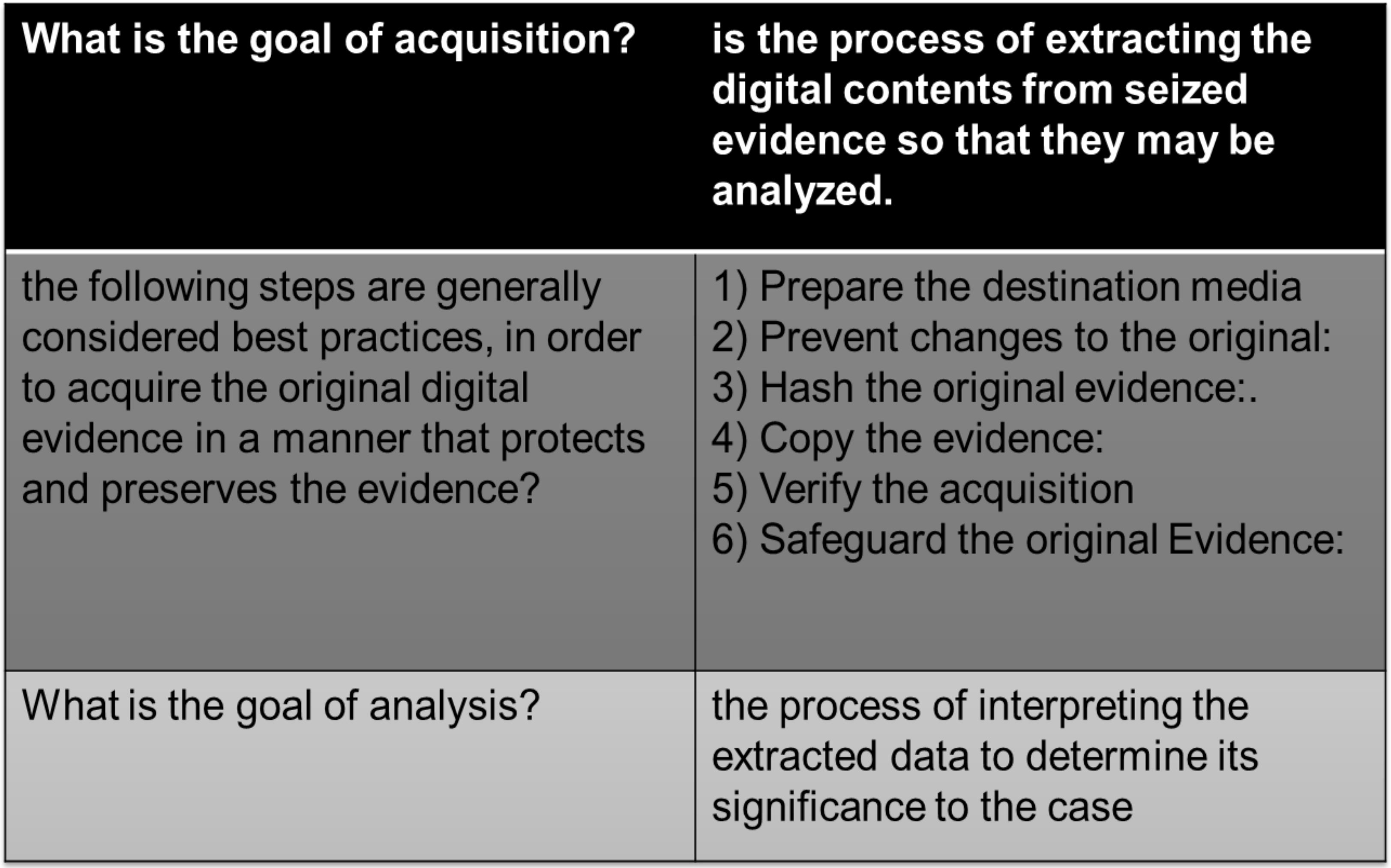
[1]

Interactive Exercise 3

What is the goal of acquisition?	
the following steps are generally considered best practices, in order to acquire the original digital evidence in a manner that protects and preserves the evidence?	
What is the goal of analysis?	

[1,2]

Interactive Exercise 3 Answers



What is the goal of acquisition?	is the process of extracting the digital contents from seized evidence so that they may be analyzed.
the following steps are generally considered best practices, in order to acquire the original digital evidence in a manner that protects and preserves the evidence?	1) Prepare the destination media 2) Prevent changes to the original: 3) Hash the original evidence:. 4) Copy the evidence: 5) Verify the acquisition 6) Safeguard the original Evidence:
What is the goal of analysis?	the process of interpreting the extracted data to determine its significance to the case

[1,2]

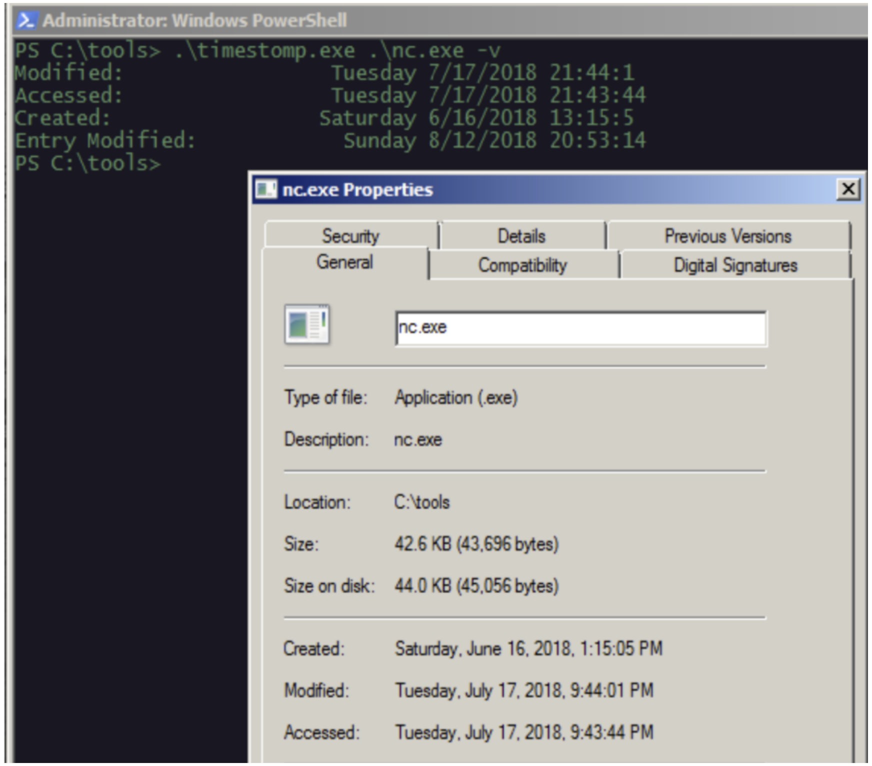
Analysis

- **Timestomping**
  - Modifies the timestamp on files
  - Used to hide the true sequence of events on a system
  - During analysis have a healthy dose of skepticism when looking at system timestamps
- **Best Practice**
  - Through your analysis, it is best to take notes of everything you do
  - EnCase and FTK will record your actions for but still best to take your notes

[1]

Timestomping Ex

Before:



```
PS C:\tools> .\timestomp.exe .\nc.exe -v
Modified:                  Tuesday 7/17/2018 21:44:1
Accessed:                  Tuesday 7/17/2018 21:43:44
Created:                  Saturday 6/16/2018 13:15:5
Entry Modified:             Sunday 8/12/2018 20:53:14
PS C:\tools>
```

nc.exe

Type of file: Application (.exe)

Description: nc.exe

Location: C:\tools

Size: 42.6 KB (43,696 bytes)

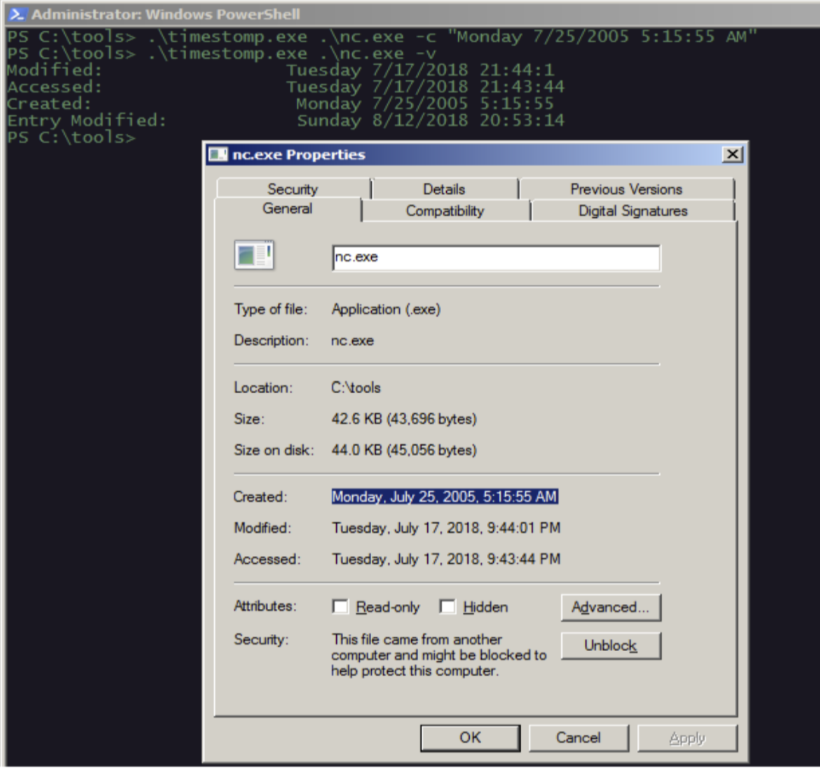
Size on disk: 44.0 KB (45,056 bytes)

Created: Saturday, June 16, 2018, 1:15:05 PM

Modified: Tuesday, July 17, 2018, 9:44:01 PM

Accessed: Tuesday, July 17, 2018, 9:43:44 PM

After:



```
PS C:\tools> .\timestomp.exe .\nc.exe -c "Monday 7/25/2005 5:15:55 AM"
PS C:\tools> .\timestomp.exe .\nc.exe -v
Modified:                  Tuesday 7/17/2018 21:44:1
Accessed:                  Tuesday 7/17/2018 21:43:44
Created:                    Monday 7/25/2005 5:15:55
Entry Modified:             Sunday 8/12/2018 20:53:14
PS C:\tools>
```

nc.exe

Type of file: Application (.exe)

Description: nc.exe

Location: C:\tools

Size: 42.6 KB (43,696 bytes)

Size on disk: 44.0 KB (45,056 bytes)

Created: Monday, July 25, 2005, 5:15:55 AM

Modified: Tuesday, July 17, 2018, 9:44:01 PM

Accessed: Tuesday, July 17, 2018, 9:43:44 PM

Attributes: ☐ Read-only ☐ Hidden

Security: This file came from another computer and might be blocked to help protect this computer.

[3]

Reporting

- Reporting
  - Notes Taken
    - All the notes that have taken so far can and should be part of your report
  - Reporting Evidence
    - Present the evidence in the report in a way that displays your arguments and conclusions in a readable fashion
  - Knowing your Audience
    - Your audience will determine how you present your findings
    - The report will be vastly different if it were geared toward executive leaders rather than the court of law
    - Major commercial suites have features that can generate customizable draft reports

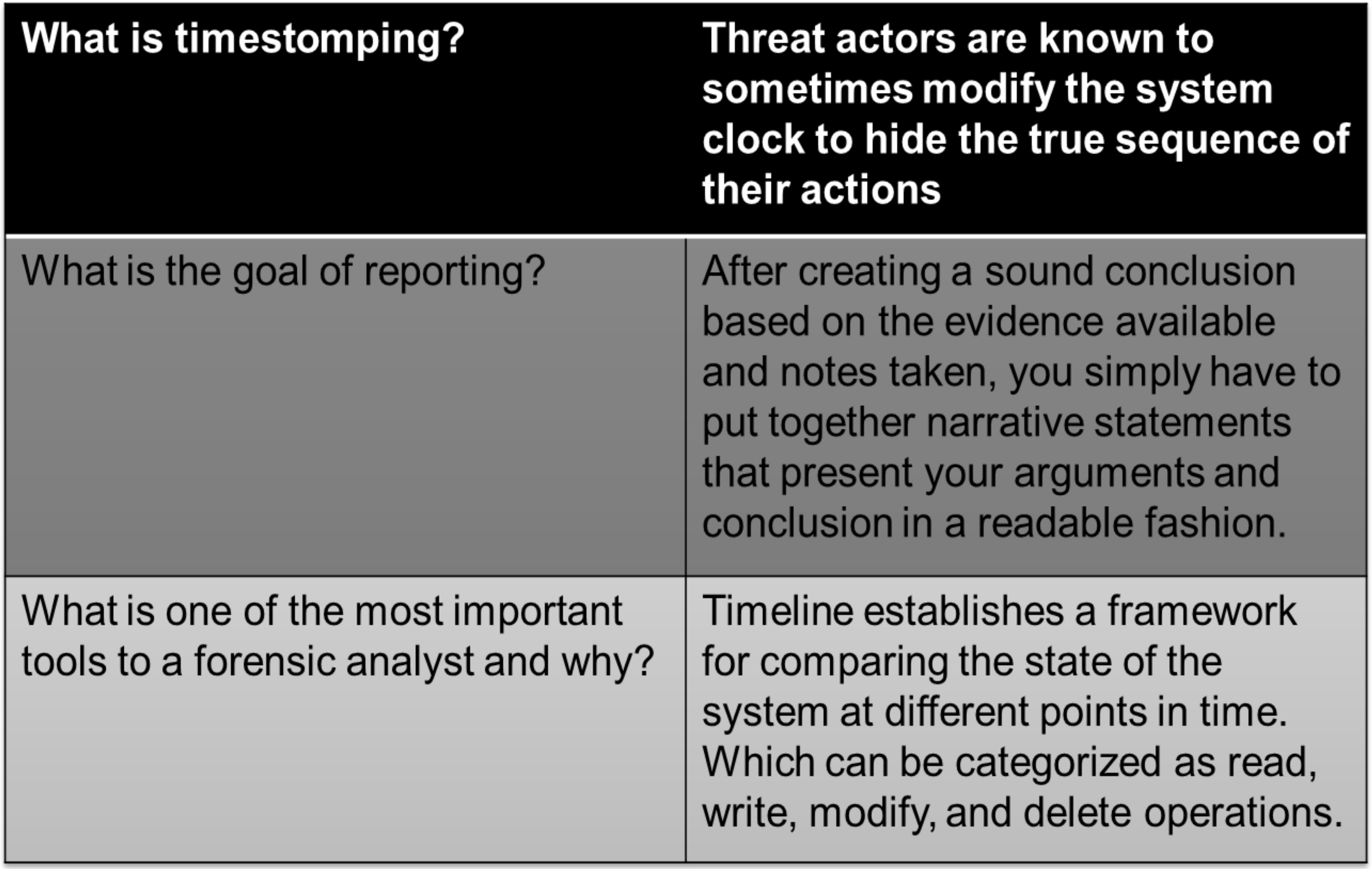
[1]

Interactive Exercise 4

What is timestomping?	
What is the goal of reporting?	
What is one of the most important tools to a forensic analyst and why?	

[1,2]

Interactive Exercise 4 Answers



What is timestomping?	Threat actors are known to sometimes modify the system clock to hide the true sequence of their actions
What is the goal of reporting?	After creating a sound conclusion based on the evidence available and notes taken, you simply have to put together narrative statements that present your arguments and conclusion in a readable fashion.
What is one of the most important tools to a forensic analyst and why?	Timeline establishes a framework for comparing the state of the system at different points in time. Which can be categorized as read, write, modify, and delete operations.

[1,2]

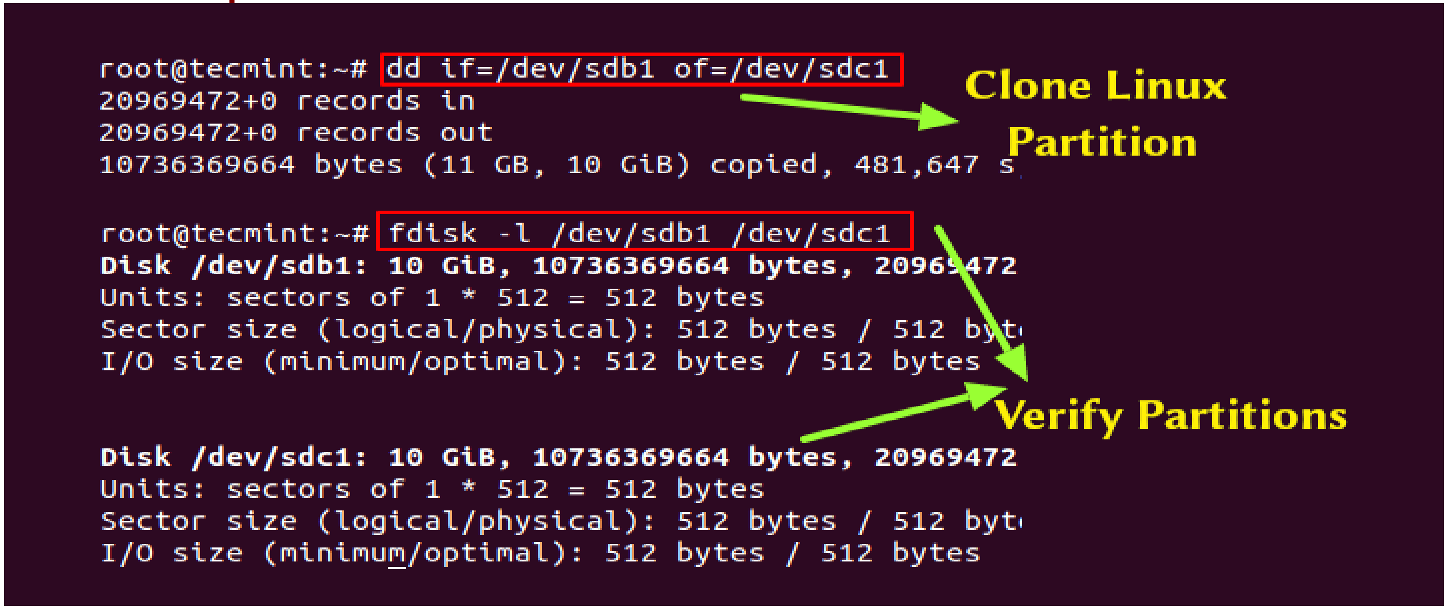
Forensic Investigation Suit

- Acquisition Phase
  - Critical point of the investigation
  - Must ensure that all evidence, analysis, and conclusions are admissible
  - Ensure no mistakes are made by slowing down and using a checklist
    - Any mistakes might possibly invalidate the work that follows
- Forensic Duplicators
  - Systems that copy data from a source to a destination
  - Ensures that not a single bit is altered in the process
  - Do not rely on file system operations
  - Can recover system artifacts such as Master File Table (MFT)

[1]

Forensic Investigation Suit

- **dd**
  - **Default link command that can perform a bit-for-bit copy of files, devices, partitions, and volumes**
  - **E.g. dd if=/dev/data of=case123.img bs=4k**
  - **Does not produce a hash of the file**
    - **Can use Linux commands sha1sum, sh256sum, or md5 to get a hash of the copied file**



```
root@tecmint:~# dd if=/dev/sdb1 of=/dev/sdc1
20969472+0 records in
20969472+0 records out
10736369664 bytes (11 GB, 10 GiB) copied, 481,647 s

root@tecmint:~# fdisk -l /dev/sdb1 /dev/sdc1
Disk /dev/sdb1: 10 GiB, 10736369664 bytes, 20969472
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 byt
I/O size (minimum/optimal): 512 bytes / 512 bytes


Disk /dev/sdc1: 10 GiB, 10736369664 bytes, 20969472
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 byt
I/O size (minimum/optimal): 512 bytes / 512 bytes
```

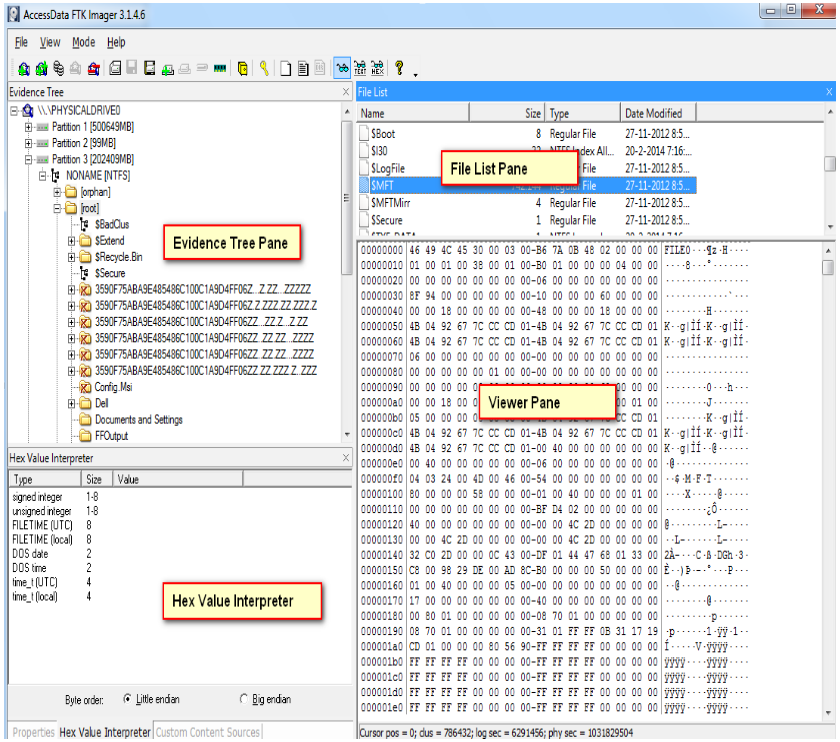
Clone Linux Partition

Verify Partitions

[1,4]

Forensic Investigation Suit

- **FTK Imager**
  - **Developed by Access Data**
  - **Data preview and imaging tool**
  - **Full-featured product**
    - **Generates MD5 and SHA-1 hashes**
    - **Can preview the files and folders in a read-only fashion**
    - **Can preview Windows registry keys and their value**
    - **Supports compression and encryption**
    - **Supports and outputs EnCase (E01) and dd (001) formats**



```
\\.\PHYSICALDRIVE0
  Partition 1 [500649MB]
  Partition 2 [99MB]
  Partition 3 [202409MB]
    NONAME [NTFS]
      [orphan]
      [root]
        $BadClus
        $Extend
        $Recycle.Bin
        $Secure
        3590F75ABA9E485486C100C1A9D4FF06Z...Z.ZZ...ZZZZZ
        3590F75ABA9E485486C100C1A9D4FF06Z.Z.ZZZ.ZZ.ZZZ.Z
        3590F75ABA9E485486C100C1A9D4FF06ZZ...ZZ.Z...Z.ZZ
        3590F75ABA9E485486C100C1A9D4FF06ZZ..ZZ.ZZ...ZZZZ
        3590F75ABA9E485486C100C1A9D4FF06ZZ..ZZ.ZZ...ZZZZ
        3590F75ABA9E485486C100C1A9D4FF06ZZ.ZZ.ZZZ.Z..ZZZ
        Config.Msi
        Dell
        Documents and Settings
        FFOutput
```

Name	Size	Type	Date Modified
$Boot	8	Regular File	27-11-2012 8:5...
$I30	32	NTFS Index All...	20-2-2014 7:16:...
$LogFile		File	27-11-2012 8:5...
$MFT	742.144	Regular File	27-11-2012 8:5...
$MFTMirr	4	Regular File	27-11-2012 8:5...
$Secure	1	Regular File	27-11-2012 8:5...

```
00000000 46 49 4C 45 30 00 03 00-B6 7A 0B 48 02 00 00 00 FILE0···¶z·H····
00000010 01 00 01 00 38 00 01 00-B0 01 00 00 00 04 00 00 ····8···°·······
00000020 00 00 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ················
00000030 8F 94 00 00 00 00 00 00-10 00 00 00 60 00 00 00 ············`···
00000040 00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00 ········H·······
00000050 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000060 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000070 06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000080 00 00 00 00 00 01 00 00-00 00 00 00 00 00 00 00 ················
00000090 00 00 00 00 0                          00 00 00 ········0···h···
000000a0 00 00 18 00 0                          00 01 00 ········J·······
000000b0 05 00 00 00 0                          CC CD 01 ········K··g|ÌÍ·
000000c0 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
000000d0 4B 04 92 67 7C CC CD 01-00 40 00 00 00 00 00 00 K··g|ÌÍ··@······
000000e0 00 40 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ·@··············
000000f0 04 03 24 00 4D 00 46 00-54 00 00 00 00 00 00 00 ··$·M·F·T·······
00000100 80 00 00 00 58 00 00 00-01 00 40 00 00 00 01 00 ····X·····@·····
00000110 00 00 00 00 00 00 00 00-BF D4 02 00 00 00 00 00 ········¿Ô······
00000120 40 00 00 00 00 00 00 00-00 00 4C 2D 00 00 00 00 @·········L-····
00000130 00 00 4C 2D 00 00 00 00-00 00 4C 2D 00 00 00 00 ··L-······L-····
00000140 32 C0 2D 00 00 0C 43 00-DF 01 44 47 68 01 33 00 2À-···C·ß·DGh·3·
00000150 C8 00 98 29 DE 00 AD 8C-B0 00 00 00 50 00 00 00 È··)Þ··°···P···
00000160 01 00 40 00 00 00 05 00-00 00 00 00 00 00 00 00 ··@·············
00000170 17 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ········@·······
00000180 00 80 01 00 00 00 00 00-08 70 01 00 00 00 00 00 ·········p······
00000190 08 70 01 00 00 00 00 00-31 01 FF FF 0B 31 17 19 ·p······1·ÿÿ·1··
000001a0 CD 01 00 00 00 80 56 90-FF FF FF FF 00 00 00 00 Í·····V·ÿÿÿÿ····
000001b0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001c0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001d0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001e0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
```

Cursor pos = 0; clus = 786432; log sec = 6291456; phy sec = 1031829504

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (UTC)	8	
FILETIME (local)	8	
DOS date	2	
DOS time	2	
time_t (UTC)	4	
time_t (local)	4	

Byte order: ● Little endian ○ Big endian

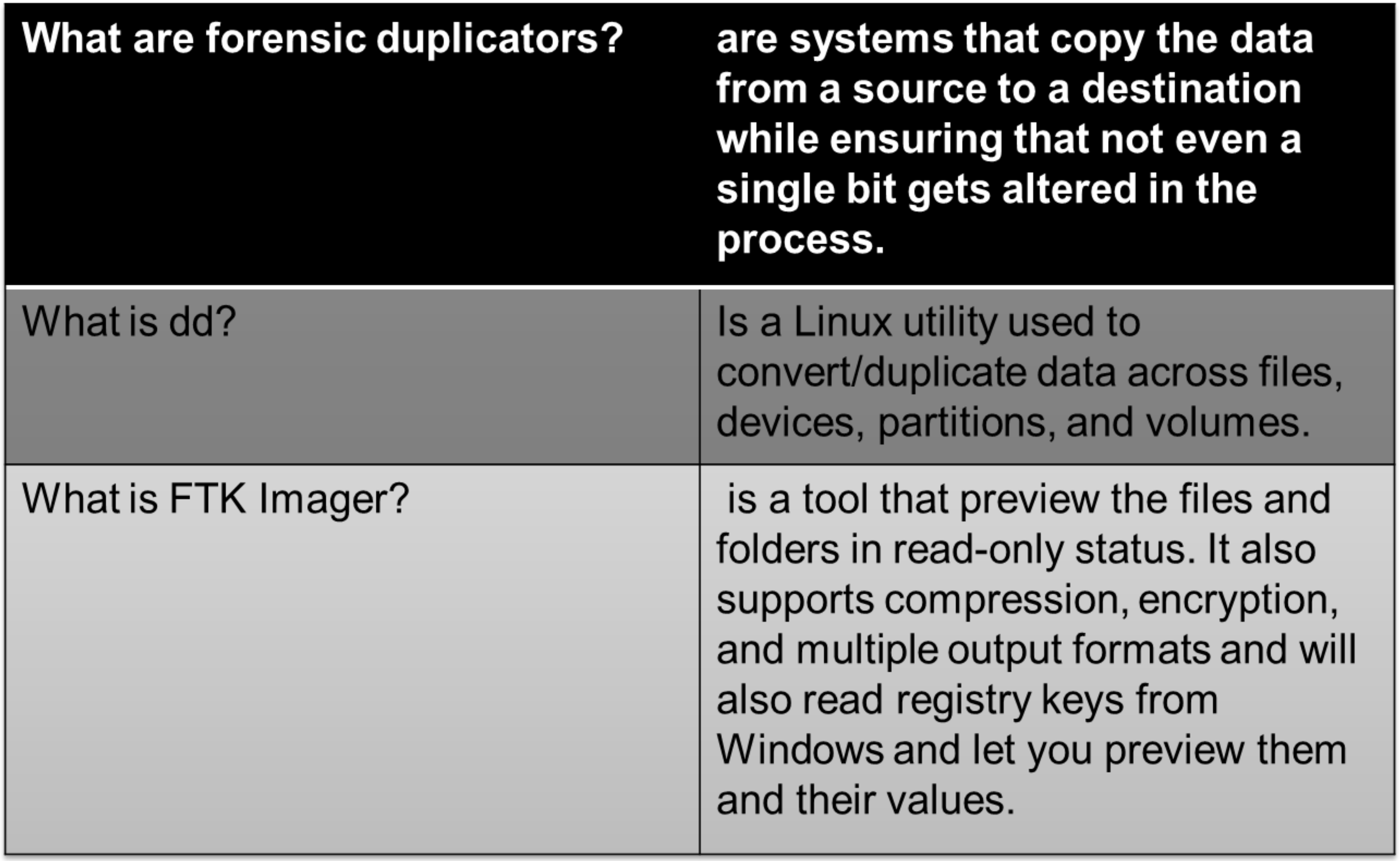
[5]

Interactive Exercise 5

What are forensic duplicators?	
What is dd?	
What is FTK Imager?	

[1,2]

Interactive Exercise 5 Answers



What are forensic duplicators?	**are systems that copy the data from a source to a destination while ensuring that not even a single bit gets altered in the process.**
What is dd?	Is a Linux utility used to convert/duplicate data across files, devices, partitions, and volumes.
What is FTK Imager?	is a tool that preview the files and folders in read-only status. It also supports compression, encryption, and multiple output formats and will also read registry keys from Windows and let you preview them and their values.

[1,2]

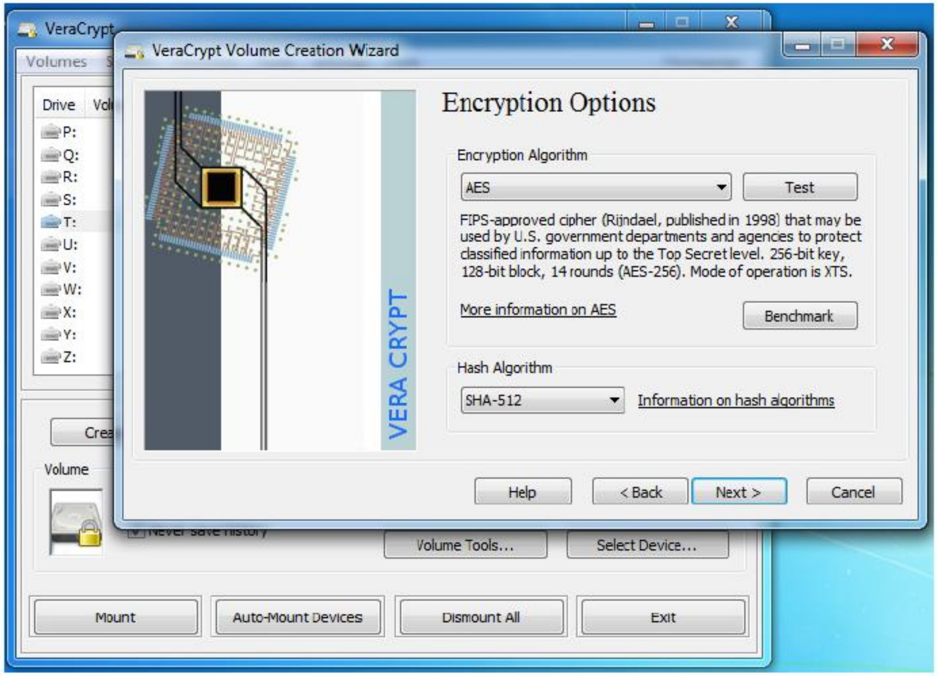
Forensic Investigation Suit

- **Password Cracker**
  - **Software designed to guess passwords and decrypt protected resources**
  - **Password Kit Forensic**
    - **Commercial option**
    - **Can be used with EnCase**
    - **Can decrypt over 280 different types of protected files such as**
      - **BitLocker, File Vault, iCloud, and Dropbox**
    - **Can utilize graphics processing units (GPUs) to accelerate the time taken to crack the password**

[1]

Forensic Investigation Suit

- Cryptography Tool
  - VeraCrypt
    - Open Source option
    - Based on TrueCrypt
    - Available for Windows, OS X, and Linux systems
    - Supports multiple cryptosystems such as
      - AES, TwoFish, and Serpent
    - Supports creation of hidden, encrypted volumes within other volumes
      - As seen in the figure to the right,



Encryption Options

Encryption Algorithm: AES

FIPS-approved cipher (Rijndael, published in 1998) that may be used by U.S. government departments and agencies to protect classified information up to the Top Secret level. 256-bit key, 128-bit block, 14 rounds (AES-256). Mode of operation is XTS.

Hash Algorithm: SHA-512

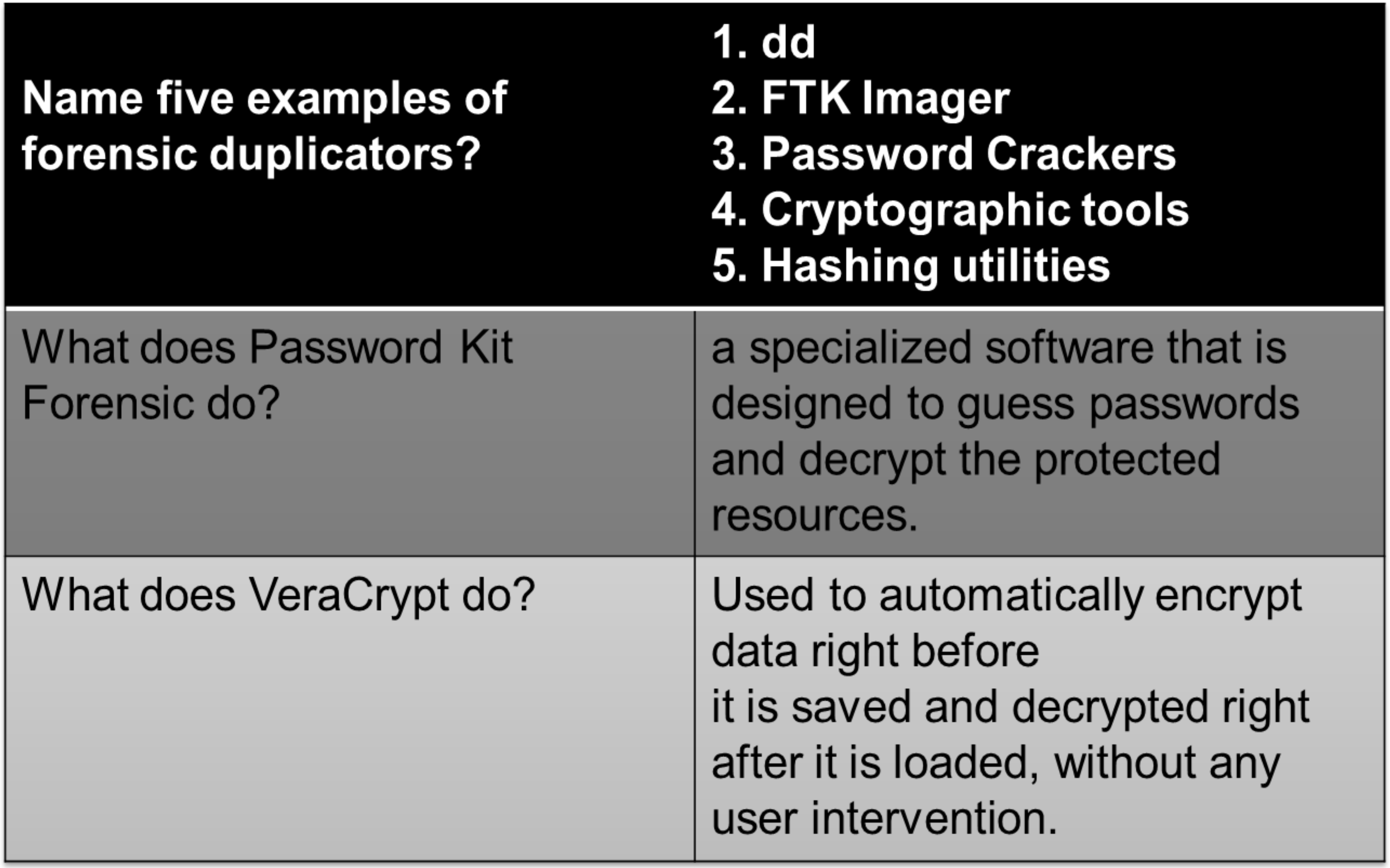
[1]

Interactive Exercise 6

Name five examples of forensic duplicators?	
What does Password Kit Forensic do?	
What does VeraCrypt do?	

[1,2]

Interactive Exercise 6 Answers



Name five examples of forensic duplicators?	**1. dd** **2. FTK Imager** **3. Password Crackers** **4. Cryptographic tools** **5. Hashing utilities**
What does Password Kit Forensic do?	a specialized software that is designed to guess passwords and decrypt the protected resources.
What does VeraCrypt do?	Used to automatically encrypt data right before it is saved and decrypted right after it is loaded, without any user intervention.

[1,2]

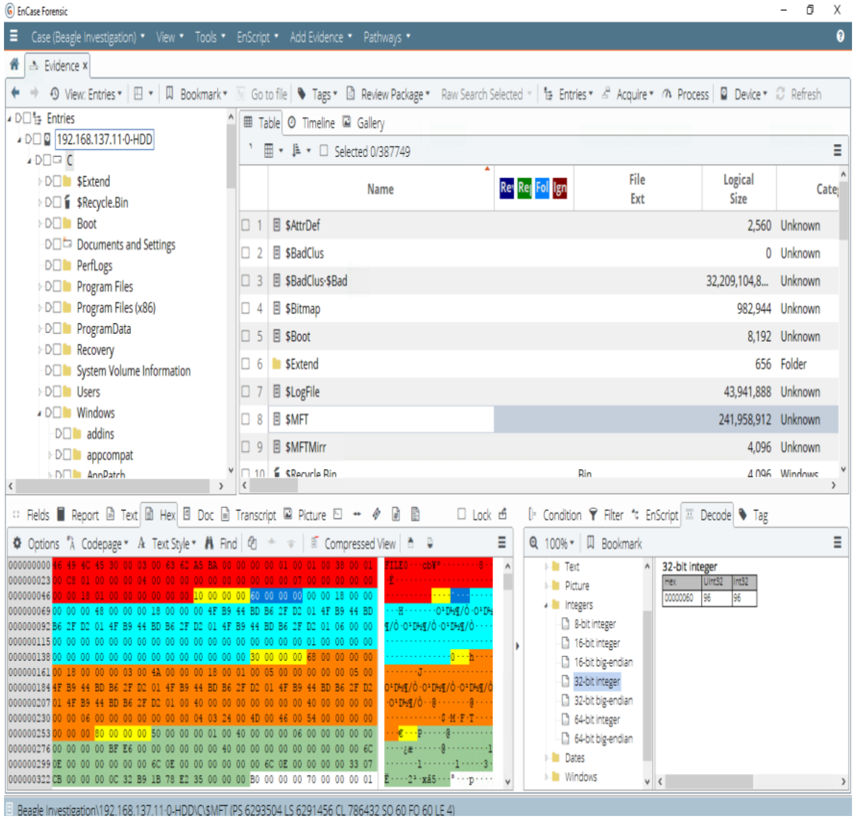
Forensic Investigation Suit

- **Hashing Utilities**
  - **MD5 and SHA-1**
    - **Most popular hashing tools for forensic analysis**
  - **Many operating system support md5 and sha-1 by default**
    - **Mac OS supports the md5 tool**
    - **Linux usually has md5 and sha1sum**
    - **Microsoft has the File Checksum Integrity Verifier (FCIV) tool**
      - **FCIV can compute md5 and sha-1 hashes**
- **Analysis Utilities**
  - **Commercial Analysis Tools**
    - **Guidance Software's EnCase**
    - **Access Data's Forensic Toolkit (FTK)**
  - **Open Source Analysis Tool**
    - **The Sleuth Kit**

[1]

Forensic Investigation Suit

- **EnCase**
  - **Law enforcement agencies and other large corporations utilize this tool**
  - **It is an analysis, acquisition, and reporting tool**
  - **Creates a widely used EnCase Evidence File Format**
    - **Files in this format usually have an .E01 file extension**
    - **The E01 format compresses and encrypts into one file**
      - **The bit-for-bit image of the evidence drive**
      - **The copy**
      - **The hash value**
      - **The metadata, such as the evidence label and case number**



	Name	Rev Rep Fol Ign	File Ext	Logical Size	Categ
□ 1	$AttrDef			2,560	Unknown
□ 2	$BadClus			0	Unknown
□ 3	$BadClus·$Bad			32,209,104,8...	Unknown
□ 4	$Bitmap			982,944	Unknown
□ 5	$Boot			8,192	Unknown
□ 6	$Extend			656	Folder
□ 7	$LogFile			43,941,888	Unknown
□ 8	$MFT			241,958,912	Unknown
□ 9	$MFTMirr			4,096	Unknown
□ 10	$Recycle.Bin		Bin	4,096	Windows

```
000000000 46 49 4C 45 30 00 03 00 63 62 A5 BA 00 00 00 00 01 00 01 00 38 00 01
000000023 00 C8 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 07 00 00 00 00 00
000000046 00 00 18 01 00 00 00 00 00 00 10 00 00 00 60 00 00 00 00 00 18 00 00
000000069 00 00 00 48 00 00 00 18 00 00 00 4F B9 44 BD B6 2F D2 01 4F B9 44 BD
000000092 B6 2F D2 01 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2 01 06 00 00
000000115 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00
000000138 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 00 00 68 00 00 00 00
000000161 00 18 00 00 00 03 00 4A 00 00 00 18 00 01 00 05 00 00 00 00 00 05 00
000000184 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2 01 4F B9 44 BD B6 2F D2
000000207 01 4F B9 44 BD B6 2F D2 01 00 40 00 00 00 00 00 00 00 40 00 00 00 00
000000230 00 00 06 00 00 00 00 00 00 00 04 03 24 00 4D 00 46 00 54 00 00 00 00
000000253 00 00 00 80 00 00 00 50 00 00 00 01 00 40 00 00 00 06 00 00 00 00 00
000000276 00 00 00 00 BF E6 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 6C
000000299 0E 00 00 00 00 00 00 6C 0E 00 00 00 00 00 00 6C 0E 00 00 00 00 33 07
000000322 CB 00 00 00 0C 32 B9 1B 78 E2 35 00 00 00 B0 00 00 00 70 00 00 00 01
```

32-bit integer

Hex	UInt32	Int32
00000060	96	96

Beagle Investigation\192.168.137.11-0-HDD\C\$MFT (PS 6293504 LS 6291456 CL 786432 SO 60 FO 60 LE 4)

[6]

Forensic Investigation Suit

- FTK
  - Supports E01 and raw dd file formats
  - Built on top of a database management system
    - FTK can efficiently process large volumes of data
    - The initial upload can take some time due to the data preprocessing and data indexing
- The Sleuth Kit
  - Collection of interoperable tools
    - Most of the tools use a command-line interface
  - Can use Autopsy with The Sleuth Kit
    - Gives the user a graphical user interface to work with
    - Collectively, these tools can mostly do what FTK and EnCase can do

[1]

Interactive Exercise 7

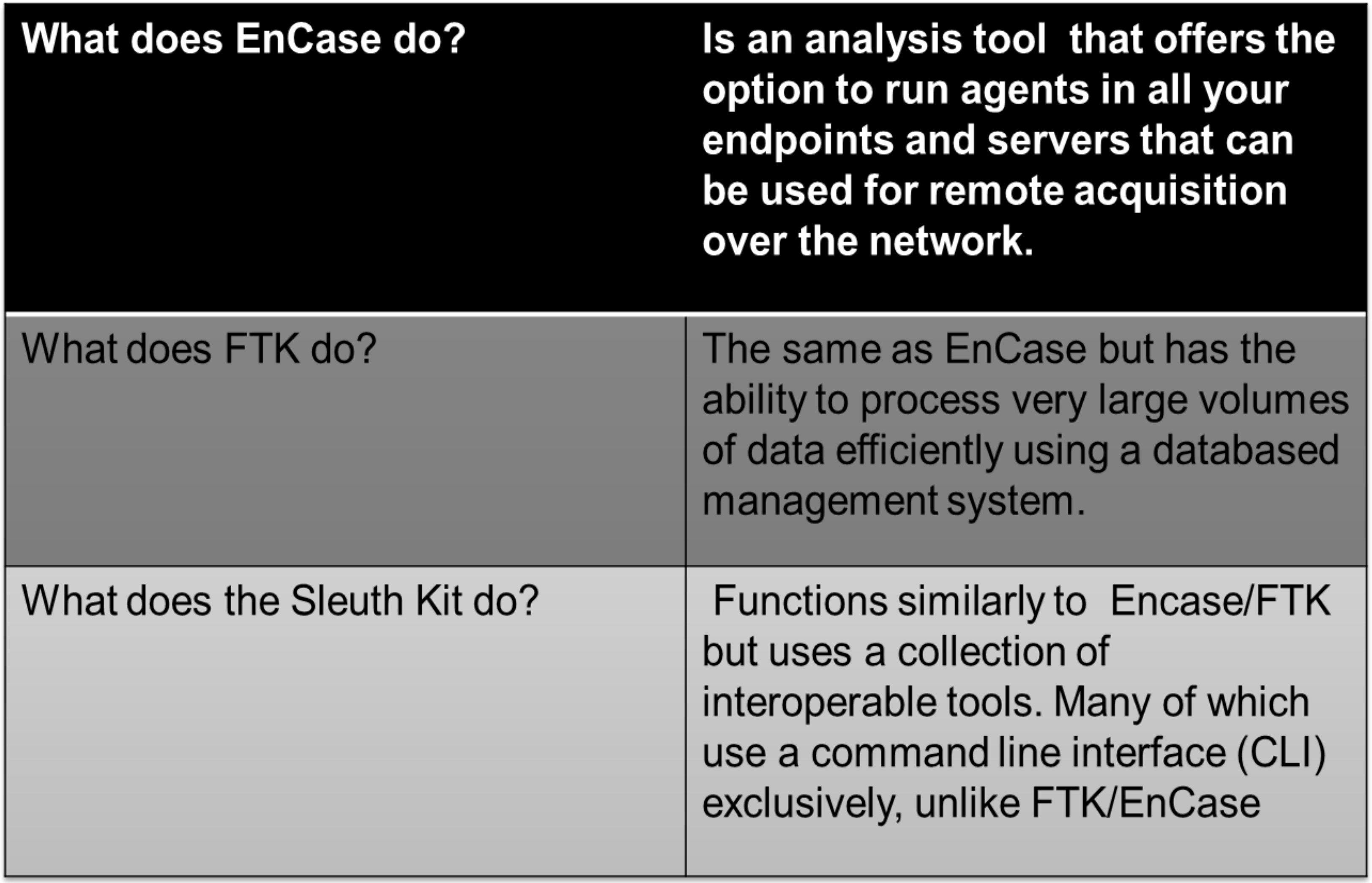
What does EnCase do?

What does FTK do?

What does the Sleuth Kit do?

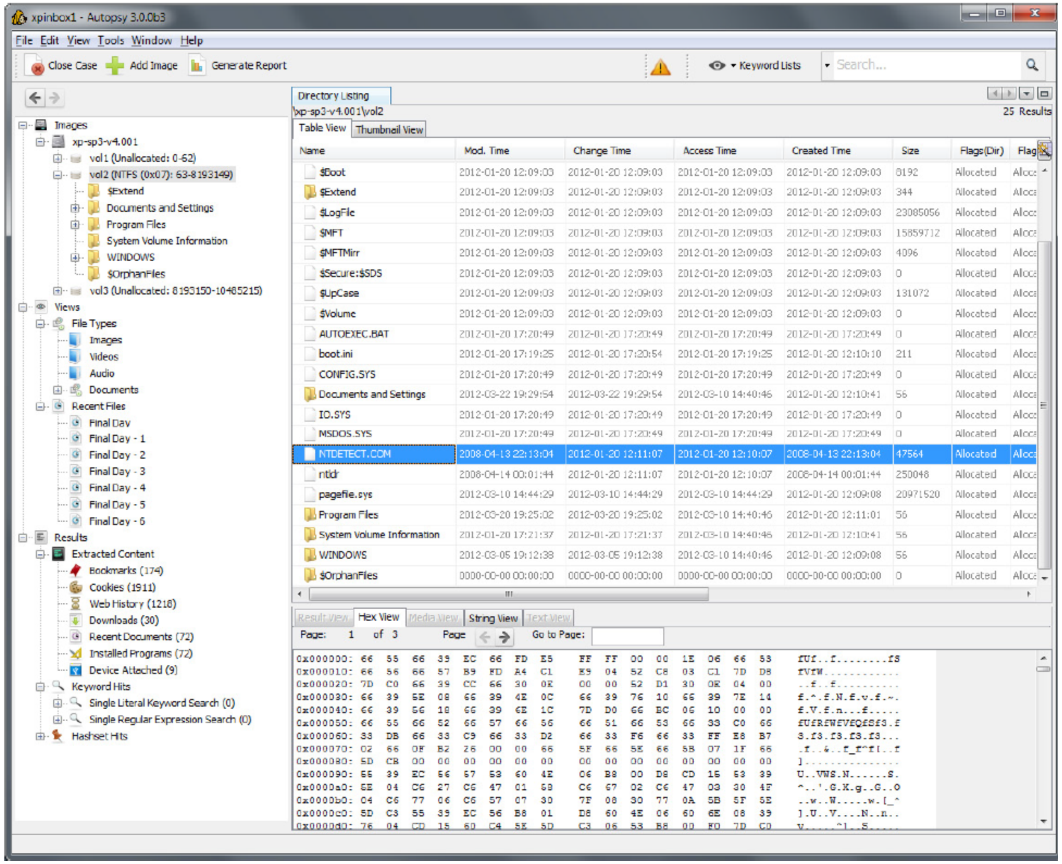
[1,2]

Interactive Exercise 7 Answers



What does EnCase do?	Is an analysis tool that offers the option to run agents in all your endpoints and servers that can be used for remote acquisition over the network.
What does FTK do?	The same as EnCase but has the ability to process very large volumes of data efficiently using a databased management system.
What does the Sleuth Kit do?	Functions similarly to Encase/FTK but uses a collection of interoperable tools. Many of which use a command line interface (CLI) exclusively, unlike FTK/EnCase

[1,2]



xpinbox1 - Autopsy 3.0.0b3

- Images
  - xp-sp3-v4.001
    - vol1 (Unallocated: 0-62)
    - vol2 (NTFS (0x07): 63-8193149)
      - $Extend
      - Documents and Settings
      - Program Files
      - System Volume Information
      - WINDOWS
      - $OrphanFiles
    - vol3 (Unallocated: 8193150-10485215)
- Views
  - File Types
    - Images
    - Videos
    - Audio
    - Documents
  - Recent Files
    - Final Day
    - Final Day - 1
    - Final Day - 2
    - Final Day - 3
    - Final Day - 4
    - Final Day - 5
    - Final Day - 6
- Results
  - Extracted Content
    - Bookmarks (174)
    - Cookies (1911)
    - Web History (1218)
    - Downloads (30)
    - Recent Documents (72)
    - Installed Programs (72)
    - Device Attached (9)
  - Keyword Hits
    - Single Literal Keyword Search (0)
    - Single Regular Expression Search (0)
  - Hashset Hits

Directory Listing

\xp-sp3-v4.001\vol2

Table View | Thumbnail View

25 Results

Name	Mod. Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flag
$Boot	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	8192	Allocated	Alloc:
$Extend	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	344	Allocated	Alloc:
$LogFile	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	23085056	Allocated	Alloc:
$MFT	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	15859712	Allocated	Alloc:
$MFTMirr	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	4096	Allocated	Alloc:
$Secure:$SDS	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc:
$UpCase	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	131072	Allocated	Alloc:
$Volume	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	2012-01-20 12:09:03	0	Allocated	Alloc:
AUTOEXEC.BAT	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc:
boot.ini	2012-01-20 17:19:25	2012-01-20 17:20:54	2012-01-20 17:19:25	2012-01-20 12:10:10	211	Allocated	Alloc:
CONFIG.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc:
Documents and Settings	2012-03-22 19:29:54	2012-03-22 19:29:54	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc:
IO.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc:
MSDOS.SYS	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	2012-01-20 17:20:49	0	Allocated	Alloc:
NTDETECT.COM	2008-04-13 22:13:04	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-13 22:13:04	47564	Allocated	Alloc:
ntldr	2008-04-14 00:01:44	2012-01-20 12:11:07	2012-01-20 12:10:07	2008-04-14 00:01:44	250048	Allocated	Alloc:
pagefile.sys	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-03-10 14:44:29	2012-01-20 12:09:08	20971520	Allocated	Alloc:
Program Files	2012-03-20 19:25:02	2012-03-20 19:25:02	2012-03-10 14:40:46	2012-01-20 12:11:01	56	Allocated	Alloc:
System Volume Information	2012-01-20 17:21:37	2012-01-20 17:21:37	2012-03-10 14:40:46	2012-01-20 12:10:41	56	Allocated	Alloc:
WINDOWS	2012-03-05 19:12:38	2012-03-05 19:12:38	2012-03-10 14:40:46	2012-01-20 12:09:08	56	Allocated	Alloc:
$OrphanFiles	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Allocated	Alloc:

Result View | Hex View | Media View | String View | Text View

Page: 1 of 3 Page Go to Page:

```
0x000000: 66 55 66 39 EC 66 FD E5  FF FF 00 00 1E 06 66 53  fUf..f........fS
0x000010: 66 56 66 57 B9 FD A4 C1  E9 04 52 C8 03 C1 7D D8  fVfW............
0x000020: 7D C0 66 39 CC 66 30 0E  00 00 52 D1 30 0E 04 00  ..f..f..........
0x000030: 66 39 5E 08 66 39 4E 0C  66 39 76 10 66 39 7E 14  f.^.f.N.f.v.f.~.
0x000040: 66 39 56 18 66 39 6E 1C  7D D0 66 BC 06 10 00 00  f.V.f.n...f.....
0x000050: 66 55 66 52 66 57 66 56  66 51 66 53 66 33 C0 66  fUfRfWfVfQfSf3.f
0x000060: 33 DB 66 33 C9 66 33 D2  66 33 F6 66 33 FF E8 B7  3.f3.f3.f3.f3...
0x000070: 02 66 0F B2 26 00 00 66  5F 66 5E 66 5B 07 1F 66  .f..&..f_f^f[..f
0x000080: 5D CB 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ]...............
0x000090: 55 39 EC 56 57 53 60 4E  06 B8 00 D8 CD 15 53 39  U..VWS.N......S.
0x0000a0: 5E 04 C6 27 C6 47 01 5B  C6 67 02 C6 47 03 30 4F  ^..'.G.K.g..G..O
0x0000b0: 04 C6 77 06 C6 57 07 30  7F 08 30 77 0A 5B 5F 5E  ..w..W.....w.[_^
0x0000c0: 5D C3 55 39 EC 56 B8 01  D8 60 4E 06 60 6E 08 39  ].U..V....N..n..
0x0000d0: 76 04 CD 15 60 C4 5E 5D  C3 06 53 B8 00 F0 7D C0  v.....^]..S.....
```

Forensic Investigation Suit

Above is an example of the use Autopsy with The Sleuth Kit.

[1]

Forensic Investigation Suit

- OS and Process Analysis
  - Operating System (OS) has three basic functions
    - Manages all computer resources such as memory, CPU, and disks
    - Provides a user interface
    - Provides services for running applications
  - Process Analysis
    - Every process that occurs on a system is mediated by its OS
    - In Windows, the most important information can be found in the
      - Registry
      - Event Log

[1]

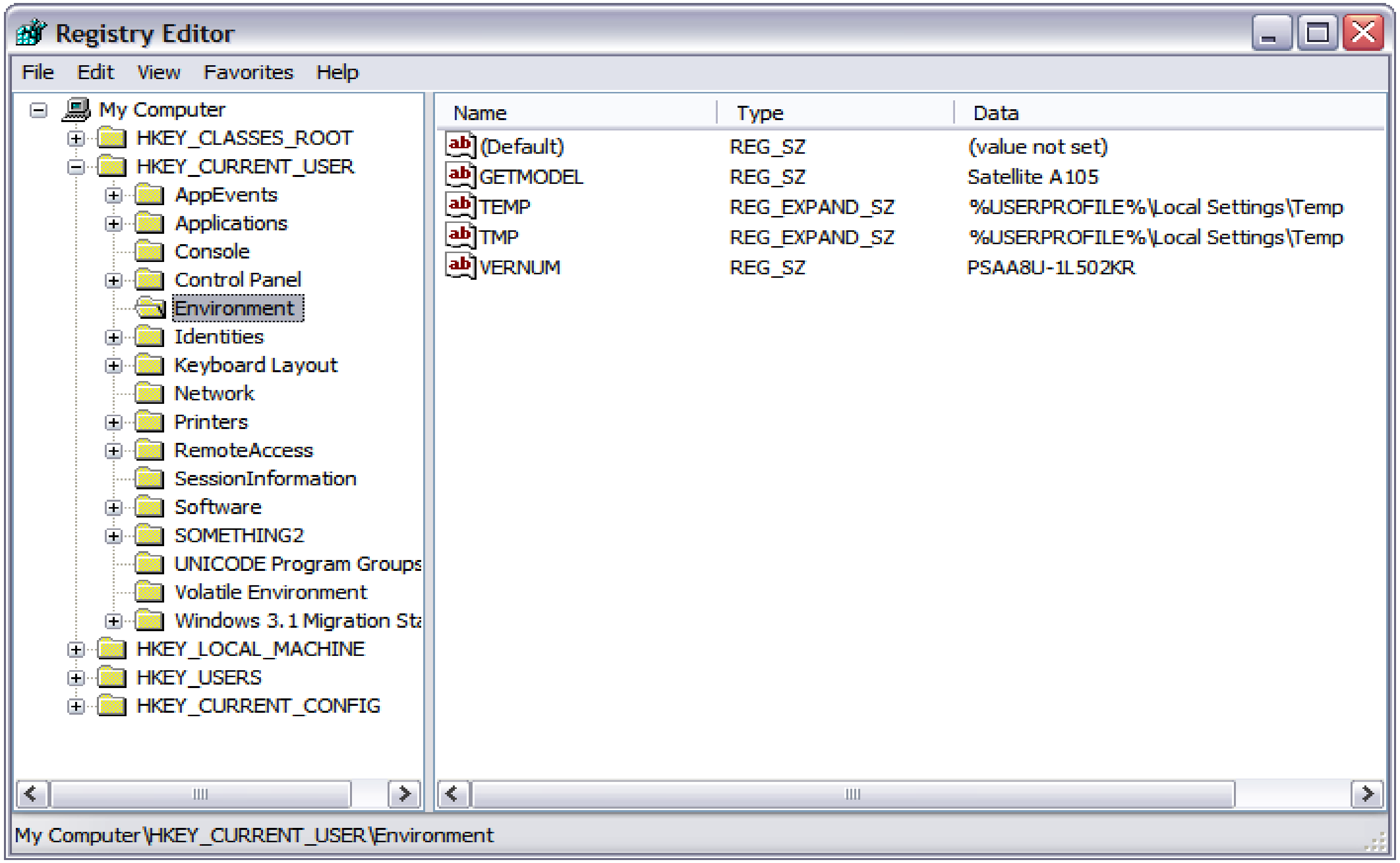
Forensic Investigation Suit

- Registry
  - Where Windows stores system-wide settings
  - Can view the Windows registry with Window’s Registry Editor
  - There is a lot of information found in the registry, such as
    - Autorun locations
      - Programs that are set to launch during the boot process
      - Malware can use this for persistence
    - Most Recently Used lists (MRUs)
      - MRUs are used to find
        - » Most recently launched applications
        - » Recently used or modified documents
        - » Recently changed registry keys
    - Wireless Networks
      - When a computer connects to a wireless network it is recorded in the Window's Registry

[1]

Forensic Investigation Suit

- **Window's Registry Editor**



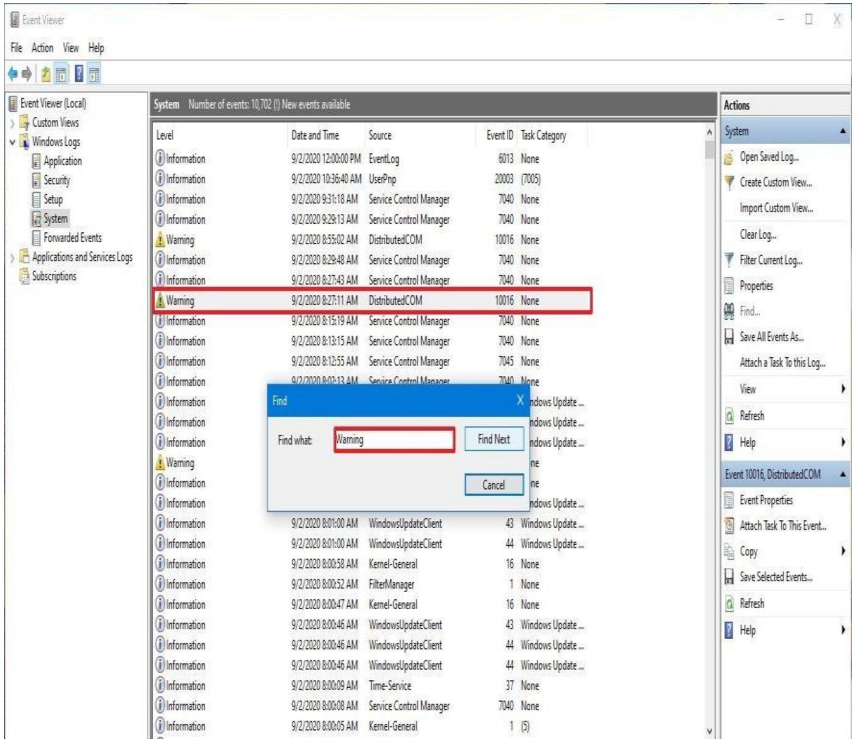
Name	Type	Data
(Default)	REG_SZ	(value not set)
GETMODEL	REG_SZ	Satellite A105
TEMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
TMP	REG_EXPAND_SZ	%USERPROFILE%\Local Settings\Temp
VERNUM	REG_SZ	PSAA8U-1L502KR

My Computer\HKEY_CURRENT_USER\Environment

[6]

Forensic Investigation Suit

- **Event Log**
  - **Can view event logs in the Window’s Event Viewer application which includes**
    - **Application log (E.g., Application report usage and errors)**
    - **Security log (E.g., Unsuccessful login attempts)**
    - **System log (E.g., system-wide events)**



System Number of events: 10,702 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	9/2/2020 12:00:00 PM	EventLog	6013	None
Information	9/2/2020 10:36:40 AM	UserPnp	20003	(7005)
Information	9/2/2020 9:31:18 AM	Service Control Manager	7040	None
Information	9/2/2020 9:29:13 AM	Service Control Manager	7040	None
Warning	9/2/2020 8:55:02 AM	DistributedCOM	10016	None
Information	9/2/2020 8:29:48 AM	Service Control Manager	7040	None
Information	9/2/2020 8:27:43 AM	Service Control Manager	7040	None
Warning	9/2/2020 8:27:11 AM	DistributedCOM	10016	None
Information	9/2/2020 8:15:19 AM	Service Control Manager	7040	None
Information	9/2/2020 8:13:15 AM	Service Control Manager	7040	None
Information	9/2/2020 8:12:55 AM	Service Control Manager	7045	None
Information	9/2/2020 8:02:13 AM	Service Control Manager	7040	None
Information				ndows Update ...
Information				ndows Update ...
Information				ndows Update ...
Warning				ne
Information				ne
Information				ndows Update ...
Information	9/2/2020 8:01:00 AM	WindowsUpdateClient	43	Windows Update ...
Information	9/2/2020 8:01:00 AM	WindowsUpdateClient	44	Windows Update ...
Information	9/2/2020 8:00:58 AM	Kernel-General	16	None
Information	9/2/2020 8:00:52 AM	FilterManager	1	None
Information	9/2/2020 8:00:47 AM	Kernel-General	16	None
Information	9/2/2020 8:00:46 AM	WindowsUpdateClient	43	Windows Update ...
Information	9/2/2020 8:00:46 AM	WindowsUpdateClient	44	Windows Update ...
Information	9/2/2020 8:00:46 AM	WindowsUpdateClient	44	Windows Update ...
Information	9/2/2020 8:00:09 AM	Time-Service	37	None
Information	9/2/2020 8:00:08 AM	Service Control Manager	7040	None
Information	9/2/2020 8:00:05 AM	Kernel-General	1	(5)

Find what: Warning

[1,7]

Forensic Investigation Suit

- **Linux Process Analysis**
  - **Linux has a different set of tools for a forensic investigation, such as**
    - **dd command (used to acquire evidence)**
    - **sha1sum command (used to hash evidence)**
    - **ps command (used to get a list of running processes)**
  - **A few Linux directories that an analyst should be familiar with are**
    - **/etc. (primary system configuration directory)**
    - **/var/log (the directory that holds all the application log files in plain text)**
    - **/home/$USER (the directory that holds all user data and configuration data)**

[1]

Forensic Investigation Suit

- Mobile Device Forensics
  - Jailbroken mobiles devices that have an OS similar to Linux can use some of the same tools discussed earlier
  - Many mobile devices require
    - Dedicated forensic tools
    - Special tools to properly view data
    - Special cables
    - Custom bootloader
      - Used to load an alternate OS that supports the acquisition
  - Mobile device storage
    - Usually uses small database management system such as SQLite
    - Almost never deletes data
      - Will mark rows to be deleted in a table. but the data will not be deleted until overwritten by other data
      - Common analysis suits can still recover deleted data

[1]

Forensic Investigation Suit

- Log Viewers
  - Every major OS has its own means to view logs
    - Built-in log viewers are not typically used for detailed analysis
  - Standalone log view is needed when an analysis needs to view logs from multiple computers at once
    - A few useful tools are
      - Splunk
      - SolarWinds Event Log Consolidator/Manager
      - Ipswitch’s WhatsUp

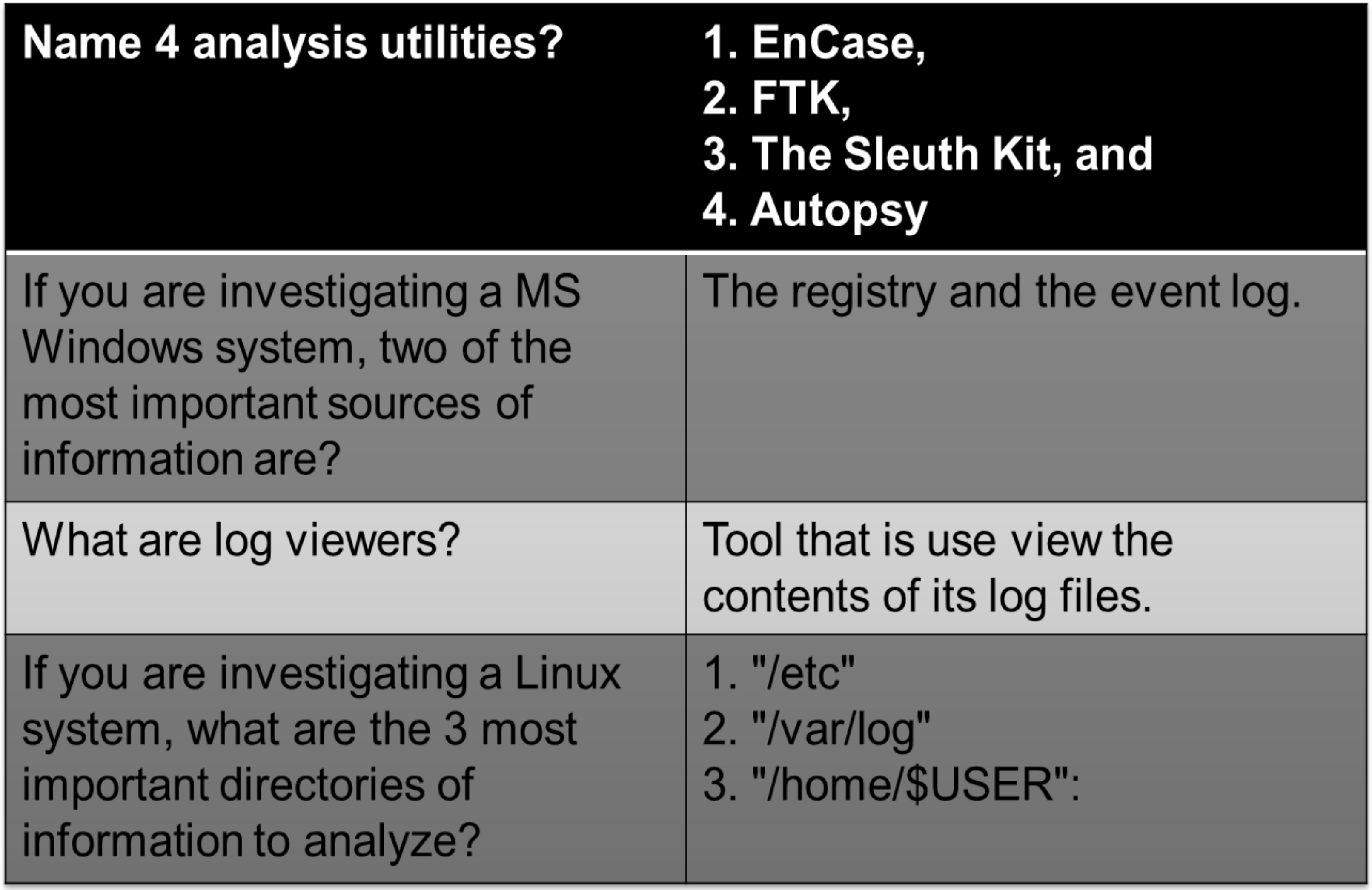
[1]

Interactive Exercise 8

Name 4 analysis utilities?	
If you are investigating a MS Windows system, two of the most important sources of information are?	
What are log viewers?	
If you are investigating a Linux system, what are the 3 most important directories of information to analyze?	

[1,2]

Interactive Exercise 8 Answers



Name 4 analysis utilities?	**1. EnCase,** **2. FTK,** **3. The Sleuth Kit, and** **4. Autopsy**
If you are investigating a MS Windows system, two of the most important sources of information are?	The registry and the event log.
What are log viewers?	Tool that is use view the contents of its log files.
If you are investigating a Linux system, what are the 3 most important directories of information to analyze?	1. "/etc" 2. "/var/log" 3. "/home/$USER":

[1,2]

Building Your Forensic Kit

- **Jump Bag**
  - Prepackaged set of tools that is always ready to go
  - Have a list of what is in the bag and ensure everything on the list is in the bag after each use
  - Each item discussed next is an item that should be in your jump bag
- **Write Blockers and Drive Adapters**
  - Hardware write blockers
    - Prevent the storage device from being modified when collecting data
  - Ensure to have an adapter and cable for each type of device in your organization

[1]

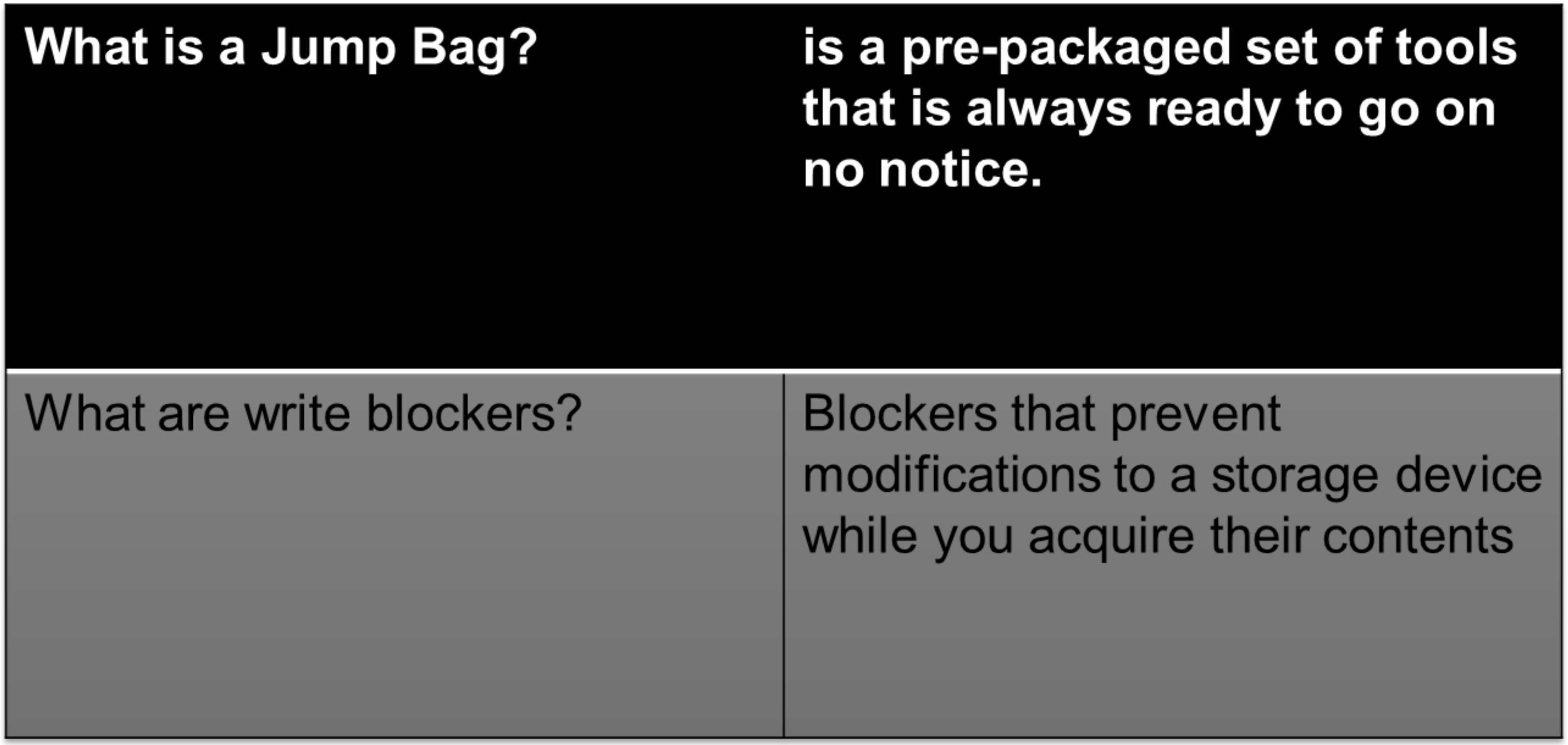
Interactive Exercise 9

What is a Jump Bag?

What are write blockers?

[1,2]

Interactive Exercise 9 Answers



What is a Jump Bag?	**is a pre-packaged set of tools that is always ready to go on no notice.**
What are write blockers?	Blockers that prevent modifications to a storage device while you acquire their contents

[1,2]

Building Your Forensic Kit

- **Cables**
  - An analysis jump bag should include various types of cables such as
    - Ethernet cable (crossover, straight-through, one-way)
    - Serial cables (various flavors of USB and RS-232)
    - Power cables
    - A small Ethernet hub
    - Antistatic wrist straps
- **Wiped Removable Media**
  - Ensure to have a few wiped devices in your jump bag to store evidence
  - Might need a portable RAID solution
    - Forensic Computers' Forensic Data Monster
    - This is needed if acquiring data from servers
  - Network-attached storage (NAS) solution
    - Used specifically for forensic images
    - Fast network will help with acquiring an image of any workstation
    - Can serve as an archival mechanism for pending investigations

[1]

Building Your Forensic Kit

- Camera
  - Ensure to include a camera with a flash to the jump bag
  - A ruler can be useful to have in photos taken
- Crime Scene Tape
  - Needed to ensure people in the area do not walk in while you are trying to seize evidence
- Tamper-Proof Seals
  - If items are being transported by anyone but the analysis, then this is needed
  - Transport evidence in containers with a tamper-resistant seal
  - If nothing else is available, then tape that the analysis signs their name on

[1]

Building Your Forensic Kit

- Documentation and Forms
  - Chain of Custody Form
    - Have several of these forms in your jump bag
    - Each seized piece of evidence should have its form
    - The form should be tailored to your organization’s requirements
  - Incident Response Plan
    - Have a copy of the plan in your jump bag
  - Incident Log
    - Ensure you have a notebook and pen in your jump bag
    - Take notes on every action taken and every considered hypothesis
  - Call/Escalation List
    - Ensure this list from the IR plan is in your jump bag

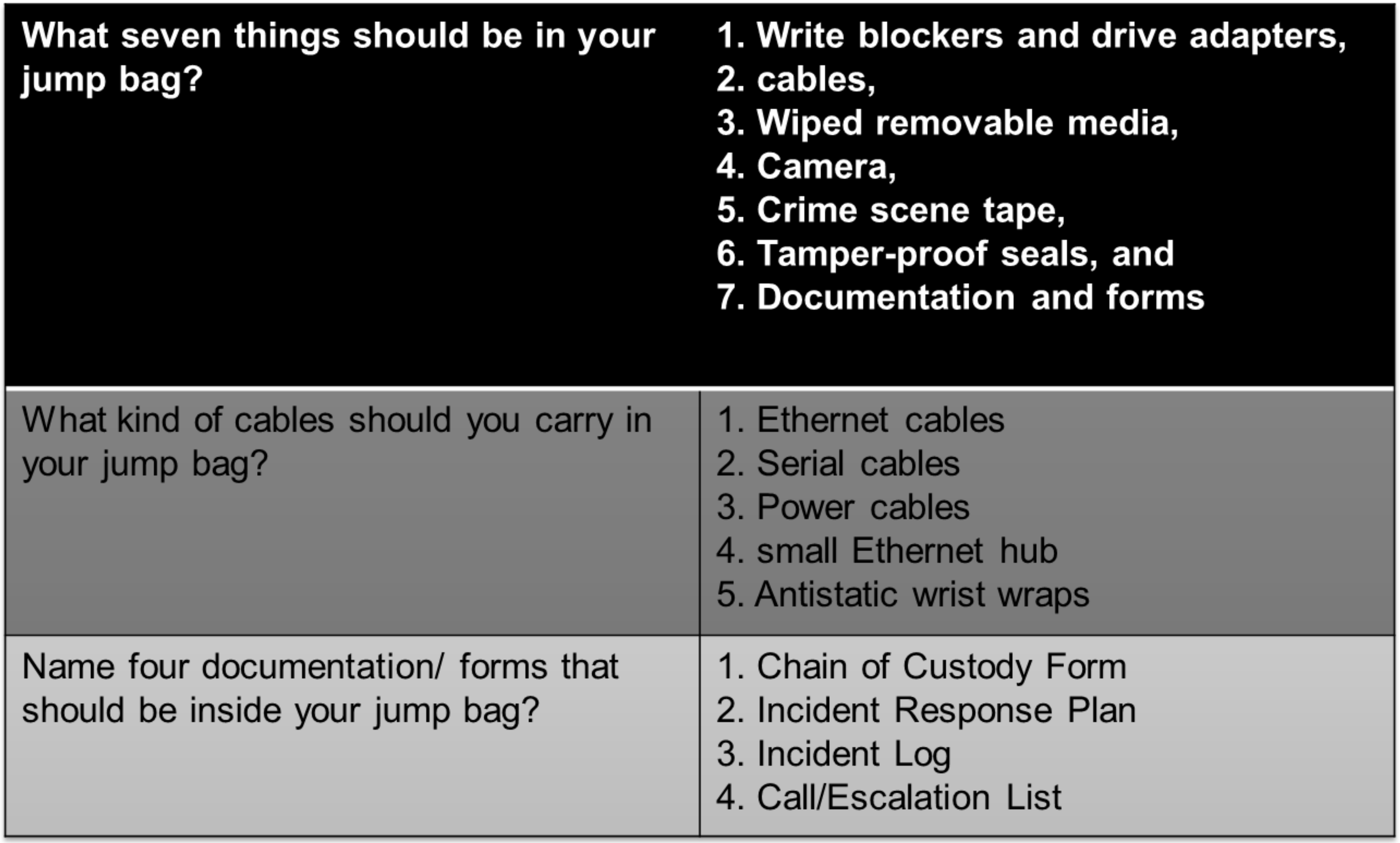
[1]

Interactive Exercise Final

What seven things should be in your jump bag?	
What kind of cables should you carry in your jump bag?	
Name four documentation/ forms that should be inside your jump bag?	

[1,2]

Interactive Exercise final Answers



What seven things should be in your jump bag?	1. Write blockers and drive adapters, 2. cables, 3. Wiped removable media, 4. Camera, 5. Crime scene tape, 6. Tamper-proof seals, and 7. Documentation and forms
What kind of cables should you carry in your jump bag?	1. Ethernet cables 2. Serial cables 3. Power cables 4. small Ethernet hub 5. Antistatic wrist wraps
Name four documentation/ forms that should be inside your jump bag?	1. Chain of Custody Form 2. Incident Response Plan 3. Incident Log 4. Call/Escalation List

[1,2]

Quiz

Chapter 9

Question #1

- **1. In the event of a serious incident, which task is not a critical step to take in controlling the crime scene?**
  A. Record any interactions with digital systems
  B. Verify roles and training for individuals participating in the investigation
  C. Removed power from currently running systems
  D. Carefully document who enters and leaves the scene

[1]

Answer #1

- C
  - Removing power should not be done unless it's to preserve life or limb, or under other exigent circumstances
  - In many cases it's possible to recover evidence residing in running memory

[1]

Question #2

- **2. What is the practice of controlling how evidence is handled to ensure its integrity during an investigation called?**
  - A. Chain of control
  - B. Chain of concern
  - C. Chain of command
  - D. Chain of custody

[1]

Answer #2

- **D**
  - **A chain of custody is a history that shows how evidence was collected, transported, and preserved at every stage of the investigation process**

[1]

Question #3

- **3. As part of the forensic analysis process, what critical activity often includes a graphical representation of process and operating system events?**
  A. Registry editing
  B. Timeline analysis
  C. Network mapping
  D. Write blocking

[1]

Answer #3

- B
  - Timeline analysis is the practice of arranging extracted data from a UNIX file system, the Windows registry, or a mobile device in chronological order to better understand the circumstances of a suspected incident

[1]

Question #4

- **4. During forensic acquisition, why is a high-level format normally insufficient when preparing the destination media?**
  A. **High-level formatting completely wipes the drive, but may add additional artifacts**
  B. **High-level formatting only erases the file data, leaving the system structure intact.**
  C. **High-level formatting only erases the file system structure data, leaving the file data intact**
  D. **High-level formatting removes bad sectors, but leaves file data intact**

[1]

Answer #4

- C
  - The destination media should be free from anything that may contaminate the evidence
  - Completely removing the data requires overwriting each block of the destination storage medium, which may always be performed if using high-level formatting tools

[1]

Question #5

- **5. The practice of modifying or deleting file modification data is referred to as what?**
  A. Timestomping
  B. Timestamping
  C. Timelining
  D. Timeshifting

[1]

Answer #5

- A
  - Timestomping is an advanced technique to manipulate file creation or modification data to thwart forensics techniques
  - Timestomping is often used by malware to make the process of timelining more difficult

[1]

Question #6

- **Use the following command line input to answer questions 6-8:**

```
dd if=/dev/sda of+/dev/sdc bs=2048 conv=noerror, syn status=progress
```

- **6. How many bits of data are read and written at a time?**
  - A. 2048
  - B. 16384
  - C. 256
  - D. 512

[1]

Answer #6

- B
  - The "bs" argument indicates the number of bytes transferring during the process
  - Because there are 8 bits in a byte, you will multiply the 2048 by 8 to get 16384 bits

[1]

Question #7

```
dd if=/dev/sda of+/dev/sdc bs=2048 conv=noerror, syn status=progress
```

- **7. What is the name of the destination image?**
  - **A. sda**
  - **B. /dev/sda**
  - **C. Sync**
  - **D. sdc**

[1]

Answer #7

- D
  - The "of" argument indicates the output file of the process

[1]

Question #8

```
dd if=/dev/sda of+/dev/sdc bs=2048 conv=noerror, syn status=progress
```

- **8. What is the purpose of the command?**
  - **A. To copy the primary partition to an image file**
  - **B. To restore the contents of a hard drive from an image file**
  - **C. To copy the entire contents of the hard drive to an image file**
  - **D. To delete the entire contents of /dev/sda**

[1]

Answer #8

- C
  - The course file is the entire hard drive, indicated by the argument "/dev/sda"
  - Be careful to double-check the spelling of both input and output files to avoid overwriting the incorrect media

[1]

Scenario for Questions 9-12

- You are called to a scene of a high-profile incident and asked to perform forensic acquisition of digital evidence. The primary objective is a Linux server that runs several services for a small company. The former administrator is suspected of running illicit services using company resources and is refusing to provide passwords for access to the system. Additionally, there are several company-owned mobile phones that appear to be functioning sitting on the desk beside the servers

Question #9

- **9. What is one of the first tasks you undertake in preparing to analyze the server's hard drive?**
  A. Hash all storage media and then make a copy of the hard drive
  B. Begin analysis on the target system and perform recurring MD5 hashes
  C. Copy the entire contents to a SAN or external storage and begin analysis
  D. Perform analysis immediately on the server before loss of power

[1]

Answer #9

- A
  - It is ideal to conduct the analysis on a copy of the evidence and not on the original
  - Be sure to take a cryptographic hash of the original evidence before copying anything

[1]

Question #10

- **10. What utility will allow you to make a bit-for-bit copy of the hard drive contents?**
  A. MFT
  B. dd
  C. MD5
  D. GPU

[1]

Answer #10

- B
  - dd is a common utility found in most Linux-based systems
  - It can duplicated data across files, devices, partitions, and volumes

[1]

Question #11

- **11. What type of specialized software might you use to recover the credentials required to get system access?**
  A. Forensic duplicator
  B. dd
  C. Password cracker
  D. MD5

[1]

Answer #11

- C
  - Password crackers are specialized software designed to guess passwords and decrypt the protected resources
  - The software can be very resource intensive since cracking usually requires a lot of processing power or storage capacity

[1]

Question #12

- **12. You want to take the mobile phones back to your lab for further investigation. Which two tools might you use to maintain device integrity as you transport them?**
  A. **Faraday bag and tamper-evident seal**
  B. **Write blocker and crime scene tape**
  C. **Thumb drive and crime scene tape**
  D. **Forensic toolkit and tamper-evident seal**

[1]

Answer #12

- **A**
  - **A Faraday container will prevent the devices from communicating over radio waves by absorbing and redistributing their RF energy**
  - **The bag should be secured with a tamper-evident seal to easily identify whether its contents were interfered with**

[1]

References

1. Maymí Fernando, and Brent Chapman. CompTIA CSA+ Cybersecurity Analyst Certification All-in-One Exam Guide (Exam CS0-001). McGraw-Hill Education, 2018.
2. friedaj friedaj, “cysa-chapter-9-Preparing-for-the-Incident-Response-Toolkit-flash-cards,” Quizlet, 17-Dec-2017. [Online]. Available: https://quizlet.com/296891139/cysa-chapter-9-preparing-for-the-incident-response-toolkit-flash-cards/. [Accessed: 20-Dec-2020].
3. M. Baranauskas, “T1099: Timestomping,” *Red Teaming Experiments*, 16-Mar-2019. [Online]. Available: https://www.ired.team/offensive-security/defense-evasion/t1099-timestomping. [Accessed: 16-Jan-2021].
4. M. Todorov, Geoffroy, F. Zimmerman, A. von Essen, Rsydw, R. S. González, and R. Saive, “Marin Todorov,” Tecmint, 18-Dec-2018. [Online]. Available: https://www.tecmint.com/clone-linux-partitions/. [Accessed: 16-Jan-2021].

References Con’t

5. H. N. Duc, “HOW TO INVESTIGATE FILES WITH FTK IMAGER,” eForensics, 05-Sep-2014. [Online]. Available: https://eforensicsmag.com/how-to-investigate-files-with-ftk-imager/. [Accessed: 16-Jan-2021].
6. O. Text, “7 key things forensic investigators need to do,” OpenText Blogs, 08-Sep-2020. [Online]. Available: https://blogs.opentext.com/7-things-forensic-investigators-need-to-do/. [Accessed: 16-Jan-2021].
7. M. Huculak, “Don't know what the problem is? The Event Viewer on Windows 10 can help.,” Windows Central, 03-Sep-2020. [Online]. Available: https://www.windowscentral.com/how-use-event-viewer-windows-10. [Accessed: 16-Jan-2021].