Digital Forensics and Cyber Laws
PE-II: CSP43B
BTech CSE, Trimester-XI, AY 2020-21

Dr Sumedha Sirsikar

Digital Evidence: Principles Understanding Challenges

Digital Evidence

Digital Evidence

Definition-

Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi

- Data is a combination of numbers that represent information in the form text, images, audio, and video

A more general definition proposed by Brian Carrier-

- digital data that support or refute a hypothesis about digital events or the state of digital data

Or

That address critical elements of the offense such as intent or alibi

Alibi

- A form of defense whereby a defendant attempts to prove that he or she was elsewhere when the crime in question was committed

Refute

- Prove (a statement or theory) to be wrong or false

Digital Evidence

Definition-

- Any data that can establish a crime has been committed

Or

Can provide a link between

- a crime and its victim or
- a crime and its perpetrator

- **Perpetrator :** [pur-pi-trey-ter]
- E.x. noun 1.
  - a person who perpetrates, or commits, an illegal, criminal, or evil act
  - E.g: The perpetrators of this heinous crime must be found and punished to the fullest extent of the law

Digital Evidence

Definition by Standard Working Group on Digital Evidence (SWGDE)-

- any information of probative value that is either stored or transmitted in a digital form

International Organization of Computer Evidence (IOCE) –

- information stored or transmitted in binary form that may be relied upon in court

Computer Systems Categories: in view of Digital Evidence

1. ***Open computer systems***:
   - hard drives, keyboards and monitors such as laptops, desktops, and servers
   - For example, details such as when a file was created, who likely created it, or that it was created on another computer

2. Communication systems

A source of digital evidence

- Traditional telephone systems
- wireless telecommunication systems
- Internet
- networks

- e.g. e-mail messages - log files from intermediate servers and routers that handled a given message
- traffic, giving digital investigators access to all communications

3. Embedded computer systems

- Mobile devices
  - contain communications, digital photographs and videos, and other personal data
- smart cards
- Navigation systems
  - to determine where a vehicle has been
  - Sensing and Diagnostic Modules in many vehicles hold data that can be useful for understanding accidents, including the vehicle speed, brake status, and throttle position during the last 5 s before impact
- Microwave ovens with embedded computers
  - download information from the Internet
- some home appliances allow users to program them remotely via a wireless network or the Internet
- In an arson investigation data recovered from a microwave oven can indicate that it was programmed to trigger a fire at a specific time

Problems of Digital Evidence

- Only few people are well versed in the evidential, technical and legal issues related to digital evidence

- It is often overlooked, collected incorrectly or analyzed ineffectively

Digital Evidence: Principles

Principles Of Digital Evidence

1. Evidence Exchange
2. Evidence Characteristics
3. Forensic Soundness
4. Authentication
5. Chain of custody
6. Evidence Integrity
7. Objectivity
8. Repeatability

1. *Evidence Exchange*

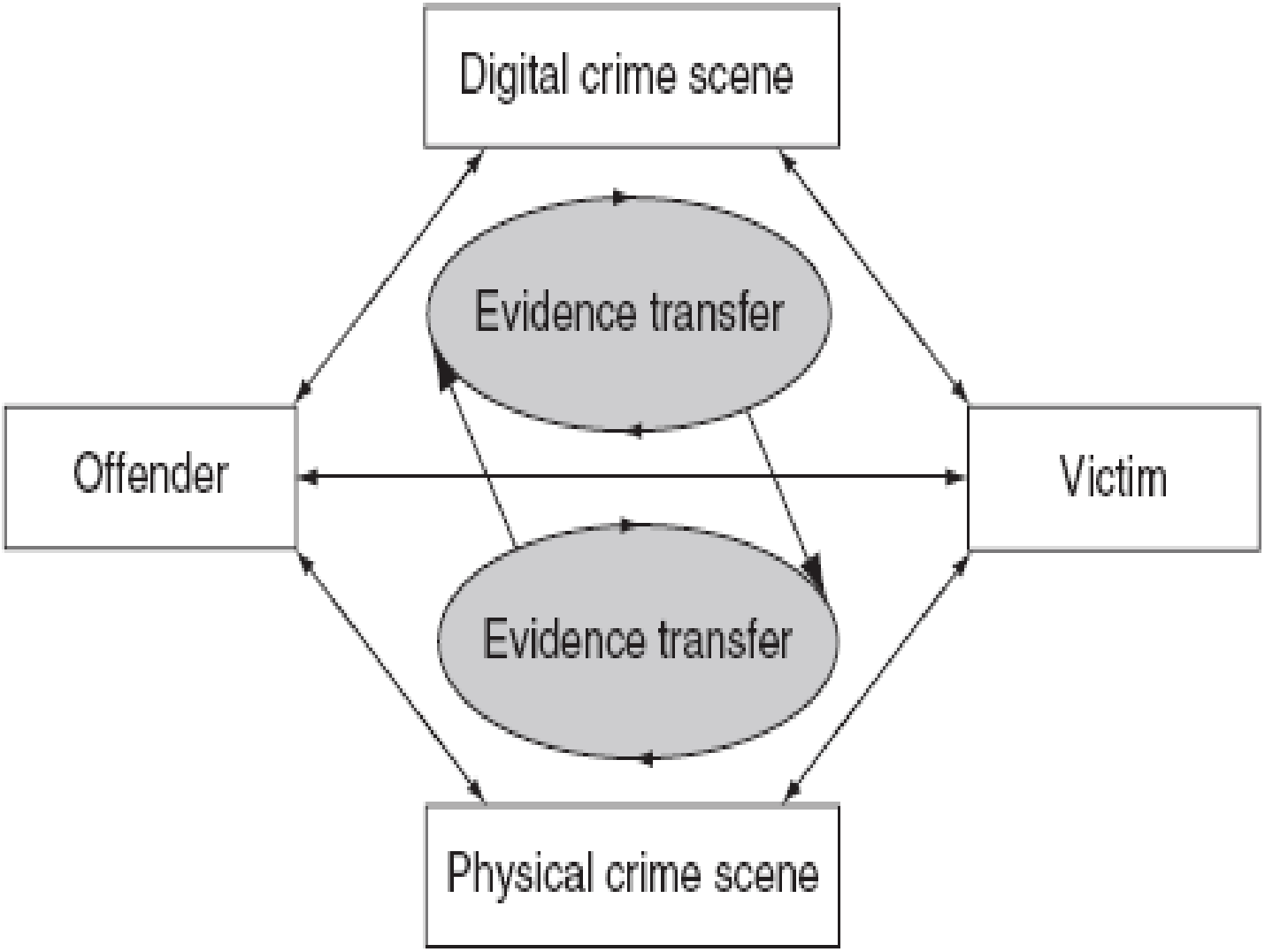
- According to **Locard's Exchange Principle**, contact between two items will result in an exchange. It applies to any contact at a crime scene including –
  - between an offender and victim
  - between a person with a weapon
  - between people and the crime scene itself
- Forensic Analysts –
  - employed to uncover compelling links between the offender, victim and crime scene
  - E.g. file systems, registry, system logs, and network-level logs

- There will always be evidence of the interaction, although in some cases it may not be detected easily

- Absence of evidence is not evidence of absence

- This transfer occurs in both the physical and digital realms and can provide links between them

Establish connections between victims, offenders, and crime scenes



The physical world:

- An offender might leave fingerprints or hair at the scene

Eg: In a homicide case the offender may attempt to misdirect investigators by creating a suicide note on the victim's computer, and in the process leave fingerprints on the keyboard.

With one such piece of evidence, investigators can demonstrate the strong possibility that the **offender was at the crime scene.**

With two pieces of evidence the link between the offender and crime scene becomes **stronger** and easier to demonstrate.

2. Evidence Characteristics

The exchanges between individual and crime scene produce trace evidence:

(i) class characteristics: Evidence with attributes that fit in common traits in similar items

(ii) individual characteristics: *Evidence* with attributes that are unique and can be linked to a specific person or activity with greater certainty

3. Forensic Soundness

- digital evidence useful in an investigation, must be preserved and examined in a forensically sound manner
- a method of preserving or examining digital evidence is only forensically sound if it does not alter the original evidence source in any way
- keys is **documentation –** report on where the evidence originated and how it was handled

- Acquiring data from a hard drive
  - even when using a hardware write-blocker, alters the original state of the hard drive
  - It includes making a hidden area of the hard drive accessible
  - maintain information using Self-Monitoring, Analysis and Reporting Technology (SMART) on modern hard drives

Write blockers:

- devices that allow acquisition of information on a drive without creating the possibility of accidentally damaging the drive contents
- by allowing read commands to pass but by blocking write commands

SMART - Self-Monitoring, Analysis and Reporting Technology

- A monitoring system for computer hard disk drives (HDDs) to detect and report on various indicators of reliability, in the hope of anticipating failures

- *absolute standard - **"preserve everything but change nothing"** is not only inconsistent with other forensic disciplines but hard too*

Forensically sound

- The acquisition process –
  - should change the original evidence as little as possible
  - Any changes should be documented and assessed in the context of the final analytical results
  - acquisition process preserves a complete and accurate representation of the original data, and validate authenticity and integrity

- Preserving volatile data-
  - digital investigators must document the date and time that data were preserved and the tools that were used, and the MD5 hash value of all outputs
- Computer data
  - it is critical to note the date and time of the computer and compare it to a reliable time source

4. Authentication

- Always not possible to compare the acquired data with the original
- The contents of RAM on a running computer are constantly changing
- Captured memory contents-
  - a snapshot in time of the running state of the computer at that moment, and there is no original to compare the copy

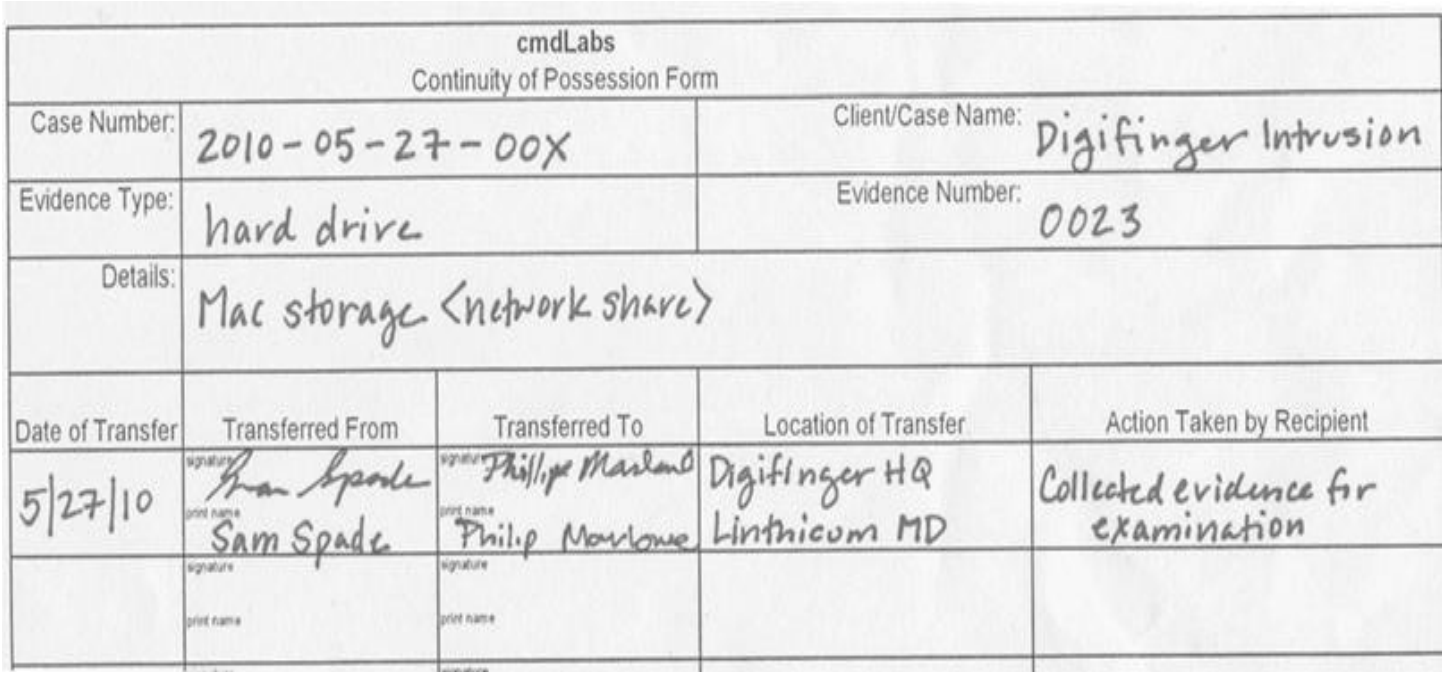
- Network traffic:
  - transient and data must be captured while it is in transit
  - captured network traffic - only copies remain and the original data are not available for comparison
  - **authentication** is the process of determining whether the evidence is worthy
  - Eg: The individual who collected the evidence can confirm that the evidence presented in court is the same as when it was collected
  - a system administrator can testify that log files presented in court originated from her/his system

5. Chain of Custody

- Aspects of authentication is maintaining and documenting the chain of custody (continuity of possession) of evidence
- recording the transfer of evidence, when, where, and why

5. Chain of Custody

- Evidence was handled improperly and may have been altered, replaced with incriminating evidence, or contaminated
- Potential consequences of breaking the chain of custody include misidentification of evidence, contamination of evidence, and loss of evidence or pertinent elements



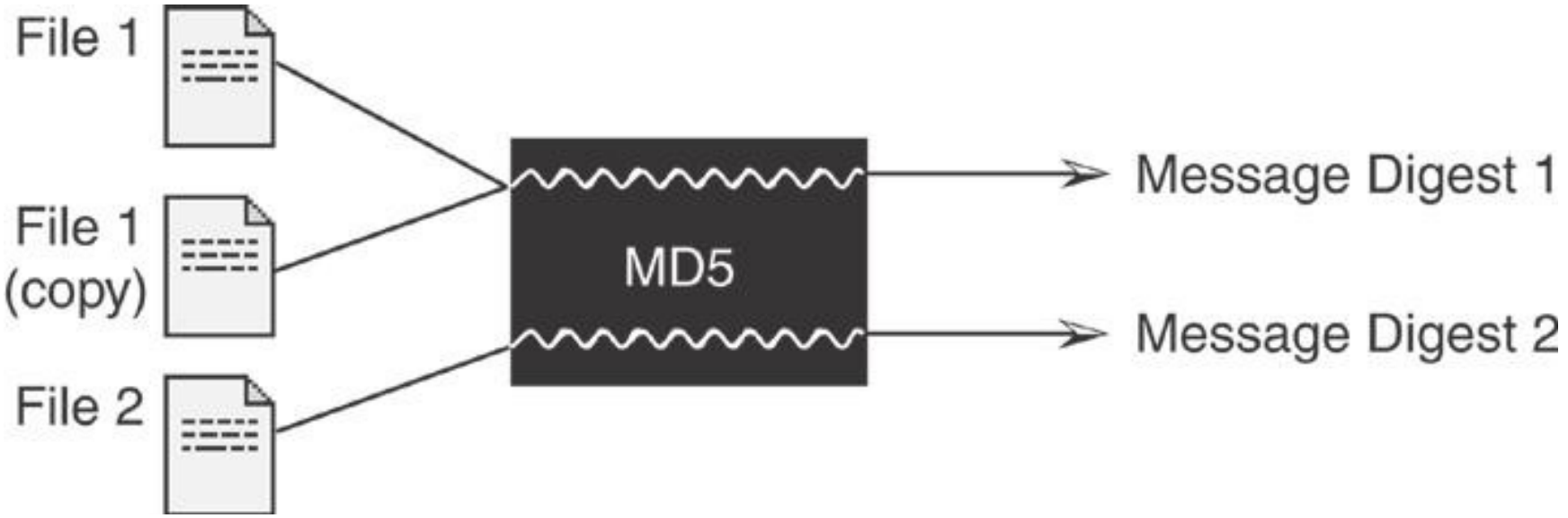
cmdLabs
Continuity of Possession Form

Case Number:	2010-05-27-00X	Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive	Evidence Number:	0023
Details:	Mac storage <network share>		

Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	signature: Sam Spade print name: Sam Spade	signature: Philip Marlowe print name: Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	signature: print name:	signature: print name:		

6. Evidence Integrity

- The purpose is –
  - to show that evidence has not been altered from the time it was collected, thus supporting the authentication process
- The process of verifying the integrity of evidence involves –
  - a comparison of the digital fingerprint for that evidence taken at the time of collection with the digital fingerprint of the evidence in its current state



- Exact copy will have the same message digest as the original but if a file is changed even slightly it will have a different message digest from the original
  e.g. MD5 and SHA-1

7. Objectivity

- The interpretation and presentation of evidence should be free from bias to provide decision makers with the clearest possible view of the facts
- to let the evidence speak for itself as much as possible
- to ensuring objectivity is to have a peer review process that assesses a forensic analyst's findings for bias or any other weakness

8. Repeatability

- any experiments or observations must be repeatable in order to be independently verifiable
- a verification of forensic findings
  - to document the steps taken to find and analyze digital evidence in sufficient detail to enable others to verify the results independently
- may include the location and other characteristics of the digital evidence, as well as the tools used to analyze the data

Digital Evidence: Challenges

Challenges of Digital Evidence

1. It is a messy, slippery form of evidence that can be very difficult to handle
   - i.e. a hard drive platter contains a messy amalgam of data—pieces of information mixed together and layered on top of each other over time
   - Only a small portion of this amalgam might be relevant to a case
   - making it necessary to extract useful pieces, fit them together, and translate them into a form that can be interpreted

2. Digital Evidence is generally an abstraction of some digital object or event

- When a person instructs a computer to perform a task such as sending an e-mail, the resulting activities generate data remnants that give only a partial view of what occurred (Venema & Farmer, 2000)
- Only certain results of the activity such as the e-mail message and server logs remain to give us a partial view of what occurred
- using a forensic tool to recover a deleted file from storage media involves several layers of abstraction from magnetic fields on the disk to the letters and numbers
- the actual data is not seen but only a representation, and each layer of abstraction can introduce errors

3. Digital evidence is usually circumstantial

- making it difficult to attribute computer activity to an individual.
- It can only be one component of a solid investigation
- If a case hinges upon a single form or source of digital evidence such as date-time stamps on computer files, then the case is unacceptably weak
- Without additional information, it could be reasonably argued that someone else used the computer at the time.
- E.g. password protection mechanisms on some computers can be bypassed, and many computers do not require a password, allowing anyone to use them
- if a defendant argues that some exonerating digital evidence was not collected from one system, this would only impact a weak case that does not have supporting evidence of guilt from other sources

4. The fact that digital evidence can be manipulated or destroyed so easily raises new challenges for digital investigators

- can be altered or obliterated either maliciously by offenders or accidentally during collection without leaving any obvious signs of distortion

Features of Digital Evidence

1. Digital evidence can be duplicated exactly and a copy can be examined as if it were the original
   - It is common practice when dealing with digital evidence to examine a copy, thus avoiding the risk of altering or damaging the original evidence
2. With the right tools, it is very easy to determine if digital evidence has been modified or tampered with by comparing it with an original copy
3. Digital evidence is difficult to destroy. Even when a file is “deleted” or a hard drive is formatted, digital evidence can be recovered
4. When criminals attempt to destroy digital evidence, copies and associated remnants can remain in places that they were not aware of

Digital Forensics and Cyber Laws
PE-II: CSP43B
BTech CSE, Trimester-XI, AY 2020-21

Dr Sumedha Sirsikar

Digital evidence in courtroom

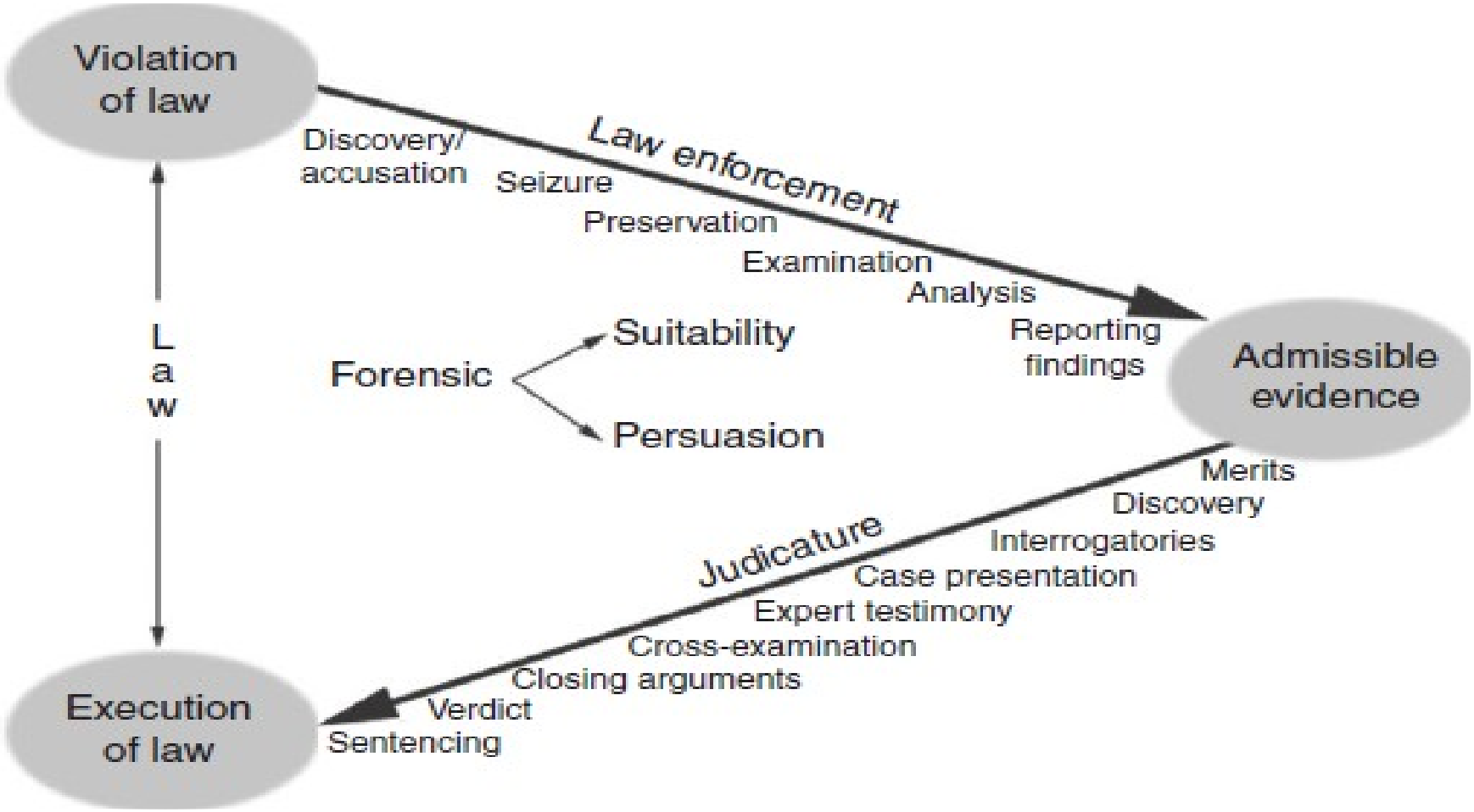
Direct versus circumstantial evidence

Digital Evidence in Courtroom

The purpose of a courtroom is to administer justice

- Role of Digital Investigators –
  - To present supporting facts and probabilities
  - Able to present technical evidence accurately
  - Duty to present findings in a clear, factual, trustworthiness and objective manner
  - Resist the influence of others' opinions and avoid jumping to conclusions
  - Can not do advocacy or judgmental assertions

Overview of case/incident resolution process



Major issues in presentation of digital evidence in court

1. Duty of experts
2. Resisting preconceived theories
3. Influence of others
4. Admissibility
5. Uncertainty

Duty of Experts

1. Should help the court to achieve the overriding objective by giving unbiased opinion on matters within his expertise
2. Overrides any obligation to the person from whom he receives instructions or by whom he is paid
3. Includes an obligation to inform all parties and the court if the expert's opinion changes from that contained in a report served as evidence or given in a statement

Most common Pitfalls in Duty of Experts

1. Resisting Influences
2. Avoiding Preconceived Theories
3. Scientific Truth and Legal Judgment

Admissibility

- a set of legal tests carried out by a judge to assess an item of evidence
  - evidence is “safe” to put before a jury and will help to provide a solid foundation for making a decision in the case

Admissibility

The magistrate admits digital evidence for assessment. It has five issues -

1. Relevance
2. Authenticity
3. Not hearsay or admissible hearsay
4. Best evidence
5. Not unduly prejudicial

Search Warrants

- Digital evidence is not admitted by courts if it is obtained without authorization
- Warrant is required to search and seize evidence
- Investigators must demonstrate probable cause and details about the place to be searched and the persons or things to be seized

Warrantless search in the United States

- plain view: investigators can seize it provided they have obtained access to the area validly
- Consent: investigators must cease the search when the owner withdraws consent. They may be able to use the evidence gathered to establish probable cause and obtain a search warrant
- Exigency: any emergency threatening life and limb or in which digital evidence is imminently likely to be altered or destroyed

Authentication of Digital Evidence

Admissible digital evidence in court -

- Recovered evidence is the same as the originally seized data
- acquired from a specific computer and/or location
- complete and accurate copy of digital evidence was acquired
- remained information is accurate, such as dates associated with a particular file
- Integrity documentation - not been altered since it was collected

Reliability of Digital Evidence

- Identify malicious tampering and destruction of a given item of digital evidence
- Two approaches -
  - the computer that generated the evidence was functioning normally
  - examine the actual digital evidence for evidence of tampering and other damage

- Increasingly impractical to examine and certify all the intricacies of computer operation
- Reliable process also can malfunction

Best Evidence

- The original purpose to ensure that decisions made in court were based on the best available information

- Contents of a writing, recording or photographs, courts sometimes require the original evidence

Hearsay

- an e-mail message may be used to prove that an individual made certain statements
- cannot be used to prove the truth of the statements it contains

Direct versus circumstantial evidence

Direct versus Circumstantial Evidence

- Digital Evidence can be used to prove facts

Direct evidence –

- establishes fact
- proper functioning of that specific system
- only suggestive of human activities
- E.g. a computer log on record

Circumstantial evidence –

- may suggest
- proper functioning of an identical system
- used to firmly establish facts
- The individual who owns the account was responsible
- required to prove that he/she actually logged in to the system

Direct versus Circumstantial Evidence

- e.g. Intellectual Property theft -
  - the defendant taking the proprietary data, it may be sufficient to show that the data in his/her possession are the same as the proprietary data and that he/ she had the opportunity for access

Scientific Evidence

Novel scientific evidence is evaluated using four criteria –

1. Whether the theory or technique can be (and has been) tested
2. Whether there is a high known or potential rate of error, and the existence and maintenance of standards controlling the technique's operation
3. Whether the theory or technique has been subjected to peer review and publication
4. Whether the theory or technique enjoys "general acceptance" within the relevant scientific community

Presenting Digital Evidence

The following is a sample report structure:

Expert Reports -

- *Introduction*
- *Evidence Summary*
- *Examination Summary*
- *File System Examination*
- *Forensic Analysis and Findings*
- *Conclusions*

Summary

- Be familiar with all aspects of the case, anticipate questions, rehearse answers, and prepare visual presentations to address important issues

Digital evidence: Level of Certainty

Levels of Certainty in Digital Forensics

The level of certainty associated with a particular finding, some digital investigators use an informal system of degrees in both the affirmative and negative sense: (1) almost definitely, (2) most probably, (3) probably, (4) very possibly, and (5) possibly

Levels of Certainty in Digital Forensics

- Analysis of digital evidence –
  - requires interpretation - basis of any conclusions
- Digital investigators –
  - able to estimate and describe the level of certainty underlying their conclusions to help fact-finders determine what weight to attach
  - lack of consistency in the way that the reliability or accuracy of digital evidence is assessed because of the complexity and multiplicity of computer systems
  - It is influenced by their knowledge and experience
  - example of IIS Web server logs showing unauthorized access to a server via a VPN concentrator

```
2009-04-03 02:38:10 W3SVC1 10.10.10.50 GET /images/snakeoil3.jpg-80-
192.168.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
```

Defining Levels of Certainty

- The Certainty Scale is proposed as a tool to formalize the process
- Digital investigators assign a level of certainty to conclusions that are based on digital evidence
- Digital investigators could conceivably assign a C-value to each piece of evidence they have analyzed
- that approach can add confusion rather than clarity

Scale for Categorizing Levels of Certainty in Digital Evidence

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts	Erroneous/incorrect
C1	Evidence is highly questionable	Highly uncertain
C2	Only one source of evidence is not protected against tampering	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g., temporal error and data loss)	Almost certain
C6	The evidence is tamperproof or has a high statistical confidence	Certain

C-value used to clarify the level of certainty

- C6 level of certainty:
  - Files containing known child pornography were found on the defendant's computer
  - hash values of the child pornography files should match with a visual inspection of the file contents
- C5 level of certainty:
  - IP address, user account and automatic number identification (ANI) information are all linked to the defendant and his home
  - Monitoring Internet traffic indicates that criminal activity is coming from the house
  - The multiple independent sources of digital evidence indicate that the activity almost certainly originated from the suspect's home

C-value used to clarify the level of certainty

- C4 level of certainty:
  - Multiple items of evidence on the defendant's Computer link him to the identity theft targeting the victim, including e-mail on May 31, 2010, confirming a Visa credit card in the victim's name USBank online loan application completed in victim's name, and a cash advance on a MasterCard credit card in the victim's name
- C0 level of certainty:
  - The conclusion that Julie Amero intentionally accessed pornography Web sites while in the classroom is contradicted by evidence that pornographic pop-ups appearing on the computer were the result of an automated "spyware" program on the computer

Advantages of Certainty Scale

- It is flexible enough to assess the evidential weight of both the process that generated a piece of digital evidence and its contents, which may be documents or statements
- It is nontechnical and therefore easily understood by nontechnical people such as those found in most juries
- When Complexities of the systems involved, it is invaluable to give them a general sense of the level of certainty and decide what evidential weight to give the evidence
- Without providing a nontechnical overview, can lead to confusion and poor decisions

Disadvantages of Certainty Scale

- It is subjective—
  - Digital investigators must use their judgment when assigning certainty values
  - Different digital investigators may reach a similar conclusion but assign different levels of certainty based on their knowledge and experience

Summary

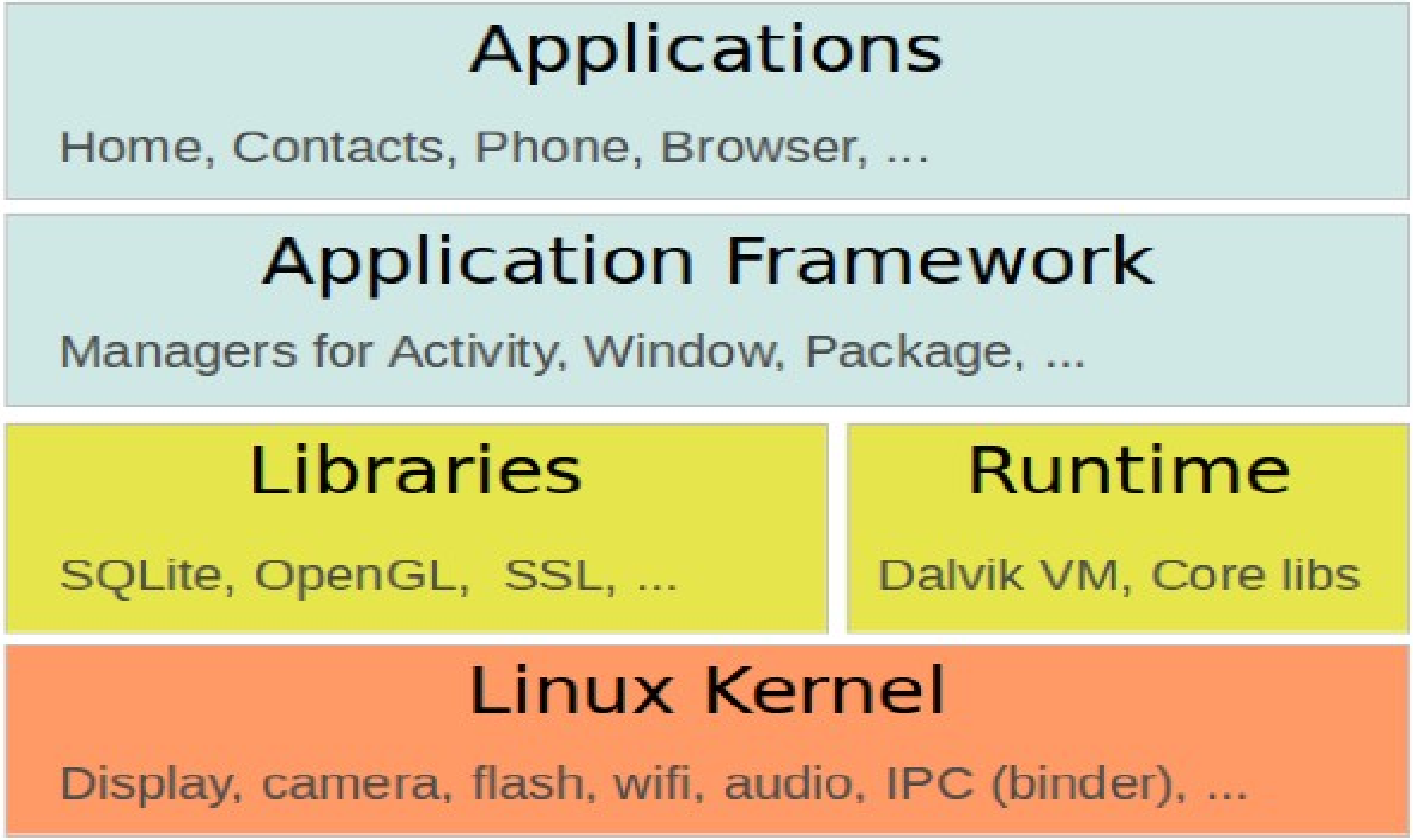
- C-values in specific cases-
  - reveal that certain types of evidence are less reliable than was initially assumed
  - For digital evidence, it may be possible to identify the main sources of error or uncertainty and develop analysis techniques for evaluating or reducing these influences
  - For digital evidence, it may be possible to identify all potential sources of error or uncertainty and develop a more formal model for calculating the level of certainty

Digital Forensics Analysis
CSN611
MTech CSE-NMCS, Trimester-IV, AY 2020-21

Dr Sumedha Sirsikar

Mobile Forensics
AFLogical

Android Platform Architecture



Challenges of Acquisition and Analysis of Data on Android Devices

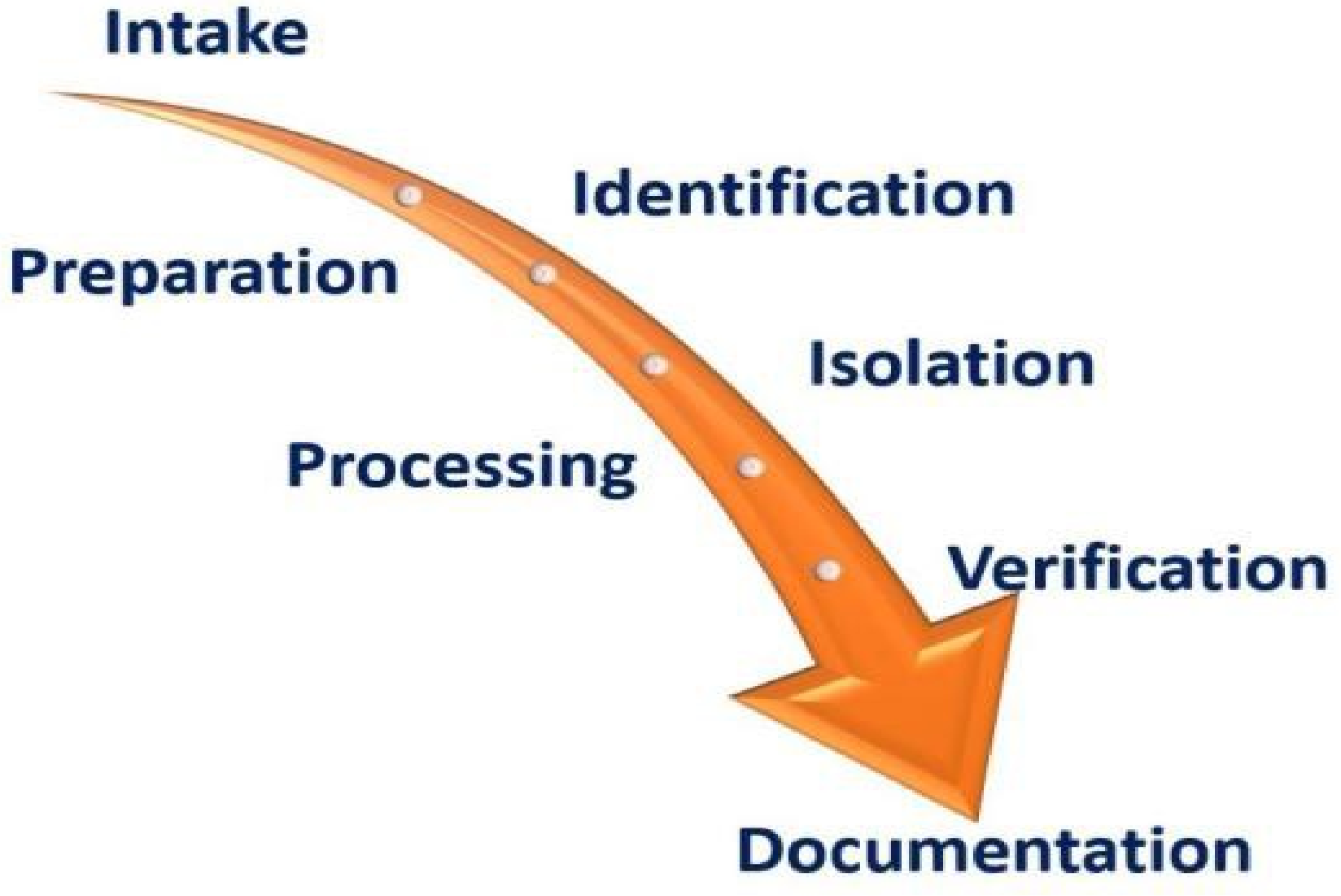
- The complexity and the diversity of Android applications and devices are based on their architecture models and their factory proprietary technology and formats
- The commercial tools that are used to acquire a logical image are highly capable, but they are too expensive.

Challenges of Acquisition and Analysis of Data on Android Devices

- There are different procedures and techniques used to obtain and verify data. it is difficult for examiners to adapt to the new devices and to choose a technique that will be suitable for their investigations and produce the most data from the simplest technique.
- It is difficult to disconnect Android devices from surrounding networks
- The hardware of the Android interface is difficult to set up and work
- It is difficult to acquire the data from the Android devices which are running custom ROMs

- Retrieving data from the storage of mobile phones may include:
  - Accessing data which are stored on SIM cards
  - Retrieving SMS/MMS outbox, inbox, and sent items
  - Reading the contents of mobile phones; Internet history

Digital Mobile Forensics Process



Identification Phase

Android mobile, identification steps:

1. Proper Legal authority for conducting a forensic testing for Android devices
2. The purpose of the forensic examination
3. The information regarding manufacture, model and type of the Android devices should be identified
4. Removing stored data to external storage
5. Checking other sources that may be considered as potential evidence

Preparation Phase

- Search related to the specific Android devices
- Identification of information regarding the manufacture, model and type of the Android devices
- Resources have “mobileforensicscentral.com" and “phonescoop.com"
- Suitable for the analysis of a mobile device and be capable of determining factors such as the target of the testing
- Tools should be compatible with the phone technology and include iDEN, SIM Card, GSM and CDMA

Isolation Phase

- From networks that can be connected with Android devices via wireless (Wi-Fi), infrared and Bluetooth network capabilities
- Prevents the adding of new data to the phone during new calls and texting
- Remote wiping or remote access via a \kill signal can result in the potential destruction of data being high
- High possibility of accidental overwriting of current data such as text messages and new calls

Processing Phase

- Desired data can be extracted
- Removable data storage cards should be processed separately from the Android devices:
  - as accessing data stored on these cards may change the data on the data storage card
- data storage/memory cards should be removed:
  - date, time information and files stored on the memory card/data storage

Verification Phase

- The accuracy of the data extracted from the devices
- Matching the data extracted from the Android device with the data displayed by the device itself is the only legal way

Documentation and Reporting Phase

1. When was the examination begun (date and time)?
2. What was the physical condition of the device?
3. Taking photos of the device and individual components, including SIM card and memory expansion card and labeling them with identifying information
4. What was the status of the device when they received it (on or off)?
5. Determining the model, manufacturer, and identifying information tools used during the examination
6. What data were documented through the examination?

Result of Identification Phase

Brand	Samsung
Device Name/ Model number	Galaxy Grand/ GT-I9082
Android Version	4.2.2
Baseband version	I9082XXUBNA3
Kernel Version	3.0.31-1257343
Build Number	JDQ39.I9082XXUBNC1
Serial Number	4100271687 2f6000
MicroSD Card	16 GB, Toshiba brand

Preparation Phase

Hardware required:

- the host machine (computer), Samsung USB Cable, USB Memory Storage and SD Adapter

Software required:

- Free tool: include Santoka Linux VM, Kali Linux VM, AccessData FTK imager, Android Studio, and EaseUS Data Recovery Wizard

Isolation Phase

- Bluetooth and wireless network (Wi-Fi) were switched off in the mobile device
- no SIM card used no need to perform extra steps

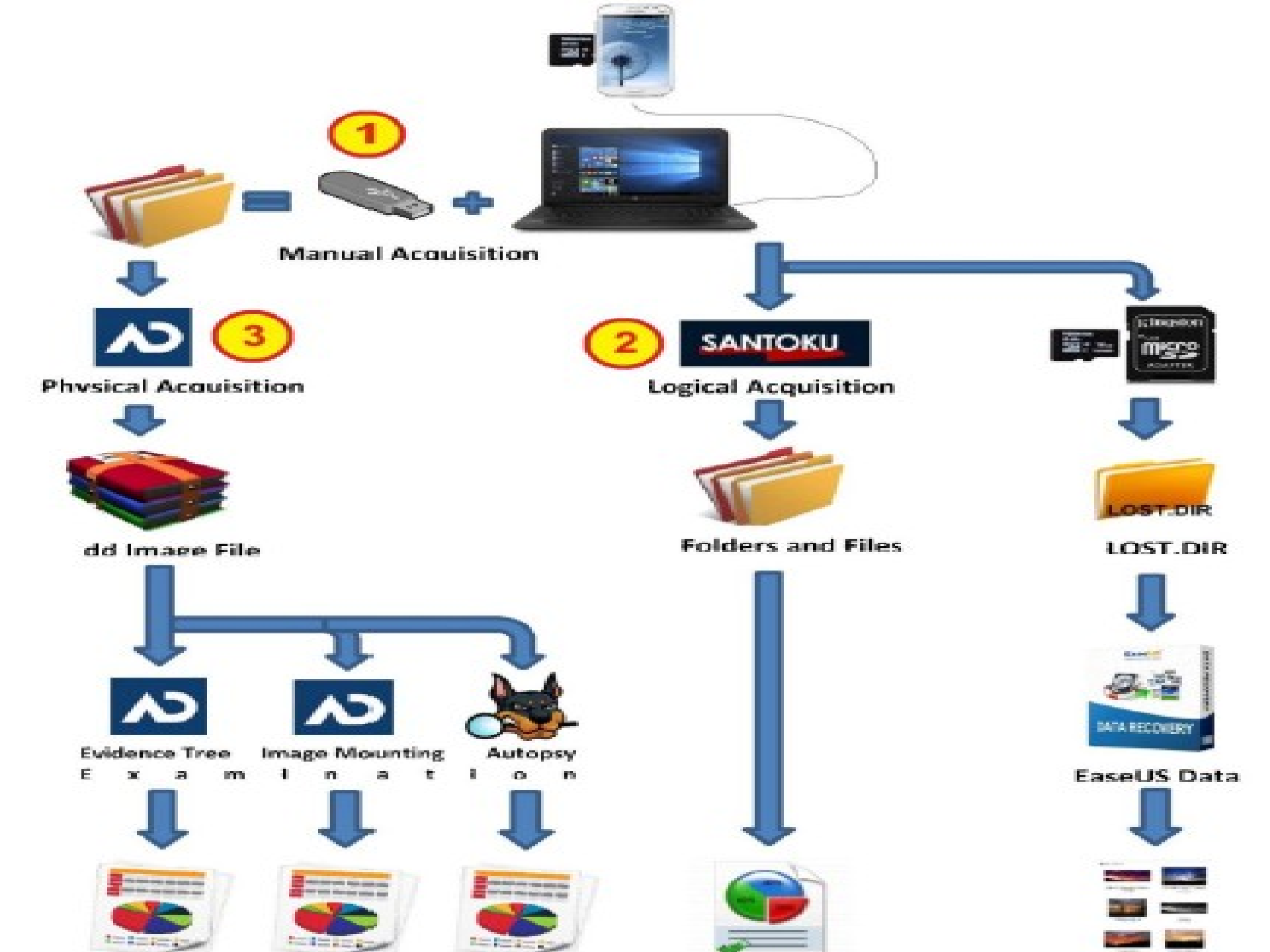
Processing Phase

Step 1:

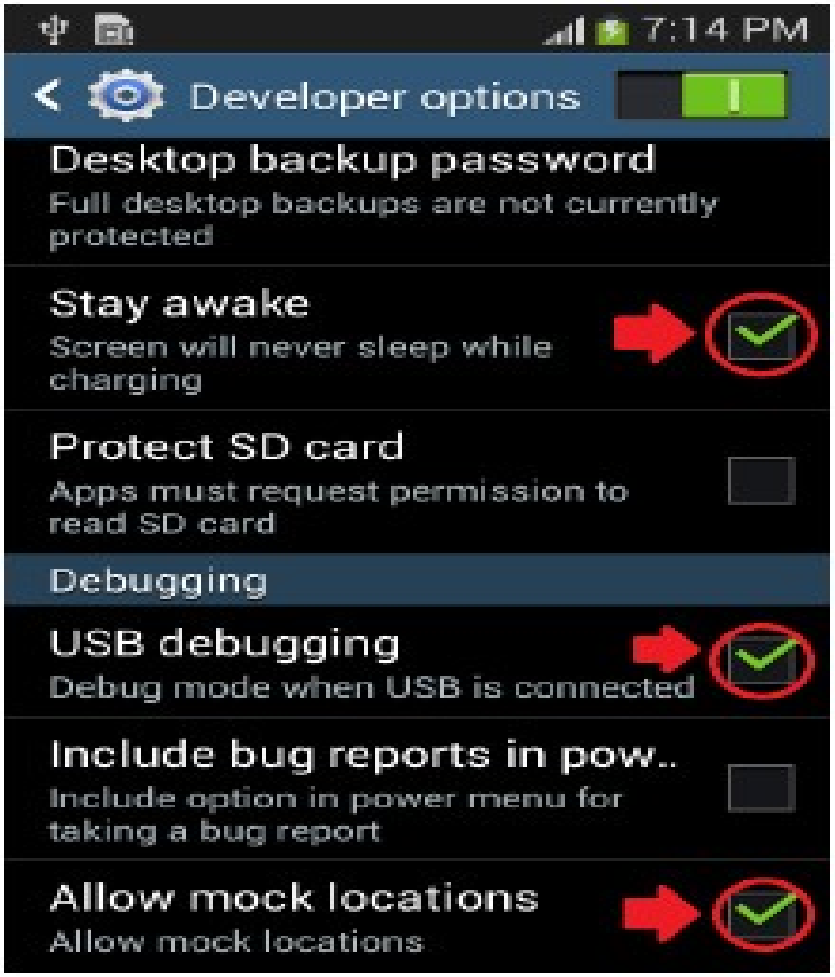
- Connection and Backup (Manual Acquisition)
- The USB driver (Google USB driver) of mobile phone applications was installed after installing Android Studio (SDK manager) to connect the mobile device with the computer
- the mobile device files were moved to the USB Memory Drive in the computer using manual full backup, which is called “Manual Direct Acquisition”

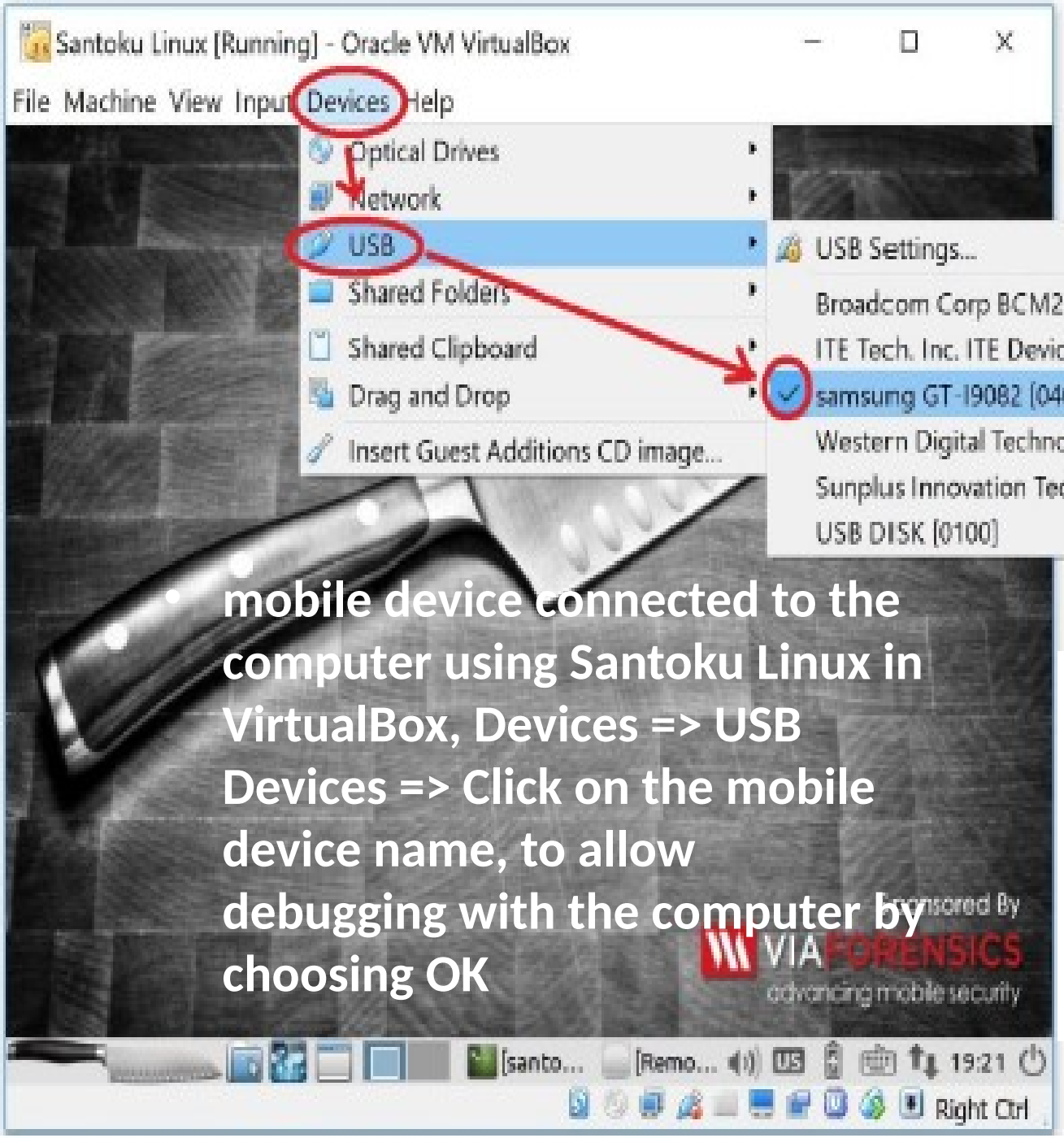
Step 2:

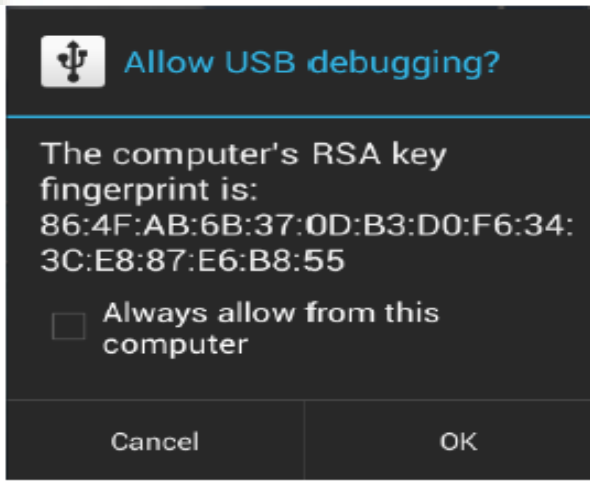
- Unlock the mobile device using the Santoku Linux Alpha tool, which is sponsored by ViaForensics (NowSecure Company)
- the mobile device can be unlocked to access the root of the devices file system

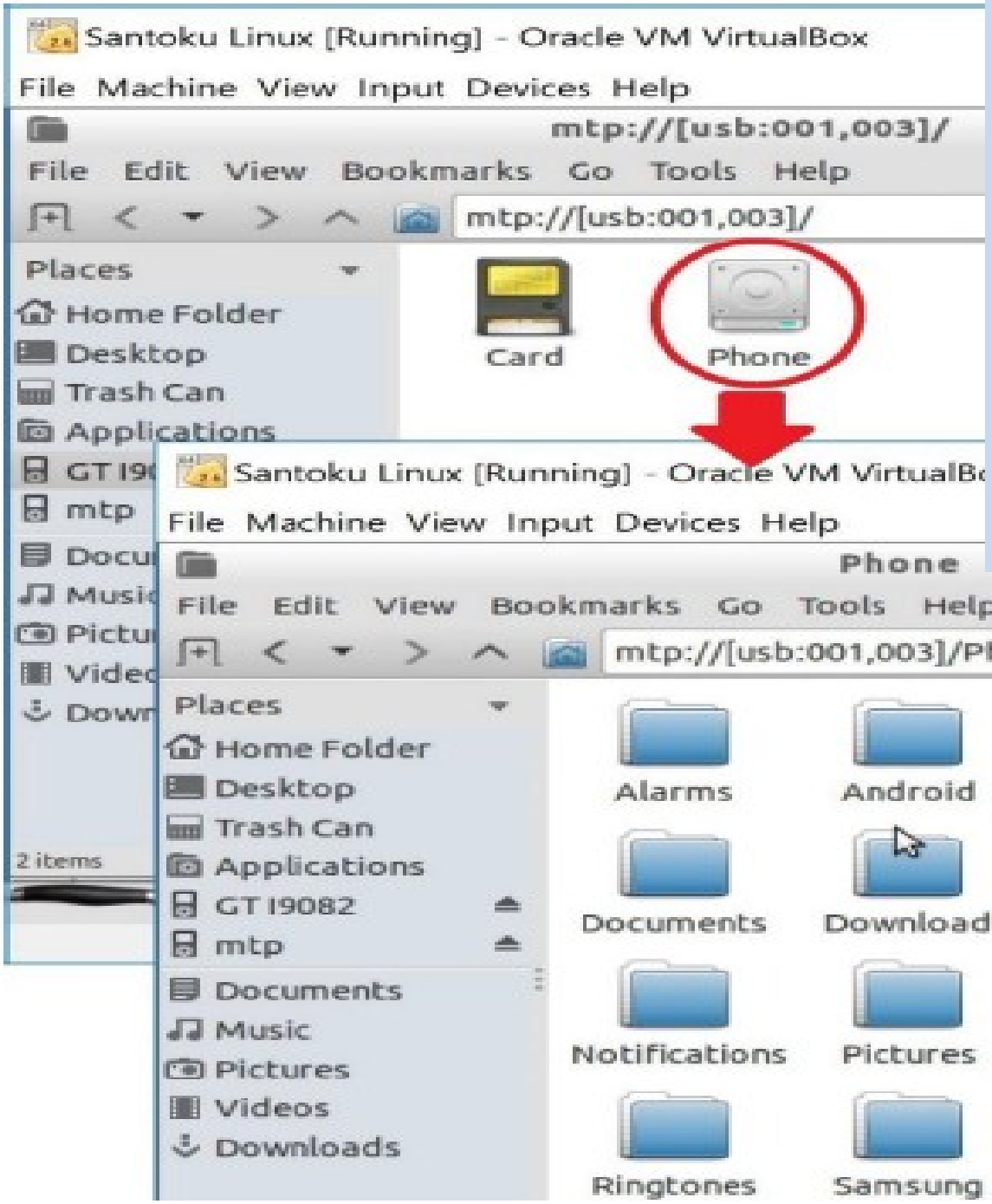

1
Manual Acquisition
3
Phvsical Acquisition
2
SANTOKU
Logical Acquisition
dd Imaee File
Folders and Files
LOST.DIR
LOST.DIR
Evidence Tree
Image Mounting
Autopsy
E x a m i n a t i o n
EaseUS Data

1. The mobile device should be enabled for USB debugging by Settings => Developer Options, then checking (Allow mock locations), (Stay awake) and (USB debugging)
2. the Developer Options setting is not visible, go to Settings => About devices => Tap on (Build Number) seven times, then Developer Options will appear.

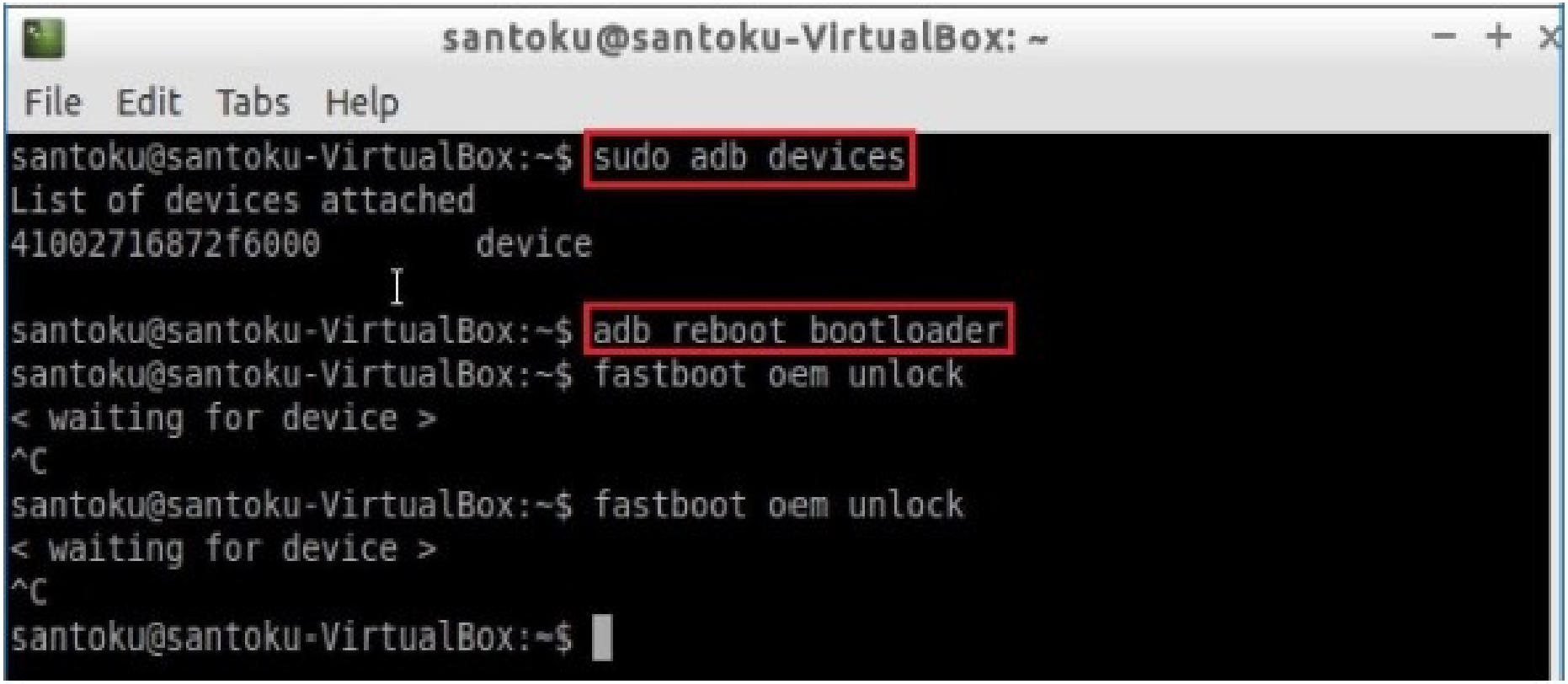



Santoku Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Optical Drives
Network
USB
Shared Folders
Shared Clipboard
Drag and Drop
Insert Guest Additions CD image...
USB Settings...
Broadcom Corp BCM20702A0 [0112]
ITE Tech. Inc. ITE Device(8386) [0004]
samsung GT-I9082 [0400]
Western Digital Technologies, Inc
Sunplus Innovation Technology I
USB DISK [0100]
Vendor ID: 04E8
Product ID: 6860
Revision: 0400
Serial No. 410027168f2f6000
State: Captured
mobile device connected to the computer using Santoku Linux in VirtualBox, Devices => USB Devices => Click on the mobile device name, to allow debugging with the computer by choosing OK
Sponsored By
VIAFORENSICS
advancing mobile security
[santo...
[Remo...
19:21
Right Ctrl


Allow USB debugging?
The computer's RSA key fingerprint is:
86:4F:AB:6B:37:0D:B3:D0:F6:34:
3C:E8:87:E6:B8:55
Always allow from this computer
Cancel
OK



open the mobile device in File Manager in Santoku Linux after revealing the interface, and then copy the mobile files manually to the Santoku Linux or to the host machine



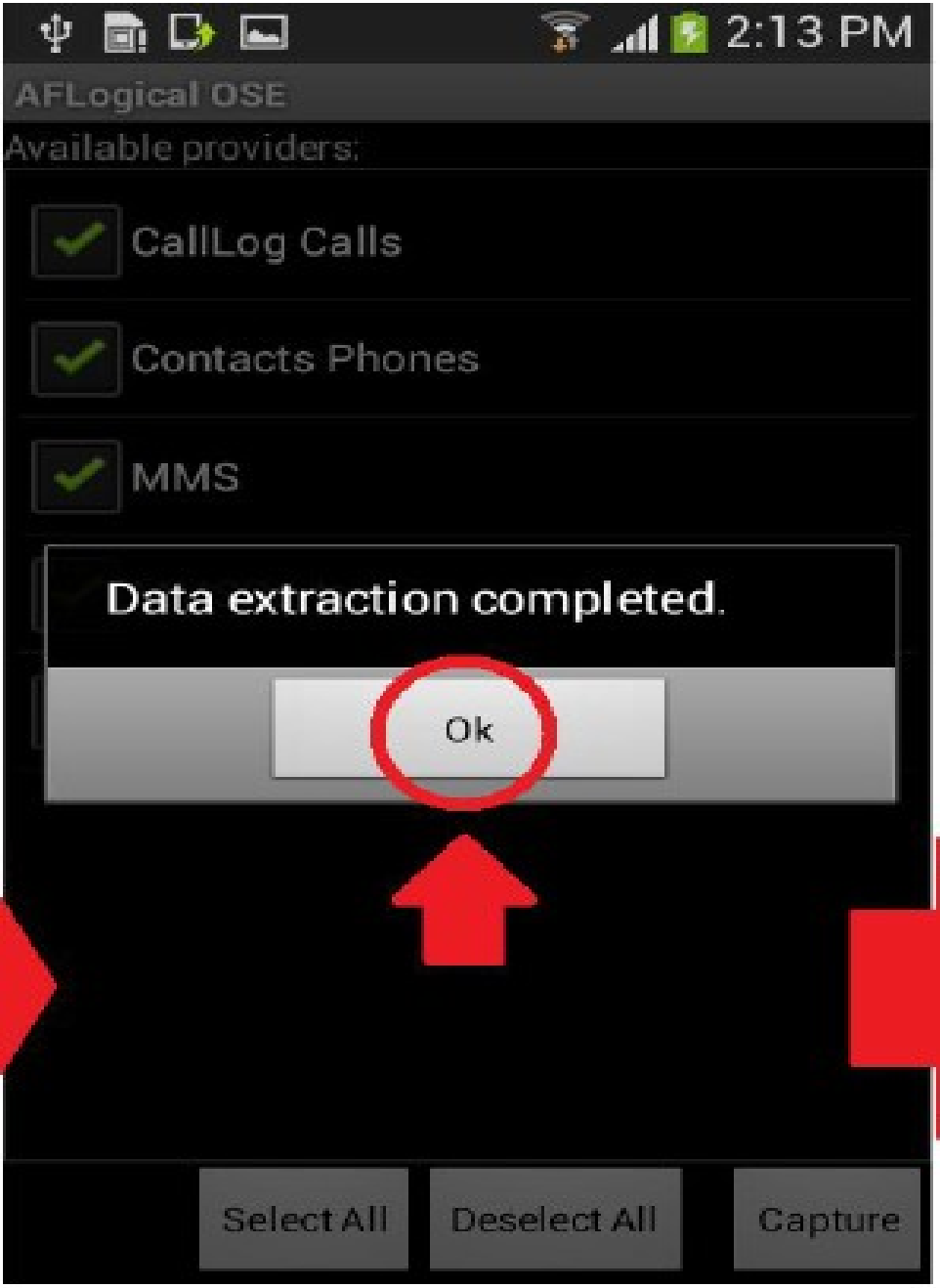
- In the Santoku Linux Virtual Machine => Device Forensics => AFLogical OSE command prompt, the command (sudo adb devices)
  - show the serial number of the mobile device
  - before typing the command (adb reboot bootloader) to reboot the mobile device into recovery mode

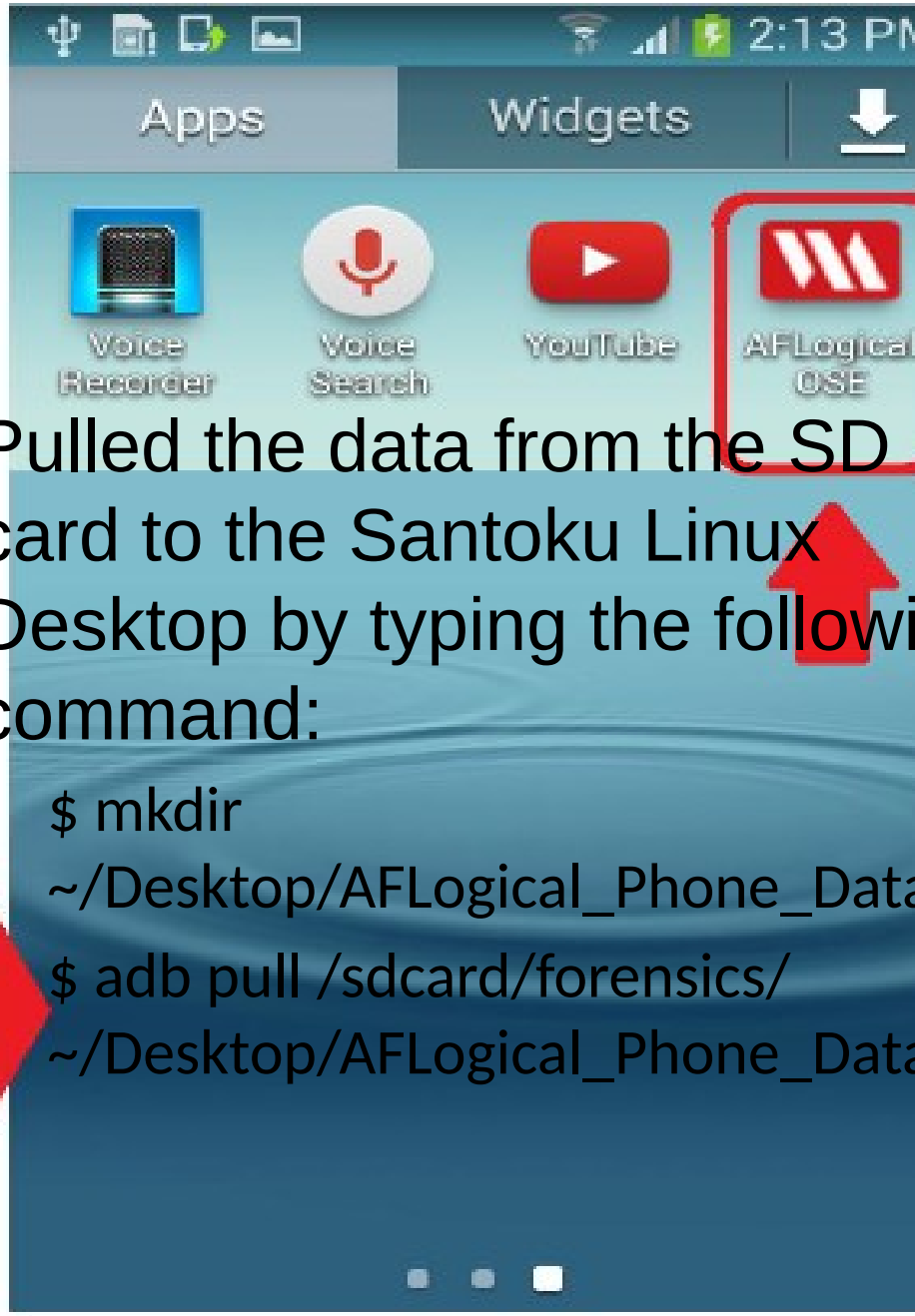
An Interface of AFLogical Command

```
santoku@santoku-VirtualBox:~$ aflogical-ose
Make sure android device is connected to USB
[sudo] password for santoku:

286 KB/s (28794 bytes in 0.098s)
        pkg: /data/local/tmp/AFLogical-OSE_1.5.2.apk
Success

Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.
ndroid.ForensicsActivity }

Press enter to pull /sdcard/forensics into ~/aflogical-data/

pull: building file list...
pull: /sdcard/forensics/20170109.1413/CallLog Calls.csv -> /home/santoku/aflogi
cal-data/20170109.1413/CallLog Calls.csv
pull: /sdcard/forensics/20170109.1413/MMSParts.csv -> /home/santoku/aflogical-d
ata/20170109.1413/MMSParts.csv
pull: /sdcard/forensics/20170109.1413/SMS.csv -> /home/santoku/aflogical-data/2
0170109.1413/SMS.csv
pull: /sdcard/forensics/20170109.1413/MMS.csv -> /home/santoku/aflogical-data/2
0170109.1413/MMS.csv
pull: /sdcard/forensics/20170109.1413/Contacts Phones.csv -> /home/santoku/aflo
gical-data/20170109.1413/Contacts Phones.csv
pull: /sdcard/forensics/20170109.1413/info.xml -> /home/santoku/aflogical-data/
20170109.1413/info.xml
6 files pulled. 0 files skipped.
165 KB/s (180562 bytes in 1.066s)

santoku@santoku-VirtualBox:~$
```

AFLogical application: device information

- Contacts Phones, MMS, SMS, MMS Parts, and call logs
- SD card installed on the mobile device (or built in) to extract the data

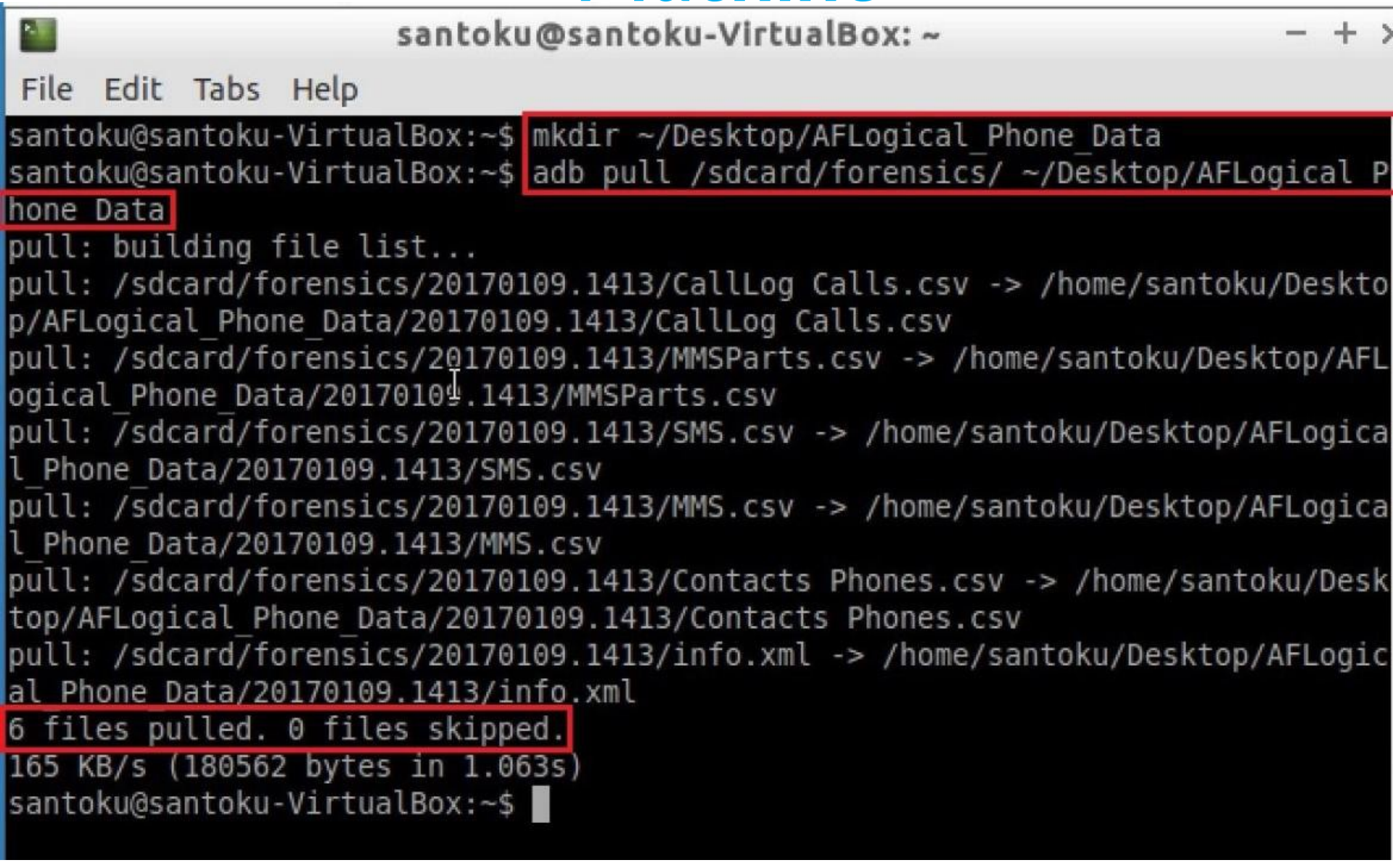




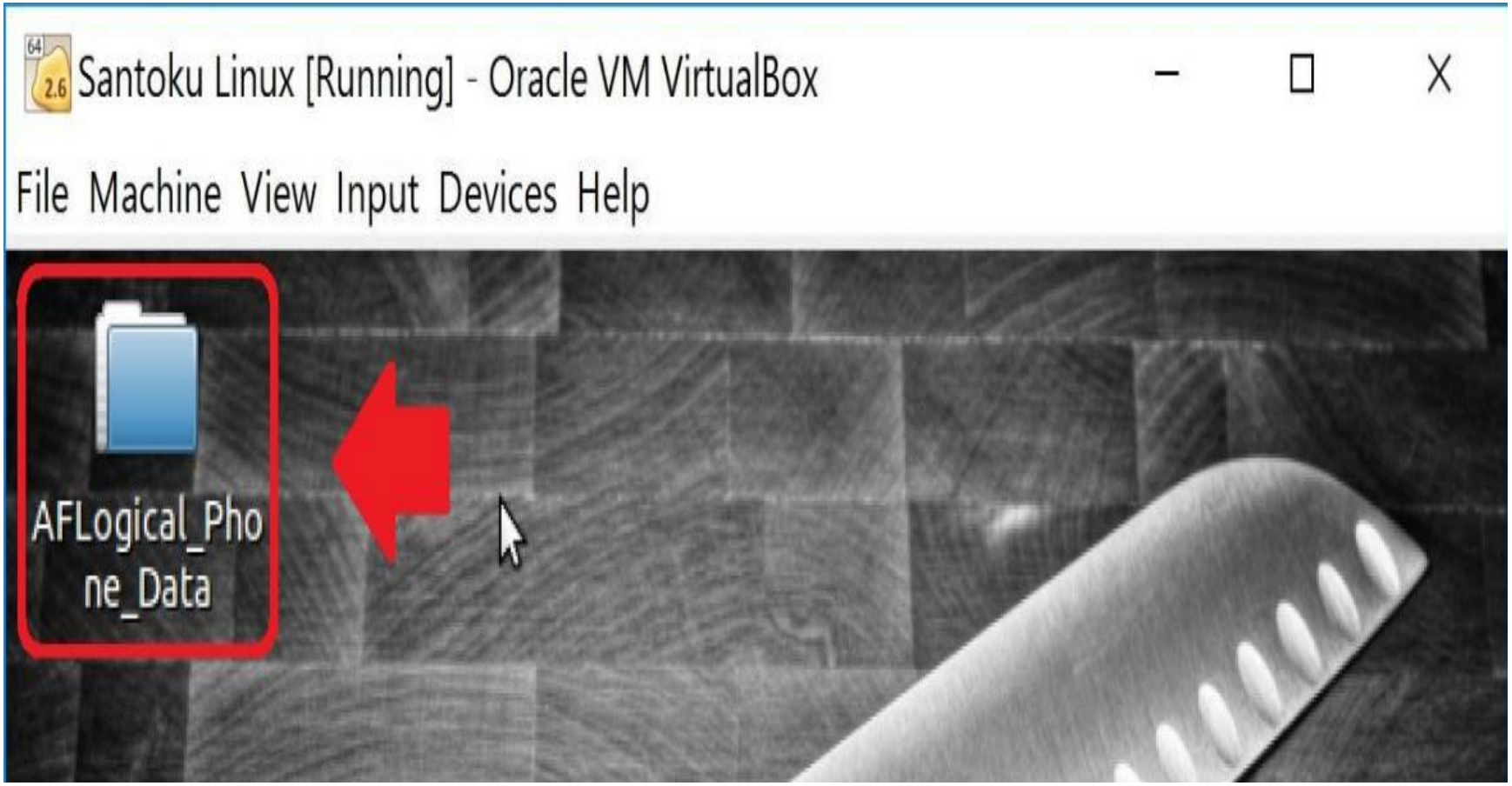
Pulled the data from the SD card to the Santoku Linux Desktop by typing the followi command:

- $ mkdir ~/Desktop/AFLogical_Phone_Data
- $ adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data

Pulling the Data to the Santoku Machine



Create AFLogical of Mobile in the Santoku Linux Desktop

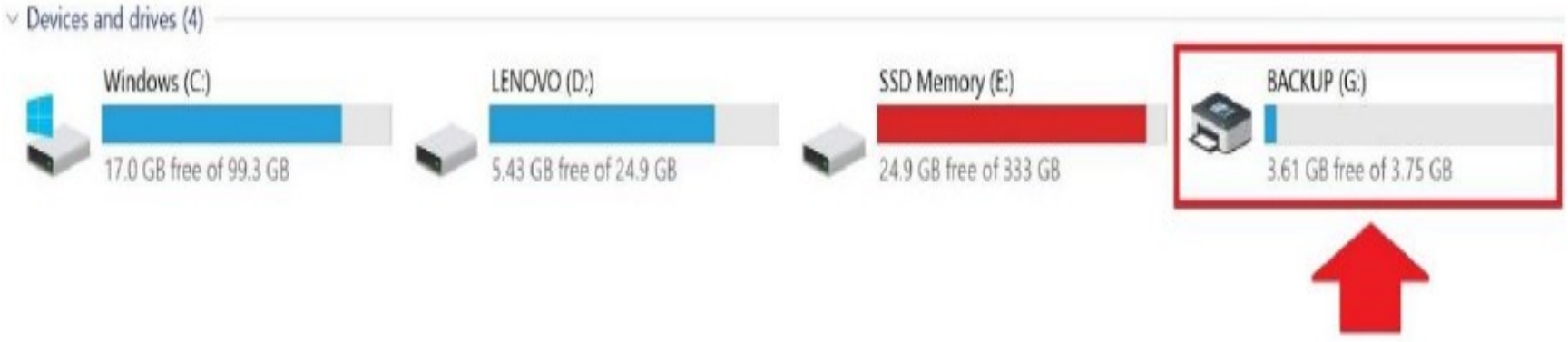


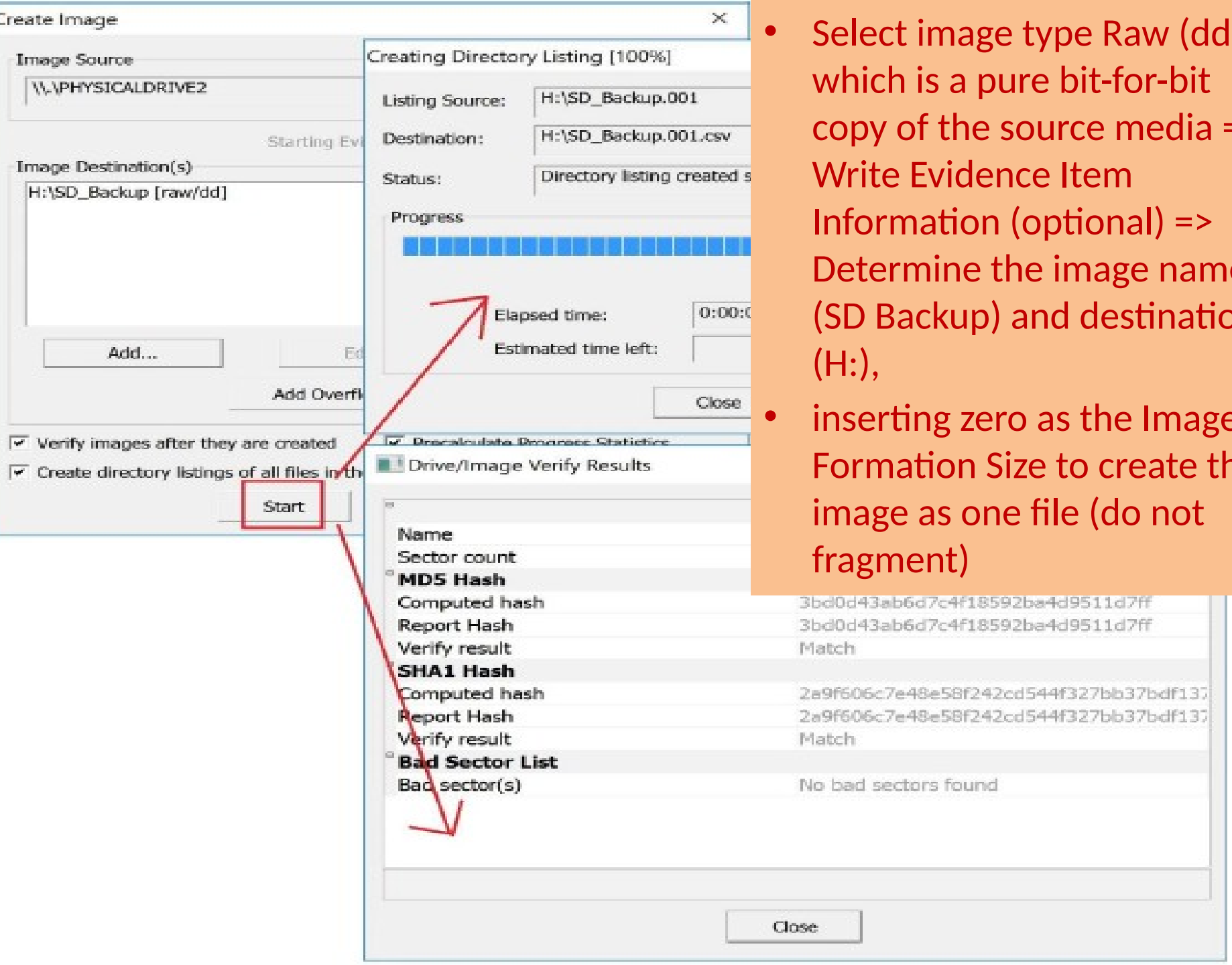
Physical Acquisition

To extract the data of the full contents of memory chips from the mobile device

- Access Data FTK Imager tool was used to obtain a Raw (dd) image of the mobile devices backup, which is located on the USB memory Drive, and save it on the computer

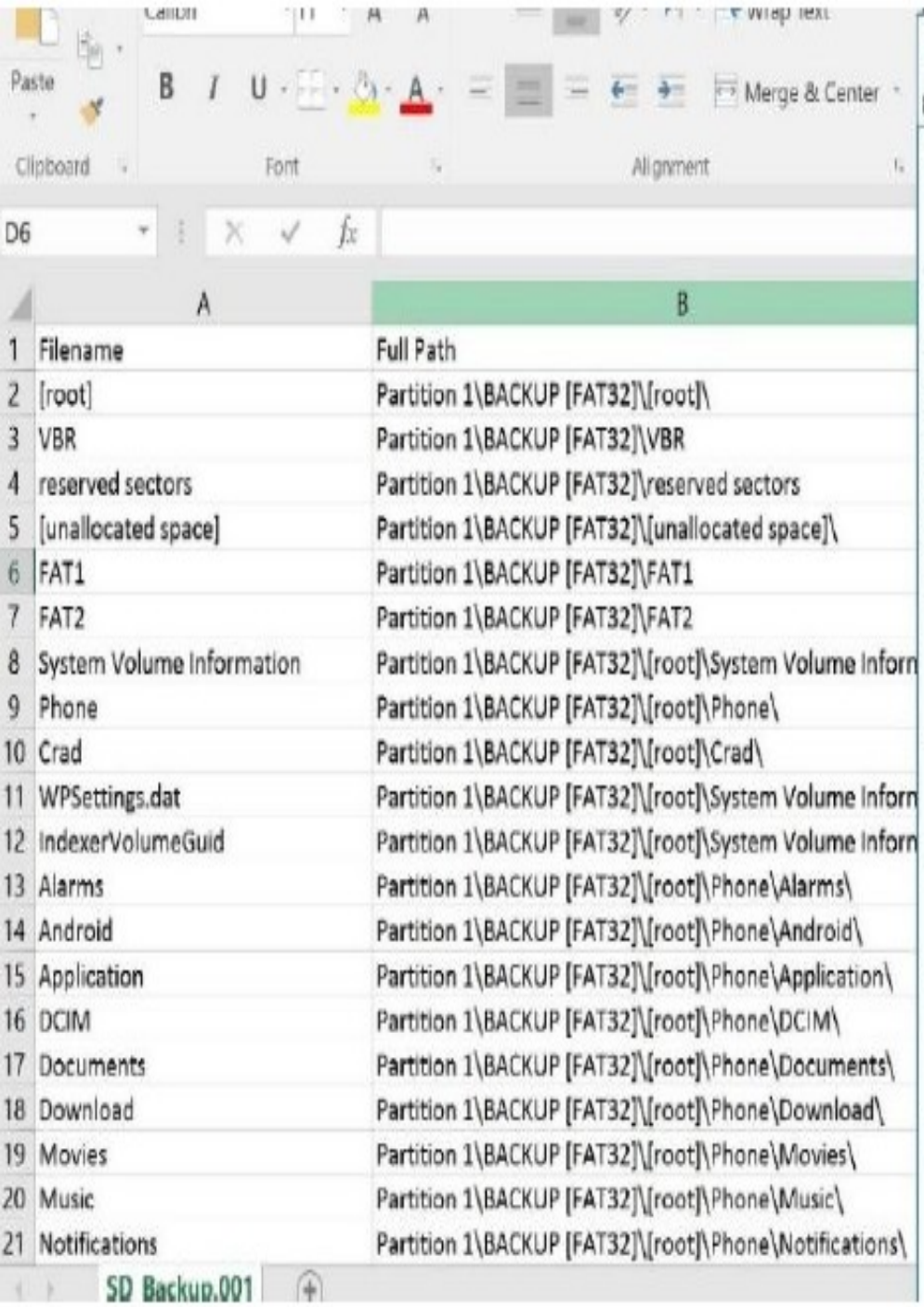
- Run Access Data FTK Imager => File => Create Disk Image => Physical Drive (data in USB Memory drive) => Select the Backup drive





- Select image type Raw (dd) which is a pure bit-for-bit copy of the source media => Write Evidence Item Information (optional) => Determine the image name (SD Backup) and destination (H:),
- inserting zero as the Image Formation Size to create the image as one file (do not fragment)

1. SD Backup:001: Big dd file image, size = 3.75 GB, raw image file is an uncompressed file format
2. SD Backup:001:csv: Microsoft Excel Comma Separated Values File, which has all files and folders with their details
3. SD Backup:001:txt: Text Document, which has all raw image file information, case information, Source Type, Cylinders, Heads,MD5, SHA1 etc.



Paste
Clipboard
Font
Alignment
Merge & Center
D6

	A	B
1	Filename	Full Path
2	[root]	Partition 1\BACKUP [FAT32]\[root]\
3	VBR	Partition 1\BACKUP [FAT32]\VBR
4	reserved sectors	Partition 1\BACKUP [FAT32]\reserved sectors
5	[unallocated space]	Partition 1\BACKUP [FAT32]\[unallocated space]\
6	FAT1	Partition 1\BACKUP [FAT32]\FAT1
7	FAT2	Partition 1\BACKUP [FAT32]\FAT2
8	System Volume Information	Partition 1\BACKUP [FAT32]\[root]\System Volume Inforn
9	Phone	Partition 1\BACKUP [FAT32]\[root]\Phone\
10	Crad	Partition 1\BACKUP [FAT32]\[root]\Crad\
11	WPSettings.dat	Partition 1\BACKUP [FAT32]\[root]\System Volume Inforn
12	IndexerVolumeGuid	Partition 1\BACKUP [FAT32]\[root]\System Volume Inforn
13	Alarms	Partition 1\BACKUP [FAT32]\[root]\Phone\Alarms\
14	Android	Partition 1\BACKUP [FAT32]\[root]\Phone\Android\
15	Application	Partition 1\BACKUP [FAT32]\[root]\Phone\Application\
16	DCIM	Partition 1\BACKUP [FAT32]\[root]\Phone\DCIM\
17	Documents	Partition 1\BACKUP [FAT32]\[root]\Phone\Documents\
18	Download	Partition 1\BACKUP [FAT32]\[root]\Phone\Download\
19	Movies	Partition 1\BACKUP [FAT32]\[root]\Phone\Movies\
20	Music	Partition 1\BACKUP [FAT32]\[root]\Phone\Music\
21	Notifications	Partition 1\BACKUP [FAT32]\[root]\Phone\Notifications\

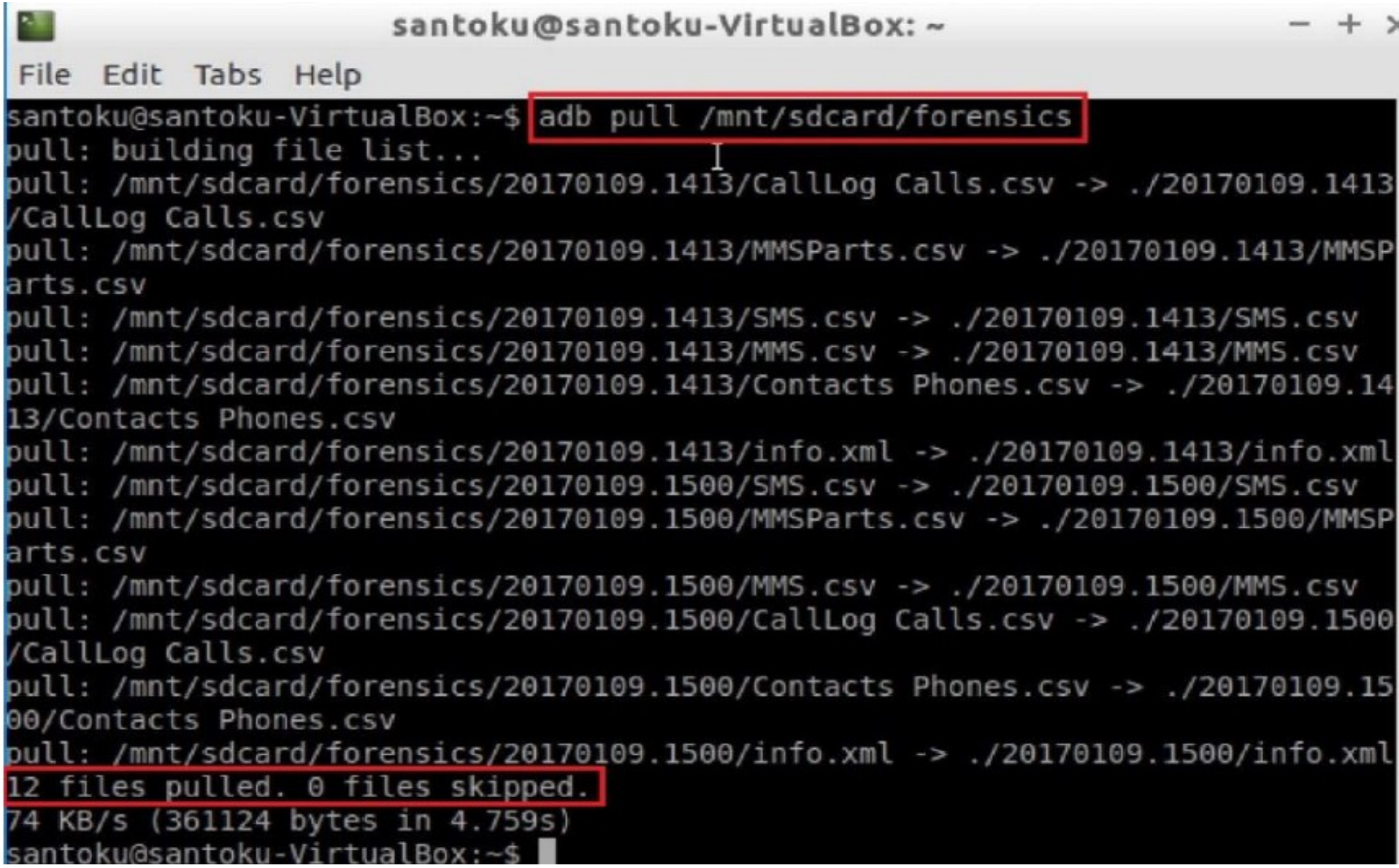
SD Backup.001

SD_Backup.001.txt Notepad

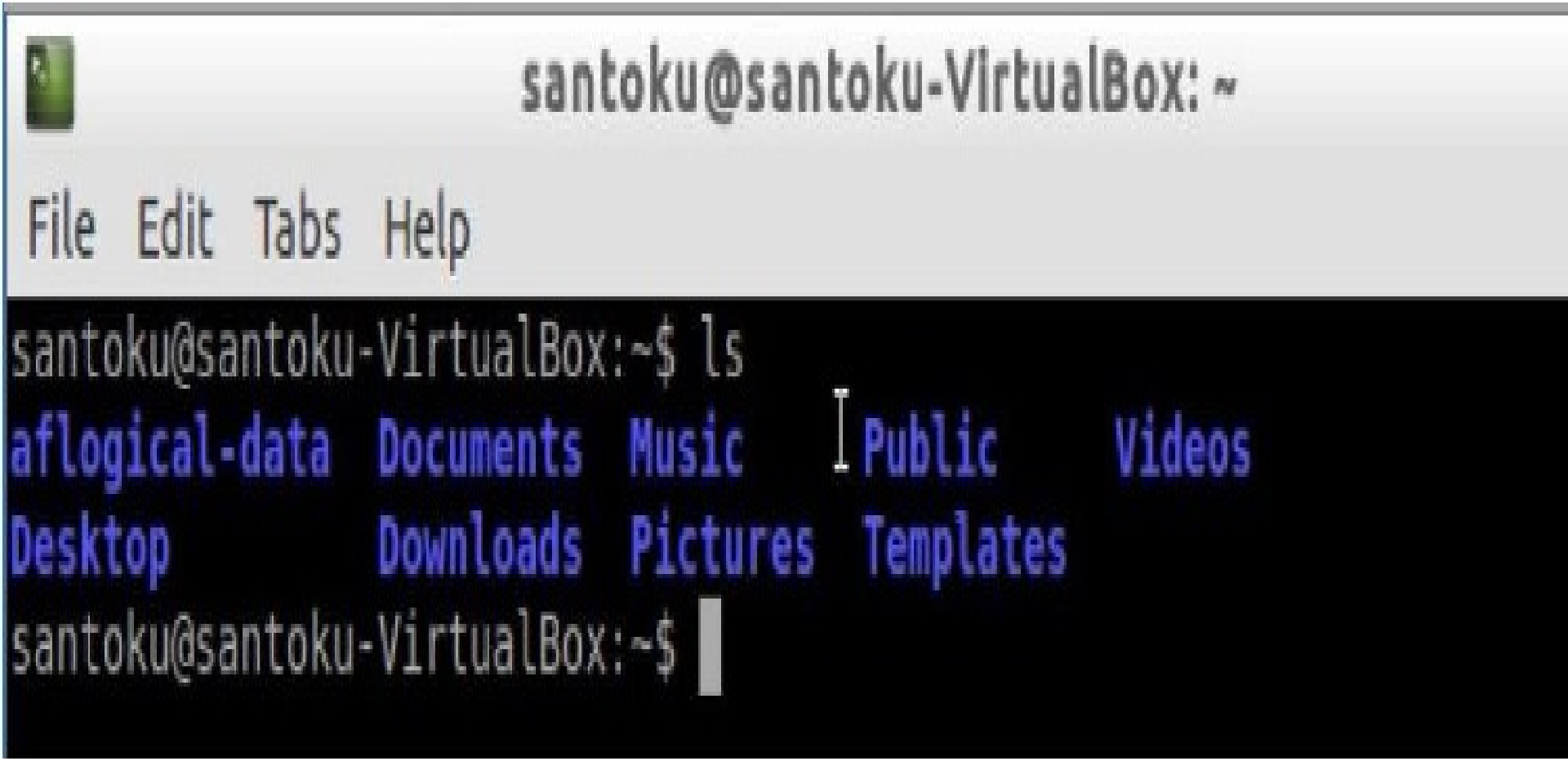
File Edit Format View Help

```
Created By AccessData® FTK® Imager 3.4.2.6

Case Information:
Acquired using: ADI3.4.2.6
Case Number: IFN701 Project 1
Evidence Number: 1
Unique description: Report
Examiner:
Notes:

---------------------------------------------

Information for H:\SD_Backup:

Physical Evidentiary Item (Source) Information:
[Device Info]
 Source Type: Physical
[Drive Geometry]
 Cylinders: 490
 Tracks per Cylinder: 255
```

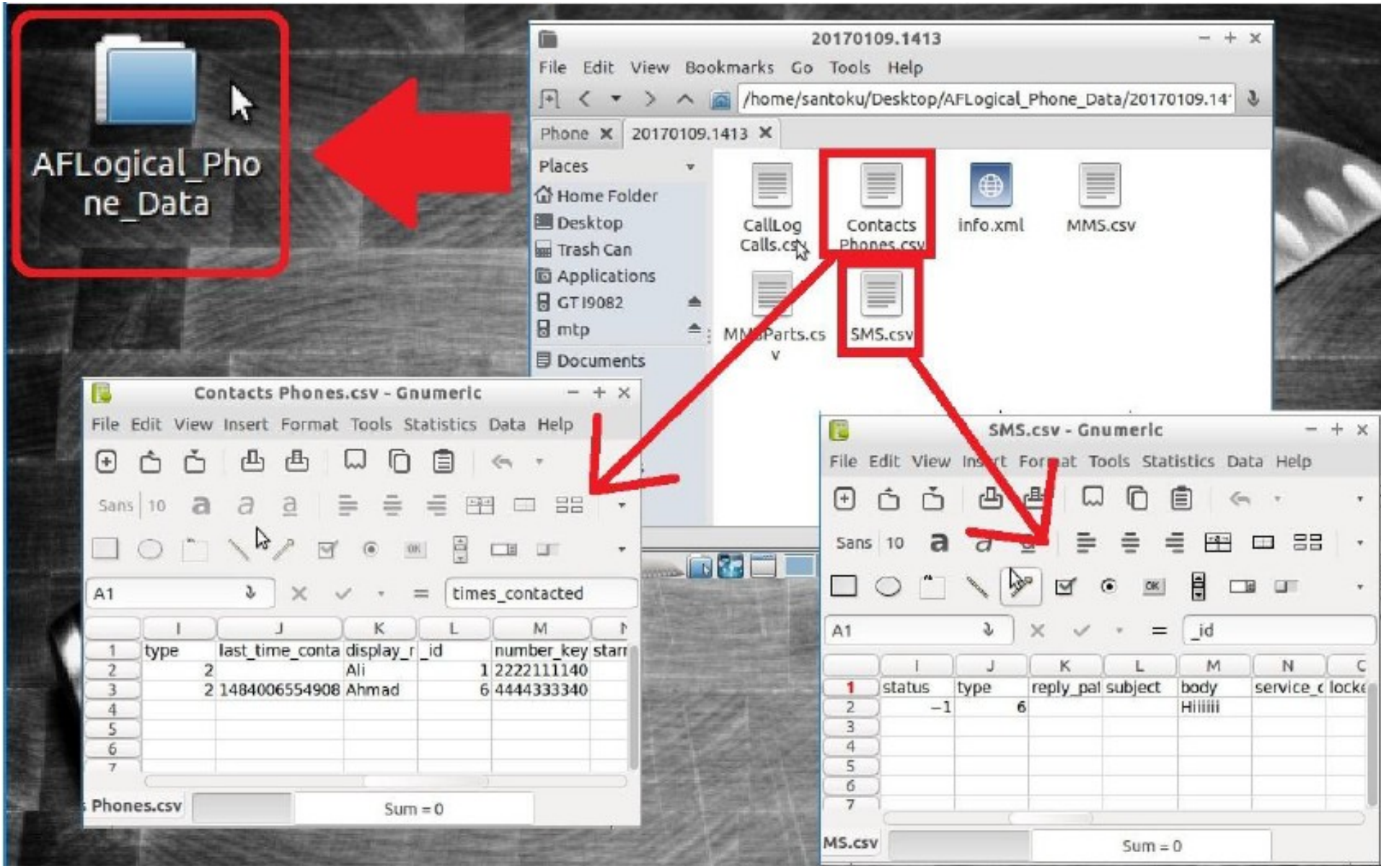
Verification Phase: Extracting Data



Directories after Aflogical-Data was Created



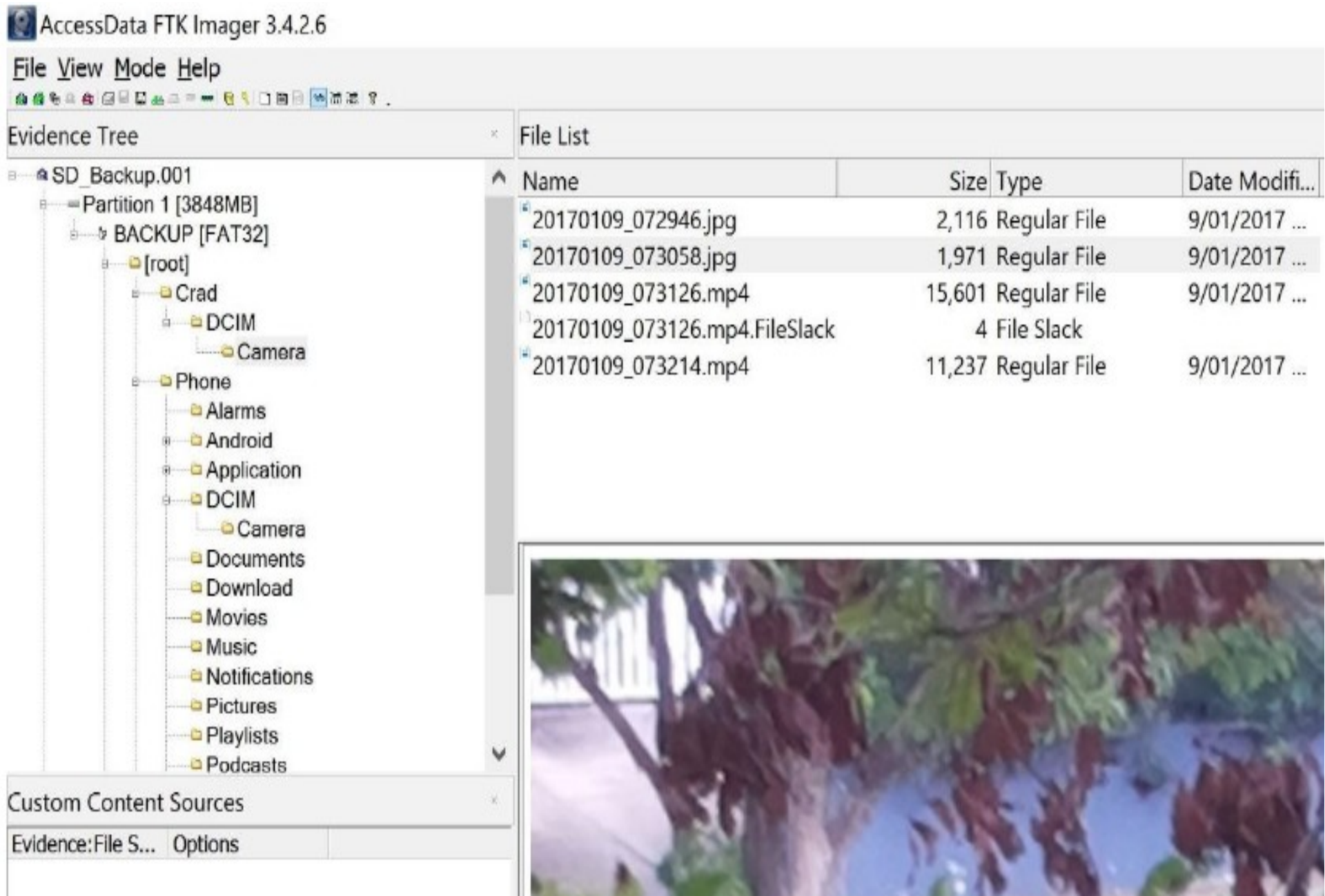
Data at the Santoku Machine



Physical Examination using dd Image Evidence Tree in AccessData FTK Imager

1. Run AccessData FTK Imager tool => File => Add Evidence Item => Image File => Enter Source Path (Raw dd Image file location) => Finish
2. This enables exploration of the image files in the Evidence tree. The full contents of the memory chips on the phone can be found. Contacts phone numbers, MMS, SMS, MMS Parts, Call Logs, Photos, and Video in the Android device were revealed

Image File Evidence Tree



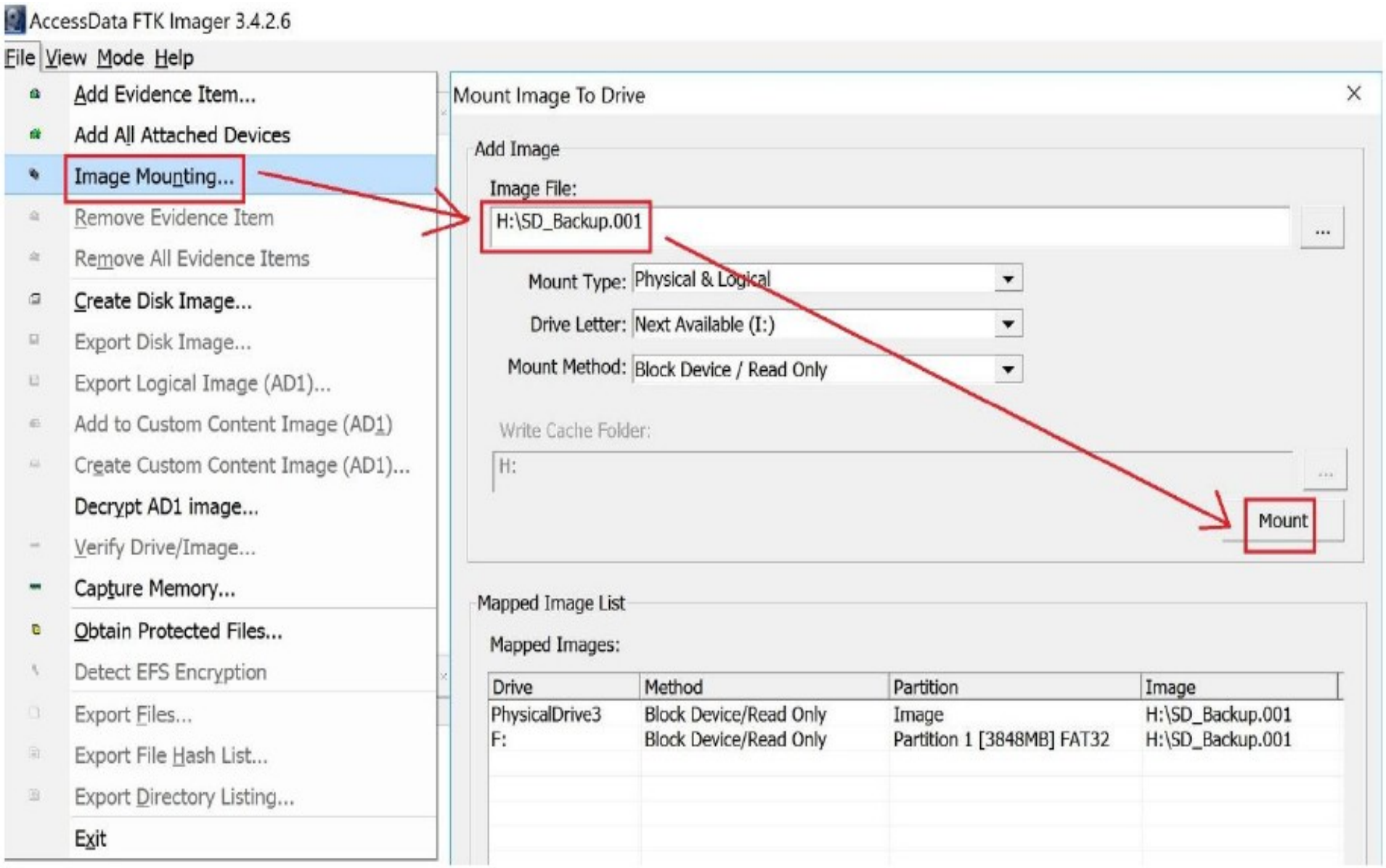
Physical Examination using Image Mounting in AccessData FTK Imager

1. Run AccessData FTK Imager tool => File => image Mounting => Browse the Backup Image (Raw dd Image file location) => Mount

A new partition, (F:), appears in Drive

This partition is created as a temporary partition to look like the mobile device storage

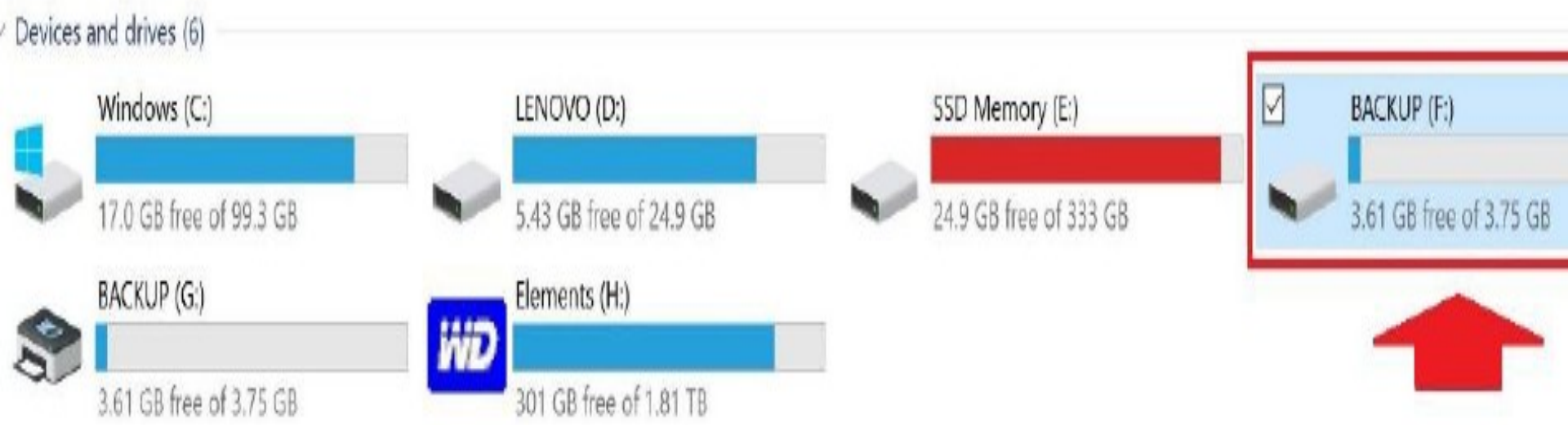
Image Mounting Examination



2. Mobile device files can then be explored in the new partition (F:)

The full contents of memory chips on the phone can be found. Contacts Phones, MMS, SMS, MMS Parts, Call Logs, Photos, and Video in the Android device were revealed

Backup Location



SD_Backup:host1:vol2

localhost:9999/autopsy?mod=1&submod=2&case=SD_Backup&host=host1&inv=Alman&vol=vol2

Most Visited | Offensive Security | Kali Linux | Kali Docs | Kali Tools | Aircrack-ng

File Analysis | Keyword Search | File Type | Image Details | Meta Data | Data Unit | Help | Close

Directory Seek

Enter the name of a directory that you want to view.
C:/

View

File Name Search

Enter a Perl regular expression for the file names you want to find.

Search

All Deleted Files

Expand Directories

Current Directory: C:/ /Phone/

Add Note | Generate MD5 List of Files

Del	Type dir / in	Name	Written	Accessed	Created	Size	UID	GID	Meta
	d / d	../	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	4096	0	0	2
	d / d	./	2017-01-09 19:06:08 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:06 (EST)	4096	0	0	8
	d / d	Alarms/	2017-01-09 19:06:14 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:13 (EST)	4096	0	0	518
	d / d	Android/	2017-01-09 19:06:14 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:13 (EST)	4096	0	0	520
	d / d	Application/	2017-01-09 19:06:26 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:25 (EST)	4096	0	0	522
	d / d	DCIM/	2017-01-09 19:06:36 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:35 (EST)	4096	0	0	523
	d / d	Documents/	2017-01-09 19:06:44 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:43 (EST)	4096	0	0	525
	d / d	Download/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	527
	d / d	Movies/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	529
	d / d	Music/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	531
	d / d	Notifications/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	533
	d / d	Pictures/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	535
	d / d	Playlists/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	537
	d / d	Podcasts/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	539
	d / d	Ringtones/	2017-01-09 19:06:46 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:44 (EST)	4096	0	0	541
	d / d	Samsung/	2017-01-09 19:06:48 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:06:47 (EST)	4096	0	0	543
	d / d	SMemo/	2017-01-09 19:07:12 (EST)	2017-01-09 00:00:00 (EST)	2017-01-09 19:07:11 (EST)	4096	0	0	545

Summary

- acquisitions and analysis technical methods by Open Source Android Forensics tools (OSAF)
- commercial tool will save time help to get accurate results
- Understanding Android architecture, forensic process and tools prior to data extraction and recovery of files

Non-invasive vs. Invasive Forensics

- Non-invasive
- Non-invasive methods can deal with other tasks, such as unlocking the SIM lock or/and the operator lock, the operating system update, IMEI number modification, etc.

- These techniques are virtually inapplicable in cases where the device has sustained severe physical damage.

- Types of non-invasive mobile forensic methods:

- **Manual extraction**
- The forensic examiner merely browses through the data using the mobile device's touchscreen or keypad.

- Information of interest discovered on the phone is photographically documented.

- **Logical extraction**
- This approach involves instituting a connection between the mobile device and the forensic workstation using a USB cable, Bluetooth, Infrared or RJ-45 cable.

- **JTAG method**
- JTAG is a non-invasive form of physical acquisition that could extract data from a mobile device even when data was difficult to access through software avenues because the device is damaged(partially operatable), locked or encrypted.

- The process involves connecting to the Test Access Ports (TAPs) on a device.

- **Hex Dump**
- Similar to JTAG, Hex dump is another method for physical extraction of raw information stored in flash memory.

- Image taken is fairly technical—in binary format.

2. Invasive Methods

- Typically, they are longer and more complex. In cases where the device is entirely non- functional.

- To retrieve data from the device might be to manually remove and image the flash memory chips of the device.

- Forensic expertize is required to acquire the chip's contents physically.

- **Chip-off**
- A process that refers to obtaining data straight from the mobile device's memory chip.

- The chip is detached from the device and a chip reader or a second phone is used to extract data stored on the device under investigation.

- The chip-off process is expensive, training is required, and the examiner should procure specific hardware.

- Experts advise having recourse to chip-off when:
  a) other methods of extraction are already attempted,
  b) it is important to preserve the current state of device's memory,
  c) the memory chip is the only element in a mobile device that is not broken.

- **Micro read**
- This method refers to manually taking an all-around view through the lenses of an electron microscope and analyzing data seen on the memory chip, more specifically the physical gates on the chip.

Mobile Jammer

Digital Forensics and Investigation [CET4033B]

TYBTech CSF, Semester-V
AY 2023-24

Dr Sumedha Sirsikar

Covert Investigation

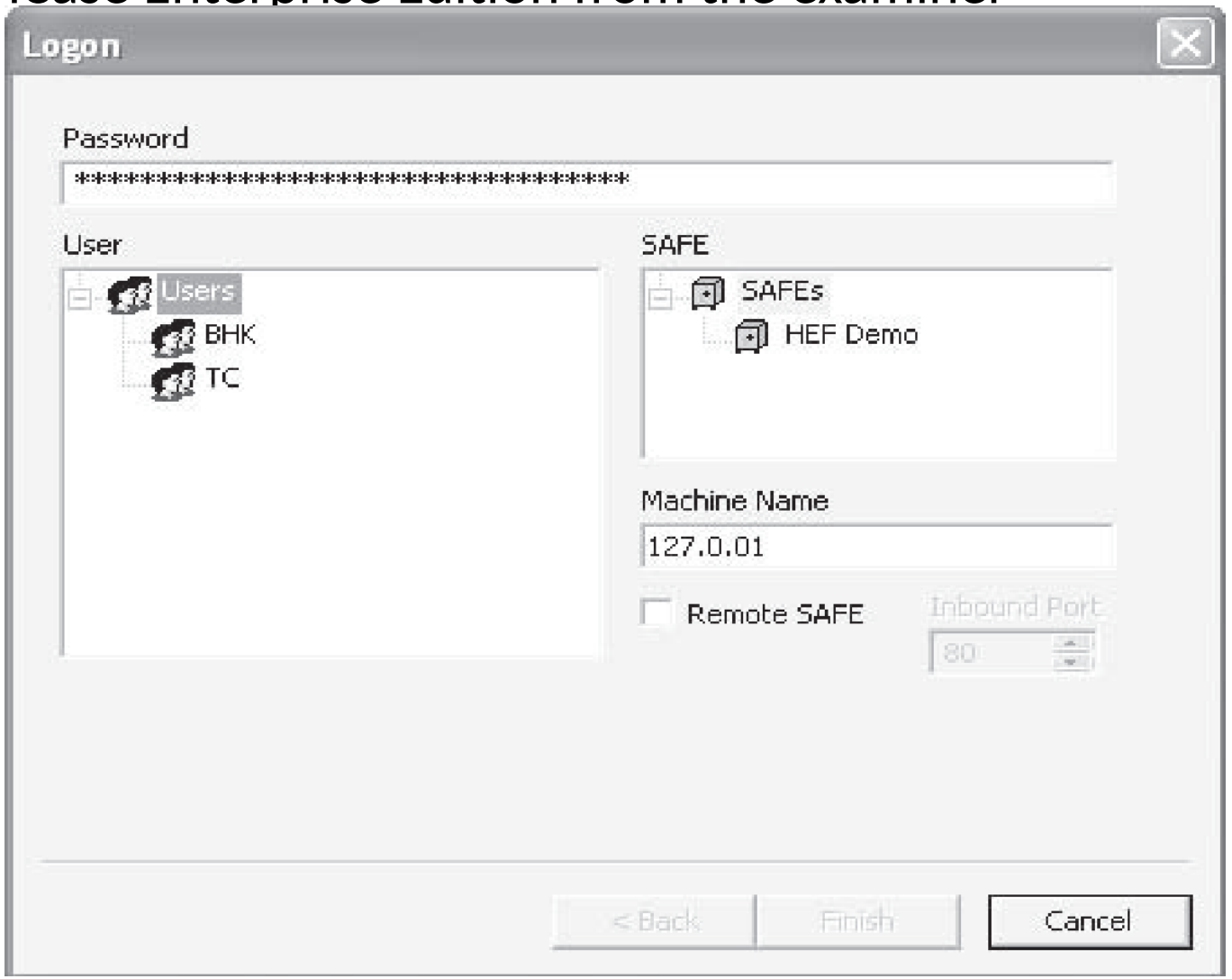
Remote Investigation Tools

Without the subject discovering that he or she is being actively investigated:

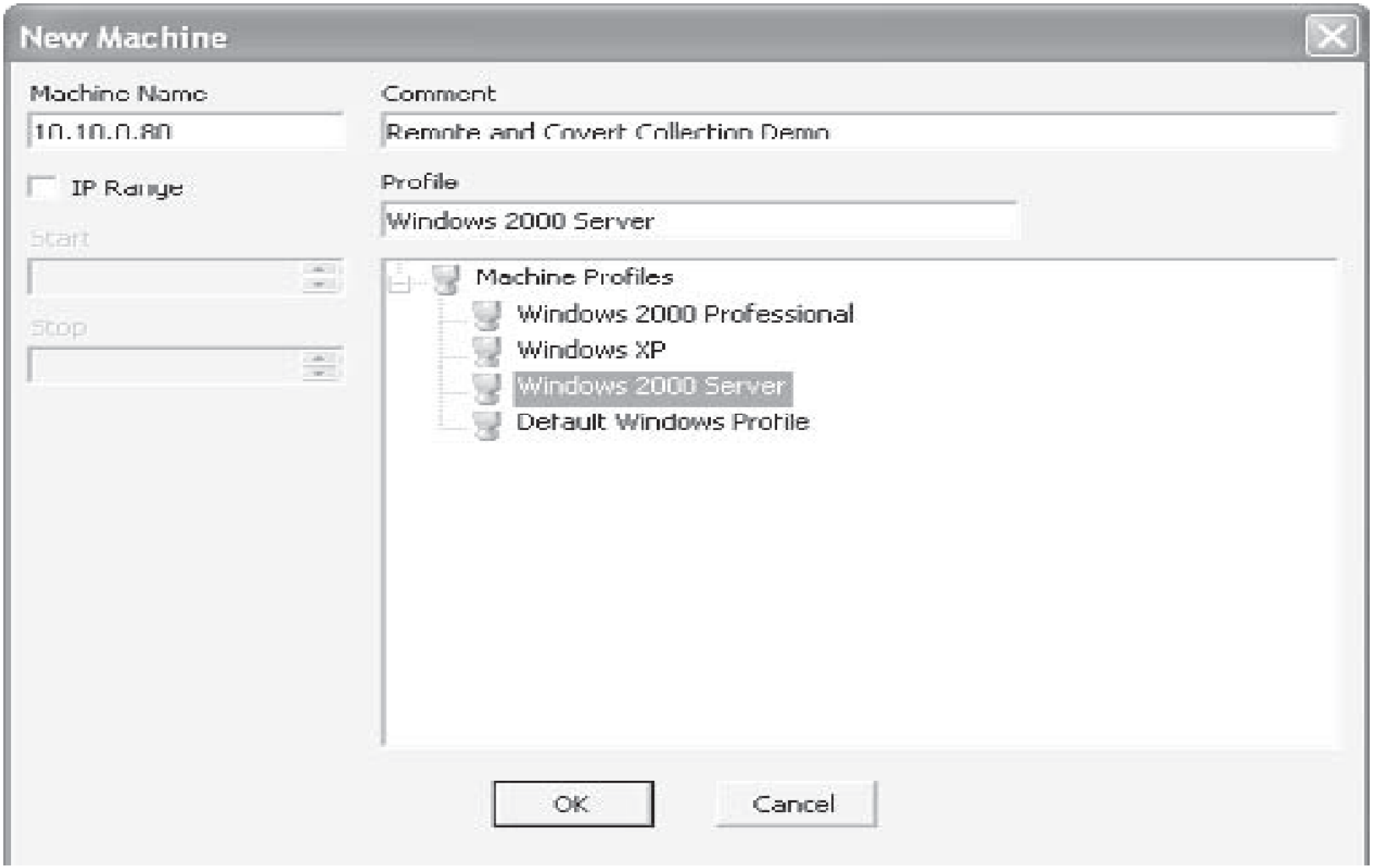
1. EnCase Enterprise Edition
2. Paraben Enterprise (P2EE)
3. ProDiscover

Remote Analysis with EnCase

1. Log on to EnCase Enterprise Edition from the examiner machine

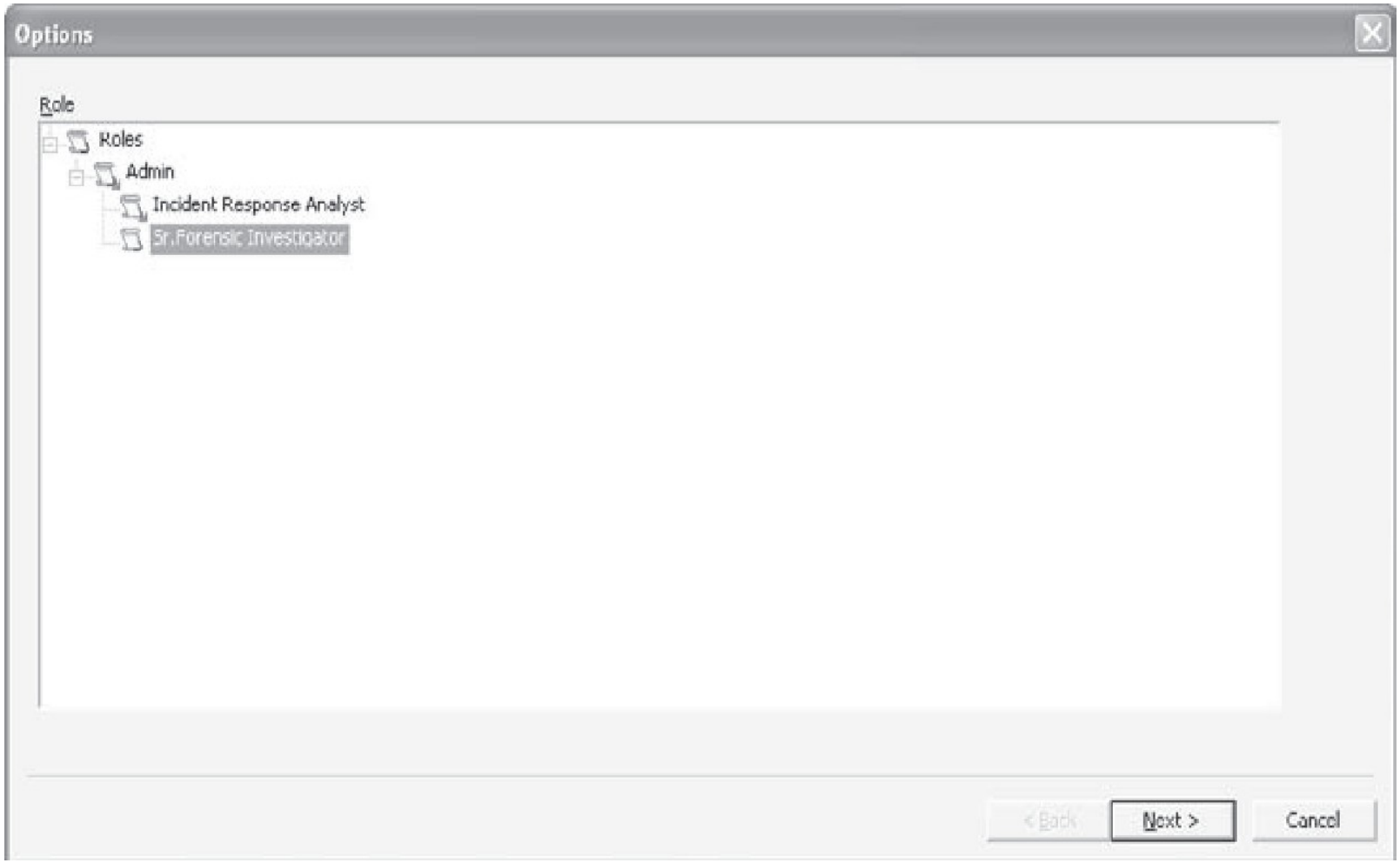


2. Select Network from the View drop-down list
3. Create a new node using an IP address or hostname within the network view -- > OK

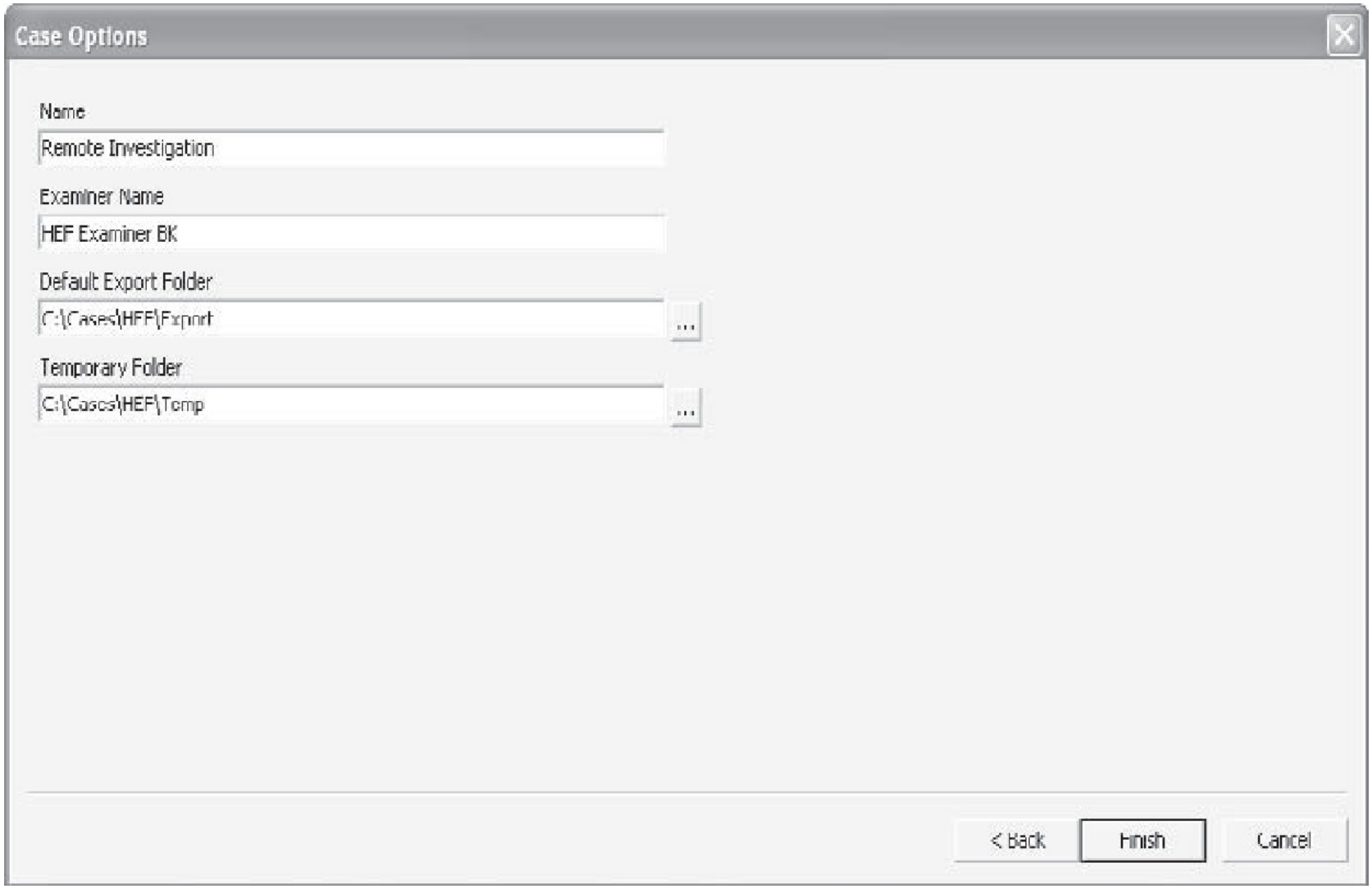


4. Click the New button -- > create a new case from which you can work

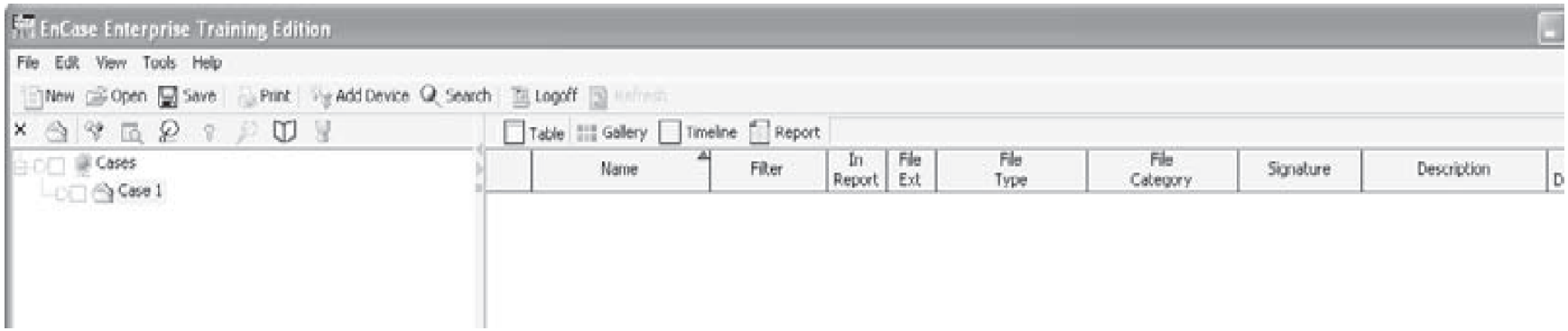
5. A new window appears -- > select the appropriate security role



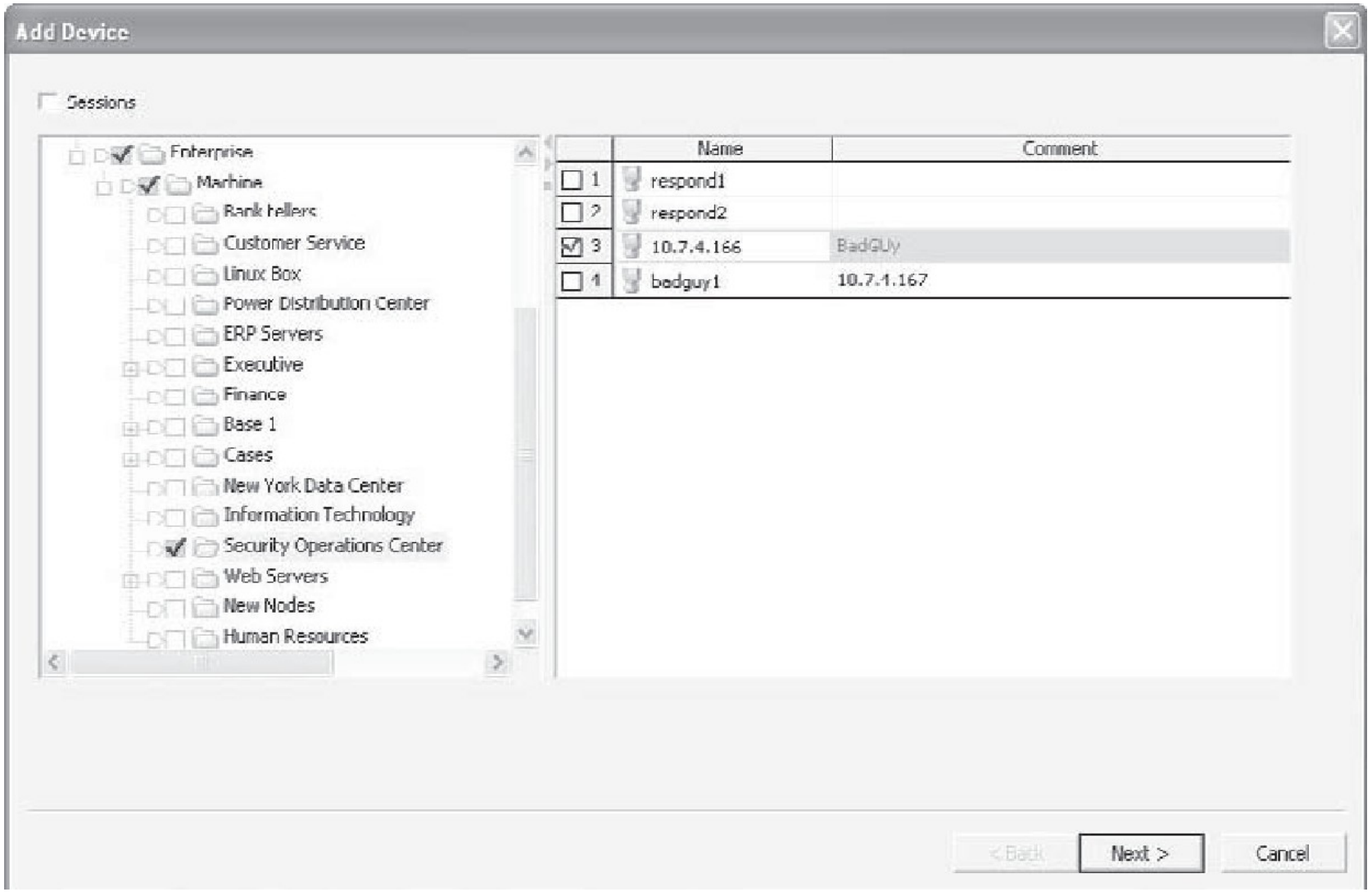
6. In the Case Options dialog -- > add the appropriate information for the new case -- > click Finish

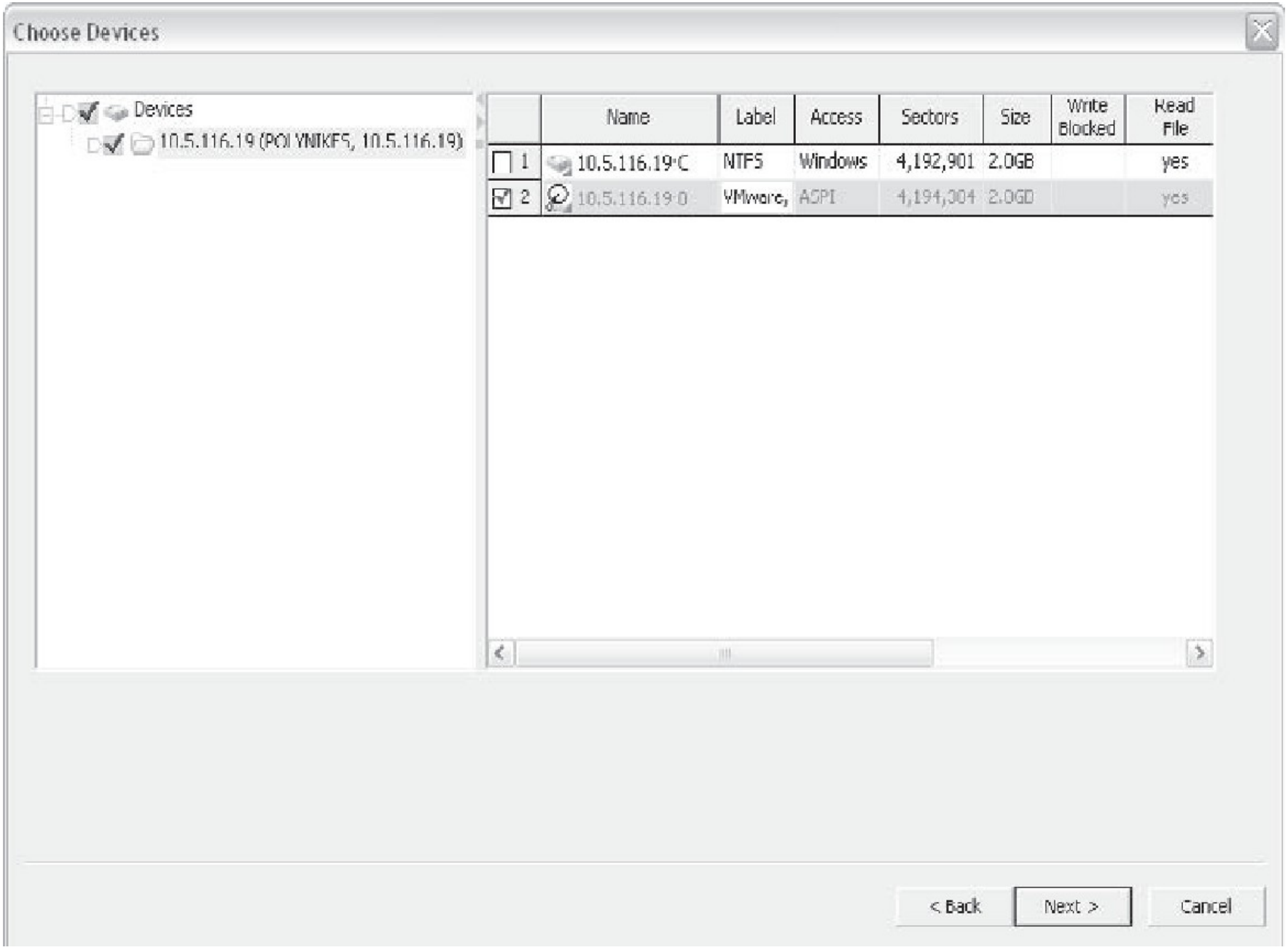


7. At the top of the EnCase Enterprise window, click the Add Device button

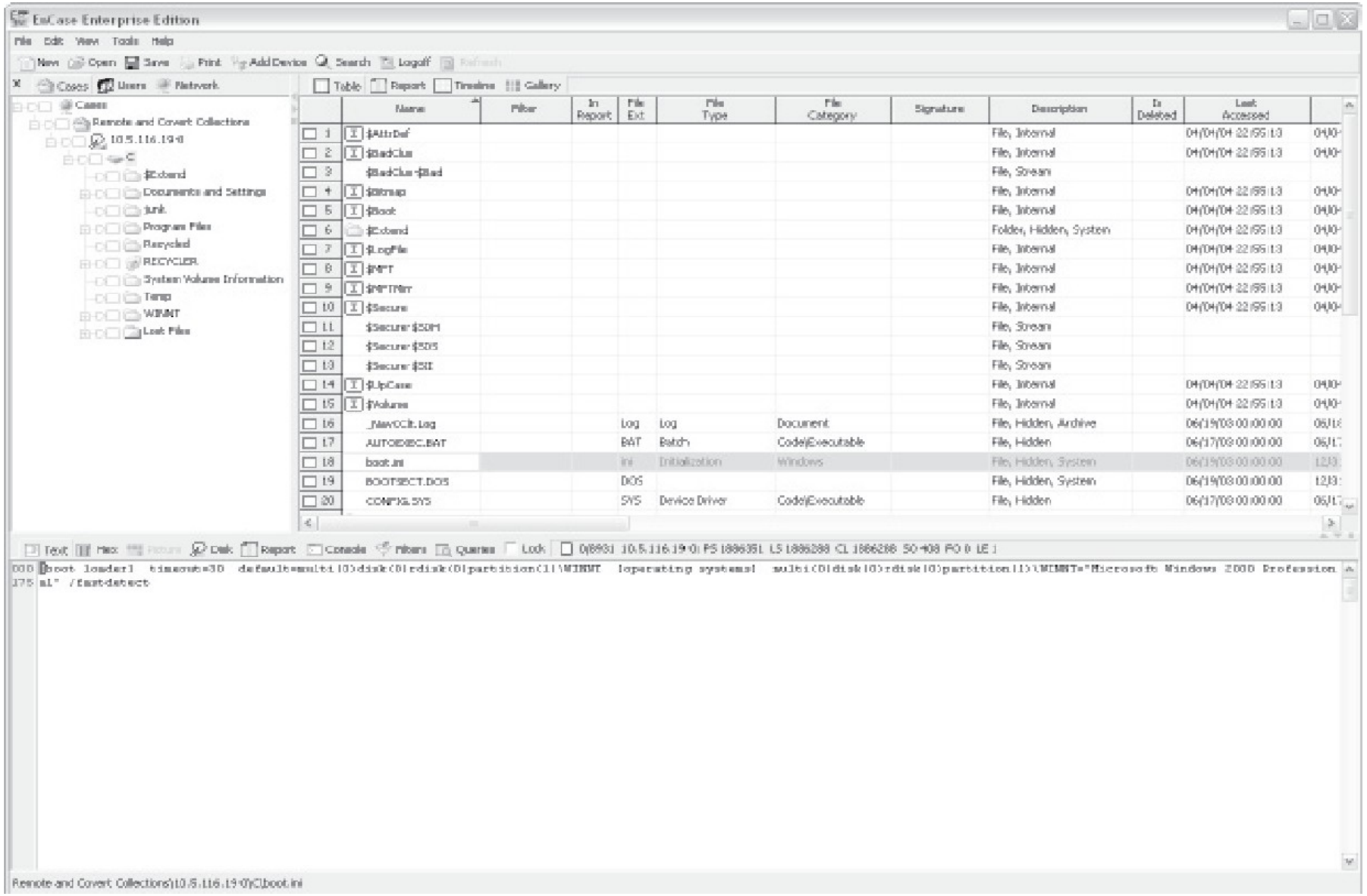


8. In the Add Device window, select the appropriate node under Enterprise and then click Next.



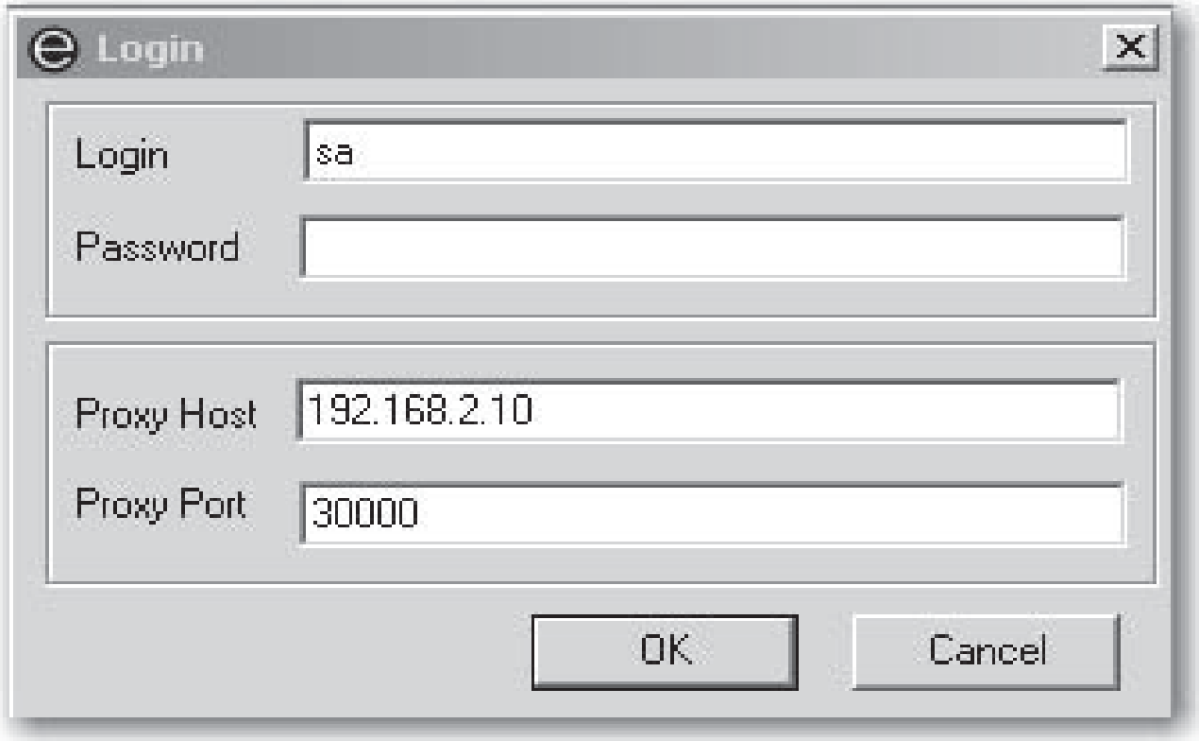

Choose Devices
Devices
10.5.116.19 (POI YNIKFS, 10.5.116.19)
Name
Label
Access
Sectors
Size
Write Blocked
Read File
1
10.5.116.19:C
NTFS
Windows
4,192,901
2.0GB
yes
2
10.5.116.19:0
VMware,
ASPI
4,194,304
2.0GB
yes
< Back
Next >
Cancel

Remote system hard drive preview

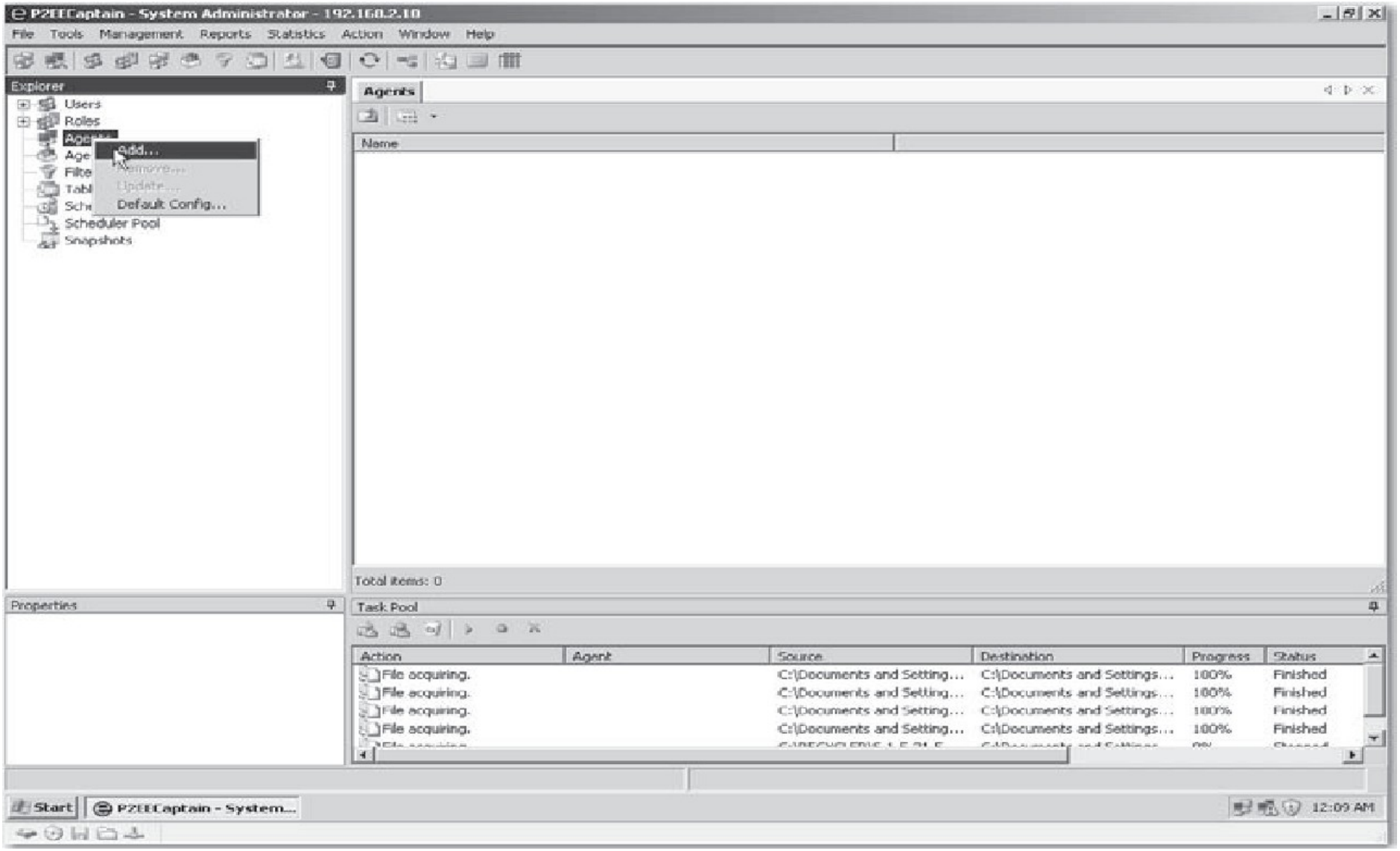


Remote Analysis with Paraben Enterprise

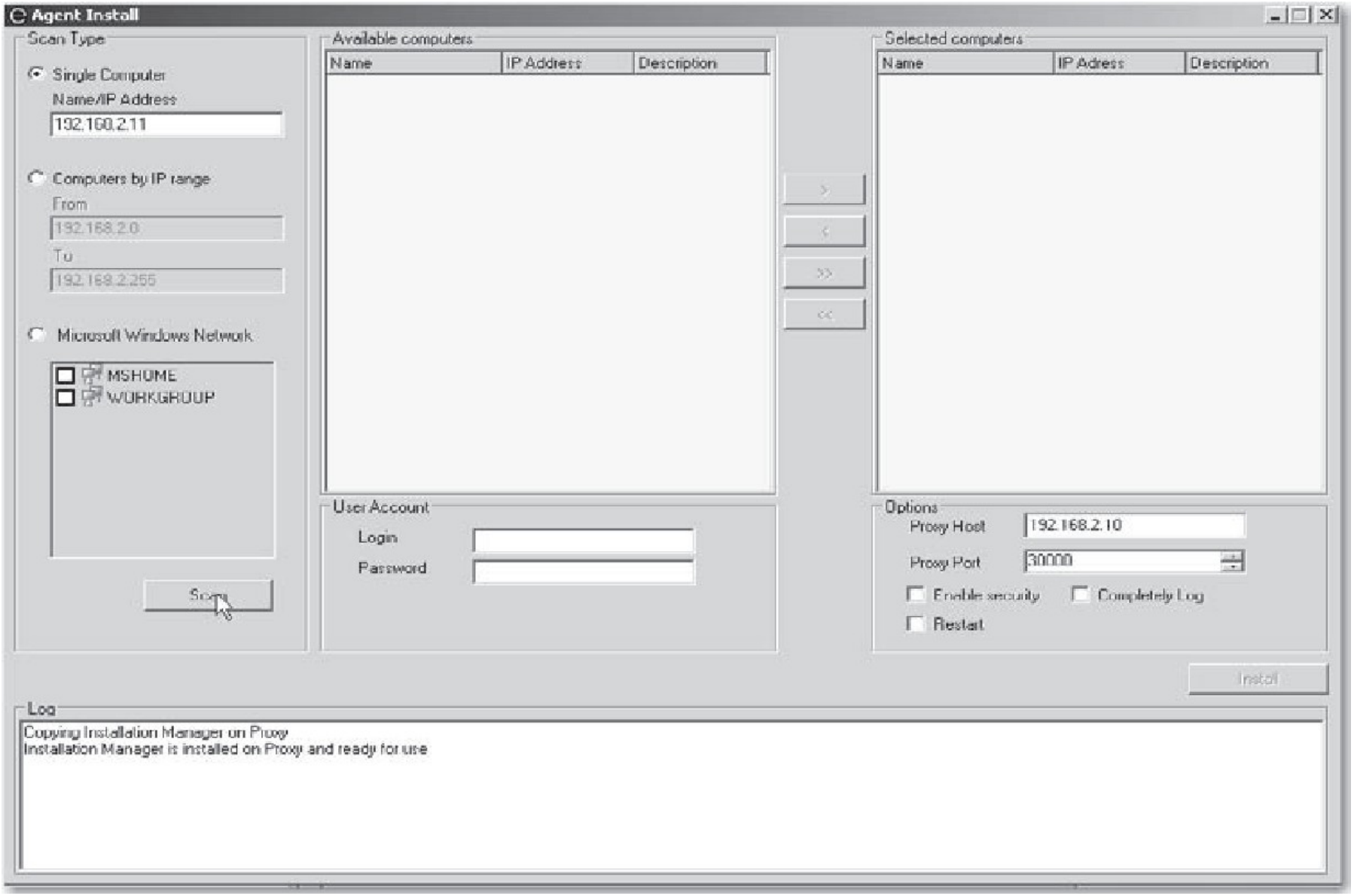
1. Launch the P2EE Captain module
2. Login dialog -- > login Captain module-- > specify the IP address for the P2EE proxy server (i.e. visible to computer you are going to inspect) -- > click OK



3. Explorer pane (main screen) -- > right-click Agent -- > Add Agent

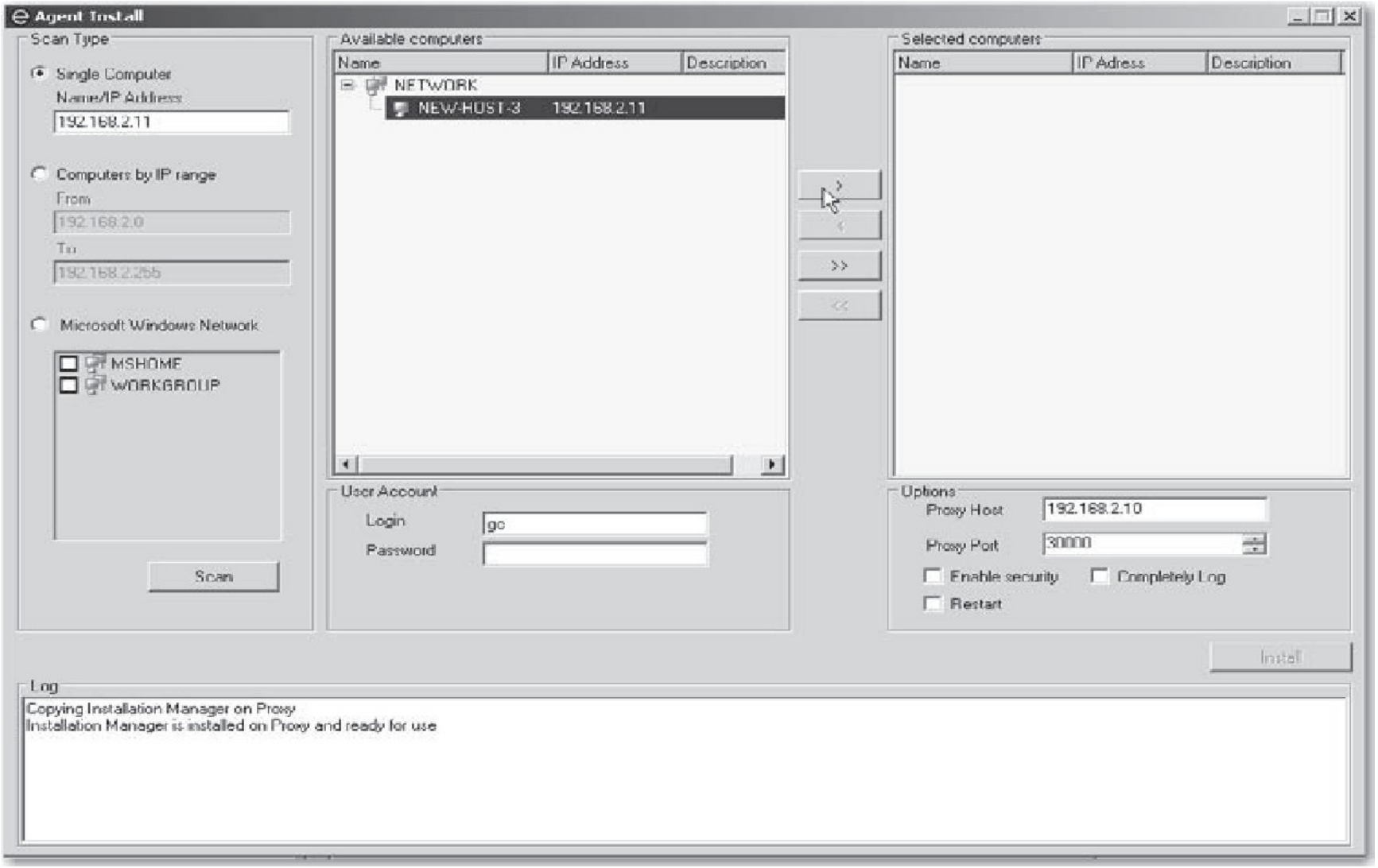


4. Agent Install window --- > type the IP address of the system to which you want to connect -- > Scan



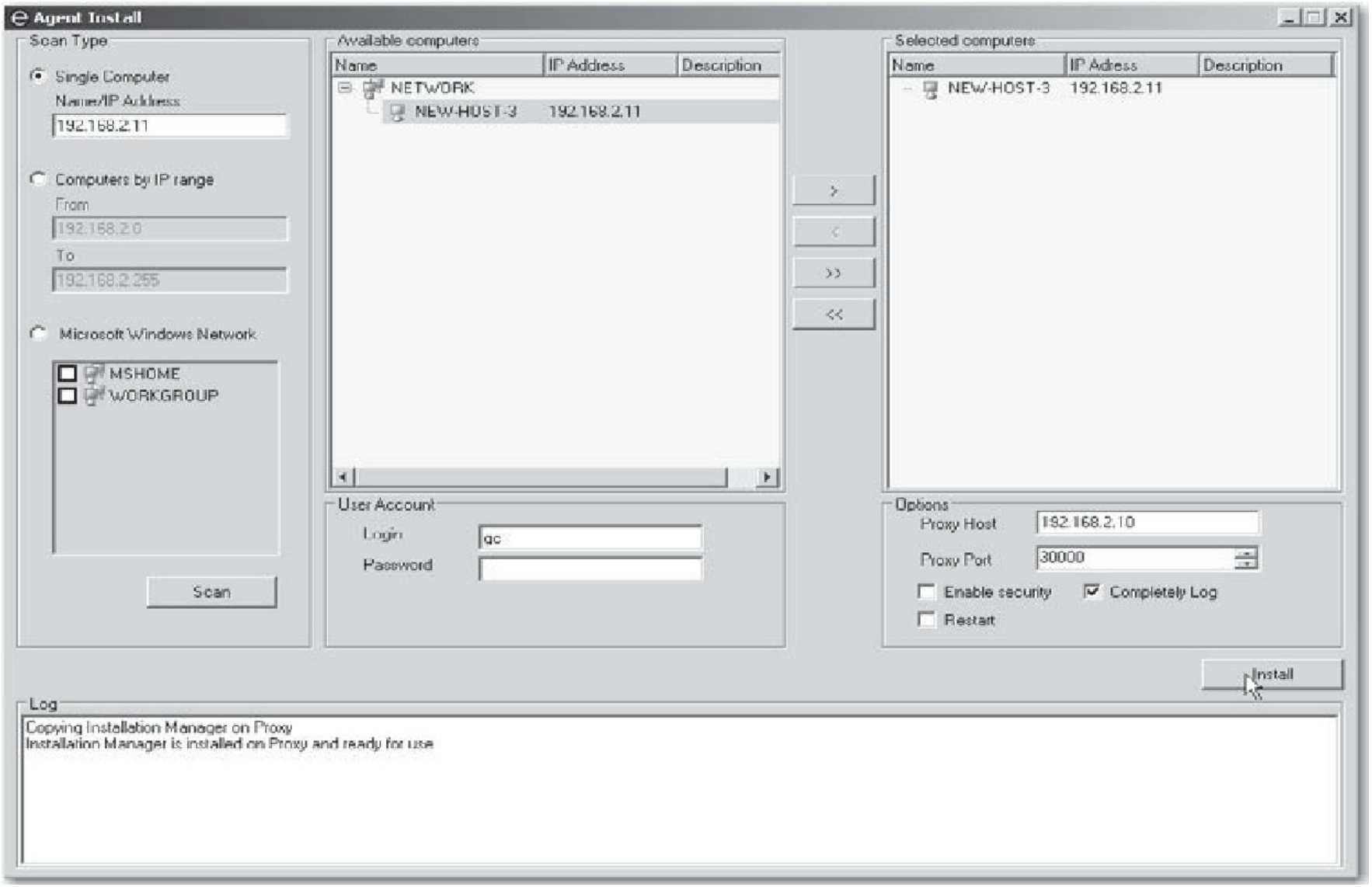
5. Enter network administrator / local administrator login information

6. Click the right arrow button --> Available Computers list to the Selected Computers list for agent deployment



7. Options ---> Enable Security (security features) (Process logged) and Restart

8. Click Install to deploy the agent



Covert Investigation

- Ability to conduct a from a safe location is critical
- Depends on the sensitivity of the case and the people involved
- Remote Investigation i.e. no longer need to acquire the machine
- Danger CI Scenarios and issues:
  - who is involved in the investigation and notifies co-conspirators, damaging the investigation
  - He/she is being investigated and destroys the evidence
  - He/she is being investigated and when coworkers find out, employee morale is damaged
  - investigation is taking place and modifies any inappropriate behavior, i.e. ceasing to perform fraudulent transactions

Covert Investigations

Techniques and actions ensures the success of a covert investigation:

- Minimize the number of simultaneous operations to minimize system resource usage
- Don't perform a keyword search, file signature analysis and hash analysis all at the same time
- Give the remote investigative agent an operating system–friendly name such as svchost.exe and run it from the system directory or choose Secure Mode
- If organization uses personal firewalls–
  - make sure a standard policy is in place to allow inbound connections from the examiner's machine
  - Otherwise, the subject could be alerted by the firewall that somebody is trying to connect to his or her system

- Ensure that the remote investigative agent does not leave any events in the event logs
- Minimize the number of people who know about the investigation
- For sensitive cases, conduct the investigation during the evening
- Time the investigation for periods when the subject expects a lot of hard drive activity
- Search only the data that is relevant to the case
- Determine whether the target machine is a laptop or desktop machine
- Be patient and don’t rush the investigation; if necessary, break it up into several phases

Successful Covert Collection

- Covert or secret, collections occur without the knowledge of the target or others
- Techniques to ensure the success of a covert collection:
  - Perform remote collections in the evening when users are not working at their machines
  - Make sure company policy and culture, ask users to leave their machines turned on at all times as part of standard maintenance procedures
  - Collect at times when the suspect expects a lot of hard drive activity, such as during regular antivirus scans or recent security vulnerability announcements
  - Acquire only the media you need to support the investigation

Successful Covert Collection

- Avoid acquiring laptops, if possible; their hard drives are slower and increased disk activity is apparent
- Time your collection so it takes place when the suspect is going to be away from his or her desk for an extended period of time
- Schedule an offsite meeting during the day and require that laptops remain in the office
- Whenever possible, acquire the machine using a high- speed network connection

Search and Seizure

- You probably won't have unobstructed access to all evidence

- Before you collect any evidence, make sure you have the right to either search or seize the evidence in question

- options and restrictions that relate to searching and seizing evidence

1. Voluntary Surrender

- The easiest method of acquiring the legal right to search or seize computer equipment
- This type of consent occurs most often incases where the primary owner is different from the suspect
- You might want written consent to search, prior to the beginning of your evidence collection activities

1. Voluntary Surrender

- The evidence you want might reside on a business-critical system
- If your activities will alter the business functions of an organization, you may need to change your plans
- Ex-disk imaging of all computers
- You would also have voluntary consent in cases in which an employee signed a search and seizure consent agreement
- Never assume you have consent to search or seize computer equipment

2. Subpoena

- Court order is a first option to use a subpoena
- Compels the individual or organization that owns computer equipment to surrender it
- It provides the owner ample time to take malicious action and remove sensitive information
- It is used when a nonsuspect equipment owner is unwilling to surrender evidence
- A court order is required by policy or regulation to document that sufficient authority exists to release such information

3. Search Warrant

- It allows law enforcement officers to acquire evidence from a suspect's machine without giving a suspect any opportunity to taint the evidence
- A court grant law enforcement officers permission is must to search and/or seize the identified computer equipment without giving the owner any prior notice
- Resort to a search warrant only when a subpoena puts evidence at risk
- For an independent investigator, you cannot execute a search warrant
- Courts are reluctant to grant such a ruling without compelling reasons to do so
- Before it, gather some preliminary evidence

Digital Forensics and Investigation [CET4033B]

TYBTech CSF, Semester-V
AY 2023-24

Dr Sumedha Sirsikar

Data Acquisition
and
Disk Imaging

Imaging Process

- The tools that helps the forensic investigator glean hidden information is imaging
- *Imaging* is the process of creating a complete sector-by-sector copy of a disk drive
- Data imaging is a part of data collection process
- Deleting is unlink the sectors from the file system table and leave the data untouched until they need those sectors again for some other purpose
- Analyzing a disk image allows a computer forensic investigator to dive deeper into a system's state and conduct a more complete investigation

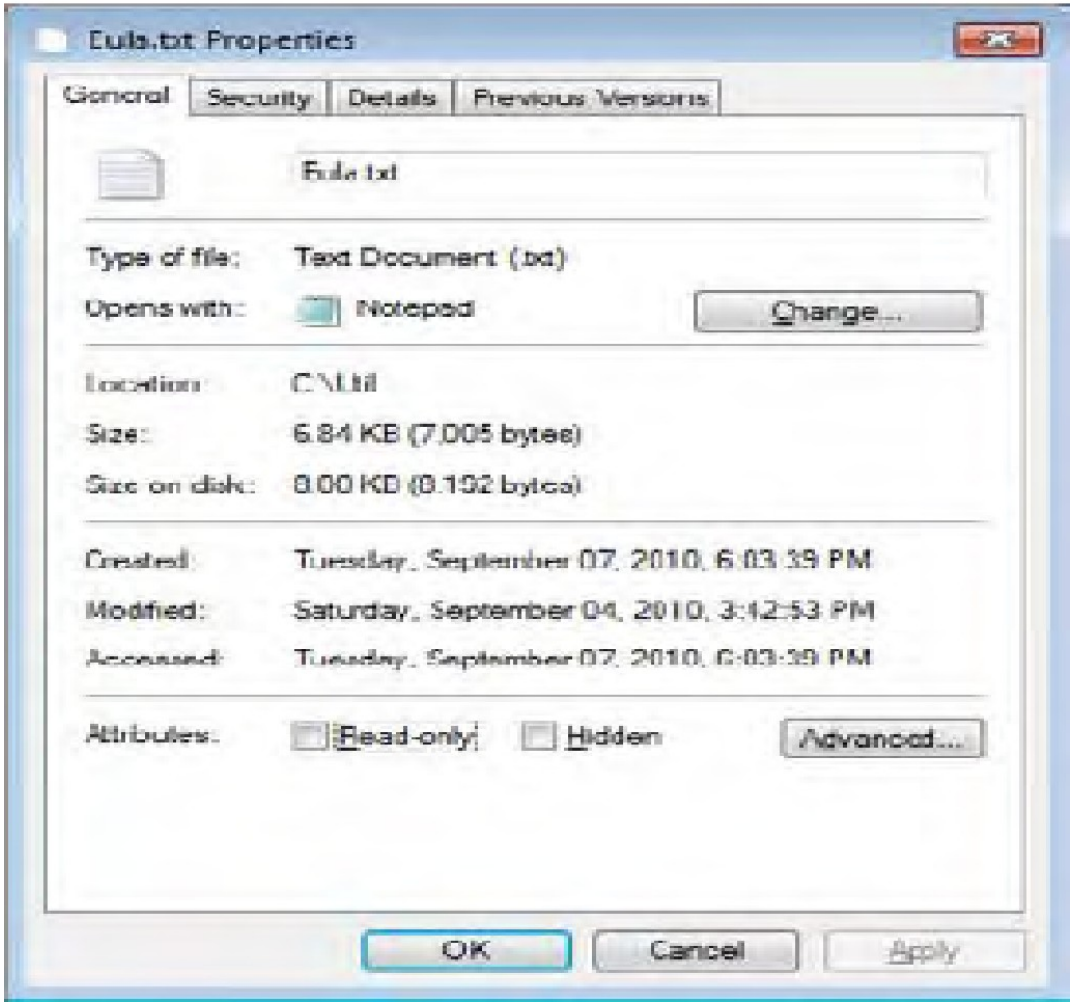
Evidence Collection Order

Order of volatility on a normal system from more to less volatile as follows:

1. Registers, cache
2. Routing table, ARP cache, process table, kernel statistics
3. Memory
4. Temporary file systems
5. Disk
6. Remote logging and monitoring data that is relevant to the system in question
7. Physical configuration, network topology
8. Archival media

Evidence Collection Methods

The “accessed” date is the last date the file was opened for reading or writing



Preparing Media and Tools

Solid-state disks: a viable alternative to electromechanical disks

- fewer failures during repetitive and long read/write streams
- Time is not wasted in restarting a task owing to mechanical failure
- solid-state disks provides faster access time to the data, which can reduce your analysis time

Preparing Media and Tools

Sanitize all media that is to be used in the examination process:

- media must not contain any viruses or other contaminants
- all data from drive must be removed and overwritten
- To sanitize media, overwrite first with a certain byte value, such as 00000000 (0x00), and then with 11111111 (0xFF), and finally with a randomly chosen byte value

Software sanitizing programs:

- open source program Darik's Boot and Nuke, or DBAN, Ontrack DataEraser and WinHex
- entire disk is overwritten several times, to destroy all traces of preexisting information
- Image MASSter Solo-4—can make multiple copies and sanitizes at full SATA-2

Image MASSter Solo-4 disk sanitizing

Image MASSter Forensic Toolkit

Tools for seizing data from computers that cannot be opened in the field

Guidelines for Evidence Collection

- RFC 3227 lists the volatile data as the first kind of data to capture
- Before unplugging the computer, get a snapshot of the system when arrived on the scene
- Collect the following information: (may choose to conduct a live acquisition)
  1. System date and time
  2. Current network connections
  3. Current open ports and applications listening on those ports
  4. Applications currently running

practical ways to acquire live information

Without impacting the data on the system:

1. Saving the information to a remote forensic system
2. Saving the information to a removable drive

Netcat: free tool

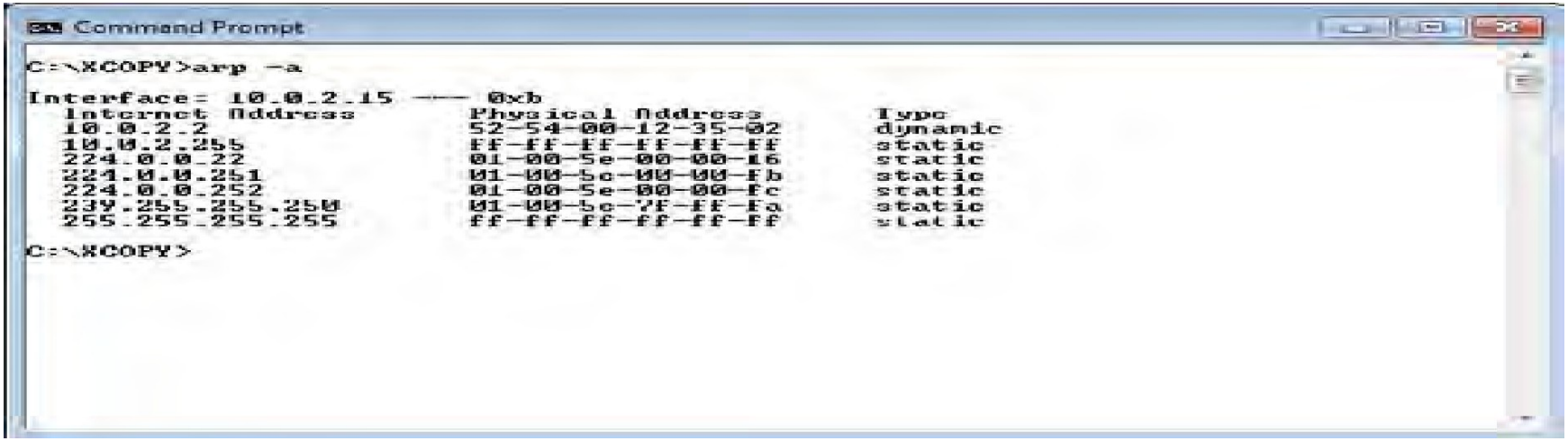
- to create a reliable TCP connection between the target system and the forensic workstation

Cryptcat-encrypted Tool:

- the risk of data contamination or compromise is nearly eliminated

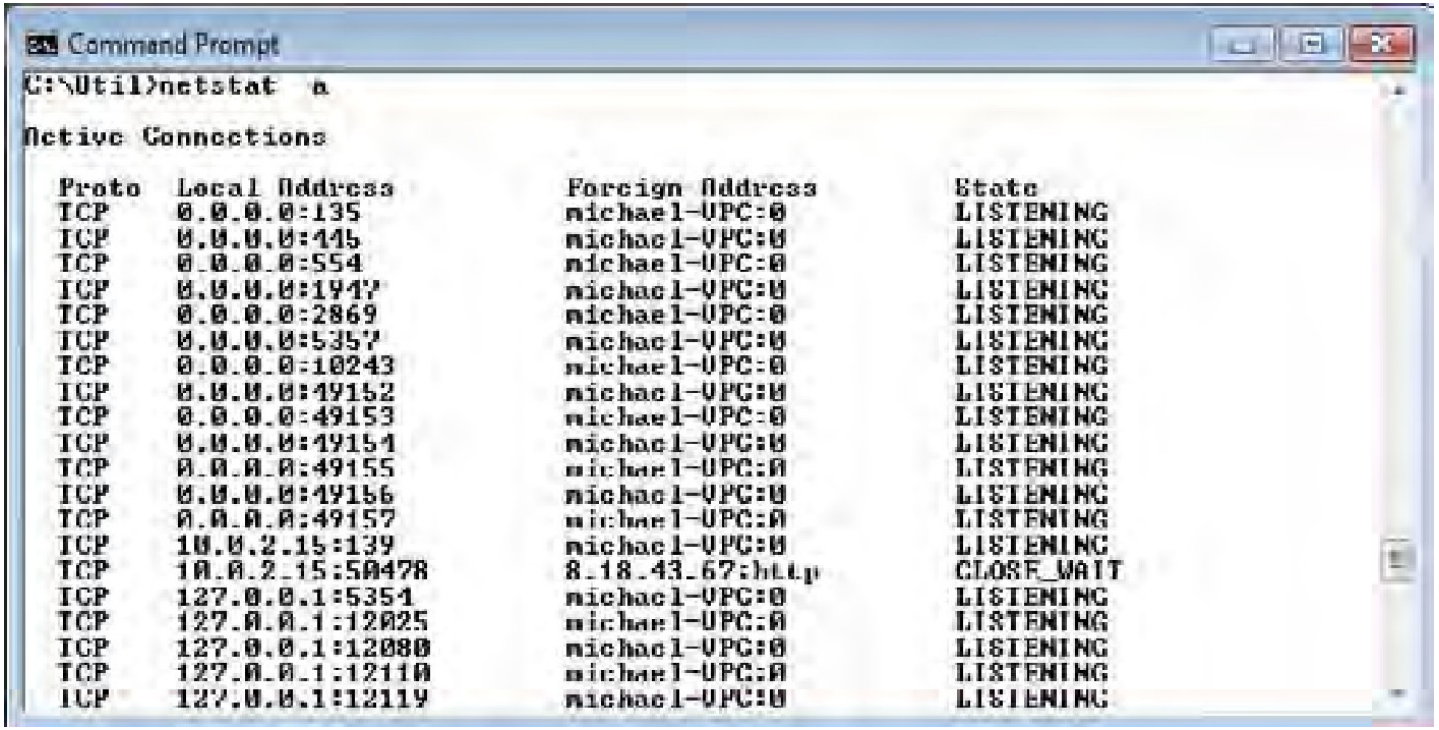
Tools for Volatile Data Collection

- ARP: *Address Resolution Protocol* cache
  - a table that maintains a mapping of each physical address and its corresponding network address
  - Connected computers network and hardware addresses
  - ARP cache is held for max 10 minutes, & then entries are deleted
  - Traceroute/tracert: track the path a packet takes to get to its destination



Netstat utility

- Displays all active computer connections
- Provides the investigator with a list of what protocols are running and what ports are open



Shutdown after data acquisition

- **Normal shutdown process**
  - file systems as well as individual files are more likely to be intact
  - each file written to the system during the shutdown process can result in fewer recoverable deleted files
  - Clears space on the disk used for virtual memory, possibly taking valuable evidence along with it

Shutdown after data acquisition

- **Disconnecting the power cord:**
  - Risk of losing data, depending on the system the suspect computer is using
  - E.x. there is an increased risk of losing data if the suspect system is running UNIX
  - Computer with an electromechanical disk causes any volatile data:
    - that haven't already collected to be lost i.e. open files or data that hasn't been flushed from the cache to the disk

Creating a Duplicate Hard Disk

- An original method:
  - booting from a floppy boot disk and then creating a bit stream backup of the hard disk
- A bit stream image/forensic imag:
  - complete and accurate copy
  - a bit-for-bit clone of the original disk
  - a recording of every single bit of data that resides on a storage device
  - backup copies hidden, erased, fragmented, corrupted, temporary, and special attribute files which may not be easily found otherwise
  - For example, temporary files might contain data from a document that was worked on but never saved to disk

Creating a Duplicate Hard Disk

Drive imaging can be performed in several ways:

- Disk–to–disk image: is mainly used to test booting
- Disk–to–image file: results in faster searches and is compressible
- Image file–to–disk: used to restore an image

- *Disk imaging is not the same as using backup software:*
  - *imaging software makes a full, exact copy of the hard drive, including the operating system, software, file organization, as well as the data*
- *Backup software programs generally copy data only*

Forensic Duplicate

A process used to copy an entire hard drive that includes all bits of information from the source drive stored in a raw bit stream format

Steps:

- in the forensic examination of a computer hard drive is to create the bit stream copy
- captures not only the existing files but also the slack and unallocated space so deleted files and file fragments can be recovered
- hardware duplicator i.e. Image MASSter Solo-4 Forensic unit or the Forensic MD5 unit

Selection of method based on use and evaluation of Information

- Text documents, spreadsheets, databases, financial data, electronic mail, digital photographs, sound, and other multimedia files
- Previously deleted data, deleted folders, slack space data, and intentionally placed data
- Extra tracks or sectors on a floppy disk, or an HPA on a hard drive
- User settings and functionality of the hardware or software
- Boot files, registry files, swap files, temporary files, cache files, history files, and log files http

Imaging/Capture Tools

- NIST Web site at http://www.cftt.nist.gov/
- Department of Justice's Office of Justice Programs Web site at http://www.ojp.usdoj.gov
- Read-only media and all Operating Systems
- Forensic tools should include the following Programs:
  - for examining processes and services running
  - for examining the system state
  - Scripts to automate evidence collection
  - for doing bit-to-bit copies
  - for generating checksums to verify the image

Imaging/Capture Utilities

dd utility (1970): the original UNIX utilities used in Linux and Windows

- in every forensic investigator's tool box
- It can make exact copies of disks suitable for forensic analysis
- It can be used as a means to build an evidence file
- It is a command-line tool to copy and convert magnetic tape formats, convert between *ASCII* and *EBCDIC*, swap bytes, and force to uppercase and lowercase
- The dd copy command supports special flags that make it suitable for copying devices such as tapes

Imaging/Capture Utilities

WinHex:

- It is a universal hexadecimal editor for Windows 95/98/Me/NT/2000/XP
- data recovery, low-level data processing and IT security
- It has minimal system requirements, operates very fast, and consumes little memory
- It is an advanced tool for inspecting and editing various types of files, and recovering deleted files or lost data from hard drives or from digital camera cards
- The disk and memory imaging features include:
  - Disk editor for both logical and physical disks, including hard disks, floppy disks, CD-ROM, DVD, Zip disks & Compact Flash
  - Supports FAT16, FAT32, NTFS, and CDFS file systems
  - RAM editor used to edit other processes'
  - virtual memory
  - Disk cloning
  - Drive images that can be compressed or split into 650 MB archives

- *Forensic compression* reduces image file size by compressing redundant sectors
- *Spanning across multiple discs* is used when target media is smaller than the image file
  - E.g., imaging or cloning a 500 GB drive and the drives used only hold 160 GB
  - Spanning automatically breaks up the image into several smaller files

Cyclic Redundancy Check (CRC)

Verification of original media and copied data:

- CrCheck.exe and CRC32: for smaller storage devices
- fingerprint checker, Message Digest 5 (MD5): for Larger storage devices require the use of a mathematical algorithm
- SHA-1and SHA-2 in place of MD5
- No corruption of the data

- Message Digest 5 (MD5):
  - MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, which is then used to verify that the message hasn’t been altered

Imaging/Capture Utilities

Grave-Robber:

- part of The Coroner's Toolkit (TCT)
- a set of tools used for collecting and analyzing forensic data on a UNIX system
- a program that controls a number of other tools, all of which work to capture as much information as possible about a potentially compromised system and its files
- collects evidence in an automated way. It gathers data in the following order:
  1. Memory
  2. Unallocated file system
  3. Netstat, ARP, route
  4. Process data
  5. Statistics and MD5 on all files and strings on directories
  6. Configurations and logs

Access Data's FTK Imager

- A snapshot of the entire disk drive and then copies every bit for analysis.
- Allows to analyze the images made using the ftk imager
- It assist the forensic examiner in conducting a complete and thorough computer forensic examination of computer disk drives
- Supported file systems include FAT 12/16/32, NTFS, NTFS compressed, and linux ext2 and ext3

EnCase

- **It** is a commercial software package that enables an investigator to image and examine data from hard disks, removable media, and some PDAs
- It enables examiners to acquire and analyze volatile data and image drives
- verify the copy is exact using MD5 and CRC, and mount evidence files of hard drives and CD-ROMs as local drives
- It includes the ability to boot the mounted drive in Vmware
- Used by many law enforcement groups throughout the world

Email Terminology

IMAP (Internet Message Access Protocol) It is a method to access bulletin boar message or emails residing on a mail server, making them visible and acting as if they were stored locally

SMTP (Simple Mail Transfer Protocol) It receives outgoing mail from clients and validates source and destination address, also sends and receives emails to and from other SMTP servers

HTTP (Hypertext Transfer Protocol)
It is used in webmail, and the message resides on the webmail server

POP3 (Post Office Protocol 3) Standard protocol for receiving email that deletes mail on the server as soon as the user downloads it. Standard port for POP3 is 110

CC (Carbon Copy)
Field in the email header that directs a copy of the message to another recipient mail ID

BCC (Blind Carbon Copy)
A field that allows you to send a copy of the message to a second recipient without notifying the primary recipient

Attachment
File that is sent along with an email message that can be of any type

Email Client
Program used to read and send emails. Typical email clients include Outlook Express or Eudora

Email Server
A server running at an Internet Service Provider or a large website that is connected to the internet to transport emails. One email server that is typically used is sendmail (Mail Transport Agent)

Encoding
Method of sending bindary (non-text) files with emails. Common encoding options include Uuencode, BinHex, Mime, etc.

Email System

Email system consists of mail clients to send or fetch emails and two different SMTP and POP3 or IMAP servers running on a server machine

Email system are based on a client-server architecture

Email is sent from clients to a central server, which reroutes the email to its intended destination

Email Clients

- Email client is a computer application that allows you to send, receive and organize emails
- Email clients perform the following functions:
- Retrieve messages from a mailbox
- Display the headers of all the messages in mailbox
- Allow you to select a message header and read the body of the email message
- Allow the user to create new messages and submit them to an email server
- Allow the user to add attachments to the messages they want to send and save the attachments from received messages
- Format the messages
- Most Commonly Used Email Clients
- Microsoft Outlook and Thunderbird (Stand alone)
- Yahoo! Mail, Gmail, Hotmail, etc. (Web based)

Email Server

- Email or mail server is a computer within the network that works as a virtual post office

- Email servers exchange email with the SMTP server

- When an email is sent the client application first directs it to the email server
- This contacts the addressee's email server and carries out a conversation in accordance with the rules defined by SMTP over the internet

- The email server checks for the validity of the username with the other email server
- If validated, it transfers the email and the receiving email server stores it until the addressee logs on and downloads it

SMTP Server

SMTP server connects with the recipient's SMTP server using port 25

SMTP server has a conversation with a Domain Name Server gets the identifying information for the Domain of the remote email server and connects to the SMTP of the remote email server

The SMTP server takes the "to" address and breaks it into two parts:
(1) The recipient's name
(2) The domain's name

Simple Mail Transfer Protocol (SMTP) Server listens on port number 25 and handles outgoing email

When the client sends an email, it connects to the SMTP server

The client has a conversation with the SMTP server, telling the SMTP server the address of the sender, the recipient, and the body of the message

POP and IMAP Server

POST OFFICE PROTOCOL (POP3) SERVER

- This email server is used only for incoming emails
- When a message arrives, the POP3 server appends it to the bottom of the recipient's account file, which can be retrieved by the email client at any preferred time
- Email client connects to the POP3 server at port 110 by default to fetch emails

INTERNET MESSAGE ACCESS PROTOCOL (IMAP) SERVER

- Email client connects to the IMAP server using default port 143
- IMAP servers allow multiple concurrent client connections to the same mailbox
- It enables accessing and fetching MIME message parts, maintaining

message state information at server, creating and manipulating multiple mailboxes on the server and Server-side searches

POP3 can be said to be a store forward service whereas IMAP is a remote file server; both are used to read email

Email Message

An email message is composed of three parts

1. **Header**
   - Email header contains information about the email origin such as the address from where it came, the routing, time of the message and the subject line
   - Some of the header information that is usually important to a technician is kept hidden by the email software
2. **Body**
   - Body contains the actual message
3. **Signature**
   - Used by sender to provide information to the recipient about the sender. Email programs can be set to enter this line automatically on all the emails sent

Subject: when can we meet?
Date: Mon, 6 Aug 2011 10:04:22 -0500 --------**Header**
From: _____
alvernia@alverno.edu To:
anthos@alverno.edu

When can we get together to work on our project?
I am available any time this week after 5.00 PM. But I do have some other appointments next week. I would like to meet before we have our next class so email me and let me know what would work for you.
Thanks! --------**Body**

--------**Signature**

Jane A. Alverno
Student, Alverno College

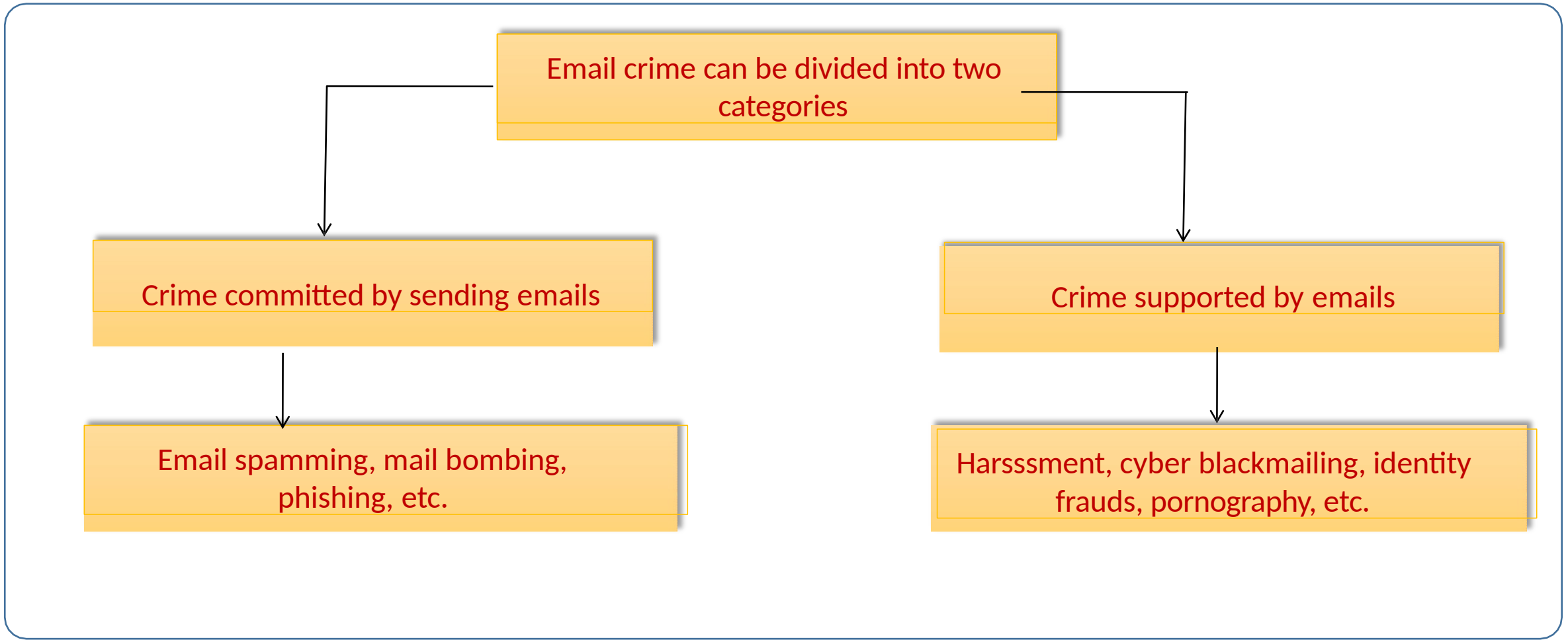
Importance of Electronic Record Management

Electronic records management may be defined as The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of electronic records, including the processes for capturing and maintaining evidence of and information for legal, fiscal, administrative and other business purposes

	IMPORTANCE OF ELECTRONIC RECORDS MANAGEMENT
1	It helps in non-repudiation of electronic communication so that someone cannot deny being the source of communication
2	It acts as a deterrent for abusive and indecent materials in email messages
3	It helps in the investigation and prosecution of email crimes

Email Crime

- Ease, speed and relative anonymity of email makes it a potent tool for criminals



Email

- Spamming can be defined as sending unsolicited emails
- Spammers obtain email addresses by gathering addresses from Usent postings, DNS listings, or web pages
- User with a valid email address can spam email address, bullet-in-board services, or newsgroups
- Common Subjects
- Header of spam emails

Mail Bombing / Mail Strom

Mail Bombing

- Sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted to cause a denial-of-service attack
- In many instances, the messages will be large and constructed from meaningless
  data in an effort to consume additional system and network resources

Mail Storm

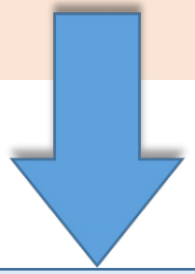
- It is a sudden spike of “Reply All” messages on an email distribution list, caused by one misdirected message

Phishing Cont'd

- It is a criminal act of sending an illegitimate email, falsely claiming to be from a legitimate site in an attempt to acquire the user's personal or account information
- Phishing emails redirect users to fake webpages of trustworthy sites that ask them to submit their personal information
- Phishing attacks can target millions of email addresses around the world using mass-mailing systems

Email spoofing

- Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source
- Spammers and perpetrators of phishing change the email header fields such as the From, Return-Path and Reply-To-Fields to hide the actual source



Example : Using the Anonymailer service, Mr. Smith, whose email address is smith@hotmail.com, can send viruses, Trojans, worms, etc. to Sam's friends using sam's email address samchoang@yahoo.com. Sam's friends would then download them believing them to be from a trustworthy source

List of Common Headers Cont'd

Apparently-To

- Messages with may recipients sometimes have a long list of headers in the form "Apparently-To:rth@bieberdorf.edu" (one line per recipient)
- These headers are unusual in legitimate emails; they are normally a sign of a mailing list, and in recent times mailing list have generally used software not sophisticated enough to generate a giant pile of headers

Bcc

- BCC stands for "Blind Carbon Copy". It is used to add addresses to the SMTP delivery list but not (usually) listed in the message data, remaining invisible to other recipients
- The idea is to be able to send copies of email to persons who might not want to receive replies or to appear in the headers
- Blind carbon copies are popular with spammers, since it confuses many inexperienced users to get email that does not appear to be addressed to them

List of Common Headers cont'd

Cc	• Cc stands for "Carbon Copy" • This header is sort of an extension of "To:"; it specifies additional recipients. The difference between "To:" and "Cc:" is essentially connotative; some email programs also deal with them differently in generating replies
Comments	• This is a nonstandard header field. Example: "Comments: Authenticated sender is rth@bieberdorf.edu" • It is added by some mailers to identify the sender; however, it is often added by hand by spammers as well

1	**Content-Transfer-Encoding :** This header relates to MIME, a standard way of enclosing non-text content in email; it has no direct relevance to the delivery of email, but it affects how compliant email programs interpret the content of the message
2	**Content-Type :** Another MIME header, telling MIME-compliant email programs what type of content to expect in the message
3	**Date :** This header does exactly what you expect; it specifies a date, normally the date the message was composed and sent. If this header is omitted by the sender's computer, it might conceivably be added by an email server by some other machines along the route
4	**Errors-To :** Specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address). This is not a particularly common header, as the sender usually wants to receive any errors at the sending address, which is what most (essentially all) email server software does by default

List of Common Headers Cont'd

Priority

- It is a free-form header that assigns a priority to the email, but most software ignore it
- It is often used by spammers, usually in the form "Priority urgent" (or something similar), in an attempt to get their messages read

Organization

- It is a completely free-form header that normally contains the name of the organization through which the sender of the message has net access
- The sender can generally control this header, and silly entries like "Royal Society for Putting Things on Top of Other Things" are common place

Sender

- This header is unusual in email

  (X-Sender: is usually used instead), but appears occasionally, especially in copies of Usenet posts
- It should identify the sender; in the case of Usenet posts as it is a more reliable identifier than the From: line

List of Common Headers Cont'd

Subject

- A completely free-form field specified by the sender, intended, of course, to describe the subject of the message

X-Confirm-Reading-To

- This header requests an automated confirmation notice when the message is received or read
- It is typically ignored; presumably some software acts on it

X-Mailer (also X-mailer)

- This is a free form header field intended for the email software used by the sender to identify itself (as advertising or whatever)
- Since much junk email is sent with mailers invented for the purpose, this field can provide much useful fodder or filters

X-Distribution

- In response to problems with spammers using his software, the author of Pegasus Mail added this header
- Any message sent with Pegasus to a sufficiently large number of recipients has a header that says "X-Distribution; bulk". It is explicity intended as something for recipients to filter against

X-PMFLAGS

- This is a header added by Pegasus Mail; its semantics are not obvious
- It appears in any message sent with Pegasus, so it does not obviously convey any information to the recipient that is not covered by the X-Mailer: header

List of Common Headers Cont'd

To
The email address (es), and optionally name(s) of the message recipient(s). It indicates primary recipients of the mail

Received
This is the message generated by the email server

X-Priority
Another priority field, used by Eudora to assign a priority (which appears as a graphical notation on the message)

X-Errors-To
Like Errors-To:, this header specifies an address for errors to be sent to. It is probably less widely obeyed

List of Common Headers Cont'd

X-Headers

- X-headers is the generic term for headers starting with a capital X and a hyphen
- The convention is that X-headers are nonstandard and provided for information only
- This convention is frequently violated

X-Sender

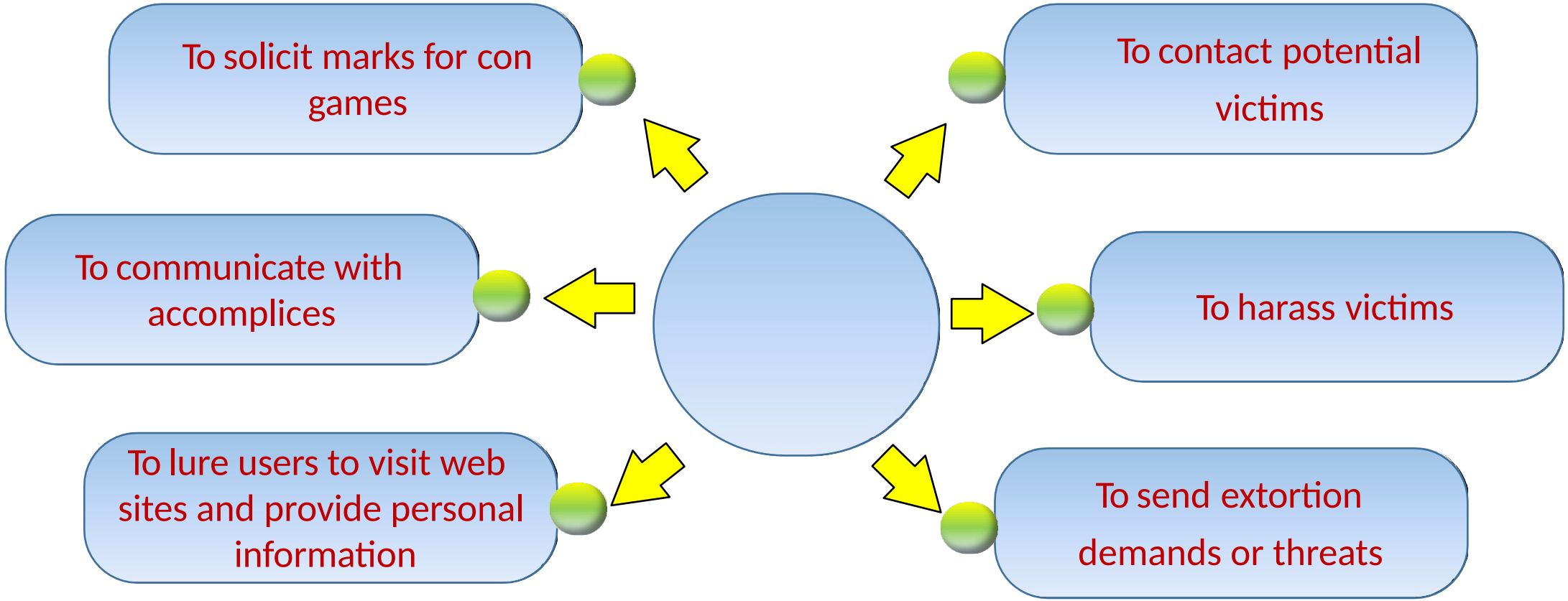
- It is the usual email analogue to the Sender: header in Usenet news
- This header purportedly identifies the sender with greater reliability than the From: header
- In fact, it is nearly as easy to forge, and should therefore be viewed with the same sort of suspicion as the From:header

X-UIDL

- This is a unique identifier used by the POP protocol for retrieving email from a server
- It is normally added between the recipient's email server and the recipient's actual email software
- If email arrives at the email server with an X-UIDL: header, it is probably junk (there is no conceivable use for such a header, but for some unknown reason many spammers add one)

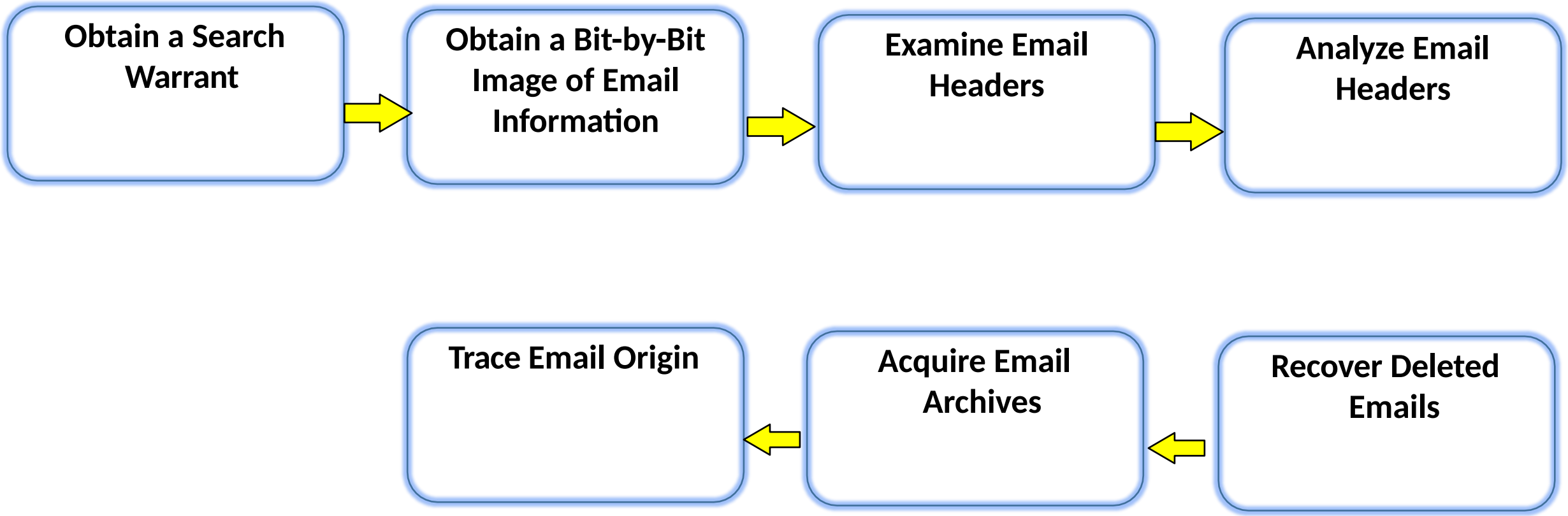
Why to Investigate Emails

Criminals usually use emails in the following ways:



Thus email stands as a clue to the criminal identity and may become the evidence

Investigate Email Crime and Violation



Obtain a Search Warrant and Seize the Computer with Email Clients

- A search warrant application should include proper language to perform an on-site examination of the computer and email server
- Conduct a forensics test on only that equipment for which you are permitted to do so
- Seize the computer and email accounts suspected to be involved in the crime
- Email accounts can be seized by changing the existing password of the email account either by asking the victim his/her password or from the email server

Obtain a Bit by Bit Image of Information

Make a bit-by-bit image of all the folders, settings and configurations present in the email account for further investigation in a removable disk using tools such as Safe Back

Encrypt the image using MD5 hashing to
maintain the integrity of the evidence

Examine Email Headers

- Know how to find emails headers in various command-line, Web based and GUI clients

- Open the email headers, copy and paste the headers to a text document

- Headers contain significant information such as Message sent time, unique identifying numbers and the IP address of the sending server

Viewing Email Headers in Microsoft Outlook

- Log on to Microsoft Outlook and open the

  received email

- Click on File → Info → properties

- Select message header text, copy and paste the

  text in any text editor and save the file

- Sign out of the Microsoft Outlook account

Viewing Email Headers in Gmail

- Log on to Gmail and open the received email
- Click on the Reply drop-down button and navigate to the show original option
- Select Message Headers – Full text and copy it
- Paste the text in any text editor and save the file
- Sign out of the Gmail account

Viewing Email Headers in Yahoo mail

- Log on to Yahoo mail and open the received email
- Click on the Actions drop-down button and navigate to the View Full Header option
- Select Message header text, copy and paste the text in any text editor and save the file
- Sign out of the Yahoo mail account

Forging Headers

This means that someone reading the lines from top to bottom, tracing the history of the message, can safely throw out anything after the first forged line; even if the Received: lines after that point look plausible, they are guaranteed to be forgeries

Another trick used by email forgers is to be add spurious Received: headers before sending the offending mail

This means that the hypothetical email sent from turmeric.com might have Received: lines that look something like this:

- Received from galangai.org ([104.128.23.115]) by mail bieberdorf.edu (8.8.5)
- Received from nowhere by fictitious-site (8.8.3/8.7.2)
- Received: No information Here, Go Away!

Since the sender has no control over the message once it leaves turmeric.com, Received: headers are always added at the top and the forged lines at the bottom of the list

Obviously, the last two lines are complete nonsense, written by the sender and attached to the message before it was sent

Analyzing Email Headers

Gather supporting evidence as given below from the email headers and track the suspect

- **Return Path**
- **Recipient's email address**
- **Type of sending email service**
- **IP address of sending server**
- **Name of the email server**
- **Unique message number**
- **Date and time email was sent**
- **Attachment files information**

Email Headers fields

Listed below are the most important fields to check in order to trace the message back to its origin and to identify the route it took from the original sender:

Field Name	Explanation
Source/Sender Header Fields	
From	Identifies email sender, usually by name and email address
Sender	Identifies actual sender of email
Reply-To	Email address to which replies should be sent
Return Path	Path (address) back to sender
Received	Except when users reside on the same server known as a message transfer agent or MTA, every email goes through at least one intermediary server as it's routed from sender to receiver. Each such intermediary appears on its own Received line
Resent-xxx	Applies to re-sent messages for From, Sender and Reply-to-fields

Field Name	Explanation
Date Headers	
Date	Date and time original message was sent
Resent date	Date and time re-sent message was sent

Field Name	Explanation
Destination Header Fields	
To	Identifies name and email address for recipient
Cc	Secondary message recipients
Bcc	Blind carbon copy message recipients
Resent-xxx	Applies to re-sent messages for To, Cc and Bcc fields

Field Name	Explanation
Optional Headers	
Subject	Topic for message
Message-ID	Unique message identifier
In-reply-to	Identifies message being replied to
References	Identifies other messages to which this message applies
Keywords	Keywords to help sort and organize message contents
Comments	Text comments about message
Encrypte	Indicates message content is encrypted
X-xxx	Identifies user-defined fields

Received : Headers

Received : headers provide a detailed log of a message's history, and so make it possible to draw some conclusions about the origin of a piece of email even when other headers have been forged

If, for instance, the machine turmeric.com, whose IP address is 104.128.23.115, sends a message to mail.bieberdorf.edu, but falsely says HELO galangal.org, the result Received: line might start like this:

Received: from galangal.org ([104.128.23.115)] by mail.bieberdorf.edu (8.8.5)…

Examining Additional Files .pst or .ost

1. Email messages are saved as files either on the client computer or server
2. Microsoft Outlook maintains email in .pst or .ost files
3. Online email programs such as AOL, Hotmail and Yahoo store Email messages in folders such as History, Cookies and Temp
4. Most of the email programs also include an electronic address book
5. Unix stores email messages as per the user

Tracking Back

1. The first step in tracing back fake mail is to view the header's information

2. The header will show the originating mail server, ex: mail.example.com

3. With a court order served by law enforcement or a civil complaint filed by attorneys, obtain the log files from mail.example.com to determine who sent the message

4. Information regarding the Internet domain registration can be found from:
   - www.arin.net
   - www.internic.com
   - www.freeality.com

Tracking Back web based Email

1

Web-based email accounts (Webmail) can make it more difficult to establish the identity of the sender

2

It is possible to create a new online webmail account easily

- www.hotmail.com
- www.yahoo.com
- www.hushmail.com

3

The above sites maintain the source IP address of each connection that accesses the online webmail

4

Contact the email provider (example: Microsoft, Google, Yahoo) to reveal the subscriber's information

Deleted Email Recovery

Recovery of deleted email messages varies based on the email client used. Examples of how deleted email works

Eudora Mail

- Messages for deletion are tagged for deletion and no longer visible in the mailbox
- However, messages reside in the trash folder until the trash folder is emptied

Outlook PST

- Data is taken from the active part of the archive to a recycle bin
- If the recycle bin is emptied, it will go to the unallocated space of the email archive where it resides for a period of weeks
- Recovery of this data varies depending on the size of the archive

US Laws Against Email Crime : CAN-SPAM Act

The CAN-SPAM Act of 2003 (Controlling the Assault of Non-Solicited Pornography and Marketing Act) establishes requirements for those who send commercial email, spells out penalties for spammers and companies whose products are advertised in spam if they violate the law, and gives consumers the right to ask emailers to stop spamming them

MAIN PROVISIONS

It bans false or misleading header infromation

It requires that the email give recipients an opt-out method

It prohibits deceptive subject lines

It requires that commercial email be identified as an advertisement and include the sender's valid physical postal address

US Laws Against Email Crime : CAN-SPAM Act

Penalties : Each violation of the provisions on the previous page is subject to fines of up to $11,000

- Additional fines are provided for commercial mailers who not only violate the rules described on the previous page, but also:
  - ✓ "Harvest" email addresses from websites or Web services that have published a notice prohibiting the transfer of email addresses for the purpose of sending email
  - ✓ Generate email address using a "dictionary attack" – combining names, letters, or numbers into multiple premutations
  - ✓ Use scripts or other automated ways to register for multiple email or user accounts to send commercial email
  - ✓ Relay emails through a computer or network without permission – for example, by taking advantage of open relays or open proxies without authorization

- The law allows the DOJ to seek criminal penalties, including imprisonment, for commercial emailers who do - or conspire to:
  - ✓ Use another computer without authorization and send commercial email from or through it
  - ✓ Use a computer to relay or retransmit multiple commercial email messages to deceive or mislead recipients or an internet access service about the origin of the message
  - ✓ Falsify header information in multiple email messages and initiate the transmission of such messages

Email Crime Law in Washington : RCW 19.190.020

This law is for residents of Washington; it states that:

- No person may initiate the transmission, conspire with another to initiate the transmission, or assist the transmission, of a commercial electronic mail message from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident that:
  - ✓ Uses a third party's internet domain name without permission of the third part, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or
  - ✓ Contains false or misleading information in the subject line

THANK YOU

Digital Forensics and Investigation
[CET4033B]

TYBTech CSF, Semester-V
AY 2023-24

Dr Sumedha Sirsikar

Incident Response

- online *International Journal of Digital Evidence* (www.ijde.org)
- This was followed closely by the publication in 2004 of the peer-reviewed journal *Digital Investigation*:
- *The International Journal of Digital Forensics and Incident Response* http://www.digitalinvestigation.net/

Incident Response Collection Report

- Incident Response Collection Report (IRCR) is similar to TCT. The program is a collection of tools that gathers and analyzes forensic data on Windows systems
- Like TCT, most of the tools within IRCR are oriented toward data collection rather than analysis
- IRCR is simple enough that anyone can run the program and forward the output to a forensic investigator for further analysis

Incident Response Teams

- A team of individuals trained and prepared to recognize and immediately respond appropriately to any security incident
- can provide this information for forensic situations, or assist with its compilation
- know how to handle workplace situations they will encounter when conducting investigations
- responsible for containing damage and getting systems back up and running properly

What incident response can do ? : plan

- The actions an organization takes when it detects an attack, whether ongoing or after the fact
- needed so that you can intelligently react to intrusions, security breaches, or other identifiable incidents
- Issue of legal liability
- An incident response team is responsible for:
  - containing damage and getting systems back up and running properly. These steps include determination of the incident, formal notification to appropriate departments, and the recovering of essential network resources
- If a plan is not in place and duties not clearly assigned, your organization may wind up in a state of disarray

Components of An Incident Response Plan

The actions an organization takes when it detects an attack, whether ongoing or after the fact

- preparation, roles, rules, and procedures
- plan is prepared
- appoint response team members

Members Of Incident Response Teams

- Security and IT staff
- Someone to handle communication with management and employees
- Someone to handle communication with vendors, business partners, and the press
- Developers of in-house applications and interfaces
- Database managers

Documentation of Evidence Logs

- Date and time of action
- Action type (choose one)
  - Initial evidence collection
  - Evidence location change
  - Remove evidence for analysis
  - Return evidence to storage
- Personnel collecting/ accessing evidence
- Computer descriptive information
  - Computer make and model
  - Serial number(s)
  - Location
  - Additional ID information
  - BIOS settings specific to disk drives
- Disk drive descriptive information
  - Disk drive manufacturer, model number, and serial number
  - Drive parameters (heads, cylinders, sectors per track)
  - Jumper settings
  - Computer connection information (adapter, master/slave)
- Handling procedure
  - Preparation (static grounding, prevention of physical shock, etc.)
  - Contamination precautions taken
  - Step-by-step events within the events of each action
  - Inventory of supporting items created/acquired (e.g., hash or checksum of drive/files)
- Complete description of action
  - Procedure used
  - Tools used
  - Description of each analysis step and its results
- Reason for action
- Notes
  - Comments not specifically requested anywhere else in the log
  - The notes section provides additional details as an investigation unfolds

Digital Forensics Analysis
CSN611
MTech CSE-NMCS, Trimester-IV, AY 2020-21

Dr Sumedha Sirsikar

Preserving the Digital Scene

Preserving the Digital Crime Scene

- Protecting the digital crime scene against unauthorized alterations
- Acquiring digital evidence in a manner that ensures its authenticity and integrity
- A delicate process because information may be lost almost immediately upon collection by virtue of the volatility of electronic devices and their design
- Necessary to perform operations on a system that contains evidence, especially in network connected environments
- Networks are involved, a crime scene may include sources of evidence in several physically distant locations

Preserving the Digital Crime Scene

1. **Controlling Entry Points to Digital Crime Scenes**
2. **Freezing the Networked Crime Scene**
3. **Considerations for "Wet" Forensics**
4. **Developing a Forensic Preservation Strategy**
5. **Preserving Data on Live Systems**
6. **Remote Preservation of Digital Evidence**
7. **Shutting Down Evidential Computers**

1. Controlling Entry Points to Digital Crime Scenes

- To secure the physical crime scene by removing everyone to prevent them from contaminating evidence
- To disable biometric access and video surveillance equipment as it is potential sources of evidence

- ACPO recommends isolation of mobile devices, from the network at all times:
  - To prevent the evidential device from receiving new calls, messages or commands that could alter or destroy evidence
  - configured to use Wi-Fi access points to communicate

Digital investigators to preserve the evidence:

- information is stored on:
  - Internet servers in different locations
  - cloud computing services
- Remote storage locations

PRACTITIONER'S TIP

In order to prevent anyone from accessing systems from outside the crime scene, it is generally advisable to disable network connectivity to all computer systems. However, this action should only be performed after careful consideration as unplugging network cables can destroy evidence and eliminate investigative opportunities. Once a network cable is removed, the opportunity to list the active connections to the system is lost and investigators may never know which other computers on the network might contain evidence. In certain cases, such as network intrusions, disconnecting network connections may eliminate an opportunity to gather network traffic of the perpetrator in action. Furthermore, removing a network cable can seriously impact a business that relies on the computer being available on the network. Disconnecting an organization's e-mail server or an e-commerce site's main transaction server can cause significant losses.

2. Freezing the Networked Crime Scene

Preserving evidence on an organization's network is a challenge to digital investigators:

- Any network-level logs with an organization
- Copy all available log files and to disable log rotation to prevent old files being automatically overwritten
- Advisable to preserve all backup media and disable any mechanisms of overwriting
- To preserve e-mail and files on centralized servers
- To disable all of a suspect employee's user accounts as a step in securing digital evidence on organization's network
- Not to allow system administrators to preserve evidence independently, may be mishandled/missed digital evidence

CASE EXAMPLE: SYSTEM ADMINISTRATORS GONE WILD!

A system administrator in a large organization was the primary suspect in a homicide investigation, and he claimed that he was at work at the time of the murder. Police were unfamiliar with digital forensics and enlisted other system administrators in the organization to preserve any digital evidence that might assist in the case. The system administrators were not trained in digital forensics and had limited investigative experience, but made an effort to answer questions that were posed to them. Rather than creating a forensic duplicate of the suspect's computer for proper forensic examination, the system administrators operated the computer extensively in an effort to determine whether it had been used during the period in question without success. This process tainted the digital crime scene, obliterating information that qualified forensic examiners could have used to determine whether the suspect had been using the computer when the murder occurred. In addition, the system administrators only preserved portions of network-level logs, not the full logs. It was later determined that the suspect was using a computer with a different IP address than originally thought. Unfortunately, by the time this information came to light, the network-level logs for the time in question had been overwritten by newer logs. As a result of these and other shortcomings in the handling of digital evidence, it was difficult for digital investigators to rely on the information that was provided to them by system administrators.

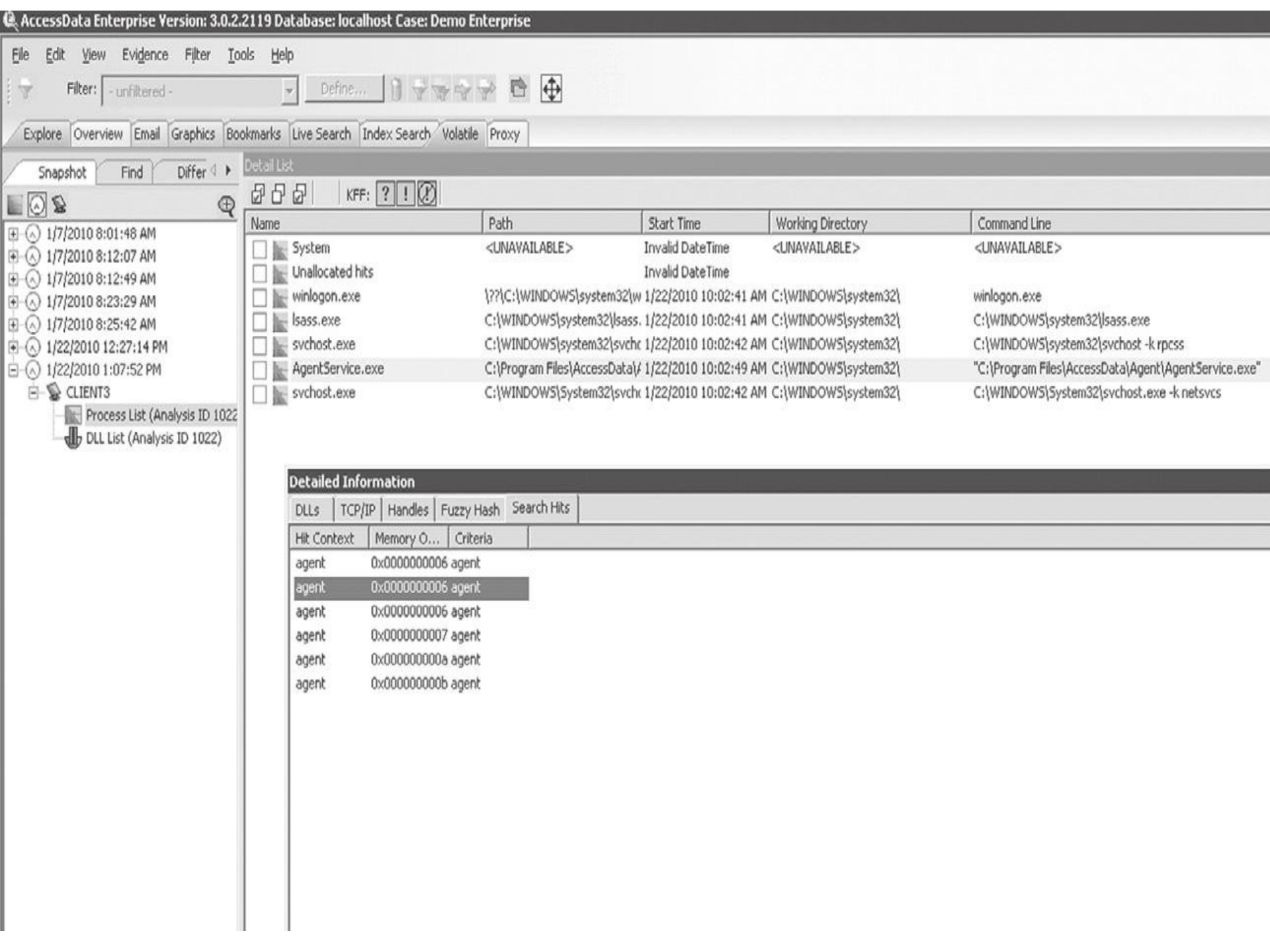
3. Considerations for 'Wet' Forensics

Additional precautions by investigators:

- Fingerprints and biological evidence may exist to generate suspects
- A suicide note was written on the victim's computer after death
- If investigators operated the computer, thus destroying any fingerprint evidence that may have existed
- In homicide case, evidence was deleted from the victim's computer after death but investigators may destroy any fingerprint evidence

ACPO Guide advises digital investigators:

- not to touch the keyboard or mouse
- not to use chemicals that may damage electronics when collecting fingerprints or biological evidence
- Using aluminium powder on electronic devices can be dangerous and result in the loss of evidence


AccessData Enterprise Version: 3.0.2.2119 Database: localhost Case: Demo Enterprise
File Edit View Evidence Filter Tools Help
Filter: - unfiltered - Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile Proxy
Snapshot Find Differ
1/7/2010 8:01:48 AM
1/7/2010 8:12:07 AM
1/7/2010 8:12:49 AM
1/7/2010 8:23:29 AM
1/7/2010 8:25:42 AM
1/22/2010 12:27:14 PM
1/22/2010 1:07:52 PM
CLIENT3
Process List (Analysis ID 1022
DLL List (Analysis ID 1022)
Detail List
KFF:
Name Path Start Time Working Directory Command Line
System <UNAVAILABLE> Invalid DateTime <UNAVAILABLE> <UNAVAILABLE>
Unallocated hits Invalid DateTime
winlogon.exe \??\C:\WINDOWS\system32\w 1/22/2010 10:02:41 AM C:\WINDOWS\system32\ winlogon.exe
lsass.exe C:\WINDOWS\system32\lsass. 1/22/2010 10:02:41 AM C:\WINDOWS\system32\ C:\WINDOWS\system32\lsass.exe
svchost.exe C:\WINDOWS\system32\svchc 1/22/2010 10:02:42 AM C:\WINDOWS\system32\ C:\WINDOWS\system32\svchost -k rpcss
AgentService.exe C:\Program Files\AccessData\A 1/22/2010 10:02:49 AM C:\WINDOWS\system32\ "C:\Program Files\AccessData\Agent\AgentService.exe"
svchost.exe C:\WINDOWS\System32\svchc 1/22/2010 10:02:42 AM C:\WINDOWS\system32\ C:\WINDOWS\System32\svchost.exe -k netsvcs
Detailed Information
DLLs TCP/IP Handles Fuzzy Hash Search Hits
Hit Context Memory O... Criteria
agent 0x0000000006 agent
agent 0x0000000006 agent
agent 0x0000000006 agent
agent 0x0000000007 agent
agent 0x000000000a agent
agent 0x000000000b agent

4. Developing a Forensic Preservation Strategy

Digital investigators prioritize preservation efforts:

- Based on volatility and importance of the data
- Type and importance of evidence, the severity of the crime
- Take print screens and make a copy of selected information from a server
- Too many files to copy individually or the deleted data that are crucial to the case, to preserve entire computer
- To seize an entire computer versus create a forensic duplicate of the internal hard drive

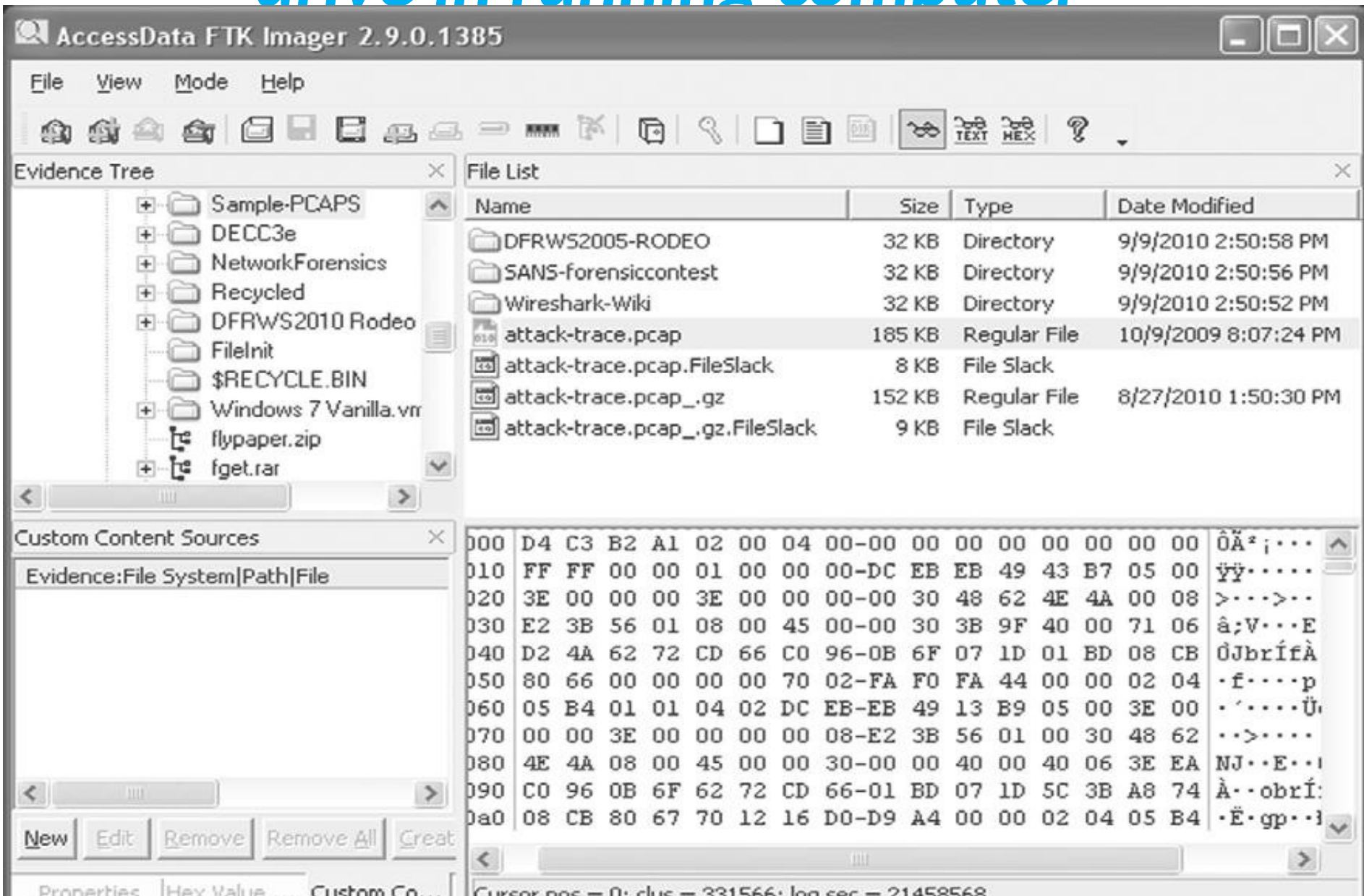
Table 7.1 Various Approaches to Preserving Digital Evidence

What to Preserve	Implications
Original hard drive	Any operations that are needed can be performed. However, physical damage/failure of the original hard drive may render its contents inaccessible.
Forensic duplicate of original hard drive	The entire contents of the hard drive are preserved, including deleted data. However, it may be infeasible or not permitted under certain circumstances (e.g., very large hard drives, legal protection of certain files).
Select files from original hard drive	Other files on the hard drive that may be relevant will not be preserved, and deleted data will not be preserved. Furthermore, for the selected files, important information or metadata may be lost or misinterpreted during acquisition.
Converted versions of files from original hard drive	For the selected files, important information or metadata may be lost or misinterpreted during conversion.
Relevant portions of files from original hard drive	Digital investigators only know what is relevant at a certain moment and may miss some relevant information, particularly if new facts come to light later.
Written notes detailing portions of files on original hard drive	The approach does not preserve the original digital evidence and is not feasible with large amounts of data

5. Preserving Data on Live Systems

- Information on volatile memory:
  - When evidence is contained on an embedded system, i.e. a personal digital assistant or wireless phone
- Avoid potential alterations of digital evidence, e.g. it may be possible to collect the necessary information by running programs (and saving the data) from an external device
- May first connect a different keyboard and mouse to the computer in order to preserve fingerprints and biological evidence

FTK Imager Lite: forensic image of hard drive in running computer



6. Remote Preservation of Digital Evidence

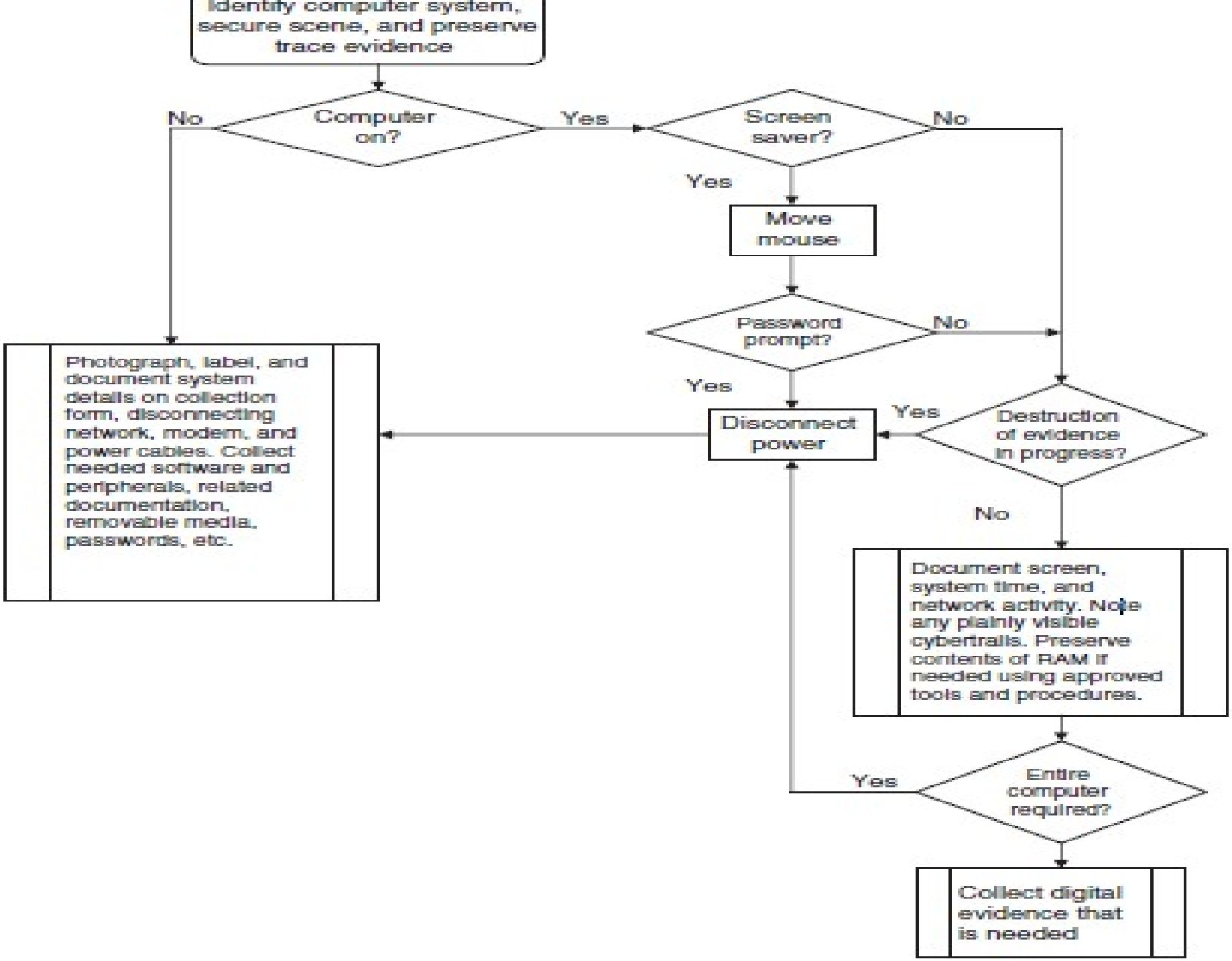
Distributed systems in a crime scene that have locations in different geographic regions:

- acquire data from remote systems
- Can preserve evidence on live, remote computer systems (Casey & Stanley, 2004)
  - Remote forensic tools: F-Response, EnCase Enterprise, FTK Enterprise and ProDiscover IR (acquire data from memory as well as hard drives)

7. Shutting Down Evidential Computers

ACPO Guide correctly advises Investigator:

- To unplug the power cable from the computer
- To avoid the possibility of an uninterrupted power support (UPS) continuing to power the computer
- To remove a computer's casing to unplug power cables from hard drives, to set all cards properly and to observe any anomalies (e.g., Missing hard drive or explosives)


Identify computer system, secure scene, and preserve trace evidence
Computer on?
No
Yes
Screen saver?
No
Yes
Move mouse
Password prompt?
No
Yes
Photograph, label, and document system details on collection form, disconnecting network, modem, and power cables. Collect needed software and peripherals, related documentation, removable media, passwords, etc.
Disconnect power
Yes
Destruction of evidence in progress?
No
Document screen, system time, and network activity. Note any plainly visible cybertrails. Preserve contents of RAM if needed using approved tools and procedures.
Yes
Entire computer required?
Collect digital evidence that is needed

CASE EXAMPLE: INSIDER THREAT (PART 3: PRESERVATION)

While conducting a survey of the area, digital investigators took actions to preserve the digital crime scene. At the entryway into the crime scene, digital investigators observed a biometric authentication system and CCTV cameras. Both of these systems were documented and, shortly thereafter, were disconnected to preserve any pertinent information they might contain. Disabling the biometric authentication system had the added benefit of restricting access to the area. Later that day the locks on all entry doors were changed and keys were strictly controlled.

In addition to restricting physical access to the area, digital investigators took immediate steps to prevent remote access to systems of interest. This isolation involved disabling user accounts on central systems, including e-mail and VPN servers, and disconnecting from the network all systems on the target list that was compiled during the preparation stage. During the survey process, some additional systems were found beside computers of interest, and these were also disconnected from the network.

Using this inventory list, digital investigators started acquiring data in a forensically sound manner. Some special attention was needed to acquire data from central e-mail servers and systems that had full disk encryption and encrypted volumes. To ensure that e-mail was properly preserved, digital investigators sat beside the system administrator of the central e-mail servers during the acquisition process. In order to acquire data from a laptop that had full disk encryption, digital investigators obtained a decryption key from one of the organization's system security administrators. While documenting the screen contents of one of the suspect employees' computers, digital investigators observed an encrypted volume that would have been closed if the system was shut down, and took steps to acquire the contents of the encrypted volume while it was still open. In addition, digital investigators used a remote forensic tool to acquire data from a proprietary server that was located elsewhere, after working with system administrators and the vendor.

Preserving the Digital Scene

- process involves protecting the digital crime scene against unauthorized alterations and acquiring digital evidence in a manner that ensures its authenticity and integrity
- Many modern computers have large amounts of random access memory (RAM) where process context information, network state information, and much more are maintained
- Preventing people from disturbing a single computer or room is relatively straightforward but, when networks are involved, a crime scene may include sources of evidence in several physically distant locations

1. Controlling Entry Points to Digital Crime Scenes

- The first step is to secure the physical crime scene by removing everyone
- It is advisable to disable biometric access and video surveillance equipment in and around the office
- Changing locks for all points of entry in an prolonged investigation
- Disable network connectivity on all systems in the crime scene
- When handling mobile devices, it is recommended that the device is isolated from the network at all times
- One challenge that arises when Internet servers are at different locations

2. Freezing the Networked Crime Scene

- Preserving evidence on an organization's network is a challenging undertaking ,and may require the assistance of system administrators
- Preserve any network-level logs
- Disable log rotation to prevent old files to be overwritten
- To preserve all backup media and disable other
- Preserve e-mail and files on centralized servers
- Digital investigators supervision is necessary
- When dealing with larger networks remote forensic tools at a central location can be used to acquire data from distributed computers

3. Considerations for "Wet" Forensics

- Additional precautions must be taken when fingerprints and biological evidence may exist on the evidential computers that could help investigators generate suspects

- It is a advice to digital investigators not to touch the keyboard or mouse, and not to use chemicals that may damage electronic devices

4. Developing a Forensic Preservation Strategy

- Digital investigators prioritize digital evidence preservation
- Depends on the type of evidence, the severity of the crime and the importance of the evidence to the investigation
- It is sufficient to take print screens and make a copy of select information from a server
- When there are too many files to copy or contains deleted data it becomes necessary to preserve the entire computer
- Seize an entire computer versus create a forensic duplicate of the internal hard drive will be influenced by the role of the computer

5. Preserving Data on live Systems

- When digital investigators encounter a computer or mobile device that is powered on and running (a.k.a. live), they must decide what actions to take prior to turning the system off
- The contents of volatile memory are becoming more important
- When dealing with multiuser systems it is useful to know which account is running a certain process
- Investigating computer intrusions, it is important to capture information related to active processes and network connections
- In an embedded system such as a personal digital assistant or wireless phone, the majority of useful information is stored in volatile memory
- The primary challenge in such cases is to capture the volatile memory while making minimal changes on the system

- Digital Evidence Collection from live System:
  - volatile data/specific files must be collected with competent individual to preserve the data
  - Trained and experienced digital investigator
  - Collect specific information from memory
  - Every action must be documented and the hash value of acquired data should be calculated
  - make a forensic image of the hard drive while the computer is running

6. Remote Preservation of Digital Evidence

- Distributed systems in a crime scene, particularly in organizations that have locations in different geographic regions, digital investigators may need to acquire data from remote systems

- Remote forensic tools such as F-Response, EnCase Enterprise, FTK Enterprise and ProDiscover IR can be used to acquire data from memory as well as hard drive

7. Shutting Down Evidential Computers

- If investigators decide that it is necessary to shut down a computer in order to preserve digital evidence, it is advisable to unplug the power cable from the computer rather than from the wall plate.

- Removing power from the back of the computer is generally recommended.

- It is also advisable to remove a computer's casing to unplug power cables from hard drives (e.g., missing hard drive or explosives)

- In addition to preserving all items that digital investigators are authorized to process, they should take related manuals, installation media and any other material that may be helpful in accessing or understanding the digital evidence