

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

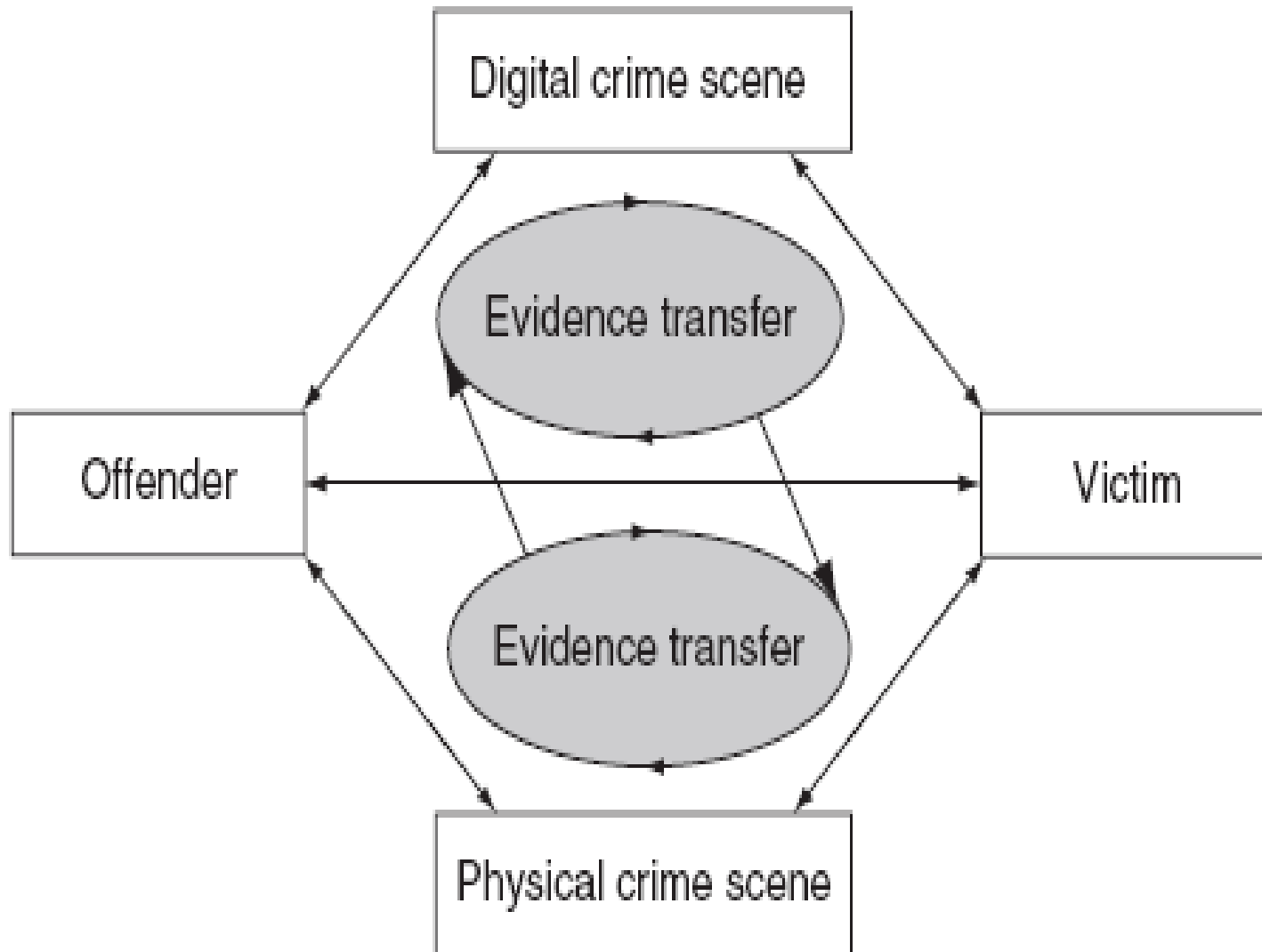
1. Evidence Exchange
2. Evidence Characteristics
3. Forensic Soundness
4. Authentication
5. Chain of custody
6. Evidence Integrity
7. Objectivity
8. Repeatability

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:


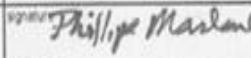
- transient and data must be captured while it is in transit
- captured network traffic - only copies remain and the original data are not available for comparison
- **authentication** is the process of determining whether the evidence is **worthy**
- Eg: The individual who collected the evidence can 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

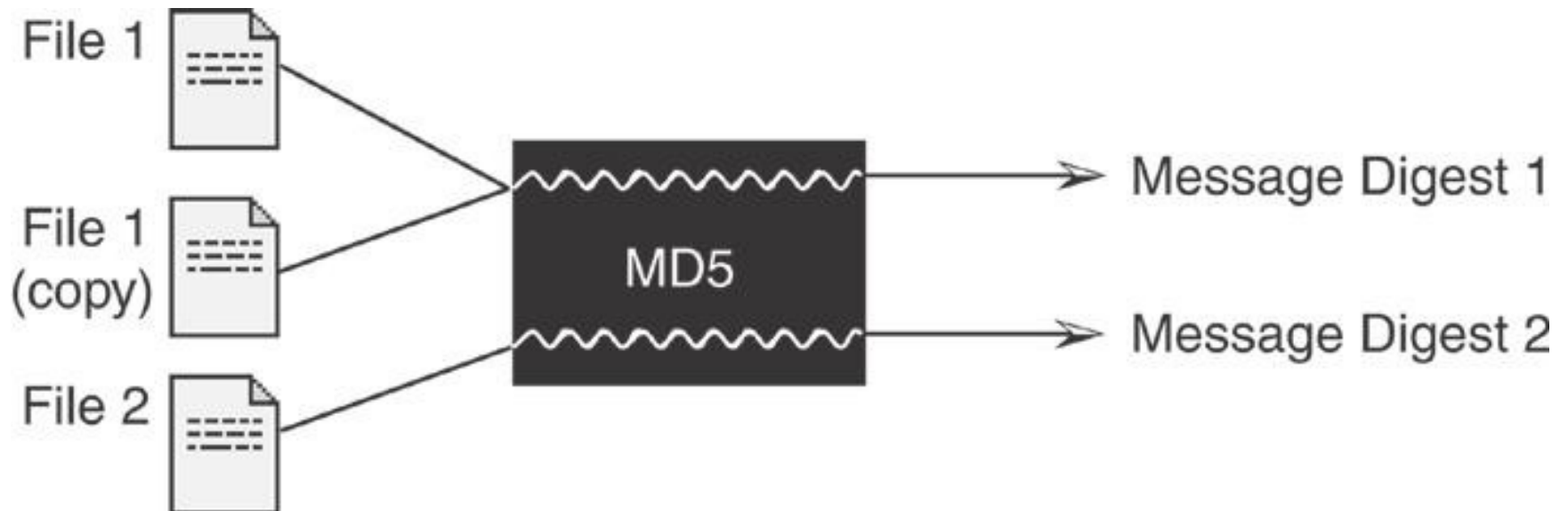
5. Chain of Custody

- 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	<small>signature</small>  <small>print name</small> Sam Spade	<small>signature</small>  <small>print name</small> Philip Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	<small>signature</small> <small>print name</small>	<small>signature</small> <small>print name</small>		

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

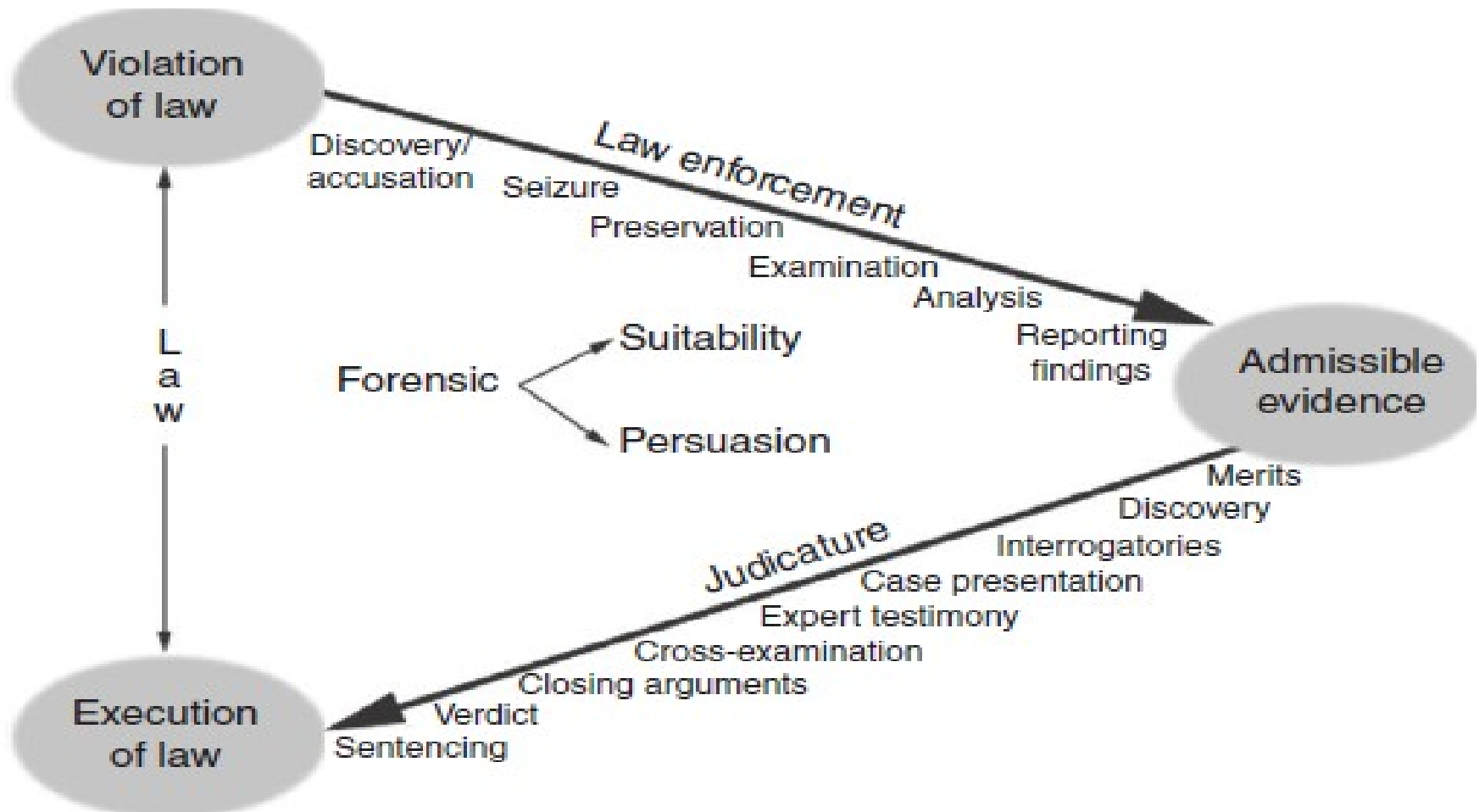
Direct versus circumstantial evidence

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

Applications

Home, Contacts, Phone, Browser, ...

Application Framework

Managers for Activity, Window, Package, ...

Libraries

SQLite, OpenGL, SSL, ...

Runtime

Dalvik VM, Core libs

Linux Kernel

Display, camera, flash, wifi, audio, IPC (binder), ...

Challenges of Acquisition and Analysis of Data on Android Devices

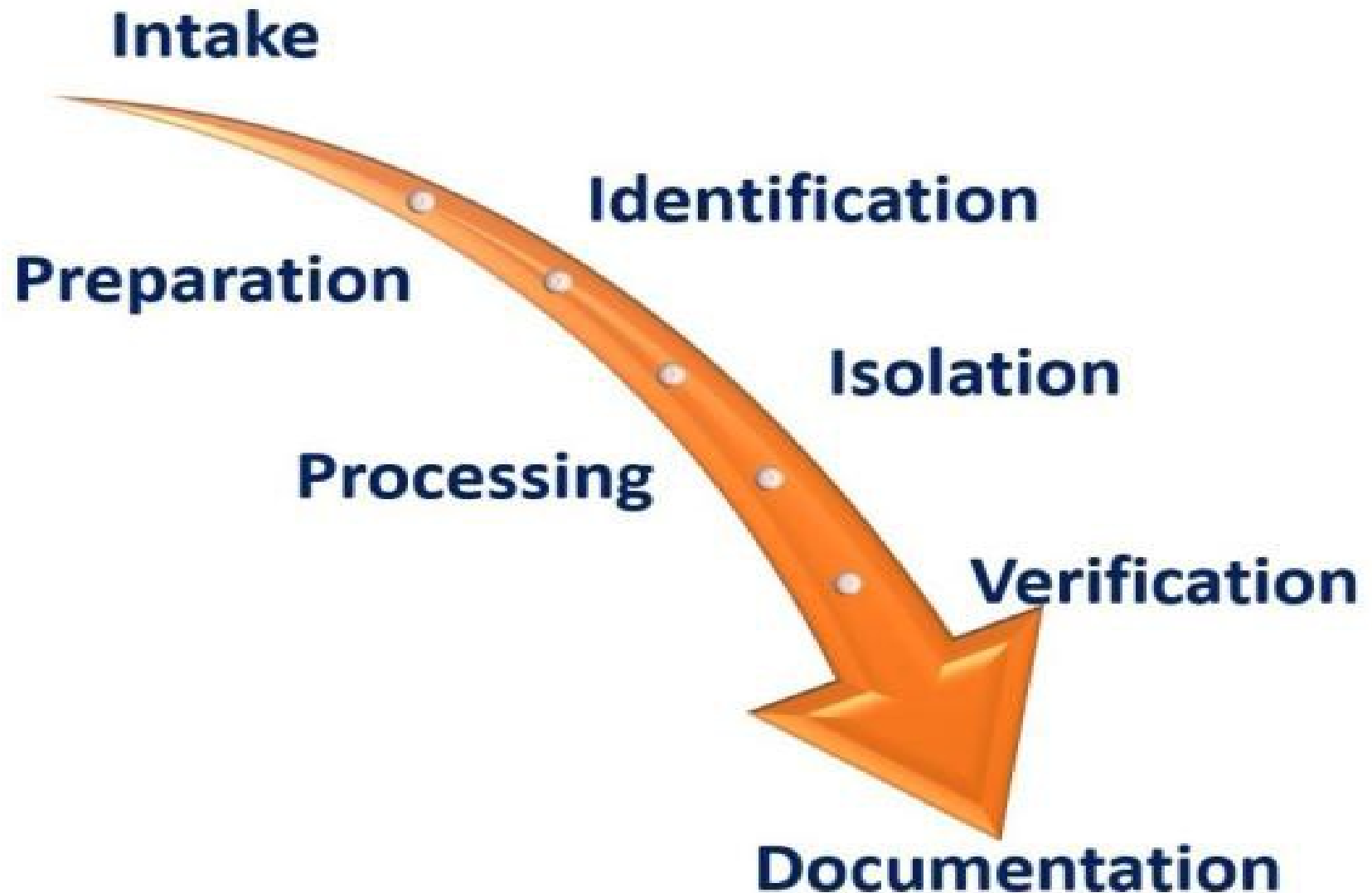
- The complexity and the diversity of Android applications and devices are based on their architecture models and their factory proprietary technology and formats
- The commercial tools that are used to acquire a logical image are highly capable, but they are too expensive.

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	41002716872f6000
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

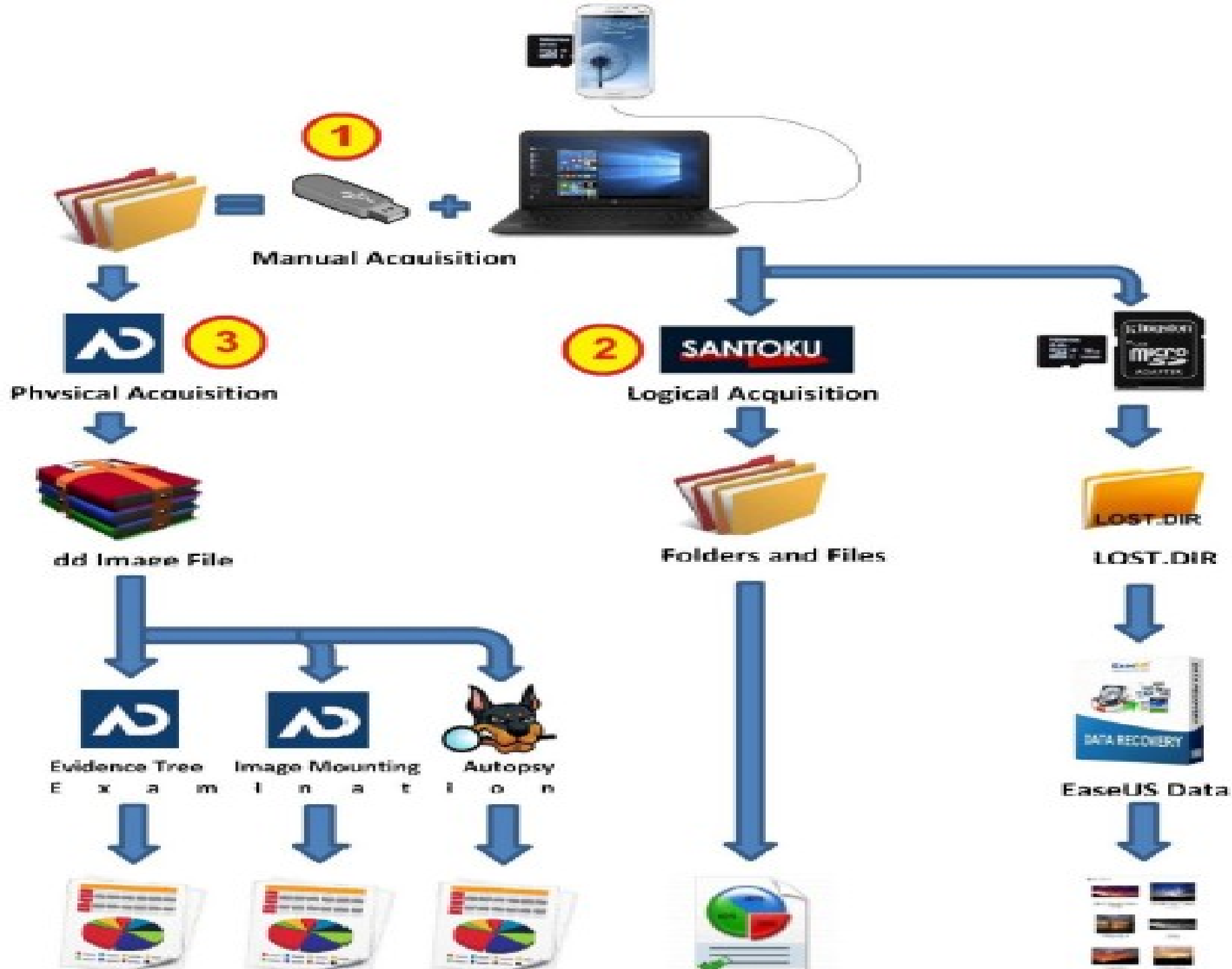
Processing Phase

Step 1:

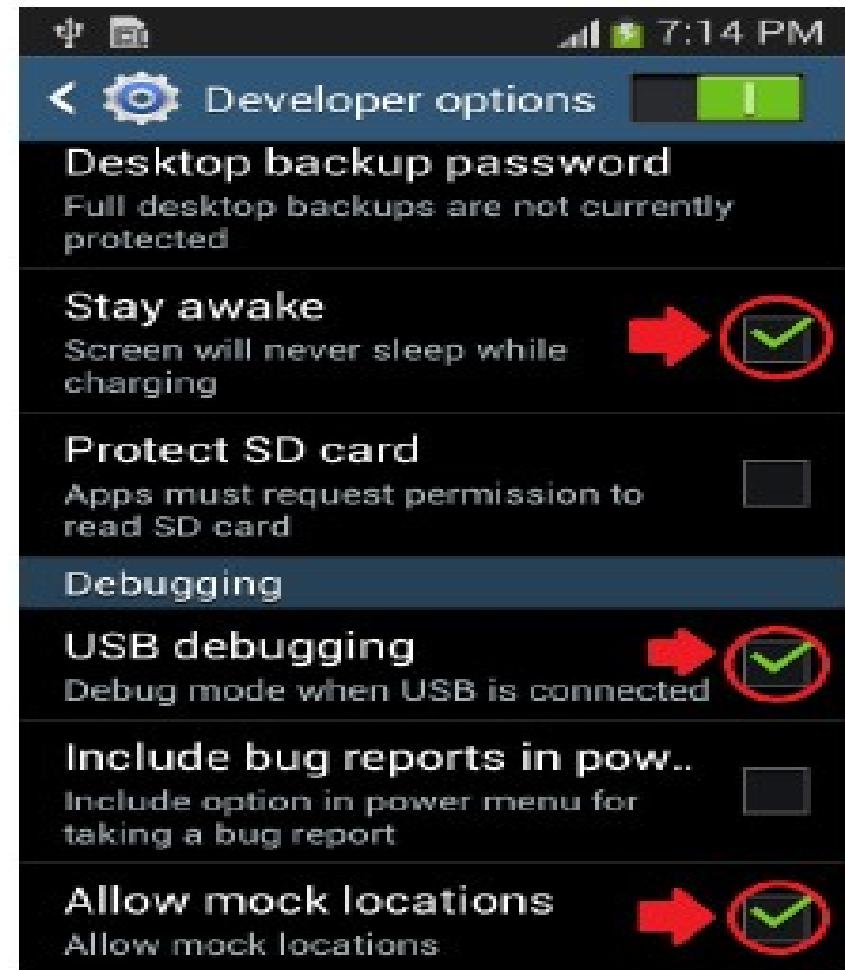
- Connection and Backup (Manual Acquisition)
- The USB driver (Google USB driver) of mobile phone applications was installed after installing Android Studio (SDK manager) to connect the mobile device with the computer
- the mobile device files were moved to the USB Memory Drive in the computer using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

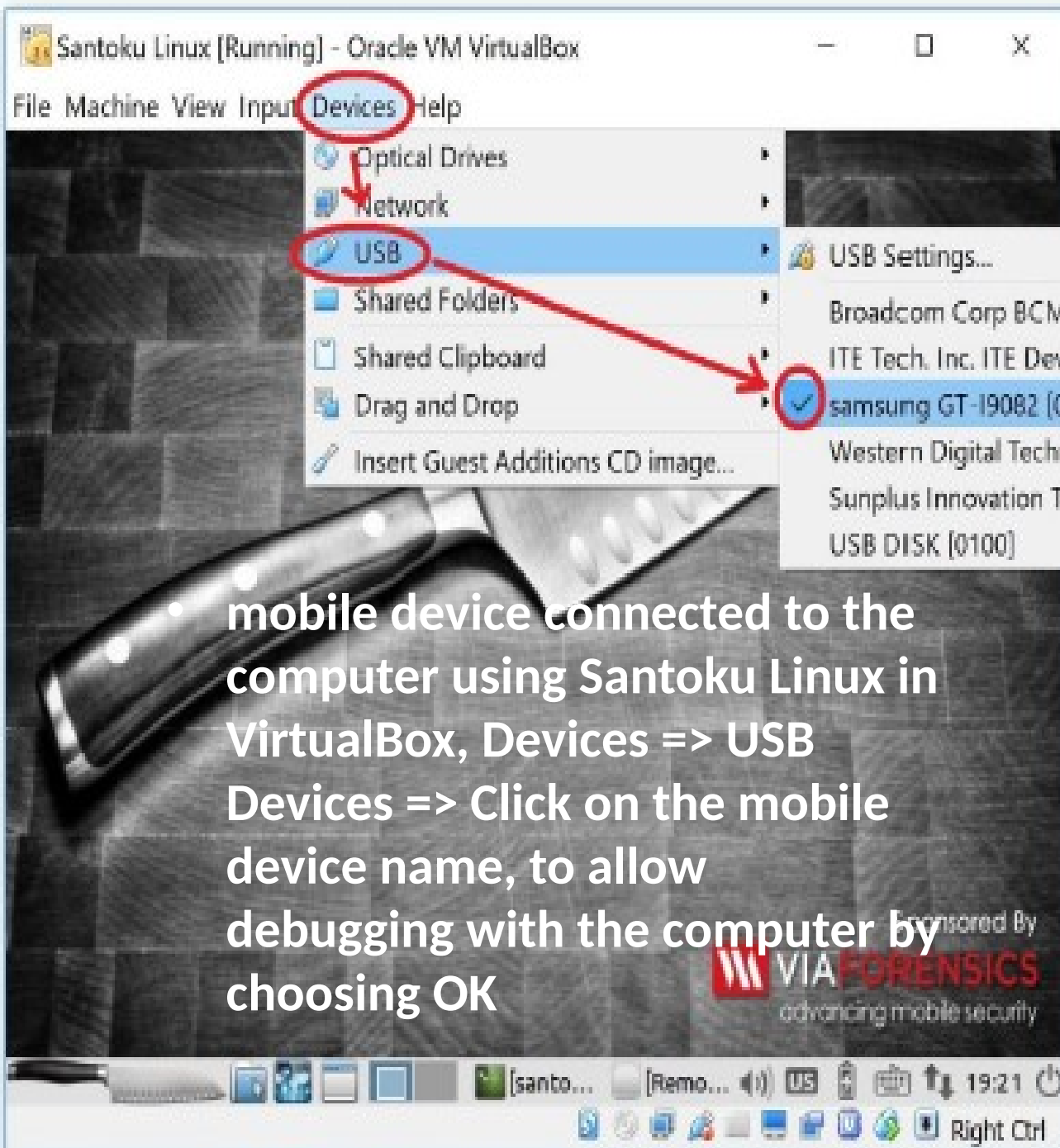
Step 2:

- 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. 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.





- 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



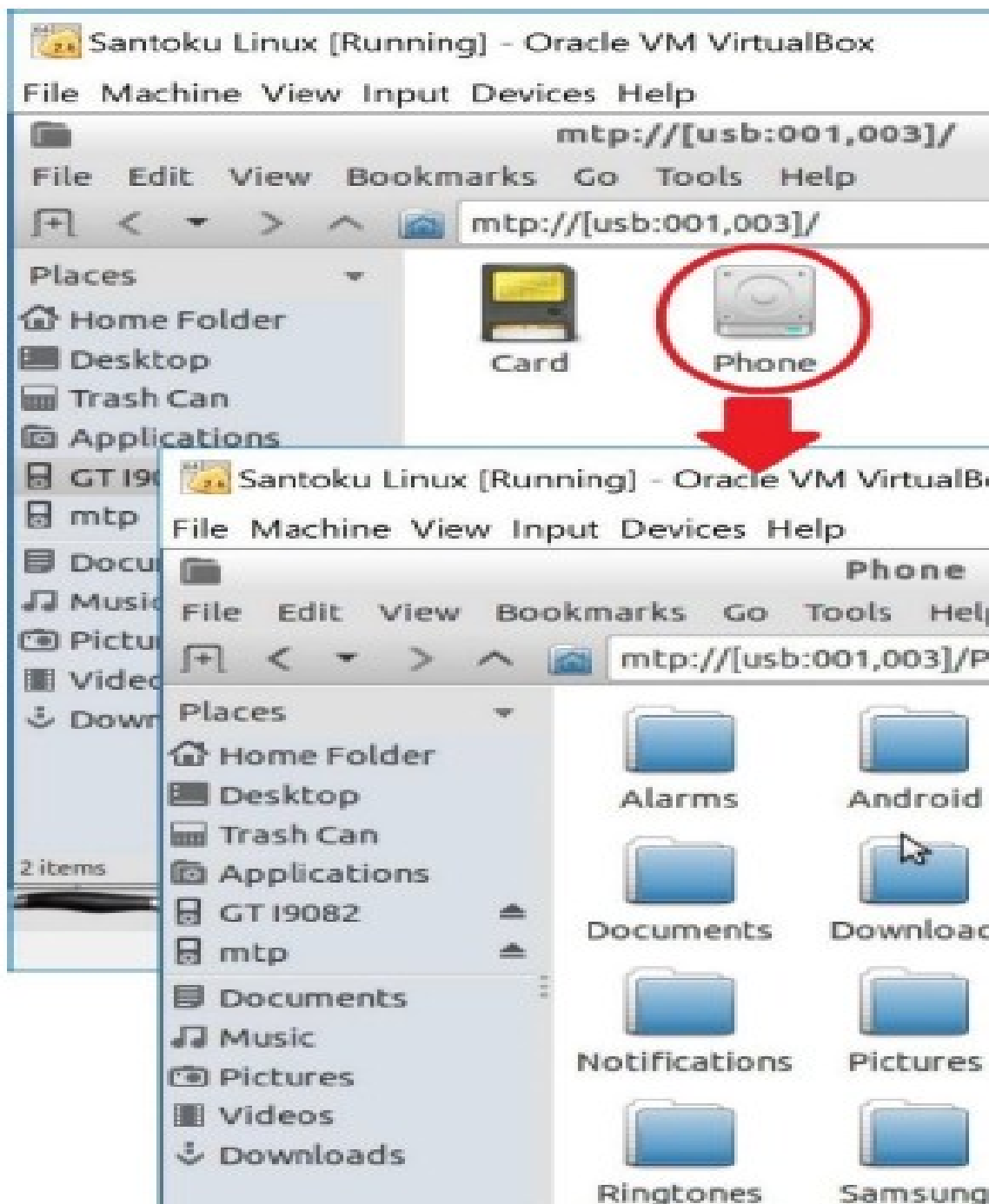
Allow USB debugging?

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

```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
santoku@santoku-VirtualBox:~$ sudo adb devices  
List of devices attached  
41002716872f6000      device  
I  
santoku@santoku-VirtualBox:~$ adb reboot bootloader  
santoku@santoku-VirtualBox:~$ fastboot oem unlock  
< waiting for device >  
^C  
santoku@santoku-VirtualBox:~$ fastboot oem unlock  
< waiting for device >  
^C  
santoku@santoku-VirtualBox:~$ █
```

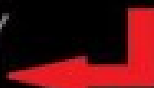
- In the Santoku Linux Virtual Machine => Device Forensics => AFLogical OSE command prompt, the command (sudo adb devices)
 - show the serial number of the mobile device
 - before typing the command (adb reboot bootloader) to reboot the mobile device into recovery mode

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-0SE_1.5.2.apk
Success

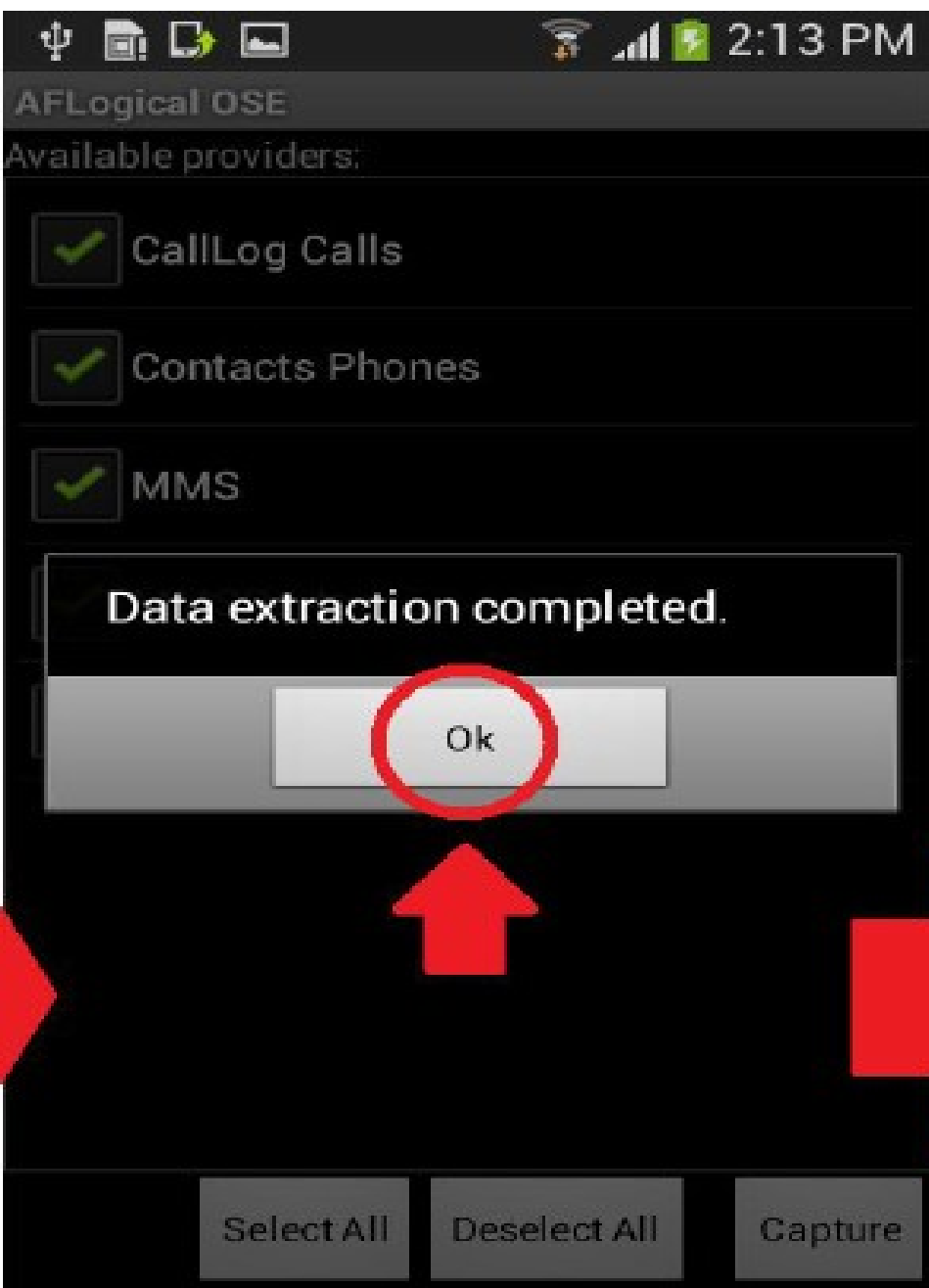
Starting: Intent { cmp=com.viaforensics.android.aflogical_ose/com.viaforensics.
android.ForensicsActivity }

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-c
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:~$
```



Pulling the Data to the Santoku Machine

```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
santoku@santoku-VirtualBox:~$ mkdir ~/Desktop/AFLogical_Phone_Data  
santoku@santoku-VirtualBox:~$ adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data  
pull: building file list...  
pull: /sdcard/forensics/20170109.1413/CallLog Calls.csv -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/CallLog Calls.csv  
pull: /sdcard/forensics/20170109.1413/MMSParts.csv -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/MMSParts.csv  
pull: /sdcard/forensics/20170109.1413/SMS.csv -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/SMS.csv  
pull: /sdcard/forensics/20170109.1413/MMS.csv -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/MMS.csv  
pull: /sdcard/forensics/20170109.1413/Contacts Phones.csv -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/Contacts Phones.csv  
pull: /sdcard/forensics/20170109.1413/info.xml -> /home/santoku/Desktop/AFLogical_Phone_Data/20170109.1413/info.xml  
6 files pulled. 0 files skipped.  
165 KB/s (180562 bytes in 1.063s)  
santoku@santoku-VirtualBox:~$
```

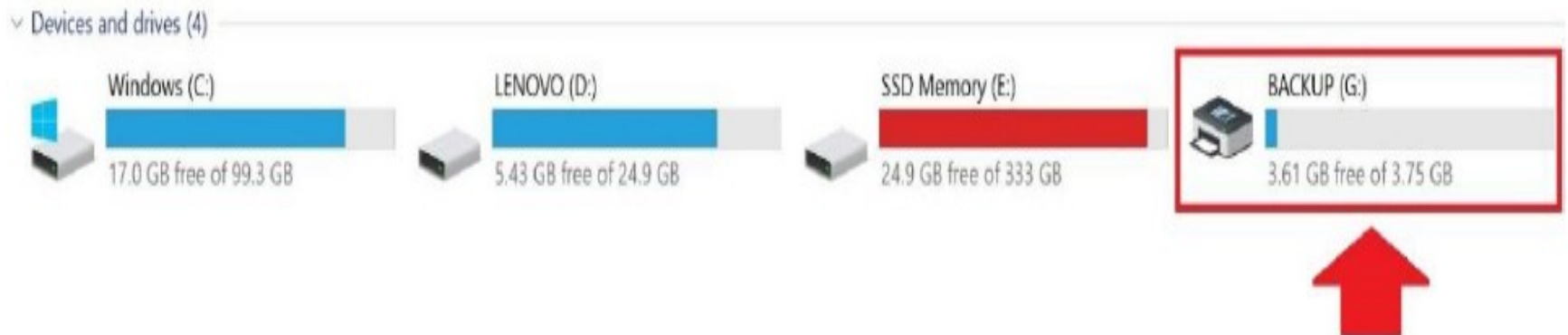
Create AFLogical of Mobile in the Santoku Linux Desktop

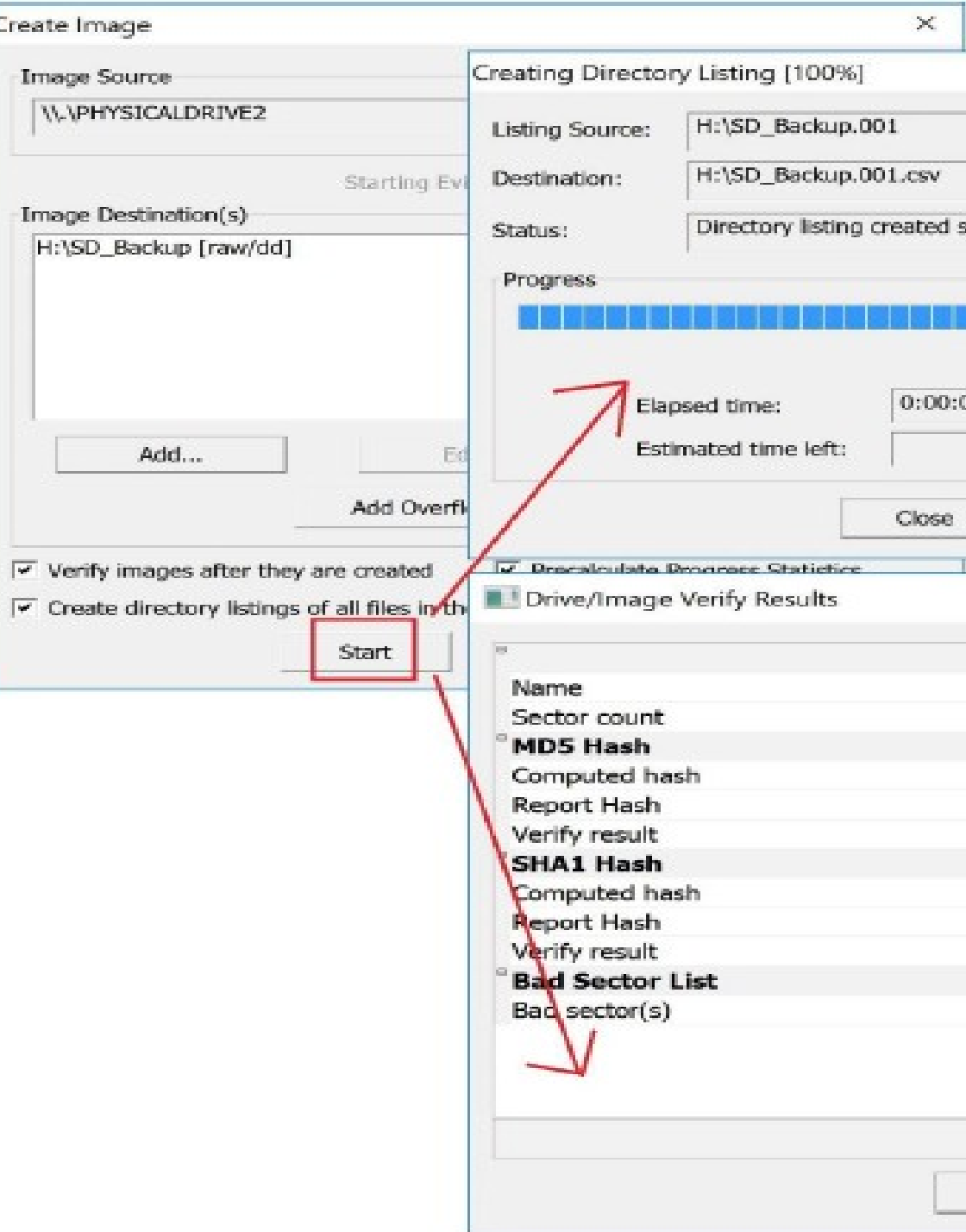


Physical Acquisition

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.

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 Inform
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 Inform
12 IndexerVolumeGuid	Partition 1\BACKUP [FAT32]\[root]\System Volume Inform
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.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]

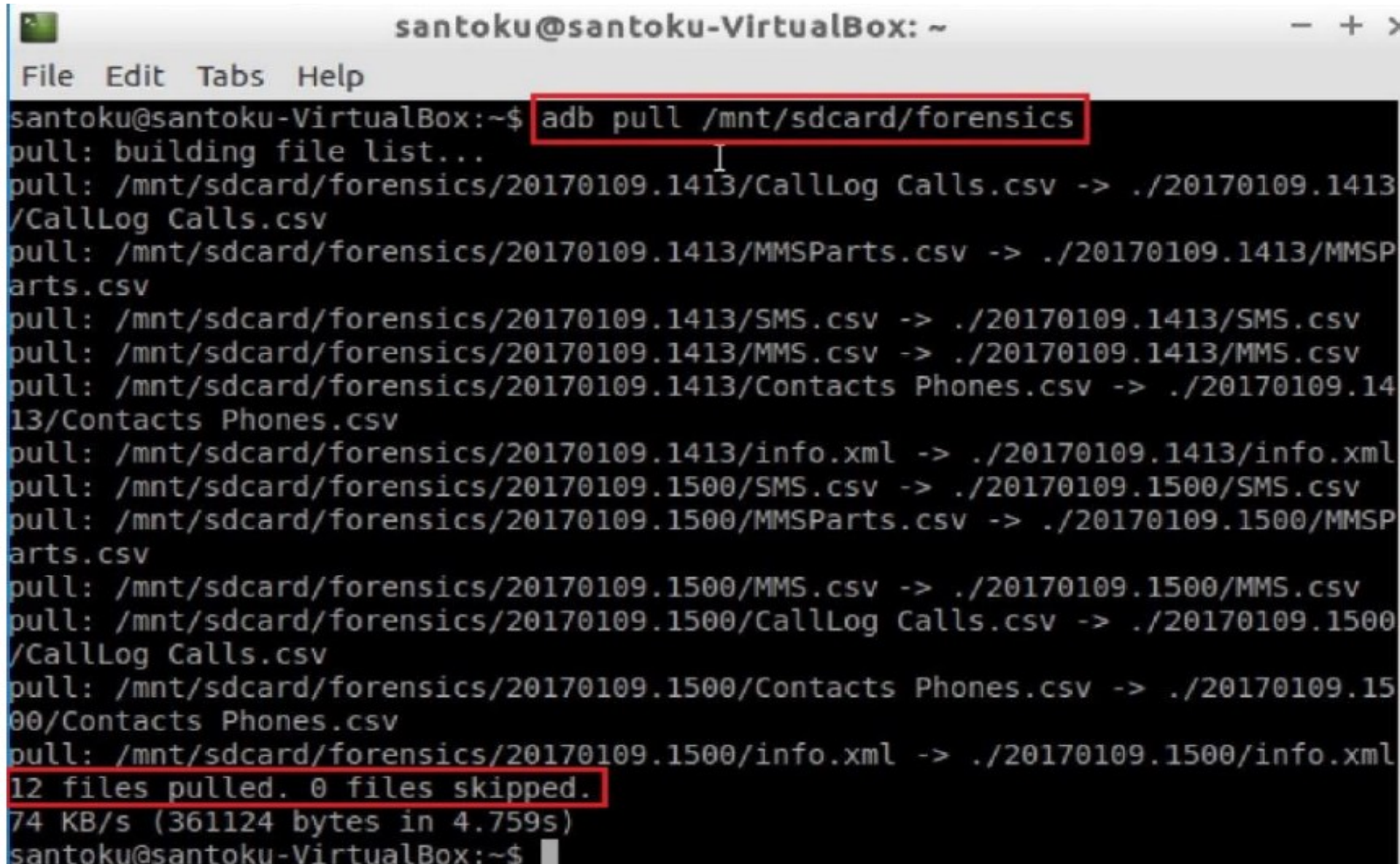
Source Type: Physical

[Drive Geometry]

Cylinders: 490

Tracks per Cylinder: 255

Verification Phase: Extracting Data



The screenshot shows a terminal window titled "santoku@santoku-VirtualBox: ~". The terminal has a menu bar with "File", "Edit", "Tabs", and "Help". The command prompt shows the user "santoku@santoku-VirtualBox" at the shell "~\$". The command `adb pull /mnt/sdcard/forensics` is entered and highlighted with a red box. The terminal output shows the process of pulling files from the virtual device's storage. It lists the files being pulled, including call logs, MMS parts, SMS, MMS, contacts, and info files for two different dates (20170109.1413 and 20170109.1500). The output concludes with "12 files pulled. 0 files skipped." and "74 KB/s (361124 bytes in 4.759s)". The final line shows the prompt "santoku@santoku-VirtualBox:~\$".

```
santoku@santoku-VirtualBox: ~  
File Edit Tabs Help  
santoku@santoku-VirtualBox:~$ adb pull /mnt/sdcard/forensics  
pull: building file list...  
pull: /mnt/sdcard/forensics/20170109.1413/CallLog Calls.csv -> ./20170109.1413/CallLog Calls.csv  
pull: /mnt/sdcard/forensics/20170109.1413/MMSParts.csv -> ./20170109.1413/MMSParts.csv  
pull: /mnt/sdcard/forensics/20170109.1413/SMS.csv -> ./20170109.1413/SMS.csv  
pull: /mnt/sdcard/forensics/20170109.1413/MMS.csv -> ./20170109.1413/MMS.csv  
pull: /mnt/sdcard/forensics/20170109.1413/Contacts Phones.csv -> ./20170109.1413/Contacts Phones.csv  
pull: /mnt/sdcard/forensics/20170109.1413/info.xml -> ./20170109.1413/info.xml  
pull: /mnt/sdcard/forensics/20170109.1500/SMS.csv -> ./20170109.1500/SMS.csv  
pull: /mnt/sdcard/forensics/20170109.1500/MMSParts.csv -> ./20170109.1500/MMSParts.csv  
pull: /mnt/sdcard/forensics/20170109.1500/MMS.csv -> ./20170109.1500/MMS.csv  
pull: /mnt/sdcard/forensics/20170109.1500/CallLog Calls.csv -> ./20170109.1500/CallLog Calls.csv  
pull: /mnt/sdcard/forensics/20170109.1500/Contacts Phones.csv -> ./20170109.1500/Contacts Phones.csv  
pull: /mnt/sdcard/forensics/20170109.1500/info.xml -> ./20170109.1500/info.xml  
12 files pulled. 0 files skipped.  
74 KB/s (361124 bytes in 4.759s)  
santoku@santoku-VirtualBox:~$
```

Directories after Aflogical-Data was Created



santoku@santoku-VirtualBox: ~

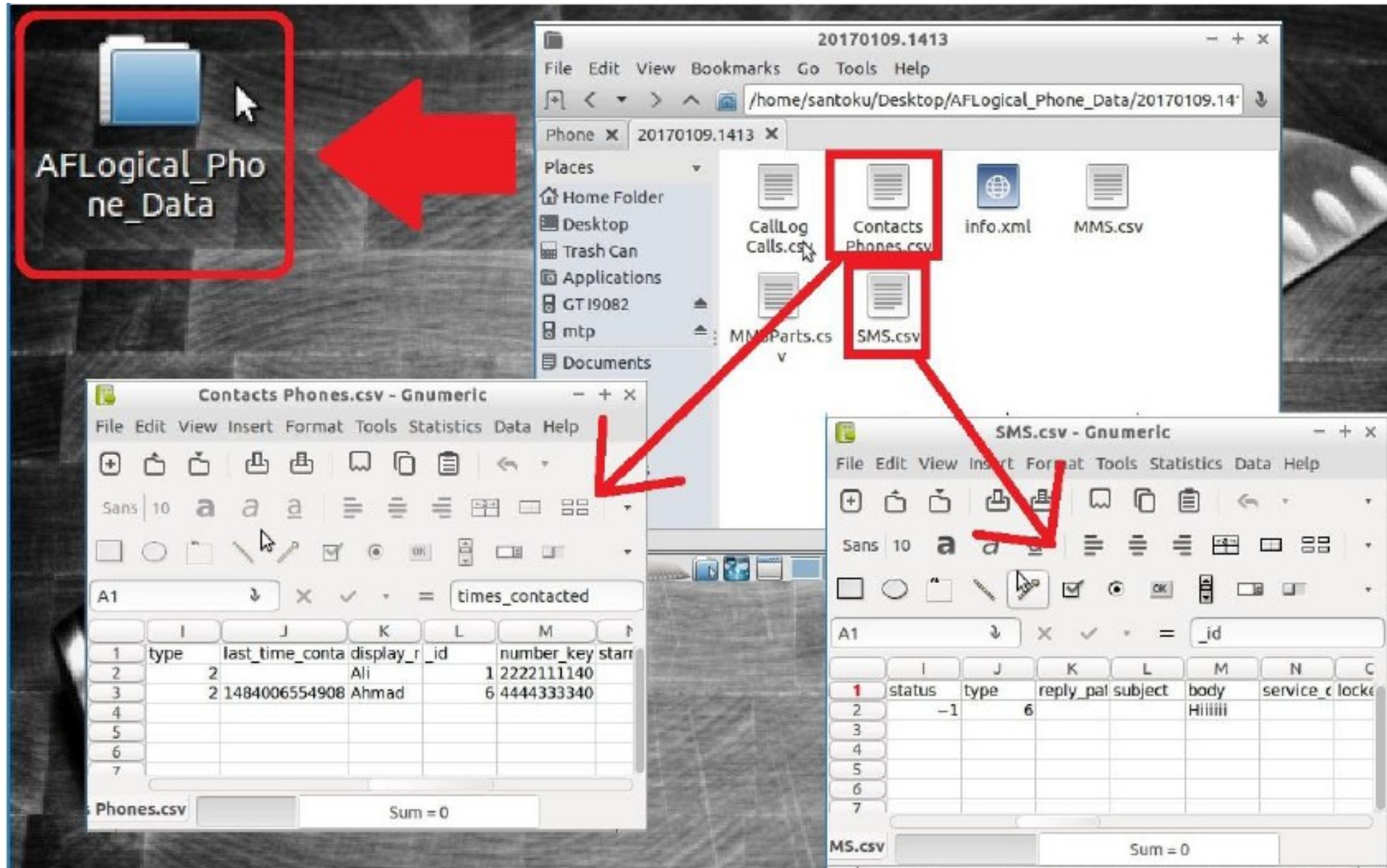
File Edit Tabs Help

```
santoku@santoku-VirtualBox:~$ ls
```

```
aflogical-data  Documents  Music      | Public      Videos
Desktop        Downloads  Pictures   Templates
```

```
santoku@santoku-VirtualBox:~$
```

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

AccessData FTK Imager 3.4.2.6

File View Mode Help

Evidence Tree

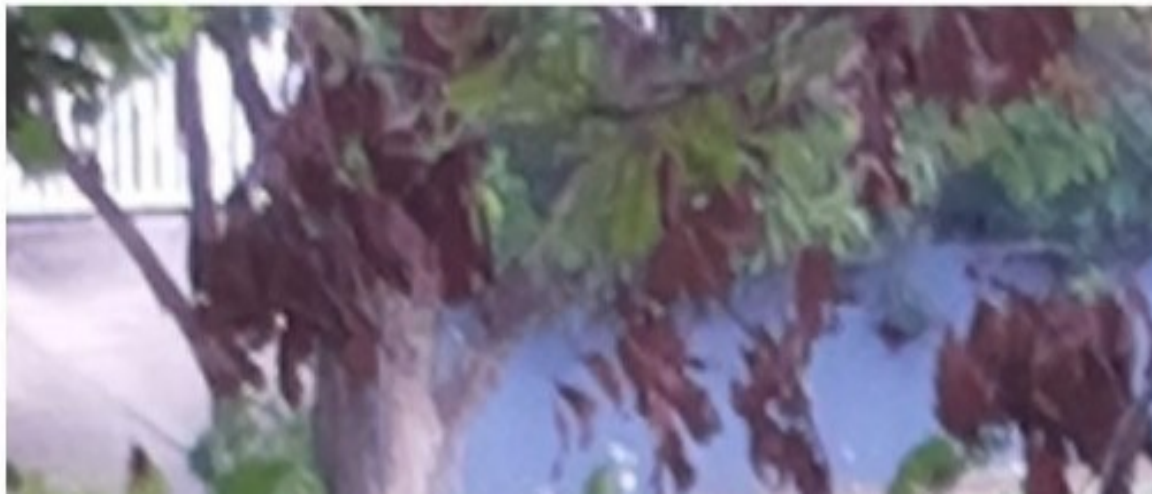
- SD_Backup.001
 - Partition 1 [3848MB]
 - BACKUP [FAT32]
 - [root]
 - Crad
 - DCIM
 - Camera
 - Phone
 - Alarms
 - Android
 - Application
 - DCIM
 - Camera
 - Documents
 - Download
 - Movies
 - Music
 - Notifications
 - Pictures
 - Playlists
 - Podcasts

File List

Name	Size	Type	Date Modified
20170109_072946.jpg	2,116	Regular File	9/01/2017 ...
20170109_073058.jpg	1,971	Regular File	9/01/2017 ...
20170109_073126.mp4	15,601	Regular File	9/01/2017 ...
20170109_073126.mp4.FileSlack	4	File Slack	
20170109_073214.mp4	11,237	Regular File	9/01/2017 ...

Custom Content Sources

Evidence:File S... Options



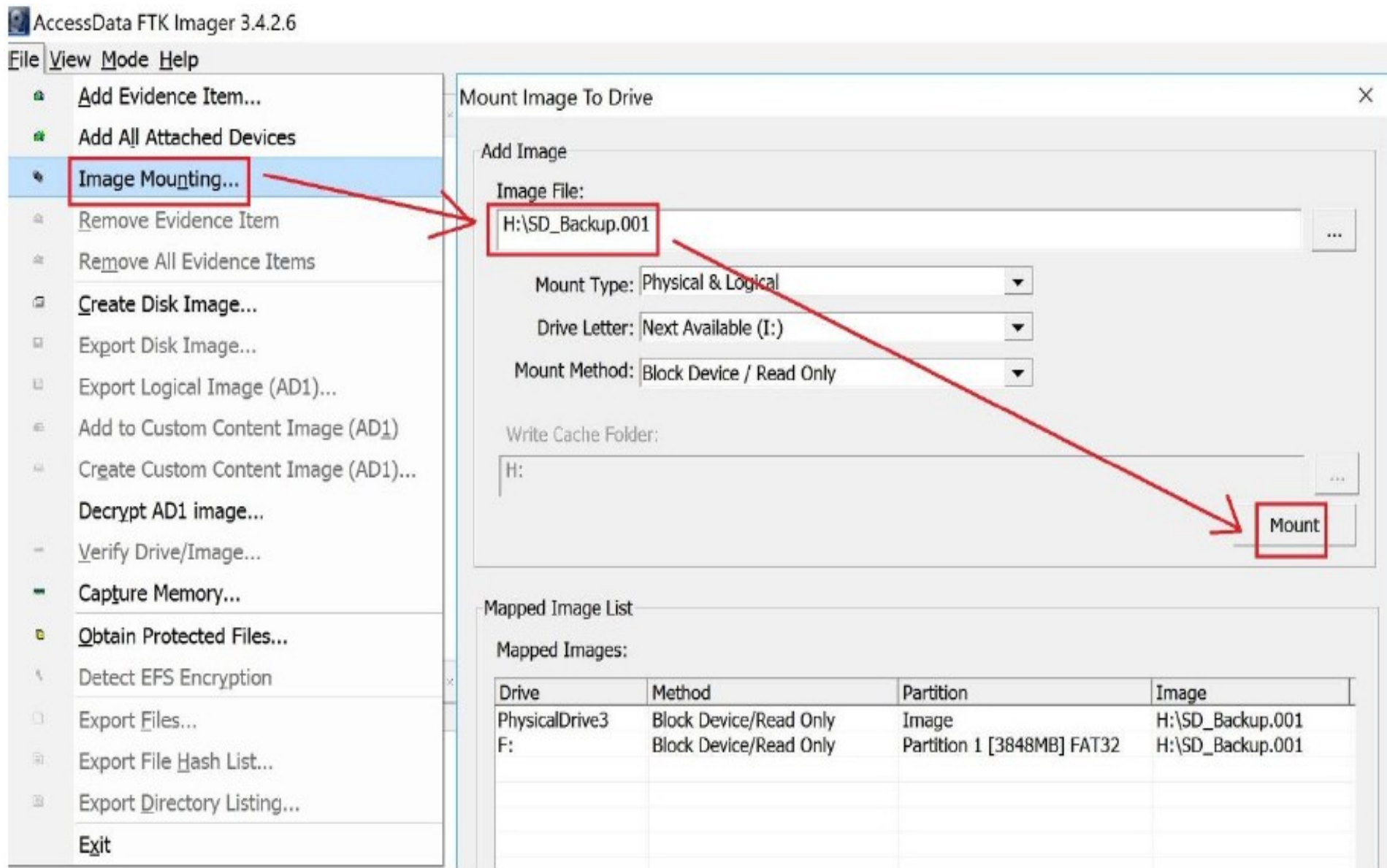
Physical Examination using Image Mounting in AccessData FTK Imager

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

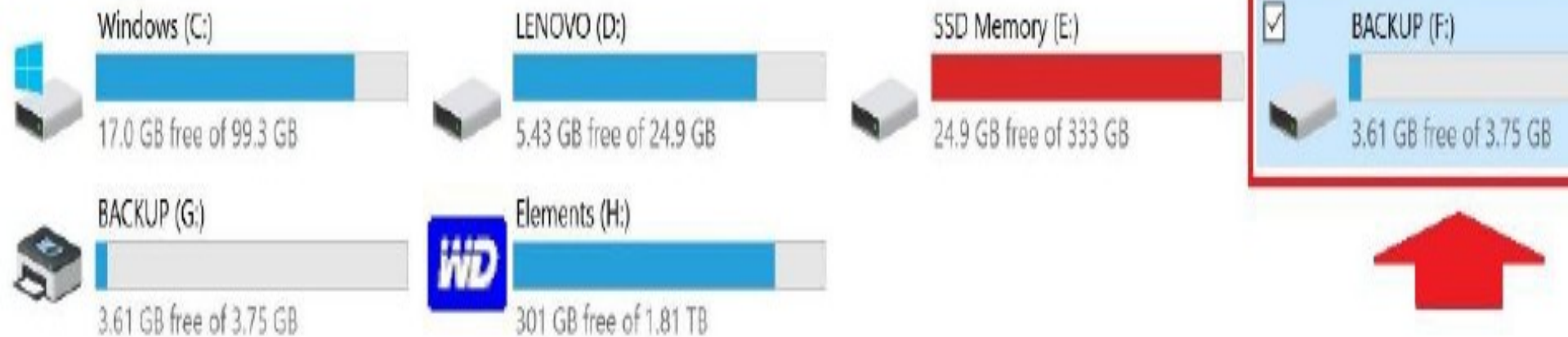


2. Mobile device files can then be explored in the new partition (F:)

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

✓ Devices and drives (6)



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	SMS/	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

