# Computer Forensics: Imaging & Integrity Verification of Digital Evidence

**Omveer Singh, GCFA**
**Additional Director**
**(In-charge, Cyber Forensics Lab)**

**Cyber Forensics Lab**
**Indian Computer Emergency Response Team (CERT-In)**
**Department of Information Technology**
**Ministry of Communications & Information Technology**
**Government of India**
**New Delhi**

# Agenda

- Imaging of Digital Evidence
- Write Blockers
- Wiping
- Integrity Verification
- References

# Imaging of Digital Evidence (Data Storage Media)

# Direct Analysis of Org. Digital Evidence : Strictly Forbidden

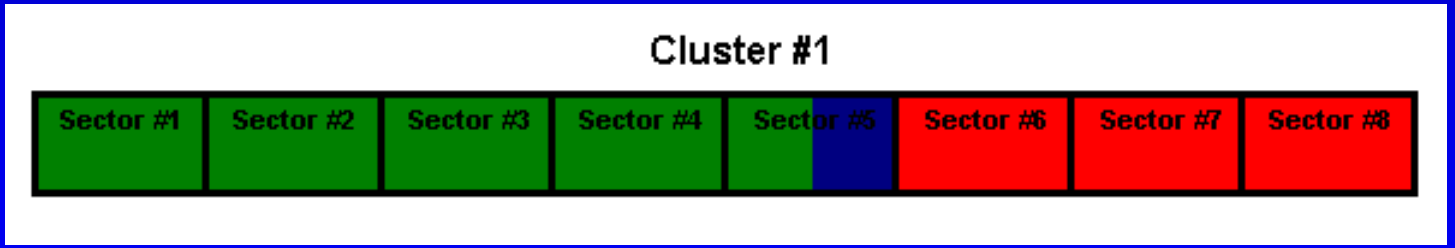
- Will change MAC (Modified, Accessed, Created) details (Date & Time) of a file
- Analysing a live file system / original evidence also changes the state of the evidence (MAC details)
- Analysis of the original digital evidence makes it a tampered digital evidence
- Such a tampered digital evidence will not be accepted by court and is useless
- Solution – analyse an identical copy (forensic image) of the original digital evidence

# Logical copy / backup of Hard Disk

- Back up or copy of a hard disk – copies only active files from the original hard disk and not all the data areas
- So ‘copy’ will not have all the data areas of the hard disk (digital evidence) for analysis; viz:
  - Deleted files (unallocated area)
  - Swap files
  - File slack

# Slack Space

- Green: Space used by the file for data storage (Sectors 1 to 5).
- Red: Unused sectors in the last cluster; called Slack Space or File Slack (Sectors 6 to 8)
- Blue: RAM Slack (Sector 5)




(1 Cluster = 8 Sectors = 8 * 512 Bytes = 4096 Bytes = 4 KB;

i.e. min. size of a file in **NTFS** on a hard disk)

# Logical Copy v/s Physical Copy

- **Logical copy**

  In a logical copy, the active directories and files only of a logical volume are copied. It does not capture other data that may be present on the media such as deleted files or residual data stored in the slack space.

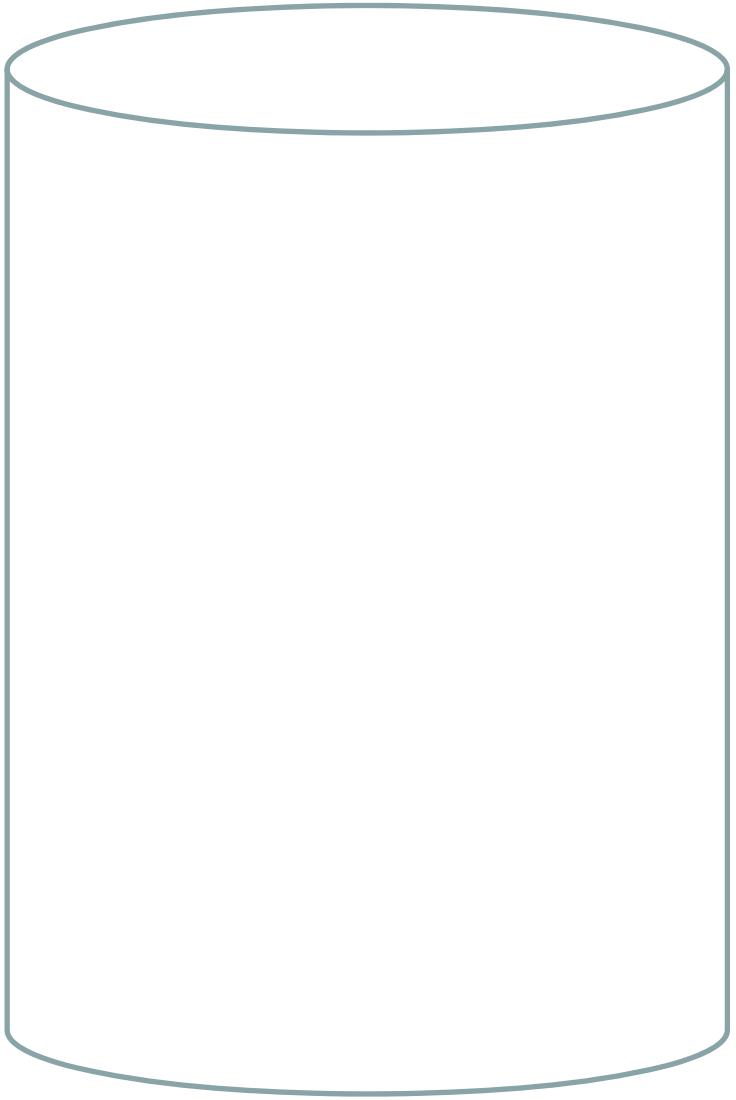
- **Physical copy (generally called forensic image, mirror image, image, or clone)**

  Generate a bit for bit copy of the original media; include free space and slack space.

# Copying of the Disk

**Suspected disk (Source)**


**Sterile disk (Target)**



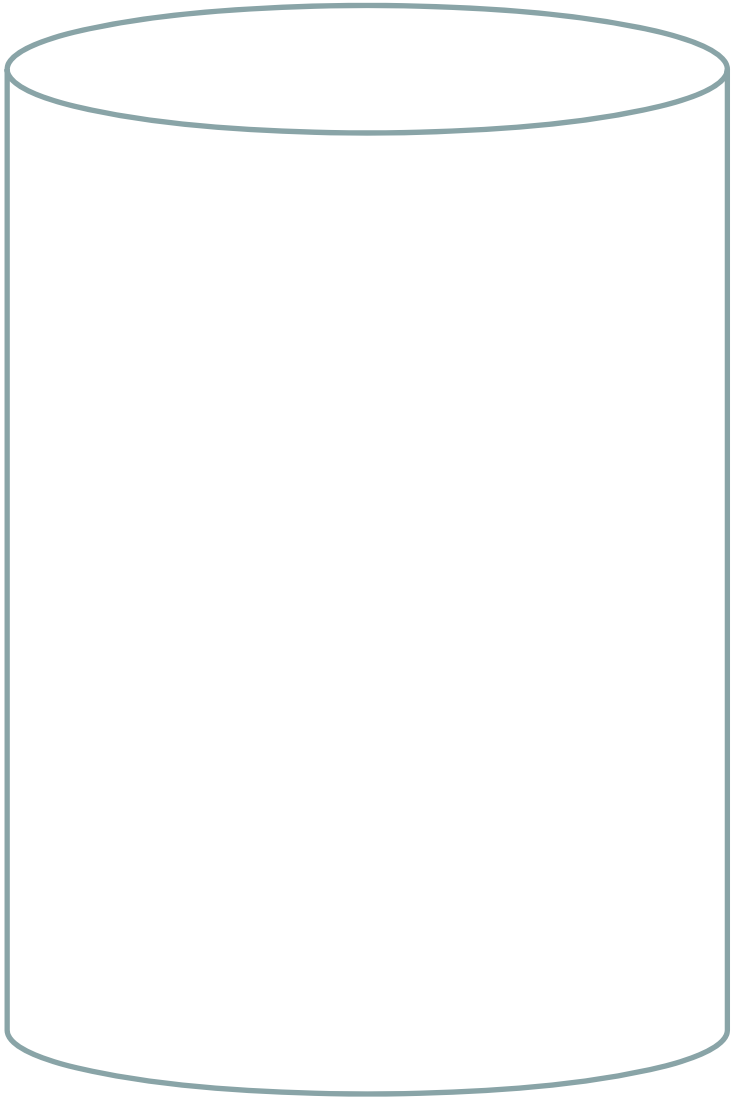
Active files

Deleted files

# Imaging of the Disk

**Suspected disk (Source)**


**Sterile disk (Target)**



Active files

Deleted files

# Advantage of an imaged Digital Evidence

- Analysing the image of the digital evidence will
  - Preserve the original evidence
  - Prevent inadvertent changes in the original evidence during examination
  - Another image may be created from original again, if required

# Imaging a Hard Disk?

- Maintain integrity & security of the org. evidence – use write protection devices during imaging
- It is a bit for bit, called ‘bit stream’ copy; there is no change in the sequence & location of data – an exact replica; storage may be on a different type of media
- Usually done by specific tools which copy sector by sector and makes a forensically sound copy of the original digital evidence
- Above means – swap file, unallocated space & slack space are also copied
- Time consuming process

# Disk imaging Tools Requirements

- The tool should make an identical bit-stream copy, generally called an image, of an original hard disk or its partitions.
- The tool should not alter the contents of the original hard disk.
- The tool should be able to verify the integrity of a hard disk's image file.
- The tool should log I/O errors, if any.
- The tool's documentation should be correct.

# Disk imaging Tools

- dd (linux, win)
- SafeBack (win)
- SnapBack DatArrest
- Drive Image Pro
- R-Drive Image
- DCFLdd
- IXimager
- Guymager

SW based imaging takes lot of time.

# Computer Forensic Toolkits: imaging SW with GUI

- TrueBack (C-DAC) - Freeware
- FTK Imager (AccessData) – Freeware
- Built-in feature in most of the computer forensic toolkits

# Disk Imaging Equipments (H/w)

- TrueImager (C-DAC)
- Talon (Logicube)
- Dossier (Logicube)
- Tableau
- Hard Copy 3 (Voom)

H/w based disk imaging equipments are faster; save time.

# Disk Imaging

Linux - Creating a disk images : Ex.

#dd if=/dev/hda of=hdisk1.img

DOS - Creating a disk images : Ex.

C:\>dd if=\\.\G: of=C:\GDrive.img --localwrt conv=noerror /v

# Disk Write Blockers

- Prevent writing of data to the suspect original drive
- Ensure the integrity of the suspect original drive
- Software Write Blockers v/s Hardware Write Blockers

# Hardware Write Blocker

- A hardware write blocker (HWB) is a device that is physically connected b/w the computer system and the hard disk (org. evidence) with the primary purpose of preventing (or 'blocking') writing to it
- Pass the signal to read data from hard disk and block the signal to write data to the hard disk


STABLEAU


DC IN A
USB 2.0
800
800
400
IDE
Power
IDE Detect
Host Detect
Write Block
Activity
DC
OUT

# Best Practices for imaging

- Always ensure that the integrity & security of the org. evidence is maintained.
- Suspected org. evidence (hard drive) must be connected through a write blocker.
- The destination disk should be a freshly wiped (sterilised) disk, even if it is new.
- Entire disk imaging should be preferred over the partition (Volume) wise imaging.
- Every action should be documented.

# Best Practices … (cont'd)

- Document the Make, Model, Serial No and Size of the hard disk into multiple forms like Chain of Custody, Seizure Note, etc as required
- Note down the size (or capacity) of the suspected (source) hard disk and always connect it through Hardware Write Blockers.
- Be cautious when you connect the SOURCE (org.) & DESTINATION (image) hard disks in the Forensic Imaging software / equipment
- Always select the Forensic Image as **raw** Image Type which could be acceptable by all – Freeware as well as Commercial Forensic S/w applications

# Best Practices … (cont'd)

- Get a sterilized hard drive (preferably new) of appropriate (Same or larger) size for storing the forensic image of the suspected hard drive; document its details e.g. Make, Model, Serial No. and Size.
- Once imaging (Acquisition) is over, document summary report of the acquisition process. (Acq. hash of the disk)
- On completion of the imaging process, disconnect the suspected (Source) hard disk and image (Destination) hard disk, label them carefully, preserve them separately into anti-static covers & store them in a safe location separately
- It is recommended to make three images.
- These should preferably be delivered by hand to a Cyber Forensic Lab and not by Post / Courier

# Hard disk Wiping Tools

- WipeDrive
- Sure delete
- Active@ KillDisk
- ObjectWipe
- Hard Disk Wipe Tool
- Autoclave
- Darik's Boot and Nuke (DBAN)
- Eraser

May take a few hours, according to size of a hard disk

# Scenario 1 (Dead Imaging)

- Hard Disk is detached from the suspected system.
- Both hard disks – source (org) & destination (image) are connected to the forensic work station (Laptop) in the lab.
- Launch forensic imaging application software, e.g. TrueBack (CDAC, Trivandrum) or FTK Imager (Access Data) or EnCase (Guidance software)

# Scenario 2 (Dead Imaging)

- Suspected system is used to make the image
- System hard disk (Org.) is not detached
- Destination Hard Disk (Image) is connected through Disk Controller or USB interface
- System is booted with bootable CD / USB Thumb Drive
- Imaging tool is run from bootable CD / USB Drive

# Scenario 3 (Dead Imaging)

- Applicable to cases, where hard disk detachment or its interface with lab forensic workstation is not available
- Suspected machine is booted with the Forensic Live CD (bootable)
- Connect Forensic Workstation to the suspected system through a crossed RJ45 LAN cable and ensure connectivity of the two systems
- Destination disk is connected to the Forensic Workstation
- Imaging S/w is run from Forensic Workstation

# Scenario 4 (Live Imaging)

- Applicable to Live Systems of critical importance, e.g. servers, etc; which are supposed to be always on; can't be stopped for a few hours to detach the hard disk for having its image
- Live Image Acquisition of the of the Suspected System's hard disk is done through Forensic Live CD (Helix) or FTK Imager (installed on USB Thumb drive).
- Forensic Live CD (Helix) or USB Thumb Drive is inserted in the suspected system and executed

# Scenario 4 (Live Imaging) (cont'd)

- Destination Hard Disk is connected to the suspected system through disk controller card or USB interface
- On a running system, hard disk data will be in dynamic state. The process can be repeated but the results will never be the same.
- In Live Acquisition, hash values of the acquired image can not be verified with the org. hard disk, since the suspected system's operating system was working during the Forensic Imaging of its hard disk

# Scenario 5 (Remote Imaging)

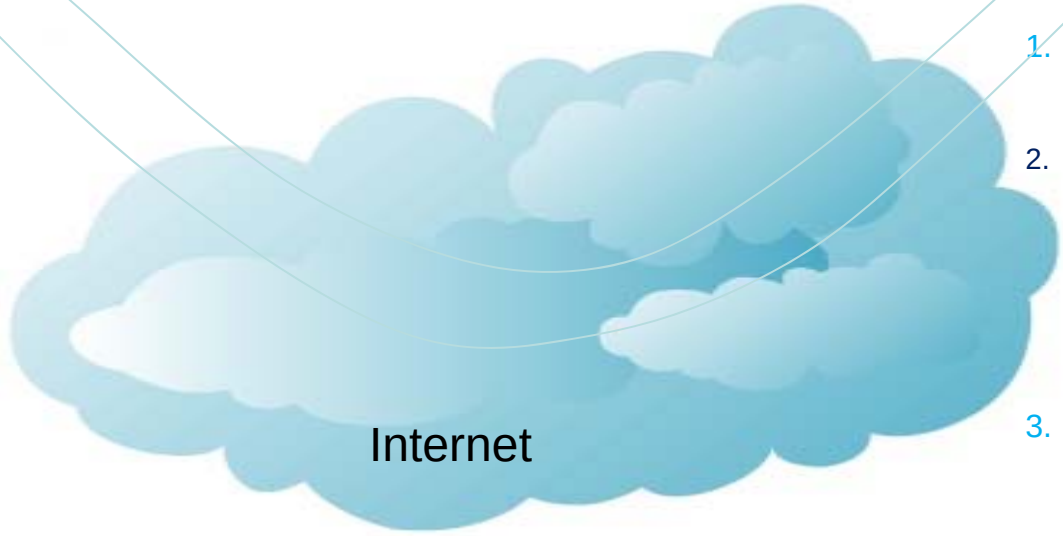
- Law Enforcement agencies sometimes face difficulty that the suspected machine is located in a remote location like beyond country borders, etc; where sending one person for imaging a hard drive is a costly affair.
- Forensic Live CD (Helix) is run in the suspected system (remote location)
- Another Forensic Live CD (Helix) is run at the lab's Forensic workstation (local machine) having destination drive connected to it
- Both the machines are connected to internet (public network)
- Will take a long time to complete, depending on size of hard drive and BW of public network.

**Local Machine (Forensic Lab)**
**IP**: 185.141.12.9 **Port**: 2222

1. Listen on specified IP & Port -
2. Ex. nc -v -n -L -p 2222 -s 202.141.12.9 -decomp lznt1 -O h:\servername\filename.img –localwrt
3. Receive through SSH
4. Write image files on your machine

**Remote Machine**
**IP**: 202.141.12.9 **Port**: 2222

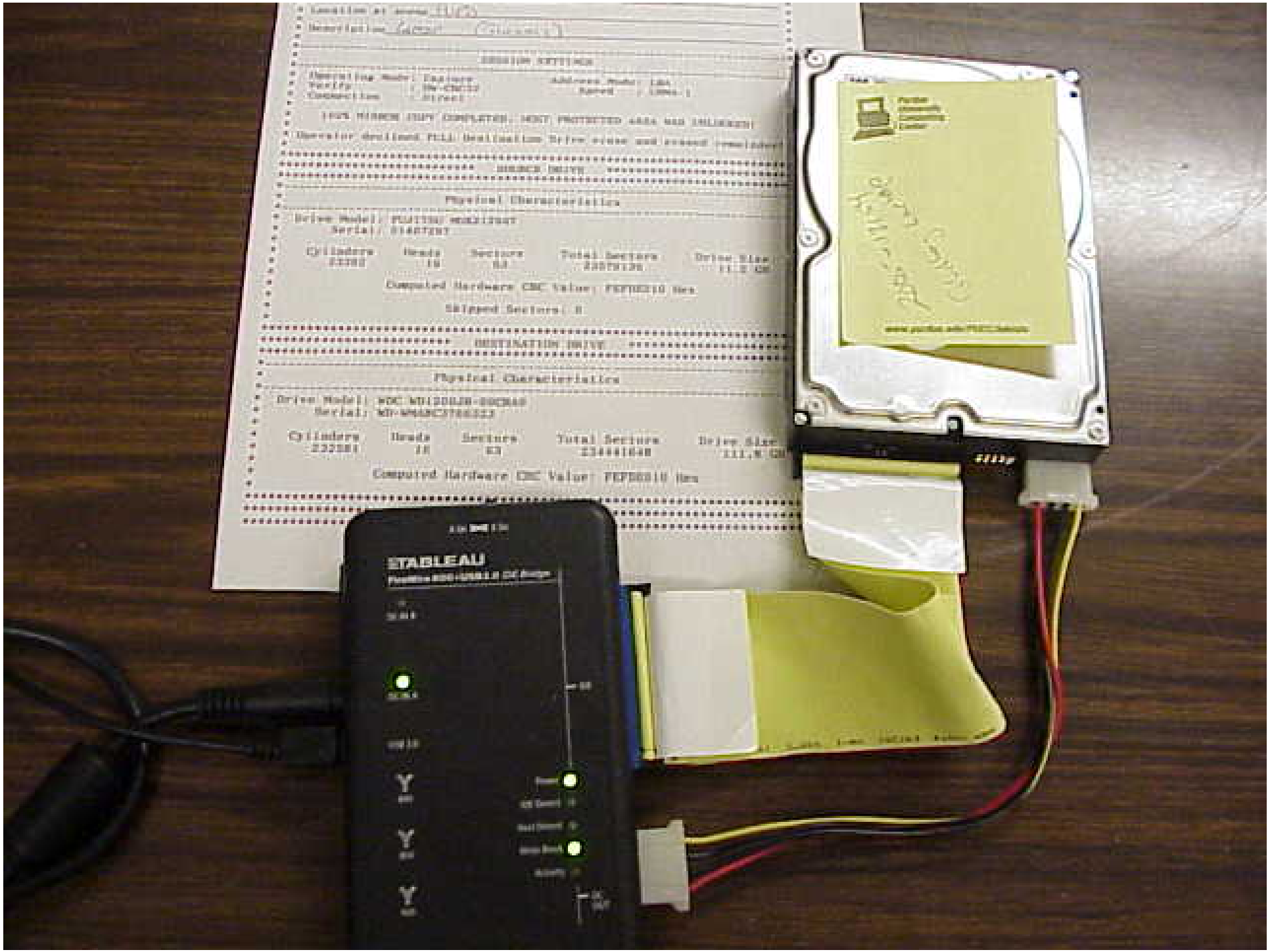
1. Load Forensic Live CD (Helix ) & execute DD ex:
2. dd.exe -v if=\\.\F: of=185.141.12.9 conv=noerror --iport 2222 --comp lznt1 --log --cryptsum md5 --cryptsum sha1
3. Send through SSH



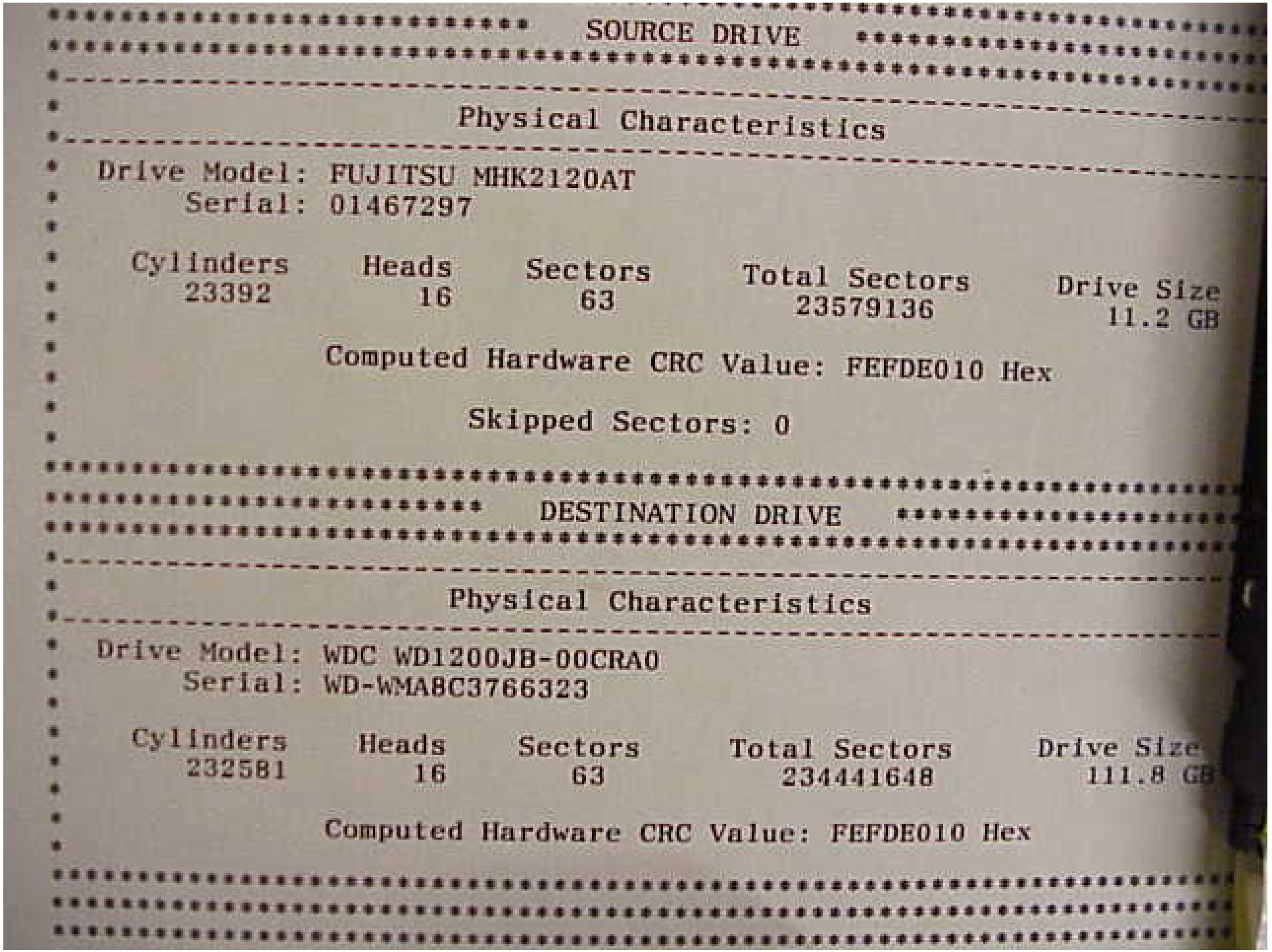

**Remote Forensic Imaging over Internet**

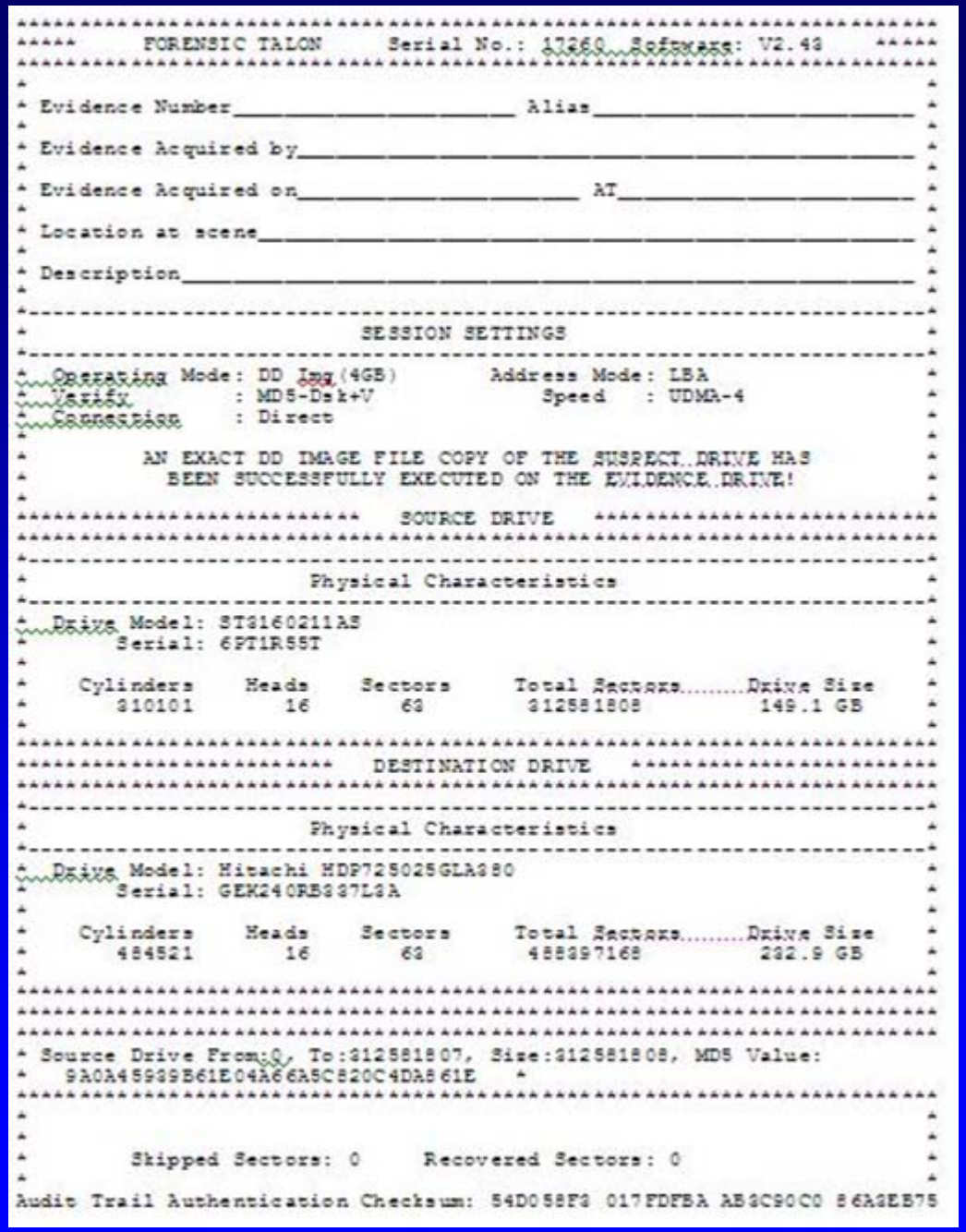
# Drive Imaging Hardware

- Forensic mobile field system (MFS)
  - Laptop with NIC
  - Portable workstation


SESSION STATISTICS
Operating Mode: Capture
Verify : ON-CRC32
Connection : Direct
Address Mode: LBA
Speed : 10Mb/s
100% MIRROR COPY COMPLETED. HOST PROTECTED AREA WAS UNLOCKED!
Operator declined full Destination Drive erase and erased (remainder)
SOURCE DRIVE
Physical Characteristics
Drive Model: FUJITSU MHA2120AT
Serial: 01407287
Cylinders 23282 Heads 16 Sectors 63 Total Sectors 23579136 Drive Size 11.2 GB
Computed Hardware CRC Value: FEFD0210 Hex
Skipped Sectors: 0
DESTINATION DRIVE
Physical Characteristics
Drive Model: WDC WD1200JB-00CBA0
Serial: WD-WMA8C3760323
Cylinders 232581 Heads 16 Sectors 63 Total Sectors 234441648 Drive Size 111.8 GB
Computed Hardware CRC Value: FEFD0210 Hex
STABLEAU


Logicube
SF-5000i
LOGICUBE FORENSICS HARD DRIVE CAPTURE SYSTEM
BACK
ERROR
STATUS
POWER
SELECT
HELP
START
STOP
SET


SOURCE DRIVE
Physical Characteristics
Drive Model: FUJITSU MHK2120AT
Serial: 01467297
Cylinders 23392
Heads 16
Sectors 63
Total Sectors 23579136
Drive Size 11.2 GB
Computed Hardware CRC Value: FEFDE010 Hex
Skipped Sectors: 0
DESTINATION DRIVE
Physical Characteristics
Drive Model: WDC WD1200JB-00CRA0
Serial: WD-WMA8C3766323
Cylinders 232581
Heads 16
Sectors 63
Total Sectors 234441648
Drive Size 111.8 GB
Computed Hardware CRC Value: FEFDE010 Hex



```
*****      FORENSIC TALON      Serial No.: 17260  Software: V2.48     *****

Evidence Number_____________________ Alias_____________________

Evidence Acquired by_____________________________________________

Evidence Acquired on_____________________ AT_____________________

Location at scene________________________________________________

Description______________________________________________________

                          SESSION SETTINGS

Operating Mode: DD Img(4GB)        Address Mode: LBA
Verify          : MD5-Dsk+V            Speed    : UDMA-4
Compression     : Direct

         AN EXACT DD IMAGE FILE COPY OF THE SUSPECT DRIVE HAS
           BEEN SUCCESSFULLY EXECUTED ON THE EVIDENCE DRIVE!

*************************    SOURCE DRIVE    *************************

                      Physical Characteristics

Drive Model: ST3160211AS
       Serial: 6PT1R55T

    Cylinders     Heads     Sectors     Total Sectors.....Drive Size
       310101        16        63         312581808          149.1 GB

************************    DESTINATION DRIVE    ************************

                      Physical Characteristics

Drive Model: Hitachi HDP725025GLA380
       Serial: GEK240RB337L3A

    Cylinders     Heads     Sectors     Total Sectors.....Drive Size
       484521        16        63         488397168          232.9 GB

* Source Drive From:0, To:312581807, Size:312581808, MD5 Value:
*   9A0A45939B61E04A66A5C820C4DA861E   *

Skipped Sectors: 0     Recovered Sectors: 0

Audit Trail Authentication Checksum: 54D058F3 017FDFBA AB3C90C0 86A3EB75
```

# Integrity Verification (Authentication)

# Integrity of Digital Evidence?

- Digital data is vulnerable to intentional or unintentional changes
- Integrity of digital evidence is required to be maintained, starting from seizure till analysis
- Forensic examiners require a tool to test / verify if the digital evidence is modified during the computer forensic analysis process.
- To do this, a unique digitized tag of a digital evidence is required to verify its integrity
  - A fingerprint of the digital evidence could be only its digest

# Data Hash / Checksum

- A hash function is a well-defined mathematical cryptographic hash algorithm for calculating the digest of data (evidence as a file) into a hexadecimal integer. The values returned by a hash function are called hash values, hash codes, checksums, message digest or hashes.
- Like a fingerprint of a file
- Can not provide any detail of the evidence (file)
- If evidence is modified in anyway, its hash value will also change.
- MD5 (128 bit), SHA-1 (160 bit)

# Verification of integrity of Evidence

- Original evidence, once identified should always be used only with write blockers for avoiding the inadvertent writing of data to it and compute its MD5 hash value
- On acquisition of an original evidence, immediately make its forensic image (using write blocker) and compute the MD5 hash value of its image.
- For storing a forensic image of a hard disk (evidence) always use freshly wiped hard disk.
- It is recommended to make two images of original evidence and authenticate these by verifying their MD5 hash values with that of the original evidence

# Integrity of Digital Evidence

Integrity verification of digital evidence through checksum / hash value –

- MD5 (Message Digest Algo.) Ver. 5
  - 128 bits (32 Hex Digits)
- SHA1 (Secured Hash Algo.)
  - 160 bits (40 Hex Digits)

# Tools for Integrity Verification

- md5sum (dos, linux)
- md5 (win)
- md5summer (win)
- Hashcalc (win)

Built-in facility in most of the disk imaging utilities

Name: test
Description: Physical Disk, 2047998 Sectors, 1000MB
Logical Size:
Physical Size: 512
Starting Extent: 0S0
File Extents: 1
Physical Location: 0
Physical Sector: 0
Evidence File: test
Full Path: Case 1\test
File Extents

| Start Sector | Sectors | Start Cluster | Clusters |
|---|---|---|---|
| | 1 | | |

**Device**

Evidence Number: exampleforjudicials90
File Path: C:\Documents and Settings\Administrator\Desktop\babu\test\test.E01
Examiner Name: Omveer Singh and Subrahmani Babu
Actual Date: 09/18/08 12:36:07PM
Target Date: 09/18/08 12:36:07PM
Total Size: 1,048,574,976 bytes (1000MB)
Total Sectors: 2,047,998
File Integrity: Completely Verified, 0 Errors
EnCase Version: 4.20
System Version: Windows XP
Acquisition Hash: 2F17E82931D9CF04E6D6DCEC0DD7E96C
Verify Hash: 2F17E82931D9CF04E6D6DCEC0DD7E96C

**Partitions**

| Code | Type | Start Sector | Total Sectors | Size |
|---|---|---|---|---|
| 06 | BIGDOS | 0 | 2,047,998 | 1000MB |

# References


- “Electronic Fingerprints – computer evidence comes of Age” by Michael R. Anderson
- “Electronic Crime Scene Investigation – A Guide for First Responders” by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- “Forensic Examination of Digital Evidence : A guide for Law Enforcement” by National Institute of Justice, USA; (http://www.ojp.usdoj.gov/nij)
- “Forensics – Tools”; http://www.forinsect.de/index.html
- Training Material on Information Security by Carnegie Mellon University, Pitsburgh, USA

# References (contd..)

- Collecting Electronic Evidence After a System Compromise" by Matthew Braid, SANS Security Essentials.
- "Computer Forensics – An Overview" by Dorothy A. Lunn, SANS Institute; http://www.giac.org/practical/gsec/Dorothy_Lunn_GSEC.pdf
- "Manual for Investigation of Computer Related Crimes" by Ashok Dohare
- Course Contents : SANS SEC508

# Questions?


Thanks!