



# WORKING PROCEDURE MANUAL COMPUTER FORENSICS



**DIRECTORATE OF FORENSIC SCIENCE SERVICES**  
**MINISTRY OF HOME AFFAIRS, GOVT. OF INDIA**  
**BLOCK NO. 9, 8<sup>TH</sup> FLOOR, CGO COMPLEX**  
**NEW DELHI - 110 003**

**Website: [dfs.nic.in](http://dfs.nic.in), Email: [cfs-dfss@nic.in](mailto:cfs-dfss@nic.in)**

**2022**

**NOTE:** This manual is solely a property of DFSS, New Delhi for use in its quality system only. Any other use or reproduction of it in part or whole by anyone else is not permitted and will not be binding on the laboratory.

डॉ. एस. के. जैन

निदेशक-सह-मुख्य न्यायालयिक वैज्ञानिक

Dr. S.K. Jain, M.Sc Ph.D

Director-cum-Chief Forensic Scientist



सत्यमेव जयते

न्यायालयिक विज्ञान सेवा निदेशालय,

गृह मंत्रालय, भारत सरकार

ब्लॉक-9, तल नं. 8, केन्द्रीय कार्यालय परिसर

लोधी रोड, नई दिल्ली-110 003

Directorate of Forensic Science Services,

Ministry of Home Affairs, Govt. of India

Block No. 9, 8th Floor, C.G.O. Complex

Lodhi Road, New Delhi-110 003 (India)

Tel. : 011-24362676 Fax : 011-24362819

E-mail : cfs-dfss@nic.in

## PREFACE

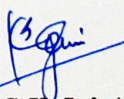
The analytical procedures for examination of forensic physical clue materials in forensic science laboratories involve a high degree of skill and expertise and play a significant role in a wide range of legal proceedings. The occurrence of errors in any of the forensic analytical activities is a serious matter for both the laboratories as well as for the end users. For the laboratory, it can lead to re-testing of samples, if available, and loss of the credibility of laboratory. The analytical techniques adopted by the scientist (s) for the forensic analysis may be one of the causes for this serious error.

The risk of committing error can be eliminated if the scientists undertake two or more independent validated techniques while undertaking forensic analysis of crime case exhibits in the laboratory. Essentially, the procedures adopted must conform to the quality, sensitivity, repeatability and reproducibility of the examination so that the chances of error are absolutely avoided. It is, therefore, one of the essential requirements of good laboratory practices to introduce a Laboratory Procedure Manual, which contains validated laboratory methods/techniques for forensic analysis of the exhibits. It is also necessary that all the Central/State Forensic Science Laboratories uniformly follow these manuals in the country.

Keeping in view the advancement in science & technology and use of various protocols & procedures in the international arena of forensic science, Directorate of Forensic Science Services (DFSS) has taken the initiative for preparing a systematic and comprehensive working procedure manual for the 'Forensic Ballistics' to bring uniformity and standardization in the examination methods. In this regard, this Directorate formed Scientific Working Groups, comprising eminent forensic scientists of the CFSLs and FSLs for each forensic discipline to compile forensic analytical techniques in the form of Laboratory Procedure Manuals. Several meetings were conducted with detailed deliberations among the scientists at National level and finally the manual has been prepared /updated in the present form.

I am sure that this Laboratory Procedure Manual, which pertains to the discipline of 'Computer Forensics' will help the Forensic laboratories to continue to follow standard and latest updated procedures in the examination of clue materials as well as to adopt quality control/ quality assurance in the forensic practices and also for obtaining accreditation from NABL.

I understand that there is always a scope of improvement and perfection can be achieved with collective efforts, therefore, stakeholders are welcome to give their feedback and suggestion, if any, in this regard.

  
( Dr S K Jain)

Director-cum-Chief Forensic Scientist



<b>Sr. No.</b>	<b>Chapter</b>	<b>Pages</b>
	Scope	2
1	Reference Document	2
2	Significance and use	3
	2.1: Computer Forensics	3
3	Procedure	4
	3.1: Equipment and system requirement	4
	3.2: General forensic principle	4-5
	3.3: Evidence acquisition manner	6
	3.4: Shutdown procedure while preserving evidence	7-9
	3.5: Acquiring a drive safely	10
	3.6: Disc imaging	11
	3.7: Collecting volatile data	12
	3.8: Evidence analysis	13
	3.9: Timeframe analysis	14
	3.10: Data hiding analysis	14
	3.11: Application and file analysis	15
	3.12: Ownership and Possession	15
	3.13: Hard Disc Examination	16
	3.14: Floppy disc Examination	16-17
4	Documenting and Reporting	18
5	Evaluation and Interpretation of results	19
6	Reporting conclusions	19
7	Case records	19
8	Quality control checks	19
	9.1: Technical Review	19
	9.2: Proficiency testing / Inter-laboratory comparison	19
9	Appendix – A: Acronyms	20
	Last Page	

## **SCOPE**

This procedure is intended to assist the computer forensics experts in forensics imaging and analysis of digital evidence in the form of magnetically, optically, or electronically stored media.

## **1. REFERENCE DOCUMENTS**

**1.1** Following documents have been used for preparation of this document:

- Quality Manual, Doc. No. 01.
- Health and Safety Manual, Doc. No. 23.
- Standard Practice for Receiving, Documenting, Storing and Retrieving Evidence in a Forensic Science Laboratory, ASTM E 1459-92.
- General Requirements for the Competence of Testing and Calibration Laboratories, ISO/IEC 17025, International Organization for Standardization, 1999.
- NABL 113: 2008 ‘Specific Guidelines for Forensic Science Laboratories
- IOCE Publication - Guidelines for Best Practice in the Forensic Examination of Digital Technology.
- Guidance Software Inc. Pasadena, CA 91101 Publication - EnCase Version 3.0, Manual Revision 3.18 by Richard Knightly.
- Guidance Software Inc. Pasadena, CA 91101 Publication - EnCase Version 4.19A, Manual Revision 4.08 by Richard Knightly.
- Guidance Software Inc. Pasadena, CA 91101 Publication - EnCase Version 6.2, Manual Revision 4.08 by Richard Knightly

## **2. SIGNIFICANCE AND USE**

### **2.1 Computer Forensics:**

a) The process of acquiring and analysing the data stored on some form of physical storage media. It involves processes and procedures whereby the acquired data is not corrupted during handling and is acceptable to the court of law. It includes the recovery of hidden, deleted data, file identification etc.

b) Computer forensics involves analysis of two types of digital data. First, the transmitted data in which the information is gathered through internet and second, the fragile data in which the data is stored in the electronic, optical or magnetic storage media such as hard disks, floppy disks which can be easily altered. This type of examination yields qualitative output and excludes from calibration of equipment or estimation of uncertainty of measurement. Use of the guideline adopted in this document will provide more information with least damage to the evidence. Rapidly changing technology encountered in casework will require periodic revisions.



### 3. PROCEDURE

#### 3.1 Equipment and System Requirements

a) Only properly evaluated tools, techniques and procedures should be used for Computer forensics. Computer forensics software application should meet or exceed the following requirements.

- Read any IDE OR SCSI hard drive or CD-ROM and save exact snapshot of the disk to an Evidence File,
- Password cracker (NTI TOOLS),
- View the entire drive image, including hidden and unallocated disk space and partitions and search it for keyboards,
- View files without changing the date time stamp and file contents,
- Analyze the folder and file structure,
- Combine any number of evidence files or folders to create the evidence,
- Have all evidence, searches, and bookmarks recorded on the typeset report,
- Analyze and authenticate the file signatures to find those that have been renamed to conceal their contents,
- Build in picture viewer and gallery view,
- Ability to acquire and preview via network cable,
- Build in picture viewer for registry files, ZIP files and DBX(outlook express files),
- En Case Version 3.0,4.19A,6.2,8.08 Manual Revision 3.18
- FTK version 6.4
- Stego tool, and
- CDAC tools.

b) Particular model or brand of a computer is not recommended. A good laboratory analysis machine should also have a “computer forensic friendly” basic Input and output systems (BIOS). The laboratory analysis machine (the Forensic PC) should meet or exceed the following system requirements.

- Windows 98, ME, 2000, XP, or NT 4.0 operating system, window vista, windows 7,8 and 10;
- Pentium/i5/i7/Xeon processor
- **2GB of RAM** or higher recommended;
- 100GB or more free disk space;
- VGA/LCD/LED/OLED/ monitor;
- Sound card, graphic card and speakers;
- Parallel/ or USB ports.

c) All equipment are to be maintained in accordance with the manufacturer's specifications and recommendations as per operating manuals. Maintenance is to be documented and retained in the appropriate log book located in the respective laboratory.

#### 3.2 General Forensic Principle

a) Appropriate anti-contamination precautions should be taken to minimize any chance of accidental contamination of items. Consideration of what anti-contamination precaution to take should be based not only on the digital evidence media and devices, but also on the other evidence types which may be potentially available. Care should be taken when handling evidence to document any suspicion of the presence of potentially dangerous or sensible substance on the material.

b) Crime scenes should be searched systematically and thoroughly during recovery of digital evidence and related material targeting and prioritising areas, which in the context of what has been alleged, are most likely to contain material of evidential significance.

c) Digital evidence items should be examined in the laboratory rather than at the scene. The digital evidence may have to be copied at the scene, where it is impracticable to recover the items for examination for laboratory examination.

d) The laboratory rules of evidence management should be applied to all digital evidence. It is essential to understand the case examination requirements and the associated legal authority. This should be expressed in terms of what the client is seeking to establish rather than a menu of tasks to be carried out.

e) All items submitted for forensic examination should be reviewed for the integrity of their packaging. Any deficiency in the packaging should be documented. The other types of forensic examination, which may have to be carried out on the same items must be checked.

f) An individual is responsible for all actions taken with respect to digital evidence whilst the digital evidence is in their possession. Responsibility for maintaining evidential value and provenance is a personal, not organizational issue. If an individual has acknowledged responsibility for an item by signing an access log, he is responsible for all actions taken in respect of that item until such time as it is returned to store or formally transferred to another individual.

g) All activity relating to the evidence access, examination process, storage and transfer of digital evidence must be documented, preserved and available for review.

h) Any anti-contamination precautions or requirements of the particular examination must be considered before any examination proceeds.

i) Health and safety considerations are extremely important in the work carried out at all stages of the forensic process. All elements of health and safety program of the laboratory should be followed in the examination of digital evidence. Personnel engaged in the examination of various forms of digital technology should operate in accordance with the regulations of the agency. All personnel involved in examinations should take adequate precautions to preserve any evidentiary material from external factors such as electrical hazards.

j) Forensic workspace for the examination of digital technology items should be equipped for efficient, secure, safe and effective use. Particular attention needs to be given to the management of the variety of trailing electrical cables and environmental conditions. Forensic workspace temperature, during examination of digital technology, should be maintained as per the recommendation of the manufacturers of the laboratory analysis equipment.

k) Read the laboratory analysis equipment manufacturer's instructions. During each step of Computer forensic imaging and analysis procedure, the forensic tools should be used in the manner recommended by the manufacturer.

l) The cardinal rules of Computer forensics are:

- Never mishandle the evidence.
- Never work on the original evidence.
- Never trust the SUBJECT'S operating system
- Document all the findings.
- Results should be repeatable, reproducible and verifiable by third party.



- m) Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
- n) Persons conducting an examination of digital evidence should be trained for that purpose.
- o) Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.
- p) Evidence Authentication: Mirror image obtained is authenticated by taking its “hash” value which is making sure that the mirror image is same as that of the suspect storage device.
- q) Evidence Analysis: Analysis is the process of interpreting the extracted data to determine their significance to the case. A thorough analysis should be done either directly on the image or use the image to make another copy of the media to be examined. Whether to examine the image directly or use it to make another copy of the media is almost entirely dependant on the facts and circumstances of the specific case and the tool selected for the imaging process.
- r) The analysis methodology will be decided by referring the investigating agency’s terms of references, tools and test methods adopted. This method will be validated through peer group interaction or through internet search.

### **3.3 Evidence Acquisition Manner**

- a) Recognizing the fragile nature of the digital data, the evidence should be acquired/preserved against accidental or intentional manipulation, usually by making a bit stream mirror image of the media on a sterile media of capacity larger than the evidence media. The sterile media will be provided either by the investigating agency or the laboratory would itself buy through its normal purchase procedures. Procedure for purchase, handling, storage preservation and delivery of test samples/ exhibit refer executive procedure manual.
- b) Acquire the original digital evidence in a manner that protects and preserves the evidence. The basic steps are:
  - Document hardware and software configuration of the examiner’s system.
  - Verify operation of the examiner’s computer system to include hardware and software
  - Disassemble the case of the computer to be examined to permit physical access to the storage devices.
  - Take care to ensure equipment is protected from static electricity and magnetic fields
  - Identify storage devices that need to be acquired. These devices can be internal, external, or both
  - Document internal storage devices and hardware configuration.
  - Drive condition (e.g., make, model, geometry, size, jumper settings, location, and drive interface).
  - Internal components (e.g., sound card, video card, network card, including media access control (MAC) address, personal computer memory card international association (PCMCIA) cards etc.).
  - Disconnect storage devices (using the power connector or data cable from the back of the drive or from the motherboard) to prevent the destruction, damage, or alteration of data.
  - Retrieve configuration information from the suspect’s system through controlled boots.
  - Perform a controlled boot to capture CMOS/BIOS information and test functionality.
  - Ascertain Boot sequence (this may mean changing the BIOS to ensure the system boots from the floppy or CD-ROM drive).
  - Note down Time and date as indicated by the suspect’s system.

- Obtain Power on passwords from the suspect or note down tools & methods used for its extraction.
- Perform a second controlled boot to test the computer's functionality and the forensic boot disk.
- Ensure the power and data cables are properly connected to the floppy or CDROM drive, and ensure the power and data cables to the storage devices are still disconnected.
- Place the forensic boot disk into the floppy or CD-ROM drive. Boot the computer and ensure the computer will boot from the forensic boot disk.
- Reconnect the storage devices and perform a third controlled boot to capture the drive configuration information from the CMOS/BIOS.
- Ensure there is a forensic boot disk in the floppy or CD-ROM drive to prevent the computer from accidentally booting from the storage devices.
- Drive configuration information includes logical block addressing (LBA), large disk, cylinders, heads, and sectors (CHS), or auto-detect.
- Power system down.

### **3.4 Shutdown Procedures while Preserving Evidence**

a) Powering down a computer system in a manner that will not corrupt the integrity of existing files is a complicated computer security procedure. In the event of a suspected computer incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible in any subsequent legal or administrative proceedings.

b) Opening a file also alters the time and date it was last accessed. On the surface this may not seem an important issue; however, it could later become extremely important in the determination of who committed the violation and when it occurred. Isolation of the computer system is ideal, but if this cannot be accomplished due to operational requirements, no attempts should be made to recover or view files at the local level.

c) The isolation of a computer system so that evidence is not lost is of the utmost importance. Consideration must also be given to other storage media, handwritten notes, and documents found in the vicinity of the computer involved. These items can be of value in an ensuing investigation. Computer disks, CD-ROMs, tape storage media, and/or additional hard drives found in the area of the computer also must be isolated and protected.

d) No one, including the individual suspected of committing the alleged computer violation, should be allowed contact with the storage media or the computer involved in the security incident. Individuals with extensive computer experience can develop programs that, with a few keystrokes, can destroy all magnetic data on a hard drive.

e) Generally the type of operating system a company uses dictates the timing and the manner in which a computer is powered down. With some operating systems, merely pulling the power plug is the preferred method. With other systems, disconnecting the power supply without allowing the operating system to initiate internal shutdown could result in the loss of files or, in rare instances, a hard drive crash. Potential evidence may reside in typical storage areas such as the spreadsheet, database, or word processing files. However, potential evidence may also be in file slack (file slack is the unused space in a data cluster that's at the end of most files), erased files, and Windows swap files. Potential evidence in these locations is usually in the form of data fragments and can be easily overwritten by booting the computer and running the operating system.

f) For example, when the Windows operating system boots up (loads), it generates new files and opens existing files. This has the potential to overwrite and destroy data or possible evidence

previously stored in the Windows swap file. To use another example, when word processing or other program files are opened and viewed, temporary files are created and overwritten by updated versions of files, making potential evidence stored in these locations subject to loss.

g) The following are the basic characteristics and procedures (broken down by operating system) that should be followed when an operating system shutdown is warranted.

### **MS-DOS Operating System**

#### **Characteristics**

- Text is on a solid background (usually black).
- The prompt contains a drive letter and uses backslashes.
- The prompt usually ends with a greater than sign (>).

#### **Shutdown Procedures**

- Photograph the screen and annotate any programs running.
- Pull the power cord from the wall.

### **Windows 7,8,10 Operating System**

#### **Characteristics**

- Program Manager
- Colored tile bar
- Standard menu options

#### **Shutdown Procedures**

- Photograph the screen and annotate any programs running.
- Pull the power cord from the wall.

### **Windows NT 3.51 Operating System**

#### **Characteristics**

- Program Manager
- Colored tile bar
- Standard menu options
- Icons representing network computers and user

#### **Shutdown Procedures**

- Photograph the screen and annotate any programs running.
- Pull the power cord from the wall.

### **Windows 95/98/NT 4.0/2000/XP/2007/2008/2010 Operating System**

#### **Characteristics**

- The Start button has a Windows symbol.

#### **Shutdown Procedures**

- Photograph the screen and annotate any programs running.
- Pull the power cord from the wall.

### **UNIX/LINUX Operating System**

#### **Characteristics**

- The Start button has a Unix/Linux version symbol.

#### **Shutdown Procedures**

- Photograph the screen and annotate any programs running.
- Right-click to the menu.
- From the menu, click Console.
- The root user prompt is set to # sign. If not present, change user to root (type su -). At that point you are prompted for the root password. If the password is available, enter it. At the # sign, type sync; sync; halt, and the system will shut down. If you do not have the root password, pull the power cord from the wall.

- If the # sign is displayed when at the console, type id and press Enter. If you see that your user ID is root, type sync; sync; halt, and press Enter. This will shut down the system. If your user ID is not root, pull the cord from the wall.

## MAC OS Operating System

### Characteristics

- An Apple symbol in the upper left corner
- Small horizontal lines on the window's menu bar
- A single button in each corner of the window
- Trash icon

### Shutdown Procedures

- Photograph the screen and annotate any programs running.
- Record the time from menu bar.
- Click Special.
- Click Shutdown.
- The window tells you it is safe to turn off the computer.
- Pull the power cord from the wall.

- Whenever possible, remove the subject storage device and perform the acquisition using the examiner's system. When attaching the subject device to the examiner's system, configure the storage device so that it will be recognized.

h) **Exceptional Circumstances:** Exceptional circumstances, including the following, may result in a decision not to remove the storage devices from the subject system:

- RAID (redundant array of inexpensive disks). Removing the disks and acquiring them individually may not yield usable results.
- Laptop systems. The system drive may be difficult to access or may be unusable when detached from the original system.
- Hardware dependency (legacy equipment). Older drives may not be readable in newer systems.
- Equipment availability. The examiner does not have access to necessary equipment ie...Network storage. It may be necessary to use the network equipment to acquire the data.
- When using the subject computer to acquire digital evidence, **reattach** the subject storage device and attach the examiner evidence storage device (e.g., hard drive, tape drive, *CD-RW*).
- Ensure that the examiner's storage device is *forensically* clean when acquiring the evidence.
- Write protection should be enabled/initiated, if available, to preserve and protect original evidence. The examiner should consider creating a known value for the subject evidence prior to acquiring the evidence (e.g., performing an independent cyclic redundancy check (CRC), *hashing*). Depending on the selected acquisition method, this process may already be completed.
- If hardware write protection is used:
- Install a write protection device
- If software write protection is used:
- Boot system with the examiner-controlled operating system.
- Activate write protection.
- Investigate the geometry of any storage devices to ensure that all space is accounted for, including host-protected data areas (e.g., non host specific data such as the partition table matches the physical geometry of the drive).
- Capture the electronic serial number of the drive and other user-accessible, host-specific data.
  - Acquire the subject evidence to the examiner's storage device using the appropriate software and/or hardware tools, as follows:
    1. Stand-alone duplication software.
    2. Forensic analysis software suite.
    3. Dedicated hardware devices.

4. Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.

### 3.5 Acquiring a Drive Safely

4.5.1 The acquisition of a hard drive can be performed in four different ways. Acquiring LOCAL, acquiring with a CABLE, and acquiring with the write Block device.

a) Local: With Write-Block

- Write Block Tool such as FastBloc FE from Guidance Software's solution can be used to allow forensic acquisitions of IDE hard drives to take place in Windows. Write-block device is one that prevents physically writing to local hard drives that Windows would otherwise write to.
- The connects to a desktop or laptop through a SCSI cable to a SCSI controller card in the Forensic computer. The write block tool IDE connects to a desktop or laptop through an IDE ribbon cable, attaching to an IDE port of the Forensic computer's motherboard.
- The suspect IDE hard drive is then connected to the IDE connector on the write block tool. Both write block tool and computer are turned on.

b) Local: "Drive To Drive"

- The Local Method means that you are 1) acquiring the suspect's hard drive from within your own computer OR 2) acquiring the suspect's hard drive in his/her computer with your Storage hard drive in his/her computer.
- Physically remove the Subject drive from suspected computer and install it so that it shares the same IDE ribbon cable as examiner Storage hard drive. This is a tricky situation because, if you accidentally boot up into Windows at this point, examiner will write to the Subject's hard drive.
- If you are going to acquire a Subject hard drive locally, then you need to boot up the subject computer with a forensic software boot disk (typically EnCase®). After booting with the boot Disk, at the A:\> prompt, type appropriate command to launch forensic tool for DOS. While using forensic tool EnCase®, on the left-hand side of the screen examiner will see as many numbers as there are physical hard drives in the machine. On the right-hand side of the screen you will see as many logical volumes as there are on the physical drives.
- At this point examiner will confirm that the suspect HD is LOCKED and examiner Storage drive (what you have to write the evidence file to) is not locked. (All drives are locked by default.) Hit ADD DEVICE, choose the right disk, and forensic software will start imaging the suspect HD.

c) Cable: Parallel-Port Method

- The Parallel-port method is best suited for when no other method of acquisition works. The Parallel-port method is slow but safe. You can safely boot your forensic computer into Windows and you will NOT write to the suspect hard drive.
- Power off the two computers. Connect the parallel-port lap-link cable that ships with forensic tool between the two machines. Boot the Subject PC with a forensic tool boot disk. At the A:\> prompt, type appropriate command, which will launch the computer into Server Mode.
- Boot up your Storage PC into Windows. Run forensic tool for Windows. Hit the ADD DEVICE button. Select the drive, fill in the fields, and begin the preview and acquisition.

d) Cross-Over Network Method

- Power off the two computers. Connect the cross-over network cable that ship with forensic tool between two machines. Boot the subject PC with an forensic tool boot CD. Select appropriate command, which will launch the computer into server mode.
- Boot up your storage PC into Windows. Run forensic tool for Windows. Hit the ADD DEVICE button. Select the Cross-over, fill in the fields, and begin the preview and acquisition.

### 3.6 Disk Imaging

a) Properly prepared media should be used when making forensic copies (imaging) to insure no commingling of data from different cases. Properly prepared media is that which has been completely overwritten with a known character.

b) “An image of the whole disk was copied. This is regardless of any software on the disk and the important point is that the complete content of the disk is copied including the location of the data. Disk imaging takes sector-by-sector copy usually for forensic purposes and as such it will contain some mechanism (internal verification) to prove that the copy is exact and has not been altered. It does not necessarily need the same geometry (as the original) as long as arrangements are made to simulate the geometry if it becomes necessary to boot into the acquired image.”

c) “Term given to creating physical sector copy of a disk and compressing this image in the form of a file. This image file can then be stored on dissimilar media for archiving or later restoration.” In simple words, disk imaging can be defined as to make a secure forensically sound copy to media that can retain the data for extended period. Disk imaging is also one of the approaches for backup except that backup only copies the active file. In backup, ambient data will not be copied. This is an area where the most important source for the evidence could be found. Ambient data is a data stored in Windows swap file, unallocated space and file slack.

d) The result of the analysis also can be duplicated to another media using disk-imaging tool. A good imaging tool will not alter the original evidence. It can copy all the information from the drive and make the contents available for forensic analysis. Even ambient data that is inaccessible to the residential of operating system will be copied.

e) Requirements for a disk-imaging tools:

The requirements for a disk-imaging tool are:

- The tool shall make a bit-stream duplicate or an image of an original disk or partition.
- The tool shall not alter the original disk.
- The tool shall be able to verify the integrity of a disk image file.
- The tool shall log I/O errors.
- The tool’s documentation shall be correct.

f) All disk-imaging tools shall be able to accomplish the tasks described as mandatory requirements. Optional requirements are tested as if they were mandatory requirements if the tool under test supports the applicable feature. If a specific tool does not provide the capabilities of a particular optional requirement, then the tool is not tested for that requirement. This means that a specific tool might provide none of the capabilities described under optional requirements.

g) Mandatory Requirements of disk imaging tools: The following requirements are mandatory and shall be met by all disk imaging tools.

- The tool shall not alter the original.

- If there are no errors accessing the source, then the tool shall create a bit-stream duplicate or image of the source.
- If there are I/O errors accessing the source, then the tool shall create a qualified bit-stream duplicate or image of the source. (A *qualified bit-stream duplicate* is defined to be a duplicate except in identified areas of the bit-stream.) The identified areas are replaced by values specified by the tool's documentation.
- The tool shall log I/O errors in an accessible and readable form, including the type of error and location of the error.
- The tool shall be able to access disk drives through one or more well-defined interfaces.
- Documentation shall be correct insofar as the mandatory and any implemented optional requirements are concerned, i.e., if a user following the tool's documented procedures produces the expected result, then the documentation is deemed correct.
- If the tool copies a source to a destination that is larger than the source, and it shall document the contents of the areas on the destination that are not part of the copy.
- If the tool copies a source to a destination that is smaller than the source, the tool shall notify the user, truncate the copy, and log this action.

h) Optional Requirements: The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

- The tool shall compute a hash value of the complete bit-stream duplicate generated from an image file of the original source, compare the computed hash value to the hash value of the original source computed at the time the image was created, and log the results of the comparison on a disk file.
- The tool shall divide the destination bit-stream into blocks, compute a hash value for each block, compare the computed hash value to the hash value of the original block of source data computed at the time the image was created, and log the results of the comparison on a disk file.
- The tool shall create a bit-stream duplicate of individual partitions as directed by the user.
- The tool shall allow the user to view the source partition table and the tool shall log the contents of the source partition table.
- The tool shall log one or more of the following items on a disk file: tool version, subject disk identification (if the identification is available, such as manufacturer, make, model, serial number, sector count, etc.), any errors encountered, tool actions, start and finish run times, tool settings, and user comments.
- The tool shall create an image file on fixed or removable electronic or magnetic media that can be used to create a bit-stream duplicate of the original.
- The tool shall create a qualified bit-stream duplicate and adjust the alignment of cylinders to cylinder boundaries of disk partitions on a destination of a different physical geometry. The identified areas of the duplicate that are allowed to be changed are the following: partition table entries to reflect the relocated partitions; boot records; fill areas required for cylinder alignment, and excess disk space. The fill areas shall be given values as specified in the tool documentation.

### 3.7 Collecting Volatile Data

a) Volatile data can be defined as active information temporarily reflecting the machines current state including registers, caches, physical and virtual memory, network connections, shares, running processes, disks, floppy, tape, CD-ROM and printing activity. Before collecting volatile data there are a few guidelines to follow:

- Avoid tools that use a GUI interface.
- Command line tools are best here.



- Use safe and tested tools you know that work.
- Create two or three floppy disks containing your volatile collection tools and write protect them.
- Generate a checksum and validation for each of your tools and store it safely within your toolkit.

b) Some of the tools for the collection of volatile data are:

- Srvcheck.exe: A NTRK utility that displays the shares locally or remotely.
- Kill.exe: A Windows 2K Support tool for terminating a selected task or process.
- Rasusers.exe: A NTRK utility that lists all user accounts on a domain or server that have been granted permission to dial in to the network.
- Dumpel.exe: A NTRK utility to create an ASCII copy of the Event Viewer Logs.
- Filemon: A monitoring tool that displays all file system activity in real time.
- Regmon: A monitoring tool that displays all registry activity in real time.
- Tokenmon: A monitoring tool that displays logons, logoff, privilege usage and impersonation.
- Handle: A tool that displays what files are open by which processes and more.
- ListDLLs: A tool that lists all DLLs that are currently loaded including the version and the full path names of the loaded modules, etc.
- Process Explorer: A tool that displays open files, object processes, registry keys, DLLs and owners of object processes.
- MD5sum: A tool that generates the checksum of a file and provides verification.
- Fport: A tool that maps application processes to the ports they listen on.
- TCPView: A tool that shows the endpoints of all open TCP and UDP connections.
- Cmd.exe: The command prompt for Win NT/2000

### 3.8 Evidence Analysis

a) General forensic principles apply when examining digital evidence. Different types of cases and media may require different methods of examination. Persons conducting an examination of digital evidence should be trained for this purpose.

b) Conducting an examination on the original evidence media should be avoided. Rather, examinations should be conducted on a forensic copy of the original evidence, or via forensic evidence files.

c) Almost all-forensic examinations of computer media are different and that each cannot be conducted in the exact same manner for numerous reasons, however there are two essential requirements of a competent forensic examination. These are:

- Forensically sterile examination media *must be* used
- The examination *must* maintain the integrity of the original media

d) All computer and digital media examinations are different: The examiner must consider the totality of the circumstances as he/she proceeds. So, then, not all components here may be needed in every situation, and examiners may need to adjust to unusual or unexpected conditions in the field.

e) Analysis is the process of interpreting the extracted data to determine their significance to the case. Some examples of analysis that may be performed include timeframe, data hiding, application and file, and ownership and possession. Analysis may require a review of the request for service, legal authority for the search of the digital evidence, investigative leads, and/or analytical leads.

f) Examination of the media should be completed logically and systematically by starting where the data of evidentiary value is most likely to be found. These locations will vary depending on the nature and scope of the case. Examples of items to be noted might include:

- If the media is a hard drive the number and type of partitions should be noted.
- If the media is an optical disc then the number of sessions should be noted.
- File systems on the media should be noted.
- A full directory listing should be made to include folder structure, filenames, date/time stamps, logical file sizes, etc..
- Installed operating systems should be noted.
- User created files should be examined using native applications, file viewers, or hex viewers. This includes such files as text documents, spreadsheets, databases, financial data, electronic mail, digital photographs, sound and other multimedia files, etc..
- Operating system files and application created files should be examined, if present. This would include, but is not limited to: Boot files, registry files, swap files, temporary files, cache files, history files, log files, etc..
- Installed applications should be noted.
- File hash comparisons may be used to exclude or include files for examination.
- Unused and unallocated space on each volume should be examined for previously deleted data, deleted folders, slack space data, intentionally placed data. Previously deleted filenames of apparent evidentiary value should be noted. Files may be automatically carved out of the unallocated portion of the unused space based upon known file headers.
- Keyword searches may be conducted to identify files or areas of the drive that might contain data of evidentiary value and to narrow the examination scope.
- The system area of the volume (i.e. FAT, MFT, etc.) should be examined and any irregularities or peculiarities noted.
- Examination of areas of the media that are not normally accessible such as extra tracks or sectors on a floppy disk, or a host-protected area on a hard drive may be required.
- When examining a computer the system date and time should be collected, preferably from the BIOS setup. The date and time should be compared to a reliable known time source and any differences noted. If the BIOS setup information is accessible then drive parameters and boot order should be noted. Depending on the BIOS other information such as system serial numbers, component serial numbers, hardware component hashes, etc. should be noted.
- To facilitate examination of data, user settings, device and software functionality, etc. the computer may be booted using either a copy of the boot drive or by using a protected device on the original device to determine functionality of the hardware and/or software.

### **3.9 Timeframe Analysis**

a) Timeframe analysis can be useful in determining when events occurred on a computer system, which can be used as a part of associating usage of the computer to an individual(s) at the time the events occurred. Two methods that can be used are:

- Reviewing the time and date stamps contained in the file system metadata (e.g., last modified, last accessed, created, change of status) to link files of interest to the timeframes relevant to the investigation. An example of this analysis would be using the last modified date and time to establish when the contents of a file were last changed.
- Reviewing system and application logs that may be present. These may include error logs, installation logs, connection logs, security logs, etc. For example, examination of a security log may indicate when a user name/password combination was used to log into a system.

### **3.10 Data Hiding Analysis**

a) Data can be concealed on a computer system. Data hiding analysis can be useful in detecting and recovering such data and may indicate knowledge, ownership, or intent. Methods that can be used include:

- Correlating the file headers to the corresponding file extensions to identify any mismatches. Presence of mismatches may indicate that the user intentionally hide data.
- Gaining access to all password-protected, encrypted, and *compressed files*, which may indicate an attempt to conceal the data from unauthorized users. A password itself may be as relevant as the contents of the file.
- Stegano analysis.
- Gaining access to a *host-protected area (HPA)*. The presence of user-created data in an HPA may indicate an attempt to conceal data.

### 3.11 Application and File Analysis

- Many programs and files identified may contain information relevant to the investigation and provide insight into the capability of the system and the knowledge of the user. Results of this analysis may indicate additional steps that need to be taken in the extraction and analysis processes. Some examples include:
  - Reviewing file names for relevance and patterns.
  - Examining file content.
  - Identifying the number and type of operating system(s).
  - Correlating the files to the installed applications.
  - Considering relationships between files. For example, correlating Internet history to cache files and e-mail files to e-mail attachments.
  - Identifying unknown file types to determine their value to the investigation.
  - Examining the users' default storage location(s) for applications and the *file structure* of the drive to determine if files have been stored in their default or an alternate location(s).
  - Examining user-configuration settings.
  - Analyzing file metadata, the content of the user-created file containing data additional to that presented to the user, typically viewed through the application that created it. For example, files created with word processing applications may include authorship, time last edited, number of times edited, and where they were printed or saved.

### 3.12 Ownership and Possession

a) In some instances it may be essential to identify the individual(s) who created, modified, or accessed a file. It may also be important to determine ownership and knowledgeable possession of the questioned data. Elements of knowledgeable possession may be based on the analysis described above, including one or more of the following factors.

- Placing the subject at the computer at a particular date and time may help determine ownership and possession (timeframe analysis).
- Files of interest may be located in non-default locations (e.g., user-created directory named "child porn") (application and file analysis).
- The file name itself may be of evidentiary value and also may indicate the contents of the file (application and file analysis).
- Hidden data may indicate a deliberate attempt to avoid detection (hidden data analysis).
- If the passwords needed to gain access to encrypted and password-protected files are recovered, the passwords themselves may indicate possession or ownership (hidden data analysis).
- Contents of a file may indicate ownership or possession by containing information specific to a user (application and file analysis).

### 3.13 Hard Disk Examination

a) For conducting a complete examination of computer Hard Disk Drive (HDD) media the recommended procedures is:

- Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.
- All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company.
- The original computer is physically examined. A specific description of the hardware is made and noted. Comments are made indicating anything unusual found during the physical examination of the computer.
- Hardware/software or other precautions are taken during any copying or access to the original media to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the original media. We recognize that because of hardware and operating system limitations and other circumstances, this may not always be possible.
- The contents of the CMOS, as well as the internal clock are checked and the correctness of the date and time is noted. The time and date of the internal clock is frequently very important in establishing file creation or modification dates and times.
- The original media is not normally used for the examination. A bit-stream copy or other image of the original media is made. The bit-stream copy or other image is used for the actual examination. A detailed description of the bit-stream copy or image process and identification of the hardware, software and media is noted.
- The copy or image of the original HDD is logically examined and a description of what was found is noted.
- The boot record data, and user defined system configuration and operation command files, such as, the CONFIG.SYS file and the AUTOEXEC.BAT file are examined and findings are noted.
- All recoverable deleted files are restored. When practical or possible, the first character of restored files are changed from a HEX E5 to “-”, or other unique character, for identification purposes.
- A listing of all the files contained on the examined media, whether they contain potential evidence or not, is normally made.
- If appropriate, the unallocated space is examined for lost or hidden data.
- If appropriate, the “slack” area of each file is examined for lost or hidden data.
- The contents of each user data file in the root directory and each sub-directory (if present) are examined.
- Password protected files are unlocked and examined.
- A printout or copy is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits are marked, sequentially numbered and properly secured and transmitted.
- Executable programs of specific interest should be examined. User data files that could not be accessed by other means are examined at this time using the native application.
- Properly document comments and findings.

### 3.14 Floppy Disk Examination

a) For conducting a complete examination of computer Floppy Diskette (FD) or similar media the recommended procedures is:

- Forensically sterile conditions are established. All media utilized during the examination process is freshly prepared, completely wiped of non-essential data, scanned for viruses and verified before use.

- All forensic software utilized is licensed to, or authorized for use by, the examiner and/or agency/company.
- The media is physically examined. A specific description of the media is made and noted. The media is marked for identification.
- Hardware/software precautions are taken during any copying process or access to the original media and examination to prevent the transference of viruses, destructive programs, or other inadvertent writes to/from the original FD or to/from the examination equipment.
- The write-protect capability of the floppy disk drive (FDD) on the examining machine is tested.
- A duplicate image of the original write protected FD is made to another FD. The duplicate image is used for the actual examination. A detailed description of the process is noted.
- The copy of the examined FD is logically examined and a description of what was found is indicated. Anything unusual is noted.
- The boot record data, and user defined system configuration and operation command files (if present) are examined and findings are noted.
- All recoverable deleted files are restored. When practical or possible, the first character of restored files are changed from a HEX E5 to “-”, or other unique character, for identification purposes.
- The unallocated space is examined for lost or hidden data.
- The “slack” area of each file is examined for lost or hidden data.
- The contents of each user data file in the root directory and each sub-directory (if present) are examined.
- Password protected files are unlocked and examined.
- If the FD holds apparent evidentiary data that is to be utilized, a listing of all the files contained on the FD, whether they contain apparent evidentiary data or not, is made. The listing will indicate which files were printed, copied or otherwise recovered.
- A printout or copy is made of all apparent evidentiary data. The file or location where any apparent evidentiary data was obtained is noted on each printout. All exhibits are marked, sequentially numbered and properly secured and transmitted.
- Executable programs of specific interest should be examined. User data files that could not be accessed by other means are examined at this time using the native applications.
- Properly document comments and findings.

b) Procedure for obtaining required utility software:

- Ask investigating agency to get the utility software from accuse.
- If it is available to download from internet.
- Use other government resources.

#### **4. DOCUMENTATION AND REPORTING**

- The examiner is responsible for completely and accurately reporting his or her findings and the results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. It is important to accurately record the steps taken during the digital evidence examination.
- All documentation should be complete, accurate, and comprehensive. The resulting report should be written for the intended audience.
- Documentation should be contemporaneous with the examination, and retention of notes should be consistent with departmental policies.
- Take notes when consulting with the case investigator and/or prosecutor.
- Maintain a copy of the search authority with the case notes.
- Maintain the initial request for assistance with the case file.
- Maintain a copy of chain of custody documentation.
- Take notes detailed enough to allow complete duplication of actions.
- Include in the notes dates, times, and descriptions and results of actions taken.
- Document irregularities encountered and any actions taken regarding the irregularities during the examination.
- Include additional information, such as network topology, list of authorized users, user agreements, and/or passwords.
- Document changes made to the system or network by or at the direction of law Enforcement or the examiner
- Document the operating system and relevant software version and current, installed patches.
- Document information obtained at the scene regarding remote storage, remote user access, and offsite backups.
- During the course of an examination, information of evidentiary value may be found that is beyond the scope of the current legal authority. Document this information and bring it to the attention of the investigating officer because the information may be needed to obtain additional search authorities.
- The report **SHOULD** include:
  1. Identity of the reporting agency.
  2. Case identifier or submission number.
  3. Case investigator.
  4. Identity of the submitter.
  5. Date of receipt.
  6. Date of report.
  7. Descriptive list of items submitted for examination, including serial number, make, and model.
  8. Identity and signature of the examiner.
  9. Any output of the recovered data should be properly marked with appropriate identifiers in accordance with policies from the examiner's agency
  10. Brief description of steps taken during examination, such as string searches, graphics image searches, and recovering erased files. The forensic software used during the examination should be noted by its version and should be used in accordance with the vendors licensing agreement. The software should also be properly tested and validated for its forensic use by the examiner or the examiner's agency.
  11. A hard copy of the collected evidence will be retained in the division in a separate envelope with case details or in the case file.
  12. Results/conclusions.

## **5. EVALUATION AND INTERPRETATION OF RESULTS**

a) Evaluation and interpretation of the case findings will require consideration of the background information available about the case and the original expectations formulated during case assessment.

## **6. REPORTING CONCLUSIONS**

a) The purpose of the report is to provide the reader with all the relevant information in a clear, concise, structured and unambiguous manner, to make the task of assimilating the information as easy as possible. Reports should include factual findings and may include interpretation and expert opinion. Expert opinion and interpretation should be clearly identified in the report. Oral evidence may also subsequently be required. The style and content of written reports must meet the requirements of the criminal justice system for the country of jurisdiction.

## **7. CASE RECORDS**

a) The exact requirements for recording casework information will depend on the policy and any requirements of the laboratory. As a minimum, however, the records should be in sufficient detail to allow another examiner, competent in the same area of expertise, to be able to identify what has been done and to assess the findings independently. Case records should include both administrative and examination documentation. Whenever appropriate standardized forms should be used to document examinations. For example, casework involving digital evidence should include details of case records such as notes, work sheets, photographs, printouts, charts, spectra and other data or records which support findings should be generated during the course of the examination, and kept.

## **8. QUALITY CONTROL CHECKS**

### **8.1 Technical Review**

a) A qualified laboratory designee should conduct technical review periodically. It should include consideration of the validity of all the critical examination findings and all the raw data used in preparation of the statement/report. It should also consider whether the conclusions drawn are justified by the work done and the information available in the case record. The review may include an element of independent testing, if circumstances warrant it. A written record of the technical review should be made and retained with the case records. A qualified laboratory designee should carry out administrative review. He must ensure that the requesters needs have been properly addressed, editorial correctness and adherence to laboratory's policies.

### **8.2 Proficiency Testing/Inter-laboratory Comparison**

a) Proficiency testing/inter-laboratory comparison is an integral part of an effective quality assurance system. It is one of many measures used to monitor performance and to identify areas where improvements may be needed. Proficiency testing measures the capability of its examiners and the reliability of its analytical results. All personnel involved in the field of forensic digital evidence/technology examinations should be required to demonstrate their competence at regular intervals.

\*\*\*\*\*



## 9. APPENDIX-A: ACRONYMS

ASCII	:	American Standard Code for Information Interchange
BIOS	:	Basic Input Output System
CHS	:	Cylinders Heads Sectors
CMOS	:	Complementary Metal-Oxide Semiconductor
CRC	:	Cyclic Redundancy Check
FAT	:	File Allocation Table
FD	:	Floppy Disk
GUI	:	Graphic User Interface
HDD	:	Hard Disk Drive
HPA	:	Host Protected Area
I/O	:	Input/output
IDE	:	Integrated Drive Electronics
MAC	:	Modified Access Created
MBR	:	Master Boot Record
MFT	:	Master File Table
NTFS	:	New Technology File System
PC	:	Personal Computer
RAID	:	Redundant Array of Independent Disks/Inexpensive Disks
SATA	:	Serial Advanced Technology Attachment
SCSI	:	Small Computer System Interface
SSD	:	Solid-State Drive
SD	:	Secure Digital
TCP/IP	:	Transmission Control Protocol/Internet Protocol

**Last page**

### Formation of committees at National Level for formulation of SOPs and Manuals:

**Background:** In view of technological advancements in the scientific arena, the Standard Operating Procedures (SOPs) and Working Procedure Manuals, around which the technical and analytical exercise takes place in the laboratory in the examination of crime exhibits, needs periodical review to keep the laboratory updated.

For uniform SOP/Manuals and reporting pattern in all the CFSLS / State FSLs following committees were formed by JS (PM), MHA by including members from Central and State FSLs in the following areas:

Discipline	CFSL Member	Member
Biology/DNA	Dr. A. K. Sharma, Director, CFSL, Kolkata/Guwahati	1. Sh. Arun Sharma, Director, FSL, HP 2. Sh. Srikumar, Director, Chemical Examiner Lab, Thiruvananthapuram.
Chemistry/ Narcotics	Sh. K. M. Varshney, Coordinator, CFSL, Pune	1. Dr. R. K. Gupta, Director, FSL, Chhattisgarh. 2. Sh. B Shanmukham, Director, FSL, Puducherry. 3. Dr. Harsh Sharma, Director, FSL, Sagar (MP)
Explosives	Dr. Sukhminder Kaur, Coordinator CFSL, Pune	1. One officer from FSL, Delhi 2. One officer from FSL, Maharashtra
Toxicology	Dr. Vimukti Chauhan, SSO, CFSL, Chandigarh	1. Dr. K. V. Kulkarni, Director, DFSL, Maharashtra 2. One officer from FSL, Karnataka.
Ballistics	Sh. S. S. Baisoya, CFSL Chandigarh	1. Dr. D. K. Kaushal, Director, FSL, Haryana 2. Sh. N. P. Waghmare, Director, FSL, Goa 3. Dr. S. S. Das, Director, FSL, Odisha
Documents	Sh. M. C. Joshi, Dy. Director, CFSL, Chandigarh (Shimla Unit) and Dr. S. Ahmad, DFSS HQs., New Delhi	1. Ms. Deepa Verma, Director, FSL, Delhi
Psychology, Computer, Audio-Video	Dr. S. K. Jain, Director, CFSL, Chandigarh and Sh. M. Krishna, AD, CFSL, Hyderabad	Officers from FSL: HP, Delhi, Gujarat and Maharashtra
Crime Scene	Dr. M. Baskar, Dy. Director (Physics), CFSL, Chandigarh	1. Dr. Harsh Sharma, Director, FSL (MP) 2. Sh. R. K. Gupta, Jt. Director, FSL, Chhattisgarh

The officers of CFSLS will coordinate with the experts of State FSLs for convening of meeting(s) in the state and Central FSLs and finalization of SOPs and manuals.