

---

For Departmental use only

# Digital Evidence

## Investigation Manual

### 2014



**CENTRAL BOARD OF DIRECT TAXES**  
**DEPARTMENT OF REVENUE**  
**MINISTRY OF FINANCE**  
**GOVERNMENT OF INDIA**

---





सत्यमेव जयते

**K. V. Chowdary**

Chairman, CBDT &

Special Secretary to the Govt. of India



भारत सरकार  
Government of India  
(वित्त मंत्रालय/राजस्व विभाग)  
Ministry of Finance/Department of Revenue  
केन्द्रीय प्रत्यक्ष कर बोर्ड  
Central Board of Direct Taxes  
नार्थ ब्लॉक, नई दिल्ली - 110001  
NORTH BLOCK, NEW DELHI-110001  
E-mail : kv.chowdary@nic.in  
chairman\_cbdt@nic.in  
Tel. : 23092648, Telefax : 23092544

## FOREWORD

We are living in a digital age. The information & communication technology revolution has significantly impacted every part of our existence today. The work of Income Tax Department (ITD) is not an exception.

Days of manual books of accounts and other documents are getting extinct. Today most of books of account and documents are maintained on digital media devices. Any worthwhile investigation of such books/documents requires proper handling and thorough analysis of such digital data while taking requisite precautions for preserving its integrity and evidentiary value. Interestingly, no Manual on the subject was available to guide our officials dealing with enormous amount of digital evidence gathered during searches, surveys and other proceedings. It was therefore considered necessary that a Manual for dealing with digital evidence is prepared that can provide basic guidance to our officials.

I compliment Shri R Ravichandran, DIT(InV) Bangalore and other officers and members of the team who have contributed in bringing out this much needed Manual which, inter alia, provides insight into the legal framework for acquiring digital evidence, a step-by-step procedure as to how the devices should be approached, how relevant data be identified and how clones have to be prepared and utilized for the purposes of investigative analysis. I also compliment my CIT(InV) Shri Ramesh Kumar Yadav for his relentless efforts in taking forward the project.

I am sure this Manual will go a long way in building requisite capacity in the ITD in the field of use of electronic evidence and expect all the officers and staff to benefit from the same.

New Delhi, dated 31<sup>st</sup> October 2014

(K. V. Chowdary)





**RAMESH K. YADAV, I.R.S.**



**आयकर आयुक्त (अन्वेषण)  
(केन्द्रीय प्रत्यक्ष कर बोर्ड)**

155ए, नार्थ ब्लॉक, नई दिल्ली-110 001

**COMMISSIONER OF INCOME TAX  
(INVESTIGATION)**

**CENTRAL BOARD OF DIRECT TAXES**

155A, North Block, New Delhi-110001

टेलीफैक्स/Telefax : 011-23092177

E-mail : citinv-cbdt@nic.in

## **PREFACE**

Fast pace of the change in the last a few decades, particularly in the field of information and communication technology, has offered enormous advantages while posing equally difficult challenges before the ITD. Our initiatives in capacity building have been lagging behind the needs. There is a huge gap between the two.

Shri K. V. Chowdary, Chairman, CBDT [also in charge of Member(Inv)], has been emphasising upon the need of capacity building particularly with regard to electronic evidence and cyber forensic and taken various initiatives during last two years, many of which have started yielding rich dividends. Hon'ble Finance Minister has also reiterated the need to build requisite capacity in this regard, during his interaction with DsGIT (Inv) and CCsIT (Central) on 23rd July 2014,

In the above background and with the objective of bridging the aforesaid gap between the need of the department and available capacity, Investigation Division of CBDT took up the project of developing a "Manual on Use of Digital Evidence". A committee headed by Shri R. Ravichandran, Director of Income Tax (Inv), Bangalore was constituted which has prepared the Manual after extensive consultation with various stakeholders within a short time. The committee has also benefitted from an earlier draft submitted by another committee headed by Shri B.P. Gaur, the then DGIT(Inv) Mumbai.

The Manual discusses about all relevant issues including types of hardware and software used for data storage, their technical specifications, do's and don'ts of handling the same, steps to be taken at different stages of a search with regard to electronic material/evidence, facilities at the existing Cyber Forensic labs set up by the department, a few illustrative case studies. Efforts have been made to make the Manual lucid and easily understandable with the help of screenshots and by keeping technical jargons at the minimum required level.

On behalf of the CBDT, I thank all the officers and other persons who have contributed in bringing out this Manual. I hope that the officers of the department will use the Manual intensively for capacity building and extensively in as many of their works as possible and doing so will only make this effort successful. As the Manual will require continuous updation, I would request all officers of the department to send suggestions, if any, to Director (Inv.II), CBDT, North Block, New Delhi-110001 or email on his official email id.

**New Delhi, the 31<sup>st</sup> October, 2014**

**(Ramesh Kumar Yadav)**



---

**आर. रविचन्द्रन, आई. आर. एस**  
**R. RAVICHANDRAN, IRS**

आयकर निदेशक (अन्वेषण)  
कर्नाटक एवं गोवा  
**DIRECTOR OF INCOME TAX (INV)**  
KARNATAKA AND GOA



टेली / Phone : 080-22865009  
फैक्स / Fax : 080-22864109  
: 080-22866251

सी. आर. बिल्डिंग अन्नेक्स, विसरी मंजिल,  
क्वीन्स रोड, बेंगलूर - 560 001  
3rd Floor, C.R. Building Annexe,  
Queen's Road, Bangalore - 560 001



## ACKNOWLEDGEMENTS

In order to fulfill the need to have a digital evidence manual for Investigation Directorate of CBDT a Committee, comprising five members, was constituted by CBDT's O.M.F.No.414/65/2008-IT (Inv.I)(PT) dated 9.2.1010 under the chairmanship of Shri. B.P.Gaur, former DGIT(Inv)Mumbai, to prepare a manual to guide the field officers in the matter of collection, handling and utilization of digital evidences found during search & seizure/survey operations. The committee submitted a draft manual, which required revision keeping in view the rapid changes that have taken place with regard to handling of digital evidence. In order to update and modify the draft manual CBDT constituted a new committee Vide DO F.No.414/65/2008-IT (Inv-1) dt 10.9.2014, under the chairmanship of Shri. R.Ravichandran, DIT(Inv.), Bangalore, for updating the manual.

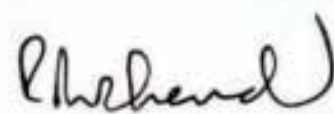
The committee gathered information relating such manual for digital evidence used by other investigation agencies of the Government for guiding their investigation team. The manual deals with the challenges posed by our investigating team to retrieve, authenticate and store digital evidence. The manual provides information on international best practices while handling digital evidence. It also collected information on various forensic tools of software and hardware used by the forensic laboratories in Mumbai and Delhi and also prepared a detailed Standard Operating Procedure for dealing with the forensic duplication and copying of digital evidence seized during search and seizure operation. The aspects relating to handling of Servers and ERP packages as well as accounting software used by corporates have been dealt with in the manual. Draft of new forms designed to be made part of the Panchnama during a search process such as Digital Evidence Collection Form, Chain of Custody Form, Mobile Device Collection Form have also been prepared. Case studies have been included to provide a detailed understanding on the usage of tools outlined in the manual. While certain hardware and software, which have been used extensively by the Investigation Directorate, have been referred to, it would be necessary to point out that there may be other tools which may also be found equally useful and relevant.

---

---

This is a continuing effort and therefore feedback and suggestions from stake holders would be welcome to ensure that next edition would be of greater relevance and more useful.

It is a work of its own kind for which all the officers and staff, who have contributed generously through their inputs need to be applauded. I would like to thank the initiative and the relentless effort taken by Shri Ramesh Kumar Yadav, CIT(Inv), CBDT in bringing out this manual. I want to make special mention of Shri M.S.Nethrapal, Dy. Director of Income Tax (Inv) and Member Secretary of the committee, without whose dedicated work, this Manual would not have seen the light of the day. I am also grateful to other members of the committee, Shri. Kumar Ajeet, Addl. Director of Income Tax (Inv), Bangalore, Shri. Kailash Gaikwad, Jt. Commissioner of Income Tax(TDS), Mumbai, Shri J X Peter, Dy. Director of Income Tax (Inv), Chennai, Ms. Swapna Devireddy, Dy. Director of Income Tax (Inv), Mumbai, Shri. .Sachin Dhanias, Asst. Director of Income Tax (Inv), New Delhi and Shri Krishna Sastri Pendyala, Practice Head- Fraud Management and Digital Forensic, TCS, Hyderabad, who made significant contributions towards the content of this manual. I would also like to thank Shri. Harish Kumar, DIT (Inv), Ahmedabad, Shri. B.R.Balakrishnan DIT (Inv)-1, Mumbai, Shri. K.K.Vyawahare DIT (Inv)-2, Mumbai, Shri.V. Nagaprasad DIT (Inv), Chennai and Smt. M.V. Bhanumathi, DIT (Inv.)-2, New Delhi for providing inputs on case studies done by their Directorate. I also wish to thank Shri. Ravi Ramachandran, Director (Investigation), CBDT for providing inputs and support. It would also be pertinent to mention the names of the members of the earlier committee constituted by CBDT in 2010, Shri. B. P. Gaur Former DGIT (Inv), Mumbai, Shri. P. K. Dash DG Expenditure monitoring cell, ECI, Shri. Shrikant Chatterjee CIT-16, Mumbai, Shri. Satish Sharma CIT (Audit), Jaipur, Shri. R.N. Parbat CIT (A)-3 Baroda, Shri. Ashish Abrol, Addl DIT (Sys), New Delhi and Shri. P. S. Shivasankarann Dy Secretary, FTD, CBDT, New Delhi without whose dedicated work, this Manual would not have been initiated. I would like to place on record my sincere thanks to Shri S.K.Misra, DGIT (Inv), Karnataka & Goa for his constant guidance and support.



**R. Ravichandran IRS**  
**Director of Income Tax (Inv), Bangalore**  
**Chairman, Digital Evidence Investigation Manual Committee**

---



---

# Index

Chapter No.	Description	Page No
1	Introduction & Background	1
2	The Digital Evidence	5
3	Introduction to Digital Evidence Investigation and International Best Practices	23
4	Important Related Terms	25
5	Pre Investigation Assessment of Digital Evidences	29
6	Forensic Collection of Digital Evidences	36
7	Analysis of Digital Evidences	49
8	Documentation and Seizure of Digital Evidences	63
9	Reporting of Analysis in Assessment Order and Archival of Digital Evidences	65
10	Mobile Forensics	68
11	Cyber Forensic Labs and Data Extraction Centres	70
12	Case Scenario's	77
<b>Annexure No.</b>		
1	Backup with Few Softwares- Examples	87
2	Imaging/Cloning- Few Examples	91
3	On the Spot Recovery of deleted data-Examples	108
4	Some Examples of Mobile Devices Backup	118
5	List of few Hardwares/Softwares that can be used	135
6	Details of Various Legal Provisions associated with Digital Evidence	138
7	Digital Evidence Collection Form	154
8	Chain of Custody Form	155
9	Mobile Phone Evidence Collection Form	156

---



# Chapter 1

## Introduction & Background

### 1.1 Introduction

One of the most significant and influential inventions of 20th century was the Computer. There has been a sea change in the purposes and the manner in which computers are used with advent of microprocessor technology and digital communication. The computer started with being a giant calculating machine. It then metamorphosed itself into a stand-alone personal tool for performing assorted routine tasks like word processing and accounting and then to today's network device permeating virtually everything including instantaneous and global personal and business interaction. The way business is conducted and records are maintained today is a far cry from days past. Accordingly, in enforcement agencies including the Income tax department, more and more information is being stored, transmitted or processed in digital form.

The law of the country has also taken cognizance of this reality. The Information Technology Act, 2000 has been enacted recognising electronic records as evidence, governing access to and acquisition of digital and electronic evidence from individuals, corporate bodies and/ or from the public domain. By way of this enactment, amendments were also brought in other laws like Indian Penal Code, Indian Evidence Act and Criminal Procedure Code, (Cr.PC). The Income-tax Act, 1961 has also been amended thrice by way of Finance Act 2001, Finance Act 2002 and Finance Act 2009 thereby according recognition to electronic evidence, facilitating access to them and giving when need be, powers to impound and seize them. By Finance Act, 2001, Clause (22AA) was inserted in Section 2 to provide that the term "document" in Income Tax Act, 1961, includes an electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000. By Finance Act, 2002, Clause (iib) was inserted in Sub-Section (1) of Section 132 requiring any person who is found to be in possession or control of any books of account or other documents maintained in the form of electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000), to afford the authorised officer the necessary facility to inspect such books of account or other documents; and by Finance Act, 2009, clause (c) was inserted in sub-section (1) of Section 282 providing that service of notice in the form of any electronic record as provided in Chapter IV of the Information Technology Act, 2000 (21 of 2000) will constitute valid service

Maintaining the integrity of electronic evidence through various processes such as identification of evidence, retrieval of deleted evidence, examination of such evidence, etc., presents problems which are different from the problems encountered in handling of traditional physical or documentary evidence. This Manual attempts to recommend basic operating procedures for handling digital evidence. This includes procedures for getting access to digital evidence, acquisition of the same, their analyses and seizure

maintaining the integrity of information taken from stand-alone electronic media, servers and networks where digital information/ evidence may be stored.

## 1.2 The Challenges

- The records including books of account maintained on papers are mostly replaced by documents in digital form.
- Most organisations use networks connecting different PCs, and servers spread across geographical locations and even sovereign jurisdictions not only for communication but also for conduct of day to day business.
- Computer data including books of account are easy to modify, alter, delete or hide.
- It is very easy to protect data by passwords and encryption making deciphering of real data an extremely difficult task
- The data storage devices come in a large variety of technology, shapes and sizes e.g.
  - Hard disks- IDE/ATA/PATA/SATA/SCSI/SAS
  - Laptop Hard Disks – 2.5” & 1.8”
  - USB Pen-drives and various types of Flash drives.
  - USB i-Pods, USB MP3 players
  - CD & DVD Media, Floppy Media
  - Mobile SIM cards, Memory Card & Device’s internal memoryDiscovery of these devices and retrieval of the data stored therein presents a challenge.
- Different kind of software, platforms and customized applications used for varied business purposes.
- Digital data being often stored on networked servers which are normally/ remotely accessed. Instances of such data being placed on shared International Networks and Platforms having transnational jurisdictions have come to light. The server may not be available for seizure during survey or search. Instead, all data may be stored in, what they call, “cloud server”, i.e., a server located in even a foreign country thousands of miles away and the searched / surveyed party is sitting merely with a monitor/ laptop.
- Specialised skills are required to identify relevant data, safely retrieve them, properly analyze them for their evidentiary value, and to subsequently produce them in a manner that their integrity can be established in any formal proceedings such as assessment/ appeals and prosecution, etc. With ever changing and improving technology, skills are also required to be honed and updated regularly.
- The environments in which Income-tax Authorities function during field actions are different from other law enforcement agencies. Thus, the requirement of standard procedure for Income-tax Department is slightly different and needs to be flexible as compared to other agencies dealing with other crimes/laws.

### 1.3 Current practices in the department

There are at present no uniform instructions on how to access computer systems, other digital devices and retrieve digital data during a search operation. Different practices are being followed:-

- Taking hard copies of data and seizing the same
- Using a CD writer or USB pen drive or USP Portable Hard Drive to take copy of data on the original hard disk
- Seizing Hard disks or computers and taking them to office

Very often, copying is done with Windows utilities and without any forensic software.

### 1.4 Shortcomings of current practices

**1.4.1** These methods are forensically unsound. If proper procedures are not followed data integrity and authenticity can be compromised. Some of the grounds on which integrity of seized data can be challenged are:

- When a system, seized on a particular date, is switched on/ booted at a later date to view its content, the date and time of opening these files automatically get modified.
- If a seized system is not booted on its own and its hard disk is attached to another system, even then Operating System has an automatic functionality to write to all attached media. Folders with the system restore-tag get created in all new disks attached to the Investigator's ( An officer/ official of the department entrusted with the task of investigation) system. Further, the anti-virus software on the Investigator's system scans files on the seized hard drive, in the process changing the date and time. The anti-virus program may even delete or quarantine critical evidence on the seized disk.
- Accessing a system or hard disk in any way without the use of 'write-protect' devices causes change in the hash value or digital fingerprint of the disk. This can render the evidence on such disks inadmissible.

**1.4.2** Sometimes even valuable data may be lost because of the use of unsound methods:

- **Logic Bombs:** Some systems are loaded with destructive software tools which get activated if the system is not shut down / started with a particular set of keystrokes. These can cause severe/ unannounced damage to the file systems as well as to critical files if programmed to do so. It is important that the investigating team does not in any way trigger them.
- **Live Data:** If a system is active or live when the search or survey team enters the premises and if these systems are made to shutdown, then the live data in systems mainly the RAM memory can not be retrieved. Such data are most vital in some cases because RAM may contain recently used passwords, details used in internet transactions etc. The programs and the processes which were running in the system may get closed leaving no clue on such information.

#### 1.4.3 Some other ill consequences of using above methods can be as under:

- **Password:** In a case where the system has password(s), shutting down the system would create problems in opening the same later without knowing the password(s) and cracking the same is a time - consuming process.
- Another major problem in the current work practices is that the retrieval of hidden, password - protected and deleted files. These files cannot be retrieved by making copies of the hard disk or taking its printouts.
- Lack of knowledge on some new server architecture such as RAID, where normal cloning process doesn't work.

### 1.5 The objective of Manual

This manual is an attempt to provide *basic* information about the digital evidence, its nature, legal implications and also to lay down/ recommend basic ingredients of standard procedure to handle digital evidence right from its identification to its acquisition/ seizure and its analysis.

The aim of this manual is to apprise the user of :

- i. The basic nature of digital evidence;
- ii. Basic legal provisions relating to digital evidence in Income-tax Act and other laws including Information Technology Act and Indian Evidence Act;
- iii. Basics of Computer Forensics and international best practices;
- iv. Identification and preliminary analysis of Digital Evidence;
- v. Recommended Standard Operating Procedures and documentation to acquire and/or seizure of Digital Evidence maintaining authenticity and integrity of Digital Evidence;
- vi. Analysis of Digital Evidence;
- vii. Archival of Digital Evidence;
- viii. Mobile Forensic
- ix. Information about cyber forensic facilities.
- x. Case Studies in Digital Evidence Forensic

Though the requisite hardware/ software and technical support is not available in several stations, the departmental officers are advised to take initiative and create necessary infrastructure and awareness and follow the recommended procedures as far as possible. Some of the examples given on various softwares/hardwares are only used for illustration and in no way recommendatory or mandatory to be used.

## Chapter 2

# The Digital Evidence

### 2.1 What is Digital Evidence?

“Digital evidence” or “Electronic Evidence” is any probative information stored or transmitted in digital form that may be used before the courts/ Income-tax authorities. Section 79A of the IT(Amendment) Act 2008 defines electronic form evidence as

*“ any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines”*





The main characteristics of the digital evidences are :

1. It is latent as fingerprints and DNA
2. Can transcend national borders with ease and speed
3. Highly fragile and can be easily altered, damaged or destroyed and also time sensitive.





For these reasons, special precautions should be taken to document, collect, preserve and examine this type of evidence.









### 2.2 Digital Devices: Sources for Digital Evidences

The use of digital devices in day to day life has increased tremendously. Accordingly, we may come across a wide range of the digital evidence which include E-mail word processing documents, data base tables, files saved from accounting programmes, digital photographs, ATM transaction logs, instant message histories, internet browser histories, the contents of computer memory, computer back-up, global positioning system tracks, digital video or sound files, data stored in mobile telephones and the data stored in all types memory storage devices. To help the understanding of the investigating officers, a compilation of various devices and the potential evidences these devices may contain is provided below:

Sl.No.	Digital Device		Potential Evidence
1	A Desktop Computer		The device contains all the files and folders stored including deleted files and information which may not be seen normally. Analysis of key document files like word documents, excel files, email's, tally data may help in unearthing potential evidences. Retrieval of deleted files using Cyber Forensics can help get key evidences that have been destroyed.
2	Pen Drives		The device stores many files and may be hidden easily. In many cases the parallel books of accounts maintained as tally data or excel sheets are kept in Pen Drives that can be easily hidden
3	Hard Drives		The device stores many files and may be hidden easily. Backup of earlier years may be kept and may be easily hidden.
4	Handheld Devices like Mobile Phones (Smart Phones), Electronic Organizer, IPAD, Personal Digital Assistant etc		Much information can be obtained from the devices like Address Book, Appointment calendars/information, documents, emails, phone book, messages (text and voices), video recording, email passwords etc. Many applications like CHAT, Whatsapp application can store many crucial conversations important for the investigations. Remittances and transactions are done by fund transfer through mobile phone service providers utilizing money deposited with the



			<p>latter bypassing banking channels. A person may do all his business through a mobile phone without any computer or laptop or warehouse for his inventory – as example, online business platform <a href="http://www.amazon.com">www.amazon.com</a> maintains huge warehouse at several places in India where online traders can store their merchandise. In such cases the trader may make all transactions through mobile phone and store in small external microchips making detection difficult.</p>
5	Smart cards, Dongles and Biometric Scanners		The device itself enables to understand the user level access to various information and places.
6	Display Monitor (CRT/ LCD/TFT etc), Screens of Mobile Phones if switched on		All the graphics and files that are open and visible on the screen in the switched on systems can be noted as electronic evidence. This evidence can be captured only in video, photographs and through description in seizure memos
7	Answering Machines		The device can store voice messages and sometimes, the time and date information about when the message was left. It may have details such as last number called, memos, phone numbers and names, caller identification information and also deleted messages.
8	Local Area Networks (LAN) Card or Network Interface Cards		The device itself is a digital evidence and may contain crucial evidences

9	Modems, Routers, Hubs and Switches		The device may contain details of IP addresses where the actual data is stored.
10	Servers		Contains crucial data on business related applications like SAP, ERP, CRM, Mail Servers. The device is a potential evidence for pulling out audit logs using forensic analysis. Analysis of emails of key persons from Mail Servers can help in finding crucial evidences required for the case.
11	Removable storage devices like SD Cards in Mobile phones		All new generation phones use these and store files in which evidence can be found.
12	Scanners and Copiers		The device itself, having the capability to scan may help prove illegal activity like making bogus bills etc. Copiers may also contains stored data which can be crucial evidences.
13	Digital Cameras		The device can be looked for images, videos, sounds, removable cartridges, time and date stamps
14	Pagers		The device can be looked for address information, Text message and phone numbers
15	CD/DVDs/		The device stores many files which may contain the evidence
16	Facsimile Machines		The device stores some documents, phone numbers, send/receive logs that can contain the evidence.

17	Global Positioning Systems (GPS)		The device may provide travel logs, home location, previous destinations etc which may be crucial in finding places where evidences may be stored.
18	Cloud Data Servers		The device is available on all smart phones and tablets. The Cloud may be used to store hidden data where crucial evidences may be stored. Some enterprises offer service for storage of commercial data in servers located in foreign countries and business data are stored there through internet – which can be accessed as per terms and conditions.

From the digital devices, two types of evidences are possible, one is persistent evidence and other is volatile evidence:

- **Persistent evidence:** *the data that is stored on a local hard drive and is preserved when the computer is turned off. For example, Documents (word, slide, sheet, pdf), Images, Chat log, Browser history, Registry, Audio / Video, Application, Email, SMS / MMS, Phone book, Call log*
- **Volatile evidence:** *any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. For example, Memory, Network status and connection, Process running, Time information*

It is to be noted that in certain cases, where volatile evidence is crucial, switching off a switched on system may result in destruction of volatile evidence.

## 2.2 Digital Forensics-What is it and its significance?

Digital forensics is the process of identifying and collecting digital evidence from any medium, while preserving its integrity for examination and reporting. It can be defined as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law.

Digital evidence gathering is becoming an increasingly powerful tool for the department in its fight against tax-evasion. It can be used individually as key evidence or alongside more traditional methods of

evidence gathering, where it could serve as a complement to other types of evidence. Furthermore, digital evidence may help in the course of the investigation phase to prepare the next steps.

In a nutshell, the significance of digital evidence analysis is that it:

- Help reconstruct past event or activity
- Show the evidence of policy violation or illegal activity
- Ensure the overall integrity of network infrastructure

### 2.3 Digital Forensics-Variou Branches

The branch of Digital forensics can be classified as follows:

1. Disk Forensics deals with extracting information from storage media in the form of active , deleted files and data from unallocated , slack spaces
2. Network Forensics is a branch of Cyber forensics dealing with monitoring and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection
3. Database Forensics is a branch of digital forensic science relating to forensic study of databases and their related meta data. This may be of help in understanding the time stamp of the database data created to see whether any manipulations where done in the original database
4. Mobile device forensics deals with examining and analyzing mobile devices to retrieve call logs, SMS/MMS, videos, audios, photos etc.
5. Email Forensics deals with recovery and analysis of emails including deleted emails, calendars and contacts
6. GPS Forensics deals with examining and analyzing GPS devices to retrieve Track logs, Track points, routes , stored locations, home offices etc

### 2.4 Key Elements of Digital Forensics

Key Elements of Digital Forensic are as follows:

1. **The identification and acquiring of digital evidence:** Knowing where the digital evidence is present, stored and what are the processes that can be used to retrieve the digital evidences is the first step. It is noticed that usually in big corporations, where huge number of digital devices is present, identification of crucial digital evidences will save time in analysis of digital evidence and also cost. Many a times it is noticed that customized software's like ERP/SAP are used and the strategy to retrieve the entire software should be discussed with the system administrator. It is also important to identify the types of information stored and the appropriate technology that can be used to extract it. After the evidence is identified the forensic examiner/investigator should image/clone the hard disk or the storage media

2. **The preservation of digital evidence** should be done in such a manner that there is no possible alteration, damage, data corruption or virus introduction during the process of examination.
3. **The analysis of digital evidences** involves discovering all the files on the subject system. This includes existing normal files, deleted yet remaining in Recycle bin, hidden files, password-protected files and encrypted files. The analysis also includes retrieval of deleted files and also gives accesses to hidden files, temporary files and protected files. In many business specific applications like customized jeweler software/real estate software, may give details of reports required for day to day functioning of the organization.
4. **Report the findings**, means giving the findings, in a simple lucid manner, so that any person can understand. The report should give description of the items, process adapted for analysis, chain of custody on the movement of digital evidence, hard and soft copies of the findings, glossary of terms etc
5. **The presentation and use of digital evidence in assessment order and presentation of the same in court** of the law in matters of appeal involves stating the credibility of the processes employed during analysis for testing the authenticity of the data.

## 2.5 What Cyber Forensics Can Reveal to AO

Digital Evidence actually has several advantages over other kinds of physical evidence:

- It can be duplicated exactly and a copy can be examined as if it were the original. **Importantly, copies made following proper procedures have the same evidentiary value as the original.** It is a common practice when dealing with digital evidence, to examine a copy thus avoiding the risk of damaging the original.
- With the right tools it is very easy to determine if digital evidence has been modified or tampered with by comparing with the original.
- It is possible to recover and analyze deleted files that have not been overwritten, as well as carving out portions of files and text from unallocated and slack space
- It is possible to do String and Key word searching for finding key files either present, deleted files etc
- It is possible to do time line analysis to see when the digital evidence was created, modified, changed, merged with other files etc
- It is possible to know manipulations in data by seeing changes done by unauthorized persons in the data.

## 2.6 The challenges in dealing with Digital Evidence

- The digital evidence collected and presented should be admissible in law and steps should be taken to maintain integrity of the data.

- Digital evidence, which is ephemeral, poses problems for searching and seizing. Computer data changes moment by moment and is invisible to the eye. It can be viewed indirectly only after applying proper procedures and processes for collecting evidence.
- Problems posed by recovery of deleted evidence are the challenges which law enforcement agencies have to tackle.
- It is very easy to keep digital data in encrypted or password protected mode. It is difficult to decipher the real information without knowing and getting the password or without having the key to the encryption

## 2.7 The Legal Background

**2.7.1** The Information Technology Act-2000 has been enacted to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information. The same enactment has also brought amendments in the **Indian Penal Code, 1861**, the **Indian Evidence Act, 1872**, the **Bankers' Books Evidence Act, 1891** and the **Reserve Bank of India Act, 1934**.

**2.7.2** As far as Income-tax Act, 1961 is concerned, it has been amended thrice by way of Finance Act, 2001, Finance Act, 2002 and Finance Act, 2009 respectively.

- By way of first amendment, provisions of sub-section (12A) of section 2 was inserted to give legal recognition to the books of account maintained on computer and sub-section (22A) to section 2 was inserted to provide definition of 'document' which included "electronic record" as defined under Information Technology Act 2000.

Under Information Technology Act 2000 an electronic record has been defined to include data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro file. This definition of electronic record is wide enough to cover person in possession of computer, storage device, server, mobile phone, i-Pod or any such device.

The above amendment has thus specifically given recognition to electronic record as admissible evidence at par with a 'document'. Further, the powers to impound/copy a document during a survey action u/s 133A and power to seize a document during a search and seizure operation has also been automatically extended to electronic records as a result of the amendment.

- By way of second amendment, provisions of section 132 (1)(iib) were inserted facilitating access to the electronic devices including computer, containing document or books of accounts in the form of electronic records by making it obligatory for the person under control of such device to afford the necessary facility to inspect such records.

By Finance Act, 2009, clause (c) was inserted in sub-section (1) of Section 282 providing that service of notice in the form of any electronic record as provided in Chapter IV of the Information Technology Act, 2000 (21 of 2000) will constitute valid service.

**2.7.3** Under Indian Evidence Act there are several references to documents and records and entries in books of account and their recognition as evidence. By way of the THE SECOND SCHEDULE to the Information Technology Act Amendments to the Indian Evidence Act have been brought in so as to, incorporate reference to Electronic Records along with the document giving recognition to the electronic records as evidence.

Further, special provisions as to evidence relating to electronic record have been inserted in the Indian Evidence Act, 1872 in the form of section 65A & 65B, after section 65. These provisions are very important. **They govern the integrity of the electronic record as evidence, as well as, the process for creating electronic record. Importantly, they impart faithful output of computer the same evidentiary value as original without further proof or production of original.** Accordingly, while handling any digital evidence, the procedure has to be in consonance of these provisions.

**2.7.4** Under Indian Penal Code several acts of omission and commission relating to various documents and records are treated as offences. By way of the THE FIRST SCHEDULE to the Information Technology Act, Amendments to the Indian Penal Code have been brought in, so as to incorporate reference to Electronic Records along with the document.

## **2.8 The sanctity and relevance of Digital Evidence**

As in the case of written or oral evidence, digital evidence can also be classified into three main categories:

- i. **Material evidence:** Material evidence is any evidence that speaks for itself without relying on anything else. In digital terms, this could be a log produced by an audit function in a computer system, the books of account maintained on a day-to-day basis on the computer, or any inventory management account maintained on the computer etc., if it can be shown to be free from contamination.
- ii. **Testimonial evidence:** Testimonial evidence is evidence supplied by a witness. This type of evidence is subject to the perceived reliability of the witness, But if the witness is considered reliable, testimonial evidence can be almost as powerful as material evidence. **For example, word processor documents written by a witness could be considered testimonial as long as the author is willing to depose that he wrote the same.**
- iii. **Hearsay:** Hearsay is any evidence presented by a person who is not a direct witness. Word processor documents written by someone without direct knowledge of the incident or documents whose authors cannot be traced fall in this category? Except in special circumstances, such evidence is not admissible in court of law. But even such evidence may constitute material and may be very relevant in Income-tax proceedings, which are not bound by technical rules of evidences. Otherwise also, they can provide important leads for further investigation.

**Accordingly, merely gathering electronic evidence is not sufficient. Efforts have to be made to**



**corroborate the contents therein vis-à-vis other evidence such as material and oral. Preliminary and detailed statements of the persons in control of computers/ electronic devices are always very important.**

## **2.9 Importance of standard procedures to deal with Digital Evidences**

From the above discussion on the nature and legality of digital evidence, it is clear that investigation in an automated environment require standard methods and procedures for the following main reasons:

- i. Evidence has to be gathered in such a way that the same would be accepted by a court of law. This should be easier if standard procedures are formulated and followed. This would also facilitate exchange of evidence in cases having interdepartmental and international ramifications especially if investigators from other departments and countries collect evidence in similar manner.
- ii. Every care must be taken to avoid doing anything which might corrupt or add to the data, even accidentally or cause any other form of damage. The use of standard methods and procedures would diminish this risk of damage. In some cases, some data may be changed or over-written during the process of examination. Thus, there is need for a thorough understanding of technology which is being used by the investigator for examination and also need for its documentation so that it would be possible to explain the causes/ effects later on in a court of law.
- iii. Some of the most important reasons for improper evidence collection are poorly written policies, lack of an established incidence response plan, incidence response training and a broken chain of custody.

**“Chain of custody”** is the roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence. Establishing a clear chain of custody is critical because electronic evidence can be easily altered. A clear chain of custody would demonstrate that electronic evidence is trustworthy. Preserving a chain of custody for electronic evidence, at a minimum, requires that:

- i. No data has been added, changed, deleted from the seized information evidence.
- ii. The seized /information evidence was duplicated exactly and completely.
- iii. A reliable and validated duplication process was used.
- iv. All media were secure and safe.

## **2.10 Fundamentals of procedure to deal with digital evidence.**

### **2.10.1 For ensuring integrity of the evidence being seized - Write Blocking**

- It is essential that no changes should be made while handling digital evidence. A change of a single **Bit** may render the whole evidence inadmissible. This can be achieved by write blocking the storage media which is intended to be acquired/seized by adopting a technology commonly referred to as “Write Block”



- This is a technology, which ensures that nothing is written on a particular storage media that has been write blocked.
- This technology can be implemented both through hardware and software.

### 2.10.2 Duplicating evidence for analysis – Acquisition of Evidence- Bit flow technology

- It is essential and advisable that the original evidence should not be used for analysis, since digital technology permits to make exact replicas of any digital evidence. This can be done safely by making a bit stream back-up.
- **Bit stream Back-up:** This is a process by which a storage media is copied by reading each bit and then transferring it to another storage media thereby ensuring that an exact copy of the original digital evidence is prepared.
- **Bit stream imaging** differs from copying in that copying applies to data that is not deleted and whose location is recorded in the FAT whereas, bit-stream imaging captures and copies all data on a disk including deleted files, swap files, slack space, FAT unallocated space and FAT un-addressed space. Bit-stream backup is a mirror image of the copied disk with the same hash value.

### 2.10.3 For Authentication and Seizure of Evidence -Mathematical Hashing:

Mathematical hashing is equivalent to one-way encryption. Every digital evidence at the lowest level translates into a big numerical number. When the digital device or data is encrypted using a hashing algorithm, it results in a new number of a fixed length called the **message digest**. The hashing algorithm has some unique characteristics, which are as follows:

- **Message digest always of a fixed length:** The digital evidence may be of any size, but on application of the hash algorithm the resultant message digest would always be of a fixed length.
- **Message digest is a randomly generated number:** The message digest is a randomly generated number. However, if the contents of the digital evidence remain the same, the hash algorithm would generate the same message digest every time it is applied on the digital evidence. This property is useful in authenticating seized digital evidence before a court of law. If application of hash algorithm on digital evidence in a court of law results in the same message digest as was obtained during the time of seizure, it indicates that the presented evidence is the same as what was seized.
- **One-way hash function:** It is computationally not feasible to determine the contents of the digital evidence if somebody knows the message digest. Hash algorithm is a one-way function. This property is of great importance from the legal point of view, since it prevents manipulation of digital evidence as no one can predict the message digest that would be generated if evidence is manipulated.
- **Collusion free hash:** The odd that two digital evidences with different contents have the same message digest is roughly  $2$  to the power  $128$  (i.e.  $34$  followed by  $37$  zeros). Their properties have two advantages:

- o Each digital evidence can be seized uniquely by specifying its message digest.
- o If two digital evidences have the same message digest there is a reasonable certainty that their contents match exactly.

## Limitations

By comparison of the message digest of acquired evidence with the message digest of the original the integrity of the acquired can be authenticated, if both message digests are same. However, if the two messages do not match, it is impossible to determine what has changed.

### 2.11 Important terms in collection of Digital Evidence

- **Seizure:** The process of generating a unique identity (Message Digest) of the digital evidence in a write block, and trusted environment, which is thereafter taken in the custody of the law enforcement official for the purpose of investigation.
- **Acquisition:** The process of making Bit-stream image of the digital evidence proposed to be seized in a write block and trusted environment. The process is deemed to be successfully completed if the message digest of the original digital evidence being seized matches with the message digest of the Bit stream backup copy made on a forensically sterile storage media.
- **Seizure and Acquisition** – The process of simultaneously generating a message digest and a bit-stream backup of the digital evidence proposed to be seized in write block and trusted environment. The process is deemed to be successfully completed if the message digest of the original digital evidence being seized matches with the message digest of the bit stream backup copy made on a forensically sterile storage media.

### 2.12 Search and seizure of Physical Evidence vs. Digital Evidence

**2.12.1** The search & seizure action u/s.132 of the I T Act is authorized when the designated authorities have reasons to believe that:

- i) A person is in possession of certain books of account/ documents which are **relevant** for or **useful** to any proceedings under Income-tax Act which the said person has not produced when asked to do so or there is a likelihood of such person not producing these documents/ books of account before Income-tax authorities.
- or
- ii) The person is in possession of money, bullion, jewellery or other valuable article or thing (assets) which represent wholly or partly some undisclosed income.

**2.12.2** In the conventional search of a premise the search team physically searches for the relevant documents/ books of account and assets in the premises. The relevant assets/ documents are also seized

during the course of search. It is very easy to visualize the search operations involving a physical item including an asset or document other than an electronic document. The rules and procedures are also well laid out in respect of search and seizure of physical items. The authorized officers are also generally very clear about identification of relevant documents and assets which are required to be seized.

**2.12.3** The act of entering the premises triggers a “search”. Once legitimately inside the premises, the Search team is entitled to force access to all places within the said premises. When the search team has a warrant, it is allowed to take away any evidence of undisclosed income/ asset. The widespread use of computers in recent years has led to a new type of situation in searches of data stored on computer hard drives and other storage devices. Though it is fundamentally similar to the search of physical evidence but in practice is substantially different. The Rules and Procedure governing search of data and its acquisition are still not well settled.

**2.12.4** The question is, how should provisions of section 132 of the I T Act apply to the retrieval of data from data storage devices? The dynamics of computer searches turn out to be substantially different from the dynamics of conventional searches. The entire-search, identification of evidence-seizure dynamic of premises searched is replaced by things like scan, acquisition, search and identification of evidence dynamics. **Computer forensics analysis is typically performed subsequent to a search operation at the Income-tax Office or cyber forensics laboratory. Weeks or months after the computer has been seized from the target’s premises, an analyst may comb through the world of information inside the computer and try to find the relevant evidence.**

**2.12.5** Computer searches and premises searches are similar fundamentally in so far as, in both cases, the search teams attempt to find and retrieve useful information hidden inside a closed container. However, the process of searching computers turns out to be considerably different from the process of searching physical spaces.

**2.12.5.1** For a physical item, the combing action is generally concluded at the premises itself, exact physical evidence or asset is identified and seized at the premises searched. For example, if the search team is looking for unaccounted jewellery - it will enter in to the premises - search each and every room - in each room it will search for various containers/secret places such as almirah, lockers, etc., - in almirah, lockers, etc., it will look for jewellery – make an attempt to find out the jewellery which is unaccounted and seize the unaccounted jewellery.

**2.12.5.2** In case some almirah or lockers are found locked – the search team will either break open the same and will look for the jewellery or put prohibitory order and subsequently after opening the almirah / locker/ room complete the search and seizure procedure. Thus, in our situation only the relevant asset will be seized.

**2.12.5.3** Just because 20 boxes are found in a premise would not mean seizure of all 20 boxes. Physically also this is not possible. The search team applies its skills and discretion at the premises to make specific seizure.

**2.12.5.4** Similarly the physical documents are also checked and the relevant documents only are seized. Even if the identification of relevant documents is not precise, the authorized officer uses his experience and skills to at least exclude the totally irrelevant documents and make seizure of only those documents which are found relevant or which at least has a possibility of being relevant. Thus, the search and seizure action of physical item is quite specific.

**2.12.5.5** Though the computer search and physical search of a place are similar fundamentally because the search team attempts to find and retrieve relevant evidence hidden inside the computer. Search of a computer is easy as well as difficult for many reasons. In computers, just like 20 boxes in above example, there may be thousands of folders. The authorized officer may not know as to in which folder relevant documents/ information is lying. He can however, acquire/seize entire data if he chooses to. But identification of specific and relevant data is very time consuming job and possibly can not be completed in the premise itself in most of the cases. The authorized officer's task, therefore is to first scan various devices to identify the device which may contain relevant evidence and acquire them, instead of acquiring each and every device containing digital evidence. **It is required to be done in a manner that proper balance is struck between indiscriminate acquisition/ seizure of huge data which will make task of identification of relevant evidence tougher and at the same time ensuring acquisition of data from device wherever there is a possibility of locating relevant evidence.**

**2.12.6** There are 4 basic differences between premises searched and computer search i.e., the environment, copying procedure, the storage mechanism and the retrieval mechanism, which authorized officer should understand. This will help him make an appropriate decision in identifying the relevant data which needs to be acquired/ seized.

#### **A. The Environment: Premises vs. Hard Drives**

Premises offer predictable, specific and discrete physical regions for physical searches. A search team can enter through a door or window and can walk from room to room. They can search individual rooms by observing their contents, opening drawers and other containers, and rummaging them.

Computer storage devices are different. They come in many forms, including hard drives, floppy disks, thumb drives, Zip disks etc.. All these devices perform the same basic function: they store zeros and ones that a computer can convert into letters, numbers and symbols. Every letter, number or symbol is understood by the computer as a string of eight zeros and ones. For example, the upper-case letter "M" is stored by a computer as "01001101," and the number "6" as "00110110." Each string is known as a "byte" of information and the number of bytes represents the total storage available on a storage device. For example, a forty gigabyte hard drive can store roughly forty billion bytes, or about 320 billion zeroes and ones.

While houses are divided into rooms, computers are more like virtual warehouses. When a user seeks a particular file, the operating system must be able to find the file and retrieve it quickly. To do this, operating systems divide all of the space on the hard drive into discrete sub parts known as "clusters" or

“allocation units.” Different operating systems use clusters of different sizes; typical cluster sizes might be four kilobytes or thirty-two kilobytes. A cluster is like a filing cabinet of a particular size placed in a storage warehouse. Just as a filing cabinet might store particular items in a particular place in the warehouse, the operating system might use a cluster to store a particular computer file in a particular place on the hard drive. The operating system keeps a list of where the different files are located on the hard drive; this list is known as the File Allocation Table or Master File Table (MFT), depending on the operating system. When a user tells his computer to access a particular file, the computer consults that master list and then sends the magnetic / optical heads over to the physical location of the correct cluster.

The search of data on digital device thus can be made by examining data lying on it, which is a very time-consuming job. Thus, **a preliminary search at the premises is generally followed by a detailed search subsequently, while in the case of search of premises, the search has to be finally concluded before the search party leaves the premises.** The decision of assessing officer to acquire/seize data from various devices should take into account this flexibility.

## **B. The Copying Process**

When a search team searches a premises, the premises and assets it searches typically belong to the target of the investigation. Once again, computers are different. To ensure the evidentiary integrity of the original evidence, the computer forensics process always begins with the creation of a perfect “bitstream” copy or “image” of the original storage device saved as a “read only” file. All analysis is performed on the bitstream copy instead of the original. The actual search occurs on the department’s computer, not on the searched party’s.

A bitstream copy is different from the copy users normally make when copying individual files from one computer to another. A normal copy duplicates only the identified file, but the bitstream copy duplicates every bit and byte on the “target” drive including all files, the “slack space”, Master File Table and metadata in exactly the same order as they appear on the original. Thus, the copying procedure ensures that all relevant as well as irrelevant information stored on computer are acquired. **Thus, identification of relevant devices is the key once a device containing relevant data is identified, copy of entire device is generally required to be made.**

## **C. The Storage Mechanism: The Premises vs. Computer Storage**

The third important difference between computers and premises concerns how much they can store and how much control people have over what they contain. Premises can store anything including computers of course, but their size tends to limit the amount of evidence they can contain. A room can only store only a limited number of packages and a premises can only contain limited number of rooms. Further, individuals tend to have considerable control over what is inside their premises. They can destroy evidence and usually know if it has been destroyed. Computers can only store data, but the amount of data is staggering.

While computers are compact at a physical level, every computer is akin to a vast warehouse of information. Computers are also remarkable for storing tremendous amount of information that most users do not know about and cannot control. For example, forensic analysts can often recover deleted files from a hard drive.

Computer operating systems and programs also generate and store a wealth of information about how the computer and its contents have been used. As more programs are used, those information, called 'metadata', become broader and more comprehensive. For example, the popular Windows operating system generates a great deal of important metadata about exactly how and when a computer has been used.

Common word processing programs such as WordPerfect and Micro-soft Word generate temporary files that permit analysts to reconstruct the development of a file. Word processing documents can also store data about who created the file, as well as the history of the file. Similarly, browsers used to surf the World Wide Web (www) can store a great deal of detailed information about the user's interests, habits, identity, and online whereabouts, which often the user also may not be aware of. Browsers are typically programmed to automatically retain information about the websites which the users have visited in recent weeks. **Understanding the above, will help authorized officer to take more appropriate decision in identification of crucial devices from where data is to be acquired.**

Importantly, the person in control of physical premises knows and has control over what has been stored in the premises. But he has a very limited control and knowledge about what is stored in the computer.

### **D. The Retrieval Mechanism: Physical vs. Logical**

Conducting physical search of a premise generally requires physical search of all processes where recovery of the evidence for which search operation is mounted is possible. Search team look from room to room for the evidence sought in the warrant. If the evidence sought is large, the search team will plan its search accordingly: If they are looking for a stolen car, for example, they can't look inside a suitcase to find it. After the search team has searched the space for the items sought, the search is done, and the search team will leave.

Computer searches tend to require fewer people but more time. Analysis of a computer hard drive takes as much time as the analyst has to give it.

In contrast to physical searches, digital evidence searches generally occur at both a "logical" or "virtual" level and a "physical" level. The distinction between physical searches and logical searches is fundamental in computer forensics: while a logical search is based on the file systems found on the hard drive as presented by the operating system, a physical search identifies and recovers data across the entire physical drive without regard to the file system.

The differences between computer searches and traditional physical searches raise difficult questions about the rules that should govern computer searches and seizures. Generally it is more difficult to plan a computer search *ex ante*; the search procedures are more flexible than procedures for physical searches, and they are more of an art than a science.

### 2.13 Other important aspects of handling digital evidence

Just like in the case of a conventional documentary evidence, merely gathering electronic evidence is not sufficient. It needs to be analyzed in the context of the facts of the case and relevant information needs to be extracted. Efforts have been made to corroborate the contents therein with material and oral evidences to reach to a conclusion useful for, or relevant to the proceedings under the Act. Unlike documentary evidence, extracting information is a tricky job in the case of a digital evidence as it can be password protected, encrypted or hidden. Further data may be properly visible only with the help of specific operating system or software. Thus, some other important aspects need careful consideration while handling digital evidence, which are briefly discussed here:

**2.13.1 Preliminary and detailed statements** of the persons in control of computers/ electronic devices (including system administrator) would be very important. In preliminary statements information regarding the hardware, operating systems, software and topography of the computers, various users and their roles and passwords should be extracted.

**2.13.2** The surrounding of the computers can sometimes prove very crucial. The search party should carefully look for:

- i) Computer Printouts in room, on table, in drawers, in dustbins, etc.
- ii) **Passwords:** On casing of computers, on tabletops, stickers, walls etc.
- iii) Manuals and reference books pertaining to computers
- iv) Physical Evidence such as documents, visiting cards, scribbling pads etc. On examination, relevant physical evidence should be seized.

**2.13.3** Under Income tax Act, **Section 132(1) (iib)** has been specifically brought in to remove difficulties in handling digital evidences found during the course of the search. This section *requires any person who is found to be in possession or control of any books of account or other documents maintained in the form of electronic record, to afford the authorized officer the necessary facility to inspect such books of account or other documents*. Thus, such person is obliged under law to provide all facilities to access the data inside, which include disclosing the passwords, details of OS and software and their functioning besides the physical access.

Further, provisions of **section 275B** make failure to comply with provisions of section 132(1)(iib) a punishable offence by imprisonment up to two years.



Thus, if the authorized officer is unable to open or have access to files containing books of account or documents maintained on electronic media, the person incharge of the premises shall be asked to make available such computer codes or passwords in statement under oath, bringing such provisions to his notice. The denial or deliberate non-furnishing of such passwords / secret codes must be brought out in the statement recorded by the authorized officer. The evidence regarding the presence of Panchas, and their statements as witnesses, recorded contemporaneously, would be important to establish the commission of offence under this section. Further, there are a few provisions under IPC also, which may be invoked, in case of non-cooperation in the form of hiding information or furnishing misleading information in sworn statements.

**2.13.4** It may be mentioned that if a person who is in control / possession of books of account / documents in electronic media, destroys the same to prevent their access by the authorized officer, it would constitute an offence u/s 204 of IPC.

### 2.14 Seizure of original device vs. Acquisition of data

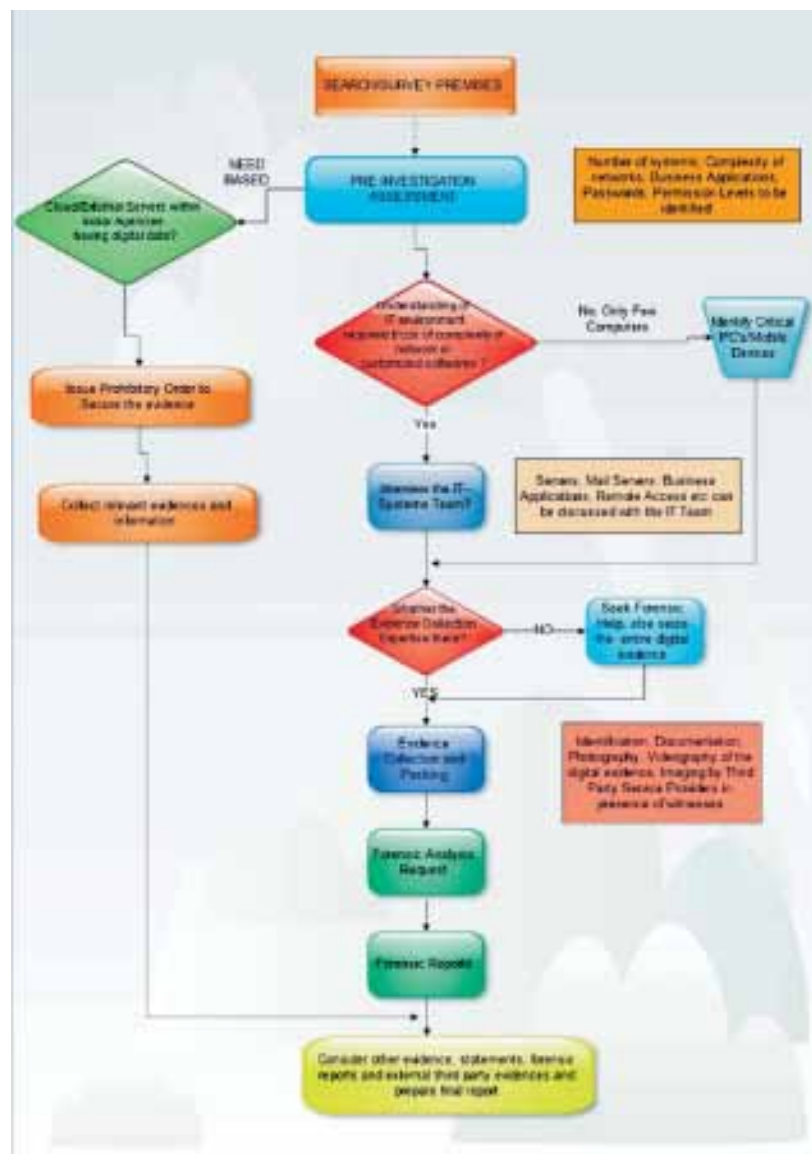
- a) In Income-tax Law, the “seizure” of documents etc., in the form of digital storage device means seizure of original device. Thus, for the crucial digital evidence, wherever possible seizure of original device is recommended.
- b) However one should understand that all computer data is a copy. Computer hard drives work by generating copies; accessing a file on a hard drive actually generates a copy of the file to be sent to the computer’s central processor. More broadly, computers work by copying and recopying information from one section of the machine to another. From a technical perspective, it usually makes no sense to speak of having an “original” set of data. Generating and analyzing bit-stream copies are routine parts of the forensics process, and no court has ever considered copies as different from originals. In terms of evidentiary value, the copy/clone made with bit flow technology using proper forensic tools is as good as original and is recognized as such in the Information Technology Act 2000 read with Indian Evidence Act. Therefore, seizure of original device may be done selectively. **But it should be kept in mind that such acquisition of data by making copy/clone may not amount to seizure of data as per the present provisions of Income Tax Act 1961 e.g section 153C of I T Act 1961 and proposed clause (e) of sub section 3 of section 159 of DTC.**



## Chapter 3

# Introduction to Digital Evidence Investigation & International Best Practices

3.1 Digital Evidence is highly fragile and can be tampered easily and precautions are required during the search, collection, preservation, transportation and examination of evidence. The flow chart for Digital Evidence is given below:



The sequences of Digital Evidence Investigation are as follows:

1. **Pre Investigation Assessment** which involves identification of key digital evidences and securing the same so that any data is not lost
2. **Collection of Evidence**
  - a. Procedure for gathering evidences from Switched off systems
  - b. Procedure for gathering evidence from live systems
3. Forensic Duplication
4. Labelling and Documenting of the evidence,
5. Packaging and transportation of the evidence
6. Analysis of Forensic Data by retrieval of deleted files and present files
7. Publication of the Forensic Report by linking all the reports and circumstantial evidences.

### 3.2 Some International Best Practices

Some important international best practices are :

- Reading/examining the data storage device under examination (subject device) through 'write blockers' which prevents any kind of writing on the subject device during the process of viewing the data on it.
- Making clones of the subject device (as distinct from copies) so that entire data on the subject device including hidden files, deleted data, slack space, formatted or deleted partition can be obtained, and using such clones for study/ examination while keeping the subject device undisturbed and safe. The cloning process produces a true image of the data storage device including the deleted data and hidden sectors.
- Authenticating the cloned disks by taking hash value of the subject device and the clones.
- Maintaining log of activities carried on the cloned disk.

### 3.3 Use of Cyber Forensic in Income-tax Department

- **Acquisition / Acquiring:** forensically acquiring digital data found during the course of a search and seizure or survey operation.
- **Analysis & Documentation:** analysing the digital data for uncovering hidden, password protected data, and deleted data
- **Archival:** safe archival of cloned disks for reference and future production
- Once all digital data have been recovered, the work of examining them for identifying violations of provisions of the Income-tax Act can be carried out.

## Chapter 4

### Important Related Terms

#### 4.1 Definitions:

- **Hash value:** A hash value is a unique and compact numerical representation of a piece of data. It is computationally improbable to find two distinct inputs that hash to the same value (or “collide”). **In short we can say Hashing is the transformation of a string of characters into a usually shorter fixed-length value or key that represents the original string.**

- **Wiper:** Wiper is a software or hardware tool which will wipe the complete Hard Disk Drive by replacing either 0 or 1 or a user defined value to its each sector. After wiping, the Hard Disk Drive will not be having data in any form on it.



- **Write blocker:** It is a hardware tool which, when used with any data storage device, will not allow to write on or modify the data in the storage device under examination.



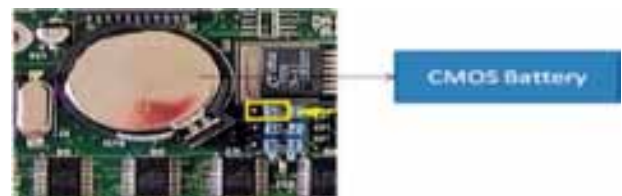
- **FRED:** It is a complete computer machine with additional in built write blocker and some drive bays, which can be used for both acquisition and analysis purpose.



- **FREDDIE:** It is almost same as FRED but is a portable one which can be taken to the premises.



- **Cyber Check:** It is software tool developed by CDAC, Trivandrum, which is used for both acquisition and analysis purpose
- **RAID:** an acronym for Redundant Array of Independent Disks. It is a technology that divides and replicate data among multiple hard disk drives. This distributes data across multiple hard disks but is seen by the computer user and operating system as one single disk. The Hard Disk Drives arrayed using RAID architecture, individually have no existence and therefore data cannot be extracted from individual hard disks.
- **Live forensics:** Live forensic implies taking the data from system (imaging or cloning) while it's running.
- **Customised software:** Softwares which are prepared by some vendor for a specific purpose for a company. Normally these softwares are based upon database such as oracle, MS-SQL etc.
- **Imaging:** Disk Imaging is the process of copying content of source digital media on destination digital media sector by sector, bit by bit, in the image file format such as .E0 or .P0 depending on the software used.
- **Cloning:** Disk cloning is same process as that of imaging. These two terms are interchangeably used. The only difference is that in the case of disk cloning, one can replace the source disk with the destination disk and the computer system will boot and work because cloning is done either for a whole disk or a partition in the same disk geometry.
- **Logical Partition & Physical Partition:** In the computer two types of partitions are present-
  - Physical Partition – A number of hard drives physically present in a computer system.
  - Logical Partition – A number of partitions on a given hard drive. Normally shown in a computer as, C, D drives and so on.
- **BIOS:** Basic I/O System is used to store the information required for starting the system.
- **Booby Traps & Logical bombs:** A booby-trap/logical bombs is usually a hostile piece of computer code that wipes out files or does damage to evidence. The hostile code may destroy critical data with great precision. Or the booby-trap could be an actual bomb that would physically damage the computer and it's disks
- **CMOS:** CMOS battery is present on mother board which is used to store time and some kind of password.



## 4.2 Types of Hard Disk Drive and their connectors:

- SATA



- IDE



- SCSI

This type of SCSI hard disk is normally used.



Ports of other different type of SCSI hard drive.



- **SAS**

There also may be many other kind of SAS HARD DISK DRIVES but normally used type is shown in figure:



#### 4.3 Types of digital Storage:

- Hard Disk Drive
- Flash Drive
- CD/DVD
- External Hard Disk Drive
- Floppy Drive
- SIM Card
- Memory card
- Tape Drives
- I-POD/ MP3 players

#### 4.4 Abbreviations:

- RAM: - Random Access Memory
- Types of HARD DISK DRIVE:-
  - SATA: Serial Advance Technology Attachment.
  - IDE: Integrated Development Environment.
  - SCSI: Small Computer System Interface
  - SAS: Serial Attached SCSI
- BIOS: Basic Input Output System
- CMOS: Complementary Metal Oxide Semiconductor
- Storage Units: GB (Gigabytes), TB (Terabytes).
- Forensic tools:-
  - FRED: Forensic Recovery of Evidence Device
  - FREDDIE: Forensic Recovery of Evidence Device Diminutive Interrogation Equipment.

# Pre Investigation Assessment of Digital Evidences

### 5.1 General Principles

When dealing with digital evidence, the following general forensic and procedural principles should be followed:

- Actions should be taken to secure and collect digital evidence in such a way that it does not affect the integrity of the evidence.
- Persons conducting an examination of digital evidence should be trained for such purpose.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review.

The first step in Digital Evidence Analysis is the Pre-Investigation Assessment of what Digital Evidences needs to be acquired, imaged etc. The officer in charge may take clue from certain guidelines discussed below when deciding the potential digital evidences which needs to be acquired or imaged.

### 5.2 Preliminary review of the Premises

Typically premises can be broadly dealt under :

1. *Residence with one or few computers, hand held devices*
2. *Office with few computers*
3. *Companies /Organizations with vast and complicated network of systems*

At the premises, the investigating officer should carefully survey the premises, observe and assess the situation and decide on the steps for proceeding further. The digital evidence is highly fragile and it will be available in a number of devices, locations and in various formats. Hence it is important to do a preliminary review of the premises to identify the key digital devices in the premises. *For example, in an organization which has multiple branches, it is not necessary to take digital evidence at all branches since all the data of the branches will be in the central database of the company at the headquarters. So the key digital device is the servers on which this data is stored in the headquarters.*

### 5.3 Evaluating the Premises

- The officer in charge should secure the premises and none should be allowed to access any computer



without the permission of the officer in charge. The officer in charge may take note of every individual physically present at the premises and their role at the time of securing the premises. In case of big organizations, ask who is the system administrator.

- **Disable the internet connection:** Internet connection should be immediately turned off to avoid remote internet access to prevent changes in data through internet.

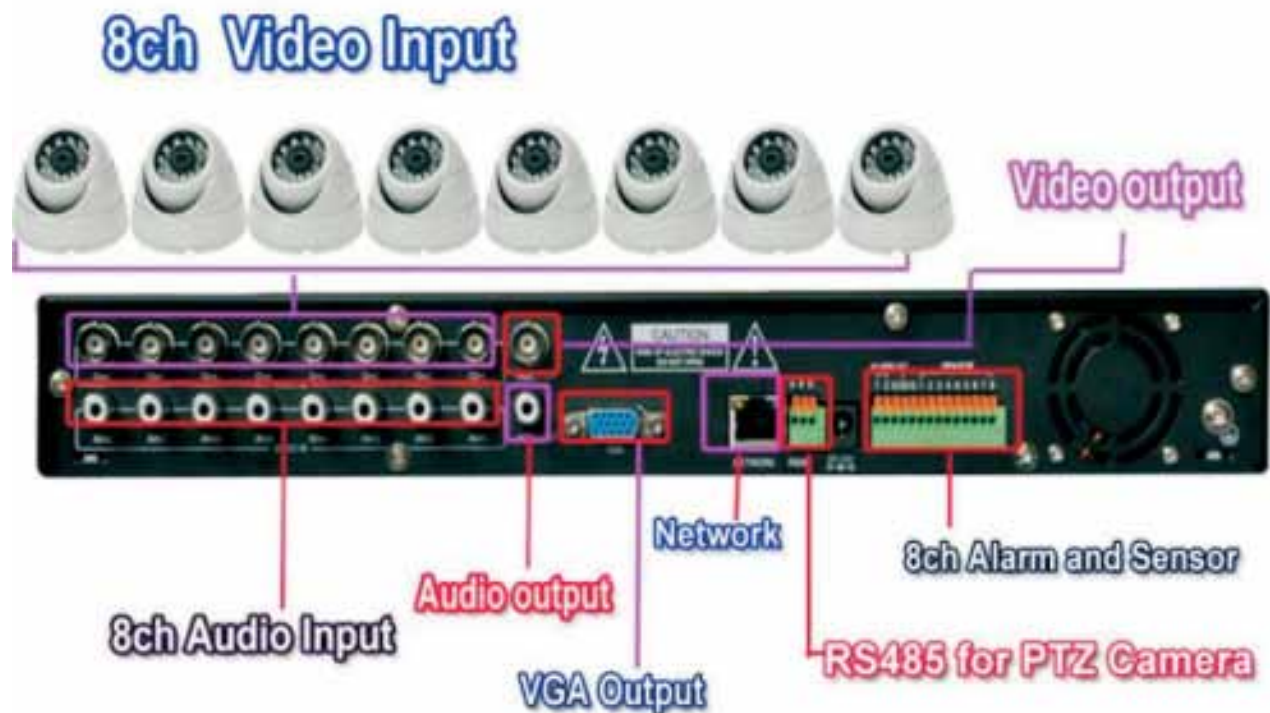
**How to disable internet:**

- Switch off modem/routers.
- If cannot find modem/routers then either switch off the LAN or unplug the LAN cable.
- **Disable the LAN:** If possible, **disable** LAN from the server. If there is no work to do through the network like taking printout or any other kind of data analysis, the LAN should be disabled to avoid unauthenticated access to data.

**How to Disable LAN:**

- Switch off the LAN switch.
- or Go to Control Panel-->Network and Sharing Center-->Local Area Network-->Disable.
- If you locate the switch or cannot find setting of LAN in the system final option can be to unplug the LAN cable from the server.
- **Disable CCTV :** Ask about the CCTV server location. Usually security guard should know.

A typical CCTV back panel looks as follows:





- Disconnect all video and audio inputs as soon as possible if you still want access to the videos. If not directly disconnect the power to turn it completely off.

- **Identify Important PC's:**

Find out if there is an organizational chart for all the senior management. If none, then ask around to create one yourself. Ask the staff to identify their offices/desks. Note all the electronic devices/computers and storage media for each person. Attach paper stick-it notes to each such device noting the person name and make/model of the device.

***E.g. 'John Doe – Laptop Dell Vostro'.***

Let the officer in command know that you have identified the computers for important personnel at the company. Wait for their instructions as to what to do with each; backup/imaging etc. If the main accounting server has not been identified yet, then try to find it by asking around. Wait for officer instruction on what to do with the accounting machine.

Ask if there is any cash counting machine on premises. Typically it would be next to a computer where data entry takes place. In case cash counting machine is present, and if officer has already verified a particular person who is responsible for data entry for cash transactions, then note down location of the computer where they do data entry on and wait for further instructions from the officer. Identify important persons who deal with sales, purchase, banking etc. Tag their machines with sticky notes to indicate what activity happens on that particular PC.

Identify the systems which have data related to the case under investigation or which belong to important persons such as computers of accountants, managers, directors or owner(s) where important digital data including deleted files can be found relevant to the case which may be required to be cloned. This step will simplify work and will help to take important information out of huge amount of data. This is a manual process and for this, the assessee has to be asked about the user for each of the computer systems available at the premises. *Some standard interviews can be conducted with the key IT personnel, the details of which are given at the end of this chapter.*

- **Identify the location of servers:** Identify different servers along with their physical location and find out which servers are related to the case under investigation such as File server, Database Servers, Mail Servers and Accounting Servers etc.

In most cases there will other machines around where CCTV server is placed. Typically this will be the server room. Ask to identify the function of each machine. There is high probability of main storage server and accounting server being in the same server room. Inform the officer in command that you have located their main accounting server and storage server. Wait for their instructions as to what to do with each; backup/imaging etc. A typical server room will contain rack mounted servers with networking hardware. It can look something like following:



- **Collect Passwords:** There may be many kinds of password in computer to get access to that computer or to the files such as:
  - **BIOS password:** *The first thing to do is to ask the assessee to provide password. If he doesn't, we can remove the BIOS password by removing the CMOS battery for half an hour, again put it in the system and restart the system. The BIOS password will be removed.*
  - **Operating System password:** *Ask the assessee for the password. If he does not provide the password, then there are some password crackers for normal use operating system such as Windows XP, and Windows Vista.*
  - **Password for MS office files:** *Ask the assessee. If he does not provide the same, then there are some password cracker tools such as Rainbow Table.*
  - **Password for Tally files and any customized software:** *In this case, it is somewhat difficult to crack. We may ask the assessee for the passwords. But with some efforts, Tally file passwords can also be cracked.*
  - **Password for Gmail, Hotmail etc:** *If web based email (Gmail, Yahoo, Hotmail, other hosted email service ) then get username and password for all important accounts.*
  - **Password for Online Accounting Software:** *If there are any web based accounting systems which are present then relevant username and passwords.*

In case of passwords, the best option is to ask the assessee to provide password. The assessee is bound by law to provide such password. It is only when the assessee has not provided passwords that we use crackers for the same.

- **Securing Mail Boxes:** Acquire the user id and password of email account of assessee and some important persons of the business concern, if there is any, and change the password immediately to secure the mail box. The changed passwords should be noted down at a secured place for further analysis of emails.
- **Identify Volatile Data if any:** Volatile data refers to data on a live system that is lost after a computer is powered down or due to the passage of time. Volatile data may be lost as a result of other actions performed on the system. So officer in charge should consider acquiring volatile data ( if crucial for investigation ) on priority over non-volatile data
- **Identify Server Hardware Architecture:** Identify the hardware architecture, whether it is a normal server or a RAID server. At the time of acquisition, this should be kept in mind because acquisition process will vary depending upon the architecture of the server.
- **Identify Customized Software Used:** Identify the customized software's which are being used by the assessee, and collect information such as vendor of the software's, database used by the software, their file format and passwords. If the software are operated with **smart card/dongle keys**, (small hardware token keys generally validated through the USB port); then one must take possession of the smart card/dongle keys as in the absence of such keys software will not function.
- **Identify Cloud Data:** Cloud data is any data which is stored on a remote server. The types of data

typically stored on remote servers can be email, ERP application data or company intranet. Cloud hosting can be of following types:

- **Physically hosted server (also known as Colocation hosting)** : Colocation hosting is when server is stored off-premises in a dedicated secure data center owned by a large service provider like Tata Communications, NetMagic, BalaSai etc. Usually this should be in the same city or a nearby metro location. Sometimes this can also be located in another state of country. Such types of installations are typically managed by third party IT consultants. Getting the name of such consultant should make extract data from such servers easy. The data backup or image acquisition is better done on premises only. This would require proper security clearance from data center staff on premises.
- **Virtually hosted server** : Typically virtually hosted servers have no dedicated physical hardware assigned to it. Examples are Amazon EC2, DigitalOcean, Linode etc. In order to extract data from such remote servers, administrator level access on the Virtual machine is required. The data backup or image acquisition has to be run remotely and it will take a very long time for such acquisition to complete because of the bandwidth issues.
- **Cloud hosted data** : There are a number of online data storage providers like Google, Yahoo, Microsoft, Dropbox, Box.net etc. Extracting data from such providers without username and password will involve lengthy legal procedures. Even if username and password is available, bandwidth limitations will seriously hamper backup process.
- **Artifacts of cloud data**: User browser history, email client settings, cloud sync applications like dropbox etc. would giveaway whether the user is utilizing cloud data or not.
- **Identify all Key Mobile Devices**: All Key Persons Mobile Devices should be taken in to control and ensure that there is no scope for deletion of data in the Mobile Devices. The Mobile Devices if no volatile data exists, should be kept in switched off mode. **Identify any cloud data which is present or not. Login into cloud and change the password so that no one else can login into the system from outside to destroy the data in cloud.**
- **Identifying Encrypted Volume of Data**: There are some cases where Assesses store its important data in encrypted volume using application like TrueCrypt, Bitlocker etc. Using a program call TCHunt we can detect an encrypted Volume. To use TCHunt open command prompt and change directory to TCHunt location.  
run the command  
**>TChunt.exe -d Drive\_Letter: 2>nul**  
e.g. >TCHunt.exe -d C: 2>nul  
similarly run the same command for other logical drives.  
  
If Tool detects any Encrypted Volume it will show you the actual path for that volume. **As per TCHunt Documentation, It may give you false positive results**
- **Identifying history of USB media connections**  
In many cases we have found a printed piece of paper of interest but no corresponding document. Even after searching all the PCs on premise no trace of such document can be found. One the possible

explanation of such a puzzling situation may be that the document it-self is stored on portable media such as USB drive. In such case, it is important to ascertain whether USB devices were connected and how recently on all on premise PCs. A tool called USBDeview.exe help in such investigation.

Double Click on USBDeview.exe it will show you the USB device history.

Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive L...	Serial Number	Created Date
Port_#0002.Hub_#0000	CDM Flash Disk USB Device	Mass Storage	No	Yes	No	No		15667403093E	7/23/2014 2:
Port_#0002.Hub_#0000	HP v100w USB Device	Mass Storage	No	Yes	No	No		145478000420FE08	7/23/2014 2:
Port_#0002.Hub_#0000	HP v100w USB Device	Mass Storage	No	Yes	No	No		CLOCK444TALL	7/23/2014 2:
Port_#0002.Hub_#0000	HP v100w USB Device	Mass Storage	No	Yes	No	No		W32VWQJ6TE0A3G3H	7/23/2014 2:
Port_#0002.Hub_#0000	HP v100w USB Device	Mass Storage	No	Yes	No	No		W32VWQJ6TE0A3G3H	7/23/2014 2:

If the USB connection log shows a regular pattern of USB device connection then let the Authorised officer know your findings so that he/she may include that in their investigation.

- If the systems are Off, they should not be turned ON for the inspection. If systems are on, it is advised to leave them ON
- If systems are ON at the scene of offence, Officer in Charge should take appropriate steps to photograph it, plan for the seizure of the evidences at the earliest and document it. Officer in Charge should ensure that perishable evidences ( volatile data) are appropriately recovered without any loss.

#### 5.4 Model Questionnaire/Checklist for Pre – Investigation Assessment at Corporate Organization with multiple computers or vast network of computers

1. Who are the key members of the Information Technology Department?
2. What applications and software, databases are being used by the Organization?
3. Who are the developers of the applications that are used?
4. Who provides the support and maintenance for the application?
5. Where are the actual servers located?
6. Who has the administrative and super user privileges?
7. What is the backup policy of the organization?
8. What kind of backups is taken and how long they are retained?
9. What levels of access are given to employees? Are they allowed to carry thumb drives, CDs, or other devices?
10. Has anybody access to remote login or VPN to any of the servers?
11. Are the employees permitted to use the official laptops for accessing internets?
12. Is there an email server present if so where is it located?

13. From where is the website hosted? Does the company own any cloud space where data is stored?
14. Whether the company is giving company owned mobile numbers to its employees? Obtain the list of mobile numbers used by the key employees.

#### **5.5 Model Questionnaire/Checklist for Pre – Investigation Assessment at Offices/Home with few PC's**

1. Identify the number of PC's/Computer System
2. Identify the type of connections ( Wi-Fi/Ethernet)
3. How many computer systems are used for internet connection?
4. Who are the persons with access to system?
5. Obtain the details about the removable storage media (including external hard disk) used/owned by the user.
6. Obtain details about the network topology and architecture(client-server) if any
7. Obtain the details of all passwords of emails
8. Secure all mobile phones and the details of the persons in whose name the SIM is registered.

The above formats for pre-investigation assessment will help the investigating officer to understand the situation in detail and decide on the kind of technical support to be requisitioned, to proceed with the acquisition of evidences.

# Forensic Collection of Digital Evidences

### 6.1 Identifying/Seizing of the devices needs to be forensically imaged for analysis

Ensure that the Pre-Investigation assessment as discussed in Chapter 5 is complete and accurate before you commence the Forensic Collection of Digital Evidences. Make an assessment of all the digital devices which are crucial for the case and that needs to be seized or imaging needs to be carried out or backup can be taken. If forensic help or technical help is available on-site then the officer in charge should plan for on-site forensic imaging or backup. Otherwise, the officer in charge should plan for a simple seizure of the equipment which would be discussed below. In case it is very difficult to make a pre-assessment on finding where the crucial evidences are available, the officer in charge may seize the same. It will increase the workload, but no loss of crucial evidence is there. It is also advisable to preview the data storage mediums found at the site (including removable storage media such as pen drives, external Hard Disk Drives, tape drive etc.) to decide which of the disks would need to be imaged/ cloned or seized by viewing contents of the media and their relevance to the case. Such previews have to be done with the help of write blockers.

### 6.2 Seizure / Impounding of the Digital Evidences under Search/Survey

If the on-site technical help is not available, the officer in charge should plan for seizure of the digital evidence so that the same can be sent to the forensic laboratory for analysis in later on stage. Proper Seizure memo and Seizure Proceedings must be drawn and the following things should be reflected in the Seizure Memo:

- Make sure that one person from the technical side, one from the assessee side and two independent witnesses are part of the search and seizure proceedings
- Please refer the Pre-Investigation Assessment of Digital Devices as discussed in Chapter 5 for cross verifying and correctly documenting the technical information regarding equipment, networks and other communication equipment
- Time Zone/System Time should be carefully noted if the system is in switched on position
- Don't switch on any devices
- Allot a unique device number and the same should be duly reflected in the Panchnama, Chain of Custody and Digital Evidence Collection Forms.
- Make sure all potential digital devices that needs to be seized are photographed along with the respective reference like cubicle number or name room surroundings etc. This is important since assessee may claim that the same was implanted without his knowledge.

- If the hard disk is removed, a photograph of the hard disk drive should be taken
- If Possible paste a serial number on the digital device so that it can be related to the exact case , date and the section under which it is searched
- Make sure that panchas have some knowledge about various digital devices. *It is advisable to include a writing from panchas that they have been explained the various digital devices that have been identified and also the various procedures used in Forensic Collection*
- Document the chain of custody and Digital Evidence Collection forms which are explained in the next paragraph. Please fill all the details in the forms before seizing the same.

### 6.3 Digital Evidence Collection Form

Digital Evidence Collection Form ensures proper documentation of all the information about the evidence that is visible to the naked eye. It should contain the following details:

- *Case Name/Date of Search/Name of the Authorised Office and Address of acquisition*
- *System Information like Device Type/Manufacturer/Model Number/Serial Number/BIOS Date(Time)*
- *Type of Media*
- *Details of Forensic Software and Version Number*

Digital Evidence Collection Form			
Name of the Authorized Officer:			
Name of the assessee :			
Date:	Time:	Premise Address:	
Examiner's Name and Details:			
Computer Information			
<input type="radio"/> Laptop	<input type="radio"/> Desktop	<input type="radio"/> Server	<input type="radio"/> File/Folder
<input type="radio"/> Others	If Others Specify		
System State		If switched On, What is visible on screen?	
<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> Hibernation/Sleep			
System Info	Make: _____ Model: _____		
	Serial No: _____ Size: _____		
Whether Volatile Memory/RAM Memory was collected? _____			
Shut Down Type	<input type="radio"/> Normal <input type="radio"/> Power Plug pulled <input type="radio"/> Battery Removed (Laptop)		
Is the suspected media encrypted?		Type of encryption Software used	
<input type="radio"/> Yes <input type="radio"/> No			
Hard Disk Handling: <input type="radio"/> Seizure <input type="radio"/> Forensic Previewing <input type="radio"/> Imaging <input type="radio"/> Backup			
Details of Imaging Software/Version to be given			
Is the hash value calculated?		Algorithm:	
<input type="radio"/> Yes <input type="radio"/> No		<input type="radio"/> MD5 <input type="radio"/> SHA <input type="radio"/> OTHERS	
MD5 hash value:			
SHA hash value:			
Other Authentication Method:			
Storage Copy Details		Working Copy Details	
Make: _____ Model: _____		Make: _____ Model: _____	
Serial No: _____		Serial No: _____	
Is the hard disk replaced back?		Date:	Time:
<input type="radio"/> Yes <input type="radio"/> No			
Is the signature of the witness taken? <input type="radio"/> Yes <input type="radio"/> No			
Note by the AO regarding the potential evidences in the digital devices:			



## 6.4 Chain of Custody Form

Chain of custody refers to the documentation that shows the people who have been entrusted with the evidence. It should document the details of the people who seized the equipment, the details of people who transferred it from the premise to forensic labs, people who are analyzing the evidence, the details on when all it was opened and so on. This is very important since the assessee may level charges of tampering and fabrication of evidence and it would be difficult to prove the integrity of the evidence, if the chain of custody is not maintained. It is advisable to maintain a Chain of Custody form along with Digital Evidence Collection Form. A Model Chain of Custody form is enclosed below:

Chain of Custody Form					
Name of the assessee :					
Date:	Time:	Premise Address:			
Description:					
Chain of Custody					
Reason/Action	Received From	Received by	Data	Time	Signature of parties

**Checklist for Fool proof chain of custody:**

1. Take photographs and systematically record observations
2. Guard against thefts and mechanical failure
3. House Multiple copies in different locations
4. Use Good Physical Security and data encryption
5. Protect digital magnetic media from external electric and magnetic fields
6. Account for all people with physical or electronic access to the data
7. Keep the number of people involved in collecting and handling the devices and data to a minimum

**6.5 Standard Operating Procedure for gathering evidence**

Some important points to consider :

**1. Stand Alone/Non Networked Computer Systems:**

- Shutting down a computer system which is up may result in loss of volatile data which may be erased in the process of switching off
- If Forensic professional notices tampering or manipulation, the computer may require a forcible shutdown
- Computer Systems should be checked for Encryption Volume being present in the system

**2. Networked Computer Systems:**

- Collection of data may be a challenge if it is in a cloud environment
- Computer Networks are technically complex and technical assistance should be asked from system/network administrator for collection of evidence in a timely manner

**3. Removable Media:**

- Removable Media like USB's is easily hidden because of their size
- Officer in charge should take control of the system since these devices are susceptible to immediate physical destruction

**4. Hand Held Devices:**

- These devices are susceptible to immediate physical destruction and should be secured immediately.
- Active devices are susceptible to data destruction due to network communication
- The device may be protected with a password or PIN

### Standard Operating Procedure for gathering digital evidence

1. Secure the premises both physically and electronically. Computers, other peripherals are likely to be found on all floors on the office space. The servers, networking devices will be usually installed in a separate enclosure. The following activities are to be taken up immediately on entering the premises
  - The employees should be kept outside the main data center, server room and should be requested not to switch on the systems
  - Check for the networking devices and also the internet access. The internet services, Wide Area Networks (WAN) and Local Area Networking (LAN) should be disconnected in all cases except in cases where mission critical applications are running
  - Photograph of the server room and other major facility should be taken
  - The personnel should be requested to empty their pockets and contents should be examined. The pen drives or other storage devices should be collected. Smartphones are also classified as computers. The smartphones used by the important persons in the value chain should be collected and examined
  - While disconnecting the network, the wireless devices should also be turned off
  - The systems that are already switched off should not be switched on. The systems that are already switched on should be examined. These systems are to be switched off or disconnected from the network. In case of systems that are supporting mission critical functions, they can be left as it is.
2. Make sure that the computer is in Switched off mode. Sometimes some screen savers may give a false notion that the computer is Off. For this the hard drive and monitor activity lights should be checked to see whether the computer is on. In case of laptops, on opening the lid, the laptop may open. So it is advisable to remove the battery from the laptop computers
3. In case of a computer, search for all wireless/wired networks connected to the computer. Document all connections to the computer. In case computer system is connected to a network, ask the system/network administrator to isolate the system from the rest of the network. Capture all the details of shared net connections, active network connections to the computer. If the system cannot be taken off the network or in switched on mode, live imaging of relevant data can be carried out using appropriate tools.
4. In case of live systems also recover volatile memory dump/RAM Memory dump using appropriate tools. Also check whether there is an encryption volume in the system. Appropriate Softwares can be used to retrieve the encryption volume.
5. In case of hard disks taken out from switched off PC's record unique identifiers like make, model and serial number.
6. Get the signatures of the assessee and witness on the hard disk using a permanent marker
7. Search for Non-electronic evidences like diaries, notebooks or pieces of papers with passwords.

8. After the Hard disk is removed, Switch on the system and go to BIOS. Note down the date and time shown in BIOS
9. Connect the Hard Disk for logical back up or forensic imaging/cloning
10. In case of switched on computers, if live imaging is not possible, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket, this will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.

## 6.6 Forensic Duplication – A Technical Introduction

**Forensic Duplication** is a process of bit-stream imaging of the digital evidence by which entire data is transferred to a storage medium. Files can be copied from suspected storage media using two different techniques

<b>Logical Backup</b>	A logical backup copies the directories and files of a logical volume. It does not capture other data such as deleted files or residual data stored in slack space
<b>Bit Stream Imaging/ Forensic Imaging/Cloning</b>	Also known as Disk Imaging/cloning/bit stream imaging generates a bit by bit copy of the original media, including free space and slack space. Disk Imaging usually takes more space and takes longer time to perform.

The Table below gives the difference between doing a backup and taking a forensic image

<b>DOING A BACKUP</b>	<b>DOING A FORENSIC IMAGE</b>
Backup is copying the selected files and folders logically.	Forensic Imaging is copying the physical sectors of the hard disk irrespective of files, folders or empty.
It changes the metadata of the files.	No change of metadata since it uses write blockers.
Assessee can allege that Departmental officers manipulated data because MAC (Media Access Control) timings change during back-up process.	MAC(Media Access Control) timings do not change and the tools are write protected.
Executable programs are not accounted.	Such programs could be examined.
Recovery of deleted files is not possible.	Deleted files could be recovered.
No hash values are generated for the system.	Hash value is generated for the whole disk and so also for single files.

Post search no detailed analysis such as registry info, timelines, and connected devices could be carried out.	Post search, all such analysis could be done.
Backup copies only visible & known files/folders.	Imaging copies whole system of the assessee.
Backup doesn't give internet history/chats/ information regarding internet usage.	Imaging gives internet history, chats and also carve out deleted skype messages / chats.

Whether to image or backup a particular device is discretion of the Authorized officer. Imaging is a much longer, time consuming process which typically requires considerable storage. Backup is relatively quicker, to-the-point procedure and storage requirements are considerably less. However if the digital device has critical data which can be challenged in the court of law, it is always advisable to image the system. One more drawback of the Data Back up is that deleted files cannot be retrieved from these Data Back Up. If the officer in charge is sure that there are substantial deleted files in the system, he should image the system instead of taking data back-up. However data back-up is very handy in places where it is difficult to get forensic teams especially in mofussil areas. Even in SAP/ERP/Accounting Servers it is advisable to clone the devices.

## 6.7 Forensic Duplication – Logical Backup

Some precautions to be taken while taking Logical Backup:

- During backups, the integrity of the original media should be maintained. Investigator should use a write blocker while backing up. This is also applicable for Forensic Imaging/Cloning. A write blocker is a hardware or a software-based tool that prevents a computer from writing to computer storage media connected to it. Hardware write blockers are physically connected to the computer and the storage media being processed to prevent any writes to that media.
- After Backup or imaging is performed, it is advisable to verify whether copied data is exact duplicate of the original data
- You can also compute hash value for this copied data to maintain the data integrity. Notice a change in one bit also will change the hash value.

Logical Backup in smaller cases may help in retrieval of data on the spot and the assessee may be confronted with the evidence immediately. Following are the most common types of user generated content relevant for assessment and investigation purposes,

- o **Excel:** Most important from financial transaction perspective.
- o **Word documents:** Can contain important agreements, other clues
- o **Email (PST) :** Can contain very relevant conversations pertaining to financial transactions
- o **Tally Data:** Can contain accounting and parallel books of accounts.

Depending on the line of business and modus operandi, the officer in charge may take data backup of other files like database files, pdf etc or may take the complete data backup of the systems. ***Some examples of backup are given in Annexure-1. These software's are only for the purpose of illustrations and neither recommendatory nor mandatory to be used.***

## 6.8 Forensic Imaging/Cloning

If on previewing, important data is found either in deleted or in active form, the storage medium is required to be cloned for evidence purpose. Otherwise a normal data backup can be taken. The following steps should be taken at the time of cloning :

- **Preparation-** As part of preparatory work, it is necessary to start with preparation of blank disks for use in cloning. These disks will need to be forensically wiped to ensure that no data is present. This eliminates any possibility of contamination of data of source disk by any old data present on the hard disk on which cloning is to be done. This will require digital wiping hardware which can wipe disks at high speed.
- After wiping the destination hard disk i.e. the hard disk on which we will clone or copy , the same is connected to the laptop or any computer system where the data acquisition software is loaded through write blockers. This will ensure that no changes take place in the data being acquired at the time of viewing, analysing or cloning. Some hardware's come with built-in write blockers. Therefore, separate use of write blocker is not required. It should be kept in mind that maintaining data integrity while imaging is essential for establishing the acquired data as admissible evidence in a court of law/ or any subsequent proceeding.
- In case of places where high end forensic equipments are not available, a simple set-up such as a high-end laptop equipped with Write blockers and forensic software kit would ensure Write-Protected previewing and acquisition of data from all types of system interfaces at the site itself.
- In cases where very high capacity disks/ servers (Over 200 GB) are found at the search premises, separate Hardware imaging devices, which are up to ten times faster, would be needed. These hardware devices have in-built authentication engines. On completion of the imaging process, the device displays the hash value of the cloned hard disk. The image/clone has to have the same hash value as that of the target hard disk. The Hash value should be recorded in the *Panchnama* and the assessee can be given the option of seeking a copy of the imaged/ cloned hard disk by paying the copying charges.

Some of the ways for acquiring data in a forensically sound manner from different devices are:

- **Hard Drives ( Desktops/Laptops/USB drives ):** Use forensic softwares like Encase, Cyber Check Suite, FTK to image the drives. Be sure to use a write blocker to protect the integrity of the data
- **Smart Phone:** Use software like Encase, Cellebrite, Paraben Device. In this case precaution should be taken while working with the mobile phones in ON mode, like usage of Network jammers/Faraday's bag.

In some cases like MAC Laptop it is not possible for the hard drive to be removed. In such cases, the entire device needs to be seized.

**Step for the Imaging/cloning** are as follows:

- **Live Forensics:** If live data is required (i.e. data which is in RAM when system is already running) then extract the live data using softwares such as Helix.
- **Shut Down Systems:** If live data is not required then shutdown the system properly by removing the power card from the Central Processing Unit (in case of Desktop) or by removing battery (in case of Laptop).
- **Identifying the Type of Hard Disks:** Take out HARD DISK DRIVE and identify the type of HARD DISK DRIVE e.g. SATA/IDE/SCSI/SAS.(ref. chapter 3)
- **Size of Hard Disk:** Determine the size of HARD DISK DRIVES and arrange the HARD DISK DRIVES accordingly in which we have to clone the hard disk.

**How to determine size of HARD DISK DRIVES:**

- Start Menu-->Control Panel-->Administrative  
Tools-->Computer Management-->Storage-->Disk Management.

It will show the size of hard disk drive.

- The size of a HARD DISK DRIVE is written on the Hard Disk Drive such as –GB.
- **Connectors:** Identify the related connectors and convertors. This can be done by identifying the type of Hard Disk Drives and their related ports.
- **Connecting Digital Evidences:** Connect evidence to cloning/imaging machine through write blockers and using connectors.
- **Imaging:** Start imaging using imaging software (e.g. Cyber Check, Encase) or hardware (i.e. Forensic Duplicator). **Do not interrupt** while the imaging process is going on.
- **Data Verification:** After completion of imaging the drive should be verified to check whether the data are written properly or not. Sometimes it may be possible that the software/hardware tool will show completion of imaging but nothing will be written on the destination Hard Disk Drive. So, always ensure that the data has been copied on destination Hard Disk Drive after completion of the imaging process. Hash Value of the evidence disk and the destination disk shall be generated. The hash value of both the discs should be the same. If they are different, then it implies that either imaging was not done properly or destination disk was not properly wiped.
- **Report:** Take printout of report generated by the imaging tool which contains the details of imaging attributes, details of Hard Disk Drives imaged, date and time and the most important thing **the hash value of the Hard Disk Drive**. Attach the report along with *panchnama* as an annexure to it.

Typically two images of each hard disk/ server would be needed to be taken- one for archival and reference, and the other for use as a working copy.

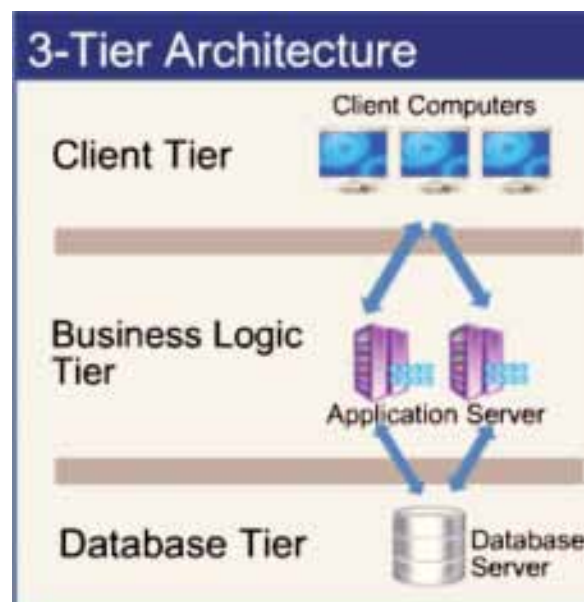
*Some examples of imaging using various software are given in Annexure-2 This is only an example given to illustrate the imaging process so that the officer in charge has an idea of the imaging process. The software explained is not mandatory to be used. Different softwares can be used according to the discretion of the respective directorate. Other Software which is popular in Imaging is Encase which is not explained below. Separate Manuals are released by OEM's which can be accessed by the user of the software.*

## 6.9 Handling Servers & ERP (Enterprise Resource Planning).

Most mid-to-large size businesses in India tend to employ some ERP system other than Tally for various reasons. Such ERP system almost invariably is a RDBMS (relational database management system) with a front end in the form of Windows/ Java/ Web based application. RDBMS is one of popular databases like MS SQL Server, Oracle, MySQL etc. Some other types of databases like PostgreSQL, IBM DB2, Sybase etc might also exist. We have observed two distinct trends when it comes to corporate ERP systems:

- a. **Custom made ERP systems:** Many companies intentionally or unintentionally develop their own in-house ERP software by employing programmers. This is one of the best case scenarios for investigation as it readily provides intricate accounting details on how transactions take place.
- b. **Readymade ERP systems:** Systems such as SAP, Microsoft Dynamics, Oracle Financials, RAMCO are examples of ERP stacks which can be bought and implemented. Although each of these systems need to be significantly customized to fit specific business needs of the firm.

The structure of a typical high level ERP is something like following:





It is very much possible that all 3 tiers are hosted on separate servers. From data perspective 'Database Tier' is most important. Hence backup of the RDBMS is must. Usually if RDBMS table structure is known standard issue reports such as 'Purchase order details by year', 'trial balance by year', 'cash transactions by year' can be extracted from the database itself. But if the goal is to recreate the complete ERP application off-site then imaging all the machines involved from 'Database' and Business logic' tier and one of the client machines is must. This is the bare minimum strategy required to recreate the entire system offline. Due to advances in storage technology through years additional challenges may exist if an advanced storage. Following are the big 3 ERP systems used by mid-to-large size businesses in India which have relational databases as their back-end.

- SAP
- Microsoft Dynamics
- Oracle Applications

There are small india specific ERP software developers like Udyog, Ramco, Quadra which are also used to a lesser extent. All of them follow a multi-tier software architecture.

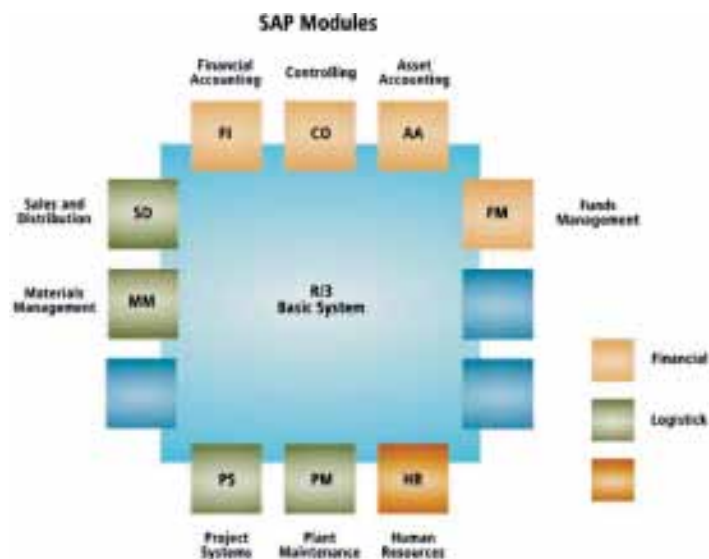
For Income Tax Department, backup perspective taking back-up of database tier is a must. In many cases Business logic tier and database tier are part of the same system. In that case imaging done for a single machine would suffice. If that's not the case then separate imaging would need to be taken for machine hosting business logic and machine hosting database. Usually there is no need to take imaging of the machine which has client as it is generally just an executable or in case of web application not even that. You can take help of the system administrator to take backup of the database tier and structure of the same and also take help of the business applications manager to recreate the environment at your office.

### ***Some Important Questions in handling ERP /SAP systems***

- Usually, the role of the server for an organisation is greater than any stand alone computer. Shutting down a server may damage the business or may lead to shutting down of key processes. Books of account, database, users data, etc often lie on the server. Hence, some times, it is difficult to seize the entire server with or without the original hard drives, or to make forensic working copy, or to get time to make necessary arrangements to clone the hard drives.
- The assessee may be using a customized accounting package or ERP solution on his server, which normally uses Oracle, SQL, MS Access, etc. as backend database. In such cases, even if an accessible cloned working copy of the server has been made, it might not be possible to access the accounting package or ERP solution because this application needs exactly same environment to run. Also, bad handling of the server may lead to corrupt the database permanently.
- How to access such accounting package/ERP fully without making alteration or corrupting the database and of course without hampering the ongoing business of the assessee?
- How to access the application packages which can run only with a Dongle key?

### *Some Simple Strategies in analyzing server data*

- Where customized accounting package or ERP is being used, a dummy server (assessee may be asked to help) with the same application and database software on an ordinary computer with proper license can be prepared. After the dummy server is ready, the cloned copy of the server can be attached with this dummy server and the database inside this cloned copy can be easily linked with the accounting package or ERP. This will give us a complete working copy of their application without disturbing their ongoing business.
- In case of customised software, we can also export all the reports, such as balance sheet, P&L account, ledger etc for each year and each company, to a readable format such as .xls, .pdf or .txt format on the premise and can write that data to a CD/DVD or Hard Disk Drive with no multisession. In that case the data will be non-editable and can be used at the office for analysis. In such case, the deleted files are also to be recovered during the course of search/surveys utilising the hardware present at spot.



- In certain cases, we can also go for backup of module specific data, since ERP has various modules like Purchase, Sales etc

### **6.11 On the Spot Deleted Files Recovery Software**

On the spot deleted files recovery helps in getting crucial evidences which can be confronted to the assessee during the course of search. Such printouts can be taken and signature of the assessee and witness taken to prove the integrity of the data retrieved. Examples of few software's are given below. It is to be noted many such recovery software's are present in the market which can be evaluated independently and decision taken on which software to be used as recovery software. *Some of the examples of recovery software's are given in Annexure-3. These software's are only for illustrations and not recommendatory or mandatory to be used.*

# Analysis of Digital Evidences

### 7.1 Analysis of Digital Evidence

The identification of tax revenue loss is the primary focus of the investigations to be carried out. This loss should be established by using the materials seized including digital data, deftly linking the information gathered to show the evasion of income tax and marshalling all the arguments supported by direct evidences and corroborated well with supporting evidences. The tax evasion can be classified broadly into three categories as given below:

- i. **Earnings made outside the books including suppression of sales**
- ii. **Inflation of expenditure**
- iii. **Abuse or misuse of provisions of exemptions and deductions**

Tax evasion detection is the primary requirement of the investigations. In addition to this strong material evidences are required for the purpose of additional punitive actions including penalty and prosecution. In order to understand the specific case the investigator should have some basic information that will guide the officer to know exactly how to proceed. Some basic tests can be performed on the data to understand the problem to be tackled :

1. **Key word Search:** You can do a key word search like “cash”, “lakhs”, “crores” etc to get the relevant data. The search should be business specific.

*For example, in case of a real estate company, you can search for key words like “agreement”, “sale”, “discount”, “cash” etc.*

In few cases the data is morphed or hidden in the system.

*For example, in one of the infrastructure companies, it was noticed that a hidden account under the name “sundry” was maintained to track all unaccounted transactions. Key word search of “sundry” in unallocated spaces resulted in recovery of key evidences.*

Encase and other forensic tools have in built key word search facility which can used to find key evidences.

2. **Excel Analysis:** Search for “\*.xls”, “\*.xlsx” files. It is noticed that in all medium and small business enterprises, excel files contain the key evidences.

*For example, in a case of medical college, no evidence was found physically that the assessee was collecting donations. However deleted \*.xls retrieved for last six years revealed donations payments by various students.*

*In case of big real estate company daily cash inflow and cash outflow statement along with various names of the parties were found in the excel sheet. It is also noticed that most of sales, pending amount to recovered from the customers, details of cash and cheque payment all are maintained in excel files.*

3. **Mail Analysis:** Retrieve the \*.pst file and mail contains crucial conversation about various transaction. In various cases unaccounted transactions have been noticed here. *For example, key cash payment confirmation from the marketing team to the customers were found in the mail.*

4. **Word Documents:** The officer in charge should try to go through key word documents.

*For example, many bills may be created using the system. Investigator can look into such bills and do consequential enquiries. In many cases, also parallel MOU's may be typed using the computer which are not kept in the office.*

Retrieval of such documents will help unearth huge unaccounted income

5. **Tally Analysis:** In many cases, parallel books of accounts are maintained in hidden pen drives.

*For example, in one real estate case, parallel books of accounts of cash inflow and out flow was maintained in Tally in secret pen drive which was unearthed from the house of the key employee of the group.*

However in many cases, analysis of existing Tally data may also give crucial evidences required for the case.

The officer in charge should open the Tally Package and there are varieties of analysis inbuilt in Tally which can be used for retrieving key evidences in the case. A set of possible analysis is enclosed below which can help the officer in charge.

***The above data also resides in many ERP's, SAP's system, however you need to take the help of the system administrator to retrieve these files.***

## 7.2 Analysis of Tally Data

Many business organizations maintain accounts on Tally and Tally package provides numerous reports, registers, statements, MIS, Statutory challans which can be used in identifying and extracting precise information facts which are relevant to the case. Some of them are listed below:

- 1. Display Balance Sheet-** Go to Gateway of Tally > Balance Sheet and Press Alt+F1 for detailed view. This will give the balance sheet in horizontal form. To view the Balance sheet in vertical form

- *Gateway to Tally> Balance Sheet*
- *Press Alt + F1 for detailed view*
- *Press F12: Configure and set Show Vertical Balance Sheet to Yes*
- *Press Enter to accept the screen and to view vertical Balance Sheet*

If you want you see the Balance Sheet with percentages and working capital then

- *Gateway to Tally> Balance Sheet*
- *Press Alt + F1 for detailed view*
- *Press F12: Configure and set yes*
  - o *Show Percentages*
  - o *Show Working Capital Figures*
- *Press Enter to accept the screen and to view vertical Balance Sheet*

- 2. Verification of Opening Balances-** The officer in charge may verify whether the balances are carried forward correctly

- *Load the previous year data by Selecting F1: Select Cmp*
- *Highlight Current year data from the List of companies' pane*
- *Go to Gateway of Tally > Balance Sheet and Press Alt+F1 for detailed view*
- *Press F2 and specify dates for current year*
- *Press Alt+C to insert column*
  - o *In the column details sub form*
  - o *Select Company data (previous year)*
  - o *Specify the previous year's data*
  - o *Set the currency as Base Currency*

*You can also compare for more number of years by inserting column by pressing Alt+C. If you want to alter already existing column press Alt+A. If you want to delete an existing column, press Alt+D. If you want to automate columns with periodic information based on the predefined criteria, Press Alt+N*

This may be very important in verifying the balances of very old sundry creditors, sundry debtors to find out possible unrecognized income and inflation of purchases. Many manipulations are also noticed in opening and closing stock valuation which can be found by verifying the balances.

### 3. Comparison of Quarterly, Half Yearly Data

- *Gateway of Tally> Balance sheet*
- *Press Alt+F1*
- *Press F2 and specify the dates*
- *Press Alt+N and select Quarterly from the drop list in Repeat using field. Using the same drop list you can also compare on 4 Week Month, Daily, Fortnightly, Quarterly basis.*

If the business is not seasonal, most of the expenditure as a percentage may not be very much different. Officer in charge can verify any abnormal rises or fall in various heads of accounts and have a systematic approach in verifying inflation or suppression those accounts. Usually abnormal changes in expenditure are noticed in the last three months of the financial year to reduce the profits.

### 4. Verification of Fixed Assets

- *Go to Gateway of Tally > Balance Sheet*
- *Press Fixed Assets group and Press Alt+F1*
- *Press F12: Configure and set YES to Show Opening Balances, Show Transactions and Show closing balances.*
- *You can also compare across years by Pressing Alt+N*

This can be used to analyse accumulated depreciation accounts and also verify vouchers/bills related to Fixed Assets.

### 5. Verifying Stock

- *Gate way of Tally> Stock Summary*
- *Press Alt+F1 for detailed view*
- *Press Alt+F2 and specify the period*
- *Press F12 and configure the items you want to look at*
- *To know product wise profitability of each stock item, Press F7: Show Profit*

To choose multiple valuation methods, Press Alt +N and select Stock Valuation methods from drop down list.

You can also compare across different Stock Valuation Methods and see whether the assessee is declaring the correct stock valuation to the department. This tool is very handy in industries like Jewellery, Retail where different assessee uses different stock valuation methods.

## 6. Verifying Receivable/Payable Balances

- *Go to Balance Sheet and Enter Sundry Debtors and Sundry Creditors*
- *Press Alt+F1 for detailed view*  
Initial analysis like ageing of outstanding bills and analysis of balances over a period of time provides hints about doubtful accounts on which the officer in charge may go for detailed examination of genuineness of the transaction. The ageing analysis for Sundry Creditors is done in the following way:
  - *Gateway of Tally> Balance Sheet*
  - *Enter Sundry Creditors Group*
  - *Press Alt+F1 for detailed view*
  - *Press F8 and select Bill wise details from the list of reports*
  - *Press F6: Age wise and select Ageing by due date and enter. If you want to alter the ageing dates, a screens appear where you can alter the ageing details*
  - *Press Enter to accept the screen*The same method can be used for viewing Sundry Debtors Account

## 7. Displaying Profit and Loss A/C

- *Gate way of Tally> Profit and Loss A/c*
- *Press Alt+F1 for detailed view*

*Drill down to every expenses to know more about the transactions*

## 8. Profit and Loss Statement Year wise analysis

- *Press F1 and load previous year's data*
- *Highlight current year data*
- *Gateway of Tally> Profit and Loss A/c*
- *Press Alt+F1 for detailed view*
- *Press Alt+C to insert column. In this specify the relevant details and press enter.*

Officer in charge can inspect any abnormal changes in expenses over a period and specifically verify those bills to detect evidences for inflation of expenses.

## 9. Ratio Analysis

To view Ratio Analysis report

- *Gateway to Tally> Ratio Analysis*

- *Highlight the relevant ratio ( Current ratio, Quick ratio, Debt Equity ratio, Gross Profit%, Net Profit %, Recv. Turnover in days, Inventory Turnover, etc) and press Alt + F1 for detailed view*

Officer in charge can inspect any abnormal changes in ratio over a period and specifically verify the reasons for the same. Usually Gross Profit is more or less constant in the industries with minor variations. However there may be substantial changes in the net profit due to different strategies used at the marketing, HR and administration levels. Any major variations in Gross Profit may be looked into after comparing with the Industry standard. Abnormally low Gross Profit Margin may indicate possibility of bogus purchases booked by the assessee.

## **10. Cash Book/Bank Book and relevant ledgers**

**To see the daily cash break up or a period specific cash book does the following :**

- *Gateway of Tally> Display> Account books> Cash/Bank Books*
- *Press Enter on Cash Ledger*
- *To see daily cash breakup, Press F6: Dly Brk-up*
- *Press F12: Configure and set the details you want.*

**To do the data mining of cash books, do the following :**

- *Enter on any month*
- *Alt+F2 and the change the period to full year*
- *Press F12: Configure and Set Show Narrations as YES*
- *Press Alt+F12: This gives the filter to get necessary vouchers based on certain conditions.*

**To get Bank Reconciliation statement :**

- *Go to Gateway of Tally> Bank Reconciliation*
- *Verification of Day Book*
- *Gateway of Tally> Display> Daybook*
- *Press Alt+F2 and specify the period*
- *Press F12 and set narrations to YES*
- *Press Alt+F12 and set the filter vouchers on predetermined conditions*

Officer in charge may inspect the cash bill voucher for specific parties which may show splitting of bills for less than Rs 20,000/- to avoid provisions of section 40A(3). Officer may also look into monthly cash



in flow and cash out flow statements to look into whether any abnormal changes are noticed over a period of time.

## **11. Audit Analysis**

### **Verification of chart of accounts**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Press Ctrl+F3 and you will get details of the following Verification of chart of accounts:*
  - o *Accounts squared off during the year*
  - o *Not available in the current year*
  - o *Not used*
  - o *Not used in current year*
  - o *Only Balances last year and used in current year*
  - o *Only Balances, No transactions*
  - o *Regrouped*
  - o *Revenue ledgers having opening balances*
  - o *Used only in current year*

Officer in charge may go deeper into these accounts since mostly these ledgers may indicate possibility of manipulations done by the assessee to declare lesser profits.

### **Verification of opening balances**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Select Verification of Balances and Press Enter*
- *Press F5: Ledger wise*
- *Press Alt+V: Balance Variance*
- *Press F4: Group, select Indirect Expenses group and Enter*

### **Verifying Periodic Payments and Receipts**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Select Periodic Payments and Receipts and Press Enter*

It is to be noted that payments like Salary, Rent, Pre Paid Taxes etc are periodic payments and abnormal changes in the same are not possible. Officer in charge should look for such abnormal changes

#### **Verifying Repeated Transactions**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Select Repeated Transactions and press Enter*
- *Drill down where there are more repetitions. This indicates splitting of bills and may attract provisions of section 40A(3)*

#### **Verifying Unusual transactions**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Select Relative Size Factor and Press Enter*
- *Huge Variation ledgers can be looked into specifically for any manipulations*

#### **Verifying Cash withdrawals/deposits to Bank**

- *Gateway of Tally> Audit and Compliance > Audit and Analysis*
- *Go to Other Analysis and Cash Withdrawals/Deposits to Bank*
- *Other Analysis possible are Interbank transactions verification, Fixed Asset Analysis, Transactions on Holiday, Highest and Lowest Value Transactions, Pending Advances, Stale Cheques/Instruments, Account Reconciliation*

### **7.3 Timeframe analysis**

Timeframe analysis can be useful in determining as to when events occurred on a computer system. It is important to note that when a file was created, used or manipulated certain time stamps related to files are stored. The most commonly used time stamps are the modification, access and creation times which are described below:

- **Modification Time:** This is the last time a file was changed in any way, including when a file is written to and when it is changed by another program
- **Access Time:** This is the last time any access was performed on a file (e.g viewed, opened, printed)
- **Creation Time:** This is generally the time and date the file was created, however when a file is copied to a system, the creation time will become the time the file was copied to the new system. The modification time will remain intact.

Different types of file system may store different types of times. For example, Windows systems retain the last modified time, the last access time, and the creation time of files. UNIX systems retain the last modification, last inode( *An inode is a set of data regarding certain characteristics of a file such as the privileges set for the file and the file's owner* ) and the last access times. In some cases, Metadata present about the file may also provide the details of the same.

If the case requires establishing an accurate timeline of events, then the file times should be preserved. In this case, imaging is a must and logical backup sometimes may change the file creation times. Some methods of checking any modification in time are as follows:

- Reviewing the time and date stamps contained in the file system, meta data (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. It narrows down the scope of our search and reduces the lead time of investigation.*
- 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.*

**Note:** *The date and time visible on the computer is the time and date set in its BIOS. It can be different from the actual time and date. The difference shall be taken into account while making analysis of any event.*

**Some of the important things to see in the time frame analysis are as follows :**

- The computer's clock does not have the correct time. *For example, the clock may not have been synchronized regularly with an authoritative time source. System Clock should be recorded in the Digital Evidence Collection Form*
- The time may not be recorded with the expected level of detail, such as omission in seconds, minutes etc
- In few cases, outside attackers may alter the recorded file times.

*These methods are very useful in cases of bogus bills which are created after the transactions have happened. Analysis of the difference between the bill date and creation of the document will help unearth key bogus bills in purchases and suppression in sales. In many cases, documents were signed post dated to avoid taxation can be easily analysed using these tools.*

## 7.4 Data hiding analysis

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 hid data.
- Gaining access to all password-protected, encrypted, and compressed files, which may indicate an attempt to conceal data from unauthorized users. The password itself may be as relevant as the contents of the file.

- **Steganography:** Hiding some text data along with some image file. It will be almost impossible to find that there are data hidden in image file through bare eyes.
- Gaining access to a host-protected area (HPA). The presence of user-created data in an HPA may indicate an attempt to conceal data.
- Deleting the files is also a kind of data hiding.

## 7.5 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 are:

- Reviewing file names for relevance and patterns.
- Examining file contents.
- Identifying the number and type of operating system(s).
- Correlating the files to the installed applications.
- Considering relationships among 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 at alternative location(s).
- Examining user-configuration settings.
- *Analyzing file metadata (data about data):* 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.*

## 7.6 Ownership and possession

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 relevant 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
- 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 passwords needed to gain access to encrypted and password-protected files are recovered, such passwords 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).

## 7.7 Format/partition Recovery

A digital storage device record during the course of search may be found formatted or partitioned just before search. It may not show any file. However, forensic tools are capable of recovering the same if the files are present on the device before formatting/ partition. It is advisable to make a forensic check on such devices also, specifically if they are used by key persons.

## 7.8 Fraud analysis using Benford's Law

This test is used as litmus test to show the reliability of any set of data comprising naturally occurring (uncontrolled) numbers like in any purchase, sales or any other ledger from the database or Tally. Idea software provides facility to do this analysis in addition to several others. There are also several addins to Microsoft Excel to do this analysis. The following table gives the expected frequencies of the digits in first, second, third or fourth place of the digit. Any deviation beyond a tolerance level to this should be viewed as an indication of manipulation of the data as the actual occurrence of the numbers is not natural. This is a powerful test to show the various frauds.

The Expected Digit Frequencies of Benford's Law

Digit	Position in Number			
	1st	2nd	3rd	4th
0		.11968	.10178	.10018
1	.30103	.11389	.10138	.10014
2	.17609	.10882	.10097	.10010
3	.12494	.10433	.10057	.10006
4	.09691	.10031	.10018	.10002
5	.07918	.09668	.09979	.09998
6	.06695	.09337	.09940	.09994
7	.05799	.09035	.09902	.09990
8	.05115	.08757	.09864	.09986
9	.04576	.08500	.09827	.09982

Source: Nigrini, M.J., 1996. "A tax payer compliance application of Benford's Law." *The Journal of the American Taxation Association* 18 (Spring): 72–91.

The table shows that the expected proportion of numbers with a first digit 2 is 0.17609 and the expected proportion of numbers with a fourth digit 4 is 0.10002.

## **7.9 Data profiling test**

Extract some set of information say sales details or purchase details. In this extracted data perform a calculation to see the number of transactions and the total value of transactions for various categories like sale value below 0, between 0 and 10, between 11 and 100, between 100 and 1000, between 1001 and 100000 and above 10000000 etc. The investigator can form his/her own set of categories. This will give an idea of how the data is distributed. He/she can spot any major deviations as red flags immediately. This also will show the completeness of the data being analysed once the investigator finds that the sum of the all the sales data is the turnover of the assessee as declared.

## **7.10 First two digits test**

This test will be usually to test the occurrence of numbers with last two digits as two zeros. This will indicate the frequency of distribution of the data based on the first two digits. This test in the presence of the business operations will indicate the distribution of expenditure which could trace bogus bills used for inflation

## **7.11 Current period and prior period tests**

This test will take the table data from the suspect system and compare the sales or purchases found in two different periods. A typical analysis will show the vendor wise purchase of raw materials and items wise supply of the materials. The test will obtain the data from the suspect database and perform the test. Any new supplier for a product whose supply is found to be excess considering the purchase patterns of the business could indicate a bogus billing being booked.

## **7.12 Largest growing subsets and largest subsets**

This test is show for instance the relative growth of purchases of any one item or purchases from any one vendor that is growing faster over the time period. This could indicate malpractice easily.

## **7.13 Tests using relative size factor**

Certain anomalies are detected using this test. Imagine a case that average bill in the case of purchase of some item of raw material is Rs 25,400. Any bill that is suddenly shooting up to Rs 75,000 is not a normal occurrence and needs to be studied as it can be mistyped item, misclassified item or a fraudulent item.

## **7.14 Correlation testing**

This test can be done in line with other such tests. This is more useful where fraud prevention guidelines are not in place. For example there could be a condition so simple as this, the purchase of petrol when all the vehicles used are diesel based. In a slightly modified condition, if all the vehicles are yielding

on average 15 KMPL and there are 30,000 KMs covered by the vehicles in a particular month, then if the diesel consumed is in excess of 3000 liters then there is mistake in correlation.

### 7.15 Timed Series

This is simple yet sophisticate regression analysis test. The weighted average of consumption of particular item of expenditure in comparison with the production of any particular product and be studied and the predicted value for any period can be estimated. If the actual consumption is in excess, this could indicate an abnormality needing further verification

### 7.16 Handling ERP or other custom made suites of applications

While examining the ERP application suite like SAP, the investigator should have certain basic information in his possession. He should know about the activity of the assessee. In a typical manufacturing concern the structure should be understood. Basic Flow of Operations in most of the cases is as follows:

- The **Design Department** prepares drawing for all the individual processes/components and accordingly, raises **Bill of Material (BOM)** for each individual component so designed for the project.
- Based on the BOM, the Material Requisition (“**MR**”) or Purchase Requisition (“**PR**”) is communicated by the **Production Planning Department**.
- Once this MR/PR is received by the **Purchase department**, a Purchase Order is generated by Purchase Department.
- The supplier then sends the material along with the Delivery Challan, where it is received by the **Stores Department**.
- The Stores Department then prepares Goods Receipt Note (GRN)/ Goods Receipts-cum-Inspection Note (GRIN)/ Goods Inward Note (GIN).
- GIN/GRIN is then handed over to **Quality Control Department** for inspection in case of raw material or component
- The GIN along with the Tax Invoice, Challans and supporting documents are sent to **Accounts Department** for payment.
- After entering the GIN, all the details of that particular GIN gets populated on the Accounts Module screen.
- Based on this data, Payment Vouchers (in short, “**PV**”) are prepared by the Accounts Department.
- PV is then printed and forwarded to internal auditor. After this, the PV is again sent to Accounts Department for preparation of banking voucher and cheque which get printed through system.

The Investigator can form a hypothesis like the following one :

*A typical bogus purchase will be booked by a person sitting in a single location preferably the corporate office who will raise the purchase request some time using the id of another person in the factory or the manufacturing facility. The purchase order PO will be raised and delivery in Goods Receipt Register GRR will be made. Following this the Payment Processing will be carried out.*

In this scenario the investigator should proceed to collect information from within the system to find out certain pertinent information

- i. The list of persons who are authorized to raise PO
- ii. The various locations from where this persons are working
- iii. The items of purchase used for manufacture that form more than say 2% of the TO
- iv. The vendors who supply the items
- v. Items wise monthly summary of purchase
- vi. Monthly summary of production
- vii. The addition of new vendors for any existing product and sudden increase in the total purchase of such item or items of materials

This analysis should reveal identity of some vendors who could be used for supplying bogus bills. This can be further studied identify the corroborative evidence like the processing of purchase. The delivery challans and further check can be carried out to the manner in which the payment was processed. The bank analysis of the vendor will reveal that the vendor facts easily.

Also discrepancies in the flow of operations may result in detection of bogus bills. *For example, "Purchase Order" may not have been raised using "Purchase Requisition". Many a times it is noticed that Purchases are directly raised by Accounts department without any intervention of Purchase and Stores Department. This clearly shows possibility of bogus bills. Time Stamp Analysis of Audit Log of ERP Systems may reveal when the bills were entered.*

### **7.17 Conclusion**

The above discussion on various steps of analysis of digital evidence deals more with the procedure to locate and analyze various files. However, the digital data found stored on devices recorded or copied may be enormous. The role of common sense of Income-tax investigation in the forensic analysis becomes very crucial in the procedure suggested above. This is in addition to the conventional investigative skills and procedure adopted by the departmental authorities in undertaking various exercise and making investigation. This of-course involves proper identification of relevant and crucial data out of a plethora of data and facts available on digital devices.



# Guidelines for Documentation and Seizure of Digital Evidences

### 8.1 Steps for seizure

- Collect all the digital evidence: either the original or the cloned copies.
- Separate out the main copy and working copies.
- Pack all the working copies in a separate box, which would later be used in the office for analysis.
- For the main copies, wrap a white tape on the connecting ports of each Hard Disk Drive along with department's seal. The seal and the tape will ensure that no one has accessed the Hard Disk Drives.
- Seal the main copies by putting them in a bubble bag and then in a storage box. And then again wrap the white tape around the storage box so that no-one can open the box without removing the tape, and then place a seal of the department.
- Take signature of assessee and officer in charge, on the seal.
- If we are seizing a system or a server or any other digital evidence, then it should be wrapped with tape and sealed in such a manner that no-one can start or open the digital evidence without breaking the seal.

### 8.2 Documentation during seizure

After the completion of acquisition and analysis process, seizure process is followed. But in case, acquisition and analysis is not possible at the site, then seizing is done. Acquisition and analysis is done at the lab. The Hard Disk Drives which are to be seized may be either the original Hard Disk Drives found at premises or the cloned copies made by technical persons. Invariably, the original storage media is seized and out of the two cloned copies taken, one cloned copy may be handed over to the assessee and the other should be used as working copy for analysis.

In case of seizure, documentation is very important:

- **Physical items:** There are well-established procedures for handling the physical items, such as the computer, the PDA, or the cellular telephone.
- **Data acquisition:** Even if the acquisition of the data is done in accordance with best practices,

concerns about chain of custody of the data contained in the forensic image become moot. Chain of custody issue is unique to the acquisition of electronic evidence. Other issues that relate are:

- **What types of digital evidence have been collected?** For example, is there a hard copy (printed) version of the e-mail/ other digital data? Is there an electronic copy? Does it contain full header information?
- **Who handled the evidence-** Document the name and job function
- **How was the digital evidence collected and stored?**
- Identify any tools or methods used to collect the digital evidence.
- Determine who had access to the digital evidence after it was collected (anyone with access to the evidence should be considered part of the chain of custody). Account for all storage of data as well.
- **When was the evidence collected?** Document the date and time when the evidence was collected. Be aware that the collection of evidence might be an ongoing process.
- **Where was the evidence when it was collected?**
  - o Geographical
  - o Hardware
    - What kind of machine/device that held the digital evidence?
    - Who had access to the machine/device?
    - Who owned the machine/device?
    - Was a serial number present?
    - Was the machine/device a shared device?
    - Was information retrieved from a network?
    - Was information password-protected?
    - Who had access to password-protected information?
  - o Offsite (e.g., servers – e- mail or remote – and web pages)
- Document the details of each Hard Disk Drives or digital evidences which have to be seized. There may be many attributes which we have to note down such as serial no of device, its capacity, used space by data, operating system used and password(if there any).
- Before seizing any of the digital evidence, their hash value must be calculated using forensic tools such as cyber check or duplicator or anything else. There will be a report generated by these tools which can be attached along with the panchnama.
- Case name, premises, date of seizure, place etc. This kind of information can also be written on each digital evidence for memory purpose.

# Reporting of Analysis in Assessment Order & Archival of Digital Evidences

**9.1 Reporting of Analysis of Digital Evidence** in the Assessment Order should be done in a simple lucid manner, so that any person can understand. The report should give description of the items, process adapted for analysis, chain of custody on the movement of digital evidence, hard and soft copies of the findings, glossary of terms etc. The presentation and use of digital evidence in assessment order and presentation of the same in court of the law in matters of appeal involves stating the credibility of the processes employed during analysis for testing the authenticity of the data.

Some guidelines that assessing officer need to follow when using the Digital Evidence Analysis in the assessment order etc, are as follows:

- Brief description of the case, details/description of the objects, date and time of collection of the objects, Status of the objects when collected (On or Off), Seized from – person, organization, location etc should be included in the Assessment Order.
- Digital Evidence Collection Form, Mobile Phone Evidence Collection Form should be enclosed in the order to show the initial state of the Digital Evidence.
- Digital Forensic Report( Given by Forensic Examiner) containing details of hash value and the details of all mahazar drawn to open the digital evidence at various times to gather further evidences should be included as an annexure to the assessment order. *If the chain of custody form is present, the same can be annexed to the assessment order. This will establish the integrity of the data before any court of law.*
- The Key digital evidences retrieved if deleted along with the description of the same. In case of business application software, a note on how the business application software is and the technical details of all critical components.
- Whether these digital evidences have been confronted to the assessee under any section of the law? The relevant portions of the statement under various sections of Income Tax Act should be included in the order.
- Circumstantial evidences and other key physical evidences seized/impounded should be linked to the digital evidence. Usually the physical evidences like loose papers, sheets gives details of one particular transaction, while the digital evidences may help in unearthing the entire consolidated data for the whole year. Such digital evidences should be linked to the physical evidences seized

during the course of search to establish the genuineness of the data and also to quantify to the total unaccounted income.

## **9.2 Archival of data means storing data for a long time so that it can be used for reference or for verification**

Archival of data is very important and it is also a crucial step. If the archival is not done properly, it can lead to the damage of digital evidence resulting in data loss. Data from digital evidence can be lost due to the following reasons:

1. Shocks
2. Scratching
3. Cracking
4. Over heating
5. Short circuit

To avoid all the above mentioned reasons, data archival should be done in a proper manner.

## **9.3 Protection from physical shocks**

All digital evidence should be put in shock- proof bags such as bubble bags. Thereafter, all the digital evidence should be placed in same hard case and should be placed in such a manner that no blank space remains allowing the digital evidence to bubble.

1. Bubble bag will protect digital evidence against shocks.
2. Tight packing will protect against scratching.
3. Hard case will protect digital evidence against cracking damage.

## **9.4 Protection from overheating**

For avoiding over-heating, none of the digital evidence should be exposed to high temperature. They should always be stored in a cool place. Over-heating can melt the circuit inside the digital evidence resulting in the data loss.

## **9.5 Protection from short circuiting**

To protect against short-circuiting, always add or remove the digital evidence safely from the device. When attaching the digital evidence to a device the power button should be turned off and only after attaching the device, power button should be turned on. While removing the digital evidence from computers it should be done by using 'safely remove' option provided in operating system.

While removing from some other device such as write blocker or duplicator, first turn off the power button of the device and then remove the digital evidence to avoid short-circuiting of digital evidences. Also, note that no digital evidence should be stored in a metal case as it interferes with the magnetic properties of the storage devices, thereby causing a loss or corruption of data stored. Care should be taken to store the data either in plastic case or wooden case only.

All these all steps, if followed properly, can avoid data loss to a great extent. But all the digital evidence archival depends upon the careful handling of the digital evidence.

In addition to the above, the media used to store the digital evidence usually depends on how long it is needed. For example :

- In case the data is stored in CD-Rs or DVDs
  - Capacity: up to 17 GB
  - Lifespan: 2 to 5 years

### 9.6 Handling the digital evidence at a later stage

In the Income Tax Department, the digital evidence stored is used in the assessment proceedings and at later stages in case of legal tangles. In order to maintain the sanctity of data stored/seized, there is a need to maintain a chain of custody while handling the digital evidence during the course of assessment proceedings and at later stages. Due to the lengthy legal proceedings involved, it may be needed to retain evidence indefinitely.

Hence, a chain of custody of digital evidence should be created in order to know the details of who is accessing data, if anyone who accessed the data had tampered with the data etc.

## Chapter 10

### Mobile Forensics

**10.1 Mobile device forensics** is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions. The phrase *mobile device* usually refers to mobile phones; however, it can also relate to any digital device that has both internal memory and communication ability, including PDA devices, GPS devices and tablet computers.

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, SMS and MMS messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

Depending on situation, the officer in charge may decide to seize the mobile or take a backup or take an image of the mobile device. Procedure for gathering evidence from Mobile Phones :

1. If the device is “OFF”, do not turn “ON”
2. If the device is “ON”, do not turn “ OFF”. Powering down device could enable password, thus preventing access to the evidence
3. Photograph device and screen display
4. Label and collect all cables ( including power supply)
5. Note that you should do the imaging prior to it gets discharged. Keep the device charged
6. Seize additional storage media like memory sticks etc
7. Document all steps involved in seizure of device and components

A Faraday bag may be used by the officer in charge to avoid in signals. This prevents any changes that may take place in the phone by receiving a signal. So evidence cannot be manipulated till acquisition.

The officer in charge should specifically fill up the Mobile Device collection form which is given below. All the details should be filled up :

Mobile Devices Collection Form-Checklist			
Name of the Authorized Officer:			
Name of the assessee :			
Date:	Time:	Premise Address:	
Examiner's Name and Details:			
System State		If switched On, What is visible on screen?	
<input type="radio"/> Or <input type="radio"/> Or <input type="radio"/> Hibernation/Sleep			
System Info	Make: _____ Model: _____		
	Mobile Type: <input type="radio"/> GSM <input type="radio"/> CDMA <input type="radio"/> 3G <input type="radio"/> Others		
	If Others Specify _____		
Time Zone Settings: _____			
Date/Time of Mobile Phone: _____ Actual Date/Time: _____			
IMEI/MEID Number			
Mobile Serial Number(If any)			
Operating System ( Including Version Number)			
Is the SIM Card Present? <input type="radio"/> Yes <input type="radio"/> No		SIM Service Provider Name:	
SIM Card Size		IMSI Card Number	
Mobile Phone State: <input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> OFFLINE		Shutdown Type <input type="radio"/> NORMAL <input type="radio"/> BATTERY PULLED	
Mobile Phone State: <input type="radio"/> YES <input type="radio"/> NO		Media Card Serial Number:	
		Media Card Make and Capacity:	
Does the Assessee phone has the ability to access Internet? <input type="radio"/> YES <input type="radio"/> NO			
Storage Copy Details		Working Copy Details	
Make: _____ Model: _____		Make: _____ Model: _____	
Serial No: _____		Serial No: _____	
Is the Media Card Removed? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Media Card Replaced after Imaging? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Is the SIM Card Removed? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
SIM Card Replaced after Imaging? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Is the signature of witness taken? <input type="radio"/> Yes <input type="radio"/> No			
Note by the AO regarding the potential evidences in the digital devices:			

*The details of various backup procedures are enclosed in Annexure 4.*

## Chapter 11

# Cyber Forensic Labs & Forensic Data Extraction Centers

Cyber forensics have become important in the recent times as most of the transactions done by the businessmen are being done on the computers, heavy and complicated accounting packages are being used and also due to the fact that the hi-tech digital devices are easily and cheaply available in recent times. Nowadays, the data is not only being stored in the word documents and excel sheets but also on mobile phones, networks, clouds, emails etc. This data may be sometimes protected by passwords or encrypted also. To retrieve this data so that the data is not altered/modified/deleted and to also to make sure that the data collected should be admissible as an evidence in the courts of law, cyber forensics is very much necessary.

Hence, ideally at each major centre of Income tax office, a Forensic lab or Forensic data extraction centre needs to be established, with some basic forensic hardware and software tools and some dedicated trained staff. At the same time the awareness and training programmes for all the officers and Inspectors in the field needs to be organized. The facilities and skills can be upgraded from time to time. Certain requirements in this regard are as under:

### 11.1 Constitution of each Forensic lab / Forensic data analysis and extraction facility:

- High-end laptops equipped with Forensic Write blockers (IDE, SATA, SCSI & USB), Forensic software toolkit, Password Recovery Software toolkit, Registry Viewer, Distributed Network Attach & Wipe Drive. Each of these needs to be bundled with external interface for enabling acquisition from external hard disks of varying interface such as SATA hard disks, SCSI hard disks, laptops, USB Pen drives/ MP3 players/ iPods, digital cameras, CDs & DVDs / floppies, mobile SIM cards, and all types of flash card memories.
- **One high speed hardware wiping device** capable of forensically wiping two disks at a time at speeds of up to 8GB/min
- **Three disk imaging devices** for IDE/ SATA/PATA/laptop hard drives Should support formatting of destination drive in both FAT and NTFS format with speeds up to 5.5 GB/minute
- **One disk imaging device for SCSI type hard drives** Should support formatting of destination drive in both FAT and NTFS format with speeds up to 9 GB/minute
- **One high end Quad processor server** Should be compatible with LTO, DLT drives and DTA drives



- **One hardware shadow device/ previewing device** with the functionality of connection between mother board and drive of subject disk, and should allow booting in forensically sound manner without altering the data.
- **Write Blockers** for IDE/ SATA/PATA drives, for SCSI drives, for SATA drives, and for USB drives. All these blockers should support both USB and firewall connectivity with source hard drive.
- **Live Server Imaging Kit** for imaging live servers.
- **SIM interrogation system/ Mobile phone forensic devices** for recovering data from SIM cards.
- **High end PCs for work stations**

## 11.2 Software

- **Rainbow tables/ other software for password cracking**  
Should fit on a DVD and should crack 98% of all 40 Bit encrypted office documents
- **Forensic software tool kit for Server**  
Should contain Forensic software (that uncovers hidden, deleted, encrypted misnamed and archived data including emails also has high speed indexed searching ability), registry viewer, distributed network attack and wipe drive software.
- **Forensic software tool kit for PCs**  
Should contain Forensic software, that uncovers hidden, deleted, encrypted misnamed and archived data including emails also has high speed indexed searching ability. It is important that the device should be easy to operate and should support hard disks in all jumper positions otherwise an officer in the field may commit a mistake. The device suggested should support all hard drives except SCSI for which other device is suggested.
- **Consumables**  
This will include a variety of blank hard disks for making images, hard disk casings, Cartridges, CDs, DVDs and pen drives

## 11.3 Reference Material

Books and Journals in the subject on computer forensics may be procured and made available to the staff working in the lab.

## 11.4 Work practices for the Forensic labs/ facilities

### 11.4.1 Support to Investigation Units

- The main function of the lab shall be to provide technical support to the Investigation units in acquiring data on subject disks through cloning/ imaging, analysing the clones to uncover deleted,

hidden and password protected data, and handing over to the Investigation unit for analysing the same for defaults relating to Income Tax.

- Each Lab will need a **custodian** of digital records for keeping record of all digital media entering and leaving the lab and for safe custody of the archived disks. A log of all forensic activities carried out on a disk will be maintained in the lab.
- Wherever possible, the Investigation unit will give a requisition for the services of the lab mentioning the computer environment expected at the site. This may include such information as-
  - Make /model /number of servers at the location
  - Number of client computers,
  - presence of any unusual media such as LTO drive systems, SAN etc.
  - Kind of networking or kind of connectivity to the internet.
  - Whether remote dial-in facilities exist or not etc.
- The brief for the search parties can, *inter alia*, contain suggestions regarding-
  - Method for performing a preview of computers and other disks found by the search team
  - Treatment regarding loose media found at the site – floppies, CDs, CF cards, Tapes, Memory sticks, USB pen drives, MP3 players, iPods, mobile phones, digital cameras etc ,
  - Whether imaging/ cloning is to be done onsite or whether hard disk would be required to be seized
  - Whether all computers found on site will be seized/ imaged or not. If not what criterion are to be applied to select the computers relevant to the investigation
- A forensic team can be deputed to the site where digital data is found. It must carry-
  - Sufficient number of pre-wiped disks for imaging/cloning
  - Disk imaging device capable of imaging all types of disks drives
  - Portable Labs for previewing computers hard disks in-case a decision has to be made as to which computers to be imaged or not.
  - Sufficient evidence bags and tags for properly packing, labelling & transporting the imaged data in a proper form

#### 11.4.2 Procedure for onsite imaging /seizure of disks

The Forensic team will examine:

- communications network and other connections and observe the screen display.
- Unplug communications connections and Modems from computers without turning off the computers, and label all connections. It is recommended to disconnect Network cables and connections at the time of investigation. This can also be done by switching off the Network Hubs and Switches and sealing them till the Search/Seizure operation is complete.

- Identify serial numbers of CPUs, monitors, hard disk drives and other electronic equipment. Decide whether to shutdown the computers that is on, recording reasons as to why and when a shut down was carried out.
- Access the computers through write blockers and make two physical images (clones) of each hard disk found using previously wiped blank disks using hardware imaging devices. It will compute hash value of each disk found and mention it in the *panchnama*.
- In case any disk is to be seized, seize the hard disk by properly labelling and placing in protective covering
- Shut down and collect the computer(s), peripherals, printouts (if any), floppies (if any) and any other potential evidence - bag and tag individually
- The following information will need to be included in the *panchnama*, copy of which will be given to the assessee
  - Inventory of all computer hard disks/ media found
  - the time displayed in the CPU clock of the PC/Server and the actual local time at that time
  - Inventory of all disks which were cloned/ imaged with number of clones created/ seized giving hash value of each disk,
  - Inventory of all disks found and seized without cloning

#### 11.4.3 Procedure for imaging seized hard disks

In cases where hard disks cannot be cloned at site and are therefore seized, two sets of images/clones should be created in the lab in presence of the assessee or his representative and the authorised officer following the same procedure as described above. A *panchnama* should be prepared for this activity recording the hash value of each of the hard disks imaged and the other particulars mentioned above. The assessee may be given an option to obtain copy of image at his cost.

#### 11.5 Manpower and Training

Each lab/ unit will need at least one ITO, two Inspectors and one Tax Assistant on full time basis for maintaining records and equipment. These personnel will need thorough training in use of the hardware and software tools. This training needs to be factored in the procurement process itself and the vendor should be obliged to provide training to a fixed number of Officers per license/ HW purchased.

#### 11.6 Cyber forensic lab in Mumbai, Delhi and Ahmedabad

As of now, there are three cyber forensic labs being operated at Mumbai, Delhi and recently at Ahmedabad. In case of other directorates/field formation who want to use the facility of these cyber forensic labs, the following steps need to be undertaken to maintain the integrity of the data:

1. The Original Digital Evidence should be collected and all the entries in Digital Evidence Collection Form (*enclosed in Annexure-7*) should be filed up and signatures should be taken by the assessee and two witnesses
2. The chain of custody form (*enclosed in Annexure-8*) should be filed up. This is a key document that should be mandatorily filed up to ensure that integrity of the data cannot be questioned by any court of law.
3. In case the Digital Evidence is a mobile phone, the Mobile Phone Evidence Collection Form (*enclosed in Annexure-9*) should be filed up.
4. Appropriate Packaging and Labelling of the evidence should be undertaken. Primary steps should be taken to choose packaging that is of proper size and material, to fit into the evidence. Do not drop your digital evidences into a plastic grocery bag you commonly find or some make shift package. Various types of special packaging should be prepared using envelopes, bags and containers. The packaging should be clean and preferably new to avoid contamination. Each piece of evidence should be packaged separately and then properly labelled, sealed and documented. Use anti-static bags to transport evidences as these will protect and prevent any localized static electricity charge from being deposited onto the devices.
5. Diskettes are fragile, so if packed loosely may get damaged during transport. Hard Disks should not be subjected to shocks. If you are transporting a CPU, Media devices in a vehicle, steps should be taken not to place the same in area where drastic change in temperature is expected. You should guard the evidence against electrostatic discharge.

Apart from this a forwarding letter to the Cyber Forensic Labs for scientific analysis and opinion should mention the following information:

- Brief History of the case
- The details of the exhibits seized and their place of seizure
- The model, make and description of the hard disk or any storage device
- The date and time of the visit to the premises
- The condition of the computer system (on or off) at the scene of crime
- Is the photograph of the scene of crime is taken?
- Is it a stand alone computer or a network?
- Is the computer has any internet connection or any means to communicate with external computers?
- The details of the operating system
- The application software used if any and details of the same
- Any Password files which have been impounded or taken as part of any statement

- Bios Date and Time Stamps
- Whether the storage media previewed, if so, is the preview done forensically or not?
- Some keywords useful for analysis like “cash”, “lakhs” etc
- The date and time at which the seizure of the digital evidence was done
- The printout of any important files relevant to the case
- The output of the business application software which is required
- The details of deleted files if any required
- Reasons on why the system in question was seized and the details which the concerned officer is looking for.

An analysis of cyber forensic lab at Mumbai throws the following details:

1. The lab is attached to one of the units with the office of DGIT(Inv), Mumbai, who has control over the functioning of the lab.
2. There is a software engineer working in the lab and this job is outsourced. This engineer is mainly used for the data extraction and acquisition and also for on-the-spot analysis of data. The analysis of data acquired is mainly done by the DDIT concerned but in case on-the-spot analysis is required, then the help of this engineer is taken.
3. Services of another private firm are also being taken, in case there is large amount of data acquisition and extraction.
4. The data extracted is kept with the DDIT concerned and then transferred to the assessment units when the case is centralized. In case of this transfer, chain of custody form should be filled up and kept in safe custody for further reference.
5. In this lab, the functions such as Files Analysis ( MS Office Files), Recovery of Deleted Files, Analysis of Hidden Files, Recovery of Formatted/deleted Partition, File Signature Verification, Internet History and cookies, Mail Box viewing, Slack space data analysis, Key Word Searching, Analysis of file meta-data etc are being done.
6. Different hardware tools which are used in this lab are Drive Wiper Vroom which can sanitize 2 HDs at a time, Wipe Master which can sanitize upto 9 HDs, write blocking devices such as Ultra Kit, Vroom Shadow-II, forensic duplicator which duplicates all sectors of evidence device to target device, UFED for mobile back up, FRED(Forensic Recovery of Evidence Device) which has an inbuilt write blocker and pre-installed forensic software is used for acquiring data during the course of search/survey etc are being used.
7. Different software tools used in this lab are Cyber Check Suite 4.0 used to acquire image from an evidence hard disk and to recover deleted data, file signature mismatch, etc., Encase 7.0 which is similar to Cyber Check Suite, Encase Portable which is software tool in a pendrive used for onsite

analysis, Passware used to crack passwords and which supports 180+ file types, Recover My files used to see the deleted files, File Salvage which is same as Recover-My-Files but it is used in case of MAC OS and Helix which is a live tool which is bootable CD, acquires RAM memory, duplicates HDD, sees Computer Configuration, software installed on it and reads System Registry in a user readable format etc.

As seen from the above, it is clear that the cyber forensic lab is helping the department to acquire and analyse complex data. Hence, there is a need for creation of cyber forensic lab at major centres and its help should be taken for proper analysis of data. Care also should be taken to keep upgrading the tools present in the labs and also upgrade the knowledge base of the people working with it.

## Chapter 12

### Case Scenario's

#### Case Scenario-1

A search was conducted by Ahmedabad Directorate in ABC group in April 2013. This group is engaged in providing accommodation entries of Share Capital & Long Term Capital Gains. During the course of search it was found that the details of the cash received and the accommodation entries provided were recorded in various excel files in the computers maintained at various premises. Mirror images of the hard discs were prepared using the services of the Forensic Experts. In all 15 hard discs were seized/impounded.

The data contained details of the cash received from the clients and accommodation entries provided to them. The hard discs were analyzed for incriminating evidence. On analysis it was found that date-wise details of cash received from various clients was maintained in the "Cash Sheets" seized in form of the digital data. It was also found that the date-wise details of the accommodation entries provided along with the details of internal layering of funds were also maintained in 'Cheques Sheets'.

On analysis of the seized data it was found that details of cash received by ABC for a particular period (01.04.2012 to 31.03.2013) were not available. Thus, forensic analysis of the seized hard discs was carried out which resulted in recovery of 'Cash Sheets' containing details of additional receipt of cash aggregating to more than Rs 420 crores for the said period.

Further, analysis and correlation of the digital data was carried out using the MS Excel functions viz. Pivot tables"; "Filters"; "VLOOK UP"; "IF" so as to identify the beneficiaries and correlate the cash paid by them and accommodation entries received there against.

This analysis led to the identification of beneficiaries of accommodation entries aggregating to Rs. 2849.48 crores.

#### Case Scenario-2

A search action was carried out by Bangalore Directorate in September 2013 on various cooperative societies and their developers. Discreet enquiry carried out by the department had revealed that one of the key employees was maintaining all the data of unaccounted cash receipts and cash payments in a pen drive/laptop. During the course of search, a laptop was recovered from the key employee. The laptop was forensically imaged and the data was previewed using a write blocker. The excel sheet revealed details of unaccounted cash receipts and cash payments which were maintained by the assessee on a day to day basis. On the spot analysis was carried out and print out of the excel sheet which ran into 300 pages

containing details of unaccounted transactions from AY 2009-10 to AY 14-15 was confronted to the key employee and the main assessee who accepted the receipt of cash and payments in cash. The assessee accepted Rs 45 crores for various years. In one more developer of a cooperative society again excel analysis revealed payments made in cash to various sanctioning authorities which were quantified and reported to the central circle for assessment. In the entire cooperative housing society, cyber forensics revealed the crucial excel sheets containing various cash transactions which has resulted in a disclosure of Rs 450 crores and an estimated concealment of Rs 570 crores as on date.

### Case Scenario-3

A search action was carried out by Ahmedabad Directorate on a Gujarat based beneficiary of accommodation entries. The said group was aware that evidence relating to bogus entries taken by them already stood seized by the department in an earlier search and they were taking necessary precautions. In this background and to preserve the element of surprise, the search action involving simultaneous search/survey at 40 premises was launched without any public requisition of officers and staff from the field formation at Ahmedabad. During the search Cyber Forensic tools were used to meticulously acquire evidence. In this action one physically damaged hard disk could not be operated during the search and thus the original of the same was seized. Multiple attempts to read the said hard disk by Cyber Forensic expert failed. Still the matter was not given up and by using the services of 'Deloitte Computer Forensics Lab' finally the said disk could be read. The forensic analysis revealed that the disk had been formatted more than 10 times in the past and one of its physical components stood damaged. With the help of these experts the data from the disk was recovered from the disk.

This disk contained detailed particulars of the on-money charged by the builder group for the period 2010-11 to 2013-14. The date-wise, transaction-wise, premise-wise details of unaccounted on-money noted in the seized data in the form of excel sheets stood at Rs. 1038.74 Crores. Apart from this, other physical evidence of charging of on money to the extent of Rs.330 Crores were also seized in the form of a diary. The noting in the said dairy also corroborated the payment of cash. In this way evidence of total "on money" receipts of Rs. 1368.74 Crores was seized.

### Case Scenario-4

The main business of XYZ Group searched by Investigation Directorate Pune was export of medicines and drugs catering to the online pharmacy market. Customers of such market are mainly located in USA. Assessee procures the generic medicines from local market, packs such medicines and exports them on retail and wholesale basis to UAE through Singapore and Mauritius. The billing of such export sale was done in the name of a group company located in Free Zone area of Sharjah, UAE. The proceeds of export sales were sent to Indian company against the purchase of goods from them by giving about 10% margin to the Indian company, whereas the UAE Company made a margin of about 200% on such exports.

During the course of search, it was noticed that the assessee had destroyed all the hard discs of the computers before search action. In the post search enquiries, he was requested to produce sale and



purchase invoices of UAE based company. About 30,000 of such invoices were submitted in electronic format. These invoices were run through **xpdf** software in order to find the source of generation of these documents. ***It was found that these documents are not printed but are auto generated on an ERP system.*** But no such ERP system was found during the course of search & seizure action. While verifying the documents, some references to the term '**Jade Pharma Ver 1.0**' were found. Metadata of the pdf documents referred above showed that such documents were prepared on an ERP package named Jade Pharma.

Through discreet enquiries it was found that '**Jade Pharma Ver 1.0**' was an ERP package employed by assessee for carrying out his business. This software was built and operated by Pune based company namely ABC Pvt Ltd. Consequent survey was carried out on this company. In the survey, architecture of '**Jade Pharma Ver 1.0**' and e-mail communications of employees of XYZ Pvt Ltd group with employees of ABC Pvt Ltd, regarding operation of this software were impounded. Analysis of these e-mails showed that assessee is carrying the entire business in India.

There were references to some IP addresses to such e-mail communications. Such IP addresses were located physically and it was found that they belong to PQR Pvt Ltd. who hosted various websites of assessee. Survey was carried out on this PQR Pvt Ltd. It was found that PQR Pvt Ltd. had hosted the websites of XYZ Pvt Ltd group but the physical servers were located in Tata Communications Ltd., Dighi, Pune. Hence, consequential survey action was carried out on Tata Communications Ltd. From this premises data of about 78 websites was located and impounded. The analysis showed the entire chain of receiving orders from the customers, processing such orders, procuring the products and exporting these products to the customers. Money was received through credit cards in bank accounts of UAE.

'**Jade Pharma Ver 1.0**' was activated in the office and its working was analyzed along with some of the data. It was seen that entire process regarding operation of the business were carried out in India whereas the assessee is showing the business profits in UAE and thus evading taxes in India.

Assessee claimed that he is having business set up in UAE which is managed by a Manager since 2007. Enquiries with passport office and FRRO, Mumbai revealed that the Manager in UAE is a relative of the assessee and was data entry operator with him before he went to UAE in 2011. The assessee was claiming the business set up managed by this manager since 2007. Further, a friend was sent to Sharjah UAE office of assessee and the video and pictures of the office were obtained discretely. Assessee did not question the validity of this video. This video showed an office of about 200 Sq. ft. with no staff at all. The facts and circumstances indicated that it was not possible to carry such a large business from UAE and that all the segments of business processes were operated in India and hence the income should be taxed in India. The assessee has approached Settlement Commission in his individual capacity. Assessment proceedings in rest of the cases are in progress.

## Case Scenario-5

A search action on PQL, a bullion dealer, was conducted by Ahmedabad Directorate (Rajkot unit) in

May 2013. **A noteworthy outcome** of the post search enquiry was the detection of the offshore trading and holding of foreign bank accounts of the assessee. During the search, cloning and imaging of the hard disc was done using Forensic Tools. All partitions of the hard disk were scanned for recovering deleted data. Forensic analysis recovered following three important deleted files.

- i. *HTML documents containing details of Trading on Metals Web platform of Standard Bank, London. It was an e-mail attachment having prima facie financial transactions (peak value) worth \$ **1,02,43,185.62 (Rs.55,09,57,395/- on 03/05/13).***
- ii. *One scanned image of a handwritten and signed direction of PQL for transferring **\$100000 (INR 55,03,968/-)** from account **with National Bank of RAS Al Khaimah, Dubai (U.A.E)** to another account **with Standard Bank**. Thus, this document detected presence of two foreign bank accounts of PQL.*
- iii. *Copy of Margin Money call Statement having prima facie transactions worth **\$28,00,589.57 (Rs. 15,36,28,861/- as on 17/5/13).** This statement was also in the form of an e-mail attachment.*

Forensic analysis established that above files were deleted just before the search and were re-checked by PQL after deletion to be doubly sure. Above documents established that the PQL had accounts in foreign banks and was also trading online on the Metals Web Platform of the Standard Bank. Assessee had neither disclosed the overseas income nor the existence of foreign bank accounts in his returns of income. In his statements before DDIT (inv.), assessee expressed his ignorance about these facts.

With a view to gather complete information about his overseas transactions; references under DTAA were made to UK, UAE & Singapore Tax Authorities on 12.8.2014 through FTTR division of the Board. Singapore authorities promptly provided all requisite information on 20.3.2014 including copy of account with Standard Bank, London and oversee Trading account from FY 2007-08 onwards. Even UAE authorities provided copy of account of PQL with National Bank of RAS, Al Khaimah, and Dubai on 15.6.2014. KYC details from Banks firmly established the ownership of Shri PQL. These documents also give incontrovertible proof of huge unaccounted foreign income from AY.2008-09 onwards.

Department has filed prosecution against PQL. His name also has been revealed to the Supreme Court and SIT.

### Case Scenario-6

A search was carried out by Ahmedabad Directorate in July 2013 in the case of a group engaged in 'Dabba Trading' in Commodity/Share Futures' on a very large scale. The evidence pertaining to off-market trading in futures seized during the course of search at Commodities Futures was largely in the electronic format in local customized accounting software viz. 'Bright Future', 'New Vayda', 'Accounts', 'AC4' and FMT 2010. As the accounting data was voluminous and pertained to multiple years, for the purpose of analysis, rather than using the limited options provided for in the front end application file, the entire data analysis was carried out with back-end raw data-files available in different format. Analysis of digital data resulted

into detection of unaccounted income/investment to the tune of Rs 480 Crores. The major areas of detection of such unaccounted income/investment are as follows:

- i. Detection of unaccounted income to the tune of Rs 83 Crores w.r.t off-market trading transactions in commodity futures
- ii. Admission of unaccounted investment to the tune of Rs 5.8 Crores in land
- i. Detection of unaccounted receipts from off market trading transactions in futures to the tune of Rs 130 Crores
- ii. Detection of unaccounted investment in real-estate to the tune of Rs 100 Crores
- iii. Detection of unaccounted brokerage income to the tune of Rs 20 Crores from off-market trading in futures
- iv. Accommodation entries of profit/loss in the regular books of account to the tune of Rs 18.7 Crores
- v. Admission of unaccounted receipts of Rs 9 Crores w.r.t land transaction by counter parties covered in consequential search. As the searched group is the payer the total impact of the evidence is Rs. 18 Crores
- vi. Client Code Modification having revenue implication of Rs 7.3 Crores
- vii. Detection of unaccounted expenses to the tune of Rs 3 Crores w.r.t off-market trading in futures

### **Case Scenario-7**

Search was mounted by Bangalore Directorate in ABC group of cases of where pre search reconnaissance work revealed that in the business of running hotels, restaurants and lodging, computer generated bills were being returned to cashier. He was befriended over a period of time and this led to obtaining the contact number of the software person maintaining the software for the entire group of restaurants. The alibi of setting up a new chain of restaurants which required similar software package finally led to the information that the package installed at the Empire Hotel group was structured to suppress sales. The suppressed data would be periodically deleted. The officials of the Central Forensic Lab, Hyderabad were contacted and forensic experts from Mumbai were called. Twenty hard disks, having a capacity of 80 GB each, were kept ready to clone all the hard disks of the assessee group.

During the course of search, the technical person working with the group was interrogated. He revealed that the customized billing software, "Restaurant Management System", gave the assessee an option to decide the percentage of sales to be accounted. The assessee would make use of the option on a daily basis and account for only a certain percentage of sales while the rest would be hidden and later deleted.

During the course of search, mirror images of all computer hard disks found in all branches of the hotel were taken by using forensic software called "ENCASE". The hard disks carrying the mirror images were seized along with the hash value certificates.

Post search, the deleted sales data were retrieved from the mirror images by using forensic software. The modus operandi was established by collating the retrieved data and the suppressed sales and the concealed income was quantified financial year wise. The assessee admitted a sum of Rs. 10.57 crore as undisclosed income spread over a period of time, from assessment years 2005-06 to 2008-09 and paid Rs. 3.50 crore as taxes. The modus operandi established that unaccounted income generated by suppressing the sales was being applied in construction of new hotels.

### Case Scenario-8

A search action was conducted by Ahmedabad Directorate in October 2013 in a group engaged in the business of construction and sale of residential and commercial premises.

During the course of search, image back up of digital data contained in hard discs/servers at various premises was taken. The files from the mirror image were restored using Encase software which succeeded in recovering many deleted files evidencing receipt of on-money. Such details were maintained in Excel formats. Deleted files recorded receipts in cash as well as cheques. On comparison with regular books of accounts maintained in Tally software, it was noted that the company resorted to systemic suppression of receipts from customers. Ledger wise analysis of customers revealed that cash receipts from customers were not entered in regular books of accounts. The suppression of receipts computed in respect of eight real estate projects aggregated to more than **Rs.82 crores**.

### Case Scenario-9

Search was conducted by the Bangalore Directorate in the case of a jeweler in Bengaluru having its last reported turnover of more than Rs. 350 crores through its five branches. Intelligence was gathered that the jeweler was using customized software which enabled it to record accounted and unaccounted transactions separately, thus suppressing part of its total sales. Forensic tools were organized beforehand to retrieve the hidden and deleted data from hard disks of all server computers.

On the day of the search Encase forensic software was used to image the hard disks of all server computers and other systems numbering more than 20 at all showrooms and offices of the jewelers.

Further, at the residence, three kinds of computer generated statements were recovered. The statements were for the previous day. Separate statements in the same format for two of its branches were found indicating-

- Maintenance of two different cash books
- Two different cash balances
- Two separate sets of data pertaining to sales for the day in quantitative and value terms

The trigger for further investigations was the fact that the figures mentioned against cash balance marked with a \* sign at the bottom of the report of each of the two branches matched with the cash found

from the branches in excess of cash balance as per books. Various hard drives imaged and cloned were searched with specified key words using Encase such as Cash Bal\*. Search on each system went on for 6 to 18 hours. The search revealed that these reports were not being saved on the system. However, search resulted in retrieval of such reports for various dates and for various branches spanning four months in FY 2009-10 and 2010-11 from the unallocated clusters of the hard disk. This data was not continuous.

However, because these reports were system generated, it was clear that the data embodied in these reports was already present in the database. To understand where to look for such data in the huge database, the data in all the computers was studied in detail. In the hard disk of the server computer of M/s PQR Soft Pvt Ltd (the company which developed the software for M/s ABC Jewellers and which was covered as part of search) documents were found relating to various modification and up-gradations made to the software package from time to time. Study of these documents revealed that the software allowed data pertaining to unaccounted transactions to be deleted from the relevant tables of the database at the end of each day and after generating the above mentioned reports for that day. It also revealed that before deleting this data, some part of the data relating to sales and actual stock would get saved in specific tables so as to enable viewing transaction history at any time.

The next logical step was to search for such specific tables in the Sequential Query Language (SQL) database. For this the virtual environment had to be recreated in the office of the Investigation Directorate by linking the data contained in the cloned hard disks with the appropriate version of SQL database application in order to be able to access the data in a readable form. Subsequently, search for the specific tables in the database using SQL revealed the entire actual sales-related and stock-related data for Feb 2009 onwards i.e. from the time the software was deployed. Unaccounted sales data of more than 1300 kg of gold of more than Rs. 210 crores spread over a span of 17 months was retrieved from the aforesaid tables. The assessee accepted the findings and admitted Rs. 21.5 crores as its undisclosed income from unaccounted sales & purchases made during the said period.

### **Case Scenario-10**

In a case investigated by the Investigation Wing in Mumbai, the assessee was a builder. The department had information that the assessee had been accepting on-money. During the course of search, the electronic records of the assessee were carefully observed and it was found that the assessee had two email accounts which were not previously disclosed to the department. On further analysis, it was found that these two email accounts contained the parallel books of accounts maintained in Tally and Excel sheet. These parallel books of accounts contained the unaccounted cash receipts and expenses of the assessee. The modus operandi of the assessee is that he maintains the accounts in Tally and also in Excel sheet and then e-mails it to the second account. When confronted with these findings, the assessee accepted the same. The estimated concealment in the group was Rs 300 crore.

### **Case Scenario-11**

In this case investigated by the Investigation Wing in Mumbai, the assessee is an individual belonging

to one of the most reputed business family who is running many businesses. It was found that a close associate of the main assessee maintains his accounts in a gmail account. The close associate was interrogated by the department about the account and it was found that the e-mails related to the undisclosed foreign accounts of the assessee were deleted. The associate was persuaded to send an email to the foreign banker to resend the mails and the Department got a copy these emails. On careful analysis of these emails, it was found that the emails contain the complete details of the assessee's undisclosed foreign bank accounts and other investments. The total investments exceed US \$ 48 billion.

### **Case Scenario-12**

In this case investigated by the Investigation Wing in Mumbai, the assessee manufactures and sells high end jewellery. They also import high end watches. Both the watches and the jewellery are sold in exclusive showrooms in high end malls. During the course of search, a secret premise was found and on searching that premise, it was found that parallel books of accounts are being maintained by the assessee in a separate hard drive. The department took the backup of the hard drive and on analysis, it was found that there is a folder containing the unaccounted cash receipts and expenses. When confronted, the assessee made a disclosure of Rs 28 crore on this issue (a further disclosure of Rs 34 crores was made on other issues).

### **Case Scenario-13**

In another case investigated by the Investigation Wing in Mumbai, the assessee is in construction business. In a search premise, the search party caught hold of the assessee trying to dispose of two pen drives. These pen drives were taken into custody and a forensic team was called so that these may be examined without destroying the evidentiary value. The search party examined these pen drives using a write blocker device and found that there are certain abbreviated names against which some numbers were written. These abbreviations were searched for in mobile phone of the assessee and it was found that there are phone numbers written against these abbreviations. Then, using True Caller application, the names of the owners of these phone numbers were identified. The assessee was confronted with these facts who admitted undisclosed income of Rs 210 crore.

### **Case Scenario-14**

In one of the search and survey action conducted by the Delhi Investigation Wing, evidences of tax evasion were predominantly gathered from the electronic data seized from different premises of the assessee group. The case was unique in the sense that final outcome of the case hinged completely on the incriminatory data retrieved from seized electronic devices. The data was available inside seized hard disks, pen drives, and back-up of the mobile phones and tablets/i-pads taken during course of search and seizure action.

The imaging and cloning of the seized electronic devices was done both on-site and off-site using standard operating procedure keeping in mind that the evidentiary value is maintained. Further, for post-



search analysis, Encase Version 7 software was used using which the data available on the target electronic devices was retrieved and categorized. Type of electronic data retrieved from the seized devices included email conversations between related parties, various types of documents in .doc, .xls formats apart from the images of scanned documents, back-up of Black Berry smart phones in .bbb/.ipd format etc.

Analysis of email conversations and various types of documents was done via different keyword searches using dtSearch Version 7.72 software. Uniqueness in the case was encountered while analyzing .ipd/.bbb files which were found stored on various seized hard-disks.

### **Methodology adopted to decode .ipd/.bbb files:**

Such files were created when back-up of the BlackBerry smart phones was taken using BlackBerry desktop manager utility. It was found that back-up of various smart phones used by the promoter-family and employees and associates of the assessee group were taken and stored on the hard-disks that were seized during search and seizure action. All such files were clubbed together for the analysis purpose. Initially, to analyze these files, Encase Version 7 utility was used. It resulted in retrieval of conversations over BlackBerry Messenger application. The conversations were essentially between two eight characters alpha-numeric codes that were referred to as PINs. It was observed from the perusal of the contents of the conversations that one individual was using multiple PINs. As such, in order to establish the identity of the individual and the nexus of the PINs with the individual concerned, inquiries were conducted and reports were sought from M/s Black Berry India Pvt. Ltd. – the service provider. From the reports that were submitted by the service provider, the identity of the individuals using BBM PINs so used in conversations was established. It was also conclusively proved that in some cases, multiple BBM PINs were used by same individual at different points of time. Significantly, the service provider intimated that different third party software tools are available in the market each having its own capability in decoding the .ipd/.bbb files. Encase 7 which was used initially was one of them. It was further found that this tool was not capable of retrieving the entire data stored inside a .bbb/.ipd file.

### **Engaging the services of CERT-in :**

In order to handle the technological challenges, services of experts of CERT-in were utilized. The seized hard-disks in which .ipd/.bbb files were found stored were handed over to them for forensic analysis. The experts used sophisticated BlackBerry Extractor Pro software to retrieve data from the target .ipd/.bbb files. The data so found was authenticated by CERT-in and was available in a readable format. This data was then analyzed and used in gathering evidences of tax-evasion against the assessee group. Investigation has led to detection of substantial amounts of tax evasion.

### **Notable outcome of the exercise:**

- Unique experience of handling .ipd/.bbb files from the perspective of gathering evidences
- Roping in the experts of CERT-in for digital forensics study

- Deploying sophisticated software tools for retrieving data and analyzing the same
- Establishing the identity of the individuals thereby unearthing clinching evidences of tax evasion

### Case Scenario-15

A search was conducted by the Bangalore Directorate in a Casino Group in Goa. To maintain the secrecy of the search action, teams were assembled at Belgaum, 175 kms away and moved early morning at 2.30 hrs to strike at 06.45 hrs. Casinos are operating offshore on ships, accessible only by dedicated feeder boats. Advance parties were sent on board to the casino ships at 0300 hrs as decoy customers to ensure safe custody of records relating to cash transactions. Search action resulted in recovery of a secret pen drive containing details of customers numbering more than 3900. Cash receipts from individual customers were unaccounted. Settlement of accounts including winnings was done in cash without TDS. Evidence of suppression of gross gaming receipts of about Rs 333 crores was gathered. The assessee admitted undisclosed income of Rs 61.25 crores. Unaccounted cash of Rs 5.16 crores was seized from the premises. Through the analysis of the data in secret pen drive, Hawala Operators and their operation network was identified which further resulted in an admission of Rs 4.12 crore.

### Case Scenario-16

A search was conducted by Bangalore Directorate in two listed real estate companies. The department had evidences for collection of on-money by these listed companies. Cash generated through these mode was used to make unaccounted cash payments towards land purchases and project approvals. The major challenge in this exercise was the huge data running more than 4 TB which was cloned and imaged during the course of search. A business specific process was adapted in this case, where emails, excel sheets running into more than 4 lakh spread across key business processes like marketing, HR and accounts. From the first spilt, all the relevant excel sheets and mail extracts with key personnel handling cash was found. Analysis of these excels sheets and mail extracts revealed evidences for collection of on-money from various customers. The same was confronted to the assessee and assessee admitted undisclosed income of Rs 380 cr. The estimated concealment in the case amounted to Rs 780 crore.



### Backup with few softwares- Examples

#### 1.1 Using Robocopy for taking Logical Backup of Windows System

Robocopy, or “Robust File Copy”, is a command-line directory and/or file replication command. It has been available as part of the Windows Resource Kit starting with Windows NT 4.0, and was first introduced as a standard feature in Windows Vista and Windows Server 2008. The command is robocopy.

`robocopy <source drive> <destination directory> /S /COPY:DAT /LEV:10 /W:0 /R:1 *.<document extension>*`

Run this Robocopy command for each source drive to copy relevant files. An example robocopy command would look like following:

`robocopy C:\H:\ADFL\John_doe_laptop\documents /S /COPY:DAT /W:0 /R:1 /LEV:10 *.doc*`

Above command would copy all Microsoft word files on drive C: to destination USB drive H: inside the folder ADFL\John\_doe\_laptop\documents.

- `/S` :- indicates that source directory structure is automatically recreated on destination drive for only those files which are copied
- `/COPY:DAT` :- copy file attributes excluding local security attributes.
- `/R:1` :- Sets number of retries in case copy failed to 1
- `/W:0` :- Indicates that in case file fails to copy wait between successive
- `/LEV:10` :- Sets depth of directory hierarchy to traverse to 10

Above process needs to be repeated for following document extensions for all local drives such as C:, D:, E: etc. The following document specific backups can be taken using the following extensions:

- **.doc\*** – for word documents (Note: Reference to doc as well as docx proprietary file format of Microsoft)
- **.xls\*** – for excels (Note: Reference to xls as well asxlsx proprietary file format Microsoft )
- **.pst** – for emails (Note: Reference to personal storage format proprietary file format Microsoft )
- **.pdf** – for PDF documents
- **.900** – for tally 9.0 ERP data
- **.500** – for tally 7 data
- **.mdf** – for MS-SQL data

## 1.2 Using Emcopy for taking Logical Backup of Windows System

Emcopy is the fastest data copying tool which uses memory pre-allocation and multithreading. Emcopy has similar switches as compared to robocopy like /s, /r:<n>, /lev:<n> etc

### Syntax for emcopy

**Emcopy source\_drive destination\_drive \*.extension /s /lev:<n> /nodf /w:<n> /r:<n>**

For copying documents

**Emcopy C:\H:\john\_doe\documents \*.doc\* /s /nodf /lev:10 /w:0 /r:1**

Similarly for spreadsheets

**Emcopy C:\H:\john\_doe\spreadsheet \*.xls\* /s /nodf /lev:10 /w:0 /r:1**

## 1.3 Live backup on Macintosh/Linux

Both Macintosh and Linux being UNIX variants, their backup procedures are same due to common set of tools being present. The procedure is as follows:

- **Make Sure you are in Home Directory.**
- Following command lets you do selective file copy based on extension. Example given is for .doc files.  
`find . -name "*.doc*" | cpio -pdm /path/to/destdir`

## 1.4 How to take Back Up of Email?

Emails contain very important conversation threads. Corporate email can be stored onsite or offsite. The most common email software in corporate is **Outlook**. All the emails accessible in Outlook are stored locally in a file format called PST. The file extension is .pst. Backup of .pst can be taken using robocopy method.

The location of \*.pst can also be got by going into Account Setting tab in Microsoft Outlook where the path for the file would be given. In case of Gmail, there is a direct option of taking a back up in account settings. One can go their and take a backup. In non-gmail cases like yahoo, rediff, you can have two options. Firstly, sync the mail with Microsoft outlook which can be then copied as a separate pst file. Secondly, create a dummy gmail account and transfer all the above emails and take backup. In case of emails, always remember change the password during the course of search so that data may not be destroyed by others.

In Gmail and Google Drive, you can take the archive by the following process also :

- Click on the Accounts
- Next click on Data Tools tab.
- From the options select download data: select data to download.
- Click on Add to Archive.

Finally select the backup for (Only check for only two options) :

- Gmail, Google Drive
- Click on Create Archive.
- After archive creation is done, download the archive on your backup media.

### 1.5 Tally.ERP backup

Tally is one of the oldest and the most popular accounting system in India. There have been several releases of tally software since it was first went to market in 80's. Still the Tally engineering team have pretty much stuck through their basic architecture of have a file based database and a DOS compliant user interface.

On a single machine, several instances of tally data/tally application can exist. Any tally application can be made to read any of the data files by simply changing settings within the application. Tally creates a separate folder for per entity per financial year. i.e. If there are 3 books of accounts for company 'XYZ Pvt Ltd', then there will be 3 corresponding folders.

**The folder structure is as follows (This is for Tally ERP 9) :**

**<directory: nomenclature 5 digit number.>**

**CmpSave.900**

**Company.900**

**LinkMgr.900**

**Manager.900**

**TranMgr.900**

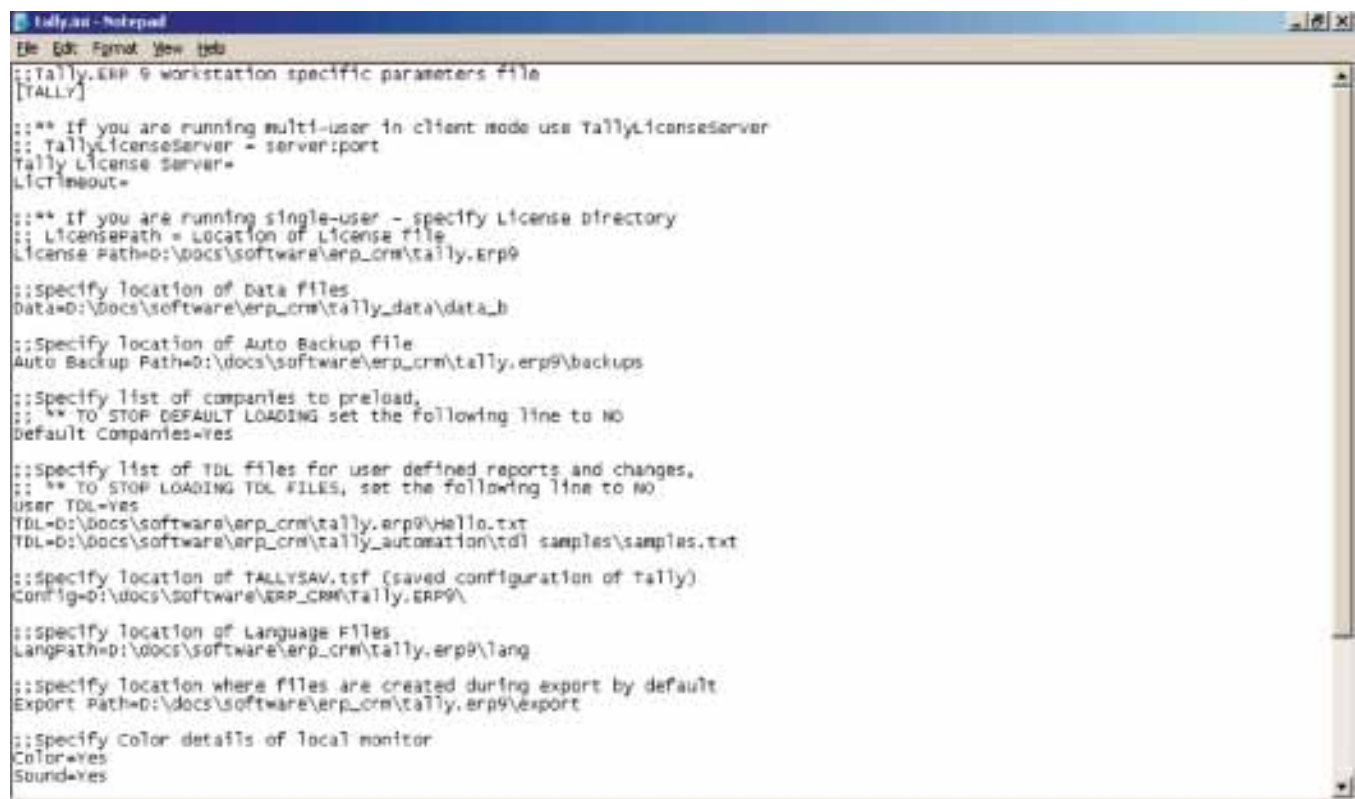
**TUPDATE.TSF**

Basically extension will be either .900 or .TSF. For tally 7.2 the directory structure will contain .500 files.

Even though there would be several DATA directories on a machine there typically would be only one active DATA directory where current accounting is being done. This could be a local or remote file share.

#### **Steps to find out active data location:**

- Open tally.ini file with notepad. It should be present in tally installation directory along with tally.exe
- Search for "Data=" string within notepad
- Open the directory path which follows "Data=" string
- Copy that entire directory to perform tally data backup (For Tally ERP9 the data folder should contain directory with 5 digit names like 00001, 10010 etc.)



```
File Edit Format View Help
::Tally.ERP 9 workstation specific parameters file
[TALLY]

::** If you are running multi-user in client mode use TallyLicenseServer
:: TallyLicenseServer = server:port
Tally License Server=
LicTimeout=

::** If you are running single-user - specify License directory
:: LicensePath = Location of License file
License Path=D:\docs\software\erp_crm\tally.erp9
::Specify location of Data files
Data=D:\docs\software\erp_crm\tally_data\data_h

::Specify location of Auto Backup file
Auto Backup Path=D:\docs\software\erp_crm\tally.erp9\backups

::Specify list of companies to preload,
:: ** TO STOP DEFAULT LOADING set the following line to NO
Default Companies=yes

::Specify list of TDL files for user defined reports and changes,
:: ** TO STOP LOADING TDL FILES, set the following line to NO
User TDL=yes
TDL=D:\docs\software\erp_crm\tally.erp9\Hello.txt
TDL=D:\docs\software\erp_crm\tally_automation\tdl samples\samples.txt

::Specify location of TALLYSAV.tsf (saved configuration of tally)
Config=D:\docs\software\ERP_CRM\tally.ERP9\

::Specify location of Language Files
LangPath=D:\docs\software\erp_crm\tally.erp9\lang

::Specify location where files are created during export by default
Export Path=D:\docs\software\erp_crm\tally.erp9\export

::Specify Color details of local monitor
Color=yes
Sound=yes
```

If the data location is on remote server then try to find out that server physically for tally backup. In many cases multiple tally folders exist on such server. In such cases use **robocopy** to traverse entire file system structure for a through backup. Tally extensions of interest would be .900, .500 and .TSF.

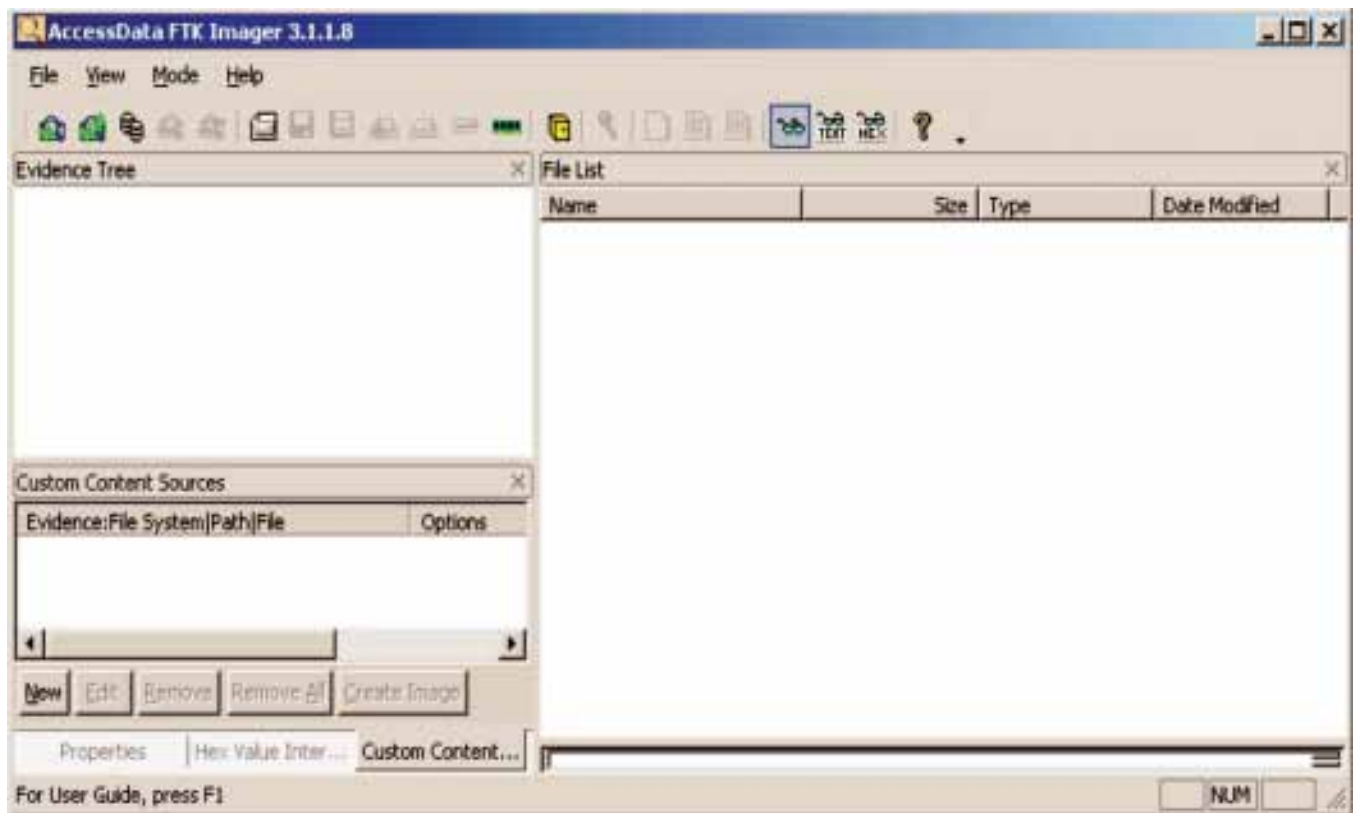
## Annexure-2

### Imaging of data- Few Examples

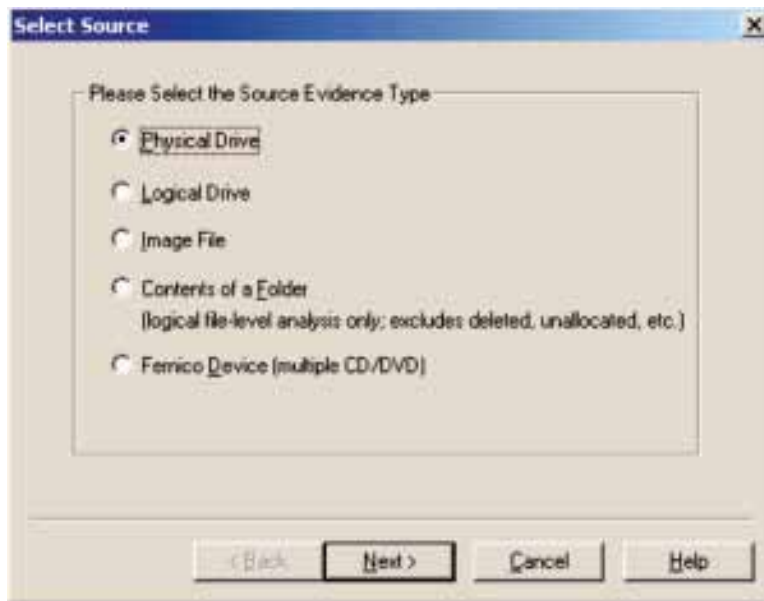
#### 2.1 Examples of Imaging on Windows Machine using FTK Imager

The process of using FTK Imager is as follows:

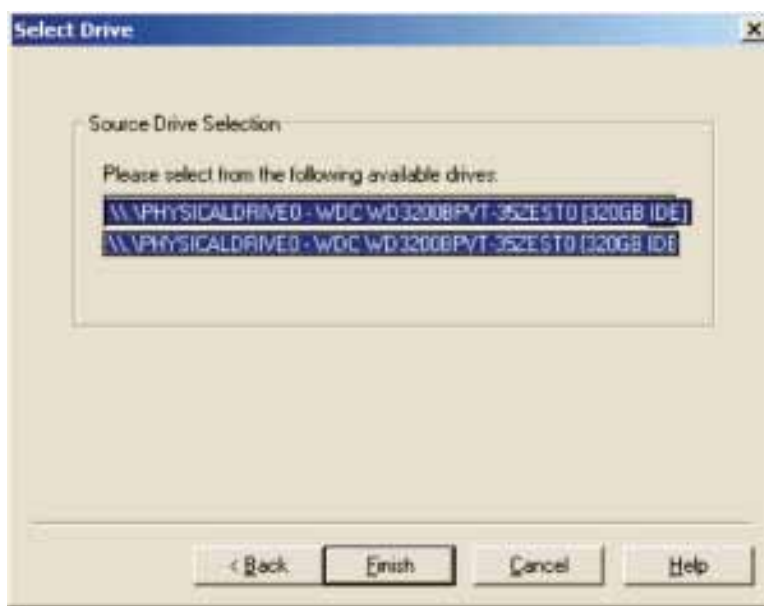
1. Prepare the USB acquisition media by copying FTK Imager software directory to the root of the USB hard-drive. Ftk Imager can run off of USB media on most target Windows machines.
2. Launch Ftk Imager so that you will see following window



3. Go to file->Create disk image to bring up following screen:

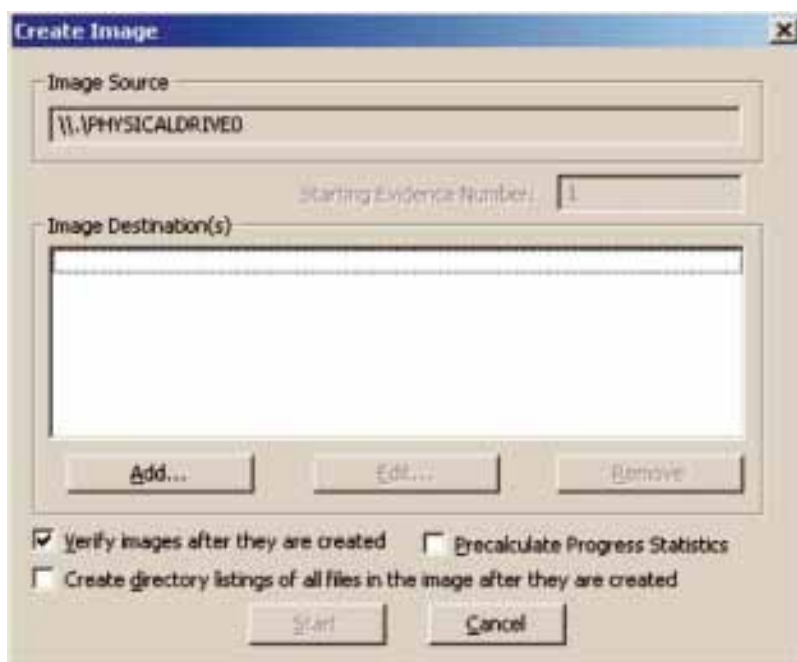


4. Keep “physical drive” selected and hit “Next” to bring up following screen:



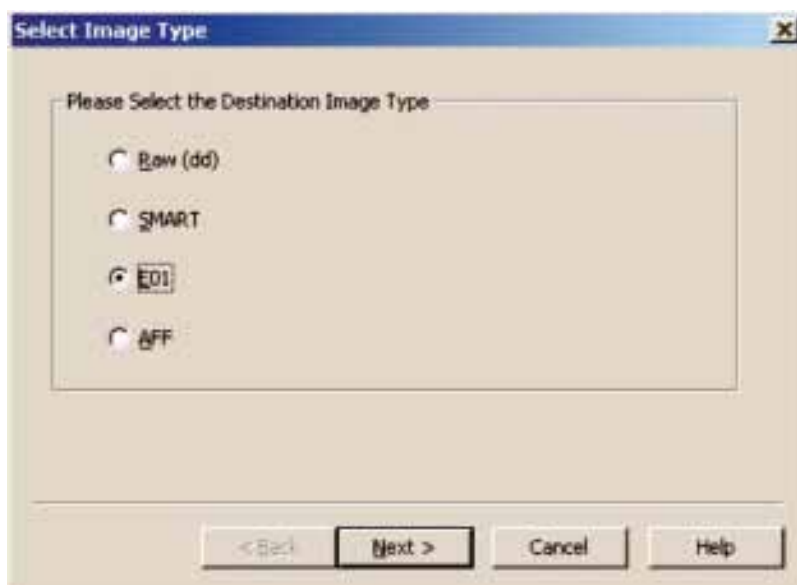
Make sure that you only select machine’s local hard-drive and not any USB media attached to the machine. Sometimes there would be more than one hard-drives attached to the same machine. In that case start a separate Image acquisition per hard-drive attached once the current one is over. In above box you will see 320 GB IDE HDD selected. Press “Finish”.

5. Following dialog will be displayed.

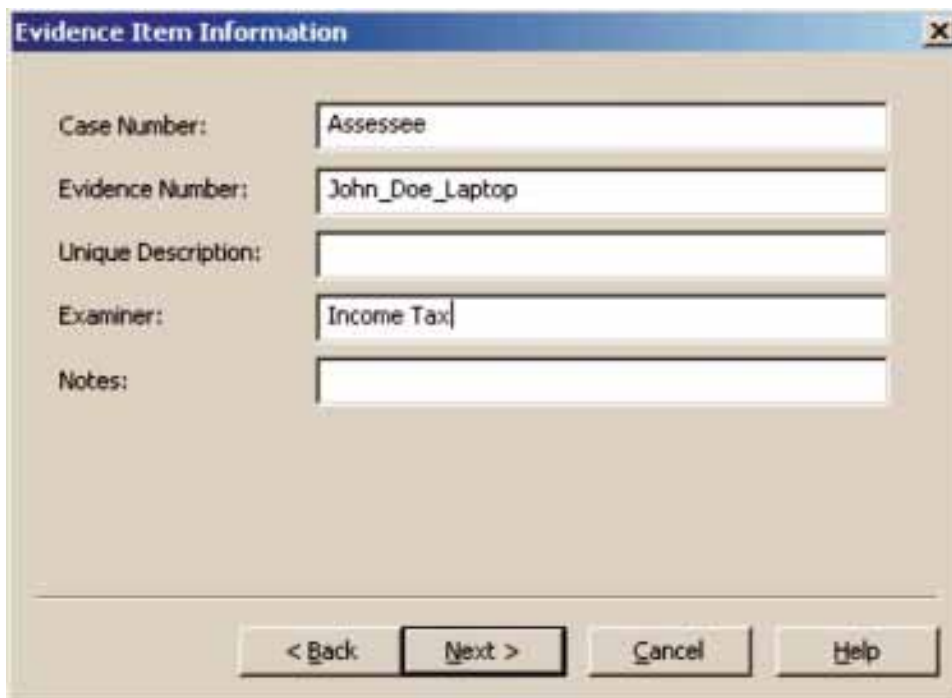


Make sure “Verify images after they are created” box is selected. Press add to create the image destination for the acquisition. This will bring up another dialog box.

6. In the following dialog box



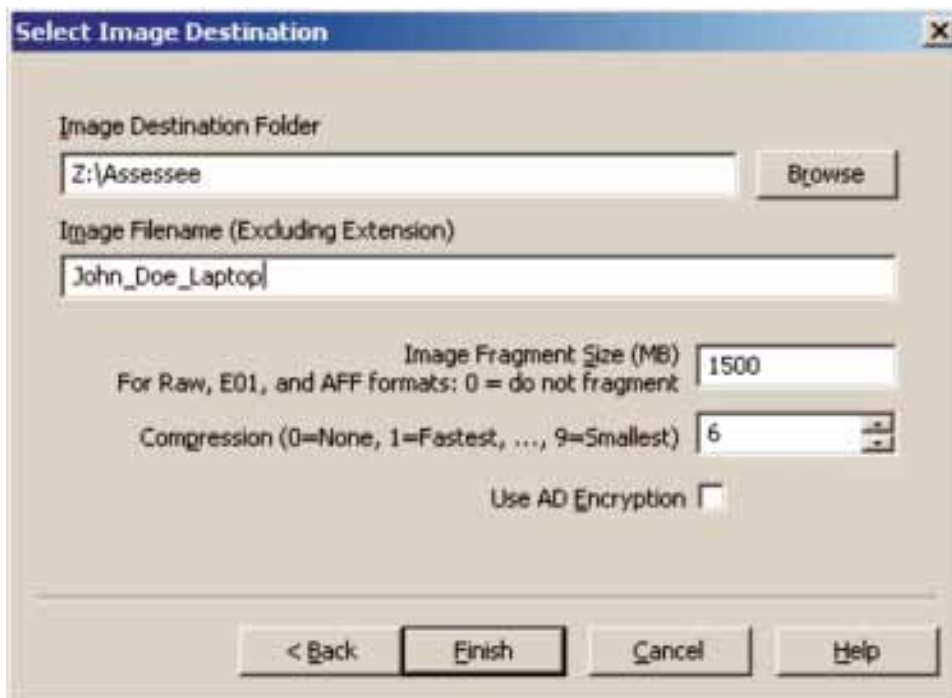
7. Next screen is where case details to be entered as follows:



The 'Evidence Item Information' dialog box contains the following fields and controls:

- Case Number: Assessee
- Evidence Number: John\_Doe\_Laptop
- Unique Description: (empty)
- Examiner: Income Tax
- Notes: (empty)
- Buttons: < Back, Next >, Cancel, Help

8. Next select final options like filename, foldername, chunk size, compression type etc.



The 'Select Image Destination' dialog box contains the following fields and controls:

- Image Destination Folder: Z:\Assessee (with a Browse button)
- Image Filename (Excluding Extension): John\_Doe\_Laptop
- Image Fragment Size (MB): 1500 (with a note: For Raw, E01, and AFF formats: 0 = do not fragment)
- Compression (0=None, 1=Fastest, ..., 9=Smallest): 6
- Use AD Encryption: ☐
- Buttons: < Back, Finish, Cancel, Help

As soon as you hit finish, Imaging will start.



After imaging is finished image verification would start. Image verification can take anywhere between 60% to 90% of the time taken to image the actual machine .So in calculating estimates for how long a certain imaging job would last, verification time overhead has to be taken into account.

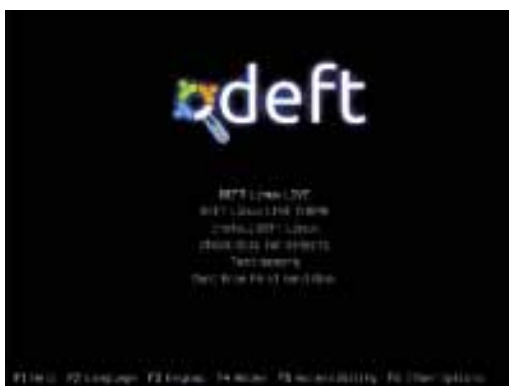
From experience rule of thumb is the entire processing can take anywhere between 1 ½ to 2 ½ min/Gigabyte of the harddrive size.

**After imaging is done make sure that there is a text file which contains the hash value report generated by FTK Imager.**

## 2.2 Examples of Imaging using GuyMager

For Imaging using GuyMager system needs to be boot in Deft Live CD.[ Deft Live CD contains Forensic Tools which primarily run with LINUX Kernel ]

1. To Boot system in Deft securely restart the system. [Do not change any file permissions/system dates].
2. After shutdown the machine, At start-up of [boot] we need to press the F2 or F12 [depends on the Motherboard] to choose boot from USB/CD-DVD Then system will start Linux as default OS.
3. You will see screen as seen below.



4. Select DEFT Linux LIVE as option.
5. After that computer will start loading drivers and then you will see screen like below.



6. Type “**deft-gui**” and Press ENTER in front of the **root@deft :#**

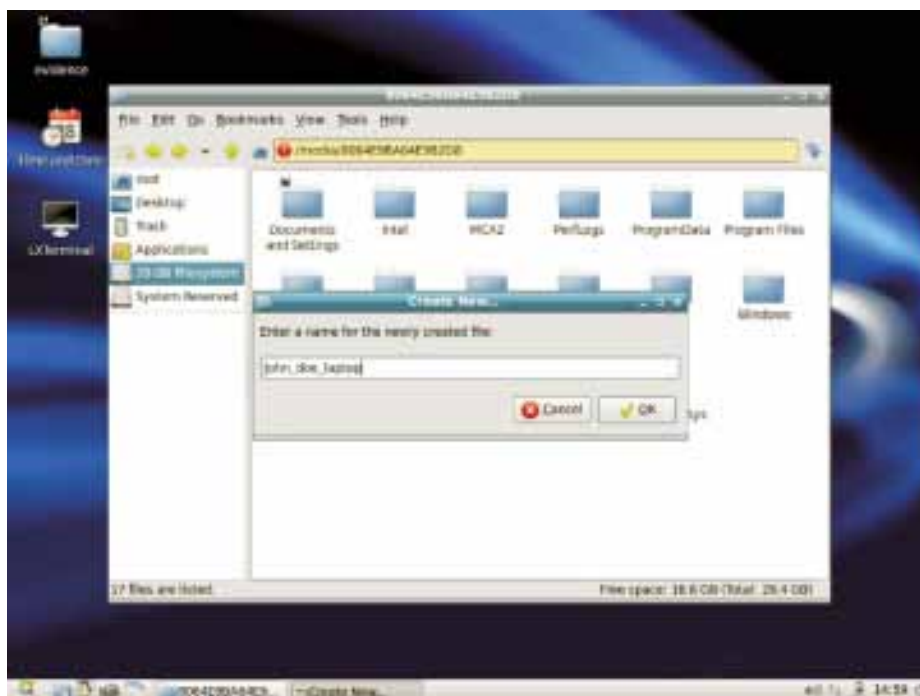


Deft GUI will load and look like this.

7. Click on Folder icon at the bottom left of the screen.  
8. Goto the root as shown below.



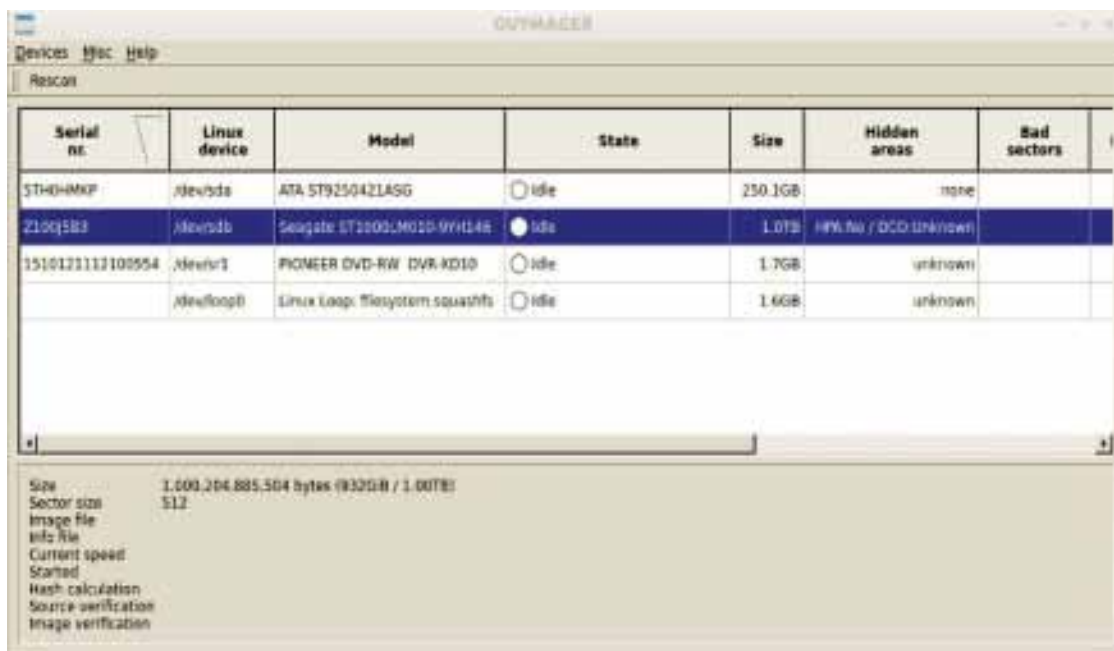
9. Goto media ? then select the Target drive ? create a NEW FOLDER with name of owner\_name like "john\_doe".



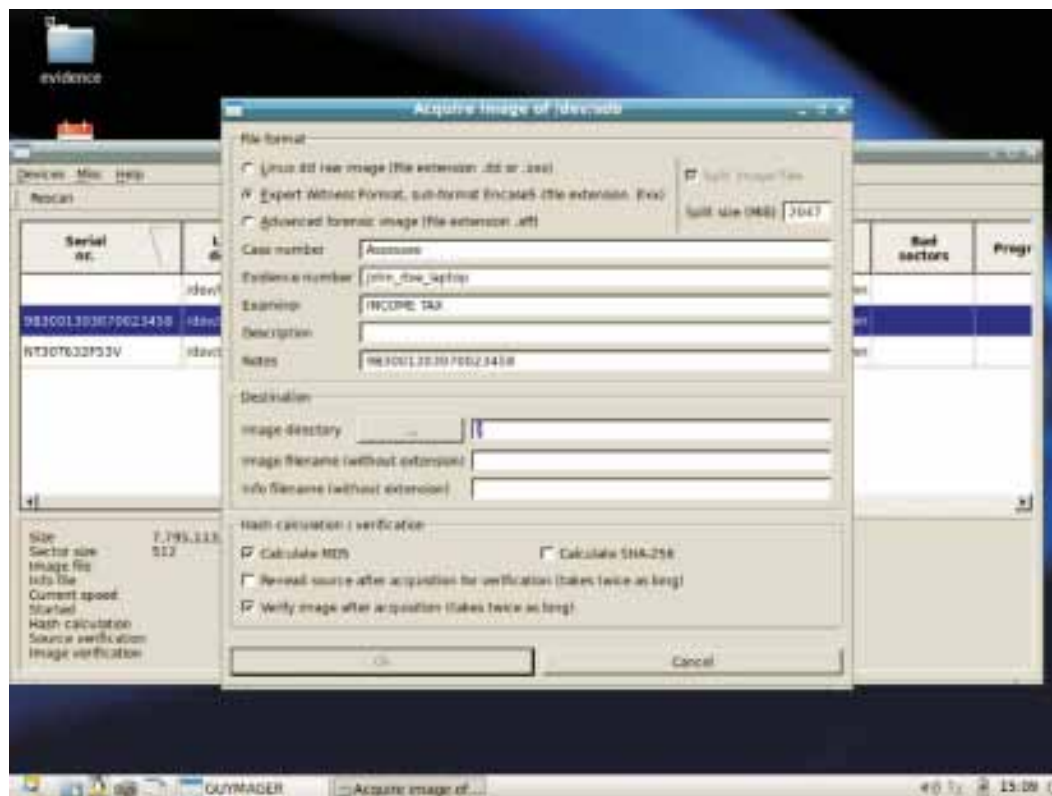
10. Then we start with acquisition software i.e. Guymager . Click on deft ICON at bottom left corner ? Disk Forensic ? Guymager.



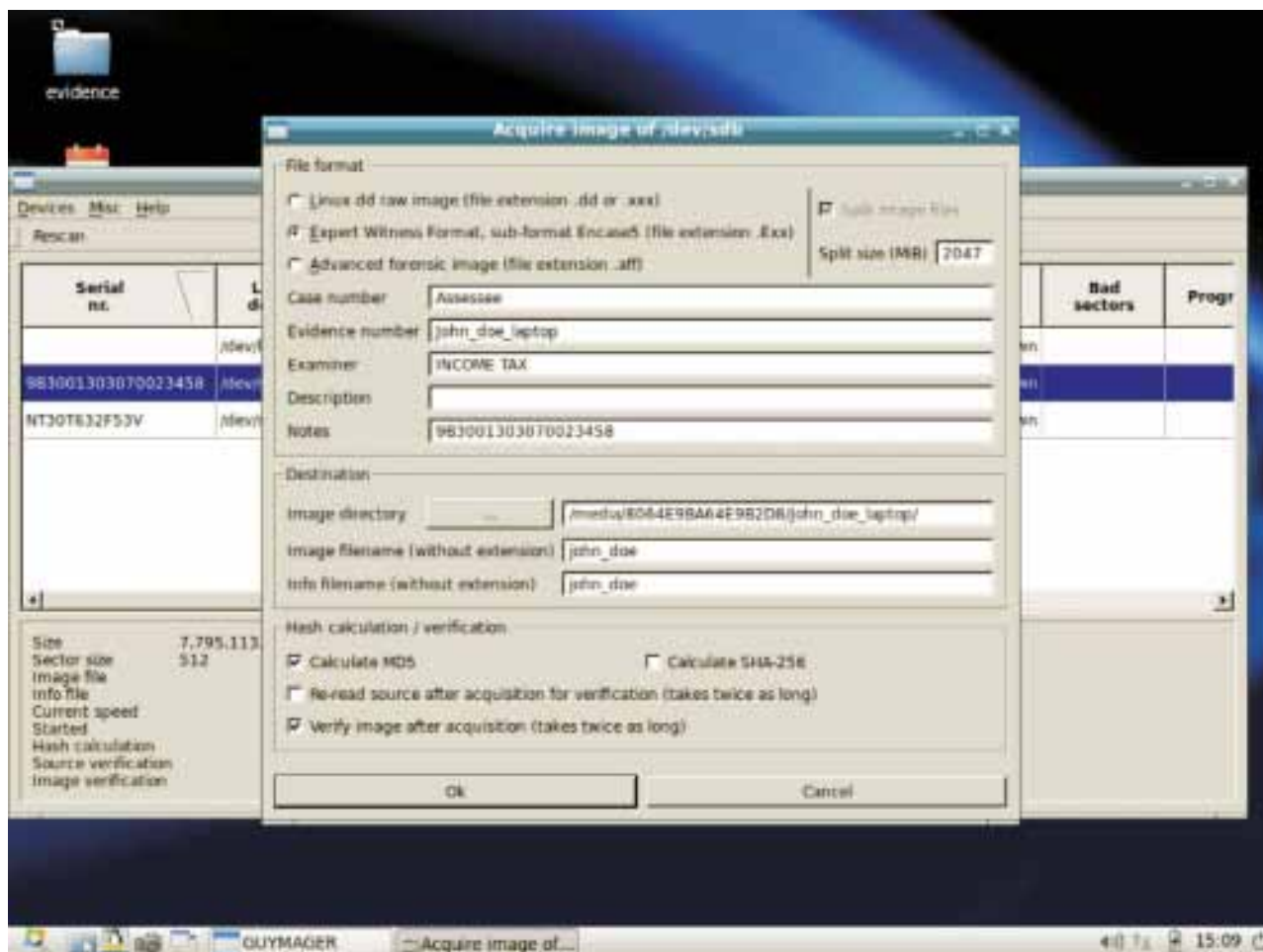
- See all the Drive and choose the target drive. Right click on the target drive and click on “acquire image.”



- After that you will see screen like below . Fill the Case number , Evidence Number , Examiner , Notes (default takes as source device number keep as it is)



13. Click on ... button show in front of the image directory. Then goto the folder that you have created in the target media .Choose the folder as destination. Also give Image Filename as device owner name like "john\_doe" you will see screen like below.



14. Make sure that calculate MD5 and Verify image after acquisition are checked. Click on Ok and wait to finish the process.
15. **After imaging is done make sure that there is a text file which contains the hash value report generated by Guymager**

### 2.3 Imaging/ Cloning with Encase

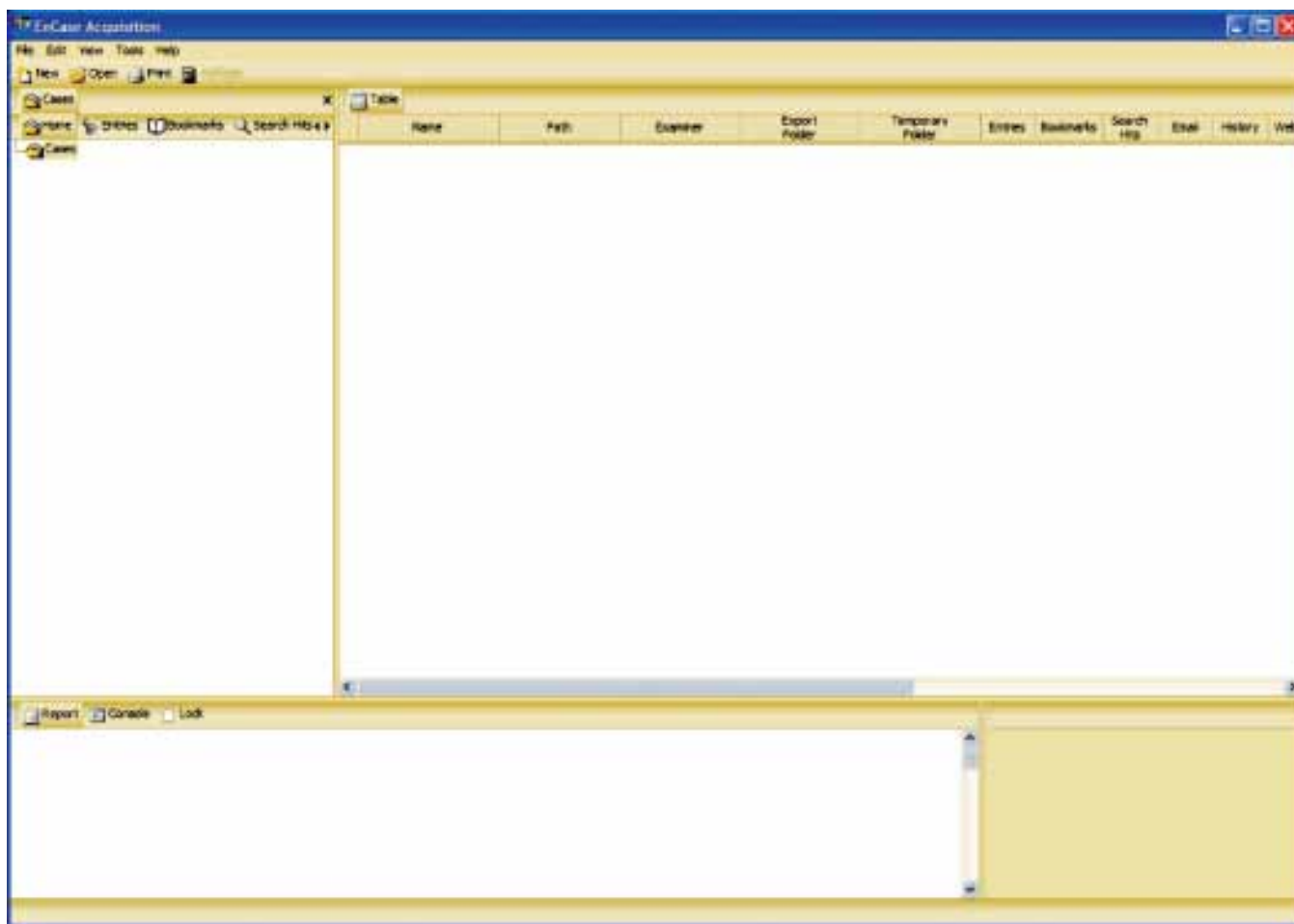
1. You must complete the chain of custody forms before taking possession of the hard drive that is to be imaged herein after called the target hard drive. Do not power on or boot the target hard drive under any circumstances



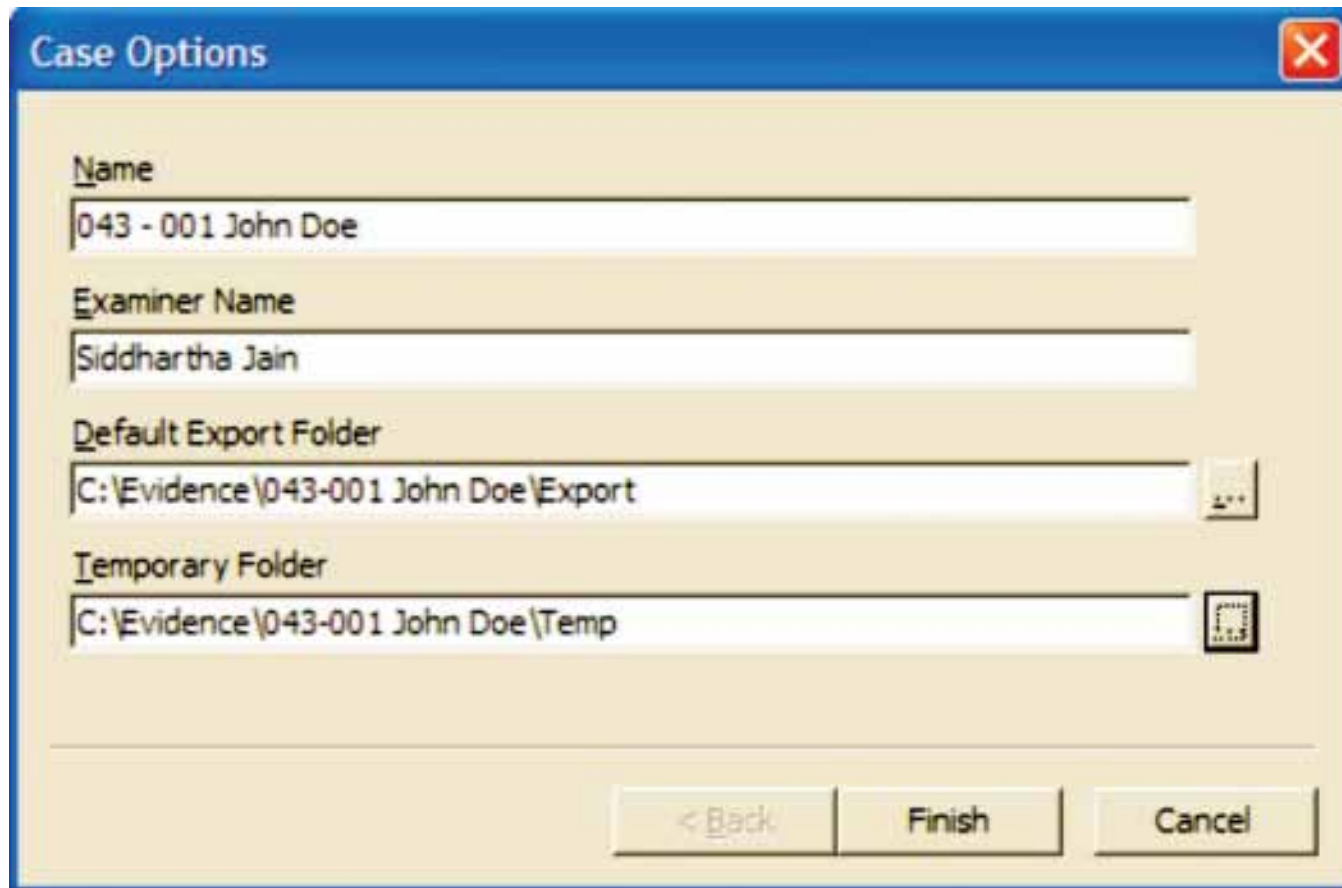


**5. Prepare the hardware:**

- A. Ensure that you have installed the Encase Forensic software and drivers on the machine that you will use for the imaging.
- B. Remove the target hard drive from the PC or laptop.
- C. Prepare the Fastbloc device by connecting it to the target hard drive. Ensure that you use cables that match the target hard drive type.
- D. Connect the Fastbloc device to the system containing Encase Forensic software using the USB connector.
- E. Turn on the Fastbloc device. Confirm that Fastbloc device appears in Explorer with a new local drive letter assignment.

**6. Image Acquisition-** Start Encase, you will see the Encase Acquisition Screen as given in Figure 2.

7. Click File —> New and enter the case details (description below) in the “Case Options” form.



- A. In the Name field, enter the case Name using the format: Case Number-Evidence Number Target Hard Drive Owner’s Name.

*In the example above the case number is “043”, the evidence number is “001” for a single disk drive and the name of the target drive owner is “John Doe”.*

- B. Enter your name in the Examiner Name field.
- C. Create an output folder and name it using the same format as above: Case Number- Evidence Number Target Hard Drive Owner’s Name. Under that folder create three directories:
- Export
  - Temp
  - Data
- D. In the field “Default Export Folder,” enter the Export folder path.
- E. In the field “Temporary Folder” enter the Temp folder path. a Click Finish.

On the next screen, click Add Device.



You will see the screen in Figure 4. Select “Local Drives” and click next.

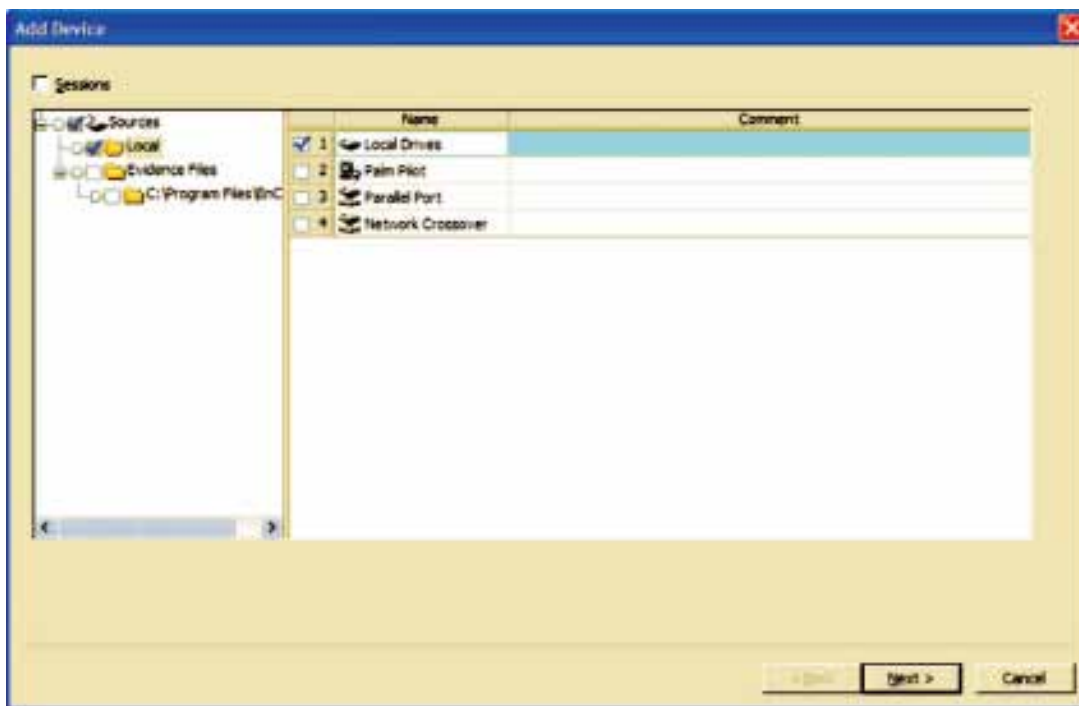


Figure 4: Add Device

Select the drive that has the label “FastBloc\_FE\_2\_Guidance” and click Next.

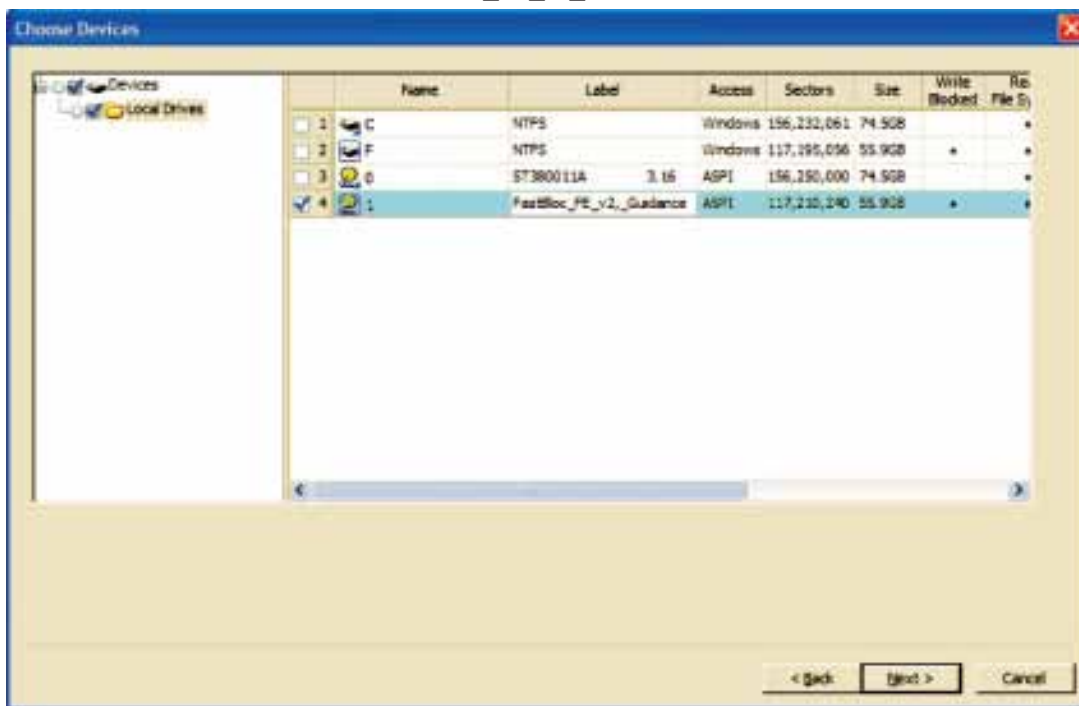


Figure 5: Choose Device

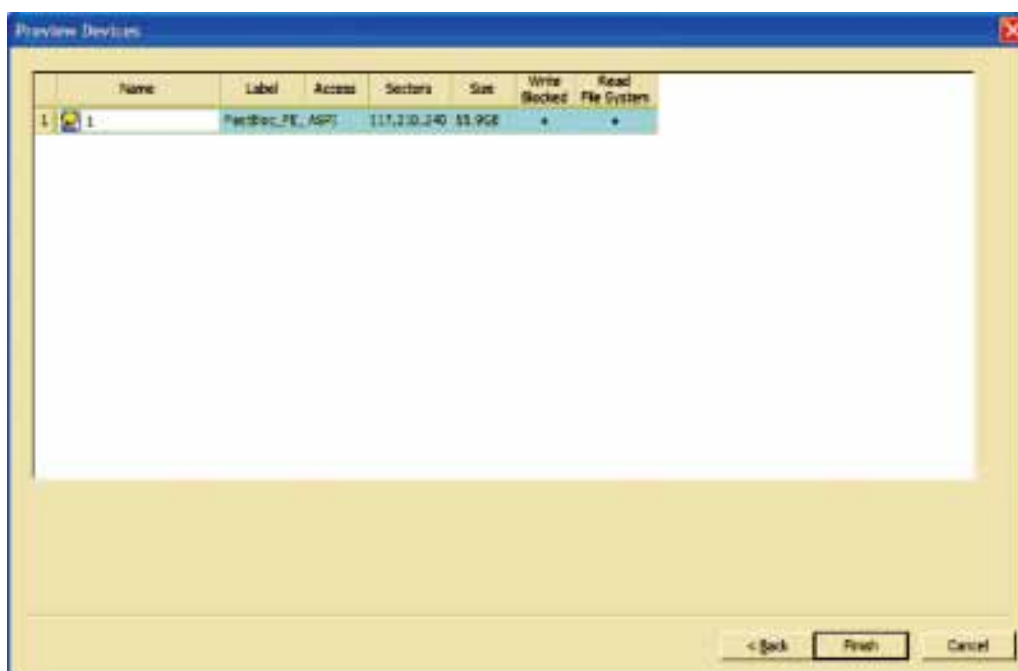


Figure 6: Preview Devices

Check the drive number under Entries then click Acquire.

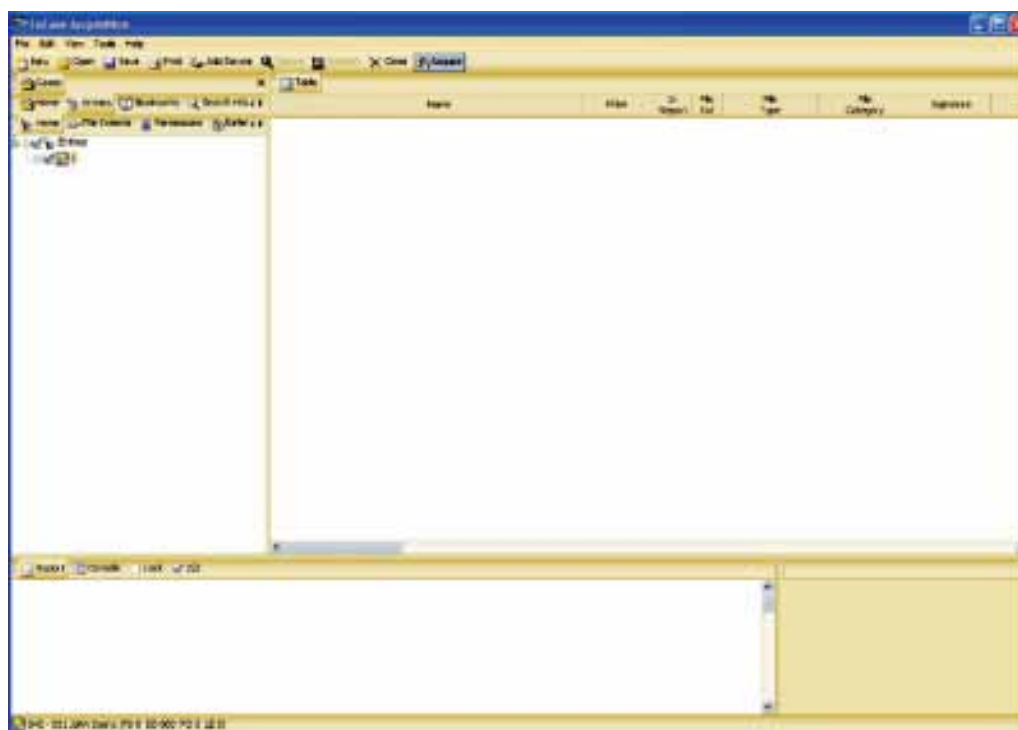


Figure 7: Acquire Drive

On the after acquisition screen, select Add to Case then Click Next

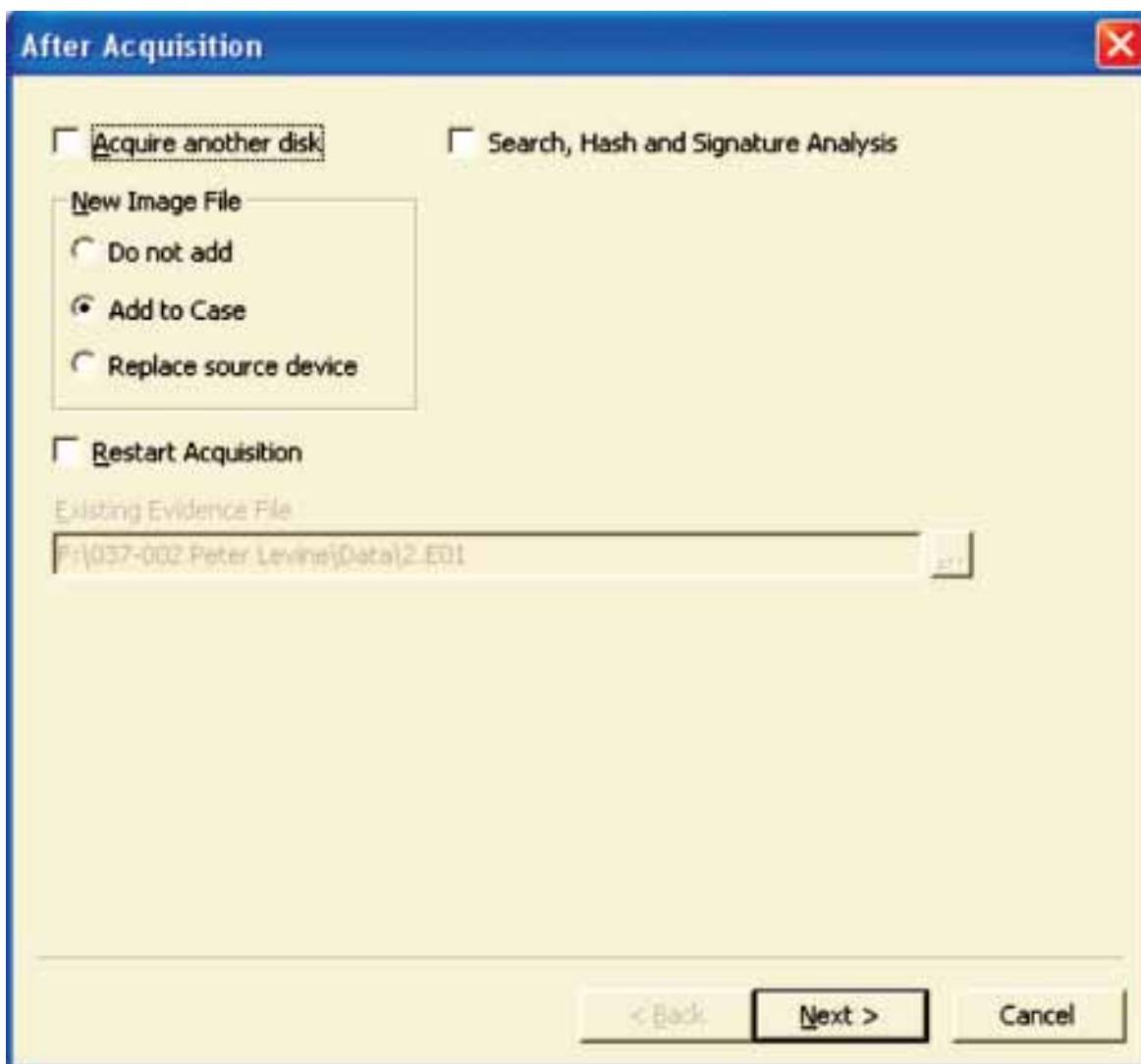


Figure 8: After Acquisition

On the Options screen:

- A. In the Name field use the format: Case Number-Evidence Number Target Hard Drive Owner's Name.
- B. In the Evidence Number field use the format: Case Number-Evidence Target Hard Drive Owner's Name.
- C. In the Notes field enter: Case Number-Evidence Number Target Hard Drive Owner's Name, Machine make and model, serial number, and target hard drive serial number.
- D. Set the File Segment Size to 2000MB.

- E. Under Compression, select Best (Slowest, Smallest). F. Accept the Start Sector and Stop Sector Default values.
- G. Leave the Password field blank.
- H. Accept the Block Size and Error Granularity defaults.
- I. Check Generate Image Hash to select it.
- J. In the Output Path, browse to the Data folder you created earlier to store the evidence image.

The 'Options' dialog box is shown with the following fields and values:

- Name:** 007-001 John Doe
- Evidence Number:** 007-001 John Doe
- Notes:** 007-001 John Doe, Dell Latitude 810 s/n E5AF2, HD Hitachi 239345SDF1122
- File Segment Size (MB):** 2000
- Start Sector:** 0
- Stop Sector:** 117210239
- Password:** (blank)
- Confirm Password:** (blank)
- Block size (Sectors):** 64
- Error granularity (Sectors):** 64
- Compression:**
  - ☐ None
  - ☐ Good (Slower, Smaller)
  - ☒ Best (Slowest, Smallest)
- ☒ Generate image hash
- ☐ Quick reacquisition
- ☐ Read ahead
- Output Path:** E:\007-001 John Doe\Data\007-001 John Doe.E01

Buttons at the bottom: < Back, Finish, Cancel

Figure 9: Options

### Click Finish and start the image Acquisition.

1. When the image acquisition is completed, you should be presented with an Open Case screen as shown in Figure 10.

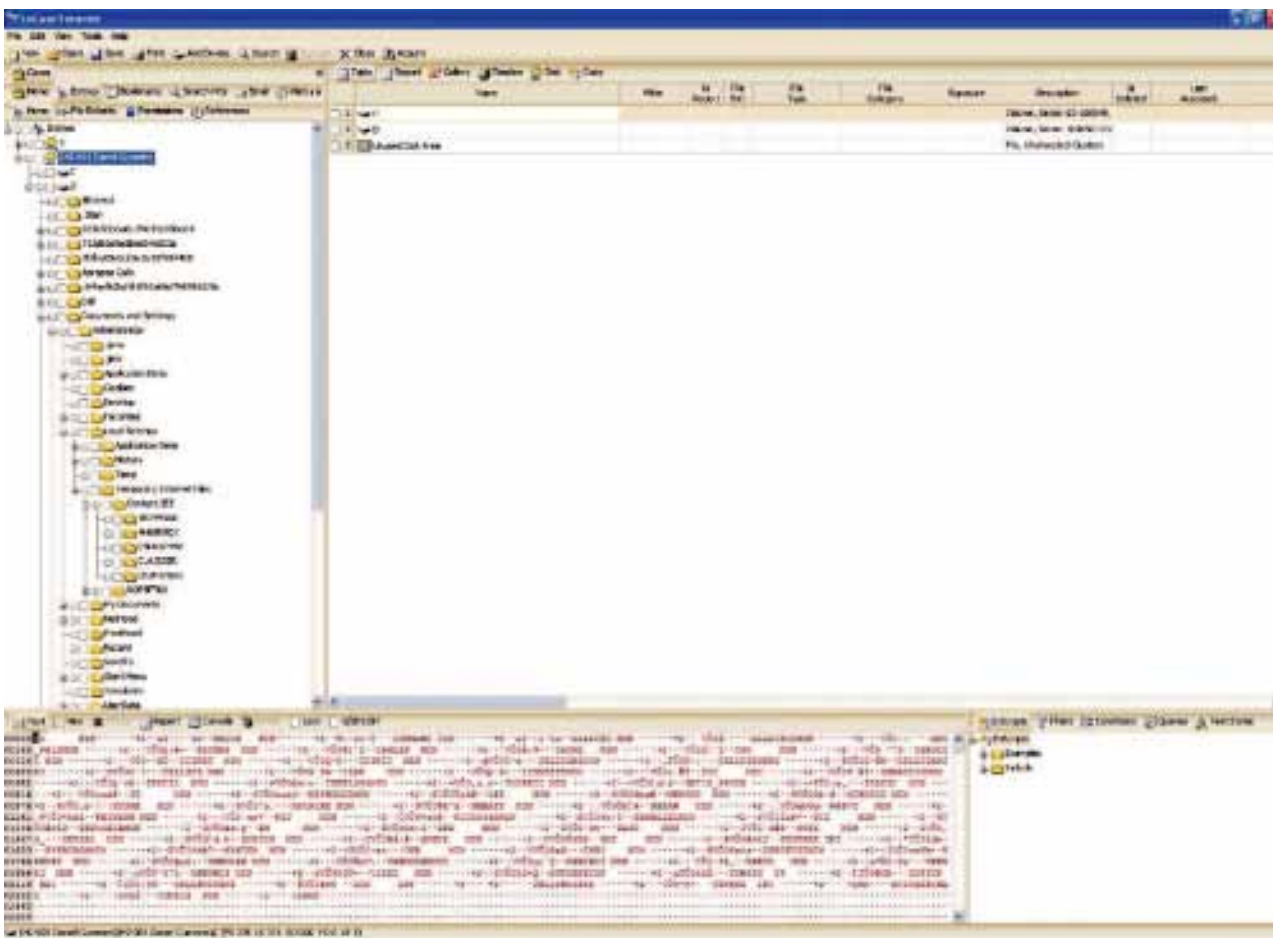


Figure 10: Open Case Screen

- Select the Report Tab above the right pane.
- After you select the Report Tab, a pink progress bar at the top will indicate that verification is in progress.
- When verification is completed, print a copy of the report. Attach the printout to the “Chain of Custody” document.
- Finally, select Save As from the File menu and save, again using the format: “Case Number-Evidence Number First Last” (for example 007-001 John Doe.cas) in the Data folder (default location). Symantec Information Security will retain these case files.

## Annexure-3

### On-the-Spot Recovery of deleted data- Examples

**Live deleted data recovery on Windows** can be done using Recuva. The steps involved are explained below.

1. Click on the executable and you get a screen



## 2. Click on the type of files

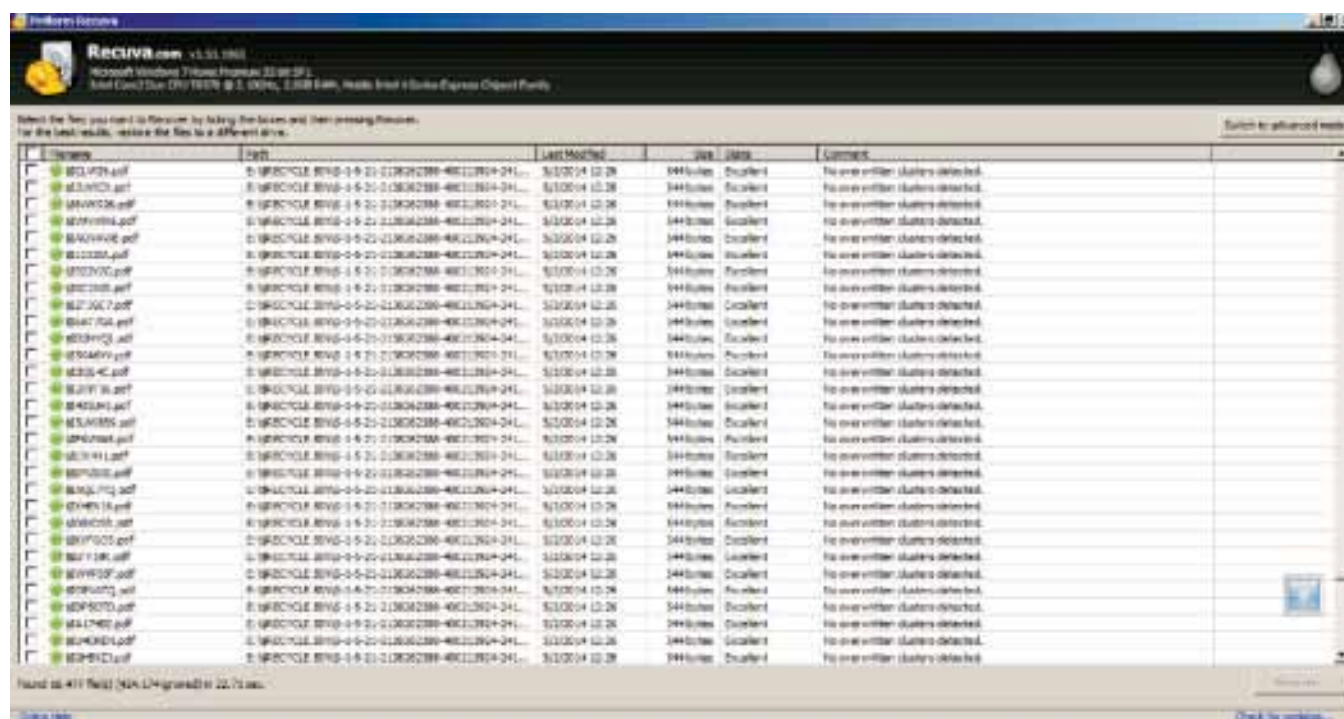


## 3. Enable Deep Scan





4. After the process is completed you get a view like this containing all the deleted files which can be examined on the spot



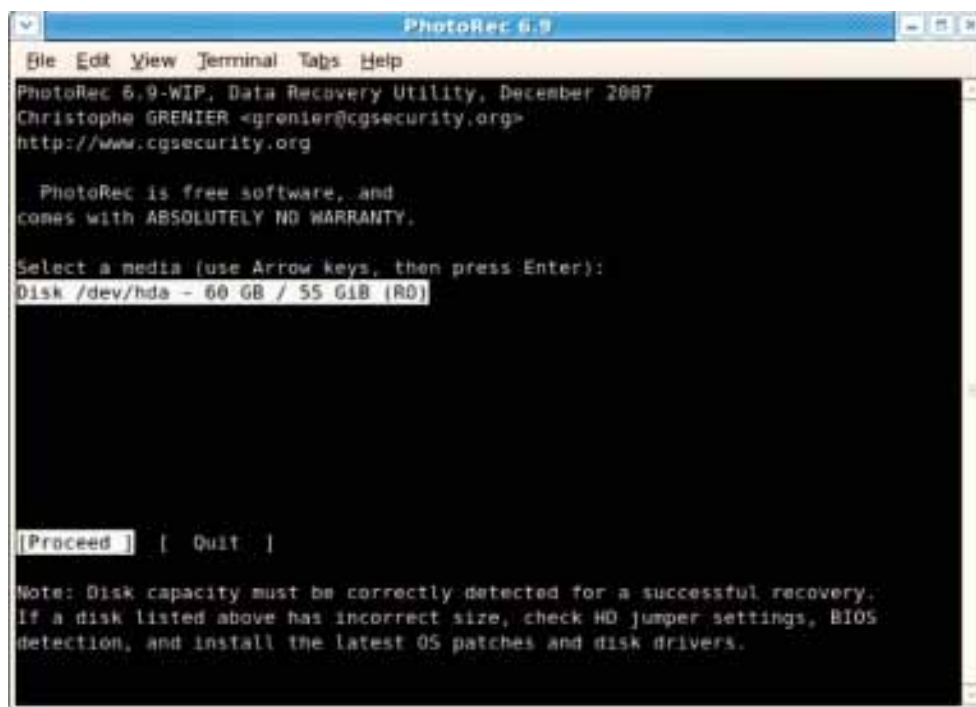
5. After that just Click on “Recover” Button. And Provide Destination Drive where you want to recovered data.

**Live deleted data recovery on Linux** can be done using Photorec tools. The steps involved are explained below.

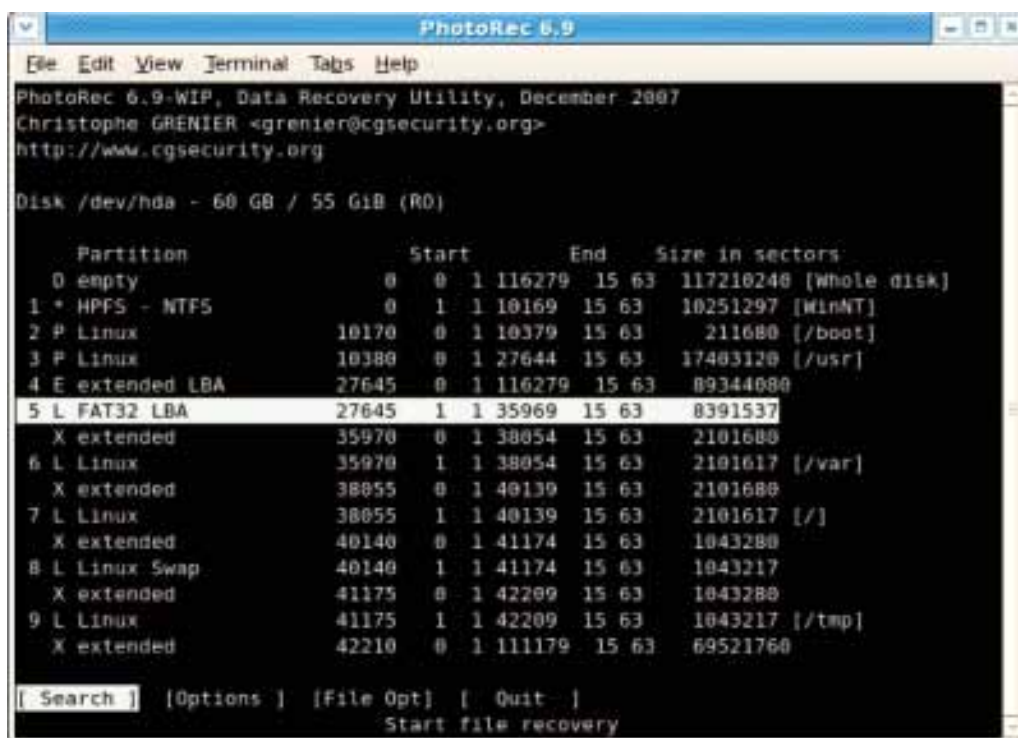
1. Connect Prepared USB drive to target machine.



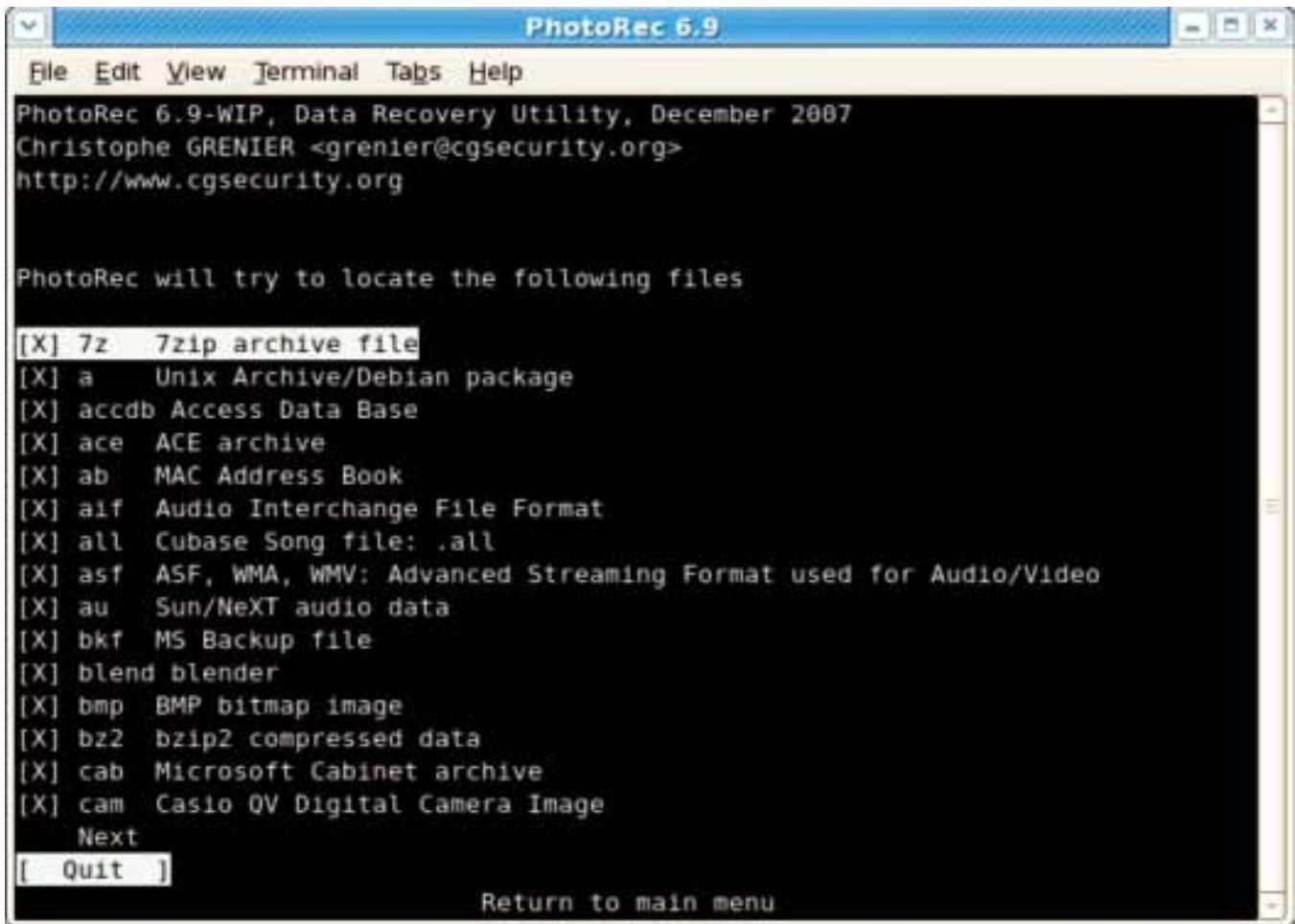
## 2. Run the Program



Select the target media we want to recover [here we have 60GB drive] using navigation keys. Make sure Proceed is highlighted and press Enter. You will see window as shown below.

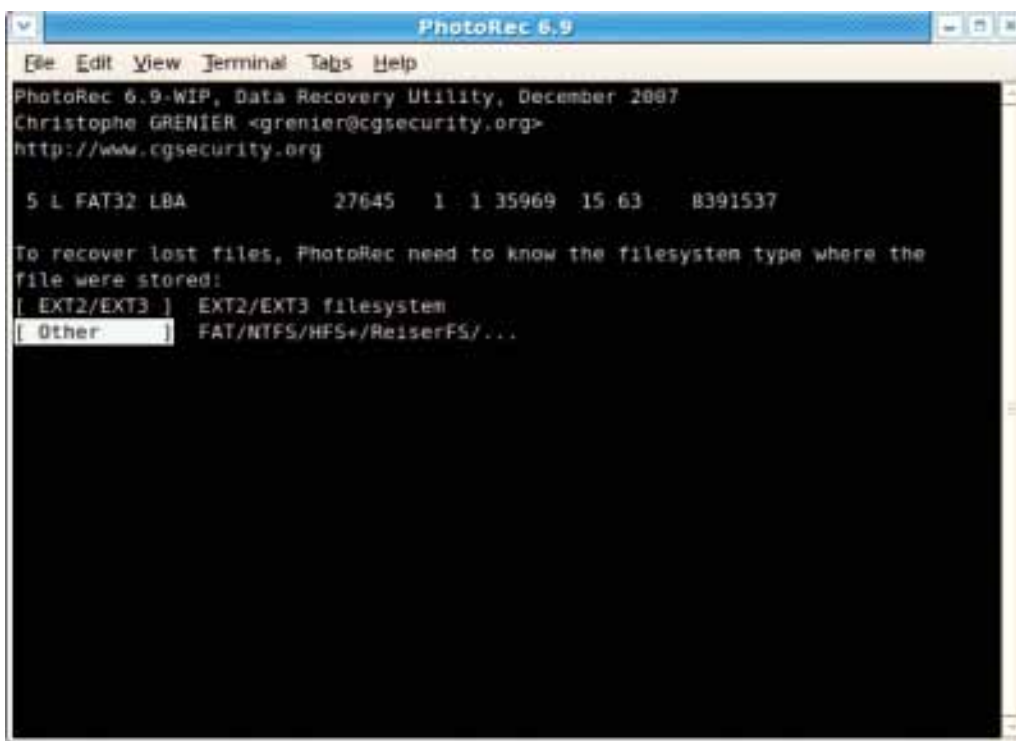


3. Select the partition you want recover [you can recover whole drive also]. Let us assume that we recovering data from whole disk then using navigation key select first option as whole disk. Now we need to specify the file type for which search gets executed, using navigation key highlight [File Opt] then press Enter.

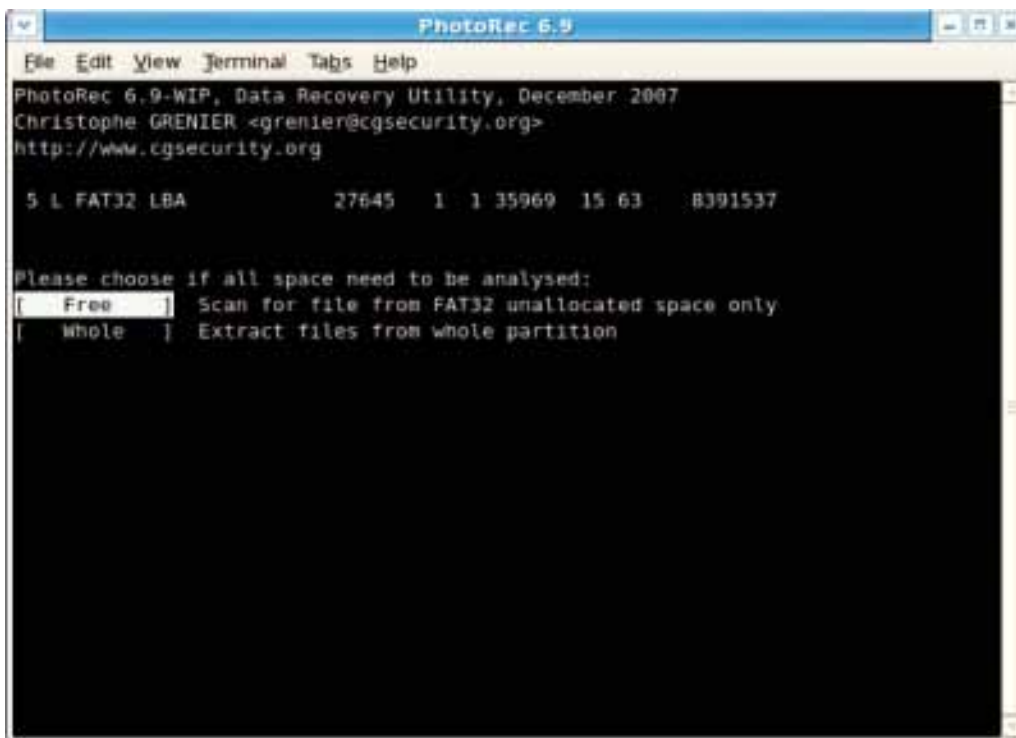


There are various file type shown with [X] in front of them. We need to deselect all the file type and select required only. [Use space\_bar to select file type] . You can deselect all the file type by pressing "S" from keyboard. After selecting the file types Press "C" to confirm.

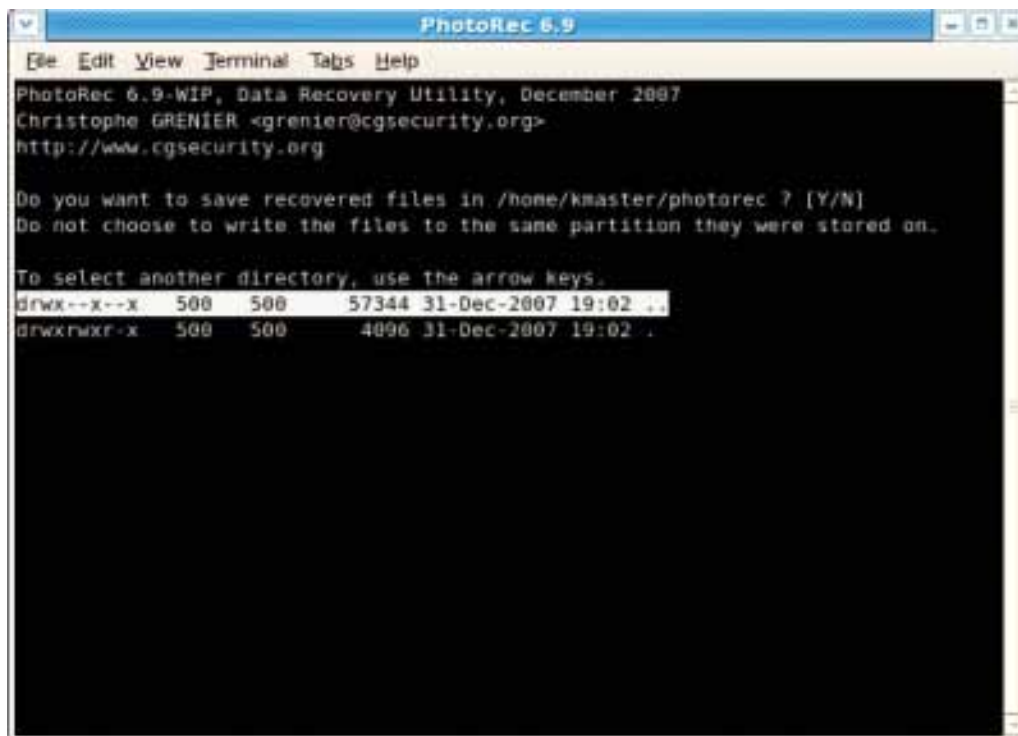
4. Now highlight to [Search] and press Enter. It will ask for destination for recovered data. Select [Other] option for destination.



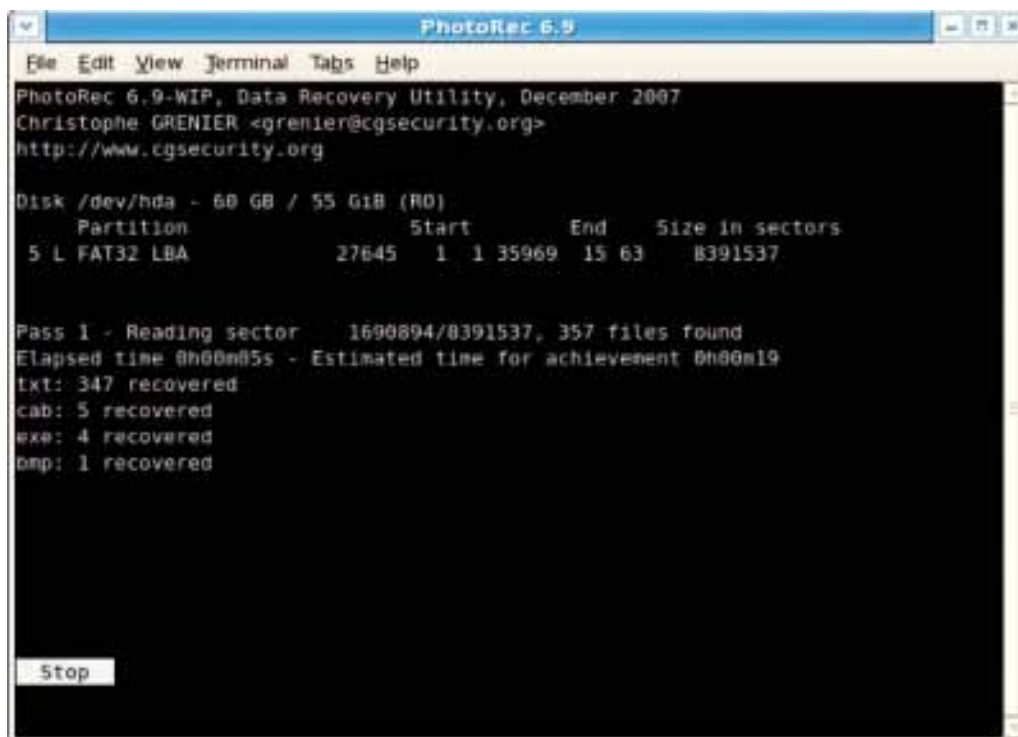
5. Select [Free] option to recover data from unallocated space only.



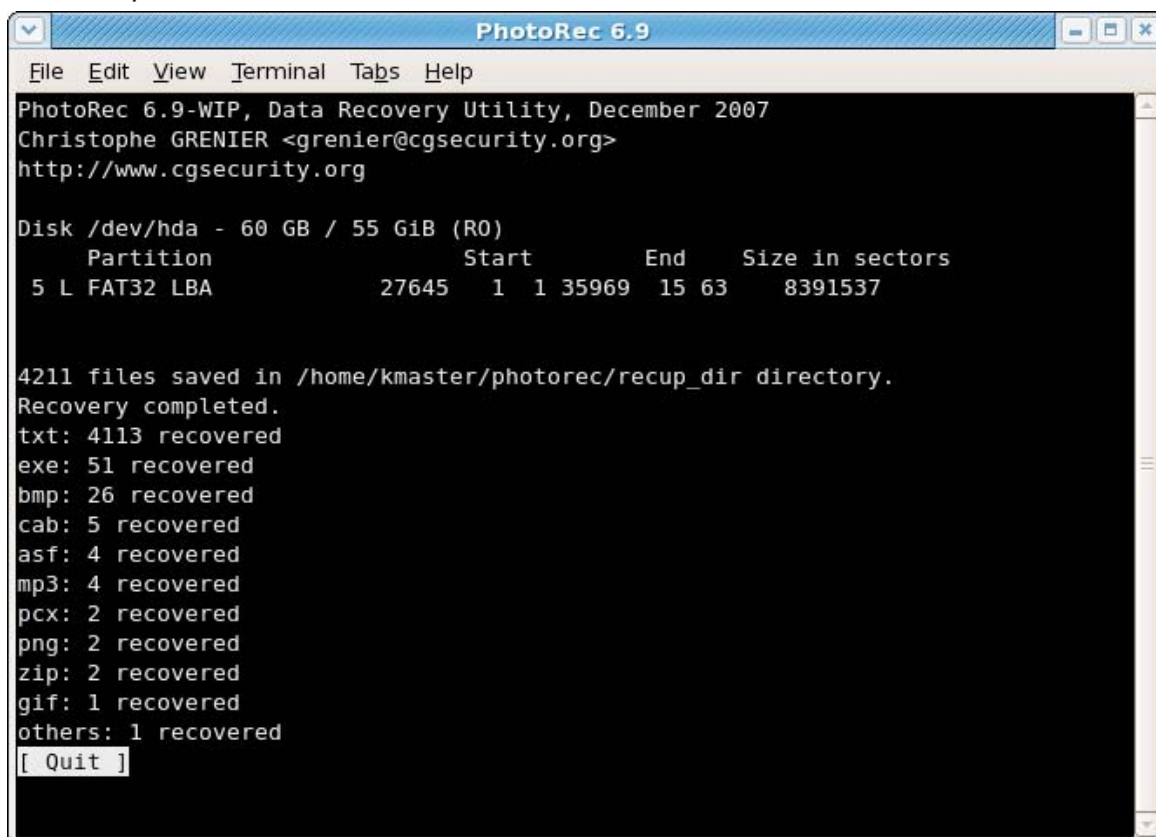
6. Choose the directory where the recovered files should be written.



Here “..” denotes back link. Go through the directory and provide destination folder. After you go to your desired destination folder press Y. Wait to process gets completed.



After Finish you see a window like this.



After process gets finished remove USB drive safely.

**Live deleted data recovery on Macintosh** can be done using Data Recovery Guru Software. The steps involved are explained below :

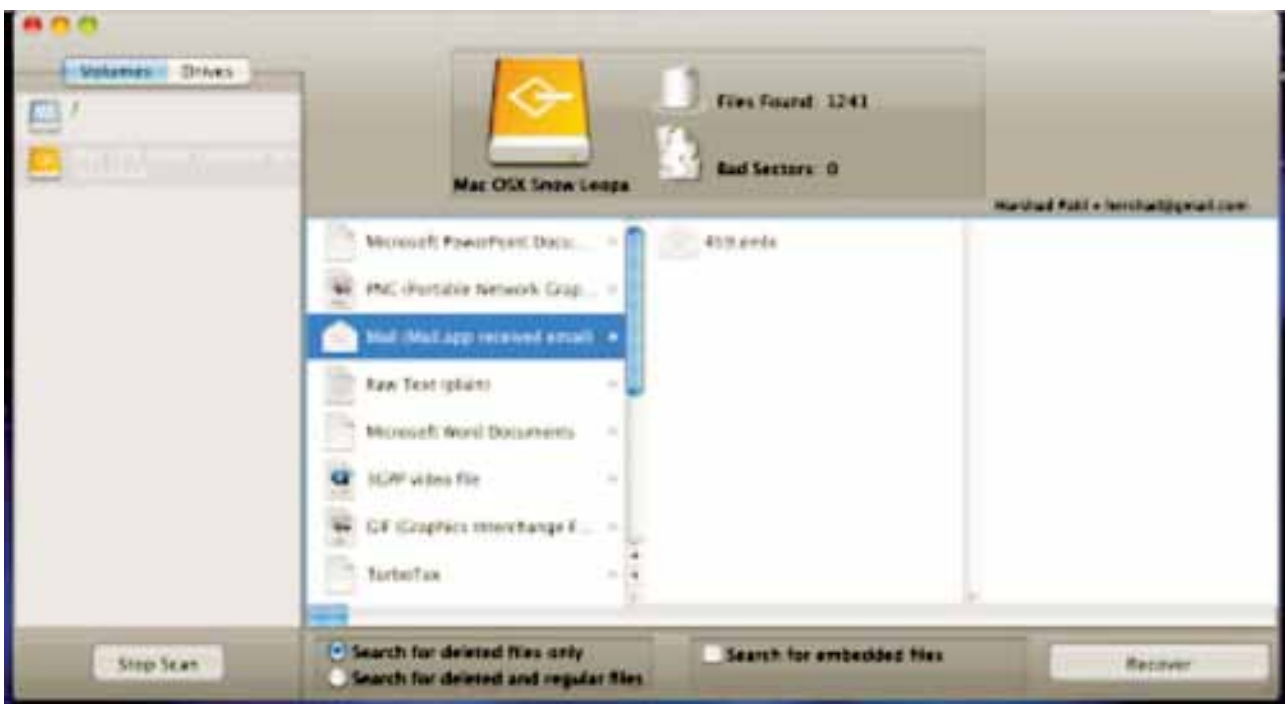
1. Make Sure we have DATA Recovery Guru Software and the KEY copied in USB drive. Double Click on DataRecoveryGuru.Zip file. After clicking on Zip File, we need to double click on Application. (Mac Data Recovery Guru).



2. After that Select Drive from Left Partition and use Search for Deleted files only. Click on “Start Scan.”



3. Wait until process gets completed.

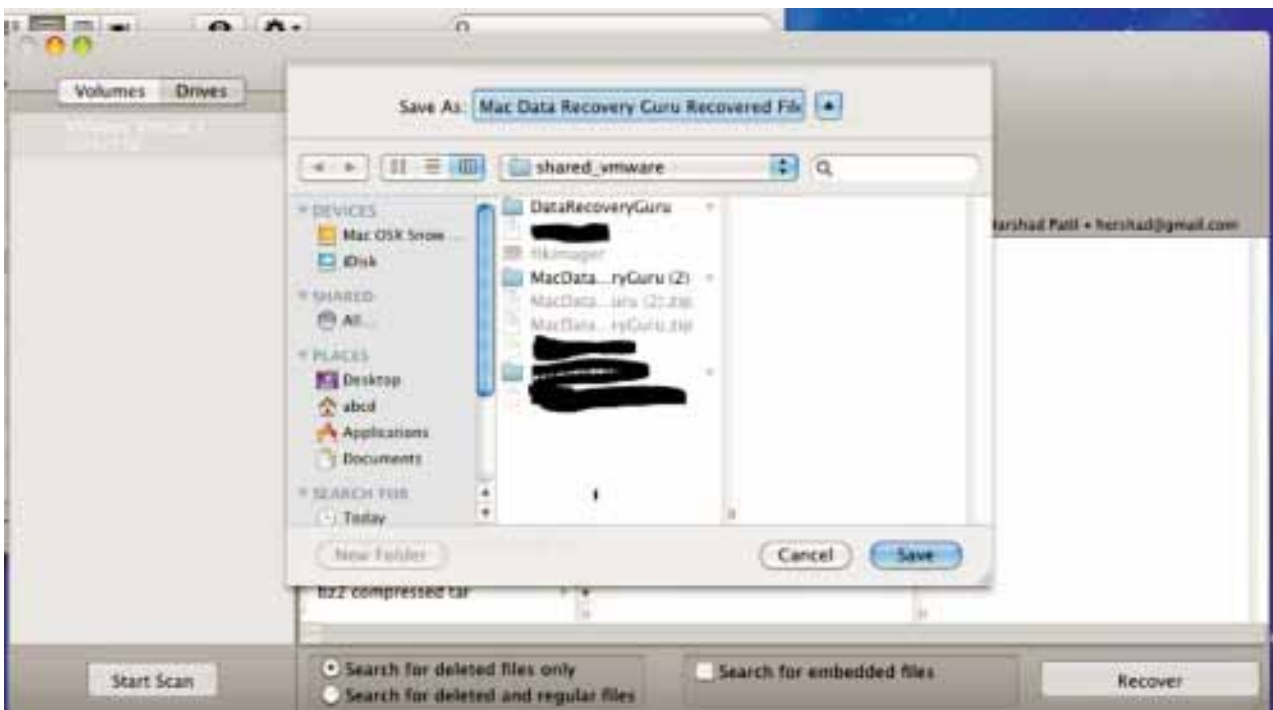




4. After Completion of the process Click on File Types that need to be Recover. Example here we have selected Email. In second window click on cmd + A selecting all documents related to that file type.



5. Click on Recover button and specify Destination Drive.



## Annexure- 4

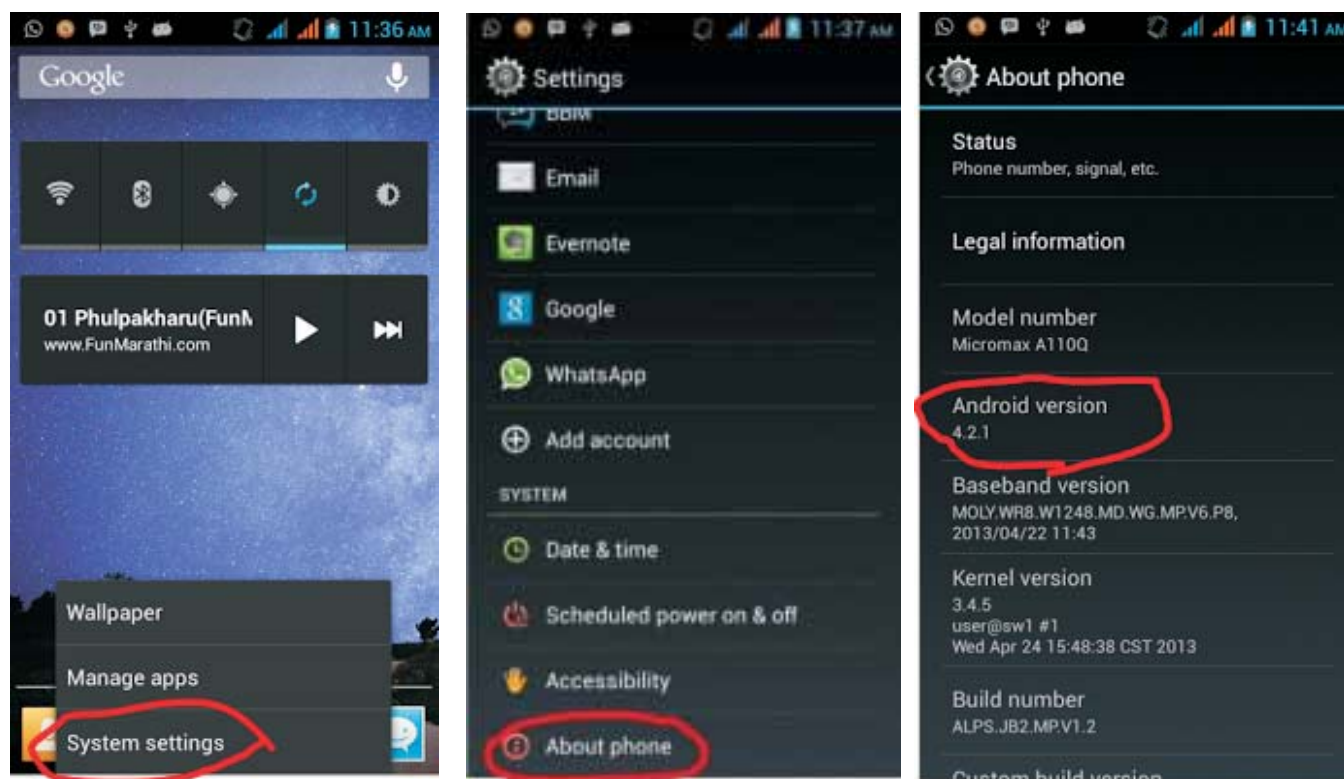
### Some Examples of Mobile Devices Backup

Most common type of mobiles encountered in the field nowadays are small phones with iPhone and Android being most common followed by Blackberry. Before starting the device acquisition make sure that you get all the security credentials like Pin Lock, swipe pattern, passwords to the phone. Please visit sub-topics to find out device specific backup procedure.

#### Android devices

This procedure is only possible if android device version is greater than 4.0, you will not get **SMS database, Google apps databases** through this.

To check the version go to **(Settings —> about phone —> android version)**





Connect the USB cable with PC. Use USB debugging mode goto (**Settings —> Accessibility —> Check in USB debugging**)



In most of the cases USB debugging option is hidden. To check it Goto

**Settings—> About Devices —> Build Number (press 7 consecutive times). You will get Developer option in Settings menu. Goto Developer Mode option and check on USB debugging.**

Then use ADB folder given in pen drive. ADB (android debugging bridge) used for communicating with android device over USB.

Adb drivers are provided with Pen drive given with us.

Goto **android\_adb** folder and run “**backup\_android\_system\_data.bat**” file.

This file contains adb drivers and some scripts.

Check whether Android device is in **ADB USB debugging mode** or not.(**Status bar will show USB debugging mode when you connect USB to it**)

After running the script follow the following procedure you will see this screen.

```

Ultimate Backup Tool v1.3.2
xda-developers.com

Notices:
I'M NOT RESPONSIBLE IF YOU DAMAGE YOUR DEVICE!
By unlocking the bootloader you will lose your warranty!
Make sure that USB Debugging is enabled!
The backup function will not back up SMS messages!
If you want to make a backup, set a desktop backup password under Developer
Options. It seems it would fail otherwise!
Make sure that you have correctly installed drivers!
The backup will be saved in C:\backup\backup.ab .

===== Device Info =====

List of devices attached
0123456789ABCDEF      device

List of fastboot devices : NO DEVICE CONNECTED

Manufacturer:      Micromax
Model:             Micromax A110Q
Android Version:   4.2.1

=====

What would you like to do?

===== Backup =====
#
# 1. Set path
# 2. Backup all without system apps
# 3. Backup all with system apps (unsafe)
# 4. Backup app and device data (not the APKs themselves)
# 5. Backup apps
# 6. Backup device shared storage / SD card contents
# 7. Backup a single app
# 8. Restore
#

=====

===== Tools =====
#
# 9. Install Drivers
# 10. Unlock Bootloader (Uses "fastboot oem unlock" command)
# 11. Install CWM/ CWM Touch (Galaxy Nexus, S2 and S3)
# 12. Root your phone (ARM) (requires custom recovery)
# 13. All in one (Galaxy Nexus, S2 and S3)
#

#
# 14. Refresh
# 15. Capture a problem
# 16. Change language
# 17. Quit

Choose a option:
  
```

NOTE : If you found NO DEVICE CONNECTED in front of Manufacturer then try to debug it using adb driver.

- \*.
- Goto adb folder given in S folder.
- \*open command prompt with current directory as S folder.
- \*run the following command.
- \* >adb devices
- \*It will show you device in front of some random id.
- \*If you find Offline in front of random id, Then use below procedure.

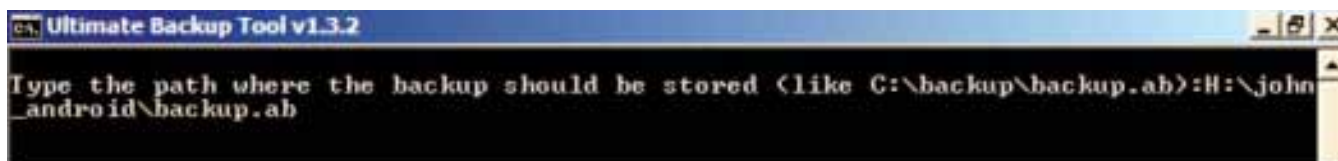
Delete the key from you PC. Goto your user directory and unhide all folders you will see a folder name with .Android, delete all the files inside the folder.

Now in Developer option of Android click on Revoke USB debugging authorization. Finally restart the device.

Test adb device check if passed follow the procedure. otherwise contact your senior person.

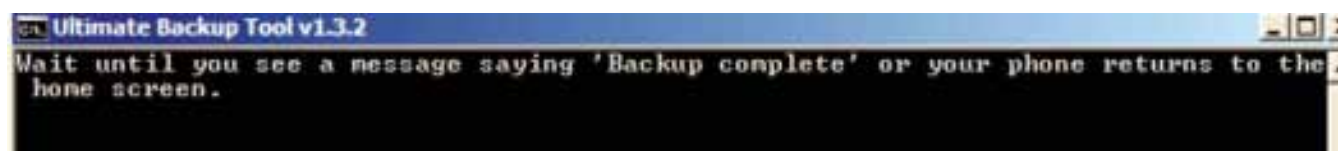
The default path for **backup.ab** file is **C:\backup**. We can set different path using **Set Path option**

**Press 1** to change the default path. You will see this type of option, type Pen Drive / Hard Drive address (like H:\john\_android\_device\backup.ab

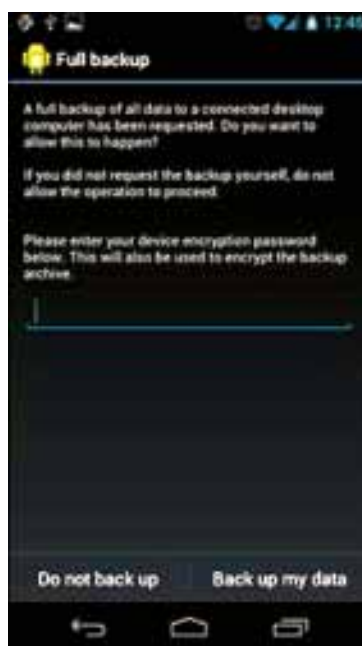


Press enter again. You will see default screen.

Press 4 i.e. **(backup app and device data (not the apk themselves ))**. This screen will come to you.



Unlock your mobile and you will see



**Do not press** any keyword in **passcode section** .Click on **Backup up my data** button.

Wait while process finishes. Immediately you will see finish box on computer screen.

We have complete android system app backup with it. Now open folder which we have set as Destination folder i.e. **C:/backup**

The **backup.ab** file is **encrypted we have to decrypt the file** in order to get the database files from it.

You will see a file name **abe.jar** in **android\_adb** folder.

Create a **hash report** for backup.ab file.

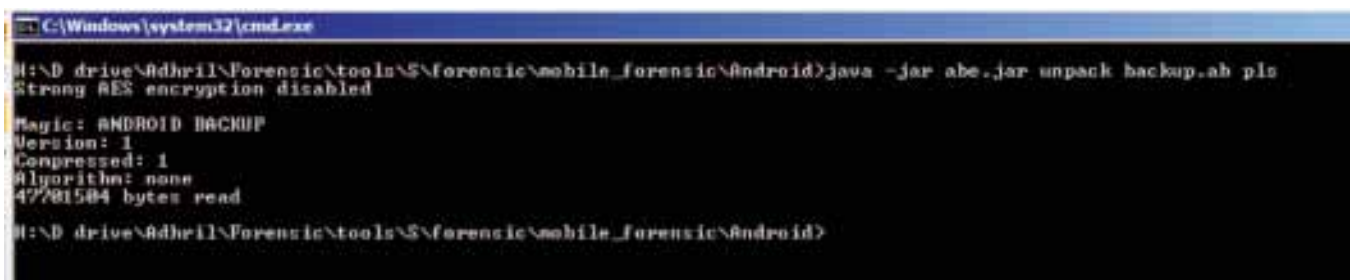
Copy **“backup.ab”** file and paste into the android\_adb folder. (Here we have backup file in H:\john\_android\backup.ab)

Type the following command (**Note: make sure that abe.jar file and backup.ab file are in the same directory**)

Open **command prompt** and **cd** to file **where abe.jar** placed.

**Java -jar abe.jar unpack backup.ab data\_backup**

**Run** the above command.



```
C:\Windows\system32\cmd.exe
H:\B drive\Adheer\Forensic\tools\S\Forensic\mobile_forensic\Android>java -jar abe.jar unpack backup.ab pls
Strong AES encryption disabled
Magic: ANDROID BACKUP
Version: 1
Compressed: 1
Algorithm: none
47781584 bytes read
H:\B drive\Adheer\Forensic\tools\S\Forensic\mobile_forensic\Android>
```

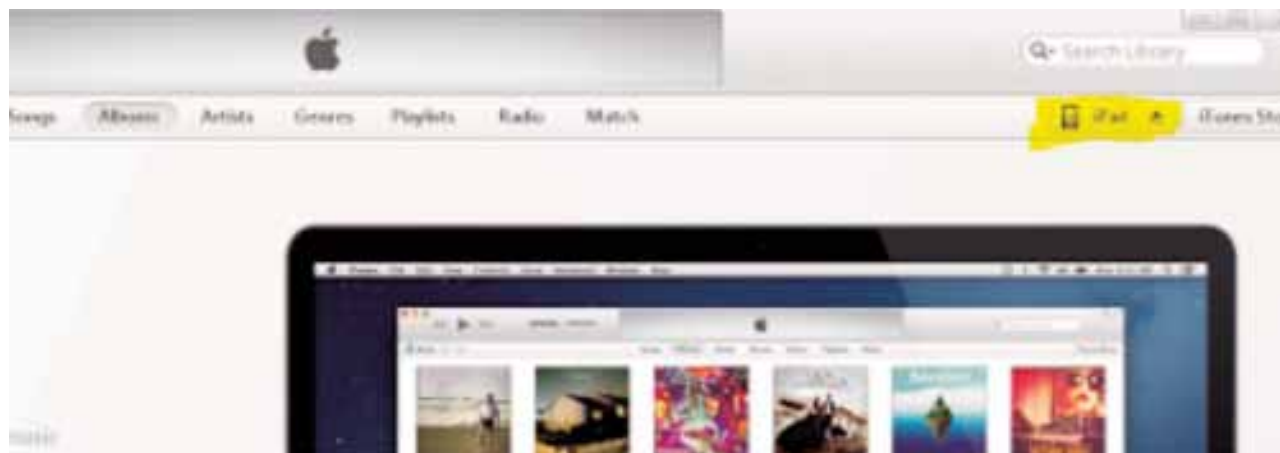
Open the **data\_backup** file using tool (like WinRar, WinZip, 7Zip). If you get any error in the opening that file. Please follow above steps again(**Uncompress the zip file to confirm backup is successful**).

## Apple devices Backup

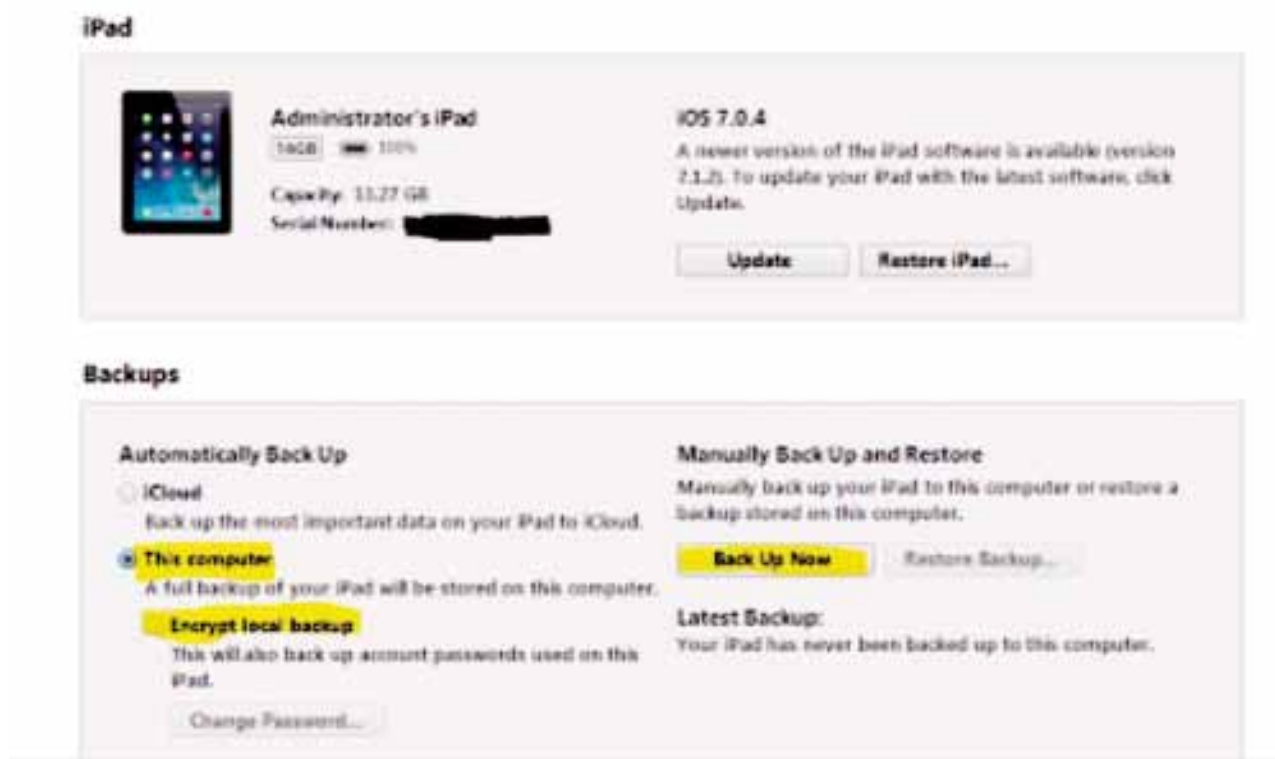
Connect your iDevice to computer using USB cable.

Make sure that you have latest itunes installed.

Open itunes



You will see device name on uppermost right corner of the itunes window. Click on that link.(Here it is ipad)



Make sure you have select This Computer as backup destination and uncheck ENCRYPT local backup.

Click on **Back Up Now**.

It will ask you to Back Up Apps or Don't Back Up Apps.



Click on Back Up Apps

It will start backup.

You may get some prompt box saying do you want to backup purchased app. Click on No.

(Apple doesn't provide internal access for purchase apps.)

You may ask for Apple id please provide the credential.

backup will store in

C:\Users\~User\_Name\AppData\Roaming\Apple Computer\MobileSync\Backup

Create hash value of it and copy the folder to Destination drive.

## Blackberry devices Backup

To take data backup for smart phone with BlackBerry 7.1 OS and earlier then BlackBerry Desktop Manager is needed. Otherwise click on Blackberry Link and follow procedure.

### STEP 1



- Run the BlackBerry Desktop Manager.
- Connect your BlackBerry to your computer.
- Wait for it to recognize your BlackBerry and then click on “Backup and Restore”.



## STEP 2



- In this window you have three options, Backup, Restore and Advanced. For this section we will work with the Backup option.

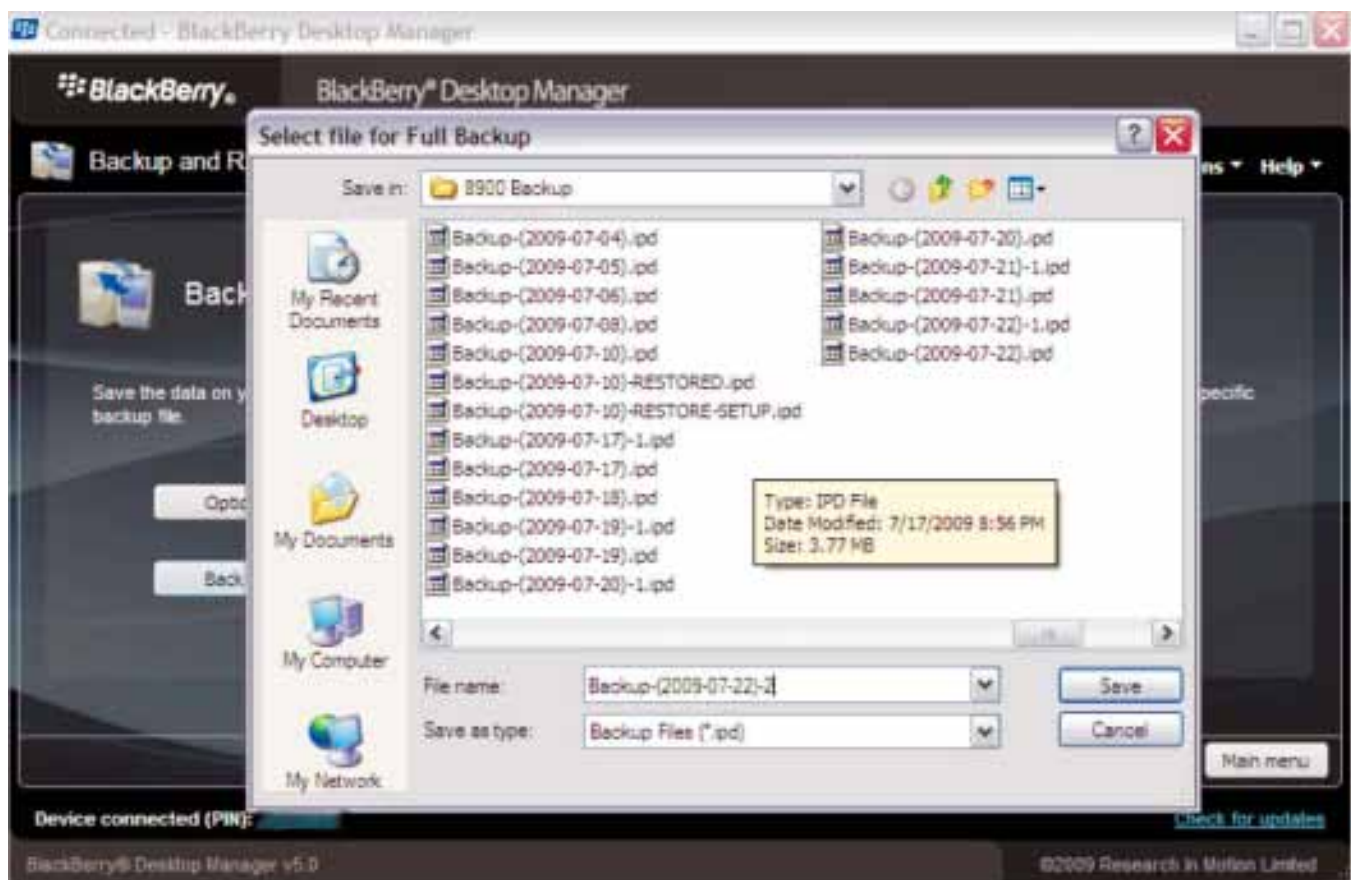


## STEP 3



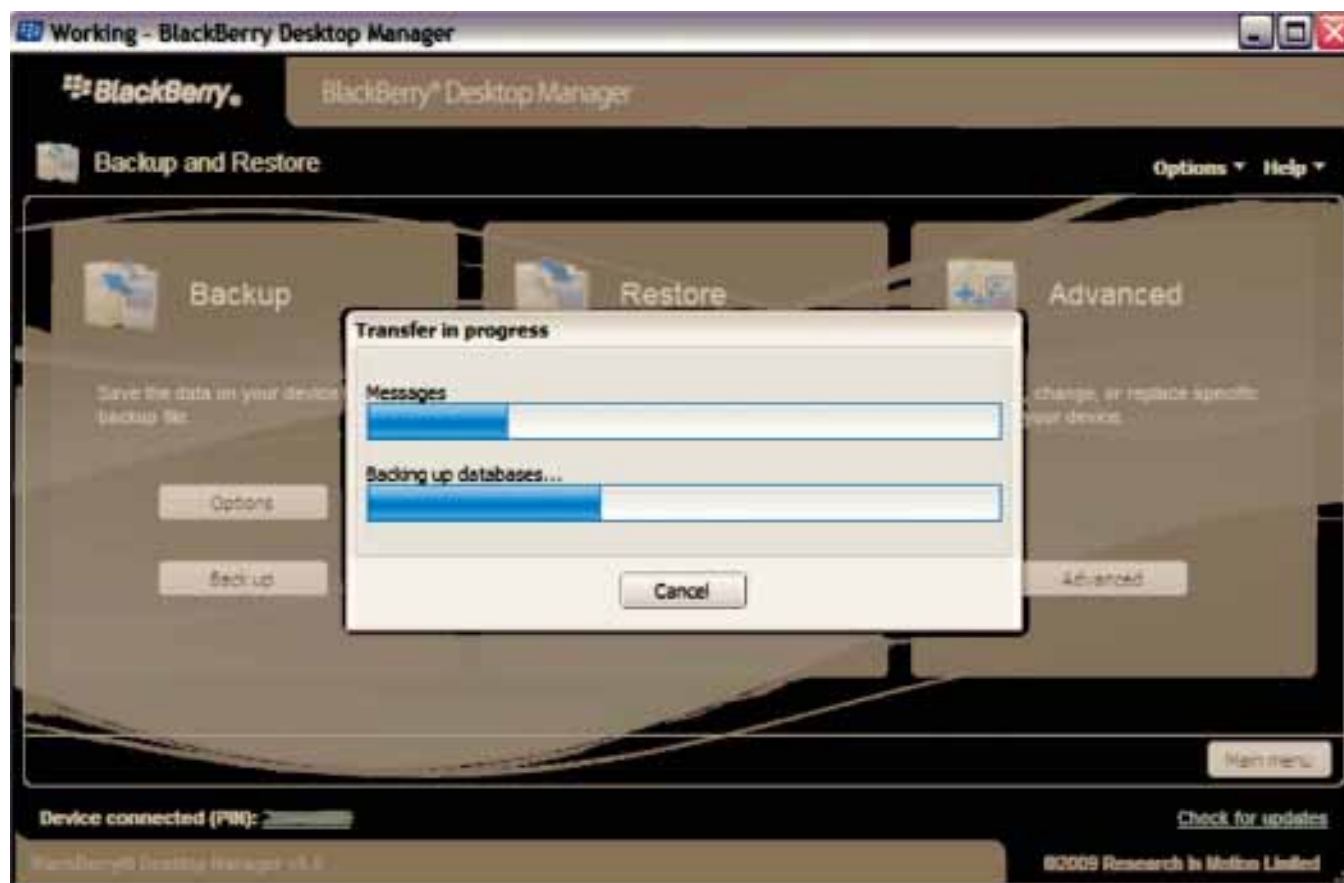
- Underneath the Backup option you will see “Options” and “Backup”.
- First click on Options and make sure everything is how you want it.
- I would recommend the settings seen in the above screenshot, but it’s up to you how you want to handle your backups.
- The “Encryption” option allows you to make your backups more secure.
- Once you are done selecting your options click OK and then click Backup.

#### STEP 4



- In this screen you will be able to specify a file name for your Backup. By default the file name is Backup-(date).
- Once you have selected your file name (or left it as default) click on Save.

## STEP 5



- Your backup will now be created.
- You can keep an eye on the transfer progress to make sure what you want to have backed up is actually being backed up.

**Use BlackBerry Link and get the backup.**

1. On your computer, open BlackBerry Link.



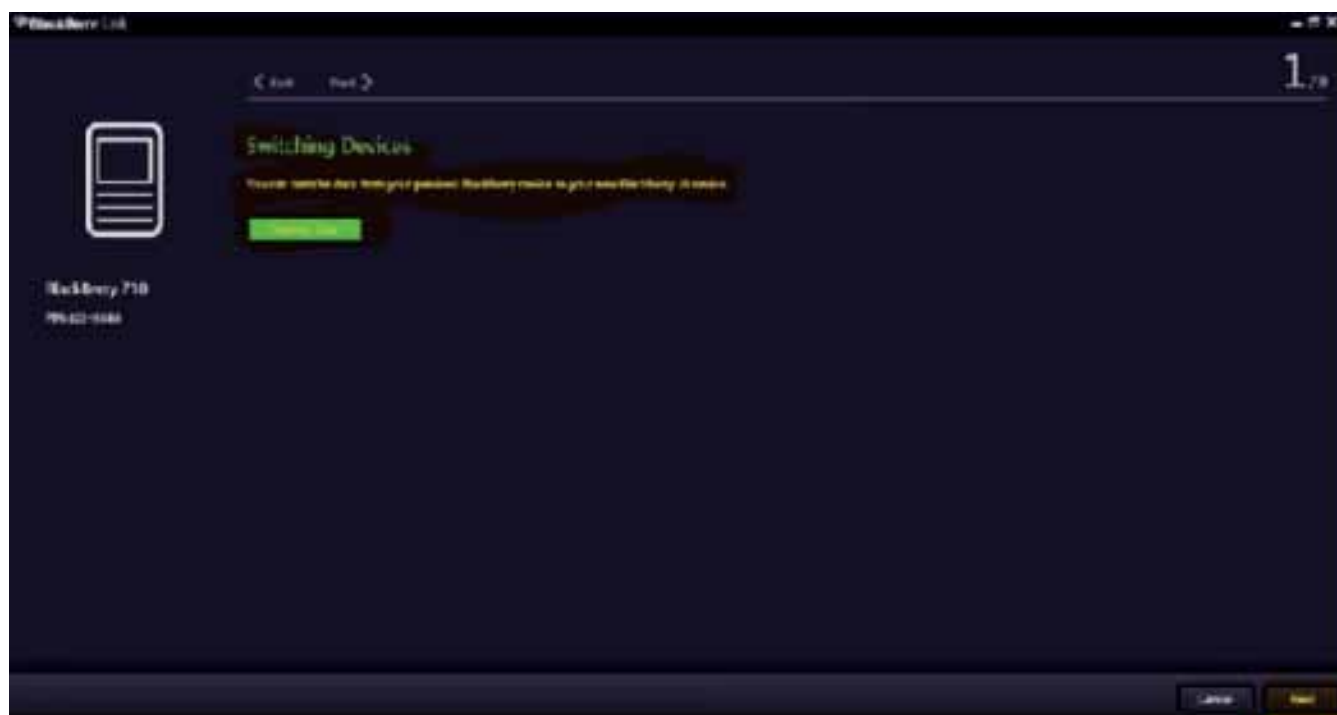
2. Connect your device to your computer using a USB cable, and click on next button



3. Select the Device in these windows, and click on continue button



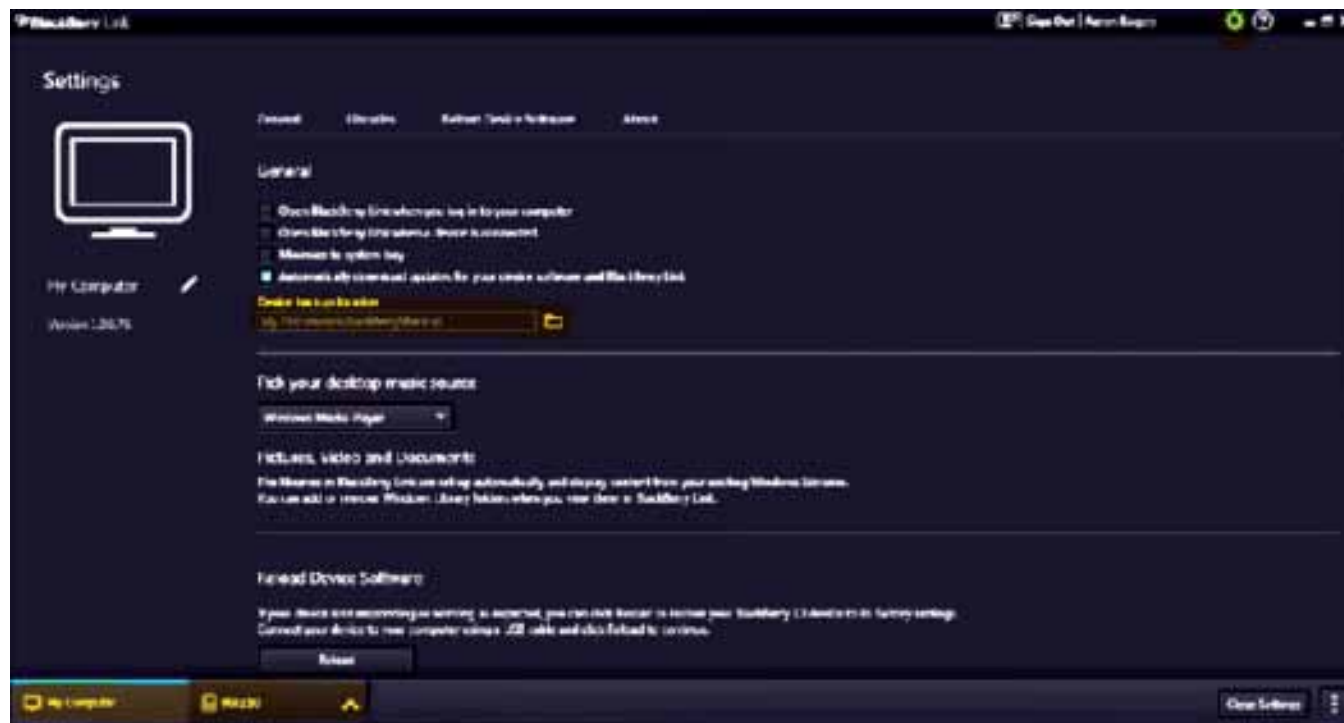
4. Data will be transfer to Blackberry link software then only click on next button.



5. At the bottom of the screen, click your device.



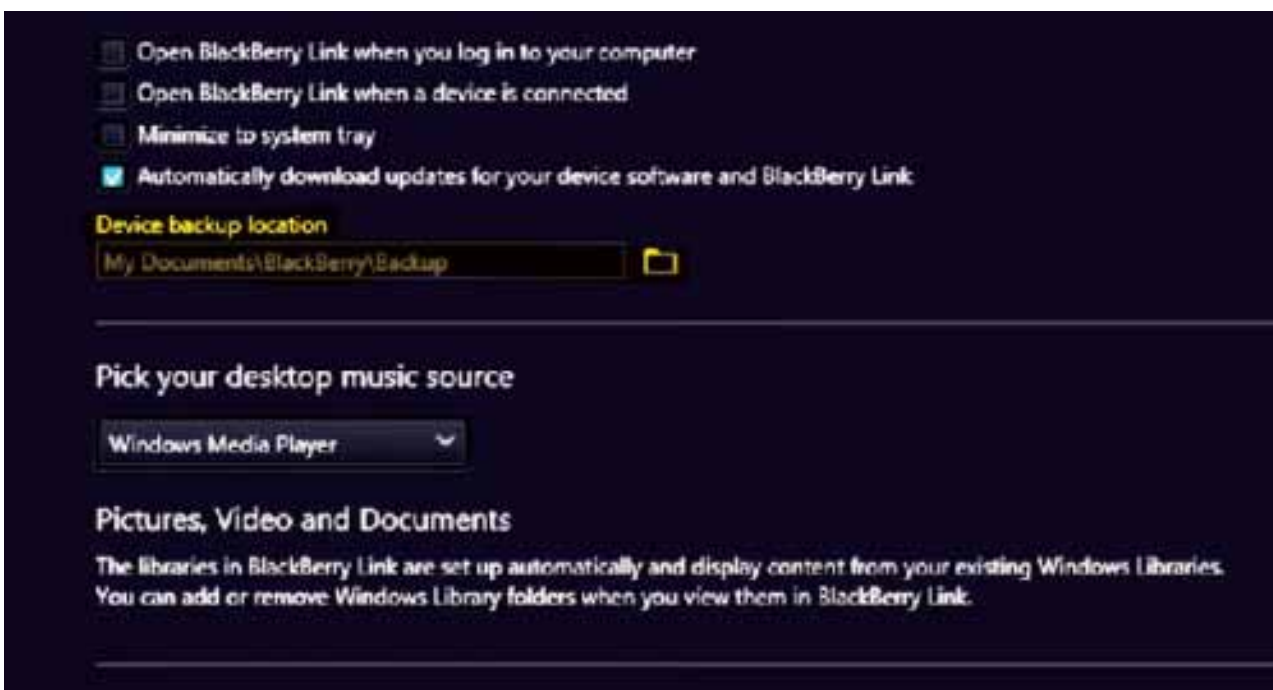
6. Click the icon right side of the screen.



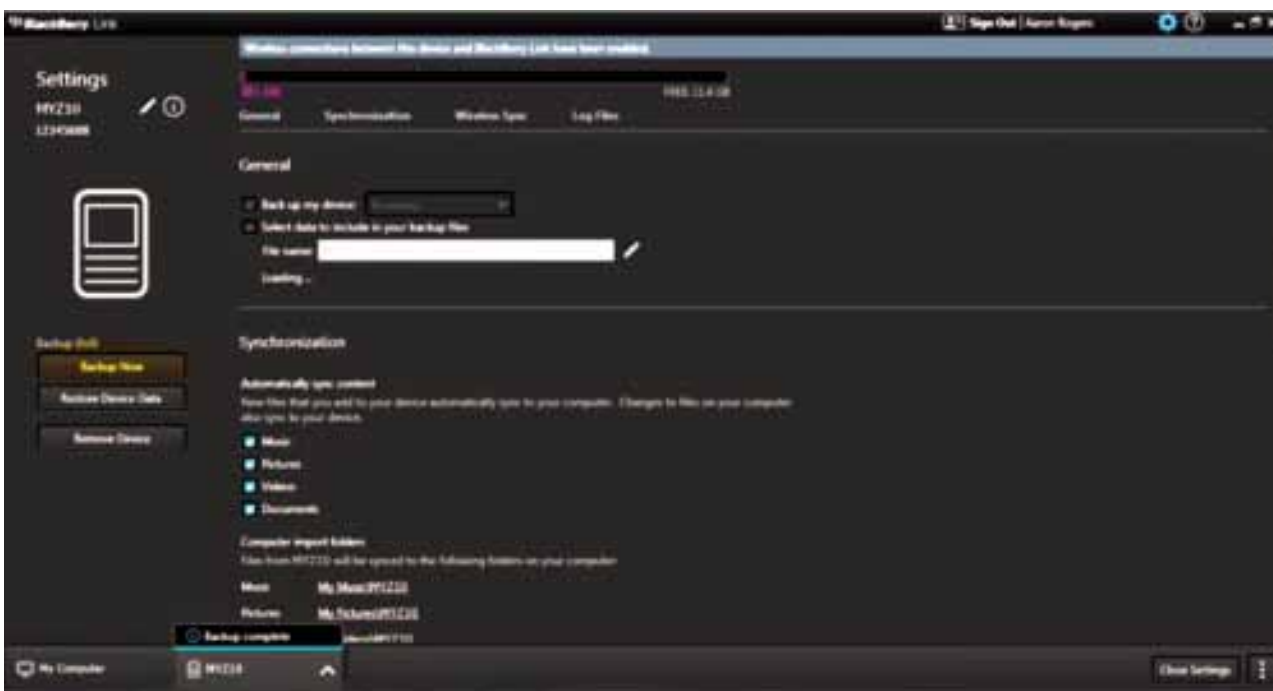
7. In the Settings view, click General.
8. To set up BlackBerry Link to automatically back up your device data, do the following:
  - o Select the Back up my device checkbox.
  - o In the drop-down list, select how often you want to back up your device data and settings.By default, BlackBerry Link backs up all of your device data.
9. To back up specific data, do the following:
  - o Select the Select data to include in your backup files checkbox.
  - o Select the checkboxes beside the data you want to include in your backup files.



- To change the backup file location, click the icon beside the folder name field and type a new backup folder name. Press Enter.

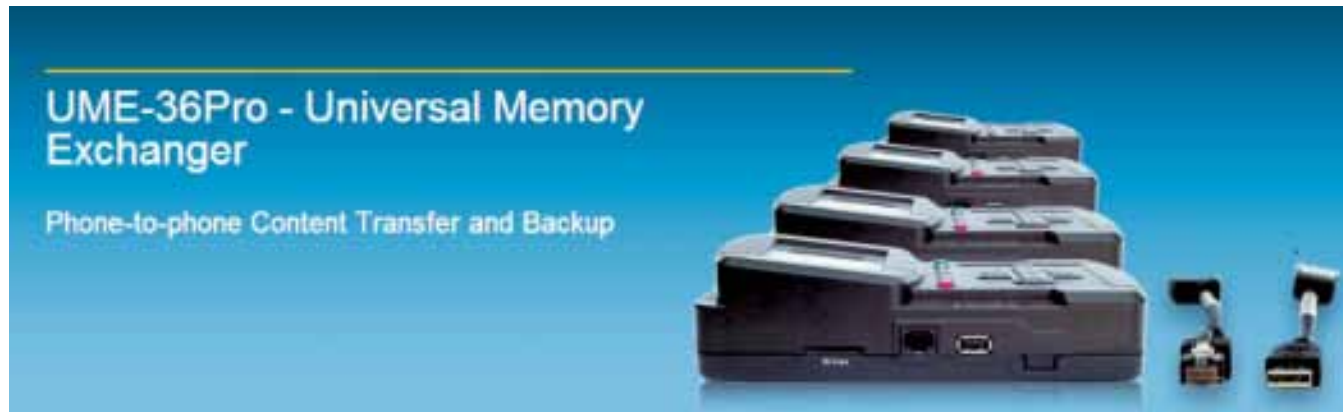


- In the Settings view, in the left pane, click Back Up Now.



## Other phones Backup

Cellebrite UME 36 pro provides wide range of mobile support for logical extraction.



First Plug the UME device to power and ON.

Select the Connector for Target device and connect to source Port.

Attach target Pen Drive at Destination Port.

From UME select Option as **Backup**.

Next Select Source Vendor.

Select Model number.

Select Source Media like SIM, Phone Memory, SD card etc

Select Backup Target as USB Disk Drive

Select Content Type as SMS

Continue...

After a while process will get finished.



### List of few hardwares/software that can be used

#### 1. Write Protect Device

- a. ICS Super DriveLock
- b. Tableau T35es-RW
- c. Fast Bloc Field Edition
- d. e-lock
- e. UltraDock v4

#### 2. Analysis & Recovery Software

- a. Guidance EnCase 6.0
- b. Access Data FTK
- c. CDAC Smart Cyber Suite\*
- d. PC Inspector File Recovery
- e. Paraben P2 Kit
- f. X-Ways Investigator

#### 3. Password Recovery Software

- a. Paraben
- b. Elcomsoft
- c. Data Doctor
- d. Portable Rainbow Table

#### 4. Hard Drive Imaging Device

- a. ICS Road Masster III
- b. ICS Solo III
- c. ICSSOLO IV
- d. Voom HARDCOPY 3
- e. Logi Cube Forensic Talon
- f. Forensic Duplicator Tableau Model TD1

**5. Wiping Device**

- a. Wipe MASter
- b. ICSSOLO-III
- c. ICSSOLO IV
- d. VOOM Drive Wiper

**6. Portable Labs**

- a. Logicube Sonix
- b. Road Master-iii
- c. Freddie (fred-L & ultimate kit)
- d. Lab-in-bag
- e. Carry a Lab

**7. Device Analysis Software/Hardware**

- a. Python
- b. Coffee
- c. Voom Shadow
- d. Live Response

**8. Mobile Analysis & Acquisition**

- a. Paraben Device Seizure
- b. Celle Brite UFED
- c. Access Data
- d. MOBILedit
- e. Simis
- f. XRY
- g. Logicube cell Desk

**9. Text Analyser**

- a. Paraben
- b. Microforensics

**10. Forensic Server (Specs given below)**

---

**11. Forensic Work Stations (Specs given below)****12. Network Access Storage (NAS) available in DGS&D rate contract.****A. FORENSIC SERVER specification**

- ATX Case with four 5.25" external bays; two 3.5" external drive bays; five 3.5" internal drive bays, Antec TruePower Trio (550 Watt), Intel® 955X Express Chipset, Intel® Pentium D 940 3.2GHz, 2X2 L2 Cache, LGA 775, 4GB DDR2 PC2-5300 DDR2-667, Gigabit LAN Controller 10/100/1000Mbps, One open PCI-X slot; Three Open PCI slots, 256MB DDR Video Card (Dual Head),
- **External Drive Bay Configuration**
  - o **Bay 1: Tableau Forensic SATA/SCSI/IDE/USB Combo Bridge with a DC Out Molex port,**
  - o **Bay 2: One CRU DataPort V Plus SATA Removable Storage Module (READ/WRITE)( Hot-Swappable) Also includes a CRU DataPort V IDE to SATA tray.**
  - o **Bay 3: 22X DVD-RW Drive (with software)**
  - o **Bay 4: 16X DVD-ROM /40X CD-ROM Drive**
- Storage: 1x150GB, 1x500GB SATA II Hard Drive, 1.44 Floppy Drive
- FireWire, eSATA, & USB Ports: One FireWire 400 port, one FireWire 800 port and four USB 2.0 ports on case front; One FireWire 400 port, two FireWire 800 ports, three USB 2.0 ports and one eSATA port on case back
- 17" LCD Panel with Built-In Speakers, Keyboard & Mouse; Surge Protector; 30-piece Security Screwdriver Set; Multi-Purpose Screwdriver; Flashlight
- Microsoft Windows XP Professional (OEM w/CD and COA), QuickView Plus Version 10 \* Norton Anti-Virus (OEM)

**B. Forensic Client System (Work Station) specification**

- Case & Power Supply: ATX, Asus Intel chipset, 2.93GHz, 4GB DDR2-667, Gigabit LAN Controller 10/100/1000Mbps
- Storage: 1x1TB SATA II Hard Drive, Floppy Drive: 1.44 Floppy Drive, DVD-RW Drive
- 17" LCD, MS Keyboard & Mouse, 500VA UPS
- Operating System: Microsoft Windows Vista Home
- *External Write Protected bay Configuration*

\* **Available through CDAC, Tiruanantpuram, with whose help Cyber Forensic Labs in New Delhi and Mumbai were established.**

### Details of Various Legal Provisions Associated with Digital Evidence

**1.** The Information technology Act-2000 has been enacted to provide legal recognition to transactions carried out by means of electronic data interchange and other means of electronic communication, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies. The same enactment has also brought amendments in the **Indian Penal Code, 1861**, the **Indian Evidence Act, 1872**, the **Bankers' Books Evidence Act, 1891** and the **Reserve Bank of India Act, 1934**. As far as Income Tax Act, 1961 is concerned, few amendments have been brought independently to enable Income Tax Authorities to administer Income Tax Law, effectively in the changed environment of functioning in this Cyber Age. It is imperative to know the relevant changes brought in the Income Tax Act, 1961, as well as other related enactments to effectively and correctly handle digital evidences. Therefore, under this chapter, important provisions of such related Laws have been incorporated for the ready reference.

#### **2. The relevant provision of Income Tax Act, 1961**

**2.1 Sub-sections (12A) and (22AA)** have been inserted in section 2 of Income Tax Act, by Finance Act, 2001, with effect from 01-06-2001, where "books of account" and "document" respectively have been defined.

**2.1.1** Sub section (12A) provides the books of account or books maintained on computer, the same sanctity as the traditional books of account. As per provisions of section 2(12A) :

*"'books or books of account', includes ledgers, day books, cash books, accounts-books and other books, whether kept in the return form or as print outs as data stored in a floppy, disk, tape or any other form of electro-magnetic data storage device".*

**2.1.2** Sub-section (22AA) brings electronic records also in the definition of Document. As per this sub section:

*"Document" includes Electronic records as defined in clause (t) of sub section 1 of section 2 of the information technology Act 2000.*

**2.1.3** As per Information Technology Act, 2000, clause (t) of sub-section (1) of section 2, an *"electronic record"* means data, record or data generated, image or sound stored, received or sent in an electronic

form or micro film or computer generated micro file. This definition of electronic record is wide enough to cover person in possession of computer, storage device, server, mobile phone, i-pod or any such device.

## 2.2 Section 132(1)(iib) of Income Tax Act, 1961

This provision was brought on Statute Finance Act, 2002, with effect from 01-06-2002 to remove difficulties in handling digital evidences found during the course of the search. This section *“require any person who is found to be in possession or control of any books of account or other documents maintained in the form of electronic record as defined in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000), to afford the authorized officer the necessary facility to inspect such books of account or other documents.”*

**2.3** Provisions of **section 275B** make failure to comply with provisions of section 132(1)(iib) a punishable offence.

As per this section, *“if a person who is required to afford the authorised officer the necessary facility to inspect the books of account or other documents, as required under [clause (iib) of sub-section (1) of section 132] fails to afford such facility to the authorised officer, he shall be punishable with rigorous imprisonment for a term which may extend to two years and shall also be liable to fine”*.

## 3. Relevant Provisions of Information Technology Act, 2000

### 3.1 Important Definitions

Some important definitions have been provided in sec 2 of the Act. Few of the relevant definitions are as under:

- (a) “access” with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network;
- (d) “affixing digital signature” with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature;
- (f) “asymmetric crypto system” means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature;
- (g) “Certifying Authority” means a person who has been granted a license to issue a Digital Signature Certificate under section 24;
- (h) “Certification practice statement” means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates;
- (i) “computer” means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic,

magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

- (j) “Computer network” means the interconnection of one or more computers through—
  - (i) The use of satellite, microwave, terrestrial line or other communication media; and
  - (ii) Terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained;
- (k) “Computer resource” means computer, computer system, computer network, data, computer data base or software;
- (l) “computer system” means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions;
- (o) “data” means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;
- (p) “Digital signature” means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;
- (r) “electronic form” with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;
- (t) “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;
- (v) “Information” includes data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche;
- (w) “Intermediary” with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message;
- (x) “key pair”, in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;
- (za) “originator” means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary;

- (zc) “Private Key” means the key of a key pair used to create a digital signature;
- (zd) “Public key” means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;
- (ze) “Secure system” means computer hardware, software, and procedure that-
  - (a) are reasonably secure from unauthorised access and misuse;
  - (b) provide a reasonable level of reliability and correct operation;
  - (c) are reasonably suited to performing the intended functions; and
  - (d) adhere to generally accepted security procedures;
- (zf) “security procedure” means the security procedure prescribed under section 16 by the Central Government;
- (zg) “Subscriber” means a person in whose name the Digital Signature Certificate is issued;
- (zh) “verify” in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether-
  - (a) the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;
  - (b) the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.

## **3.2 Digital signature and Authentication of electronic records**

The Information Technology Act, 2000 has also provided mechanism for authentication of electronic records in the form of digital signatures. The provisions of this Act have provided definition and legal recognition of digital signatures. The relevant provisions

### **3.2.1 Sec. 3. Authentication of electronic records.**

- (1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.
- (2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Explanation.- For the purposes of this sub-section, “hash function” means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as “hash result” such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible:-

- (a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;



- (b) that two electronic records can produce the same hash result using the algorithm.
- (3) Any person by the use of a public key of the subscriber can verify the electronic record.
- (4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

### **3.2.2 Sec.4. Legal recognition of electronic records.**

Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is-

- (a) rendered or made available in an electronic form; and
- (b) accessible so as to be usable for a subsequent reference.

### **3.2.3 Sec.5. Legal recognition of digital signatures.**

Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person (hen, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

Explanation. - For the purposes of this section, “signed”, with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression “signature” shall be construed accordingly.

### **3.2.4 Sect. 7. Retention of electronic records.**

- (1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if-
  - (a) the information contained therein remains accessible so as to be usable for a subsequent reference;
  - (b) the electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;
  - (c) the details which will facilitate the identification of the origin, destination, date and time of despatch or receipt of such electronic record are available in the electronic record:

Provided that this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be despatched or received.

- (2) Nothing in this section shall apply to any law that expressly provides for the retention of documents, records or information in the form of electronic records.

### 3.3 Penalties and Adjudication:

Provisions of section 43 of Information Technology Act, 2000 provides penal consequences, various Acts of omission and commission of offences. The provisions are as under:

**Sec. 43.** Penalty for damage to computer, computer system, etc. If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network,-

- (a) accesses or secures access to such computer, computer system or computer network;
- (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
- (e) disrupts or causes disruption of any computer, computer system or computer network;
- (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
- (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one Crore rupees to the person so affected.

Explanation. - For the purposes of this section,-

- (i) "Computer contaminant" means any set of computer instructions that are designed-
  - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
  - (b) by any means to usurp the normal operation of the computer, computer system, or computer network;
- (ii) "computer data base" means a representation of information, knowledge, facts, concepts or

instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;

- (iii) “computer virus” means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- (iv) “damage” means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

### **3.4 Offences punishable under the Information Technology Act, 2000**

Under the provisions of section 65 of this Act whoever knowingly or intentionally, conceals, destroys or alters, or causes another person so to do, any computer source code used for a computer, computer programme, computer system or computer network (where such source code is required to be kept or maintained by law for the time being in force), shall be punishable with rigorous imprisonment for a term upto three years or with fine which may extend to two lakh rupees or with both. For this purpose, computer source code means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form. Similarly, under section 66 of that Act, whoever with intent to cause, or knowing that he is likely to cause wrongful loss or damage to the public, or any person destroys or deletes or alters any information residing in a computer resource (such act is called hacking) shall be punishable with imprisonment upto three years, or with fine which may extend to two lakh rupees, or with both. Under section 71 of that Act, any misrepresentation or suppression of material facts from the Controller or Certifying Authority under that Act for obtaining any licence or Digital Signature Certificate also constitutes an offence.

## **4. The relevant Provisions of Indian Evidence Act, 1872**

By way of the THE SECOND SCHEDULE to the Information Technology Act, Amendments to the Indian evidence act, 1872 have been brought, so as to, give electronic records, a legal recognition as evidence. Few such relevant amendments are as under:

### **4.1 In section 3,-**

- (a) in the definition of “Evidence”, for the words “all documents produced for the inspection of the Court”, the words “all documents including electronic records produced for the inspection of the Court” shall be substituted;

**4.2** In section 17, for the words “oral or documentary,” the words “oral or documentary or contained in electronic form” shall be substituted.

**4.3** After section 22, the following section shall be inserted, namely: -

When oral admission as to contents of electronic records are relevant.

Sec.22A. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.”

**4.4** In section 34, for the words “Entries in the books of account”, the words “Entries in the books of account, including those maintained in an electronic form” shall be substituted.

**4.5** In section 35, for the word “record”, in both the places where it occurs, the words “record or an electronic record” shall be substituted.

**4.6** After section 47, the following section shall be inserted, namely: -

Opinion as to digital signature where relevant.

Sec.47A. When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact.”

**4.7** In section 59, for the words “contents of documents” the words “contents of documents or electronic records” shall be substituted.

**4.8 Admissibility of electronic records.**

Special provisions as to evidence relating to electronic record have been inserted in the form of section 65A & 65B, after section 65. These provisions are very important and they govern the integrity of the electronic record as evidence, as well as, the process for creating electronic record.

**4.8.1** Sec.65A. The contents of electronic records may be proved in accordance with the provisions of section 65B.

**4.8.2** Sec. 65B. (1) Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section

(1) in respect of a computer output shall be the following, namely:

- (a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities regularly carried on over that period by the person having lawful control over the use of the computer;
- (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
- (c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
- (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.

(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether-

- (a) by a combination of computers operating over that period; or
- (b) by different computers operating in succession over that period; or
- (c) by different combinations of computers operating in succession over that period; or
- (d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.

(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say, -

- (a) identifying the electronic record containing the statement and describing the manner in which it was produced;
- (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
- (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this

sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

(5) For the purposes of this section,-

- (a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
- (b) whether in the course of activities carried on by any official, information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
- (c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Explanation. - For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.

#### **4.9 Evidential value of Digital Signature.**

**4.9.1** For the **proof of digital signature**, section 67A has been inserted after section 67. The section is as under:

**Sec.67A.** Except in the case of a secure digital signature, if the digital signature of any subscriber is alleged to have been affixed to an electronic record the fact that such digital signature is the digital signature of the subscriber must be proved.”

**4.9.2** With regard to **Proof as to verification of digital signature**, **section 73A** has been inserted after section 73, which is as under:

**Sec.73A.** In order to ascertain whether a digital signature is that of the person by whom it purports to have been affixed, the Court may direct-

- (a) That person or the Controller or the Certifying Authority to produce the Digital Signature Certificate;
- (b) any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person.

Explanation. - For the purposes of this section, “Controller” means the Controller appointed under sub-section (1) of section 17 of the Information Technology Act, 2000’.

#### **4.10 Presumption relating to electronic agreements, electronic records, digital signatures, etc.**

After section 85 section 85A, 85B & 85C have been inserted which provides for presumptions with respect to Electronic Agreement, Record & Digital Signatures, etc. These provisions are as under:

**4.10.1** Sec. 85A. The Court shall presume that every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signature of the parties.

**4.10.2** Sec. 85B(1) In any proceedings involving a secure electronic records, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the specific point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that –

- (a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;
- (b) except in the case of a secure electronic record or a secure digital signature, nothing in this section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.

**4.10.3** Sec. 85C The Court shall presume, unless contrary is proved, that the information listed in a Digital Signature Certificate is correct, except for information specified as subscriber information which has not been verified, if the certificate was accepted by the subscriber.

#### **4.11 Presumption relating to electronic messages**

After section 88 section 88A has been inserted which provide for presumptions with respect to Electronic messages. These provisions are as under:

**4.11.1 Sec. 88A.** The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

Explanation.- For the purposes of this section, the expressions “addressee” and “originator” shall have the same meanings respectively assigned to them in clauses (b) and (za) of sub-section (1) of section 2 of the Information Technology Act, 2000.’.



#### **4.12 Presumption relating to electronic records**

After section 90 section 90A has been inserted which provide for presumptions with respect to Electronic records. These provisions are as under:

**4.12 .1** Sec.90A. Where any electronic record, purporting or proved to be five years old, is produced from any custody which the Court in the particular case considers proper, the Court may presume that the digital signature which purports to be the digital signature of any particular person was so affixed by him or any person authorised by him in this behalf.

Explanation. - Electronic records are said to be in proper custody if they are in the place in which, and under the care of the person with whom, they naturally be; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render such an origin probable.

This Explanation applies also to section 81A.”

#### **5. The Relevant Provisions of Indian Penal Code, 1861**

Indian Penal Code refers to various documents and records with reference to several offences. By way of the THE FIRST SCHEDULE to the Information Technology Act Amendments to the Indian penal code have been brought, so as to, incorporate reference to Electronic Records, wherever it is necessary. Few such relevant amendments are as under:

**5.1** After section 29, the following section shall be inserted, namely:-

Electronic record.

Sec.29A. the words “electronic record” shall have the meaning assigned to them in clause (t) of sub-section (1) of section 2 of the Information Technology Act, 2000.”

**5.2** In section 192, for the words “makes any false entry in any book or record, or makes any document containing a false statement”, the words “makes any false entry in any book or record, or electronic record or makes any document or electronic record containing a false statement” shall be substituted.

**5.3** In section 204, for the word “document” at both the places where it occurs, the words “document or electronic record” shall be substituted.

**5.4** In section 463, for the words “Whoever makes any false documents or part of a document with intent to cause damage or injury”, the words “Whoever makes any false documents or false electronic record or part of a document or electronic record, with intent to cause damage or injury” shall be substituted.

In various other sections also wherever the word “document” occurs, it has been substituted by the words “document or electronic record”, while the digital signature has been given same recognition as normal signature.

**5.5** There are some other Provisions of Indian Penal Code, 1861, which are otherwise relevant as certain acts relating to handling of digital evidence may constitute offence under them. They are reproduced as under:

**Section 175:**

Whoever, being legally bound to produce or deliver up any [document or electronic record] to any public servant, as such, intentionally omits so to produce or deliver up the same, shall be punished with simple imprisonment for a term which may extend to five hundred rupees, or with both;

Or if the [document or electronic record] it is to be produced or delivered up to a Court of Justice, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

**Section 176:**

Whoever, being legally bound to give any notice or to furnish information on any subject to any public servant as such, intentionally omits to give any such notice or to furnish such information in the manner and at the time required by law, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to five hundred rupees, or with both;

or, if the notice or information required to be given respects the commission of an offence, or is required for the purpose of preventing the commission of an offence, or in order to the apprehension of an offender, with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both;

or, if the notice or information required to be given is required by an order passed under sub-section (1) of section 565 (now 356) of the Code of Criminal Procedure, 1898 (now 1973) with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

**Section 177:**

Whoever, being legally bound to furnish information on any subject to any public servant, as such, furnishes, as true, information on the subject which he knows or has reason to believe to be false, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both;

or, if the information which he is legally bound to give respects the commission of an offence, or is required for the purpose of preventing the commission of an offence, or in order to the apprehension of an offender, with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

**Section 178:**

Whoever refuses to bind himself by an oath of affirmation to state the truth, when required so to bind himself by a public servant legally competent to require that he shall so bind himself, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

**Section 179:**

Whoever, being legally bound to state the truth on any subject to any public servant refuses to answer any question demanded of him touching that subject by such public servant, in the exercise of the legal powers of such public servant, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

**Section 180:**

Whoever refuses to sign any statement made by him, when required to sign that statement by a public servant legally competent to require that he shall sign that statement, shall be punished with simple imprisonment for a term which may extend to three months, or with fine which may extend to five hundred rupees, or with both.

**Section 181:**

Whoever, being legally bound by an oath or affirmation to state the truth on any subject to any public servant or other person authorised by law to administer such oath or affirmation, makes, to such public servant or other person as aforesaid, touching that subject, any statement which is false, and which he either knows or believes to be false or does not believe to be true, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine.

**Section 182:**

Whoever gives to any public servant any information which he knows or believes to be false, intending thereby to cause, or knowing it to be likely that he will thereby cause, such public servant-

- (a) to do or omit anything which such public servant ought not to do or omit if the true state of facts respecting which such information is given were known to him, or
- (b) to use the lawful power of such public servant to the injury or annoyance of any person,

Shall be punished with imprisonment of either description for a term which may extend to six months, or with fine which may extend to one thousand rupees, or with both.

**Section 187:**

Whoever, being bound by law to render or furnish assistance to any public servant in the execution of his public duty, intentionally omits to give such assistance, shall be punished with simple imprisonment for a term which may extend to one month, or with fine which may extend to two hundred rupees, or with both;

and if such assistance be demanded of him by a public servant legally competent to make such demand for the purposes of executing any process lawfully issued by a Court of Justice, or of preventing the commission of an offence, or of suppressing a riot or affray, or of apprehending a person charged with or guilty of an offence, or of having escaped from lawful custody, shall be punished with simple imprisonment for a term which may extend to six months, or with fine which may extend to five hundred rupees, or with both.

#### **Section 191:**

Whoever, being legally bound by an oath or by an express provision of law to state the truth, or being bound by law to make a declaration upon any subject, makes any statement which is false, and which he either knows or believes to be false or does not believe to be true, is said to give false evidence.

#### **Section 192:**

Whoever causes any circumstance to exist or [makes any false entry in any book or record or electronic record, or makes any document or electronic record containing a false statement], intending that such circumstance, false entry or false statement may appear in evidence in a judicial proceeding, or in a proceeding taken by law before a public servant as such, or before an arbitrator, and that such circumstance, false entry or false statement so appearing in evidence, may cause any person who in such proceeding is to form an opinion upon the evidence, to entertain an erroneous opinion touching any point material to the result of such proceeding, is said "to fabricate false evidence."

#### **Section 201:**

Whoever, knowing or having reason to believe that an offence has been committed, causes any evidence of the commission of that offence to disappear, with the intention of screening the offender from legal punishment, or with that intention gives any information respecting the offence which he knows or believes to be false,

Shall, if the offence which he knows or believes to have been committed is punishable with death, be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine;

and if the offence is punishable with imprisonment for life, or with imprisonment which may extend to ten years, shall be punished with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine;

and if the offence is punishable with imprisonment for any term not extending to ten years, shall be punished with imprisonment of the description provided for the offence, for a term which may extend to one-fourth part of the longest term of the imprisonment provided for the offence, or with fine, or with both.

#### **Section 202:**

Whoever, knowing or having reason to believe that an offence has been committed, intentionally omits to give any information respecting that offence which he is legally bound to give, shall be punished

with imprisonment of either description for a term which may extend to six months, or with fine, or with both.

**Section 203:**

Whoever, knowing or having reason to believe that an offence has been committed, gives any information respecting that offence which he knows or believes to be false, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

**Section 204:**

Whoever secretes or destroys any [document or electronic record] which he may be lawfully compelled to produce as evidence in a Court of Justice, or in any proceeding lawfully held before a public servant, as such, or obliterates or renders illegible the whole or any part of such [document or electronic record] with the intention of preventing the same from being produced or used as evidence before such Court or public servant as aforesaid, or after he shall have been lawfully summoned or required to produce the same for that purpose, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine, or with both.

## Annexure-7

Digital Evidence Collection Form			
Name of the Authorized Officer:			
Name of the assessee :			
Date:	Time:	Premise Address:	
Examiner's Name and Details:			
Computer Information			
<input type="radio"/> Laptop	<input type="radio"/> Desktop	<input type="radio"/> Server	<input type="radio"/> File/Folder
<input type="radio"/> Others	If Others Specify		
System State		If switched On, What is visible on screen?	
<input type="radio"/> On <input type="radio"/> Off <input type="radio"/> Hibernation/Sleep			
System Info	Make: _____ Model: _____		
	Serial No: _____ Size: _____		
Whether Volatile Memory/RAM Memory was collected? _____			
Shut Down Type	<input type="radio"/> Normal <input type="radio"/> Power Plug pulled <input type="radio"/> Battery Removed (Laptop)		
Is the suspected media encrypted?	Type of encryption Software used		
<input type="radio"/> Yes <input type="radio"/> No			
Hard Disk Handling: <input type="radio"/> Seizure <input type="radio"/> Forensic Previewing <input type="radio"/> Imaging <input type="radio"/> Backup			
Details of Imaging Software/Version to be given			
Is the hash value calculated?	Algorithm:		
<input type="radio"/> Yes <input type="radio"/> No	<input type="radio"/> MD5 <input type="radio"/> SHA <input type="radio"/> OTHERS		
MD5 hash value:			
SHA hash value:			
Other Authentication Method:			
Storage Copy Details		Working Copy Details	
Make: _____ Model: _____		Make: _____ Model: _____	
Serial No: _____		Serial No: _____	
Is the hard disk replaced back?	Date:	Time:	
<input type="radio"/> Yes <input type="radio"/> No			
Is the signature of the witness taken? <input type="radio"/> Yes <input type="radio"/> No			
Note by the AO regarding the potential evidences in the digital devices:			

Annexure-8

Chain of Custody Form					
Name of the assessee :					
Date:	Time:	Premise Address:			
Description:					
Chain of Custody					
Reason/Action	Received From	Received by	Data	Time	Signature of parties



## Annexure-9

Mobile Devices Collection Form-Checklist			
Name of the Authorized Officer:			
Name of the assessee :			
Date:	Time:	Premise Address:	
Examiner's Name and Details:			
System State		If switched On, What is visible on screen?	
<input type="radio"/> Or <input type="radio"/> Or <input type="radio"/> Hibernation/Sleep			
System Info		Make: _____ Model: _____ Mobile Type: <input type="radio"/> GSM <input type="radio"/> CDMA <input type="radio"/> 3G <input type="radio"/> Others If Others Specify _____	
Time Zone Settings: _____			
Date/Time of Mobile Phone: _____ Actual Date/Time: _____			
IMEI/MEID Number			
Mobile Serial Number(If any)			
Operating System ( Including Version Number)			
Is the SIM Card Present? <input type="radio"/> Yes <input type="radio"/> No		SIM Service Provider Name:	
SIM Card Size		IMSI Card Number	
Mobile Phone State: <input type="radio"/> ON <input type="radio"/> OFF <input type="radio"/> OFFLINE		Shutdown Type <input type="radio"/> NORMAL <input type="radio"/> BATTERY PULLED	
Mobile Phone State: <input type="radio"/> YES <input type="radio"/> NO		Media Card Serial Number:	
		Media Card Make and Capacity:	
Does the Assessee phone has the ability to access Internet? <input type="radio"/> YES <input type="radio"/> NO			
Storage Copy Details		Working Copy Details	
Make: _____ Model: _____		Make: _____ Model: _____	
Serial No: _____		Serial No: _____	
Is the Media Card Removed? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Media Card Replaced after Imaging? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Is the SIM Card Removed? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
SIM Card Replaced after Imaging? <input type="radio"/> Yes <input type="radio"/> No		Date: Time:	
Is the signature of witness taken? <input type="radio"/> Yes <input type="radio"/> No			
Note by the AO regarding the potential evidences in the digital devices:			