IT Forensics and Digital Methods for Investigations:

- **CA Dr Vishnu Kanhere**

Computer Forensics encompasses the process, methods, techniques and tools for investigating frauds and crimes both in the real world and cyber world. In fact with the proliferation of Information Technology computers are around us everywhere. We use them in our daily lives to communicate, interact, lead our personal lives and manage our business, industry and services. Our infrastructure, our governance even our health care and legal systems are heavily using IT.

With the proliferation, use and dependence on information technology, the use of paper documents and evidence as we know it has become much less and digital records and evidence have gained prominence. This has led to the increasing use and importance of computer forensics.

Digital forensics is the use of scientific methods for the identification, preservation, extraction and documentation of digital evidence derived from digital sources to enable successful prosecution

Silent in Nature: Computer frauds and crimes could be committed in privacy without reaching to scene of crime physically i.e. no eye witnesses. There is no signs of physical violence or struggle.

Global in character: No national borders. By sitting comfortably far away from the country the entire economy of the country could be destroyed. As digital evidences are fragile in nature one has to respond quickly.

Non existence of Physical Evidence: No physical evidence to indicate that crime has been committed. Only on a closer look the trained person could find out the evidences which are not in the traditional format but are in digital format.

Fraud operators…like other criminals…are always among the first to appreciate the potential of a new technology. Hence as professionals, it becomes imperative that we also understand the technology and upgrade ourselves to help reduce the scope and impact of frauds and crimes in an IT setting

What is Forensics?

"Assaying the correspondence (or otherwise) of actual events, episodes and happenings & conformance of forensic approaches (tools and techniques) used with established criteria to provide improved information to deliver justice in accordance with criminal jurisprudence."

Forensics covers

Determining potential / committed abuse.

Establishing the fact of abuse

Preservation of the proof – by adducing reliable external evidence.

Presentation of the evidence and findings in a manner required by courts / public enquiries

The digital forensic examiner has to follow the digital forensic process in order for evidence to be admissible in a court of law. The four phases are

acquisition,

examination,

analysis and

reporting

The process is common in different fields including mobile and network forensics. The process is used in investigations and has gained recognition in science

The acquisition phase describes how data will be acquired from different types of digital information sources. Data has to be acquired in a manner that maintains its integrity and authenticity. The different methods and tools for acquiring data are covered in detail.

The examination phase covers analysis of

Physical media

Media management

File system analysis

Application analysis

Network analysis

Memory analysis

The analysis phase describes how the data is processed. A hash analysis search can be conducted using hashing tools. By comparing hash values

investigators can exclude large numbers of files that have no value to the case and hash comparing can be done between fingerprint and hash values of the data being examined.

This covers the following techniques

Recovering deleted files

Production of time stamps and other Meta data

Removing known files

File signatures verifications

String searching and file fragments

Web activity reconstruction

Email activity reconstruction

Registry activity reconstruction

Analyzing unknown files

Software assisted analysis

Alternate data streams

Live forensics

Self organizing maps

Recovering hidden files

Geo-location

The reporting phase covers compilation and presentation of the data in the form of a case report which covers and provides case information

based on agreed goals and additional goals of the investigation. An example is given below

Based on Case Goals –Required information

•Keywords / mail domains for email analysis

•Keywords for document identification

•Documents located

•System Images

–Beneficial Information

•Full case background or timeline of events

•Work-product names / external associated names

•Specific dates and times

Computer Evidence...

...is like any other evidence, it must be:

• admissible

• authentic

• accurate

• complete

• convincing to juries

The most common tools used are

Forensic Replicators replicates the hard disk of the suspect without altering a single bit of data and without the system being switched on. The original can be sealed and protected as evidence. The copy is manipulated using search techniques to trace missing lost and deleted files to re–construct the criminal / fraudulent act.

Case Agent Tools – these provide following functions -

• Captured data can be fed into a case agent tool for review

• powerful all viewing and searching options for easy use

• complete analysis, book marking and note taking functions

• final report generated for a proper presentation and closing of the case.

It is only through the practice of preventive rather than reactive techniques that forensics will become visibly effective and become credible.

Awareness of human element, organization's behavior, knowledge of the system, the technology in use and expected to be used, knowledge of crimes and fraud, evidence and the standard of proof, potential for crimes and fraud and appreciation of the so called clues and flags are key issues.

Fraud Prevention Measures

It is often said prevention is better than cure. This is very much applicable to fraud and crime. The genesis of fraud is based on fraud triangle comprising opportunity, rationalization and motivation or pressure.

Most organizations have internal controls and procedures / processes in place to prevent frauds. But these focus on only one vertex of the triangle viz. opportunity. This leaves the other two open. A comprehensive anti fraud policy promotes ethical values in an organization and deters fraud by acting on reducing the motivation and pressure to commit frauds.

Such a policy framework is based on promoting transparency, creating awareness and education, and takes the help of techniques like whistle blowing, hotline and others.

Key elements of effective fraud prevention include:

a robust Fraud Policy and Code of Conduct;

sound fraud risk management processes;

a comprehensive fraud control plan;

prudent employee, and third party, due diligence;

regular fraud awareness training;

fraud-related controls for activities with a high fraud risk exposure;

system controls to ensure accurate and up-to-date data; and

communication about investigation outcomes to demonstrate that allegations and incidences of fraud are serious and appropriately dealt with.

Anti fraud policy – An anti-fraud policy (sometimes called a 'fraud policy statement') outlines an organisation's attitude to, and position on, fraud and sets out responsibilities for its prevention and detection

Whistle blower policy – It is a good practice to put a whistleblower protection policy in place to encourage people to bring their concerns forward without fear of retaliation. Organizations that encourage complaints by having an "open door" policy and have a standard of "no retaliation" for raising concerns are considered more transparent. These organizations will be in a better position to address all concerns, whether they are about fraudulent accounting practices, unsafe conditions, or alleged discrimination.

Hotline – a safe effective and confidential mode of communication to enable persons to report on fraud and voice concerns to management.

Other measures – employee screening, customer screening, random checks and audits, mystery shopping, segregation of duties and rotation of staff, compulsory leave etc.

An effective use of both preventive and detective techniques will better enable us as chartered accountants to provide effective counter to the growing fraud menace and help organizations in minimizing their fraud losses.