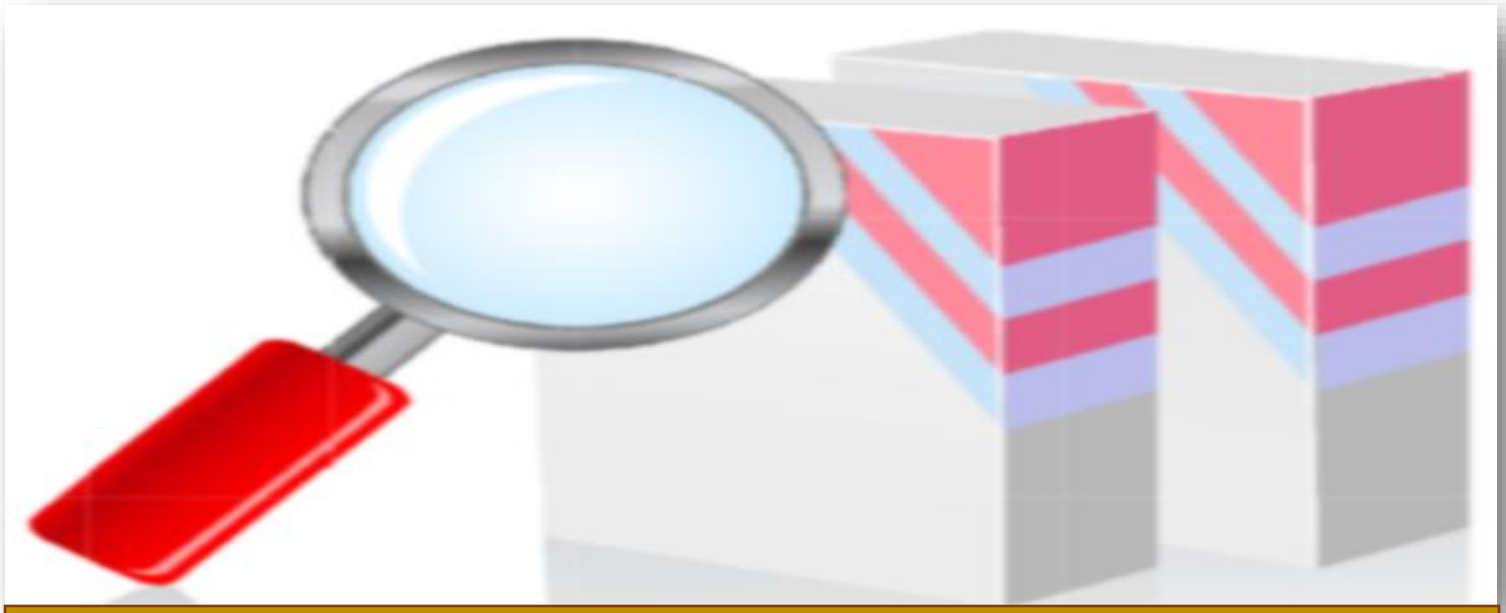


UNIT-11 Computer Crimes

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Understand what is Computer Crime
- ✓ Explore the Features of the Computer Environment
- ✓ Identify the Types of Computer Crimes and Source of Digital Data

Unit 11

Computer Crimes

Systems and data are powerful tools in preventing, detecting and investigating fraud; therefore, technology plays an important role in the fraud environment. A computer, which can be broadly defined as a device for storing data and performing calculations, is typically the mechanism through which technology is used to commit fraud. Sometimes, technology itself is the criminal's target. Technology, by virtue of being a part of society, also becomes a part of fraudulent activities and crime.

Even before the age of computers and computer-related crime, blue- and white-collar crime existed. Therefore, the computer did not bring about a new form of crime; it merely changed the nature of the old crimes. Computer-related crime is usually committed by insiders or former employees who have the required skills, knowledge and access. For this reason, computer-related crime is an occupational crime. Insiders (those who are working inside the organization) are more likely to obtain unauthorized access than outsiders.

What is Computer Forensics?

According to the U.S. Department of Justice, computer forensics can be defined as "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events."

Computer forensics involves the process of determining any activity that took place on a particular computer device and of restoring deleted or corrupted data. Computer forensics is an important part of a fraud investigation as it determines the key players involved in the fraud, the information possessed by those players, the time when they acquired that information, the documents to which those involved in the fraud had access, the actions they took, the people with whom they communicated, and their efforts, if any, to hide their actions. Forensic accountants are able to make use of data such as internet history, lost or deleted files, web-based e-mails, and logging and registry files in order to collect evidence of the fraud.

The Benefits of Computer Forensics and Data Analysis

Let us suppose that a forensic accountant has to analyze thousands of line items of journal entries, receipts, invoice items and disbursements. How will he/she identify items to perform further tests and analyses for risk elements? This would be a tedious, time-consuming and inefficient process without computer-assisted data analysis. With the help of sophisticated, powerful software and technological ability, 100% of the information can be analyzed. There are several sources from which data might be retrieved, such as the company's general ledger, sales database, time and expense systems, user files, network drives, web logs, building access logs, and any other source of electronic data. Benefits of using data analysis include:

- Reduction, and even elimination, of sampling risk.
- Comparing relevant data from different sources and systems to show a fuller picture.
- Monitoring relevant data trends over periods of time, analyzing fluctuating trends, and identifying false positives and potential risk factors.
- Quickly identifying and extracting certain risk criteria from the entire data population for further analysis.
- Testing internal controls and organizational policies for their efficacy in identifying weaknesses.
- Identifying trends that are unknown to company personnel, consultants and forensic accountants.

These days, forensic accountants assist auditors through SAS 99 procedures. Computer forensics helps forensic accountants to electronically analyze manual journal entries and identify anomalies and potential risks with the help of analytical tools. Testing supporting documentation for higher-risk manual entries to better understand potential risk is another area in which forensic accountants might help auditors. This process either assures accountants and auditors that journal entries were made properly or identifies errors and irregularities. Forensic accountants may even be able to design procedures to review e-mails when dealing with certain high-risk scenarios. These procedures may involve developing a list of search items and custodians and analyzing the output of e-mail searches.

Planning Computer Forensics Engagement

The forensic accountant needs to plan all procedures properly in order to meet his/her objectives, produce solid results and satisfy standards. At the very outset of the investigation, it is important that the forensic accountant's role, i.e. the scope of the engagement, is specified and agreed upon and that the results expected from the engagement are clarified. The forensic accountant should arrange with the client in advance for access to required information and documents. The forensic accountant should share with the client his/her expectations of the computer forensic investigation. During forensic investigation, it is important to consider and analyze the ways in which people in whom the forensic accountant is interested have used technology.

Sometimes, knowledge of what kind of information someone had access to and who tried to delete data or documents can solve a fraud case. This is the information that computer forensics can provide, as it can help determine what the user knew, when they knew it, whether they transmitted that information to other parties or not, and whether someone tried to cover their tracks by deleting data.

Computer forensics can also indicate dates and times when the computer was used and the websites that were visited. Information such as the time when a particular document was created or amended, when a PowerPoint presentation was created and by whom, etc. can also be provided by computer forensics. The investigators must ensure that the proper chain of custody was followed and documentation was provided in order that the results of the examination might be authenticated and

any challenge to the conclusions drawn might be countered. Computer forensics best practices have to be systematic rather than ad hoc and temporary. A systematic computer forensic analysis has the following characteristics:

- Ability to apply sound and replicable methodologies.
- Using practices that have been able to withstand challenges in the past.
- Using software that is acceptable in the forensic profession.
- Ability to apply methods that yield reproducible results.
- Documenting everything comprehensively.

Objective of a Computer Forensic Engagement

In order to understand the objectives of engagement, it is important to have an understanding of the context of the forensic engagement. Usually, computer forensic engagements are carried out for the following purposes: fraud prevention and detection control assessments; investigations and consultations involving bankruptcy; advisory assistance for disputes such as family law, valuation assistance, non-testifying privileged consulting, and damages calculation and expert services; investigations, including financial reporting and security investigations, regulatory compliance, and misappropriation of assets. Corporate security professionals, internal and external audit teams, outside law firms and individuals, and in-house counsel can all request computer forensic assistance.

Forensic accountants might benefit from the knowledge of various commercially available forensic software tools that can help them with computer forensics. It is important to be aware of the advantages of using these tools, and to upgrade them regularly.

Legal Parameters

The following are some of the legal factors that have to be considered before embarking on an engagement:

- Is there a subpoena that allows collection of data?
- Is counsel available to the engagement team under privilege?
- Does the expert have the necessary qualifications and licenses to provide sound advice? In other words, is the forensic accountant able to withstand challenges?
- According to state law, is it necessary for data to be collected and analyzed only by a licensed private investigator?
- In cases where data are being collected internationally, is the engagement team aware of laws pertaining to international privacy?
- Does the forensic accountant or client have legal authority to gather the data?
- Does the team know to whom the data belong, and are there any privacy concerns?
- Is the scope of the examination limited to relevant data?
- Does the team expect to find data, such as those related to national security issues or child pornography, on the devices that would need to be reported to law enforcement authorities?

Before beginning a computer forensics engagement, it is important to address all legal issues and follow the legal counsel's advice. It is also advisable to design protocols to ensure compliance.

The forensic accountant must obtain initial facts and documents before he/she starts working on computer forensics. He/she must confirm the following facts with the clients:

(1) The nature and scope of the engagement;

(2) The computer systems

and technology involved; and (3) the expected results and conclusions. Given below is a list of questions that the accountant would want to consider:

- What type of engagement are they carrying out (i.e., investigation, dispute, regulatory compliance assessment)?
- Is the matter a civil, criminal or regulatory proceeding?
- What are the relevant dates during which the activity occurred?
- Which corporate departments (accounting, marketing, executive or legal) were affected?
- Which are the known key documents?
- Can the forensic accountant obtain copies of litigation documents, subpoenas, or any other legal documents?
- Are documents or any other collected data subject to preservation orders?
- Is there any controversy regarding monetary value?
- Does the person requesting the examination have the legal authority to possess and examine the equipment?
- What is the expected scope of the examination, i.e. how many devices are expected to be required?
- Would data have to be collected from a computer network?
- What is the identification and contact information of the investigative team?
- What important information, e.g. known associates, account numbers, key e-mails, and product names, does the investigation team have?
- Which computer systems and what kind of technology, i.e. type of computers (Mac, PC, etc.), type of servers (Outlook or SQL), and smartphones (iPhone or Blackberry) need to be examined?
- What is the number, make, model and storage capacity of every device or medium to be examined?
- Who is the key point of contact with the organization's internal IT department?
- Which operating systems, e-mail systems, application and document management systems are being used?
- Are any encryption tools being used, and if so, which ones?
- What is the nature and type of structured data stores that are under analysis?
- Does the network have a data map?
- What, if any, forensic work has been performed previously?
- What are the policies regarding privacy, confidentiality, usage, and IT security?

- What are the usernames, passwords and employee numbers?
- What is the users' personal identifiable information, such as date of birth?
- What access level was each user granted?

Where Might Data Reside?

Forensic data might reside in any device that is used for data storage. Given below is a list of all the equipment where forensic data might be found:

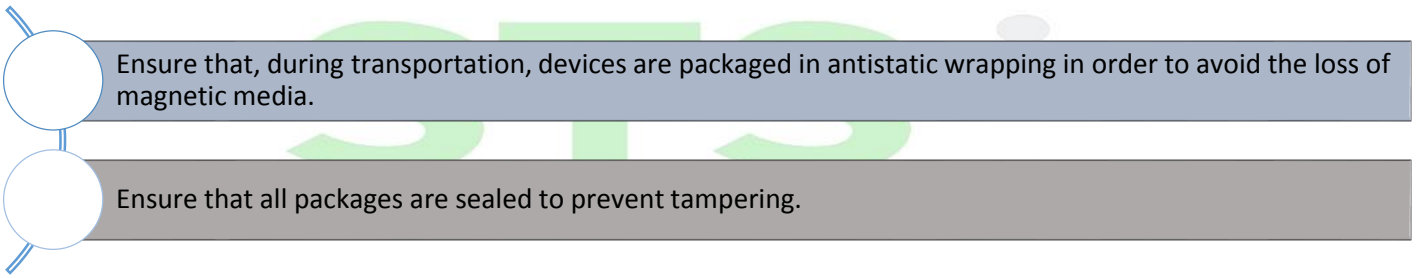
- Laptop computers
- Removable disks
- PCs and workstation printers
- Solid state storage
- Fax machines
- Thumb-drives
- IP telephones
- Tapes
- Personal digital assistants
- CDs and DVDs
- Cell phones
- E-mail – server or remotely stored
- Scanners
- Voicemail on telephone systems
- Copiers
- Recycle bin
- iPods and MP3 players
- Instant messenger
- Mainframes and servers
- Data stored in the "cloud"

Execution of the Computer Forensic Engagement

After clarifying the scope, timing, budget and product expectations, the forensic accountant should formulate a work plan for the process through which data can be identified and collected. Details regarding the chain of custody that data collection and analysis must follow are another vital element of the plan. Electronic information, like a weapon in a criminal investigation, must be handled properly in order to ensure that it is admissible in court and not vulnerable to criticism.

A forensic accountant who is a technology expert uses a chain of custody form with the following information:

- Name(s) and signature(s) of the person(s) who is(are) providing and collecting the device.
- The exact physical location of each device including the address and room number.
- Every device's condition, description, make, model number and serial number.
- The date and time at which each device was collected
- Markings on the device including a case/project number, item number, and the initials of the person who has marked the device. It is important to avoid any damage to the device. The following are alternative methods of grouping small items into sealed and marked bags:



After being transported to a secure location for examination, every device should be stored in an evidence locker. This locker might be as elaborate as a secure vault or as simple as a locked cabinet. Anyone who wants to remove the evidence from the locker must provide the time and date of the removal of evidence along with their name and signature. It is critical that once the chain of custody has been established, it is maintained in order to avoid lapses in protocol, which may impact the credibility of the entire examination.

Examination of the Device(s) to be Collected

Determining the ways of examining the device is the next step in planning. The forensic accountant has a number of methodologies from which to choose, and the following are some commonly used steps, listed from least to most invasive:

Initial Response: Evaluating the reported incident or anomaly urgently in order to determine the necessity of further computer forensic methods. This generally involves collecting any available information, such as identifying people in possession of important facts and knowledge, determining

computers and devices that may have been involved, and assessing the extent and magnitude of damage. Securing or isolating systems, obtaining advice from counsel, and notifying the entity's management and owners are other factors that should be taken into consideration.

Forensic Preview: Reviewing the entity's information and technology assets in order to determine the existence of data and the need, desirability, and practicality of further forensic methods. This may involve scanning a computer or a device for data, such as software commonly used by law enforcement for detecting pornographic images in computers.

Static Forensics: Performing forensic processes against static data in order to help the engagement. This is how most forensic engagements are performed. This process involves taking an image of a hard drive and analyzing it in a secure environment, while ensuring that the forensic image is not altered and is a mirror image of the actual hard drive.

Live Forensics: Performing forensics on live or dynamic data. Typically this process involves performing a forensic process on a computer or a server that is never switched off due to its importance for the company's performance and sustainability. Sometimes, in the process of collecting data, irrelevant information may be collected as well, which is called "over collection". For example, if the company's entire e-mail server is collected, it is entirely possible that irrelevant accounts will be included. However, in cases involving structured data such as accounting information or Human Resource records, it is necessary to copy entire servers so that customized reports can be run. In cases where entire servers are not required, over-collection can be avoided by devising a detailed plan according to which the forensic accountant knows the portion of the server that is relevant to the engagement.

Expertise

Many companies prefer their own internal IT departments to carry out computer forensic examinations. This may be cost-efficient, as hiring external experts may be expensive; however, some issues need to be addressed. Firstly, it should be established that the company's own department has the necessary forensic knowledge. Although most IT professionals are able to copy hard drives, they may not know how to collect data in a manner that is consistent with forensic examination norms. Therefore, it is necessary to ensure that professionals are adequately trained and experienced in handling forensic software. Every IT professional has a different skill set; therefore, it is important that due attention be given to the collection and handling of data by competent professionals to prevent their integrity from being compromised.

Now we will discuss the importance of technology and methodologies used in evaluating collected data, ensuring completeness, preparing data for analysis, performing inquiries and analysis, and the tools available to a forensic accountant for data analysis.

Are the Imported Data Complete and Accurate?

Ensuring that records are accurate and complete is the forensic accountant's responsibility after overcoming technological problems. There are certain problems that a forensic accountant may encounter while collecting data. There is a serious risk of missing relevant and important details as data are collected from multiple sources and different systems. Moreover, the forensic accountant may also make the mistake of categorizing data into accounts that have not been extracted properly, thereby limiting the analysis of important accounts.

Do the Data Extracted Need to be Normalized or Cleansed?

The forensic accountant should scrutinize extracted data for normalization of fields and type of data, after which he/she may decide that it is necessary to normalize or clean up the data. Normalization or cleaning up of data refers to the process of data standardization in order that they might be analyzed efficiently. For example, if the data contain dates written in both mm/dd/yy and dd/mm/yy formats, the forensic accountant should normalize the date pattern to make it consistent throughout the data and easy to analyze. There are various issues that forensic accountants need to be aware of when normalizing data fields. Software such as Excel, Text Pad, and ASAP Utilities can aid the normalization process.

The forensic accountant has a number of tools that can help with data analysis.

TYPE	DESCRIPTION	EXAMPLES
Basic Productivity Software	The forensic accountant would need intermediate or advanced expertise in the use of the product. They may use software used for other business purposes as well.	Excel, Access
Excel/Office Add-on Data Analysis Software	Intuitive programs with user-friendly utilities that leverage Excel and other Microsoft products in order to perform data analysis. They enable users	ActiveData, TopCaats

	who are beginners in data analysis to experiment without incurring high training or implementation expenses.	
Data Analysis Software	Comprehensive data analysis programmes that support various investigative activities, such as converting multiple electronic formats into a single format that can be used.	IDEA, ACL
Specialty Software	Special purpose software to facilitate advanced data analysis inquiry or special investigative purposes, e.g., data mining, security and access.	WizSoft, SAS, SPSS, Qualys

Data Analysis Versus Data Mining

One of the challenges of data implementation is the requirement for the forensic accountant to define his/her preferred exception conditions. In other words, the forensic accountant needs to define the specific conditions after obtaining data. For example, while analyzing the data obtained, the forensic accountant would have to specify the exact field and amount to identify an exception for further scrutiny and follow-up. The basic assumption of this approach is that the forensic accountant has reason to suspect specified patterns of unusual activity and that fraudulent activity can be identified by reviewing all transactions and by conducting thorough inquiries.

Data mining refers to the use of mathematical algorithms to analyze data and predict relationships between various fields in the data along with future trends and behaviours. It provides a solution to challenges posed by data analysis. For example, not only can an accounts payable file be analyzed, but the relationship between the employee who initiated the transaction, the date, time and amount of the transaction, and other such fields can also be determined. Algorithms determine the probability of that relationship. For example, if 98% of the transactions exhibit a certain relationship and 2% do not, this 2% anomaly would be of interest to forensic accountants.

Although data mining has its merits, it is far from perfect. Anomalies alone do not indicate the existence of fraud. Forensic accountants may have to encounter false negatives (false indications of fraud) through data mining techniques. Combining data analysis and data mining can be an interesting technique. After first identifying trends through data mining, the forensic accountant can analyze them further using data analysis tools.

Further Reading:

- ✓ ***Saurav K. Dutta; Published Jun 18, 2013 : Statistical Techniques for Forensic Accounting: Understanding the Theory and Application of Data Analysis***
- ✓ ***Golden, T.W., Skalak, S., Clayton, M. (2006) A Guide to Forensic Accounting Investigation***
  Albrecht, C.C., Albrecht, W. (2005)
- ✓ ***Fraud Examination***
  Brown, A., Doig, A., Summers, G., Dobbs, L. (2004)
  Practically Fraud