Introduction to Digital Forensics

MODULE 1

Contents

Introduction to Digital Forensic

1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the history and evolution of digital forensics
- Describe various types of cyber crime
- Understand benefits of computer forensics
- Know about forensics readiness
- Implement forensics readiness plan

1.2 INTRODUCTION TO COMPUTER FORENSICS

Digital forensics[1], the art of recovering and analysing the contents found on digital devices such as desktops, notebooks/netbooks, tablets, smartphones, etc., was little-known a few years ago. However, with the growing incidence of cyber crime, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, augmenting what was conventionally limited to the recovery and analysis of biological and chemical evidence during criminal investigations.

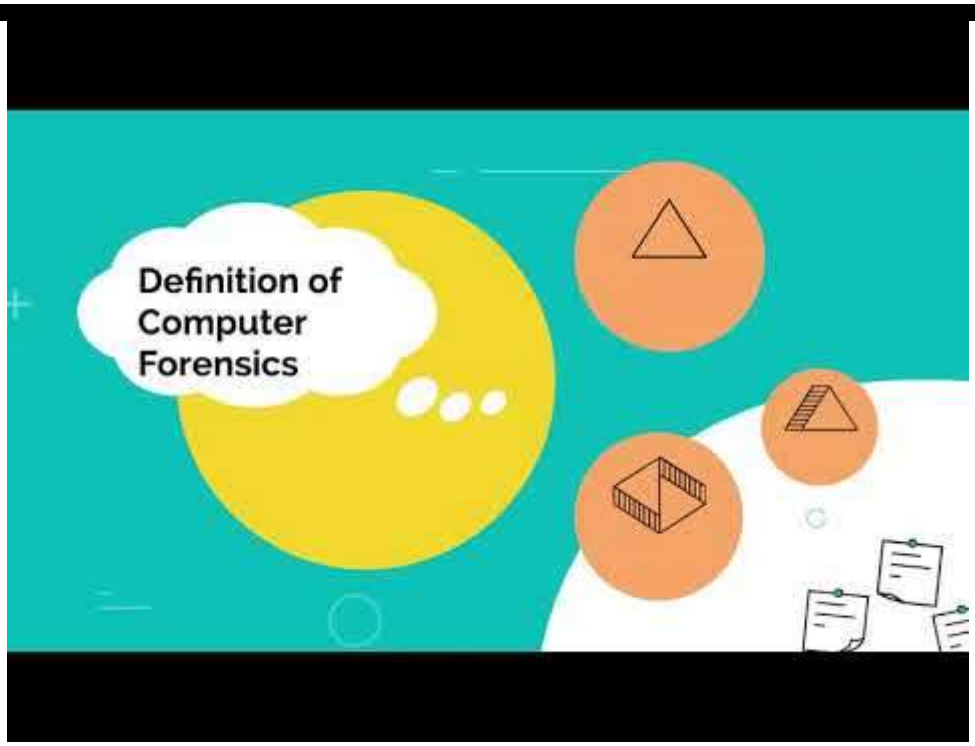
VIDEO LECTURE

[1] http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/

1.2.1 Definition of Computer Forensics

Computer forensics[2] is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. It is the use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, and authentication of data by technical analysis or explanation of technical features of data and computer usage[3]. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel. Similar to all forms of forensic science, computer forensics is comprised of the application of the law to computer science. Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. Like many other forensic sciences, computer forensics involves the use of sophisticated technological tools and procedures that must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. It use specialized techniques for recovery, authentication, and analysis of computer data, typically of data which may have been deleted or destroyed.

VIDEO LECTURE



[2] https://forensiccontrol.com/resources/beginners-guide-computer-forensics/
[3] http://www.edrm.net/resources/glossaries/glossary/c/computer-forensics

1.2.2 Cyber crime

Computer crime[4], or **cybercrime**, is any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr. Debarati Halder and Dr. K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare. Digital forensics is traditionally associated with criminal investigations and, as you would expect, most types of investigation centre on some form of computer crime. This sort of crime can take two forms; computer-based crime and computer facilitated crime[5].

VIDEO LECTURE

[4] https://en.wikipedia.org/wiki/Computer_crime
[5] https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types

1.2.2.1 Computer based crime

This is criminal activity that is conducted purely on computers, for example cyber-bullying or spam. As well as crimes newly defined by the computing age it also includes traditional crime conducted purely on computers (for example, child pornography).

1.2.2.2 Computer facilitated crime

Crime conducted in the "real world" but facilitated by the use of computers. A classic example of this sort of crime is fraud: computers are commonly used to communicate with other fraudsters, to record/plan activities or to create fraudulent documents.

Not all digital forensics investigations focus on criminal behaviour; sometimes the techniques are used in corporate (or private) settings to recover lost information or to rebuild the activities of employees.

1.3 EVOLUTION OF COMPUTER FORENSICS

It is difficult to pinpoint the first "computer forensic" examination or the beginning of the field for that matter[6]. But most experts agree that the field of computer forensics began to evolve more than 30 years ago. The field began in the United States, in large part, when law enforcement and military investigators started seeing criminals get technical. Government personnel charged with protecting important, confidential, and certainly secret information conducted forensic examinations in response to potential security breaches to not only investigate the particular breach, but to learn how to prevent future potential breaches. Ultimately, the fields of information security, which focuses on protecting information and assets, and computer forensics, which focuses on the response to hi-tech offenses, started to intertwine.

Over the next decades, and up to today, the field is evolving. Both Government and private organizations and corporations have followed suit – employing internal information security and computer forensic professionals or contracting such professionals or firms on an as-needed basis. Significantly, the private legal industry has more recently seen the need for computer forensic examinations in civil legal disputes, causing an explosion in the e-discovery field.

The history of forensic science dates back thousands of years. Fingerprinting was one of its first applications. The ancient Chinese used fingerprints to identify business documents. In 1892, a eugenicist named Sir Francis Galton established the first system for classifying fingerprints. Sir Edward Henry, commissioner of the Metropolitan Police of London, developed his own system in 1896 based on the direction, flow, pattern and other characteristics in fingerprints. The Henry Classification System became the standard for criminal fingerprinting techniques worldwide.

In 1835, Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to the murder weapon. Bullet examination became more precise in the 1920s, when American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings. And in the 1970s, a team of scientists

[6] http://colbycriminaljustice.wikidot.com/cyberforensics

at the Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.

In 1836, a Scottish chemist named James Marsh developed a chemical test to detect arsenic, which was used during a murder trial. Nearly a century later, in 1930, scientist Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups. His work paved the way for the future use of blood in criminal investigations. Other tests were developed in the mid-1900s to analyze saliva, semen and other body fluids as well as to make blood tests more precise.

In 1984, FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.

In 1988, the International Association of Computer Investigative Specialists(IACIS), an international non-profit corporation composed of volunteer computer forensic professionals dedicated to training and certifying practitioners in the field of forensic computer science was formed.

VIDEO LECTURE

It was followed by formation of International Organization on Computer Evidence(IOCE)[7] in 1995, which aims to brings together organizations actively engaged in the field of digital and

[7] https://en.wikipedia.org/wiki/Scientific_Working_Group_on_Digital_Evidence

multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.

With the rise in cyber crime, the G8 nations realised the importance of computer forensic, and in 1997 declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes". In 1998, G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. In the same year INTERPOL Forensic Science Symposium was held. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.
The timeline of computer forensics could be summarised as:

Table 1: Computer Forensics Timeline

Year	Event
1835	Scotland Yard's Henry Goddard became the first person to use physical analysis to connect a bullet to the murder weapon.
1836	James Marsh developed a chemical test to detect arsenic, which was used during a murder trial.
1892	Sir Francis Galton established the first system for classifying fingerprints.
1896	Sir Edward Henry, based on the direction, flow, pattern and other characteristics in fingerprints.
1920	American physician Calvin Goddard created the comparison microscope to help determine which bullets came from which shell casings.
1930	Karl Landsteiner won the Nobel Prize for classifying human blood into its various groups.
1970	Aerospace Corporation in California developed a method for detecting gunshot residue using scanning electron microscopes.
1984	FBI Magnetic Media program, which was later renamed to Computer Analysis and Response Team (CART), was created and it is believed to be the beginning of computer forensic.
1988	International Association of Computer Investigative Specialists(IACIS) was formed.
1995	International Organization on Computer Evidence (IOCE) was formed.
1997	G8 nations declared that "Law enforcement personnel must be trained and equipped to address high-tech crimes".
1998	• G8 appointed IICE to create international principles, guidelines and procedures relating to digital evidence. • 1st INTERPOL Forensic Science Symposium was held.
2000	First FBI Regional Computer Forensic Laboratory established.

1.4 STAGES OF COMPUTER FORENSICS PROCESS

The overall computer forensics process is sometimes viewed as comprising four stages[8]:

- Acquire: Identifying and Preserving
- Analyze: Technical Analysis
- Evaluate: What the Lawyers Do
- Present: Present digital evidence in a manner that is legally acceptable in any legal proceedings.

[8] http://computer-forensics.safemode.org/index.php?page=Four_Step_Process

1.5 BENEFITS OF COMPUTER FORENSICS

With the ever-increasing rate of cyber crimes, from phishing to hacking and stealing of personal information not only confined to a particular country but the globally at large, there is a need for forensic experts to be available in public and private organizations[9]. To be able to handle this, it's vital for network administrator and security staff of networked organizations to have this course in practice making sure that they have the laws pertaining to this on their finger tips. This would ensure that should need for the service avail itself, then they would come in and rescue the situation.

The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics. They should be taken as the main element of computer and network security. It would be a great benefit for a company if it has knowledge of all the technical and legal aspects of this field. Should the company's network be under attack and the intruder caught in the act, then an understanding about computer forensics will be of help in provision of evidence and prosecution of the case in the court of law.

New laws aimed at the protection of customer's data are continuously being developed. Should they lose data, then naturally the liability goes to the company. Such cases, if they occur will automatically result in the company or organization being brought to the court of law for failure to protect personal data, this can turn out to be very expensive. But through the application of forensic science, huge chunks of money can be saved by the firms concerned. A lot of money is lately being spent on network and computer security. Software for vulnerability assessment and intrusion detection has passed the billion dollar mark, this is according to experts. It simply means that there is a necessity in investment in either employing an expert in computer forensic in the firms, or having part of their staff trained into this venture so as to help in detection of such cases should they arise.

1.6 USES OF COMPUTER FORENSICS

There are few areas of crime or dispute where computer forensics cannot be applied[2]. Law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field.

Computers may constitute a 'scene of a crime', for example with hacking or denial of service attacks or they may hold evidence in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking.

It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions.

More recently, commercial organisations have used computer forensics to their benefit in a variety of cases such as:

- Intellectual Property theft
- Industrial espionage
- Employment disputes

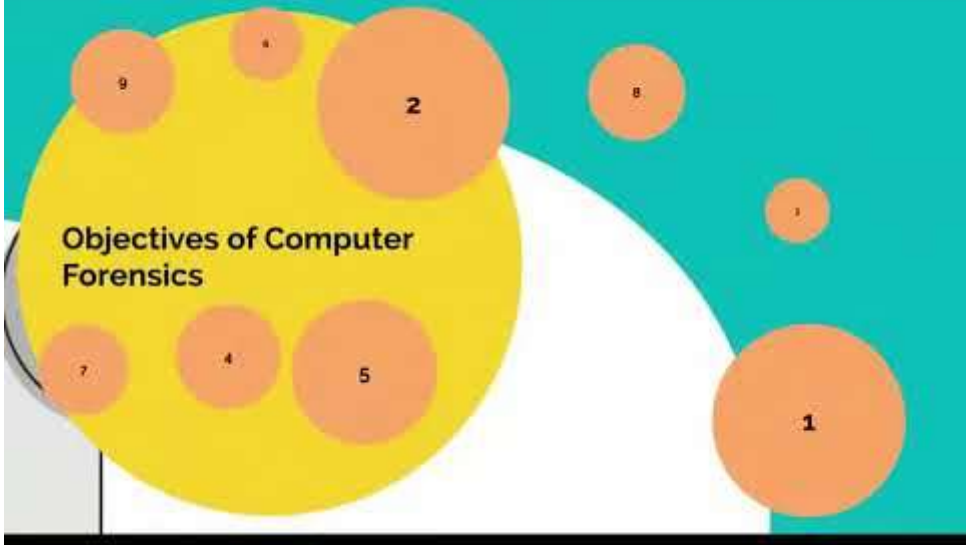
[9] http://computer-forensics.wikidot.com/

- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

1.7 OBJECTIVES OF COMPUTER FORENSICS

We all will agree to the fact that we are depending more on more on Information & Communication Technology(ICT) tools and internet for digital services to an extent that today we talk online using chat application, we depend on email to communicate with relatives and office, we stay in touch with our friends and update status using social engineering platforms like facebook, etc., we work online by staying connected to our office/ clinet using internet, we shop online, we teach online, we learn online, we submit our bill online today. Our dependency on Computer and Internet have increased so much that we are "online" most of the time. Therefore, there is an increased need of protecting our information from being misused by following Information security guidelines. However, if the security of our computer is compromised, computer forensics comes handy for post- incident investigation.

VIDEO LECTURE



The objectives of Computer forensics are to provide guidelines for:

- Following the first responder procedure and access the victim's computer after incident.
- Designing procedures at a suspected crime scene to ensure that the digital evidence obtained is not corrupted.

- Data acquisition and duplication.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Provide guidelines for analyzing digital media to preserve evidence, analysing logs and deriving conclusions, investigate network traffics and logs to correlate events, investigate wireless and web attacks, tracking emails and investigate email crimes.
- Producing computer forensic report which provides complete report on computer forensic investigation process.
- Preserving the evidence by following the chain of custody.
- Employing the rigorous procedures necessary to have forensic results stand up to scrutiny in a court of law.
- Presenting digital forensics results in a court of law as an expert witness.

1.8 ROLE OF FORENSICS INVESTIGATOR

Following are some of the important duties of a forensic investigator:

- Confirms or dispels whether a resource/network is compromised.
- Determine extent of damage due to intrusion.
- Answer the questions: Who, What, When, Where, How and Why.
- Gathering data in a forensically sound manner.
- Handle and analyze evidence.
- Prepare the report.
- Present admissible evidence in court.

VIDEO LECTURE

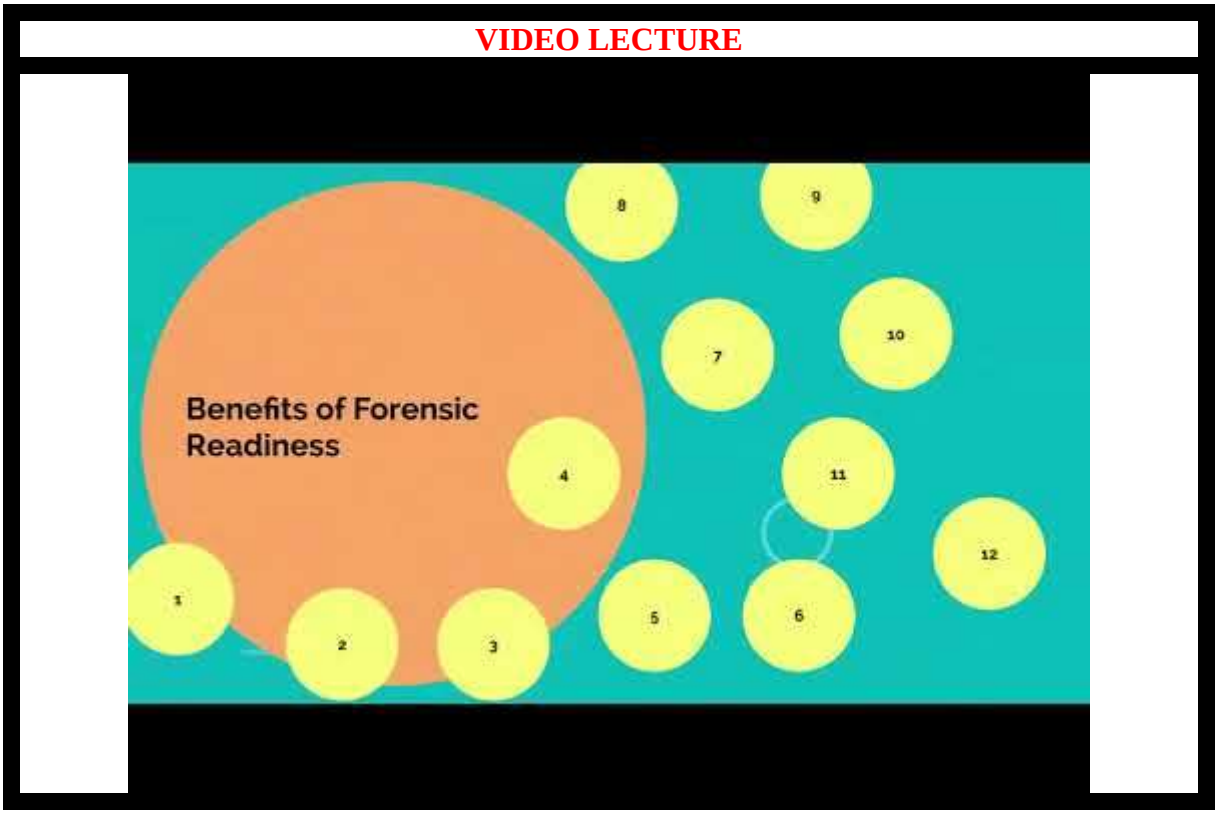
1.9 FORENSICS READINESS

There are several reasons for this field's growth; the most significant being that computers are everywhere[10]. You'd be hard pressed to find a household today without at least one computer. And it is not just computers that computer forensic examiners get involved with. Computer forensic examiners analyze all types of technical devices. Look around you while you walk down the street – people are on their cell phones, using iPods, PDAs, and text messaging. Computer forensic examiners analyze all of these electronic devices! Cyber forensics is a rapidly changing field. There are new technologies coming out daily that are becoming smaller, but storing more and more data. This leads to why cyber forensics is import. In computer related crimes, such identity fraud, it is becoming easier to hide data. With the proper analysis of digital evidence, better security can be made to protect computer users, but also catch those who are committing the crimes. Organizations have now realised the importance of being prepared to combat cyber criminals with their forensic readiness plan ready.

1.9.1 What is Forensics Readiness?

Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation[11]. In a business context there is the opportunity to actively collect potential evidence in the form of logfiles, emails, back-up disks, portable computers, network traffic records, and telephone records, amongst others. This evidence may be collected in advance of a crime or dispute, and may be used to the benefit of the collecting organisation if it becomes involved in a formal dispute or legal process.

VIDEO LECTURE



[10] http://colbycriminaljustice.wikidot.com/cyberforensics
[11] http://www.cpni.gov.uk/Documents/Publications/2005/2005008-TN1005_Forensic_readiness_planning.pdf

1.9.2 Goals of Forensic Readiness

Some of the important goals of forensics readiness are:

- to gather admissible evidence legally and without interfering with business processes;
- to gather evidence targeting the potential crimes and disputes that may adversely impact an organisation;
- to allow an investigation to proceed at a cost in proportion to the incident;
- to minimise interruption to the business from any investigation; and
- to ensure that evidence makes a positive impact on the outcome of any legal action.

1.9.3 Benefits of Forensic Readiness

Forensic readiness can offer an organisation the following benefits:

- evidence can be gathered to act in an organisation's defence if subject to a lawsuit;
- comprehensive evidence gathering can be used as a deterrent to the insider threat (throwing away potential evidence is simply helping to cover the tracks of a cyber-criminal);
- in the event of a major incident, an efficient and rapid investigation can be conducted and actions taken with minimal disruption to the business;
- a systematic approach to evidence storage can significantly reduce the costs and time of an internal investigation;
- a structured approach to evidence storage can reduce the costs of any court-ordered disclosure or regulatory or legal need to disclose data (e.g. in response to a request under data protection legislation);
- forensic readiness can extend the scope of information security to the wider threat from cyber crime, such as intellectual property protection, fraud, extortion etc;
- it demonstrates due diligence and good corporate governance of the company's information assets;
- it can demonstrate that regulatory requirements have been met;
- it can improve and facilitate the interface to law enforcement if involved;
- it can improve the prospects for a successful legal action;
- it can provide evidence to resolve a commercial dispute; and
- it can support employee sanctions based on digital evidence (for example to prove violation of an acceptable use policy)

1.9.4 Steps for Forensic Readiness Planning

The following ten steps describe the key activities in forensic readiness planning:

1. Define the business scenarios that require digital evidence;
2. Identify available sources and different types of potential evidence;
3. Determine the evidence collection requirement;
4. Establish a capability for securely gathering legally admissible evidence to meet the requirement;
5. Establish a policy for secure storage and handling of potential evidence;

6. Ensure monitoring is targeted to detect and deter major incidents;
7. Specify circumstances when escalation to a full formal investigation (which may use the digital evidence) should be launched;
8. Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence;
9. Document an evidence-based case describing the incident and its impact; and
10. Ensure legal review to facilitate action in response to the incident.

VIDEO LECTURE

The remainder of this section gives a brief description of each of the ten steps.

1. **Define the business scenarios that require digital evidence:** The first step in forensic readiness is to define the purpose of an evidence collection capability. The rationale is to look at the risk and potential impact on the business from the various types of crimes and disputes. What is the threat to the business and what parts are vulnerable? This is, in effect, a risk assessment, and is performed at the business level. The aim is to understand the business scenarios where digital evidence may be required and may benefit the organisation the event that it is required. In general the areas where digital evidence can be applied include:
    - reducing the impact from computer-related crime;
    - dealing effectively with court orders to release data;
    - demonstrating compliance with regulatory or legal constraints;
    - producing evidence to support company disciplinary issues;
    - supporting contractual and commercial agreements; and
    - proving the impact of a crime or dispute.

In assessing these scenarios, this step provides an indication of the likely benefits of being able to use digital evidence. If the identified risks, and the potential benefits of forensic readiness, suggest a good return on investment is achievable, then an organisation needs to consider what evidence to gather for the various risk scenarios.

2. **Identify available sources and different types of potential evidence:** The second step in forensic readiness is for an organisation to know what sources of potential evidence are present on, or could be generated by, their systems and to determine what currently happens to the potential evidence data. Computer logs can originate from many sources. The purpose of this step is to scope what evidence may be available from across the range of systems and applications in use. Some basic questions need to be asked about possible evidence sources to include.
    - Where is data generated?
    - What format is it in?
    - How long is it stored for?
    - How is it currently controlled, secured and managed?
    - Who has access to the data?
    - How much is produced?
    - Is it archived? If so where and for how long?
    - How much is reviewed?
    - What additional evidence sources could be enabled?
    - Who is responsible for this data?
    - Who is the formal owner of the data?
    - How could it be made available to an investigation?
    - What business processes does it relate to?
    - Does it contain personal information?

    Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving & auditing and retrieval. But this is not the only means of communication used over the internet, there is also instant messaging, web-based email that bypasses corporate email servers, chat-rooms and newsgroups, even voice over the internet. Each of these may need preserving and archiving. The range of possible evidence sources includes:
    - equipment such as routers, firewalls, servers, clients, portables, embedded devices etc;
    - application software such as accounting packages etc for evidence of fraud, erp packages for employee records and activities (e.g. in case of identity theft), system and management files etc;
    - monitoring software such as intrusion detection software, packet sniffers, keyboard loggers, content checkers, etc;
    - general logs such as access logs, printer logs, web traffic, internal network logs, internet traffic, database transactions, commercial transactions etc;
    - other sources such as: cctv, door access records, phone logs, pabx data etc; and
    - back-ups and archives.

3. **Determine the Evidence Collection Requirement:** It is now possible to decide which of the possible evidence sources identified in step 2 can help deal with the crimes and disputes identified in step 1 and whether further ways to gather evidence are required. This is the evidence collection requirement. The purpose of this step is to produce an evidence requirement statement so that those responsible for managing the business risk can communicate with those running and monitoring information systems through an agreed requirement for evidence. One of the key benefits of this step is the bringing together of IT with the needs of corporate security. IT audit logs have been traditionally configured by systems administrators independently of corporate policy and where such a policy exists there is often a significant gap between organisational security objectives and the 'bottom-up' auditing actually implemented. The evidence collection requirement is moderated by a cost benefit analysis of how much the required evidence will cost to collect and what benefit it provides (see above). The critical question for successful forensic readiness is what can be performed cost effectively. By considering these issues in advance and choosing storage options, auditing tools, investigation tools, and appropriate procedures it is possible for an organisation to reduce the costs of future forensic investigations.
4. **Establish a capability for securely gathering legally admissible evidence to meet the requirement:** At this point the organisation knows the totality of evidence available and has decided which of it can be collected to address the company risks and within a planned budget. With the evidence requirement understood, the next step is to ensure that it is collected from the relevant sources and that it is preserved as an authentic record. At this stage legal advice is required to ensure that the evidence can be gathered legally and the evidence requirement can be met in the manner planned. For example, does it involve monitoring personal emails, the use of personal data, or 'fishing trips1 ' on employee activities? In some countries, some or all of these activities may be illegal. Relevant laws, in the areas of data protection, privacy and human rights, will inevitably constrain what can actually be gathered. Some of the guidelines are:
    - monitoring should be targeted at specific problems.
    - it should only be gathered for defined purposes and nothing more; and
    - staff should be told what monitoring is happening except in exceptional circumstances.

    Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage. As well as preventative measures such as secure rooms and swipe card access it is also prudent to have records of who has access to the general location and who has access to the actual machines containing evidence. Any evidence or paperwork associated with a specific investigation should be given added security by, for example, storing in a safe. Additional security of logs can also be achieved through the use of WORM storage media.
5. **Establish a policy for secure storage and handling of potential evidence:** The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required. It concerns the long-term or off-line storage of information that might be required for evidence at a later date. A policy for

secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence. In the parlance of investigators this is known as continuity of evidence (in the UK) and chain of custody (in the US). The continuity of evidence also includes records of who held, and who had access to, the evidence (for example from swipe control door logs). A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office. The problem it addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability? The current edition broadens the scope to all information management systems, Ad hoc opportunistic searches, without justification, for potentially incriminating activities or communication such as those where information is transmitted over networks such as email systems for example. It points out that methods of storage, hardware reliability, operation and access control, and even the programs and source code, may be investigated in order to determine admissibility. A closely related international standard is being developed as ISO 15801. The required output of this step is a secure evidence policy. It should document the security measures, the legal advice and the procedural measures used to ensure the evidence requirement is met. Upon this document rests the likely admissibility and weight of any evidence gathered.

6. **Ensure monitoring and auditing is targeted to detect and deter major incidents:** In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner. This is directly analogous to Intrusion Detection Systems (IDS), extended beyond network attack to a wide range of behaviours that may have implications for the organisation. It is all very well collecting the evidence. This step is about making sure it can be used in the process of detection. By monitoring sources of evidence we can look for the triggers that mean something suspicious may be happening. The critical question in this step is when should an organisation be suspicious? A suspicious event has to be related to business risk and not couched in technical terms. Thus the onus is on managers to explain to those monitoring the data what they want to prevent and thus the sort of behaviour that IDS might be used to detect for example. This should be captured in a ‘suspicion’ policy that helps the various monitoring and auditing staff understand what triggers should provoke suspicion, who to report the suspicion to, whether heightened monitoring is required, and whether any additional security measures should be taken as a precaution. Each type of monitoring should produce a proportion of false positives. The sensitivity of triggers can be varied as long as the overall false positive rate does not become so high that suspicious events cannot be properly reviewed. Varying triggers also guards against the risk from someone who knows what the threshold on a particular event is and makes sure any events or transactions he wishes to hide are beneath it.
7. **Specify circumstances when escalation to a full formal investigation (which may use digital evidence) is required:** Some suspicious events can be system generated,

such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness. Each suspicious event found in step 6 needs to be reviewed. Either an event will require escalation if it is clearly serious enough, or it will require enhanced monitoring or other precautionary measures, or it is a false positive. The purpose of this step is to decide how to react to the suspicious event. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed. The decision criteria should be captured in an escalation policy that makes it clear when a suspicious event becomes a confirmed incident. At this point an investigation should be launched and policy should indicate who the points of contact are (potentially available on a 24x7 basis) and who else needs to be involved. As with steps 3 and 6, the network and IT security managers and the non-IT managers need to understand each other's position. What level of certainty or level of risk is appropriate for an escalation? What strength of case is required to proceed? A preliminary business impact assessment should be made based on whether any of the following are present:

- evidence of a reportable crime
- evidence of internal fraud, theft, other loss
- estimate of possible damages (a threshold may induce an escalation trigger)
- potential for embarrassment, reputation loss
- any immediate impact on customers, partners or profitability
- recovery plans have been enacted or are required; and
- the incident is reportable under a compliance regime.

8. **Train staff, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence:** A wide range of staff may become involved in a computer security incident. The aim of this step is to ensure that appropriate training is developed to prepare staff for the various roles they may play before, during and after an incident. It is also necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence. There will be some issues relevant to all staff if they become involved in an incident. The following groups will require more specialised awareness training for example:
    - the investigating team;
    - corporate HR department;
    - corporate PR department (to manage any public information about the incident);
    - 'owners' of business processes or data;
    - line management, profit centre managers;
    - corporate security;
    - system administrators;
    - IT management;
    - legal advisers; and
    - senior management (potentially up to board level).

    At all times those involved should act according to 'need to know' principles. They should be particularly aware whether any staff, such as 'whistle blowers' and

investigators, need to be protected from possible retaliation by keeping their names and their involvement confidential. Training may also be required to understand the relationships and necessary communications with external organisations that may become involved.

9. **Present an evidence-based case describing the incident and its impact:** The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible. The questions go along the lines of who, what, why, when, where and how. Credibility is provided by evidence and a logical argument. The purpose of this step is to produce a policy that describes how an evidence-based case should be assembled. A case file may be required for a number of reasons:
    - to provide a basis for interaction with legal advisers and law enforcement;
    - to support a report to a regulatory body;
    - to support an insurance claim;
    - to justify disciplinary action;
    - to provide feedback on how such an incident can be avoided in future;
    - to provide a record in case of a similar event in the future (supports the corporate memory so that even if there are changes in personnel it will still be possible to understand what has happened); and
    - to provide further evidence if required in the future, for example if no action is deemed necessary at this point but further developments occur.
10. **Ensure legal review to facilitate action in response to the incident:** At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions. Legal advisers should be able to advise on the strength of the case and suggest whether additional measures should be taken; for example, if the evidence is weak is it necessary to catch an internal suspect red handed by monitoring their activity and seizing their PC? Any progression to a formal action will need to be justified, cost-effective and assessed as likely to end in the company's favour. Although the actual decision of how to proceed will clearly be post-incident, considerable legal preparation is required in readiness. Legal advisors should be trained and experienced in the appropriate cyberlaws and evidence admissibility issues. They need to be prepared to act on an incident, pursuant to the digital evidence that has been gathered and the case presented in step 9. Legal advice should also recognise that the legal issues may span legal jurisdictions e.g. states in the US, member states in the EU. Advice from legal advisers will include:
    - any liabilities from the incident and how they can be managed;
    - finding and prosecuting/punishing (internal versus external culprits);
    - legal and regulatory constraints on what action can be taken;
    - reputation protection and PR issues;
    - when/if to advise partners, customers and investors;
    - how to deal with employees;
    - resolving commercial disputes; and
    - any additional measures required.

1.10 SUMMARY

1. Computer forensics is the practice of collecting, analysing and reporting on digital data in a way that is legally admissible.
2. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel.
3. Computer crime, or cybercrime, is any crime that involves a computer and a network.
4. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyberwarfare.
5. The ancient Chinese used fingerprints to identify business documents.
6. Sir Francis Galton established the first system for classifying fingerprints.
7. International Association of Computer Investigative Specialists(IACIS) is an international non-profit corporation composed of volunteer computer forensic professionals dedicated to training and certifying practitioners in the field of forensic computer science.
8. The First FBI Regional Computer Forensic Laboratory established in 2000 at San Diego.
9. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics.
10. Forensic readiness is the ability of an organisation to maximise its potential to use digital evidence whilst minimising the costs of an investigation.
11. Monitoring should be targeted at specific problems.
12. Physical security of data such as back-up files or on central log servers is important from the data protection point of view, and also for secure evidence storage.
13. A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.
14. In addition to gathering evidence for later use in court, evidence sources can be monitored to detect threatened incidents in a timely manner.
15. Some suspicious events can be system generated, such as by the rule-base of an IDS, or the keywords of a content checker, and some will be triggered by human watchfulness.
16. The decision as to whether to escalate the situation to management will depend on any indications that a major business impact is likely or that a full investigation may be required where digital evidence may be needed.
17. It is necessary to ensure that staff is competent to perform any roles related to the handling and preservation of evidence.
18. The aim of an investigation is not just to find a culprit or repair any damage. An investigation has to provide answers to questions and demonstrate why those answers are credible.
19. At certain points during the collating of the cyber-crime case file it will be necessary to review the case from a legal standpoint and get legal advice on any follow-up actions.

1.11 CHECK YOUR PROGRESS

1. Fill in the blanks

i. _____ was one of the first applications of forensics.

ii. FBI Magnetic Media program was later renamed to _____.

iii. _____is provided by evidence and a logical argument.

iv. At all times those involved should act according to _____principles.

v. IACIS stands for _____.
vi. The first step in forensic readiness is to define the _____of an evidence collection capability.
vii. It is not just the content of emails, documents and other files which may be of interest to investigators but also the _____associated with those files.
viii. IDS stands for _____.
ix. The decision criteria should be captured in an _____ policy that makes it clear when a suspicious event becomes a confirmed incident.
x. IOCE stands for International_____.

2. State true or false

i. Cybercrime, is any crime that involves a computer and a network.
ii. Computer based crime is criminal activity that is conducted purely on computers, for example cyber-bullying or spam.
iii. The goal of forensic readiness is to gather admissible evidence legally and without interfering with business processes.
iv. FBI Magnetic Media program started in 1994.
v. IOCE aims to bring together organizations actively engaged in the field of digital and multimedia evidence to foster communication and cooperation as well as to ensure quality and consistency within the forensic community.
vi. Logs can originate from only one source in a computer.
vii. The range of possible evidence sources includes equipment such as routers, firewalls, servers, clients, portables, embedded devices etc.
viii. Email is an obvious example of a potential rich source of evidence that needs careful consideration in terms of storage, archiving and auditing and retrieval.
ix. Staff should not be told what monitoring is happening except in exceptional circumstances.

1.12 ANSWERS TO CHECK YOUR PROGRESS

1. Fill in the blanks
   i. Fingerprinting
   ii. Computer Analysis and Response Team (CART).
   iii. Credibility
   iv. need to know
   v. International Association of Computer Investigative Specialists
   vi. purpose
   vii. metadata
   viii. Intrusion Detection Systems.
   ix. escalation
   x. International Organization on Computer Evidence.
2. State true or false
   i. True
   ii. True
   iii. True
   iv. False

v. True
vi. False
vii. True
viii. True
ix. False

1.13 SUGGESTED READINGS

1. Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified ExaminorStudy Guide.* Wiley Publishing Inc.

2. Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations.* Cengage Learning.

3. Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic.* CERT Training and Education.

4. Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Retrieved Sep. 26, 2015, from http://kb.cu-portland.edu/Password+Security

1.14 MODEL QUESTIONS

1. What are the four stages of computer forensic process?
2. What are the uses of computer forensics?
3. What are the objectives of computer forensics?
4. What is the role of a forensics investigator?
5. What is forensics readiness plan?
6. What are the benefits of forensic readiness?
7. What are various steps involved in forensic readiness planning?
8. What is continuity of evidence?

References, Article source and Contributors

1. Edson, J. (2011, July 25). *A Brief History Of Forensic Science*. Retrieved Oct. 04, 2015, from riaus.org.au: http://riaus.org.au/articles/a-brief-history-of-forensic-science/

2. Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Retrieved Oct. 03, 2015, from OpenSourceForU: http://opensourceforu.efytimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/

3. *Introduction to computer forensics*. (n.d.). Retrieved Oct. 03, 2015, from Forensic Control: https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

4. *Introduction to computer forensics*. (n.d.). Retrieved Oct. 03, 2015, from Forensic Control: https://forensiccontrol.com/resources/beginners-guide-computer-forensics/

5. Morton, T. (2013, Sep. 13). *Types of investigations*. Retrieved Oct. 04, 2015, from Introduction to Digital Forensics: https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics/Types

6. Peterson, D. (2015, July 06). *Computer Forensics Miami*. Retrieved Oct. 03, 2015, from computer-forensics.wikidot: http://computer-forensics.wikidot.com/

7. Rowlingson, R. (2005). *An Introduction to Forensic Readiness Planning*. available under Open Government Licence http://www.nationalarchives.gov.uk/doc/open-government-licence/version/2/, Centre for the Protection of National Infrastructure.

8. The National Archives. (2011). *Digital Continuity to Support Forensic Readiness*. Retrieved Oct. 04, 2015, from nationalarchives: http://www.nationalarchives.gov.uk/documents/information-management/forensic-readiness.pdf

9. Wheelbarger, S. (2009, Aug. 27). *CyberForensics*. Retrieved Oct. 04, 2015, from Wikidot: http://colbycriminaljustice.wikidot.com/cyberforensics

EXPERT PANEL

Dr. Jeetendra Pande, Associate Professor- Computer Science, School of Computer Science & IT, Uttarakhand Open University, Haldwani

Dr. Ajay Prasad, Sr. Associate Professor, University of Petroleum and Energy Studies, Dehradun

Dr. Akashdeep Bharadwaj, Professor, University of Petroleum and Energy Studies, Dehradun

Mr. Sridhar Chandramohan Iyer, Assistant Professor- Universal College of Engineering, Kaman, Vasai, University of Mumbai

Mr. Rishikesh Ojha, Digital Forensics and eDiscovery Expert

Ms. Priyanka Tewari, IT Consultant

Mr. Ketan Joglekar, Assistant Professor, GJ College, Maharastra

Dr. Ashutosh Kumar Bhatt, Associate Professor, Uttarakhand Open University, Haldwani

Dr. Sangram Panigrahi, Assistant Professor, Siksha 'O' Anusandhan,, Bhubaneswar

This MOOC has been prepared with the support of