Forensic Analysis for Computer Systems

Plan of the course:

1. Introduction
2. Evolution of Computer Forensics
3. Computer Forensics process
4. Types of Computer Forensics
5. Forensics Readiness

Course 1: Introduction

1.1 Overview
1.2 Definitions
1.3 Computer forensics history and scope
1.4 Cybercrime
1.5 Objectives and Advantages of Computer forensics

FORENSIC

1.1 Overview

Historically, the Internet and its services are experiencing periods of great progress and improvement. These improvements have created opportunities for :

- ✓ E-commerce,
- ✓ Distance learning,
- ✓ Cloud computing,
- ✓ Education,
- ✓ Research,
- ✓ And public discourse.

1.1 Overview

Also, this worldwide connectivity has greatly improved our :

- ✓ life,
- ✓ work,
- ✓ and communications

Surpassing the traditional limitations of telecommunication systems.

For example:

The increased automation of the printing process and the introduction of digital mass media and storage greatly enhanced information sharing by increasing the availability, integrity, and confidentiality of huge data sources.

1.1 Overview

Unfortunately, this digital progress has several drawbacks:

- ✓ It has led to criminal innovation
- ✓ And created a new forum for both terrorist activities and criminal behaviours.

It has been further increased by adapting new technologies like:

- ✓ wireless communications,
- ✓ social networking,
- ✓ and smart phones,

which has more complicated the investigative scope. This issue has led to exacerbating the vulnerabilities of government, organizations, institutions, and individuals alike.

1.2 Definitions

What's Computer forensics ?

→ **Digital forensics is** the art of recovering and analysing the contents found on digital devices such as:

- ✓ Desktops,
- ✓ Notebooks/netbooks,
- ✓ Tablets, smartphones, etc.

→ However, with the augmentation of cybercrime assaults, and the increased adoption of digital devices, this branch of forensics has gained significant importance in the recent past, giving new solutions in recovery and analysis of digital evidences during criminal investigations.

1.2 Definitions

What's Computer forensics ?

→ **Forensic analysis** is a science interested in the search for evidence in digital media to understand behavior, remedy an incident and help make informed decisions.

→ It is the process of using scientific techniques during the identification, collection, examination and reporting the evidence to the court. This evidence is traces, digital artifacts* that provide information that, when put together, provides a factual scenario of events and answers questions that the plaintiff may have. Forensic analysis is also called digital forensics, inforensics, computer forensics or digital investigation.

*Windows artifacts which focus on the events that can be derived by the system such as Windows registry, file recovery, volume shadow copy (VSC), Windows volume shadow service (VSS), and Windows event logs. User artifacts in which they focus on the unique activity of the system user such as deleted data, network and system information, user accounts, event logs and more.

1.3 Computer forensics History and scope

Here are important landmarks from history of Computer Forensics

- ✓ Hans Gross (1847-1915): first use of scientific study to head criminal investigations.
- ✓ FBI (1932): set up a laboratory to offer forensics services to all field agents and other law authorities across the usa.
- ✓ In 1978 the first computer crime was recognized in the Florida Computer Crime Act.
- ✓ Francis Galton (1982 - 1911): Conducted first recorded study of fingerprints
- ✓ In 1992, the term Computer Forensics was used in academic literature.
- ✓ In 1995 International Organization on Computer Evidence (IOCE) was formed.
- ✓ In 2000, the First FBI Regional Computer Forensic Laboratory established.
- ✓ In 2002, Scientific Working Group on Digital Evidence (SWGDE) published the first book about digital forensic called "Best practices for Computer Forensics".
- ✓ In 2010, Simson Garfinkel identified issues facing digital investigations.

1.3 Computer forensics History and scope

In recent time, commercial organizations have used computer forensics in following cases:

- ✓ Intellectual property theft.
- ✓ Industrial espionage.
- ✓ Employment secret disputes.
- ✓ Fraud investigations.
- ✓ Inappropriate use of Internet and emails in the workplace.
- ✓ Forgeries related matters.
- ✓ Bankruptcy investigations.

1.3 Computer forensics History and scope (Cont.)

The scope of computer forensics is not limited to investigating a crime only. Apart from this, computer forensics can be used for:

- ✓ Data recovery
- ✓ Log monitoring
- ✓ Data acquisition (from the retired or damaged devices)
- ✓ Achieve the compliance needs

1.4 Cyber Crime

→ Computer crime, 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 defines 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)".

1.4 Cyber Crime

→ Such crimes may menace a nation's security and financial health, 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 most types of digital investigation centre on some form of computer crime. This sort of crime can take two forms: *computer-based crime and computer-facilitated crime.*

1.4 Cyber Crime (Cont.)

→ *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, deep-fake Multimedia).

→ *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 a 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 to incorporate (or private) settings to recover lost information or to rebuild the activities of employees.

1.4 Cyber Crime (Cont.)

A Computer forensic scenario

→ Suppose Mr X is the computer forensics investigator* in Odisha and he has been appointed to inspect data-stealing case in an MNC in Bhubaneswar.

→ The general manager of the organization has confidence in that some of his employees are involved in the case including the network crack and the transfer of the confidential data.

*Investigator needs extensive knowledge of computer hardware and software, including operating systems, file systems, and cryptographic algorithms. Evidence has to be identified among normal files, and may be found in slack space, unallocated space, registries, hidden files, encrypted files, password-protected files, system logs, etc. Evidence can be found on any number of media sources such as hard drive, CD/DVD, mobile phones, flash drives etc.

1.4 Cyber Crime (Cont.)

A Computer forensic scenario

→ Mr X has started his investigation, Analyze, Evaluate the case and collected the evidence and then he submitted his final report to the Authority (Court Law).

→ According to the report, four employees were found accountable for data theft/data-stealing. Based on this report, a case has been lodged against them.
In the situation mentioned here, the organization was the client, Mr X was the service provider (i.e. investigator) and the service that was being provided is called *computer forensics* & *digital investigation services.*

1.5 Objectives and advantages of Computer forensics

Here are the essential objectives of using Computer forensics:

* It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.
* It helps to postulate the motive behind the crime and identity of the main culprit.
* Designing procedures at a suspected crime scene which helps us 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.
* Helps us to identify the evidence quickly, and also allows us to estimate the potential impact of the malicious activity on the victim.
* Producing a computer forensic report which offers a complete report on the investigation process.
* Preserving the evidence by following the chain of custody.

1.5 Advantages of Computer forensics

There are several advantages to conducting a digital investigation:

For a client, it may be:

- to find answers to the questions he was asking himself,
- to make informed decisions or judgments based on factual evidence,
- to resume the company's activity serenely.

More generally, the community potentially gets:

- the discovery of new Indicators of Compromise (IOC)
- the consolidation of the content of Threat Intelligence, arising from the first point,
- the prevention of attacks in other contexts arising from the first two points.

In brief

→ Computer forensics is the process of preservation, identification, extraction, and documentation of computer or digital evidence* which can be used by the court of law.

→ It's a science of finding evidence from digital media like : Computers, mobile phones, servers or networks. It provides the forensic team with the best technics and tools to solve complicated digital-related cases.

→ Computer or Digital forensics helps the forensic team to analyse, inspect, identify and preserve the digital evidence residing on various types of electronic devices.

→ The large scale use of Windows based systems has made Windows artifacts critical and of great importance for digital forensic examiners. The artifacts can be interpreted as system and user-based activities. It includes file system information, network share information, operating system information, time-zone information, user accounts and Windows event logs.

→ The practice of collecting, analyzing and reporting digital evidence in a way legally admissible in court is known as digital or computer forensics and the experts who practice this kind of science are known as forensic examiners or investigators. However, the acquisition, analysis, and reporting of the digital evidence depends on the nature of the crime scene, types of available evidence and the digital forensic tools employed.

* Digital evidence is information of value to an investigation that is stored and transmitted in a digital form, search for evidences should also consider physical evidence in a non-digital format that may be of value e.g. notebooks, pieces of paper with potential passwords.

What is IoC ?

An indicator of compromise is **digital evidence that an attack has already occurred**. An indicator of an attack is evidence that an attack is likely to occur. For example, a phishing campaign is an indicator of attack because there's no evidence that the attacker has breached the company

Indicators of compromise (IOCs) serve as forensic evidence of potential intrusions on a host system or network. These artifacts enable information security (InfoSec) professionals and system administrators to detect intrusion attempts or other malicious activities. Security researchers use IOCs to better analyze a particular malware's techniques and behaviors. IOCs also provides actionable threat intelligence that can be shared within the community to further improve an organization's incident response and remediation strategies.

Some of these artifacts are found on event logs and time stamped entries in the system, as well as on its applications and services. InfoSec professionals and IT/system administrators also employ various tools that monitor IOCs to help mitigate, if not prevent, breaches or attacks.

Here are some indicators of compromise information security professionals and system administrators watch out for:

- Unusual traffic going in and out of the network
- Unknown files, applications, and processes in the system
- Suspicious activity in administrator or privileged accounts
- Irregular activities such as traffic in countries an organization doesn't do business with
- Dubious log-ins, access, and other network activities that indicate probing or brute force attacks
- Anomalous spikes of requests and read volume in company files
- Network traffic that traverses in unusually used ports
- Tampered file, Domain Name Servers (DNS) and registry configurations as well as changes in system settings, including those in mobile devices
- Large amounts of compressed files and data unexplainably found in locations where they shouldn't be

What is threat intelligence ?

Threat intelligence is **data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors**. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.
Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets.

What is compliance?

Compliance is the state of being in accordance with established guidelines or specifications, or the process of becoming so. Software, for example, may be developed in compliance with specifications created by a standards body, and then deployed by user organizations in compliance with a vendor's licensing agreement.
The definition of can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation.
Compliance is a prevalent business concern, partly because of an ever-increasing number of regulations that require companies to be vigilant about maintaining a full understanding of their regulatory requirements for compliance. To adhere to compliance standards, an organization must follow requirements or regulations imposed by either itself or government legislation.