

Digital Forensics

Lecture 10

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

- **Today, computers are used the world over. The pervasiveness of computers has led to an ever-increasing number of computer-related court cases, such as electronic commerce disputes and cybercrimes. In the process of judging or handling disputes and criminal cases, a new form of litigation evidence has emerged, namely, digital evidence. The characteristics that distinguish digital evidence and digital forensics from traditional physical evidence and forensic methods pose new research topics in the field of law and computer science.**
- **This document describes the digital forensic process and presents the technologies and tools used in digital forensics.**

Objectives

- **Upon completion of this course, you will be able to:**
 - ❑ **Describe the process of digital forensics.**
 - ❑ **Describe digital forensic technologies.**
 - ❑ **Use digital forensic tools.**

Cybercrime

- **Definition:**

- ❑ In violation of legal regulations, a bad actor deliberately:

- Invades a computer information system or compromises the functionality of the system and its related data and applications

- Produces or disseminates computer viruses

- Affects the normal operation of a system or causes detrimental effects

- **Cybercrimes usually take two forms:**

- ❑ Use of computers to store information related to criminal activities

- ❑ Direct use of computers as a crime tool to launch criminal activities



Characteristics of Cybercrimes

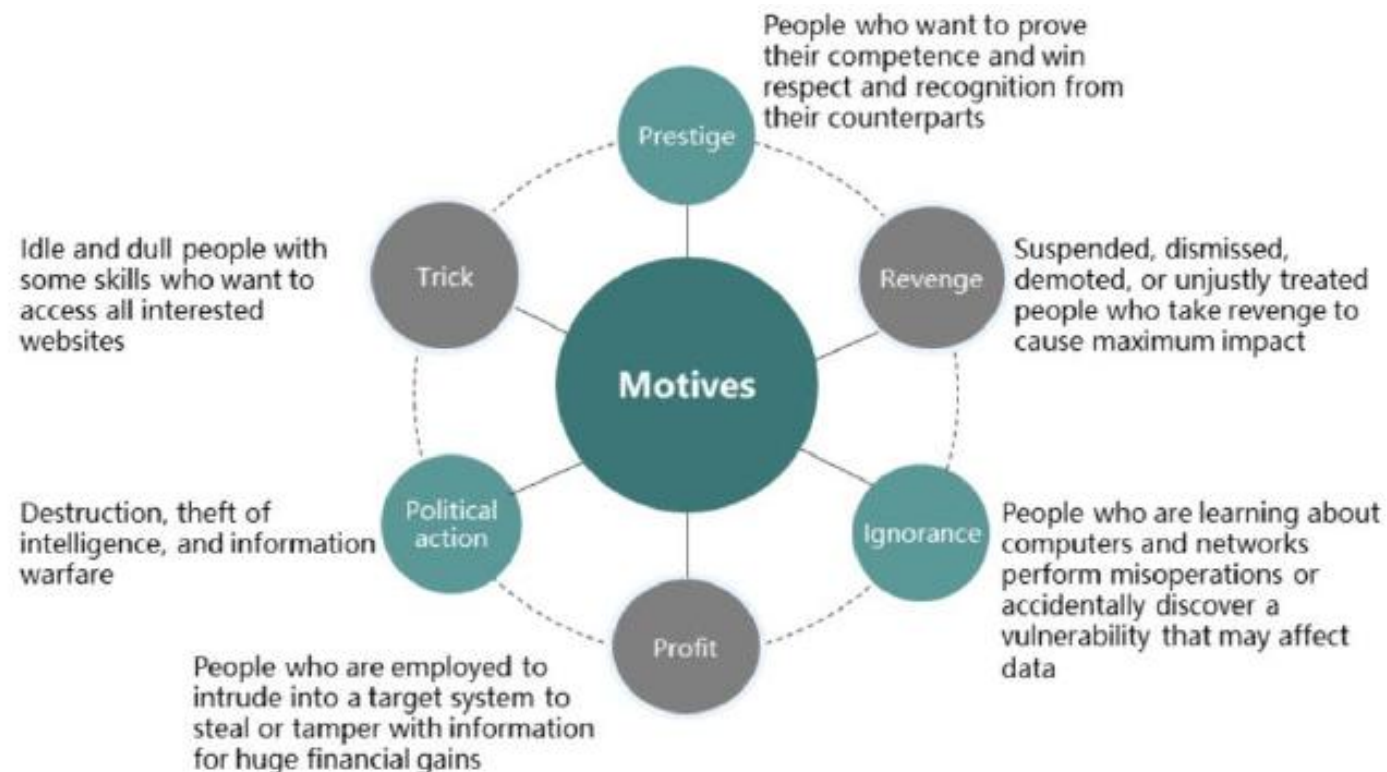
- Over the past decade or so, the number of cybercrimes have risen year on year.

Cybercrimes generally have the following characteristics:



Cybercrime Motives

- The motives of cybercrime are complicated and diverse.



Forms of Cybercrime

- Cybercrimes take various forms. Common forms are listed as follows:



Overview of Digital Forensics

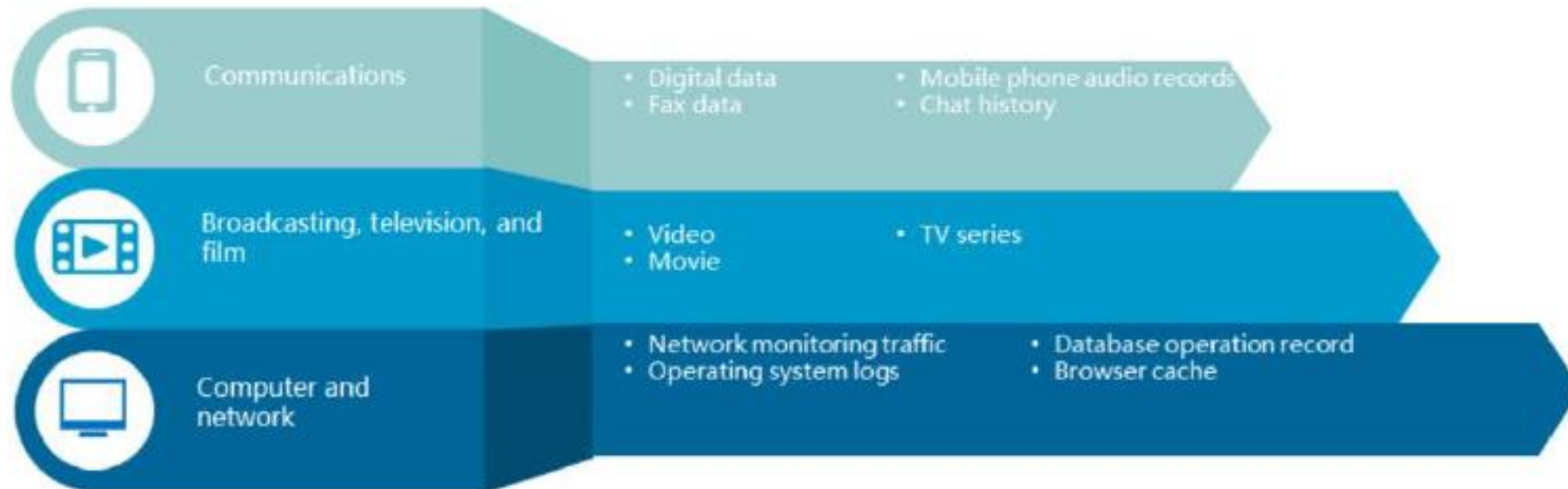
- **Digital evidence**

- **Digital evidence is information stored or transmitted in binary form during the operation of a computer or computer system and is used in a court case.**
- **Digital evidence is also known as electronic evidence and computer evidence.**

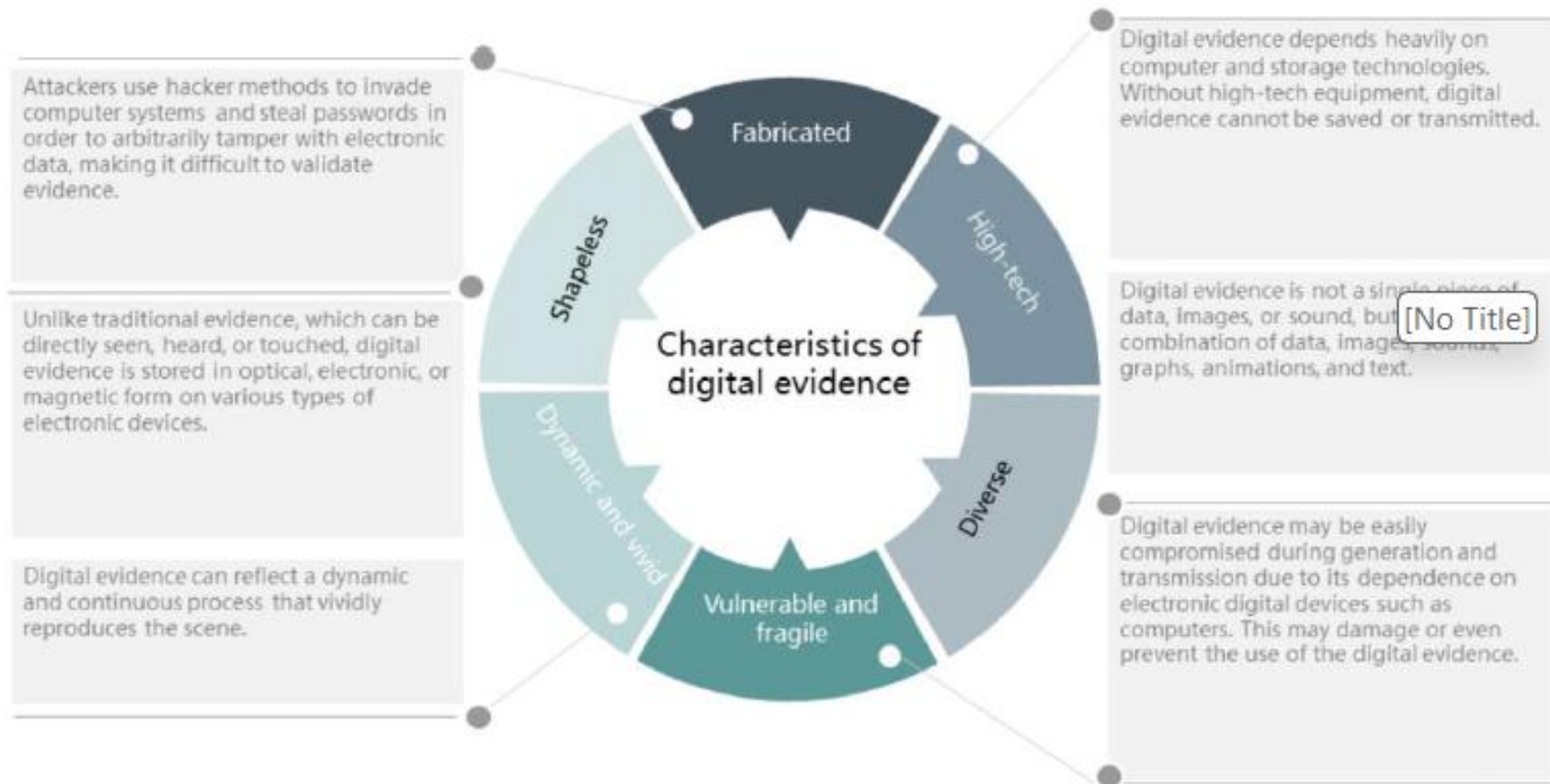


Analysis of System Time Change Events

- Common digital evidence in judicial practices falls into three categories:
 - ❑ Digital evidence related to modern communications technologies
 - ❑ Digital evidence related to other modern information technologies, such as broadcasting, television , and film
 - ❑ Digital evidence related to computer technologies or network technologies



Characteristics of Digital Evidence



Concept of Computer Forensics

- Computer forensics is also known as digital forensics or electronic forensics.

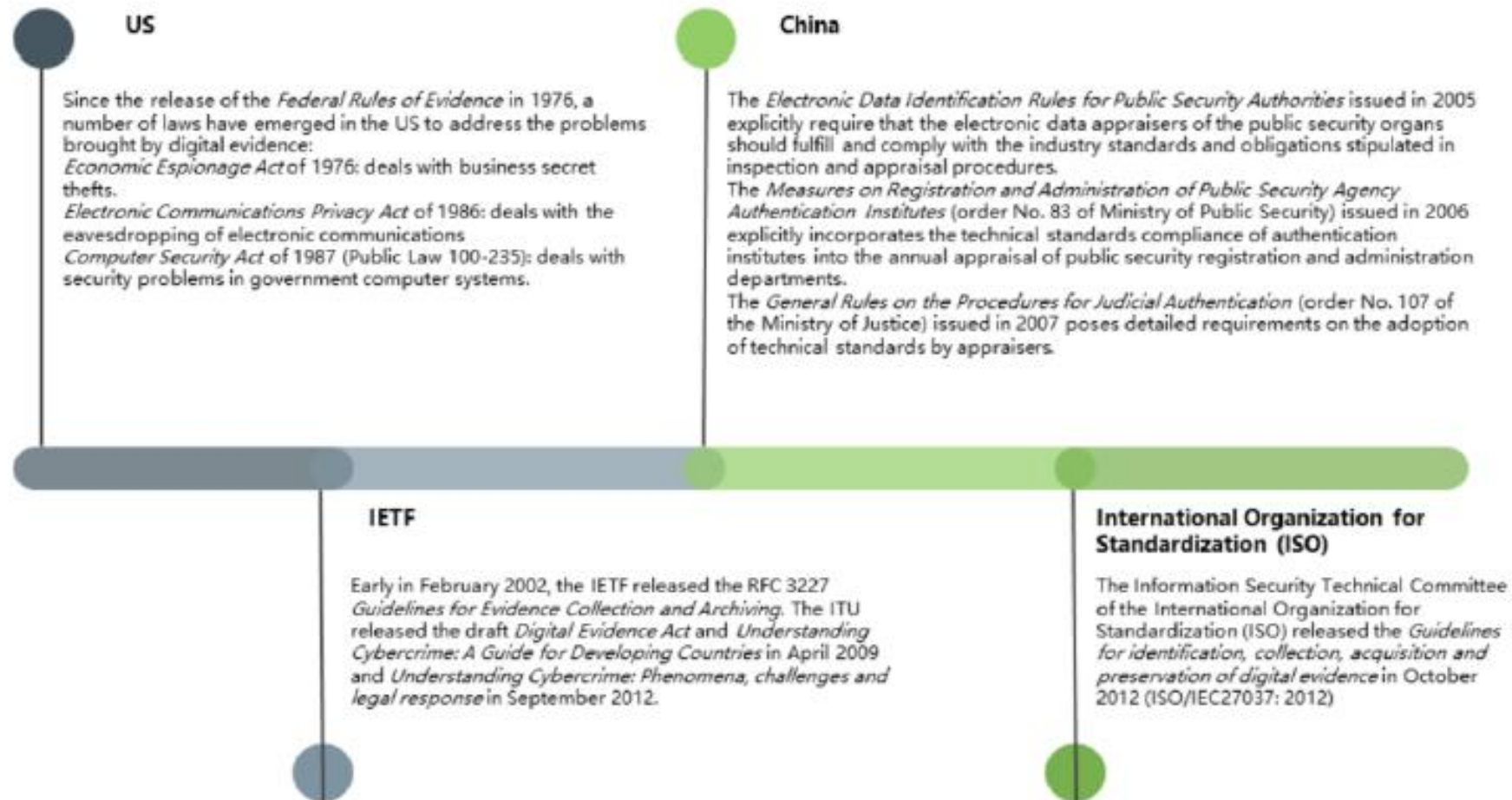
Definition:

- Computer forensics refers to the process of confirming, protecting, extracting, archiving, and presenting at a court digital evidence that exists in computers and related peripherals. This evidence must be reliable, persuasive, and acceptable by the court.



Chapter
10

Regulations & Standards for Digital Forensics



Status & Trend of Digital Forensics



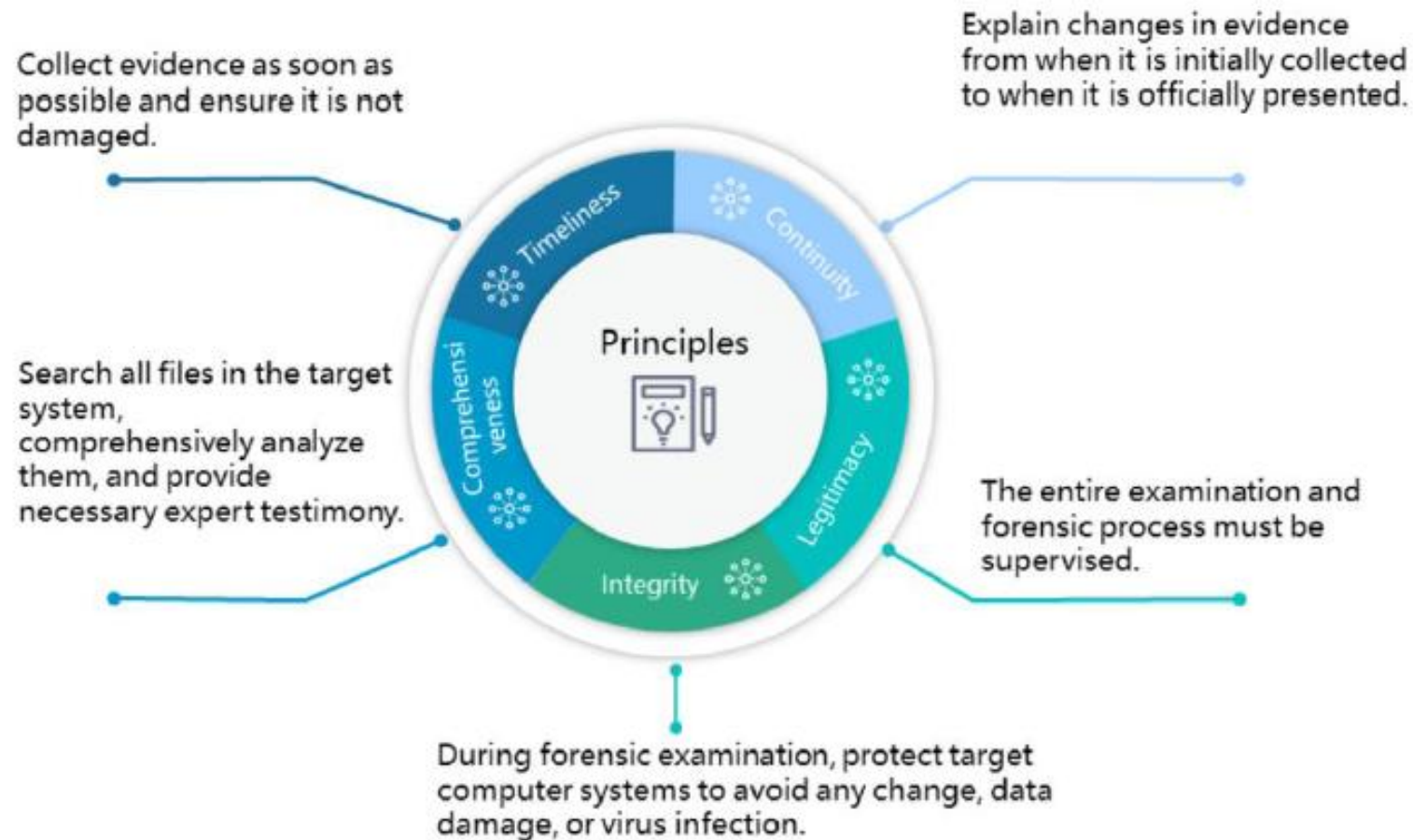
Status:

1. China was a late adopter of computers and therefore relevant laws and regulations are insufficient.
2. Academic research on cybercrimes mainly focuses on its characteristics, preventive measures, and impact on people. Forensics technologies are no longer sufficient to combat cybercrimes or to protect network and information security.
3. China must independently develop computer forensic tools and software that can meet its specific requirements and comprehensively check computers and network systems.

Trend:

1. Integration of other theories and technologies (such as AI, machine learning, neural network, data mining, and information security technologies) into forensic technologies
2. Specialization and automation of forensic tools
3. Sufficient information reserved during network protocol design for potential forensic activities

Principles of Digital Forensics

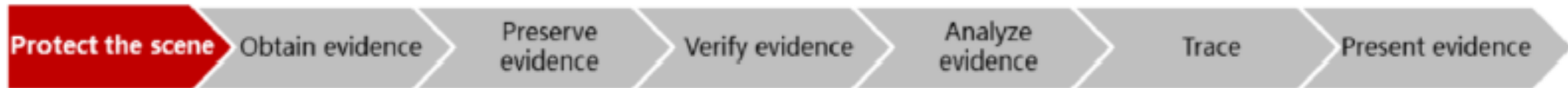


Digital Forensic Process

- According to the characteristics of digital evidence, it is essential to collect evidence as soon as possible during digital forensics to ensure that it has not been damaged. Digital forensics usually involves the following steps:



Protecting the Scene



- Before digital forensics is performed, freeze the target computer system so that the criminal suspect cannot damage evidence. Avoid any changes to system settings, damage to hardware or data, or virus infection.
- Avoid changes in evidence. However, if changes occur from when evidence is initially collected to when it is officially presented, they must be explained. In addition, the whole process of digital forensics must be supervised.



Chapter

10

Obtaining Evidence



- Search all files in the target system, including existing normal files, deleted files that still exist on disks (for example, files not overwritten by new files), hidden files, password-protected files, and encrypted files.
- Forensic tools:

- ☐ Hardware tools
- ☐ Software tools



Hardware Forensic Tools (1)

- **Hard disk duplicator** : mirrors the content of a hard disk to ensure that the data in the original hard disk is not modified. This must be ensured because direct operation is not permitted on the original hard disk during forensics.
- **Hard disk read-only lock** : blocks the write channel of a hard disk to ensure that data in the storage medium is not modified during data obtaining and analysis, thereby ensuring data integrity.



Hard disk
duplicator



Hard disk read-only
lock

Hardware Forensic Tools (2)

All-in-one forensic appliance: a forensic device that clones, reads, and destructs evidence.

Forensic tower: provides functions such as mobile phone forensic analysis, mobile phone mirroring, mobile phone chip mirroring, and media forensics.

Media repair device: repairs electronic data storage media, such as electronic hard disks, mechanical hard disks, mirroring files, USB drives, and TF cards.



All-in-one forensic appliance



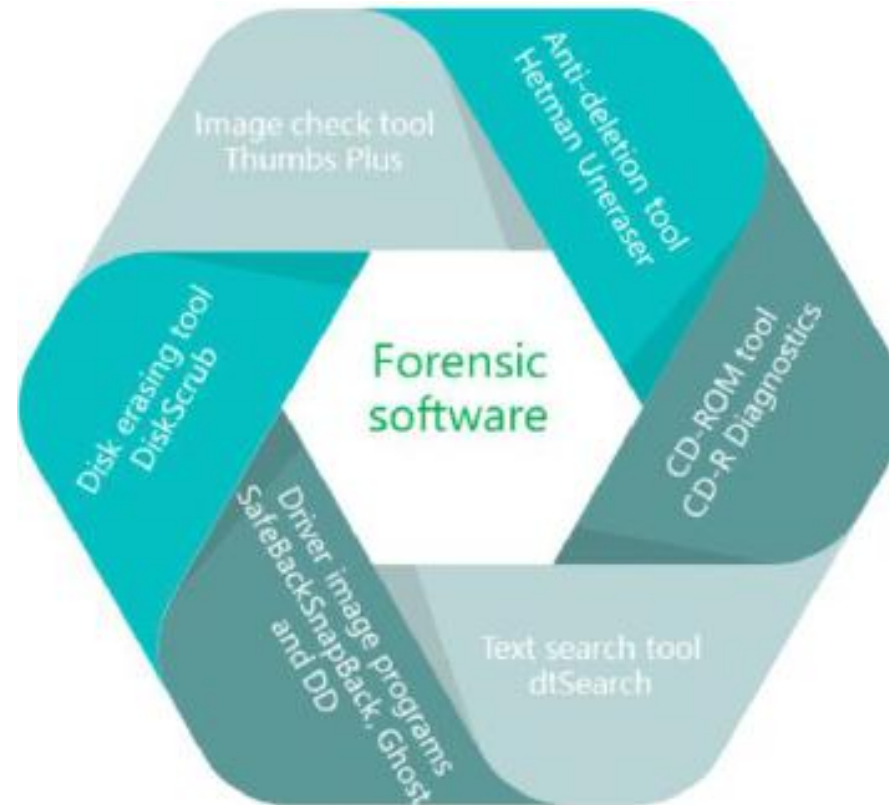
Forensic tower



Media repair device

Software Forensic Tools

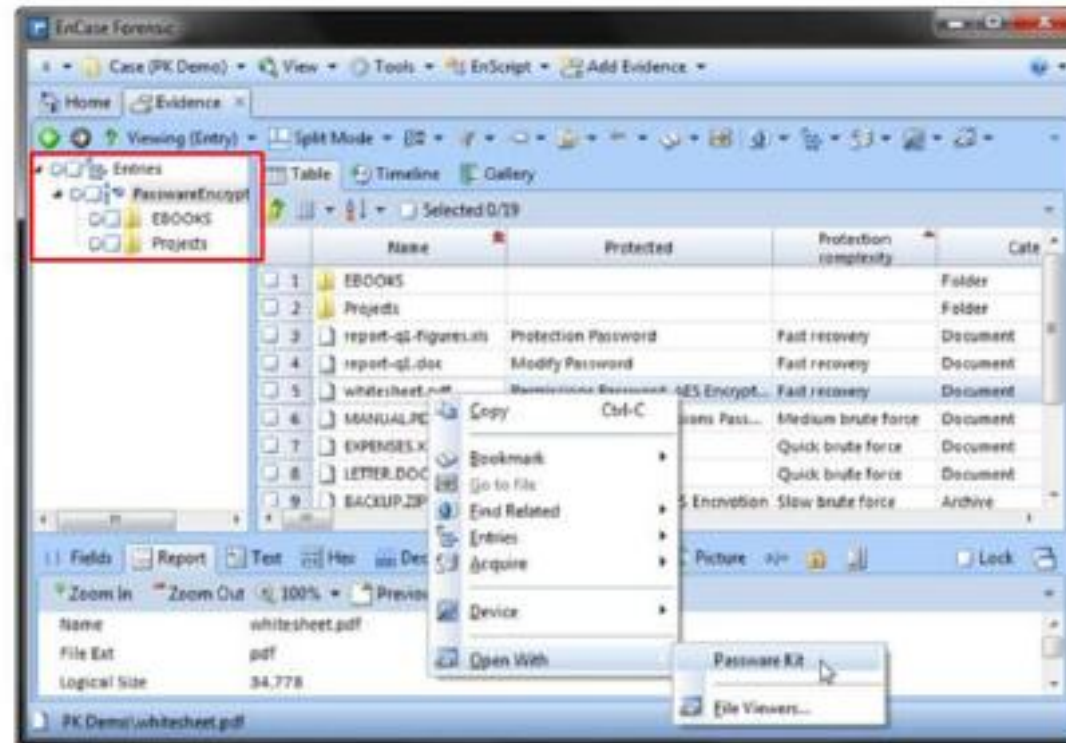
- For ease of research, developers have created a wide variety of computer forensic tools as follows:



Chapter
10

Example Software Forensic Tool - EnCase

- EnCase is a forensic application completely integrated with the Windows UI. It provides functions such as data browsing, search, disk browsing, data preview, case creation, evidence file creation, and case saving.



Digital Forensics Related Technologies

- **Digital forensics related technologies:**

- ☐ **Network packet analysis and forensics**
- ☐ **Log forensics**
- ☐ **Honeypot forensics**
- ☐ **Covert code forensics**
- ☐ **Data mining**

- **Emerging forensic technologies:**

- ☐ **Chip forensics**
- ☐ **Cloud forensics**
- ☐ **IoT forensics**
- ☐ **Side-channel attack (SCA) forensics**



Packet Analysis & Forensics

- Packet capture tools and their features:

Tool	Working Environment	Feature
Tcpdump	Linux	Collection and filtering
WireShark	Linux & Windows	Collection and filtering
Sleuth Kit	Linux	Collection, filtering, stream reassembly, and data association
Argus	Linux	Collection, filtering, and log analysis
Sniffers	Linux & Windows	Network traffic and packet analysis

Chapter

10

Chip Forensics

- **Joint Test Action Group analysis:** Access the internal register of the analysis processor through the Test Access Port (TAP) inside the chip. Forensics can be implemented even if the phone is damaged.
- The red box in the figure shows the phone chip. You can use the analysis tool to collect evidence from the damaged phone chip.



Damaged phone



Analysis tool interface

Dynamic Simulation

- **Dynamic simulation** is used to simulate a mobile phone in order to restore the chat history and group discussion information, extract files in chat software, and analyze the number of reposts, impact scope, source of information, and more.

As shown in the following figure, a simulator is used to simulate the operational environment of a mobile phone and display the digital red envelop records.



Preserving Evidence



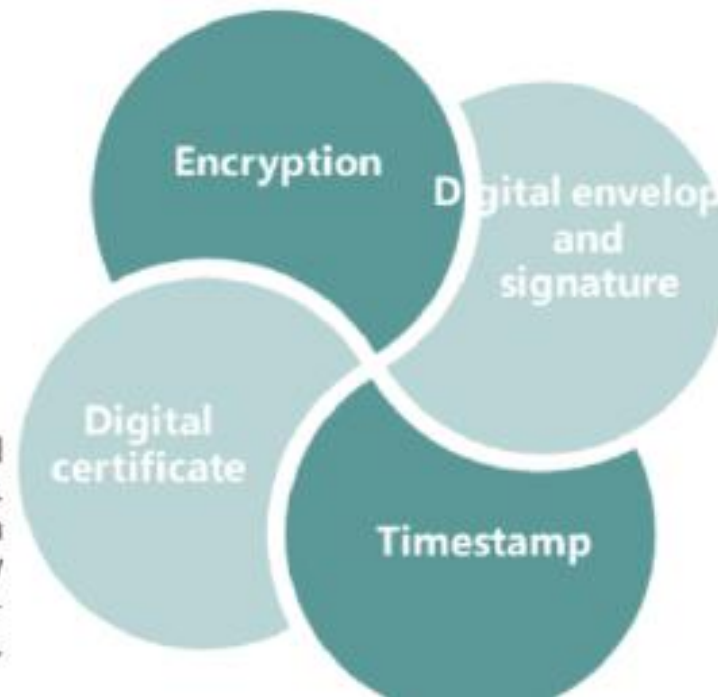
- The preservation of evidence directly affects the legal effect of the evidence. Only preservation technologies that conform to legal regulations can guarantee the authenticity and reliability of evidence.
- Evidence preservation technologies:
 - ☐ Encryption
 - ☐ Digital envelope and digital signature
 - ☐ Digital certificate
 - ☐ Timestamp

Evidence Preservation Technologies

- Avoid changes in system settings, hardware damage, data damage, and virus infection during forensics to preserve evidence in its initial state.

Symmetric encryption: DES, 3DES, and AES
Asymmetric encryption: DH, RSA, and DSA

A digital certificate is bound to the real identity of the public key and its holder. The information is electronic data approved by the certification authority and can be flexibly applied in e-commerce and e-government.



The public key in the asymmetric key pair of a digital envelope is used for information integrity verification. Digital signatures use private keys to implement non-repudiation of information.

A timestamp is digital evidence that proves the generation time of certain data.

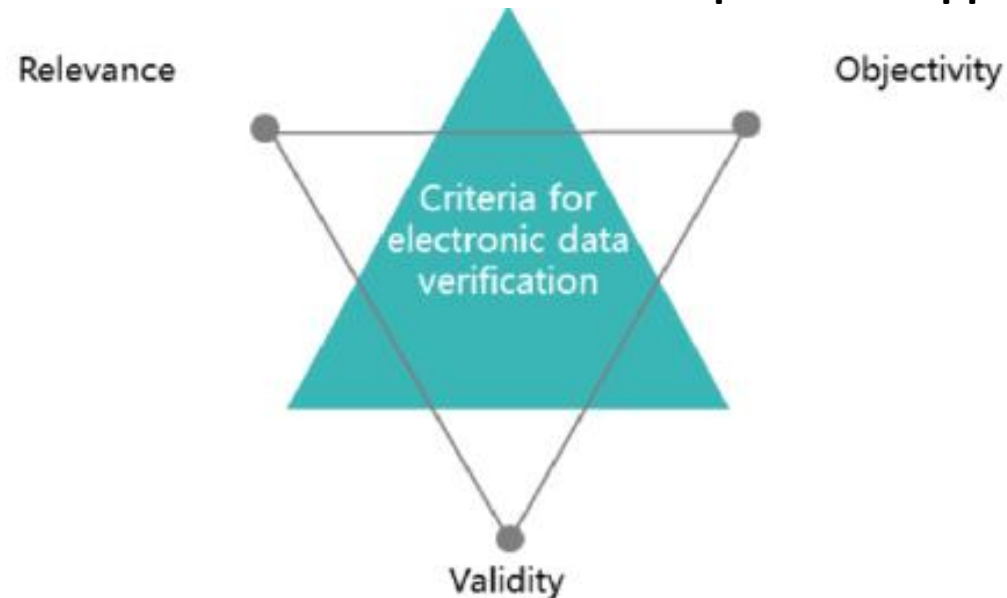
Chapter

10

Verifying Evidence

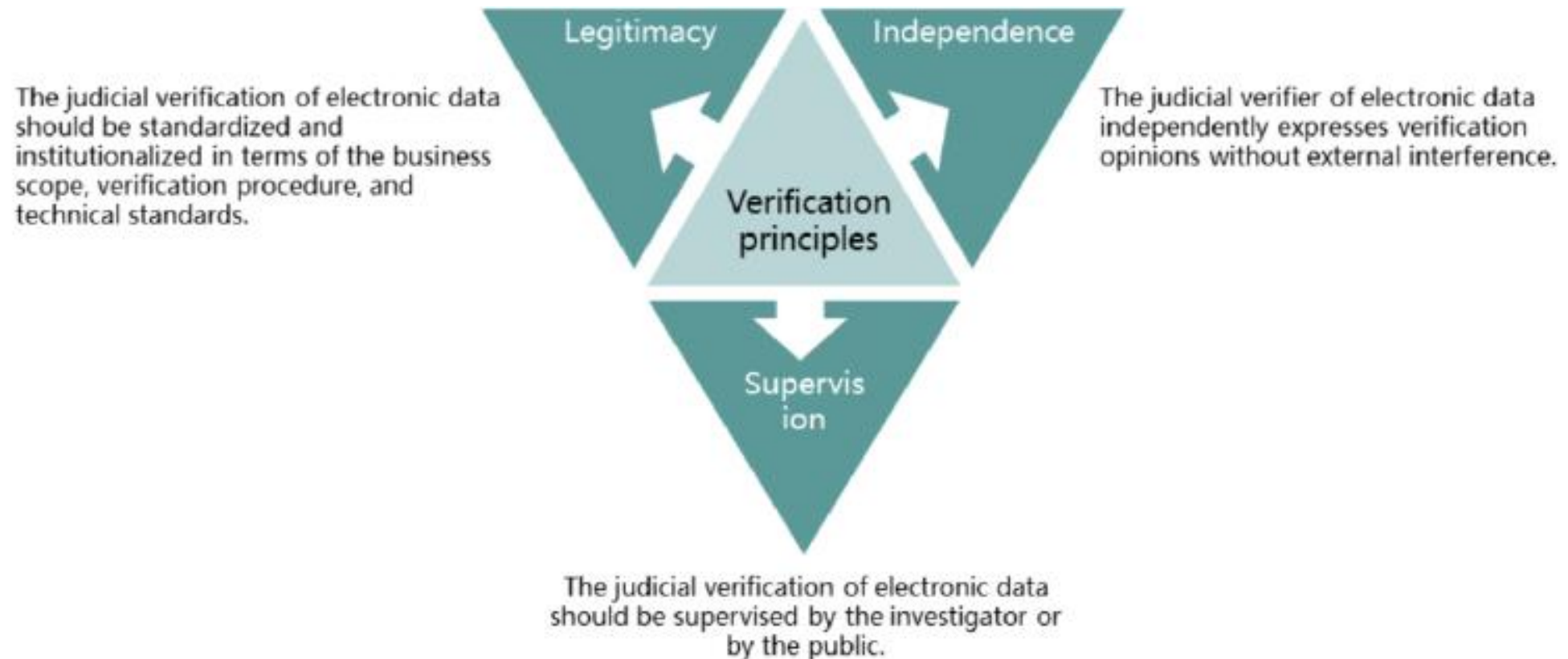


- Verify the integrity of evidence and determine whether it complies with applicable standards.



Principles of Digital Evidence Verification

- Electronic data verification is a special scientific and technical activity and has its own specific principles.



Analyzing Evidence



• **Evidence analysis:** Search for and match keywords or key phrases in the obtained data flows or information flows to analyze the relevance of events. Evidence analysis technologies include:

- ☐ Password cracking and data decryption
- ☐ File attribute analysis
- ☐ Digital digest analysis
- ☐ Log analysis
- ☐ Reverse engineering

Tracing

- With the upgrade of cybercrime technologies, forensics has been combined with network security tools, such as intrusion detection, to implement dynamic forensics. The purpose of tracing is to find the attack source.
- Forensic tracing technologies:
 - ☐ Log analysis
 - Operating system logs
 - Firewall logs
 - Application software logs
 - ☐ Trapping (honeypot)
 - ☐ Tracing and capturing suspects using related devices



Forensic Tracing Technologies

• Hackers usually use data encryption, log clearing, sniffer, stepping stone, or a bastion host to hide or clear intrusion traces. Therefore, it is necessary to implement forensic tracing on intrusion information. Common tracing technologies are as follows:

- ❑ ping, netstat, traceroute, and nslookup commands
- ❑ Packet analysis
- ❑ Log analysis
- ❑ Link test
- ❑ Packet record
- ❑ Packet tag tracing
- ❑ Spam tracing



Chapter

10

Presenting Evidence



- Mark the extraction time, place, device, extractor, and witness of the evidence, submit the evidence to the judicial authority in a visible form, and provide a complete supervision chain.





Thank You