Cyber Forensics & Incident Response (01CY0301)

Lecture - 2

Cyber forensics

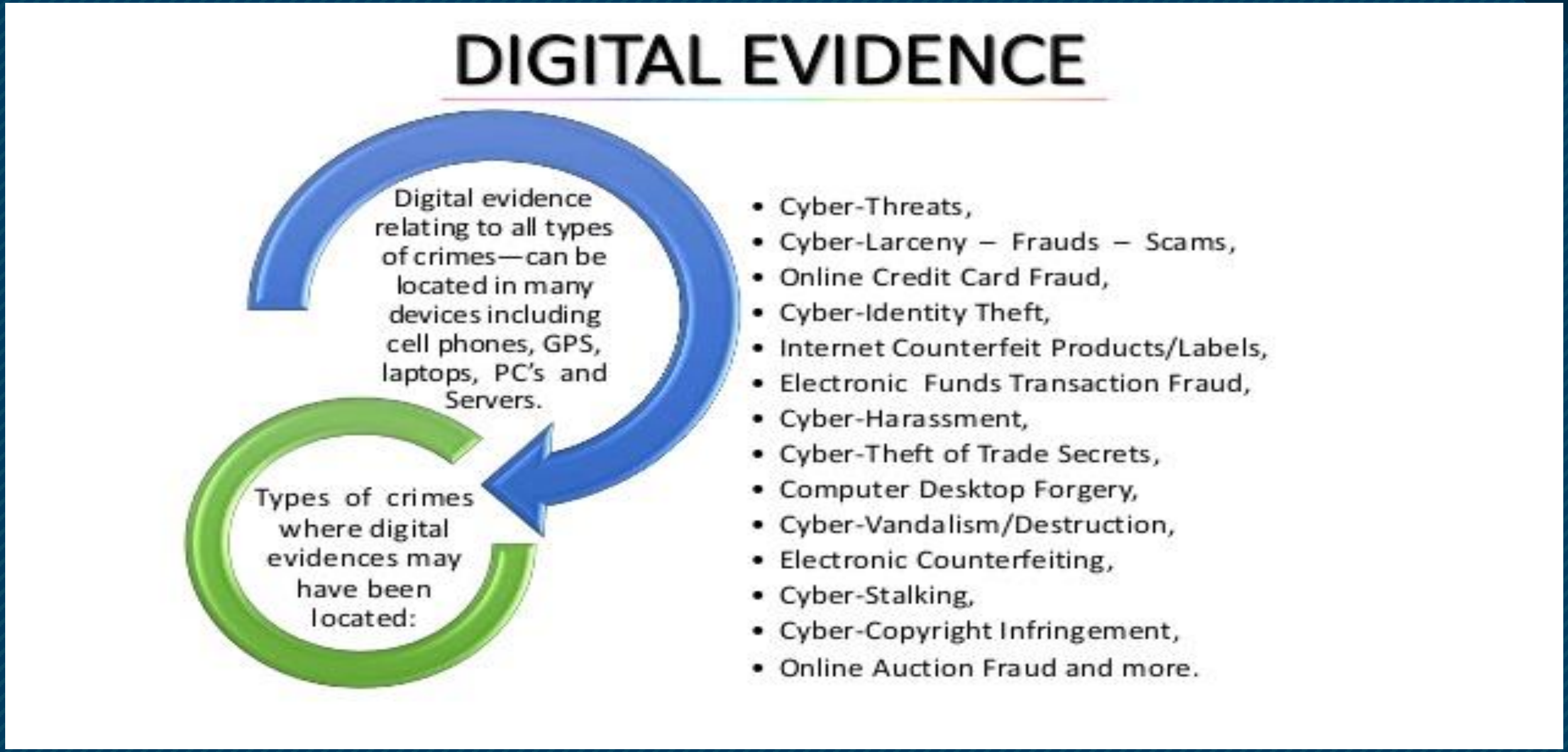
Cyber Forensics is the scientific processes of identification, seizure, acquisition, authentication, analysis, documentation and preservation of digital evidence.

Computer forensics (also known as **computer forensic science)** is a branch of digital forensic science pertaining to evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery , but with additional guidelines and practices designed to create a legal audit trail.

Digital Evidence

Digital evidence is defined as information and data of value to an investigation that is stored on, received or transmitted by an electronic device[1]. This **evidence** can be acquired when electronic devices are seized and secured for examination. **Digital evidence**: Is latent (hidden), like fingerprints or DNA **evidence**.

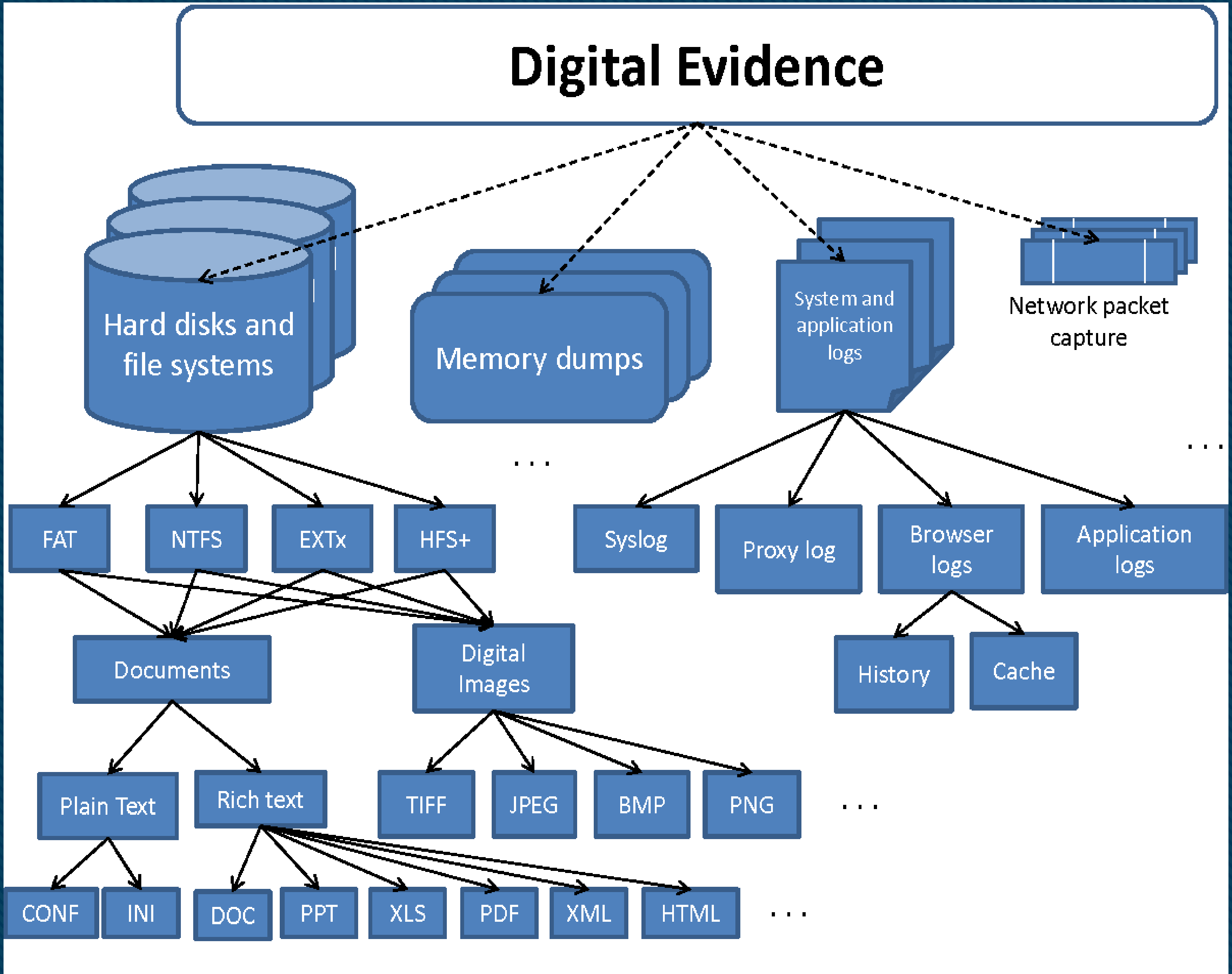


DIGITAL EVIDENCE

Digital evidence relating to all types of crimes—can be located in many devices including cell phones, GPS, laptops, PC's and Servers.

Types of crimes where digital evidences may have been located:

- Cyber-Threats,
- Cyber-Larceny – Frauds – Scams,
- Online Credit Card Fraud,
- Cyber-Identity Theft,
- Internet Counterfeit Products/Labels,
- Electronic Funds Transaction Fraud,
- Cyber-Harassment,
- Cyber-Theft of Trade Secrets,
- Computer Desktop Forgery,
- Cyber-Vandalism/Destruction,
- Electronic Counterfeiting,
- Cyber-Stalking,
- Cyber-Copyright Infringement,
- Online Auction Fraud and more.



Digital Evidence

Hard disks and file systems

Memory dumps

System and application logs

Network packet capture

. . .

FAT

NTFS

EXTx

HFS+

Syslog

Proxy log

Browser logs

Application logs

. . .

Documents

Digital Images

History

Cache

Plain Text

Rich text

TIFF

JPEG

BMP

PNG

. . .

CONF

INI

DOC

PPT

XLS

PDF

XML

HTML

. . .

The rules of evidence.

❖ Admissible

- Evidence Must be able to used in Court

❖ Authentic

- Tie the evidence positively to an incorrect

❖ Complete

- Evidence that can cover all perspectives

❖ Reliable

- There should be no doubt that proper procedures were used

❖ Believable

- Understandable and believable to a jury

Unauthorized activities

- **Unauthorized activity** means an act or practice in this state by a person without a charter, license, permit, registration, or other authority issued or granted by the banking commissioner or other appropriate regulatory authority for which such a charter, license, permit, registration, or other authority is required.

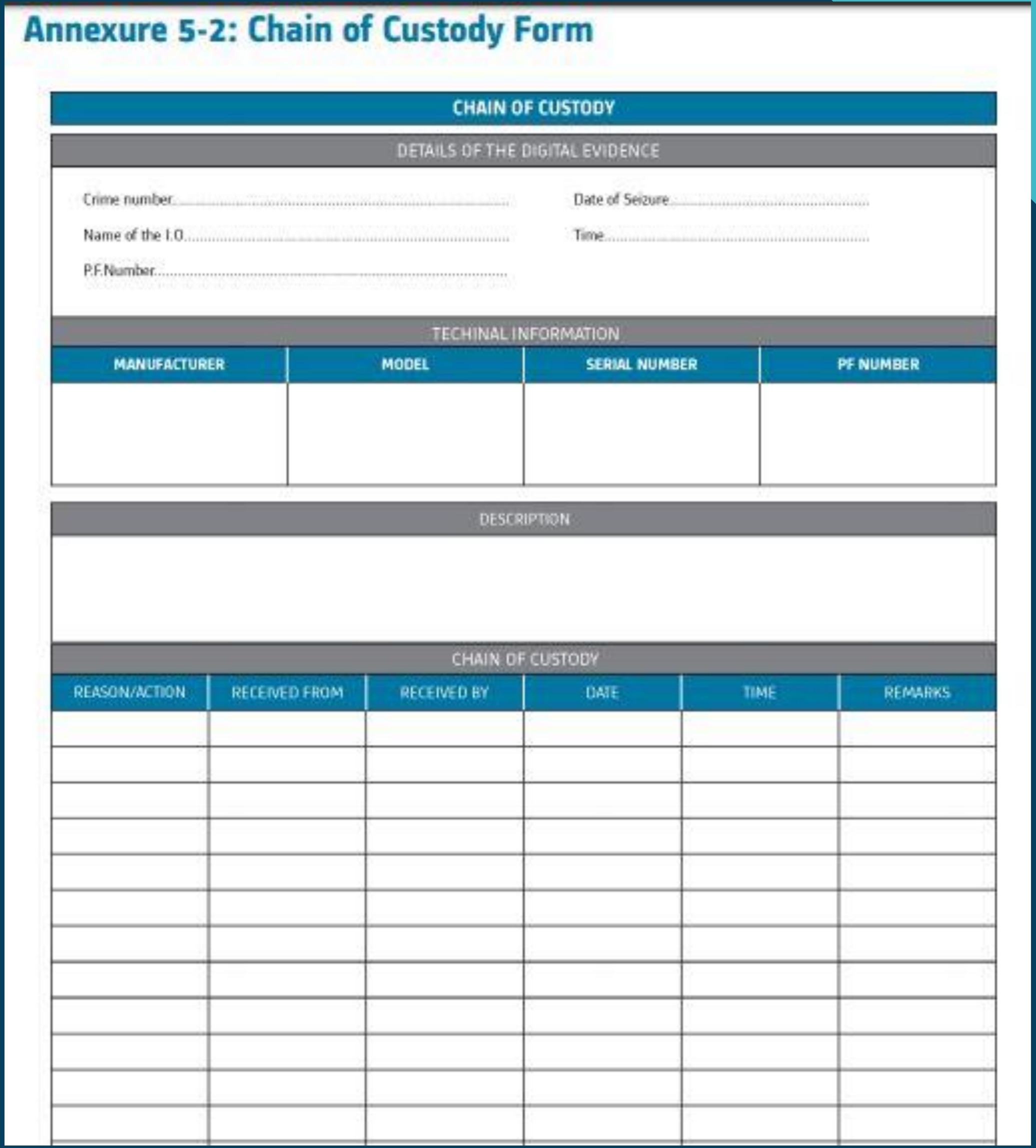
List

Physical vs Logical

- ➢ Stealing data Remotely
- ➢ Stealing Laptop.

Chain of Custody

Chain of custody (CoC), in legal contexts, is the chronological documentation or paper trail that records the sequence of **custody**, control, transfer, analysis, and disposition of physical or electronic evidence.



Annexure 5-2: Chain of Custody Form

CHAIN OF CUSTODY

DETAILS OF THE DIGITAL EVIDENCE

Crime number.. Date of Seizure..

Name of the I.O... Time...

P.F.Number..

TECHINAL INFORMATION

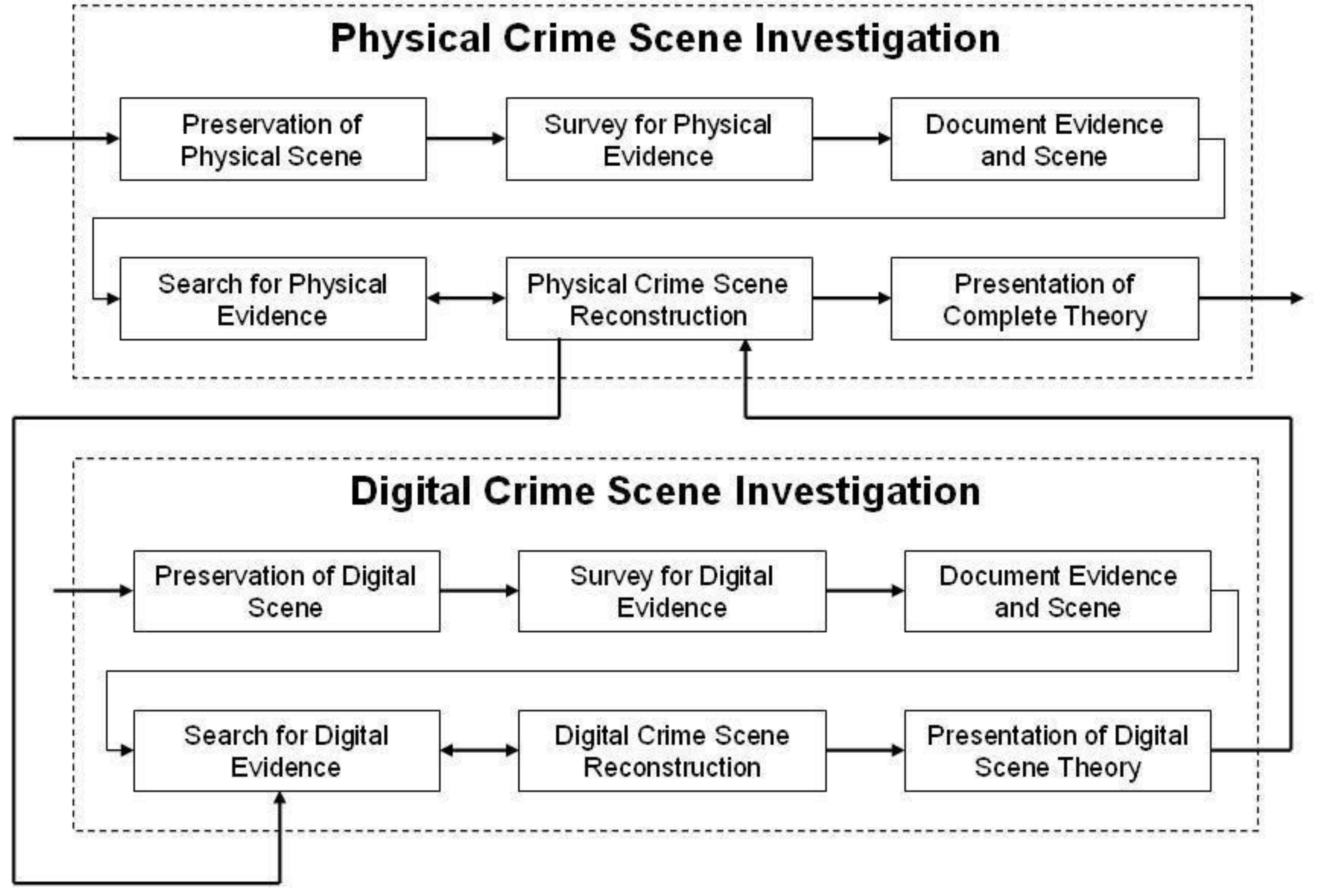
MANUFACTURER	MODEL	SERIAL NUMBER	PF NUMBER

DESCRIPTION

CHAIN OF CUSTODY

REASON/ACTION	RECEIVED FROM	RECEIVED BY	DATE	TIME	REMARKS

Chain of Custody Step


Physical Crime Scene Investigation
Preservation of Physical Scene
Survey for Physical Evidence
Document Evidence and Scene
Search for Physical Evidence
Physical Crime Scene Reconstruction
Presentation of Complete Theory
Digital Crime Scene Investigation
Preservation of Digital Scene
Survey for Digital Evidence
Document Evidence and Scene
Search for Digital Evidence
Digital Crime Scene Reconstruction
Presentation of Digital Scene Theory

Any Question ?

Thank You