Digital Forensics

KRESTON
OPR ADVISORS

Contents

01 Digital Forensics

Definition of Digital Forensics
Who require Digital Forensics

02 Digital Evidence

Definition of Digital Evidence
Types of Digital Evidence

03 Security Investigation

Areas of analysis for security investigations
Methods for such analysis

04 Types of Digital Forensics

Various types of Digital Forensics
Overview of such types

KRESTON
OPR ADVISORS

Contents

Stages of Forensic Investigation 05

Stages of Forensic Investigation
Description of such stages

Tools and Techniques 06

Techniques for Digital Forensics
Tools for Digital Forensics

Challenges to Digital Forensics 07

Challenges faced by an investigator

Acknowledgement 08

Digital Forensics

Definition of Digital Forensics

Who require Digital Forensics

Digital Forensics

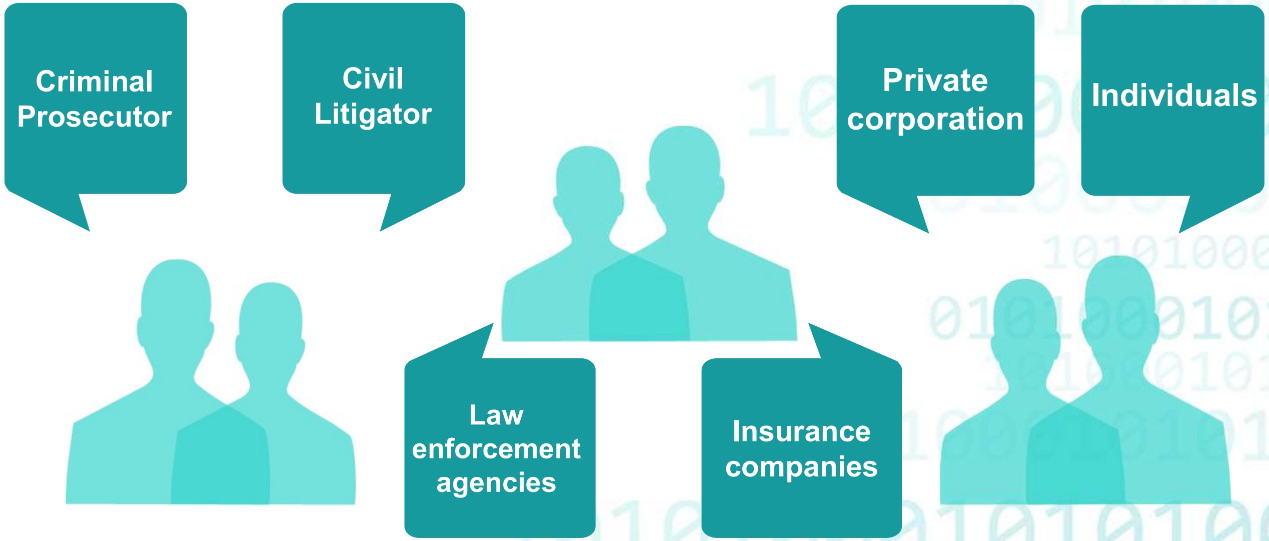
Definition and Users of Digital Forensics

Digital Forensics

The science of recovery and investigation of material found in digital devices, often in relation to computer crime. It is the process of gathering and interpreting electronic data.

The purpose of digital forensics is to preserve any evidence in its original form during collection, validation, identification, analysis, interpretation and presentation the digital evidences for reconstruction of past events.

Who require Digital Forensics



Criminal Prosecutor

Civil Litigator

Private corporation

Individuals

Law enforcement agencies

Insurance companies

KRESTON OPR ADVISORS

Digital Evidence

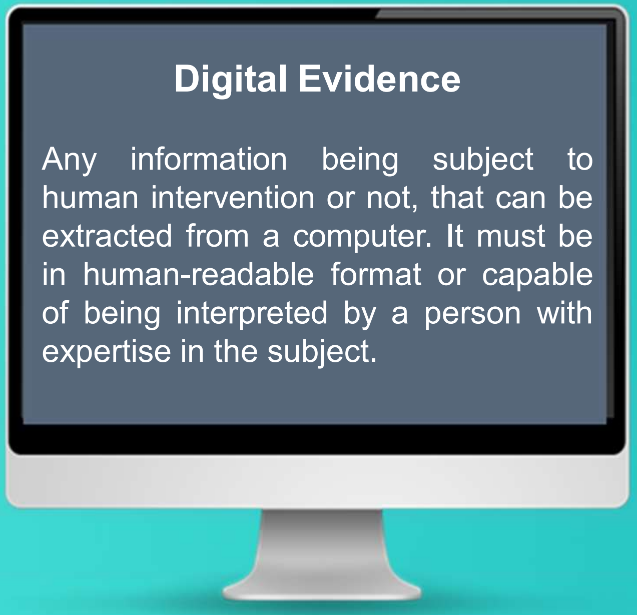
Definition of Digital Evidence

Types of Digital Evidence

KRESTON
OPR ADVISORS

Digital Evidence

Definition and Types of Digital Evidence



Digital Evidence

Any information being subject to human intervention or not, that can be extracted from a computer. It must be in human-readable format or capable of being interpreted by a person with expertise in the subject.

Persistent Data

The data that remains intact even when the computer is turned off.

For e.g. hard drives, disk drives and removable storage devices.

Volatile Data

The data that would be lost once the computer session is terminated.

For e.g. deleted files, computer history, the computer's registry and temporary files.

KRESTON
OPR ADVISORS

Security Investigation

Areas of analysis for security investigations

Methods for such analysis

Security Investigation

Network/ Host Traffic Security

Security Information and Event Management (SIEM)
Network Monitoring
Application Monitoring

Web Transactions

Authentication data
Transaction monitoring
Application logs
SQL server logs
Network Session data

Identity

Authentication data
Active Directory Information
Server logs
SIEM
Asset Management
Network Monitoring

Infrastructure

IT assets management
Governance and Risk Compliance
System configuration management
Vulnerability management

Information

Data Loss Prevention
Data Classification
Governance and Risk Compliance

KRESTON
OPR ADVISORS

Types of Digital Forensics

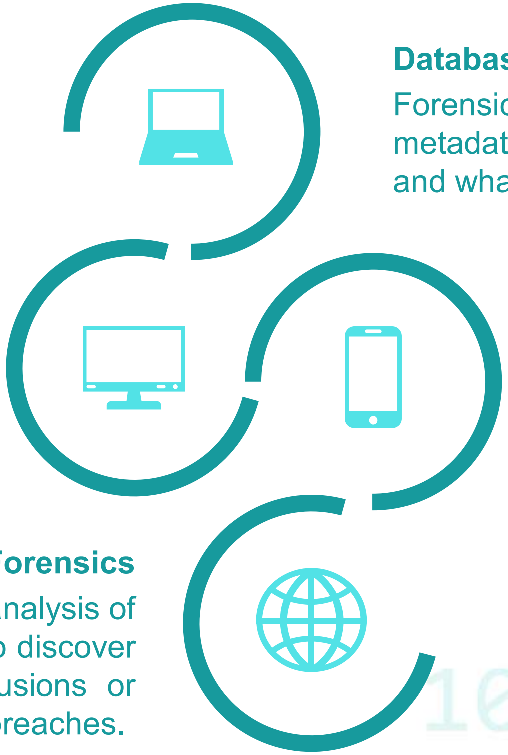
Various types of Digital Forensics

Overview of such types

KRESTON OPR ADVISORS

Types of Digital Forensics

Types of Digital Forensics and Overview



Database Forensics

Forensic study of databases and their related metadata. It look at who has access to the database and what actions are performed.

Computer Forensics

The identification, preservation, collection, analysis and reporting on evidence found on computers, laptops and storage media.

Mobile Device Forensics

The recovery of electronic evidence from mobile phones, smartphones, SIM cards, PDAs, GPS devices, tablets and game consoles.

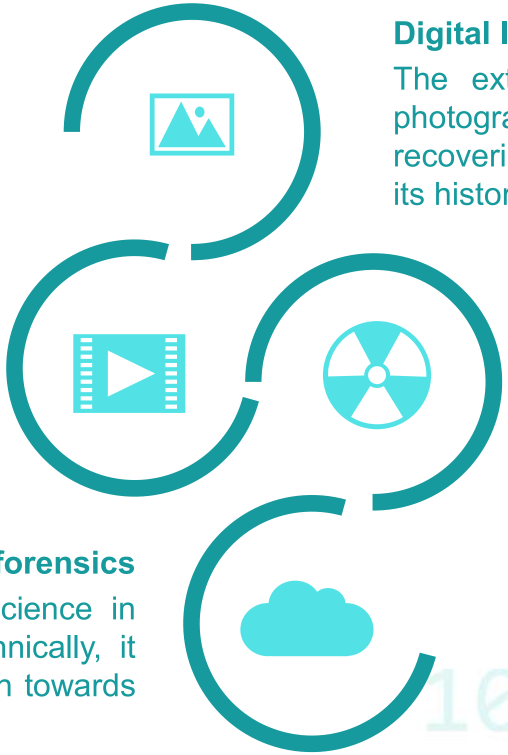
Network Forensics

The monitoring, capture, storing and analysis of network activities or events in order to discover the source of security attacks, intrusions or other problem incidents and security breaches.

KRESTON
OPR ADVISORS

Types of Digital Forensics

Types of Digital Forensics and Overview



Digital Image Forensics

The extraction and analysis of digitally acquired photographic images to validate their authenticity by recovering the metadata of the image file to ascertain its history.

Digital Video/ Audio Forensics

The collection, analysis and evaluation of sound and video recordings to establish authenticity as to whether it is original and whether it has been tampered with, either maliciously or accidentally.

Memory forensics

The recovery of evidence from the RAM of a running computer, also called live acquisition.

Cloud forensics

The application of digital forensic science in cloud computing environments. Technically, it consists of a hybrid forensic approach towards the generation of digital evidence.

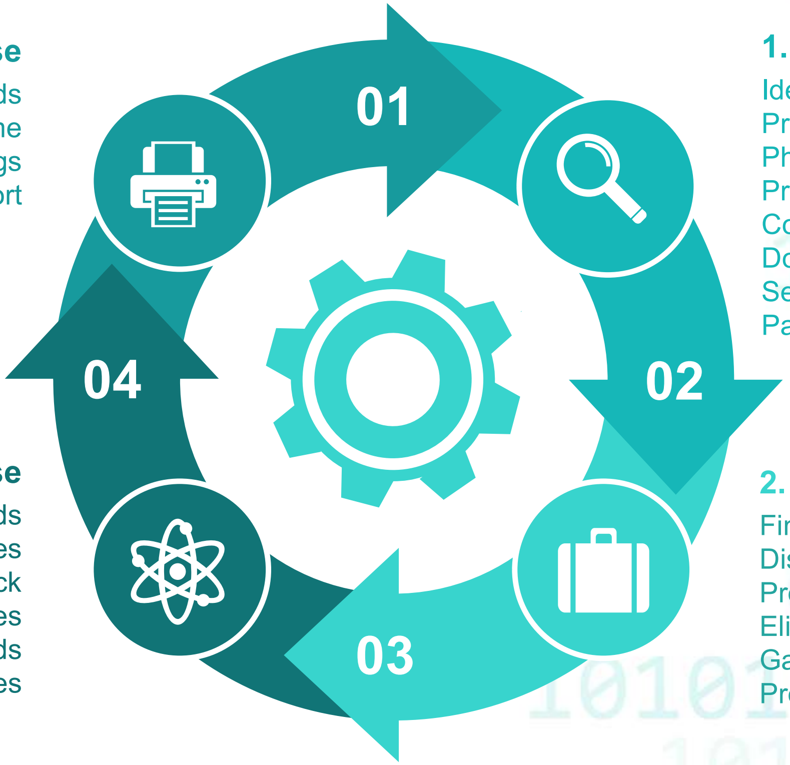
Stages of Forensic Investigation

Stages of Forensic Investigation

Description of such stages

Stages of Forensic Investigation

Stages of Forensic Investigation and Description thereof



1. Assess the Crime scene

Identifying the crime scene
Protecting the crime scene
Photograph the crime scene
Preserving temporary and fragile evidence
Collecting information about the incident
Document all the finding
Seizure of Electronic Equipment
Packaging and transporting digital evidence

2. Collection Phase

Finding the evidence
Discovering relevant data
Preparing an Order of Volatility
Eliminating external possibilities of alteration
Gathering the evidence
Preparing a chain of custody

3. Analysis phase

Making a list of key search words
Evaluating the windows swap files
Evaluating the file slack
Evaluating the unallocated spaces
Search for the key searched words
Analyze of the files

4. Reporting Phase

Tagging the files with relevant keywords
Documenting the file name, date and time
Documenting the findings
Generation of the report

KRESTON
OPR ADVISORS

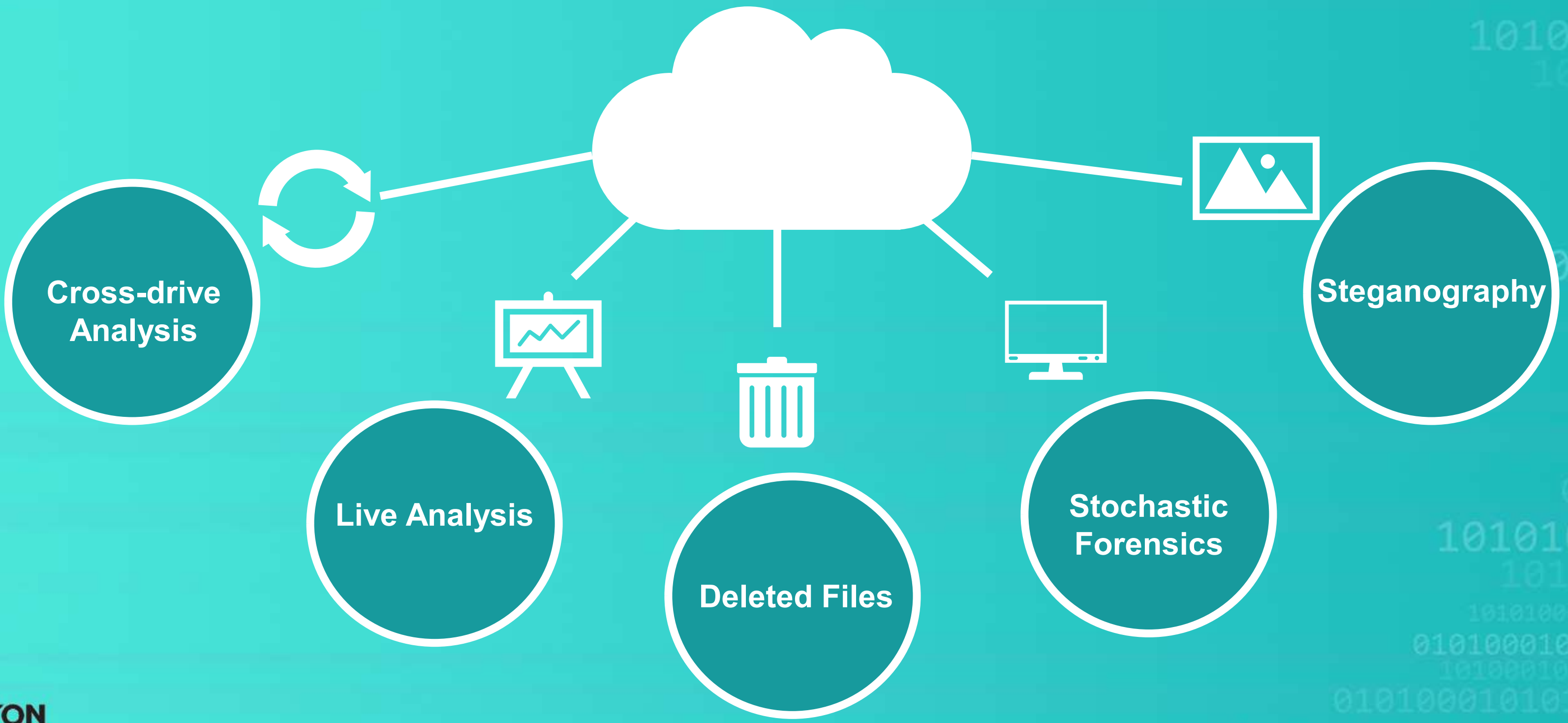
Tools and Techniques

Tools and techniques for Digital Forensics

Use of various Log Tools

Tools and techniques

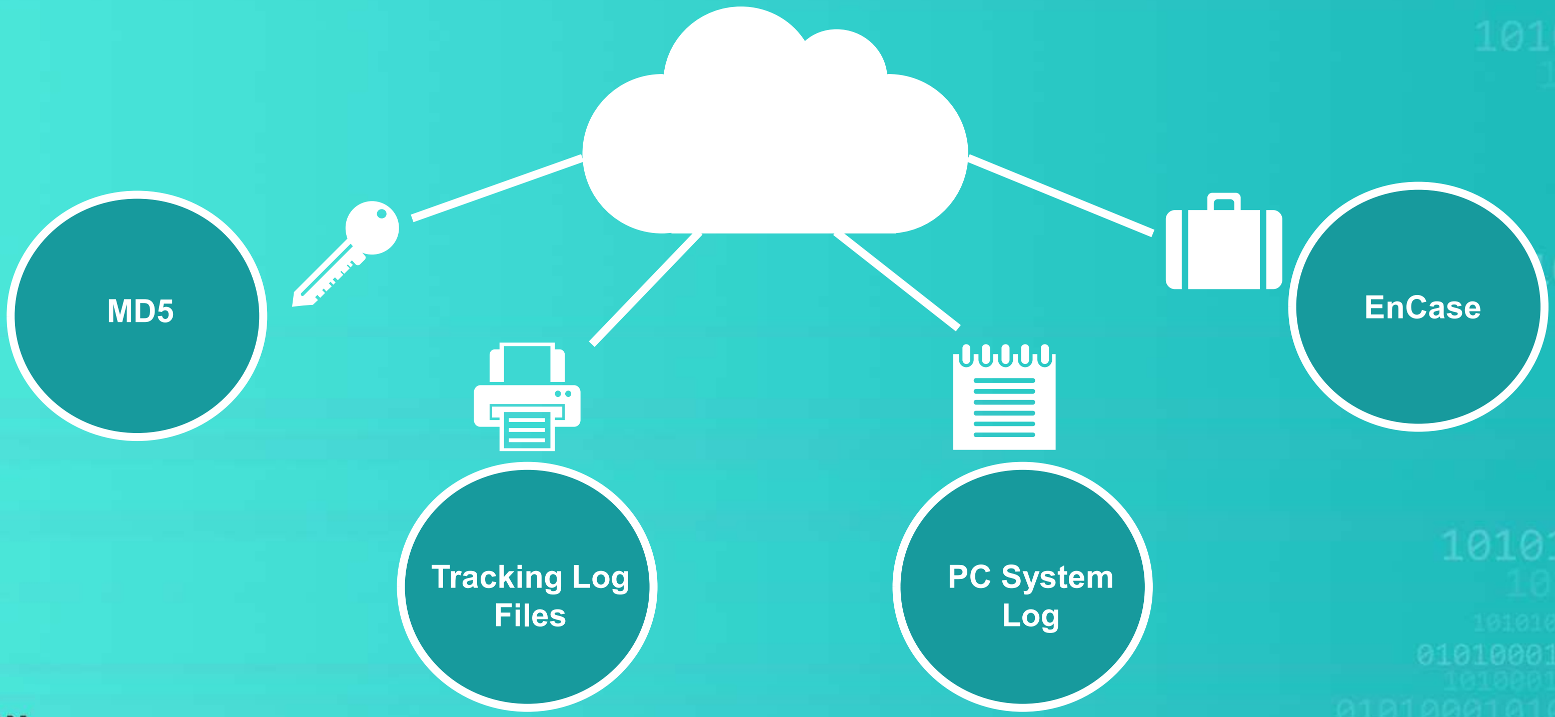
Tools and techniques for Digital Forensics



KRESTON
OPR ADVISORS

Tools and techniques

Tools and techniques for Digital Forensics



MD5

Tracking Log Files

PC System Log

EnCase

KRESTON
OPR ADVISORS

Tools and techniques

Use of Tools

Deleted File Recovery

Calculating starting and end of the file in Hex format and copy it into a text file and saving it with corresponding extension

Slack space

Retrieving deleted and partially overwritten date from the slack spaces.

Faked Bad Clusters

Retrieving sensitive information hidden in the space allocated for bad clusters.

Hidden data analysis

Recovery of hidden data in storage media in file system such as Volume slack, file slack, bad clusters, deleted file spaces.

Partition Tables

Recovery of the data residing on the hard disk partition.

Free space

Recovery of sensitive information from the free space after deletion of files.

KRESTON
OPR ADVISORS

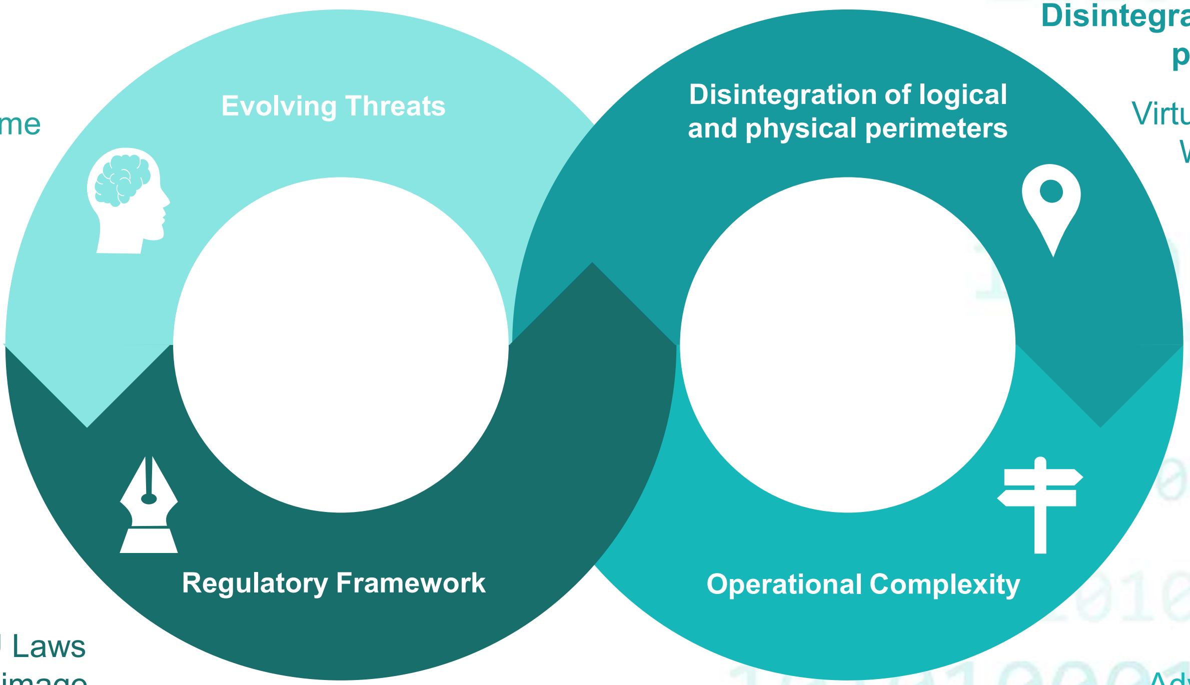
Challenges to Digital Forensics

Challenges faced by an investigator

Challenges to Digital Forensics

Evolving Threats

Organized cybercrime
Automated attacks
Zero-day worms



Evolving Threats

Disintegration of logical and physical perimeters

Regulatory Framework

Operational Complexity

Disintegration of logical and physical perimeters

Virtual Private Networks
Wireless Technology
Cloud Computing
Walk-in Vector
Mobility

Regulatory Framework

Federal, State, EU Laws
Fines, Damage to image
Liabilities, damages, Fines

Operational Complexity

New businesses
Advanced applications
Mergers and Acquisitions

KRESTON
OPR ADVISORS

Thank you!

CA Mahesh Kodwani
Assistant Manager - Assurance & Advisory
Kreston OPR Advisors LLP
+91 265 238 7747, +91 265 238 7757

Vadodara | Ahmedabad | Pune | Mumbai

KRESTON
OPR ADVISORS