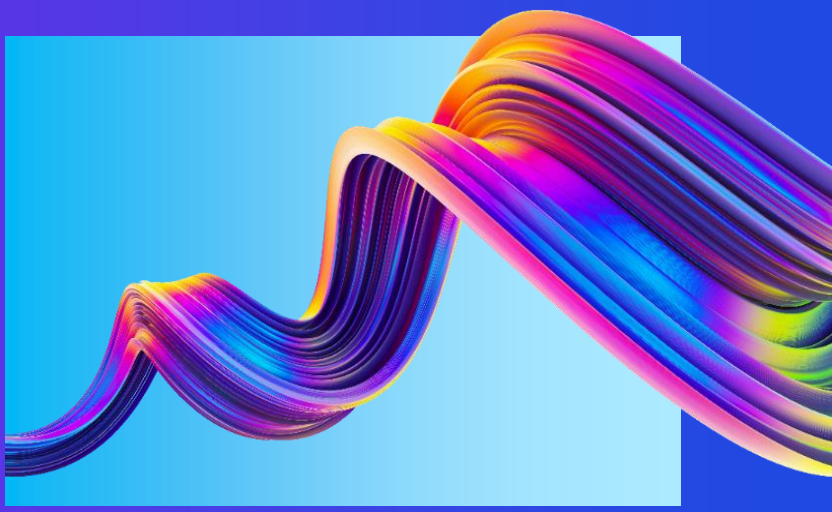
KPMG

Thriving in a digital world



Digital Evidence Recovery (DER)

KPMG Forensic

Forensic Technology (“FTech”) is a service line within KPMG’s Forensic Business Unit that assist clients in their efforts to achieve the highest levels of compliance and efficiency in managing records and information, developing efficient, repeatable business processes for responding to legal and regulatory requests for ESI and providing effective collection, processing and hosting of ESI for review and production.

Forensic technology examiner objectives

- Help 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.
- Preserving the evidence by following the chain of custody.
- Designing a procedure that to ensure that the digital evidence obtained is not corrupted.
- Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.
- Helps to identify the evidence quickly.
- Producing a digital forensic report which offers a complete report on the investigation process.

What is digital forensic

Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing and reporting on data stored on a computer, digital devices or other digital storage media e.g. desktop, laptops, hard disk, memory card, mobile devices, servers, flash sticks, network infrastructures (both physical or in the Cloud), etc.

“Our team of highly skilled, certified forensics examiners can help companies to uncover and interpret electronic data effectively and cost efficiently while ensuring legal admissibility of the digital evidence.”

The main goal of digital forensics is to extract data from the electronic evidence, process the data into useful information and present the findings for further investigation or prosecution.

Digital forensic investigation can be used for:

- Intellectual Property theft,
- Industrial espionage,
- Employment disputes,
- Inappropriate use of the Internet and email in the workplace,
- Fraud investigations, etc.

Types of Digital Forensics

Computer Forensics: It deals with extracting data from storage media by searching active, modified, or deleted files.

Mobile Forensics: It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Cloud Forensics: Cloud computing is an emerging technology, which many organizations are adopting the trend. A cloud forensic implies the application of forensic investigation in a cloud environment.

We can acquire evidence from the following cloud platforms and services: Amazon Web Services (AWS), Apple, Box.com, Dropbox, IMAP/POP Email, Facebook, Google, Instagram, Microsoft, Microsoft Azure, Microsoft Teams, Slack, Twitter, and WhatsApp (Google Drive backups and QR code access).

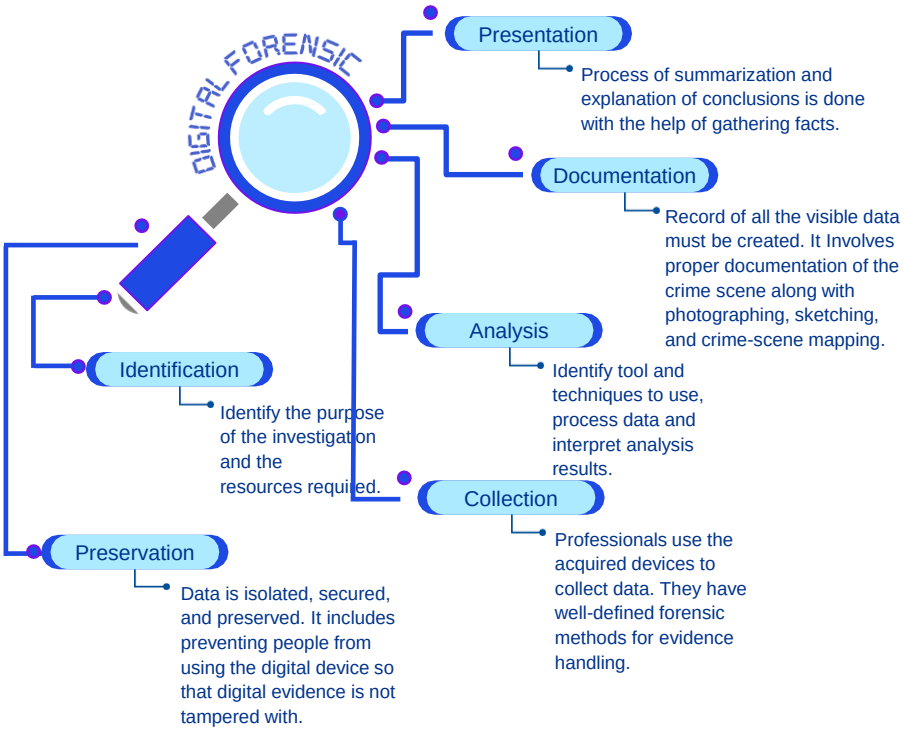
Remote digital forensics: Remote digital forensics is also an emerging technology, where digital evidence collection is acquired remotely from remote device or remote location.

In practice, digital forensic investigators used to leave their laboratory to visit the crime scene, where they collect all the relevant evidence, and bring it back to the forensic laboratory for secure storage and analysis.

Nowadays they could remotely transfer an image from any suspect computer directly to a forensic lab, and it helps to significantly reduce the investigation time used to conduct on-site collection of evidence.

Methodology

Forensic technologies are designed to prepare and extract evidence from computer systems. Any electronic devices that store data (e.g. computers, laptops, smartphones, memory cards or external hard drives) are within the ambit of digital forensics. The forensics process is outlined as follows:



Digital Evidence Recovery Tools

Today's digital forensics tools are multipurposed and automated, tailored to meet the need to perform remote acquisitions and need to collect and analyze evidence from cloud storage and communication services, computers, and mobile devices. They help us to simplify digital forensic investigations task quickly and effectively, save time and reduce the costs.

FORENSIC Falcon NEO

MAGNET AXIOM CYBER

Cellebrite

EnCase Cybersecurity

Intella
Process | Search | Filter | Produce. Simple.

kpmg.com/socialmedia

Contact us

Déan Friedman
Director/Head of Forensic
T: +27 (82) 719 0336
E: dean.friedman@kpmg.co.za

Godfrey Gabara
Manager
T: +27 (82) 393 2556
E: Godfrey.Gabara@kpmg.co.za