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 assists 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 Electronically Stored Information ("ESI") and providing effective collection, processing and hosting of ESI for review and production.

Forensic technology examiner objectives

- Identify, preserve, recover and analyse digital evidence stored on computers and other electronic devices in such a manner so as to aid an investigation team in presenting such evidence in a court of law.
- Preserving the evidence by following a strict chain of custody.
- Following procedures to ensure that the integrity of digital evidence obtained is maintained.
- Recovering deleted files and deleted partitions from digital media to extract and validate crucial evidence.
- Identify the evidence quickly.
- Producing a digital forensic report detailing the investigative process, with supporting annexures and exhibits.

What is digital forensic

Digital Forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing and reporting on digital evidence stored on computers, electronic devices or external storage media e.g. desktop, laptops, hard disks, memory cards, mobile devices, servers, memory sticks, network infrastructures (both physical or in the Cloud), etc.

> **"Our team of highly skilled, certified forensics examiners can help companies uncover and interpret digital evidence effectively and cost efficiently while ensuring legal admissibility of such digital evidence."**

The main goal of digital forensics is to extract digital evidence from electronic devices, and present such digital evidence as findings to support the objectives of an investigation e.g. to prove or disprove allegations relating to fraud, misconduct, cyber attacks/incidents, to support disputes and other legal proceedings such as disciplinary hearings and civil/criminal prosecutions.

Digital forensics can be used in the following types of investigations:

- 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: Deals with the extraction of digital evidence from electronic devices and storage media by searching active, modified, or deleted files.

Mobile Forensics: Deals with the examination and analysis of digital evidence on mobile devices, such as phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

Cloud Forensics: Cloud computing is an emerging technology, which many organisations are now adopting. Cloud forensics involves the application of digital forensic and investigation principles 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).

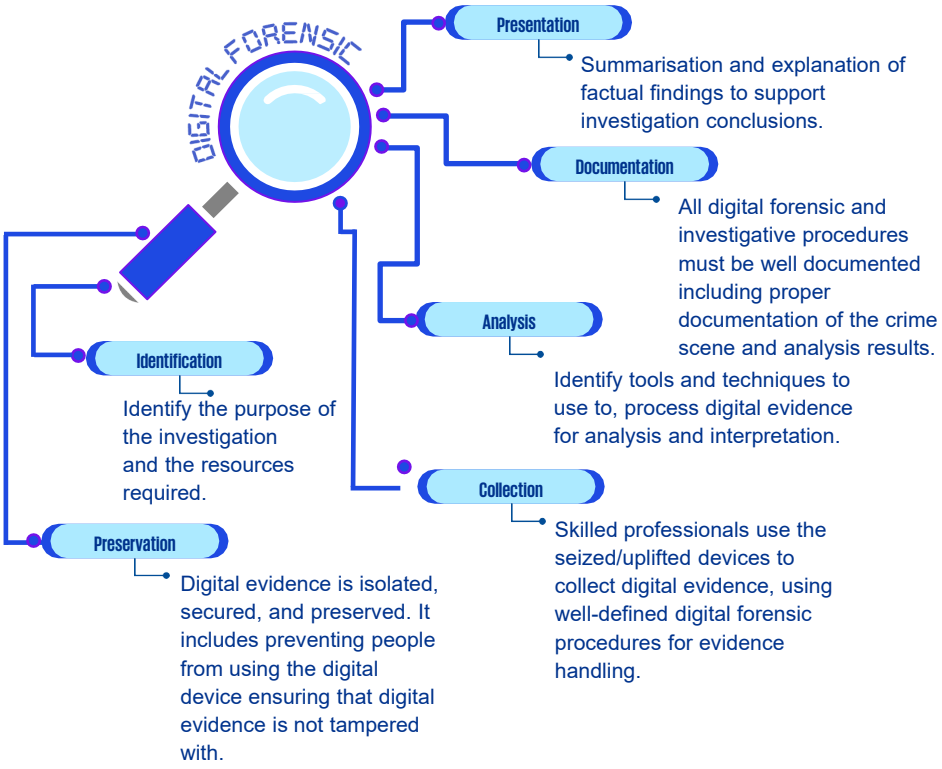
Remote digital forensics: Remote digital forensics is also an emerging technology, whereby digital evidence is acquired remotely from a remote device or a remote location.

Historically and still In practice today, digital forensic investigators generally leave their laboratories to visit the crime scene, where they collect all the relevant evidence. Once collected, the said evidence is brought back to the forensic laboratory for secure storage and analysis.

Nowadays digital evidence can be remotely transferred rom any suspect computer directly to a forensic laboratory, which significantly reduces the overall investigation time.

Methodology

Forensic technology methodologies are designed to extract and prepare digital evidence from electronic devices and computer systems. Any electronic device that stores data (e.g. computers, laptops, smartphones, memory cards or external hard drives) are within the ambit of digital forensics. The digital forensic process is outlined in the diagram eblow:



Digital Evidence Recovery Tools

Digital forensic tools are multipurposed and automated, tailored to meet the needs of an investigation, be it to perform remote acquisitions, collect and analyse evidence from cloud storage and communication services, computers or mobile devices. They help simplify digital forensic investigations allowing investigators to execute tasks quickly and effectively, thereby saving time and reducing costs.

FORENSIC Falcon NEO

MAGNET AXIOM CYBER

Cellebrite

EnCase Cybersecurity

Intella
Process | Search | Filter | Produce. Simple.

kpmg.com/socialmedia

Contact us

Déan Friedman
Director, Forensic, KPMG South Africa
T: +27 (82) 719 0336
E: dean.friedman@kpmg.co.za

Sameer Vyadally
Senior Manager, Forensic, KPMG South Africa
T: +27 (66) 010 7878
E: sam.vyadally@kpmg.co.za