TECDT61231

# Assist in implementing digital forensic processes

## Overview

This standard is about assisting in implementing digital forensic processes whilst maintaining evidential integrity.

This involves helping with identifying, collecting and analysing digital information in support of investigations to determine the circumstances of events of concern to an organisation. This includes applying ethical considerations as well as knowing when not to act.

This standard covers the competencies needed to assist in implementing digital forensic processes. It is for those who need to assist in implementing digital forensic processes as part of their duties.

## Performance criteria

*You must be able to:*

1. Assist with identifying potential sources of information from digital devices and systems whilst preserving evidence
2. Undertake disassembly and reassembly of digital devices to perform forensic imaging and data capture
3. Assist with accurately reporting appropriate incident information in line with organisational standards
4. Assist with data recovery from digital devices and systems using approved digital forensic tools in line with organisational procedures
5. Assist with analysing digital evidence using approved tools and techniques to produce information in a format ready for full examination by digital forensic analysts
6. Contribute to documenting event information to maintain accurate and auditable records
7. Assist in the maintenance of the digital forensic hardware and software infrastructure and tools
8. Produce reports of digital forensic work undertaken in line with organisational procedures
9. Apply the primary features of law, regulations and organisational standards relevant to digital forensics activities

## Knowledge and understanding

*You need to know and understand:*

1. That digital forensics is the identification, collection, examination and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data
2. The types of computer misuse that can occur and how to identify them
3. Computer forensic principles and the importance of ensuring that evidence is not contaminated
4. The Computer Misuse Act and civil and criminal laws relevant to digital forensic investigations
5. When not to act during digital forensic investigations
6. The need to consider ethics when dealing with personal information during forensic investigations
7. The types of digital device that may be investigated, including mobile phones, laptops, tablets and personal computers, fixed and cloud networked system log files and portable digital storage devices
8. The main principles, tools and techniques used in the eDiscovery process
9. How to apply investigation skills and evidence handling in digital forensic investigations
10. Triage basic examination, processing and reporting of mobile phone devices.
11. The role of chain of custody in preserving the value of digital evidence
12. The volatile nature of data
13. How to investigate operating systems
14. The file structures used for hard disk drives, network files and solid state drives
15. The importance of hash values in digital forensics for data integrity
16. The industry standard digital forensic tools used to extract and analyse digital

evidence and how to apply them

17. How to undertake network forensics in a client-server and virtual network
18. How to read data from mobile phones
19. Data subject access request, redaction and disclosure
20. Organisational digital forensic procedures, regulatory and international standards and industry codes of practice

TECDT61231

# Assist in implementing digital forensic processes

| | |
|---|---|
| **Developed by** | e-skills |
| **Version Number** | 1 |
| **Date Approved** | 30 Mar 2022 |
| **Indicative Review Date** | 30 Mar 2025 |
| **Validity** | Current |
| **Status** | Original |
| **Originating Organisation** | ODAG Consultants Ltd. |
| **Original URN** | TECDT61231 |
| **Relevant Occupations** | Information and Communication Technology Professionals |
| **Suite** | IT and Telecoms Professional (procom) |
| **Keywords** | cyber security, digital forensics |