TECDT61241

Deliver digital forensic services

Overview

This standard is about delivering digital forensic services.

The growth of digital device use for organisational and social purposes has led to behaviours that may need investigation for professional conduct or legality.

This involves ethically identifying and reconstructing the relevant sequence of events that has led to the investigation of a target IT system or digital devices and the importance of digital evidence. This includes carefully identifying, collecting and analysing digital information in support of investigations to determine the circumstances of events of concern to an organisation whilst maintaining evidential integrity.

This standard covers the competencies needed to deliver digital forensic services. It is for those who need to deliver digital forensic services as part of their duties.

Performance criteria

You must be able to:

1. Attend incident scenes to conduct searches for digital data, ensuring proper continuity of evidence
2. Conduct physical examinations of digital devices, including disassembly and reassembly
3. Perform preliminary forensic analysis to identify storage device specifications, and system and file types
4. Triage information systems and digital devices when required to prioritise and plan data recovery and analysis
5. Carry out forensic acquisition of data in accordance with organisational guidelines
6. Locate and interpret relevant system logs, to identify anomalies or evidence of compromise, including from firewalls, proxies, web servers, system files, and packet captures
7. Perform detailed forensic analysis of data to tell the story of the digital activity for the user scenario under investigation
8. Prepare evidential data for use in further investigations and potential legal proceedings
9. Record all digital forensic activities and results in line with organisational standards
10. Produce reports of digital forensic activities and findings
11. Present digital forensics findings to management, legal and other stakeholders

Knowledge and understanding

You need to know and understand:

1. That the need for digital forensic analysis can result from incidents, suspected data breaches, intellectual property theft, insider threat investigations, fraud and abuse, asset misuse, and violations of organisational policy
2. The starting point for a digital forensic analysis of data is a snapshot of the state of the system of interest, including the current content of data storage drives, cloud storage, system data or other storage medium
3. How to extract and produce a mirror image of data, whilst retaining its integrity
4. That an operating system maintains a variety of monitoring logs that can provide useful information of individual account user activity
5. Computer architecture, operation, connectivity and fixed and virtual networking
6. The legislation in relation to Computer Misuse and Cybercrime
7. The Data Protection Act, the Freedom of Information Act, and the Criminal Procedure and Investigations Act
8. How to effectively manage digital forensic projects to ensure stakeholder requirements and expectations are fulfilled
9. How to access and examine digital devices, including hard disk drives solid state drives, mobile phone SIM cards and other storage media
10. The industry standard digital forensic imaging and analysis tools and techniques and how to apply them
11. How to search and filter data sources to identify data of interest
12. How to read and extract data to identify individual facts and relationships that can support or disprove a hypothesis under investigation
13. The steps involved in performing forensic examination of digital devices or systems in accordance with organisational policies and procedures
14. That as storage devices evolve, it is increasingly difficult to obtain a true physical copy of the media and a logical or partial acquisition may be the only possibility
15. How to apply forensic analysis that can explain the digital data evidence

obtained

16. How to report on forensic examinations to tell the story of the data from user digital activities under investigation

17. The need to maintain digital forensic knowledge to maintain awareness of new digital devices and data storage technologies

18.

That the results of a forensic investigation may need to be presented in a form that is admissible in a court of law

19.

Know when to act and when not to act

20.

The need to operate ethically when dealing with personal data

TECDT61241

Deliver digital forensic services

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	TECDT61241
Relevant Occupations	Information and Communication Technology Professionals
Suite	IT and Telecoms Professional (procom)
Keywords	cyber security, digital forensics