TECIS60633

Contribute to digital forensic examination activities

Overview

Digital forensic examination procedures are used to uncover and interpret electronic data to aid the investigation of information security issues. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying and validating the digital information for the purpose of reconstructing past events. The context is most often for usage of data in a court of law, though digital forensics can be used in other instances.

This standard defines the competencies required to assist with digital forensic examination under supervision. It includes following digital forensic examination processes to ensure that security issues are investigated appropriately.

Performance criteria

You must be able to:

1. assist collecting information and evidence as part of a digital forensic examination in line with organisational procedures
2. apply relevant tools and techniques to examine information systems for issues, intrusions or compromise
3. confiscate digital equipment and devices whilst maintaining evidential weight in line with organisational standards
4. analyse and recover or preserve data from digital storage media using digital forensic tools in line with organisational standards
5. operate with integrity and confidentiality during digital forensic examinations
6. analyse data from protective monitoring sources for malicious intent
7. analyse accounting and audit logs generated by IT systems for signs of suspicious or malicious behaviour
8. analyse software for malicious intent
9. preserve a compromised information system "crime scene" from alteration
10. document all information relating to a digital forensic examination in line with organisational standards

Knowledge and understanding

You need to know and understand:

1. what is meant by a digital forensic examination
2. what is the purpose of a digital forensic examination
3. how to correctly follow the procedures and standards relating to digital forensic examination activities
4. how to assess and prioritise the collection of digital forensic evidence
5. what the capabilities of digital forensics tools are
6. what information can be collected to support digital forensic examination
7. the regulatory and organisational policy requirements to preserve digital forensic evidence
8. how to apply digital forensic examination procedures to help to identify accounts and individuals connected to security issues
9. the processes, procedures, methods, tools and techniques used to conduct digital forensic examinations and how to use and apply them
10. the existence of relevant legislation; e.g. principles in Data Protection Act, Regulations of Investigatory Powers Act
11. where to seek information to support forensic examinations
12. the legal requirements for preservation of digital forensic evidence
13. the technical aspects of data storage including hard disk configuration and slack space as applied for digital forensics
14. the need for forensic examinations to be undertaken in accordance with any codes of conduct and organisational policies and standards
15. how to collect evidence relating to information systems under investigation
16. the need to operate with integrity and confidentiality during digital forensic examinations
17. how to preserve the "digital crime scene" from alteration
18. how to collect and analyse data as part of a digital forensic examination
19. how to document the findings of a digital forensic examination

TECIS60633

Contribute to digital forensic examination activities

Developed by	e-skills
Version Number	1
Date Approved	March 2016
Indicative Review Date	April 2019
Validity	Current
Status	Original
Originating Organisation	The Tech Partnership
Original URN	TECIS60633
Relevant Occupations	Information and Communication Technology; Information and Communication Technology Officer; Information and Communication Technology Professionals
Suite	Information Security
Keywords	Information security, cyber security, digital forensic analysis