



Australian Government

DEFFOR018 Gather and analyse digital information

Release: 1

DEFFOR018 Gather and analyse digital information

Modification History

Release 1. This is the first release of this unit of competency in the DEF Defence Training Package.

Application

This unit describes the skills and knowledge required to gather and analyse digital information to support digital forensic investigations. It includes identifying, collecting, analysing, presenting and maintaining information; compiling notes and statements of evidence; and removing portable digital storage from machines. It also covers the use of initial screening technology.

This unit applies to those working in the gathering and analysis of digital information.

The skills and knowledge described in this unit must be applied within the legislative, regulatory and policy environment in which they are carried out. Organisational policies and procedures must be consulted and adhered to, particularly those relating to work health and safety (WHS) and the gathering and analysis of digital information.

Those undertaking this unit would work independently or as part of a team, under indirect supervision, while performing complex tasks in a broad range of contexts. They must be able to use discretion and judgement and take responsibility for the quality of their outputs.

No licensing, legislative or certification requirements apply to unit at the time of publication.

Pre-requisite Unit

Not applicable.

Competency Field

Digital Forensics.

Unit Sector

Not applicable.

Elements and Performance Criteria

ELEMENTS

PERFORMANCE CRITERIA

Elements describe the essential Performance criteria describe the performance needed to

outcomes.

demonstrate achievement of the element.

- | | |
|---|---|
| 1 Detect and record digital evidence | 1.1 Detect digital evidence using observational techniques and technological methods |
| | 1.2 Record digital evidence prior to examination |
| | 1.3 Document the recorded digital evidence |
| 2 Collect and analyse digital evidence | 2.1 Collect digital evidence by handpicking or removal of portable digital storage from machine to prevent contamination or loss |
| | 2.2 Ensure collected digital evidence is sufficient in detail, where possible, to allow all potential examinations/analysis to be carried out |
| | 2.3 Conduct initial analysis of collected digital evidence and report on outcomes |
| 3 Package digital evidence | 3.1 Package and store items to maintain continuity and prevent degradation or contamination |
| | 3.2 Enter details of digital evidence collected in case notes and, where appropriate, in the exhibit register to maintain the chain of custody |

Foundation Skills

Foundation skills essential to performance are explicit in the performance criteria of this unit of competency.

Range of Conditions

Range is restricted to essential operating conditions and any other variables essential to the work environment.

Non-essential conditions may be found in the DEF Defence Training Package Companion Volume Implementation Guide.

Unit Mapping Information

This unit supersedes and is equivalent to DEFFOR003 Gather and analyse electronic information.

Links

Companion Volume Implementation Guides are found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6bdbab1e-11ed-4bc9-9cba-9e1a55d4e4a9>

Assessment Requirements for DEFFOR018 Gather and analyse digital information

Modification History

Release 1. This is the first release of this unit of competency in the DEF Defence Training Package.

Performance Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria on at least one occasion and include:

- analysing digital information
- detecting digital evidence from digital and analogue recording and communication equipment, including at least one digital storage device
- handling exhibits and preserving continuity of evidence
- maximising the evidentiary value of the digital evidence
- operating safely
- packaging, preserving and storing specific evidence types with consideration of:
 - digital stability
 - exhibit labels
 - packaging medium
 - physical nature of exhibit
 - storage temperature
 - tamper-evident seals
- recording evidence using methods, including at least one of:
 - audio recording
 - computer generated data
 - digital imaging
 - global positioning system (GPS)
 - handwritten notes
 - photographic
 - physical capture
 - sketch plan
 - video recording
- removing and installing electronic equipment on at least one digital storage device
- removing and installing software, including at least one of:
 - application software
 - digital forensic software
 - operating systems

- removing digital storage
- solving problems and making analytical decisions in response to a range of digital evidence contexts, including the systematic examination of digital evidence items
- using specialised evidence recording technology and equipment.

Knowledge Evidence

Evidence required to demonstrate competence in this unit must be relevant to and satisfy all of the requirements of the elements and performance criteria and include knowledge of:

- legislative, policy and quality system context and requirements
- licensing, hardware and security requirements
- range of techniques available for gathering, collecting, packaging and preserving digital evidence
- required forensic documentation for recording and collecting digital evidence
- roles and functions of other forensic discipline specialists in the recording, collection, preservation and continuity of digital evidence
- the purposes and basic functions of internal and external hardware components
- the purposes and basic functions of operating systems and application software
- work health and safety (WHS) practices to be followed when recording, collecting and packaging digital evidence.

Assessment Conditions

Assessors must hold credentials specified within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must satisfy the Principles of Assessment and Rules of Evidence and all regulatory requirements included within the Standards for Registered Training Organisations current at the time of assessment.

Assessment must occur in workplace operational situations. Where this is not appropriate, assessment must occur in simulated workplace operational situations that reflect workplace conditions.

Assessment processes and techniques must be appropriate to the language, literacy and numeracy requirements of the work being performed and the needs of the candidate.

Resources for assessment must include access to:

- a range of relevant exercises, case studies and/or simulations
- applicable documentation, including workplace procedures, regulations, codes of practice and operation manuals
- relevant materials, tools, equipment and personal protective equipment (PPE) currently used in industry.

Links

Companion Volume Implementation Guides are found on VETNet -

<https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=6bdbab1e-11ed-4bc9-9cba-9e1a55d4e4a9>