



Australian Government

DEFFOR019 Give evidence of digital media crime

Release: 1

DEFFOR019 Give evidence of digital media crime

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 give evidence as a digital forensics' expert witness in legal proceedings. The unit includes preparation for proceedings, presenting evidence and following up on outcomes of proceedings. Proceedings may be to criminal, coronial, civil or military courts.

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 search and seizure of digital evidence.

Those undertaking this unit would work independently, with minimal supervision, while performing complex tasks, including making complex judgements. They would use discretion and judgement and take responsibility for the quality of their outputs.

No licensing, legislative or certification requirements apply to this 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 Prepare for legal proceedings | 1.1 Confirm arrangements for role and involvement in legal proceedings
1.2 Prepare documents and other exhibits
1.3 Identify precedents relevant to the procedures
1.4 Provide assistance to counsel as required |
| 2 Present expert evidence | 2.1 Apply rules of evidence relevant to the jurisdiction
2.2 Translate technical practices and concepts into non-technical language, with explanations of technologies involved
2.3 Present evidence in a clear, concise and articulate manner
2.4 Provide considered expert evidence consistent with relevant qualifications and expertise in the area of digital forensics |
| 3 Monitor and follow up the outcomes of legal proceedings | 3.1 Note and file the outcomes of proceedings and complete reports where required
3.2 Note and action feedback from counsel and/or legal authority and comments by deciding authority
3.3 Review outcomes of proceedings to ensure knowledge of trends and precedents is current
3.4 Recommend changes to organisational policy and proceedings arising from rulings and decisions |

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 DEFFOR009 Give evidence of electronic media crime.

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 DEFFOR019 Give evidence of digital media crime

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:

- applying the constraints of individual qualifications
- applying the rules of evidence
- describing complex technical procedures in simple non-technical language
- maximising the potential evidentiary value of the digital evidence
- presenting expert evidence
- writing complex reports.

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:

- constraints and limitations of individual qualifications
- court procedures relevant to the specific legal process
- legislative requirements of presenting evidence
- legislative, policy and procedural context in which digital forensic evidence is given
- procedures and protocols in different judicial systems
- prosecution process
- role of expert witnesses
- role of legal personnel
- rules of evidence
- types of evidence admissible in judicial systems
- use of forensic documentation and notes in giving 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>