



**Australian Government**

# **DEFFOR003 Gather and analyse electronic information**

**Release: 1**

# DEFFOR003 Gather and analyse electronic information

## Modification History

| Release | Comments                                                                                                          |
|---------|-------------------------------------------------------------------------------------------------------------------|
| 1       | This unit was released in DEF Defence Training Package release 1.0 and meets the Standards for Training Packages. |

## Application

This unit describes the skills required to gather and analyse electronic information to support electronic forensic investigations. It includes identifying, collecting, analysing, presenting and maintaining information, compiling notes and statements of evidence, and removing portable media from machines. It also covers the use of initial screening technology. In the context of this unit, portable media refers to external hard drives, SIM cards, recording media, flash drives, tape drives and other peripherals.

This unit applies to those working in the gathering and analysis of electronic 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 WHS and the gathering and analysis of electronic 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.

## Competency Field

Electronic Forensics

## Elements and Performance Criteria

| ELEMENTS                                        | PERFORMANCE CRITERIA                                                                                                                                                                                    |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Elements describe the essential outcomes        | Performance criteria describe the performance needed to demonstrate achievement of the element. Where bold italicised text is used, further information is detailed in the range of conditions section. |
| <b>1. Detect and record electronic evidence</b> | 1.1 Detect electronic evidence using observational techniques and technological methods.<br>1.2 Record electronic evidence prior to examination.                                                        |

|                                                   |                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                   | 1.3 Document the recorded electronic evidence.                                                                                                                                                                                                                                                                                                                           |
| <b>2. Collect and analyse electronic evidence</b> | 2.1 Collect electronic evidence by handpicking or removal of portable media from machine to prevent contamination or loss.<br>2.2 Ensure collected electronic evidence is sufficient in detail, where possible, to allow all potential examinations/analysis to be carried out.<br>2.3 Conduct initial analysis of collected electronic evidence and report on outcomes. |
| <b>3. Package electronic evidence</b>             | 3.1 Package and store items to maintain continuity and prevent degradation or contamination.<br>3.2 Enter details of electronic evidence collected in case notes and, where appropriate, in the exhibit register to maintain the chain of custody.                                                                                                                       |

## Foundation Skills

The foundation skills demands of this unit have been mapped for alignment with the Australian Core Skills Framework (ACSF). The following tables outline the performance levels indicated for successful attainment of the unit.

ACSF levels indicative of performance:

|                       |   |   |   |   |         |   |   |   |   |                 |   |   |   |   |                    |   |   |   |   |              |   |   |   |   |
|-----------------------|---|---|---|---|---------|---|---|---|---|-----------------|---|---|---|---|--------------------|---|---|---|---|--------------|---|---|---|---|
| 1                     | 2 | 3 | 4 | 5 | 1       | 2 | 3 | 4 | 5 | 1               | 2 | 3 | 4 | 5 | 1                  | 2 | 3 | 4 | 5 | 1            | 2 | 3 | 4 | 5 |
| Learning              |   |   |   |   | Reading |   |   |   |   | Writing         |   |   |   |   | Oral communication |   |   |   |   | Numeracy N/A |   |   |   |   |
| Performance variables |   |   |   |   |         |   |   |   |   |                 |   |   |   |   |                    |   |   |   |   |              |   |   |   |   |
| 1                     | 2 | 3 | 4 | 5 | 1       | 2 | 3 | 4 | 5 | 1               | 2 | 3 | 4 | 5 | 1                  | 2 | 3 | 4 | 5 | 1            | 2 | 3 | 4 | 5 |
| Support               |   |   |   |   | Context |   |   |   |   | Text complexity |   |   |   |   | Task complexity    |   |   |   |   |              |   |   |   |   |

Further information on ACSF and the foundation skills underpinning this unit can be found in the Foundation Skills Guide on the GSA website.

## Unit Mapping Information

No equivalent unit.

## Links

Companion Volume implementation guides are found in VETNet -

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

Companion Volume implementation guides are found in VETNet -

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

Companion Volume implementation guides are found in VETNet -

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

# Assessment Requirements for DEFFOR003 Gather and analyse electronic information

## Modification History

| Release | Comments                                                                                                                              |
|---------|---------------------------------------------------------------------------------------------------------------------------------------|
| 1       | These Assessment Requirements were released in DEF Defence Training Package release 1.0 and meet the Standards for Training Packages. |

## Performance Evidence

Evidence required to demonstrate competence must satisfy all of the requirements of the elements and performance criteria. If not otherwise specified the candidate must demonstrate evidence of performance of the following on at least one occasion.

- detecting electronic evidence from digital and analogue recording and communication equipment including at least one of:
  - hard drives
  - recording media
  - flash drives
  - tape drives
  - random-access memory (RAM)
  - read-only memory (ROM)
  - basic input/output system (BIOS)
  - other peripherals
- solving problems and making analytical decisions in response to a range of electronic evidence contexts, including the systematic examination of electronic evidence items
- removing media
- analysing electronic information
- maximising the evidentiary value of the electronic evidence
- handling exhibits and preserving continuity of evidence
- using specialised evidence recording technology and equipment
- packaging, preserving and storing specific evidence types with consideration of:
  - physical nature of exhibit
  - electronic stability
  - packaging medium
  - tamper-evident seals
  - exhibit labels
  - storage temperature

- operating safely
- recording evidence using methods including at least one of:
  - photographic
  - sketch plan
  - handwritten notes
  - video recording
  - digital imaging
  - physical capture
  - computer generated data
  - audio recording
  - global positioning system (GPS)

## Knowledge Evidence

Evidence required to demonstrate competence must satisfy all of the requirements of the elements and performance criteria. If not otherwise specified the depth of knowledge demonstrated must be appropriate to the job context of the candidate.

- legislative, policy and quality system context and requirements
- WHS practices to be followed when recording, collecting and packaging electronic evidence
- range of techniques available for gathering, collecting, packaging and preserving electronic evidence
- required forensic documentation for recording and collecting electronic evidence
- roles and functions of other forensic discipline specialists in the recording, collection, preservation and continuity of electronic evidence

## Assessment Conditions

Competency should be assessed in an actual workplace or in a simulated environment, with access to equipment and infrastructure appropriate to the outcome. Competency should be demonstrated over time to ensure the candidate is assessed across a variety of situations, with access to electronic devices with content suitable for forensic extraction including mobile devices, computers or communications equipment.

Assessors must satisfy the NVR/AQTF mandatory competency requirements for assessors.

## Links

Companion Volume implementation guides are found in VETNet -

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

Companion Volume implementation guides are found in VETNet -

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