Australian Government

ICTCYS607 Acquire digital forensic data

Release: 1

ICTCYS607 Acquire digital forensic data

Modification History

Release	Comments
Release 1	This version first released with ICT Information and Communications Technology Training Package Version 6.0.

Application

This unit describes the skills and knowledge required to acquire, extract and analyse data from devices and workstations, including mobile devices, networked devices, smart devices, Internet of Things (IoT) devices and microcontrollers, USBs, applications, networks and systems. It applies to skills needed to extract evidence pertaining to either a forensic investigation directly caused on a computer, or as part of evidence relating to a crime or e-crime.

It applies to those working in cyber and forensic roles including, digital forensic examiners, incident responders and corporate investigators and are responsible for forensic data retrieval.

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

Unit Sector

Cyber security

Elements and Performance Criteria

ELEMENT	PERFORMANCE CRITERIA
Elements describe the essential outcomes.	*Performance criteria describe the performance needed to demonstrate achievement of the element.*
1. Confirm incident and prepare to acquire data	1.1 Confirm and gather initial information on reported incident according to organisational policies and procedures 1.2 Research and assess occurrence according to organisational forensic data extraction requirements 1.3 Research and identify all laws and legislation required for data extraction tasks 1.4 Discuss and confirm if acquisition is required with required personnel 1.5 Consult and gather key incident information from required

ELEMENT	PERFORMANCE CRITERIA
	personnel 1.6 Identify device and components pertaining to incident according to task requirements 1.7 Develop and document data extraction plan and information gathered according to organisational requirements 1.8 Submit documentation to required personnel and seek and respond to feedback
2. Acquire forensic data	2.1 Contact and gather information from required personnel 2.2 Seize device pertaining to incident according to incident and legislation 2.3 Access and open device according to data extraction task requirements 2.4 Secure device's networks, data logs, firewalls and hashing according to task requirements 2.5 Initiate data extraction according to task requirements and confirm that no data is tampered or deleted 2.6 Confirm completion of retrieval according to task requirements 2.7 Verify the hash according to task requirements 2.8 Document observations and findings and methodology
3. Analyse forensic data	3.1 Analyse data and verify against incident scope, information, devices and evidence 3.2 Document findings and analysis and submit to required personnel 3.3 Discuss abnormalities and confirm further evidence, devices and information needed 3.4 Make additional extractions according to task and technical requirements 3.5 Analyse network conversations according to task requirements 3.6 Verify chain of custody according to hash according to task requirements 3.7 Update findings and methodology in documentation according to organisational needs
4. Finalise data acquisition	4.1 Prepare data extracts and documentation for submission according to organisational and legislative requirements 4.2 Submit data extracts and analysis according to organisational and legislative requirements 4.3 Retrieve sign off from required personnel and gather feedback according to organisational policies and procedures

Foundation Skills

This section describes those language, literacy, numeracy and employment skills that are essential to performance but not explicit in the performance criteria.

SKILL	DESCRIPTION
Reading	• Interprets information from technical, manufacturer, organisational and legislative documentation to determine and confirm job requirements
Writing	• Develops workplace and legislative documentation for a specific audience, using detailed language to convey explicit information, requirements and recommendations
Planning and organising	• Develops a strategic plan form task specification that include developing the operational detail in stages, regularly reviewing priorities and performance during data extraction tasks, and identifying and addressing issues as they arise
Problem solving	• Initiates ways to engage in strategic problem-solving approaches that incorporates linear and non-linear methodologies
Self-management	• Uses systematic processes, setting goals, gathering required information and identifying and evaluating options against agreed criteria
Technology	• Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world

Unit Mapping Information

No equivalent unit. New unit.

Links

Companion Volume Implementation Guide is found on VETNet - https://vetnet.gov.au/Pages/TrainingDocs.aspx?q=a53af4e4-b400-484e-b778-71c9e9d6aff2