SINGAPORE
WORKFORCE SKILLS
QUALIFICATIONS

NATIONAL
COMPETENCY STANDARD

Framework	:	National Infocomm Competency Framework
Competency Category	:	Security Services
Competency Code	:	IT-SSE-305S-1
Competency Unit	:	Conduct digital forensic investigation
Competency Descriptor	:	This unit defines the competency required to conduct digital forensic investigation. It covers the activities and steps necessary to perform collection and preservation of digital evidences, examining and analysing digital evidences, reporting findings for legal proceedings.
Complexity Level	:	3 (Entrant level)
Credit Value	:	4
Version Number	:	1
Effective Date	:	27 August 2009
Review Date	:	-
Developer	:	IDA
Custodian	:	IDA

iDA
SINGAPORE

Competency Unit Code IT-SSE-305S-1	Complexity Level 3 (Entrant level)
Competency Unit Title Conduct digital forensic investigation	

Relevant Job Roles /Occupations
The job roles that this unit would be relevant to include: **Expert / Management:** • Digital Forensic Investigation Manager **Specialist (Technical):** • Digital Forensic Investigator **Entrant:** • Associate Digital Forensic Investigator Please refer to the NICF portal for their job descriptions.

Performance Statements The critical aspects of job performance, stating the evaluative criterion and expected outcome of tasks.
A competent individual must be able to successfully perform the following: 1. Perform collection and preservation of digital evidences from the source using appropriate tools and technologies 2. Examine the preserved digital evidence for suitability 3. Analyse the preserved digital forensic evidences 4. Document the digital evidences and conclusions of findings 5. Present the digital forensic findings which comply to legal or corporate requirements

Competency Unit Code	**Complexity Level**
IT-SSE-305S-1	3 (Entrant level)
Competency Unit Title Conduct digital forensic investigation	

Underpinning Knowledge

Knowledge that is acquired during the course of training and is essential to support competent performance. May include principles, processes, methods, procedures, legislative/legal requirements, interactions with others.

A competent individual needs to know and understand:

1. Knowledge of various computer, network and mobile evidences
2. Knowledge of computer, network and mobile forensic tools and techniques
3. Knowledge of various threats and vulnerabilities
4. Knowledge of applicable law and regulations
5. Concepts of chain of custody
6. Procedures and steps required for digital evidence acquisition including preserving and maintaining integrity of evidence
7. Knowledge of safe handling of evidence including packaging, transporting and storing of incident
8. Knowledge of various methods used to examine and analyse digital evidence

Range of Application

Types of contexts or circumstances under which competent performance may be demonstrated. It gives further references to specific areas or terms in the Performance Statements.

STANDARDS AND GUIDELINES

Digital forensic investigation phases are:

- Assessment
- Acquisition
- Examination
- Reporting

Digital forensic tools may include:

Competency Unit Code	**Complexity Level**
IT-SSE-305S-1	3 (Entrant level)
Competency Unit Title Conduct digital forensic investigation	

Range of Application

Types of contexts or circumstances under which competent performance may be demonstrated. It gives further references to specific areas or terms in the Performance Statements.

- Write Blocker
- Open source / commercial multipurpose forensic software
- Data or partition recovery software
- Data wiping
- Disk Imaging
- Digital Forensics String Search (DFSS)
- Hashing
- Mobile Data Acquisition
- Packet Capturing / Protocol Analyzer

Digital forensics acquisition concepts:

- Live acquisition and dead acquisition
- Volatile data and non volatile data

Digital forensics examination and analysis concepts:

- Volume analysis
- File system analysis
- Application analysis
- Network analysis
- Correlation

Evidence Sources

Types of proof (product, process and knowledge evidences) an individual may produce to demonstrate competent performance.

Product evidence:

- Samples of computer, network and mobile evidence
- Computer forensic investigation report that may document:

Competency Unit Code	**Complexity Level**
IT-SSE-305S-1	3 (Entrant level)
Competency Unit Title	
Conduct digital forensic investigation	

Evidence Sources

Types of proof (product, process and knowledge evidences) an individual may produce to demonstrate competent performance.

- Assessment of case, location and evidence
- Acquisition procedures
- Packaging, transportation and storage procedures
- Analysis and examination procedures
- Conclusion of case

Process evidence:

- Demonstrate the ability to identify a suitable acquisition strategy to collect digital evidences
- Demonstrate the ability for proper handling of evidence including the packaging, transporting and storing of evidence
- Demonstrate the ability to examine and analyse digital evidence including recovering hidden, deleted or corrupted data
- Demonstrate the ability to use software or hardware forensic tools to perform digital forensic investigation

Knowledge evidence:

- Written report detailing the acquisition plans of digital evidence
- Written report describing evaluation and analysis result of the digital evidence
- Written report documenting the handling of evidence that maintain the chain of custody concept

Version Control Record

Version	Effective Date	Changes	Author
1.0	27 August 2009	Initial version	IDA