Next Generation Higher National Unit Specification

Digital Forensics (SCQF level 8)

Unit code: J7E4 48

SCQF level: 8 (16 SCQF credit points)

Valid from: session 2023–2024

Prototype unit specification for use in pilot delivery only (version 1.0) June 2023

This unit specification provides detailed information about the unit to ensure consistent and transparent assessment year on year.

This unit specification is for teachers and lecturers and contains all the mandatory information required to deliver and assess the unit.

This edition: June 2023 (version 1.0)

Unit purpose

This unit introduces learners to the digital forensics process as it relates to computers, networks, and virtual infrastructures, as well as other digital devices, such as laptops and mobile technology.

This is a specialist unit, intended for learners who wish to gain detailed knowledge and understanding of the digital forensics investigatory process. It is particularly suitable for learners who wish to develop specific knowledge and skills in the following areas:

- identifying different sources of evidence
- using tools to acquire, preserve and analyse digital evidence
- relevant laws and quality processes in the preparation of forensic documentation for a court of law

Entry to the unit is at your centre’s discretion. Learners should have prior knowledge and understanding of:

- using application programs on a computer
- computer hardware components
- networks and the internet
- file system operation

They can evidence this by achievement of computing units at SCQF level 7.

On completion of the unit, learners may progress to digital forensics-related units at SCQF level 9 and beyond, or to other cyber security-related qualifications.

Unit outcomes

Learners who complete this unit can:

1 explore methods for digital forensic evidence examination
2 perform digital forensic acquisition and preservation
3 analyse digital forensic evidence
4 present forensic documentation

Evidence requirements

Learners must provide knowledge evidence and product evidence.

Knowledge evidence

Knowledge evidence comprises the descriptions and explanations required for outcomes 1 and 4, and parts of outcomes 2 and 3. Learners must be able to identify the different methods that are available to examine digital evidence. They must demonstrate knowledge of the tools and techniques they can use to acquire and preserve digital evidence, as well as the relevant evidence that they must consider when preparing forensics documentation.

You can sample the knowledge evidence when testing is used, but you must include one or more questions on each of the following:

- forensically safe working environments
- live and dead analysis
- volatile and non-volatile evidence
- storage and management of evidence
- sources of evidence
- tools used in the digital forensics process
- contemporaneous procedures
- relevant laws and policy
- consideration for quality processes
- confidentiality

Learners’ knowledge evidence can be written, oral, or a combination of both. Evidence can be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

Product evidence

Product evidence relates to parts of outcomes 2 and 3 and demonstrates that learners can produce desired outputs and appropriate evidence analysis under lightly controlled conditions as part of the forensic acquisition and analysis process. For example, you could use the acquisition of a forensic image from a USB device, the use of an appropriate analysis tool on the forensic image, and the outcomes of that analysis.

You can give learners access to resources and reference materials at this stage, however learners should produce evidence for outcomes 2 and 3 under more controlled (laboratory) conditions — as they would be if they were conducted as part of an official digital forensic investigation.

Learners can produce product evidence over an extended period in lightly controlled conditions or generate it holistically in conjunction with other units in a group award. Evidence produced in lightly controlled conditions must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The standard of evidence should be consistent with the SCQF level of the unit.

Knowledge and skills

The following table shows the knowledge and skills covered by the unit outcomes:

Knowledge	Skills
Learners should understand: ♦ forensically safe environments ♦ live and dead analysis ♦ volatile and non-volatile information ♦ storage mechanisms ♦ sources of evidence ♦ chain of custody ♦ disk images ♦ virtual systems ♦ system and network information ♦ alternative file systems ♦ slack space	Learners can: ♦ examine and validate digital forensic evidence ♦ maintain a forensically safe environment ♦ carry out forensic imaging ♦ maintain data integrity ♦ analyse digital forensic evidence ♦ report on the outcomes of an investigation

Meta-skills

Throughout the unit, learners develop meta-skills to enhance their employability in the computing sector.

The unit helps learners develop the meta-skills of self-management, social intelligence and innovation. Learners should develop meta-skills naturally throughout the unit. You should encourage learners to develop a minimum of one area in each of the three categories, but they do not need to cover all suggested subsections. The following suggestions may help shape delivery and assessment, and vary depending on the chosen topics and assessment method.

Self-management

This meta-skill includes:

- focusing: sorting and filtering information in relation to a task; understanding a defined range of core theories, concepts, principles and terminology
- integrity: displaying current professional and ethical codes and practices
- adapting: using a range of approaches to formulate and critically evaluate evidence-based solutions and responses to defined and/or routine problems and issues
- initiative: displaying independent thinking; having a responsible attitude

Social intelligence

This meta-skill includes:

- communicating: sharing information with a range of audiences and for a range of purposes
- collaborating: working effectively with others; social perceptiveness
- leading: having a clear vision that enables others to be inspired, influenced and motivated

Innovation

This meta-skill includes:

- curiosity: carrying out routine lines of enquiry, development or investigation into professional-level problems and issues
- creativity: generating ideas; problem solving
- sense-making: analysing and synthesising; seeing the bigger picture
- critical thinking: evaluating and drawing conclusions from information

Delivery of unit

We recommend that you teach the outcomes for this unit in sequential order. This ensures that, from outcome 1, learners have the required understanding of:

- how to implement a forensically safe environment
- the methodologies available
- how to manage a project

This leads to the practical elements of outcomes 2 and 3 and then the final documentation stages of outcome 4.

The time required varies depending on the previous experience of individual learners. Based on 40 hours delivery and assessment time, we suggest the following distribution:

Outcome 1 — Explore methods for digital forensic evidence examination
(10 hours)

Outcome 2 — Perform digital forensic acquisition and preservation
(10 hours)

Outcome 3 — Analyse digital forensic evidence
(10 hours)

Outcome 4 — Present forensic documentation
(10 hours)

Additional guidance

The guidance in this section is not mandatory.

Content and context for this unit

There are many delivery methods that you can use for this unit, such as presentations, demonstrations, practical exercises, films, videos and podcasts. Using these methods, you must provide context, set objectives along with experiences and outcomes, and regularly review progress. We encourage group discussions and other collaborative techniques. Ideally, you should simulate a practical forensic laboratory environment for practical aspects of the unit.

Early in the unit, you should make learners aware of the various UK guidelines and legislation that are prevalent in the digital forensics and investigatory process, including the:

- Computer Misuse Act 1990
- Data Retention and Investigatory Powers Act 2014
- Police and Criminal Evidence Act 1984
- Investigatory Powers Act 2016
- Association of Chief Police Officers (ACPO) ‘Good Practice Guide for Digital Evidence’, (published 2012)

Approaches to assessment

You can carry out testing at any time, however we recommend that you do it towards the end of the unit (but with sufficient time for remediation and re-assessment). When you use continuous assessment (such as the use of a blog), this should begin early and continue throughout the duration of the unit.

There are opportunities for formative assessment at various stages in the unit. For example, you can carry it out on the completion of each outcome to ensure that learners have grasped the knowledge contained within it. This provides you with an opportunity to diagnose misconceptions, and to intervene to remedy them before progressing to the next outcome.

Equality and inclusion

This unit is designed to be as fair and as accessible as possible with no unnecessary barriers to learning or assessment.

You should take into account the needs of individual learners when planning learning experiences, selecting assessment methods or considering alternative evidence.

Guidance on assessment arrangements for disabled learners and/or those with additional support needs is available on the assessment arrangements web page: www.sqa.org.uk/assessmentarrangements.

Information for learners

Digital Forensics (SCQF level 8)

This information explains:

- what the unit is about
- what you should know or be able to do before you start
- what you need to do during the unit
- opportunities for further learning and employment

Unit information

This unit is designed to provide you with an introduction to the more detailed aspects of the digital forensic investigatory process as it relates to computers, networks, and virtual infrastructures, as well as other digital devices, such as laptops and mobile technology.

It is suitable if you have an interest in cyber security or you are working towards the HND Cyber Security at SCQF level 8 or HND Networking and Cloud Infrastructure at SCQF level 8.

Before starting the unit, it is helpful if you have knowledge and understanding of:

- using application programs on a computer
- computer hardware components
- networks and the internet
- file system operation

The unit broadly covers the following topics:

- methods used for digital forensics investigation
- forensically safe environments
- types of analysis
- managing the forensics process
- digital forensics acquisition
- digital evidence analysis
- relevant legislation
- policy and quality processes
- confidentiality

The unit provides you with the opportunity to study a contemporary topic in the field of digital forensics in the broader context of cyber security.

There is a mix of both theoretical and practical tasks in the unit. The theoretical tasks provide you with the experience of implementing pre-requisite environments to ensure that you carry out the digital forensic acquisition and analysis with minimal risk of evidence contamination.

You learn where to look for digital evidence. Practical tasks give you the experience of using appropriate tools to acquire and analyse digital evidence, again, while ensuring that evidence is not contaminated. You also examine up-to-date UK legislation and determine the role of company policy and quality processes in the preparation of forensic documentation.

You can learn in a variety of ways. This could be through active, project-based and collaborative learning, and you could be assessed using a real-world scenario. You may collect your assessment evidence in an e-portfolio where you can showcase your work.

By the end of the unit, you understand the importance of the environments in which digital forensics investigations take place, and how to look for, acquire, analyse and manage digital evidence. You also learn how to prepare the finer details of forensic documentation.

Throughout the unit, you develop meta-skills covering self-management, social intelligence and innovation.

On completion of the unit, you may progress to digital forensics-related units at SCQF level 9 and beyond, or to other cyber security-related qualifications.

Administrative information

Published: June 2023 (version 1.0)

Superclass: CB

History of changes

Version	Description of change	Date

Note: please check SQA's website to ensure you are using the most up-to-date version of this document.