## Higher National Unit Specification

## General information

**Unit title:** Digital Forensics Case Studies (SCQF level 7)

**Unit code:** J0HG 34

**Superclass:** CC

**Publication date:** June 2018

**Source:** Scottish Qualifications Authority

**Version:** 01

## Unit purpose

The purpose of this unit is to introduce learners to perform digital forensics in different scenarios. The unit covers knowledge and skills related to digital forensics, including guidelines, best practices, chain of custody, analysis and report writing for different types of cases.

This is a **specialist** unit, intended for learners with an interest in cyber security. It is suitable for learners who are undertaking the HNC in Cyber Security or related area, and is particularly appropriate for learners who have completed J0HL 34 *Digital Forensics* or H1EN 34 *Computer Forensics: Fundamentals*.

The unit explores the importance of memory acquisition techniques, software tools, preserving a digital environment, memory dump formats, volatile memory, disk artefacts, master file table and extracting files. Learners will also gain experience in creating and presenting a case.

At the completion of this unit, learners will be able to perform digital forensics on volatile and non-volatile data, memory interrogation, digital artefacts, evidence gathering, maintaining confidentiality, integrity, guidelines, and chain of custody.

## Outcomes

On successful completion of the unit, the learner will be able to:

1 Perform analysis on volatile data for digital forensics.
2 Perform analysis on non-volatile data for digital forensics.
3 Perform analysis on network data for digital forensics.

## Higher National Unit Specification: General information (cont)

**Unit title:** Digital Forensics Case Studies (SCQF level 7)

## Credit points and level

1 Higher National unit credit at SCQF level 7: (8 SCQF credit points at SCQF level 7)

## Recommended entry to the unit

No previous knowledge or experience is required. However, it would be beneficial if learners possessed knowledge of operating system structures, network device logs, mobile operating systems, cloud, and virtual machines.

Some previous knowledge of digital forensics is recommended but not essential. This may be evidenced by possession of J0HL 34 *Digital Forensics* or H1EN 34 *Computer Forensics: Fundamentals*.

## Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification. This module provides opportunities to achieve *Working With Others*, *Problem Solving*.

There is no automatic certification of Core Skills or Core Skill components in this unit.

## Context for delivery

If this unit is delivered as part of a group award, it is recommended that it should be taught and assessed within the subject area of the group award to which it contributes.

This unit should, ideally, be delivered and assessed as part of the HNC Cyber Security at SCQF level 7. The unit can, however, be delivered on a standalone basis. It is suggested that this unit be delivered alongside J0HL 34 *Digital Forensics*, in order to provide learners with broader knowledge and skills in this area.

## Equality and inclusion

This unit specification has been designed to ensure that there are no unnecessary barriers to learning or assessment. The individual needs of learners should be taken into account when planning learning experiences, selecting assessment methods or considering alternative evidence.

Further advice can be found on our website **www.sqa.org.uk/assessmentarrangements**.

## Higher National unit specification: Statement of standards

## Unit title: Digital Forensics Case Studies (SCQF level 7)

Acceptable performance in this unit will be the satisfactory achievement of the standards set out in this part of the unit specification. All sections of the statement of standards are mandatory and cannot be altered without reference to SQA.

Where evidence for outcomes is assessed on a sample basis, the whole of the content listed in the knowledge and/or skills section must be taught and available for assessment. Learners should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

## Outcome 1

Perform analysis on volatile data for digital forensics.

### Knowledge and/or skills

- Definition of volatile data
- Chain of custody, including relevant legislation
- Methods and tools to acquire volatile data
- Types of data in volatile memory
- Processes, registry, network information, passwords
- Ways of preserving confidentiality, integrity and availability during investigation phases
- String search, memory-mapped files, file signature search
- Analysis documentation

## Outcome 2

Perform analysis on non-volatile data for digital forensics.

### Knowledge and/or skills

- Definition of non-volatile data
- Methods and tools to acquire non-volatile data
- Chain of custody, including relevant legislation
- Identification of data sources
- Imaging, hashing and accessing data
- File system analysis, web archives, listing users
- Analysis documentation

## Outcome 3

Perform analysis on network data for digital forensics.

### Knowledge and/or skills

- Types of network data
- Methods and tools to acquire network data
- Live packet capture analysis
- Client and server operating system, network devices logs
- Protocols, ports and log analysis
- Web proxy, firewalls and intrusion detection system logs
- Wireless network forensics

## Higher National unit specification: Statement of standards (cont)

## Unit title: Digital Forensics Case Studies (SCQF level 7)

### Evidence requirements for this unit

Learners will need to provide evidence to demonstrate the knowledge and/or skills across all outcomes. The evidence requirements for this unit will take two forms.

1 Knowledge evidence
2 Product evidence

The **knowledge evidence** will relate to all three outcomes. Knowledge evidence is required for all knowledge and/or skills statements except those explicitly relating to skills. The following knowledge must be demonstrated:

- Definitions of volatile, non-volatile and network data
- Identification of forensically sound methods of gathering volatile, non-volatile and network data
- Identification of various different tools used to gather forensic evidence
- Description of chain of custody in forensics investigations
- Identification of relevant legislation
- Identification of **at least** three types of data found in volatile memory
- Recognition of importance of forensic case study report writing
- Ways of preserving confidentiality, integrity, and availability during investigation phases
- Identification of various file systems, files and strings to perform search operations on non-volatile data
- Identification of network data in forensic analysis and different types of network data that can be collected
- Identification of core network protocols, logging protocols, intrusion detection systems and firewalls
- Identification of wireless network protocols, capture methodologies, inherent weaknesses, typical attack methodologies

Knowledge evidence may be sampled when testing is used. When testing is used, it must be under supervised conditions and it must be controlled in terms of location and timing. Access to reference material is not permitted.

The knowledge evidence may be written or oral or a combination of these. Evidence may be captured, stored and presented in a range of media (including audio and video) and formats (analogue and digital).

The **product evidence** will relate to all three outcomes. It will demonstrate that the learner can carry out forensic investigation, analysis, and documentation tasks to a given scenario using appropriate tools, methods and processes.

It is recommended to use a holistic approach to assessment that covers all the knowledge and practical skills across the three outcomes. More information will be provided in the support notes.

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. Appropriate level descriptors should be used when making judgements about the evidence.

## Higher National unit specification: Statement of standards (cont)

**Unit title:** Digital Forensics Case Studies (SCQF level 7)

When evidence is produced in uncontrolled or loosely controlled conditions it must be authenticated. The Guide to Assessment provides further advice on methods of authentication.

The support notes section of this specification provides specific examples of instruments of assessment that will generate the required evidence.

## Higher National Unit Support Notes

## Unit title: Digital Forensics Case Studies (SCQF level 7)

Unit support notes are offered as guidance and are not mandatory.

While the exact time allocated to this unit is at the discretion of the centre, the notional design length is 40 hours.

## Guidance on the content and context for this unit

The context for this unit is the increase in cybercrime that has taken place over the past decade and the associated demand for cybersecurity professionals. There has been a huge demand for cybersecurity professionals over recent years. However, it is anticipated that this demand will increase. This unit is a specialist unit and is offered as an optional unit within the HN Cyber Security framework. Learners entering this course should, ideally, have some knowledge of computer architecture, fundamentals of computer systems, hardware and computer networks.

The purpose of this unit is to introduce learners to practical aspects that comprise the digital forensics investigatory process. The unit covers the three types of data that can be collected and used for digital forensics ie, volatile, non-volatile and network data. As well as learning the theoretical elements associated with digital investigations, learners will also learn how to identify malicious activity and acquire the necessary research skills to keep up with changes in both law and forensic computing research methodologies.

This is an introductory unit; therefore, learners need not cover topics in a detailed manner. It is important, however, that good coverage is given to each of the knowledge statements in order to provide the learner with a broad view of the outcomes and the steps to be taken throughout the investigatory process. The unit must ensure that the learner is understanding the difference between the different types of data; the importance of the chain of custody and of forensic case study report writing.

Please note that the following guidance, relating to specific outcomes, does not seek to explain each knowledge/skills statement, which is left to the professionalism of the teacher. It seeks to clarify the statement of standards where it is potentially ambiguous. It focuses on non-apparent teaching and learning issues that may be over-looked, or not emphasised, during unit delivery. As such, it is not representative of the relative importance of each knowledge/skill.

**Outcome 1**

This outcome introduces the learner to perform a forensic investigation on volatile data. Learners must be made aware of volatile data and places to acquire volatile data in a crime scene. Learners must be made aware of different types of information that can be extracted from volatile data. For example, how to see running processes in memory, network information, performing string search operations, file signature search, and extracting registry from memory. Learners must learn where to look to find evidence, how to preserve evidence, maintaining integrity of evidence and how to follow chain of custody.

## Higher National Unit Support Notes (cont)

## Unit title: Digital Forensics Case Studies (SCQF level 7)

**Outcome 2**

This outcome introduces the learner to perform forensic investigation on non-volatile data. Learners must be made aware of types of non-volatile data that can be gathered for forensic analysis. Learners must be made aware of types of information that can be extracted from non-volatile data. For example, performing analysis for different operating system file systems, finding deleted files, searching through slack space, web archives, e-mail extraction, temporary files, user sids, listing users, etc.

**Outcome 3**

This outcome introduces the learner to perform forensic investigation on network data. The learner must be made aware of network data and different means of capturing and analysing existing or live data. For example, the learner must know about different protocols like ARP, DHCP, DNS, Telnet, SSH, HTTP, HTTPS, TLS, IKE, IPSEC and how to identify these packet streams in network data. The learner must be taught the importance of logs produced by various devices like IDS, IPS, Firewalls, Web proxys, and how to analyse them.

There are some National Occupational standards (NOS) to which this unit relates well, these are:

- TECIS60643 Carry out digital forensic examination activities
- ESKISP6074.03 Conduct forensic examination under supervision
- SFJ CO7 Conduct network investigations

## Guidance on approaches to delivery of this unit

It is recommended that the outcomes for this unit are taught sequentially. This is to make sure that learners have the required background and theoretical knowledge to perform digital forensics case studies, as specified in Outcome 1, 2 and 3.

Given the practical nature of the unit, it is recommended that the unit is delivered alongside the unit J0HL 34 *Digital Forensics*. This will provide learners with theoretical knowledge required to perform Digital Forensic case studies.

There are many different delivery methods that can be used for this unit. For example, presentations, demonstrations and practical exercises can be used, as well as the use of film, video and podcast. However, when this approach is used, it is vital that the educator provides the context, sets objectives, and regularly reviews progress. Group discussions and other collaborative techniques are encouraged.

Learners should be made aware early in the unit of the various UK legislation and laws that are prevalent in the digital forensics and investigatory process, such as the Computer Misuse Act 1990, the Data Retention and Investigatory Powers Act 2014 and the Police and Criminal Evidence Act 1984, for example.

A suggested distribution of time, across the outcomes, is:

Outcome 1: 15 hours
Outcome 2: 15 hours
Outcome 3: 10 hours

Summative assessment may be carried out at any time. However, when testing is used (see evidence requirements), it is recommended that this is carried out towards the end of the unit (but with sufficient time for remediation and re-assessment). When continuous assessment is used (such as the use of a web log), this could commence early in the life of the unit and be carried out throughout the duration of the unit.

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

## Guidance on approaches to assessment of this unit

Evidence can be generated using different types of assessment. The following are suggestions only. There may be other methods that would be more suitable to learners.

Centres are reminded that prior verification of centre-devised assessments would help to ensure that the national standard is being met. Where learners experience a range of assessment methods, this helps them to develop different skills that should be transferable to work or further and higher education.

A variety of methods can be used to gain evidence: a case study or group project for Outcomes 1 and 2. Outcome 3 can be performed on pre-captured packets in a controlled environment to demonstrate knowledge and product evidence. All of the outcomes can be achieved through one single project to demonstrate key knowledge and skills.

A more contemporary approach to assessment would involve the use of a web log (blog) to record learning (and the associated activities) throughout the life of the unit. The blog would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings). The blog should be assessed using defined criteria to permit a correct judgement about the quality of the digital evidence. In this scenario, every knowledge and skill must be evidenced; sampling would not be appropriate.

Formative assessment could be used to assess learners' knowledge at various stages throughout the life of the unit. An ideal time to gauge their knowledge would be at the end of each outcome. This assessment could be delivered through an item bank of selected response questions, providing diagnostic feedback to learners (when appropriate).

If a blog is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent from the blog, and intervention could take place to correct misunderstandings on an on-going basis.

## Opportunities for e-assessment

E-assessment may be appropriate for some assessments in this unit. By e-assessment we mean assessment which is supported by Information and Communication Technology (ICT), such as e-testing or the use of e-portfolios or social software.

## Higher National Unit Support Notes (cont)

## Unit title: Digital Forensics Case Studies (SCQF level 7)

Centres which wish to use e-assessment must ensure that the national standard is applied to all learner evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. The most up-to-date guidance on the use of e-assessment to support SQA's qualifications is available at **www.sqa.org.uk/e-assessment**.

## Opportunities for developing Core and other essential skills

There are opportunities to develop the Core Skills in *Information and Communication Technology*, working with others and *Problem Solving* (at SCQF level 6) during this unit.

The unit will also provide opportunities to develop broader skills, such as citizenship, which will be required when considering the ethical aspects associated with cybercrime and the investigatory process.

## History of changes to unit

| Version | Description of change | Date |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

## General information for learners

## Unit title: Digital Forensics Case Studies (SCQF level 7)

This section will help you decide whether this is the unit for you by explaining what the unit is about, what you should know or be able to do before you start, what you will need to do during the unit and opportunities for further learning and employment.

This unit serves as an introduction to the field of digital forensics case studies. It is suitable for learners with an interest in cyber security. Previous knowledge of digital forensics is not required before you begin this unit. However, it would be advantageous for you to have beginner level experience in computer systems, computer hardware and networks.

The unit covers the practical aspects of the overall process that encompasses the digital forensics process. The unit broadly covers the following topics:

- Identifying digital evidence
- Recording evidence securely
- Managing the chain of custody
- Relevant legislation
- Maintaining confidentiality
- Volatile, non-volatile and network information
- Analysing forensic data
- Analysis findings and documenting

The unit is intended to be delivered in a broad sense and will provide you with the opportunity to study a contemporary topic in the field digital forensics in the broader context of cyber security.

Although there is a strong technical element to this unit, it has been written in such a way that theory elements will provide you with solid grounding in the elements that comprise the digital forensics process. If taking this unit alongside J0HL 34 *Digital Forensics*, the theoretical experience gained with that unit will help you to understand the 'how and why' when it comes to working with digital evidence.

Teaching methodologies for this unit incorporate a variety of techniques, for example, active, project-based and collaborative learning, and can be assessed in a variety of ways; for example, using a case study project or by using more contemporary means, for example by using a blog or e-portfolio, where you can showcase your work.

At the completion of this unit, you will be able to perform digital forensics on volatile and non-volatile data, memory interrogation, digital artefacts, evidence gathering, maintaining confidentiality, integrity, guidelines, and chain of custody. By completing this unit, you may be able to progress to further units in cyber security or other related areas at SCQF level 8 and beyond.