SQA Advanced Unit Specification

General information

Unit title: Digital Forensics (SCQF level 7)

Unit code: J0L3 47

Superclass: CC

Publication date: June 2018

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The purpose of this unit is to introduce learners to the fundamental activities involved in carrying out the digital forensics process as it relates to computers and other digital devices, for example, laptops and mobile devices.

This is a **non-specialist** unit, intended for learners who wish to gain knowledge and understanding in the digital forensics investigatory process. It is particularly suitable for learners with an interest in developing specific knowledge and skills in the following areas: identification, preparation and processing of crime scenes, how to manage and work with digital evidence, as well as the preparation of forensic documentation.

On completion of this unit, learners will know how to: perform incident response procedures, manage digital evidence and prepare forensic documentation.

On completion of this unit, learners may progress to digital forensics related units at SCQF level 8 or other cyber security related qualifications.

Outcomes

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

1 Describe incident response procedures.
2 Manage digital evidence.
3 Prepare forensic documentation.

Credit points and level

1 SQA Advanced unit credit at SCQF level7: (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 good Computing/IT, problem solving and communications skills at SCQF level 5/6.

It would be desirable, although not essential, if learners could demonstrate a basic understanding of: computer applications, hardware, networks/internet and file systems. This may be evidenced by the achievement of appropriate National Units in Computing and IT and, in particular, NPA Cyber Security units at SCQF level 6.

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes for this unit specification.

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 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, ideally, should be delivered and assessed as part of the SQA Advanced Certificate in Cyber Security at SCQF level 7. The unit, however, can be delivered on a standalone basis.

The Assessment Support Pack (ASP) for this unit provides assessment and marking guidelines that exemplify the national standard for achievement. It is a valid, reliable and practicable assessment. Centres wishing to develop their own assessments should refer to the ASP to ensure a comparable standard. A list of existing ASPs is available to download from SQA's website **(http://www.sqa.org.uk/sqa/46233.2769.html)**.

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**.

SQA Advanced Unit Specification: Statement of standards

Unit title: Digital Forensics (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

Describe incident response procedures.

Knowledge and/or skills

- Secured crime scenes
- Sources of digital evidence
- Secure recording of actions
- Different secure methods
- Continuity of evidence (chain of custody)
- Relevant legislation

Outcome 2

Manage digital evidence.

Knowledge and/or skills

- Forensically safe working environments
- Forensic acquisition
- Tools and techniques to obtain digital evidence
- System, volatile and non-volatile information
- Forensic data analysis from different sources

Outcome 3

Prepare forensic documentation.

Knowledge and/or skills

- Justification for forensic investigation
- Steps taken throughout an investigation
- Evaluation of forensic findings
- Recommendations based on findings

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 the following forms:

1 Knowledge evidence
2 Product evidence

The **knowledge evidence** will comprise the descriptions and explanations required in Outcomes 1 and 2 in relation to how learners are able to identify incident response procedures and associated management of digital evidence. Particular attention must be given to the following aspects:

- Securing a crime scene
- Sources of digital evidence
- Secure recording of actions
- Managing continuity of evidence
- Relevant legislation
- The implementation of a forensically safe working environment
- The identification of system information and the analysis of forensic data from different sources

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).

This evidence may be produced over the life of the unit under loosely controlled conditions (including access to resources and reference materials). The knowledge evidence may be sampled when testing is used. When testing is used, it must be controlled in terms of location, timing and access to reference materials. Learners are expected to demonstrate a breadth of understanding across all the knowledge statements; as a result, sampling need not be of a detailed nature.

The **product evidence** produced for Outcome 3 will demonstrate that the learner has been able to produce appropriate outputs as a result of the overall investigative process. The product will detail the steps the learner has taken through the investigation, including the deliverables from each of these stages (from knowledge demonstrated throughout Outcomes 1 and 2). For example, the justification behind the investigation, the steps that have been taken throughout the investigation, the evaluation of findings from the investigation and recommendations based on the results of findings and analysis.

Again, this evidence may be produced over the life of the unit under loosely controlled conditions (including access to resources and reference materials).

The SCQF level of this unit (level 7) provides additional context on the nature of the required evidence and the associated standards. The following level descriptors are particularly relevant to the evidence.

- An overall appreciation of the body of knowledge
- Knowledge that is embedded in the main theories, concepts and principles
- An awareness of the dynamic nature of knowledge and understanding
- Use some of the basic and routine professional skills, techniques, practices and materials
- Use a range of approaches to address defined and/or routine problems
- Exercise some initiative and independence in carrying out defined activities at a professional level

These level descriptors should be used (explicitly or implicitly) when making judgements about the evidence.

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.

SQA Advanced Unit Support Notes

Unit title: Digital Forensics (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.[1] This unit is intended for non-specialists and is offered as a core unit in the SQA Advanced Cyber Security frameworks. 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 the theoretical aspects that comprise the digital forensics investigatory process. The unit covers the three overall stages of the investigatory process: securing crime scenes, how to manage digital evidence and how to prepare documentation from the output of the digital forensics process (for example, for law enforcement or a court of law). As well as learning the theoretical elements associated with digital investigations, learners will also learn how to identify malicious activity, as well as the research skills necessary 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 nature. 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 taken throughout the investigatory process. The unit must ensure that learners are understanding the crucial aspects of how to respond to incidents and secure crime scenes; the importance of managing evidence, so as not to jeopardise investigations; also, how to properly prepare clear and unambiguous documentation, should a case end up moving into the hands of law enforcement.

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 also 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.

[1] https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs

Outcome 1

This outcome introduces the steps that must be taken when confronted with a crime scene involving digital technologies, for example, a PC, a laptop, a tablet or any other mobile digital device (including phones, smartphones and digital music devices). Learners must be made aware that, at this stage of an investigation, particular actions/initial reactions can easily corrupt evidence. Learners must know how to act when confronted with a particular scenario. For example, if the crime involves a PC, then the investigator must know what to do if the PC is either switched on or off; if it is connected to a network and has attached storage medium. Learners must learn where to look to find evidence, how all actions are contemporaneously recorded and how to initiate the chain of custody process (bagging and tagging).

Outcome 2

This outcome prepares the learner to move to the next level with the investigatory process. This sees the evidence that has been gathered as part of the incident response now moving to a crime laboratory environment. Learners must describe the important features of a secure lab and the tools and techniques that can be used to obtain digital evidence either from system information or from volatile/non-volatile locations (for example, memory). Learners must then be able to analyse the data that has been obtained.

Outcome 3

Outcome 3 moves to the final stage of the investigatory process, where learners must be able to justify the reasons for the forensic investigation process, as well as the clear steps that have been taken throughout the process. Evaluations must be made of any analysis of data that has taken place, and findings presented, which will then subsequently form recommendations for actions (either within a business scenario or involving law enforcement, for example).

The following sites and documentation can provide relevant support for this unit:

- **National Cyber Security Centre: Incident Management website**
- **National Cyber Security Centre: Forensic Readiness Planning (2016)**
- **The Good Practice Guide for Digital Evidence (2012)**
- **Houses of Parliament: Digital Forensics and Crime**

Guidance on approaches to delivery of this unit

It is recommended that that the outcomes for this unit are taught sequentially. This is to make sure that learners have the required background and theoretical knowledge to the digital forensics process as identified in Outcomes 1 and 2, before progressing to the reporting stages of Outcome 3.

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 along with experiences and outcomes, 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 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, 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 traditional approach to summative assessment for Outcomes 1, 2 and 3 would be for learners to complete a holistic project-based assessment, where learners would work from a given case study/scenario. Learners would complete written research tasks (knowledge evidence) for Outcomes 1 and 2. For Outcome 3 (product evidence), learners would produce a report relating to the findings from Outcomes 1 and 2.

A more contemporary approach to assessment would involve the use of a digital product, for example, a web log (blog), e-portfolio or website to record learning (and the associated activities) throughout the life of the unit. The digital product would provide knowledge evidence (in the descriptions and explanations) and product evidence (using, for example, video recordings and/or images). The digital product 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 digital product is used for summative assessment, it would also facilitate formative assessment since learning (including misconceptions) would be apparent, 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. 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* 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

SQA acknowledges the valuable contribution that Scotland's colleges have made to the development of SQA Advanced Qualifications.

FURTHER INFORMATION: Call SQA's Customer Contact Centre on 44 (0) 141 500 5030 or 0345 279 1000. Alternatively, complete our Centre Feedback Form.

General information for learners

Unit title: Digital Forensics (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. It is suitable for learners who have an interest in cyber security and may be undertaking units as part of the SQA Advanced Cyber Security qualification at SCQF level 7. No previous knowledge of digital forensics is 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 theoretical aspects of the overall process that encompasses the digital forensics process. The unit broadly covers the following topics:

- Securing crime scenes
- Identifying digital evidence
- Recording evidence securely
- Relevant legislation
- Managing the chain of custody
- Forensic acquisition
- System, volatile and non-volatile information
- Analysing forensic data
- Evaluating forensic findings
- Preparing forensic documentation

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 theoretical element to this unit, it has been written in such a way that theory elements will provide you with solid grounding of the fundamentals that comprise the digital forensics process. The theoretical experience gained during the early stages of the unit will help you to understand the 'how and why' when it comes to working with digital evidence. As you progress through the unit, you will develop an understanding of how analysis and findings, as a result of investigation, can be presented in forensic report format. You will gain experience in the importance of working with crime scenes and digital devices, also the associated pitfalls and how these processes can be appropriately managed in order to present a case to law enforcement and courts of law.

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.

By the end of the unit you will have learned the importance of securing a crime scene, how to look for, retrieve and analyse digital evidence, and present the findings of your investigation. By completing this unit, you may be able to progress to more advanced cyber security units at SCQF level 8 and beyond.

There are opportunities to develop *Information and Communication Technology* Core Skills through your use of ICT. The unit will also provide opportunities to develop broader skills, such as citizenship.