National Unit specification

General information

Unit title: Digital Forensics (SCQF level 4)

Unit code: H9J0 44

Superclass: CC

Publication date: September 2015

Source: Scottish Qualifications Authority

Version: 02

Unit purpose

This Unit is aimed at beginners who want to acquire the basic knowledge and skills relevant to digital forensics.

The purpose of this Unit is to introduce learners to the basic principles of, and the integrity of the process involved in, forensically examining digital evidence. It is intended to give learners a **basic** knowledge of data acquisition, analysis, and reporting of simple forensic examinations.

The Unit also introduces basic practical skills in identifying preliminary sources of evidence across a range of digital devices and media. Using these sources of evidence, learners will analyse and interpret data, identify its relevancy to an enquiry under investigation, and subsequently report that information.

On completion of this Unit, learners will gain basic knowledge and skills in data acquisition, analysis and reporting of digital evidence. Learners will have a basic understanding of the legal, professional and ethical application of the digital forensics analyst. Learners may progress to the *Digital Forensics* at SCQF level 5 or similar National Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF level 4.

National Unit specification: General information (cont)

Unit title: Digital Forensics (SCQF level 4)

Outcomes

On successful completion of the Unit the learner will be able to:

1 Describe the steps in the digital forensics process.
2 Apply basic techniques of data acquisition.
3 Examine digital evidence.

Credit points and level

1 National Unit credit at SCQF level 4: (6 SCQF credit points at SCQF level 4)

Recommended entry to the Unit

Whilst entry is at the discretion of the centre, it would be beneficial if learners gained basic IT Skills. This may be evidenced by possession of:

H3LJ 09 *Computer Basics* (SCQF level 3)
or equivalent qualifications or experience.

Core Skills

Achievement of this Unit gives automatic certification of the following:

Complete Core Skill	Information and Communication Technology at SCQF level 4
Core Skill component	None

There are also opportunities to develop aspects of Core Skills which are highlighted in the Support Notes of the Unit Specifications for this Course.

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.

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**.

National Unit specification: Statement of standards

Unit title: Digital Forensics (SCQF level 4)

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.

Outcome 1

Describe the steps in the digital forensics process.

Performance Criteria

(a) Describe the role of forensic readiness in conducting a digital forensics investigation.
(b) Identify the legal, professional and ethical issues in digital forensics.
(c) Describe the phases of acquisition, analysis and reporting.
(d) Identify the tools and techniques which could be used during the digital forensics process.

Outcome 2

Apply basic techniques of data acquisition.

Performance Criteria

(a) Identify the type of data under investigation.
(b) Apply software tools to acquire the data from a basic investigation.
(c) Describe the importance of preservation in data acquisition.

Outcome 3

Examine digital evidence.

Performance Criteria

(a) Select appropriate tools.
(b) Perform analysis of the digital evidence.
(c) Construct a timeline of events using the digital evidence.

National Unit specification: Statement of standards (cont)

Unit title: Digital Forensics (SCQF level 4)

Evidence Requirements for this Unit

Assessors should use their professional judgement, subject knowledge and experience, and understanding of their learners to determine the most appropriate ways to generate evidence and the conditions and contexts in which they are used.

Evidence is required to demonstrate that learners have achieved all Outcomes and Performance Criteria. However, sampling may be used in certain circumstances (see below).

The evidence for this Unit 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). Particular consideration should be given to digital formats and the use of multimedia.

Given the level of this Unit, the amount of evidence, and corresponding time spent on assessment, should be minimised but sufficient to satisfy the Performance Criteria. Whenever possible, evidence should be a naturally occurring by-product of teaching and learning. However, it must be produced by the learner. Authentication must be used where this is uncertain.

Evidence is required for two types of competence: **cognitive competence** (knowledge and understanding) and **practical competence** (practical abilities).

The evidence of cognitive competence will relate to Outcome 1 (all Performance Criteria) and Outcome 2 (PC (a) and (c)).

Evidence of cognitive competence may be sampled across the knowledge domain defined by this Unit Specification, so long as the sample is unknown, and unpredictable, to the learner. Where sampling is used to assess the learner's knowledge and understanding, an appropriate pass mark should be set.

The practical evidence will relate to Outcome 2 (PC (b)) and Outcome 3 (all Performance Criteria). The practical evidence will demonstrate the forensic analysis of digital evidence from a **simple** investigation and will include (but may not be limited to) a timeline of events based on their interpretation of the forensic analysis.

Evidence of practical competence may not be sampled and may be produced over an extended period of time. Where it is generated without supervision, some means of authentication must be carried out. The Guide to Assessment provides advice on methods of authentication.

The Guidelines on Approaches to Assessment (see the Support Notes section of this specification) provide specific examples of instruments of assessment.

National Unit Support Notes

Unit title: Digital Forensics (SCQF level 4)

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

This Unit focuses on digital forensics in the context of cyber security. Society's increasing reliance on technology, in both the workplace and in people's personal lives has brought cyber security to the forefront of not only the computing field, but also businesses, organisations and those looking to protect their personal assets. Digital forensics plays a very important part in this as our use of technology means we are constantly leaving a trace, or 'digital fingerprint' of our digital behaviour and lifestyle. For example, deleted emails, internet searches and geo-location data from mobile devices can all be recovered using digital forensic techniques and the evidence used to prove or disprove criminal activity. Digital Forensic techniques can also be used to recover lost or deleted data from damaged hardware or software. As people's use of technology continues to grow, digital forensics skills will be increasingly valuable in both the workplace and in enhancing personal digital skills.

The purpose of this Unit is to introduce learners to the principles and integrity of the digital forensics process. It is intended to give learners a basic understanding of data acquisition, data analysis and the reporting of forensics examinations. It is expected that the learners will learn the broad principles of conducting a digital forensics examination and develop some practical skills in the identification and preservation of evidential content from a digital medium. Using some sources of evidence, learners will analyse, reconstruct and interpret the data, identify its relevancy to an enquiry under investigation, and subsequently report that information.

The practical elements of the Unit should introduce skills in data acquisition, analysis and reporting of digital evidence. A short report of their findings with a timeline of events would make good assessment evidence.

It is important that learners have an understanding of the legal, professional and ethical application of the digital forensic analyst and this could be evidenced through practical skills and from the report.

This Unit is intended for beginners and should be delivered in that context. At this level (SCQF level 4), treatment of every topic should be **non-complex** and **foundational**. It is anticipated that this Unit will prepare learners for the *Digital Forensics* Unit at SCQF level 5.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

The significance of networking to every Outcome should be explained, given the importance of this technology to the forensic process. A **basic** introduction to networking **fundamentals** (such as the IP address scheme) is required.

Throughout this Unit learners must adhere to basic ethical standards of practice.

This Unit is split into two main areas; the theory and background of the digital forensics process in Outcomes 1 and 2 (PC (a) and (c)) and the practical skills necessary to conduct an investigation in Outcomes 2 (PC (b)) and 3 (all PC).

Outcomes 1 and 2 (PC (a) and (c))

The theoretical aspects of the digital forensics process (Outcome 1) should include making learners aware of the different stages of the digital forensics investigation. Learners should be taught the importance of conducting the stages in a particular order and have a superficial understanding of what each stage is and how it is linked to other stages. It is imperative that learners understand the legal, ethical and professional issues — these issues should underpin the teaching of all topics and Outcomes where appropriate, but can be addressed explicitly as part of Outcome 1. Tutors may wish to get learners to consider recent high-profile cases where digital evidence has been crucial in making a conviction and consider the steps which will have been undertaken to gather the evidence for that conviction. Tutors may wish to outline the steps in a non-digital forensic investigation and then compare the similarity of these steps in the digital process and the need conduct the procedure in such a rigorous manner.

Outcome 1 (PC (a)): Describe the role of forensic readiness in conducting a digital forensics investigation.

- What is forensic readiness?
- Why is forensic readiness important to a business?
- How does forensic readiness help a digital forensic investigation?

Outcome 1 (PC (b)): Identify the legal, professional and ethical issues in digital forensics.

- Describe the laws which may affect a digital forensics investigation.
- Describe the professional issues which may affect a digital forensics investigation.
- Describe the ethical issues which may affect a digital forensics investigation.

Outcome 1 (PC (c)): Describe the phases of acquisition, analysis and reporting.

- What is the acquisition stage of the digital forensics process?
- What is the analysis stage of the digital forensics process?
- What is the role of the reporting stage of the digital forensics process?

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

Outcome 1 (PC (d)): Identify the tools and techniques which could be used during the digital forensics process.

- Describe some of the software which could be used during the digital forensics process.
- Describe some of the techniques which could be used during the digital forensics process.

Outcome 2 (PC (a)): Identify the type of data under investigation.

- The learner should be able to recognise where the data has come from, for example web browser history, an image file, an email conversation.
- In some cases, part of the investigation may involve identifying unknown data. Learners would have to evidence the steps that they took to identify the data type and demonstrate how they were able to recognise it. This could involve analysing header data, or simply using a tool which recognised the data on their behalf.

Outcome 2 (PC (c)): Describe the importance of preservation in data acquisition.

- What does the term 'preservation' mean in the context of a digital forensics investigation?
- How do some computing tasks, for example powering off a computer affect the data which could be useful in a forensics investigation?
- Why is it necessary to conduct an investigation on a copy of the data, rather than the original?

Outcomes 2 (PC (b)) and 3 (all PC)

Learners should be taught the practical elements associated with a digital investigation using various tools and how to translate the evidence uncovered with these tools into a timeline of events. Tutors may want to consider evidence which the learners would already be familiar with and have some understanding of, for example browser forensics and the recovery of deleted or corrupted files. Tutors may wish to get learners to execute some basic tasks, for example making, editing and deleting files, and conducting online searches. Tutors could then ask learners to consider the different types of evidence which could be generated from these activities and explore the role of file properties and meta-data. The internet cache, cookies and browser history should also be explored. Tutors may choose to ask the learners to generate evidence themselves, which could be used to complete the practical work necessary for all the associated Performance Criteria in Outcomes 2 and 3 or use some of readily available sources of evidence files online (suggested links will be provided). Learners should consider how the data analysed could be best presented using a timeline of events.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

Outcome 2 (PC (b)): Apply software tools to acquire the data from a basic investigation.

- Learners should identify the full range of tools which they have used to acquire the data and provide evidence of the steps that they have completed, as appropriate.

Outcome 3 (PC (a)): Select appropriate tools.

- Learners should identify the full range of tools which they have used in their investigation and, where appropriate, justify why they decided to use some tools instead of others.

Outcome 3 (PC (b)): Perform analysis of the digital evidence.

- Learners can evidence this through a number of different mechanisms but where a report is used, learners may wish to take screen shots of the steps that they complete as part of their analysis, and consider how best to present the results of their analysis, for example using a table.

Outcome 3 (PC (c)): Construct a timeline of events using the digital evidence.

- A timeline of events should be constructed to summarise the evidence which has been found. This evidence should include the results of the analysis in Outcome 3 (PC (b)) and may include additional information which has been provided as part of the scenario. The timeline should provide a visual representation of all the key evidence, and where relevant the timescale and order in which the related events occurred.

Guidance on approaches to delivery of this Unit

A practical, hands-on approach to learning should be adopted in order to engage learners and exemplify key concepts. However, all practical activities should be underpinned with appropriate knowledge before learners commence these activities. The maturity, and life experience, of learners should be taken into account.

At this level, learning should be a mix of tutor-led and learner-led. It is anticipated that some initial introduction and explanation will be required for each Outcome. However, there is significant scope for learners to research and explore the topics once this initial seeding has taken place. Tutors should expect some independent learning to take place and support students with this where appropriate.

Case studies (including video presentations) could be used to provide concrete examples of aspects of a digital forensics investigation and associated issues.

The distribution of time over the three Outcomes is at the discretion of the centre and thus will be influenced by a number of factors such as the actual technologies utilised. However a possible distribution is as follows:

- Outcome 1: 8 hours
- Outcome 2: 16 hours
- Outcome 3: 16 hours

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

A significant proportion of the time is given to Outcomes 2 and 3 because of the scope of the practical problem that learners are expected to address.

Throughout this Unit learner activities should relate to their personal or vocational interests. Learners should be encouraged to become confident with as wide a range of digital technologies as possible.

The following documents may be useful:

- Association of Chief Police *Officers 'Good Practice Guide for Computer-Based Electronic Evidence'*
  http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

- Forensic Examination of Digital Evidence*: 'A Guide for Law Enforcement'*
  http://www.ncjrs.gov/pdffiles1/nij/199408.pdf

- Ministry of Justice Practice Direction 35*: Experts and Assessors Reports*
  http://www.justice.gov.uk/civil/procrules_fin/contents/practice_directions/pd_part35.htm#IDASFFR

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 the 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.

This Unit is intended to provide candidates with suitable basic knowledge and grounding in carrying out computer and/or digital based forensic investigations and is likely to form part of the Cyber Security Group Award.

The evidence of cognitive competence in Outcomes 1 (all Performance Criteria) and 2 (PC (a) and (c)) may take the form of a written test that shows the candidate satisfies all of the associated Performance Criteria. The written test should be taken under closed-book conditions. The sample must be sufficiently random and robust to clearly infer competence in the whole knowledge domain. Every performance criterion should be covered in the test; the relative weighting of each one is left to the discretion of the assessor. An appropriate pass mark must be set, the pass mark will be influenced by the instrument of assessment.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

The evidence of practical competence in Outcomes 2 (PC (b)) and 3 (all Performance Criteria) may take the form of an activity log from a practical assessment and it would record all of the practical activities carried out by the candidate that satisfies all of the associated Performance Criteria. It may be in the form of a practical exercise/case study giving details of an incident that candidates are to investigate. Candidates can then utilise the practical skills they have learned throughout the Unit. Tutors can choose how these skills should be evidenced, but a report describing the analysis of the data and a timeline of the results could be useful. The report could address all the associated Performance Criteria with some examples.

Another approach to assessment would be the creation and maintenance of a web log, which would record candidate activity throughout the Unit. This would log, on a daily or weekly basis, what candidates learn and what they do. However, their posts would have to satisfy the relevant Performance Criteria. Practical activities could also be recorded *via* the blog. When practical activity is recorded on a blog (narratively), authentication could involve a photograph or video of candidate activity (this could be included as part of their post). Not every practical task would require authentication; at this level it is acceptable for some posts to be a simple description of appropriate practical activities. When necessary, separate authentication (such as oral questioning) could be used for verification purposes.

The critical aspect is that the blog is an **overall** accurate reflection of the practical activities (and, therefore, the associated skills) carried out by the learner during the life of the Unit.

Another approach would involve the creation and maintenance of an e-portfolio. The e-portfolio would include all of the statements, identifications, descriptions and selections necessary to satisfy the criteria relating to cognitive competencies, together with digital artefacts that provide evidence of their practical abilities. Digital artefacts would include screenshots, digital photographs, audio and video recordings, etc that collectively evidence candidates' competencies. Some form of authentication would be required. This could be as simple as a statement of originality, signed by the candidate and the assessor.

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**.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 4)

Opportunities for developing Core and other essential skills

This Unit provides opportunities to deliver some of the following Core Skills:

Information and Communication Technology (ICT) (SCQF level 4)
Problem Solving (SCQF level 4)
Communication (SCQF level 4)

Most of the Core Skill components in *Information and Communication Technology (ICT)* can be addressed in this Unit. Depending on delivery, the entire Core Skill may be covered. There are opportunities to use straightforward techniques to assist in a search, carry out straightforward searches for information, use a range of sources/criteria (eg internet, intranet, local files) or a sustained search using one source and a range of criteria.

Some of the Core Skill components in *Problem Solving* can be addressed in this Unit. There are opportunities to develop a plan, identify and gather the resources to carry out the plan and carry out the plan.

One or more of the Core Skill components in *Communication* may be covered in this Unit for example Written Communication.

This Unit has the Core Skill of Information and Communication Technology embedded in it, so when candidates achieve this Unit their Core Skills profile will be updated to show that they have achieved Information and Communication Technology at SCQF Level 4.

History of changes to Unit

Version	Description of change	Date
02	Core Skill Information and Communication Technology at SCQF level 4 embedded.	09/09/2015

General information for learners

Unit title: Digital Forensics (SCQF level 4)

This section will help you decide whether you would like to do this Unit 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 aims to provide you with the fundamental knowledge and skills of Digital Forensics. Digital Forensics is a type of Forensic Science, which involves looking at evidence which comes from a computer to understand what someone has been doing on that computer. This might involve trying to recover deleted e-mails, seeing what people have been searching for on google and what kind of files they have been using.

This Unit is an introduction to the knowledge and skills used by digital forensics investigators. There will be an emphasis in this Unit to gain as much practical skills throughout this course, with a lot of opportunity for you to develop your practical skills. This will give you a greater understanding into the approaches used to analyse computer devices that have been used to commit a crime.

The Unit is designed for beginners. It covers a wide range of knowledge and skills including:

- What happens during a digital forensics investigation.
- How to find data on a computer which could be used as evidence.
- How to use different kinds of software to find the data.
- How to read the data and understand what it means.
- How to present the data so that it can be understood by other people.

No previous knowledge or experience of computers is presumed. It is designed for the beginner who wants to gain a basic understanding of the current methods used to conduct a digital forensics investigation.

The assessment may take different forms. It will be straight-forward and not take much time away from your learning. It may involve a short test of your knowledge and some practical tasks, or it may simply be a record of your activities during the Unit. The focus of the Unit is on learning — not assessing.

This Unit is part of a series of Units on Digital Forensics. You may progress to the next Unit in the series (the *Digital Forensics* Unit at SCQF level 5) on completion of this Unit if you wish to improve your knowledge and skills in this area.