National Unit specification

General information

Unit title: Digital Forensics (SCQF level 5)

Unit code: H9J0 45

Superclass: CC

Publication date: July 2015

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

The Unit is aimed at learners to develop their awareness of the knowledge, principles and skills relevant in digital forensics.

The purpose of this Unit is to develop learners' knowledge of the principles and integrity of the digital forensics process. It is intended to augment learners' knowledge of data acquisition, data analysis and the reporting of forensics examinations.

The Unit develops learners' practical skills in identifying evidential sources 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 knowledge and skills in data acquisition, analysis and reporting of digital evidence. Learners will have an understanding of the legal, professional and ethical application of the digital forensic analyst. Learners may progress to the *Digital Forensics* Unit at SCQF level 6 or similar national Units.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF 5.

Outcomes

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

1 Explain the digital forensics process.
2 Apply relevant techniques in acquiring data.
3 Examine digital evidence.

National Unit specification: General information (cont)

Unit title: Digital Forensics (SCQF level 5)

Credit points and level

1 National Unit credit at SCQF level 5: (6 SCQF credit points at SCQF level 5)

Recommended entry to the Unit

Entry and access to this Unit shall be at the discretion of the centre. It is recommended that the learner should have knowledge of using application programs on a PC and a basic understanding of computer hardware, computer networks and file system operation would also be beneficial.

Successful completion of the relevant *Digital Forensics* Unit at SCQF level 4 would also display recommended knowledge to attempt this Unit.

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 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 5)

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

Explain the digital forensics process.

Performance Criteria

(a) Explain the legal, professional and ethical issues in conducting a digital forensics examination.
(b) Explain the tools and techniques used to conduct a digital forensics examination
(c) Explain the phases of the digital forensics process.
(d) Explain the importance of recording all actions.

Outcome 2

Apply relevant techniques in acquiring data.

Performance Criteria

(a) Identify forensically sound techniques to acquire data.
(b) Select appropriate forensic tools.
(c) Use forensic tools to acquire data.
(d) Preserve acquired data.
(e) Record relevant actions.

Outcome 3

Examine digital evidence.

Performance Criteria

(a) Identify system specific information.
(b) Perform an analysis of the evidence using software tools.
(c) Record the findings of the process.

National Unit specification: Statement of standards (cont)

Unit title: Digital Forensics (SCQF level 5)

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.

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: evidence of **cognitive competence** (knowledge and understanding) and evidence of **practical competence** (practical abilities).

The evidence of cognitive competence will relate to Outcome 1 (all Performance Criteria), Outcome 2 (PC (a)) and Outcome 3 (PC (a)).

Evidence of cognitive competence may be sampled 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 evidence of practical competence will relate to Outcome 2 (PC (b), (c), (d), (e)) and Outcome 3 (PC (b) and (c)). The evidence will be the findings of **one** forensic analysis of **one** data source (**one** data acquisition and **one** data examination). The data source should be non-trivial but non-complex, and the examination should be routine.

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 5)

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 develop learners' understanding and application of the principles and integrity of the digital forensics process. It is intended to provide learners with a sound understanding of data acquisition, data analysis and the reporting of forensic examinations.

It is expected that the learner will learn and develop their knowledge on the recognised principles of forensic investigations. This Unit shall enhance and develop the practical skills in the identification and preservation of evidential content across a range of digital devices and media.

Using these 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 develop skills in data acquisition, analysis and reporting of digital 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. Throughout this Unit learners must adhere to basic ethical standards of practice.

At this level (SCQF level 5), treatment of every topic should be non-complex but non-trivial. It is anticipated that this Unit will prepare learners for the *Digital Forensics* Unit at SCQF level 6 building on learning achieved in the *Digital Forensics* Unit at SCQF level 4.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 5)

The significance of networking to every Outcome should be emphasised, given the importance of this technology to the forensic process. At this level, learners should understand the principles of networking (such as the IP address scheme and the TCP/IP protocol) and be able to apply this knowledge to the digital forensic process.

Outcome 1

This Outcome should expand learners' awareness 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.

PC (a) Explain the legal, professional and ethical issues in conducting a digital forensics examination:

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

PC (b) Explain the tools and techniques which could be used during the digital forensics process:

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

PC (c) Explain the phases of the digital forensics process:

- 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?

PC (d) Explain the importance of recording all actions:

- What is the importance of recording contemporaneous notes throughout the examination process?

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 5)

Outcomes 2 and 3

These two Outcomes cover a combination of cognitive and practical competence.

Learners should be taught the practical elements associated with a digital investigation using various tools and how to translate and review 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 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.

Outcome 2:

PC (a) Identify forensically sound techniques to acquire data.

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

PC (b) Select appropriate forensic tools.

- 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.

PC (c) Use forensic tools to acquire data.

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

PC (d) Preserve acquired data.

- Learners should conduct the forensic imaging of the relevant data in such a manner to ensure integrity of image using hash techniques and preserve same to suitable medium such as a HDD.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 5)

Outcome 3:

PC (a) Identify system specific information.

- Learners can evidence system information to include physical characteristics of the system, hard disc drives, operating system and age.

PC (b) Perform an analysis of the evidence using software tools.

- Learners can evidence this through a number of different mechanisms by recording contemporaneous notes and taking screenshots through their examination.

PC (c) Record the findings of the process.

- Learners can evidence this through the completion of an evidential standard written report with conclusions, relevance and forensic findings.

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.

Case studies (including video presentations) could be used to provide concrete examples of how information can be used.

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

A significant proportion of the time is given to Outcomes 2 and 3 due to the practical nature of this Unit.

Applying the practical elements associated with digital investigations through the use of various forensic tools, learners will also learn how to identify malicious activity as well as the research skills necessary to keep abreast with changes in both law and forensic computing research methodologies.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 5)

Although this Unit is expressed in generic terms, whenever possible it should relate directly to situations with which the learner is familiar and in particular the following documentation:

- 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 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 knowledge and grounding in conducting a computer and/or digital based forensic investigation and is likely to form part of the NPA in Cyber Security at SCQF level 5 Group Award.

The evidence of **cognitive competence** in Outcome 1 (all Performance Criteria), Outcome 2 (PC (a) and Outcome 3 (PC (a) 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.

The evidence of **practical competence** in Outcomes 2 (PC (b)–(e)) and 3 (PC (b)–(c)) could take the form of a practical assignment involving the forensic analysis of one data source (such as the contents of a smartphone's SIM card). Candidates would be required to carry out, and record, this analysis. The record could take one of several forms including reports, activity logs, presentations, video recordings or web logs. Successful completion would be based on the candidate satisfying all of the associated Performance Criteria.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 5)

Outcomes 2 and 3 may be given as a practical exercise/case giving details of an incident that candidates are to investigate. This shall include the data requisition, data analysis, preparation and delivery of forensic findings and system information gained whilst conducting a forensic examination. Tutors can choose how these skills should be evidenced, for example, an observation checklist completed and signed by the assessor after observing candidates carry out practical tasks. A report describing the process of acquiring data and findings of a forensic examination 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 5)

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 5)
Problem Solving (SCQF level 5)
Communication (SCQF level 5)

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 a range of *ICT* devices, observing security procedures, carry out complex searches for information, evaluate reliability of information,

Additionally, the Core Skill components of *Problem Solving* can be addressed in this Unit. There are opportunities to choose and obtain resources, develop a plan, identify and ensure you have the resources to carry out the plan, carry out an action plan.

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

History of changes to Unit

Version	Description of change	Date

General information for learners

Unit title: Digital Forensics (SCQF level 5)

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.

The purpose of this Unit is to enhance your understanding of the principles and integrity of the digital forensics process. It is intended to give you a sound understanding of data acquisition, data analysis and the reporting of forensics examinations. It is expected that you will learn the principles and develop practical skills in the identification and preservation of evidential content across a broad range of digital devices and media.

Using these sources of evidence you will analyse, reconstruct and interpret the data, identify its relevancy to an enquiry under investigation and subsequently report that information. At the time of writing, current Scottish and UK legislation relating to cybercrime are:

- Data Protection Act (1998)
- Computer Misuse Act (1990)
- Regulation of Investigatory Powers Act

The assessment may take different forms. It may involve a short test of your knowledge and some practical tasks, or it may be a record (such as activity log or web log) of your activities during the Unit. The practical elements of the Unit should develop and enhance skills in data acquisition, analysis and reporting of digital evidence. A short report of your findings would make good assessment evidence, although this is decided by your centre.

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 6) on completion of this Unit if you wish to improve your knowledge and skills in this area.