National Unit specification

General information

Unit title: Digital Forensics (SCQF level 6)

Unit code: H9J0 46

Superclass:	CC
Publication date:	September 2015
Source:	Scottish Qualifications Authority
Version:	02

Unit purpose

The purpose of this Unit is to introduce learners to the breadth of knowledge that constitutes a digital forensics examination. The Unit enhances learners' understanding of the principles and integrity of the digital forensics process. It is intended to give learners a comprehensive understanding of data acquisition, data analysis and the reporting of forensics examinations.

The Unit also develops learners' practical skills in the identification and preservation of evidential content across a broad range of digital devices and media. Using these sources of evidence, learners will analyse, reconstruct and interpret data, understand its relevancy to an enquiry under investigation, and subsequently report that information.

On completion of this Unit, learners will be able to demonstrate their understanding of the digital forensics process, the main job roles associated in the process, and the legal, professional and ethical issues involved. Learners will also be able to apply complex techniques to acquire data, conduct data analysis and effectively communicate the evaluation of complex contemporary digital forensics examinations.

Learners may progress to National Certificates or Higher National Certificates in Computing or related qualifications.

This Unit is a mandatory Unit within the National Progression Award in Cyber Security at SCQF level 6.

National Unit specification: General information (cont)

Unit title: Digital Forensics (SCQF level 6)

Outcomes

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

1 Explain the digital forensics process and job roles.
2 Apply complex techniques in acquiring data.
3 Evaluate digital evidence.

Credit points and level

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

Recommended entry to the Unit

Access to this Unit will be at the discretion of the centre; however it is recommended that the learner should have the 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. This may be demonstrated by the achievement of appropriate National Units in Computing and IT. Successful completion of the relevant *Digital Forensics* Units at SCQF level 4 or 5 would also display recommended knowledge to attempt this Unit.

Core Skills

Achievement of this Unit gives automatic certification of the following:

Complete Core Skill	Information and Communication Technology at SCQF level 6
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 6)

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 and job roles.

Performance Criteria

(a) Explain the main stages in the digital forensics process.
(b) Explain the main job roles associated with the digital forensics process.
(c) Explain the legal, professional and ethical issues in conducting a forensic examination.
(d) Describe the essential elements involved in securing a crime scene.
(e) Identify potential sources of digital evidence.
(f) Explain the tools and techniques used to conduct a digital forensics examination.
(g) Explain the importance of recording all actions.

Outcome 2

Apply complex techniques in acquiring data.

Performance Criteria

(a) Explain complex forensic techniques used to acquire data.
(b) Select a range of forensic tools to acquire data.
(c) Use a range of relevant forensic tools to acquire data.
(d) Preserve acquired data.
(e) Verify acquired data.

Outcome 3

Evaluate digital evidence.

Performance Criteria

(a) Identify system specific information.
(b) Perform hard disk analysis.
(c) Perform network analysis.
(d) Record the findings of the process.
(e) Evaluate the results of the digital forensic examination.
(f) Communicate the evaluation results of the forensic examination.

Unit title: Digital Forensics (SCQF level 6)

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)–(f)). The evidence will be the communication of the evaluation of at least **one complex** contemporary digital forensics examination. The communication is an end-product, and can take any appropriate form, however it should demonstrate **all** associated Performance Criteria in Outcomes 2 and 3. The communication should indicate the use of **complex** forensic techniques and a range of forensic tools to acquire data.

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 6)

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 purpose of this Unit is to enhance learners' understanding of the principles and integrity of the digital forensics process. It is intended to give learners a comprehensive understanding of data acquisition, data analysis and the reporting of forensics examinations. It is expected that the learner 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, learners will analyse, reconstruct and interpret the data, understand its relevancy to an enquiry under investigation, and subsequently report that information. In order to reconstruct, it is recommended that a copy of the data is made preferably using industry techniques such as a write blocker, although this is not essential as long as the learner understands why this would be used.

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

It is important that learners have an understanding of the legal, professional and ethical issues in conducting a forensic examination and this could be evidenced through practical skills and from the report. The critical importance of ethics must be emphasised throughout this Unit since it has a vital importance to each Outcome.

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, public and private addresses, and the TCP/IP protocol) and be able to apply this knowledge to the digital forensic process.

On completion of Outcome 1, learners will be able to:

- identify the legal, professional and ethical issues in conducting a forensic examination.
- explain the laws which may affect a digital forensics investigation and understand why these are important and must be adhered to.
- explain the professional issues which may affect a digital forensics investigation, this overlaps with the section above in terms of adherence to current legislation.

- explain the ethical issues which may affect a digital forensics investigation, this also overlaps with the areas above and should cover the ethics behind an investigation and how evidence is collated.
- explain the main job roles associated with the digital forensics process, for example what essential knowledge and skills a digital forensics analyst should have, what their responsibilities are.
- describe the essential elements involved in securing a crime scene.
- describe the importance of securing a crime scene, learners will require an understanding of how this relates to using the evidence gathered from a crime scene in a court of law.
- identify potential sources of digital evidence, sources of digital evidence can come from many places, not just the obvious computer system. The data from devices capable of storing data, such as tablets, mobile phones, removable drives, printers, smart televisions, and smart household devices have all been used as evidence in court.
- explain the tools and techniques used to acquire and maintain evidence.
- explain the tools and techniques used to analyse data.
- describe how to acquire and maintain evidence, the maintenance of evidence is crucial in court cases. The learner should be able to describe the types of software/hardware that can be employed and how they should be used.
- explain the importance of recording all actions.
- be clear in knowing what and to what level of detail notes must be taken. It is not required that the learners should know how to create industry standard contemporaneous notes at this level, but to be aware that it is very important to record all actions so that a third party may replicate every action.

The practical elements of the Unit should develop and enhance skills in data acquisition, analysis and reporting of digital evidence. A short report of their findings would make good assessment evidence.

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.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 6)

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 using various tools, 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.

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 breadth and depth of knowledge and grounding in carrying out computer and/or digital based forensic investigations and is likely to form part of the NPA Cyber Security at SCQF level 6 Group Award.

Unit title: Digital Forensics (SCQF level 6)

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 (multiple-choice questioning or short response) that shows the candidate satisfies all of the associated Performance Criteria. The written test should be taken under closed-book conditions. The sample of must be sufficient random and robust to clearly infer competence in the whole knowledge domain. Every performance criterion must 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 Outcome 2 (PC (b), (c), (d), (e)) and Outcome 3 (PC (b)–-(f)) could take the form of a practical assignment involving the forensic analysis of at least **one** complex contemporary digital forensics examination. Candidates would be required to carry out this analysis and communicate on the evaluation of the analysis. The communication 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.

Outcomes 2 and 3 could be given as 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. This shall include the data requisition, data analysis. Candidates will then evaluate the forensic findings. An evaluation report on the findings of the digital forensic examination that addresses all the associated Performance Criteria could be useful. 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. This could be carried out under open-book conditions.

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.

National Unit Support Notes (cont)

Unit title: Digital Forensics (SCQF level 6)

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

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

Information and Communication Technology (ICT) (SCQF level 6)
Problem Solving (SCQF level 6)
*Communication (*SCQF level 6)

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 and evaluate reliability of information

Some of the Core Skill components in *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 and 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 such as the production of a report on the evaluation of the forensic findings.

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 6.

History of changes to Unit

Version	Description of change	Date
02	Core Skill Information and Communication Technology at SCQF level 6 embedded.	09/09/2015

Additional copies of this Unit specification can be purchased from the Scottish Qualifications Authority. Please contact the Business Development and Customer Support team, telephone 0303 333 0330.

General information for learners

Unit title: Digital Forensics (SCQF level 6)

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 comprehensive 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 and understand its relevancy to an enquiry under investigation. You will then evaluate the forensic findings and communicate your evaluation in an efficient way.

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. An evaluation report of your findings would make good assessment evidence, although this is decided by your centre.

You may progress to National Certificates or Higher National Certificates in Computing or related qualifications.

You may also develop skills that may lead to employment, skills in sustainable development and citizenship skills during your learning experience.