SQA Advanced Unit specification: general information

Unit title: Computer Forensics: Fundamentals

Unit code: HP28 47

Superclass: QH

Publication date: August 2017

Source: Scottish Qualifications Authority

Version: 01

Unit purpose

This unit is designed to introduce candidates to the fundamental issues involved in carrying out computer/digital related forensic investigations. It is intended for candidates undertaking an SQA Advanced Certificate/Diploma in Computing, or a related area, who require a broad knowledge of the elements that comprise the digital investigatory process.

On completion of the unit the candidate should be able to:

1 Perform incident response procedures.
2 Maintain and acquire digital evidence.
3 Examine digital evidence.
4 Prepare forensic documentation.

Recommended prior knowledge and skills

Access to this unit will be at the discretion of the centre; however it is recommended that candidates should have achieved the Core Skill of *Communication* at SCQF level 5. Knowledge of using application programs on a PC and a basic understanding of computer hardware, networks/internet and file system operation would also be beneficial. This may be demonstrated by the achievement of appropriate National Units or Courses in Computing and IT.

Credit points and level

1 SQA credit at SCQF level 7: (8 SCQF credit points at SCQF level 7*)

**SCQF credit points are used to allocate credit to qualifications in the Scottish Credit and Qualifications Framework (SCQF). Each qualification in the Framework is allocated a number of SCQF credit points at an SCQF level. There are 12 SCQF levels, ranging from National 1 to Doctorates.*

Core Skills

Opportunities to develop aspects of Core Skills are highlighted in the support notes of 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.

Unit specification: statement of standards

Unit title: Computer Forensics: Fundamentals

Unit code: HP28 47

The sections of the unit stating the outcomes, Knowledge and/or Skills, and evidence requirements are mandatory.

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. Candidates should not know in advance the items on which they will be assessed and different items should be sampled on each assessment occasion.

Outcome 1
Perform incident response procedures.

Knowledge and/or Skills
- Securing a crime scene.
- Identifying sources of digital evidence.
- Recording actions.

Evidence requirements
Assessment for this outcome will be in the form of a practical assignment. Candidates must produce evidence that **all** of the Knowledge and/or Skills items have been covered.

A **pro-forma** must be provided by the candidate for Outcome 1 that must record the successful completion of the following tasks:

- **Securing a crime scene**
  Identification and logging of PCs, devices and peripherals, 'freezing' the crime scene.

- **Identifying sources of digital evidence**
  PCs, Hard disks (internal and external), files, network activity, handheld devices, network devices, log files, volatile data, tracking offenders, ownership and possession.

- **Recording actions**
  Contemporaneous notes, Inventories, bagging and tagging.

Outcome 2
Maintain and acquire digital evidence.

Knowledge and/or Skills
- Maintain Continuity of Evidence (Chain of Custody).
- Implement a forensically safe working environment.
- Perform forensic acquisition.

Evidence requirements
Assessment for this outcome will be in the form of a practical assignment. Candidates must produce evidence that **all** of the Knowledge and/or Skills items have been covered.

A **pro-forma** must be provided by the candidate for Outcome 2 that must record the successful completion of the following tasks:

- **Continuity of evidence (Chain of Custody)**
  Chain of Custody procedures, evidence storage, recording evidence electronically.

- **Forensically safe working environments**
  Forensic tools, write blocking methods.

- **Forensic acquisition**
  Disk imaging, network/internet forensics, mobile/USB devices, live acquisition, dead acquisition, data verification.

Outcome 3
Examine digital evidence.

Knowledge and/or Skills
- Identify system information and volatile data.
- Perform hard disk/disk image analysis.
- Perform network and internet analysis.

Evidence requirements
- **System information and volatile data**
  Log files, user accounts, system time, running processes and services, memory information, open files, scheduled jobs.

- **Hard disk/disk image analysis**
  Deleted files, metadata, file fragments, slack space, string searching, encrypted data.

- **Network and internet analysis**
  Network connections, open ports, routing tables, session data, web browsing activity, email activity.

Outcome 4

Prepare forensic documentation.

Knowledge and/or Skills

- Identify reasons for carrying out an investigation.
- Identify steps taken throughout an investigation.
- Identify sources of evidence.
- Produce results based on analysis.
- Provide recommendations.

Evidence requirements

The candidates' Knowledge and/or Skills for Outcome 4 must be demonstrated in the evidence generated.

The candidate will produce a report of in the region 1,000 words covering:

- the reasons for carrying out a forensic investigation, including information pertaining to relevant laws, investigator background details and codes of conduct.
- details of contemporaneous notes generated during an investigation.
- identification of sources of evidence and appropriate procedures for handling evidence.
- findings based on the analysis of digital evidence during an investigation.
- recommendations made based on the analysis of results.

Unit specification: support notes

Unit title: Computer Forensics: Fundamentals

This part of the unit specification is offered as guidance. The support notes 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 is intended to provide candidates with suitable knowledge and grounding in carrying out computer and/or digital based forensic investigations and is likely to form part of a group award which is primarily designed to prepare candidates for employment in an IT/computer forensics and security related role.

As well as learning the practical elements associated with digital investigations using various tools, candidates 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 candidate is familiar and in particular the following documentation:

- Association of Chief Police Officers *'Good Practice Guide for Computer-Based Electronic Evidence'*

  https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].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/courts/procedure-rules/civil/rules/part35

Guidance on the delivery of this unit

This unit is assessed by one report of at least 1,000 words that covers the knowledge and skills of all outcomes. It is recommended that the assessment be based on an appropriate extended case study or suitable workplace situation. It should be noted that additional evidence generated through practical activity should be included as appendixes to the report, for example screenshots/photographic images, proprietary software output.

The main areas of study for this unit should centre upon the following elements:

- Candidates know how to respond to crime scenes and gather evidence in a methodical fashion.
- Candidates know where to look for sources of evidence based on the type of incident.
- Candidates are able to maintain evidence in such a way that it is admissible in a court of law.
- Candidates are able to use appropriate tools for forensic acquisition.
- Candidates are able to perform tests and analyse results that should be repeatable by a third party.
- Candidates are able to prepare forensic documentation for a third party be it senior executives or for a court of law.

The approach taken in this unit is designed in such a way that for each of the stages above relating to Outcomes 1, 2 and 3, the output produced is gathered together to produce one complete forensic report, as demonstrated in Outcome 4.

It is recommended that 30 hours be allocated to teaching of the above activities and 15 hours allocated to assessment and remediation.

The unit should be delivered in a way that enables candidates to appreciate its relevance to the occupational area of computer forensics and security.

Guidance on the assessment of this unit

Outcomes 1, 2 and 3 will be assessed using a series of assignments testing practical abilities. Evidence for these outcomes must be gathered using logbooks and/or appropriate software to record activity. Outcome 4 will be assessed by candidates producing a written report of 1,000 words detailing findings produced in Outcomes 1, 2 and 3.

Any assessment activity involving practical work must be carried out in supervised conditions sufficient to ensure the confidence in the authenticity of submissions and that a candidate is working within the correct procedures.

Candidates may be able to work from a given case study to which they apply practical methods and then produce a written report of analysis, findings and recommendations. The case study must be presented prior to any practical work being undertaken.

There is also opportunity for e-assessment within this unit whereby e-portfolios may be used for recording evidence arising from practical elements.

Assessment guidelines

Outcomes 1–4

Outcomes 1–4 are combined. This should be in the form of an extended case study giving details of an 'incident' to which candidates have to respond to by completing Outcomes 1, 2 and 3. Output from Outcomes 1, 2 and 3 form the basis of the forensic report produced during Outcome 4.

The assessor should feel free to answer questions or clarify any misunderstandings relating to the case study that a candidate may have. The assessor should encourage discussion of the case study in relation to necessity and proportionality tests, laws associated with digital forensic investigations, codes of conduct, ethical problems and forensic duplication methodologies.

Online and distance learning

If this unit is delivered by open or distance learning methods, additional planning and resources may be required for candidate support, assessment and quality assurance. A combination of new and traditional authentication tools may have to be devised for assessment and re-assessment purposes.

For further information and advice, please see *Assessment and Quality Assurance of Open and Distance Learning* (SQA, February 2001 — publication code A1030).

Opportunities for the use of 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 candidate evidence and that conditions of assessment as specified in the evidence requirements are met, regardless of the mode of gathering evidence. Further advice is available in *SQA Guidelines on Online Assessment for Further Education (AA1641, March 2003).*

Opportunities for developing Core Skills

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

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.

History of changes

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 candidates

Unit title: Computer Forensics: Fundamentals

This unit is designed to enable candidates to identify the main factors involved in carrying out a computer/digital based investigation. In order to work effectively as a digital forensic investigator, professionals need to identify the elements that comprise the life cycle of an investigation. The aim of this unit is to enable you to gain an understanding and appreciation of a number of areas of concerns to investigators and organisations alike.

You will be expected to be able to apply much of the practical skills and theoretical elements to issues in the work place or to case study situations. You will be provided with the opportunity to gain knowledge in a number of different working environments.

Work for all outcomes will assessed by using one case study in which you will be confronted by a scenario whereby you will carry out various practical investigatory tasks and then produce a written report of approximately 1,000 words based on the findings of the practical tasks.

Outcome 1 you will learn how to perform incident response procedures; what to do upon arrival at a crime scene, where to look for digital evidence, based on the type of incident and/or crime that has been committed and how to apply best practice procedures when recording evidence.

Outcome 2 takes the investigation a step further with initiation of the Chain of Custody process and subsequent management, how to safeguard digital evidence through forensic acquisition and the type of tools and methodologies used in forensic duplication.

Outcome 3 deals with the analysis of different types of evidence based on the source of evidence; system information, hard disk information and network/internet information.

Outcome 4 deals with the production of a forensic report that will be based on the investigation and analysis carried out during the previous outcomes and aims to identify the skills needed in the production of a formal report for use by business executives or law enforcement in a court of law.