Unit 37: Forensic Science Informatics

Unit code: J/502/5582

QCF Level 3: BTEC National

Credit value: 10

Guided learning hours: 60

Aim and purpose

The aim of this unit is to enable learners to develop ICT skills in relation to producing documents suitable for use in forensic science. Learners will also investigate internet crime and computer sabotage.

Unit introduction

This unit gives learners the opportunity to develop their ICT skills to produce an integrated document for use in forensic science. Learners will use word processing, spreadsheet, database, image editing and webpage software. They will also gain a theoretical knowledge of the use of the laws governing, and the criminal activities associated with, the internet and the worldwide web.

This unit will give learners the opportunity to understand how the criminal community and forensic information technology crime investigators use computers. This is a fast-expanding area and much new legislation has been written, or is being considered, to cover this relatively new area of crime.

Learning outcomes

On completion of this unit a learner should:

1 Be able to use information and communication technologies to obtain forensic information

2 Know how internet misuse is policed

3 Know the common methods of computer sabotage

4 Be able to use computer software to produce a document that could be used for forensic purposes.

Unit content

1 Be able to use information and communication technologies to obtain forensic information

The internet: uses; connections eg modems; service providers; wireless technology; hand-held devices eg mobile phones, palmtops, personal digital assistant (PDA)

Using the internet and intranet: download files or program; connecting to the internet; uses and abuse of internet; the worldwide web; how the web works; intranets and extranets; protocols (TCP/IP, FTP, SMTP, POP3, HTTP); transferring information

2 Know how internet misuse is policed

Jurisdiction: local; European; international; internet boundaries; laws eg Computer Misuse Act 1990, Data Protection Acts (1984, 1988 and 1994 Guidelines), Copyright, Designs and Patents Act 1988, Race Relation Acts, Disability of Discrimination Act 1995, Sex Discrimination Act 1986, Employment Act 1963, 1988, 1989, Companies Act 1985; common laws; laws on torts; criminal laws eg offences against minors, public moral/decency; warrants eg PACE Act 1984; power of goods/equipment seizure

Investigation of computer crimes: identification of crime; agency which has jurisdiction or multi-agency approach (police, HM Revenue and Customs, Serious Fraud Squad, MI5, Trading Standards Office); methodologies of gathering evidence eg doctrine of documentary evidence, verbal and real evidence, copying of the entire target computer system onto a media for examination, protection of files by encryption software, protection of system by physical devices (locks), level of security code

Forensic agencies' aids: Police National Computer (PNC); DVLA; National Finger Print Identification System (NAFIS); treadmate; national DNA database (NDNAD); Information recording system (IRS) for the Fire Service, storage of data and analysis; statistical analysis; mapping; method of operandi (MO) eg suspects, vehicle, criminal record number, computer imaging

3 Know the common methods of computer sabotage

Hacking or cracking: profile of victims and offenders; intellectual challenge; selling sensitive information; phishing; military secrets; commercial loss/gain; white-collar crime

Software disablers: home-made program; program converted for the purpose; commercial encryption packages; self-destruct program (start-up of computer); DOS; Unix; unformatting program

Hardware disablers: preserve an accurate record (exhibits)

Computer sabotage: clipper chip; encryption; logic bomb; pinging; remailer; trapdoor; Trojan horse; virus; worm; spyware

Sabotage protection: firewall; anti-virus software; pop-up blockers; anti-spyware

4 Be able to use computer software to produce a document that could be used for forensic purposes

Computer systems architecture: setting up a computer system (input and output devices, storage systems, operating systems, computer network)

Word-processing packages: toolbars; basic terminology; online help; grammar and spelling; export and import documents and files; different methods of data storage

Spreadsheet packages: screen components; toolbars; basic terminology; keying data; selection technique; moving around in worksheets; switching between worksheets; use of statistical and mathematical functions; chart wizard; import/export data; online help

Database packages: types of data; manipulation of data; help menu; creating a database; datasheet display; sorting and searching; forms and reports; import and export data

Graphics packages: uses eg to produce a scene of crime image from photo/graphic/text; amendments; export and import; drawing tools; colours; opening and saving file in different formats; commercially available sector-specific software

Web-page packages: HTML; opening and closing tags; web-page creation software

Assessment and grading criteria

In order to pass this unit, the evidence that the learner presents for assessment needs to demonstrate that they can meet all the learning outcomes for the unit. The assessment criteria for a pass grade describe the level of achievement required to pass this unit.

Assessment and grading criteria					
To achieve a pass grade the evidence must show that the learner is able to:		**To achieve a merit grade the evidence must show that, in addition to the pass criteria, the learner is able to:**		**To achieve a distinction grade the evidence must show that, in addition to the pass and merit criteria, the learner is able to:**	
P1	use information and communication technologies to access valid information related to a forensic case study [IE1]	**M1**	demonstrate methods available to exchange forensic information using information and communication technologies	**D1**	evaluate the safety of methods available to transfer forensic information
P2	describe crimes which can be committed using the internet, indicating how they are policed [IE1]	**M2**	explain the main UK laws which apply to computer misuse	**D2**	evaluate methods used for policing the internet
P3	describe common methods of computer sabotage [IE1]	**M3**	explain the role of the internet in computer sabotage	**D3**	evaluate methods available to prevent computer sabotage
P4	use appropriate software to produce a document that could be used for forensic purposes. [CT1,5; SM3]	**M4**	explain how the document would be used for forensic purposes.	**D4**	evaluate your choice of software, considering whether alternatives would have been more appropriate.

PLTS: This summary references where applicable, in the square brackets, the elements of the personal, learning and thinking skills applicable in the pass criteria. It identifies opportunities for learners to demonstrate effective application of the referenced elements of the skills.

Key	IE – independent enquirers	RL – reflective learners	SM – self-managers
	CT – creative thinkers	TW – team workers	EP – effective participators

Essential guidance for tutors

Delivery

This unit is largely skills based. Tutors should use an active and investigative approach to enable learners to achieve the learning outcomes. Learners should be encouraged to be independent and, over time, to reflect and act critically.

Tutors could use a range of techniques to deliver the unit content, including formal lectures, discussions, seminars, internet research and use of library resources. The aim is to stimulate and educate learners so they will be in a position to understand the main ways in which crime is committed using computers and the internet, and how to track online use. This understanding enables learners to see the range of job opportunities available, and the range of courses that higher education can offer.

The latest acts and regulations should always be used.

Learning outcome 1 requires learners to use ICT equipment to obtain and exchange forensic information. This learning outcome can be covered while learners are completing learning outcome 4. It is recommended that learners are fluent with the range of internet and email protocols and how these ensure the correct passage of data.

For learning outcome 2 case studies would be an interesting way to learn how internet crimes are committed and investigated and whether the investigation was ultimately successful. This can then be linked to stating which computer laws have been broken in the case study.

Learning outcome 3 covers identifying internet activity and computer sabotage methods. Learners could be taught how to search the WHOIS database, but if this is not possible the learning outcome could be taught alongside learning outcome 3 using case studies.

Learning outcome 4 covers the selection and use of software packages to put together a document that could be used for forensic purposes. This learning outcome should involve formal lectures showing learners how to use software packages to produce a portfolio of a forensic nature. Digital photographs of recreated crime scenes would enable learners to gain experience of editing photographs for forensic purposes. Documentaries and case studies could be used as a basis for the forensic portfolio.

Outline learning plan

The outline learning plan has been included in this unit as guidance and can be used in conjunction with the programme of suggested assignments.

The outline learning plan demonstrates one way in planning the delivery and assessment of this unit.

Topic and suggested assignments/activities and/assessment
Introduction to unit and programme of assignments.
Tutor input: hardware and software available.
Introduction to forensic case studies. Practical sessions on using the internet to perform searches.
Assignment 1 – Accessing Forensic Information (P1, M1, D1)
Internet policy. Investigation of computer crimes.
Assignment 2 – It's the Law (P2, M2, D2)
Introduction to methods of computer sabotage. Use of methods of sabotage protection.
Assignment 3 – Hacking (P3, M3, D3)
Practical sessions on using computer software.
Assignment 4 – Forensic Documents (P4, M4, D4)
Review of unit and programme of assignments.

Assessment

Assessment should be based on a series of practical and theoretical assignments. It should ideally be problem based, enabling learners to investigate the associated grading criteria.

All the pass grade criteria must be met in order for a learner to achieve this unit.

For P1, learners must be able to navigate their way around the internet efficiently. They must also be able to ascertain the validity of the information they find. For M1, learners must use the ping command to test the response of a host computer, and in the process calculate the time taken for data to reach its destination. It is recommended that learners use the command prompt, but firewall restrictions may prohibit this. In this case, the website www.dnsstuff.com has a ping utility which can be used as a substitute. These tools record packet details to and from the www.dnsstuff.com website rather than from the learner's PC, but it is a useful substitute. For D1 learners must evaluate whether the methods available to transfer forensic information are suitable and safe.

For P2, learners must describe how crimes can be committed using the internet. This could be done by using case studies. Learners can then use the study to indicate which laws were broken and how the case was investigated. For M2, learners must demonstrate awareness of the legislation covering misuse of computers. They must explain their purpose and how they contribute to policing the internet. For D2, learners must assess whether the current UK legislation is effective and sufficient in controlling computer and internet misuse. Learners are required to make conclusions if legislation is deficient, and suggest more effective ways of controlling computer misuse.

For P3, learners must define the computer sabotage terms and describe the destructive nature of the defined computer sabotage terms. For M3, learners must give details of how the internet is used in computer sabotage. For D3, learners must evaluate the current methods used to prevent computer sabotage. The difficulties in controlling the internet should be explored and suggestions of more effective methods given.

For P4, learners must, with guidance, use common commercial software to produce a document which could be used for forensic purposes. It is important that data and a graph are imported into the document rather than added as separate sheets into the assignment. Database activities could involve entering data relating to serial murders or other crimes. Graphs could be related to criminal profiling, for example geographical.

For M4, learners must explain how their document would be used for forensic purposes. In this way they will show synthesis between their knowledge of the forensic investigation process and how to produce a suitable document.

For D4, learners must evaluate the suitability of their document, considering the software used and whether other formats would have been more suitable.

Programme of suggested assignments

The table below shows a programme of suggested assignments that cover the pass, merit and distinction criteria in the assessment and grading grid. This is for guidance and it is recommended that centres either write their own assignments or adapt any Edexcel assignments to meet local needs and resources.

Criteria covered	Assignment title	Scenario	Assessment method
P1, M1, D1	Accessing Forensic Information	You have a new position as a forensic assistant working on a new case. You have been asked to search for information related to the case and send this information to the team.	Portfolio of evidence which compiles the information gathered. Evidence of exchanging information with peers.
P2, M2, D2	It's the Law	As part of your professional development you need to produce a report on how the internet is policed.	Report.
P3, M3, D3	Hacking	The local police station is having an open day and you have been asked to contribute towards an information leaflet/presentation on computer sabotage.	Information leaflet or presentation.
P4, M4, D4	Forensic Documents	You have been asked to produce a document related to the case you are working on.	Presentation of a document that could be used for forensic purposes.

Links to National Occupational Standards, other BTEC units, other BTEC qualifications and other relevant units and qualifications

This unit forms part of the BTEC Applied Science sector suite. This unit has particular links with the units shown below in the BTEC Applied Science suite of qualifications:

Level 2	Level 3
Investigating a Crime Scene	Informatics in Science
	Forensic Photography
	Criminal Investigation Procedures
	Criminal Investigations in Practice

Essential resources

To complete this unit, learners will need access to computers and the internet to access the websites shown below. Learners can edit photographs taken in *Unit 33: Forensic Photography* and include them in the forensic document.

Employer engagement and vocational contexts

Learners should be encouraged to visit a police station and to use local media and ideally talk to community groups. Guest speakers from the criminal justice system would be a very useful resource and would be beneficial in strengthening links between academic centres and their local communities. Visits to courtrooms will enable learners to witness the presentation of evidence and how the adversarial system works in practice.

Indicative reading for learners

Textbooks

Beales R P – *PC Systems, Installation and Maintenance* (Newnes, 2003) ISBN 9780750660747

Bejtlich R et al – *Real Digital Forensics: Computer Security and Incident Response* (Addison Wesley, 2005) ISBN 9780321240699

Casey E – *Digital Evidence and Computer Crime* (Academic Press Inc. US, 2004) ISBN 9780121631048

Jones R – *internet Forensics* (O'Reilly, 2005) ISBN 9780596100063

Websites

www.antionline.com	IT security website
www.apnet.com	Academic Press
www.cops.org	International Association of Computer Investigative Specialists
www.dnsstuff.com	WHOIS lookup, ping and tracert commands
www.findlaw.com	Legal website
www.guidancesoftware.com	Forensic website
www.htcia.org	High Tech Crime Investigation Association
www.lawcrawler.com	Legal website
www.oreilly.com	Computer books, conferences and online publishing
www.virtuallibrarian.com	Virtual librarian
www.warriorsofthe.net	Looking at how the internet works
www.whatis.com	IT encyclopaedia and learning centre

Delivery of personal, learning and thinking skills

The table below identifies the opportunities for personal, learning and thinking skills (PLTS) that have been included within the pass assessment criteria of this unit.

Skill	When learners are …
Independent enquirers	[IE1] identifying questions to answer when searching for information on the internet
Creative thinkers	[CT1,5] designing and producing a forensic document, trying out alternatives when necessary and following through ideas
Self-managers	[SM3] organising time and resources when collecting data and planning the document.

Although PLTS are identified within this unit as an inherent part of the assessment criteria, there are further opportunities to develop a range of PLTS through various approaches to teaching and learning.

Skill	When learners are …
Independent enquirers	[IE6] supporting conclusions drawn from the evaluation of methods available to police the internet and prevent computer sabotage
Creative thinkers	[CT2] asking questions to extend thinking when exploring a particular area of interest related to forensic informatics
Reflective learners	[RL4,5] inviting feedback on other presentations, evaluating own work and recommending improvements for the future
Team workers	[TW6] providing feedback to peers.

Functional Skills – Level 2

Skill	When learners are …
ICT – Find and select information	
Select and use a variety of sources of information independently for a complex task	planning and carrying out an internet search and selecting the relevant information which relates to a forensic crime case
Access, search for, select and use ICT-based information and evaluate its fitness for purpose	evaluating the methods that exist to prevent computer sabotage
ICT – Develop, present and communicate information	
Enter, develop and format information independently to suit its meaning and purpose including: • text and tables • images • numbers • records	entering a range of information to produce a document for forensic purposes
Evaluate the selection and use of ICT tools and facilities used to present information	selecting ICT tools that are appropriate to produce a document for forensic purposes
Mathematics	
Identify the situation or problem and the mathematical methods needed to tackle it	carrying out calculations from a forensic science data source
Select and apply a range of skills to find solutions	planning and interpreting information
Interpret and communicate solutions to practical problems in familiar and unfamiliar routine contexts and situations	interpreting the results of calculations
English	
Speaking and listening – make a range of contributions to discussions and make effective presentations in a wide range of contexts	taking part in group discussions about a complex subject such as computer fraud
Reading – compare, select, read and understand texts and use them to gather information, ideas, arguments and opinions	using literature sources to read and synthesise information
Writing – write documents, including extended writing pieces, communicating information, ideas and opinions, effectively and persuasively	preparing a document for forensic purposes.