Unit title:	Digital forensics
Unit number:	30
Level:	5
Credit value:	15
Guided learning hours:	60
Unit reference number:	D/601/1939

UNIT AIM AND PURPOSE

To provide learners with an understanding of digital forensics in social and commercial environments. The learner will explore current computer forensic techniques and apply these to an investigation and analyse their findings.

LEARNING OUTCOMES AND ASSESSMENT CRITERIA

A pass grade is achieved by meeting **all** the requirements in the assessment criteria.

Learning Outcome (LO) The Learner will:	**Pass** The assessment criteria are the pass requirements for this unit. The Learner can:
LO1 Understand the impact of digital forensics on the social and commercial environments	1.1 evaluate current forensic practice 1.2 discuss the potential impact of a forensic investigation 1.3 discuss the impact of ‘motivation’, data manipulation and malware
LO2 Understand the principles of evidence gathering	2.1 discuss the principles of evidence gathering 2.2 evaluate current evidence gathering practices and assess their impact
LO3 Be able to plan and implement digital forensics investigations	3.1 based on a given scenario, plan a digital forensics investigation 3.2 implement a digital forensics investigation 3.3 systematically record each process during investigation
LO4 Be able to analyse the outcomes of digital forensics investigations	4.1 present findings of forensics investigation 4.2 critically review and analyse findings

GRADING CRITERIA

A merit grade is achieved by meeting **all** the requirements in the pass criteria **and** the merit descriptors.

A distinction grade is achieved by meeting **all** the requirements in the pass criteria **and** the merit descriptors **and** the distinction descriptors.

Merit Criteria (M1, M2, M3) (M1, M2, and M3 are mandatory to achieve a merit grade. Each must be achieved at least once per unit to achieve a merit grade.)	**Distinction Criteria (D1, D2, D3)** (D1, D2, and D3 are mandatory to achieve a distinction grade. Each must be achieved at least once per unit to achieve a distinction grade.) (In order to achieve a distinction grade, all merit criteria must also have been achieved.)
MANDATORY TO ACHIEVE A MERIT GRADE	MANDATORY TO ACHIEVE A DISTINCTION GRADE
M1 Analyse concepts, theories or principles to formulate own responses to situations.	D1 Evaluate approaches to develop strategies in response to actual or anticipated situations.
M2 Analyse own knowledge, understanding and skills to define areas for development.	D2 Evaluate and apply strategies to develop own knowledge, understanding and skills.
M3 Exercise autonomy and judgement when implementing established courses of action.	D3 Determine, direct and communicate new courses of action.

TEACHING CONTENT

The Teaching Content describes what has to be taught to cover **all** Learning Outcomes.

Learners must be able to apply relevant examples to their work although these do not have to be the same as the examples specified.

LO1 Understand the impact of digital forensics on the social and commercial environments	
Digital	Storage devices, operating systems, forensic analysis, how data is stored, networks, hiding techniques
Threat	Virus, Trojan, worm, spyware, screen recorder, manipulation of customers
Social impact	e.g. loss of confidence, loss of access, financial loss to customers
Commercial impact	e.g. financial implications, customer confidence, corporate image.
LO2 Understand the principles of evidence gathering	
Tools	Evidence preservation, software applications packages available e.g. EnCase, LinEn, legislation, civil action
Evidence	Legal authorities both international and local, records, system images, interviewing witnesses.
LO3 Be able to plan and implement digital forensics investigations	
Imaging	Maintain data integrity, range of storage devices, data recovery
Network	Topology, network security, hexadecimal, binary and IP addressing, traffic monitoring, intrusion detection, workstation forensics
Planning	Legal authorities, legal representatives, corporate personnel, record keeping, time line, evidence gathering, best practice for preserving evidence.
LO4 Be able to analyse the outcomes of digital forensics investigations	
Findings	Evidence, issues, records, impartial information, legal proceedings
Recommendations	Amendments to policies and procedures, staff issues, legal implications.

GUIDANCE

Delivery guidance
It will be beneficial to deliver this unit in a way that uses actual events, industry forecasts or sector specific contexts which offer the learner the opportunity to explore, develop and apply the fundamental principles of the sector or subject area. Typical delivery contexts could include guest speakers and industrial visits. Learners will benefit from being encouraged to exercise autonomy and judgement to analyse case studies, adapt their thinking and reach considered conclusions when evaluating the impact of digital forensics on social and commercial environments. Learners would benefit from being presented with subject/sector-relevant problems from a variety of perspectives, and being given the opportunity to explore them using diverse approaches and schools of thought. For example, industrial visits to see a range of investigations being carried out.

Assessment evidence guidance
Evidence must be produced to show how a learner has met each of the Learning Outcomes. This evidence could take the form of assignments, project portfolios, presentations or, where appropriate, reflective accounts. Where group work/activities contribute to assessment evidence, the individual contribution from each learner must be clearly identified. All evidence must be available for the visiting moderator to review. Where learners are able to use real situations or observations from work placement, care should be taken to ensure that the record of observation accurately reflects the learner's performance. This should be signed, dated, and included in the evidence. It is best practice to record another individual's perspective of how a practical activity was carried out. Centres may wish to use a witness statement as a record of observation. This should be signed and dated and included in the evidence.

RESOURCES

Books

Britz, Marjie, *Computer Forensics and Cyber Crime: An Introduction,* Prentice Hall, 2003, ISBN 9780130907585

Jones, Keith J., Bejtlich, Richard,. Rose, Curtis W., Farmer, Dan., Venema, Wietse., Carrier, Brian., *Computer Forensics Library,* Addison-Wesley Educational Publishers Inc, 2007, ISBN 9780321525642

Laykin, Erik., *Investigative Computer Forensics: The Practical Guide for Lawyers, Accountants, Investigators, and Business Executives,* John Wiley & Sons Ltd, 2013, ISBN 9780470932407

Bunting, Steve., *EnCase Computer Forensics - The Official EnCE: EnCase Certified Examiner Study Guide,* John Wiley & Sons Ltd, 2012, ISBN 9780470901069

Altheide, Cory., Carvey, Harlan., *Digital Forensics with Open Source Tools: Using Open Source Platform Tools for Performing Computer Forensics on Target Systems: Windows, Mac, Linux, Unix, Etc*. Syngress Media, 2011, ISBN 9781597495868

Solomon, Michael G., Rudolph, K., Tittel, Ed., Broom, Neil., Barrett, Diane., *Computer Forensics JumpStart,* John Wiley & Sons Ltd, 2011, ISBN 9780470931660

Journals

The International Journal of Forensic Computer Science, Print ISSN: 1809-9807 - Online ISSN: 1980-7333

Websites

Computer Forensics, Malware Analysis & Digital Investigations
www.forensickb.com/