Unit 49: Digital Forensics

Unit code: D/601/1939
QCF Level 5: BTEC Higher National
Credit value: 15

- **Aim**

To provide learners with an understanding of the principles of digital forensics and the impact on commerce, society and the individual.

- **Unit abstract**

With the evolution of information technology and the increasing adoption of telecommunication-based systems, opportunities for criminal and illegal practice have expanded exponentially. For an ICT professional, managing the security of any complex corporate system comes with many challenges. When a breach of the system occurs a criminal act takes place against an organisation or an individual.

As with a real-world crime scene, a computer system can be used as a tool to implicate criminal activity. The need to preserve the crime scene and ensure the analysis is completed in a manner conducive to the fair and unbiased pursuit of justice is of the greatest importance.

In legal proceedings, the evidence presented is often called into doubt by the presence of unsafe practice in the acquisition of forensic evidence from a computer system. In taking this unit, the learner is introduced to IT forensics and the critical need for accurate, detailed and recorded investigation of the fact.

The practice of IT forensics has to be supported by individuals trained in national or international law enforcement practice. In preserving the scene learners must ensure system logs, operating system data and other relevant information is acquired and stored as an image of the time of forensic acquisition. Learners must be in a position to assist any potential legal process and ensure the evidence acquired supports a successful and fair legal outcome.

Learners will need to understand and review cases where the process of forensic analysis determines the absence of direct criminal intent and serves as a process to improve security and administrative processes as well as technological implementation.

- **Learning outcomes**

On successful completion of this unit a learner will:

1. Understand the impact of digital forensics on the social and commercial environments
2. Understand the principles of evidence gathering
3. Be able to plan and implement digital forensics investigations
4. Be able to analyse the outcomes of digital forensics investigations.
Unit content

1. **Understand the impact of digital forensics on the social and commercial environments**

   *Approach:* types eg legal forensic analysis, illegal forensic analysis, defensive forensics, offensive forensics

   *Data manipulation:* digital data/information hiding techniques eg steganography, encryption, obfuscation; tools available

   *Malware:* types eg virus, trojan, worm, zombie, botnet, keylogger, screen recorder; social engineering; exploitation of personal confidence

   *Motivation:* deliberate eg commercial, criminal, personal, political, ideological, investigative; casual eg explorative, leading to deliberate motivation

   *Commercial:* impacts eg loss of faith, financial loss, competitive advantage, unfavourable corporate image

   *Social:* impacts eg financial loss, loss of resource, loss of access, loss of trust

2. **Understand the principles of evidence gathering**

   *Evidence:* chain of custody; evidence preservation; local legislation on evidence; international evidence requirements; jurisdiction

   *Evidential challenges:* technological change; technological behaviours; adaptability of the opponent; change in legislative practice; legal challenge

   *Involvement of legal authorities:* international law enforcement; local law enforcement; criminal proceedings; civil action

   *Record keeping:* methods eg reporting, recording, statements, system logs, operating system images

   *Interview of witnesses:* methods eg keeping a record, with a co-interviewer, interviewees right to counsel; involvement of corporate personnel management eg disciplinary management, criminal proceedings, civil action; background checks
3 Be able to plan and implement digital forensics investigations

**Network forensics:** sources eg traffic monitoring, traffic signatures, Simple Mail Transfer Protocol (SMTP) logging, span ports, traffic redirection, traffic reassembly, intrusion detection systems, email trails, firewall logs, anomaly identification and management, scanning tools, Address Resolution Protocol (ARP) poisoning

**Workstation or server forensics:** sources eg analysis of file systems, different operating system profiles, malware detection and removal, working on images of systems, application MD5 fingerprint, registry (system database) change analysis

**Data Forensics:** sources eg storage device data recovery, analysis of data change, database rollback and audit

**Device specific behaviour:** devices eg server, desktop computer, mobile device, file system, communication medium, protocol, application used, power status

**Tools:** commercial eg encase, fdk, helix, cloning software, virtualisation environments, virus scanning, network scanning, network analysis; open source; system logs; access logs

**Planning:** evidence gathering techniques; involvement of legal authority; involvement of corporate personnel management; record keeping; time constraint; diligence

**Safe practice:** procedures eg handling evidence on first receipt, creation of images, disk cloning, safe shutdown of an active system for forensic analysis.

4 Be able to analyse the outcomes of digital forensics investigations

**Presentation of the fact:** impartial information; absence of supposition; detailed delivery; independent analysis eg second opinion

**Reporting:** legal proceedings (civil, criminal, disciplinary, technical review, security audit, procedural audit)

**Procedural change:** update policy eg security, technology, forensic analysis technique, staff vetting
# Learning outcomes and assessment criteria

<table>
<thead>
<tr>
<th>Learning outcomes</th>
<th>Assessment criteria for pass</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>On successful completion of this unit a learner will:</strong></td>
<td><strong>The learner can:</strong></td>
</tr>
</tbody>
</table>
| **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. |
Guidance

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

The learning outcomes associated with this unit are closely linked with:

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Unit 46: Network Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit 48: IT Security Management</td>
</tr>
</tbody>
</table>

This unit has links to the Level 4 and Level 5 National Occupational Standards for IT and Telecoms Professionals, particularly the areas of competence of:

- IT Security Management.

Essential requirements

As recommended in the delivery guidance, a centre delivering this unit must have access to suitable forensic applications and ‘investigative’ artefacts to deliver this unit. The primary focus is practice based and therefore this unit cannot be delivered in a theoretical context.

Learners must have access to facilities which allow them the opportunity to fully evidence all of the criteria of the unit. If this cannot be guaranteed then centres should not attempt to deliver this unit.

The learner will need to evaluate a system, using an existing system or live computer.

The investigation must be systematic and procedural based on the planning and current ‘local’ forensic practice. Please refer to local law, international law and the accepted practice of managing criminal evidence.

Resources

Books


Websites
www.digitalforensicsmagazine.com/
www.e-evidence.info/thiefs_page.html

Employer engagement and vocational contexts

Liaison with local or national law enforcement would enhance the delivery of this unit. If the learner is employed, a contextual assessment based on their working environment with the support of their supervisory management would be of considerable value. Extreme care must be taken to ensure any real work projects are not detrimental to their employer or employment, or prejudicial to any potential legal outcome.