SFJ CO9
Take first response actions in investigations involving digitally related evidence

Overview

This standard is about taking the appropriate lawful actions in first response to encountering potential electronic evidence in the form of digital devices and media. These actions are in relation to investigation of criminal activity or intelligence gathering in relation to crime prevention and community safety.

The standard is also about identifying evidence and intelligence opportunities related to digital activity such as internet service providers, mobile phone service providers, social media accounts, internet transaction accounts and memberships.

A definition of context of digitally related crime is provided in the glossary.

SFJ CO9
Take first response actions in investigations involving digitally related evidence

Performance criteria

You must be able to:

- P1 take first response actions which are in accordance with provisions of law enforcement powers and warrants in relation to digital evidence
- P2 assess situations to identify possible involvement of digital devices and media
- P3 identify materials related to digital communications which are relevant to the investigation:
  - P3.1 usernames/IDs
  - P3.2 passwords
  - P3.3 email addresses
  - P3.4 membership of social media networks/forums
- P4 identify and validate types of digital devices and media to determine appropriate actions to take to preserve evidence
- P5 record current state, condition and configuration of digital devices and media in accordance with organisational procedures
- P6 preserve the integrity of digital devices and storage to prevent contamination, interference or deletion
- P7 handle digital devices and media consistent with preserving other potential evidence sources including fingerprints or DNA
- P8 access specialist guidance and support on actions to take for handling and preserving digital devices and media

SFJ CO9
Take first response actions in investigations involving digitally related evidence

Knowledge and understanding

You need to know and understand:

- K1 how to identify the digital devices and media used to access the internet
- K2 legislation, codes of practice and local policy in relation to searching and seizing digital devices and media
- K3 basic principles of communication and internet technology
- K4 current and emerging technologies in communications and their potential uses
- K5 how to access specialist guidance and support related to procedures for handling digital devices, media and evidence
- K6 specialist services and techniques available to analyse digital material
- K7 how to identify material evidence to aid the investigation into an individual's digital footprint including:
  - K7.1 usernames/IDs
  - K7.2 passwords
  - K7.3 email addresses
  - K7.4 membership of social media networks/forums
- K8 what a digital footprint is and the implications of own actions on them
- K9 purpose and use of open source
- K10 action required to preserve evidence and prevent interference and deletion
- K11 how actions taken can contaminate or destroy digital evidence
- K12 implications of the international nature of the internet and lack of boundaries
- K13 typical types and uses of digital devices and media in current use

SFJ CO9

Take first response actions in investigations involving digitally related evidence

Additional Information

Scope/range related to performance criteria

1 Record of current state (P5)
- 1.1 Note book
- 1.2 Photo
- 1.3 Video

SFJ CO9
Take first response actions in investigations involving digitally related evidence

Glossary

There is a variety of terms used in describing crimes involving the internet and electronic communications. The core wording seems to be inter-changeable depending on which published materials are used as the source. The core words include:

1 Cyber
2 Electronic
3 Digital
4 Technology
5 e- (as in e-crime)

This NOS predominantly uses ‘digital’ as the core word.

There are two applications of this terminology in relation to crime:

1 crime which is committed through the internet or electronic communications such as fraudulent transactions, phishing etc.

2 crimes committed against individuals or organisations in which technology may have been a tool such as grooming vulnerable people for exploitation.

Devices used in digitally related crime are constantly evolving in terms of their type, purpose and use. They may include computers; laptop, desktop, servers; data communication equipment; router, modem, network equipment; storage; hard drives, flash drives, CD/DVD; personal devices; phones, PDAs, tablets/iPads, MP3/iPods.

SFJ CO9

Take first response actions in investigations involving digitally related evidence

Developed by	Skills for Justice
Version number	1
Date approved	January 2013
Indicative review date	January 2018
Validity	Current
Status	Original
Originating organisation	Skills for Justice
Original URN	SFJ CO9
Relevant occupations	Police Officers; Forensic Scientists
Suite	Countering Cybercrime
Key words	Cyber; electronic; e-crime; digital; technology; initial response