SFJ CO1
Identify and secure electronic evidence sources

Overview

This standard covers identifying and securing electronic evidence sources to assist an investigation. The subjects of the investigations covered by this standard may be individuals and/or organisations.

The standard may relate to a criminal or civil investigation, or to due diligence and internal discipline. The work described in this standard could also be carried out over a network.

SFJ CO1
Identify and secure electronic evidence sources

Performance criteria

You must be able to:

P1 check that the necessary **authorisations** are in place
P2 conduct **preparatory research** concerning the **capabilities** of the individual subject of the investigation and / or the functionality of the relevant digital evidence source to which they have access
P3 identify and select the appropriate processes and consider multiple options to meet the needs of capture or seizure
P4 recognise **devices** capable of storing electronic evidence and determine whether they require capturing or seizing
P5 identify any health and safety risks associated with the electronic **devices**
P6 consider the volatility of data and its preservation
P7 identify external connections to and from **devices**
P8 isolate the scene and secure the electronic evidence sources to prevent contamination and external interference
P9 determine whether to capture electronic data or to seize electronic **devices**
P10 keep an accurate contemporaneous record of the securing of electronic evidence using appropriate methods

SFJ CO1
Identify and secure electronic evidence sources

Knowledge and understanding

You need to know and understand:

K1 legal and organisational requirements
- K1.1 relevant legislation, policies, procedures, codes of practice, guidelines and applicable standards for identifying and securing electronic evidence sources
- K1.2 relevant legislation and other organisational requirements
- K1.3 the limits of your responsibility and level of competence
- K1.4 the impact of your actions on victims and witnesses

K2 electronic evidence
- K2.1 the types of devices that contain electronic evidence and external connections to such devices
- K2.2 how to obtain information concerning electronic evidence sources that you are unfamiliar with
- K2.3 methods of protecting and concealing electronic information including encryption
- K2.4 how to identify and, if appropriate, deal with systems running methods of protecting and concealing electronic information including encryption
- K2.5 the types of operating systems that you may come across and how to deal with these
- K2.6 the volatility of data and how to preserve it
- K2.7 the types of actions necessary to preserve third party and volatile data sources

K3 identifying and securing electronic evidence sources
- K3.1 the reasons for carrying out preparatory research
- K3.2 how to carry out preparatory research
- K3.3 the processes for identifying and securing electronic evidence sources and how to use them
- K3.4 the different options for the capture or seizure of electronic evidence sources
- K3.5 the importance of maintaining an accurate contemporaneous record using appropriate methods

SFJ CO1
Identify and secure electronic evidence sources

Scope/range related to performance criteria

1 Authorisations
- 1.1 seizure
- 1.2 capture
- 1.3 contract or due diligence
- 1.4 consent
- 1.5 limitations

2 Preparatory research
- 2.1 open source research
- 2.2 background checks
- 2.3 electronic scoping

3 Capabilities
- 3.1 expertise
- 3.2 resources

4 Devices
- 4.1 a local ‘stand alone’ device
- 4.2 a device linked to a network

SFJ CO1
Identify and secure electronic evidence sources

Developed by	Skills for Justice
Version number	2
Date approved	January 2012
Indicative review date	December 2016
Validity	Current
Status	Original
Originating organisation	Skills for Justice
Original URN	SfJ CO1
Relevant occupations	Public Services; Public Services and Other Associate Professionals
Suite	Countering Cybercrime
Key words	e-crime, cybercrime, investigation, identify, secure, electronic sources