SFJ CO2
Seize and record electronic evidence sources

Overview

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

It may relate to a criminal or civil investigation, or to due diligence and professional standards.

SFJ CO2
Seize and record electronic evidence sources

Performance criteria

You must be able to:

- P1 check that the necessary **authorisations** are in place
- P2 keep a record of the condition and **state of the device** and potentially **relevant information** in the immediate vicinity
- P3 take appropriate action to safeguard the **device** and **relevant information** for the application of physical forensic examinations
- P4 assess the contents of the **device** in an appropriate manner
- P5 choose and apply when appropriate, the appropriate power off method for the **device**
- P6 photograph and label the components of the **device** making specific reference to ancillary leads and connections to the **device**
- P7 appropriately **package**, seal and label the **device** in accordance with current procedures
- P8 keep an accurate contemporaneous record of the seizure using appropriate methods

SFJ CO2
Seize and record 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 seizing and recording 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 them
- K2.7 how to preserve the information on battery powered devices
- K2.8 the types of actions necessary to preserve third party and volatile data sources

K3 seizing and recording electronic evidence sources
- K3.1 the reasons for seizing electronic evidence sources
- K3.2 how to keep a record of the seizure process, the condition and state of the device and the reasons why this is important
- K3.3 the importance of considering potentially relevant information in the immediate vicinity
- K3.4 the actions necessary to safeguard the device for forensic examinations
- K3.5 how to conduct a preview of the contents of electronic devices
- K3.6 the need to consider physical forensic examinations and the implications for your work
- K3.7 the importance of maintaining an accurate contemporaneous record using appropriate methods

SFJ CO2
Seize and record 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 State of the device
- 2.1 on or off
- 2.2 open encryption
- 2.3 network/remote connections
- 2.4 running programs/open files

3 Relevant information
- 3.1 passwords
- 3.2 phone numbers
- 3.3 URLs
- 3.4 user account details
- 3.5 open encrypted volumes
- 3.6 information stored remotely

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

5 Package
- 5.1 faraday bag
- 5.2 box
- 5.3 opaque
- 5.4 anti-static

SFJ CO2
Seize and record 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 CO2
Relevant occupations	Public Services; Public Services and Other Associate Professionals
Suite	Countering Cybercrime
Key words	e-crime, cybercrime, seize, record, electronic, evidence sources