SFJ CO3
Capture and preserve electronic evidence

Overview

This standard covers capturing and preserving electronic evidence. It applies to work carried out in a laboratory, but may also be applied to the capturing of electronic evidence at the scene.

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

SFJ CO3
Capture and preserve electronic evidence

Performance criteria

You must be able to:

P1 check that the necessary **authorisations** are in place

P2 conduct a preliminary **risk assessment** of the evidentially sound and safe capture of data from the source

P3 take appropriate action to safeguard the device and relevant information for the application of physical forensic examinations

P4 select the process and tools appropriate for the capture of **electronic evidence**

P5 ensure the preservation of third party and volatile data sources

P6 preserve the captured data to a suitable medium in line with **local protocols**

P7 keep an accurate contemporaneous record of the capture and preservation of **electronic evidence** using appropriate methods

SFJ CO3
Capture and preserve electronic evidence

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 capturing and preserving electronic evidence
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 capturing and preserving electronic evidence
K2.1 sources of electronic evidence
K2.2 the process and tools available for the capture of data and how to use such equipment
K2.3 how to obtain information on data sources that you are unfamiliar with
K2.4 methods of protecting and concealing electronic information including encryption
K2.5 how to identify and, if appropriate, deal with systems running methods of protecting and concealing electronic information including encryption
K2.6 the types of operating systems that you may come across and how to deal with these
K2.7 the types of actions necessary to preserve third party and volatile data sources
K2.8 how to document the data capture
K2.9 how to select a suitable medium to preserve data
K2.10 where solutions and additional support might be available to address problems arising in the capture of electronic evidence

SFJ CO3
Capture and preserve electronic evidence

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 Risk assessment
- 2.1 health and safety
- 2.2 physical integrity of the evidence
- 2.3 continuity
- 2.4 legality
- 2.5 authority
- 2.6 priority

3 Local protocols
- 3.1 good practice guides (e.g. ACPO, local operating procedures)
- 3.2 relevant legislation
- 3.3 note taking requirements
- 3.4 disclosure requirements

4 Electronic evidence
- 4.1 selected
- 4.2 partial
- 4.3 complete

SFJ CO3
Capture and preserve electronic evidence

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 CO3
Relevant occupations	Public Services; Public Services and Other Associate Professionals
Suite	Countering Cybercrime
Key words	e-crime, cybercrime, capture, preserve, electronic, evidence