SFJ CO6
Conduct Open Source Internet investigations

Overview

This standard covers conducting investigations or research and intelligence gathering from open source material obtained over the Internet.

The investigation can relate to a case in which the Internet has been used to facilitate a crime. Many of these cases will have international dimensions.

SFJ CO6
Conduct Open Source Internet investigations

Performance criteria

You must be able to:

P1 assess all **immediately available electronic evidence**, determine its volatility and take all necessary steps to preserve it

P2 assess all other readily available evidence, information and intelligence

P3 develop objectives for the investigation based on the evidence, information and intelligence

P4 conduct a **risk assessment**, assess the **factors** likely to impact on the investigation and take the appropriate action

P5 check that the necessary **authorisations** are in place, if appropriate

P6 determine the geographical and legal jurisdictions that apply and take any necessary steps to preserve and obtain evidence from abroad

P7 ensure that all **material** is **retained** and recorded in a durable and retrievable form

P8 identify and develop all **relevant lines of enquiry** fairly and without bias, and prioritise actions

P9 identify victim(s) and potential witnesses in accordance with legislation and policy

P10 brief others about the status of the investigation, where appropriate, to ensure continuity

P11 pass on any relevant information and intelligence that may be relevant to other actions promptly to the appropriate person or department

P12 fully document all decisions, actions, options and rationale in accordance with current policy and legislation

P13 identify relevant and / or primary evidence sources

P14 create evidential product, if appropriate

P15 review the scope of the investigation throughout the process, based on on-going findings

SFJ CO6
Conduct Open Source Internet investigations

Knowledge and understanding

You need to know and understand:

K1 legal and organisational requirements

K1.1 current, relevant legislation, policies, procedures, codes of practice, guidelines and applicable standards for conducting internet investigations

K1.2 current, relevant legislation and other organisational requirements in relation to race, diversity and human rights

K1.3 the impact of your actions on victims and witnesses

K2 ICT and the Internet

K2.1 how to use ICT equipment and internet based communication systems

K2.2 basic principles of how the Internet works

K2.3 internet based communication systems

K2.4 web site structures and protocols

K2.5 the global nature of the Internet

K2.6 methods of protecting and concealing electronic information including encryption and issues arising from its use

K2.7 how to identify and, if appropriate, deal with systems running methods of protecting and concealing electronic information including encryption

K2.8 the types of operating systems that you may come across and how to deal with these

K3 internet investigation

K3.1 how to obtain evidence, information and intelligence for an internet investigation

K3.2 the sources of relevant evidence, information and intelligence

K3.3 how to assess the available information and intelligence for an internet investigation

K3.4 how to assess the factors that may impact on the internet investigation

K3.5 the additional support which is available and may be required for the internet investigation

SFJ CO6
Conduct Open Source Internet investigations

Scope/range related to performance criteria

1 Immediately available electronic evidence
- 1.1 presented volatile evidence
- 1.2 portable and mobile electronic devices
- 1.3 remotely stored
- 1.4 live session/on-screen data
- 1.5 communications service providers and registry records

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 Factors
- 3.1 vulnerability
- 3.2 language
- 3.3 culture
- 3.4 lifestyle
- 3.5 repeat/linked incidents
- 3.6 geographical and legal jurisdiction
- 3.7 technological complexity
- 3.8 social and economic impact

4 Authorisations
- 4.1 preservation
- 4.2 capture
- 4.3 contract or due diligence
- 4.4 consent
- 4.5 limitations

5 Material
- 5.1 information
- 5.2 objects
- 5.3 identity of potential witnesses
- 5.4 third party material or the existence of it

6 Retained
- 6.1 preserve
- 6.2 package
- 6.3 store

7 Relevant lines of enquiry
- 7.1 suspects
- 7.2 witnesses/victims
- 7.3 forensic/scientific
- 7.4 intelligence
- 7.5 property
- 7.6 sources of electronic evidence

SFJ CO6
Conduct Open Source Internet investigations

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 CO6
Relevant occupations	Public Services; Public Services and Other Associate Professionals
Suite	Countering Cybercrime
Key words	e-crime, cybercrime, conduct, open source, investigation, investigations