SFJCECCO6
Conduct internet investigations

Overview

This unit covers conducting investigations where part or all of the crime is conducted over the internet. These crimes can be where the internet has been used to facilitate a crime, for example malicious e-mails, indecent images, fraudulent purchases, identity theft etc. Many of these cases will have international dimensions.

There is one element

1 Conduct internet investigations

Target Group

This unit is aimed at trained members of staff who work in the specialist area of e-crime investigation.

SFJCECCO6
Conduct 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 accurately establish the nature of the incident to be investigated 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
P6 determine the geographical and legal jurisdictions that apply and take any necessary steps to preserve and obtain evidence from abroad
P7 identify the need for any **additional support** and take the appropriate action
P8 ensure that all **material** is **retained** and recorded in a durable and retrievable form
P9 identify and develop all **initial lines of enquiry** fairly and without bias, and prioritise actions
P10 identify victim(s) and potential witnesses in accordance with legislation and policy
P11 take the appropriate steps to identify and deal with any suspect(s)
P12 provide appropriate support for the immediate needs of victims, witnesses and suspects
P13 deal with individuals in an ethical manner, recognising their needs with respect to race, diversity and human rights
P14 brief others about the status of the investigation, where appropriate, to ensure continuity
P15 pass on any relevant information and intelligence that may be relevant to other actions promptly to the appropriate person or department
P16 fully document all decisions, actions, options and rationale in accordance with current policy and legislation

SFJCECCO6
Conduct internet investigations

Knowledge and understanding

Legal and organisational requirements

You need to know and understand:

K1 current, relevant legislation, policies, procedures, codes of practice and guidelines for conducting internet investigations
K2 current, relevant legislation and organisational requirements in relation to race, diversity and human rights
K3 current, relevant legislation and organisational requirements in relation to health and safety
K4 the support which should be provided to victim(s), potential witnesses and suspects within the limits of your responsibility
K5 the restrictions that apply to the disclosure of confidential information
K6 the policies and procedures that apply to contact with the media during investigations

Risk assessment

You need to know and understand:

K7 the purpose and importance of risk assessments
K8 how to conduct risk assessments

ICT and the Internet

You need to know and understand:

K9 how to use ICT equipment and internet based communication systems
K10 how the internet works
K11 internet based communication systems
K12 web site structures and protocols
K13 the global nature of the internet
K14 methods of encryption
K15 how to identify and deal with systems running encryption
K16 the types of non-standard operating systems that you may come across and how to deal with these

Internet Investigation

You need to know and understand:

K17 how to obtain evidence, information and intelligence for an internet investigation
K18 the sources of relevant evidence, information and intelligence
K19 how to assess the available information and intelligence for an internet investigation
K20 how to assess the factors that may impact on the internet investigation
K21 the additional support which is available and may be required for the internet investigation

SFJCECCO6
Conduct internet investigations

Additional Information

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. **Additional support**
   - 5.1. specialist support
   - 5.2. line management
   - 5.3. external agencies

6. **Material**
   - 6.1. information
   - 6.2. objects
   - 6.3. identity of potential witnesses
   - 6.4. third party material or the existence of it

7. **Retained**
    - 7.1. preserve
    - 7.2. package
    - 7.3. store

8. **Initial lines of enquiry**
    - 8.1. suspects
    - 8.2. witnesses/victims
    - 8.3. forensic/scientific
    - 8.4. intelligence
    - 8.5. property
    - 8.6. sources of electronic evidence

SFJCECCO6
Conduct internet investigations

Developed by	Skills for Justice
Version number	1
Date approved	February 2006
Indicative review date	February 2008
Validity	Current
Status	Original
Originating organisation	Skills for Justice
Original URN	SfJ CO6
Relevant occupations	Public Services; Information and Communication Technology; ICT for practitioners; Financial Institution and Office Manager; Public Service Professionals; IT Service Delivery Occupations; Public Service and Other Associate Professionals
Suite	Countering E-Crime
Key words	malicious emails, indecent internet images, fraudulent internet purposes, international internet investigations, conduct internet investigations