Handling Digital Evidence

Presentation by Bryan Sykes, Judge of the Supreme Court, at IP on Effective Protection and Enforcement, Montego Bay, October 14 - 15, 2014

Definition

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

http://nij.gov/publications/ecrime-guide-219941/introduction/Pages/what-is-digitial-evidence.aspx (Accessed October 15, 2014)

Important Factors

Easily altered, damaged or destroyed

Time sensitive

Crosses borders easily and quickly

http://nij.gov/publications/ecrime-guide-219941/introduction/Pages/what-is-digitial-evidence.aspx (Accessed October 15, 2014)

Four Basic Rules

Relevant – must be connected to some issue in case

Admissible – meets evidence law criteria

Authentic – it is what you say it is

All evidence including exculpatory evidence

First Responders

Recognise, identify, seize and secure

Document entire scene and specific location where evidence found

http://nij.gov/publications/ecrime-guide-219941/introduction/Pages/handing-evidence.aspx (accessed October 15, 2014)

First Responders

Collect, label and preserve

Package and transport in secure manner

http://nij.gov/publications/ecrime-guide-219941/introduction/Pages/handing-evidence.aspx (Accessed October 15, 2014)

Legal Authorisation

Make sure legal authority exists

Scene secured and documented

http://nij.gov/publications/ecrime-guide-219941/introduction/Pages/handing-evidence.aspx (Accessed on October 15, 2014)

Care in Handling

Digital evidence is susceptible to corruption and alteration

Secondary copies should be made where possible to work with

Any changes in digital evidence should be accounted for and explained

Handling Digital Evidence

If some alteration is necessary then nature, extent and reason should be stated

Capturing an accurate image of the hard drive should be done

Handling Digital Evidence

If computer found actually running – get material before shutting it down

Volatile evidence may be lost – browser be on privacy setting which does not store cookies and sites visited

Handling Digital Evidence

Distinguish evidence from junk

Evidence must be properly stored – any change must be accounted for

All techniques and procedures used in collection and analysis was be explained

Handling of Digital Evidence

Practical steps

Have a log that record everything from collection to presentation

Presentation of Digital Evidence

Prosecutor must understand the evidence and the terminology, the method of collection, the method of analysis

Prosecutor must be able to present case effectively – communicate technical information in ordinary language to fact finders