Regulating Digital Investigations

Sarah Hargreaves, Exterro

22 June 2021
A bit about me

• 18 years experience in digital forensics, supporting Police, Defence and Regulatory Organisations
• I joined AccessData, now Exterro, in September 2018 as Director of Training
• I now develop and deliver training classes to digital forensic professionals.
• I am very interested in the processes and procedures relating to the field.
Performing Internal Digital Investigations

• Internal investigation is commonplace within an organisation.
• It can include:
  • Internal disputes
  • Third party intrusion and incidents
  • Criminal matters
  • HR related issues

• Many of these investigations stay within the boundaries of internal investigation.
• But what if the investigation turns into a criminal matter?
  • Matter is reported to the Police at the early stage
  • Matter is reported to the Police after preliminary investigation
  • Matter is reported to the Police after full investigations
Digital Forensic Analysis – A Short History

- Digital Investigations has largely been unregulated for a long time.
- It was determined that there was a need for standardisation.
- It was recognised that digital forensic investigations were as scientifically relevant as traditional forensic techniques.
- It was identified that ISO17025 was the suitable standard. But this isn’t a ‘forensic standard’.
- Additional documents were referenced and produced so as to apply a suitable context to the standard.
- The Forensic Science Regulator was appointed.
- The Forensic Regulators Code of Practice and Conduct (now v.7).
- .........
The Forensic Regulators Code of Practice & Conduct

1.1.1 The Code of Practice is aimed at all those providing forensic science services to the Criminal Justice System (CJS), whether individual practitioners, academics, public or private sector forensic science providers, and refers to all as forensic units in line with the terminology used in ILAC-G19:08/2014. These can be small teams in larger organisations, sole practitioners or large providers and can be instructed by the prosecution or the defence.

3.1.1 The Codes are for all forensic units supplying forensic science services to the CJS. Forensic science is taken to include the sciences performed by the police service, the fire and rescue services, the public and private sector forensic units and, to a lesser extent, academia.

FSR Act 2021

• A new Forensic Science Regulator, Gary Pugh, was appointed recently.
• The Forensic Science Regulator’s Act 2021 came into force in May.
• The Act provides the FSR with the ability to investigate those that are conducting forensic science services to which the code applies.
What Does the FSR Act 2021 Mean for Internal Forensic Teams?

• Difficult to answer because the legislation is very new.
• A number of Police Forces are still not accredited and are continuing to gain accreditation.

• Make yourself familiar with the FSR Codes of Practice and the accompanying documents.
• Observe some of the opportunities to validate internal procedures.
• Watch and wait as a minimum!
Method Validation

Validation involves demonstrating that a method used for any form of analysis is fit for the specific purpose intended, i.e. the results can be relied on.

Validation is a demonstration of fitness for purpose. The first step is to define what the requirements are in terms of inputs, effects, constraints and desired outputs. Validations that skip this step may miss the key quality issues. Unfocused testing can lead to amassing of data that may or may not increase understanding or give confidence in the method.

Basically…

What Is the purpose of this process?
Method Validation

• What do you currently do?
• What is the method intended to do?
• Who is your end user? Who is the person/entity that utilises the results?
• Build a testing specification – how will you test that this process works?
• Perform a risk assessment – what if something goes wrong?
• Build some testing criteria (sample evidence) that is appropriate for the purpose.
• Consider
  • OS types
  • Artefacts
  • Location of artefacts
  • Make it ‘real life’
  • Needs to be suitably challenging
  • Needs to be within the scope of your work