Digital Forensics Capability Analysis

The ICT KTN, on behalf of the Forensic Science Special Interest Group (FSSIG), is conducting a survey of the UK's Digital Forensics Capability. This work is being managed by Angus Marshall, of n-gate ltd., to whom any initial queries should be directed. The project team also includes the CyberSecurity Centre at De Montfort University.

Background

Traditional Digital Forensics activities involve the recovery and investigation of material found in digital devices. Such data is at rest on static devices such as hard drives and in solid-state memory on camcorders, mobile phones, GPS navigation devices etc. The market for this activity was driven by Law Enforcement and other public sector organisations, hence it was necessary for all activities to be conducted in line with UK evidential criteria so that it was admissible in a court of law.

Our digital age has seen requirements evolve. With the ubiquitous use of email came a requirement for a new field of expertise – that known as "e-discovery". E-discovery refers to discovery in civil litigation, which deals with the exchange of information in electronic format (electronically stored information or ESI). This data is subject to local rules and processes and is often reviewed for privilege and relevance before being turned over to opposing counsel, where the burden of proof rests on the balance of probability.

However our digital evolution has not remained static. The growth of cyberspace, the trend towards mobile devices (BYOD) and cloud services has seen data take on a far more transitory nature, and the physical location of data at rest can be difficult if not impossible to determine. Data is versioned, distributed and stored across differing networks, devices, borders and boundaries.

The traditional digital forensics practice of imaging and extracting information from disparate physical devices no longer suffices for incident investigation in cyberspace. There is an increasing requirement from businesses in the private sector, and emerging capabilities are required to keep pace so that these requirements can be met.

The team will produce a report detailing the current stakeholders, existing capabilities and challenges. This will enable the identification of areas in which there are capability gaps. Attention will then be paid to how these gaps may be reduced and any specific challenges which will need to be overcome in order to do so. Further, a glossary of terms of key digital forensics concepts with simple definitions will be produced to assist with knowledge transfer both within and outside of the FoSci community.

Your involvement

You can assist with this first stage of the survey by completing the attached questionnaire and returning it to DFCA@n-gate.net no later than Monday, 4th March please. All responses will be treated in strictest confidence and your answers will be anonymised before they are included in the report(s).

Forensic Science Special Interest Group

For more information about the FSSIG, and to get involved in the community, please see https://connect.innovateuk.org/web/forensics

Digital Forensics Capability Analysis - Questionnaire

If you are willing to assist with this phase of the project, please complete and return to DFCA@n-gate.net by Monday 4th March 2013

1) What do you understand by the term "Digital Forensics". (one or two sentence answer)

2) In which context do you use digital forensics (e.g. law enforcement, civil law, criminal law, private sector, internal investigation, information security)

3) What types of technology do you deal with in the context of digital forensics ?

4a) What is the single greatest DF challenge you, personally, face in your everyday activities ?

4b) How do you think this challenge could be addressed ?

4c) What is the single greatest DF challenge that your organisation faces in its everyday activities ?

4d) How do you think this challenge could be addressed ?

5a) What challenges do you think you will face in the near (1-2 years) and medium-term (2-5 years) future ?

5b) How do you think these challenges could be addressed ?

6) When you are looking for solution to digital forensics problems, who do you turn to for

a) off-the shelf solutions ?

b) bespoke solutions/product customisation ?

7) Who would you consider to be the key people or organisations relevant to your experience and usage of digital forensics ?

8) What other innovations, relating to technology, services or any other issues affecting digital forensics, do you think would be beneficial ?

9) May we contact you again for more information ?

(If "Yes", please also provide your name and a contact phone number or email)