Abstract:

The increasing volume and variety of digital evidence encountered in a criminal investigation is both a help and a hindrance: whilst it is now more difficult for suspects to hide all traces of their crimes, it is also more difficult for investigators to keep track of the location and significance of potential evidential sources. Because of this, connections between disparate artefacts may not be made and so vital evidence is missed. The use of the Digital Evidence Semantic Ontology (DESO) is proposed to address this issue.

This talk will first use real-life examples from cases the speaker has investigated to illustrate the problem and explain why current tools and techniques are not addressing the issue. It will then describe DESO – which provides an index to a repository of known digital evidence artefacts which are classified according to the location that they are found and the information they represent.

DESO will then be demonstrated to show how it can be applied to criminal investigations to assist lines of enquiry.

About the Speaker:

Owen Brady was formerly a Detective Senior Inspector in the Hong Kong police but now works as a technical specialist in the UK's Financial Conduct Authority – the equivalent of Hong Kong's Security and Futures Commission. A large part of his job involves the investigation and presentation of digital evidence relating to insider dealing investigations. He is also a part-time PhD candidate in digital forensics at King's College London under the supervision of Dr Richard Overill.