Digital Forensics and related topics

The Cyber Security Centre at UH is interested at the issue of collecting and analysing forensic intelligence from the cyber domain (including virtualisation and IoT technologies) and how it can assist the digital forensic analyst in the extraction of evidence from digital artefacts.

Digital crime scenes nowadays can contain a number of technologies found in a range of devices from small embedded systems to games consoles and virtual computers that are interconnected over one or more networks. Where in the past, the culture of digital forensic analysis was based around wet forensic principles, nowadays it has been recognised that not only it is not feasible but also it is not appropriate. Instead, the new school of thought follows a smarter approach in the seizure of artefacts by ensuring that only the relevant items will be collected following a thorough and appropriate triage process. Apropos, this has magnified the need for forensic intelligence.

If we accept that intelligence is the timely, accurate and usable product of logically processed information then forensic intelligence is the timely, accurate and usable product of logically processing forensic case data.

When digital evidence are properly processed and recorded, they are a major intelligence source for crime investigators and digital forensic analysts. The majority of publications about digital forensic science cover best practices and basic advice about digital evidence recovery, analysis and storage. Forensic Intelligence as a research concept, will take the subject of digital forensics one step further and describe how to use the digital evidence recovered at digital crime scenes for extended analysis and the dissemination of new forensic intelligence.

We think that forensic intelligence should inform the analysis of forensic evidence as part of a digital forensic investigation. Therefore, we are looking for candidates to join our group in designing new methodologies and developing tools to allow for the development of the aforementioned capability.

The prospective candidates should have a strong background in Computer Science or another relevant discipline. In particular, they should demonstrate very strong programming skills in one or more major programming languages. Ideally, they should have some background in the areas of digital forensics, computer networks and security. Active Law Enforcement Officers are particularly welcome.

For informal inquiries please contact Professor Andy Jones (a.jones26@herts.ac.uk)