Artefact Capture of Digital and Online Content for Law Enforcement Purposes

Dr Joseph Williams (j.williams30@herts.ac.uk)

Internet Intelligence and Investigations (i3) are a fundamental investigative tool of the modern law enforcement official (LEO) in an always-connected online era. Ensuring LEOs follow good procedure for such investigations is critical for both law enforcement and society, as it ensures consistency, rigor, and transparency.

Procedural issues lie with online evidential capture, however. For example, it is not feasible to directly apply digital evidence methodologies one would for 'offline' digital forensics, such as ACPO/NPCC guidelines; instead, one must apply best practices and a consistent approach. How those best practices and consistent approaches apply will typically fall to individual police forces or even individual officers depending upon role.

These projects naturally fall under both the software engineering and cyber security discipline.

Continued development of OSIRT

OSIRT (Open Source Internet Research Tool) has been in development since 2016 and requires updates and enhancements for its users within law enforcement and other agencies. This research project will look to provide new functionality to OSIRT, as required by key stakeholders, as well as formally test functionality by means of usability testing and other software engineering metrics. OSIRT has a strong user base and links to the UK's College of Policing, enabling quality research participants to test and use OSIRT.

Creation of a new tool for the capture of online artefacts across digital platforms

Artefact capture is mainly conducted using a dedicated desktop/laptop computer. However, as social media platforms are diverging away from traditional browser-based platforms to bespoke apps on mobile devices, as seen with Snapchat/Telegram/TikTok et al., there is a growing need for law enforcement to be able to capture artefacts from these app-based platforms for evidential and other research purposes.

This project will conceive, design, and implement a new digital artefact capture tool.

A formal and methodological approach to online digital artefact capture

This research project aims to formalise the capture and retention of artefacts from an online environment. Presently, the approach to artefact collection and retainment of online material largely follows principles for 'static' digital forensics. This project will look to formalise that approach with a formal method.

Application and contact

We are looking for candidates with a background in Computer Science, ideally with good competency in programming and software engineering practices. Those with a Cyber Security background are also encouraged to apply if they have good programming skills. Professionals with no previous degree, but excellent industry experience, are also encouraged to get in touch.

Queries are encouraged and welcome to Dr Joseph Williams (j.williams30@herts.ac.uk).