Licensing Opportunity

Digital Forensics Triage Tool [Andvari]

Overview:

Andvari is a digital forensic triage tool that uses statistical techniques along with machine learning to improve the efficiency of identifying potential data of interest during digital forensic investigation.

A probabilistic framework "learns" which data is of interest to an investigator based on file metadata, for each case type undertaken (e.g. fraud, child exploitation etc.). The framework is initially populated via expert input with a feedback loop to refine the framework.

The tool has been implemented in MATLAB to work with Windows XP.

Key Benefits:

Once the framework has sufficiently "learnt" which data is of interest, it can be used to scan a device and present a priority-ordered list to either an expert investigator or a person with case knowledge. This allows the investigator to save a significant amount of time compared to a random search by focussing on the data which is most relevant to their case.

Applications:

Applicable to all fields of digital forensics in which metadata is to be analysed and prioritised. The framework is also potentially applicable to other data types, but the proof of concept has been applied to metadata.

IP Status:

Know-how – MATLAB code, concept documentation.

Commercial Opportunity:

Triage and digital forensics are a pervasive issue for large organisations. In particular law enforcement and the defence end users are driving significant growth in the digital forensics market.

For more information contact: dstleasyip@dstl.gov.uk

EasyAccessIP