School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Application instructions:
Detailed instructions are available at :
https://www.napier.ac.uk/research-and-innovation/doctoral-college/how-to-apply

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Dr Gordon Russell (Email: g.russell@napier.ac.uk)
- 2ND SUPERVISOR: Prof. Richard Macfarlane

Subject Group: Cyber Security and System Engineering

Research Areas: Cyber Security, Artificial Intelligence

Project Title: Forensic storage carving using AI

Project description:

In computer forensics, investigators need to be able to analyse storage devices. Storage devices tend to store information in blocks, and the arrangement of blocks in a certain order is the thing which represents a data object. However, if the information about each block is lost, then it can almost impossible to piece the blocks back together in order to reform all the data objects.

In storage drives, each block is arranged into file objects using the filesystem metadata. If this metadata is lost or deleted, recovery is challenging. Such recovery might be useful during a forensic examination of a drive where some of the data was deleted. Some work has been done in this area of forensics, but the processes are mechanical and the effectiveness limited to only certain cases.

Blocks themselves can be any sort of data, so categorising each block is a good first step. In a file system this could for instance be differentiating pdf blocks from jpeg blocks. Some algorithms exist already in this area, but these are largely algorithmic and lack high precision. Joining different blocks of the same time

together to form the original file or memory object would also be a useful step, and this is certainly an area with many opportunities to explore.

Many current approaches rely on the hope that a single data object will most likely be available in contiguous blocks. Such unfragmented sets of data blocks is relatively easy to extract. However many filesystems now utilise non-contiguous areas regularly, instead using tree-based version branching for files which leads to greater degrees of fragmentation and of block reuse between file versions. In addition, the continuous switch to solid-state storage devices can further confound the process, where such memory blocks are highly fragmented in the storage layer, and where blocks may be more easily recovered than the mapping tables in the storage manager.

This PhD proposes to examine block-based data found in a variety of storage systems, and develop systems to analyse data blocks and understand how such blocks relate to each other through the use of artificial intelligence. Such techniques could be neural networks or based on data mining approaches. In block-storage systems the resulting methodologies should allow whole files to be recreated without referencing the accompanying metadata.

References:

[1] https://www.forensicfocus.com/articles/a-survey-on-data-carving-in-digital-forensics/
[2] https://www.diva-portal.org/smash/get/diva2:1671149/FULLTEXT02.pdf

Candidate characteristics

Education:

A second class honour degree or equivalent qualification in Computing

Subject knowledge:

- Good knowledge of operating systems and storage devices.
- Strong motivation, with a keen interest in the area of proposed work.

Essential attributes:

- Good written and oral communication skills
- Good time management

Desirable attributes:

- Digital forensics, Artificial Intelligence, Neural Networks, Software Engineering, Python.