Department	School of Computing
Supervisors	Dr Gordon Russell, Richard Macfarlane
Project Title	Forensic storage carving using AI

PROJECT DESCRIPTION

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.

Perspective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisors.

Academic qualifications
A first degree (at least a 2.1) ideally in Computing with a good fundamental knowledge of Operating Systems.

English language requirement
IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

Essential attributes:

- Experience of fundamental Computing
- Competent in Operating Systems and Storage Devices
- Knowledge of Cybersecurity
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:
Digital Forensics, Artifial Intelligence, Neural Networks, Software Engineering, Python

Indicative Bibliography	https://www.forensicfocus.com/articles/a-survey-on-data-carving-in-digital-forensics/ https://www.diva-portal.org/smash/get/diva2:1671149/FULLTEXT02.pdf
Enquiries	For informal enquiries about this PhD project, please contact g.russell@napier.ac.uk
Web page	https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process