Call for CSC PhD Studentship – Computer Science, University of Exeter

TruGreen AI Lab: https://trugreen-ai-lab.github.io/TruGreen-AI-Lab/#/

Project: FILA: Digital Forensics with LLM Agents

Main Supervisors: Dr Yunxiao Zhang and Professor Lu Liu

The PhD student will also join the TurGreen AI Lab, with full support from all Principal Investigators.

Project Description: Digital forensics follows well-established procedural models (e.g., NIST standards, ACPO guidelines), requiring investigators to proceed through a series of steps, including evidence acquisition, establishing a premise, generating hypotheses, testing them against artefacts, and drawing defensible conclusions, followed by a recommendation. ***While current tools can extract and visualise artefacts well, they do not automate the reasoning workflow***. Investigators and cyber security analysts must still manually structure the investigation steps, evaluate competing hypotheses, and generate formal reports and briefings.
This project proposes the use of Large Language Model (LLM) agents as active forensic actors capable of executing standardised investigation workflows. The proposed system will formalise forensic reasoning by encoding investigative stages – artefact collection, premise, hypothesis generation, testing, conclusion, and reporting – into a structured agentic reasoning chain. LLM agents will be designed to integrate with established forensic tools (e.g., Wireshark, NetworkMiner, Zeek, etc.), orchestrating their use and selecting appropriate actions in response to investigative needs. These agents will also automate hypothesis testing, dynamically generating and refining investigative hypotheses from available evidence and evaluating them against relevant artefacts. To ensure trust and transparency, the system will maintain explainability through structured logs and intermediate reasoning traces that enable reproducibility and evidential reliability. Finally, outputs will be aligned with legal and professional standards, addressing admissibility requirements, chain-of-custody constraints, and the need for human investigator oversight.
In short, this research aims to demonstrate a **proof-of-concept forensic investigation agent** that can move from data to defensible conclusions, with human oversight, and provide a blueprint for AI adoption in digital forensic science.

Project Requirement: This project sits at the intersection of **artificial intelligence, cybersecurity, and digital forensics**. It will suit students with strong technical ability, curiosity about forensic investigation, and an interest in AI applications for high-stakes domains.

Essential skills/knowledge:

- Solid programming experience (e.g., Python, scripting, API integration).
- Demonstrated expertise in at least one of the following: **forensic science, cyber security, or artificial intelligence.**

- Strong analytical and problem-solving skills.

Desirable (but trainable during PhD):

- Experience with forensic toolkits (Volatility, Wireshark, NetworkMiner, Zeek, etc.).
- Knowledge of digital forensic workflows and evidential standards (e.g., ACPO, NIST).
- Knowledge of LLM agent frameworks (LangChain, LlamaIndex, AutoGen, etc.).
- Awareness of legal/ethical considerations in AI and forensic science.