Team Project in IT Security

Cryptocurrency forensics:
Tracing and identifying payments in public ledgers

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

What is this about?

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

- Public ledgers
  - Many cryptocurrencies have open and public ledgers („blockchain“)
  - Transactions and currency flows are visible to everyone

- Forensics
  - “Using the methods of science to provide information about a crime” (Cambridge Dictionary)
  - Make inference on the modus operandi of criminals based on public information
    - Darknet Markets, Ransomware, Extortion,…

What is this about?

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

- Previous team projects
  - Reverse engineered the payment systems of three darknet markets
  - Found a large number of Bitcoin addresses belonging to vendors on these markets
- Depending on the size of the team, your tasks will be
  - To follow the money obtained from criminal activities to known addresses
  - To reverse engineer payment systems of cryptocurrency exchanges
  - To check if cryptocurrency exchanges were used for money laundering
  - To undo the money laundering by performing cross-ledger payment tracing

What can you expect?

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

- You will have the chance to
  - Get an understanding of cryptocurrencies and their (privacy) problems that goes far beyond the usual buzzwords
  - Gain experience in the growing field of cryptocurrency forensics
- Support from the chair:
  - Access to previous work (earlier team projects, research of the chair)
  - Access to powerful server for analysis
    - 1 TB NVMe-SSD, 256 GB RAM, 16-Core AMD Epyc
  - Regular meetings and practical assistance throughout the project

What are the prerequisites?

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

- Skills:
  - Programming skills in Python
  - Basic Knowledge of SQL
  - An understanding of how Bitcoin-based cryptocurrencies work or the willingness to learn about it
  - Knowledge of Neo4j Graph Databases and Cypher QL or willingness to learn
  - Prior experience in working with graphs would be a plus
- MMDS students welcome
- Project capacity: 3-6 Students
- Project duration: 6 Months
- Online classes possible, students can decide

UNIVERSITÄT MANNHEIM
Fakultät für Wirtschaftsinformatik und Wirtschaftsmathematik

Questions?

jochen.schaefer@uni-mannheim.de

https://www.wim.uni-mannheim.de/ths/teaching/master-courses/team-project-fss-2022/