DIGITAL FORENSICS

CENTR SHORT COURSE - 3 WEEKS

PROGRAM OVERVIEW

As more criminal behavior is directed online, it is vital that cybersecurity professionals understand how to investigate a cyber incident in a manner that adheres to the proper rules of evidence and legal admissibility standards.

The identification, collection, and preservation of digital data and evidence are essential to the mitigation and prosecution of cybercrimes. This course will introduce learners to the fundamentals of digital forensics and cyber crime scene analysis, including relevant laws and regulations, international standards for forensic analysis, and methods for conducting forensic investigations.

STUDENTS WILL BE ABLE TO:

- Describe the fundamentals of digital forensics and cybercrime scene analysis
- Discuss the relevant laws and regulations
- Apply methods for conducting forensic investigations
- Evaluate the digital evidence process model and digital evidence life cycle

DELIVERY MODE

Live Virtual Sessions
Schedule: M & F 6:30 p.m. - 9:00 p.m. EST

COURSE SCHEDULE

Week 1:

- Context
- Criminalistics
- Laws
- Disk Structures

Week 2:

- Crime Scenes
- Bag & Tag
- Write Blockers/Acquisition
- Examination

Week 3:

- Chronologies
- User Profiles
- Report/Experts
- Challenges/Conclusions

FACULTY MEMBER

Dr. Marcus K. Rogers, CISSP, DFCP-F, FAAFS, Fellow of CERIAS, Professor and Executive Director of Cybersecurity Programs in the Computer & Information Technology Department, Purdue University. He is the Chief Scientist at the Purdue Tippecanoe High Tech Crime Unit (HTCU), and the Editor-in-Chief Journal of Digital Forensics Security & Law (JDFSL). Dr. Rogers also sits on the Board of Directors American Academy of Forensic Sciences (AAFS). Dr. Rogers is a former computer crime detective from Canada. His research and publications focuse on cybercrime, cyber criminal behavioral profiling and cybersecurity education.