

Advanced Digital Forensics; ERC Course E520

Course fee: \$795, includes software/all course materials; practitioners, corporate, law enforcement [Laid-off IT techs, senior year and grad computer science students; Course fee: \$595]

Class length; 4 days, class size limited to 26 participants; laptop computer required

Lead Instructor: Tony Robinson, CISM, NSA-IAM

Learning Outcomes

Designed specifically for digital forensic practitioners and those having computer science/engineering backgrounds who are considering entering or expanding their IT services in this growth field; course participants will come away from this concentrated program with new technology skills, a better understanding of client need, building trusted relationships, legal frameworks; many other tools to enhance and streamline your practice.

Training Modules Covered

Computer Forensics

- Overview – Past, Present, Future.
- Best practices, standards, and process
- Regulatory compliance - Gramm-Leach-Bliley, HIPPA, Sarbanes-Oxley, SEC, others
- Rules of evidence Documentation, chain of custody, and evidence handling procedures
- Prepare for Questions - advising your Client/Counsel
- Privacy issues; personal, home, public areas, workplace
- Working and testifying as an expert technical witness and Subject Matter Expert

Software and Tools

- Manual and automated data recovery
- Creating forensically sound working copies or images of media
- Capturing data from multiple electronic storage media
- Active, archival and latent data
- Hashes and Checksums
- Conducting keyword searches
- Creating understandable and accurate reports
- File (OS) systems and Header formats
- Allocated and unallocated space

Special Forensic Environments

- Vehicle ECU, MP3 players, Cell Phone, Compact Disc analysis, other electronic media
- PDA, PC, Server hardware issues
- Overview of SCADA, DOD, DHS Mission Critical issues

Interpretation

- Right Tool for the Right Engagement
- Interpretation of various log formats
- Interpreting Internet History, HTTP (web code) and Proxy issues
- File Signatures – who, what, when, where
- Overcoming encryption mechanisms and password protection
- Anti-Forensic tools and methods
- Viruses/malware

Business Matters

- Client issues [as the expert, educating your client], scope of work, billing rates
- Teaming Partners
- Insurance/liability considerations