INTERNATIONAL SECURITY INSTITUTE

MEDUNARODNI INSTITUT ZA BEZBEDNOST

Course name: Digital forensic investigator „DFI“

- Digitall forensics and digital evidence (digital forensics basic concepts, concept of digital evidence, working with digital evidence, types of forensic investigations)
- Digital forensic investigations process (four phases of forensic investigation: data acquisition, examination of collected data, analysis of collected data, Reporting – expert witness)
- Data acquisition (two approaches to data collection: live and clasic data acquisition)
- Volatile and other relevant forensic files (relevant files for forensic investigation on Windows, Linux and MacOS)
- Examination of collected data (three-phase investigation, software analysis, hardware analysis and network analysis)
- Forensic Tools (hardware and software tools, tools with GUI interfase and command line forensic tools)
- Reporting (results of forensic investigations through the expertise of cyber crime in court or through reports to management firms in the event of a corporate private investigation, judicial education)
- Windows forensics (NTFS and FAT file system, registry, volatile files, encrypted and compressed files, file and folder locations for a forensic investigation into the Windows environment)
- Linux/Unix forensics (EXT2, EXT3, RaiserFS file system, volatile files, encrypted and compressed files, file and folder locations for a forensic investigation into the Unix/Linux environment)

- Image forensics (techniques of image manipulation and automatic detection techniques, copy-move, patcmatch algorithm, SIFT algorithm)
- Digital forensics smart phones, tablets and PDA (forensic analysis of smart devices with Android or iOS operating system, Oxygene forensic and UFED, extraction of various data such as SMM and MMS messages, contacts, , email messages, GPS locations, picture and video files files, log files)
- Cloud forensics (concept of cloud, types of clouds, forensics data in the cloud, specific data collection from the cloud, problems in the collection of legal and technical, five effective techniques for gathering data from the cloud environment)
- Email forensics (techniques and tools for collecting and analyzing data related to the use of e-mail, find specific mails on different criteria, overview of the different tools for email investigations)
- Router forensics (specific area where forensics are not using the computer as evidence, but part of an active network equipment - router, overview of routing tables, router architecture, Internet work Operating System(IOS), types of router attacks)
- Investigating Logs (analysis of relevant log files for forensic investigation, locations of relevant log files, types of log files, tools for the analysis of log files)
- Investigating network traffic (special kind of active forensic investigation is performed during the attack because it monitors network traffic, OSI Model, sources of evidence on a network, tools: WinDump, Ethereal, NetIntersect, SNORT)
- Anti-forensic techniques (hide evidence that a crime had some computer crime, Traditional anti-forensics and Other Anti Forensics tehniques and tools, BackTrack, EvidenceEliminator, use of virtual machines as anti-forensic tools)

Course Duration: two working days (14 teaching hours)

Instructor: Igor Franc – Expert Information Systems Security and Digital Forensic

COURSE WHICH RECOMMENDS: experts in the field of ICT, researchers in the field of computer crime, system administrators for security, other persons with basic ICT skills.