RN Trust
The Digital Trust Company

INCIDENT RESPONSE (5 DAYS)

Incident response class will teach students how to gather digital forensic evidence and conduct forensic investigations of computer-related incidents. The Workshop is based on quick acquisition of most important evidence related to different types of situations, analysis of acquired evidence, reporting on findings and suggesting remediation techniques that can be implemented to harden the compromised system and possibly related network. Techniques that will be taught will be related to identifying important artefacts, how to create detailed and summarized reports and suggest remediation techniques to prevent futures vulnerabilities. Focus will be on the Windows operating systems and analysis of artefacts found within them.

Course Objectives:

By the end of this workshop, all the students will be able to:

- Search warrant planning and execution
- Notes taking and retention
- Identification of potential evidence
- Triage of evidence and encryption detection
- Recognize the incident
- Follow triage procedures on the crime scene
- Seizure evidence by respecting forensic rules
- "Bag & Tag" of the evidence
- Perform memory analysis at the crime scene
- Recognize important artefacts with memory analysis
- Create forensic report

Prerequisites:

To obtain the maximum benefits from this class, students should be comfortable and conversant with critical internal structures of the Windows family of operating systems and with file systems in general, specifically NTFS. Additionally, students are expected to have a strong command of baseline computer forensic principles and methodologies as well as having computer forensic examination experience with Windows based computers

Syllabus

DAY 1

Workshop starts with the legal aspects of the investigation, search warrants, things included in the search warrants. Workshop continues with the tool introduction, commercial and open source tools, their advantages and differences.

I. Search warrant planning and search execution
- Equipment considerations
- Examples of search warrants
- Legal considerations
- Note taking and retention
- Procedures at the scene

II. Introduction to tools
- FTK imager
- Open source tools
- Access Data triage
- F-response

DAY 2

On second day students learn how to recognize the incident, how to categorize it and what kind of investigation to start based on the incident. It is shown difference between live data present on the crime scene and the data in "Dead box". On real case scenarios trainers explain how to recognize encrypted files, what to do with them and what are the common protocols. Day 2 ends with triage procedures and variations that can some across based on the situation on the scene.

I. Recognizing the incident

II. Identifying potential evidence
- Live data
- Dead Box issues
- Recognizing cryptocurrency related evidences

III. Encryption detection

IV. Protocols

V. Triage procedures
- The system is "ON"
- The system is "OFF"
- Passwords
- Interviewing the suspect
- Documentation

DAY 3

Day 3 is dedicated to data collection and preservation, bag & tag the evidence and taking them to the laboratory.

I. Basic principles of data collection
- Selective collection
- Customized settings
- Scripts and automation
- Data preview

II. Evidence seizure
- Cell Phones, tablets and mobile devices
- Magnet Card Readers / Skimmers
- Drones
- Vehicle infotainment systems
- Navigations
- GPS Devices
- Wearable technology
- Smart home devices
- Home intelligent personal assistant
- Gaming consoles
- Location

III. Bag & Tag evidence

DAY 4

On day four students learn basics of memory analysis, specialties with the capture and analysis of the same. There is a practical assignment that shows how memory capture and analysis works in normal environment. At the end of the day students are introduced to the remote acquisition and data preview and virtualization.

I. Memory analysis
- Introduction to memory analysis
- Preparing the capturing device
- Free tools for capturing RAM
- Random Access Memory
- Other sources of memory
  - Pagefile.sys
  - Hiberfil.sys
  - Swapfile.sys
  - Memory.dmp
- Guidelines for capturing RAM
- RAM capture practical
- RAM analysis practical

IV. Remote acquisition
V. Data preview and virtualization

DAY 5

On the last day of the workshop, students get checklist for seizure of electronic evidence and learn how to correctly create and prepare report. The workshop ends with the final exam, survey and certification ceremony for the successful students.

I. Checklist for seizure of electronic evidence
II. Reporting
- Forensic artefacts important for the report
- Format of the reports

III. Recommendations for the future
IV. Final exam
V. Survey and certification ceremony