2.1 INFORMATION COMMUNICATION TECHNOLOGIES – COMPUTER FORENSICS

IoT Security Technician Skill Zone – CSSIA.ORG

2. Information Communication Technologies

2.1 Computer Forensics

1. Describe basic concepts and practices of processing digital forensics data.
2. Explain the use of data carving tools and techniques used in digital forensic analysis.
3. Describe the system files that contain relevant information and where to find those system files.
4. Describe the data acquisition from smart devices including SIM cards, registry, logs and memory.
5. Demonstrate the use of commands and tools to perform basic forensic analysis.

Computer Forensics

Computer Forensics is the process and practices of collecting and analyzing data. As an IoT security technician computer forensics may be used to investigate a security incident, attack or data breach. Computer Forensics requires the knowledge of many special tools, hardware and programs. Computer Forensics also requires an in depth knowledge of computer encoding and decoding, program structures, memory architectures and data structures. Computer Forensics can include searching for and identifying attack signatures and possession of unauthorized data.

Most IoT systems include locks, sensors, surveillance equipment and authentication systems. Computer Forensics will enable an IoT security technician to better manage and protect the security of their data devices and systems. There are two major applications of Computer Forensics. Network Forensics is the process of analyzing and capturing data during transmission. Digital Forensics is locating and analyzing data on storage devices and in system memory.

2.1 INFORMATION COMMUNICATION TECHNOLOGIES – COMPUTER FORENSICS

Existing Course Cross Reference

Cisco Networking Academy Courses

IT Essentials

Introduction to IoT

NDG Linux Essentials

Cisco Partner Courses

Digital Forensics (NDG)

Curriculum Resources

Textbooks

Internet of Things with Python
Chapter 1, 2, 3, 4, 5, 6, 7, 8, 9, 10
IoT: Building Arduino-Based Projects
1, 2, 3, 4, 5, 6, 7, 8, 9, 10
Practical Digital Forensics by R. Boddington
Publisher: Packt 2016 ISBN:978-1-78588-108-4,ISBN 10:1-78588-108-6
Digital Forensics with Open Source Tools By: Cory Altheide, Harlan Carvey
Publisher: Elsevier/Syngress, March 2011
ISBN:978-1-59749-587-5 | ISBN 10:1-59749-587-5
NIST Special Publication 800-86
Guide to Integrating Forensic Techniques into Incident Response
Computer Forensic Legal Standards and Equipment SANS Institute InfoSec Reading Room

Assessment Resources

Labs

Forensics Lab 01 - Introduction to File Systems
Forensics Lab 02 - Common Locations of Windows Artifacts
Forensics Lab 03 - Hashing Data Sets
Forensics Lab 04 - Drive Letter Assignments in Linux
Forensics Lab 05 - The Imaging Process
Forensics Lab 06 - Introduction to Single Purpose Forensic Tools
Forensics Lab 07 - Introduction to Autopsy Forensic Browser
Forensics Lab 08 - Introduction to PTK Forensics Basic Edition
Forensics Lab 09 - Analyzing a FAT Partition with Autopsy
Forensics Lab 10 - Analyzing a NTFS Partition with PTK
Forensics Lab 11 - Browser Artifact Analysis
Forensics Lab 12 - Communication Artifacts
Forensics Lab 13 - User Profiles and the Windows Registry
Forensics Lab 14 - Log Analysis
Forensics Lab 15 - Memory Analysis
Forensics Lab 16 - Forensic Case Capstone

Quizzes/Exams

CSSIA Digital Forensics – Chapter Exams

Quizlet.com

Computer Forensics

Digital Forensic Tools