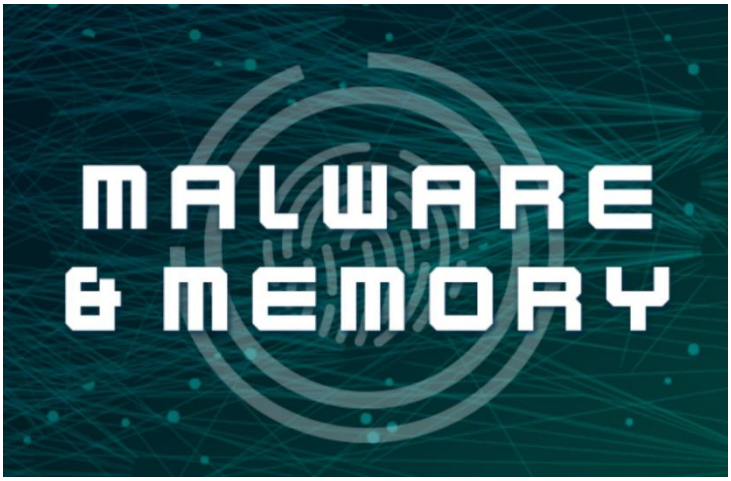

Course Outline

Types of Analysis

- Swap space analysis
- Memory Analysis
- Data acquisition as per RFC 3227

In-memory data

- Current processes
- Memory mapped files
- Caches
- Open Ports

Memory Architectural Issues

- Data structures
- Windows Objects
- Processes
- Handles
- Pool-tag scanning

Tools used

- Using volatility
- Dumpit.exe
- hibr2bin
- Win32dd
- Win64dd
- OSForensics

Registry in Memory