

Syllabus

- Day 1 – Memory Forensics with Trufflepig Nexus
 - What is memory forensics
 - Why memory forensics
 - speed
 - special artifacts
 - forensically sound working
 - History of memory forensics
 - acquisition
 - different methods
 - available tools
 - artifacts
 - memory only artifact
 - common artifacts
 - special artifacts
- Day 2 – Malware and Disk Forensics with Trufflepig Nexus
 - malware behavior & analysis
 - detection methods
 - persistence
 - evasion techniques
 - limitations
 - disk forensics
- Day 3 – Incident Response Workshop
 - Introduction
 - case work time
 - Review and wrap-up
- Day 4 – Fraud Analysis Workshop
 - introduction
 - case work time
 - Review and wrap-up
- Day 5 – Law Enforcement Workshop
 - Introduction
 - case work time
 - Review and wrap-up