The International Association of Computer Investigative Specialists

---

RAM Capture Analysis

Course Schedule

Day	
Monday	Lecture: ➢ Computer Setup ➢ Bypassing a lock screen ➢ Understanding the Kernel and Address translation Labs: ➢ Building tools to bypass a Windows lock screen ➢ Bypass a Windows 11 lock screen ➢ Capturing RAM on a locked Windows machine.
Tuesday	Lecture: ➢ Additional sources of RAM ➢ Linux and Macintosh ➢ Tools to capture RAM and the differences Labs: ➢ RAM capture with several commercial and open source programs ➢ Remote RAM Capture
Wednesday	Lecture: ➢ Tools to analyze RAM ➢ Understand what can be found in RAM Labs: ➢ Using command line to parse memory dumps
Thursday	Lecture: ➢ Advanced RAM analyzing ➢ Open source intelligence gathering for password creation ➢ Password cracking programs Labs: ➢ RAM analysis with Memproc-FS ➢ Password cracking files with john the ripper and hashcat (docx, pdf, xls, SAM, NTLM)
Friday	Lecture: ➢ Encryption- Bitlocker, Truecrypt/veracrypt Labs: ➢ Opening and examining a bitlocker OS drive using command line. ➢ Opening and examining a truecrypt file using command line