

WINDOWS FORENSICS

This course provides students with the knowledge and skills necessary to conduct an effective Windows based investigation. Attendees should already be conducting computer based investigations and be familiar with the AccessData suite of tools.

In addition to using advanced search and filtering techniques, students will use the Ultimate Toolkit (with the new Registry Viewer) to address the following Windows artifacts:

- o The Recycled / Recycler Bin --- (deleted files, place-holders and INFO2 databases)
- o File Meta Data and OLE Items --- (dates and times and file summary data)
- o Print Spools and Remnants --- (print jobs and temp files that remain behind)
- o Unallocated Data Carving --- (recovering files from unallocated and embedded space)
- o Windows Log & Link Files --- (other system device access / login records)

Registry File Data - Using the new Registry Viewer - specifically:

- o NTUSER.DAT / SYSTEM files --- (protected storage data / user info)
- o SAM / SOFTWARE / SECURITY / SYSTEM --- (machine time bias / USER-SID / login)

Students will also learn how to gain access to files that have been encrypted with the Microsoft Encrypted File System (EFS) component, parse thumbnail lists from Windows and other popular applications, and more.

This advanced level, hands-on intensive course is intended for Forensic Investigators, Law Enforcement Personnel and security and network administrators who desire a greater understanding of the Windows registry and other various operating system artifacts as they relate to computer forensic investigations.

The Windows Forensics course includes an optional Practical Skills Assessment (PSA) that requires participants to apply concepts presented during the course to complete a practical exercise. Participants who successfully complete this exercise receive a certificate of PSA completion.