FOR500

WINDOWS FORENSIC ANALYSIS

FOR500 builds in-depth digital forensics knowledge of Microsoft Windows workstations and servers. Learn how to recover, analyze, and authenticate forensic data, track individual user activity on your network, and organize findings for use in incident response, internal investigations, intellectual property theft inquiries, and civil or criminal litigation. New skills provide the means to validate security tools, enhance vulnerability assessments, identify insider threats, track hackers, and improve security policies.

The US Federal Bureau of Investigations recorded over 50 billion dollars of losses due to Business Email Compromise (BEC) targeting both small businesses and large corporations between October 2013 and December 2022.
Source: FBI PSA I-050422-PSA

Spring 2024 Update

The new update focused on testing and documenting significant changes across the Windows platform, including cloud storage, the Windows Search Index database, email forensics, and major shifts in browser-based artifacts. Hands-on labs were enhanced, taking advantage of the latest tools and techniques.

NEW CONTENT

- Email forensics improved to provide even more insight into the wealth of information present in email headers, including a focus on email authenticity using technologies like SPF, DKIM, ARC, and DMARC.
- New instruction on email collections with important discussions about host-based and server-based retrieval and the differences between vendor provided tools and API collection.
- Exchange mail, Microsoft 365, Microsoft Purview, Google Workspace, and Google Vault are all covered in depth.
- Microsoft OneDrive databases have changed significantly, requiring changes in analysis techniques while still offering massive insight into cloud storage contents.
- New databases and capabilities in Google Drive analysis include MD5 hashes of both local and cloud-only files and a list of removable devices previously present on the system.

UPDATED FEATURES

- Web Storage use by browsers and Electron-based apps has exploded, providing gigabytes of extra data per user. These new data sources are detailed along with techniques for taking advantage of the extra information largely ignored by mainstream forensic tools.
- Business Email Compromise investigative steps improved, including updates to logging provided by Microsoft and Google
- Universal Windows Platform Application artifacts expanded, including tracking installation and analysis of new registry hives, local storage, and Internet evidence recorded by these sandboxed applications.
- Windows Search Index database analysis supplemented with new Windows 11 changes. The index tracks up to a million items of 900 possible file types and includes detailed metadata and user activity artifacts.
- SQLite deleted item recovery and carving techniques improved.

LAB REFRESH

- Nearly every lab was enhanced along with many new updates to support new tool versions and capabilities.
- An expansive new email forensics lab was added with detailed analysis and authentication of email headers and metadata using an exciting new tool, Metaspike Forensic Email Intelligence
- Windows Search Index analysis was expanded to include new capabilities offered by the powerful new Search Index DB Reporter tool.
- Hands-on IndexedDB browser analysis added, including analysis of recoverable chat messages present in browser web storage and Electron-based LevelDB parsing.

GIAC Certified Forensic Examiner (GCFE)

The global forensic technology market is expected to expand at a "stunning" compound annual growth rate of 10.9%, generating almost 28 billion dollars per year by 2028.
Source: Vantage Market Research

For more information:
sans.org/FOR500

SANS | GIAC CERTIFICATIONS