

Advanced Internet Forensics

Using CacheBack

Advanced • Three-day Instructor-led Course



This advanced SiQuest training course provides the knowledge and skills necessary to use CacheBack to recover and analyze Internet artifacts from today's top leading browsers. Participants will learn how to decode cache entries and rebuild web pages using CacheBack.

During this three-day hands-on course, participants perform the following tasks:

- Use CacheBack to examine and analyze History and Cache artifacts from:
 - Microsoft Internet Explorer
 - Mozilla Firefox (Version 2 and 3)
 - Safari
 - Opera
 - Google Chrome
- Use CacheBack to parse the following particular Cache and History file types:
 - index.DAT files used by Internet Explorer (History, Temporary Internet Files)
 - history.dat (mork database format) for Firefox 2
 - _CACHE_MAP_, _CACHE_001_, _CACHE_002_ and _CACHE_003_ (Firefox 2/3)
 - index, data_0, data_1, data_2, and data_3 (Google Chrome)
- Use CacheBack to perform advanced analysis that includes:
 - Structure Query Language (SQL) syntax in creating and saving advanced custom queries.
 - Understanding Hypertext Markup Language (HTML) and the use and meaning of query parameters in URLs.
 - Identifying HTML elements that can be used as search (GREG) expressions for custom queries.
 - Validation of cache record entries using independent third party tools (eg: hex editors, online converters).
- Participants will be shown:
 - Decipher the cache mapping systems for Firefox and Google Chrome
 - How to create and manage custom queries using the new Query Builder
 - How to rebuild web pages and use advanced Link Analysis to zero-in on user activity
 - How to create compelling, rich HTML reports (Graphical and Tabular formats)
- **The above descriptions represent only some highlights of the course. Additional content includes the identification, decoding and rebuilding of Facebook chat and creating Chatters List Reports. It will also cover CacheBack's powerful Picture and Movie Analysis, storyboard reporting for Movies (by frame), and Bookmark / Exclude / Quarantine queries.**

Prerequisites

This hands-on course is intended for forensic investigators, law enforcement personnel, and security and network administrators who are, or are considering using CacheBack for their investigation of Internet cache and history data.

To obtain the maximum benefit from this course, you should meet the following requirements:

- Read and understand the English language.
- No previous experience of CacheBack required.
- Have previous experience in forensic investigations.

Course Materials and Software

You will receive the student training manual and CD containing lab exercises and course-related information.

DAY 1

Module 1: Introduction

Topics

- Introductions
- Course materials and software
- Prerequisites
- Course outline
- Helpful information
- CacheBack environments (installation, paths, libraries)

Lab

- Locate cache and history files using Windows Explorer.
- Check user rights, Internet connection status.
- Configure Internet Explorer script options.

Module 2: Internet Explorer Artifacts

Objectives

- Explore file locations for MSIE History (Master, Daily and Weekly histories), Cookies and Temporary Internet Files.
- Understand the differences between Daily and Weekly histories.
- Break down the INDEX.DAT file which is the main tracking file for both History and Temporary Internet Files:
 - Decode the HASH table to locate URL records and other linked HASH tables.
 - Decode timestamps (Last Visited, Server Modified).
 - Extract URL record metadata using Record offsets (cache filename, visit count, dates, web page title).
 - Decipher cached file locations within the Content.IE5 folder.

Lab

- Recover URL records from each type of INDEX.DAT file.

Module 3: Firefox Artifacts

Objectives

- Explore file locations for Firefox 2 and 3 history and cache.
- Decipher the Mork Database file format (history.dat).
- Introduction to the open-source SQLite3 database file format through the analysis of the "places.sqlite" history file.

- (_CACHE_001_, _CACHE_002_, _CACHE_003_). This mapping system is the 2nd most complex system among today's
- top browsers. Participants learn how to manually trace and validate Firefox artifacts.

Lab

- Recover URL records from Firefox cache and history.

Module 4: Opera Artifacts

Objectives

- Explore cache and history file locations for Opera 9x.
- Examine key files: "typed_history.xml", "global.dat" (history), "download.dat", and "cookies4.dat".
- Decipher the "dcache4.url" cache indexing file and map artifacts within the cache.

Lab

- Recover select artifacts from one or more files.

Module 5: Safari Artifacts

Objectives

- Explore cache and history file locations for Safari 3x.
- Examine key history files: "History.plist" and "Cookies.plist"
- Decipher the cache "Cache.db" file (SQLite format).
- Understand BLOB data and how to export to disk as specific file types.

Lab

- Recover select artifacts from one or more files.

Module 6: Google Chrome

Objectives

- Explore file locations for Google Chrome 1x.
- Continued look into to the open-source SQLite3 database file format through the analysis of the key history files: "History", "Archived History", "History Index YYYY-MM"
- Covert timestamps for history entries.
- Decode Chrome's cache map files (index, data_0, data_1, data_2 and data_3). This cache mapping system is by far the most complex system in use among the top browsers. Participants

- Convert timestamps for Firefox 3 history entries.
- Decode Firefox's cache map files (_CACHE_MAP_

will gain a previously unavailable insight into this complex architecture and understand how to manually trace and validate artifacts.

Lab

- Recover URL records from select cache and history files.

Module 7: Creating CacheBack Projects

Objectives

- Create a new project file and configure program options.
- Review the Graphical User Interface (GUI) - Explore the four (4) user panes: Features, Data, Properties and Viewer. This includes the different Table column headings and the new consolidated HTML + Picture "Gallery".
- Configure case options via the Options Window.
- Look inside the CacheBack Project File (.CBP) using Microsoft Access and understanding stored queries.
- Import cache and history files using CacheGrab, a standalone data mining tool that comes with CacheBack.
- Discuss the use of Base Path and "orphaned" record status.
- Introduction to the new PARD (Photograph Aspect Ratio Differential) feature to expedite the analysis of pictures using the Gallery.
- *Child exploitation related investigations*: Learn how to maximize the use of PARD and Bookmarks (to be able to categorize pictures only. Generate and publish rich, HTML thumbnail based reports for disclosure.

- *RE: Bookmarks (* see notice at bottom of syllabus)*

Lab

- Create a case.
- Examine evidence in the Table view.

DAY 2

Module 8: Examining Record Data

Objectives

- Explore Table column headings, data types, and sorting features. A special look into URL MD5 hashing.
- Understand checkboxes, row highlighting and context menu for record selection.
- Learn about “tagging” of records and DB persistence.
- Tailor / refine datasets using Quick Queries, Filters and customer query definitions via the Query Tab.
- Preview record data using multiple data Viewers: Browser, Text, Hex and Picture.
- Use the Gallery to navigate and view URL records.
- Learn how to use the Notes feature to create comments for select URL records.
- Explorer the various metadata from the new Properties Pane.

Module 9: Time Zones and UTC

Objectives

- Learn how to determine the time zone and daylight saving settings from a user’s Windows Registry.
- Understand how and why Windows stores Bias offsets.
- History and understanding of Universal Coordinated Time (UTC) and Time Zone offsets.
- Learn how Northern and Southern Hemispheres impact daylight saving calculations! (eg: United States vs. Australia).
- Understand how CacheBack uses time zone settings to display and report dates and times.
- Learn how to incorporate / format timestamps in custom queries.

Lab

- Case scenario (Use skills learned to examine data and create report).

Module 10: Rebuilding Web Pages

Objectives

- Gain a hands-on understanding to HTML (Hypertext Markup Language) tags, attributes, relative and fully qualified paths, and linked objects (eg: javascript files, cascading stylesheets).
- Learn to identify and edit Cascading Stylesheet contents.
- Use an IE cache web page as a case study. Understand what logical processes go on in behind the scenes.
- A close look at web page source code BEFORE and AFTER.
- A close look at the Temp folder contents and files critical to the rebuilding process.
- Review results using the Audit tab.
- Create Graphical, Tabular and Timechart reports. Explore features on the Report Window and embeddable options for reports.
- Learn to publish reports to a target folder. Know how to use the “autorun.inf” as an auto loader for removable media.

Lab

- Rebuild and publish select web pages.

DAY 3

Module 11: Creating Custom Queries

Objectives

- Review of available query options in CacheBack.
- Learn how to use the Query Builder and SQL Query Builder to create simple to complex queries.
- Examine SQL syntax and optimizing conditional statements using precedent / grouping characters.
- Understand stored procedures (queries) and how they are managed by CacheBack's Quick Queries option. Taking a look behind the scenes using Microsoft Access.
- Learn how to validate queries using the Microsoft Access built-in Query Builder tool.

Lab

- Create a simple query to target specific evidence.

Module 12: Advanced Queries & Reporting

Objectives

- Learn to create complex queries using multiple search parameters.
- Learn how to use wildcards to create loose search expressions.
- Understand the ORDER BY keyword statement to sort query results.
- Create "queries that use queries" to define sophisticated and succinct datasets.
- Know how to use Microsoft Access to validate or explore CacheBack Project Files and how to create custom reports and graphs (eg: pie charts).

Module 13: Creating and Managing Templates

** See notice at bottom of syllabus*

Objectives

- Learn how CacheBack can rebuild web pages from Unallocated Clusters using a new feature called "Templates". This capability has never before been considered until now and is a feature unique to only CacheBack.
- Discuss forensic integrity issues about using Templates and the "second best" evidence rule in court.
- Learn how to create custom Templates using CacheBack.
- Learn how to recover web pages from Unallocated Clusters and then rebuild them using selected Templates from the CacheBack Template Library.

Learn how to manage the Template library.

- Know how to distribute and share Template libraries.

Lab

- Recover and rebuild web pages from Unallocated Clusters.

Module 14: Link Analysis

Objectives

- Introduce "Link Analysis" as a way of identifying and exposing relationships between History URLs and hyperlinks embedded in web pages.
- Understand the prerequisites to running Link Analysis.
- Run Link Analysis and explore results in the Table "Links" column.
- Use the Links viewer to navigate between related records.

PRACTICAL SKILLS ASSESSMENT

- The Advanced Internet Browser Forensics *Using CacheBack* course includes an optional Practical Skills Assessment (PSA). This performance based assessment requirements participants to apply key concepts presented during the course to complete a practical exercise. Participants who successfully complete the exercise receive a PSA certificate of completion.

*** NOTE:** *These features are not presently inherent in the software, and are planned for a future release of CacheBack.*