

Falcon 280:

Investigating with Falcon Forensics

Course Overview:

Enhance your investigative capabilities with CrowdStrike Falcon® Forensics, a powerful tool for collecting and analyzing on-disk artifacts during host-based investigations. This specialized course equips incident response analysts and threat hunters with the skills needed to effectively navigate Falcon Forensics' comprehensive dashboards and utilize its advanced data collection capabilities.

Through practical exercises and real-world scenarios, participants will develop proficiency in analyzing forensic data, utilizing CrowdStrike Query Language (CQL) syntax, and conducting thorough host-based investigations. The course emphasizes efficient use of key features — including the Windows hunting leads, Host timeline, and Host info dashboards — to effectively collect and correlate forensic artifacts.

What You Will Learn:

In this course, you will learn how to:

- » Identify information collected and artifacts created when running Falcon Forensics
- » Navigate and utilize Falcon Forensics dashboards effectively
- » Analyze the Windows hunting leads dashboard for potential threats
- » Conduct timeline analysis using the Host timeline dashboard
- » Execute focused investigations using the Host info dashboard
- » Perform custom investigations using CQL queries

1-day program | 2 credits

This instructor-led course includes various walkthroughs, hands-on learner exercises, and a multi-hour capstone project

Take this class if you are:
A security analyst or threat hunter

Registration:

For a list of scheduled courses and registration access, please log in to your CrowdStrike University account. This course requires two (2) training credits. If you do not have access to CrowdStrike University, need to purchase training credits, or need more information, please contact sales@crowdstrike.com.

Recommended Prerequisites

- » Completion of FALCON 180: Falcon Forensics Fundamentals
- » Completion of CQL 101: CrowdStrike Query Language Fundamentals 1, CQL 102: CrowdStrike Query Language Fundamentals 2, and FALCON 202: Investigating and Querying Event Data with Falcon EDR (or FALCON 202a)
- » Intermediate knowledge of cybersecurity incident investigation and the incident lifecycle
- » Working knowledge of Windows forensic artifacts, including amcache/shimcache/prefetch, registry, event logs, scheduled tasks/jobs, users/groups, etc.
- » Ability to perform basic operations on a personal computer
- » Familiarity with the Microsoft Windows environment
- » Ability to comprehend course curriculum presented in English

Requirements

- » Broadband internet connection, web browser, microphone and speakers
- » Dual monitors and headset are recommended

Class Material

Associated materials may be accessed from CrowdStrike University on the day of class.

Topics

Introduction to Falcon Forensics

- » Use Falcon Forensics to conduct forensic investigations
- » Describe how Falcon Forensics works
- » Recall information that Falcon Forensics collects
- » List the artifacts created when running Falcon Forensics

Investigate with Dashboards

- » Navigate the Falcon Forensics dashboards
- » Use the Windows hunting leads dashboard to identify interesting items
- » Pivot to an Advanced event search query from a dashboard panel
- » Export data from a panel
- » Use the Host timeline dashboard to view a specific timeline and host
- » Use the Host info dashboard to investigate interesting information

Investigate with CQL Searches

- » Explain what CQL is and how to use it
- » Investigate using CQL queries
- » Use CQL macros in an investigation
- » Use Advanced event search commands

Custom Dashboards

- » Explain what custom dashboards are and how to use them
- » Use CQL to build custom dashboards
- » Generate a PDF report from a custom dashboard
- » Export custom dashboards as a template



