CrowdStrike University

FHT 280
INVESTIGATING WITH FALCON FORENSICS

COURSE OVERVIEW

This course is for any analyst or threat hunter who will utilize CrowdStrike Falcon® Forensics to collect on-disk artifacts to perform host-based investigations. The course utilizes Falcon Forensics to perform basic investigations using various dashboards. Course participants will learn about the forensic data collected, basic Splunk syntax and searches related to investigations.

WHAT YOU WILL LEARN

- Identify the information collected and artifacts created when running Falcon Forensics
- Navigate the Falcon Forensics dashboards
- Recall the Event Data Dictionary and sourcetypes
- Identify interesting items in the Windows Hunting Leads dashboard
- Use the Host Timeline dashboard to effectively narrow in on a specific timeline and host
- Investigate interesting information in the Host Info dashboard
- Investigate using Splunk queries

PREREQUISITES

- Completion of FHT 180: Falcon Forensics Fundamentals
- 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.

1-day program | 2 credits

This instructor-led course utilizes Falcon Forensics to perform basic investigations and allows learners to conduct investigations through hands-on labs by performing searches.

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.

CrowdStrike University

FHT 280 Investigating with Falcon Forensics

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 a Splunk query from a dashboard panel
- Export data from a panel
- Use the Host Timeline dashboard to view a specific timeline and host
- Use a Host Info dashboard to investigate interesting information

INVESTIGATE WITH SPLUNK SEARCHES

- Explain what Splunk is and how to use it
- Investigate using Splunk queries
- Use Splunk macros in an investigation
- Use advanced Splunk search commands