Working with Time

This three-hour course is for power users who want to become experts at using time in searches. Topics will focus on searching and formatting time in addition to using time commands and working with time zones.

Course Topics

▪ Searching with Time
▪ Formatting Time
▪ Comparing Index Time versus Search Time
▪ Using Time Commands
▪ Working with Time Zones

Prerequisite Knowledge
To be successful, students should have a solid understanding of the following:
▪ How Splunk works
▪ Creating search queries
▪ The eval command

Course Format
Instructor-led or eLearning

Course Objectives

Topic 1 – Searching with Time
▪ Understand the _time field and timestamps
▪ View and interact with the Event Timeline
▪ Use the earliest and latest time modifiers
▪ Use the bin command with the _time field

Topic 2 – Formatting Time
▪ Use various date and time eval functions to format time

Topic 3 – Using Time Commands
▪ Use the timechart command
▪ Use the timewrap command

Topic 3 – Working with Time Zones
▪ Understand how time and timezones are represented in your data
▪ Determine the time zone of your server
▪ Use strftime to correct timezones in results

About Splunk Education
Splunk classes are designed for specific roles such as Splunk Administrator, Developer, User, Knowledge Manager, or Architect.

Certification Tracks
Our certification tracks provide comprehensive education for Splunk customer and partner personnel according to their areas of responsibility.

To view all Splunk Education’s course offerings, or to register for a course, go to http://www.splunk.com/education
To contact us, email Education_AMER@splunk.com

Splunk, Inc.
270 Brannan St. San Francisco, CA 94107
+1 866.GET.SPLUNK (1 866.438.7758)
Contact sales