Overview of event processing
Overview of event processing

Events are records of activity that reside in log files and machine data. They are primarily what Splunk software indexes. Events provide information about the systems that produce the machine data. The term **event data** refers to the contents of a Splunk index.

Here is a sample event:

172.26.34.223 - - [01/Jul/2017:12:05:27 -0700] "GET /trade/app?action=logout HTTP/1.1" 200 2953

When Splunk software indexes events, it:

- Configures character set encoding.
- Configures linebreaking for multi-line events.
- Identifies event timestamps (and applies timestamps to events if they do not exist).
- Extracts a set of useful standard fields such as `host`, `source`, and `sourcetype`.
- Segments events.
- Dynamically assigns metadata to events, if specified.
- Anonymizes data, if specified.

For an overview of the indexing process, see the Indexing overview chapter of the Managing Indexers and Clusters manual.