Dealing with Time >

Timestamp

(n) A default field that represents time information in an event. Most events contain timestamps. In cases where an event does not contain timestamp information, Splunk Enterprise attempts to assign a timestamp value to the event at index time.

From the Splexicon

http://docs.splunk.com/Splexicon

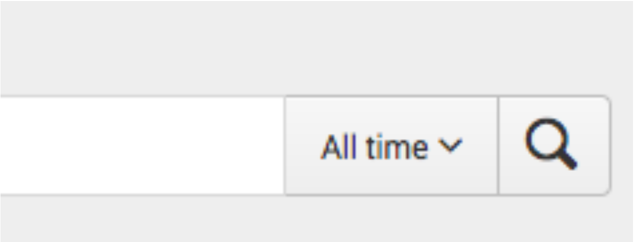
Dealing with Time >

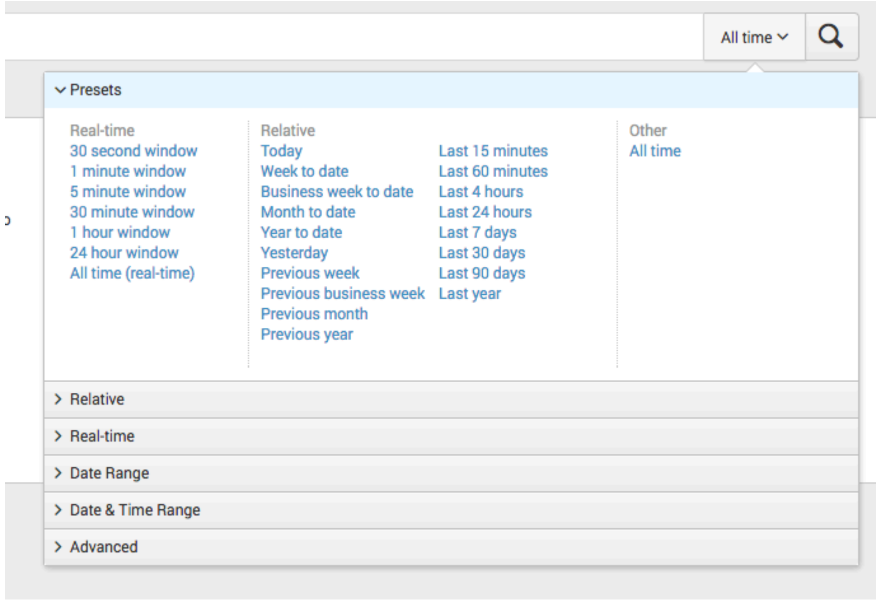
The `_time` field

- A Splunk-generated default field that represents time.
- Timestamps are usually added automatically based on the event raw data.
- If time and date information are not included in the event raw data, Splunk attempts to "guess" at a timestamp.
- As a last resort, Splunk will set the timestamp to the system time.

Dealing with Time >

Splunk uses the timestamp information for the time selector in the search bar.





Dealing with Time >

Time Conversion

- Time can be converted from Splunk’s default to a format of your choice using the `strftime()` eval function

```
| eval time=strftime(_time, “%H:%M”)
```

06:34

Dealing with Time >

Time Conversion

Time variable	Description
%H	Hour (24 hour clock)
%I	Hour (12 hour clock)
%M	Minute
%S	Second
%p	AM or PM

Dealing with Time >

Date Conversion

Time variable	Description
%A	Full day name
%d	Day of the month (01 – 31)
%e	Day of the month without leading zero (1 – 31)
%B	Full month name (January)
%b	Abbreviated month name (Jan)
%m	Month as a number (01 – 12)
%Y	Four digit year (2017)
%y	Two digit year (17)

Dealing with Time >

Time Conversion for 1:07:32 p.m.

String	Timestamp
%I:%M %p	[redacted]
%H:%M	[redacted]
%H:%M:S	[redacted]
%S	[redacted]
%p	[redacted]

Dealing with Time >

Time Conversion for January 20, 2017 1:07:32 p.m.

String	Timestamp
%d %B %Y %I:%M %p	[redacted]
%H:%M %b %y	[redacted]
%y%Y%y%Y	[redacted]

Demo: Time

Dealing with Time >

Review

- _time is a Splunk-generated default field that represents time.
- Timestamps are usually added automatically based on the event raw data.
- Time data is used for the time picket in the web GUI.
- You can force your own time format using variables that begin with %.

Thanks, Splunkers!