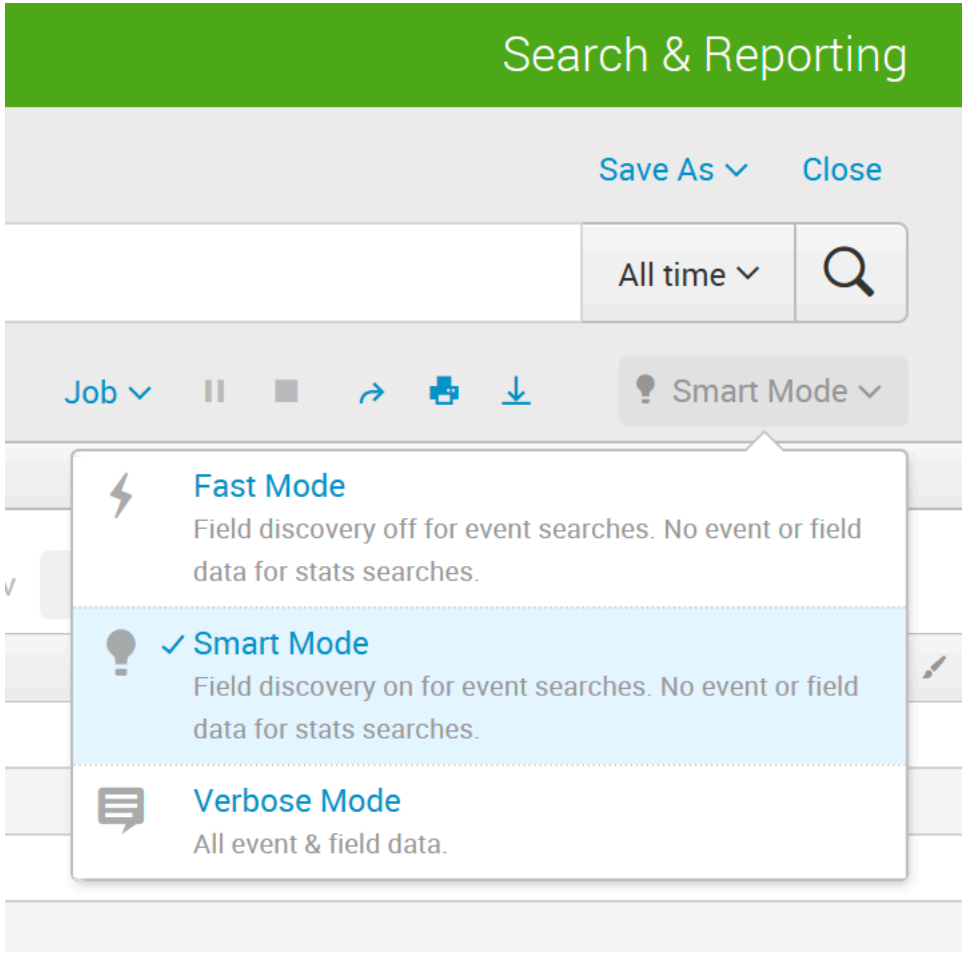
Search Modes, Fields, Discovery >

The Search App has three modes

1. Fast
2. Smart
3. Verbose



Search Modes, Fields, Discovery >

1. Fast
   - No field discovery, except the default metadata fields
   - Use if you know exactly which fields you need and can specify them in the search string
2. Smart
   - Returns the best results for whatever search you are running
3. Verbose
   - Discovers all fields it can
   - Use if you are not sure what fields you will want to report on

Search Modes, Fields, Discovery >

Field Discovery

- During field discovery, Splunk detects `key=value` pairs
  - `error=failed`
  - `level=critical`
- The first 50 `key=value` pairs are displayed on the field browser on the left

Search Modes, Fields, Discovery >

Field Extraction

- What if fields are not in nice, neat `key=value` pairs?

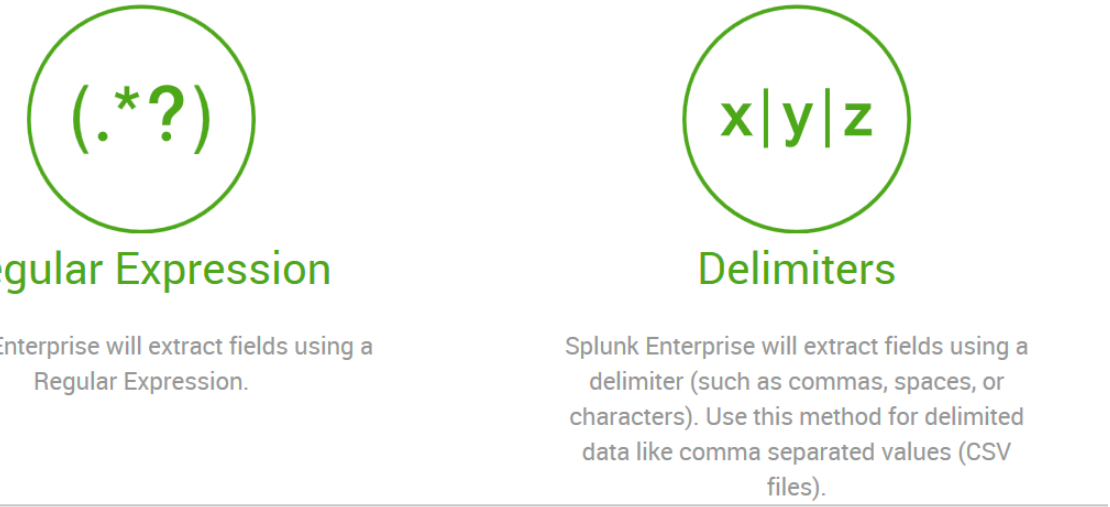
```
165.49.77.181   2017-03-18T13:14:26Z    video/quicktime 90cf0e570bb330f9ba0010ac54764ad9d75ae0b6f86280d965ee70dc4a7d6876
217.93.55.126   2016-06-24T10:14:53Z    video/quicktime da9991be2a85f56aae092951741ed5b0963a9cdd33f0dc36169c858770c9a444
3.228.18.131    2017-01-03T15:07:46Z    image/jpeg  f28782e6fda6a86cc33edd9999c285f4500a3afb72c01d4d3edb424f241017eb
51.241.86.255   2016-12-03T21:29:38Z    video/mpeg  9eaf3b8dc51c9f98d6c8a9050c5a98d41e1038e1c61e3c08191e8dbbf1a83d1f
154.168.245.39  2016-06-21T15:21:01Z    video/mpeg  1a1185c4e1dfa5fcffb32fd77575936f126466e35c0b0ae85915eae50537d132
35.110.86.98    2017-03-11T11:48:45Z    video/msvideo   5e6e1896e3c8f8f3593985b2c3054907dcfbf4cd573bd53806cf5905fe97e3a2
124.0.75.53 2016-07-30T17:01:06Z    application/excel   fa10511a83d17eac32594a3ba96c6b04ee7b5c391c35ec3d8045bafb99cab4f7
206.147.22.191  2016-05-11T22:55:24Z    video/x-msvideo 8340a7c3197f79c6f87a4d7b24fa464b54079b62e183b1f0552de50ba0ee0559
218.192.10.160  2016-06-15T21:09:41Z    application/powerpoint  b586bc9cfc0ec2a5936d4d60a31964f09dcdb6d24772c623a40d33f5a9f18773
```

- You can extract your own fields using the field extraction tools!

Search Modes, Fields, Discovery >

Field Extraction

- Field extraction works by using regular expressions.
- Splunk comes with built-in tools to help you



Demo: Search Modes, Fields, and Field Extraction

Thanks, Splunkers!