.conf2015

Understanding and Using Fields

Jesse Miller

Product Manager, Splunk

Clara Lee

Software Engineer, Splunk

splunk>

Disclaimer

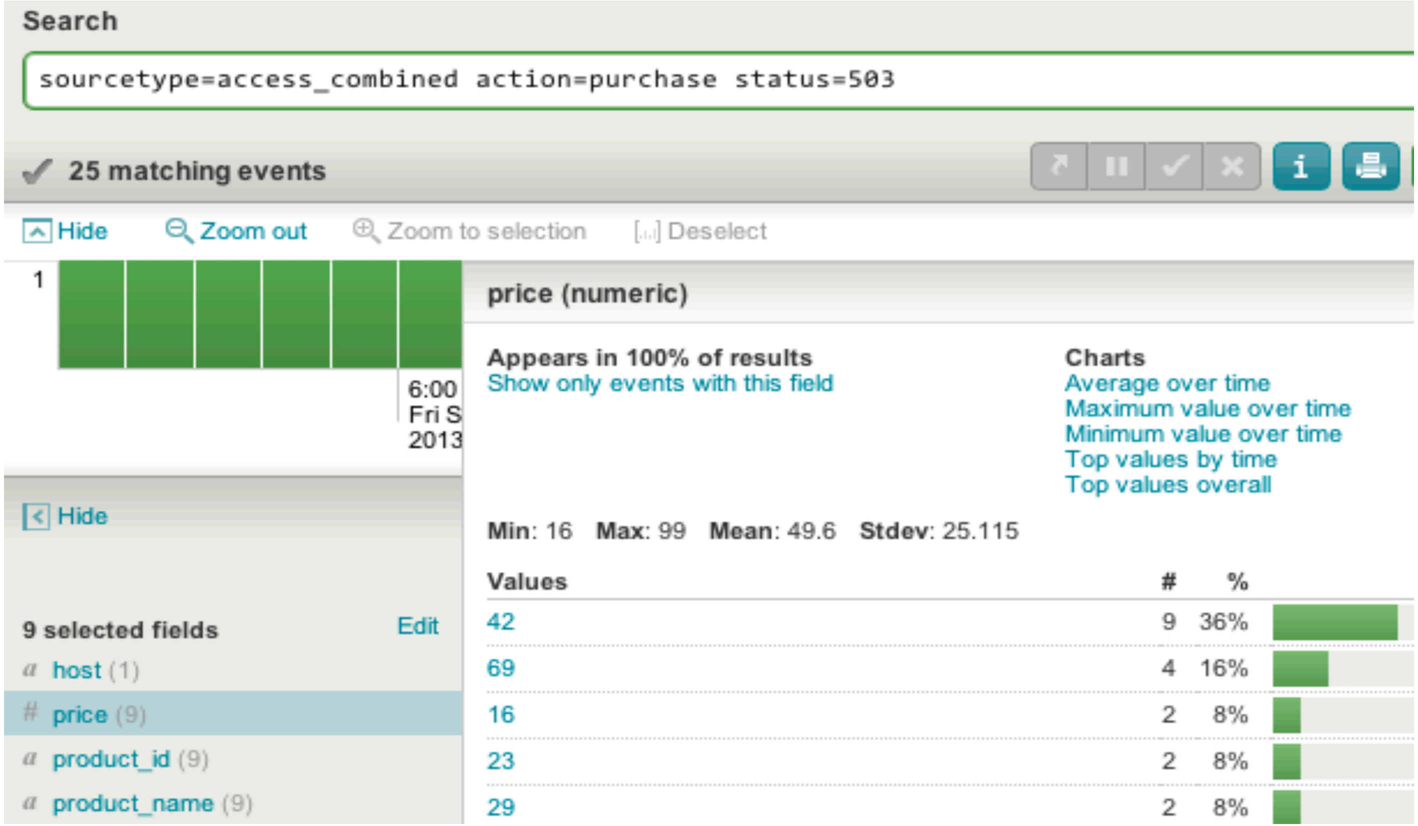
During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Agenda

- Why you should use fields
- What are fields?
- Field maturity
- Field extractor **DEMO**
- Multivalued fields **DEMO**
- More fun with fields
- Q&A

Why You Should Use Fields



Search

```
sourcetype=access_combined action=purchase status=503
```

25 matching events

price (numeric)

Appears in 100% of results
Show only events with this field

Charts
Average over time
Maximum value over time
Minimum value over time
Top values by time
Top values overall

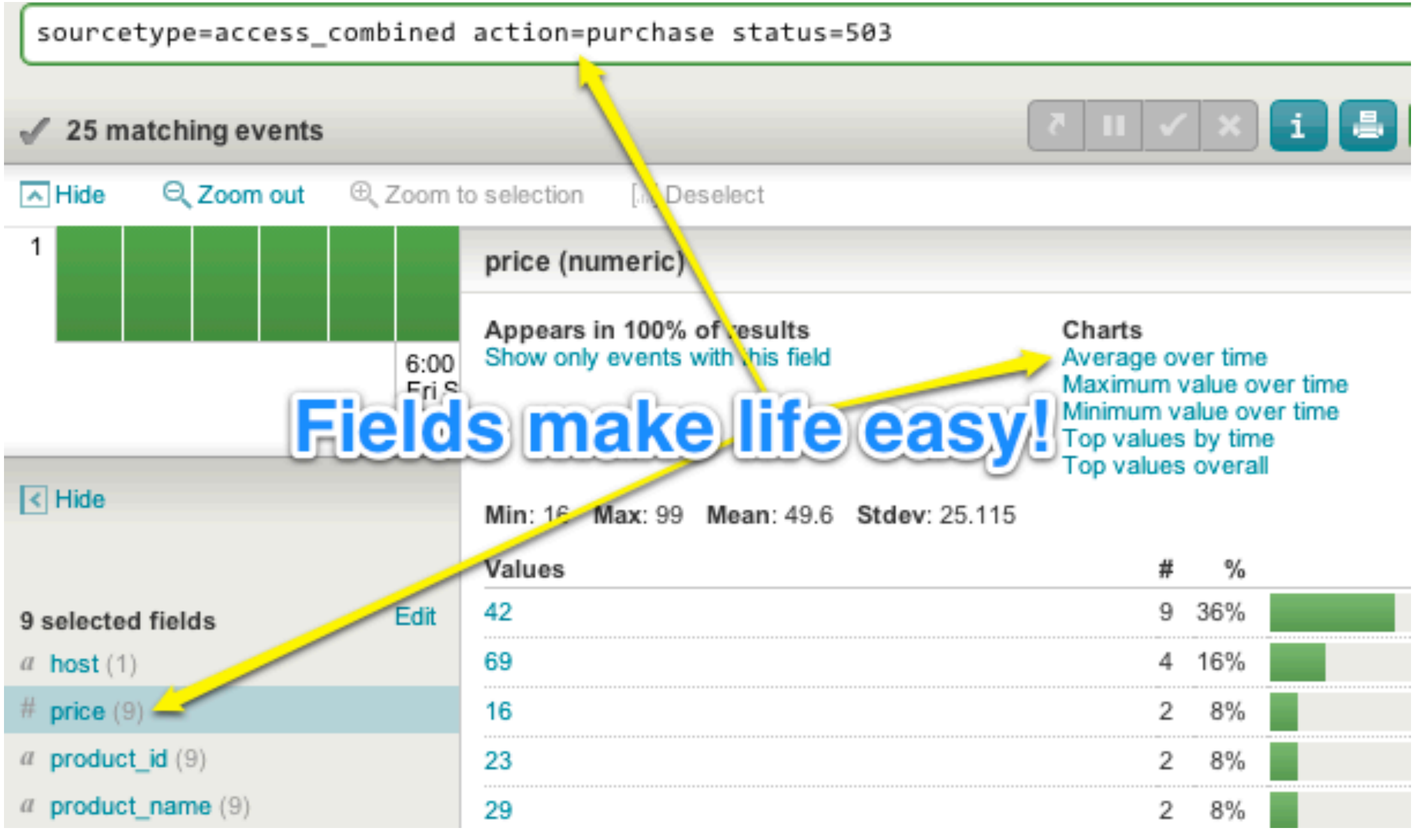
Min: 16 **Max**: 99 **Mean**: 49.6 **Stdev**: 25.115

Values	#	%
42	9	36%
69	4	16%
16	2	8%
23	2	8%
29	2	8%

9 selected fields Edit

- a host (1)
- # price (9)
- a product_id (9)
- a product_name (9)

Why You Should Use Fields



```
sourcetype=access_combined action=purchase status=503
```

25 matching events

Fields make life easy!

price (numeric)

Appears in 100% of results
Show only events with this field

Charts
- Average over time
- Maximum value over time
- Minimum value over time
- Top values by time
- Top values overall

Min: 16 **Max:** 99 **Mean:** 49.6 **Stdev:** 25.115

Values	#	%
42	9	36%
69	4	16%
16	2	8%
23	2	8%
29	2	8%

9 selected fields

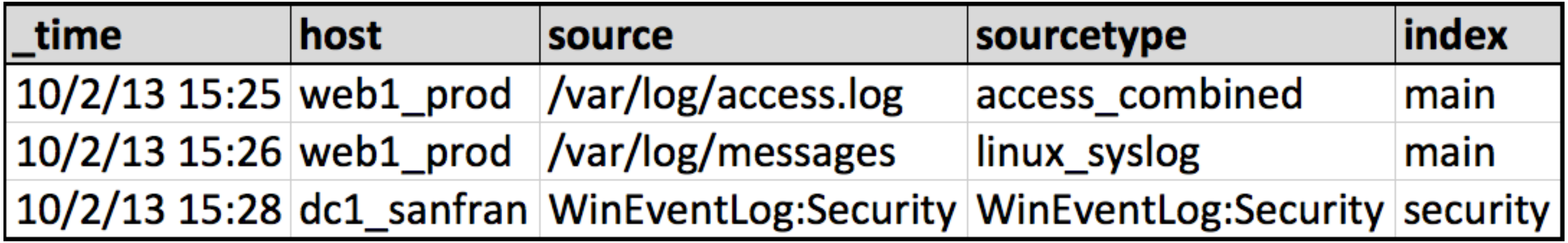
- a host (1)
- # price (9)
- a product_id (9)
- a product_name (9)

What Are Fields?

- **Searchable name/value pairings in event data**
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)

What Are Fields?

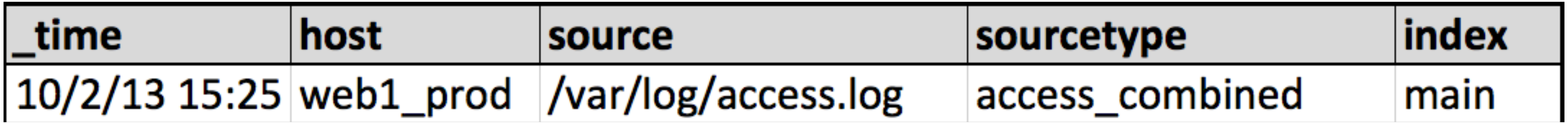
- Searchable name/value pairings in event data
  - **Index-time** fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)



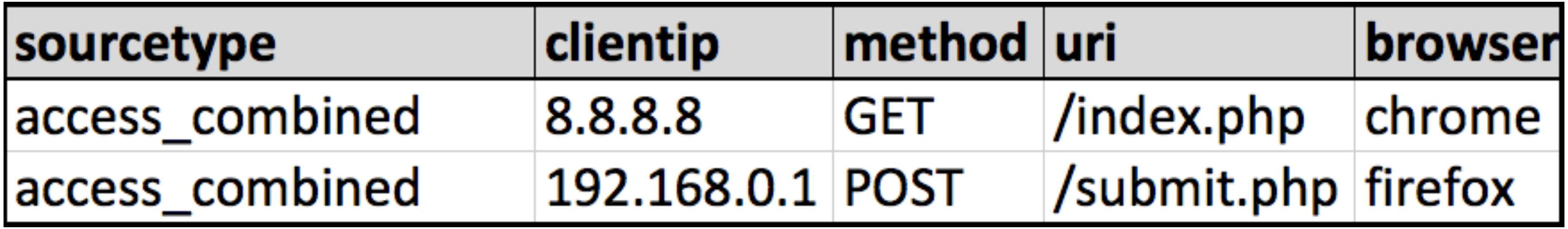
_time	host	source	sourcetype	index
10/2/13 15:25	web1_prod	/var/log/access.log	access_combined	main
10/2/13 15:26	web1_prod	/var/log/messages	linux_syslog	main
10/2/13 15:28	dc1_sanfran	WinEventLog:Security	WinEventLog:Security	security

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - **Search-time** fields (everything else!)



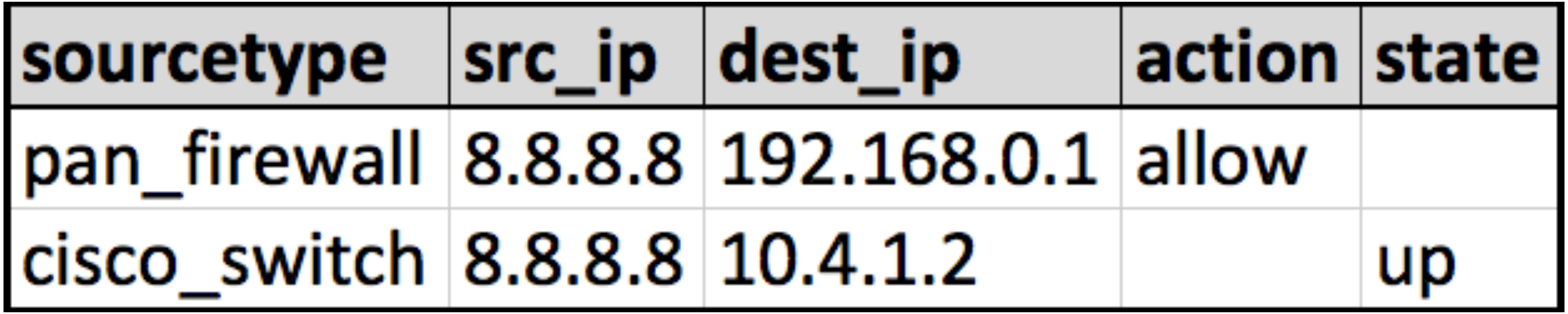
_time	host	source	sourcetype	index
10/2/13 15:25	web1_prod	/var/log/access.log	access_combined	main



sourcetype	clientip	method	uri	browser
access_combined	8.8.8.8	GET	/index.php	chrome
access_combined	192.168.0.1	POST	/submit.php	firefox

What Are Fields?

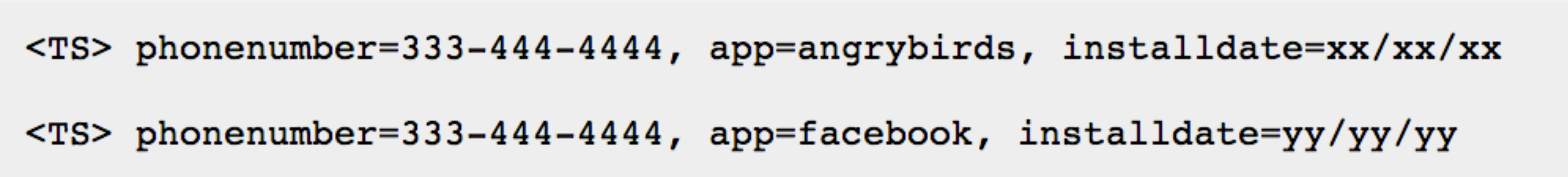
- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)



sourcetype	src_ip	dest_ip	action	state
pan_firewall	8.8.8.8	192.168.0.1	allow	
cisco_switch	8.8.8.8	10.4.1.2		up

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - **Automatic extraction** (props/transforms, **key=value**)

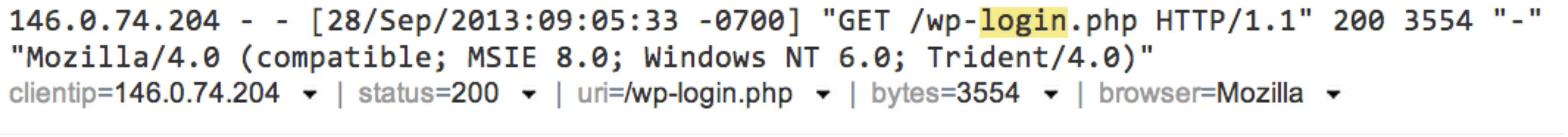


```
<TS> phonenumber=333-444-4444, app=angrybirds, installdate=xx/xx/xx

<TS> phonenumber=333-444-4444, app=facebook, installdate=yy/yy/yy
```

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)



```
146.0.74.204 - - [28/Sep/2013:09:05:33 -0700] "GET /wp-login.php HTTP/1.1" 200 3554 "-"
"Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0)"
```

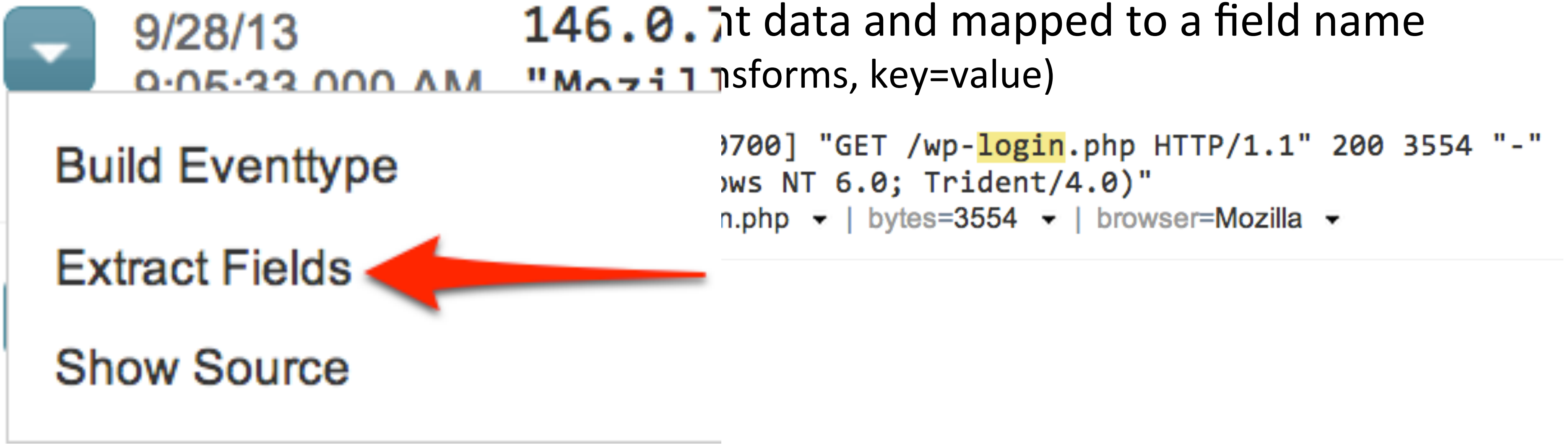
clientip=146.0.74.204 ▾ | status=200 ▾ | uri=/wp-login.php ▾ | bytes=3554 ▾ | browser=Mozilla ▾

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)

nt data and mapped to a field name

nsforms, key=value)



9/28/13
9:05:33.000 AM

```
146.0.7
"Mozill
)700] "GET /wp-login.php HTTP/1.1" 200 3554 "-"
)ws NT 6.0; Trident/4.0)"
```

n.php | bytes=3554 | browser=Mozilla

What Are Fields?

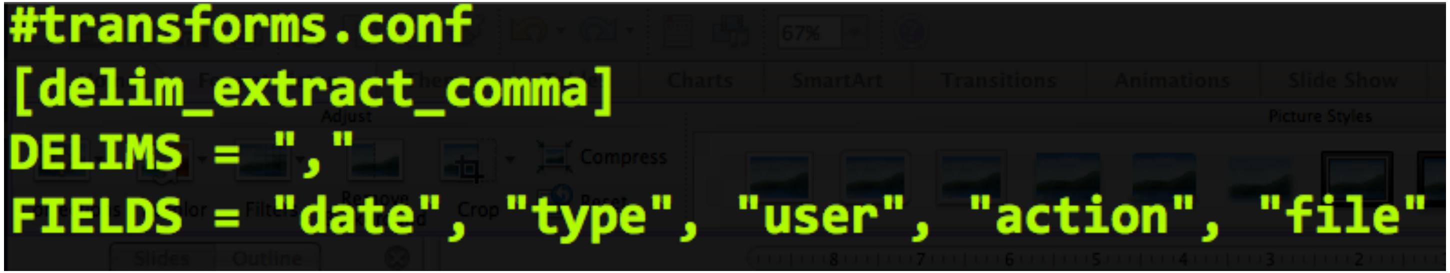
- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)

2013/10/03,audit,jesse,write,/etc/rc.local

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - **Automatic extraction** (**props/transforms**, key=value)

2013/10/03,audit,jesse,write,/etc/rc.local



```
#transforms.conf
[delim_extract_comma]
DELIMS = ","
FIELDS = "date", "type", "user", "action", "file"
```

What Are Fields?

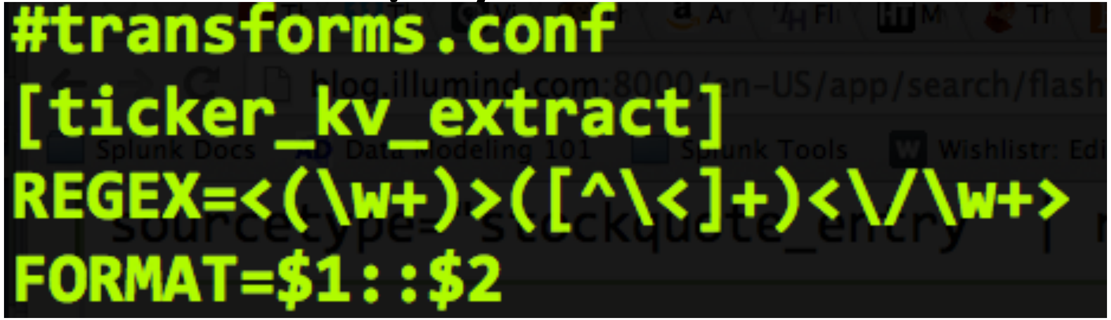
- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)

```
<Symbol>SPLK</Symbol><Last>62.02</Last>
<Change>+0.05</Change><Open>61.80</Open>
<Low>61.09</Low><Volume>450618</Volume>
```

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - **Automatic extraction** (**props/transforms**, key=value)

<Symbol>SPLK</Symbol><Last>62.02</Last>



```
#transforms.conf
[ticker_kv_extract]
REGEX=<(\w+)>([^\<]+)<\/\w+>
FORMAT=$1::$2
```

What Are Fields?

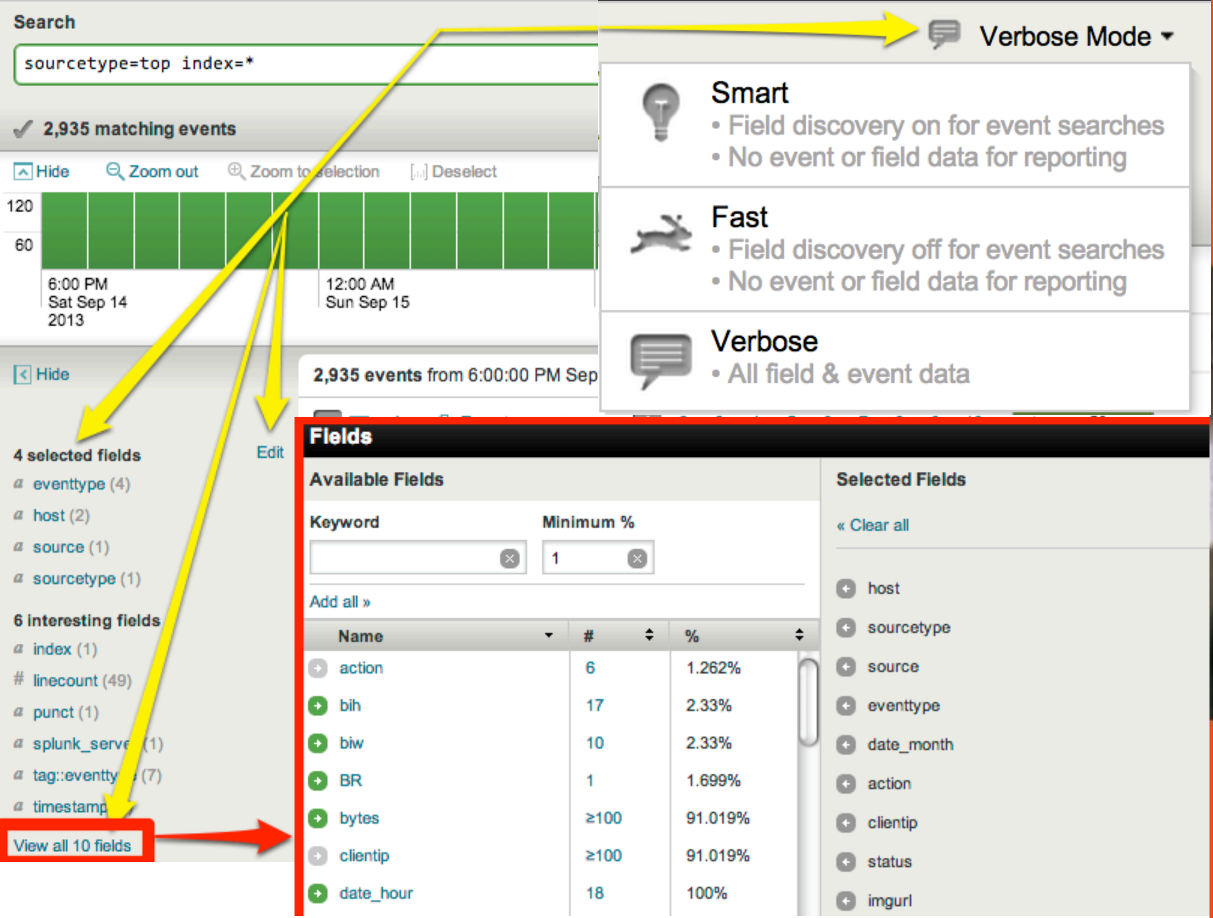
- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)
  - **Manual extraction (rex)**

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)
  - Manual extraction (rex)
- **Fields can be defined and calculated within a search**
  - Stats, Eval, Transaction
- You can use lookups to create fields for context and translation

What Are Fields?

- Searchable name/value pairings in event data
  - Index-time fields (timestamp, host, source, sourcetype, index)
  - Search-time fields (everything else!)
- Values are extracted from event data and mapped to a field name
  - Automatic extraction (props/transforms, key=value)
  - Manual extraction (rex)
- Fields can be defined and calculated within a search
  - Stats, Eval, Transaction
- **You can use lookups to create fields for context and translation**



Search

```
sourcetype=top index=*
```

✓ 2,935 matching events

Hide | Zoom out | Zoom to selection | [...] Deselect

Hide

2,935 events from 6:00:00 PM Sep

Verbose Mode

- **Smart**
  - Field discovery on for event searches
  - No event or field data for reporting
- **Fast**
  - Field discovery off for event searches
  - No event or field data for reporting
- **Verbose**
  - All field & event data

4 selected fields Edit

- a eventtype (4)
- a host (2)
- a source (1)
- a sourcetype (1)

6 interesting fields

- a index (1)
- # linecount (49)
- a punct (1)
- a splunk_serve (1)
- a tag::eventty (7)
- a timestamp

View all 10 fields

Fields

Available Fields

Keyword: [ ] Minimum %: 1

Add all »

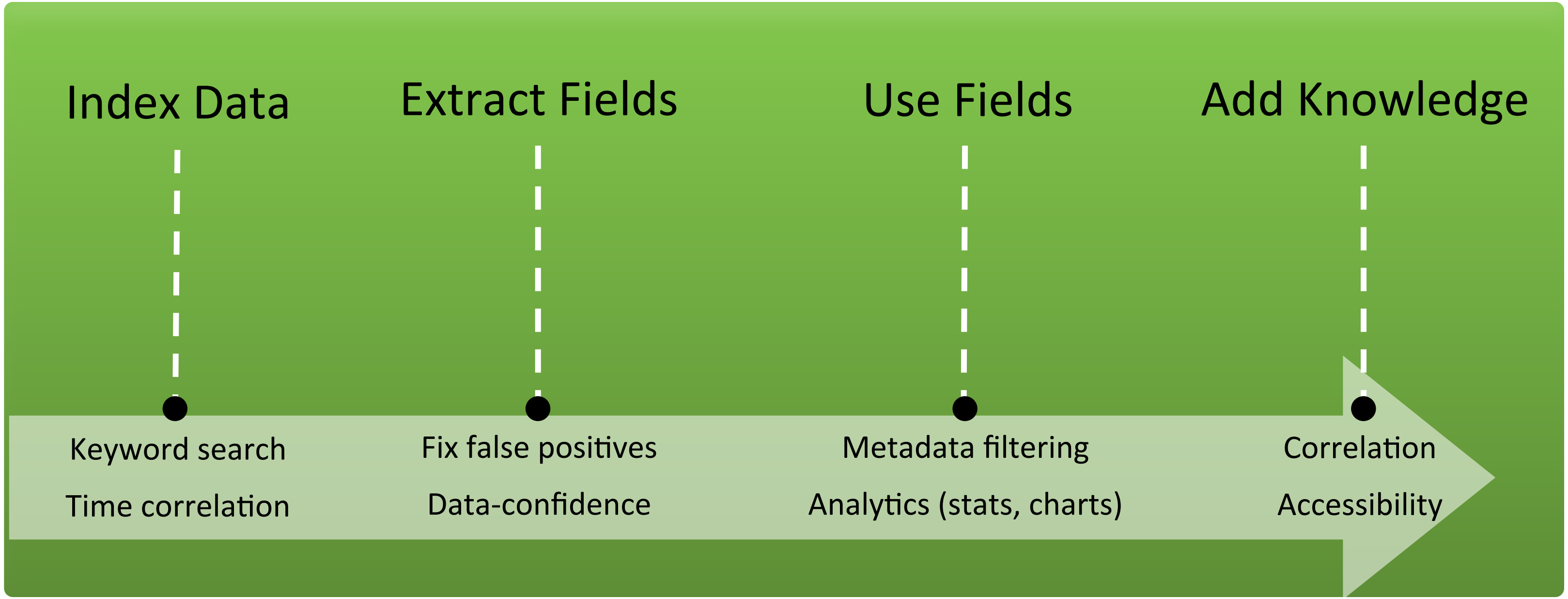
Name	#	%
action	6	1.262%
bih	17	2.33%
biw	10	2.33%
BR	1	1.699%
bytes	≥100	91.019%
clientip	≥100	91.019%
date_hour	18	100%

Selected Fields

« Clear all

- host
- sourcetype
- source
- eventtype
- date_month
- action
- clientip
- status
- imgurl

Field Maturity



Index Data

Keyword search

Time correlation

Extract Fields

Fix false positives

Data-confidence

Use Fields

Metadata filtering

Analytics (stats, charts)

Add Knowledge

Correlation

Accessibility

Field Extractor Demo

- Field extraction using the Advanced Field Extractor
- Regex/pattern based & delimiter based
- Validating extractions and eliminating false +/-

Multivalued Fields

Recipients	Open Ports	Files Changed	Ingredients
jmiller@splunk	25	Props.conf	Gin
boss@splunk	80	Transforms.conf	Lillet Blanc
support@splunk	443		Cointreau
	514		Lemon Juice
	53		Absinthe

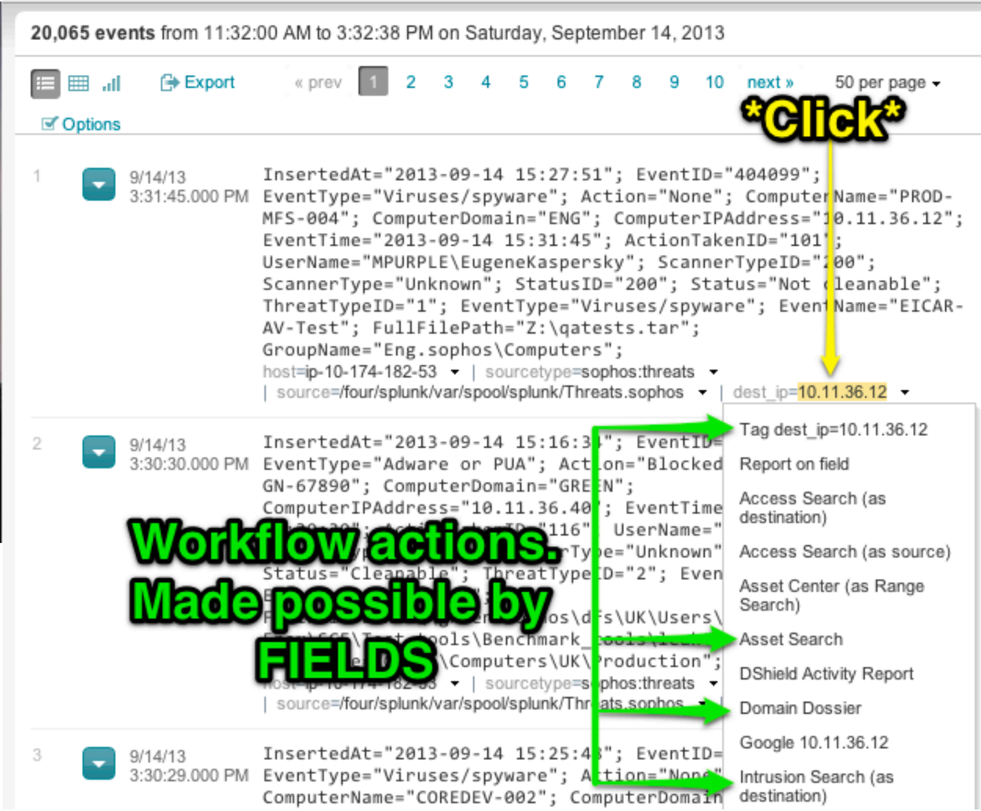
Multivalued Fields Demo

- Extraction (props, transforms, rex)
- Manipulation (mvexpand, nomv)
- Evals (mvcount, mvfilter, mvfind, mvindex)

More Fun With Fields

YO DAWG, I HEARD YOU LIKE FIELDS
SO I REX'D ON A REX SO YOU CAN EXTRACT FROM AN EXTRACTION

putting punctuation in its place



20,065 events from 11:32:00 AM to 3:32:38 PM on Saturday, September 14, 2013

```
1  9/14/13          InsertedAt="2013-09-14 15:27:51"; EventID="404099";
   3:31:45.000 PM   EventType="Viruses/spyware"; Action="None"; ComputerName="PROD-
                    MFS-004"; ComputerDomain="ENG"; ComputerIPAddress="10.11.36.12";
                    EventTime="2013-09-14 15:31:45"; ActionTakenID="101";
                    UserName="MPURPLE\EugeneKaspersky"; ScannerTypeID="200";
                    ScannerType="Unknown"; StatusID="200"; Status="Not cleanable";
                    ThreatTypeID="1"; EventType="Viruses/spyware"; EventName="EICAR-
                    AV-Test"; FullFilePath="Z:\qatests.tar";
                    GroupName="Eng.sophos\Computers";
                    host=ip-10-174-182-53 | sourcetype=sophos:threats
                    | source=/four/splunk/var/spool/splunk/Threats.sophos | dest_ip=10.11.36.12

2  9/14/13          InsertedAt="2013-09-14 15:16:3"; EventID=
   3:30:30.000 PM   EventType="Adware or PUA"; Action="Blocked
                    GN-67890"; ComputerDomain="GREEN";
                    ComputerIPAddress="10.11.36.40"; EventTime
                    "116"; UserName="
                    rType="Unknown"
                    Status="Cleanable"; ThreatTypeID="2"; Even
                    os\dfs\UK\Users\
                    ools\Benchmark_
                    \Computers\UK\Production";
                    | sourcetype=sophos:threats
                    | source=/four/splunk/var/spool/splunk/Threats.sophos

3  9/14/13          InsertedAt="2013-09-14 15:25:4"; EventID=
   3:30:29.000 PM   EventType="Viruses/spyware"; Action="None"
                    ComputerName="COREDEV-002"; ComputerDomain
```

Tag dest_ip=10.11.36.12
Report on field
Access Search (as destination)
Access Search (as source)
Asset Center (as Range Search)
Asset Search
DShield Activity Report
Domain Dossier
Google 10.11.36.12
Intrusion Search (as destination)

.conf2015

THANK YOU

splunk>