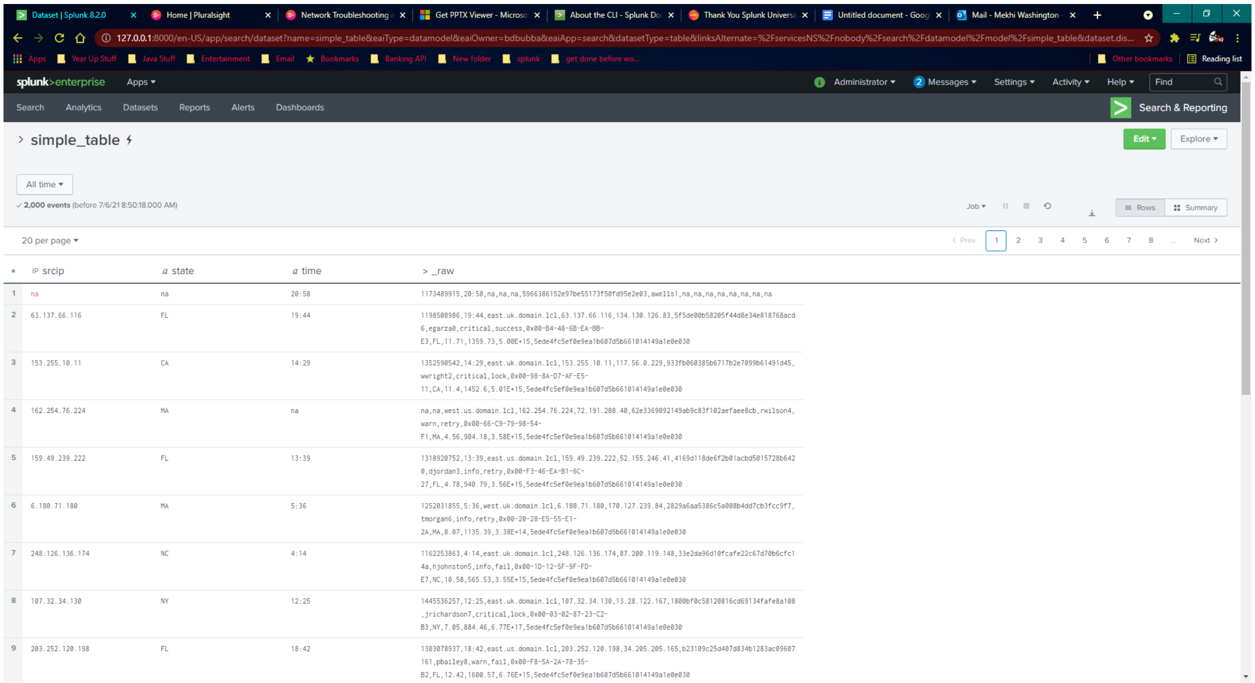
The Complete Splunk Beginner Course (2021)

Homeworkdata.cvs Dataset

Search Queries

- host="MEKHIS-PC"

- host="splunk/main"
  - aka homeworkdataset (creating a table view from this data) Fields are “ip”, “time”, “state”.

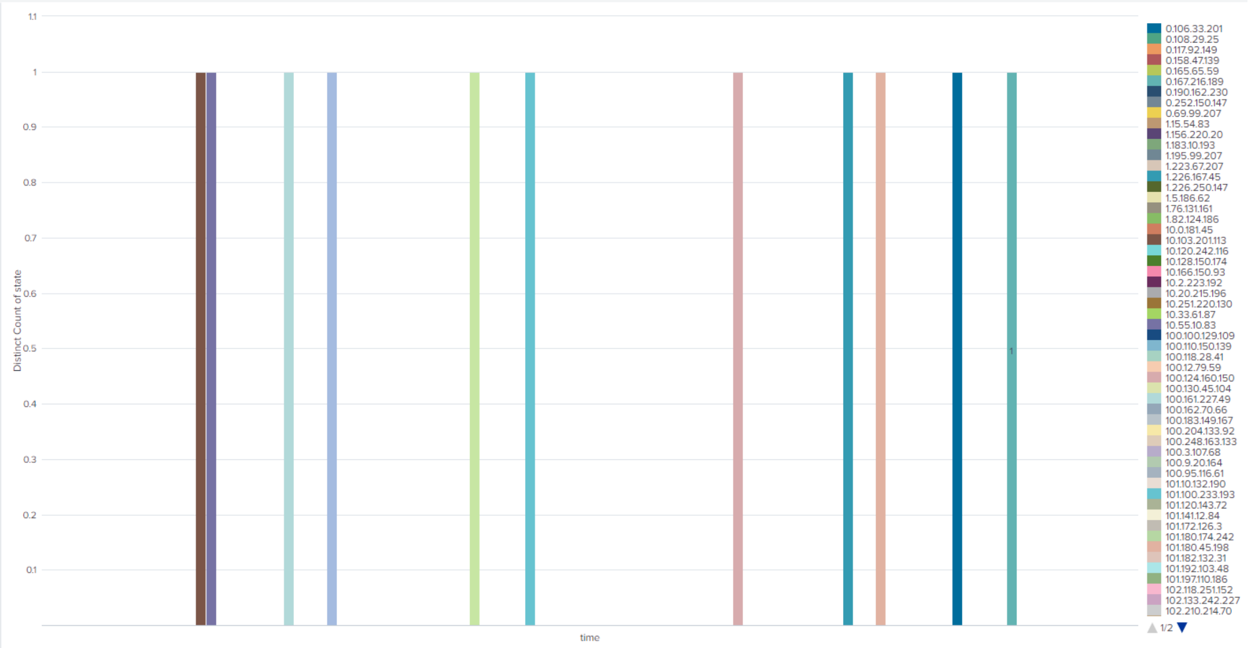


✓ 2,000 events (before 7/6/21 8:50:18.000 AM)

20 per page

*	IP srcip	a state	a time	> _raw
1	na	na	20:58	1173489915,20:58,na,na,na,5966386152e97be55173f50fd95e2e03,awells1,na,na,na,na,na,na,na,na
2	63.137.66.116	FL	19:44	1198508986,19:44,east.uk.domain.lcl,63.137.66.116,134.130.126.83,5f5de00b58205f44d8e34e818768acd6,egarza0,critical,success,0x00-B4-48-6B-EA-BB-E3,FL,11.71,1359.73,5.00E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
3	153.255.10.11	CA	14:29	1352590542,14:29,east.uk.domain.lcl,153.255.10.11,117.56.0.229,933fb060385b6717b2e7099b61491d45,wwright2,critical,lock,0x00-98-8A-D7-AF-E5-11,CA,11.4,1452.6,5.01E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
4	162.254.76.224	MA	na	na,na,west.us.domain.lcl,162.254.76.224,72.191.208.40,62e3369092149ab9c83f102aefaee8cb,rwilson4,warn,retry,0x00-66-C9-79-98-54-F1,MA,4.56,904.18,3.58E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
5	159.49.239.222	FL	13:39	1318920752,13:39,east.us.domain.lcl,159.49.239.222,52.155.246.41,4169d118de6f2b01acbd5015728b6420,djordan3,info,retry,0x00-F3-46-EA-B1-6C-27,FL,4.78,940.79,3.56E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
6	6.180.71.180	MA	5:36	1252031855,5:36,west.uk.domain.lcl,6.180.71.180,170.127.239.84,2829a6aa5386c5a008b4dd7cb3fcc9f7,tmorgan6,info,retry,0x00-20-28-E5-55-E1-2A,MA,8.07,1135.39,3.38E+14,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
7	248.126.136.174	NC	4:14	1162253863,4:14,east.uk.domain.lcl,248.126.136.174,87.200.119.148,33e2da96d10fcafe22c67d70b6cfc14a,hjohnston5,info,fail,0x00-1D-12-5F-9F-FD-E7,NC,10.58,565.53,3.55E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
8	107.32.34.130	NY	12:25	1445536257,12:25,east.uk.domain.lcl,107.32.34.130,13.28.122.167,1800bf0c58120816cd69134fafe8a108,jrichardson7,critical,lock,0x00-03-02-87-23-C2-B3,NY,7.05,884.46,6.77E+17,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030
9	203.252.120.198	FL	18:42	1303078937,18:42,east.us.domain.lcl,203.252.120.198,34.205.205.165,b23109c25d407d834b1283ac09607161,pbailey8,warn,fail,0x00-F8-5A-2A-78-35-B2,FL,12.42,1600.57,6.76E+15,5ede4fc5ef0e9ea1b607d5b661014149a1e0e030

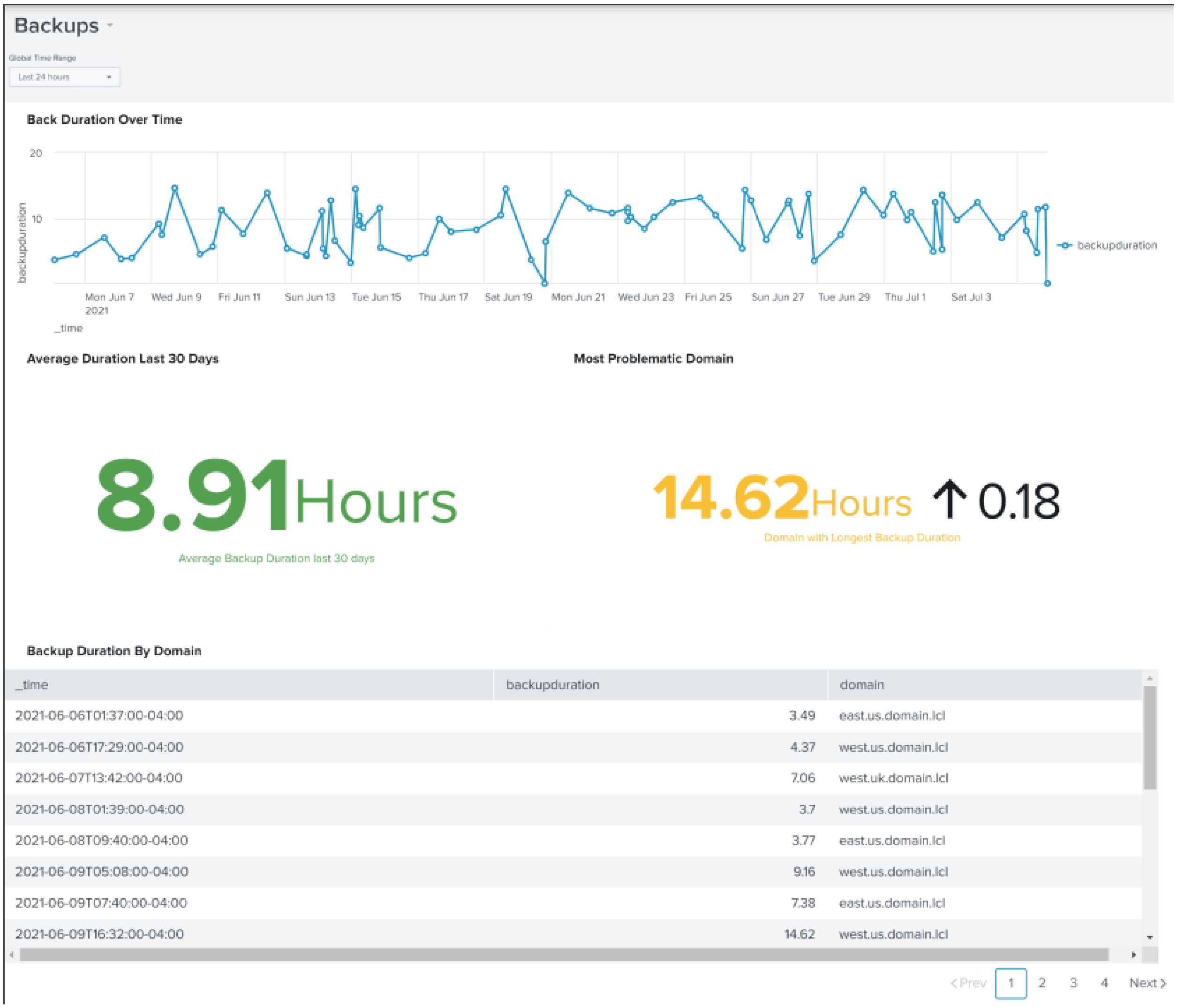
Creating a pivot



Demo

Searches:

- host="splunk/main" backupduration=* domain=* | table _time backupduration domain
- host="splunk/main" backupduration=* domain=* | stats max(backupduration) by domain
- host="splunk/main" backupduration=* domain=* | stats max(backupduration)
- host="splunk/main" backupduration=* domain=* | stats avg(backupduration)



Backups

Global Time Range

Last 24 hours

Back Duration Over Time

Average Duration Last 30 Days

8.91Hours

Average Backup Duration last 30 days

Most Problematic Domain

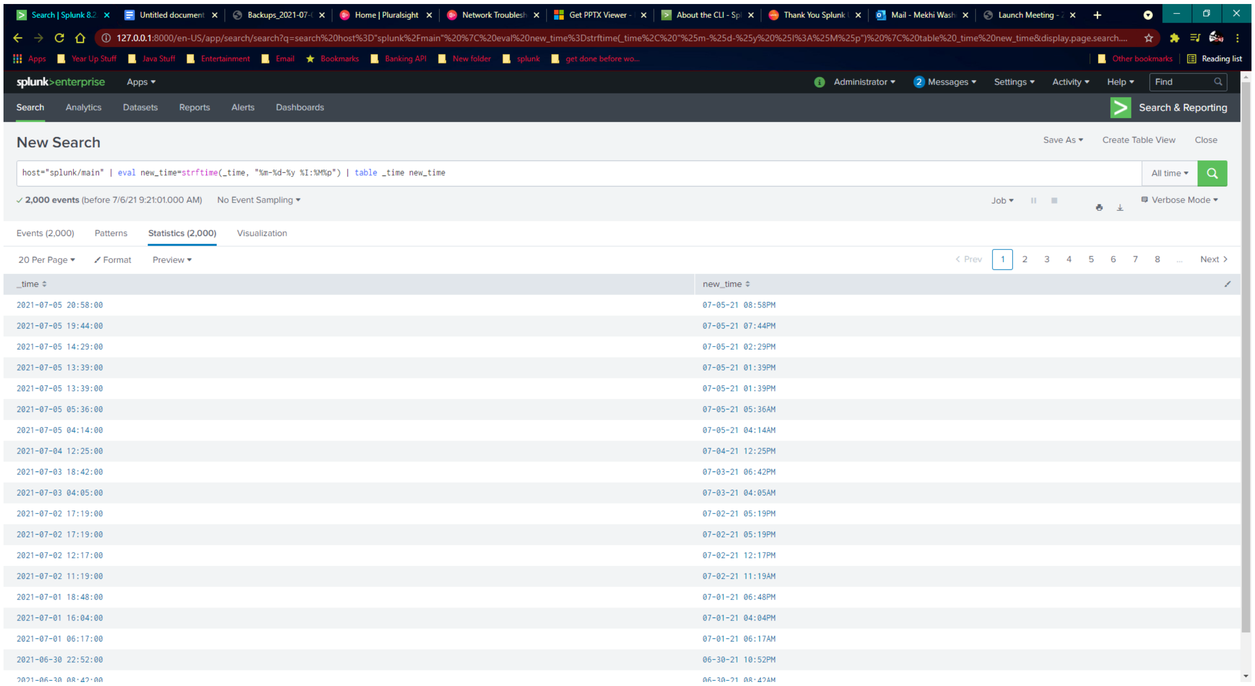
14.62Hours ↑ 0.18

Domain with Longest Backup Duration

Backup Duration By Domain

_time	backupduration	domain
2021-06-06T01:37:00-04:00	3.49	east.us.domain.lcl
2021-06-06T17:29:00-04:00	4.37	west.us.domain.lcl
2021-06-07T13:42:00-04:00	7.06	west.uk.domain.lcl
2021-06-08T01:39:00-04:00	3.7	west.us.domain.lcl
2021-06-08T09:40:00-04:00	3.77	east.us.domain.lcl
2021-06-09T05:08:00-04:00	9.16	west.us.domain.lcl
2021-06-09T07:40:00-04:00	7.38	east.us.domain.lcl
2021-06-09T16:32:00-04:00	14.62	west.us.domain.lcl

- host="splunk/main" | eval new_time=strftime(_time, "%m-%d-%y %I:%M%p") | table _time new_time



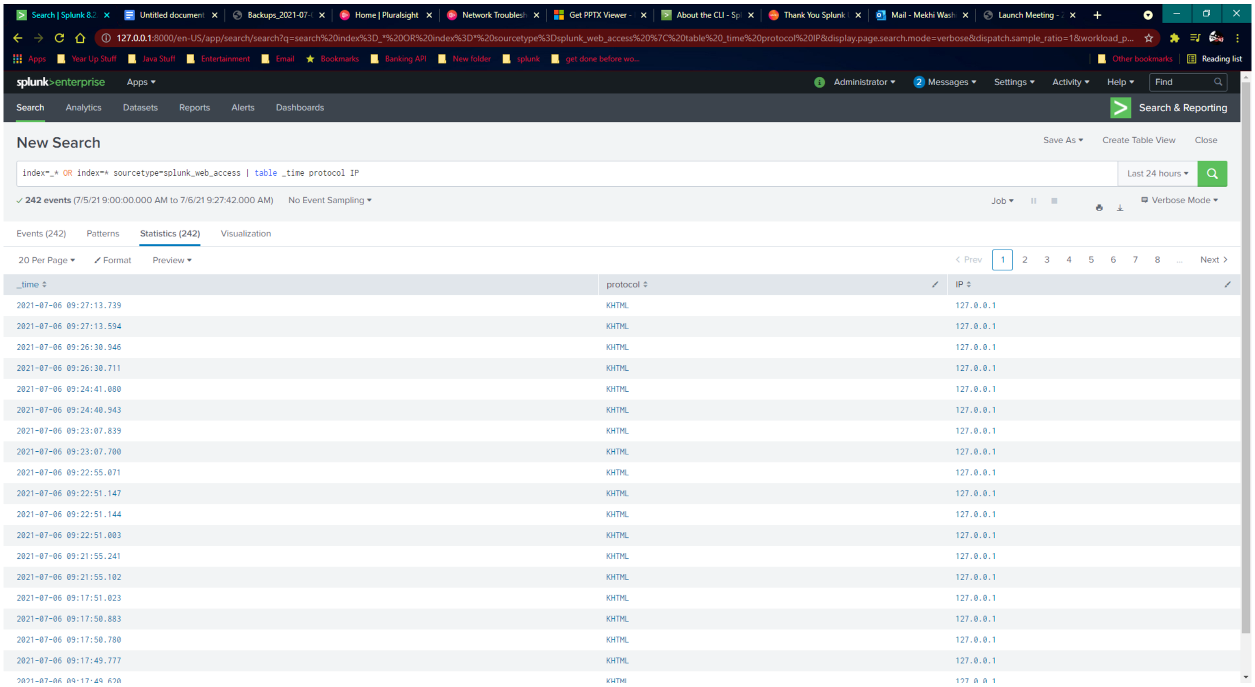
New Search

```
host="splunk/main" | eval new_time=strftime(_time, "%m-%d-%y %I:%M%p") | table _time new_time
```

✓ 2,000 events (before 7/6/21 9:21:01.000 AM) No Event Sampling

_time	new_time
2021-07-05 20:58:00	07-05-21 08:58PM
2021-07-05 19:44:00	07-05-21 07:44PM
2021-07-05 14:29:00	07-05-21 02:29PM
2021-07-05 13:39:00	07-05-21 01:39PM
2021-07-05 13:39:00	07-05-21 01:39PM
2021-07-05 05:36:00	07-05-21 05:36AM
2021-07-05 04:14:00	07-05-21 04:14AM
2021-07-04 12:25:00	07-04-21 12:25PM
2021-07-03 18:42:00	07-03-21 06:42PM
2021-07-03 04:05:00	07-03-21 04:05AM
2021-07-02 17:19:00	07-02-21 05:19PM
2021-07-02 17:19:00	07-02-21 05:19PM
2021-07-02 12:17:00	07-02-21 12:17PM
2021-07-02 11:19:00	07-02-21 11:19AM
2021-07-01 18:48:00	07-01-21 06:48PM
2021-07-01 16:04:00	07-01-21 04:04PM
2021-07-01 06:17:00	07-01-21 06:17AM
2021-06-30 22:52:00	06-30-21 10:52PM
2021-06-30 08:42:00	06-30-21 08:42AM

- index="_internal"



New Search

```
index=_* OR index=* sourcetype=splunk_web_access | table _time protocol IP
```

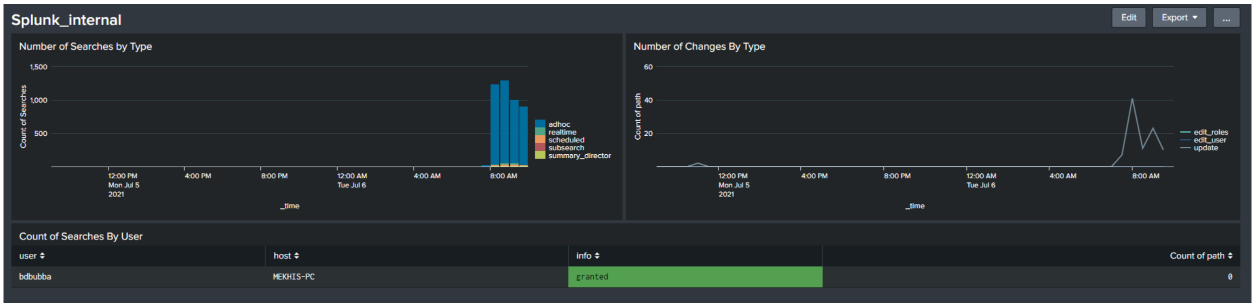
✓ 242 events (7/5/21 9:00:00.000 AM to 7/6/21 9:27:42.000 AM) No Event Sampling

_time	protocol	IP
2021-07-06 09:27:13.739	KHTML	127.0.0.1
2021-07-06 09:27:13.594	KHTML	127.0.0.1
2021-07-06 09:26:30.946	KHTML	127.0.0.1
2021-07-06 09:26:30.711	KHTML	127.0.0.1
2021-07-06 09:24:41.080	KHTML	127.0.0.1
2021-07-06 09:24:40.943	KHTML	127.0.0.1
2021-07-06 09:23:07.839	KHTML	127.0.0.1
2021-07-06 09:23:07.700	KHTML	127.0.0.1
2021-07-06 09:22:55.071	KHTML	127.0.0.1
2021-07-06 09:22:51.147	KHTML	127.0.0.1
2021-07-06 09:22:51.144	KHTML	127.0.0.1
2021-07-06 09:22:51.003	KHTML	127.0.0.1
2021-07-06 09:21:55.241	KHTML	127.0.0.1
2021-07-06 09:21:55.102	KHTML	127.0.0.1
2021-07-06 09:17:51.023	KHTML	127.0.0.1
2021-07-06 09:17:50.883	KHTML	127.0.0.1
2021-07-06 09:17:50.780	KHTML	127.0.0.1
2021-07-06 09:17:49.777	KHTML	127.0.0.1
2021-07-06 09:17:49.620	KHTML	127.0.0.1

- index=_* OR index=* sourcetype=splunk_web_access | table _time protocol IP

Added 2 new fields called “protocol and “IP”

Building Dashboard WIth pivot (Not using the SPL)



Splunk_internal

Number of Searches by Type

Number of Changes By Type

Count of Searches By User

user ⬍	host ⬍	info ⬍	Count of path ⬍
bdbubba	MEKHIS-PC	granted	0