# Splunk Knowledge Transfer

[Reference Guide](https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf)

## Topics

1. App: IPS > IPS\_Generic > **IPS/EPCS ECC Dashboard**
   1. Error Messages (sorting)
   2. Incident Locator Events
      1. Show Searching for text and observing all the actions
      2. Can input any data here, policy number, message text, etc.
   3. CDC/eCheck Transaction Counts
      1. Only successful
   4. Medod Durations
      1. Shows all of our method calls and running time for all to determine any long running
2. Searching
   1. First part of your search is the search string
   2. Different commands can be added using the pipe (|) character
      1. This is what organizes data into usable formats
   3. For our applications, we always specify the index we would like to search first
      1. ips\_cdc
      2. ips\_ebill
      3. ips\_echeck
      4. ips\_epas
      5. ips\_ezp
      6. ips\_inq
      7. ips\_misc
      8. ips\_rcc
      9. ips\_spi
      10. epcs
   4. Searching all of IPS is simple as you can use the asterisk (\*) sort of like the parentheses(%) in SQL. So index=ips\* will search all applications
      1. We have transactional data for CDC and Echeck, and event logs for all data
3. Some of the most common commands are
   1. Chart
   2. Timechart
   3. Dedup
   4. Eval
   5. Fields
   6. Rename
   7. Sort
   8. Stats
   9. Table