Parsed out from the \_raw field since there are commas in the data

* BIS\_ID – The identifier in the Paychex Benefits database
* BRANCH – The Paychex branch that is assigned to a client
* CHECK\_DATE – The date that a check was issued to a client employee
* CLIENT – the client number from our payroll system
* **DURATION – the amount of time a database query took to execute, only logged if it took longer than 10000ms**
* INFO – IGNORE THIS (it parsed out strange when the data was exported from splunk)
* PID – the Linux process id for the process/ app
* REPORT – the ORS report ID
* RUN\_DTTM – the date & time stamp that the report was generated and loaded into ORS

General fields

* **\_raw – the raw splunk data, will be the focus of our effort and will likely need to be groomed/ formatted**
* \_time – the time stamp on the splunk log
* date\_hour – the hour (24 hour time)
* date\_mday – the day of the month
* date\_minute – minute timestamp
* date\_month – month
* date\_second – second time stamp
* date\_wday – day of the week
* date\_year – year
* date\_zone – I think splunk metadata (we can likely ignore this)
* eventtype – Splunk metadata (we can likely ignore this)
* host – the server name that the log file was on
* index – the splunk “index” where the data is saved – basically metadata ((we can likely ignore this)
* linecount – don’t know what this is – likely splunk metadata (we can likely ignore this)
* punct – don’t know what this is – likely splunk metadata (we can likely ignore this)
* source – the source log file that that splunk scanned for the data
* sourcetype – used for grouping logs, splunk metadata (we can likely ignore this)
* splunk\_server – the splunk server that collected the data (we can likely ignore this)
* splunk\_server\_group – Splunk cluster (we can likely ignore this)
* **tag – not totally sure what this is**
* tag::eventtype – likely splunk metadata (we can likely ignore this)
* tag::source – likely splunk metadata (we can likely ignore this)
* tag::sourcetype – likely splunk metadata (we can likely ignore this)
* timeendpos – likely splunk metadata (we can likely ignore this)
* timestamp – likely splunk metadata (we can likely ignore this)
* timestartpos – likely splunk metadata (we can likely ignore this)