1001_M5_Search_Language_Fundamentals_Quiz

1. In the search pipeline, command modifiers within the search string are shown in which color?
    A. Pink
    B. Blue
    C. Orange
    D. Black

2. When sorting by multiple fields using the sort command, what delimiter separates the field names?
    A. |
    B. $
    C. #
    D. ,

3. How can fields be added to or removed from search results?
    A. Use fields + to add and fields - to remove.
    B. Use table+ to add and table- to remove
    C. Use fields+ to add and fields to remove
    D. Use fields Plus to add and fields Minus to remove

4. Which command, when used early in a search, is most effective for improving execution speed?
    A. dedup
    B. rename
    C. sort –
    D. fields +

5. The syntax of Splunk Search Language can be divided into which components?
    A. Search Term, Command, Pipe
    B. Search Terms Only
    C. Commands Only
    D. Search Term, Pipe, Command, Functions, Arguments, Clause

6. Which command would rename the field action to Customer Action?
    A. | rename action = CustomerAction
    B. | rename Action as “Customer Action”

C. | rename Action to Customer Action
D. | rename action as “Customer Action”

7. In search strings, when should the pipe (`|`) character be used?
   A. Before clauses. For example: stats sum(bytes) | by host
   B. Before commands. For example: | stats sum(bytes) by host
   C. Before arguments. For example: stats sum | (bytes) by host
   D. Before functions. For example: stats | sum(bytes) by host

8. Which search returns only events containing the word “error” and displays them as a table with the fields action, src, and dest?
   A. error | table action, src, dest
   B. error | tabular action, src, dest
   C. error | stats table action, src, dest
   D. error | table column=action column=src column=dest