Which of the following commands will show the maximum bytes?

A. sourcetype=access_* | maximum totals by bytes
B. sourcetype=access_* | avg (bytes)
C. sourcetype=access_* | stats max(bytes)
D. sourcetype=access_* | max(bytes)

Correct Answer: C

QUESTION 96
Highlighted search terms indicate __________ search results in Splunk.

A. Display as selected fields.
B. Sorted
C. Charted based on time
D. Matching

Correct Answer: D

QUESTION 97
When you mouse over and click to add a search term this (thesE. Boolean operator(s) is(arE. not implied. (Select all that apply).

A. OR
B. ( )
C. AND
D. NOT

Correct Answer: ABD

QUESTION 98
A data model consists of which three types of datasets?

A. Constraint, field, value.
B. Events, searches, transactions.
C. Field extraction, regex, delimited.
D. Transaction, session ID, metadata.

Correct Answer: B

QUESTION 99
Which workflow uses field values to perform a secondary search?

A. POST
B. Action
C. Search
D. Sub-Search

Correct Answer: C

QUESTION 100

In the following eval statement, what is the value of description if the status is 503? index=main | eval description=case(status==200, "OK", status==404, "Not found", status==500, "Internal Server Error")

A. The description field would contain no value.
B. The description field would contain the value 0.
C. The description field would contain the value "Internal Server Error".
D. This statement would produce an error in Splunk because it is incomplete.

Correct Answer: A

QUESTION 101
Which type of visualization shows relationships between discrete values in three dimensions?

A. Pie chart
B. Line chart
C. Bubble chart
D. Scatter chart

Correct Answer: C

QUESTION 102
Which of the following searches will return events containing a tag named Privileged?

A. tag=Priv
B. tag=Priv*
C. tag=priv*
D. tag=privileged

Correct Answer: B

QUESTION 103
When using a field value variable with a Workflow Action, which punctuation mark will escape the data

A. *
B. !
C. ^
D. #

Correct Answer: B

QUESTION 104
This function of the stats command allows you to return the middle-most value of field X.

A. Median(X)
B. Eval by X
C. Fields(X)
D. Values(X)

Correct Answer: A

QUESTION 105
Which is not a comparison operator in Splunk

A. <=
B. =
C. !=
D. >
E. ?=

Correct Answer: E

QUESTION 106
There are several ways to access the field extractor. Which option automatically identifies data type, source type, and sample event?

A. Event Actions > Extract Fields
B. Fields sidebar > Extract New Field
C. Settings > Field Extractions > New Field Extraction
D. Settings > Field Extractions > Open Field Extraction

Correct Answer: B

QUESTION 107
This clause is used to group the output of a stats command by a specific name.

A. Rex
B. As
C. List
D. By

Correct Answer: B

QUESTION 108
How many ways are there to access the Field Extractor Utility?

A. 3
B. 4
C. 1
D. 5

Correct Answer: A

QUESTION 109
Which of the following statements about tags is true? (select all that apply.)

A. Tags are case-insensitive.
B. Tags are based on field/vale pairs.
C. Tags categorize events based on a search.
D. Tags are designed to make data more understandable.

Correct Answer: BD

QUESTION 110
Which workflow action method can be used the action type is set to link?

A. GET
B. PUT
C. Search
D. UPDATE

Correct Answer: A

QUESTION 111
What is the correct way to name a macro with two arguments?

A. us_sales2
B. us_sales(1,2)
C. us_sale,2
D. us_sales(2)

Correct Answer: D

QUESTION 112
In the Field Extractor Utility, this button will display events that do not contain extracted fields. Select your answer.

A. Selected-Fields
B. Non-Matches
C. Non-Extractions
D. Matches

Correct Answer: B

QUESTION 113
A user wants to create a new field alias for a field that appears in two sourcetypes. How many field aliases need to be created?

A. One.
B. Two.
C. It depends on whether the original fields have the same name.
D. It depends on whether the two sourcetypes are associated with the same index.

Correct Answer: B

QUESTION 114
A report scheduled to run every 15 mins. but takes 17 mins. to complete is in danger of being_____.

A. skipped or deferred

B. automatically accelerated
C. deleted
D. all of the above

Correct Answer: A

QUESTION 115
Which search would limit an "alert" tag to the "host" field?

A. tag=alert
B. host::tag::alert
C. tag==alert
D. tag::host=alert

Correct Answer: D

QUESTION 116
The limit attribute will____________.

A. override default of 10
B. only work with top command
C. override default of 20
D. override default of 15

Correct Answer: A

QUESTION 117
Which statement is true?

A. Pivot is used for creating datasets.
B. Data models are randomly structured datasets.
C. Pivot is used for creating reports and dashboards.
D. In most cases, each Splunk user will create their own data model.
Correct Answer: C

QUESTION 118
The time range specified for a historical search defines the _____________ .------questionable on ans

A. Amount of data shown on the timeline as data streams in
B. Amount of data fetched from index matching that time range
C. Time range for the static results

Correct Answer: B

QUESTION 119
Which of the following statements describes calculated fields?

A. Calculated fields are only used on fields added by lookups.
B. Calculated fields are a shortcut for repetitive and complex eval commands.
C. Calculated fields are a shortcut for repetitive and complex calc commands.