Question 1

Which of the statements are correct? (Choose three.)

Options:

A- Zoom to selection: Narrows the time range and re-executes the search.

B- Zoom to selection: Narrows the time range and doesn't re-executes the search.

C- Format Timeline: Hides or shows the timeline in different views.

D- Zoom-Out: Expands the time focus and doesn't re-executes the search.

E- Zoom-out: Expands the time focus and re-executes the search.

Answer:

A, C, E

Question 2

Which symbol is used to snap the time?

Question 3

Question Type: **MultipleChoice**

Which of the statements is correct regarding click and drag option in timeline?

Options:

A- The new result after selecting the range by dragging filters the events and displays the most recent first.

B- There is no functionality like click and drag in Splunk's timeline.

C- Using this option executes a new query.

D- This doesn't execute a new query

Answer:

A

Question 4

Question Type: **MultipleChoice**

Splunk Parses data into individual events, extracts time, and assigns metadata.

Options:

A- False

B- True

Answer:

B

Question 5

You are able to create new Index in Data Input settings.

Options:

A- No

B- Yes

Answer:

B

Question 6

Events in Splunk are automatically segregated using data and time.

Options:

A- Yes

B- No

Answer:

A

Question 7

The default host name used in Inputs general settings can not be changed.

Options:

A- False

B- True

Answer:

A

Question 8

Question Type: MultipleChoice

You can use the following options to specify start and end time for the query range:

Options:

A- earliest=

B- latest=

C- beginning=

D- ending=

E- All the above

F- Only 3rd and 4th

Answer:

F

Question 9

Question Type: MultipleChoice

The new data uploaded in Splunk are shown in _____.

Options:

A- Real-time

B- 10 Minutes

C- Overnight Download

D- 30 Minutes

Question 10

Question Type: **MultipleChoice**

@ Symbol can be used in advanced time unit option.

Options:

A- No

B- Yes

Answer:

B