Question 1

Splunk automatically determines the source type for major data types.

Options:

A- False

B- True

Answer:

B

Question 2

Select the correct option that applies to Index time processing (Choose three.).

A- Indexing

B- Searching

C- Parsing

D- Settings

E- Input

Answer:

A, C, E

Question 3

Question Type: MultipleChoice

Data sources being opened and read applies to:

Options:

A- None of the above

B- Indexing Phase

C- Parsing Phase

D- Input Phase

E- License Metering

Answer:

D

Question 4

Question Type: MultipleChoice

You can on-board data to Splunk using following means (Choose four.):

Options:

A- Props

B- CLI

C- Splunk Web

D- savedsearches.conf

E- Splunk apps and add-ons

F- indexes.conf

G- inputs.conf

H- metadata.conf

Answer:

B, C, E, G

Question 5

Question Type: MultipleChoice

Forward Option gather and forward data to indexers over a receiving port from remote machines.

Options:

A- False

B- True

Question 6

Question Type: MultipleChoice

Monitor option in Add Data provides _____.

Options:

A- Only continuous monitoring.

B- Only One-time monitoring.

C- None of the above.

D- Both One-time and continuous monitoring

Answer:

D

Question 7

Parsing of data can happen both in HF and Indexer.

Options:

A- Only HF

B- No

C- Yes

Answer:

C