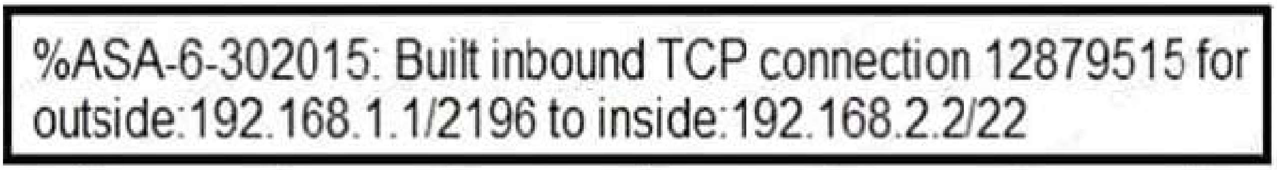
210-255$^{\text{Q\&As}}$

Cisco Cybersecurity Operations

Pass Cisco 210-255 Exam with 100% Guarantee

QUESTION 1

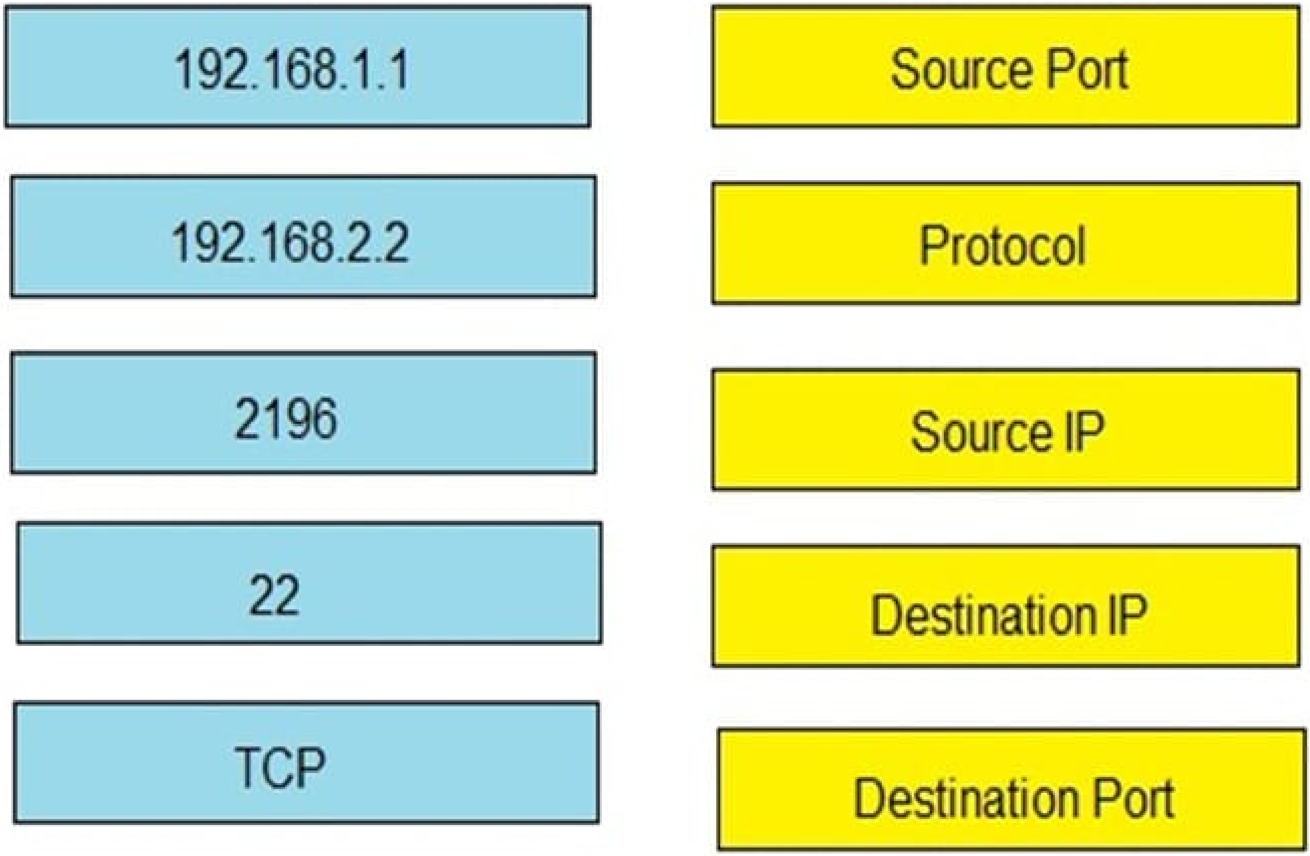
Refer to exhibit.



```
%ASA-6-302015: Built inbound TCP connection 12879515 for
outside:192.168.1.1/2196 to inside:192.168.2.2/22
```

Drag and drop the items from the left onto the correct 5-tuples on the right.

Select and Place:



192.168.1.1

192.168.2.2

2196

22

TCP

Source Port

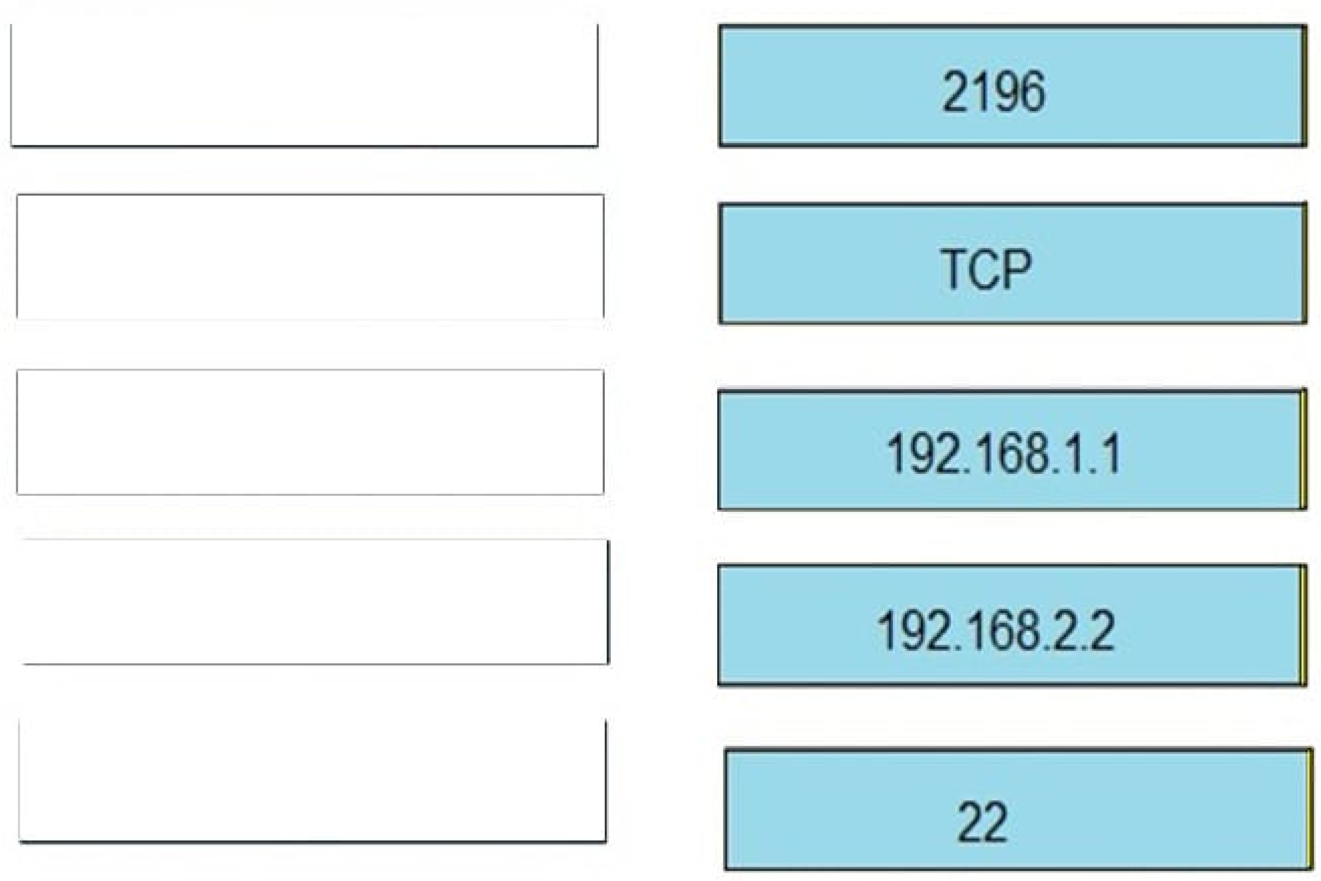
Protocol

Source IP

Destination IP

Destination Port

Correct Answer:



QUESTION 2

Which two potions are the primary 5-tuple components? (Choose two)

A. destination IP address

B. header length

C. sequence number

D. checksum

E. source IP address

Correct Answer: AE

QUESTION 3

During which phase of the forensic process is data that is related to a specific event labeled and recorded to preserve its integrity?

A. collection

B. examination

C. reporting

D. investigation

Correct Answer: A

QUESTION 4

According to NIST-SP800-61R2, why is it important to keep clocks synchronized?

A. event correlation

B. to link with other countries easily

C. to not lose track of time

D. to measure the effectiveness of an attack

Correct Answer: A

QUESTION 5

Which evidence is considered to be the most volatile?

A. disk

B. registers and cache

C. removable media

D. logging

Correct Answer: D