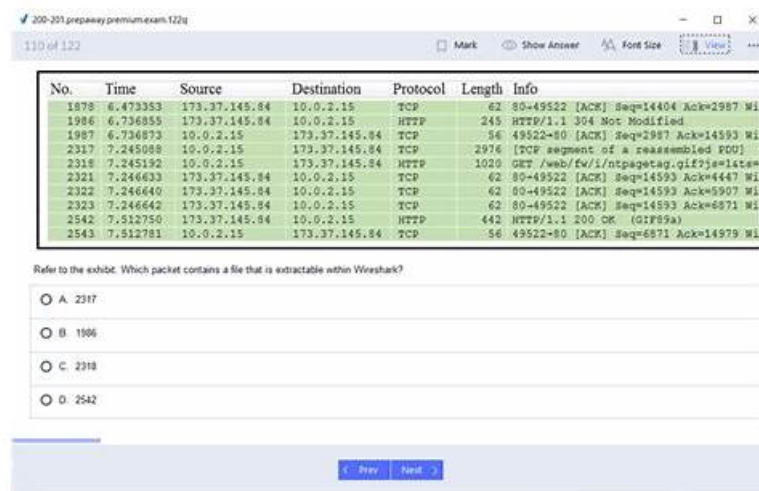


# 200-201 Lab Questions | 200-201 Valid Exam Testking



No.	Time	Source	Destination	Protocol	Length	Info
1878	6.473353	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14404 Ack=2987 Win=
1986	6.736855	173.37.145.84	10.0.2.15	HTTP	245	HTTP/1.1 304 Not Modified
1987	6.736873	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=2987 Ack=14593 Win=
2317	7.245088	10.0.2.15	173.37.145.84	TCP	2976	[TCP segment of a reassembled PDU]
2318	7.245192	10.0.2.15	173.37.145.84	HTTP	1020	GET /web/fw/i/ntpgetag.gif?js=1&js=
2321	7.246633	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=4447 Win=
2322	7.246640	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=5907 Win=
2323	7.246642	173.37.145.84	10.0.2.15	TCP	62	80->49522 [ACK] Seq=14593 Ack=6871 Win=
2542	7.512750	173.37.145.84	10.0.2.15	HTTP	442	HTTP/1.1 200 OK (GIF89a)
2543	7.512781	10.0.2.15	173.37.145.84	TCP	56	49522->80 [ACK] Seq=6871 Ack=14579 Win=

BTW, DOWNLOAD part of Free4Torrent 200-201 dumps from Cloud Storage: [https://drive.google.com/open?id=1LIZlg\\_rT2xlQ-WVrD74trv04FNPwnhUu](https://drive.google.com/open?id=1LIZlg_rT2xlQ-WVrD74trv04FNPwnhUu)

If you also need to take the 200-201 exam and want to get the related certification, you can directly select our study materials. We can promise that our 200-201 study question has a higher quality than other study materials in the market. If you want to keep making progress and transcending yourself, we believe that you will harvest happiness and growth. So if you buy and use the 200-201 test dump from our company, we believe that our study materials will make study more interesting and colorful, and it will be very easy for a lot of people to pass their exam and get the related certification if they choose our 200-201 Test Dump and take it into consideration seriously. Now we are willing to introduce the 200-201 exam reference guide from our company to you in order to let you have a deep understanding of our study materials. We believe that you will benefit a lot from our 200-201 study question.

Cisco 200-201 exam is an important certification for individuals looking to establish themselves in the field of cybersecurity operations. 200-201 exam is designed to test the fundamental knowledge and skills required to identify and respond to security incidents in a network environment. 200-201 Exam is intended for those who are new to cybersecurity operations or those who are seeking to expand their knowledge and skills in this field.

>> 200-201 Lab Questions <<

## 200-201 Lab Questions 100% Pass | Latest 200-201: Understanding Cisco Cybersecurity Operations Fundamentals 100% Pass

It is quite convenient to study with our 200-201 study materials. If you are used to study with paper-based materials you can choose the PDF version which is convenient for you to print. If you would like to get the mock test before the real 200-201 exam you can choose the software version, and if you want to study in anywhere at any time then our online APP version is your best choice since you can download it in any electronic devices. And the price of our 200-201 learning guide is favorable.

Cisco 200-201 exam consists of 100 questions, which must be completed within 120 minutes. 200-201 exam is available in multiple languages, including English, Japanese, and Spanish. It is a computer-based exam that can be taken at Pearson VUE testing centers or online through the Pearson OnVUE platform.

Cisco 200-201 exam is a certification program that is designed to test your understanding of cybersecurity operations fundamentals. 200-201 Exam is intended for individuals who are interested in pursuing a career in cybersecurity or those who already work in the field and want to advance their knowledge and skills. Passing the exam will provide you with a Cisco Certified CyberOps Associate certification, which is a valuable asset in the cybersecurity industry.

## Cisco Understanding Cisco Cybersecurity Operations Fundamentals Sample Questions (Q175-Q180):

### NEW QUESTION # 175

Refer to the exhibit.

- Drag and drop the element name from the left onto the correct piece of the PCAP file on the right.
- 

**Answer:**

Explanation:

□ Explanation:

In a PCAP file, which is used to capture network packets, each packet contains various pieces of information that can be analyzed. The source and destination addresses refer to the IP addresses of the sender and receiver of the packets. The source and destination ports refer to the port numbers used for the communication, with common ports like 443 indicating HTTPS traffic. The network protocol here is TCP, which is responsible for establishing a connection and ensuring the delivery of packets. The transport protocol is IPv4, which is the underlying protocol for routing packets across the network. Lastly, the application protocol is TLS v1.2, which is used for secure communication over the internet.

References = The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) course material covers the analysis of network traffic and the interpretation of PCAP files, which includes identifying the different elements within a packet capture1.

□

### NEW QUESTION # 176

Why is encryption challenging to security monitoring?

- A. Encryption analysis is used by attackers to monitor VPN tunnels.
- **B. Encryption is used by threat actors as a method of evasion and obfuscation.**
- C. Encryption introduces larger packet sizes to analyze and store.
- D. Encryption introduces additional processing requirements by the CPU.

**Answer: B**

### NEW QUESTION # 177

Which step in the incident response process researches an attacking host through logs in a SIEM?

- A. containment
- B. eradication
- **C. detection and analysis**
- D. preparation

**Answer: C**

### NEW QUESTION # 178

Refer to the exhibit.

□ What must be interpreted from this packet capture?

- A. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 74 to destination port 49098 using TCP protocol
- B. IP address 192.168.88.12 is communicating with 192.168.88.149 with a source port 49098 to destination port 80 using TCP protocol.
- C. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 49098 to destination port 80 using TCP protocol.
- **D. IP address 192.168.88.149 is communicating with 192.168.88.12 with a source port 80 to destination port 49098 using TCP protocol.**

**Answer: D**

Explanation:

The packet capture shows that IP address 192.168.88.149, using source port 80 (common for HTTP traffic), initiated communication with IP address 192.168.88.12 at destination port 49098, using the TCP protocol, indicating a typical client-server interaction over the web.

References: = These explanations are based on general cybersecurity principles as outlined in Cisco's training and certification content, such as the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) and other related Cisco resources.

### NEW QUESTION # 179

Which two pieces of information are collected from the IPv4 protocol header? (Choose two.)

- A. UDP port from which the traffic is sourced
- B. source IP address of the packet
- C. UDP port to which the traffic is destined
- D. destination IP address of the packet
- E. TCP port from which the traffic was sourced

**Answer: B,D**

Explanation:

Section: Network Intrusion Analysis

### NEW QUESTION # 180

• • • • •

**200-201 Valid Exam Testking:** <https://www.free4torrent.com/200-201-braindumps-torrent.html>

- [illegible]

2026 Latest Free4Torrent 200-201 PDF Dumps and 200-201 Exam Engine Free Share: <https://drive.google.com/open?>

id=1LIZlg rT2xlQ-WVrD74trv04FNPwnhUu