

Wireshark

WCA-101

Wireshark Certified Analyst (WCA-101)



For More Information – Visit link below:

<https://www.examsboost.com/>

Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

Latest Version: 6.0

Question: 1

Of the following, which are calculated by Wireshark and are not fields in the TCP/IP header? (Choose three.)

- A. Flags
- B. Urgent Pointer
- C. IP Identification
- D. Sequence Number (raw)
- E. Source Port
- F. TCP Segment Length
- G. Stream Index
- H. iRTT

Answer: F,G,H

Question: 2

Which of the following features are available in the pcapng file format and not the pcap file format? (Choose four.)

- A. Complete packet including headers and data
- B. Timestamps
- C. File level comments in Capture File Properties
- D. Packet length
- E. Embedded decryption secrets
- F. Protocol dissectors
- G. Network Interface used to capture traffic
- H. Per packet comments

Answer: C,E,G,H

Question: 3

You are analyzing a problem with a slow application that was captured on the server side. You have applied a display filter for the IP address of the client that was experiencing the issue. Next you would like to save these packets to a separate file.

Which Wireshark option can create a new file with only the displayed packets?

- A. Export Packet Bytes...
- B. Save As...
- C. Export PDUs to File...
- D. Export Specified Packets...
- E. Export Objects >
- F. Merge...
- G. Strip Headers...
- H. Export Packet Dissections >

Answer: D

Question: 4

You are analyzing a capture provided by a client. The client informs you that a problematic event occurs approximately 3 seconds after a user clicks a link on a website. The client has provided a comprehensive capture that includes several minutes before and after the event. You have successfully pinpointed the exact packet corresponding to the user's click, and there are no display filters applied. Which Wireshark feature would be best to quickly identify the packets that occurred about 3 seconds later?

- A. Add a column with "Time since previous frame in this TCP stream"
- B. Mark Packet
- C. View > Time Display Format
- D. Set Time Reference
- E. Apply a Display Filter
- F. Packet Comment

Answer: D

Question: 5

You need to capture traffic in a data center on a 10Gbps link. Which capture method would you use to get the most accurate timestamps?

- A. On the hypervisor
- B. SPAN port
- C. On the load-balancer
- D. Network tap
- E. Directly on the server

Answer: D

Thank You for Trying Our Product

For More Information – **Visit link below:**

<https://www.examsboost.com/>

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email Attachment**
- ✓ **24/7 Live Chat Support**
- ✓ **PDF file could be used at any Platform**
- ✓ **50,000 Happy Customer**



Visit us at: <https://www.examsboost.com/test/wca-101>