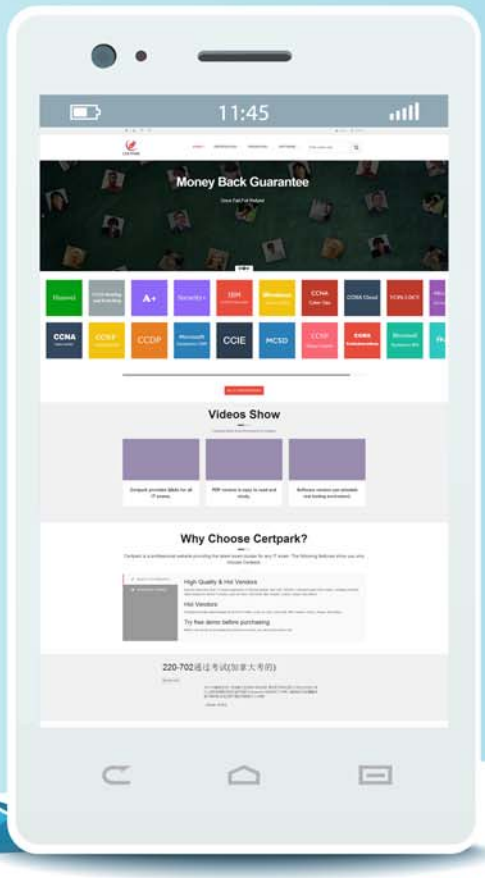
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **CWAP-403**

Title : Certified Wireless Analysis Professional

Version : DEMO

1.Which one of the following should be the first step when troubleshooting a WLAN issue?
A. Identify capture locations
B. Identify probable causes
C. Perform an initial WLAN scan and see if any obvious issues stand out
D. Define the problem
Answer: D

2.Which one of the best following is an advantage of using display filters instead of capture-time filters?
A. Display filters allow for focused analysis on just the packets of interest
B. Once created display filters are reusable for later captures
C. Display filters only hide the packets from view and the filtered packets can be enabled for view later
D. Multiple display filters can be applied simultaneously
Answer: A
Explanation:
display filters allow you to focus on things of interest and to ignore things you don't care about.
Reference: https://searchnetworking.techtarget.com/tip/How-to-manage-Wireshark-display-filters

3.Using a portable analyzer you perform a packet capture next to a client STA and you can see that the STA is associated to a BSS. You observe the STA sending packets to the AP and the AP sending packets to the STA. Less the 2% of all packets are retransmissions. You move to capture packets by the AP and, while the retry rate is still very low, you now only see unidirectional traffic from the AP to the client.
How do you explain this behavior?
A. There is a transmit power mismatch between the client and the AP and while the client can hear the Aps traffic, the AP cannot hear the client.
B. The portable analyzer has a lower receive sensitivity than the AP and while it can’t capture the packets from the client STA, the AP can receive them OK.
C. The STA is transmitting data using more spatial streams than the potable analyzer can support
D. The portable analyzer is too close to the AP causing CCI, blinding the AP to the client’s packets
Answer: B

4.Given a protocol analyzer can decrypt WPA2-PSK data packets providing the PSK and SSID are configured in the analyzer software.
When performing packet capture (in a non-FT environment) which frames are required in order for PSK frame decryption to be possible?
A. Authentication
B. Reassociation
C. 4-Way Handshake
D. Probe Response
Answer: C

5.When configuring a long term, forensic packet capture and saving all packets to disk which of the following is not a consideration?
A. Total capture storage space
B. Individual trace file size

C. Real-time packet decodes
D. Analyzer location
Answer: B