Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

WSA-101 MCQs
WSA-101 TestPrep
WSA-101 Study Guide
WSA-101 Practice Test
WSA-101 Exam Questions

killexams.com

Wireshark

WCA-101

Wireshark Certified Network Analyst

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/WCA-101

Question: 961

What is the correct tshark command to export all HTTP objects from a pcapng file named capture.pcapng to a directory named objects?

A. tshark -r capture.pcapng --export-objects http,objects
B. tshark -r capture.pcapng -z http,objects
C. tshark -r capture.pcapng --export http > objects
D. tshark -r capture.pcapng -F pcapng --http-export objects

Answer: A

Explanation: The correct command is tshark -r capture.pcapng --export-objects http,objects, which reads the pcapng file and exports all HTTP objects to the specified objects directory. The -z option is for statistics, not exporting objects, --export is not a valid option, and -F specifies file format, not object export.

Question: 962

In a Wireshark capture of an SMB session, slow performance is suspected. Which TCP parameters should be analyzed to determine if the network flow control contributes to delay?

A. TCP Window Size
B. TCP Urgent Pointer
C. TCP Sequence Number
D. TCP Timestamp Option

Answer: A,D

Explanation: TCP Window Size controls data flow and limits throughput. TCP Timestamps help assess RTT and network delays. Sequence Number relates to data order, while Urgent Pointer is rarely used and not relevant for flow delays in SMB.

Question: 963

Which display filter uses membership filters to show only DNS and DHCP traffic on their standard ports (53 and 67/68) for a specific subnet (192.168.1.0/24)?

A. (udp.port in {53 67 68}) && ip.addr == 192.168.1.0/24
B. (dns || dhcp) && ip.src == 192.168.1.0/24
C. udp.port in {53, 67, 68} && ip.addr == 192.168.1.0/24
D. (dns || dhcp) && ip.addr == 192.168.1.0/24

Answer: A

Explanation: The filter must use membership filters for DNS (udp.port == 53) and DHCP (udp.port == 67 or 68) and limit to the subnet (ip.addr == 192.168.1.0/24). A correctly uses udp.port in {53 67 68} and ip.addr. B uses protocol filters (dns || dhcp), which are less precise for port-specific traffic. C uses incorrect comma-separated syntax. D doesn't use membership filters and is less specific.

Question: 964

When following a UDP stream, you observe fragmented packets. Which Wireshark filter confirms if these fragments are correctly reassembled?

A. ip.reassembled
B. udp.fragment
C. udp.reassembled.in
D. ip.frag_offset > 0

Answer: C

Explanation: The filter "udp.reassembled.in" identifies packets where UDP fragments have been successfully reassembled by Wireshark, showing the frame where reassembly occurs. The filter "ip.reassembled" is not specific to UDP, and "udp.fragment" is not a valid filter. The filter "ip.frag_offset > 0" identifies fragments but does not confirm reassembly.

Question: 965

Given the following filter: !(ip.addr == 192.168.0.1 or tcp.port == 443) and udp, which packets will be displayed?

A. Packets that are UDP and neither from/to IP 192.168.0.1 nor using TCP port 443
B. Packets with IP 192.168.0.1 and UDP protocol only
C. Packets with TCP port 443 and that are UDP as well
D. Packets that are TCP with ports other than 443 or IP other than 192.168.0.1

Answer: A

Explanation: The NOT operates on the OR expression, negating it so neither condition can be true, combined with UDP protocol filter, so only UDP packets excluding those involving IP 192.168.0.1 or TCP port 443 are matched.

Question: 966

Which TCP option is used to pad the options field to align with a 32-bit boundary?

A. EOL
B. MSS

C. NOP
D. SACK

Answer: C

Explanation: The No Operation (NOP) option is used in TCP headers to pad the options field to align with a 32-bit boundary, ensuring proper formatting when other options are present. EOL marks the end of options, MSS sets the segment size, and SACK acknowledges specific byte ranges.

Question: 967

Which ICMPv4 message type and code would a router send if a packet's destination IP address matches a network that is administratively prohibited?

A. Type 3, Code 10
B. Type 3, Code 13
C. Type 5, Code 0
D. Type 11, Code 0

Answer: B

Explanation: An ICMPv4 Destination Unreachable message with Type 3 and Code 13 indicates "Communication Administratively Prohibited," sent when a packet is dropped due to a policy or firewall rule, such as an access control list (ACL) blocking the destination network.

Question: 968

In "Capture File Properties," which metric helps estimate the average packet size?

A. File Size divided by Total Packets
B. Maximum Packet Length field
C. Average Packet Duration
D. Capture Duration divided by Total Packets

Answer: A

Explanation: Average packet size estimate is obtained by dividing the capture file size by the total number of packets.

Question: 969

To optimize the Wireshark GUI for analyzing DNS anomalies, which layout adjustment ensures both Packet Details and Packet Bytes panes are equally sized and visible?

A. Go to View > Layout > Two Panes Equal

B. Drag divider to balance Packet Details and Packet Bytes panes
C. Select View > Interface Options > Equal Pane Distribution
D. Use View > Layout > Maximize Packet Details and Bytes

Answer: B

Explanation: Dragging the divider between the Packet Details and Packet Bytes panes allows manual adjustment to make them equally sized. Wireshark does not have specific menu options like Two Panes Equal or Equal Pane Distribution for this task.

Question: 970

To quickly add a column displaying the HTTP URI, which field name should be used in the column preferences?

A. http.request.uri
B. http.user_agent
C. tcp.stream
D. ip.proto

Answer: A

Explanation: The field http.request.uri corresponds exactly to the URI requested in HTTP traffic, making it ideal for dedicated columns. The others refer to user agents, TCP stream numbers, or IP protocol types.

Question: 971

Which of the following DHCP requests indicates a client restarting and trying to obtain a new IP address after a power cycle?

A. DHCPREQUEST with server identifier for renewal
B. DHCPDISCOVER broadcast message
C. DHCPDECLINE broadcast message
D. DHCPACK unicast message

Answer: B

Explanation: After a reboot, a client sends DHCPDISCOVER broadcast to find available servers.

Question: 972

After applying "Decode As" for TCP port 8443 as HTTPS, which Wireshark field confirms the protocol change?

A. Protocol column shows "TLS" or "SSL" instead of "TCP"
B. Info column shows "Encrypted Application Data"

C. Packet bytes pane shows decrypted payload automatically
D. Service names in Transport layer update to HTTPS

Answer: A,B

Explanation: Protocol column changes to TLS/SSL after decoding port 8443 as HTTPS; Info column reflects encrypted data indication. Payload is not decrypted automatically with Decode As.

Question: 973

What steps are required to create a new Wireshark profile with a custom display filter for SMB protocol analysis?

A. Edit > Configuration Profiles > New > Name "SMB_Analysis" > Set Filter to "smb"
B. File > New Profile > Name "SMB_Analysis" > Add smb Filter
C. Tools > Profile Editor > Create > SMB_Analysis > Apply smb Filter
D. View > Profiles > Add > SMB_Analysis > Set smb Filter

Answer: A

Explanation: To create a new profile, go to Edit > Configuration Profiles, click New, name it "SMB_Analysis," and set a display filter like "smb" in the profile settings. Other options do not align with Wireshark's profile creation process.

Question: 974

Which command or expression would you use in the Wireshark filter toolbar to locate all packets marked by the user?

A. _ws.marked == 1
B. tcp.flags.ack == 1
C. frame.marked == 1
D. ip.addr == 127.0.0.1

Answer: C

Explanation: The correct filter syntax to show all marked packets is frame.marked == 1. _ws.marked is incorrect, tcp.flags.ack filters for TCP ACK flags, and ip.addr is used for filtering IP addresses.

Question: 975

Which of the following filters can be used to create an I/O graph showing bits per second only for UDP traffic?

A. udp
B. udp && frame.len>0

C. udp.port==53
D. frame.protocols contains udp

Answer: A

Explanation: The simple filter "udp" matches all UDP packets; the other filters are either too specific or redundant for this use.

Question: 976

When using the display filter "tcp.port in {80 443}", you observe excess packets that include non-HTTP/HTTPS traffic on these ports. What is the most likely cause?

A. The filter includes TCP control packets without application-layer data
B. The filter captures all TCP traffic regardless of protocol
C. The filter is misconfigured and captures UDP traffic
D. The filter includes packets from other protocols using ports 80 or 443

Answer: D

Explanation: The filter tcp.port in {80 443} captures all TCP traffic on ports 80 or 443, which may include non-HTTP/HTTPS protocols if other applications use these ports. A is incorrect as control packets are expected but not the primary issue. B is incorrect as the filter is port-specific. C is incorrect as the filter specifies TCP, not UDP.

Question: 977

You are analyzing a DHCPv4 packet in Wireshark and notice the Option 3 field. What does this option represent?

A. Default Gateway
B. DNS Server
C. Subnet Mask
D. Time Server

Answer: A

Explanation: In DHCPv4, Option 3 specifies the Default Gateway (router) address provided to the client. Option 6 is for DNS servers, Option 1 is for the subnet mask, and Option 4 is for time servers.

Question: 978

To locate packets with high TCP round-trip time (RTT) using the minimap, which filter should be applied before scrolling the sidebar?

A. tcp.analysis.ack_rtt > 0.1

B. tcp.time_delta > 0.1
C. tcp.window_size < 1000
D. tcp.flags.syn == 1

Answer: A

Explanation: The filter "tcp.analysis.ack_rtt > 0.1" identifies packets with RTT greater than 100ms, which will be highlighted in the minimap for quick location. "tcp.time_delta" measures inter-packet time, not RTT. Window size and SYN flags are unrelated to RTT.

Question: 979

Which command-line tool supports reading pcapng files for export operations?

A. tshark
B. tcpdump
C. traceroute
D. ping

Answer: A

Explanation: TShark supports pcapng files; tcpdump does not fully support pcapng files.

Question: 980

In the Statistics > Conversations window, you identify a VoIP conversation using SIP between 192.168.1.5:5060 and 10.0.0.10:5060. Which filter isolates this conversation?
A. sip && ip.addr == 192.168.1.5 && ip.addr == 10.0.0.10 && udp.port == 5060
B. (ip.src == 192.168.1.5 && ip.dst == 10.0.0.10 && udp.srcport == 5060 && udp.dstport == 5060) || (ip.src == 10.0.0.10 && ip.dst == 192.168.1.5 && udp.srcport == 5060 && udp.dstport == 5060)
C. udp && ip.src == 192.168.1.5 && ip.dst == 10.0.0.10 && udp.port == 5060
D. sip.conversation == (192.168.1.5:5060, 10.0.0.10:5060)

Answer: B

Explanation: To isolate a SIP-based VoIP conversation between 192.168.1.5:5060 and 10.0.0.10:5060 from the Statistics > Conversations window, the filter must capture both directions of the UDP conversation, including specific ports. The filter (ip.src == 192.168.1.5 && ip.dst == 10.0.0.10 && udp.srcport == 5060 && udp.dstport == 5060) || (ip.src == 10.0.0.10 && ip.dst == 192.168.1.5 && udp.srcport == 5060 && udp.dstport == 5060) correctly captures both directions. The filter sip && ip.addr == 192.168.1.5 && ip.addr == 10.0.0.10 && udp.port == 5060 is incorrect because it requires both IP addresses and ports in the same packet. The filter udp && ip.src == 192.168.1.5 && ip.dst == 10.0.0.10 && udp.port == 5060 only captures one direction and does not ensure SIP traffic. The filter sip.conversation == (192.168.1.5:5060, 10.0.0.10:5060) is invalid, as Wireshark does not support a sip.conversation field.

Question: 981

When using the 'Colorize Conversation' feature to track an HTTP session, which of the following steps ensures accurate tracking?

A. Right-click a packet, select "Colorize Conversation," and choose "TCP"
B. Apply a display filter like "http" before colorizing
C. Select "Colorize Conversation" > "IP" to track all HTTP sessions on the same IP pair
D. Use the filter "tcp.stream eq " after colorizing

Answer: A,D

Explanation: To track an HTTP session, right-click a packet and select "Colorize Conversation" > "TCP" to colorize the specific TCP stream. After colorizing, applying "tcp.stream eq " isolates the conversation. Filtering by "http" first is unnecessary, and IP-based colorizing may include unrelated sessions.

Question: 982

Which IP header field differentiates packets belonging to fragmented messages?

A. Identification
B. Protocol
C. TTL
D. Header Length

Answer: A

Explanation: The Identification field is used to uniquely identify fragments of the same original packet for reassembly.

Question: 983

In a capture with 200,000 packets, you need to decode UDP port 123 as NTP. Which "Decode As" rule is correct?

A. Analyze > Decode As > Add rule: UDP, Port 123, Decode as NTP
B. Edit > Preferences > Protocols > NTP > Add 123 to "UDP ports"
C. View > Name Resolution > Add custom port mapping: UDP 123 to NTP
D. View > Name Resolution > Enable "Resolve transport addresses"

Answer: A

Explanation: To decode UDP port 123 as NTP, use Analyze > Decode As, add a rule for UDP, port 123, and select NTP as the decode type. Other options modify protocol settings, reference invalid mappings, or enable unrelated resolution.

Question: 984

Which methods can be used to create a Display Filter to isolate TCP packets with a window size less than 1024 bytes from a specific IP (192.168.0.1)?

A. Drag the "tcp.window_size" field and combine with "ip.src == 192.168.0.1"
B. Manually enter "tcp.window_size < 1024 && ip.src == 192.168.0.1"
C. Right-click the window size field and select "Apply as Filter"
D. Use the Expression Builder to select "tcp.window_size" and "ip.src"

Answer: A,B,D

Explanation: Valid methods include dragging the "tcp.window_size" field and combining it with "ip.src == 192.168.0.1", manually entering "tcp.window_size < 1024 && ip.src == 192.168.0.1", and using the Expression Builder to select "tcp.window_size" and "ip.src". Right-clicking the window size field and selecting "Apply as Filter" applies the filter for the specific packet's window size, not necessarily less than 1024 or combined with the IP condition.

Question: 985

When following a TCP stream, you observe a client sending multiple HTTP POST requests without responses. Which filter confirms if the server sent RST packets?

A. tcp.flags == 0x004
B. tcp.flags.reset == 1
C. tcp.rst == 1
D. tcp.stream == && tcp.flags == 0x014

Answer: B

Explanation: The filter "tcp.flags.reset == 1" isolates packets with the RST flag set, confirming if the server sent RST packets to terminate the connection. The filter "tcp.flags == 0x004" is equivalent but less readable. There is no "tcp.rst" filter, and "tcp.flags == 0x014" matches RST and ACK, which is not specific to RST-only packets.

Question: 986

Which IPv4 header field specifies the length of the entire packet, including header and data, and what is its maximum value in bytes?

A. Total Length; 65,535
B. Total Length; 1,500
C. Payload Length; 65,535
D. Payload Length; 1,500

Answer: A

Explanation: The Total Length field in the IPv4 header specifies the entire packet's length, including the header and data, in bytes. As a 16-bit field, its maximum value is 65,535 bytes. Payload Length is not an IPv4 field, and 1,500 is a typical MTU, not the maximum.

Question: 987

Which Tshark command captures traffic on interface eth0, saving to "capture.pcapng" with a ring buffer of 20 files, each 10 MB, and stops after 1 hour?

A. tshark -i eth0 -w capture.pcapng -b files:20 -b filesize:10000 -a duration:3600
B. tshark -i eth0 -w capture.pcapng -b files:20 -b filesize:10M -a duration:3600
C. tshark -i eth0 -w capture.pcapng -b filesize:10000 -b files:20 -a time:3600
D. tshark -i eth0 -w capture.pcapng -b files:20 -b filesize:10000 -a duration:1h

Answer: A

Explanation: The command tshark -i eth0 -w capture.pcapng -b files:20 -b filesize:10000 -a duration:3600 sets a ring buffer with 20 files, each 10 MB (10,000 KB), and stops after 1 hour (3600 seconds) using -a duration:3600. Option B uses an invalid filesize unit (10M). Option C uses an invalid -a time parameter. Option D's duration:1h is not a valid Tshark duration format.

Question: 988

You observe an ICMPv6 Neighbor Advertisement message with the Router flag set to 1. What does that imply about the sender?

A. The sender is a host only
B. The sender can act as a router
C. The sender is signaling for duplicate address detection
D. The sender has invalid link-layer info

Answer: B

Explanation: The Router flag in a Neighbor Advertisement set to 1 signals that the sender is a router on the network.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.