CYBS 7357 Lab 01 Quiz

\* Answers are highlighted in yellow

1. Which of the following statements is true regarding Wireshark?

a. Wireshark is probably the most widely used packet capture and analysis software in the world.

b. The expense of Wireshark makes it cost-prohibitive for most organizations.

c. Compared to similar commercial products, Wireshark has the most sophisticated diagnostic tools.

d. Wireshark saves frame details in a format that is incompatible and unusable by other software tools.

2. The main screen of Wireshark includes several shortcuts. Which shortcut category displays a list of the network interfaces, or machines, that Wireshark has identified, and from which packets can be captured and analyzed?

a. Capture Help

b. Capture

c. Files

d. Online

3. Which of the following enables Wireshark to capture packets destined to any host on the same subnet or virtual LAN (VLAN)?

a. Capture Help

b. Host mode

c. Subnet mode

d. Promiscuous mode

4. The top pane of the Wireshark window, referred to as the \_\_\_\_\_\_\_\_\_\_, contains all of the packets that Wireshark has captured, in time order, and provides a summary of the contents of the packet in a format close to English.

a. data summary

b. hex pane

c. frame detail

d. frame summary

5. The middle pane of the Wireshark window, referred to as the \_\_\_\_\_\_\_\_\_\_, is used to display the packet structure and contents of fields within the packet.

a. data summary

b. hex pane

c. frame detail

d. frame summary

6. The bottom pane of the Wireshark window, referred to as the \_\_\_\_\_\_\_\_\_\_, displays all of the information in the packet in hexadecimal and in decimal when possible.

a. data summary

b. hex pane

c. frame detail

d. frame summary

7. Wireshark can be used in a variety of ways; however, the most common configuration for Wireshark, and the configuration that you ran in the lab, has the software running:

a. in a peer-to-peer configuration.

b. from a probe or hub.

c. on a local area network.

d. on a local host.

8. In the simplest terms, Wireshark is used to capture all packets:

a. from a computer workstation to the Wireshark application window.

b. to and from a computer workstation and the Wireshark application window.

c. to and from a computer workstation and the server.

d. to and from the Wireshark Network Analyzer and the Capture section of the Wireshark application window.

9. Which of the following statements is true regarding how Wireshark works?

a. Where packets are captured and how they are captured does not have any impact on how the packets are analyzed.

b. By running the Wireshark software on the same computer that generates the packets, the capture is specific to that machine.

c. Wireshark has no impact on the operation of the machine itself or its applications.

d. No timing information is provided when using a network probe or hub device, or the capture port of a LAN switch.

10. Which of the following statements is true regarding how Wireshark handles time?

a. Clock time may or may not be the same as the system time of the device or devices used to run Wireshark and capture packets.

b. The timestamp used by Wireshark is the current local time in the time zone where the machine resides.

c. Any discrepancies regarding time are insignificant when capturing packets from high-speed interfaces.

d. In order to overcome time zone mismatches, a common best practice is to use the Eastern Time Zone.

11. When examining a frame header, a difference between bytes on the wire and bytes captured can indicate that:

a. all packets are being captured effectively.

b. partial or malformed packets might be captured.

c. the interface speed is low and the computer cannot keep up with Wireshark.

d. the computer is infected with some form of malware.

12. In the lab, the Ethernet II detail of the provided packet capture file indicated that Wireshark had determined that the \_\_\_\_\_\_\_\_\_\_ was Intel Core hardware.

a. frame type

b. source

c. destination

d. type of traffic carried in the next layer

13. In the lab, the Ethernet II detail of the provided packet capture file indicated that Wireshark had determined that the \_\_\_\_\_\_\_\_\_\_ was Internet Protocol (IP).

a. frame type

b. source

c. destination

d. type of traffic carried in the next layer

14. In the lab, the Ethernet II detail of the provided packet capture file indicated that Wireshark had determined that the \_\_\_\_\_\_\_\_\_\_ was IPv4 multicast.

a. frame type

b. source

c. destination

d. type of traffic carried in the next layer

15. The \_\_\_\_\_\_\_\_\_\_ IP address is the IP address of the local IP host (workstation) from which Wireshark captures packets.

a. origination

b. destination

c. host

d. source

16. Which of the following statements is true regarding filtering packets in Wireshark?

a. Filters are not a particularly useful tool in Wireshark.

b. Filters allow a complex set of criteria to be applied to the captured packets and only the result is displayed.

c. Filter expressions must be built with the Filter Edit dialog window and cannot be typed directly into the Filter field.

d. Once packets have been filtered, they are lost and cannot be restored.

17. Selecting a TCP flow in the Flow Graph Analysis tool tells Wireshark that you wanted to see all of the elements in a TCP three-way handshake, which are:

a. SYN, SYN-ACK, and ACK.

b. SYN, ACK-SYN, and PSH.

c. ACK, ACK-PSH, and PSH-ACK.

d. PSH-ACK, ACK, and PSH-ACK.

18. In the center pane of the \_\_\_\_\_\_\_\_\_\_, the direction of each arrow indicates the direction of the TCP traffic, and the length of the arrow indicates between which two addresses the interaction is taking place.

a. Wireshark frame header

b. Flow Graph Analysis results

c. Frame Summary pane

d. Ethernet II frame detail

19. Within the frame detail pane, what does it mean when the DNS Flags detail specifies that recursion is desired?

a. DNS will continue to query higher level DNSs until it is able to resolve the address.

b. DNS will continue to query lower level DNSs until it is able to resolve the address.

c. DNS will discontinue querying other DNSs in attempts to resolve the address.

d. DNS will be guaranteed show the response “No such name.”

20. Within the frame detail pane, the DNS Flags detail response to the query for issaseries.org was “No such name,” indicating that the:

a. issaseries.org domain never existed.

b. issaseries.org domain existed at one time but no longer exists.

c. issaseries.org is not known to any of the Domain Name Servers that were searched.

d. search was ineffective or unsuccessful.

NAME:

Natnael kebede