

✔ Congratulations! You passed!

Grade
received 86.20%

Latest Submission
Grade 86.21%

To pass 80% or
higher

Go to next item

1. A network is defined as a what?

1 / 1 point

- ☐ A collection of programs linked together for communication and sharing of data and other resources
- ☒ A collection of computers linked together for communication and sharing of data and other resources
- ☐ a collection of files linked together for communication and sharing of data and other resources
- ☐ A collection of networks linked together for communication and sharing of data and other resources

✔ Correct

A computer network is a collection of computers linked together for communication and sharing of data and other resources

2. A LAN is a what?

1 / 1 point

- ☒ Local Area Network
- ☐ Long Area Network
- ☐ Legal Area Network
- ☐ Large Area Network

✔ Correct

A LAN is a local area network.

3. A packet has a header, a footer and a payload. The payload contains what?

1 / 1 point

- ☒ The packet data
- ☐ A CRC redundancy check
- ☐ Destination IP address
- ☐ The source IP address

✔ Correct

Payload is the packet's data.

4. Routers use what to route packets to their destination?

1 / 1 point

- ☐ MAC addresses
- ☒ IP addresses
- ☐ DNS
- ☐ ARP

✔ Correct

Routers use IP addresses to route packets to their destination.

5. _____ have multiple connections. They pass on anything received on one connection to all other connections (no filtering by IP or MAC address).

1 / 1 point

- ☐ Ports
- ☒ Hubs
- ☐ Routers
- ☐ Switches

✔ Correct

Hubs have multiple connections; they pass on anything received on one connection to all other connections (no filtering by IP or MAC address).

6. Switches use what to route packets to their destination address?

0 / 1 point

- ☐ MAC addresses
- ☐ Ports
- ☒ IP addresses
- ☐ ARP

Incorrect

7. IPv4 is a set of ___ numbers (32 bits) separated by dots in sets of three.

0 / 1 point

- ☐ 5
- ☒ 3
- ☐ 14
- ☐ 12

Incorrect

8. NAT translates the _____ of devices in a local network to a single public IP address and vice versa

1 / 1 point

- ☒ Private IP addresses
- ☐ MAC addresses
- ☐ Port numbers
- ☐ Public IP address

Correct

NAT translates the private IP addresses of devices in a local network to a single public IP address and vice versa.

9. What translates the alphanumeric web address into an IP address or vice versa?

1 / 1 point

- ☐ ARP
- ☒ DNS
- ☐ Port forwarding
- ☐ FTP

Correct

DNS (Domain Name Service) translates the alphanumeric web address into an IP address or vice versa.

10. A _____ address is a hardware identification number that uniquely identifies each device on a network.

1 / 1 point

- ☐ DNS
- ☐ IP
- ☐ ARP
- ☒ MAC

Correct

A MAC address is a hardware identification number that uniquely identifies each device on a network.

11. A _____ is a set of rules that dictate how data is transmitted between devices in a network.

1 / 1 point

- ☐ Internet protocol
- ☐ Hub protocol
- ☒ Network protocol
- ☐ Router protocol

Correct

A network protocol is a set of rules that dictate how data is transmitted between devices in a network.

12. What is the principal communications protocol in the internet protocol suite for relaying data across network boundaries?

1 / 1 point

- ☒ IP
- ☐ UDP
- ☐ SMTP
- ☐ FTP

Correct

IP is the principal communications protocol in the internet protocol suite for relaying data across network boundaries.

13. _____ is a communications standard that allows computing devices to exchange messages over a network.

1 / 1 point

- ☐ CPU

- ☐ DNS
- ☒ TCP
- ☐ UDP

✓ **Correct**

The Transmission Control Protocol (TCP) is a communications standard that allows computing devices to exchange messages over a network.

14. TCP is a _____-oriented protocol.

1 / 1 point

- ☒ Connection
- ☐ UDP
- ☐ Connection-less
- ☐ Network

✓ **Correct**

TCP is a connection-oriented protocol.

15. _____ is a connectionless protocol and doesn't guarantee delivery.

1 / 1 point

- ☐ HTTP
- ☐ TCP
- ☒ UDP
- ☐ FTP

✓ **Correct**

UDP (used datagram protocol) is a connectionless protocol and doesn't guarantee delivery.

16. _____ is a protocol used to map IP addresses to the hardware addresses (MAC addresses).

1 / 1 point

- ☐ IP
- ☐ TCP
- ☒ ARP
- ☐ UDP

✓ **Correct**

ARP is a protocol used to map IP addresses to the hardware addresses (MAC addresses).

17. _____ is the lowest layer of the OSI Model. It covers electrical and physical compounds of the system, including cables and the radio frequency link (as in an 802.11 wireless systems).

1 / 1 point

- ☒ Physical layer
- ☐ Transport layer
- ☐ Data Link Layer
- ☐ Network layer

✓ **Correct**

The physical layer is the lowest layer of the OSI Model, including electrical and physical compounds of the system such as cables and radio frequency link (as in an 802.11 wireless systems).

18. What is NOT something a forensic examiner needs to consider when developing a keyword search list?

0 / 1 point

- ☐ The computer operating system
- ☐ Elements of the allegation
- ☒ Suspect's personal information
- ☐ Existing leads and associates

✗ **Incorrect**

19. What are the two categories of keywords?

1 / 1 point

- ☐ File and directory types
- ☐ The suspect's personal information
- ☒ Case-specific keywords and generic case keywords
- ☐ The NSRL and notables

✓ **Correct**

There are two categories of keywords: generic case keywords and case-specific keywords.

20. Generic case keywords are what?

1 / 1 point

- ☐ A large list of keywords
- ☐ Keywords that are specific to one certain case
- ☐ A large list of hash values
- ☒ Keywords that can be used to search for in any case of a certain type

✓ **Correct**
Generic case keywords are ones that you can search for in any case of a certain type.

21. Case-specific keywords are what?

1 / 1 point

- ☐ A keyword list with hash values
- ☐ An alphanumeric keyword list
- ☐ Keywords that relate to a case of a certain type
- ☒ Keywords that relate to one specific case

✓ **Correct**
Case-specific keywords are keywords that relate to one specific case.

22. The limitations of keyword searches do NOT include what?

0 / 1 point

- ☒ Bit-shifted
- ☐ Encrypted
- ☐ Compressed
- ☐ Plaintext

✗ **Incorrect**

23. This regular expression below can be used to locate what? `grep '([0-9]{3})||[0-9]{3}[-.]?[0-9]{3}[-.]?[0-9]{4}' Test.txt`

1 / 1 point

- ☐ IP addresses
- ☐ MAC addresses
- ☒ Phone numbers
- ☐ URLs

✓ **Correct**
Phone number (grep) example: `grep '([0-9]{3})||[0-9]{3}[-.]?[0-9]{3}[-.]?[0-9]{4}' phone_numbers.txt`

24. Report writing preparation includes what?

1 / 1 point

- ☐ Using a write blocker
- ☐ Using grep searches
- ☐ A search warrant
- ☒ Good note-taking

✓ **Correct**
Part of preparing to write a good report includes good note-taking.

25. Parts of a written report include what?

1 / 1 point

- ☐ Photos
- ☐ Files and folders
- ☒ Narrative and exhibits
- ☐ Search warrant

✓ **Correct**
Parts of a report include a narrative; what you did and what you found; exhibits; and interpretation of findings.

26. Reporting considerations do NOT include what?

1 / 1 point

- ☐ Software tools and versions used during the exam
- ☐ Supporting your opinions with artifacts
- ☐ Answering all investigative questions
- ☒ A list of every file in the case

✓ **Correct**
Reporting considerations do NOT include: answering all investigative questions; supporting your opinions with artifacts; the software tools and versions used; explaining everything in the report; and omitting any

mistakes made.

27. A consideration when using software tool generated reports is what?

1 / 1 point

- ☐ These reports are very costly
- ☐ These reports are not customizable
- ☐ These reports are hard to generate
- ☒ These reports may contain unneeded and/or unwanted information

✔ **Correct**

Considerations when using software tool-generated reports are: these reports may contain unneeded and or unwanted information; and that most are very technical.

28. Peer review is defined as what?

1 / 1 point

- ☐ Allowing a peer to write the case report
- ☐ When the same investigator proofreads their own report
- ☐ An evaluation conducted by a less qualified examiner of reports, notes, data, conclusions and other documents
- ☒ An evaluation conducted by a second qualified examiner of reports, notes, data, conclusions and other documents

✔ **Correct**

SWEDG defines peer review as: "An evaluation conducted by a second qualified examiner of reports, notes, data, conclusions and other documents."

29. _____ are a known technique for reducing errors.

1 / 1 point

- ☐ Well-written reports
- ☐ Hash values
- ☒ Peer reviews
- ☐ Software tool-generated reports

✔ **Correct**

Peer reviews are a known technique for reducing errors.