# Free Questions for 200-201 by vceexamstest

## Shared by Bishop on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

# Question 1

**Question Type: MultipleChoice**

During which phase of the forensic process are tools and techniques used to extract information from the collected data?

## Options:

**A-** investigation

**B-** examination

**C-** reporting

**D-** collection

## Answer:

D

# Question 2

**Question Type: MultipleChoice**

An engineer must compare NIST vs ISO frameworks The engineer deeded to compare as readable documentation and also to watch a comparison video review. Using Windows 10 OS. the engineer started a browser and searched for a NIST document and then opened a new tab in the same browser and searched for an ISO document for comparison

The engineer tried to watch the video, but there 'was an audio problem with OS so the engineer had to troubleshoot it At first the engineer started CMD and looked fee a driver path then locked for a corresponding registry in the registry editor The engineer enabled "Audiosrv" in task manager and put it on auto start and the problem was solved Which two components of the OS did the engineer touch? (Choose two)

## Options:

**A-** permissions

**B-** PowerShell logs

**C-** service

**D-** MBR

**E-** process and thread

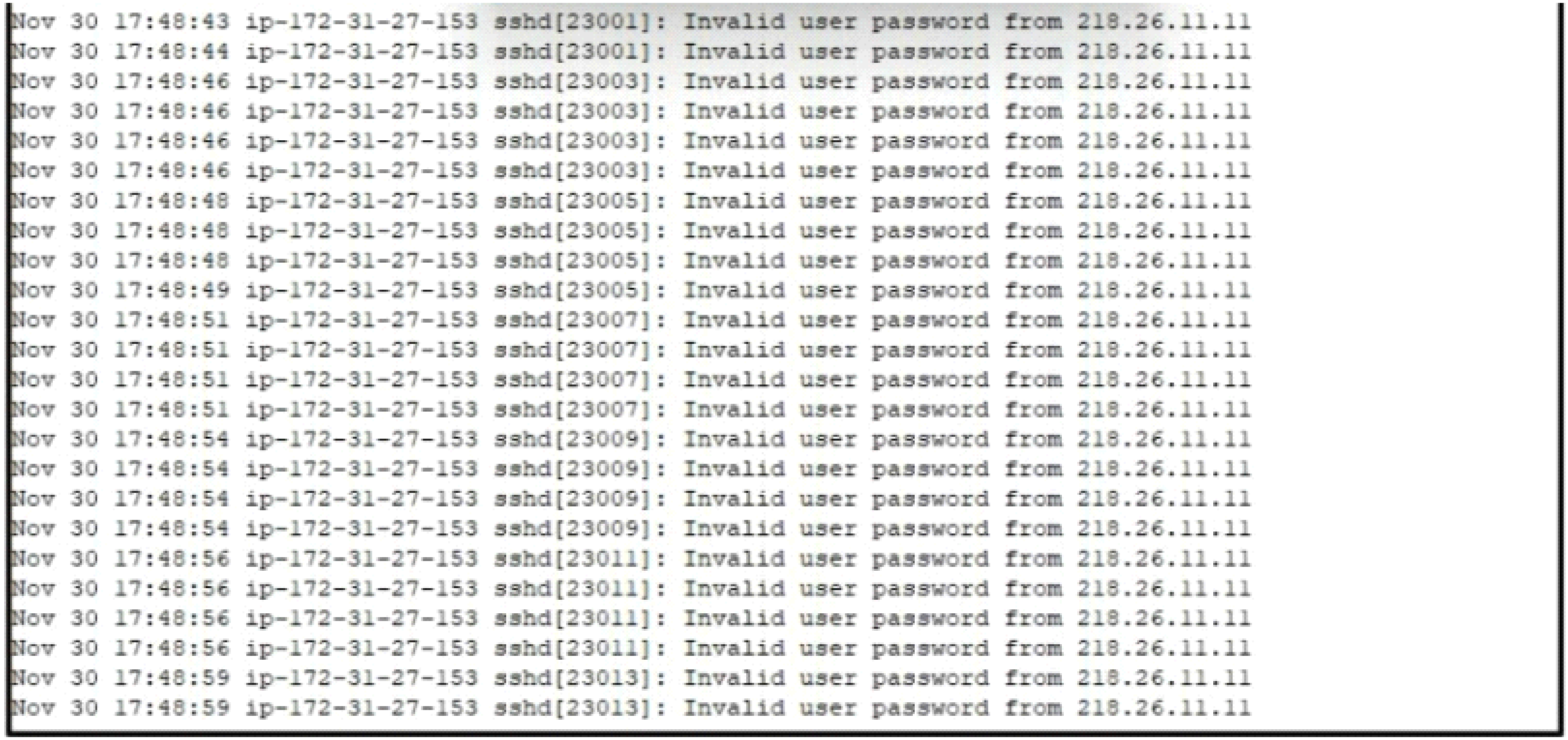
## Answer:

A, C

# Question 3

**Question Type:** MultipleChoice

Refer to the exhibit.



```
Nov 30 17:48:43 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:44 ip-172-31-27-153 sshd[23001]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:46 ip-172-31-27-153 sshd[23003]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:48 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:49 ip-172-31-27-153 sshd[23005]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:51 ip-172-31-27-153 sshd[23007]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:54 ip-172-31-27-153 sshd[23009]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:56 ip-172-31-27-153 sshd[23011]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
Nov 30 17:48:59 ip-172-31-27-153 sshd[23013]: Invalid user password from 218.26.11.11
```

A security analyst is investigating unusual activity from an unknown IP address Which type of evidence is this file1?

## Options:

**A-** indirect evidence

**B-** best evidence

**C-** corroborative evidence

**D-** direct evidence

## Answer:

A

# Question 4

**Question Type:** **MultipleChoice**

An engineer received a flood of phishing emails from HR with the source address HRjacobm@companycom. What is the threat actor in this scenario?

## Options:

**A-** phishing email

**B-** sender

**C-** HR

**D-** receiver

### Answer:

B

## Question 5

**Question Type:** **MultipleChoice**

What is the difference between vulnerability and risk?

### Options:

**A-** A vulnerability is a sum of possible malicious entry points, and a risk represents the possibility of the unauthorized entry itself.

**B-** A risk is a potential threat that an exploit applies to, and a vulnerability represents the threat itself

**C-** A vulnerability represents a flaw in a security that can be exploited, and the risk is the potential damage it might cause.

**D-** A risk is potential threat that adversaries use to infiltrate the network, and a vulnerability is an exploit

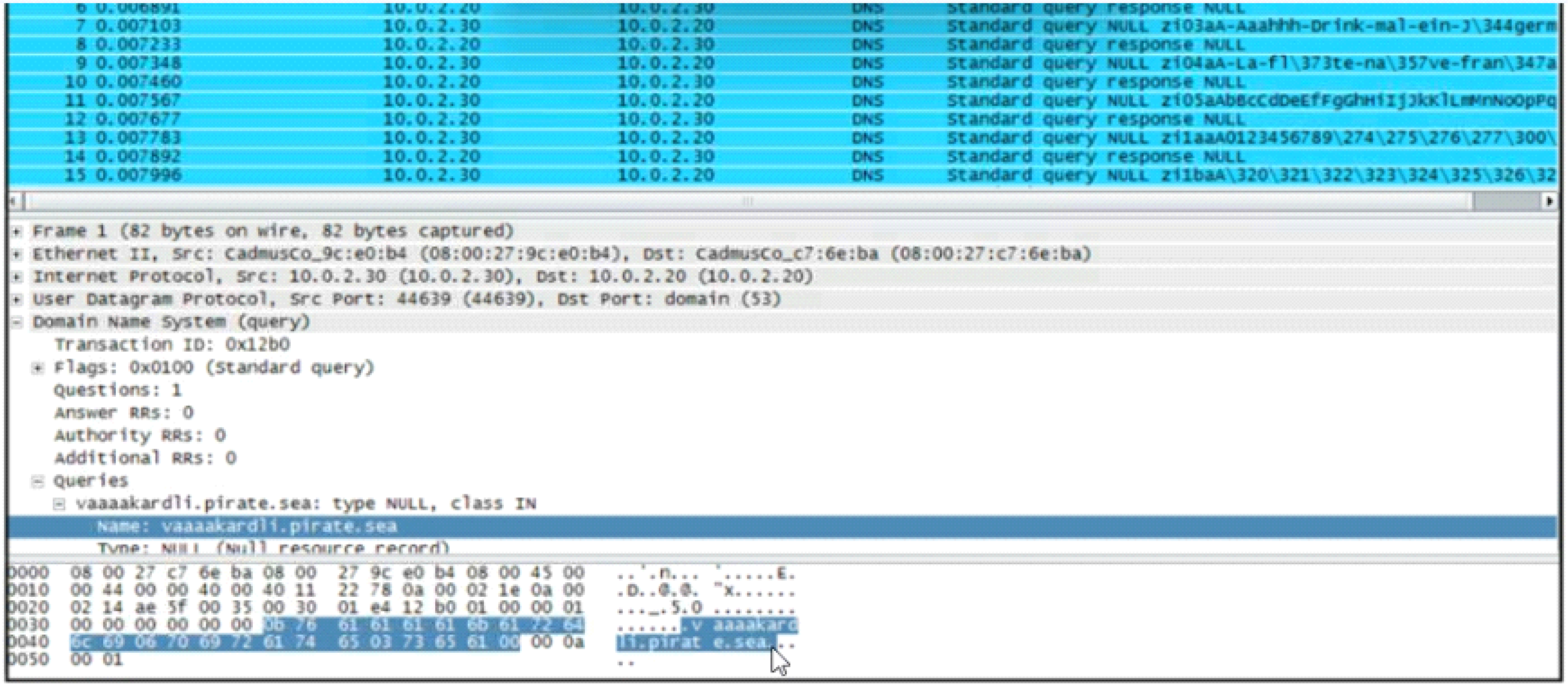
### Answer:

C

# Question 6

**Question Type:** **MultipleChoice**

Refer to the exhibit.



```
 6 0.006891   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
 7 0.007103   10.0.2.30   10.0.2.20   DNS   Standard query NULL zi03aA-Aaahhh-Drink-mal-ein-J\344germ
 8 0.007233   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
 9 0.007348   10.0.2.30   10.0.2.20   DNS   Standard query NULL zi04aA-La-fl\373te-na\357ve-fran\347a
10 0.007460   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
11 0.007567   10.0.2.30   10.0.2.20   DNS   Standard query NULL zi05aAbBcCdDeEfFgGhHiIjJkKlLmMnNoOpPq
12 0.007677   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
13 0.007783   10.0.2.30   10.0.2.20   DNS   Standard query NULL zi1aaA0123456789\274\275\276\277\300\
14 0.007892   10.0.2.20   10.0.2.30   DNS   Standard query response NULL
15 0.007996   10.0.2.30   10.0.2.20   DNS   Standard query NULL zi1baA\320\321\322\323\324\325\326\32
```

```
+ Frame 1 (82 bytes on wire, 82 bytes captured)
+ Ethernet II, Src: CadmusCo_9c:e0:b4 (08:00:27:9c:e0:b4), Dst: CadmusCo_c7:6e:ba (08:00:27:c7:6e:ba)
+ Internet Protocol, Src: 10.0.2.30 (10.0.2.30), Dst: 10.0.2.20 (10.0.2.20)
+ User Datagram Protocol, Src Port: 44639 (44639), Dst Port: domain (53)
- Domain Name System (query)
    Transaction ID: 0x12b0
  + Flags: 0x0100 (Standard query)
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  - Queries
    - vaaaakardli.pirate.sea: type NULL, class IN
        Name: vaaaakardli.pirate.sea
        Type: NULL (Null resource record)
```

```
0000  08 00 27 c7 6e ba 08 00  27 9c e0 b4 08 00 45 00   ..'.n...  '.....E.
0010  00 44 00 00 40 00 40 11  22 78 0a 00 02 1e 0a 00   .D..@.@.  "x......
0020  02 14 ae 5f 00 35 00 30  01 e4 12 b0 01 00 00 01   ..._.5.0  ........
0030  00 00 00 00 00 00 0b 76  61 61 61 61 6b 61 72 64   .......v  aaaakard
0040  6c 69 06 70 69 72 61 74  65 03 73 65 61 00 00 0a   li.pirat  e.sea...
0050  00 01                                              ..
```

What is occurring?

## Options:

**A-** ARP flood

**B-** DNS amplification

**C-** ARP poisoning

**D-** DNS tunneling

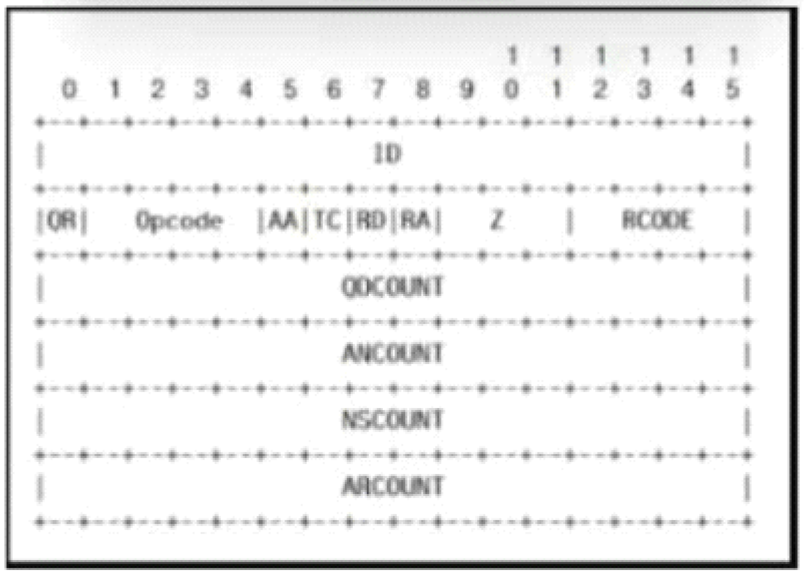
### Answer:

D

## Question 7

**Question Type:** **MultipleChoice**

Refer to the exhibit.



```
                                1  1  1  1  1  1
  0  1  2  3  4  5  6  7  8  9  0  1  2  3  4  5
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                      ID                       |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|QR|   Opcode  |AA|TC|RD|RA|   Z    |   RCODE   |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    QDCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ANCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    NSCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                    ARCOUNT                    |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Which field contains DNS header information if the payload is a query or a response?

## Options:

**A-** Z

**B-** ID

**C-** TC

**D-** QR

## Answer:

B

# Question 8

**Question Type:** **MultipleChoice**

What is the difference between deep packet inspection and stateful inspection?

## Options:

**A-** Deep packet inspection gives insights up to Layer 7, and stateful inspection gives insights only up to Layer 4.

**B-** Deep packet inspection is more secure due to its complex signatures, and stateful inspection requires less human intervention.

**C-** Stateful inspection is more secure due to its complex signatures, and deep packet inspection requires less human intervention.

**D-** Stateful inspection verifies data at the transport layer and deep packet inspection verifies data at the application layer

## Answer:

B

# Question 9

**Question Type:** **MultipleChoice**

Which metric in CVSS indicates an attack that takes a destination bank account number and replaces it with a different bank account number?

### Options:

**A-** availability

**B-** confidentiality

**C-** scope

**D-** integrity

### Answer:

D

## Question 10

**Question Type:** **MultipleChoice**

What is a difference between tampered and untampered disk images?

## Options:

**A-** Tampered images have the same stored and computed hash.

**B-** Tampered images are used as evidence.

**C-** Untampered images are used for forensic investigations.

**D-** Untampered images are deliberately altered to preserve as evidence

## Answer:

B

20%
DISCOUNT