1. Fill in the blank: _____ describes the amount of data that moves across a network. **1 / 1 point**

- ○ Data exfiltration
- ○ Traffic flow
- ◉ Network traffic
- ○ Network data

✓ **Correct**

2. Which of the following behaviors may suggest an ongoing data exfiltration attack? Select two answers. **1 / 1 point**

- ☑ Unexpected modifications to files containing sensitive data

✓ **Correct**

- ☐ Network performance issues
- ☐ Multiple successful multi-factor authentication logins
- ☑ Outbound network traffic to an unauthorized file hosting service

✓ **Correct**

3. What information do packet headers contain? Select three answers. **1 / 1 point**

- ☑ Protocols

✓ **Correct**

- ☐ Payload data
- ☑ IP addresses

✓ **Correct**

- ☑ Ports

✓ **Correct**

4. Fill in the blank: Network protocol analyzers can save network communications into files known as a _____. **1 / 1 point**

- ◉ packet capture
- ○ payload
- ○ protocol
- ○ network packet

✓ **Correct**

5. How do network protocol analyzers help security analysts analyze network communications? Select two answers. **1 / 1 point**

- ☑ They provide the ability to collect network communications.

✓ **Correct**

- ☑ They provide the ability to filter and sort packet capture information to find relevant information.

✓ **Correct**

- ☐ They take action to improve network performance.
- ☐ They take action to block network intrusions.

6. Which layer of the TCP/IP model does the Internet Protocol (IP) operate on? **1 / 1 point**

- ○ Network Access
- ◉ Internet
- ○ Transport
- ○ Application

✓ **Correct**

7. Which IPv4 header fields involve fragmentation? Select three answers. **1 / 1 point**

- ☑ Fragment Offset

✓ **Correct**

- ☐ Type of Service
- ☑ Identification

✓ **Correct**

- ☑ Flags

✓ **Correct**

8. What is the process of breaking down packets known as? **1 / 1 point**

- ○ Fragment Offset
- ○ Checksum
- ◉ Fragmentation
- ○ Flags

✓ **Correct**

9. Which tcpdump command outputs detailed packet information? **1 / 1 point**

- ○ `sudo tcpdump -v any -i`
- ○ `sudo tcpdump -i any -n`
- ○ `sudo tcpdump -i any -c 100`
- ◉ `sudo tcpdump -i any -v`

✓ **Correct**

10. Examine the following tcpdump output: **1 / 1 point**

```
22:00:19.538395 IP (tos 0x10, ttl 64, id 33842, offset 0, flags [P], proto TCP (6), length 196) 198.168.105.1.41012
> 198.111.123.1.61012: Flags [P.], cksum 0x50af (correct), seq 169, ack 187, win 501, length 42
```

What is the value of the Type of Service field?

- ○ `0x50af`
- ◉ `0x10`
- ○ `6`
- ○ `501`

✓ **Correct**