Lab 4x – Network-Based Incident Detection and Analysis

**1. What is the hostname and MAC address for the IP 10.0.0.201?**

Hostname: BLANCO-DESKTOP.local  
MAC Address: 00:16:17:18:66:c8

**2. What is the operating system used by the IP 10.0.0.201?**

Likely Windows 10 or 11. This is based on the NetBIOS hostname format and the presence of NetBIOS traffic

**3. What is the approximate time of the supposed incident / activity?**

The BitTorrent activity begins on July 15, 2018 at 00:17:37 UTC. This timestamp is visible in Frame 4520 of the PCAP file. (As shown in the screenshot below)

**4. Is there evidence that there is torrent activity?**

Yes. BitTorrent related traffic is evident in the capture.

**5. What files or programs are being utilized as part of the possible torrent activity?**

A torrent file named 'Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent' was downloaded.

**6. Is there evidence of illegal torrent activity?**

No. The file was downloaded from 'publicdomaintorrents.com', a legal site distributing public domain content. Therefore, this torrent activity is legal.

**7. What is the protocol used to identify the download?**

BitTorrent protocol for peer-to-peer activity and HTTP protocol for the initial .torrent metadata download.

**Wireshark Screenshots**

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

**Wireshark Screenshot - BitTorrent Traffic**

A screenshot of a computer

AI-generated content may be incorrect.

**Wireshark Screenshot - HTTP Stream 165 (.torrent file)**

A screenshot of a computer

AI-generated content may be incorrect.