**NWIT 291 – Cybersecurity Capstone**

**Hands-on Lab**

**Lab 4x - Network-Based Incident Detection and Analysis**

**Nimesh Giri**

**Montgomery College**

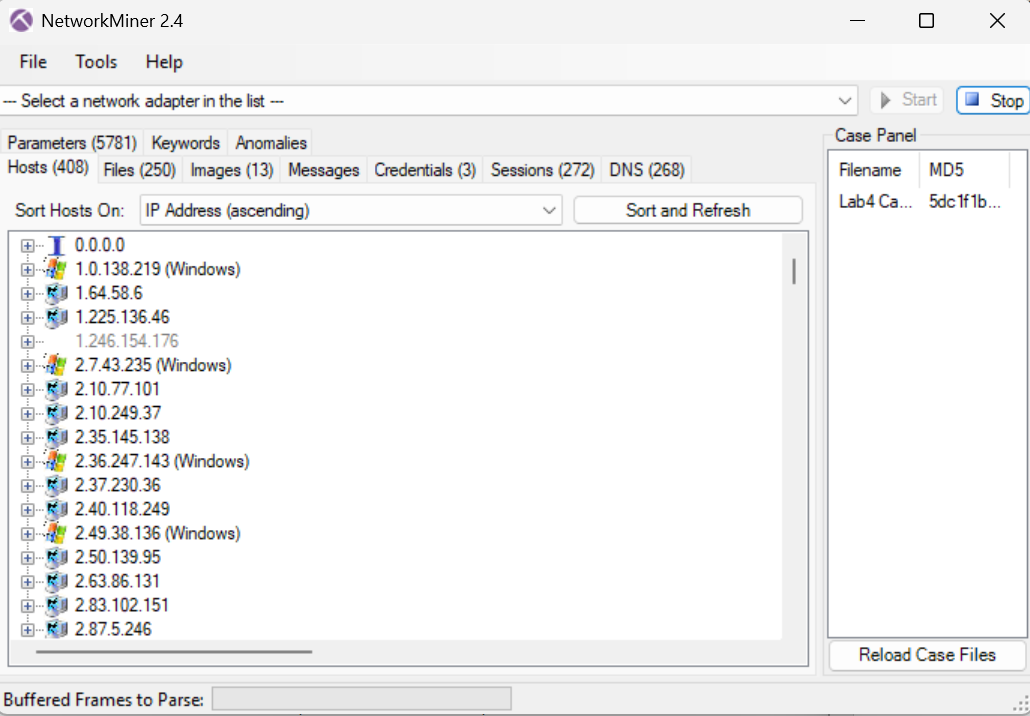
**NWIT-291-41341**

**Tesfaye Lemma**

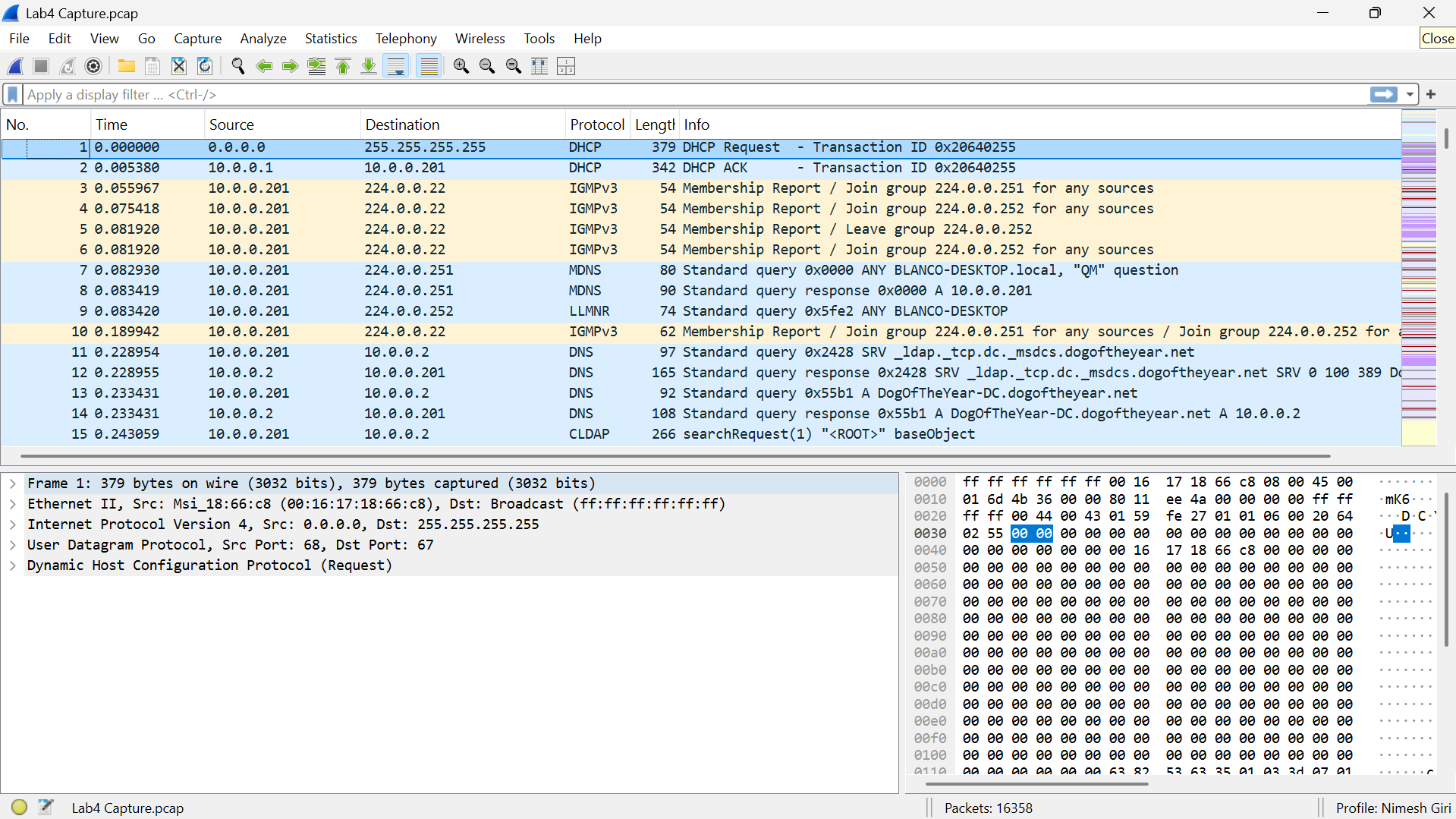
**Lab 4x - Network-Based Incident Detection and Analysis**

**1. Loading the PCAP file:**

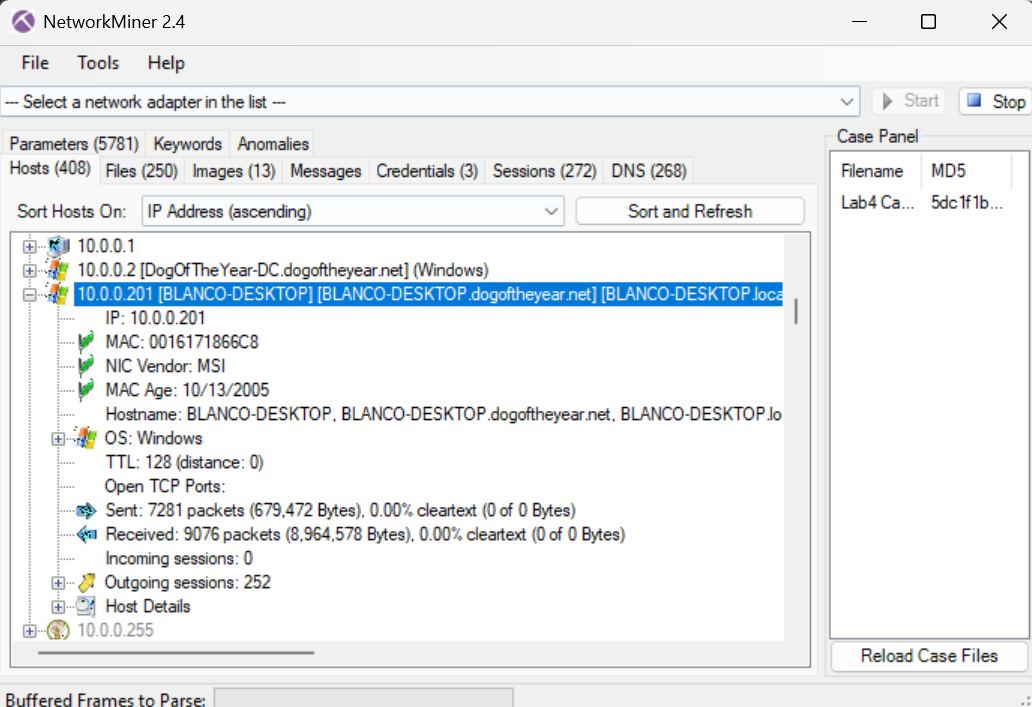
i) NetworkMiner



ii) Wireshark



**2. Identify a packet with either a source or destination of 10.0.0.201**



**Key Observations:**

The host 10.0.0.201 is identified as BLANCO-DESKTOP, a Windows machine on the local network.

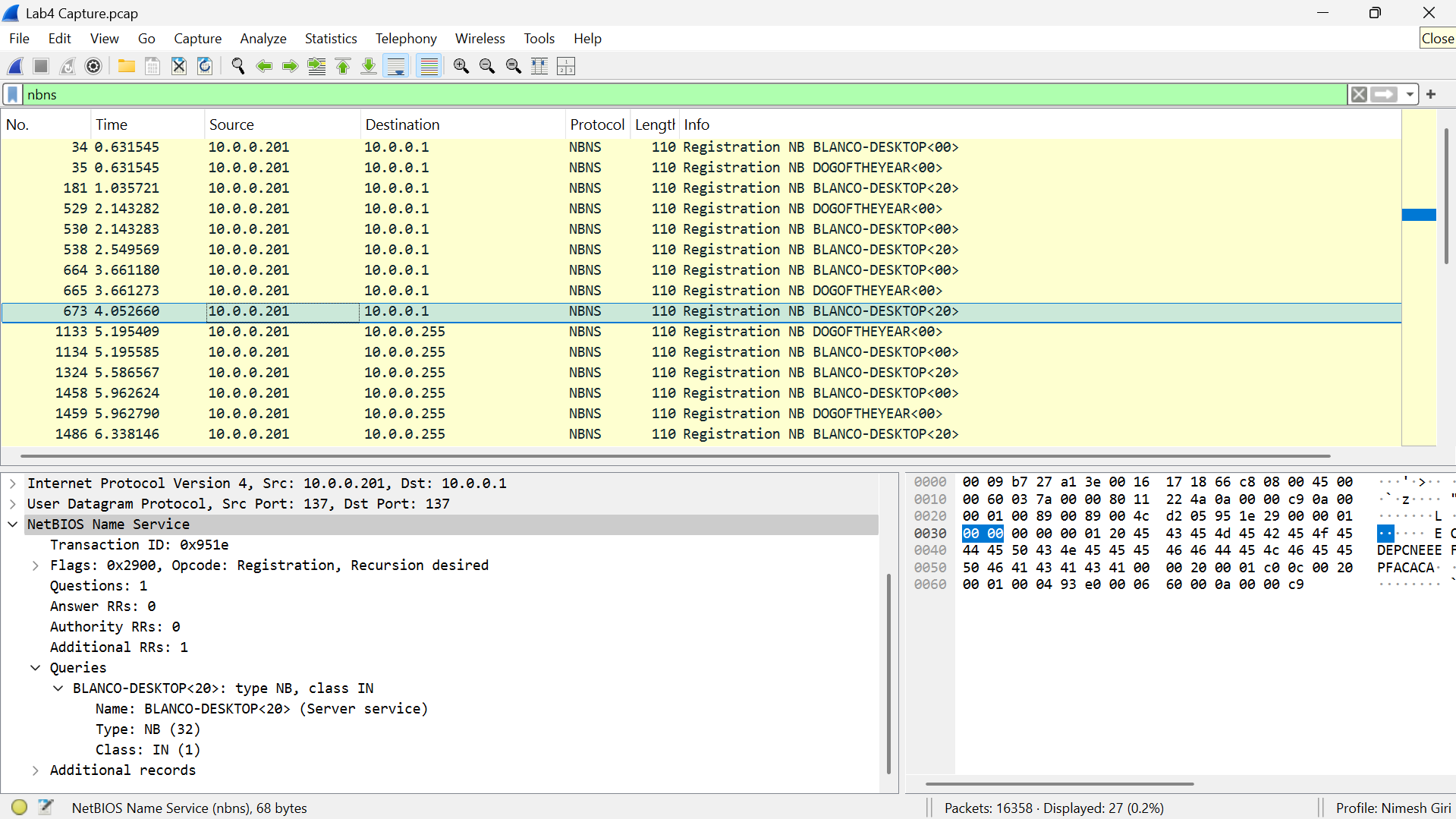
The MAC address is explicitly listed under the host details.

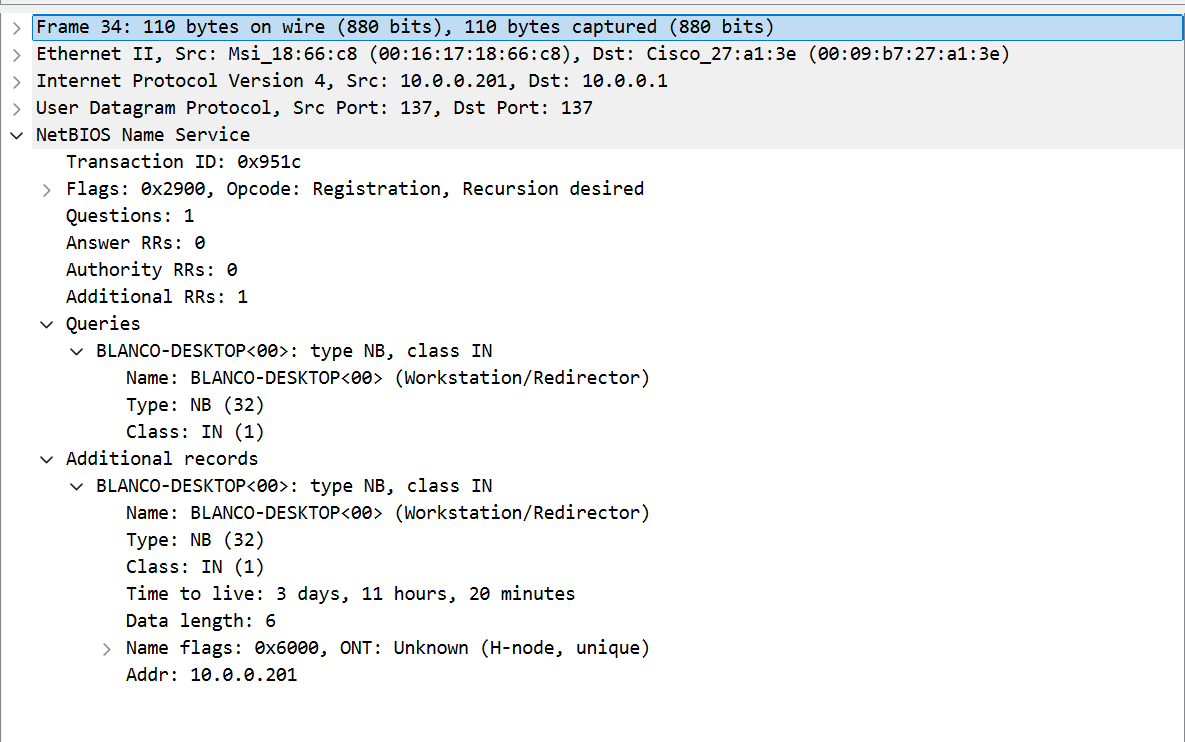
The host sent 7,281 packets and received 9,076 packets, indicating active communication (likely including the BitTorrent traffic from earlier analysis).

**Hostname:** BLANCO-DESKTOP

**MAC Address:** 00:16:17:18:66:C8

**3. NetBIOS Name Service filter to identify OS of 10.0.0.201**

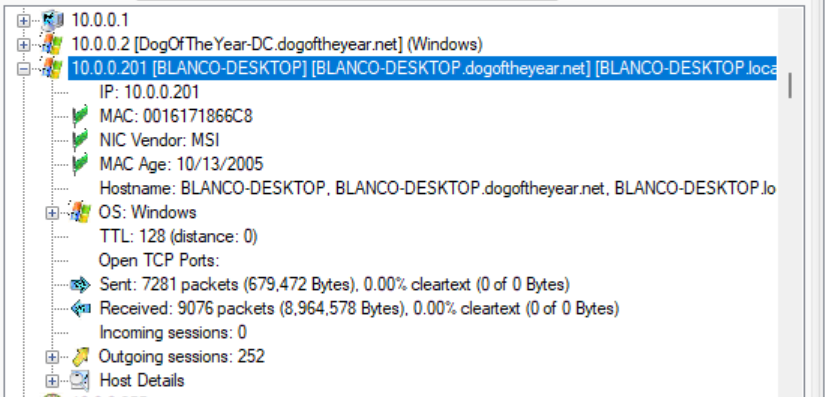




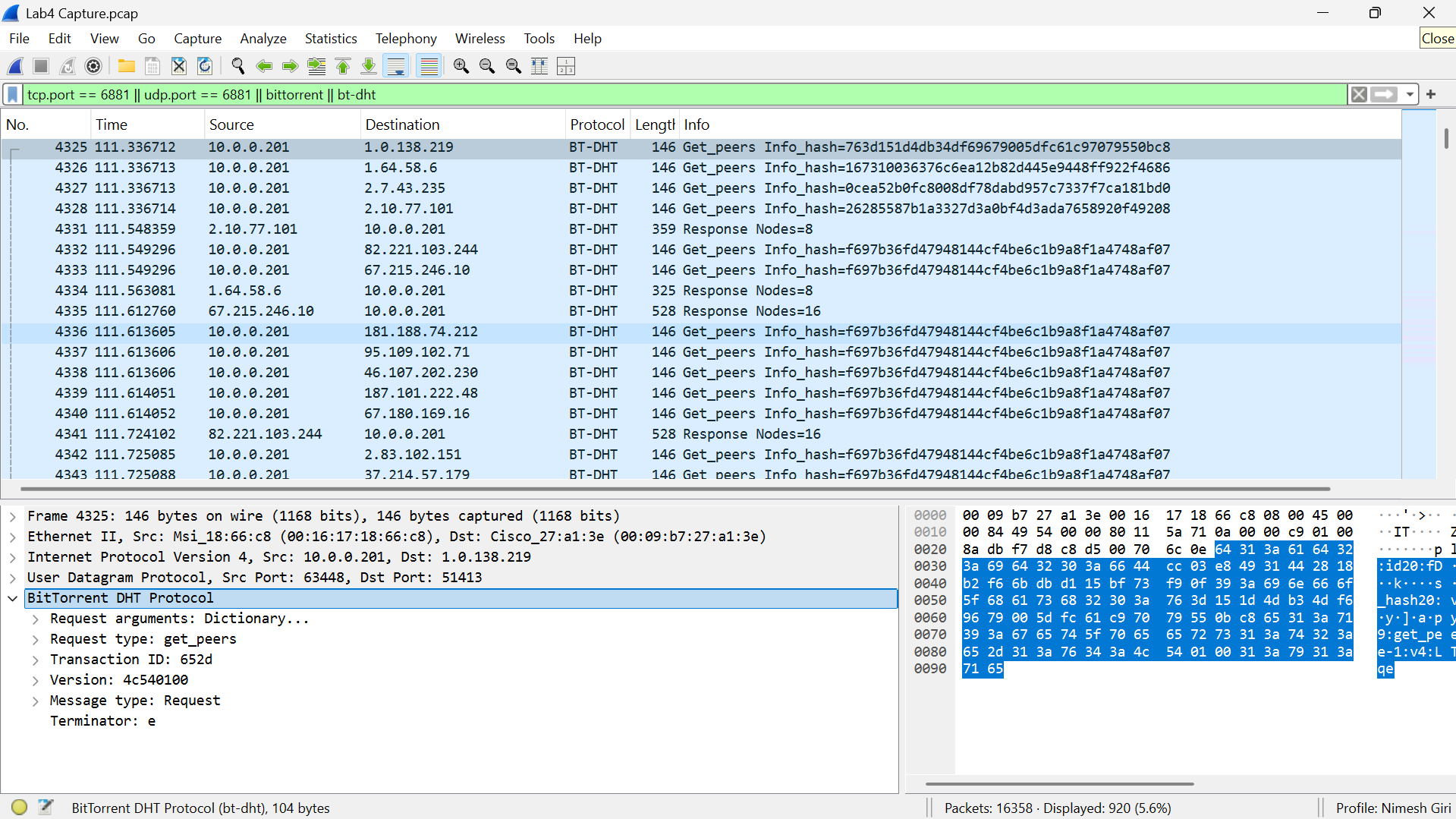
The hostname BLANCO-DESKTOP

* NetBIOS names like <00> and <20> (standard Windows services)
* Use of Hybrid node (H-node) resolution
* MAC address OUI pointing to MSI, a Windows-compatible PC vendor
* No evidence of Linux-style NetBIOS emulation (like Samba)

**Operating System:** The device at 10.0.0.201 is running a Microsoft Windows OS. This is confirmed in NetworkMiner below:



**4. Use appropriate filter to display potential BitTorrent traffic**

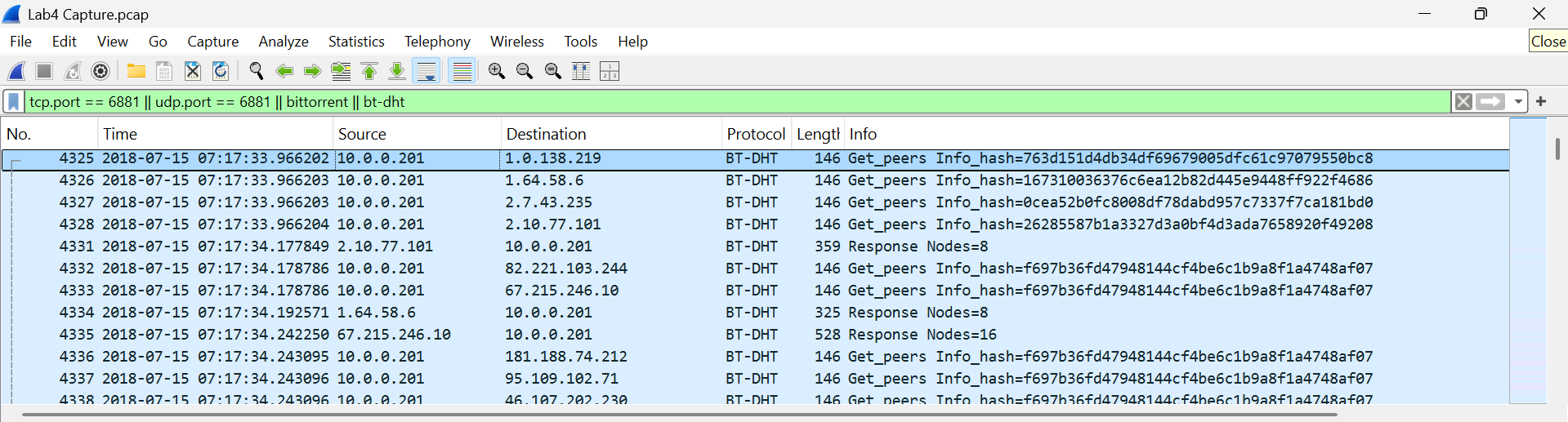


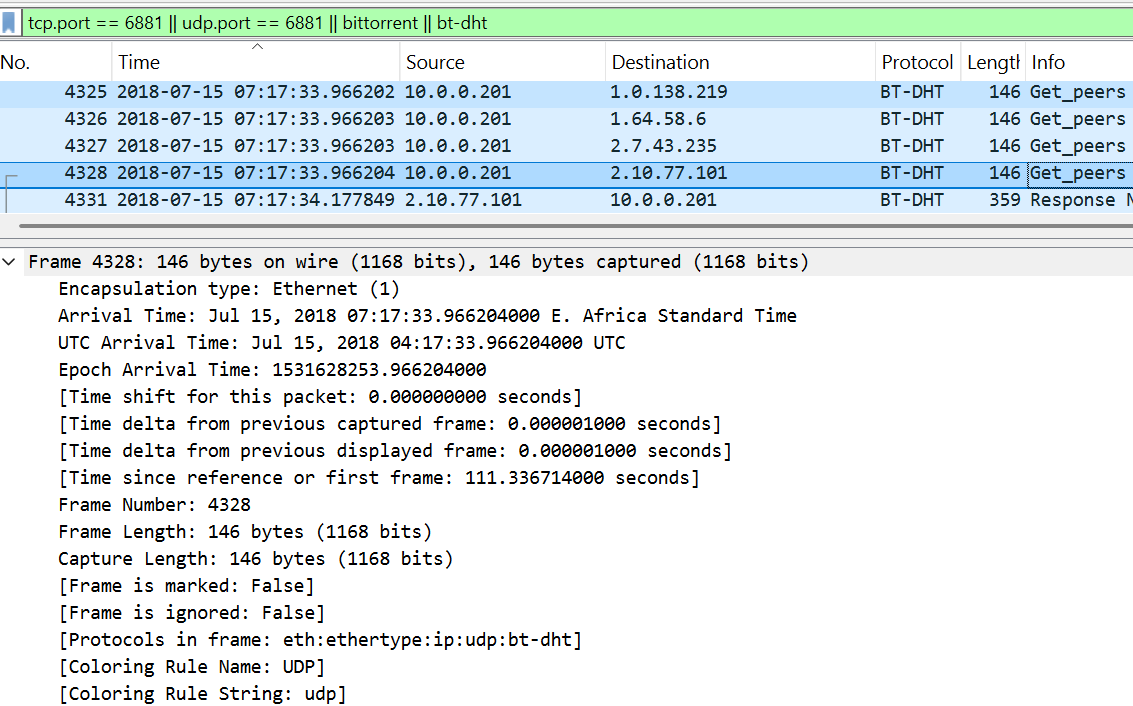
Observations:

* Protocol: BT-DHT
* Info: Get\_peers with Info\_hash
* Ports: UDP source ports vary, destination is often 51413, a known BitTorrent port

This confirms active BitTorrent DHT communication from host 10.0.0.201.

**5. Identify the time period of BitTorrent activity**

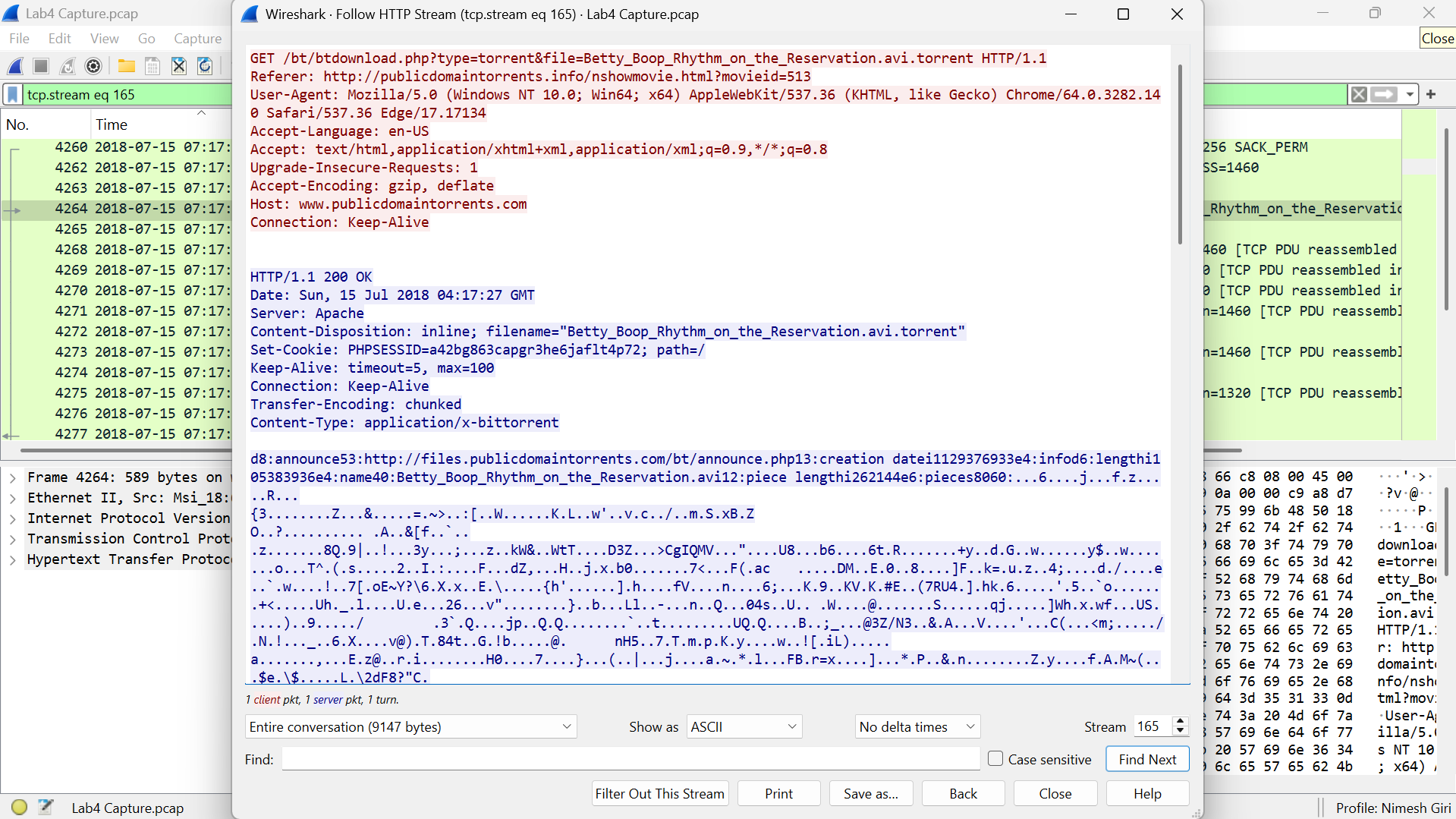




**Date:** July 15, 2018

**Time of Day:** Between 07:17:33.966202 and 07:17:34.177849 (E. Africa Standard Time / UTC+3).

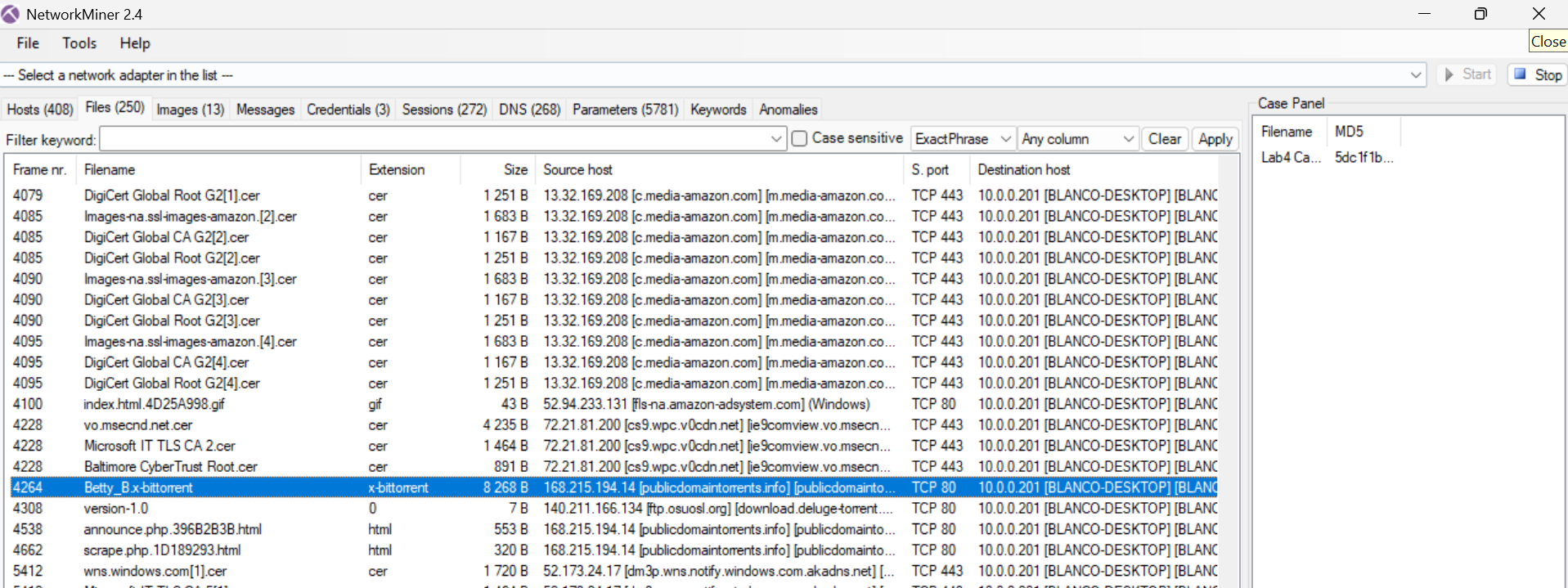
**6. Identify file names via HTTP Stream (Stream 165)**



The name of the file being transferred over the BitTorrent protocol in Stream 165 is:

Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent

This is confirmed in NetworkMiner:



**7. Research the file names for legality**

The file "Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi" is a public domain cartoon from the 1930s, meaning its copyright has expired, and it is legal to share under U.S. law. The file is legally available for download and distribution. There is no copyright violation or illegal torrent activity in this case.

**Questions:**

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

**Ans:**

**Hostname: BLANCO-DESKTOP**

**MAC Address: 00:16:17:18:66:C8**

**This was confirmed in both Wireshark (via Ethernet II layer) and NetworkMiner under the Hosts tab. The host was actively communicating, sending 7,281 packets and receiving 9,076.**

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

**Ans: Windows**

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

**Ans:**

**Date: July 15, 2018**

**Time of Activity: Between 07:17:33.966202 and 07:17:34.177849 (East Africa Standard Time / UTC+3)**

**This was observed from the timestamps of BitTorrent DHT packets in Wireshark with the display format set to Date and Time of Day.**

4. Is there evidence that there is torrent activity?

**Ans:**

**Yes, there is clear evidence of BitTorrent activity, particularly:**

* **Protocol: BT-DHT (BitTorrent Distributed Hash Table)**
* **Traffic Type: get\_peers requests with info\_hash values**
* **Destination Ports: 51413 and other known BitTorrent ports**
* **IP Address: Activity was initiated from host 10.0.0.201**

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

**Ans:**

**The torrent file being downloaded is:**

**Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi.torrent**

6. Is there evidence of illegal torrent activity?

**Ans:**

**No, there is no evidence of illegal torrent activity.**

* **The file in question is a 1939 public domain cartoon.**
* **It was downloaded from publicdomaintorrents.com, a legitimate site that distributes only public domain content.**
* **The sharing of this file is legal under U.S. copyright law.**

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

**Ans:**

* **Application Protocol: BitTorrent**
* **Sub-protocol: BT-DHT (Distributed Hash Table)**
* **Transport Protocols: UDP and TCP**
* **Other protocols used: HTTP (used to request the .torrent file prior to BitTorrent session initiation)**