Ropafadzo Mushayi

Nwit 230

Prof Lemma

Network Miner and Wireshark based on PCAP

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

**Ans: Source: Msi\_18:66:c8(00:16:17:18:66:c8)**

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

**Ans: windows**

* 1. What is the approximate time of the supposed activity?

**Ans: around 17 minutes 37 seconds**

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

**Ans: yes There is evidence of torrent activity**

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

**Ans: Betty\_Boop\_R.torrent.bittorrent**

* 1. Is there evidence of illegal torrent activity?

**Ans: no**

PCAP in wireshark  
A screenshot of a computer

Description automatically generated

Obtaining the Ip address and hostname

A screenshot of a computer

Description automatically generated

Networkminer and PCAPA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated