# Network Forensic Analysis Report

\_TODO\_ Complete this report as you complete the Network Activity on Day 3 of class.

## Time Thieves

You must inspect your traffic capture to answer the following questions:

1. What is the domain name of the users' custom site?

**frank-n-Ted.com**

****

2. What is the IP address of the Domain Controller (DC) of the AD network?

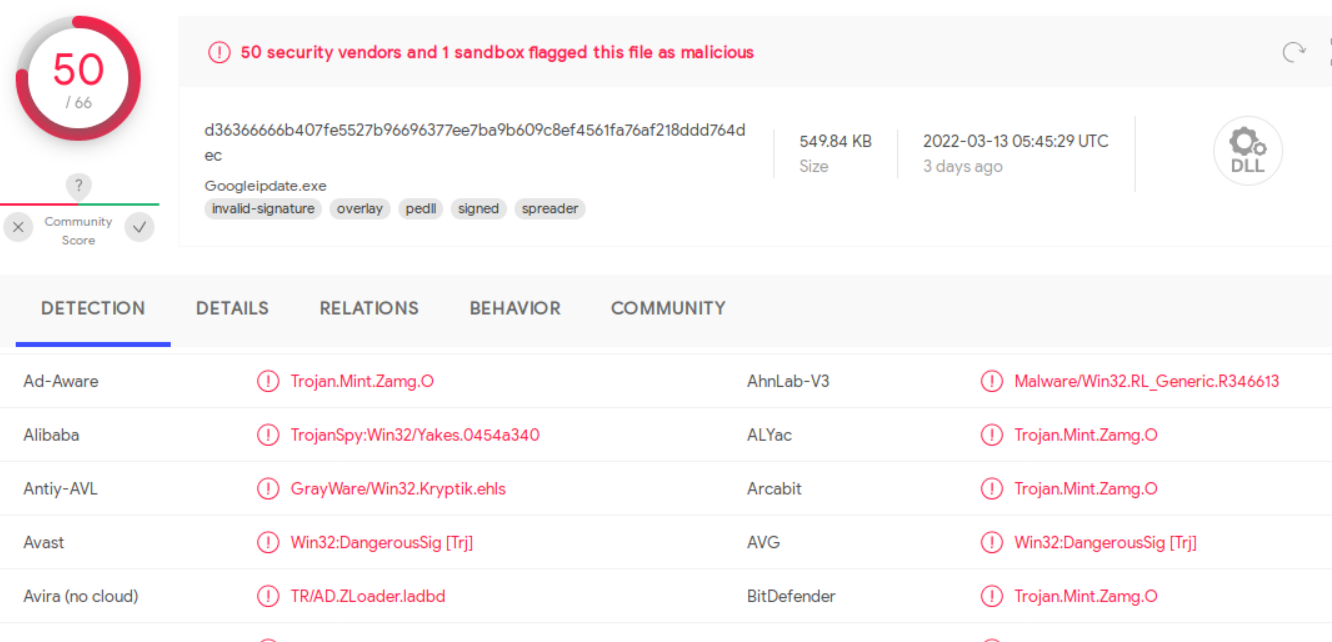
**10.6.12.12 - frank-n-Ted-DC.frank-n-ted.com**

3. What is the name of the malware downloaded to the 10.6.12.203 machine?

**june11.dll**

- Once you have found the file, export it to your Kali machine's desktop.

4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/).



5. What kind of malware is this classified as?

**Trojan**

**Malware was downloaded to 10.6.12.203**

---

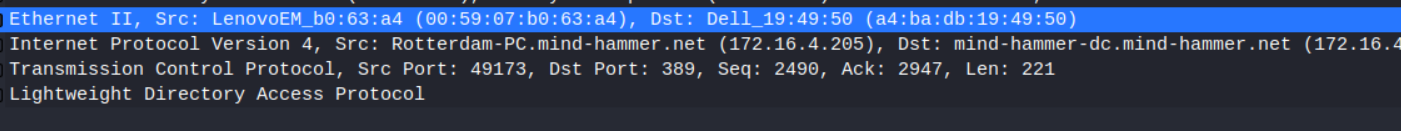
## Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:

- Host name: **Rotterdam-PC.mindhammer.net**

- IP address:**172.16.4.205**

- MAC address:**00:59:b0:63:a4**

****

2. What is the username of the Windows user whose computer is infected?

**rotterdam-pc$**

****

**Matthijs.devries**

****

3. What are the IP addresses used in the actual infection traffic?

**Initial HTTp request made from 172.16.4.205 to 205.185.216.10**

**This request downloaded malware to the machine at 172.16.4.205**

4. As a bonus, retrieve the desktop background of the Windows host.



---

## Illegal Downloads

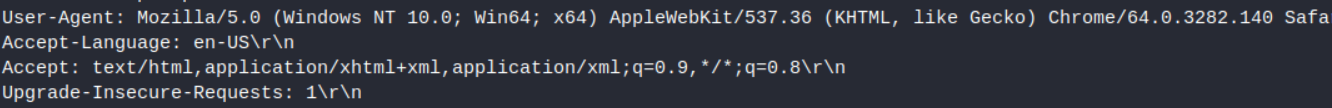
1. Find the following information about the machine with IP address `10.0.0.201`:

- MAC address **00:16:17:18:66:c8**

- Windows username: **elmer.blanco**

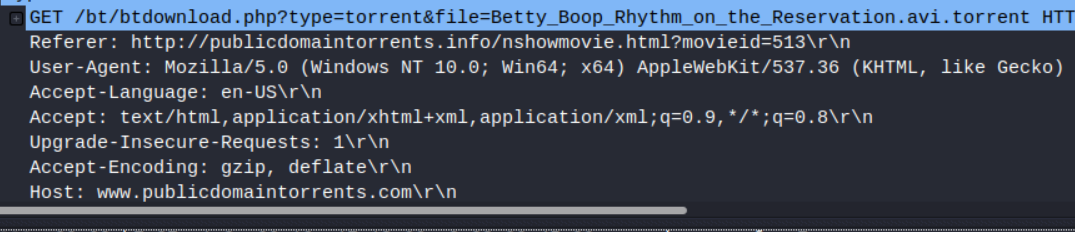
****

- OS version: **Windows 10 NT 10.0**

****

2. Which torrent file did the user download?

**Betty\_Boot\_Rythym\_on\_the\_Reservation.avi**

****