# Network Analysis

## Time Thieves

1. What is the domain name of the users' custom site?
   1. frank-n-ted.com

A screenshot of a computer

Description automatically generated with medium confidence

1. What is the IP address of the Domain Controller (DC) of the AD network?
   1. 10.6.12.12 as the DNS query response came from that IP.
2. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop.
   1. june11.dll

A screenshot of a computer

Description automatically generated

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

Graphical user interface, text, application

Description automatically generated

1. What kind of malware is this classified as?
   1. It is a trojan program that accesses system files and registries for modification and posts the information to specific websites for collection.

## Vulnerable Windows Machines

1. Find the following information about the infected Windows machine:
   * Host name: Rotterdam-PC
   * IP address: 172.16.4.205
   * MAC address: 00:59:07:b0:63:a4

A screenshot of a computer

Description automatically generated with medium confidence

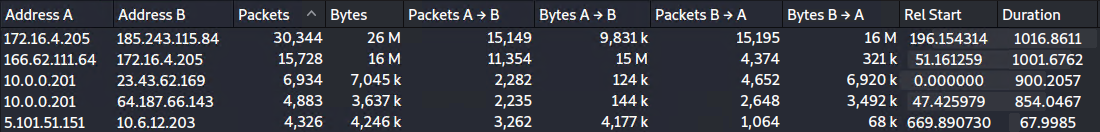
The infected machine is making several unique requests to the DC (1417 specifically) that varied in protocol, leading to the likelihood of remote control.

1. What is the username of the Windows user whose computer is infected?
   * matthijs.devries

Graphical user interface, application

Description automatically generated

1. What are the IP addresses used in the actual infection traffic?
   * 172.16.4.205, 185.243.115.84, and 166.62.111.64 based on the number of packets relative to all other forms of traffic.



Table

Description automatically generated

Table

Description automatically generated

There were also numerous POST requests for an odd appearing “empty.gif” file, as well as a high number of continuation requests with the infected computer being the destination IP.

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

A picture containing bird, gallinaceous bird, pigeon

Description automatically generated

## 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

A screenshot of a computer

Description automatically generated with medium confidence

1. Which torrent file did the user download?
   * Btdownload.php?type=torrent&file=Betty\_Boop\_Rhythm\_on\_the \_Reservation.avi.torrent

A screenshot of a computer

Description automatically generated with medium confidence