# Network Analysis

## Time Thieves

DESKTOP-86J4BX.frank-n-ted.com (10.6.12.157)

LAPTOP-5WKHX9YG.frank-n-ted.com (10.6.12.203)

1. What is the domain name of the users' custom site?
   1. frank-n-ted.com
2. What is the IP address of the Domain Controller (DC) of the AD network?
   1. 10.6.12.12
3. 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. Malware file June11.dll
   2. Zloader
4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/). What kind of malware is this classified as?
   1. Trojan

## 

## 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
2. What is the username of the Windows user whose computer is infected?
   * Matthijs Devries
3. What are the IP addresses used in the actual infection traffic?
   * 31.7.62.214
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
2. Which torrent file did the user download?
   * Betty Boop rhythm on the reservation.avi