Network Forensic Analysis Report

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

3. What is the name of the malware downloaded to the 10.6.12.203 machine?
   june11.dll

4. What kind of malware is this classified as?
   Trojan

Vulnerable Windows Machine

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?
   185.243.115.84 As witnessed by a post of a file **empty.gif** and the running of the file after placing it on the server. This resulted in a large stream of data being constantly sent between the 2 machines.

Illegal Downloads

1. Find the following information about the machine with IP address `10.0.0.201`:
   - MAC address: **00:09:B7:27:A1:3E**
   - Windows username: **elmer.blanco**
   - OS version: **Windows 10.0; Win64; x64**

2. Which torrent file did the user download?
   Betty_Boop_Rhythm_on_the_Reservation.avi.torrent