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-DC. 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. Upload the file to VirusTotal.com.
5. What kind of malware is this classified as?
   Trojan.Mint.Zamg.O

Vulnerable Windows Machine

1. Find the following information about the infected Windows machine:
   1. Host name: Rotterdam-PC
   2. IP address: 172.16.4.205
   3. 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, 172.16.4.205, 23.43.62.169, 64.187.66.143

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`:
   1. MAC address: 00:16:17:18:66:c8
   2. Username: elmer.blanco
   3. OS version: BLANCO-DESKTOP Windows NT 10.0
2. Which torrent file did the user download?
   Betty_Boop_Rhythm_on_the_Reservation.avi.torrent