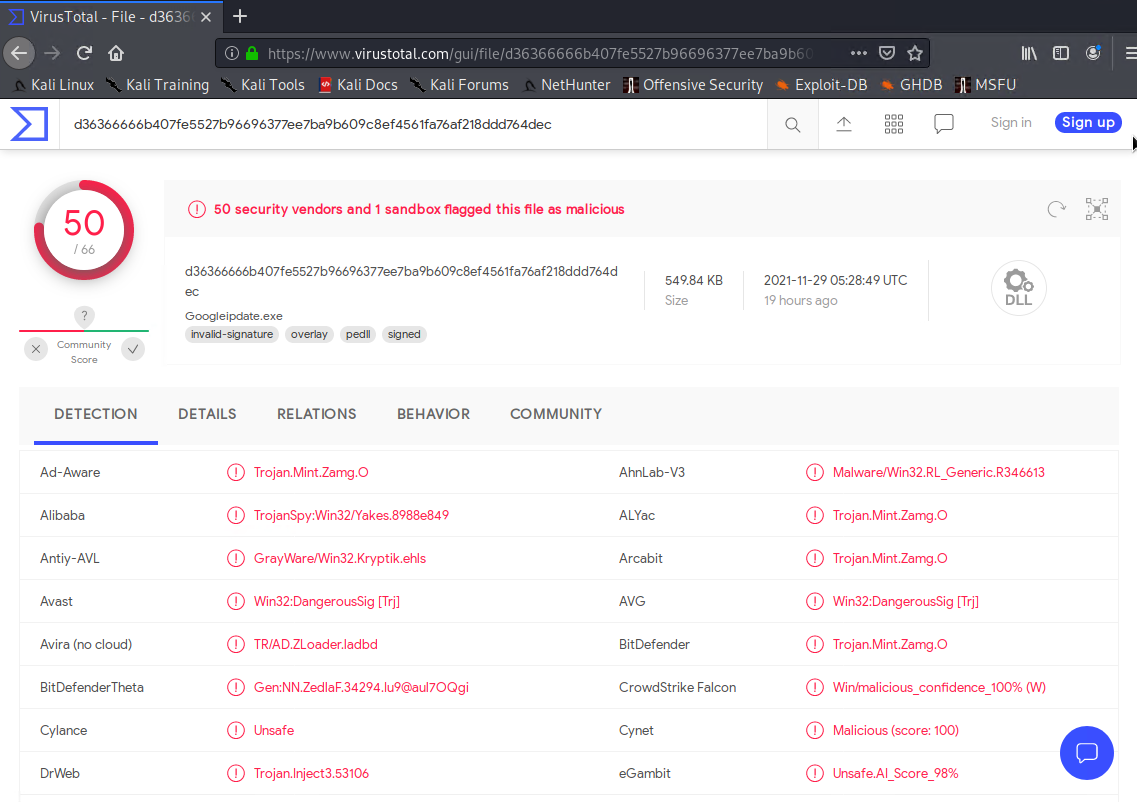
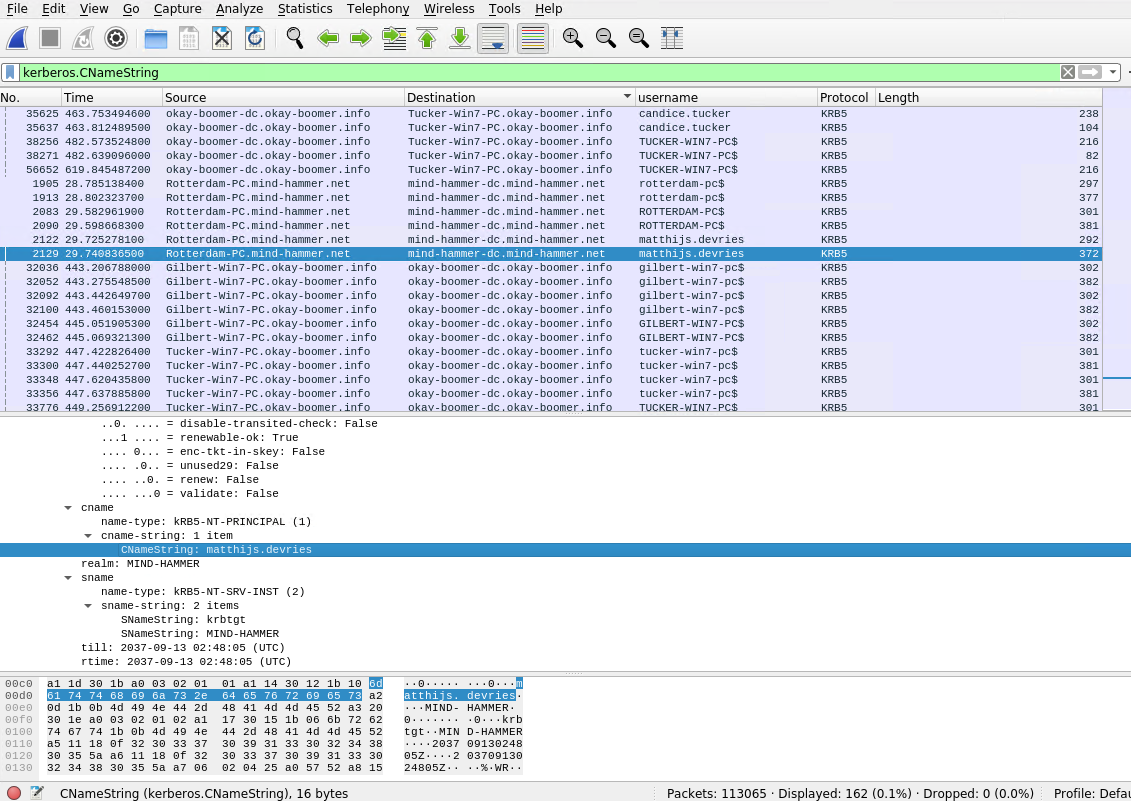
# Network Forensic Analysis Report

## 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 (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
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?
   * Filter: ip.src==10.0.0.205 and kerberos.CNameString
   * User: matthijs.devries 
3. What are the IP addresses used in the actual infection traffic?

## 172.16.4.205, 185.243.115.84, 166.62.11.64

## 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: BLANCO-DESKTOP
2. Which torrent file did the user download?
   * Filter: ip.addr==10.0.0.201 and http.request.method==GET
   * The torrent file is Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent 