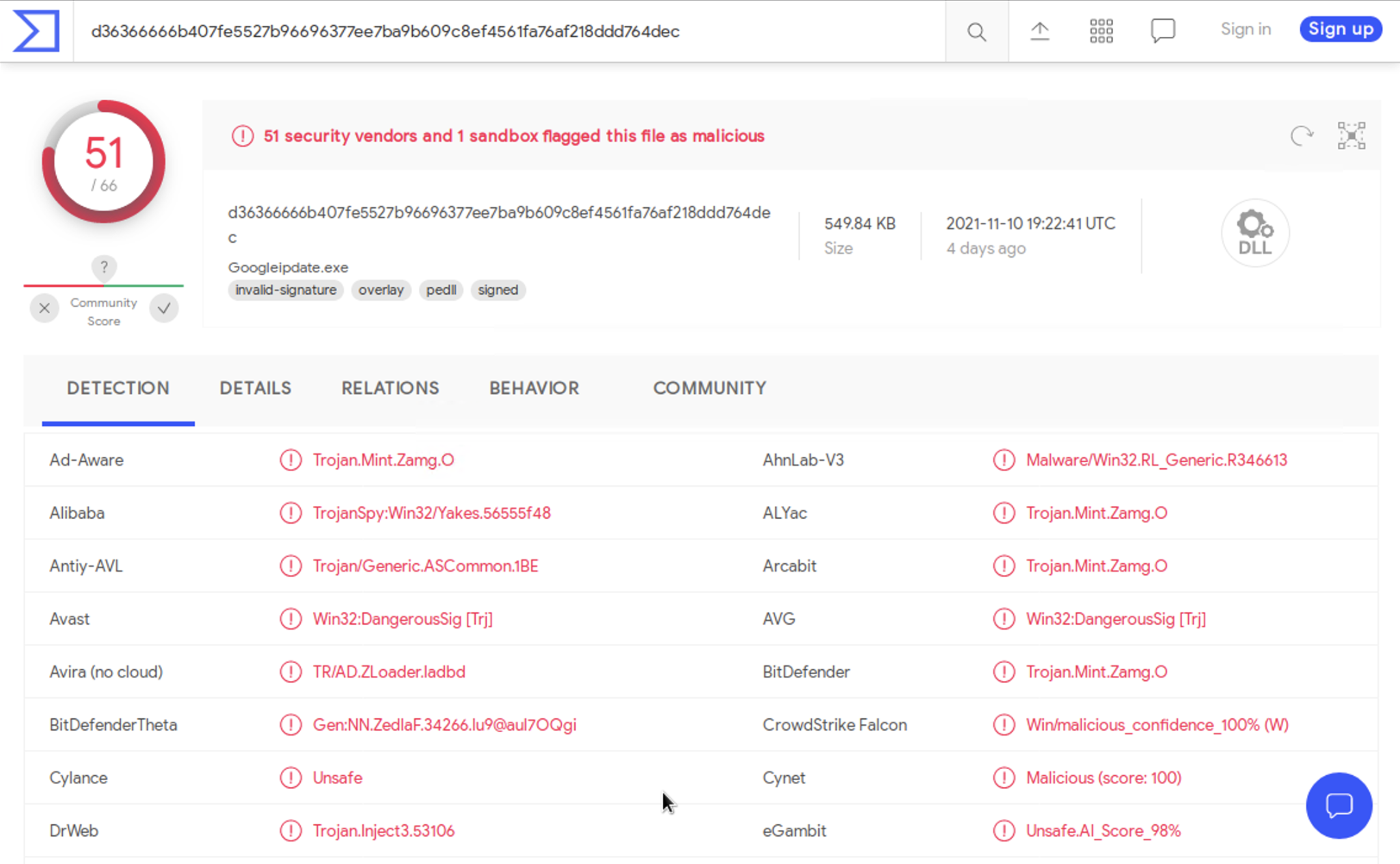
## **Network Forensic Analysis Report**

### **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  
   Filter: ip.addr==10.6.12.0/24
2. What is the IP address of the Domain Controller (DC) of the AD network?  
   IP address is 10.6.12.12 (Frank-n-Ted-DC.frank-n-ted.com)  
   Filter: ip.addr==10.6.12.0/24
3. What is the name of the malware downloaded to the 10.6.12.203 machine?  
   Malware file is june11.dll.  
   Filter: ip.addr==10.16.12.203 and http.request.method==GET  
   Export: File > Export Objects > HTTP
4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/).



1. What kind of malware is this classified as?  
   It was classified as a 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

* Filter: ip.src==172.16.4.4 and kerberos.CNameString

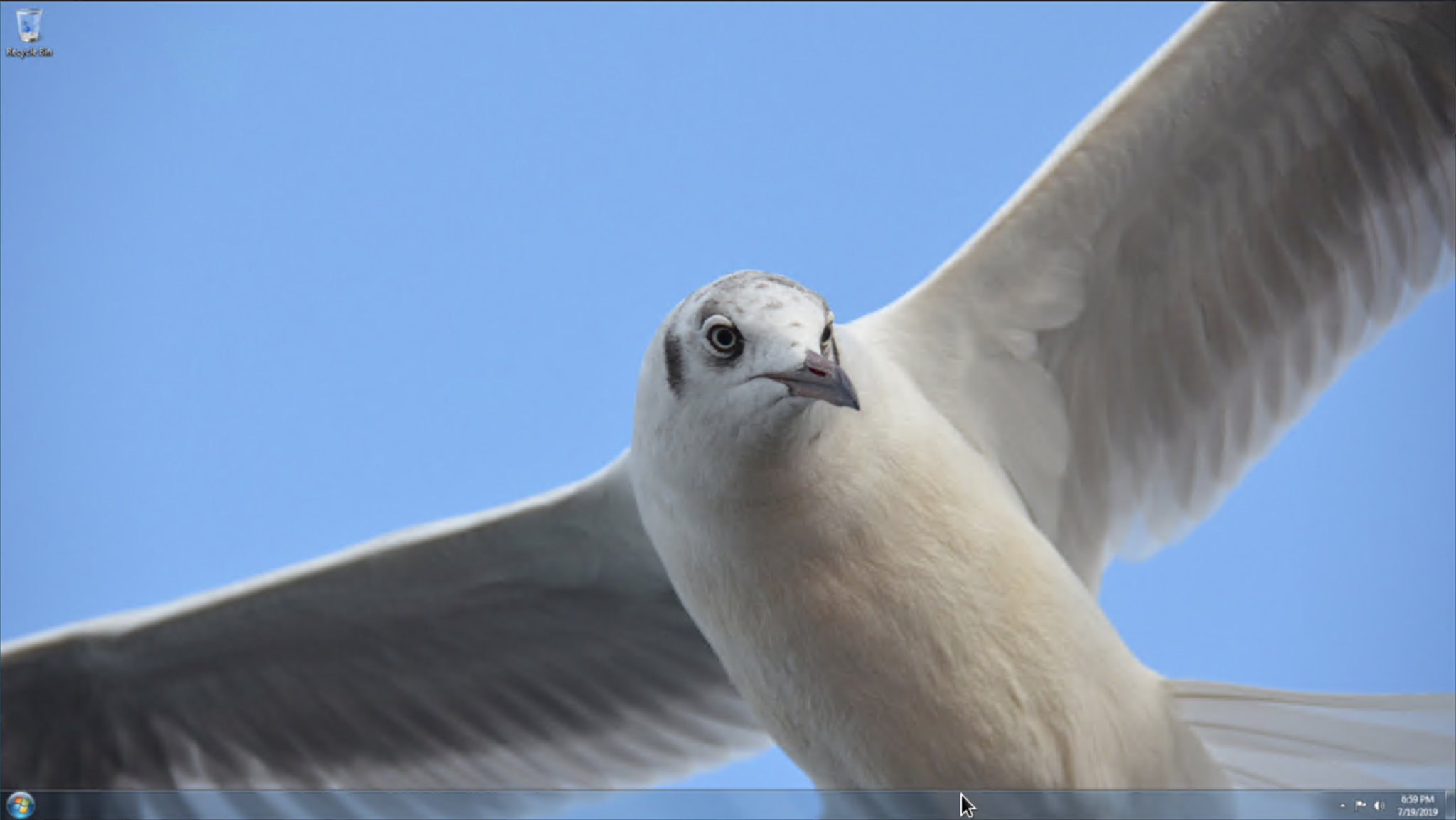
1. What is the username of the Windows user whose computer is infected?
   * matthijs.devries

* Filter: ip.src==172.16.4.205 and kerberos.CNameString

1. What are the IP addresses used in the actual infection traffic?
   * 172.16.4.205, 185.243.115.84, 166.62.11.64 are the infected traffic

* Filter: ip.addr==172.16.4.205 and ip.addr==185.243.115.84

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



## **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 NT 10.0; Win64; x64

* Filter: ip.src==10.0.0.201 and kerberos.CNameString

1. Which torrent file did the user download?
   * The torrent file is Betty\_Boop\_Rythm\_on\_the\_Reservation.avi.torrent.

* Filter: ip.addr==10.0.0.201 and (http.request.uri contains “.torrent”)