# **Network Forensic Analysis Report**

## **Time Thieves**

You must inspect your traffic capture to answer the following questions:

* They have set up an Active Directory network.
* They are constantly watching videos on YouTube.
* Their IP addresses are somewhere in the range 10.6.12.0/24

1. What is the domain name of the users' custom site?

Frank-n-TEd-DC.frank-n-ted.com is the domain name

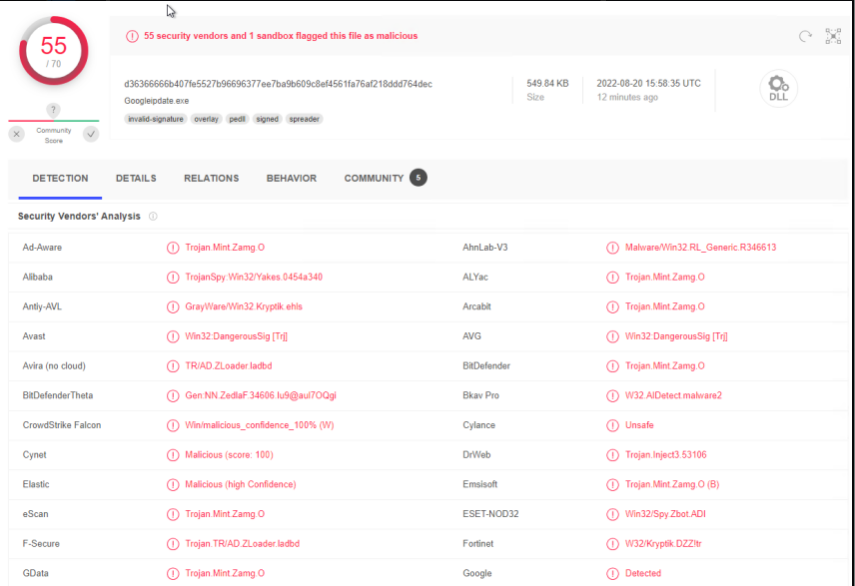
1. What is the IP address of the Domain Controller (DC) of the AD network?

10.6.12.12

1. What is the name of the malware downloaded to the 10.6.12.203 machine?

June11.dll is the name of the file

1. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/)

.

1. What kind of malware is this classified as?

It is 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
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?  
   185.243.114.84 and 172.16.4.205
4. As a bonus, retrieve the desktop background of the Windows host.

