

Network Analysis

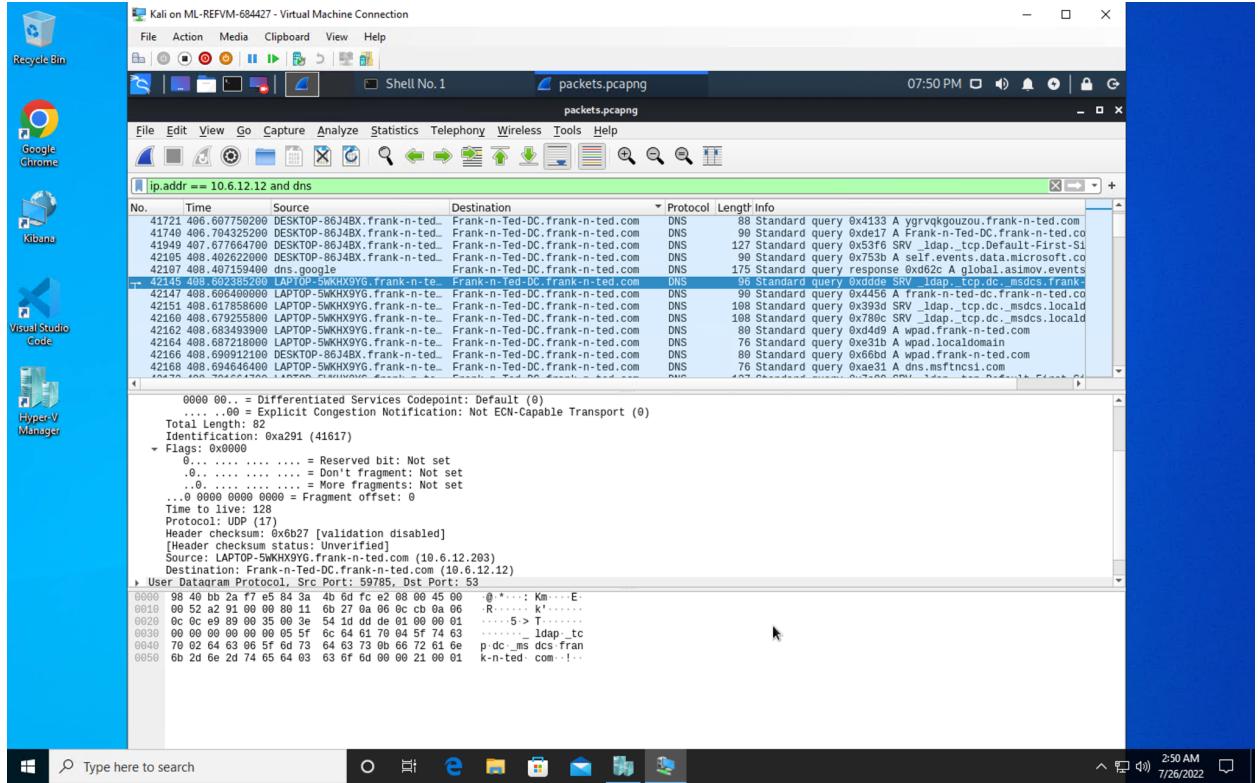
Time Thieves

At least two users on the network have been wasting time on YouTube. Usually, IT wouldn't pay much mind to this behavior, but it seems these people have created their own web server on the corporate network. So far, Security knows the following about these time thieves:

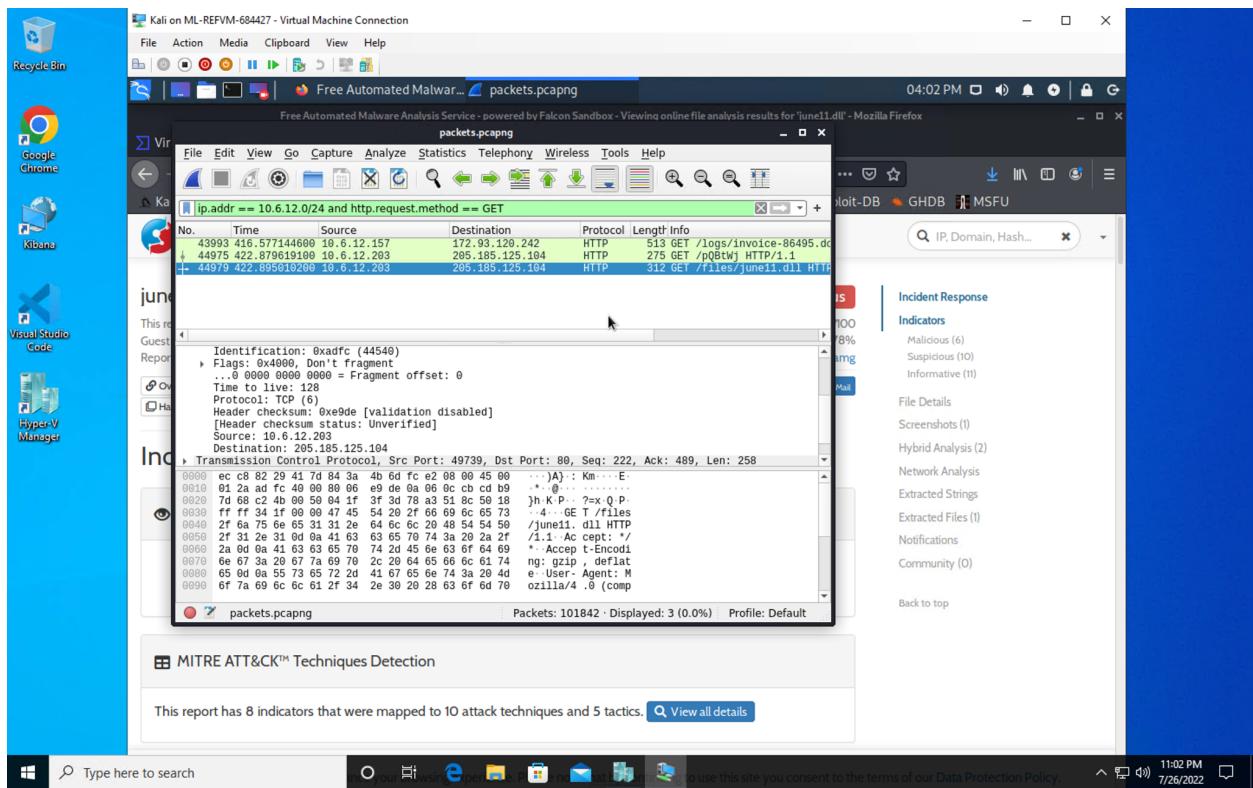
- They have set up an Active Directory network.
- They are constantly watching videos on YouTube.
- Their IP addresses are somewhere in the range 10.6.12.0/24.

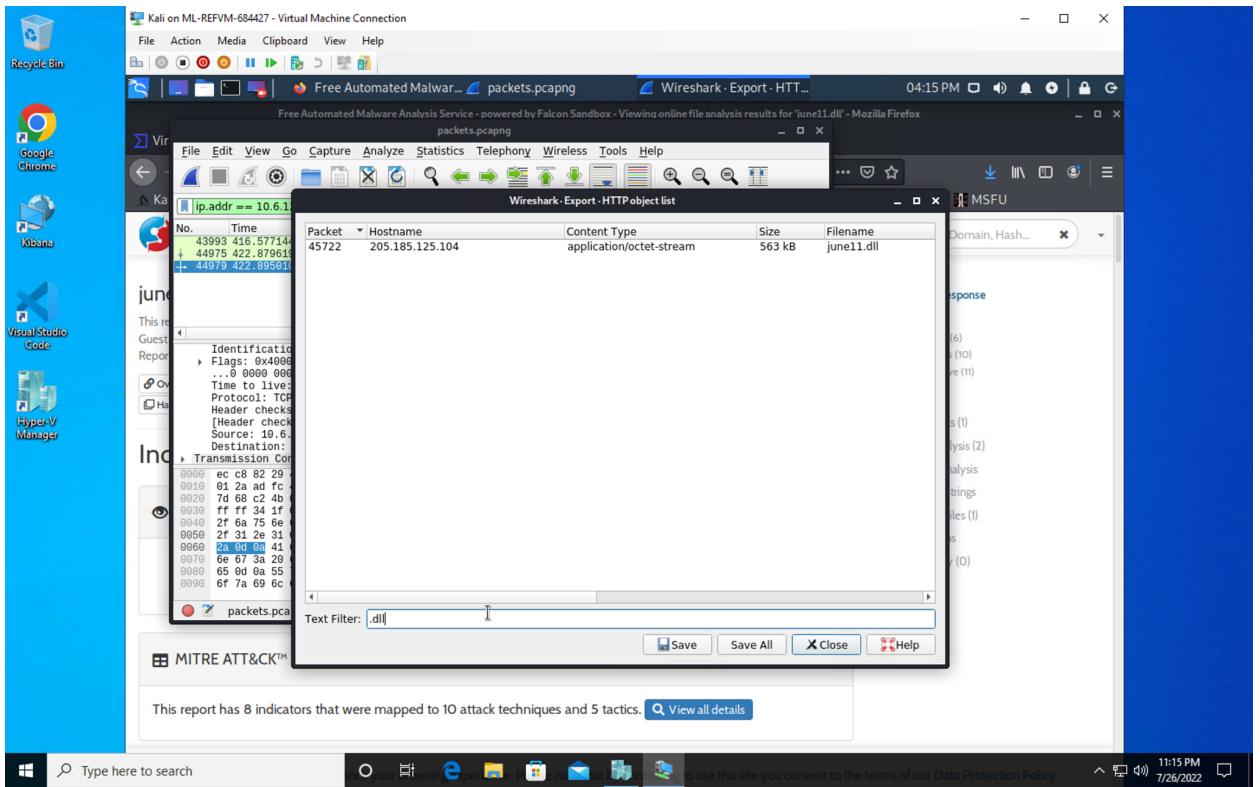
You must inspect your traffic capture to answer the following questions:

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

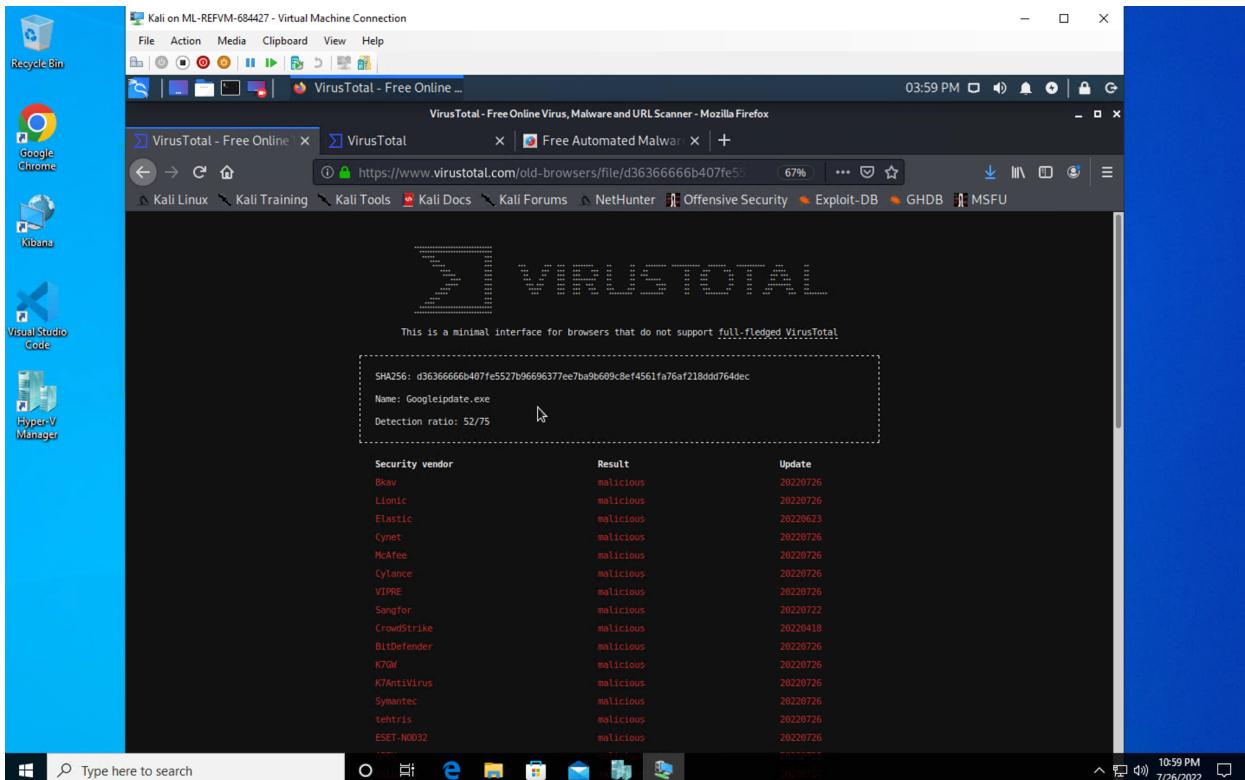


3. What is the name of the malware downloaded to the 10.6.12.203 machine? Once you have found the file, export it to your Kali machine's desktop. june11.dll





4. Upload the file to [VirusTotal.com](https://www.virustotal.com). What kind of malware is this classified as?
Trojan.Mint.Zamg (Malicious)



A screenshot of a Windows desktop environment. On the left, there's a pinned taskbar with icons for Recycle Bin, Google Chrome, Kibana, Visual Studio Code, and Hyper-V Manager. The main window is a Mozilla Firefox browser displaying the Hybrid Analysis website. The address bar shows the URL: https://hybrid-analysis.com/sample/d36366666b407fe5527b96696377ee7ba9b69c8ef4561fa76af218ddd764dec. The page title is "Free Automated Malware Analysis Service - powered by Falcon Sandbox - Viewing online file analysis results for 'june11.dll' - Mozilla Firefox". The content of the page shows the analysis results for "june11.dll". It includes a "malicious" classification, a Threat Score of 100/100, and an AV Detection rate of 78%. The report was generated by Falcon Sandbox v8.31. The page features a sidebar for "Incident Response" with sections for "Indicators", "File Details", and "Network Analysis". The "File Details" section lists "Screenshots (1)", "Hybrid Analysis (2)", and "Network Analysis". The "Network Analysis" section lists "Extracted Strings", "Extracted Files (1)", and "Notifications". The "Community" section shows 0 entries. At the bottom, there's a "Risk Assessment" section with a "Spreading" note about ARP broadcast requests and a "Network Behavior" note about contacts with 7 domains. There's also a "MITRE ATT&CK™ Techniques Detection" section indicating 8 mapped indicators across 10 attack techniques and 5 tactics.

Vulnerable Windows Machines

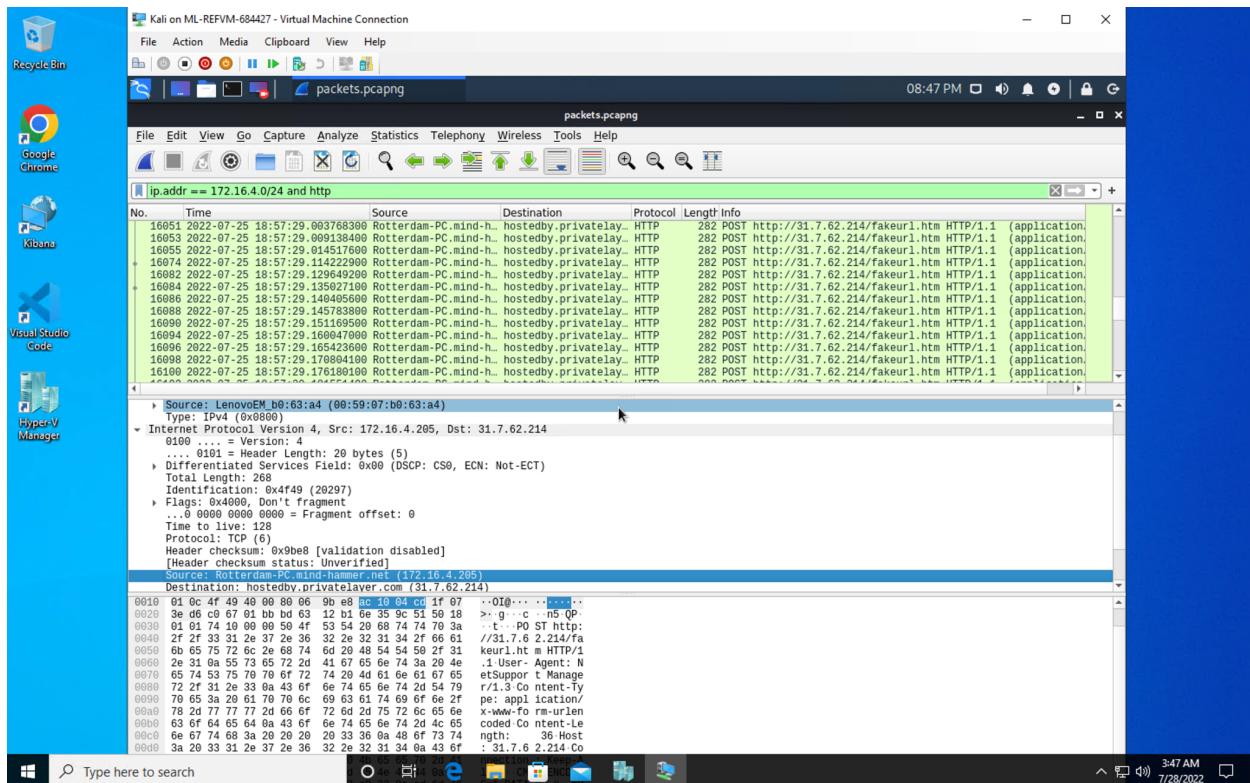
The Security team received reports of an infected Windows host on the network. They know the following:

- Machines in the network live in the range 172.16.4.0/24.
- The domain mind-hammer.net is associated with the infected computer.
- The DC for this network lives at 172.16.4.4 and is named Mind-Hammer-DC.
- The network has standard gateway and broadcast addresses.

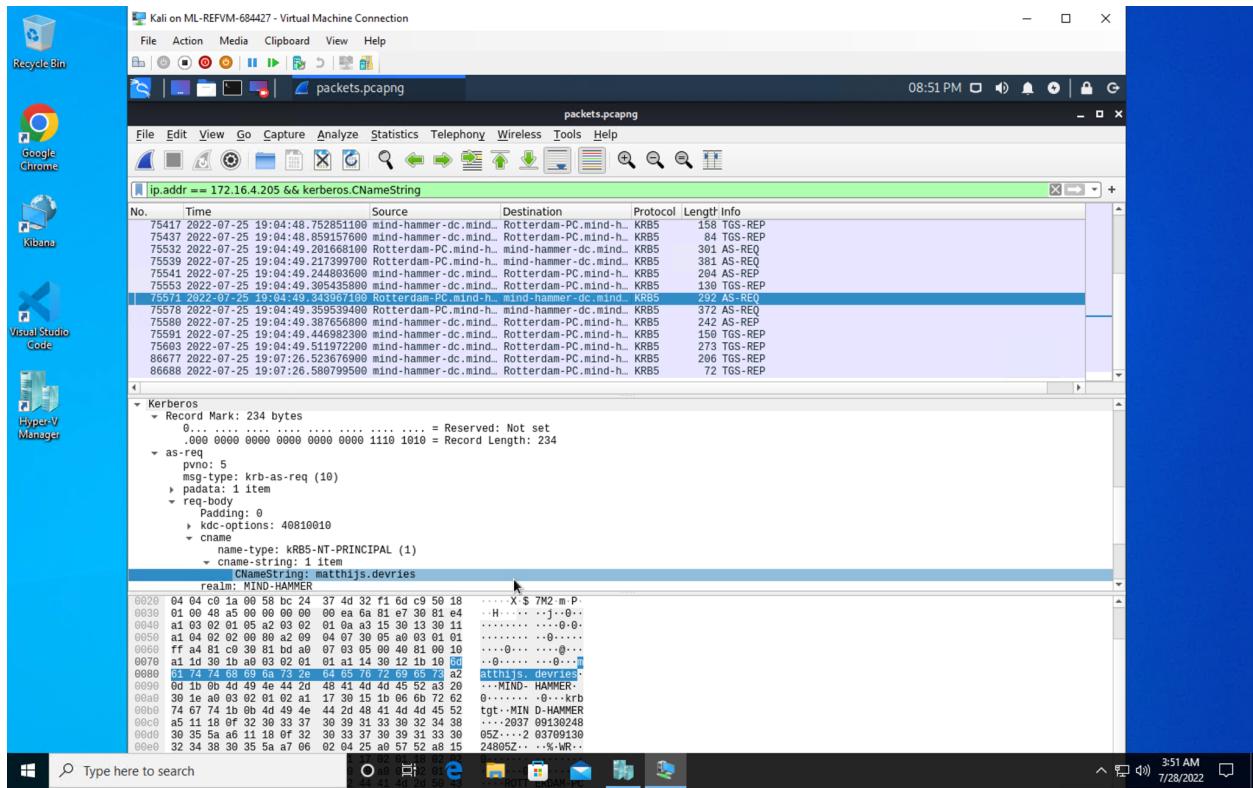
Inspect your traffic to answer the following questions:

1. Find the following information about the infected Windows machine:

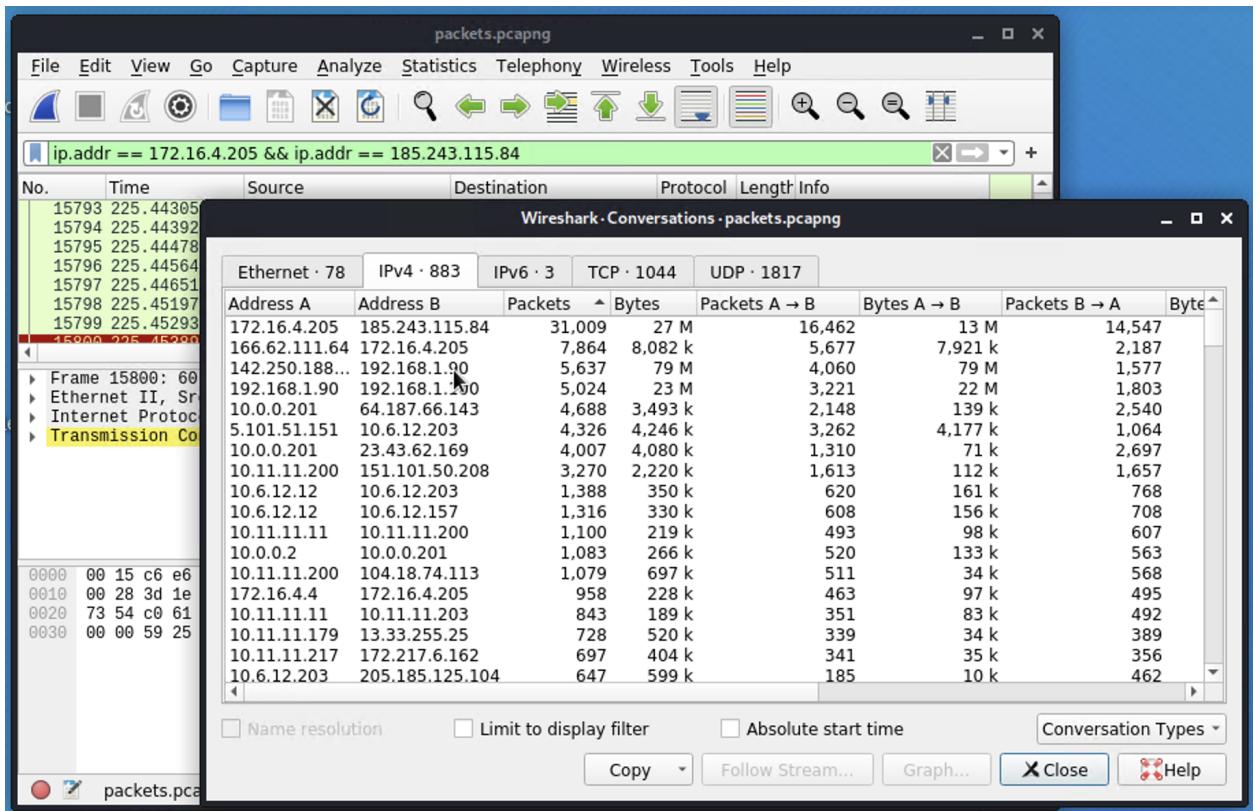
- Host name: ROTTERDAM-PC
- IP address: 172.16.4.205
- MAC address: 00:59:07:b0:63:a4



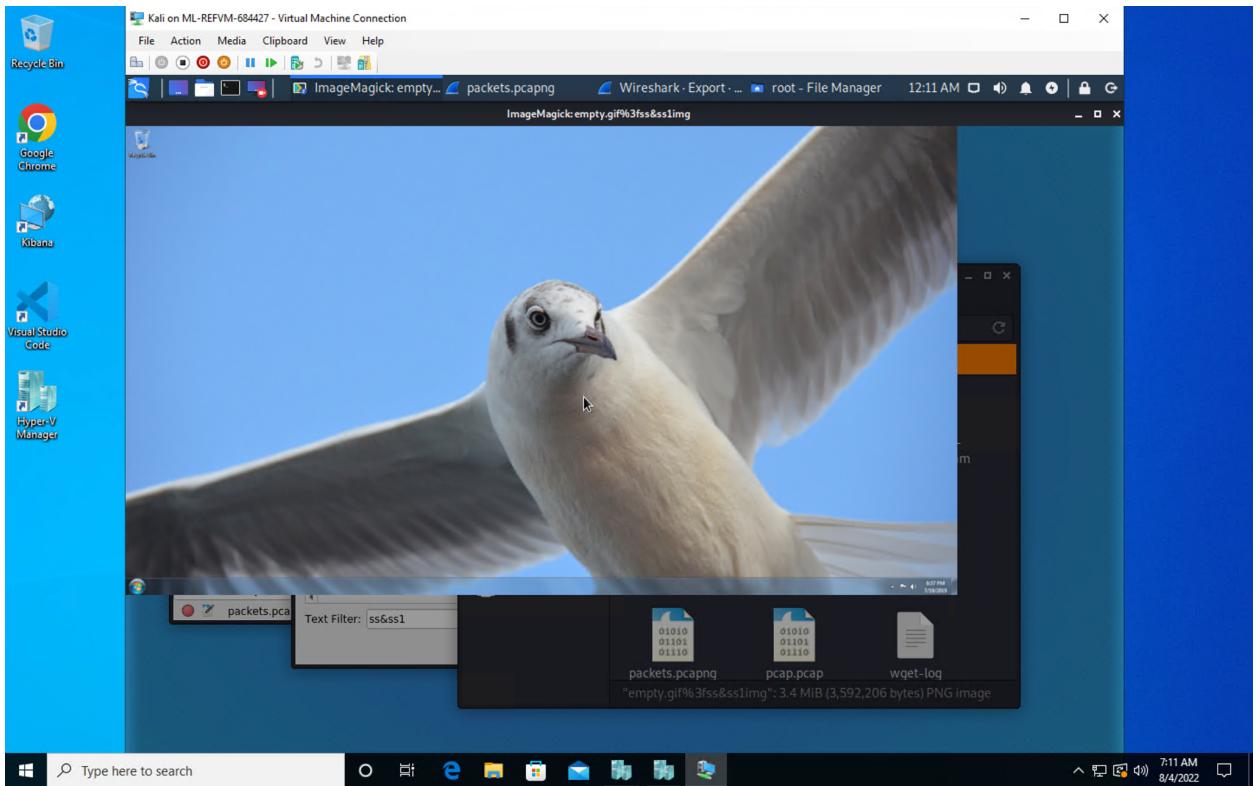
2. What is the username of the Windows user whose computer is infected?
Matthijs.devries



3. What are the IP addresses used in the actual infection traffic? 172.16.4.205 & 185.243.115.84



4. As a bonus, retrieve the desktop background of the Windows host.



Illegal Downloads

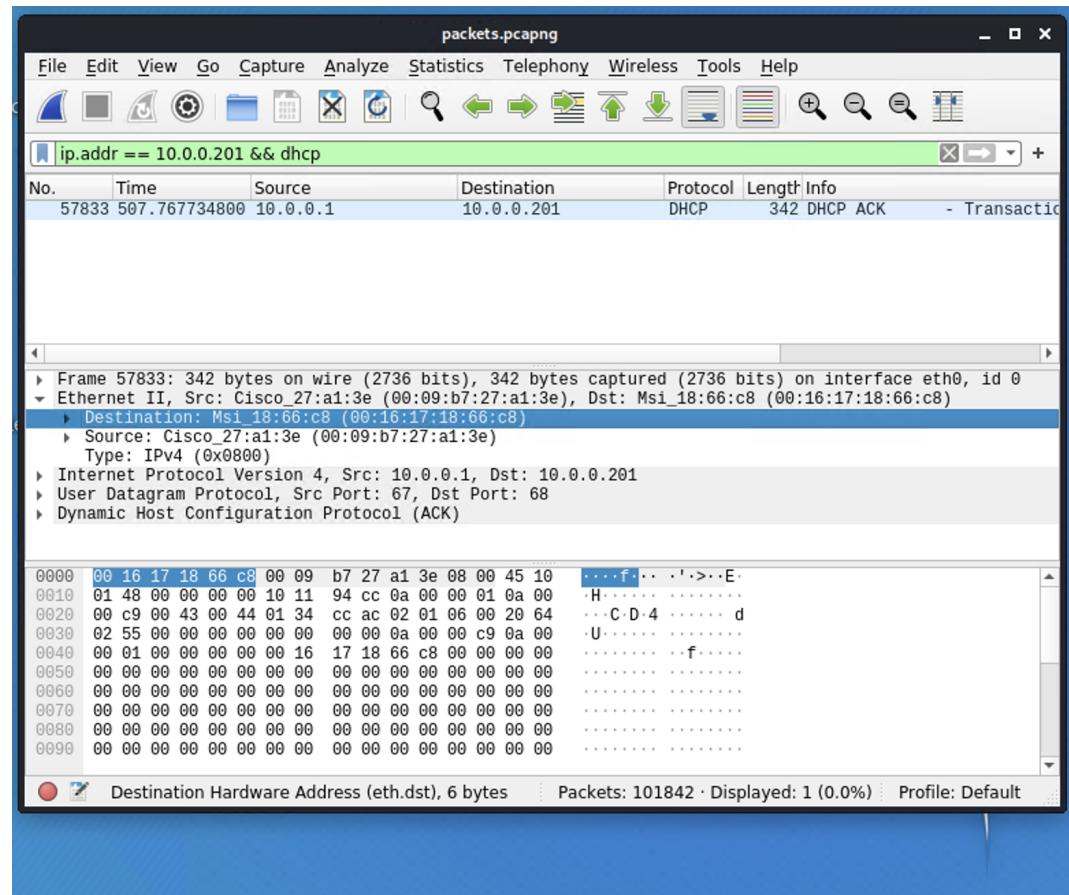
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

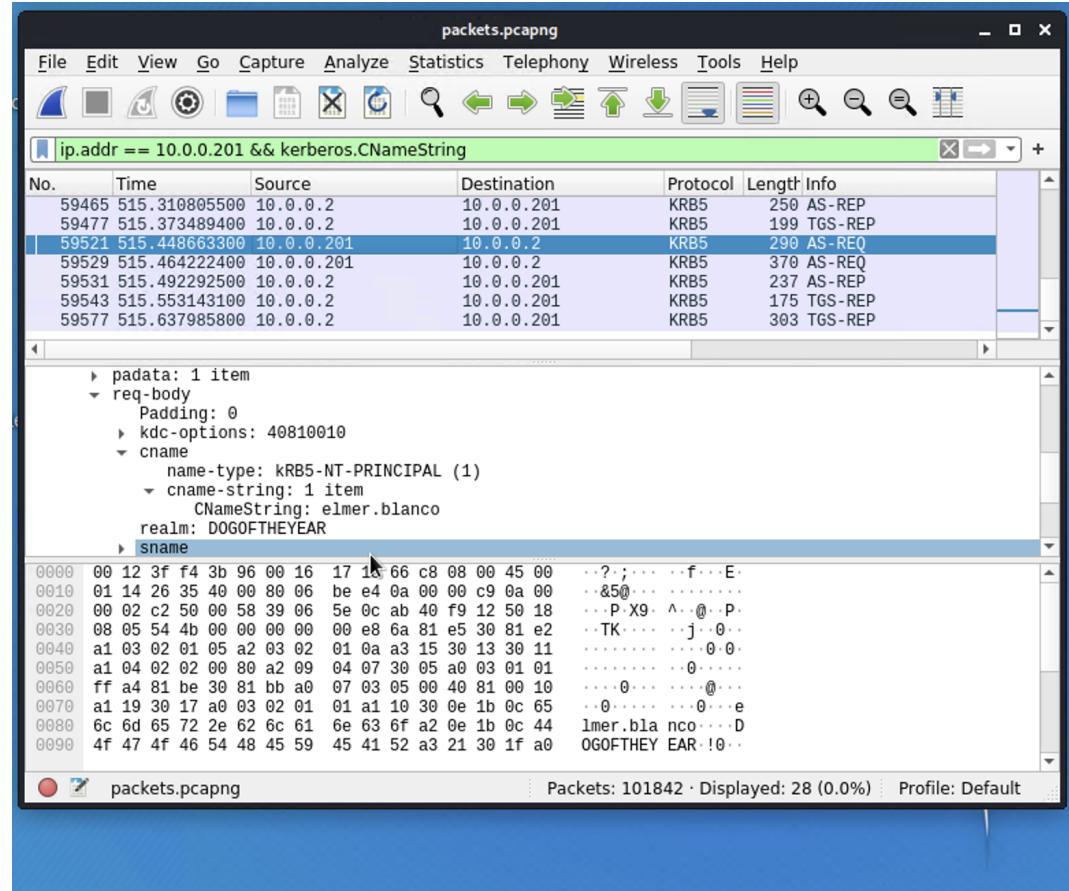
- The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
- The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
- The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions in your Network Report:

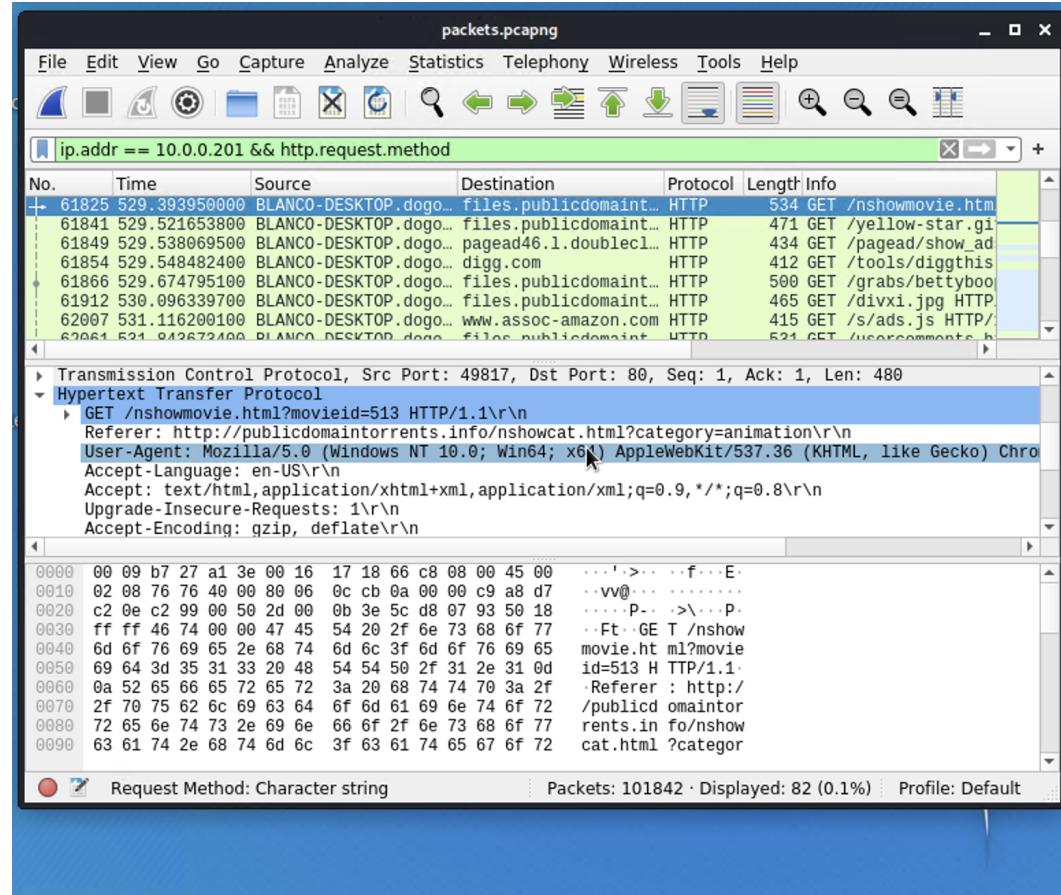
1. Find the following information about the machine with IP address 10.0.0.201:
 - MAC address: 00:16:17:18:66:c8



- Windows username: elmer.blanco



- OS version: Windows NT 10.0



2. Which torrent file did the user download?

Betty_Boop_Rhythm_on_the_Reservation.avi.torrent

