# Network Analysis

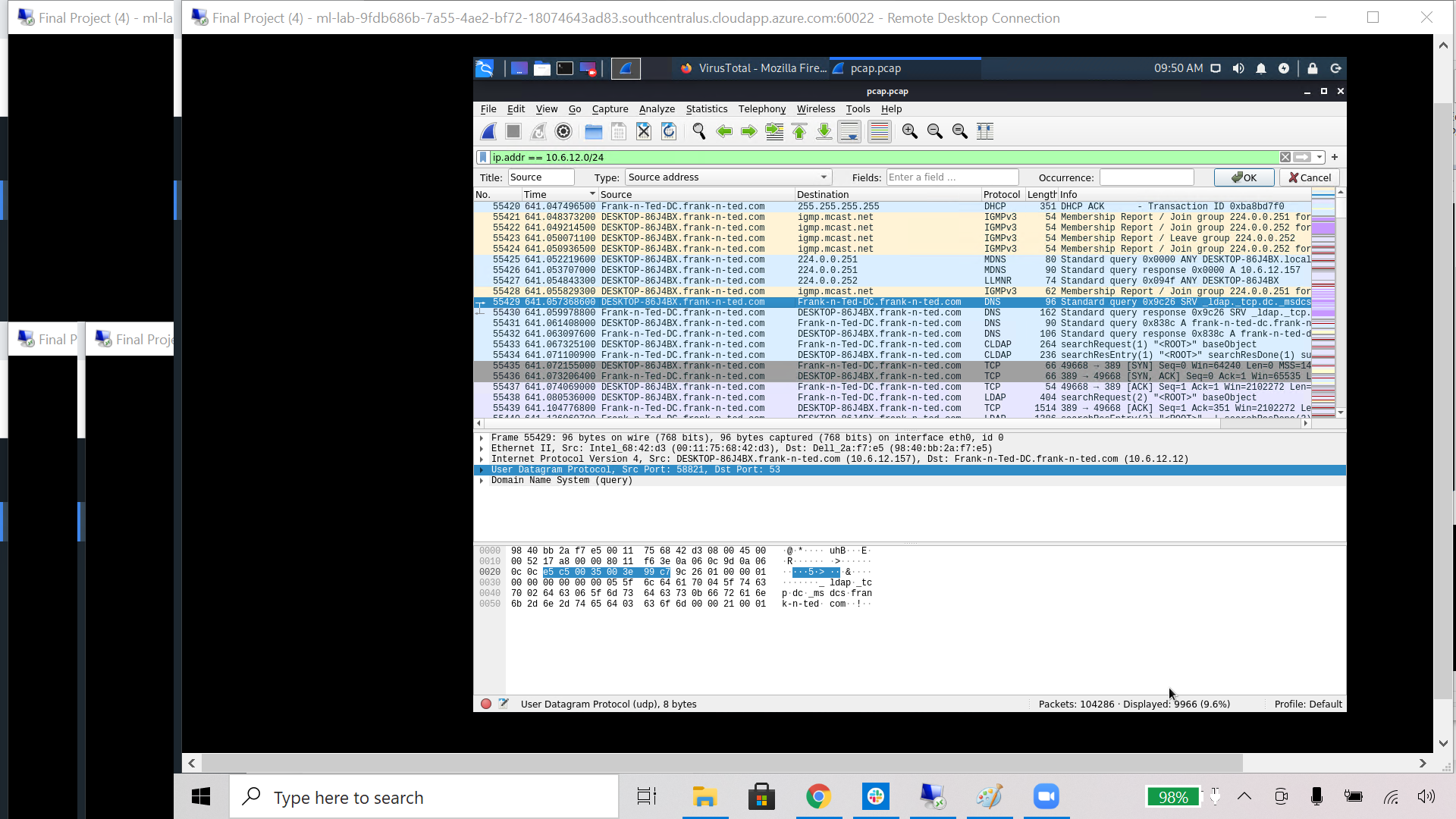
## Time Thieves

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?

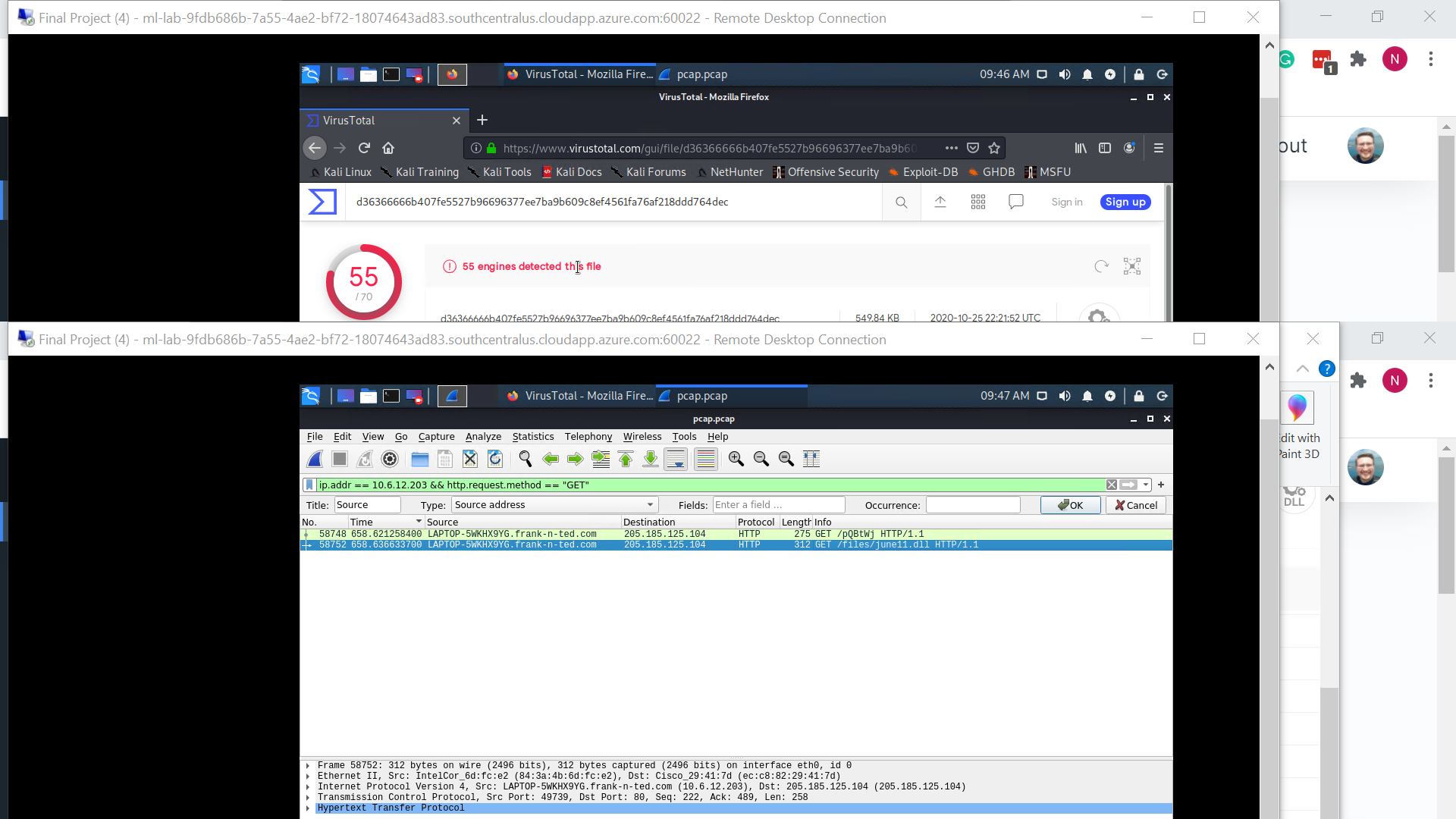


I used a basic ip address filter to filter traffic from the subnet and found the users custom site Frank-n-Ted.com.

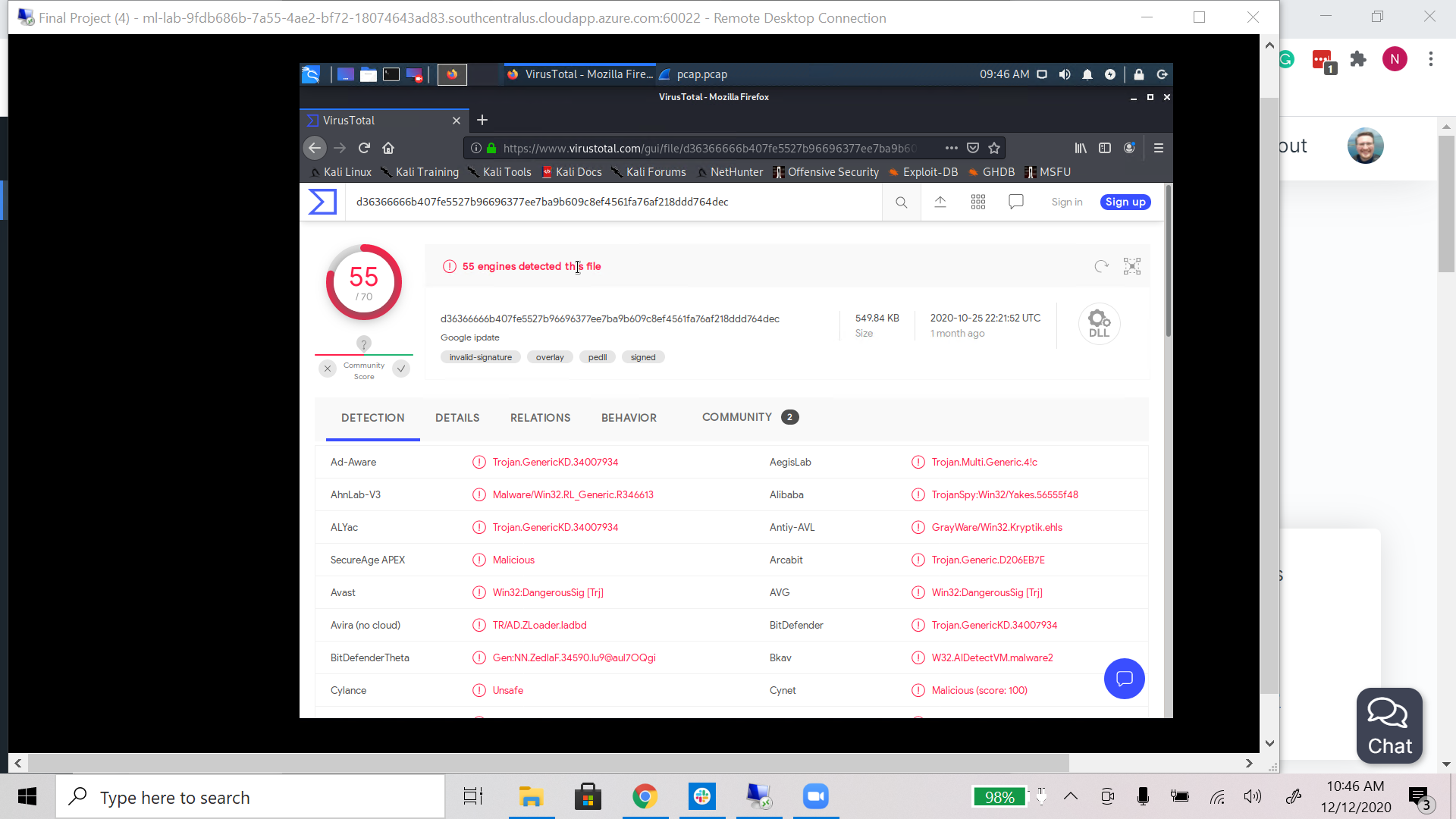
1. What is the IP address of the Domain Controller (DC) of the AD network?

In the above screen shot you can see the IP address of the rogue active directory domain controller in the IPV4 Src portion. It is 10.6.12.12. Additionally the IP address of the native domain controller is 10.6.12.1.

1. 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.



Using an ip.addr and an http.request.method get filter we can see that 10.6.12.203 downloaded june11.dll. They also downloaded an html page pqBtWj but after pulling this file it is empty.

1. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/). What kind of malware is this classified as?

As we can see the virus we uploaded is categorized by VirusTotal as a trojan with 55 different engines detecting the trojan.

#### 

#### 

#### 

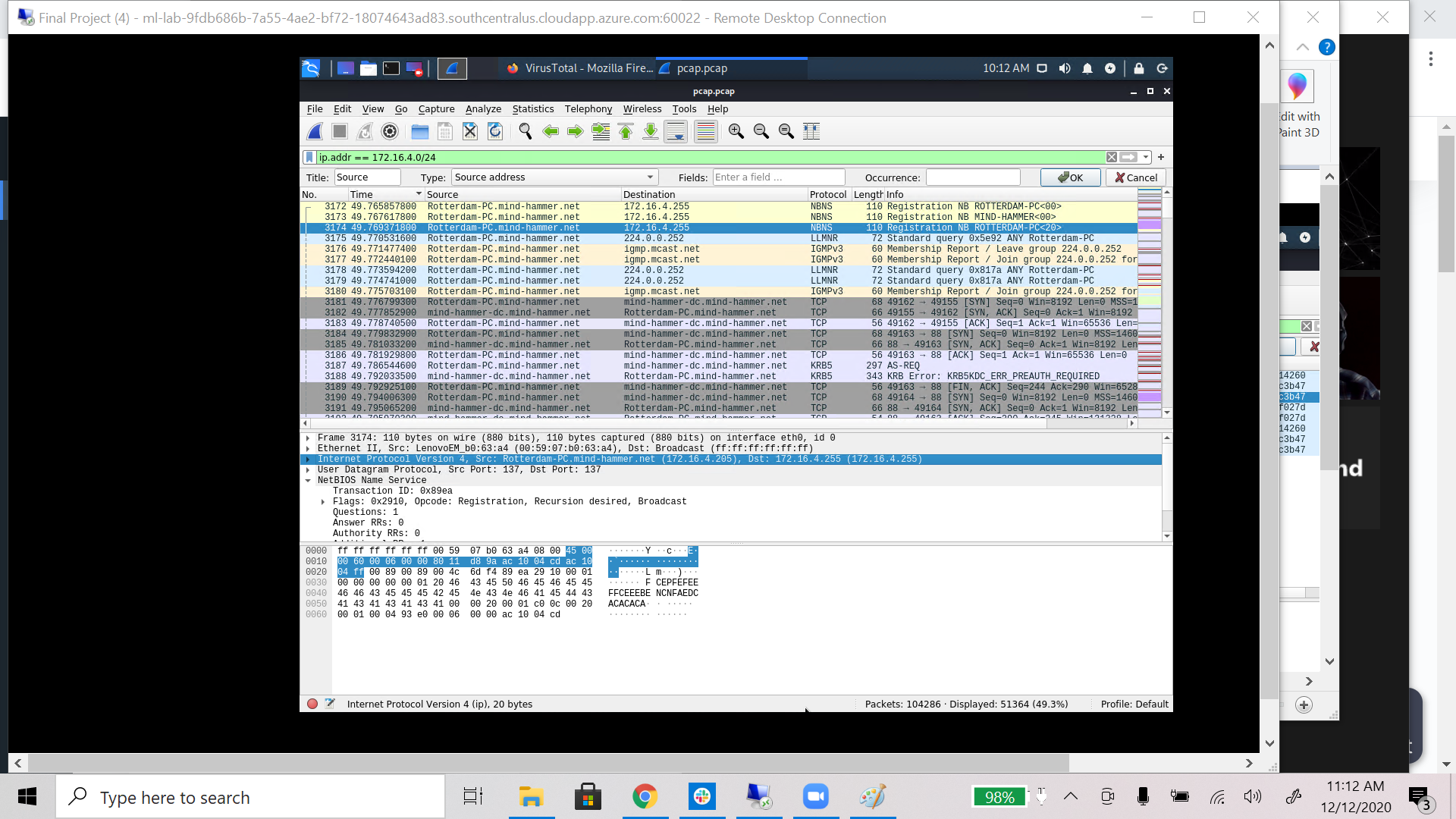
## Vulnerable Windows Machines

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:
   1. Host name: Rottardamn-PC.mind-hammer.net
   2. IP address: 172.16.4.205
   3. MAC address: 00:59:07:b0:63:a4 LenovoEM\_b0:63:a4



I have resolved host names from IPs selected which is why the username shows up for the source ip.

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

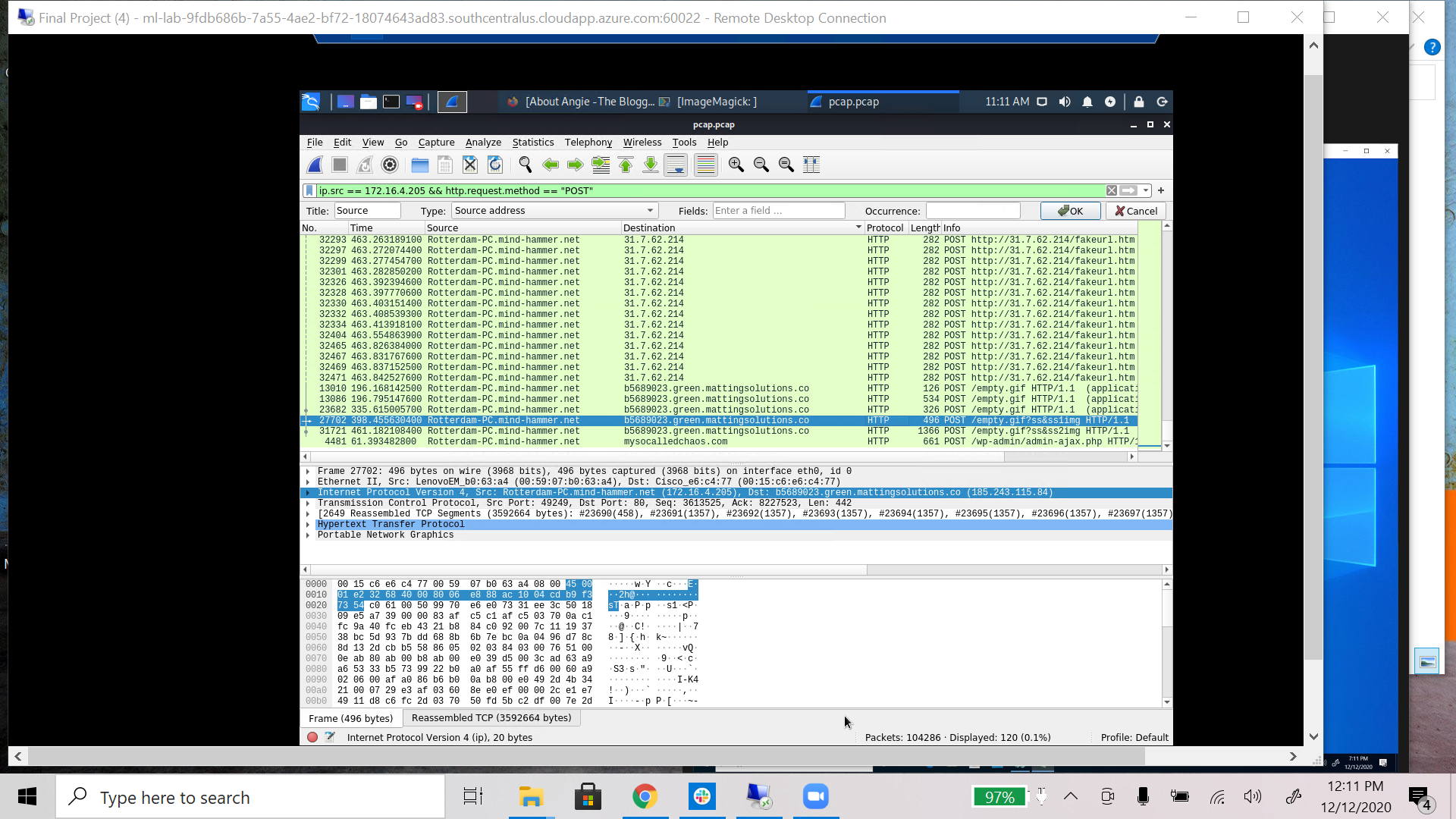
I found this PC’s name using the dhcp protocol. Inside the Host Name (option 12) you can see the target’s pc name which is Rotterdam-PC.

1. What are the IP addresses used in the actual infection traffic?

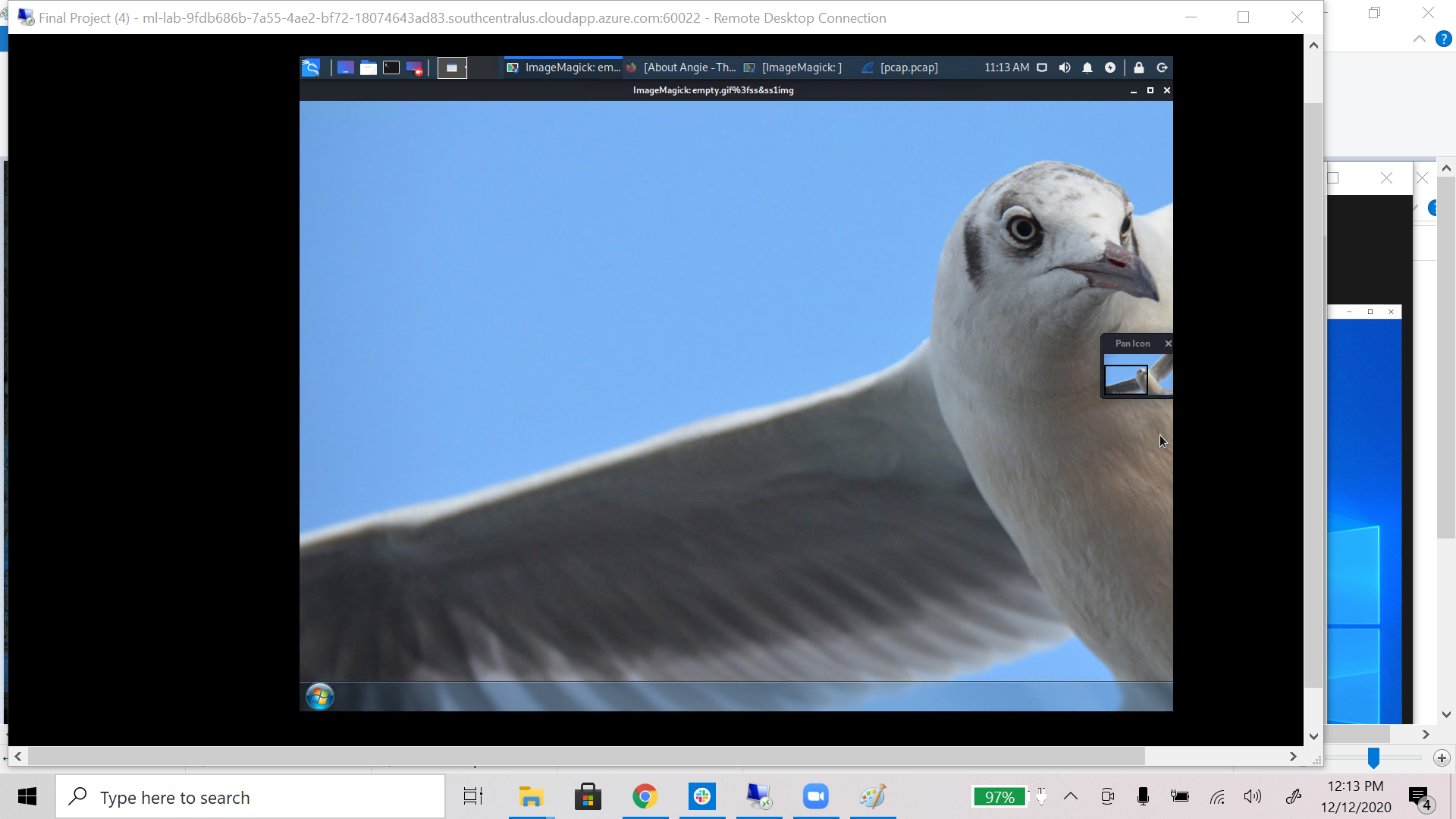
185.243.115.84 green.mattingsolutions.co -this is the device that Rotterdam-PC talks to after it is infected.

166.62.111.64 mysocalledchaos.com - this is normal network traffic. The pc routinely goes to this blog.

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

In the communications with green.mattingsolutions.co you can filter for http post requests and see that a lot of empty.gif requests have come through. When going through them two packets; packet 27702 & packet 31721 have an image file titled empty.gif?ss&ss1imp & empty.gif?ss&ss2imp.

When downloaded this image appears to be a picture of the desktop of the infected machine. This is most likely due to the infected machine remotely sending data to it’s command and control computer, green.mattingsolutions.co.



## Illegal Downloads

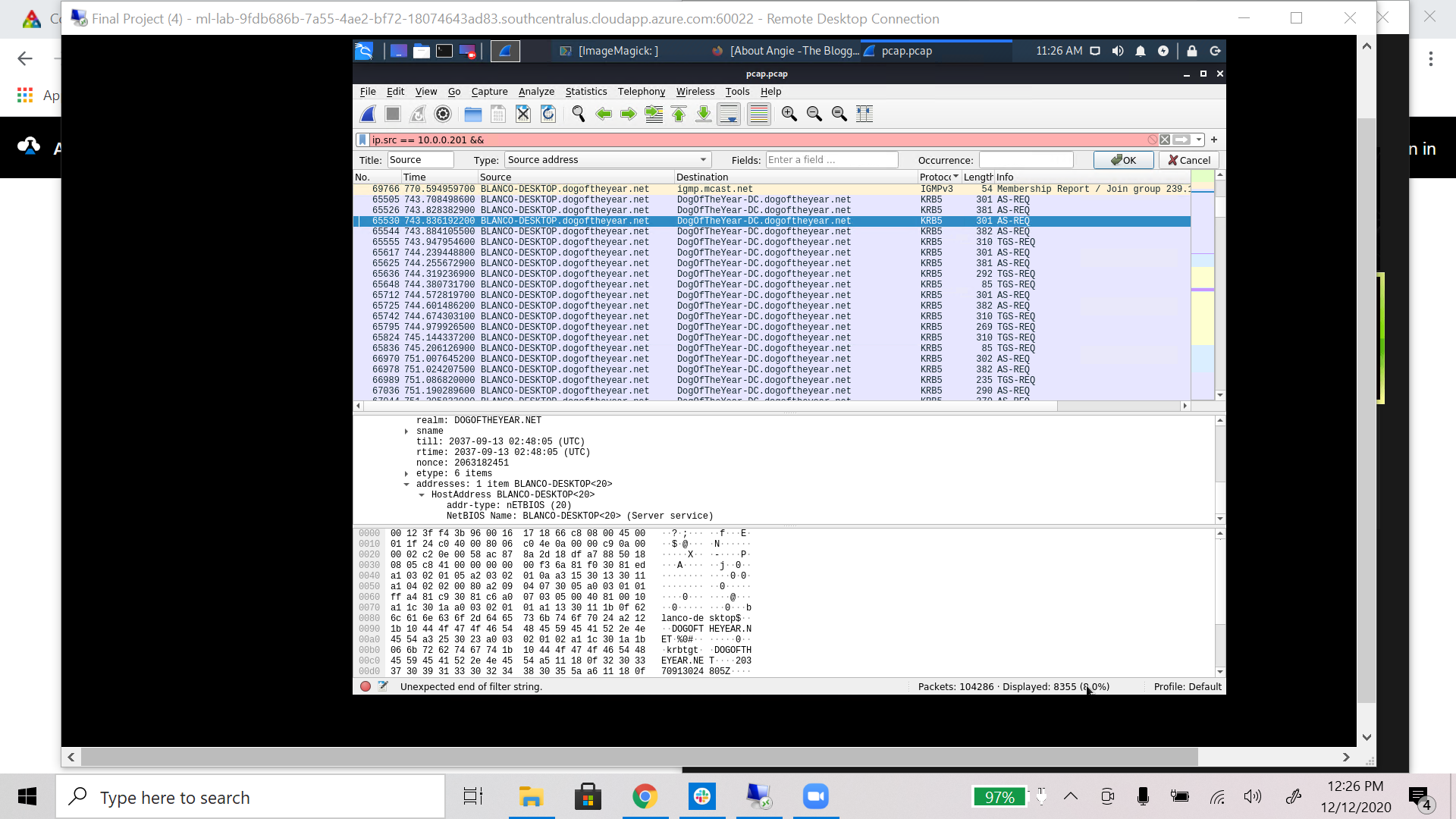
IT was informed that some users are torrenting on the network. The Security team does not forbid the use of torrents for legitimate purposes, such as downloading operating systems. However, they have a strict policy against copyright infringement.

IT shared the following about the torrent activity:

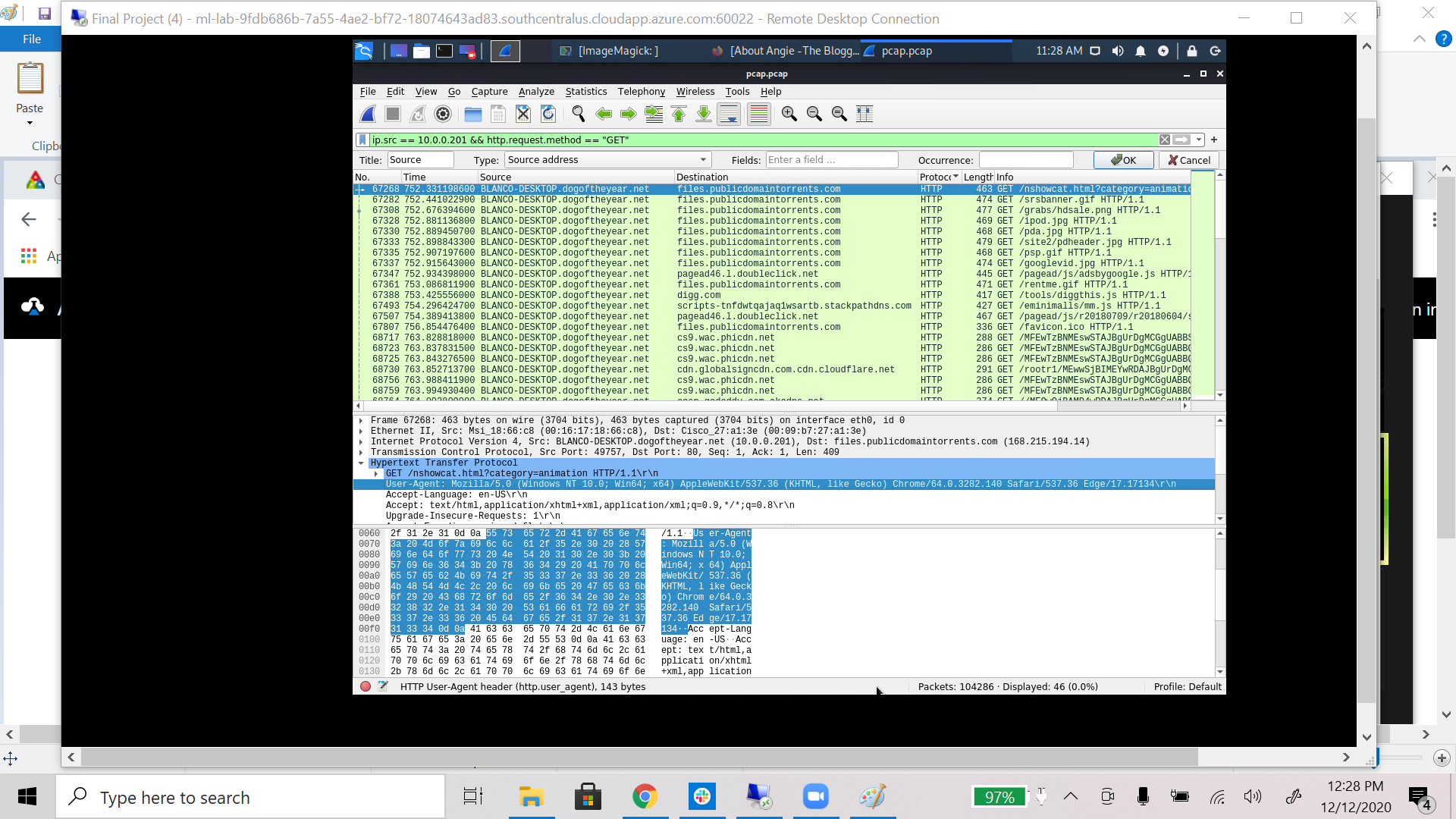
* The machines using torrents live in the range 10.0.0.0/24 and are clients of an AD domain.
* The DC of this domain lives at 10.0.0.2 and is named DogOfTheYear-DC.
* The DC is associated with the domain dogoftheyear.net.

Your task is to isolate torrent traffic and answer the following questions:

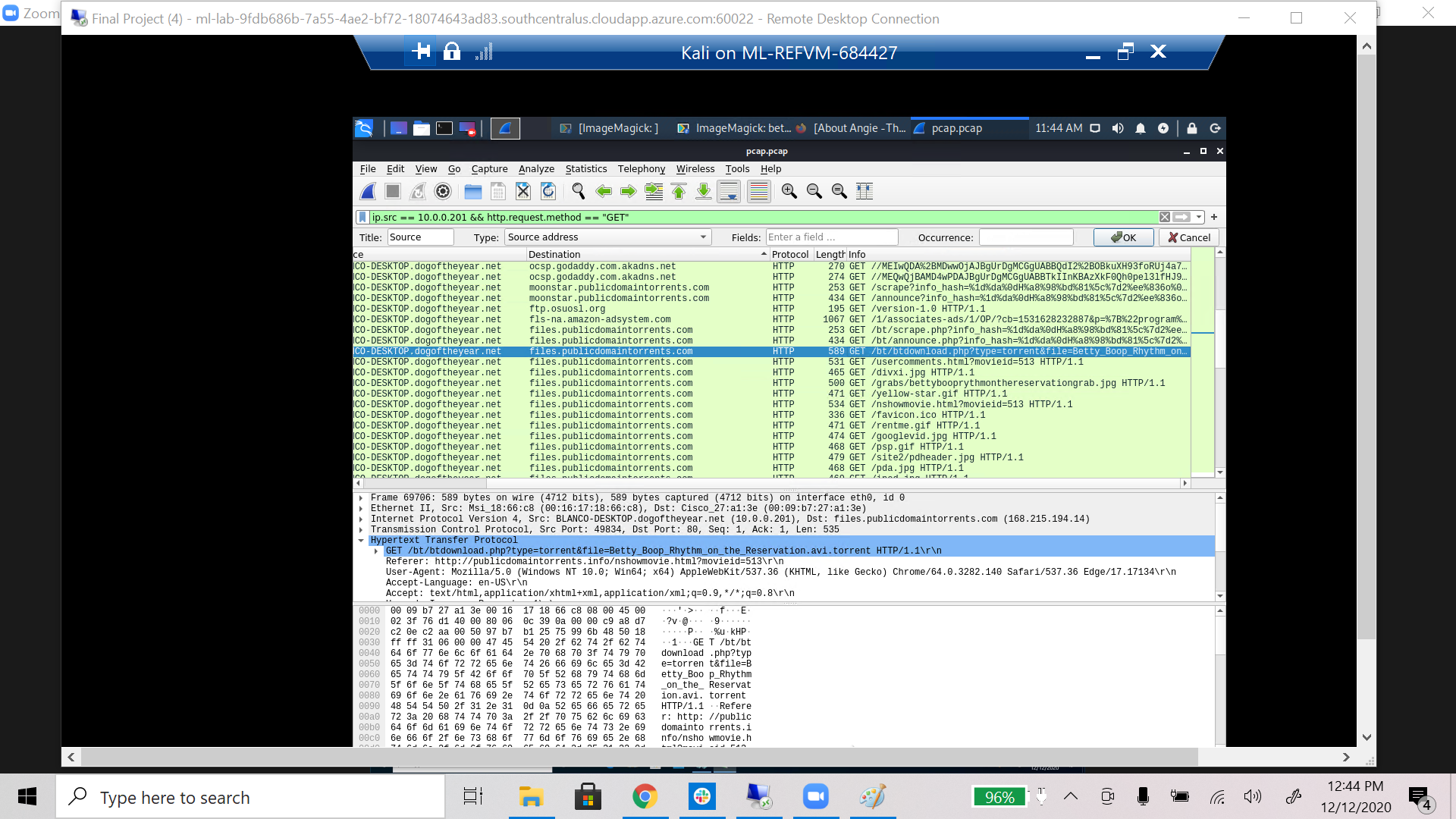
1. Find the following information about the machine with IP address 10.0.0.201:
   * MAC address: 00:16:17:18:66:c8 Msi\_18:66:c8
   * Windows username: BLANCO-DESKTOP
   * OS version: Windows NT 10.0; Win64: x64

I located the windows username, mac address and os version fairly easily. Since this is a windows computer it will use Kerberos to authenticate. Using that knowledge we can find the KRB5 protocol and under addresses you can see the host address and NetBios name BLANCO-DESKTOP. 

In order to find the OS version I did a simple HTTP Request filter. Knowing HTTP request protocol structure we can see inside the User-Agent portion not only the browser they are using but also the OS they are running.



1. Which torrent file did the user download?

In order to find the torrents that we downloaded I browsed through the http get requests using a very similar filter as above. In this filter I sorted by destination. This brought me a lot of torrent sites. 

From here we can see that only two torrents are really accessed. One is hidden via a torrent hash, the other a download from publicdomaintorrents.com. While this is not technically illegal as public domain content is past it’s copyright life. It is still worrying because it could be illegal. The hidden torrent can be found using google to be a linux torrent which is not an illegal act and has been deemed fine by the security team.

Going into the files exported via wireshark we can find a .avi file that shows various screen grabs from the torrented movie. This is not work and has the potential to be dangerous as you are torrenting content.

