* Network Forensic Analysis Report

Complete this report as you complete the Network Activity on Day 3 of class.

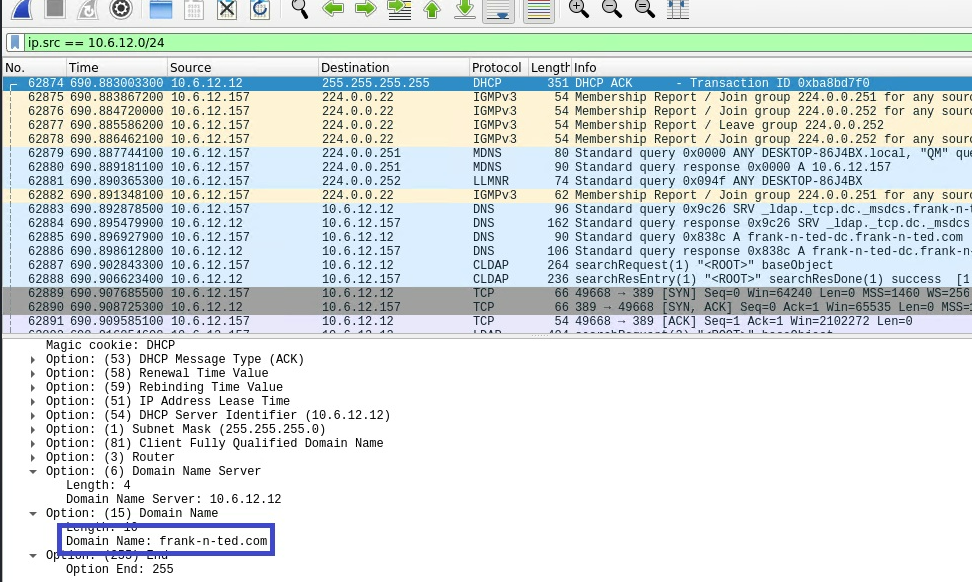
* Time Thieves

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

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

Ans. **frank-n-ted.com**

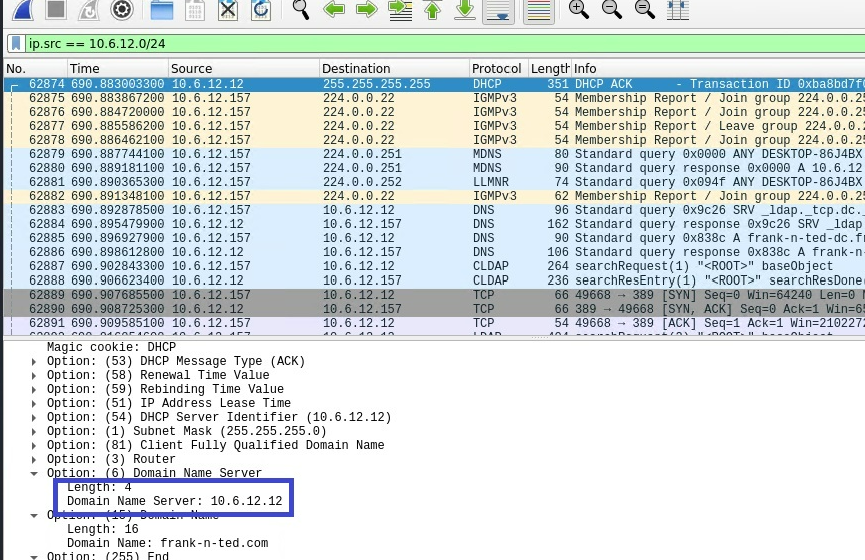
Filter: **ip.src==10.6.12.0/24 or ip.addr==10.6.12.0/24**



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

Ans. **10.6.12.12**

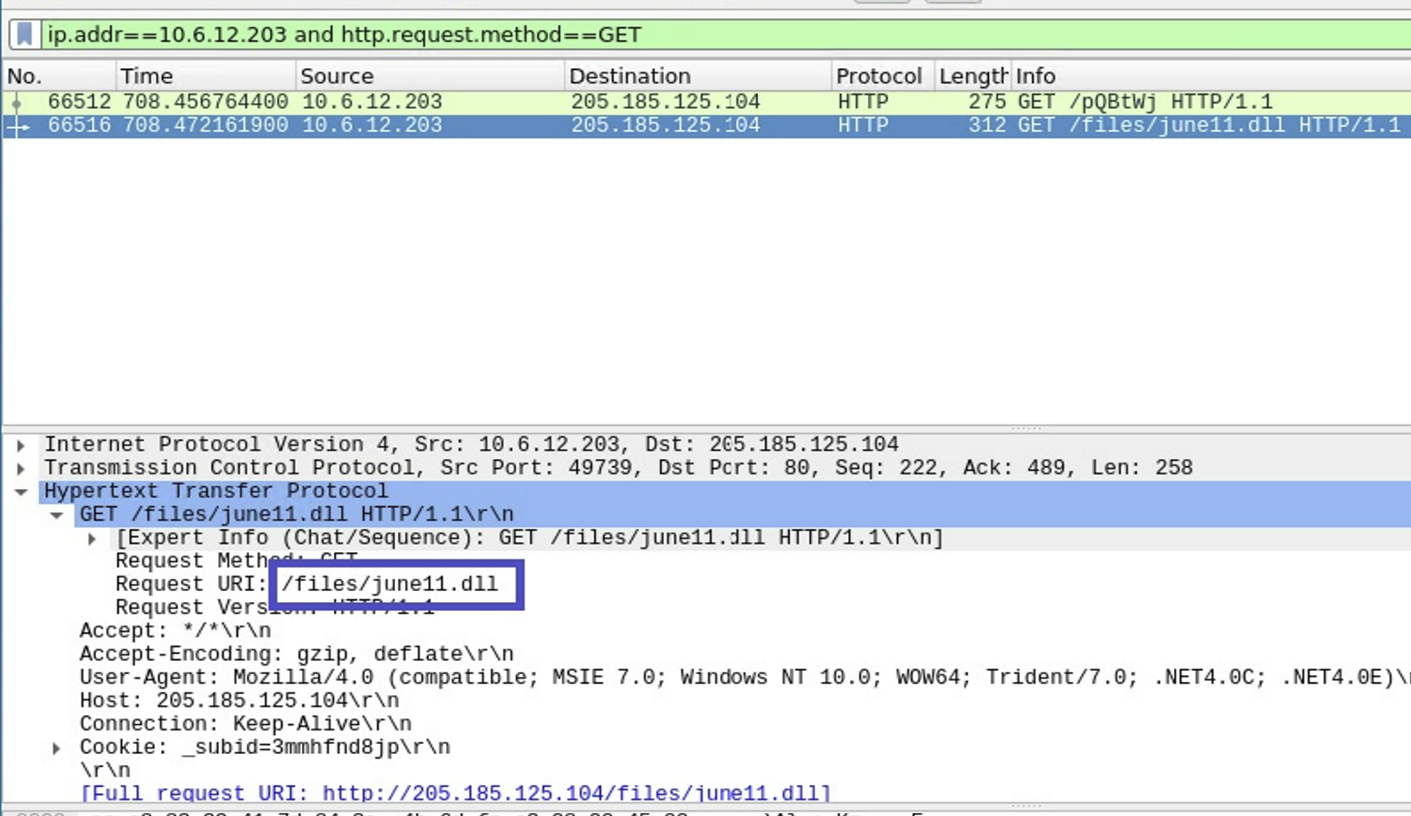
Filter: **ip.src==10.6.12.0/24 or ip.addr==10.6.12.0/24**



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

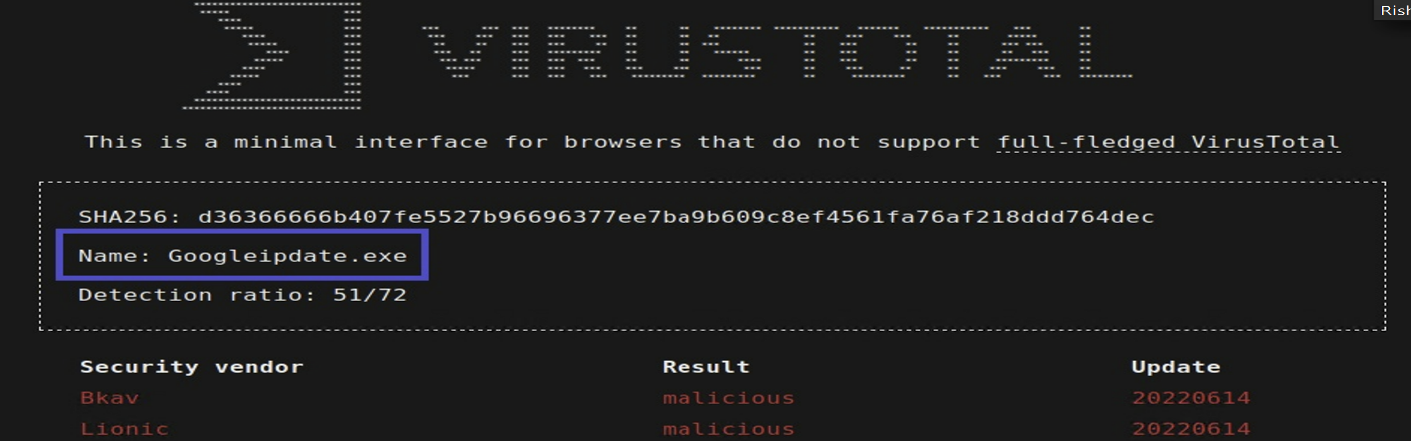
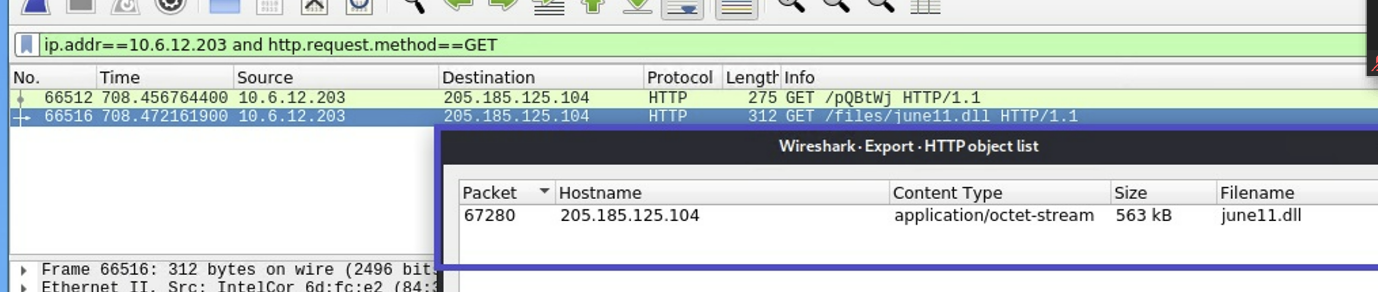
Ans. **june11.dll**

Filter: **ip.addr==10.6.12.203 and http.request.method==GET**



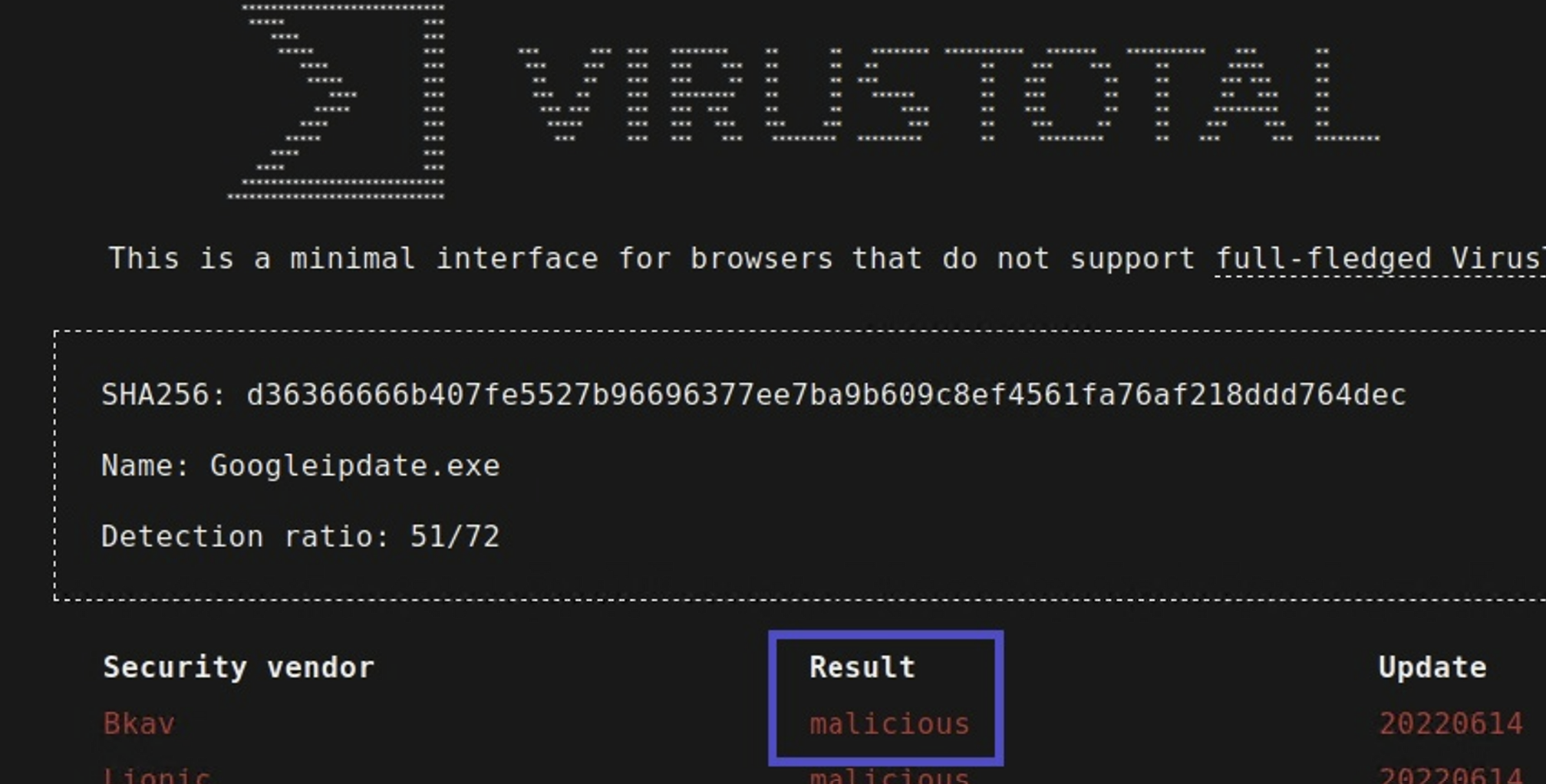
4. Upload the file to [VirusTotal.com](https://www.virustotal.com/gui/).

Ans. **Googleupdate**



5. What kind of malware is this classified as?

Ans. **Malicious**



---

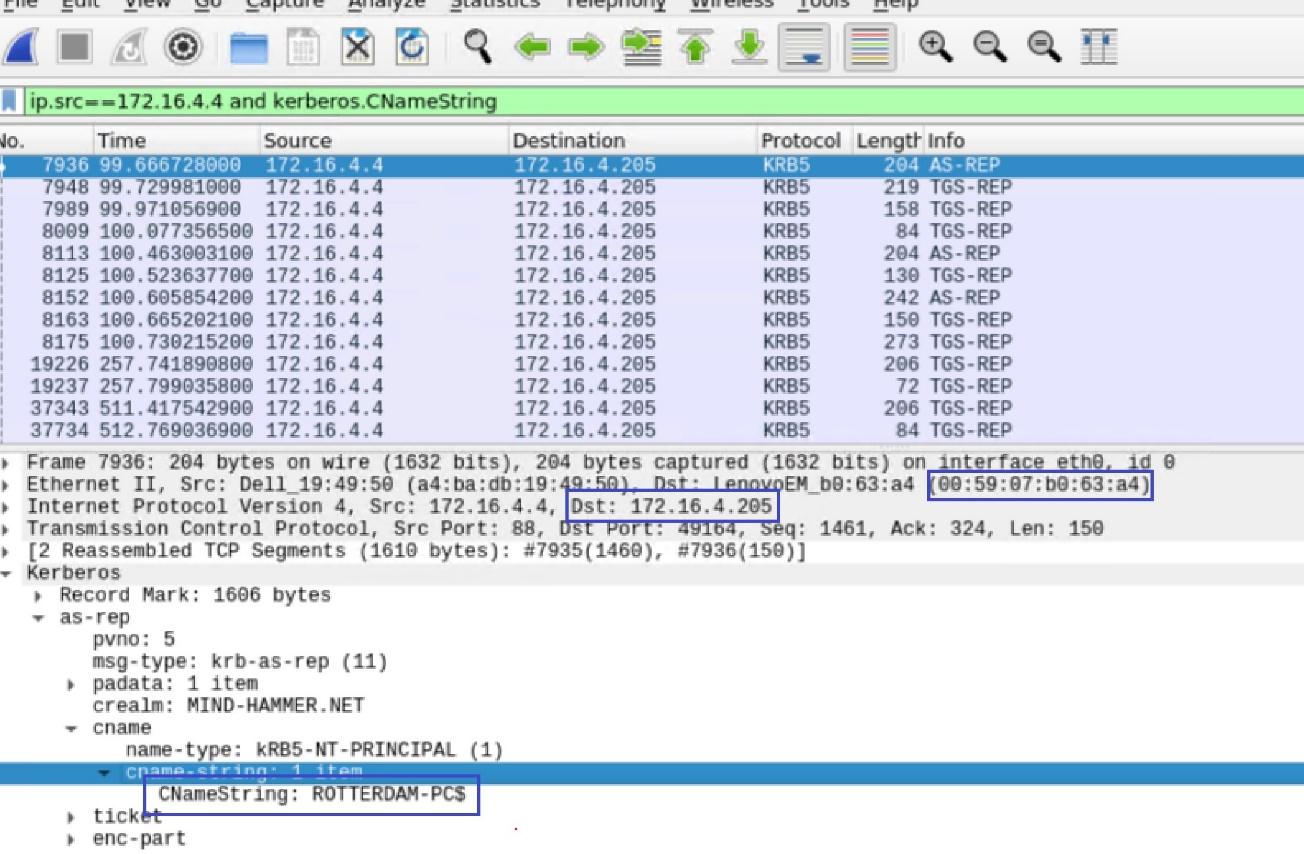
## Vulnerable Windows Machine

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?

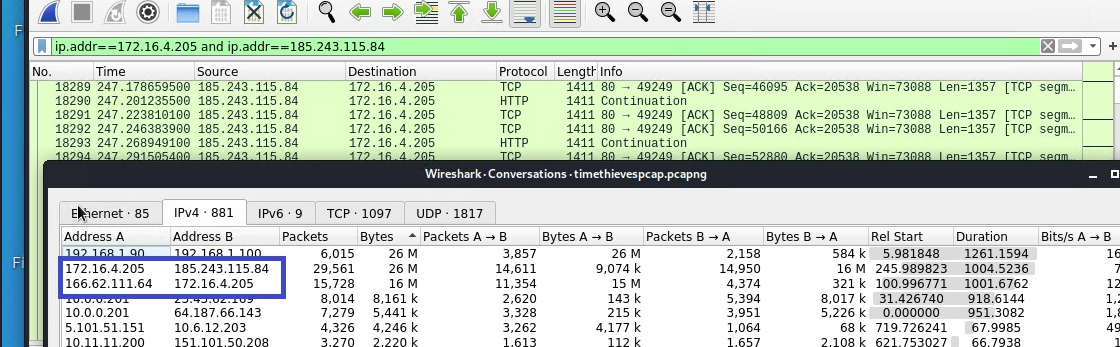
Ans:

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

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

Ans. IP addresses used in the actual infection traffic are:

* + - * **166.62.111.64**
      * **172.16.4.205**
      * **185.243.115.84**



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

Ans. **Two Windows desktop background were retrieved by exporting objects: File > Export Objects > HTTP** 