**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?

A picture containing text

Description automatically generated- frank-n-ted.com

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

- 10.6.12.12

Text

Description automatically generated

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.

* june11.dll
* Graphical user interface, application, table

  Description automatically generatedTo export: FIle. Export Objects. HTTP. Search June and save

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

* Graphical user interface, text

  Description automatically generatedMalware has been identified as a trojan horse.

**Vulnerable Windows Machine**

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

* Host name: Rotterdam-PC
* IP address: 172.16.4.205
* Graphical user interface, application, table

  Description automatically generatedMAC address: 00 :59:07:b0:63:a4

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

* Table

  Description automatically generatedmatthijs.devries

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

* 31.7.62.214
* 166.62.111.64
* Graphical user interface, table

  Description automatically generated with medium confidence185.243.11.84

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

* Graphical user interface, text, application

  Description automatically generatedFound image with ‘ip.addr ==172.16.4.205 && http.request.method == POST’ find the post that indicates to be an image. Export Image with ‘export objects, http’

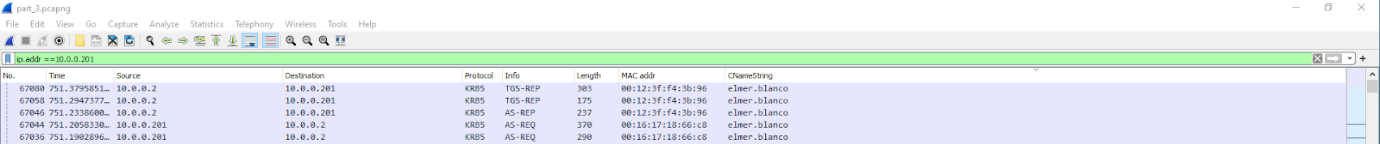
A picture containing sky, bird, outdoor, gallinaceous bird

Description automatically generated

**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
* Graphical user interface, table

  Description automatically generatedOS version: Windows NT 10.0 x64

1. Which torrent file did the user download?

* Betty\_Boop\_Rhythm\_on\_the\_Reservation.avi

Graphical user interface, application, table

Description automatically generated