# **Network Analysis: Summary of Operations**

## 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?

* 10.6.12.157(DESKTOP-86J4BX IP address) > 10.6.12.12 (DC IP Address): frank-n-ted.com

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

* From “Frank-n-Ted-DC.frank-n-ted.com”: The IP Address is 10.6.12.12

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.

* There is a file that was uploaded called june11.dll

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

* The Malware is considered a Trojan Spy from many of the detection sites.