Introduction

A Windows system has shown some unusual behavior. A colleague has already recorded network traffic and has taken a full memory dump with FTK Imager of the system.

In the resources section you will find the zip file of your colleague. It contains the following files:

- memdump.mem: the memory dump of the suspicious system
- traffic_memdump.pcap: the PCAP dump of the network traffic of the suspicious system
- checksums.sha256: SHA-256 checksums for any binary files required for this task

Goal & Tasks

Investigate and analyze the given files for suspicious activity and reply to the following four topics directly in the template from the resources section.

- Identify running suspicious processes and explain briefly why they are unusual.
- Identify the origin / file path from which the malicious activity started. If you cannot find the malicious program, provide the full path of the executable FTK Imager.exe instead. Provide the commands you used.
- According to the log files it seems that the malware has been downloaded as a zip file. What is the full URL of the download?
- Investigate the traffic and provide the SHA256 hashes of suspected malicious files.

Hint: The following volatility commands might get you started (replace 'XXX' with the correct profile):

```
# Volatility is written in Python, and is executed using the following syntax:
# vol.py -f [name of image file] --profile=[profile] [plugin]
volatility -f memdump.mem imageinfo
volatility -f memdump.mem --profile 'XXX'
volatility -f memdump.mem --profile 'XXX' pslist
volatility -f memdump.mem --profile 'XXX' --help
```