Introduction

Some computers of Batnet Laboratories Inc. were compromised by an unidentified actor. Therefore, the infection has to be investigated forensically based on a given memory image.

Goals and Tasks

Investigate the given memory image in the resources section with Volatility 2.6.1 and the profile Win10x64_17763 by performing the following tasks. Answer to all questions in a written report. Make sure that your answers can be clearly assigned to the task numbers and to provide a proof of evidence for your answers (e.g., used command or plugin, screenshots with results).

- What date and time the infected memory image was collected?
- Which plugin of Volatility generates a list of processes as a tree?
- What is the IP address of the investigated computer?
- What is the name and the PID of the malicious process?
  - Hint: Identify the process through command line executions plugin.
- List a maximum of 5 additional executables that reside in the same path as the malicious process and that have the same execution timestamp as the malicious process.
  - Hint: Check timestamps of execution in the Master File Table (MFT).
- Dump the malicious process into a file and search the file for a suspicious ASCII URL string that most likely is hosting other malware components. What's the registrar of that domain? Record the ASCII URL and the domain name registrar.
- Which of the DLLs linked to the malicious process is most likely responsible for initiating HTTP Internet connections?
- What is the SID of the user account under which the process was executed?

Submission

Submit a report with your results as PDF document. Make sure that your answers can be clearly assigned to the question numbers in the goal and task section.