Summary

I will make a forensic analysis on a machine that has been compromised by a cyber attack scenario. I will use virtualization tools such as VirtualBox, Windows and Linux command line tools, plus some forensics and data manipulation tools.

Important!!!: There are some timelines inconsistencies because the .pdfs are made over several days. But the forensic techniques are in place for analysis.

Update:

New possible Timeline acquired because of Shellbags:

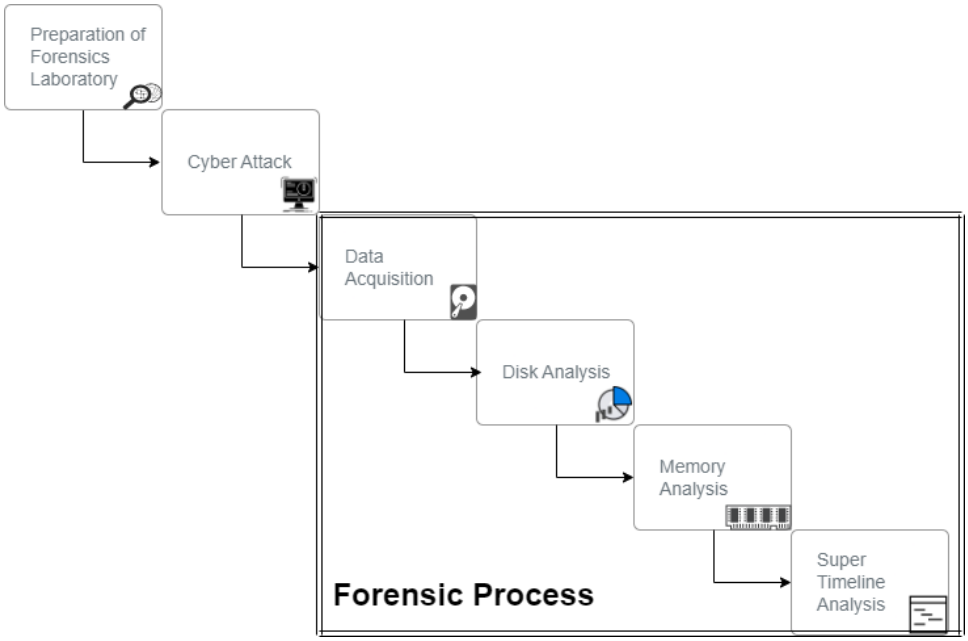
2023-02-13 17:21:03

2023-02-13 17:26:03

I followed the tutorial of BlueCapeSecurity. You can review different kinds of tutorials about DFIR (Digital Forensics and Incident Response).

The tools needed to conduct a forensic analysis I have used are either freeware, on trial or for personal use only.

Steps



Lab Setup

- System Requirements:
  - 4 GB RAM
  - 150 GB Storage (Dynamically Allocated)
    - Compromised System:
      - 40 GB Disk
      - 4 GB RAM
    - Forensics System:
      - 100 GB Disk
      - 4 GB RAM

The more the system resources allocation the better. I have used this resources on my lab setup:

- Forensics Workstation:
  - 120 GB Disk
  - 8 GB RAM
- Compromised Host:
  - 40 GB Disk
  - 4 GB RAM

On the Forensics Workstation you will need around 120 GB Disk for the images of the disk and memory. The more the better. The VMs does not need to be running at the same time.