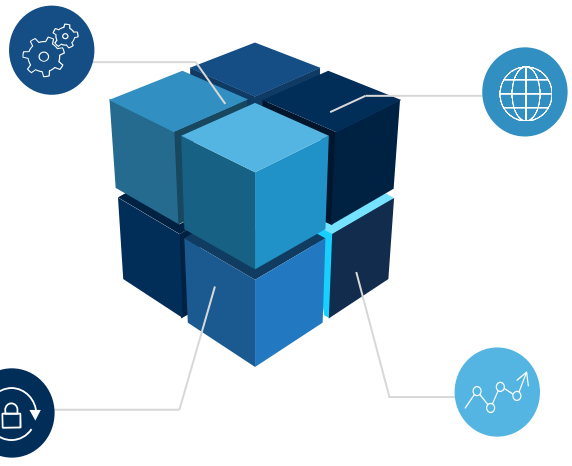
OPERATION ORDER

Computer investigations are based on the investigator's ability to extract information from the investigated computer using automation, we can reduce errors and extract useful information faster.

1. VISION

Cyber units operating in an automated way.



2. MISSION

Working with memory and HDD files and performing automatic analysis.

3. STRATEGY

Using automation tools, which extract sensitive information and present the findings to the researcher.

4. OBJECTIVES

- File Analysis: Memory, HDD, and general files
- Using carvers to extract sensitive information
- Analyzing memory using Volatility
- All information should be saved in an easy way for the investigator to work

Project Structure

1. Automate HDD and Memory Analysis
    - 1.1 Check the current user; exit if not 'root'
    - 1.2 Allow the user to specify the filename; check if the file exists
    - 1.3 Create a function to install the forensics tools if missing
    - 1.4 Use different carvers to automatically extract data
    - 1.5 Data should be saved into a directory
    - 1.6 Attempt to extract network traffic; if found, display to the user the location and size
    - 1.7 Check for human-readable (exe files, passwords, usernames, etc.)

2. Memory Analysis with Volatility
    - 2.1 Check if the file can be analyzed in Volatility; if yes, run Volatility
    - 2.2 Find the memory profile and save it into a variable
    - 2.3 Display the running processes
    - 2.4 Display network connections
    - 2.5 Attempt to extract registry information

3. Results
    - 3.1 Display general statistics (time of analysis, number of found files, etc.)
    - 3.2 Save all the results into a report (name, files extracted, etc.)
    - 3.3 Zip the extracted files and the report file

4. Creativity

General

- Suggested tools: Bulk Extractor, Binwalk, Foremost, Strings, Volatility.
- Everything other than the user input should be automated.
- Use functions.

Comments

Use comments in your code to explain what you did.
If you are using code from the internet, add credit and links.
In the script, write the student's name and code, the class code, and the lecturer's name.

Submitting

Submit the source code (.sh) and a pdf file with screenshots proving the functions work.
Send the project to the trainer's email.
In the email subject type project: **Analyzer <student name>.**