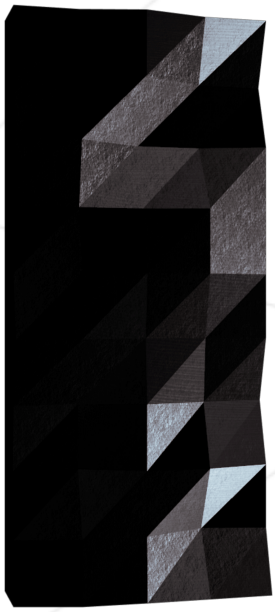

Bootcamp Ciberseguridad | 42 Madrid

recovery

Summary: Evidence gathering

Version: 1

Contents

Chapter I

Foreword

"social engineering" — the casual or calculated manipulation of people to influence them to do things they would not ordinarily do. And convincing them without raising the least hint of suspicion.

Source: https://es.wikipedia.org/wiki/Kevin_Mitnick

Chapter II

Introduction

Evidence gathering is an essential process that has to be done before performing any kind of forensics analysis. Having the evidence clear and organized will make your labor easier. The objective of this project is making a program that is able to extract some artifacts on a given time lapse:

`General Instructions`

You'll always work on a Win10 VM. You can use a Vagrant machine for ex this one. You are allowed to use any programming language. In case you decide to use a compiled language you will have to hand in your source code and it will be compiled during the evaluation.

You are allowed to use any library that helps you develop this tool, however you have to be able to justify why you are using them during the evaluation.

Chapter III

Mandatory Part

III.1 recovery

You will have to develop a program that extracts the following artifacts on a given time lapse:

- Registry branches changes date (CurrentVersionRun)
- Recent used/opened files.
- Installed programs
- Processes on execution
- Web browser history
- Connected devices
- Events logs

If the user doesnt give your program a time range it should fall back to a default value, for ex: last 24h, last week, last month...

Chapter IV

Bonus Part

Bonus evaluations will only be done if your mandatory part is `PERFECT`. Otherwise bonuses will be IGNORED.

You can improve your project with the following functionalities:

- Compose a time line where all the evidence is displayed organized by categories and time.
- Show the directory tree on some kind of graphic view

Chapter V

Peer evaluation

This project will be evaluated by your peers. Hand in your files on the git repo and make sure everything works as expected.