TP1: Memory Dumping

1. Before we begin

In this **Practice**, we'll achieve a memory dump with two different tools.

2. What we'll learn

⊡ How to create a memory dump or RAM capturing using dedicated tools.

3. How to create a memory dump:

Capturing the RAM from a physical device can be done using several tools, among of them:

- WinPmem[1].

To begin a memory capture use the following command in CMD prompt to create a raw output file.

```
C:/ winpmem_mini_x64.exe  <filename>.raw
```

- JumpBag[2]

For JumpBag we execute **DumpIt.exe** to launch a memory dump then type **y**es for the interactive question and the memory image will be created.

[1] https://github.com/Velocidex/WinPmem/releases

[2] https://sourceforge.net/projects/jumpbag/