

TP : Volatility

1) Testez et expliquez en détail le format et les résultats des commandes suivantes.

```
C:\Users\UtecPC\volatility3> python .\vol.py -f .\CC_Niveau2.dmp windows.info
```

```
C:\Users\UtecPC\volatility3> python .\vol.py -f .\CC_Niveau2.dmp windows.pslist
```

```
python vol.py -f CC_Niveau2.dmp windows.pstree
```

```
C:\Users\UtecPC\volatility3> python .\vol.py -f .\CC_Niveau2.dmp windows.handles --pid 1136 | more
```

```
python .\vol.py -f .\CC_Niveau2.dmp windows.handles --pid 1136 | select-string File | more
```

```
python .\vol.py -f .\CC_Niveau2.dmp windows.handles --pid 1136 | select-string File | select-string "John Doe"
```

```
python .\vol.py -f .\CC_Niveau2.dmp -o "fichiers_dump" windows.dumpfile --pid 1136 --virtaddr 0x87c4a1e0
```

```
python .\vol.py -f .\CC_Niveau2.dmp windows.cmdline | more
```

```
python .\vol.py -f .\CC_Niveau2.dmp windows.registry.userassist.UserAssist | more
```

```
python .\vol.py -f .\CC_Niveau2.dmp windows.hashdump | more
```

```
python vol.py -f CC_Niveau2.dmp windows.registry.hivelist
```

```
python vol.py -f .\CC_Niveau2.dmp windows.registry.printkey --offset 0x8b21c008 --key "ControlSet001\Control\ComputerName\ComputerName"
```

2) Votre tâche consiste à réaliser les challenges 3 et 4. Pour ce faire, vous devrez adapter les solutions Volatility 2 présentes dans le fichier PDF fourni afin qu'elles fonctionnent avec Volatility 3. Expliquez chaque étape.