1. A quelle heure ai-je démarré mon PC (format attendu MCTF{hh:mm:ss} ?
2. Quelle processus a exécuté le bloc note (format attendu MCTF{PID_DU_PROCESSUS})?
3. Quel est le nom du PC (format attendu MCTF{HOSTNAME})?
4. Les attaquants persistent souvent à l'intérieur… (format attendu MCTF{Flag_trouver})
5. Le flag a été inscrit sur le bloc-notes. (format attendu MCTF{Flag_trouver})
6. Un utilisateur flag807 a été créé, pouvez-vous me dire à quelle date à t-il été créé (format attendu MCTF{dd:mm:aaaa}) ?

Utilisation de volatility

1. A quelle heure ai-je démarré mon PC (format attendu MCTF{hh:mm:ss} ?

```
vol.py -f dump.raw --profile=Win10x64_19041 pslist  voir le process système
12:31:34
```

2. Quelle processus a exécuté le bloc note (format attendu MCTF{PID_DU_PROCESSUS})?

```
vol.py -f dump.raw --profile=Win10x64_19041 pstree
PID 5080
```

3. Quel est le nom du PC (format attendu MCTF{HOSTNAME})?

```
vol.py -f dump.raw --profile=Win10x64_19041 printkey -K
"ControlSet001\Control\ComputerName\ActiveComputerName"
DESKTOP-8Q3PC39
```

4. Les attaquants persistent souvent à l'intérieur… (format attendu MCTF{Flag_trouver})

```
vol.py -f dump.raw --profile=Win10x64_19041 printkey -K
"SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
flag{807forever}
```

5. Le flag a été inscrit sur le bloc-notes. (format attendu MCTF{Flag_trouver})

```
vol.py -f dump.raw --profile=Win10x64_19041 memdump dans la mémoire de notepad
flag{Azerty807}
```

6. Un utilisateur flag807 a été créé, pouvez-vous me dire à quelle date à t-il été créé (format attendu MCTF{dd:mm:aaaa}) ?

```
vol.py -f dump.raw --profile=Win10x64_19041 timeliner | grep flag807
18:06:2023
```