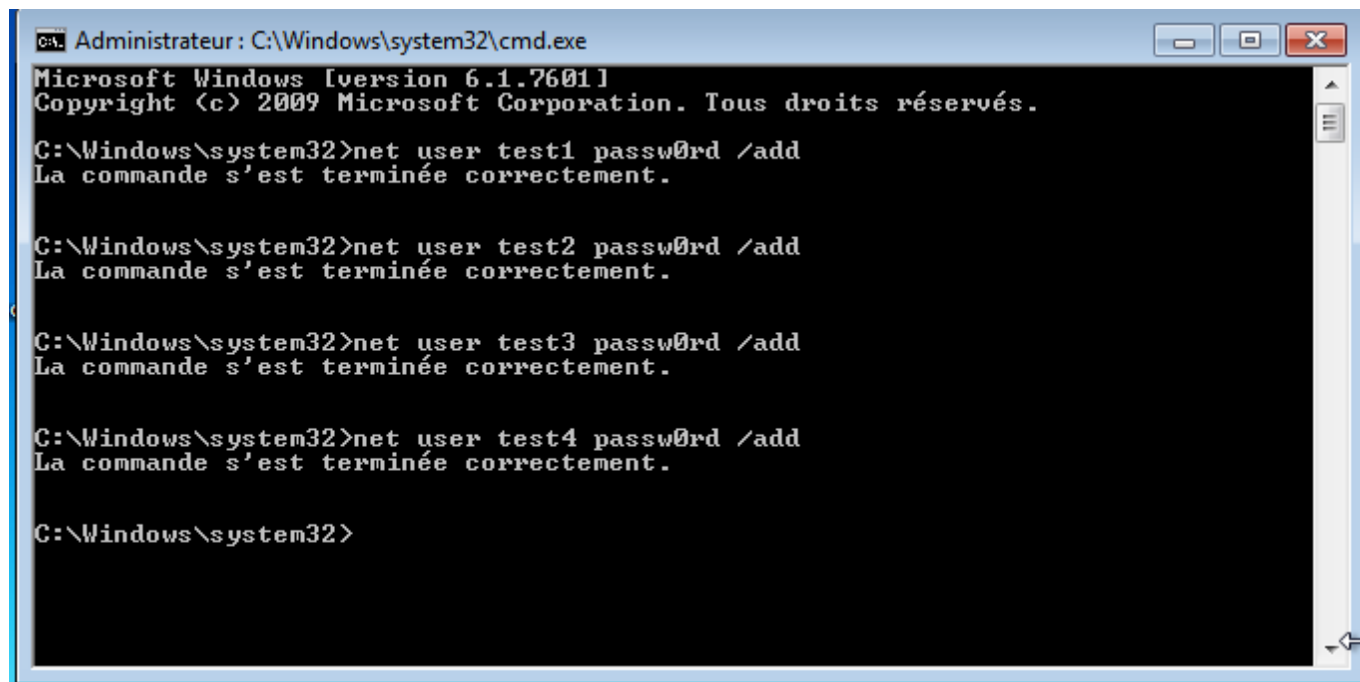


SAE6C01 - Image mémoire

J'ai installé une machine virtuelle sous Windows 7 pour réaliser cet exercice.

2. Création des utilisateurs locaux

J'ai crée les utilisateurs suivants:



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>net user test1 password /add
La commande s'est terminée correctement.

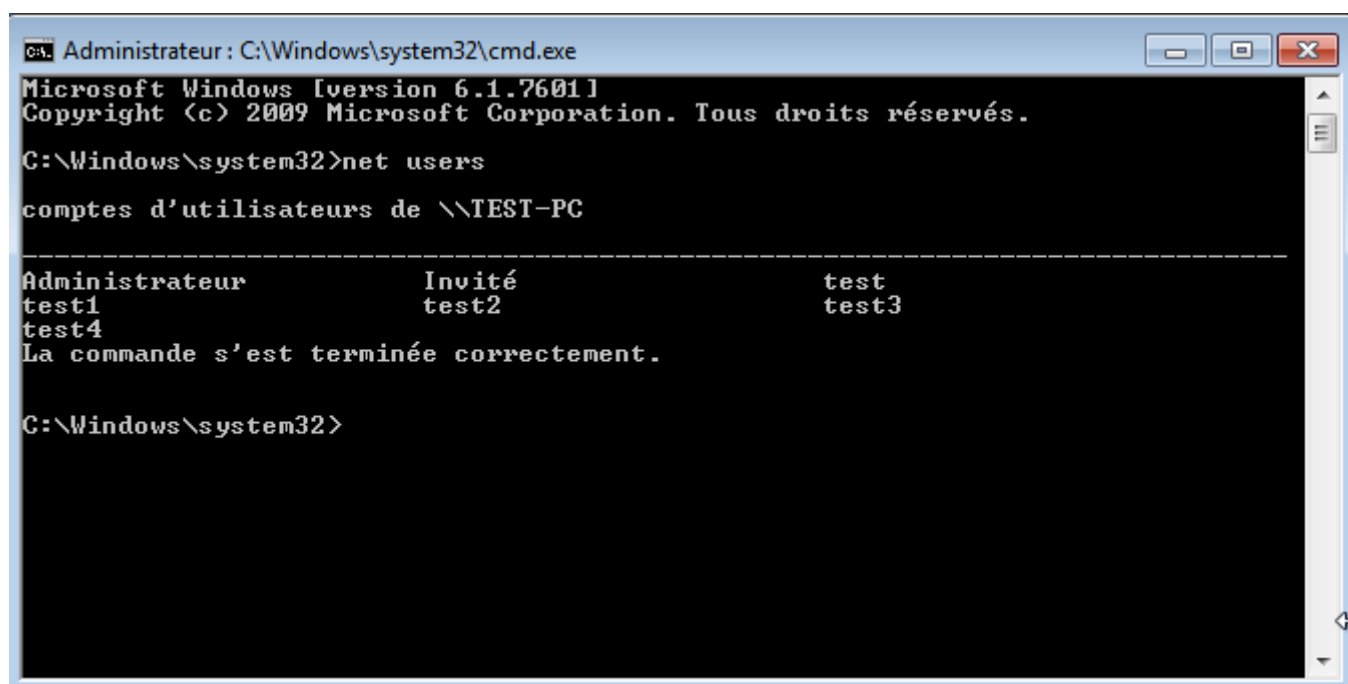
C:\Windows\system32>net user test2 password /add
La commande s'est terminée correctement.

C:\Windows\system32>net user test3 password /add
La commande s'est terminée correctement.

C:\Windows\system32>net user test4 password /add
La commande s'est terminée correctement.

C:\Windows\system32>
```

3. Vérification de la liste des utilisateurs



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>net users
comptes d'utilisateurs de \\TEST-PC

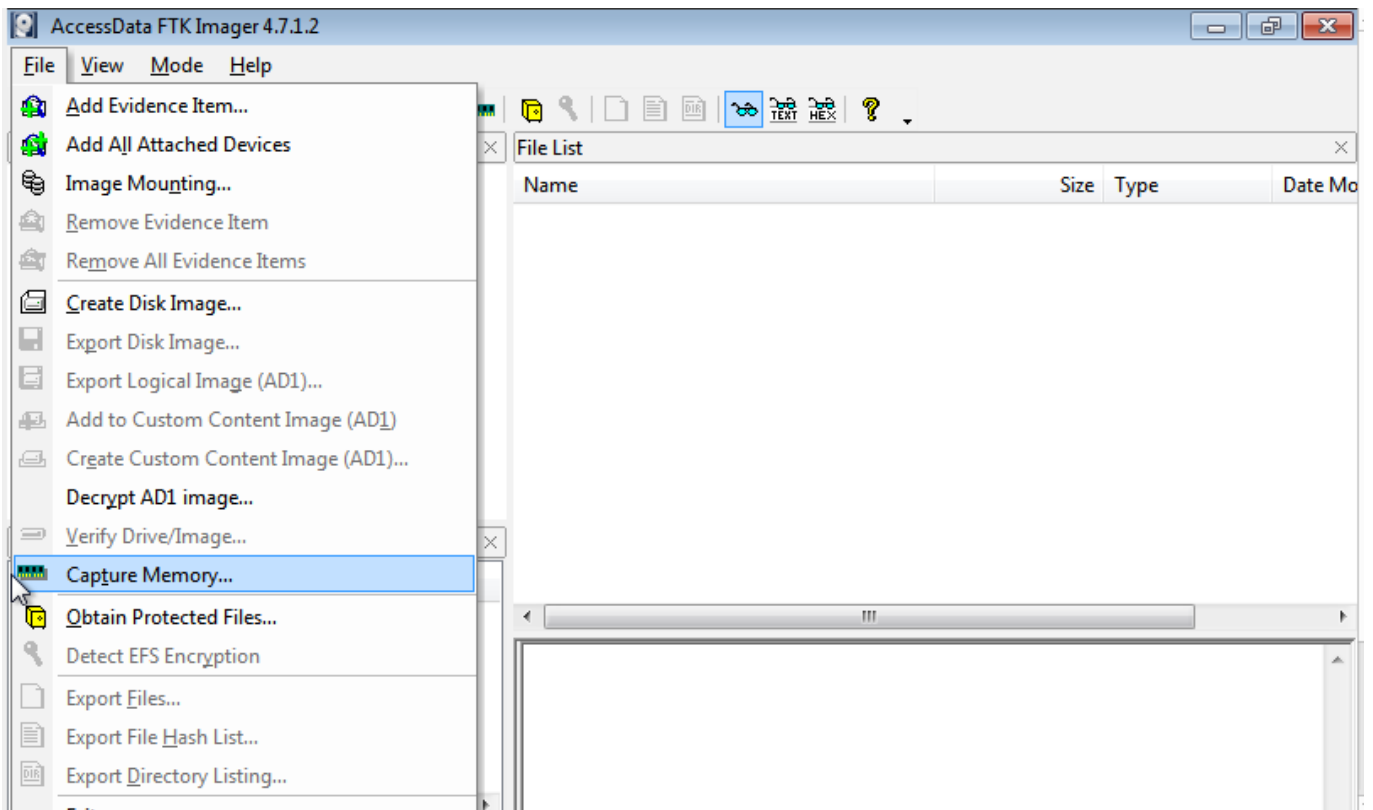
-----
Administrateur          Invité                test
test1                  test2                test3
test4
La commande s'est terminée correctement.

C:\Windows\system32>
```

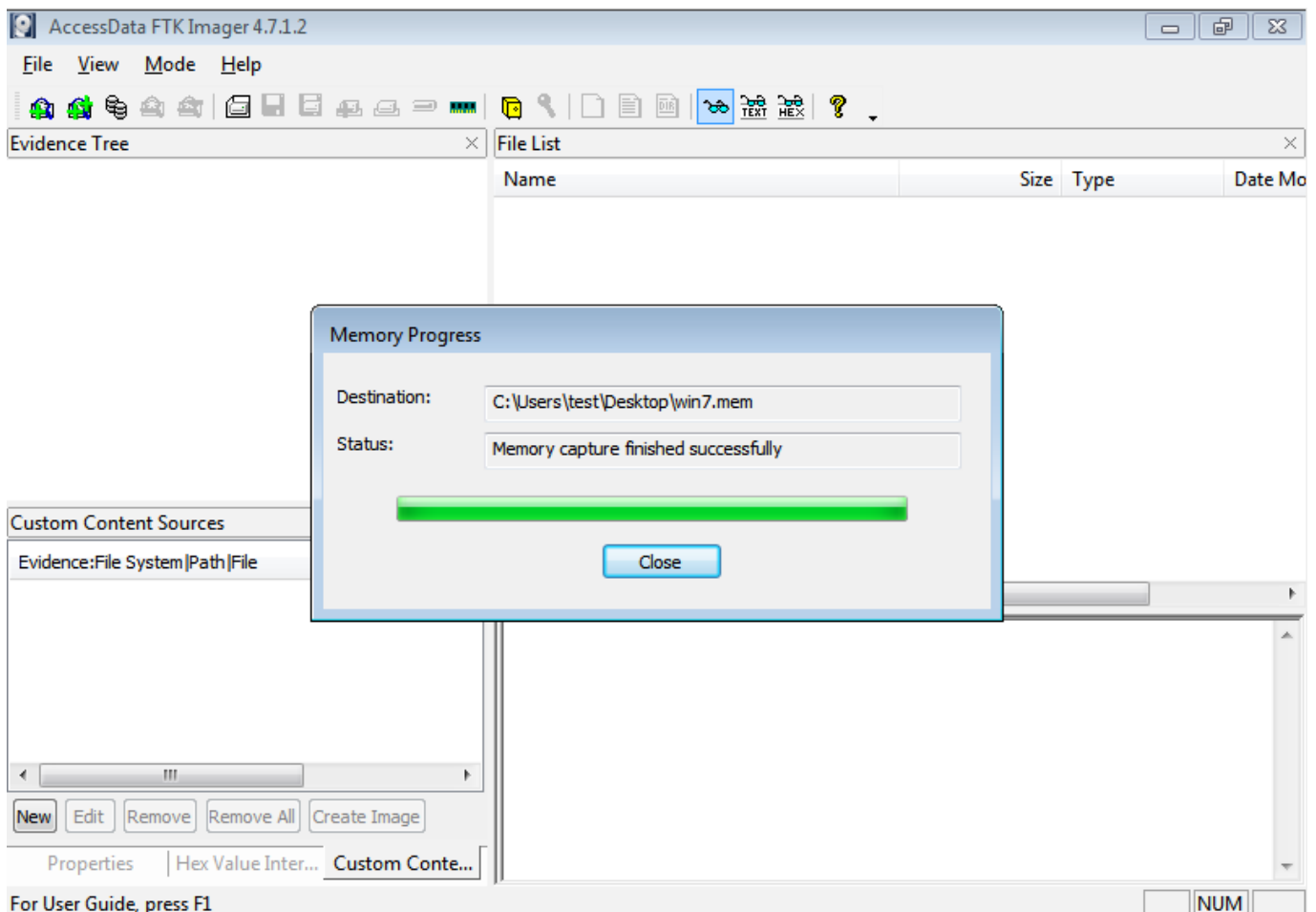
Les utilisateurs créés sont bien présent dans la liste des utilisateurs locaux de la machine.

4. Image locale de la machine avec FTK Imager

Pour réaliser une image mémoire on va dans File > Capture Memory



On donne le nom de la capture de RAM et on lance cette dernière. On obtient le fichier win7.mem qu'il faut maintenant exporter sur la machine Linux afin d'utiliser volatility.



5. Verification avec Volatility

On indentifie le profile à utilisé:

```
> volatility -f win7.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
      AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
      AS Layer2 : FileAddressSpace (/home/val/Downloads/win7.mem)
      PAE type : No PAE
      DTB : 0x187000L
      KDBG : 0xf800028540a0L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0xffffffff8000285d00L
      KUSER_SHARED_DATA : 0xffffffff7800000000L
      Image date and time : 2024-02-12 13:31:30 UTC+0000
      Image local date and time : 2024-02-12 14:31:30 +0100
```

On utilisera le profile Win7SP1x64 afin de récupérer le hashdump la machine:

```
> volatility -f win7.mem --profile Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6
Administrateur:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
Invit:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
test:1000:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537 :::
test1:1001:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930 :::
test2:1002:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930 :::
test3:1003:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930 :::
test4:1004:aad3b435b51404eeaad3b435b51404ee:b9f917853e3dbf6e6831ecce60725930 :::
```

On verifie avec crackstation que le hash NTLM des utilisateurs correspond bien au mot de passe des utilisateurs crée (Ils ont tous le mot de passe **passw0rd** (comme montrer sur la capture en partie 2) sauf test qui a le mot de passe **test**).

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

0cb6948805f797bf2a82807973b89537
b9f917853e3dbf6e6831ecce60725930

I'm not a robot

reCAPTCHA

Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
0cb6948805f797bf2a82807973b89537	NTLM	test
b9f917853e3dbf6e6831ecce60725930	NTLM	passw0rd

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Les hash NTLM correspondent bien au mot de passe des utilisateurs.

3 / 3