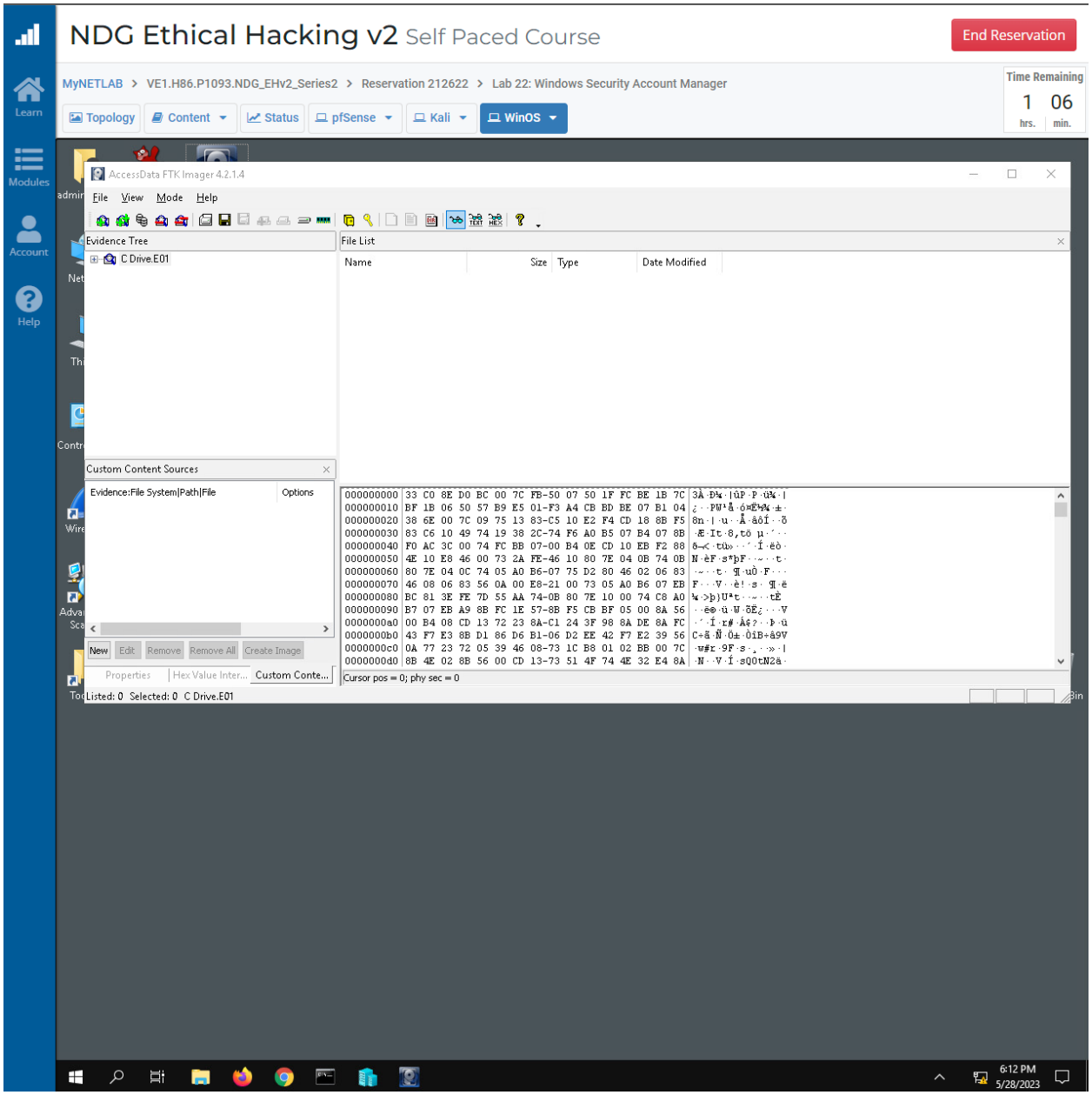
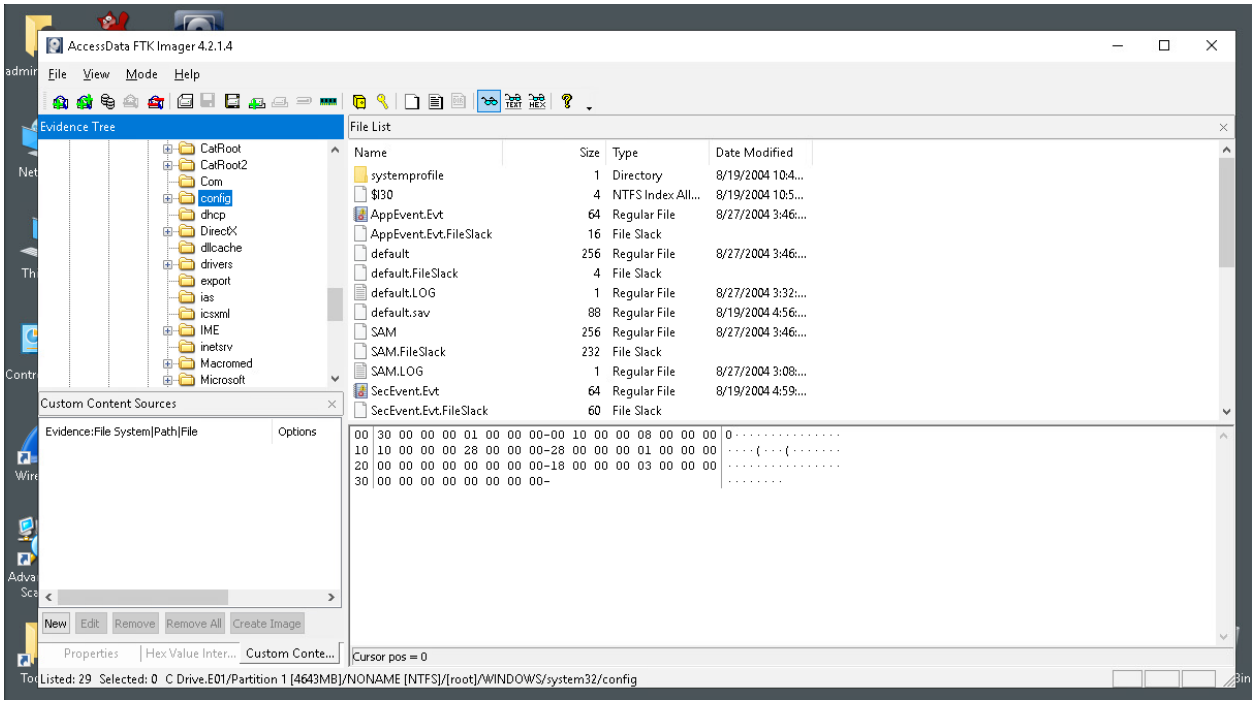
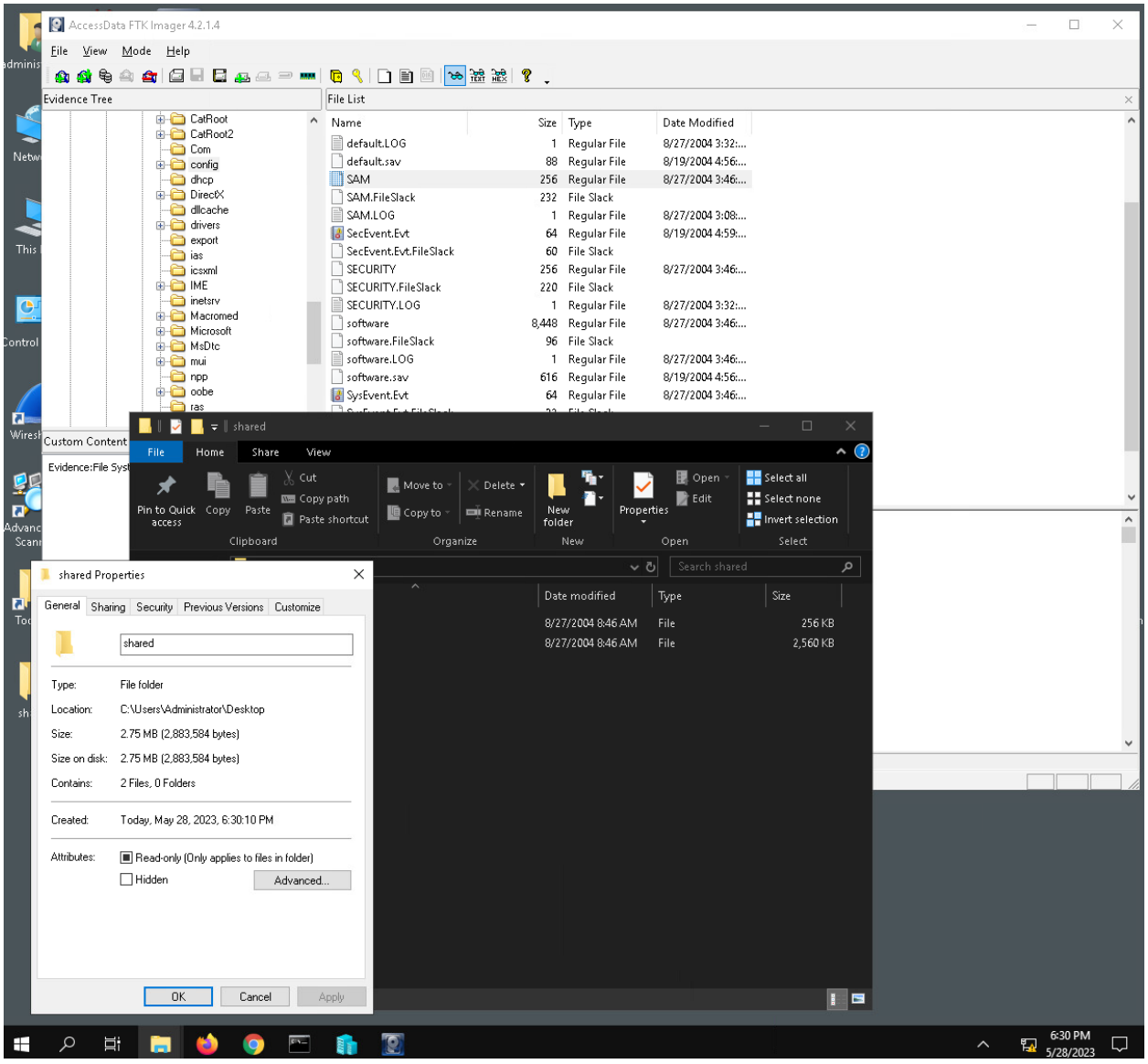
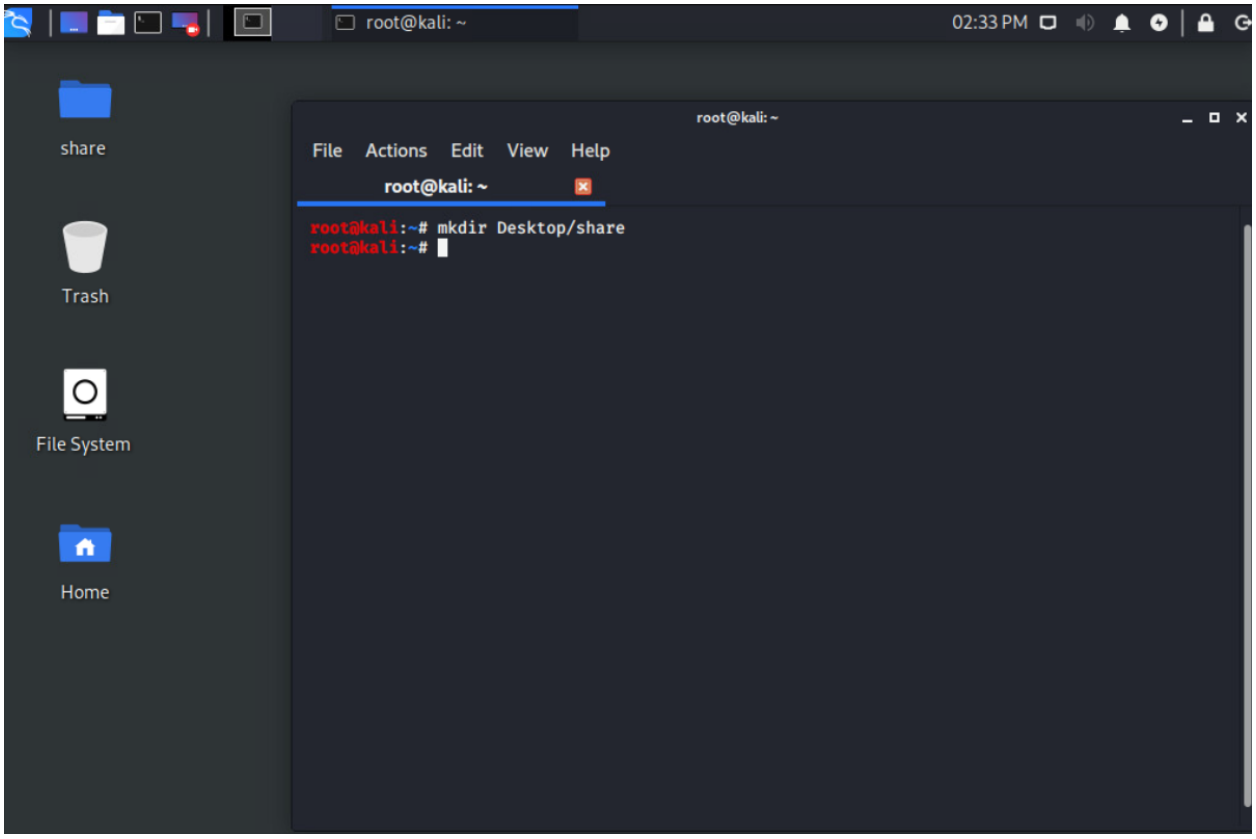
Jason Palmeri
CS53C
Lab 22
Timothy Ryan

Windows Security Account Manager

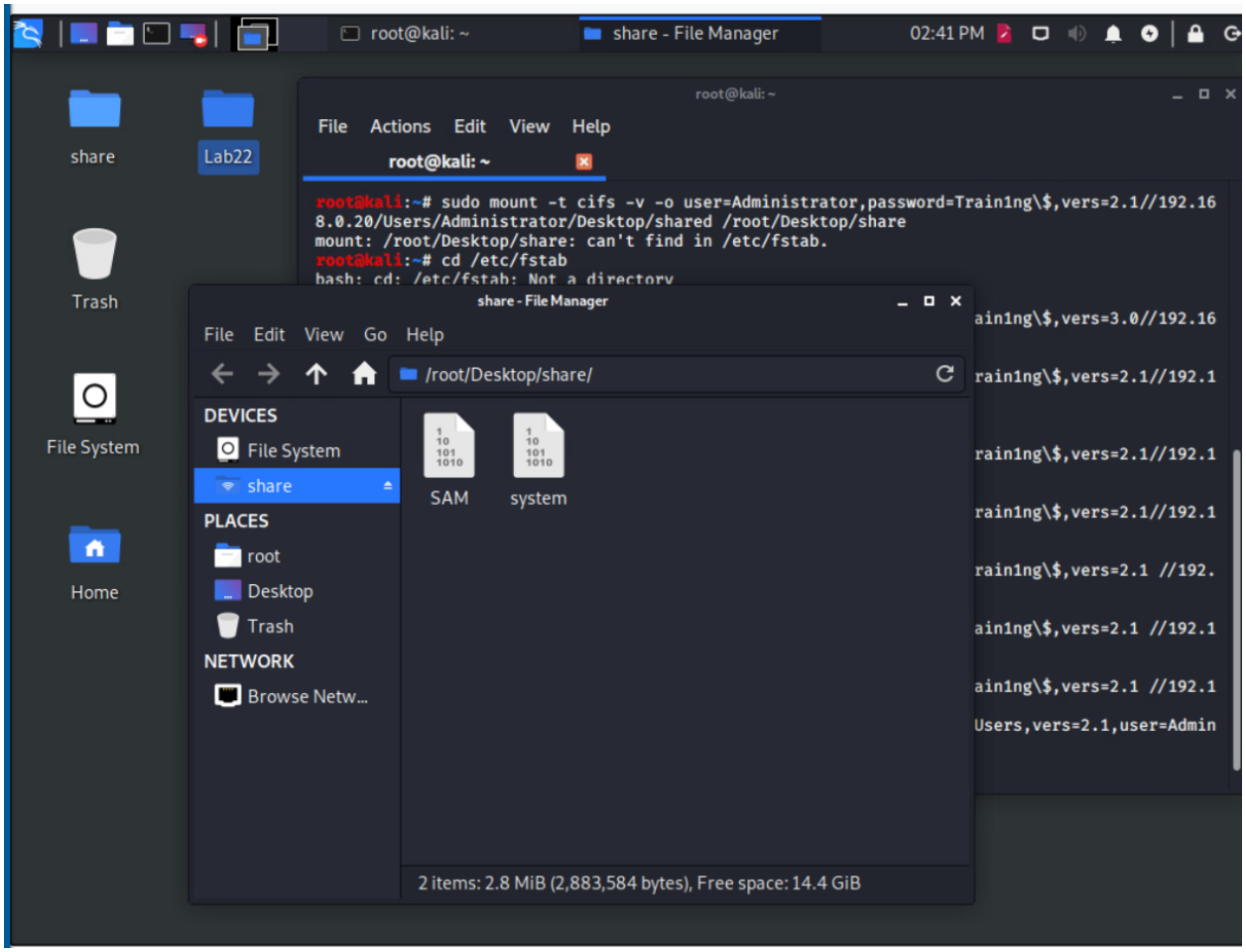


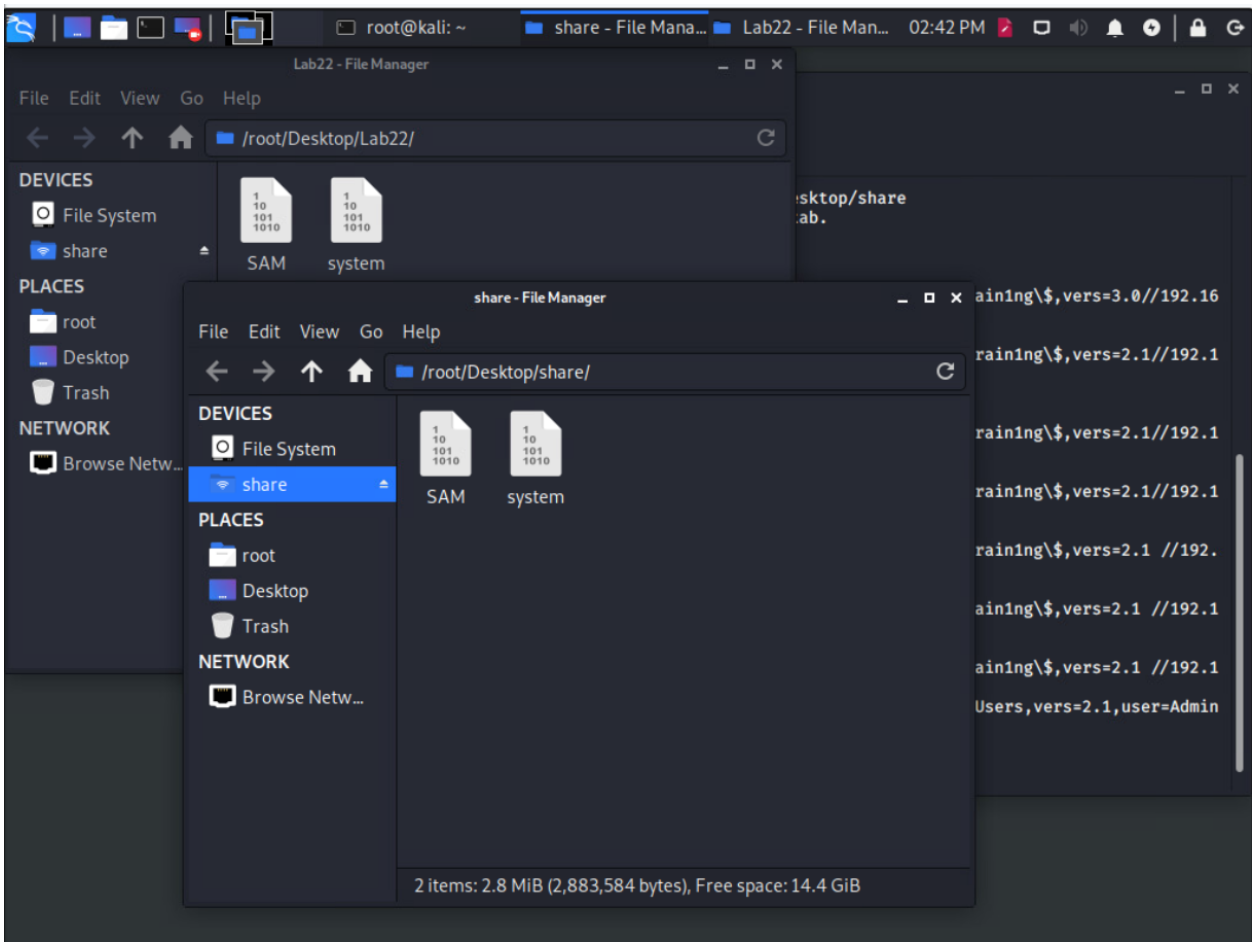

AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
CatRoot
CatRoot2
Com
config
dhcp
DirectX
dllcache
drivers
export
ias
icsxml
IME
inetsrv
Macromed
Microsoft
File List
Name Size Type Date Modified
systemprofile 1 Directory 8/19/2004 10:4...
$I30 4 NTFS Index All... 8/19/2004 10:5...
AppEvent.Evt 64 Regular File 8/27/2004 3:46:...
AppEvent.Evt.FileSlack 16 File Slack
default 256 Regular File 8/27/2004 3:46:...
default.FileSlack 4 File Slack
default.LOG 1 Regular File 8/27/2004 3:32:...
default.sav 88 Regular File 8/19/2004 4:56:...
SAM 256 Regular File 8/27/2004 3:46:...
SAM.FileSlack 232 File Slack
SAM.LOG 1 Regular File 8/27/2004 3:08:...
SecEvent.Evt 64 Regular File 8/19/2004 4:59:...
SecEvent.Evt.FileSlack 60 File Slack
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Inter... Custom Conte...
00 30 00 00 00 01 00 00 00-00 10 00 00 08 00 00 00
10 10 00 00 00 28 00 00 00-28 00 00 00 01 00 00 00
20 00 00 00 00 00 00 00 00-18 00 00 00 03 00 00 00
30 00 00 00 00 00 00 00 00-
Cursor pos = 0
Listed: 29 Selected: 0 C Drive.E01/Partition 1 [4643MB]/NONAME [NTFS]/[root]/WINDOWS/system32/config

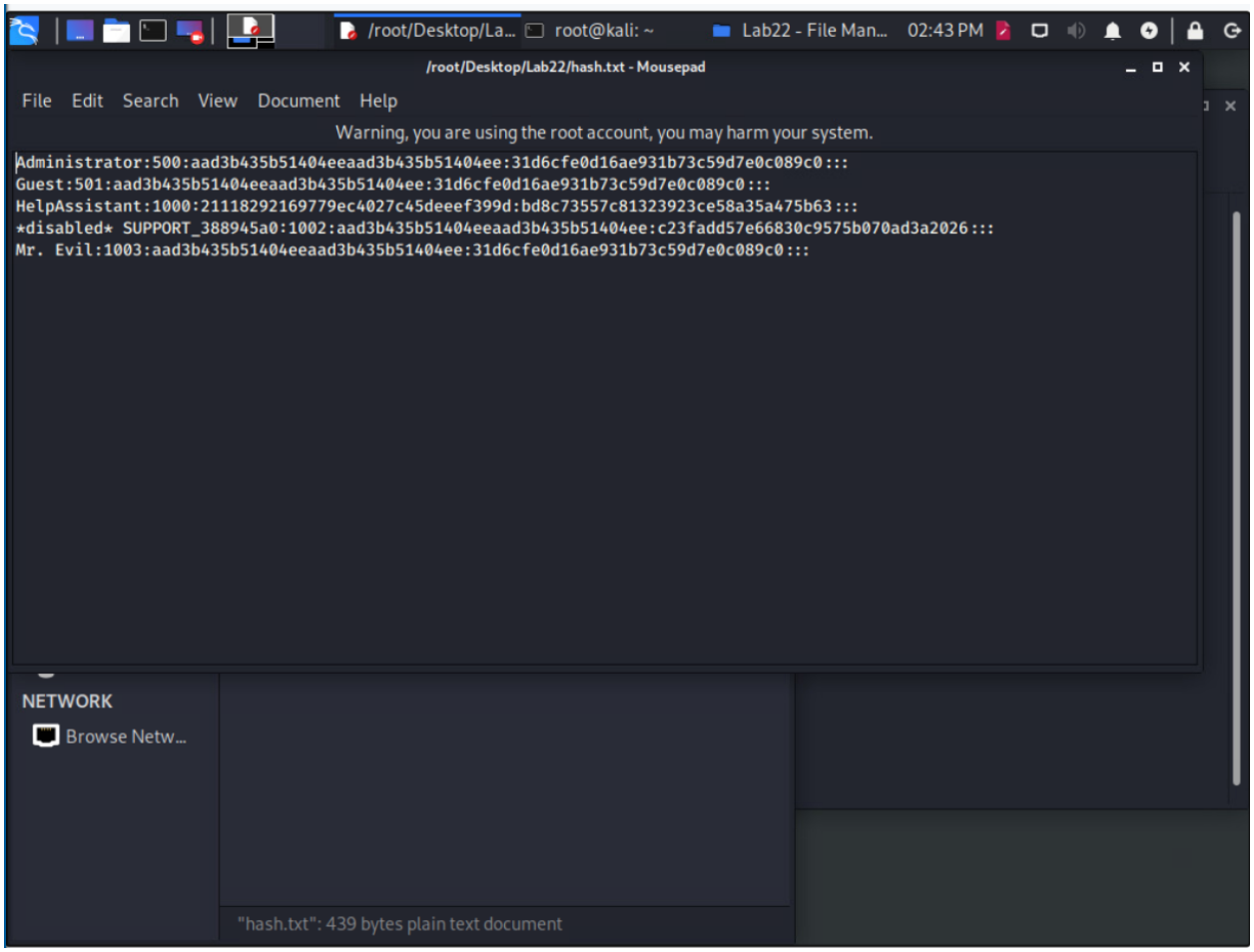

AccessData FTK Imager 4.2.1.4
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
default.LOG 1 Regular File 8/27/2004 3:32:...
default.sav 88 Regular File 8/19/2004 4:56:...
SAM 256 Regular File 8/27/2004 3:46:...
SAM.FileSlack 232 File Slack
SAM.LOG 1 Regular File 8/27/2004 3:08:...
SecEvent.Evt 64 Regular File 8/19/2004 4:59:...
SecEvent.Evt.FileSlack 60 File Slack
SECURITY 256 Regular File 8/27/2004 3:46:...
SECURITY.FileSlack 220 File Slack
SECURITY.LOG 1 Regular File 8/27/2004 3:32:...
software 8,448 Regular File 8/27/2004 3:46:...
software.FileSlack 96 File Slack
software.LOG 1 Regular File 8/27/2004 3:46:...
software.sav 616 Regular File 8/19/2004 4:56:...
SysEvent.Evt 64 Regular File 8/27/2004 3:46:...
CatRoot
CatRoot2
Com
config
dhcp
DirectX
dllcache
drivers
export
ias
icsxml
IME
inetsrv
Macromed
Microsoft
MsDtc
mui
npp
oobe
ras
Custom Content
Evidence:File Syst
shared
File Home Share View
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New
Properties
Open
Edit
Open
Select all
Select none
Invert selection
Select
Search shared
Date modified Type Size
8/27/2004 8:46 AM File 256 KB
8/27/2004 8:46 AM File 2,560 KB
shared Properties
General Sharing Security Previous Versions Customize
shared
Type: File folder
Location: C:\Users\Administrator\Desktop
Size: 2.75 MB (2,883,584 bytes)
Size on disk: 2.75 MB (2,883,584 bytes)
Contains: 2 Files, 0 Folders
Created: Today, May 28, 2023, 6:30:10 PM
Attributes: Read-only (Only applies to files in folder)
Hidden
Advanced...
OK
Cancel
Apply
6:30 PM
5/28/2023

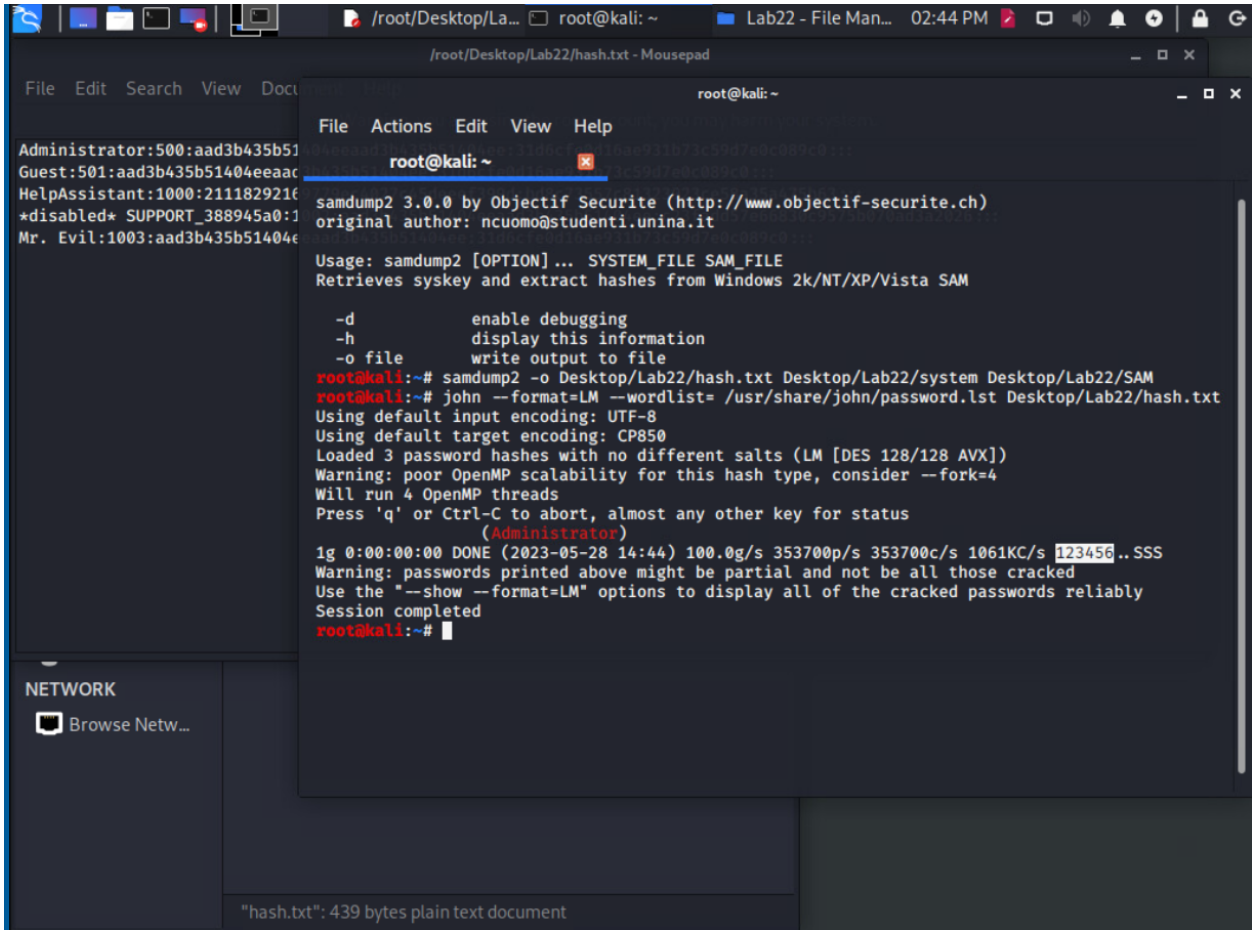



```
root@kali:~# sudo mount -t cifs -v -o user=Administrator,password=Train1ng\$,vers=2.1 //192.1
68.0.20/Users/Administrator/Desktop/shared /root/Desktop/share/
mount.cifs kernel mount options: ip=192.168.0.20,unc=\\192.168.0.20\Users,vers=2.1,user=Admin
istrator,prefixpath=Administrator/Desktop/shared,pass=********
root@kali:~#
```


root@kali: ~
share - File Manager
02:41 PM
share
Lab22
Trash
File System
Home
root@kali: ~
File Actions Edit View Help
root@kali: ~
root@kali:~# sudo mount -t cifs -v -o user=Administrator,password=Train1ng\$,vers=2.1//192.16
8.0.20/Users/Administrator/Desktop/shared /root/Desktop/share
mount: /root/Desktop/share: can't find in /etc/fstab.
root@kali:~# cd /etc/fstab
bash: cd: /etc/fstab: Not a directory
share - File Manager
File Edit View Go Help
/root/Desktop/share/
DEVICES
File System
share
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
SAM
system
2 items: 2.8 MiB (2,883,584 bytes), Free space: 14.4 GiB


root@kali: ~
share - File Mana...
Lab22 - File Man...
02:42 PM
Lab22 - File Manager
File Edit View Go Help
/root/Desktop/Lab22/
DEVICES
File System
share
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
SAM
system
share - File Manager
File Edit View Go Help
/root/Desktop/share/
DEVICES
File System
share
PLACES
root
Desktop
Trash
NETWORK
Browse Netw...
SAM
system
2 items: 2.8 MiB (2,883,584 bytes), Free space: 14.4 GiB
ain1ng\$,vers=3.0//192.16
rain1ng\$,vers=2.1//192.1
rain1ng\$,vers=2.1//192.1
rain1ng\$,vers=2.1//192.1
rain1ng\$,vers=2.1 //192.
ain1ng\$,vers=2.1 //192.1
ain1ng\$,vers=2.1 //192.1
Users,vers=2.1,user=Admin


/root/Desktop/La...
root@kali: ~
Lab22 - File Man...
02:43 PM
/root/Desktop/Lab22/hash.txt - Mousepad
File Edit Search View Document Help
Warning, you are using the root account, you may harm your system.
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:21118292169779ec4027c45deeef399d:bd8c73557c81323923ce58a35a475b63:::
disabled SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:c23fadd57e66830c9575b070ad3a2026:::
Mr. Evil:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
NETWORK
Browse Netw...
"hash.txt": 439 bytes plain text document


/root/Desktop/La...
root@kali: ~
Lab22 - File Man...
02:44 PM
/root/Desktop/Lab22/hash.txt - Mousepad
File Edit Search View Docu
Administrator:500:aad3b435b51
Guest:501:aad3b435b51404eeaad
HelpAssistant:1000:211829216
disabled SUPPORT_388945a0:1
Mr. Evil:1003:aad3b435b51404e
root@kali: ~
File Actions Edit View Help
root@kali: ~
samdump2 3.0.0 by Objectif Securite (http://www.objectif-securite.ch)
original author: ncuomo@studenti.unina.it
Usage: samdump2 [OPTION]... SYSTEM_FILE SAM_FILE
Retrieves syskey and extract hashes from Windows 2k/NT/XP/Vista SAM
-d enable debugging
-h display this information
-o file write output to file
root@kali:~# samdump2 -o Desktop/Lab22/hash.txt Desktop/Lab22/system Desktop/Lab22/SAM
root@kali:~# john --format=LM --wordlist= /usr/share/john/password.lst Desktop/Lab22/hash.txt
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 3 password hashes with no different salts (LM [DES 128/128 AVX])
Warning: poor OpenMP scalability for this hash type, consider --fork=4
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(Administrator)
1g 0:00:00:00 DONE (2023-05-28 14:44) 100.0g/s 353700p/s 353700c/s 1061KC/s 123456..SSS
Warning: passwords printed above might be partial and not be all those cracked
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed
root@kali:~#
NETWORK
Browse Netw...
"hash.txt": 439 bytes plain text document