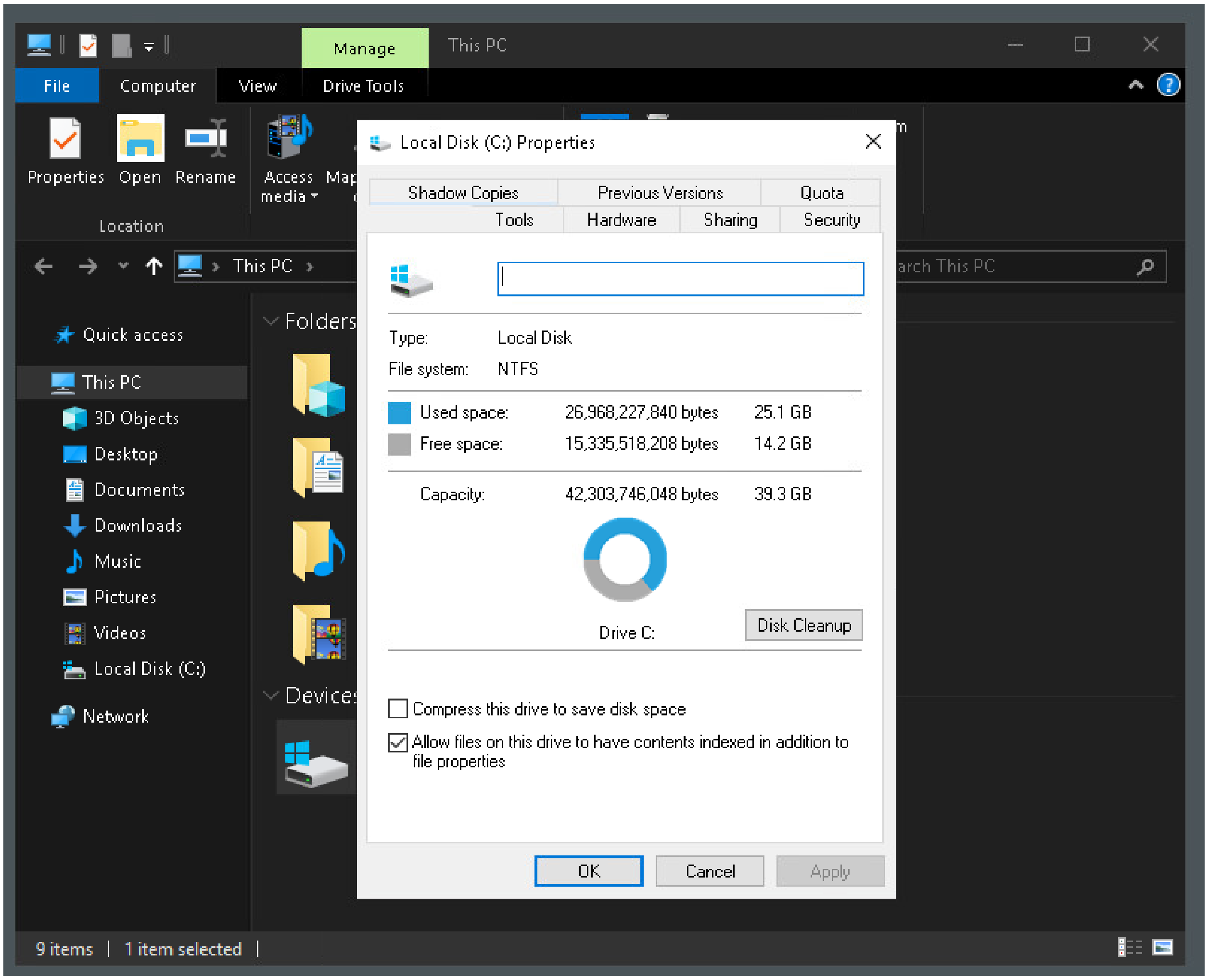
Jason Palmeri
CS53C
Lab 23
Timothy Ryan

# Covering Your Tracks



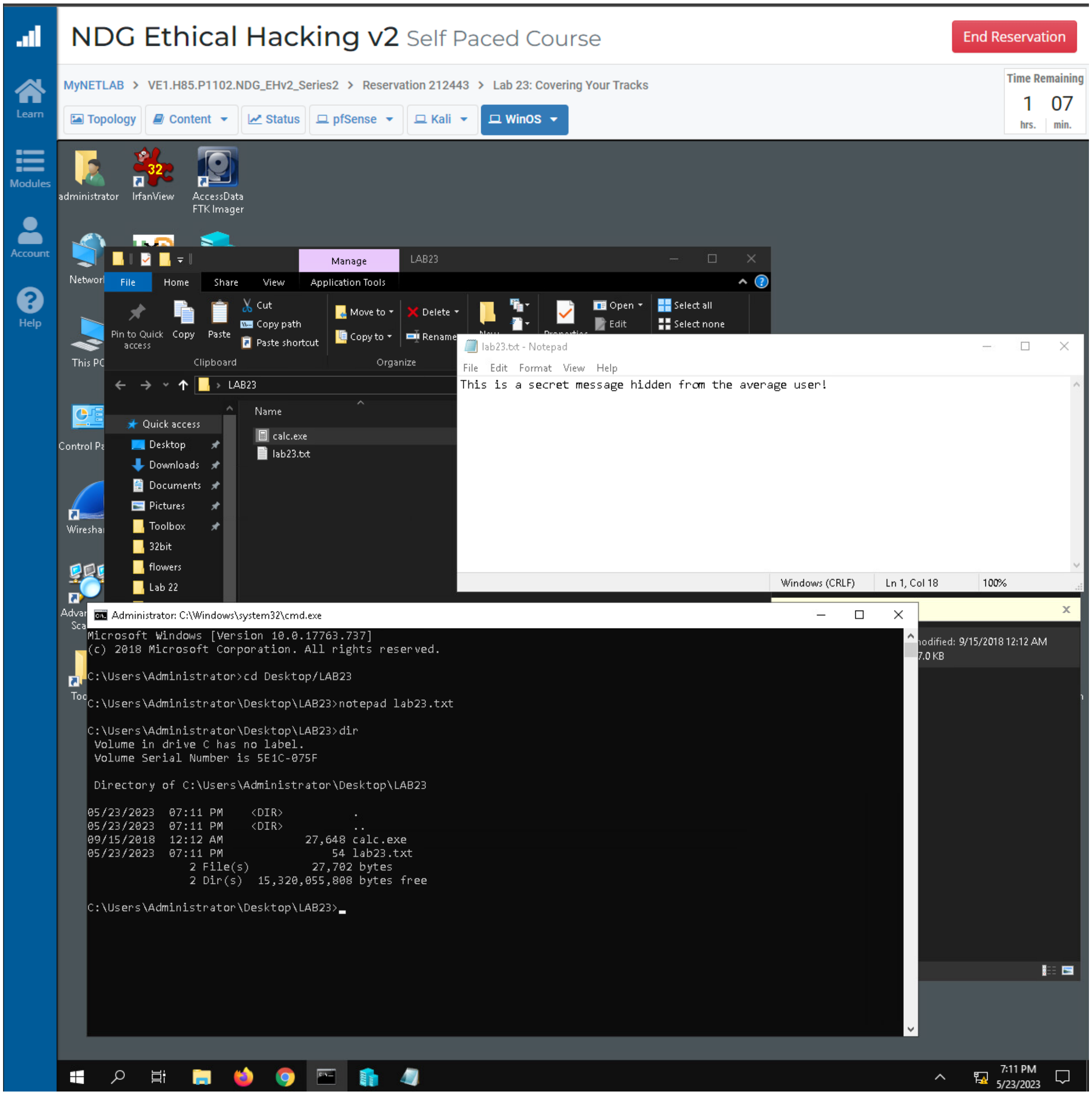
Local Disk (C:) Properties

| | | |
|---|---|---|
| Type: | Local Disk | |
| File system: | NTFS | |
| 🟦 Used space: | 26,968,227,840 bytes | 25.1 GB |
| ⬜ Free space: | 15,335,518,208 bytes | 14.2 GB |
| Capacity: | 42,303,746,048 bytes | 39.3 GB |

Drive C:

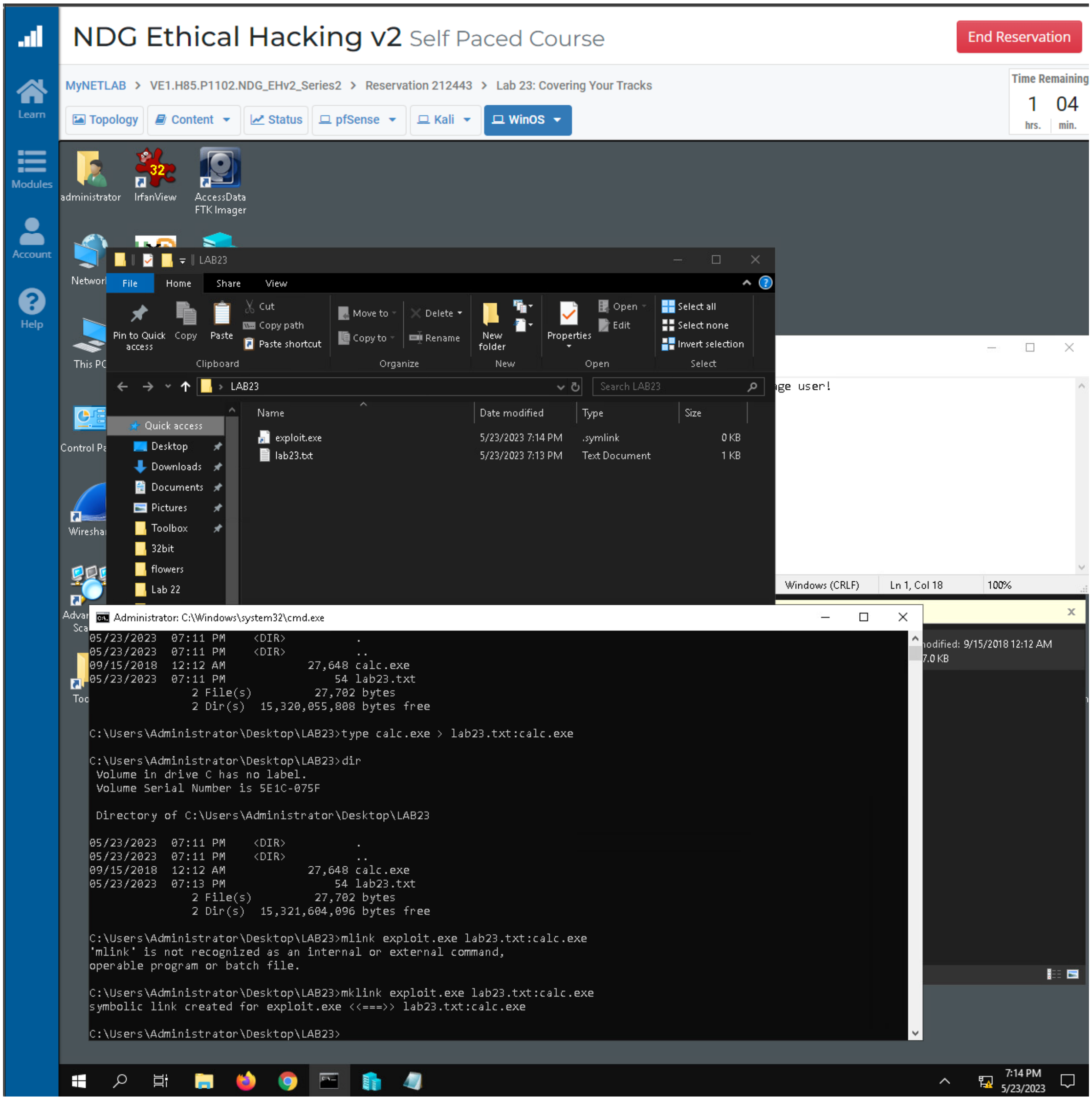
□ Compress this drive to save disk space

☑ Allow files on this drive to have contents indexed in addition to file properties



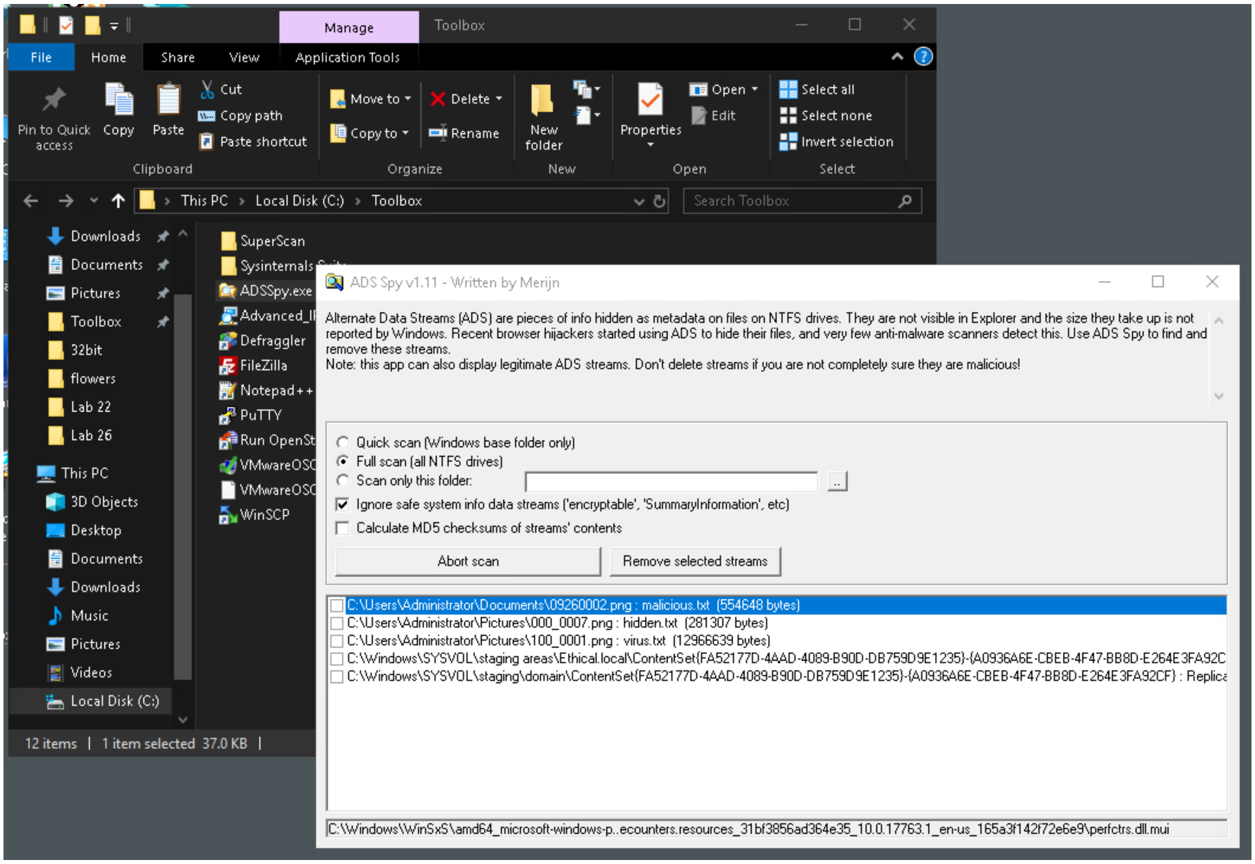
```
This is a secret message hidden from the average user!
```

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd Desktop/LAB23

C:\Users\Administrator\Desktop\LAB23>notepad lab23.txt

C:\Users\Administrator\Desktop\LAB23>dir
 Volume in drive C has no label.
 Volume Serial Number is 5E1C-075F

 Directory of C:\Users\Administrator\Desktop\LAB23

05/23/2023  07:11 PM    <DIR>          .
05/23/2023  07:11 PM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
05/23/2023  07:11 PM                54 lab23.txt
               2 File(s)         27,702 bytes
               2 Dir(s)  15,320,055,808 bytes free

C:\Users\Administrator\Desktop\LAB23>
```



| Name | Date modified | Type | Size |
|---|---|---|---|
| exploit.exe | 5/23/2023 7:14 PM | .symlink | 0 KB |
| lab23.txt | 5/23/2023 7:13 PM | Text Document | 1 KB |

```
05/23/2023  07:11 PM    <DIR>          .
05/23/2023  07:11 PM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
05/23/2023  07:11 PM                54 lab23.txt
               2 File(s)         27,702 bytes
               2 Dir(s)  15,320,055,808 bytes free

C:\Users\Administrator\Desktop\LAB23>type calc.exe > lab23.txt:calc.exe

C:\Users\Administrator\Desktop\LAB23>dir
 Volume in drive C has no label.
 Volume Serial Number is 5E1C-075F

 Directory of C:\Users\Administrator\Desktop\LAB23

05/23/2023  07:11 PM    <DIR>          .
05/23/2023  07:11 PM    <DIR>          ..
09/15/2018  12:12 AM            27,648 calc.exe
05/23/2023  07:13 PM                54 lab23.txt
               2 File(s)         27,702 bytes
               2 Dir(s)  15,321,604,096 bytes free

C:\Users\Administrator\Desktop\LAB23>mlink exploit.exe lab23.txt:calc.exe
'mlink' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\Administrator\Desktop\LAB23>mklink exploit.exe lab23.txt:calc.exe
symbolic link created for exploit.exe <<===>> lab23.txt:calc.exe

C:\Users\Administrator\Desktop\LAB23>
```

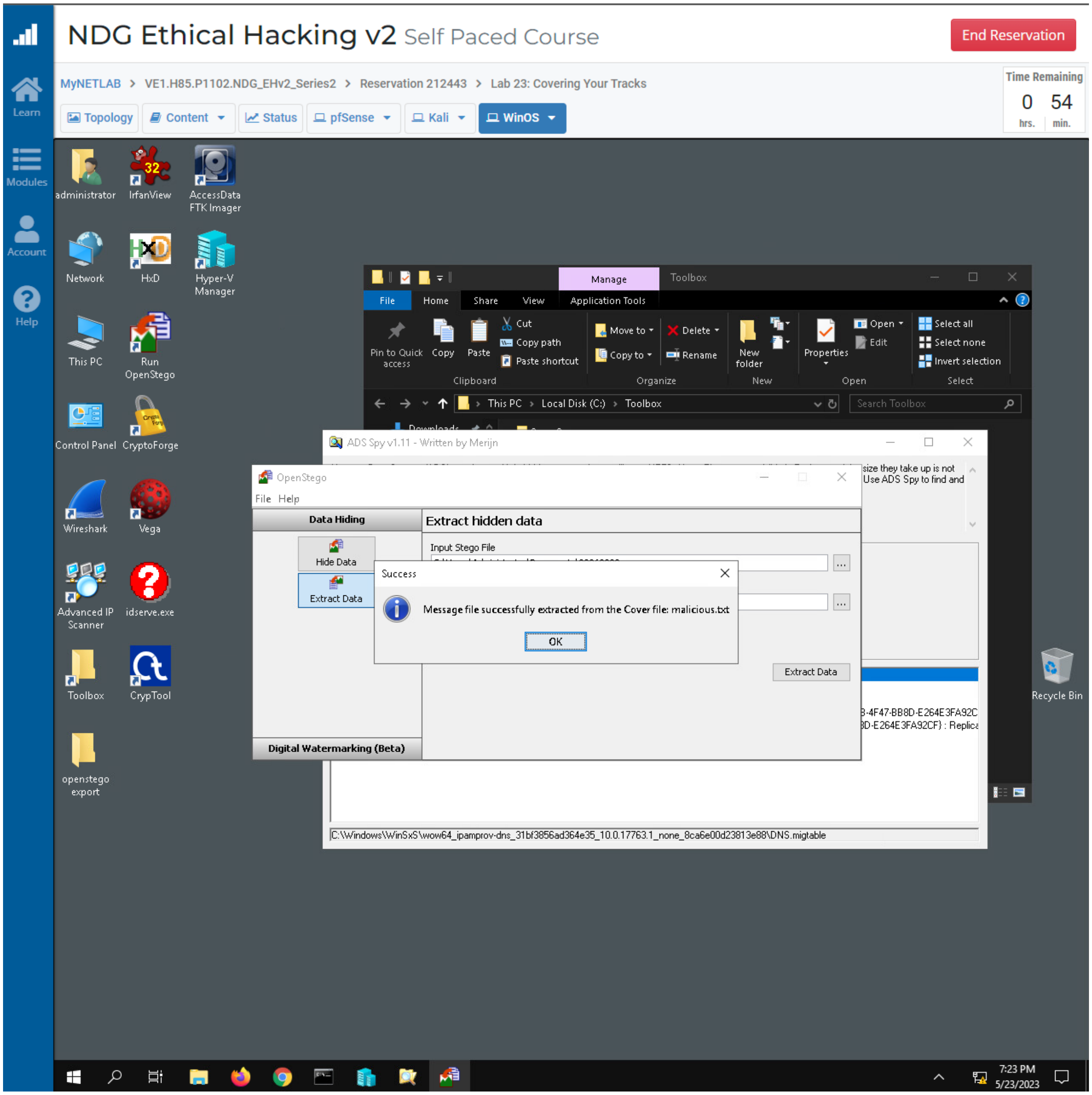


Alternate Data Streams (ADS) are pieces of info hidden as metadata on files on NTFS drives. They are not visible in Explorer and the size they take up is not reported by Windows. Recent browser hijackers started using ADS to hide their files, and very few anti-malware scanners detect this. Use ADS Spy to find and remove these streams.
Note: this app can also display legitimate ADS streams. Don't delete streams if you are not completely sure they are malicious!

○ Quick scan (Windows base folder only)
● Full scan (all NTFS drives)
○ Scan only this folder:
☑ Ignore safe system info data streams ('encryptable', 'SummaryInformation', etc)
☐ Calculate MD5 checksums of streams' contents

```
☐ C:\Users\Administrator\Documents\09260002.png : malicious.txt  (554648 bytes)
☐ C:\Users\Administrator\Pictures\000_0007.png : hidden.txt  (281307 bytes)
☐ C:\Users\Administrator\Pictures\100_0001.png : virus.txt  (12966639 bytes)
☐ C:\Windows\SYSVOL\staging areas\Ethical.local\ContentSet{FA52177D-4AAD-4089-B90D-DB759D9E1235}-{A0936A6E-CBEB-4F47-BB8D-E264E3FA92C
☐ C:\Windows\SYSVOL\staging\domain\ContentSet{FA52177D-4AAD-4089-B90D-DB759D9E1235}-{A0936A6E-CBEB-4F47-BB8D-E264E3FA92CF} : Replica
```

C:\Windows\WinSxS\amd64_microsoft-windows-p..ecounters.resources_31bf3856ad364e35_10.0.17763.1_en-us_165a3f142f72e6e9\perfctrs.dll.mui



NDG Ethical Hacking v2 Self Paced Course

MyNETLAB > VE1.H85.P1102.NDG_EHv2_Series2 > Reservation 212443 > Lab 23: Covering Your Tracks

Time Remaining 0 hrs. 54 min.

This PC > Local Disk (C:) > Toolbox

ADS Spy v1.11 - Written by Merijn

size they take up is not
Use ADS Spy to find and

3-4F47-BB8D-E264E3FA92C
3D-E264E3FA92CF} : Replica

C:\Windows\WinSxS\wow64_ipamprov-dns_31bf3856ad364e35_10.0.17763.1_none_8ca6e00d23813e88\DNS.migtable

OpenStego

Extract hidden data

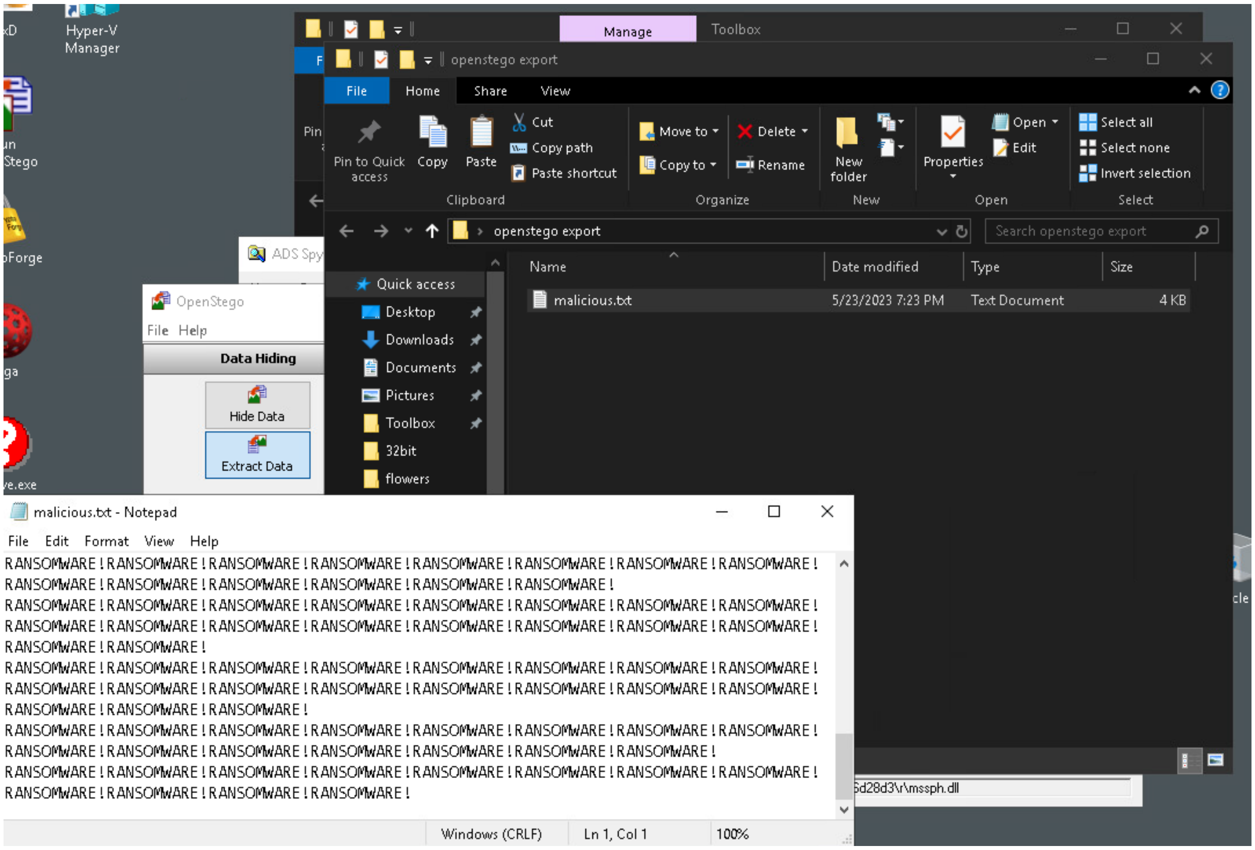
Input Stego File

Success

Message file successfully extracted from the Cover file: malicious.txt

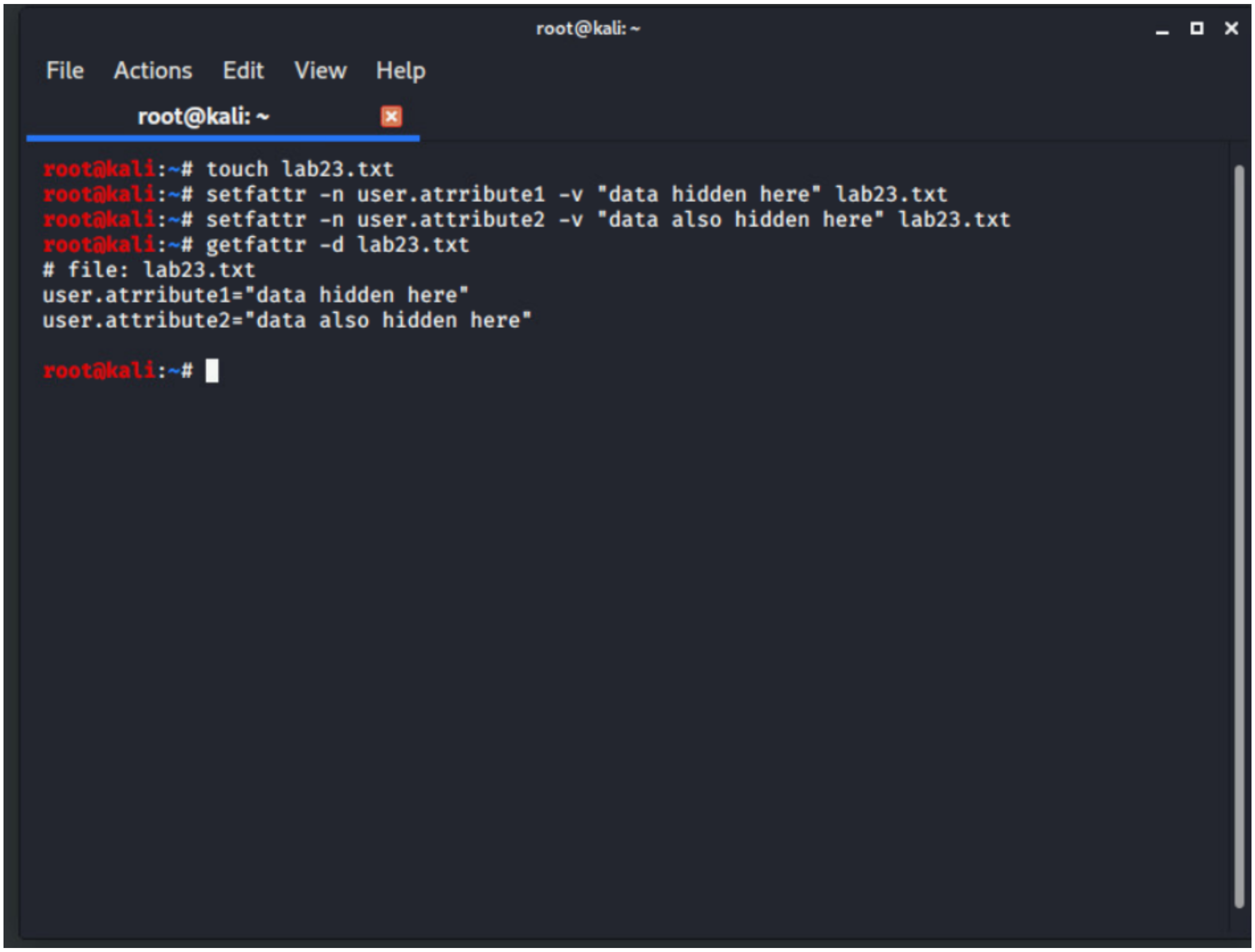
OK

7:23 PM
5/23/2023

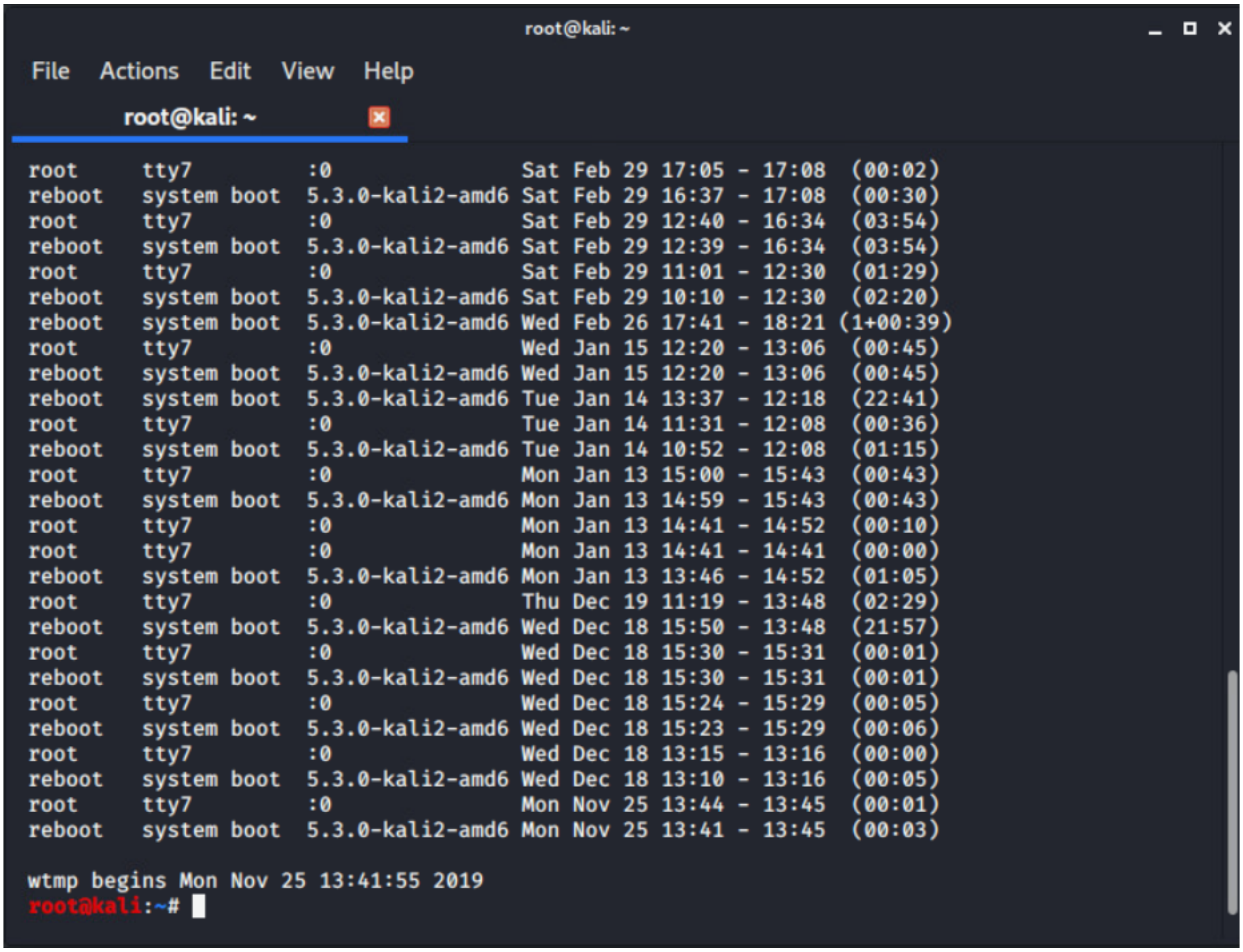


| Name | Date modified | Type | Size |
|---|---|---|---|
| malicious.txt | 5/23/2023 7:23 PM | Text Document | 4 KB |

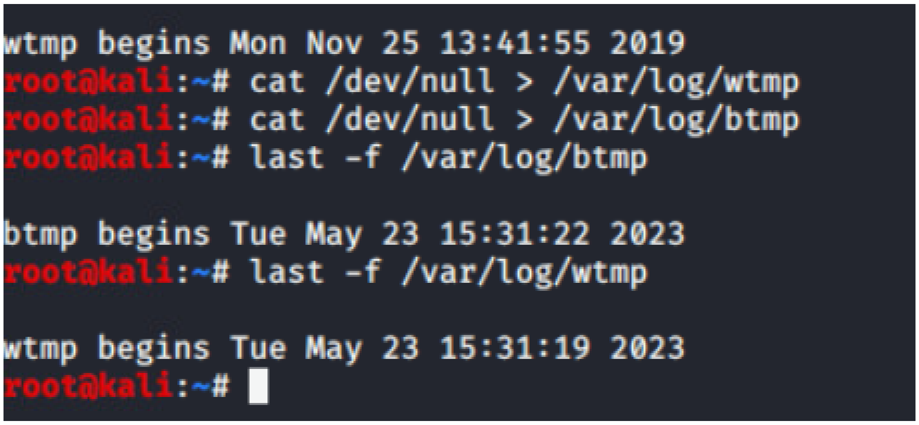
```
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
RANSOMWARE!RANSOMWARE!RANSOMWARE!RANSOMWARE!
```



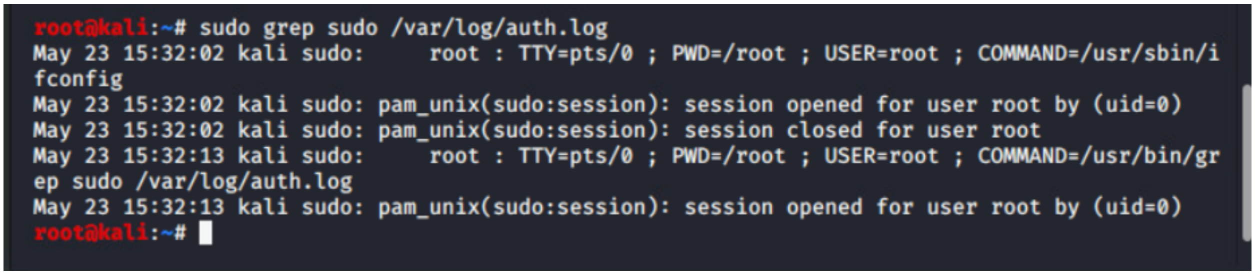
```
root@kali:~# touch lab23.txt
root@kali:~# setfattr -n user.atrribute1 -v "data hidden here" lab23.txt
root@kali:~# setfattr -n user.attribute2 -v "data also hidden here" lab23.txt
root@kali:~# getfattr -d lab23.txt
# file: lab23.txt
user.atrribute1="data hidden here"
user.attribute2="data also hidden here"

root@kali:~# 
```



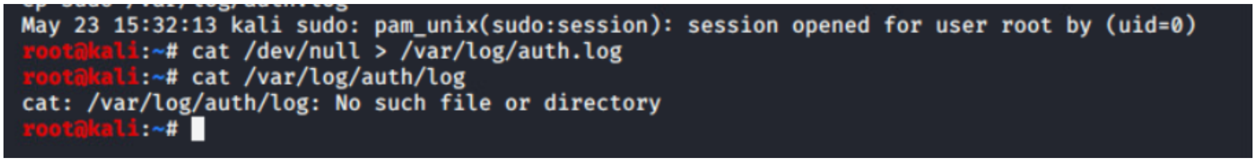
```
root     tty7         :0               Sat Feb 29 17:05 - 17:08  (00:02)
reboot   system boot  5.3.0-kali2-amd6 Sat Feb 29 16:37 - 17:08  (00:30)
root     tty7         :0               Sat Feb 29 12:40 - 16:34  (03:54)
reboot   system boot  5.3.0-kali2-amd6 Sat Feb 29 12:39 - 16:34  (03:54)
root     tty7         :0               Sat Feb 29 11:01 - 12:30  (01:29)
reboot   system boot  5.3.0-kali2-amd6 Sat Feb 29 10:10 - 12:30  (02:20)
reboot   system boot  5.3.0-kali2-amd6 Wed Feb 26 17:41 - 18:21 (1+00:39)
root     tty7         :0               Wed Jan 15 12:20 - 13:06  (00:45)
reboot   system boot  5.3.0-kali2-amd6 Wed Jan 15 12:20 - 13:06  (00:45)
reboot   system boot  5.3.0-kali2-amd6 Tue Jan 14 13:37 - 12:18  (22:41)
root     tty7         :0               Tue Jan 14 11:31 - 12:08  (00:36)
reboot   system boot  5.3.0-kali2-amd6 Tue Jan 14 10:52 - 12:08  (01:15)
root     tty7         :0               Mon Jan 13 15:00 - 15:43  (00:43)
reboot   system boot  5.3.0-kali2-amd6 Mon Jan 13 14:59 - 15:43  (00:43)
root     tty7         :0               Mon Jan 13 14:41 - 14:52  (00:10)
root     tty7         :0               Mon Jan 13 14:41 - 14:41  (00:00)
reboot   system boot  5.3.0-kali2-amd6 Mon Jan 13 13:46 - 14:52  (01:05)
root     tty7         :0               Thu Dec 19 11:19 - 13:48  (02:29)
reboot   system boot  5.3.0-kali2-amd6 Wed Dec 18 15:50 - 13:48  (21:57)
root     tty7         :0               Wed Dec 18 15:30 - 15:31  (00:01)
reboot   system boot  5.3.0-kali2-amd6 Wed Dec 18 15:30 - 15:31  (00:01)
root     tty7         :0               Wed Dec 18 15:24 - 15:29  (00:05)
reboot   system boot  5.3.0-kali2-amd6 Wed Dec 18 15:23 - 15:29  (00:06)
root     tty7         :0               Wed Dec 18 13:15 - 13:16  (00:00)
reboot   system boot  5.3.0-kali2-amd6 Wed Dec 18 13:10 - 13:16  (00:05)
root     tty7         :0               Mon Nov 25 13:44 - 13:45  (00:01)
reboot   system boot  5.3.0-kali2-amd6 Mon Nov 25 13:41 - 13:45  (00:03)

wtmp begins Mon Nov 25 13:41:55 2019
root@kali:~# 
```



```
wtmp begins Mon Nov 25 13:41:55 2019
root@kali:~# cat /dev/null > /var/log/wtmp
root@kali:~# cat /dev/null > /var/log/btmp
root@kali:~# last -f /var/log/btmp

btmp begins Tue May 23 15:31:22 2023
root@kali:~# last -f /var/log/wtmp

wtmp begins Tue May 23 15:31:19 2023
root@kali:~# 
```



```
root@kali:~# sudo grep sudo /var/log/auth.log
May 23 15:32:02 kali sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/sbin/i
fconfig
May 23 15:32:02 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
May 23 15:32:02 kali sudo: pam_unix(sudo:session): session closed for user root
May 23 15:32:13 kali sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/gr
ep sudo /var/log/auth.log
May 23 15:32:13 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
root@kali:~# 
```



```
cp sudo /var/log/auth.log
May 23 15:32:13 kali sudo: pam_unix(sudo:session): session opened for user root by (uid=0)
root@kali:~# cat /dev/null > /var/log/auth.log
root@kali:~# cat /var/log/auth/log
cat: /var/log/auth/log: No such file or directory
root@kali:~# 
```