

Lab 10: File search based on metadata

What You Need for this lab

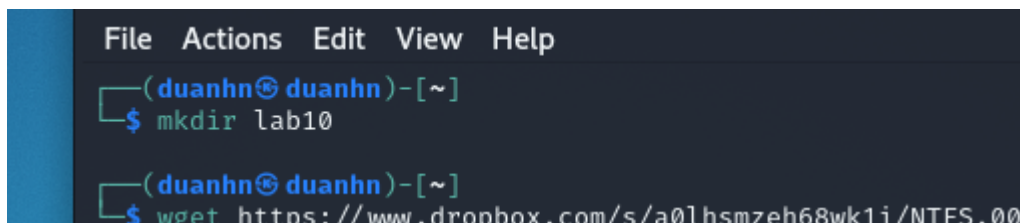
- Install Virtualbox : <https://www.virtualbox.org/wiki/Downloads>
- Install Kali 2021.4. : <https://old.kali.org/kali-images/kali-2021.4/>
 - Notes: Suggest You configure the disk size of Kali VM 80G because the size of each leakage cases image is 30G+

- A USB image

<https://www.dropbox.com/s/a0lhsmzeh68wk1i/NTFS.001>

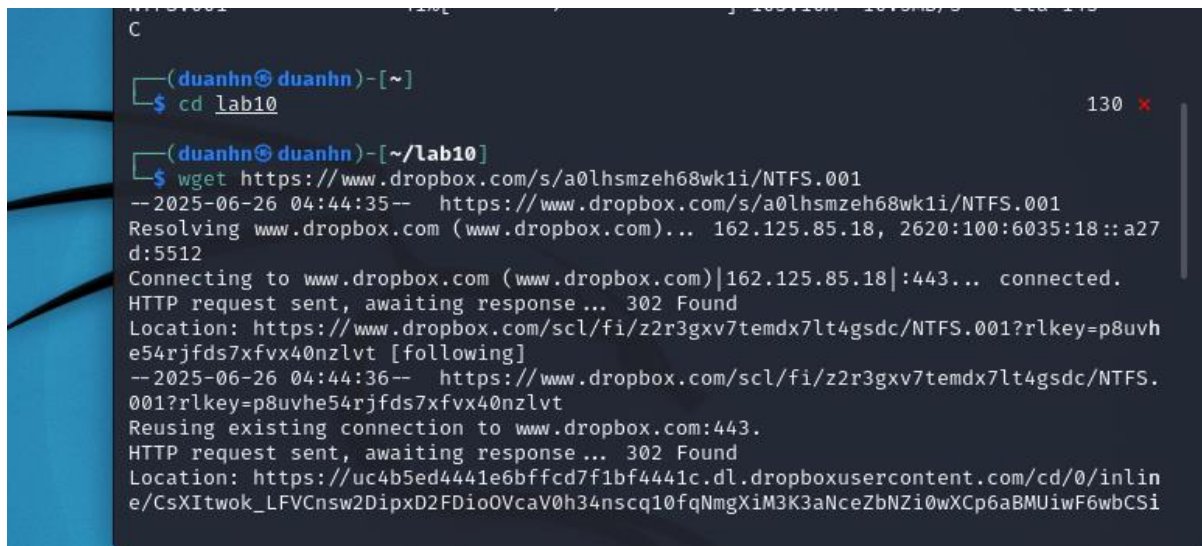
Step 1.

- Create a working folder

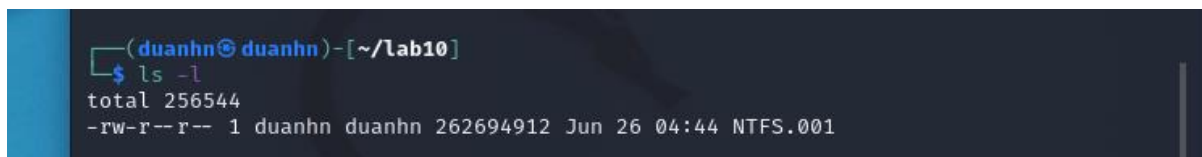


```
File Actions Edit View Help
(duanh@duanh)-[~]
$ mkdir lab10
(duanh@duanh)-[~]
$ wget https://www.dropbox.com/s/a0lhsmzeh68wk1i/NTFS.001
```

- Download a USB image



```
(duanh@duanh)-[~]
$ cd lab10
(duanh@duanh)-[~/lab10]
$ wget https://www.dropbox.com/s/a0lhsmzeh68wk1i/NTFS.001
--2025-06-26 04:44:35-- https://www.dropbox.com/s/a0lhsmzeh68wk1i/NTFS.001
Resolving www.dropbox.com (www.dropbox.com)... 162.125.85.18, 2620:100:6035:18::a27d:5512
Connecting to www.dropbox.com (www.dropbox.com)|162.125.85.18|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://www.dropbox.com/scl/fi/z2r3gxv7temdx7lt4gsdc/NTFS.001?rlkey=p8uvhe54rjfds7xfvx40nzlvt [following]
--2025-06-26 04:44:36-- https://www.dropbox.com/scl/fi/z2r3gxv7temdx7lt4gsdc/NTFS.001?rlkey=p8uvhe54rjfds7xfvx40nzlvt
Reusing existing connection to www.dropbox.com:443.
HTTP request sent, awaiting response... 302 Found
Location: https://uc4b5ed4441e6bffd7f1bf4441c.dl.dropboxusercontent.com/cd/0/inlin
e/CsXItwok_LFVCnsw2DipxD2FDio0VcaV0h34nscq10fqNmgXiM3K3aNceZbNZi0wXCp6aBMUiwF6wbCSi
```



```
(duanh@duanh)-[~/lab10]
$ ls -l
total 256544
-rw-r--r-- 1 duanh duanh 262694912 Jun 26 04:44 NTFS.001
```

```
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44
(duanhn@duanhn)-[~/lab10]
$ md5sum NTFS.001
fa7eecd50a691ab3245653ae91b762b2 NTFS.001
(duanhn@duanhn)-[~/lab10]
```

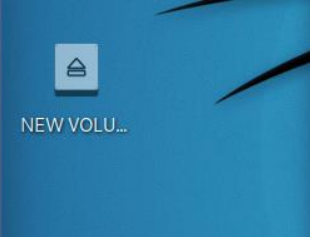
file

- Show image information

```
fa7eecd50a691ab3245653ae91b762b2 NTFS.001
(duanhn@duanhn)-[~/lab10]
$ file NTFS.001
NTFS.001: DOS/MBR boot sector MS-MBR Windows 7 english at offset 0x163 "Invalid partition table" at offset 0x17b "Error loading operating system" at offset 0x19a "Missing operating system", disk signature 0x9940673b; partition 1 : ID=0x7, start-CHS (0x0,2,3), end-CHS (0x1e,254,63), startsector 128, 509952 sectors
```

Step 2.

Mount the USB to Linux as a read-only loop device



```
NTFS.001: DOS/MBR boot sector MS-MBR Windows 7 english at offset 0x163 "Invalid partition table" at offset 0x17b "Error loading operating system" at offset 0x19a "Missing operating system", disk signature 0x9940673b; partition 1 : ID=0x7, start-CHS (0x0,2,3), end-CHS (0x1e,254,63), startsector 128, 509952 sectors
(duanhn@duanhn)-[~/lab10]
$ sudo losetup --partscan --find --show --read-only NTFS.001
[sudo] password for duanhn:
/dev/loop0
(duanhn@duanhn)-[~/lab10]
$
```

- View file structure

```
(duanhn@duanhn)-[~/lab10]
$ tree /media/duanhn/"NEW VOLUME"
/media/duanhn/NEW VOLUME
├── forTeaching
│   ├── crack_word_lab.TXT
│   ├── encrypted_file_123abc_2013_v.docx
│   ├── hash.txt
│   ├── HelloFAT.docx
│   ├── how_to_crack_pwd_123.pdf
│   ├── how_to_crack_pwd_abc123.pdf
│   ├── M57-Jean_Solution.pdf
│   ├── nps-2008-jean_outlook.pst
│   ├── office2john.py
│   ├── pdf2john.py
│   ├── pdfM57-Jean-hash.txt
│   ├── HelloNTFS.docx
│   ├── System Volume Information
│   ├── IndexerVolumeGuid
│   └── WPSettings.dat
```

- Syntax

\$find [where to start searching from] [expression determines what to find]

FIND(1)
General Commands Manual
FIND(1)

NAME

find - search for files in a directory hierarchy

SYNOPSIS

```
find [-H] [-L] [-P] [-D debugopts] [-Olevel] [starting-point...] [expression]
```

DESCRIPTION

This manual page documents the GNU version of **find**. GNU **find** searches the directory tree rooted at each given starting-point by evaluating the given expression from left to right, according to the rules of precedence (see section OPERATORS), until the outcome is known (the left hand side is false for **and** operations, true for **or**), at which point **find** moves on to the next file name. If no starting-point is specified, **.'** is assumed.

- Find Files/directories starts from Current Directory (recursively)

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find .
.
./forTeaching
./forTeaching/crack_word_lab.TXT
./forTeaching/encrypted_file_123abc_2013_v.docx
./forTeaching/hash.txt
./forTeaching/HelloFAT.docx
./forTeaching/how_to_crack_pwd_123.pdf
./forTeaching/how_to_crack_pwd_abc123.pdf
./forTeaching/M57-Jean_Solution.pdf
./forTeaching/nps-2008-jean_outlook.pst
./forTeaching/office2john.py
./forTeaching/pdf2john.py
./forTeaching/pdfM57-Jean-hash.txt
./HelloNTFS.docx
./System Volume Information
./System Volume Information/IndexerVolumeGuid
./System Volume Information/WPSettings.dat
```

-name and **-iname**: find file/directory names

- find a file

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find ./forTeaching -name hash.txt
./forTeaching/hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find . -name hash.txt
./forTeaching/hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$
```

- find a file and ignore case

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find . -name hash.TXT

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find . -iname hash.TXT
./forTeaching/hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
```

- find a directory

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find . -name forTeaching
./forTeaching
```

type: specify string types

- Specify the search type *d*: directory

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find -type d -name forTeaching
./forTeaching
```

- Specify the search type *f*: file

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find -type f -name hash.txt
./forTeaching/hash.txt
```

- Search all files with extension *.txt*

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find -type f -name "*.txt"
./forTeaching/hash.txt
./forTeaching/pdfM57-Jean-hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
```

- Match all files which first and four letters are “h”

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find -type f -name "h??h*"
./forTeaching/hash.txt
```

- Match all files contains “123” (in the middle of the file name)

```
./forTeaching/hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find -type f -name "*123*"
./forTeaching/encrypted_file_123abc_2013_v.docx
./forTeaching/how_to_crack_pwd_123.pdf
./forTeaching/how_to_crack_pwd_abc123.pdf

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
```

- Find Files With 777 Permissions

```
(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ find ./forTeaching -type f -perm 777 -print
./forTeaching/crack_word_lab.TXT
./forTeaching/encrypted_file_123abc_2013_v.docx
./forTeaching/hash.txt
./forTeaching/HelloFAT.docx
./forTeaching/how_to_crack_pwd_123.pdf
./forTeaching/how_to_crack_pwd_abc123.pdf
./forTeaching/M57-Jean_Solution.pdf
./forTeaching/nps-2008-jean_outlook.pst
./forTeaching/office2john.py
./forTeaching/pdf2john.py
./forTeaching/pdfM57-Jean-hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$ ls -l ./forTeaching
total 4082
-rwxrwxrwx 1 root root 57 Oct 2 2018 crack_word_lab.TXT
-rwxrwxrwx 1 root root 17920 Oct 2 2018 encrypted_file_123abc_2013_v.docx
-rwxrwxrwx 1 root root 194 Oct 2 2018 hash.txt
-rwxrwxrwx 1 root root 11514 Oct 8 2018 HelloFAT.docx
-rwxrwxrwx 1 root root 1185208 Oct 1 2018 how_to_crack_pwd_123.pdf
-rwxrwxrwx 1 root root 380207 Oct 1 2018 how_to_crack_pwd_abc123.pdf
-rwxrwxrwx 1 root root 96290 Oct 5 2018 M57-Jean_Solution.pdf
-rwxrwxrwx 1 root root 2326528 Jul 20 2008 nps-2008-jean_outlook.pst
-rwxrwxrwx 1 root root 134772 Oct 2 2018 office2john.py
-rwxrwxrwx 1 root root 13904 Oct 5 2018 pdf2john.py
-rwxrwxrwx 1 root root 191 Oct 5 2018 pdfM57-Jean-hash.txt

(duanhn@duanhn)-[/media/duanhn/NEW VOLUME]
$
```

Step 3.

- “atime”, “mtime” and “ctime”


```
(duanhn@duanhn)-[~/lab10]
$ echo hello world > myFile.txt

(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256548
-rw-r--r-- 1 duanhn duanhn      12 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001

(duanhn@duanhn)-[~/lab10]
$ echo hello world again! >> myFile.txt

(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256548
-rw-r--r-- 1 duanhn duanhn      31 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001

(duanhn@duanhn)-[~/lab10]
$ cat myFile.txt
hello world
hello world again!

(duanhn@duanhn)-[~/lab10]
$
```

Can you recreate the file changing history? Answer and explain

```
(duanhn@duanhn)-[~/lab10]
$ stat myFile.txt
File: myFile.txt
Size: 31          Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d Inode: 1057928    Links: 1
Access: (0644/-rw-r--r--)  Uid: ( 1000/  duanhn)   Gid: ( 1000/  duanhn)
Access: 2025-06-26 05:25:50.400543761 -0400
Modify: 2025-06-26 05:25:43.345017722 -0400
Change: 2025-06-26 05:25:43.345017722 -0400
Birth: 2025-06-26 05:25:09.972339542 -0400

(duanhn@duanhn)-[~/lab10]
$
```

Answer

- Timestamp changes when changing permission

```
(duanhn@duanhn)-[~/lab10]
$ echo test for deletion > testTimeStamp.txt

(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256552
-rw-r--r-- 1 duanhn duanhn      31 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001
-rw-r--r-- 1 duanhn duanhn      18 Jun 26 05:28 testTimeStamp.txt

(duanhn@duanhn)-[~/lab10]
$ sudo chmod 664 testTimeStamp.txt
[sudo] password for duanhn:

(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256552
-rw-r--r-- 1 duanhn duanhn      31 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001
-rw-rw-r-- 1 duanhn duanhn      18 Jun 26 05:28 testTimeStamp.txt

(duanhn@duanhn)-[~/lab10]
$
```

Find Files With “-perm=664” Permissions ?

```
(student@kali80)-[~/searchLab]
$ ls -l
total 256548
-rw-r--r-- 1 student student      31 Sep 17 21:17 myFile.txt
-rw-r--r-- 1 student student 262694912 Sep 17 14:23 NTFS.001
-rw-rw-r-- 1 student student      18 Sep 17 22:53 testTimeStamp.txt
```

Answer

-rw-rw-r-- 1 duanhn duanhn 18 Jun 26 05:28 testTimeStamp.txt

```
(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256552
-rw-r--r-- 1 duanhn duanhn      31 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001
-rw-rw-r-- 1 duanhn duanhn      18 Jun 26 05:28 testTimeStamp.txt
```

Find Files With /u=r /u=w /u=x Permissions

```

(student@kali80)-[~/searchLab]
$ ls -l
total 256548
-rw-r--r-- 1 student student      31 Sep 17 21:17 myFile.txt
-rw-r--r-- 1 student student 262694912 Sep 17 14:23 NTFS.001
-rw-rw-r-- 1 student student      18 Sep 17 22:53 testTimeStamp.txt

```

Answer

Not available

```

(duanhn@duanhn)-[~/lab10]
$ ls -l
total 256552
-rw-r--r-- 1 duanhn duanhn      31 Jun 26 05:25 myFile.txt
-rw-r--r-- 1 duanhn duanhn 262694912 Jun 26 04:44 NTFS.001
-rw-rw-r-- 1 duanhn duanhn      18 Jun 26 05:28 testTimeStamp.txt

```

Find Changed Files in Last 1 Hour ?

```

(student@kali80)-[~/searchLab]
$ date
Fri 17 Sep 2021 11:31:53 PM EDT

(student@kali80)-[~/searchLab]
$ find . -type f -cmin -60
./testTimeStamp.txt

```

Answer

./testTimeStamp.txt

./myFile.txt

```

(duanhn@duanhn)-[~/lab10]
$ date
Thu Jun 26 05:55:46 AM EDT 2025

(duanhn@duanhn)-[~/lab10]
$ find . -type f -cmin -60
./testTimeStamp.txt
./myFile.txt

```

Find Accessed Files in Last 1 Hour ?


```

(student@kali80)-[~/searchLab]
$ date
Fri 17 Sep 2021 11:38:16 PM EDT

(student@kali80)-[~/searchLab]
$ find . -type f -amin -60
./testTimeStamp.txt

```

Answer

```

(duanh@duanh)-[~/lab10]
$ find . -type f -amin -60
./testTimeStamp.txt
./myFile.txt

```

./testTimeStamp.txt

./myFile.txt

Find files that size that is great than 10MB ?

```

(student@kali80)-[~/searchLab]
$ find . -size +10M
./NTFS.001

```

Answer

```

(duanh@duanh)-[~/lab10]
$ find . -size +10M
./NTFS.001

```

YOU MUST SUBMIT A FULL-SCREEN IMAGE FOR FULL CREDIT!

Save the document with the filename "**YOUR NAME Lab 10.pdf**", replacing "YOUR NAME" with your real name.

Email the image to the instructor as an attachment to an e-mail message. Send it to: **xxx@fe.edu.vn** with a subject line of "**Lab 10 From YOUR NAME**", replacing "YOUR NAME" with your real name.

