

Lab - Finding Out About the Organization

Objectives

In this lab, you will complete the following objectives:

- Find information about email breaches.
- View file metadata.

Background / Scenario

The purpose of reconnaissance in penetration test is gathering information about a client that can be used later for exploitation. There are many resources that help with this process. In this lab, you will learn about online resources that can provide information about an enterprise.

Required Resources

- Kali VM customized for the Ethical Hacker course
- Internet access

Instructions

Part 1: Find Information about Email Breaches.

It is possible to learn more about a person or organization by searching on a known email address. It is useful to determine if employees of a company have had their work email addresses compromised. Several online services provide the ability to search on individual email addresses and entire domains to reveal breaches. Some of those sites are:

- haveibeenpwned.com
- f-secure.com
- hacknotice.com
- breachdirectory.com
- keepersecurity.com

Step 1: Investigate your email status.

Explore the different sites and search for your own email address or the domain of a company that you know of. It is especially concerning if a recent data breach has occurred for a domain. It is also possible that a penetration testing client is unaware of the breach.

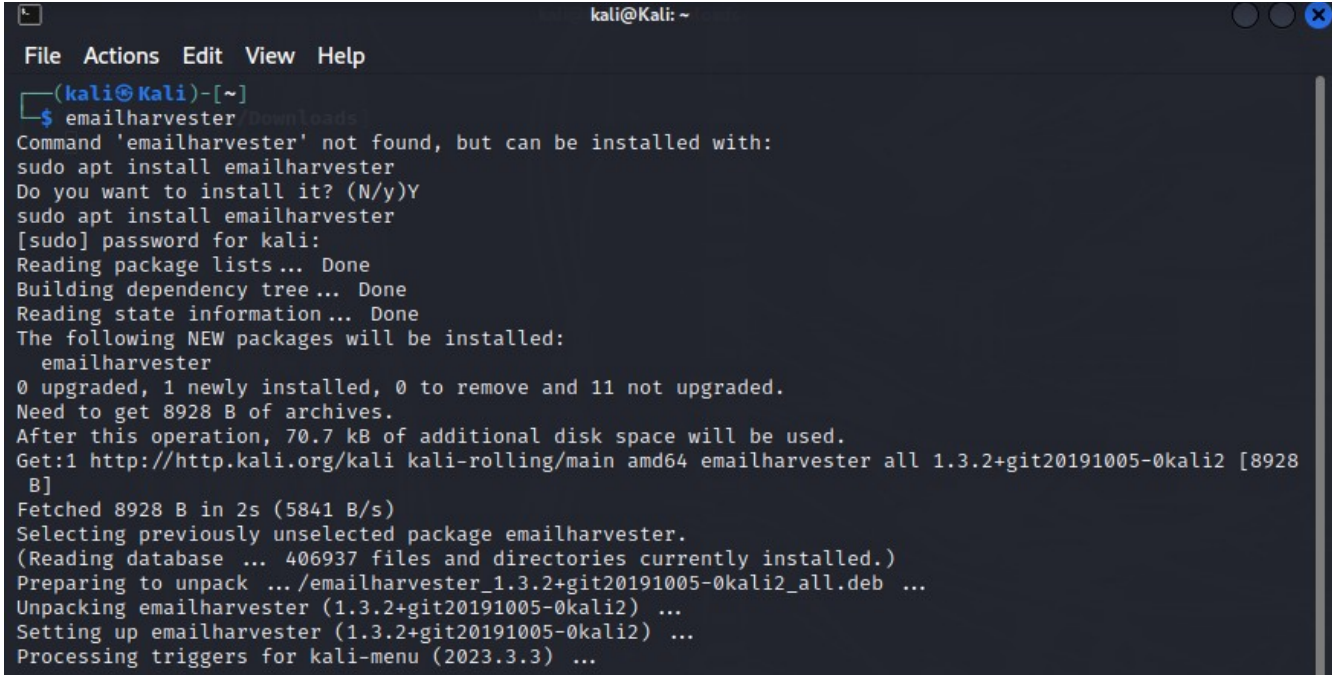
Resources exist that will allow access to these data breach files. From there, you may be able to find usernames, email addresses, passwords, and other information about employees. This information will be very useful in the exploitation part of the PenTesting process.

In my case I used haveibeenpwned.com and [breachedirectory.com](https://breachdirectory.com) and my email has 0 data breaches

Step 2: Use a tool to find email addresses for a domain.

You will use a tool called **EmailHarvester** to find information about a domain, including email addresses of personnel.

- a. Open a terminal and enter the command **emailharvester**. The tool has not yet been installed in Kali, but it is part of the Kali toolset. Enter **y** to agree to install the tool and provide the password for the user **kali** if prompted.

A screenshot of a Kali Linux terminal window. The window title is 'kali@Kali: ~'. The terminal shows the command 'emailharvester' being entered, which results in a message that the command is not found but can be installed with 'sudo apt install emailharvester'. The user enters 'y' to confirm installation. The terminal then shows the progress of the installation, including reading package lists, building the dependency tree, and fetching the package. The installation is successful, and the terminal shows the package being unpacked and triggers being processed.

```
kali@Kali: ~  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ emailharvester/Downloads  
Command 'emailharvester' not found, but can be installed with:  
sudo apt install emailharvester  
Do you want to install it? (N/y)Y  
sudo apt install emailharvester  
[sudo] password for kali:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  emailharvester  
0 upgraded, 1 newly installed, 0 to remove and 11 not upgraded.  
Need to get 8928 B of archives.  
After this operation, 70.7 kB of additional disk space will be used.  
Get:1 http://http.kali.org/kali kali-rolling/main amd64 emailharvester all 1.3.2+git20191005-0kali2 [8928 B]  
Fetched 8928 B in 2s (5841 B/s)  
Selecting previously unselected package emailharvester.  
(Reading database ... 406937 files and directories currently installed.)  
Preparing to unpack .../emailharvester_1.3.2+git20191005-0kali2_all.deb ...  
Unpacking emailharvester (1.3.2+git20191005-0kali2) ...  
Setting up emailharvester (1.3.2+git20191005-0kali2) ...  
Processing triggers for kali-menu (2023.3.3) ...
```

- b. After installation is complete, use the **-h** option to see the options available in the tool


```
(kali㉿kali)-[~]
$ emailharvester -d scanme.nmap.org
[+] User-Agent in use: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1
[+] Searching everywhere
[+] Searching in ASK: 10 results
[+] Searching in ASK: 20 results
[+] Searching in ASK: 30 results
[+] Searching in ASK: 40 results
[+] Searching in ASK: 50 results
[+] Searching in ASK: 60 results
[+] Searching in ASK: 70 results
[+] Searching in ASK: 80 results
[+] Searching in ASK: 90 results
[+] Searching in ASK: 100 results
[+] Searching in Reddit
[+] Searching in Yahoo + Reddit: 101 results
[+] Searching in Bing + Reddit: 50 results
[+] Searching in Bing + Reddit: 100 results
[+] Searching in Google + Reddit: 100 results
[+] Searching in Baidu + Reddit: 10 results
[+] Searching in Baidu + Reddit: 20 results
[+] Searching in Baidu + Reddit: 30 results
[+] Searching in Baidu + Reddit: 40 results
[+] Searching in Baidu + Reddit: 50 results
[+] Searching in Baidu + Reddit: 60 results
[+] Searching in Baidu + Reddit: 70 results
[+] Searching in Baidu + Reddit: 80 results
[+] Searching in Baidu + Reddit: 90 results
[+] Searching in Baidu + Reddit: 100 results
[+] Searching in Exalead + Reddit: 50 results
[+] Searching in Exalead + Reddit: 100 results
[+] Searching in Dogpile: 11 results
[+] Searching in Dogpile: 21 results
[+] Searching in Dogpile: 31 results
[+] Searching in Dogpile: 41 results
[+] Searching in Dogpile: 51 results
[+] Searching in Dogpile: 61 results
[+] Searching in Dogpile: 71 results
[+] Searching in Dogpile: 81 results
[+] Searching in Dogpile: 91 results
[+] Searching in Dogpile: 101 results
[+] Searching in Bing: 50 results
[+] Searching in Bing: 100 results
[+] Searching in Baidu: 10 results
[+] Searching in Baidu: 20 results
[+] Searching in Baidu: 30 results
[+] Searching in Baidu: 40 results
[+] Searching in Baidu: 50 results
[+] Searching in Baidu: 60 results
[+] Searching in Baidu: 70 results
[+] Searching in Baidu: 80 results
[+] Searching in Baidu: 90 results
[+] Searching in Baidu: 100 results
```

Check some of the emails addresses that you have obtained to determine if they have been part of a data breach. If so, this indicates that account details are available on the dark web. A penetration tester who has access to breach databases could search for additional information there.

Your results can be output to a file that can be used by other tools as an input list. Use the `-s` option to specify a file name. Emailharvester creates both XML and text files. Supply a path if desired.

Otherwise, the files will appear in the `/user/share/emailharvester` folder. Inspect the contents of the files.

Step 3: Use Spiderfoot to research email addresses.

- a. Open the Spiderfoot GUI:

```
File Actions Edit View Help
(kali㉿kali)-[~]
└─$ spiderfoot -l 127.0.0.1:5001
2025-12-20 19:16:43,663 [INFO] sf : Starting web server at 127.0.0.1:5001 ...

*****
Use SpiderFoot by starting your web browser of choice and
browse to http://127.0.0.1:5001/
*****

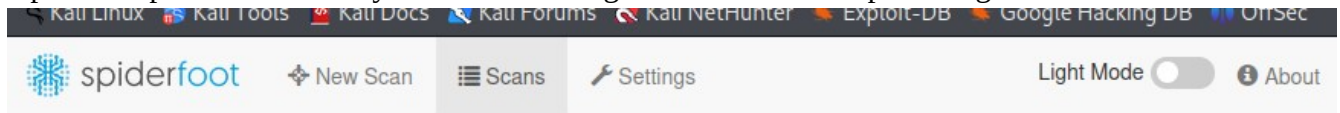
2025-12-20 19:16:43,691 [WARNING] sf :
*****
Warning: passwd file contains no passwords. Authentication disabled.
Please consider adding authentication to protect this instance!
Refer to https://www.spiderfoot.net/documentation/#security.
*****

[+] Searching in Baidu + Youtube: 50 results
[+] Searching in Baidu + Youtube: 100 results
[+] Searching in Exalead + Youtube: 50 results
[+] Searching in Exalead + Youtube: 100 results

--kali㉿kali-
~$ emailharvester -d Hackxor.net
[+] User-Agent in user: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.0
[+] Searching everywhere
[+] Searching in ASK: 50 results
[+] Searching in ASK: 70 results
[+] Searching in ASK: 30 results
[+] Searching in ASK: 40 results
[+] Searching in ASK: 50 results
[+] Searching in ASK: 60 results
[+] Searching in ASK: 70 results
[+] Searching in ASK: 80 results
[+] Searching in ASK: 90 results
[+] Searching in ASK: 100 results
[+] Searching in Bing
[+] Searching in Bing
```

Minimize (don't close) the terminal.

Open the Spiderfoot GUI in your browser using the IP address and port assigned above.



Click the **Settings** menu item and investigate the available modules.

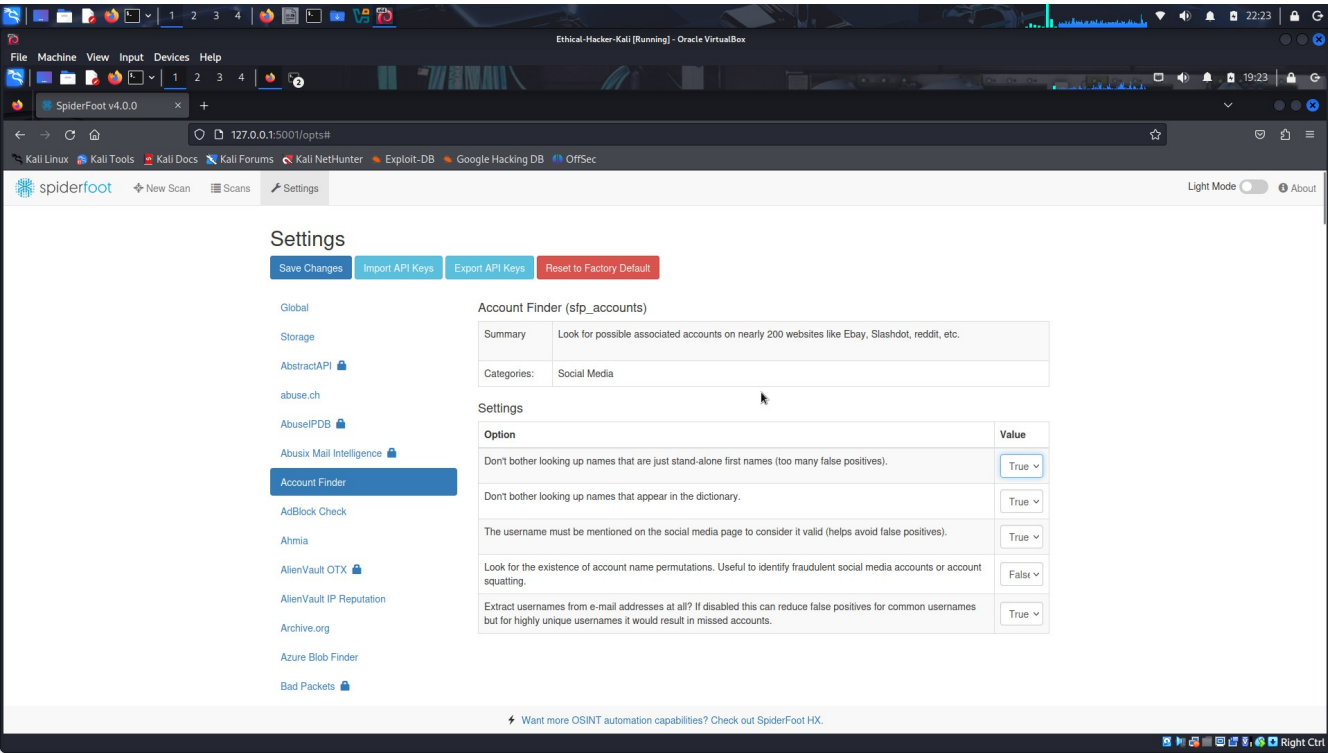
Settings

[Save Changes](#)[Import API Keys](#)[Export API Keys](#)[Reset to Factory Default](#)

Global

[Storage](#)[AbstractAPI](#) [abuse.ch](#)[AbuseIPDB](#) [Abusix Mail Intelligence](#) [Account Finder](#)[AdBlock Check](#)[Ahmia](#)[AlienVault OTX](#) [AlienVault IP Reputation](#)[Archive.org](#)[Azure Blob Finder](#)[Bad Packets](#) 

Read the descriptions of the modules and investigate the API requirements if any. Optionally, register for some of the free API keys. Configure the modules with the keys.



Look for modules that would be useful for doing email scans. For example, you would like to know whether the address is part of breach, what accounts are registered to the address on social media sites and code repositories, link sharing, and technical forums. Make note of your findings.

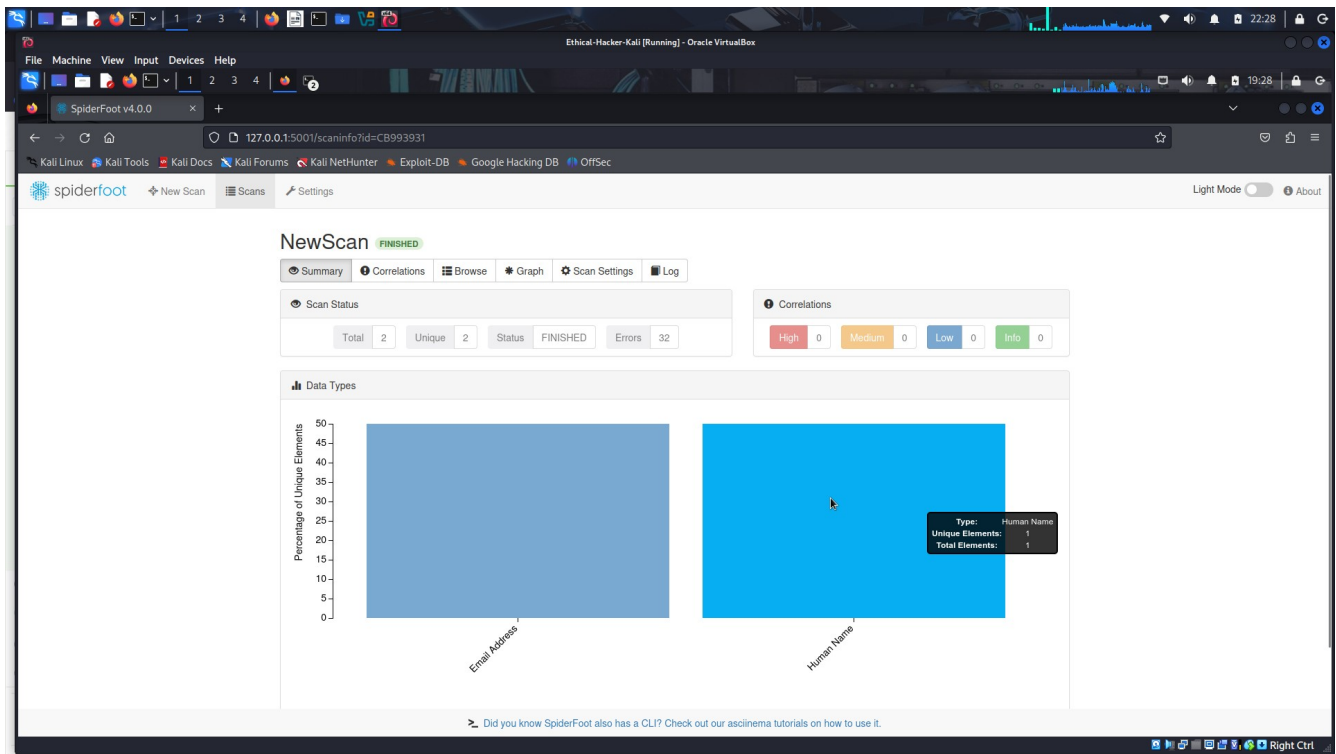
A few interesting modules are:

Ahmia	AccountFinder	Archive.org
Bing	Leak-Lookup	CommonCrawl
Dehashed	DuckDuckGo	EmailCrawlr

There are others.

Try running a new scan on an interesting email address by selecting the interesting modules in the **New Scan > By Module** tab.

After making your selections and supply scan name and target, scroll to the bottom of the page and click **Run Scan Now**.



Part 2: View File Metadata.

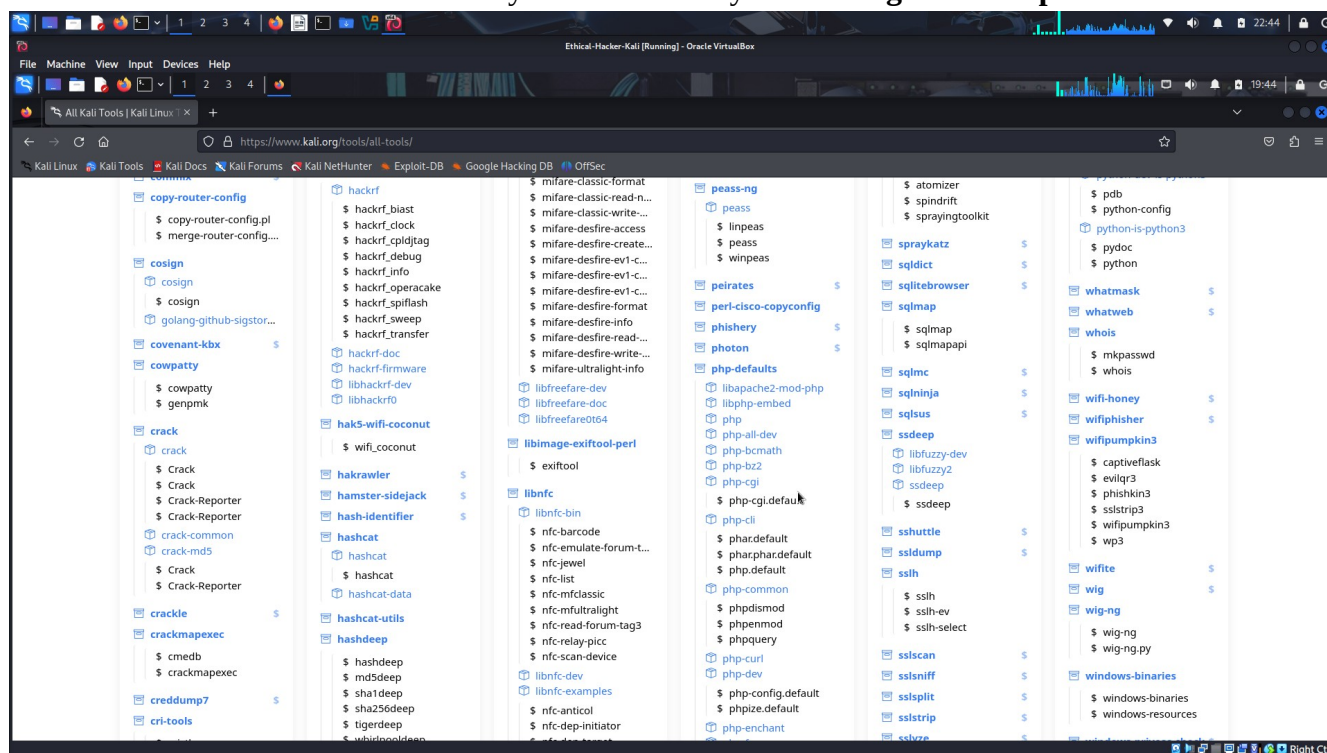
File metadata can provide hackers with insights into organizations and personnel. For example, metadata within an image file can reveal the device that was used create the image. This can reveal information that can be used to determine if the device is potentially vulnerable. Some files have metadata consisting of comments, the author's name, usernames, the operating system, or the location at which the file was created. Metadata varies by the type of file and the device on which it was created. Hackers can use this information to piece together a means of attack.

In general, files that are posted on the public internet should have their metadata stripped or at least scrutinized. You can use ExifTool, among others, to remove or edit tags from individual files or a directory of files.

ExifTool comes in a GUI version that is available for Windows, MacOS, and Linux.

Step 1: Install ExifTool.

- In Firefox, click the **Kali Tools** shortcut or navigate to <https://www.kali.org/tools>.
- Select **List all tools** as necessary. Locate the entry for **libimage-exiftool-perl**.



The screenshot shows a Kali Linux desktop environment. A web browser window is open, displaying the Kali.org website. The browser's address bar shows the URL <https://www.kali.org/tools/libimage-exiftool-perl/Hexiftool>. The website's header includes the Kali logo and navigation links: JOIN FREE CTF, GET KALI, BLOG, DOCUMENTATION, COMMUNITY, COURSES, DEVELOPERS, and ABOUT. The main content area is titled 'Libimage-Exiftool-Perl' and features a logo with a blue circle and a green gear. Below the logo, it states 'version: 13.36 arch: all'. There are links to the 'Libimage-Exiftool-Perl Homepage', 'Package Tracker', 'Source Code Repository', and 'Edit This Page'. The 'Metapackages' section lists 'default', 'everything', and 'large'. The 'Packages & Binaries' section lists 'libimage-exiftool-perl' and 'exiftool'. The right sidebar, titled 'Packages and Binaries:', provides a detailed description of 'libimage-exiftool-perl' as a library and program to read and write meta information in multimedia files. It lists recommended modules/packages for specific features, such as decoding compressed and/or encrypted information from the indicated file types, calculating digest values for some information types, etc. The installed size is 27.36 MB, and the installation command is 'sudo apt install libimage-exiftool-perl'.

c. Follow the instructions to install ExifTool.
Download ExifTool from <https://exiftool.org/>

```
(kali㉿kali)-[~]
$ cd Downloads

(kali㉿kali)-[~/Downloads]
$ ls
HJ6jhE-3.cer.part      SA.pcap      exiftool-13.44_64.zip
Image-ExifTool-13.44.tar.gz  Sampleimage.jpeg  t720Cjcu.cer.part

(kali㉿kali)-[~/Downloads]
$ gzip -dc Image-ExifTool-13.44.tar.gz | tar -xf -

(kali㉿kali)-[~/Downloads]
$ ls
HJ6jhE-3.cer.part      Image-ExifTool-13.44      Sampleimage.jpeg      t720Cjcu.cer.part
Image-ExifTool-13.44  SA.pcap      exiftool-13.44_64.zip

(kali㉿kali)-[~/Downloads]
$ cd Image-ExifTool-13.44

(kali㉿kali)-[~/Downloads/Image-ExifTool-13.44]
$ ./exiftool t/images/ExifTool.jpg
ExifTool Version Number      : 13.44
File Name                    : ExifTool.jpg
Directory                   : t/images
File Size                    : 26 kB
File Modification Date/Time  : 2025:01:26 17:47:08+00:00
File Access Date/Time       : 2025:12:20 20:02:11+00:00
File Inode Change Date/Time  : 2025:12:20 20:02:11+00:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            : A witty caption
Orientation                  : Horizontal (normal)
Software                     : Adobe Photoshop 7.0
Modify Date                  : 2004:02:26 09:36:46
Artist                       : Phil Harvey
Y Cb Cr Positioning          : Co-sited
F Number                     : 3.5
Exposure Program             : Program AE
ISO                           : 100
Exif Version                 : 0210
Create Date                  : 2001:05:19 18:36:41
Components Configuration     : Y, Cb, Cr, -
Compressed Bits Per Pixel    : 1.6
Brightness Value             : 2
Max Aperture Value           : 3.5
Metering Mode                : Multi-segment
```

- d. ExifTool refers to metafile attributes as tags. Use the **-list** option to view all the tags that ExifTool can process.
- e. Issue the **exiftool -listf** command to review the file types that ExifTool can analyze.

```
(kali@kali)-[~]
$ exiftool -listf
Supported file extensions:
360 3FR 3G2 3GP 3GP2 3GPP 7Z A AA AAE AAX ACFM ACR AFM AI AIF AIFC AIFF AIT
AMFM APE APNG ARQ ARW ASF AVI AVIF AZW AZW3 BMP BPG BTIF CHM CIFF COS CR2 CR3
CRM CRW CS1 CSV CUR CZI DC3 DCM DCP DCR DFONT DIB DIC DICM DIVX DJV DJVU DLL
DNG DOC DOCM DOCX DOT DOTM DOTX DPX DR4 DS2 DSS DV DVB DVR-MS DYLIB EIP EPS
EPS2 EPS3 EPSF EPUB ERF EXE EXIF EXR EXV F4A F4B F4P F4V FFF FIT FITS FLA
FLAC FLIF FLIR FLV FPF FPX GIF GLV GPR GZ GZIP HDP HDR HEIC HEIF HIF HTM HTML
ICAL ICC ICM ICO ICS IDML IIQ IND INDD INDT INSP INSV INX ISO ITC J2C J2K JNG
JP2 JPC JPE JPEG JPF JPG JPM JPS JPX JSON JXL JXR K25 KDC KEY KTH LA LFP LFR
LIF LNK LRV M2T M2TS M2V M4A M4B M4P M4V MACOS MAX MEF MIE MIF MIFF MKA MKS
MKV MNG MOBI MODD MOI MOS MOV MP3 MP4 MPC MPEG MPG MPO MQV MRC MRW MTS MXF
NEF NEWER NKSC NMBTEMPLATE NRW NUMBERS O ODB ODC ODF ODG ODI ODP ODS ODT OFR
OGG OGV ONP OPUS ORF ORI OTF PAC PAGES PBM PCD PCT PCX PDB PDF PEF PFA PFB
PFM PGF PGM PICT PLIST PMP PNG POT POTM POTX PPAM PPAX PPM PPS PPSM PPSX PPT
PPTM PPTX PRC PS PS2 PS3 PSB PSD PSDT PSP PSPFRAME PSPIMAGE PSPSHAPE PSPTUBE
QIF QT QTI QTIF R3D RA RAF RAM RAR RAW RIF RIFF RM RMVB RPM RSRC RTF RV RW2
RWL RWZ SEQ SKETCH SO SR2 SRF SRW SVG SWF THM THMX TIF TIFF TORRENT TS TTC
TTF TUB TXT VCARD VCF VNT VOB VRD VSD WAV WDP WEBM WEBP WMA WMV WOFF WOFF2
WPG WTV WV X3F XCF XHTML XLA XLAM XLS XLSB XLSM XLSX XLT XLTM XLTX XMP ZIP
```

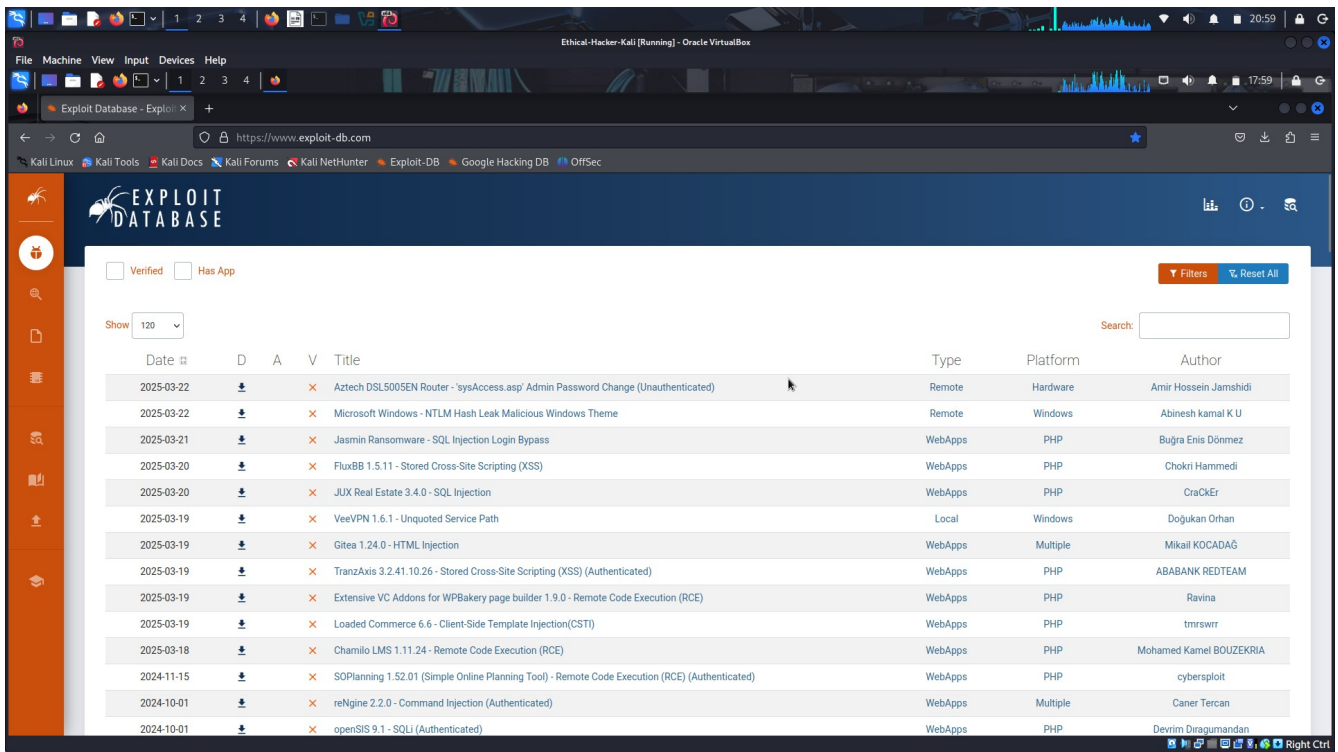
ExifTool can read metadata from a wide range of files. Review the output and complete the table with some of the common file formats that ExifTool can read by type.

Type	File Formats (extension)
Documents	PDF, TXT, DOC, DOCM, DOCX, HTML
Audio	FLAC, MP3, WAV, AIFF, RA, WMA
Video	AVI, DV, FLV, MOV, QT, MP4, MPEG, RM, WEBM, WMV
Graphics	BMP, EXIF, GIF, JPEG, JPG, PNG, SVG, TIFF
Archives	GZ, GZIP, RAR, ZIP

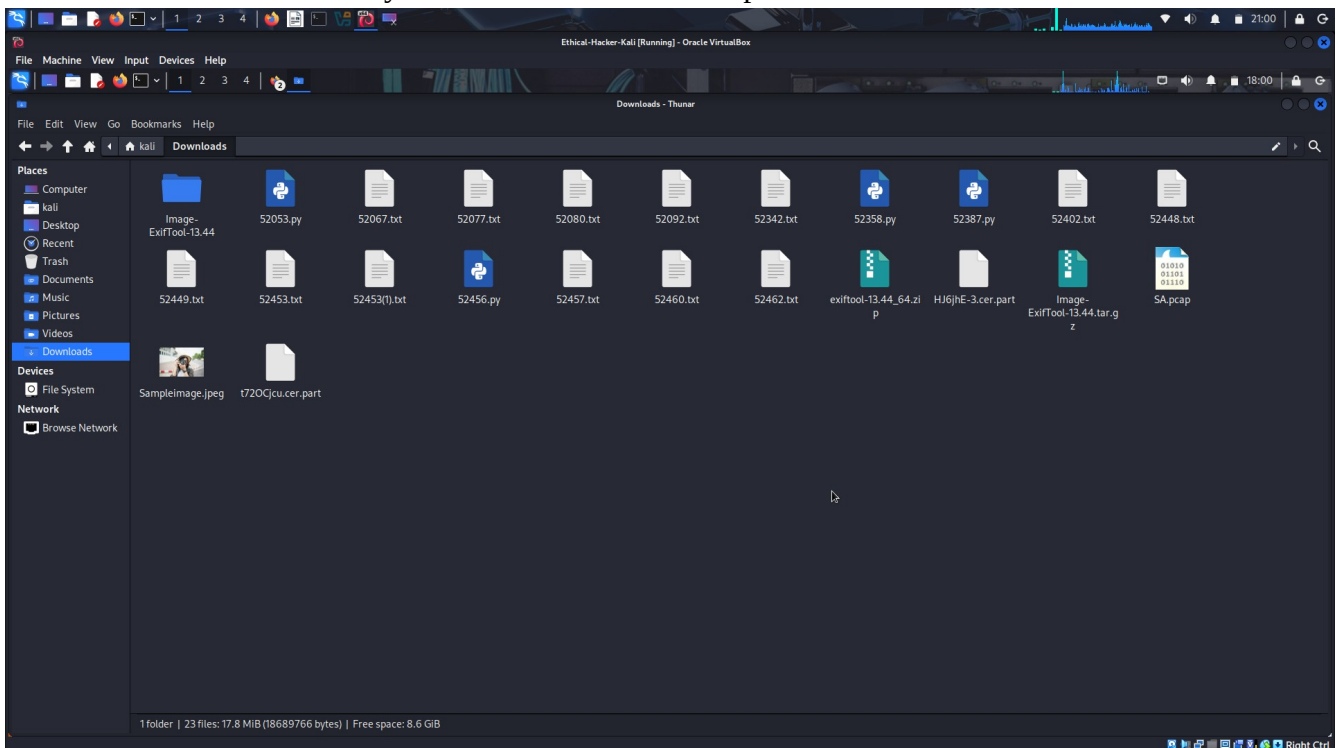
Step 2: Use ExifTool.

You will need some files that you can use to explore metadata with the tool. You can do so with files that you have on your PC, or better yet, files that you can find openly available online.

- a. Go to the Google Hacker Database (GHDB). Locate dorks that will help you to find a variety of files of various types or modify the dorks that you find to do so.



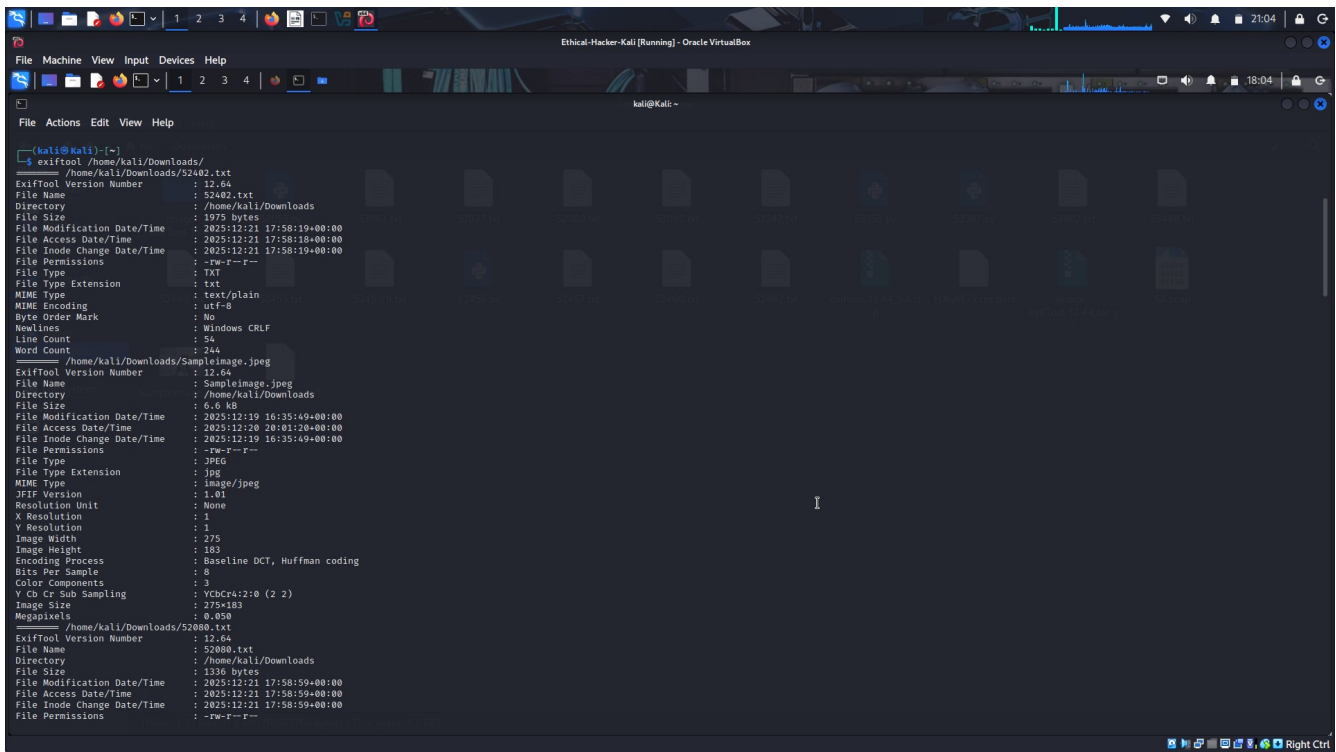
b. Download the files to your VM. Make note of the path to the folder.



c. Experiment with ExifTools. Start by simply running the exiftool command followed by the path and file name for the target file. Review the metadata that is returned. Do this for a number of files.

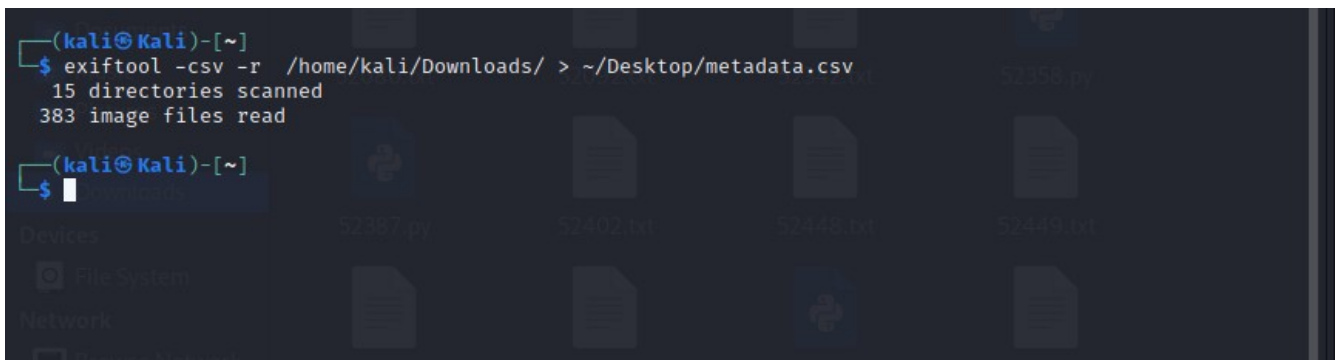

```
kali@Kali: ~  
File Actions Edit View Help  
(kali@Kali)-[~]  
$ exiftool /home/kali/Downloads/52053.py  
ExifTool Version Number      : 12.64  
File Name                    : 52053.py  
Directory                    : /home/kali/Downloads  
File Size                     : 2.2 kB  
File Modification Date/Time   : 2025:12:21 17:59:07+00:00  
File Access Date/Time        : 2025:12:21 17:59:07+00:00  
File Inode Change Date/Time   : 2025:12:21 17:59:07+00:00  
File Permissions              : -rw-r--r--  
File Type                     : TXT  
File Type Extension          : txt  
MIME Type                     : text/plain  
MIME Encoding                 : us-ascii  
Newlines                      : Windows CRLF  
Line Count                    : 62  
Word Count                    : 204  
  
(kali@Kali)-[~]  
$ exiftool /home/kali/Downloads/52448.txt  
ExifTool Version Number      : 12.64  
File Name                    : 52448.txt  
Directory                    : /home/kali/Downloads  
File Size                     : 999 bytes  
File Modification Date/Time   : 2025:12:21 17:58:02+00:00  
File Access Date/Time        : 2025:12:21 17:58:02+00:00  
File Inode Change Date/Time   : 2025:12:21 17:58:02+00:00  
File Permissions              : -rw-r--r--  
File Type                     : TXT  
File Type Extension          : txt  
MIME Type                     : text/plain  
MIME Encoding                 : us-ascii  
Newlines                      : Windows CRLF  
Line Count                    : 28  
Word Count                    : 120  
  
(kali@Kali)-[~]  
$
```

Now try running ExifTool for the entire folder. For this, you only supply the path.



```
(kali@kali)-[~]
└─$ exiftool /home/kali/Downloads/
===== /home/kali/Downloads/52402.txt
ExifTool Version Number      : 12.64
File Name                    : 52402.txt
Directory                    : /home/kali/Downloads
File Size                    : 1975 bytes
File Modification Date/Time   : 2025:12:21 17:58:19+00:00
File Access Date/Time        : 2025:12:21 17:58:18+00:00
File Inode Change Date/Time   : 2025:12:21 17:58:19+00:00
File Permissions              : -rw-r--r--
File Type                    : TXT
File Type Extension          : txt
MIME Type                    : text/plain
MIME Encoding                 : utf-8
Byte Order Mark               : No
Newlines                     : Windows CRLF
Line Count                   : 54
Word Count                   : 244
===== /home/kali/Downloads/SampleImage.jpeg
ExifTool Version Number      : 12.64
File Name                    : SampleImage.jpeg
Directory                    : /home/kali/Downloads
File Size                    : 6.6 KB
File Modification Date/Time   : 2025:12:19 16:35:49+00:00
File Access Date/Time        : 2025:12:20 20:01:20+00:00
File Inode Change Date/Time   : 2025:12:19 16:35:49+00:00
File Permissions              : -rw-r--r--
File Type                    : JPEG
File Type Extension          : jpg
MIME Type                    : image/jpeg
JFIF Version                 : 1.01
Resolution Unit              : None
X Resolution                  : 1
Y Resolution                  : 1
Image Width                  : 275
Image Height                 : 183
Encoding Process              : Baseline DCT, Huffman coding
Bits Per Sample               : 8
Color Components              : 3
Y Cb Cr Sub Sampling          : YCbCr4:2:0 (2 2)
Image Size                   : 275x183
Megapixels                   : 0.050
===== /home/kali/Downloads/52080.txt
ExifTool Version Number      : 12.64
File Name                    : 52080.txt
Directory                    : /home/kali/Downloads
File Size                    : 2336 bytes
File Modification Date/Time   : 2025:12:21 17:58:59+00:00
File Access Date/Time        : 2025:12:21 17:58:59+00:00
File Inode Change Date/Time   : 2025:12:21 17:58:59+00:00
File Permissions              : -rw-r--r--
```

- You can save the metadata for each image in the folder, or for individual images by adding the **-csv** option. For example:



```
(kali@kali)-[~]
└─$ exiftool -csv -r /home/kali/Downloads/ > ~/Desktop/metadata.csv
15 directories scanned
383 image files read

(kali@kali)-[~]
└─$
```

- On the internet, research some of the values that you find in the file. For example, the tag **CREATOR: gd-jpeg v1.0** indicates that the image was generated by the PHP GD library version 1.0. Search the internet **for PHP GD vulnerability** to learn more.

