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.

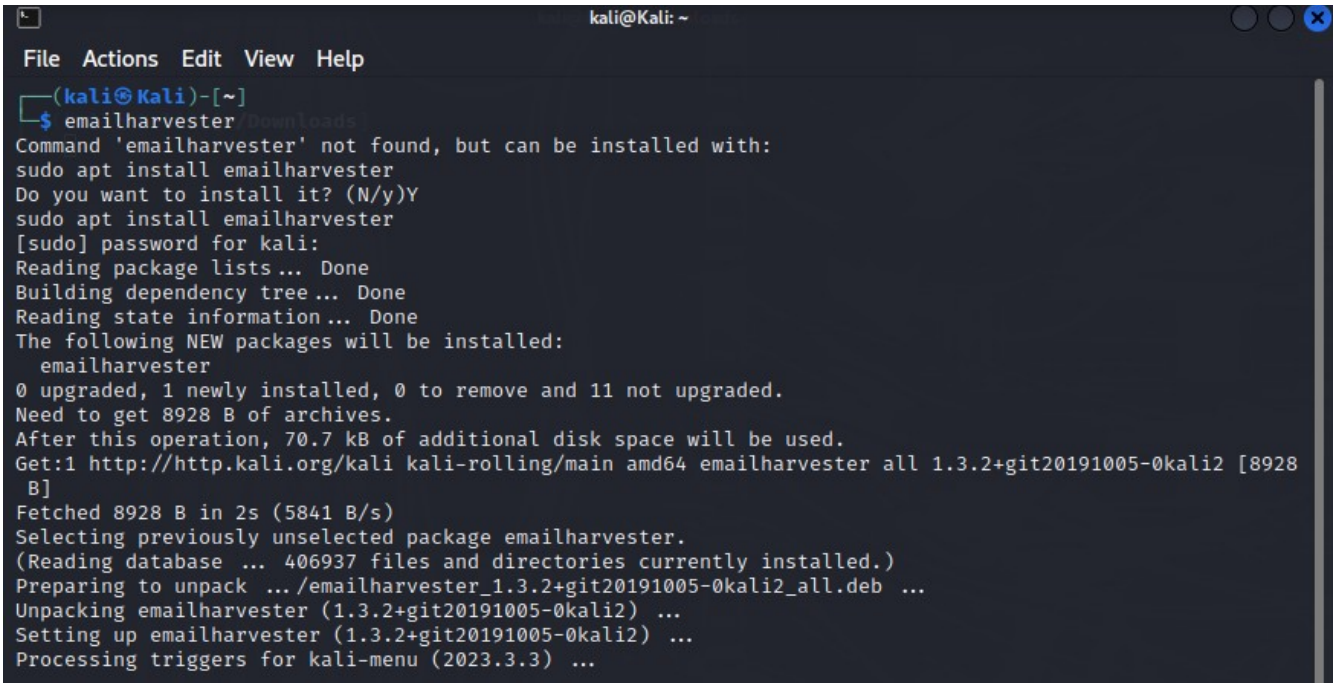
Resources exist that will allow access to these data breach files. From there, you may be able to find usernames, email addresses, passwords, and other information about employees. This information will be very useful in the exploitation part of the PenTesting process.

In my case I used haveibeenpwned.com and breachedirectory and my email has 0 data breaches

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

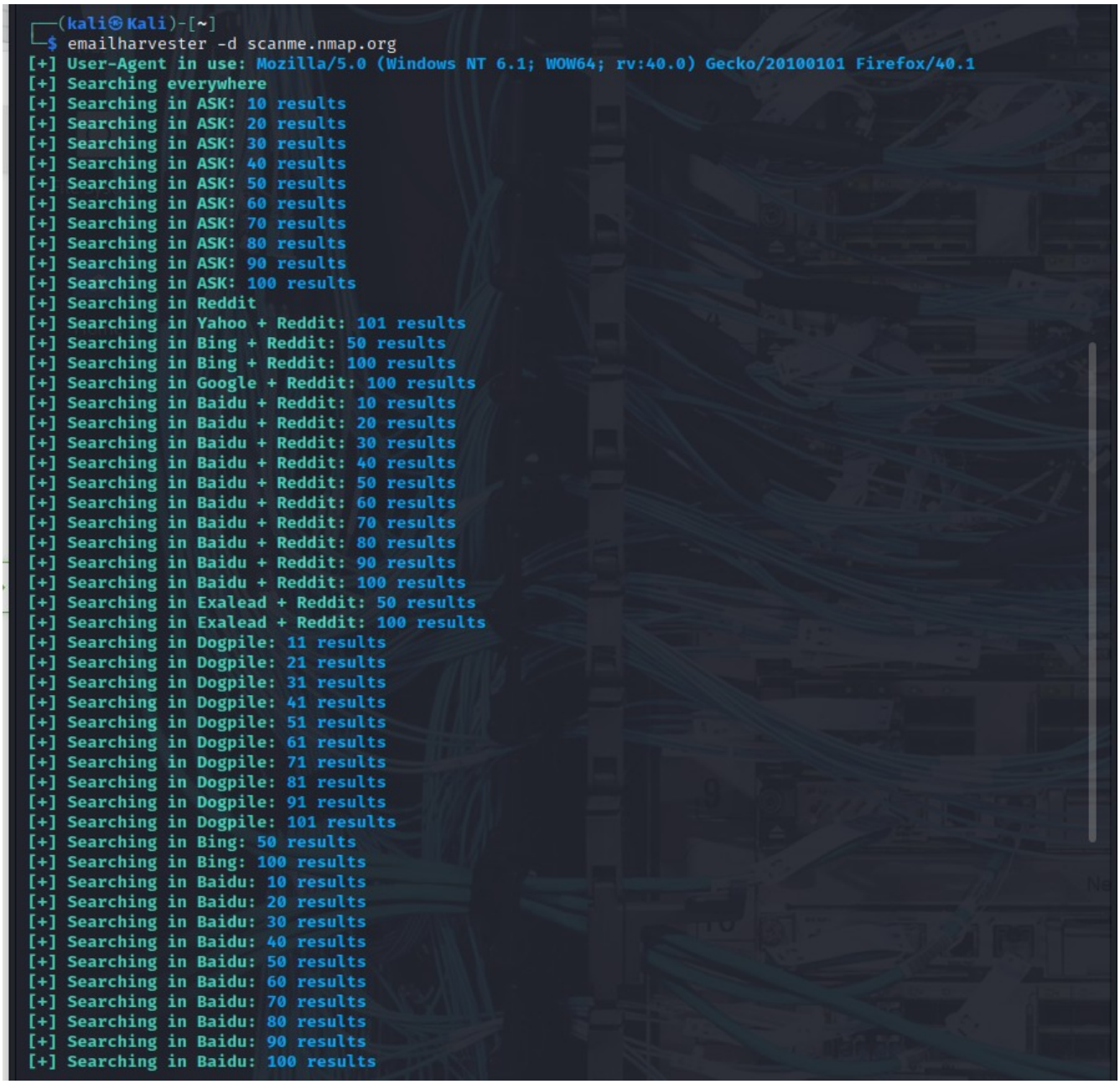
You will use a tool called **EmailHarvester** to find information about a domain, including email addresses of personnel.

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.



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

Investigate domains such as **h4cker.org**, **hackxor.net**, and **scanme.nmap.org**. You may also try other domains that you are familiar with as long as you do not violate the terms of this course. For example, use the command **emailharvester -d h4cker.org**.

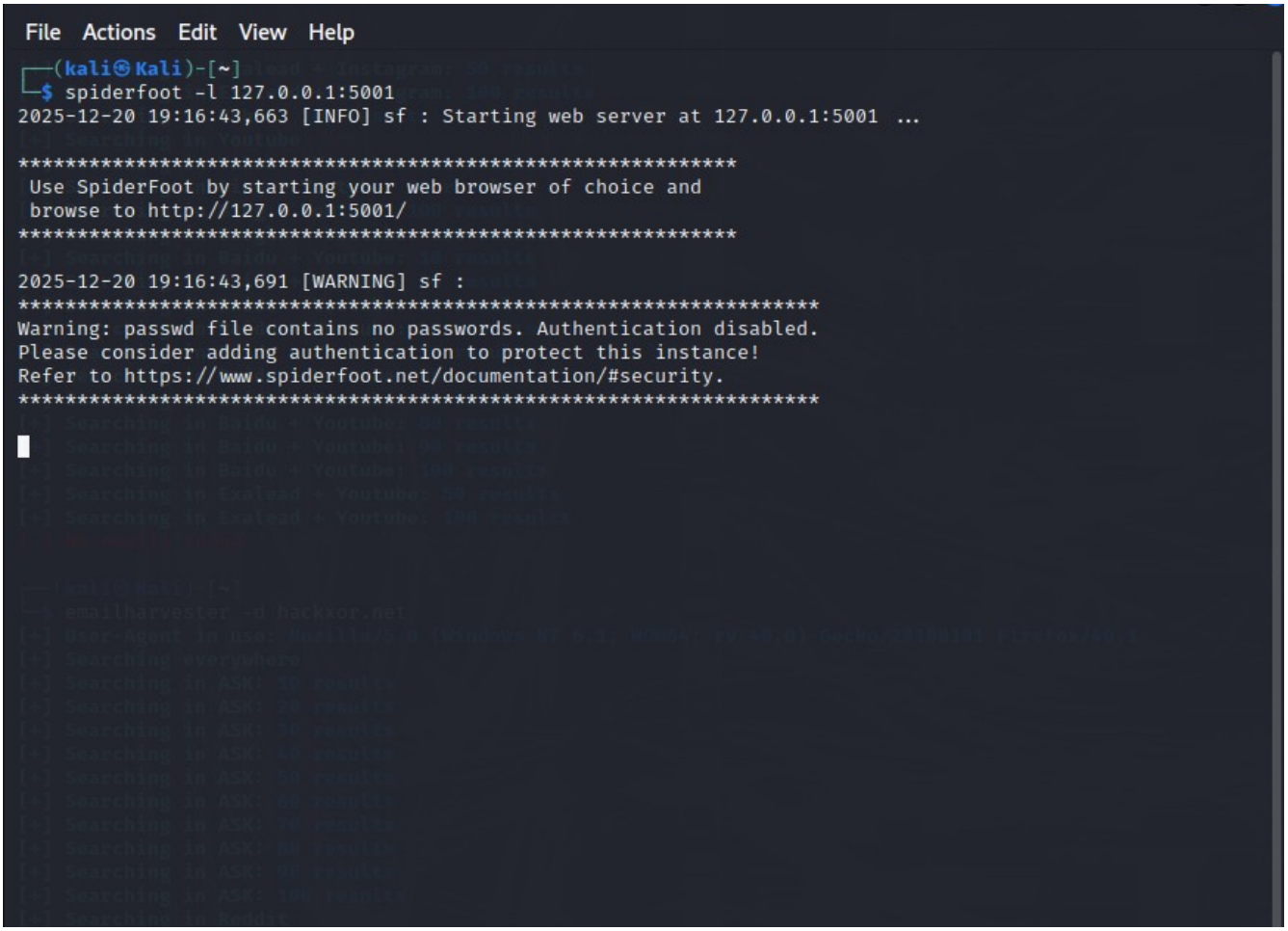


Check some of the emails addresses that you have obtained to determine if they have been part of a data breach. If so, this indicates that account details are available on the dark web. A penetration tester who has access to breach databases could search for additional information there.

Your results can be ouput 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.

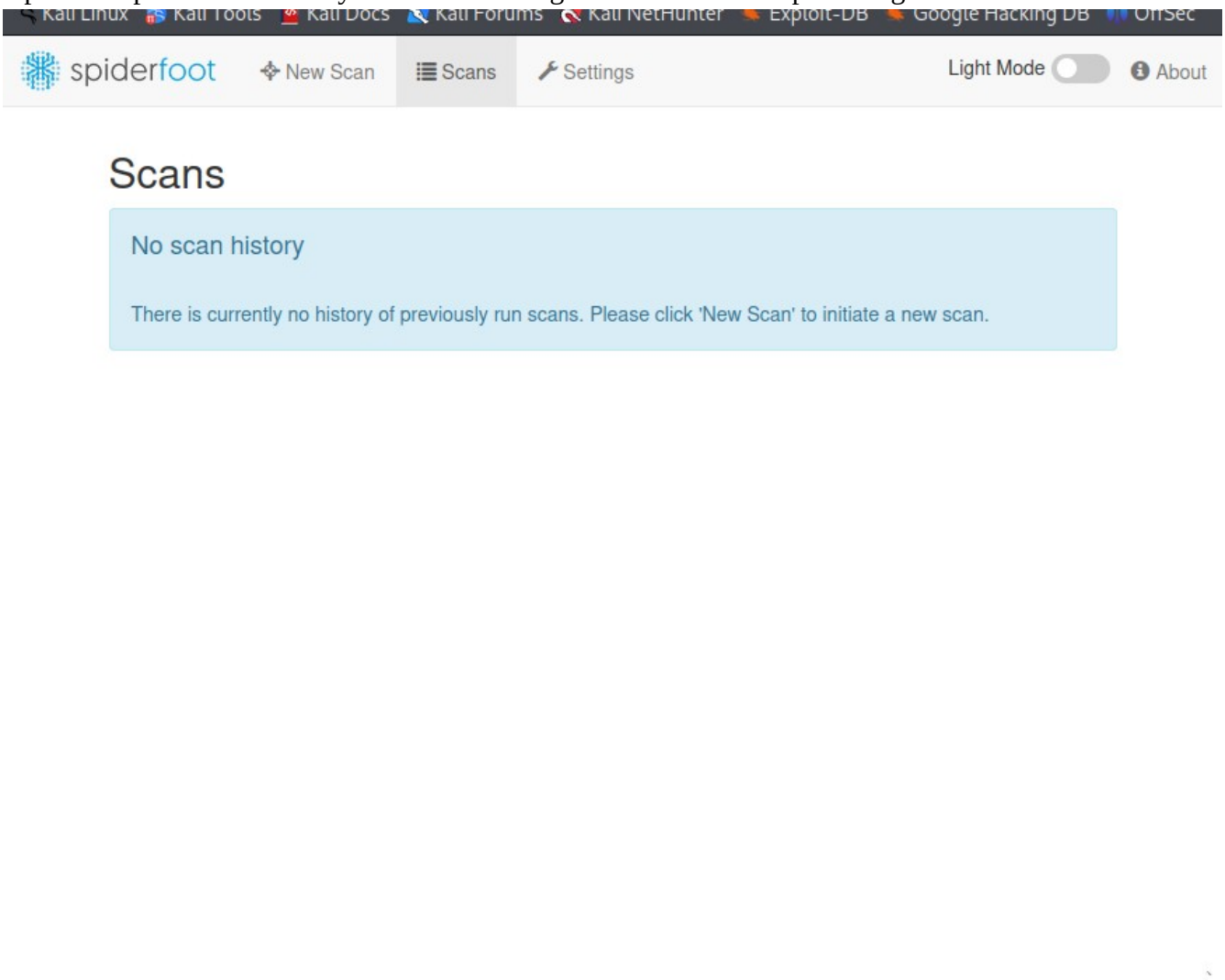
Step 3: Use Spiderfoot to research email addresses.

a. Open the Spiderfoot GUI:

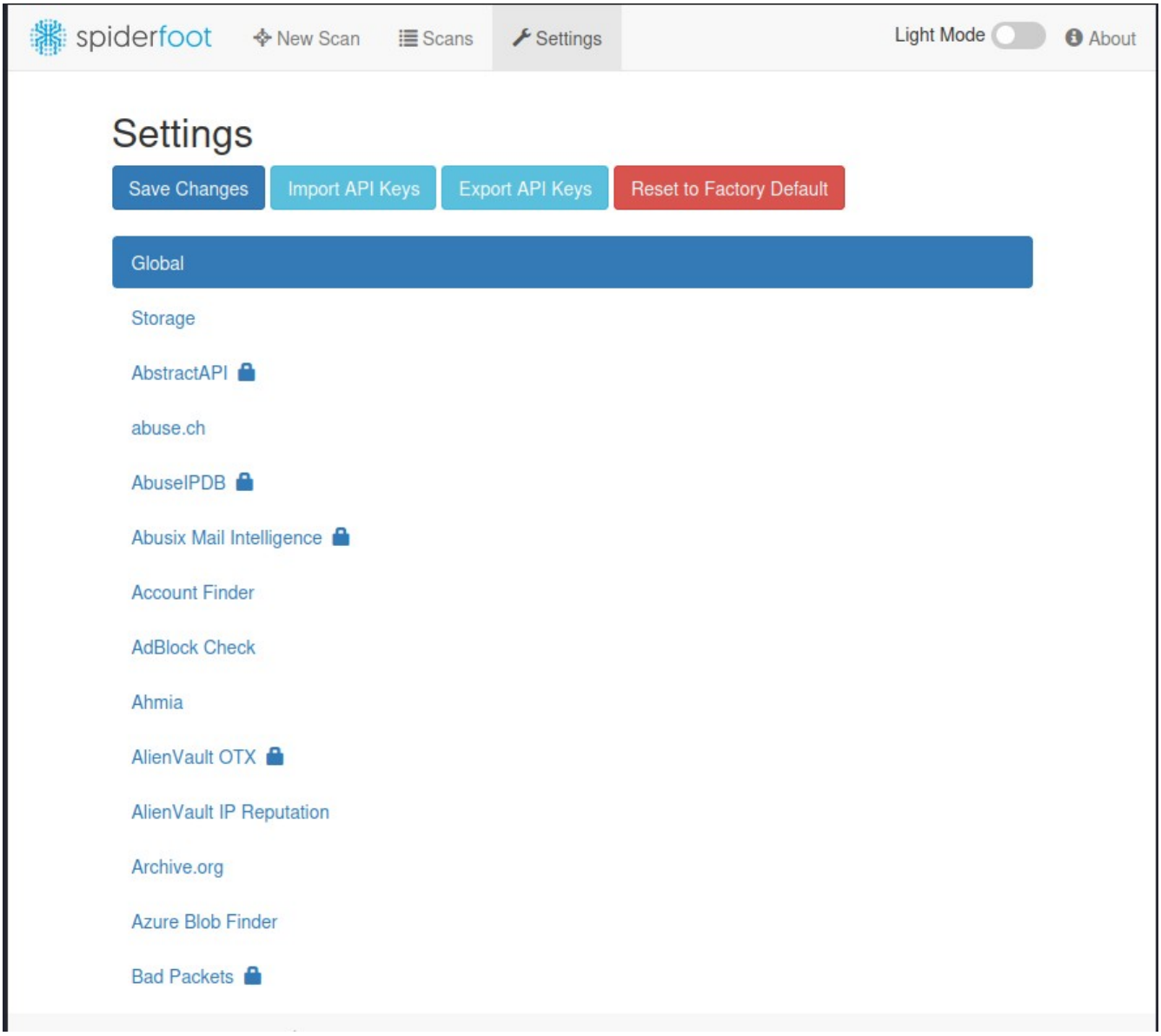


Minimize (don’t close) the terminal.

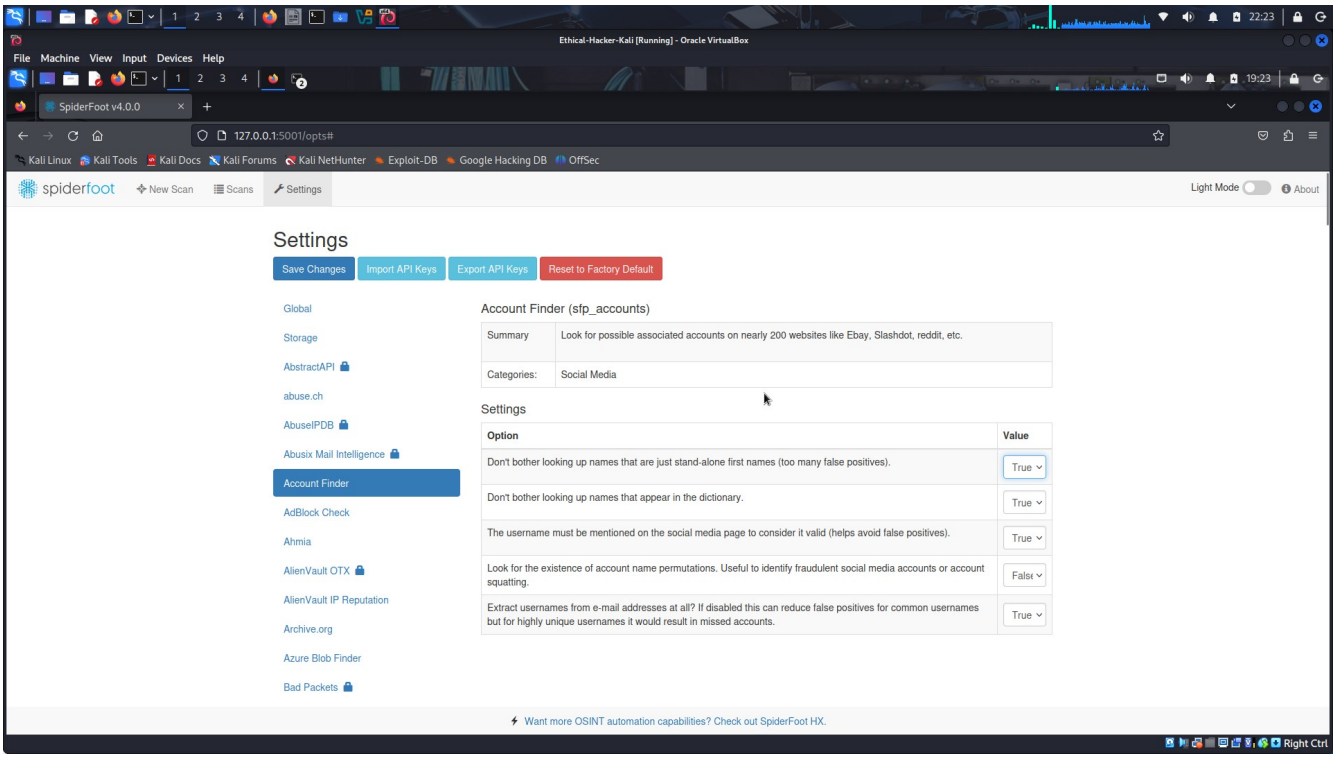
Open the Spiderfoot GUI in your browser using the IP address and port assigned above.



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


spiderfoot
New Scan
Scans
Settings
Light Mode
About
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.

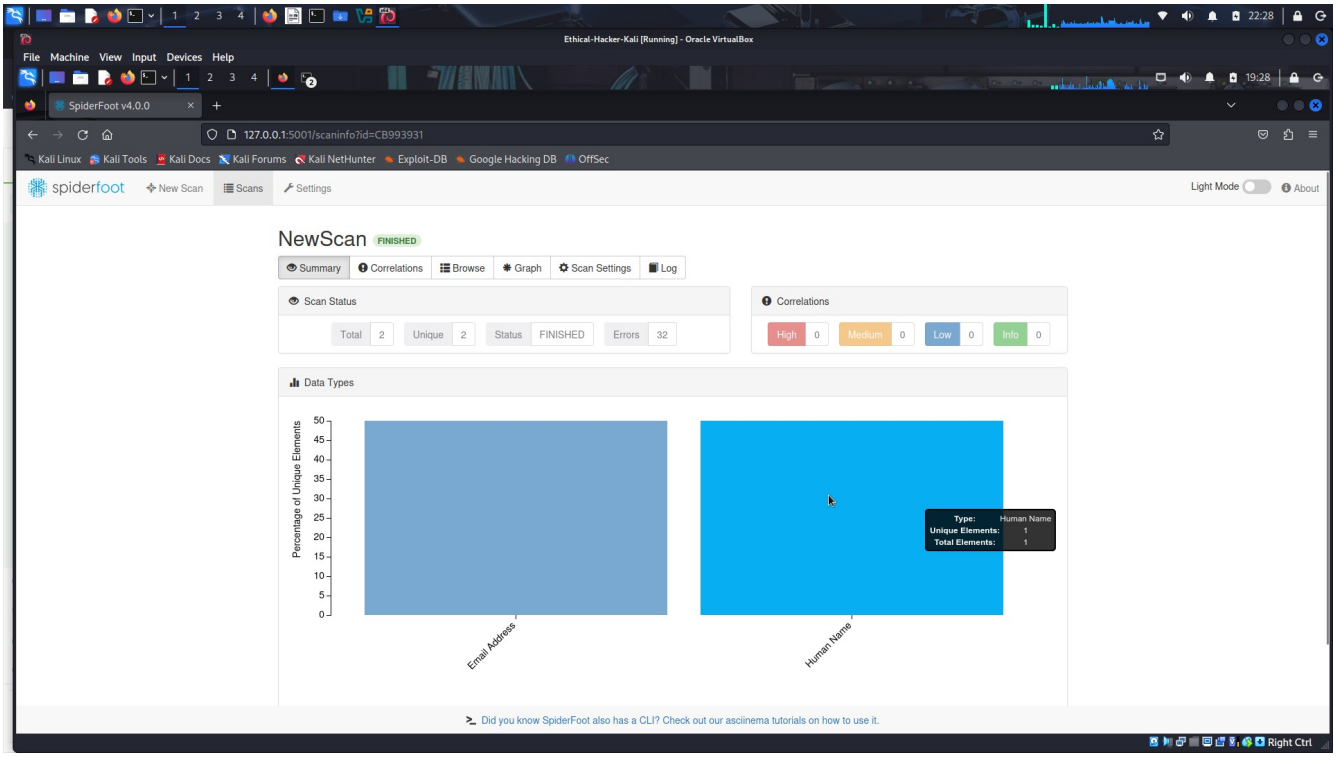
A few interesting modules are:

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.

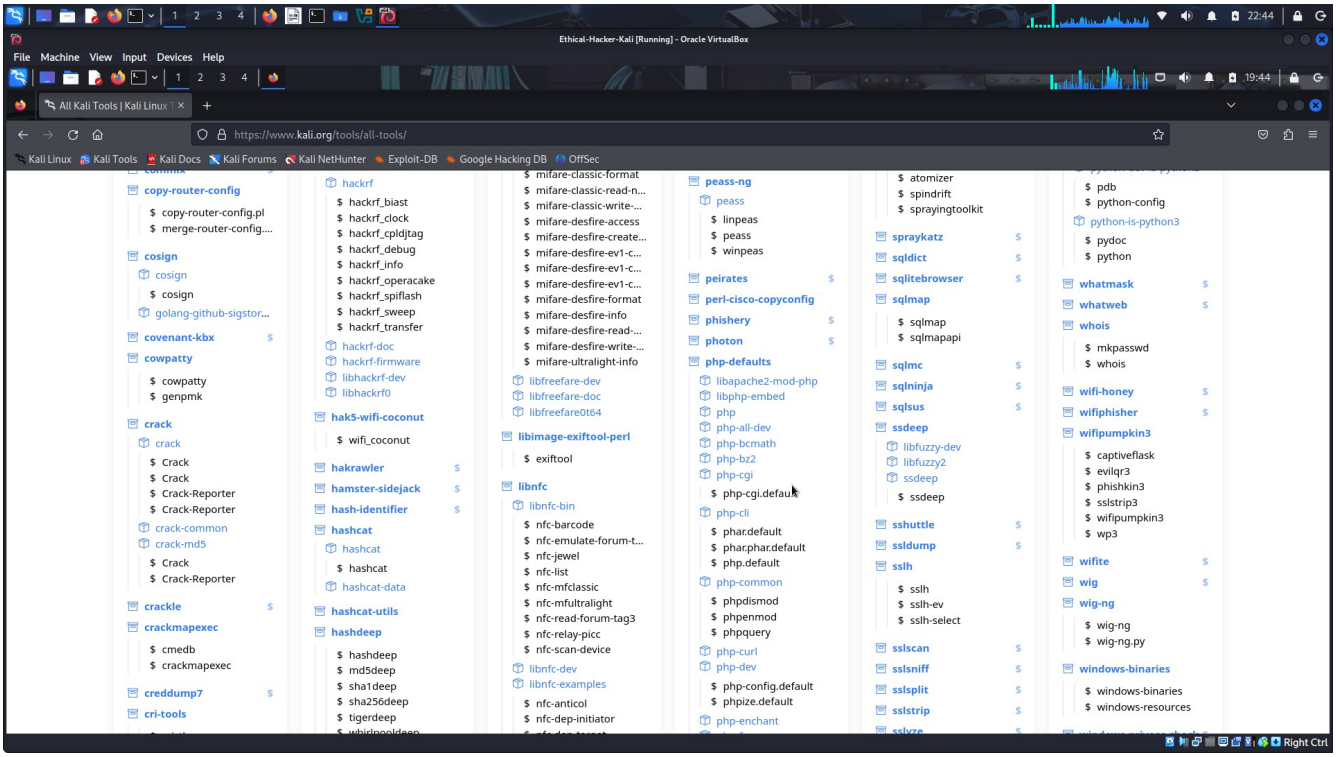
File metadata can provide hackers with insights into organizations and personnel. For example, metadata within an image file can reveal the device that was used create the image. This can reveal information that can be used to determine if the device is potentially vulnerable. Some files have metadata 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.

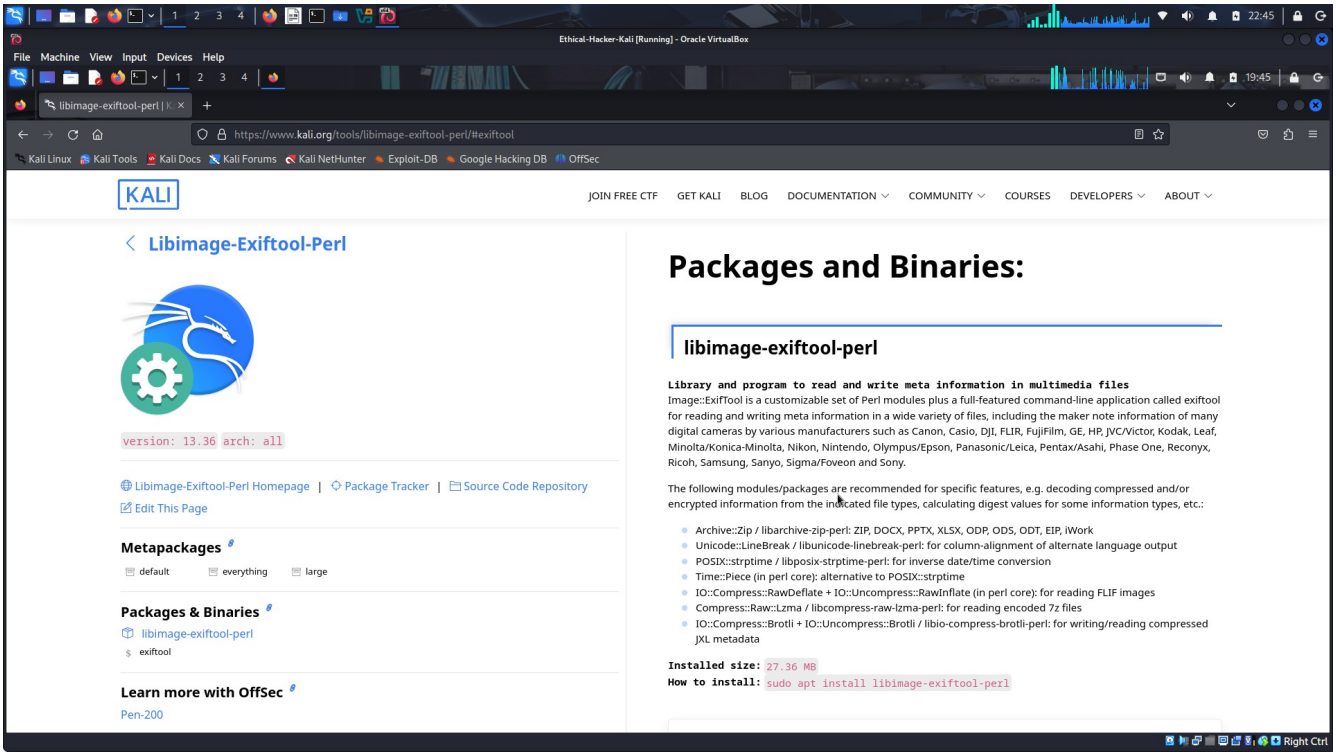
In general, files that are posted on the public internet should have their metadata stripped or at least scrutinized. You can use ExifTool, among others, to remove or edit tags from individual files or a directory of files.

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

Step 1: Install ExifTool.

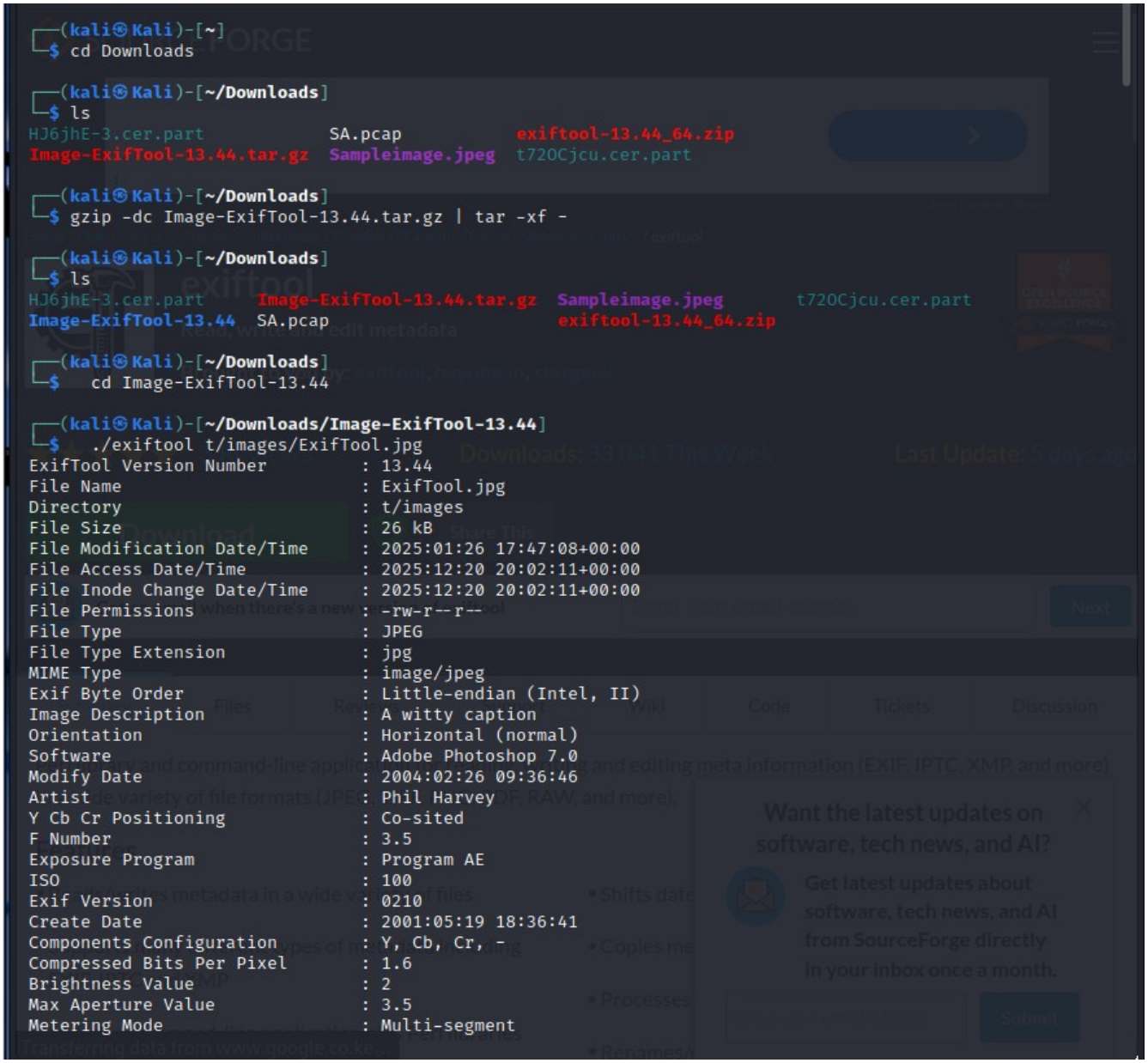
a. In Firefox, click the **Kali Tools** shortcut or navigate to https://www.kali.org/tools.
b. Select **List all tools** as necessary. Locate the entry for **libimage-exiftool-perl**.



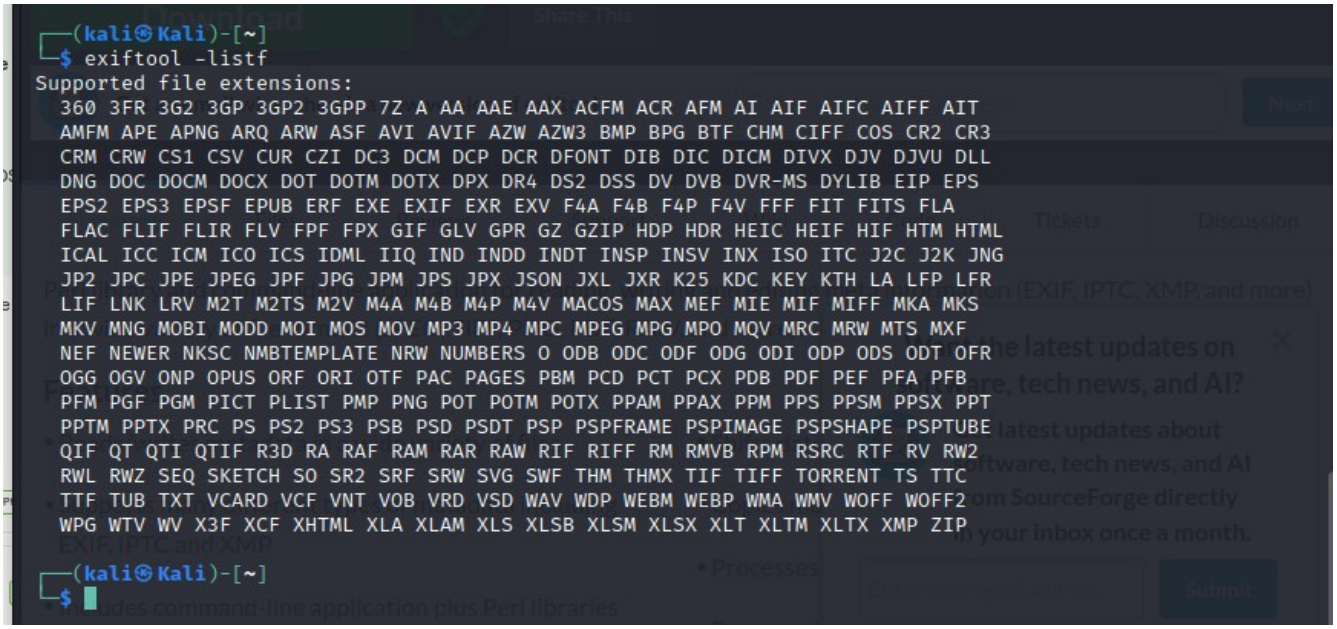


c. Follow the instructions to install ExifTool.

Download ExifTool from https://exiftool.org/



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.



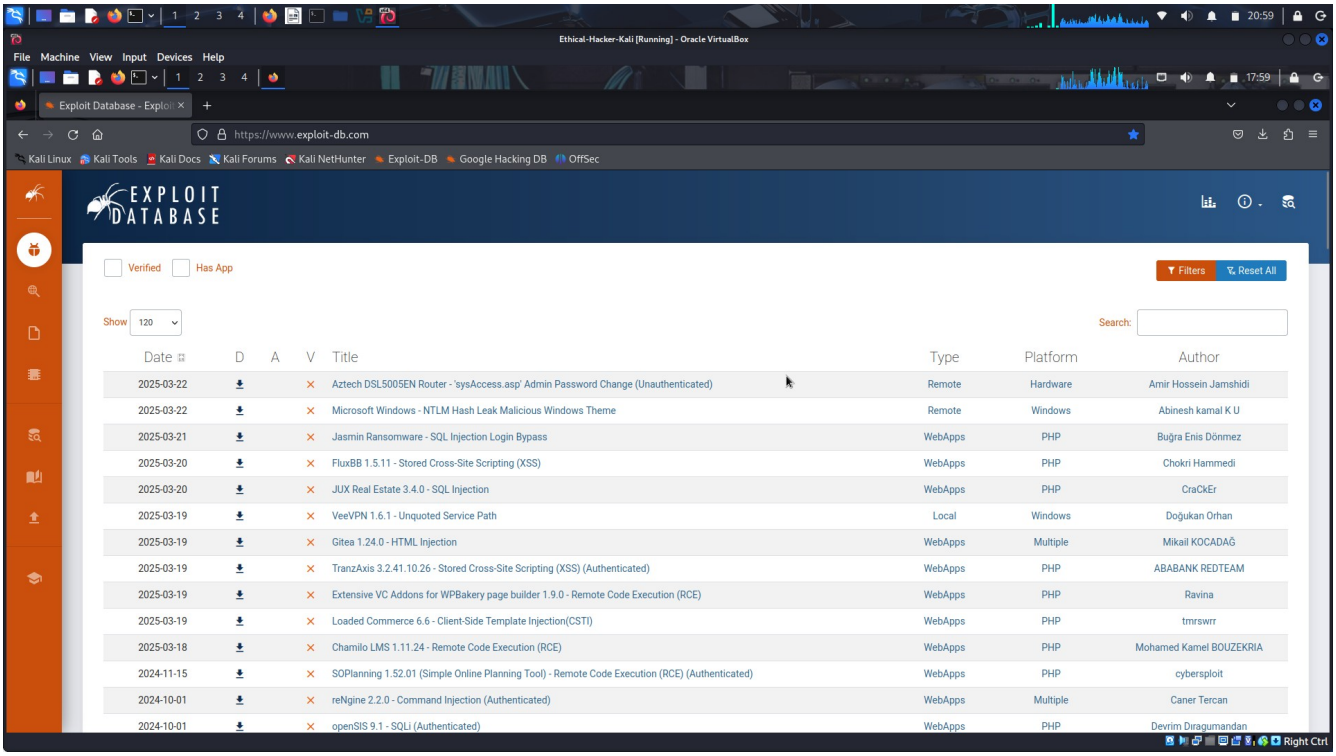
ExifTool can read metadata from a wide range of files. Review the output and complete the table with some of the common file formats that ExifTool can read by type.

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

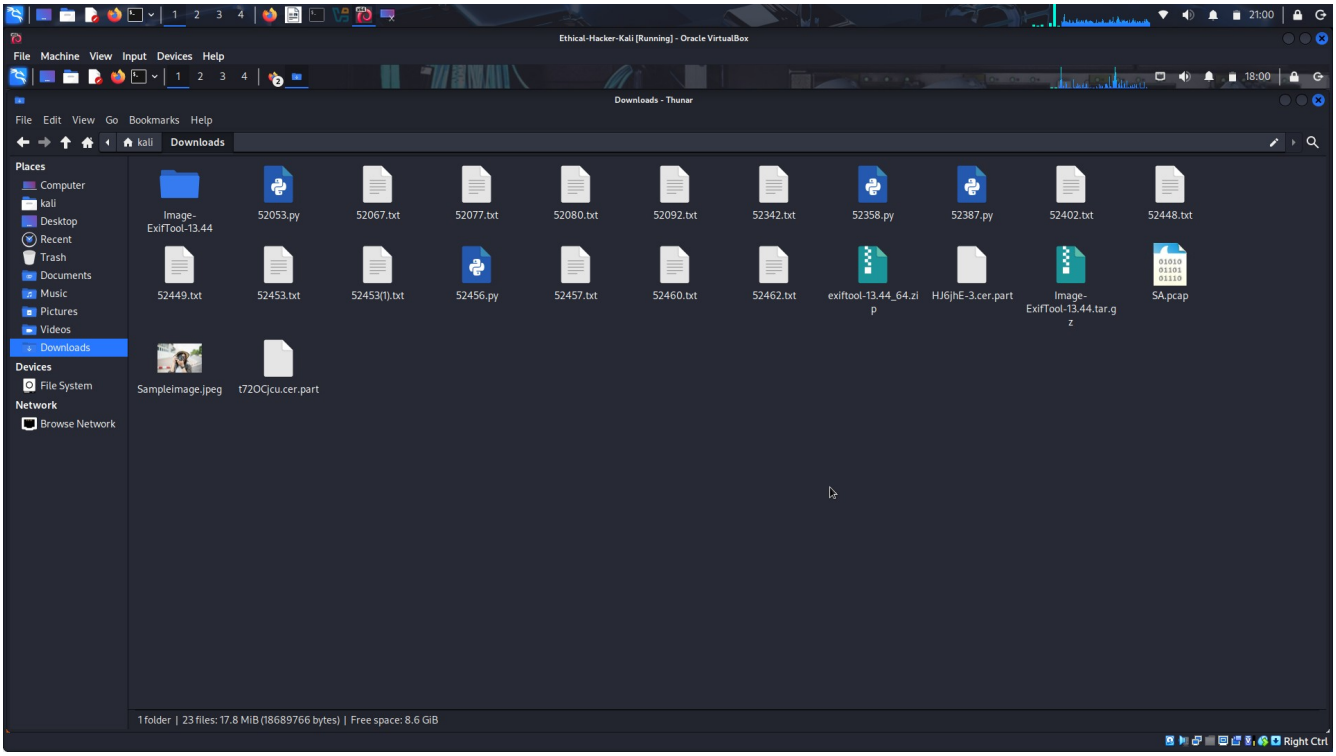
Step 2: Use ExifTool.

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.

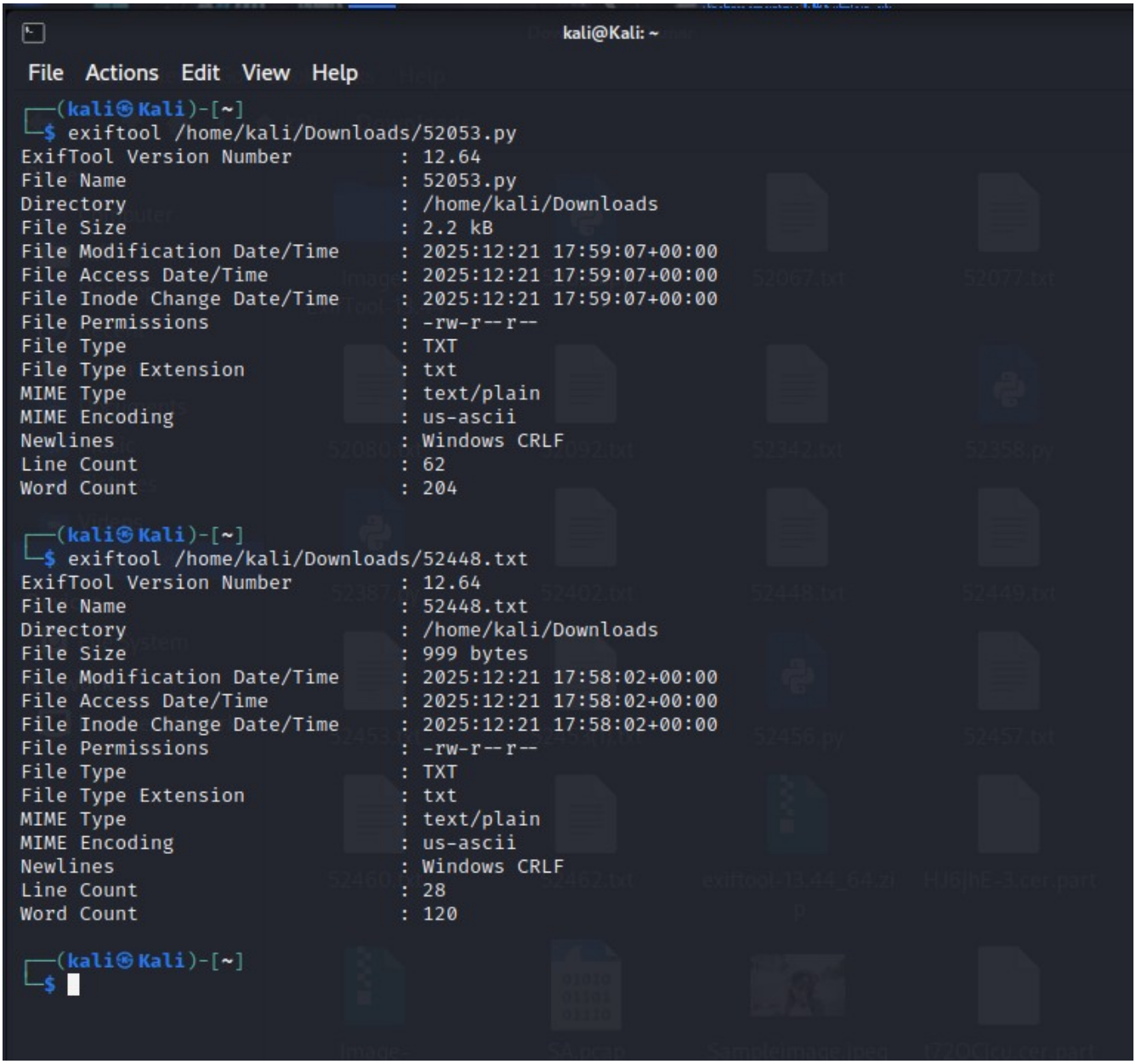
a. Go to the Google Hacker Database (GHDB). Locate dorks that will help you to find a variety of files of various types or modify the dorks that you find to do so.



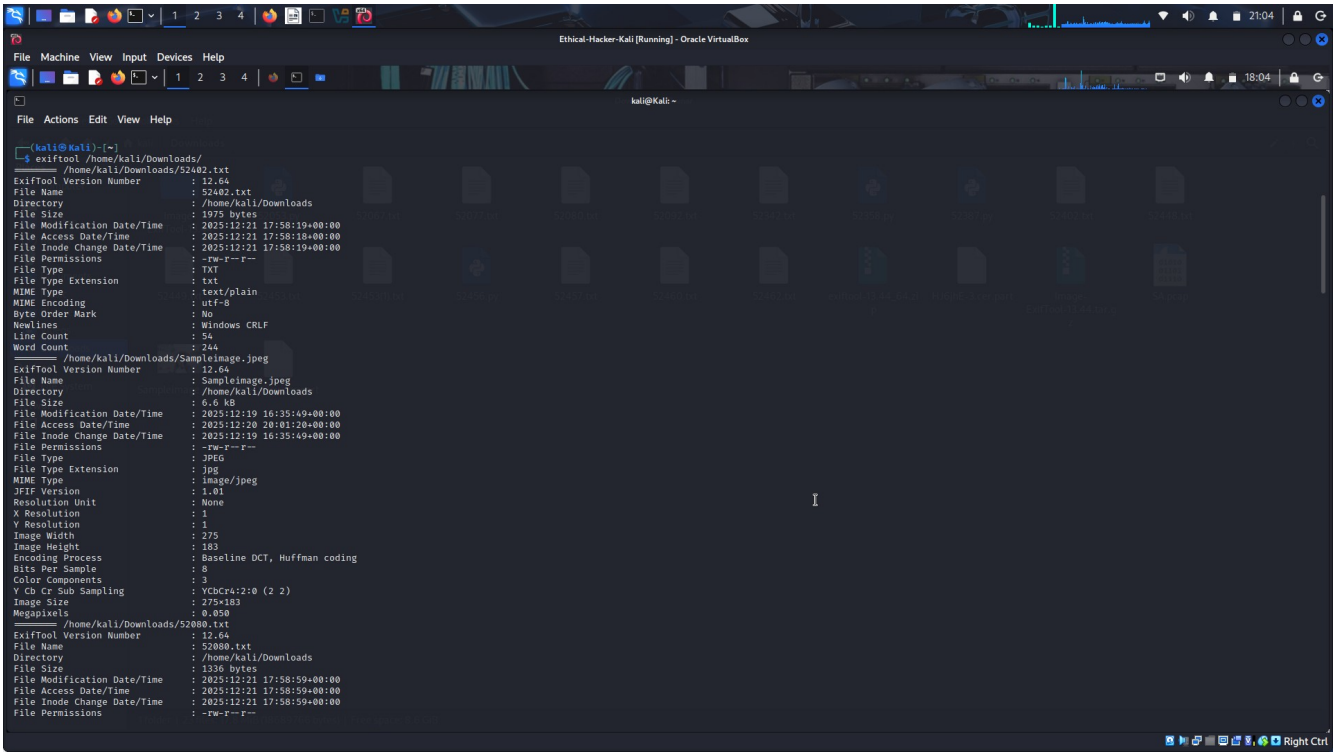
b. Download the files to your VM. Make note of the path to the folder.



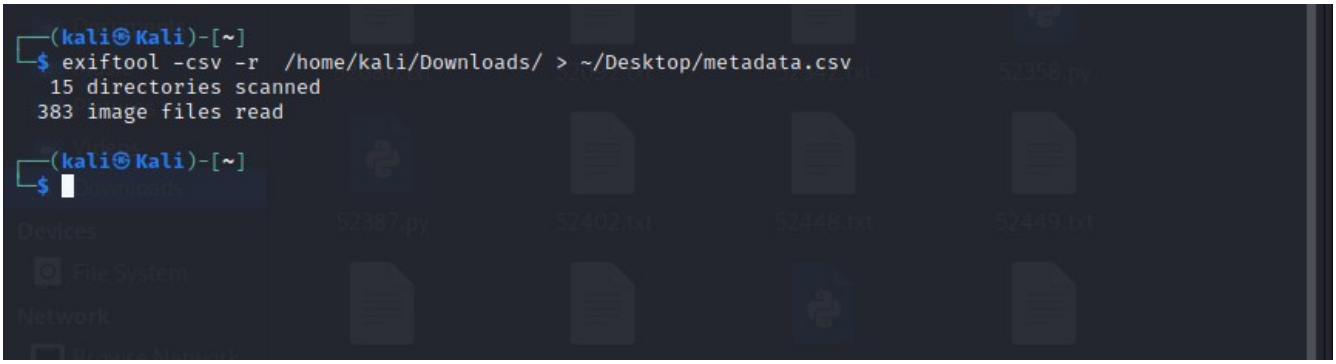
c. Experiment with ExifTools. Start by simply running the exiftool command followed by the path and file name for the target file. Review the metadata that is returned. Do this for a number of files.



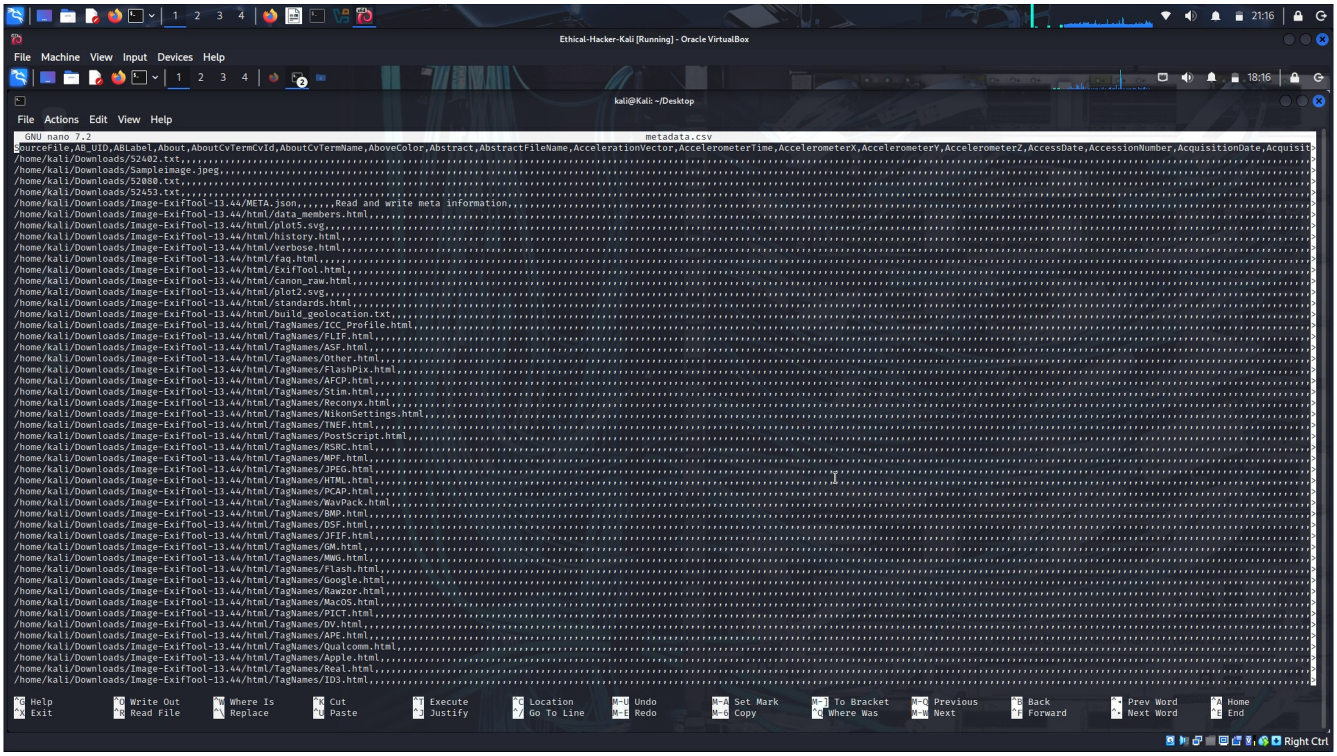
Now try running ExifTool for the entire folder. For this, you only supply the path.



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



- 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.



Ethical-Hacker-Kali [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@Kali: ~/Desktop
File Actions Edit View Help
GNU nano 7.2 metadata.csv
SourceFile,AB_UID,ABLabel,About,AboutCvTermCvId,AboutCvTermName,AboveColor,Abstract,AbstractFileName,AccelerationVector,AccelerometerTime,AccelerometerX,AccelerometerY,AccelerometerZ,AccessDate,AccessionNumber,AcquisitionDate,Acquisit
/home/kali/Downloads/52402.txt
/home/kali/Downloads/Sampleimage.jpeg
/home/kali/Downloads/52080.txt
/home/kali/Downloads/52453.txt
/home/kali/Downloads/Image-ExifTool-13.44/META.json,,,,,,Read and write meta information
/home/kali/Downloads/Image-ExifTool-13.44/html/data_members.html
/home/kali/Downloads/Image-ExifTool-13.44/html/plot5.svg
/home/kali/Downloads/Image-ExifTool-13.44/html/history.html
/home/kali/Downloads/Image-ExifTool-13.44/html/verbose.html
/home/kali/Downloads/Image-ExifTool-13.44/html/faq.html
/home/kali/Downloads/Image-ExifTool-13.44/html/ExifTool.html
/home/kali/Downloads/Image-ExifTool-13.44/html/canon_raw.html
/home/kali/Downloads/Image-ExifTool-13.44/html/plot2.svg
/home/kali/Downloads/Image-ExifTool-13.44/html/standards.html
/home/kali/Downloads/Image-ExifTool-13.44/html/build_geolocation.txt
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/ICC_Profile.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/FLIF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/ASF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Other.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/FlashPix.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/AFCP.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Stim.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Reconyx.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/NikonSettings.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/TNEF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/PostScript.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/RSRC.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/MPF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/JPEG.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/HTML.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/PCAP.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/WavPack.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/BMP.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/DSF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/JFIF.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/GM.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/MWG.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Flash.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Google.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Rawzor.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/MacOS.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/PICT.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/DV.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/APE.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Qualcomm.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Apple.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/Real.html
/home/kali/Downloads/Image-ExifTool-13.44/html/TagNames/ID3.html
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous ^B Back ^◂ Prev Word ^A Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward ^▸ Next Word ^E End
Right Ctrl