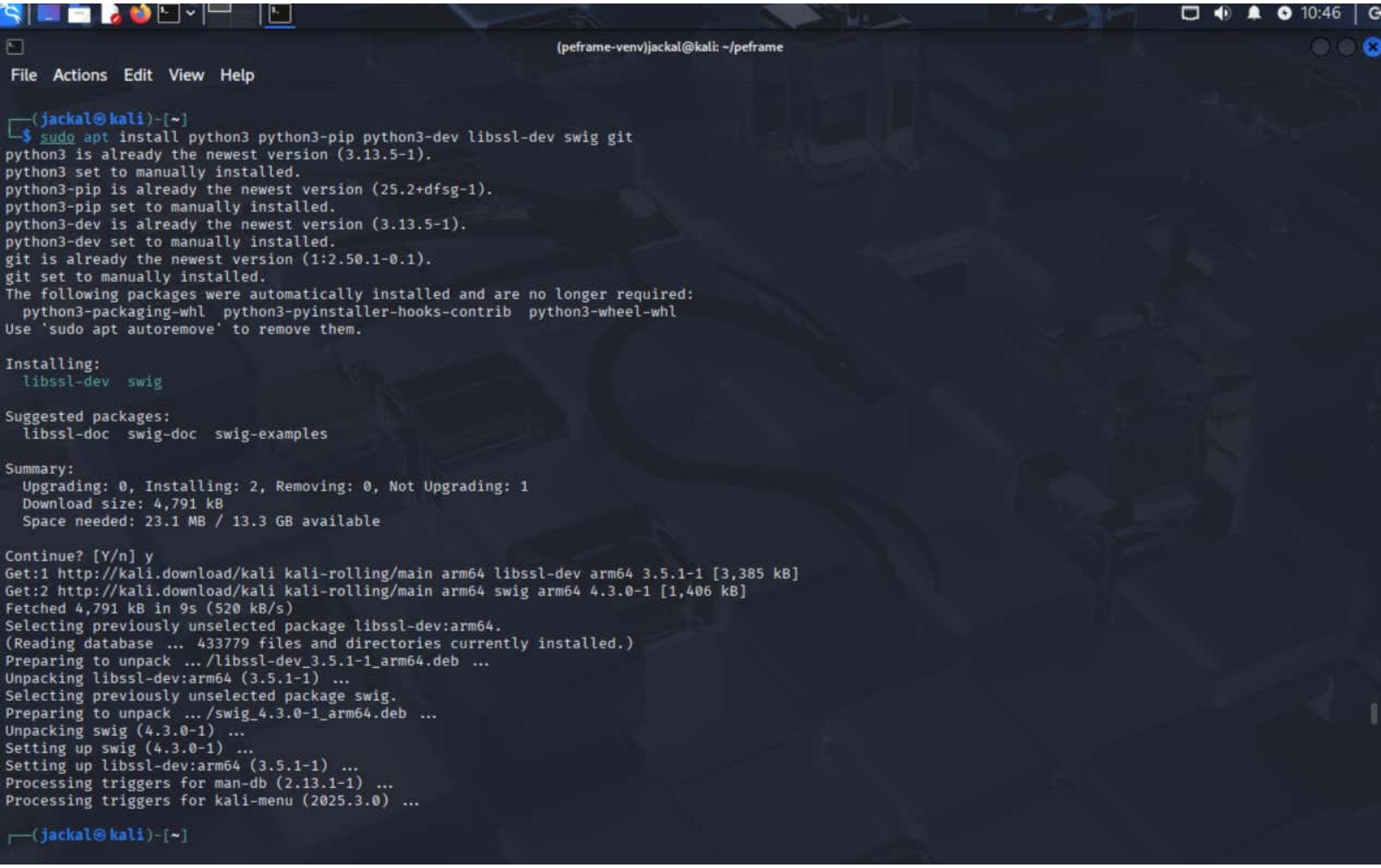
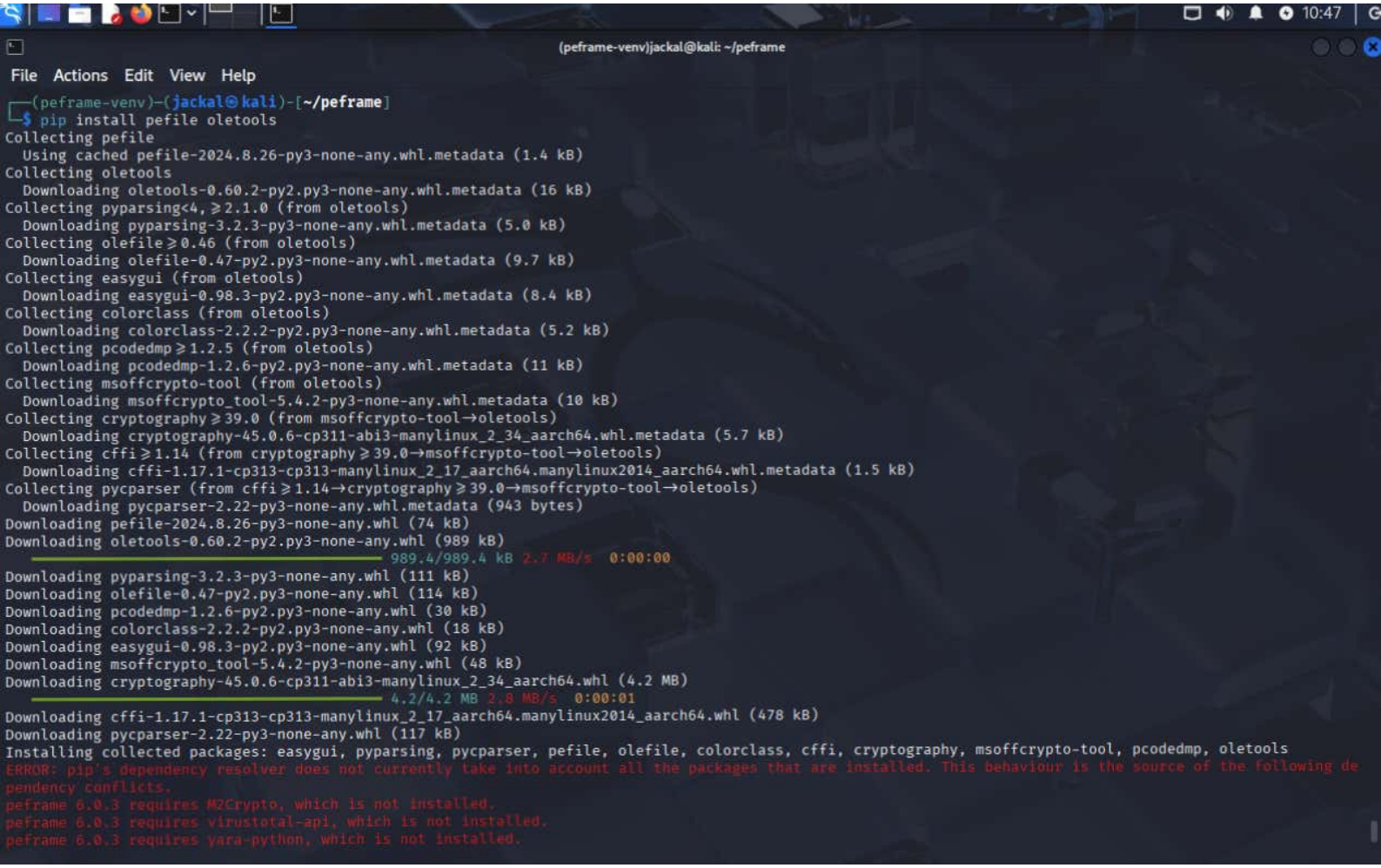
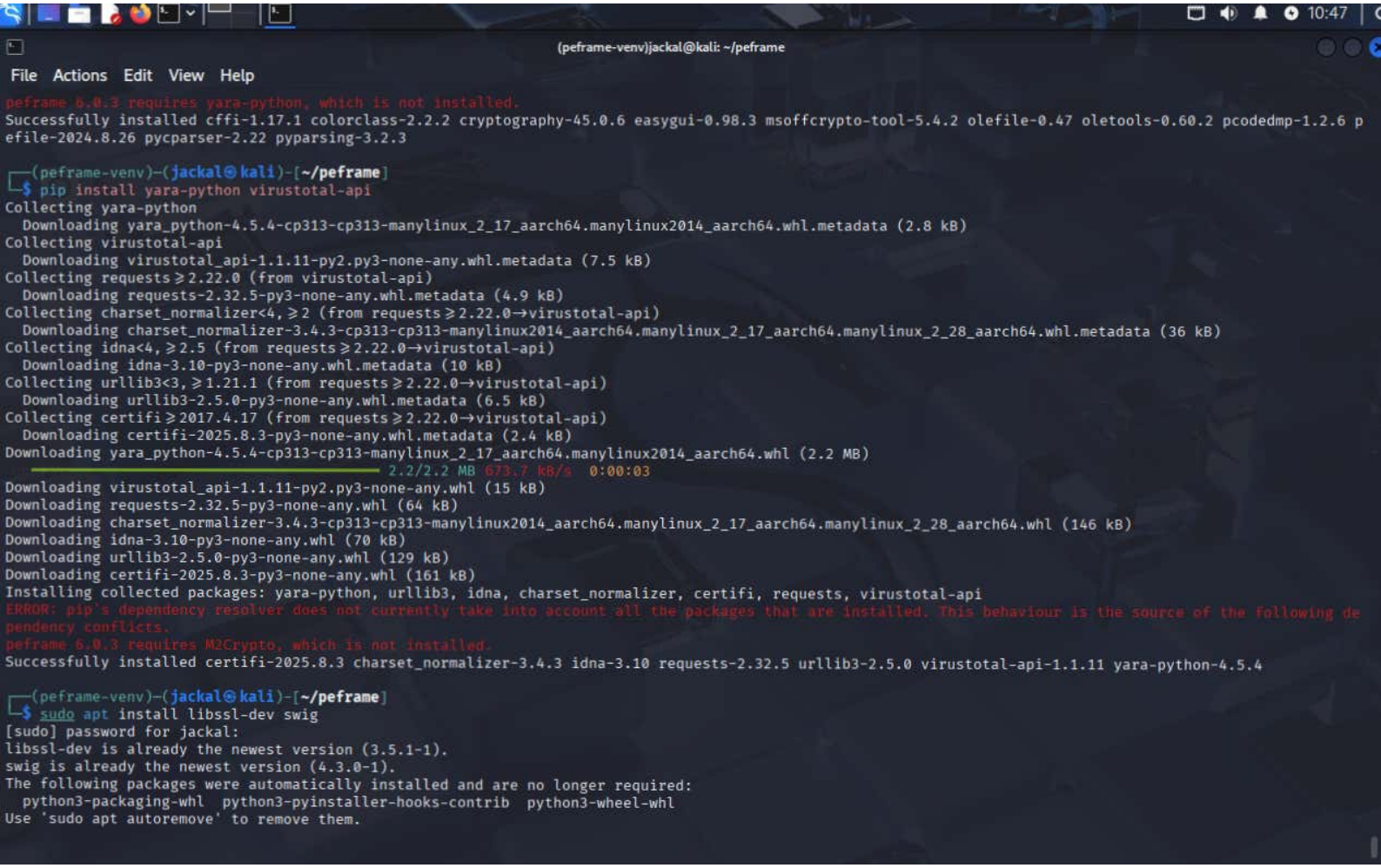
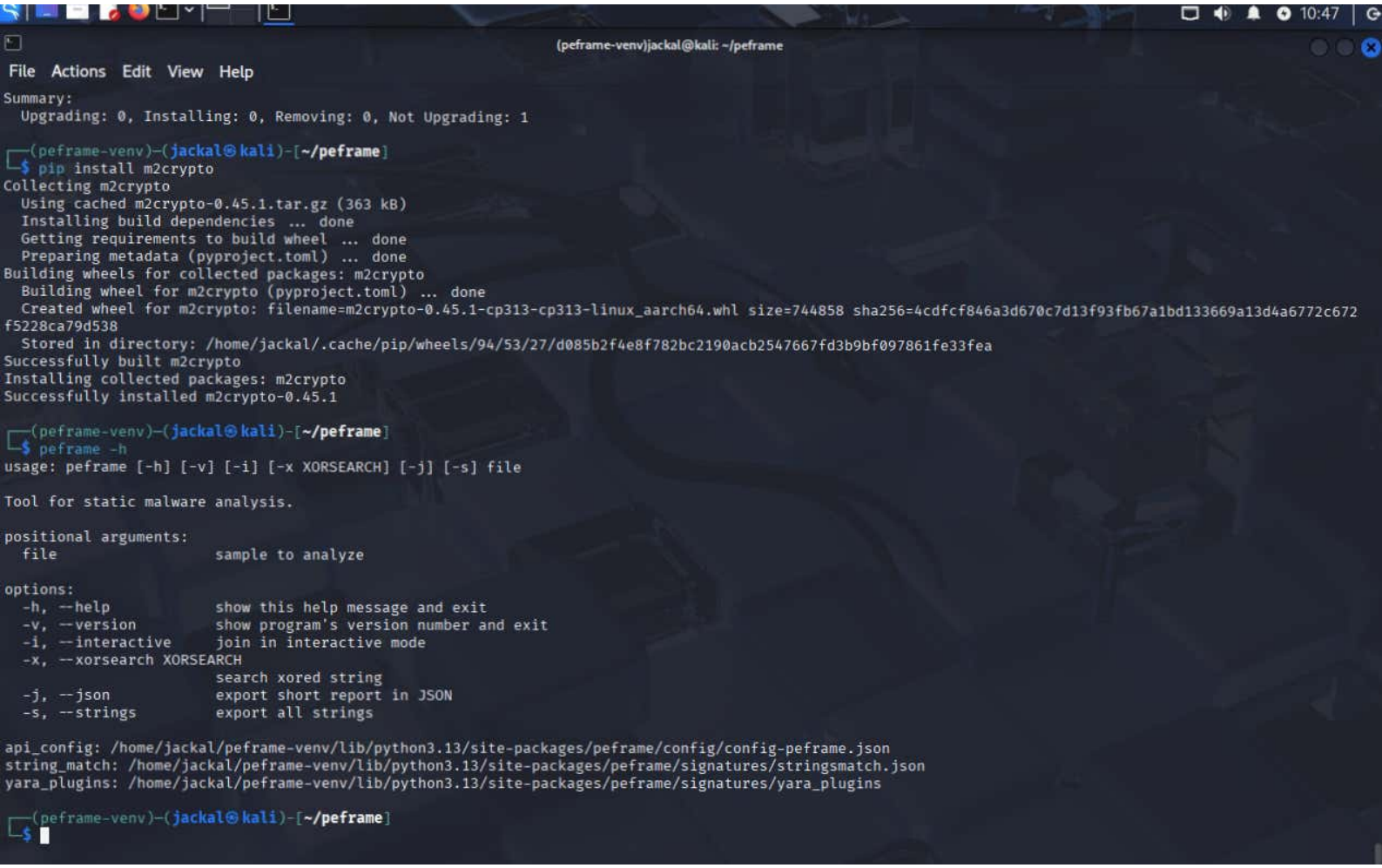
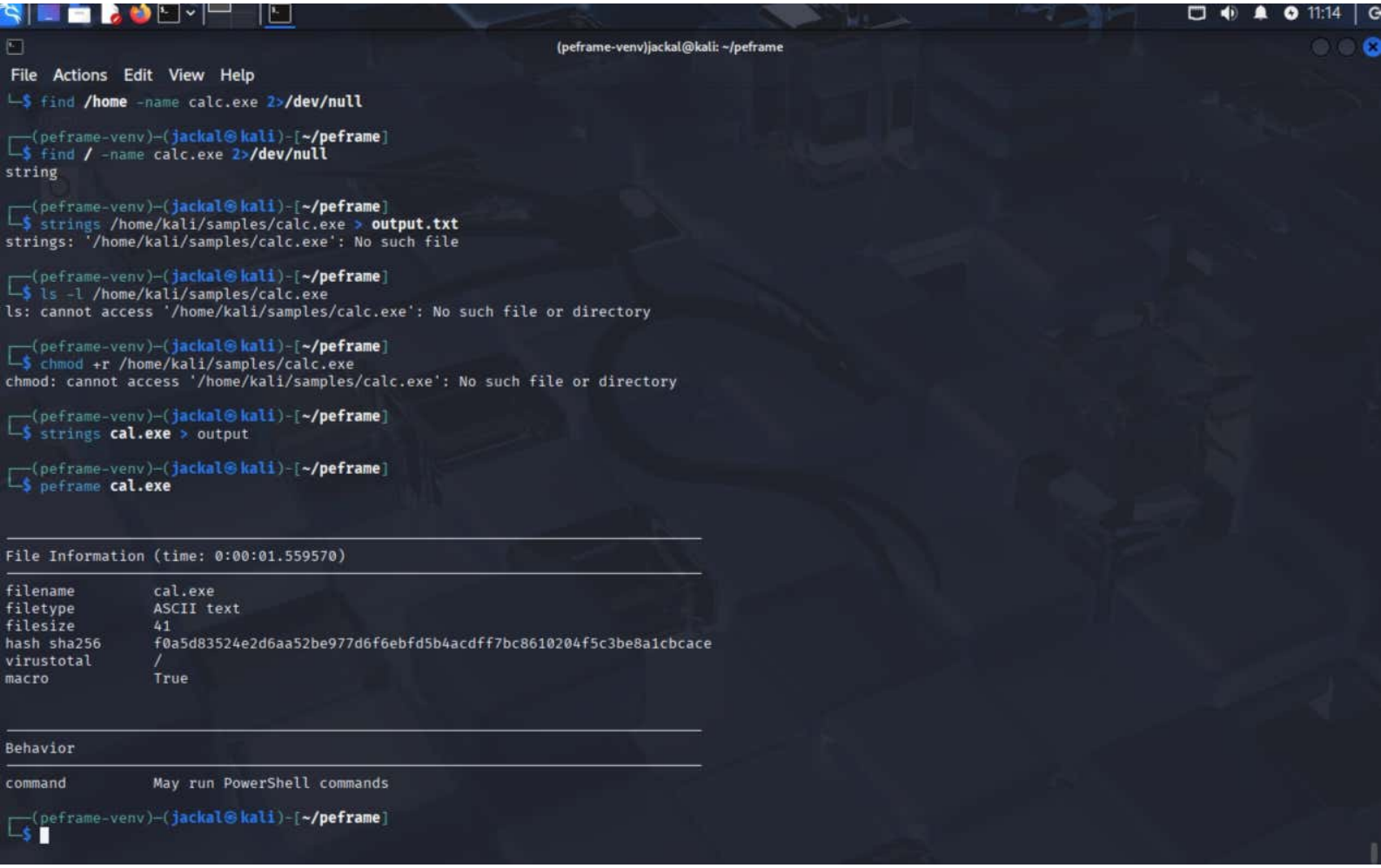

10:46
(peframe-venv)jackal@kali: ~/peframe
File Actions Edit View Help
┌──(jackal㉿kali)-[~]
└─$ sudo apt install python3 python3-pip python3-dev libssl-dev swig git
python3 is already the newest version (3.13.5-1).
python3 set to manually installed.
python3-pip is already the newest version (25.2+dfsg-1).
python3-pip set to manually installed.
python3-dev is already the newest version (3.13.5-1).
python3-dev set to manually installed.
git is already the newest version (1:2.50.1-0.1).
git set to manually installed.
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.
Installing:
libssl-dev swig
Suggested packages:
libssl-doc swig-doc swig-examples
Summary:
Upgrading: 0, Installing: 2, Removing: 0, Not Upgrading: 1
Download size: 4,791 kB
Space needed: 23.1 MB / 13.3 GB available
Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main arm64 libssl-dev arm64 3.5.1-1 [3,385 kB]
Get:2 http://kali.download/kali kali-rolling/main arm64 swig arm64 4.3.0-1 [1,406 kB]
Fetched 4,791 kB in 9s (520 kB/s)
Selecting previously unselected package libssl-dev:arm64.
(Reading database ... 433779 files and directories currently installed.)
Preparing to unpack .../libssl-dev_3.5.1-1_arm64.deb ...
Unpacking libssl-dev:arm64 (3.5.1-1) ...
Selecting previously unselected package swig.
Preparing to unpack .../swig_4.3.0-1_arm64.deb ...
Unpacking swig (4.3.0-1) ...
Setting up swig (4.3.0-1) ...
Setting up libssl-dev:arm64 (3.5.1-1) ...
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.3.0) ...
┌──(jackal㉿kali)-[~]


10:47
(peframe-venv)jackal@kali: ~/peframe
File Actions Edit View Help
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$ pip install pefile oletools
Collecting pefile
Using cached pefile-2024.8.26-py3-none-any.whl.metadata (1.4 kB)
Collecting oletools
Downloading oletools-0.60.2-py2.py3-none-any.whl.metadata (16 kB)
Collecting pyparsing<4,≥2.1.0 (from oletools)
Downloading pyparsing-3.2.3-py3-none-any.whl.metadata (5.0 kB)
Collecting olefile≥0.46 (from oletools)
Downloading olefile-0.47-py2.py3-none-any.whl.metadata (9.7 kB)
Collecting easygui (from oletools)
Downloading easygui-0.98.3-py2.py3-none-any.whl.metadata (8.4 kB)
Collecting colorclass (from oletools)
Downloading colorclass-2.2.2-py2.py3-none-any.whl.metadata (5.2 kB)
Collecting pcodedmp≥1.2.5 (from oletools)
Downloading pcodedmp-1.2.6-py2.py3-none-any.whl.metadata (11 kB)
Collecting msoffcrypto-tool (from oletools)
Downloading msoffcrypto_tool-5.4.2-py3-none-any.whl.metadata (10 kB)
Collecting cryptography≥39.0 (from msoffcrypto-tool→oletools)
Downloading cryptography-45.0.6-cp311-abi3-manylinux_2_34_aarch64.whl.metadata (5.7 kB)
Collecting cffi≥1.14 (from cryptography≥39.0→msoffcrypto-tool→oletools)
Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_aarch64.manylinux2014_aarch64.whl.metadata (1.5 kB)
Collecting pycparser (from cffi≥1.14→cryptography≥39.0→msoffcrypto-tool→oletools)
Downloading pycparser-2.22-py3-none-any.whl.metadata (943 bytes)
Downloading pefile-2024.8.26-py3-none-any.whl (74 kB)
Downloading oletools-0.60.2-py2.py3-none-any.whl (989 kB)
989.4/989.4 kB 2.7 MB/s 0:00:00
Downloading pyparsing-3.2.3-py3-none-any.whl (111 kB)
Downloading olefile-0.47-py2.py3-none-any.whl (114 kB)
Downloading pcodedmp-1.2.6-py2.py3-none-any.whl (30 kB)
Downloading colorclass-2.2.2-py2.py3-none-any.whl (18 kB)
Downloading easygui-0.98.3-py2.py3-none-any.whl (92 kB)
Downloading msoffcrypto_tool-5.4.2-py3-none-any.whl (48 kB)
Downloading cryptography-45.0.6-cp311-abi3-manylinux_2_34_aarch64.whl (4.2 MB)
4.2/4.2 MB 2.8 MB/s 0:00:01
Downloading cffi-1.17.1-cp313-cp313-manylinux_2_17_aarch64.manylinux2014_aarch64.whl (478 kB)
Downloading pycparser-2.22-py3-none-any.whl (117 kB)
Installing collected packages: easygui, pyparsing, pycparser, pefile, olefile, colorclass, cffi, cryptography, msoffcrypto-tool, pcodedmp, oletools
ERROR: pip's dependency resolver does not currently take into account all the packages that are installed. This behaviour is the source of the following de
pendency conflicts.
peframe 6.0.3 requires M2Crypto, which is not installed.
peframe 6.0.3 requires virustotal-api, which is not installed.
peframe 6.0.3 requires yara-python, which is not installed.


10:47
(peframe-venv)jackal@kali: ~/peframe
File Actions Edit View Help
peframe 6.0.3 requires yara-python, which is not installed.
Successfully installed cffi-1.17.1 colorclass-2.2.2 cryptography-45.0.6 easygui-0.98.3 msoffcrypto-tool-5.4.2 olefile-0.47 oletools-0.60.2 pcodedmp-1.2.6 pefile-2024.8.26 pycparser-2.22 pyparsing-3.2.3
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$ pip install yara-python virustotal-api
Collecting yara-python
Downloading yara_python-4.5.4-cp313-cp313-manylinux_2_17_aarch64.manylinux2014_aarch64.whl.metadata (2.8 kB)
Collecting virustotal-api
Downloading virustotal_api-1.1.11-py2.py3-none-any.whl.metadata (7.5 kB)
Collecting requests≥2.22.0 (from virustotal-api)
Downloading requests-2.32.5-py3-none-any.whl.metadata (4.9 kB)
Collecting charset_normalizer<4,≥2 (from requests≥2.22.0→virustotal-api)
Downloading charset_normalizer-3.4.3-cp313-cp313-manylinux2014_aarch64.manylinux_2_17_aarch64.manylinux_2_28_aarch64.whl.metadata (36 kB)
Collecting idna<4,≥2.5 (from requests≥2.22.0→virustotal-api)
Downloading idna-3.10-py3-none-any.whl.metadata (10 kB)
Collecting urllib3<3,≥1.21.1 (from requests≥2.22.0→virustotal-api)
Downloading urllib3-2.5.0-py3-none-any.whl.metadata (6.5 kB)
Collecting certifi≥2017.4.17 (from requests≥2.22.0→virustotal-api)
Downloading certifi-2025.8.3-py3-none-any.whl.metadata (2.4 kB)
Downloading yara_python-4.5.4-cp313-cp313-manylinux_2_17_aarch64.manylinux2014_aarch64.whl (2.2 MB)
2.2/2.2 MB 673.7 kB/s 0:00:03
Downloading virustotal_api-1.1.11-py2.py3-none-any.whl (15 kB)
Downloading requests-2.32.5-py3-none-any.whl (64 kB)
Downloading charset_normalizer-3.4.3-cp313-cp313-manylinux2014_aarch64.manylinux_2_17_aarch64.manylinux_2_28_aarch64.whl (146 kB)
Downloading idna-3.10-py3-none-any.whl (70 kB)
Downloading urllib3-2.5.0-py3-none-any.whl (129 kB)
Downloading certifi-2025.8.3-py3-none-any.whl (161 kB)
Installing collected packages: yara-python, urllib3, idna, charset_normalizer, certifi, requests, virustotal-api
ERROR: pip's dependency resolver does not currently take into account all the packages that are installed. This behaviour is the source of the following dependency conflicts.
peframe 6.0.3 requires M2Crypto, which is not installed.
Successfully installed certifi-2025.8.3 charset_normalizer-3.4.3 idna-3.10 requests-2.32.5 urllib3-2.5.0 virustotal-api-1.1.11 yara-python-4.5.4
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$ sudo apt install libssl-dev swig
[sudo] password for jackal:
libssl-dev is already the newest version (3.5.1-1).
swig is already the newest version (4.3.0-1).
The following packages were automatically installed and are no longer required:
python3-packaging-whl python3-pyinstaller-hooks-contrib python3-wheel-whl
Use 'sudo apt autoremove' to remove them.


10:47
(peframe-venv)jackal@kali: ~/peframe
File Actions Edit View Help
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$ pip install m2crypto
Collecting m2crypto
Using cached m2crypto-0.45.1.tar.gz (363 kB)
Installing build dependencies ... done
Getting requirements to build wheel ... done
Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: m2crypto
Building wheel for m2crypto (pyproject.toml) ... done
Created wheel for m2crypto: filename=m2crypto-0.45.1-cp313-cp313-linux_aarch64.whl size=744858 sha256=4cdfcf846a3d670c7d13f93fb67a1bd133669a13d4a6772c672f5228ca79d538
Stored in directory: /home/jackal/.cache/pip/wheels/94/53/27/d085b2f4e8f782bc2190acb2547667fd3b9bf097861fe33fea
Successfully built m2crypto
Installing collected packages: m2crypto
Successfully installed m2crypto-0.45.1
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$ peframe -h
usage: peframe [-h] [-v] [-i] [-x XORSEARCH] [-j] [-s] file
Tool for static malware analysis.
positional arguments:
file sample to analyze
options:
-h, --help show this help message and exit
-v, --version show program's version number and exit
-i, --interactive join in interactive mode
-x, --xorsearch XORSEARCH
search xored string
-j, --json export short report in JSON
-s, --strings export all strings
api_config: /home/jackal/peframe-venv/lib/python3.13/site-packages/peframe/config/config-peframe.json
string_match: /home/jackal/peframe-venv/lib/python3.13/site-packages/peframe/signatures/stringsmatch.json
yara_plugins: /home/jackal/peframe-venv/lib/python3.13/site-packages/peframe/signatures/yara_plugins
(peframe-venv)-(jackal㉿kali)-[~/peframe]
$


(peframe-venv)jackal@kali: ~/peframe
File Actions Edit View Help
└─$ find /home -name calc.exe 2>/dev/null
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ find / -name calc.exe 2>/dev/null
string
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ strings /home/kali/samples/calc.exe > output.txt
strings: '/home/kali/samples/calc.exe': No such file
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ ls -l /home/kali/samples/calc.exe
ls: cannot access '/home/kali/samples/calc.exe': No such file or directory
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ chmod +r /home/kali/samples/calc.exe
chmod: cannot access '/home/kali/samples/calc.exe': No such file or directory
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ strings cal.exe > output
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$ peframe cal.exe
File Information (time: 0:00:01.559570)
filename cal.exe
filetype ASCII text
filesize 41
hash sha256 f0a5d83524e2d6aa52be977d6f6ebfd5b4acdff7bc8610204f5c3be8a1cbcace
virustotal /
macro True
Behavior
command May run PowerShell commands
┌──(peframe-venv)─(jackal㉿kali)-[~/peframe]
└─$