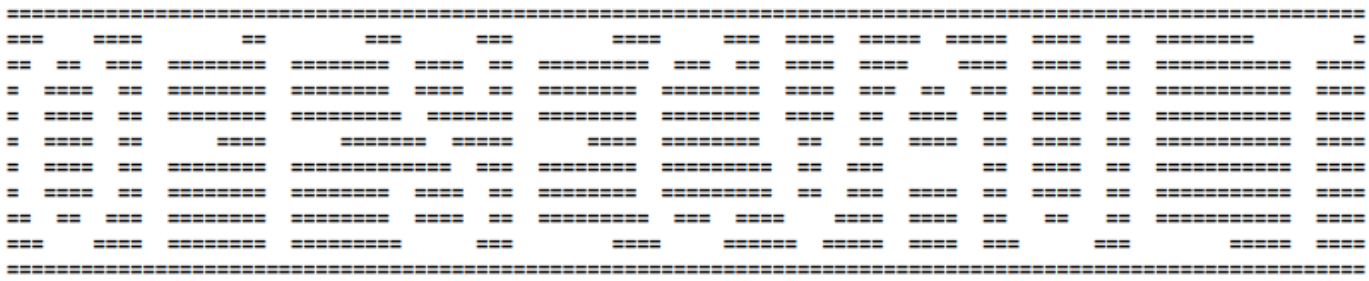
Punbup | how to install



offsecvault - Since 2021

Is a python script to "unbup" similar to decrypt McAfee .bup (backup files) files normally obtained during malware investigations were the McAfee EPO is involved.

For this post we are using the following specs:

```
-Ubuntu 20.04 Focal Fossa (updated)

-Python 2.7 [pre-installed Python 3.8.5]

-punbup.py
```

[current scenario i found]

```
_1: get the punbup script & unzip the file
```

remnux@remnux-VM:/home/mcafee_alerts$ wget
https://github.com/herrcore/punbup/archive/refs/heads/master.zip

remnux@remnux-VM:/home/mcafee_alerts$ unzip punbup-master.zip

```
_2: move to the new folder created and inspect the content
```

remnux@remnux-VM:/home/mcafee_alerts$ cd punbup-master/
remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ ls
LICENSE punbup.py README.md setup.py

```
_3: check current python version
```

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ python3 -V
Python 3.8.5

So far the python version installed is 3.8.5, If you run the punbup.py script with python3 it will not work. (for now) it shows an error related to the script itself. Running the script with python2.7 works better.

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ sudo python3 punbup.py -h
File "punbup.py", line 27
print 'Warning: The "%s" stream reports a size of 0. Possibly a corrupt bup.' % fname[0]
^
SyntaxError: Missing parentheses in call to 'print'. Did you mean print('Warning: The "%s" stream reports a size of 0. Possibly a corrupt bup.' % fname[0])?

`_4: run the script to get the help menu (using python2.7)`

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ python2.7 punbup.py --h

Command 'python2.7' not found, but can be installed with:

sudo apt install python2.7

Looks like the python version 2.7 is not installed, next step: install

`_5: install python version 2.7`

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ sudo apt install python2.7
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libfprint-2-tod1 libllvm10
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libpython2.7-minimal libpython2.7-stdlib python2.7-minimal
Suggested packages:
python2.7-doc binfmt-support
The following NEW packages will be installed:
libpython2.7-minimal libpython2.7-stdlib python2.7 python2.7-minimal
0 upgraded, 4 newly installed, 0 to remove and 20 not upgraded.
Need to get 3,755 kB of archives.
After this operation, 16.2 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libpython2.7-minimal amd64 2.7.18-1~20.04.1 [335 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python2.7-minimal amd64 2.7.18-1~20.04.1 [1,285 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 libpython2.7-stdlib amd64 2.7.18-1~20.04.1 [1,887 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python2.7 amd64 2.7.18-1~20.04.1 [248 kB]
Fetched 3,755 kB in 1s (2,553 kB/s)

Selecting previously unselected package libpython2.7-minimal:amd64.
(Reading database ... 166927 files and directories currently installed.)
Preparing to unpack .../libpython2.7-minimal_2.7.18-1~20.04.1_amd64.deb ...
Unpacking libpython2.7-minimal:amd64 (2.7.18-1~20.04.1) ...
Selecting previously unselected package python2.7-minimal.
Preparing to unpack .../python2.7-minimal_2.7.18-1~20.04.1_amd64.deb ...
Unpacking python2.7-minimal (2.7.18-1~20.04.1) ...
Selecting previously unselected package libpython2.7-stdlib:amd64.
Preparing to unpack .../libpython2.7-stdlib_2.7.18-1~20.04.1_amd64.deb ...
Unpacking libpython2.7-stdlib:amd64 (2.7.18-1~20.04.1) ...
Selecting previously unselected package python2.7.
Preparing to unpack .../python2.7_2.7.18-1~20.04.1_amd64.deb ...
Unpacking python2.7 (2.7.18-1~20.04.1) ...
Setting up libpython2.7-minimal:amd64 (2.7.18-1~20.04.1) ...
Setting up python2.7-minimal (2.7.18-1~20.04.1) ...
Linking and byte-compiling packages for runtime python2.7...
Setting up libpython2.7-stdlib:amd64 (2.7.18-1~20.04.1) ...
Setting up python2.7 (2.7.18-1~20.04.1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...

Now that python2.7 was installed, let's run the script once again,

`_6: run the punbup.py script with python2.7 to get the help menu`

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ python2.7 punbup.py --h
Error - Please ensure you install the olefile library before running this script (https://github.com/decalage2/olefile): No module named olefile

Note: The specific requirement for this script to successfully run is the "olefile". You have two options to install it on your ubuntu/linux. [pip command / manually]

`_7: update and install the olefile using "pip" command`

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ pip install olefile
Requirement already satisfied: olefile in /usr/lib/python3/dist-packages (0.46)

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ pip install -U olefile
Requirement already up-to-date: olefile in /usr/lib/python3/dist-packages (0.46)

`_8: install the olefile manually`

`_8.1: create folder & move to the folder`

```
remnux@remnux-VM:/home/mcafee_alerts$ sudo mkdir olefile
remnux@remnux-VM:/home/mcafee_alerts$ cd olefile/
remnux@remnux-VM:/home/mcafee_alerts/olefile$
```

_8.2: download the olefile

```
remnux@remnux-VM:/home/mcafee_alerts/olefile$ sudo wget
https://github.com/decalage2/olefile/archive/master.zip
--2021-06-18 03:19:45-- https://github.com/decalage2/olefile/archive/master.zip
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://codeload.github.com/decalage2/olefile/zip/master [following]
--2021-06-18 03:19:45-- https://codeload.github.com/decalage2/olefile/zip/master
Resolving codeload.github.com (codeload.github.com)... 140.82.113.9
Connecting to codeload.github.com (codeload.github.com)|140.82.113.9|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/zip]
Saving to: ‘master.zip’

master.zip [ <=> ] 107.67K 416KB/s in 0.3s

2021-06-18 03:19:46 (416 KB/s) - ‘master.zip’ saved [110249]
```

_8.3: confirm the file was downloaded & unzip the file

```
remnux@remnux-VM:/home/mcafee_alerts/olefile$ ls -l
total 108
-rw-r--r-- 1 root root 110249 Jun 18 03:19 master.zip

remnux@remnux-VM:/home/mcafee_alerts/olefile$ sudo unzip master.zip
Archive: master.zip
375a2d782bb75f11dfb6e15b08fe38f93ca507a8
creating: olefile-master/
inflating: olefile-master/.coveragerc
inflating: olefile-master/.editorconfig
creating: olefile-master/.github/
creating: olefile-master/.github/ISSUE_TEMPLATE/
inflating: olefile-master/.github/ISSUE_TEMPLATE/bug_report.md
inflating: olefile-master/.github/ISSUE_TEMPLATE/feature_request.md
inflating: olefile-master/.gitignore
inflating: olefile-master/.travis.yml
inflating: olefile-master/CHANGELOG.md
inflating: olefile-master/CONTRIBUTORS.txt
inflating: olefile-master/LICENSE.txt
```

inflating: olefile-master/MANIFEST.in
inflating: olefile-master/README.md
inflating: olefile-master/appveyor.yml
creating: olefile-master/doc/
inflating: olefile-master/doc/Contribute.rst
inflating: olefile-master/doc/FAQ.rst
inflating: olefile-master/doc/Features.rst
inflating: olefile-master/doc/History.rst
inflating: olefile-master/doc/Howto.rst
inflating: olefile-master/doc/Install.rst
inflating: olefile-master/doc/License.rst
inflating: olefile-master/doc/Makefile
inflating: olefile-master/doc/OLE_Overview.rst
inflating: olefile-master/doc/OLE_VBA_sample.png
inflating: olefile-master/doc/conf.py
inflating: olefile-master/doc/index.rst
inflating: olefile-master/doc/make.bat
inflating: olefile-master/doc/olefile.rst
inflating: olefile-master/install.bat
inflating: olefile-master/make_dist.py
creating: olefile-master/olefile/
inflating: olefile-master/olefile/**init**.py
inflating: olefile-master/olefile/olefile.py
extracting: olefile-master/setup.cfg
inflating: olefile-master/setup.py
creating: olefile-master/tests/
extracting: olefile-master/tests/**init**.py
creating: olefile-master/tests/images/
inflating: olefile-master/tests/images/flower.jpg
inflating: olefile-master/tests/images/test-ole-file.doc
inflating: olefile-master/tests/test_olefile.py
creating: olefile-master/winbuild/
inflating: olefile-master/winbuild/appveyor_install_pypy.cmd

`_8.4: install the olefile with the setup.py script`

remnux@remnux-VM:/home/mcafee_alerts/olefile/olefile-master$ sudo python2.7 setup.py install
Traceback (most recent call last):
File "setup.py", line 12, in
from setuptools import setup
ImportError: No module named setuptools

Note: The "setuptools" module is required to continue.

_9: install the "setuptools" module

remnux@remnux-VM:/home/mcafee_alerts/olefile/olefile-master$ sudo apt install python-setuptools
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
libfprint-2-tod1 libllvm10
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
libpython2-stdlib python-pkg-resources python2 python2-minimal
Suggested packages:
python-setuptools-doc python2-doc python-tk
The following NEW packages will be installed:
libpython2-stdlib python-pkg-resources python-setuptools python2 python2-minimal
0 upgraded, 5 newly installed, 0 to remove and 20 not upgraded.
Need to get 520 kB of archives.
After this operation, 2,373 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 python2-minimal amd64 2.7.17-2ubuntu4 [27.5 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 libpython2-stdlib amd64 2.7.17-2ubuntu4 [7,072 B]
Get:3 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 python2 amd64 2.7.17-2ubuntu4 [26.5 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 python-pkg-resources all 44.0.0-2 [129 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu focal/universe amd64 python-setuptools all 44.0.0-2 [330 kB]
Fetched 520 kB in 1s (590 kB/s)
Selecting previously unselected package python2-minimal.
(Reading database ... 167645 files and directories currently installed.)
Preparing to unpack .../python2-minimal_2.7.17-2ubuntu4_amd64.deb ...
Unpacking python2-minimal (2.7.17-2ubuntu4) ...
Selecting previously unselected package libpython2-stdlib:amd64.
Preparing to unpack .../libpython2-stdlib_2.7.17-2ubuntu4_amd64.deb ...
Unpacking libpython2-stdlib:amd64 (2.7.17-2ubuntu4) ...
Setting up python2-minimal (2.7.17-2ubuntu4) ...
Selecting previously unselected package python2.
(Reading database ... 167674 files and directories currently installed.)
Preparing to unpack .../python2_2.7.17-2ubuntu4_amd64.deb ...
Unpacking python2 (2.7.17-2ubuntu4) ...
Selecting previously unselected package python-pkg-resources.
Preparing to unpack .../python-pkg-resources_44.0.0-2_all.deb ...

Unpacking python-pkg-resources (44.0.0-2) ...
Selecting previously unselected package python-setuptools.
Preparing to unpack .../python-setuptools_44.0.0-2_all.deb ...
Unpacking python-setuptools (44.0.0-2) ...
Setting up libpython2-stdlib:amd64 (2.7.17-2ubuntu4) ...
Setting up python2 (2.7.17-2ubuntu4) ...
Setting up python-pkg-resources (44.0.0-2) ...
Setting up python-setuptools (44.0.0-2) ...
Processing triggers for man-db (2.9.1-1) ...

`_9.1: run again to install the olefile with the setup.py script`

remnux@remnux-VM:/home/mcafee_alerts/olefile/olefile-master$ sudo python2.7 setup.py install
running install
running bdist_egg
running egg_info
writing olefile.egg-info/PKG-INFO
writing top-level names to olefile.egg-info/top_level.txt
writing dependency_links to olefile.egg-info/dependency_links.txt
reading manifest file 'olefile.egg-info/SOURCES.txt'
reading manifest template 'MANIFEST.in'
no previously-included directories found matching 'doc/_build'
writing manifest file 'olefile.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
running install_lib
running build_py
creating build/lib.linux-x86_64-2.7
creating build/lib.linux-x86_64-2.7/olefile
copying olefile/**init**.py -> build/lib.linux-x86_64-2.7/olefile
copying olefile/olefile.py -> build/lib.linux-x86_64-2.7/olefile
creating build/bdist.linux-x86_64/egg
creating build/bdist.linux-x86_64/egg/olefile
copying build/lib.linux-x86_64-2.7/olefile/**init**.py -> build/bdist.linux-x86_64/egg/olefile
copying build/lib.linux-x86_64-2.7/olefile/olefile.py -> build/bdist.linux-x86_64/egg/olefile
byte-compiling build/bdist.linux-x86_64/egg/olefile/**init**.py to **init**.pyc
byte-compiling build/bdist.linux-x86_64/egg/olefile/olefile.py to olefile.pyc
creating build/bdist.linux-x86_64/egg/EGG-INFO
copying olefile.egg-info/PKG-INFO -> build/bdist.linux-x86_64/egg/EGG-INFO
copying olefile.egg-info/SOURCES.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
copying olefile.egg-info/dependency_links.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
copying olefile.egg-info/top_level.txt -> build/bdist.linux-x86_64/egg/EGG-INFO
zip_safe flag not set; analyzing archive contents...
creating 'dist/olefile-0.47.dev4-py2.7.egg' and adding 'build/bdist.linux-x86_64/egg' to it
removing 'build/bdist.linux-x86_64/egg' (and everything under it)

Processing olefile-0.47.dev4-py2.7.egg
Copying olefile-0.47.dev4-py2.7.egg to /usr/local/lib/python2.7/dist-packages
Adding olefile 0.47.dev4 to easy-install.pth file

Installed /usr/local/lib/python2.7/dist-packages/olefile-0.47.dev4-py2.7.egg
Processing dependencies for olefile0.47.dev4
Finished processing dependencies for olefile0.47.dev4

At this time it was successfully executed, now let's try to run the script once again.

`_10: run the punbup.py script`

remnux@remnux-VM:/home/mcafee_alerts/punbup-master$ sudo python2.7 punbup.py -h
usage: punbup.py [-h] [-d] [-o] [-c {md5,sha1,sha256}] [-f] [-x] [-X] [-a]
[-A]
infile

This script can be used to extract quarantined files from a McAfee .bup file.
If run with no additional options the script will extract all files from the
.bup and place them in a folder with the same name as the supplied .bup file.

positional arguments:
infile The file that you wish to un-bup.

optional arguments:
-h, --help show this help message and exit
-d, --details Only print the contents of the Details file. Don't
extract any files.
-o, --original Rename all quarantine files to their original names as
noted in the Details file. Some assumptions have been
made for this to feature to work. Use at your own
risk.
-c {md5,sha1,sha256}, --hash {md5,sha1,sha256}
Calculates the hash for all of the files in the bup.
-f, --firstfile Output the first quarantined file.
-x, --hexdumpfirst Perform a hexdump of the first quarantined file.
-X, --hexdumpall Perform a hexdump of all quarantined files.
-a, --hexasciidumpfirst
Perform a hex & ASCII dump of the first quarantined
file.
-A, --hexasciidumpall
Perform a hex & ASCII dump of all quarantined files.
remnux@remnux-VM:/home/mcafee_alerts/punbup-master$

Note: To successfully execute the punbup.py script was necessary to install the olefile manually due to using the pip command the system was recognizing the olefile as requirement already satisfied, however, it was not working. The quick fix was to manually install the olefile and run the script.