【ctf秀】【MISC】MISC入门misc10

原创

远古某人 已于 2022-03-29 11:41:18 修改 4017 收藏

分类专栏： CTF # CTF秀 文章标签： python 安全

于 2022-03-29 11:31:03 首次发布

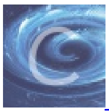
本文链接：https://blog.csdn.net/guggle15/article/details/123811817

版权

CTF 同时被 2 个专栏收录

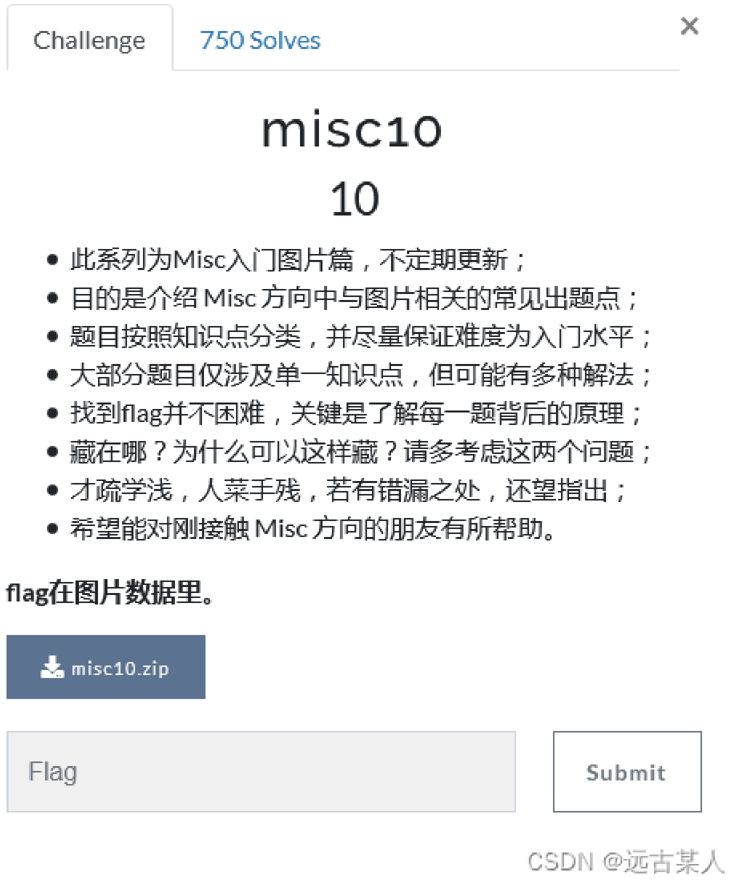
4 篇文章 0 订阅

订阅专栏


CTF秀

3 篇文章 0 订阅

订阅专栏



misc10

10

- 此系列为Misc入门图片篇，不定期更新；
- 目的是介绍 Misc 方向中与图片相关的常见出题点；
- 题目按照知识点分类，并尽量保证难度为入门水平；
- 大部分题目仅涉及单一知识点，但可能有多种解法；
- 找到flag并不困难，关键是了解每一题背后的原理；
- 藏在哪？为什么可以这样藏？请多考虑这两个问题；
- 才疏学浅，人菜手残，若有错漏之处，还望指出；
- 希望能对刚接触 Misc 方向的朋友有所帮助。

flag在图片数据里。

一、解题环境

windows7

二、考点:binwalk的使用

考点发现及解题过程（所有的png图片misc题均可这么做）：

1.解压zip文件，用winhex打开misc10.png

2.判断文件格式是否篡改，检查png的文件头和文件尾，文件格式正常

PNG文件头(hex)：89 50 4e 47 0d 0a 1a 0a

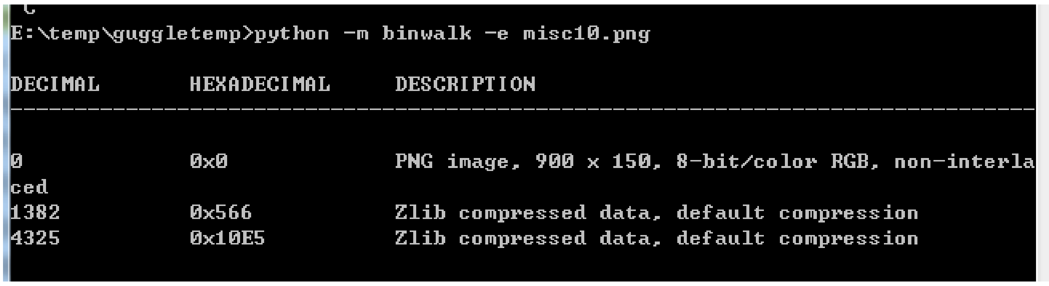
PNG文件尾(hex)： 00 00 00 00 49 45 4E 44 AE 42 60 82

3.判断否有文件二进制合并，搜索png文件头8950，发现只有一个，未使用二进制合并文件

4.判断是否修改png图片宽高，使用TweakPNG或者pngcheck等crc校验工具，发现图片宽高正常。

5.用Stegsolve.jar查看图片是否有变换背景色及隐藏色块，发现misc10.png一切正常

6.最后用binwalk，执行 `python -m binwalk -e misc10.png`，发现有情况(如果熟悉zlib文件解析，也可自行写python脚本进行解析~)

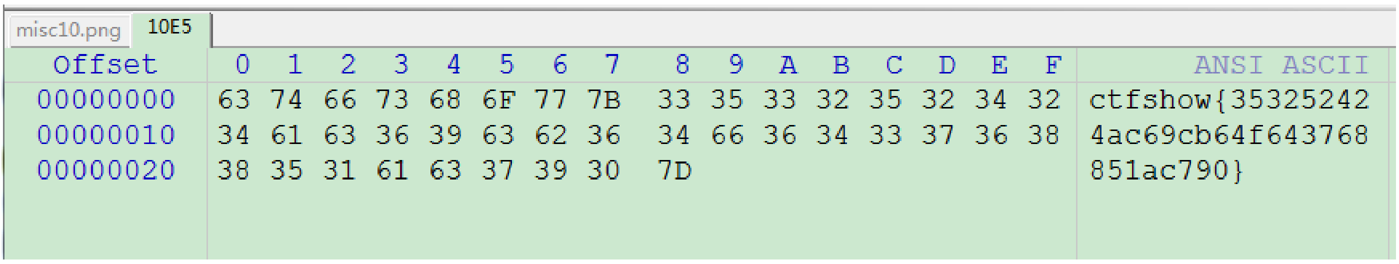


```
E:\temp\guggletemp>python -m binwalk -e misc10.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

0             0x0             PNG image, 900 x 150, 8-bit/color RGB, non-interla
ced
1382          0x566           Zlib compressed data, default compression
4325          0x10E5          Zlib compressed data, default compression
```

7.用winhex打开10E5这个文件即可看到flag



```
Offset      0  1  2  3  4  5  6  7   8  9  A  B  C  D  E  F   ANSI ASCII
00000000   63 74 66 73 68 6F 77 7B  33 35 33 32 35 32 34 32   ctfshow{35325242
00000010   34 61 63 36 39 63 62 36  34 66 36 34 33 37 36 38   4ac69cb64f643768
00000020   38 35 31 61 63 37 39 30  7D                        851ac790}
```

三、难点：windows下安装binwalk!!!

binwalk安装步骤如下：

1.安装python环境

参考本人文章中【一、安装python环境】

一、安装python环境

1. 确认系统版本

查看计算机系统版本是32位还是64位，右击【计算机】-【属性】

查看有关计算机的基本信息

Windows 版本

Windows 7 旗舰版

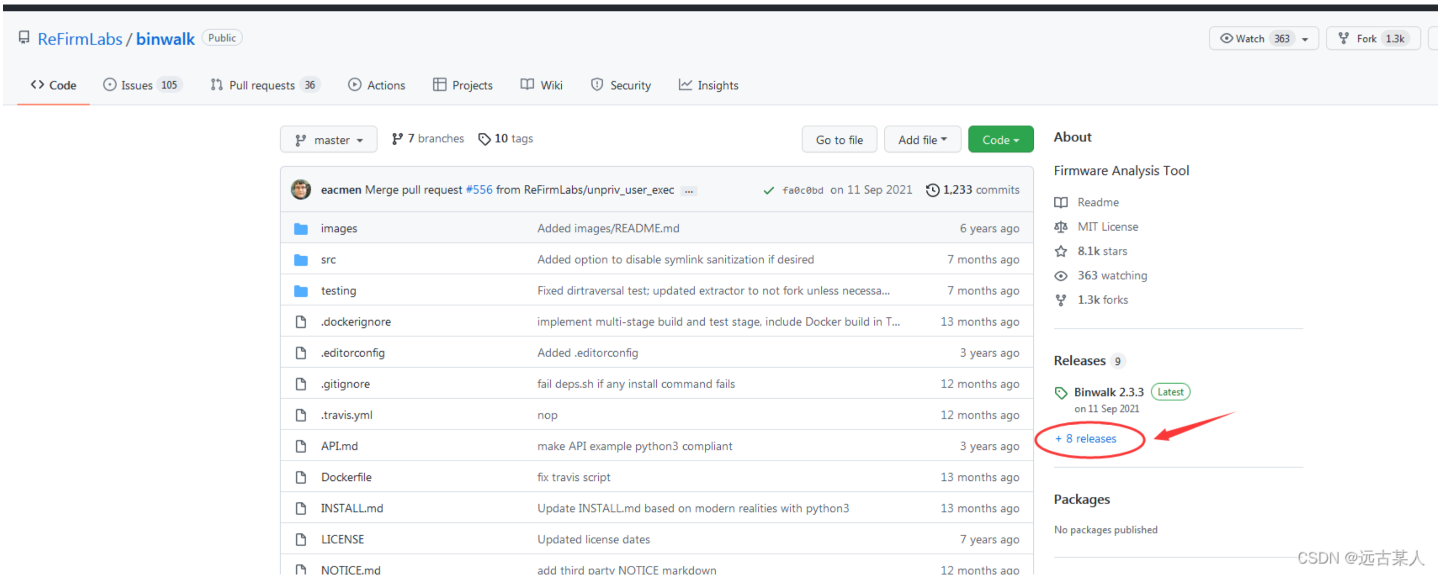
版权所有 © 2009 Microsoft Corporation。保留所有权利。

Service Pack 1

系统

2.下载binwalk

binwalk github地址中点击【+8 releases】中找到历史版本【Binwalk 2.3.2】,binwalk的最新版本(Binwalk2.3.3)只能在linux下运行，`一定要选2.3.2`



eacmen Merge pull request #556 from ReFirmLabs/unpriv_user_exec … ✓ fa0c0bd on 11 Sep 2021 1,233 commits

images	Added images/README.md	6 years ago
src	Added option to disable symlink sanitization if desired	7 months ago
testing	Fixed dirtraversal test; updated extractor to not fork unless necessa...	7 months ago
.dockerignore	implement multi-stage build and test stage, include Docker build in T...	13 months ago
.editorconfig	Added .editorconfig	3 years ago
.gitignore	fail deps.sh if any install command fails	12 months ago
.travis.yml	nop	12 months ago
API.md	make API example python3 compliant	3 years ago
Dockerfile	fix travis script	13 months ago
INSTALL.md	Update INSTALL.md based on modern realities with python3	13 months ago
LICENSE	Updated license dates	7 years ago
NOTICE.md	add third party NOTICE markdown	12 months ago

About

Firmware Analysis Tool

Readme
MIT License
8.1k stars
363 watching
1.3k forks

Releases 9

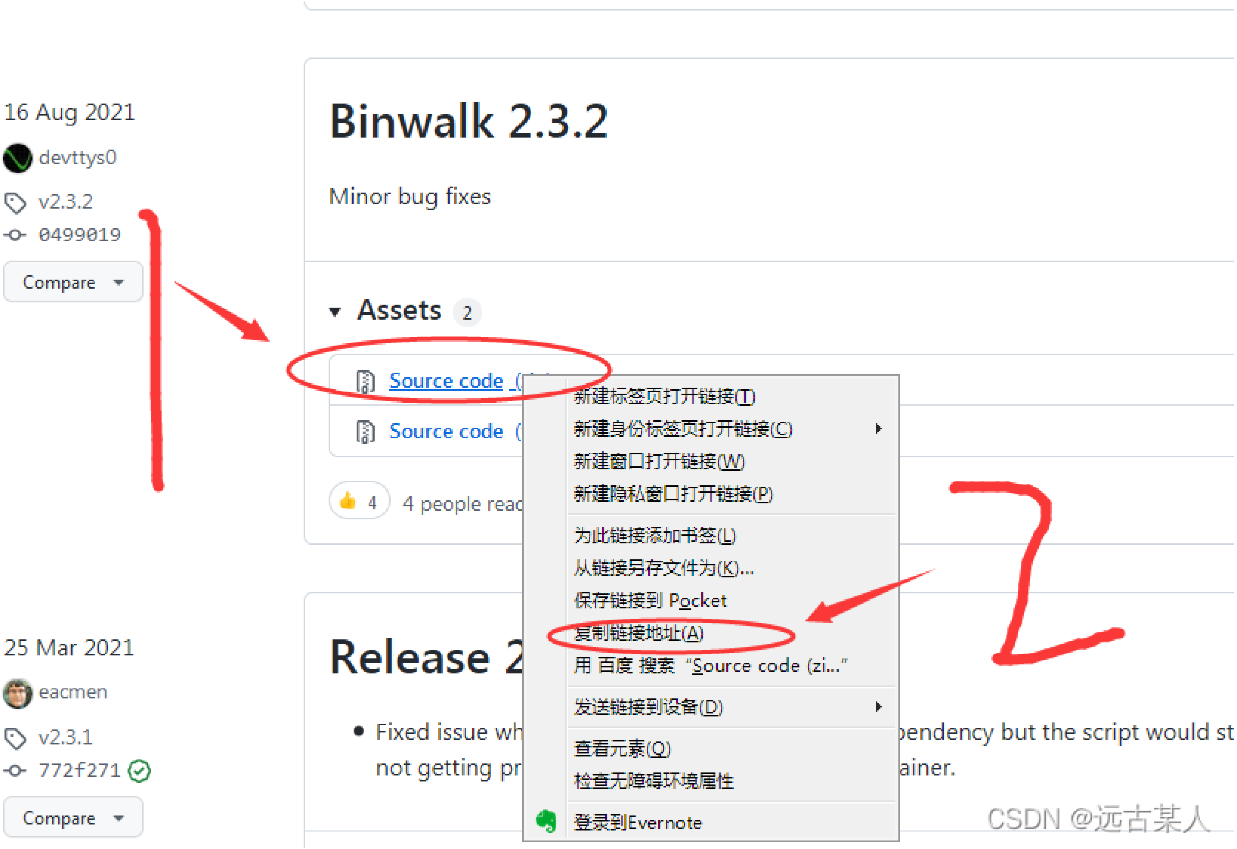
Binwalk 2.3.3 Latest
on 11 Sep 2021
+ 8 releases

Packages

No packages published

嫌弃github下载速度慢的可使用以下方法

a)右击下载链接，【复制链接】


16 Aug 2021
devttys0
v2.3.2
0499019

Binwalk 2.3.2

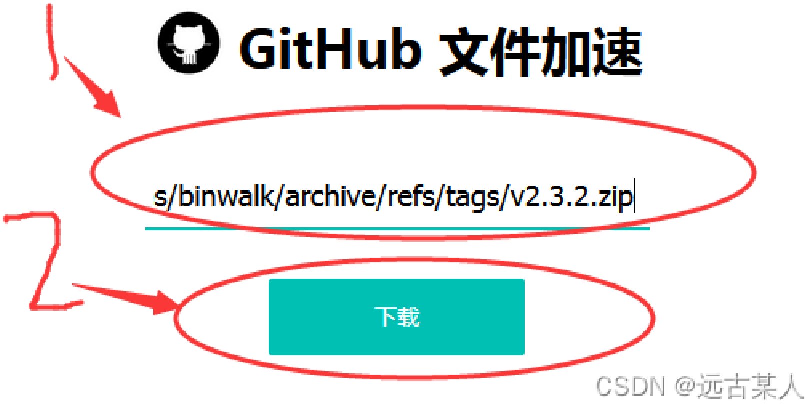
Minor bug fixes

25 Mar 2021
eacmen
v2.3.1
772f271

Release 2

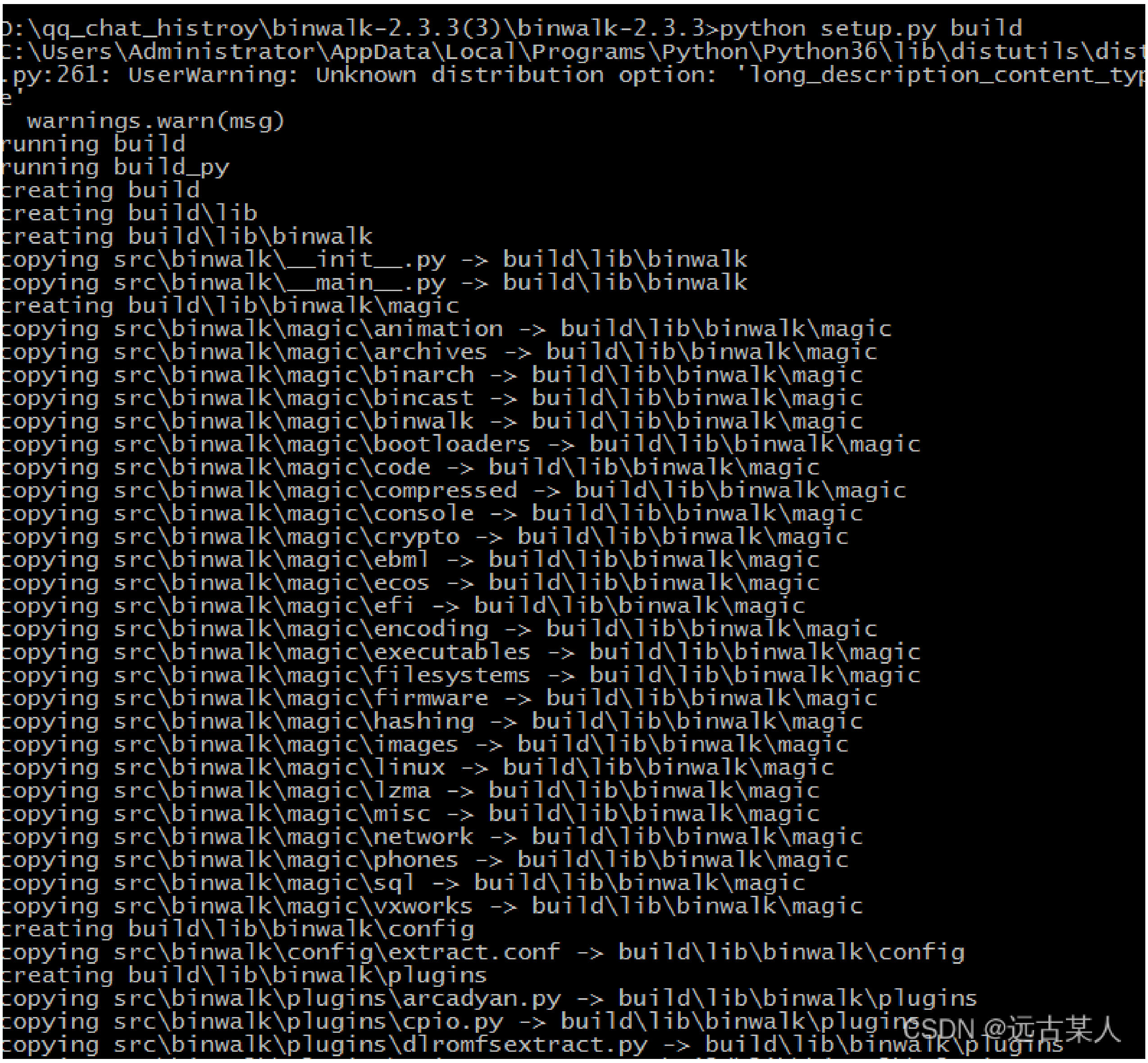
- Fixed issue wh … pendency but the script would st
not getting pr … ainer.

b) 打开github文件下载加速网站，把链接粘贴进去即可



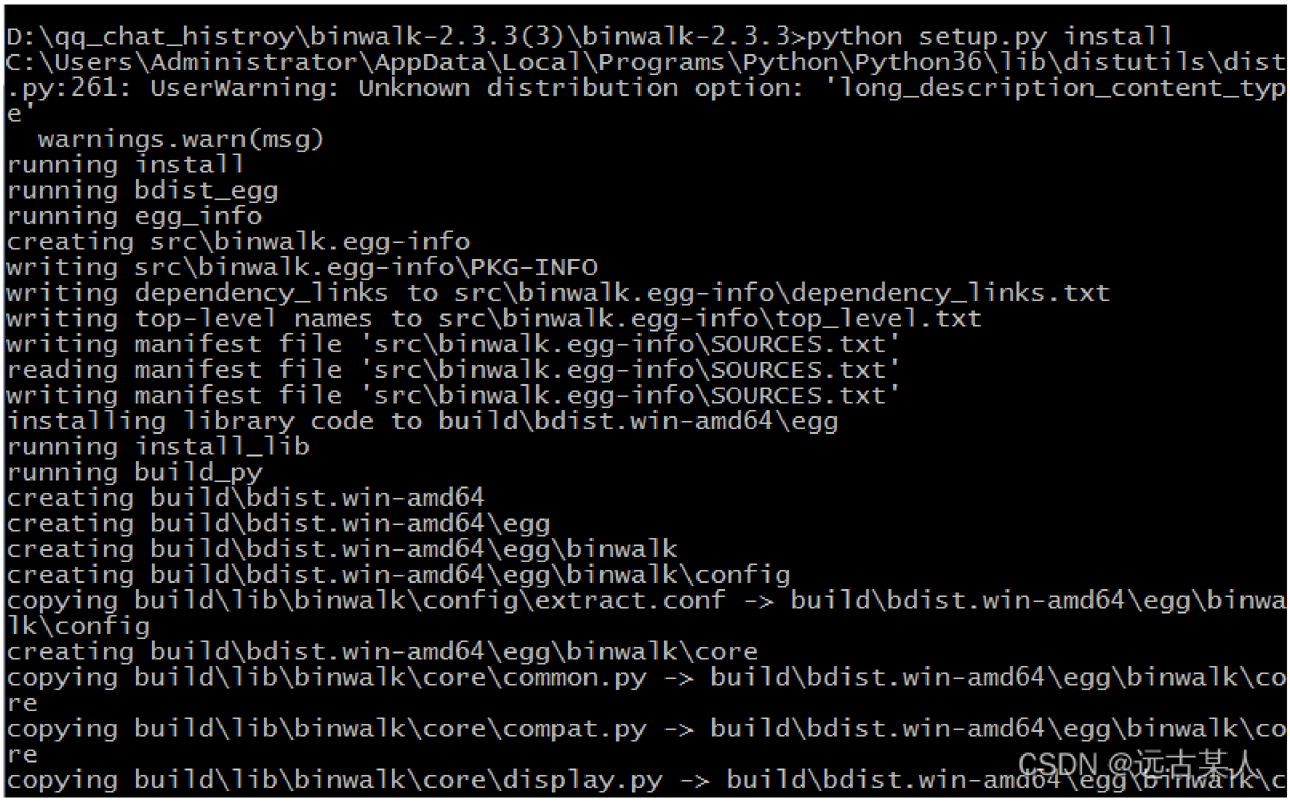
3.解压zip包，安装binwalk

a).在zip包解压目录中执行`python setup.py build`



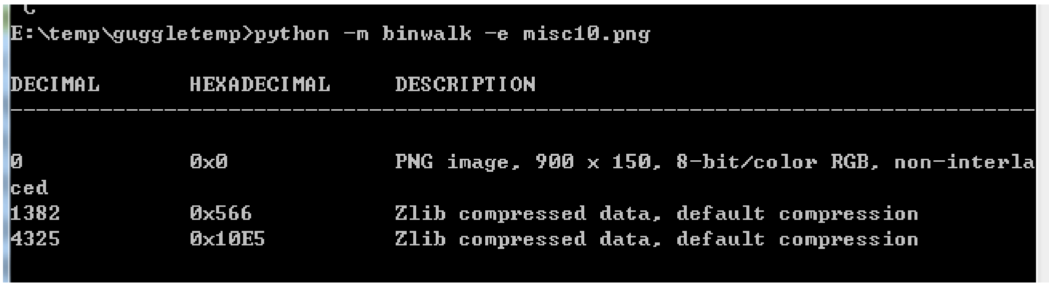
```
D:\qq_chat_histroy\binwalk-2.3.3(3)\binwalk-2.3.3>python setup.py build
C:\Users\Administrator\AppData\Local\Programs\Python\Python36\lib\distutils\dist
.py:261: UserWarning: Unknown distribution option: 'long_description_content_typ
e'
  warnings.warn(msg)
running build
running build_py
creating build
creating build\lib
creating build\lib\binwalk
copying src\binwalk\__init__.py -> build\lib\binwalk
copying src\binwalk\__main__.py -> build\lib\binwalk
creating build\lib\binwalk\magic
copying src\binwalk\magic\animation -> build\lib\binwalk\magic
copying src\binwalk\magic\archives -> build\lib\binwalk\magic
copying src\binwalk\magic\binarch -> build\lib\binwalk\magic
copying src\binwalk\magic\bincast -> build\lib\binwalk\magic
copying src\binwalk\magic\binwalk -> build\lib\binwalk\magic
copying src\binwalk\magic\bootloaders -> build\lib\binwalk\magic
copying src\binwalk\magic\code -> build\lib\binwalk\magic
copying src\binwalk\magic\compressed -> build\lib\binwalk\magic
copying src\binwalk\magic\console -> build\lib\binwalk\magic
copying src\binwalk\magic\crypto -> build\lib\binwalk\magic
copying src\binwalk\magic\ebml -> build\lib\binwalk\magic
copying src\binwalk\magic\ecos -> build\lib\binwalk\magic
copying src\binwalk\magic\efi -> build\lib\binwalk\magic
copying src\binwalk\magic\encoding -> build\lib\binwalk\magic
copying src\binwalk\magic\executables -> build\lib\binwalk\magic
copying src\binwalk\magic\filesystems -> build\lib\binwalk\magic
copying src\binwalk\magic\firmware -> build\lib\binwalk\magic
copying src\binwalk\magic\hashing -> build\lib\binwalk\magic
copying src\binwalk\magic\images -> build\lib\binwalk\magic
copying src\binwalk\magic\linux -> build\lib\binwalk\magic
copying src\binwalk\magic\lzma -> build\lib\binwalk\magic
copying src\binwalk\magic\misc -> build\lib\binwalk\magic
copying src\binwalk\magic\network -> build\lib\binwalk\magic
copying src\binwalk\magic\phones -> build\lib\binwalk\magic
copying src\binwalk\magic\sql -> build\lib\binwalk\magic
copying src\binwalk\magic\vxworks -> build\lib\binwalk\magic
creating build\lib\binwalk\config
copying src\binwalk\config\extract.conf -> build\lib\binwalk\config
creating build\lib\binwalk\plugins
copying src\binwalk\plugins\arcadyan.py -> build\lib\binwalk\plugins
copying src\binwalk\plugins\cpio.py -> build\lib\binwalk\plugins
copying src\binwalk\plugins\dlromfsextract.py -> build\lib\binwalk\plugins
```

b).build成功后执行`python setup.py install`



```
D:\qq_chat_histroy\binwalk-2.3.3(3)\binwalk-2.3.3>python setup.py install
C:\Users\Administrator\AppData\Local\Programs\Python\Python36\lib\distutils\dist
.py:261: UserWarning: Unknown distribution option: 'long_description_content_typ
e'
  warnings.warn(msg)
running install
running bdist_egg
running egg_info
creating src\binwalk.egg-info
writing src\binwalk.egg-info\PKG-INFO
writing dependency_links to src\binwalk.egg-info\dependency_links.txt
writing top-level names to src\binwalk.egg-info\top_level.txt
writing manifest file 'src\binwalk.egg-info\SOURCES.txt'
reading manifest file 'src\binwalk.egg-info\SOURCES.txt'
writing manifest file 'src\binwalk.egg-info\SOURCES.txt'
installing library code to build\bdist.win-amd64\egg
running install_lib
running build_py
creating build\bdist.win-amd64
creating build\bdist.win-amd64\egg
creating build\bdist.win-amd64\egg\binwalk
creating build\bdist.win-amd64\egg\binwalk\config
copying build\lib\binwalk\config\extract.conf -> build\bdist.win-amd64\egg\binwa
lk\config
creating build\bdist.win-amd64\egg\binwalk\core
copying build\lib\binwalk\core\common.py -> build\bdist.win-amd64\egg\binwalk\co
re
copying build\lib\binwalk\core\compat.py -> build\bdist.win-amd64\egg\binwalk\co
re
copying build\lib\binwalk\core\display.py -> build\bdist.win-amd64\egg\binwalk\c
```

4.在需要分析的图片目录中执行`python -m binwalk -e misc10.png`



```
E:\temp\guggletemp>python -m binwalk -e misc10.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

0             0x0             PNG image, 900 x 150, 8-bit/color RGB, non-interla
ced
1382          0x566           Zlib compressed data, default compression
4325          0x10E5          Zlib compressed data, default compression
```