





CTF Series Forensics

原创

置顶  VIP文章 [tiny\](#)  于 2019-08-26 17:52:55 发布  1140  收藏 1

分类专栏: [渗透&APT 渗透](#)

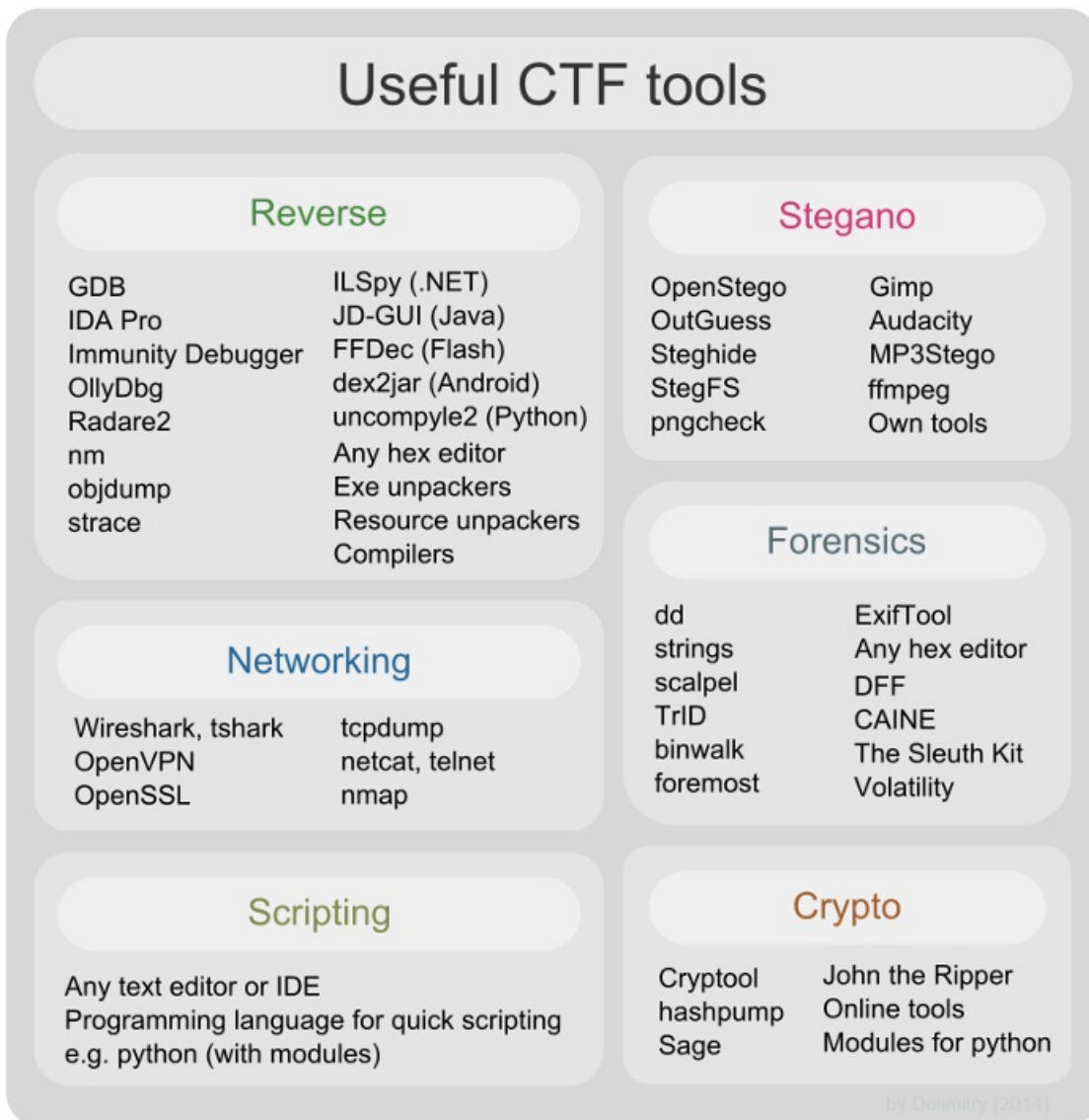
版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/vevencf/article/details/100082827>

版权

描述

这篇文章列出了CTF中Forensics（取证）类型题的技巧和窍门，展示了CTF中常用工具的使用场景和使用方法。



文件格式（File Formats）

十六进制文件头和对应ASCII码

通过查看文件头前四到五个字节的十六进制数来识别文件类型。参考[Hex file and Regex Cheat Sheet](#) 和 [Gary Kessler File Signature Table](#)

Filetype	Start	Start ASCII Translation
----------	-------	-------------------------

ani	52 49 46 46	RIFF
-----	-------------	------

au	2E 73 6E 64	snd
----	-------------	-----

bmp	42 4D F8 A9	BM
-----	-------------	----

bmp	42 4D	
-----	-------	--