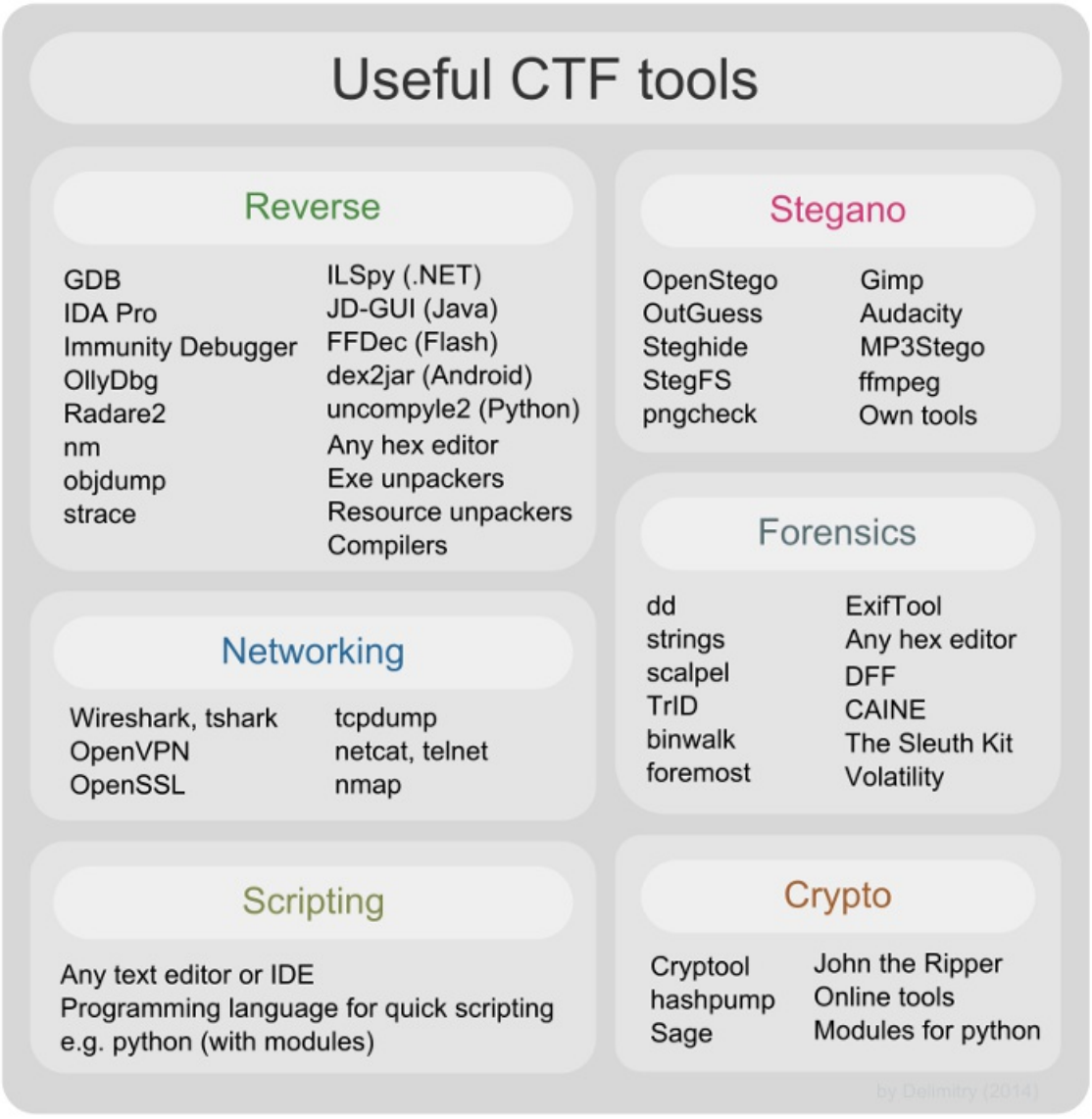
CTF Series Forensics

原创

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
```