

## A.1 数据包分析工具

除了 Wireshark 之外，还有一些实用的数据包分析工具。在这里，我会介绍一些我认为最有用的。

### 1. Tcpdump 和 Windump

虽然 Wireshark 很流行，但它可能没有 Tcpdump 用得广泛。考虑到一些人群对数据包捕获和分析的实际需求，Tcpdump 是完全基于文本的。

虽然 Tcpdump 缺少图形特性，但它处理海量数据时非常靠谱。因为你可以用管道将它的输出重定向输入给其他命令，比如 Linux 的 sed 和 awk。随着对数据包分析的深入钻研，你会发现 Wireshark 和 Tcpdump 都很有用。

Windump 只是 Tcpdump 在 Windows 平台的发行版而已。

### 2. Cain & Abel

第 2 章已经讨论过，Cain & Abel 是 Windows 平台上最好的 ARP 缓存中毒攻击工具之一。Cain & Abel 实际上是一个非常健壮的工具套件，你一定能发现其他用途。

### 3. Scapy

Scapy 是一个非常强大的 Python 库，允许使用基于命令行脚本的方法创建、修改数据包。简单地说，Scapy 是一款强大、灵活的数据包操纵程序。

### 4. Netdude

如果你不需要像 Scapy 那样高级的工具，那么 Netdude 是 Linux 下的一个较好的替代品。虽然 Netdude 功能有限，但它提供了图形用户界面，因而出于研究目的，需要创建、修改数据包时，它显得极其方便。图 A-1 演示了使用 Netdude 的一个例子。

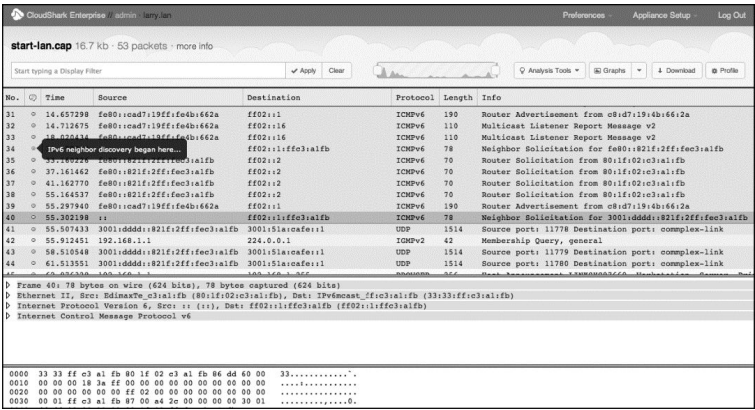


图 A-1 在 Netdude 上修改数据包

5. Colasoft Packet Builder

如果你是 Windows 用户，并且想要与 Netdude 类似的 GUI，那么你可以考虑使用 Colasoft Packet Builder，一款超棒的免费工具。Colasoft 还提供了一个简便的用于数据包创建和修改的 GUI。

6. CloudShark

CloudShark（由 QA Café 开发）是我很喜爱的一个工具，可以用它在线分享数据包捕获记录。如图 A-2 所示，CloudShark 网站可以在浏览器里以 Wireshark 的方式显示网络捕获文件。你可以上传捕获文件，并将链接发送给同事，以便共同分析。

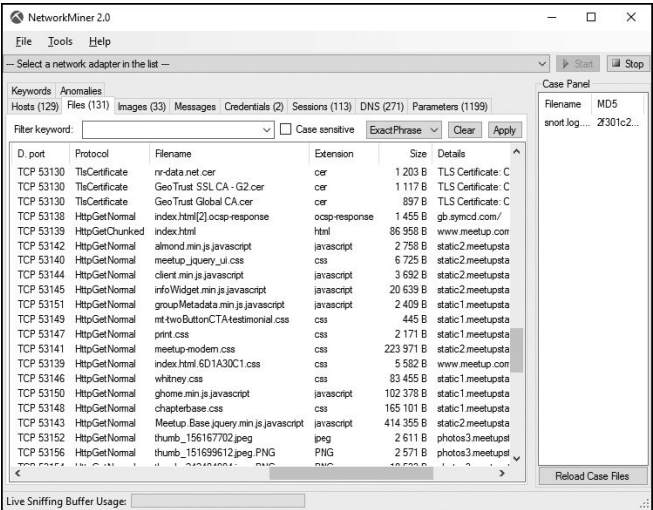
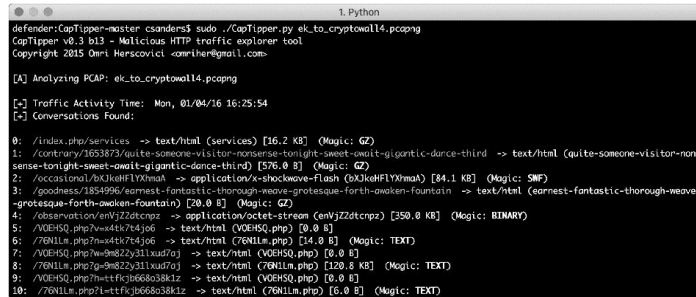


图 A-2 用 CloudShark 查看一个捕获文件示例

关于 CloudShark，我最赞赏的是它不需要注册，并能通过 URL 直接链接获取。这意味着，当我在博客上发布一个 PCAP 文件的链接时，其他人只需要单击就能查看数据包，而不需要在下载文件后，再用 Wireshark 打开。

7. pcapr

pcapr 是 Mu Dynamics 创建的一个非常健壮的用于分享 PCAP 文件的 Web 2.0 平台。在撰写本文时，pcapr 包含了将近 3000 个 PCAP 文件，涉及 400 多种不同协议的例子。图 A-3 显示了 pcapr 上的 DHCP 流量捕获的例子。



```
defender@captipper-master csanders$ sudo ./CapTipper.py ek_to_cryptowall4.pcapng
CapTipper v0.3 b13 - Malicious HTTP traffic explorer tool
Copyright 2015 Omer Herscovici <omher@gmail.com>

[A] Analyzing PCAP: ek_to_cryptowall4.pcapng

[-] Traffic Activity Time: Mon, 01/04/16 16:25:54
[-] Conversations Found:

0: /index.php/services -> text/html (services) [16.2 KB] (Magic: GZ)
1: /contrary/1653873/quite-someone-visitor-nonsense-tonight-sweet-sweet-gigantic-dance-third -> text/html (quite-someone-visitor-nonsense-tonight-sweet-sweet-gigantic-dance-third) [576.0 B] (Magic: GZ)
2: /occasional/bXJkeHFLYXhmaA -> application/x-shockwave-flash (bXJkeHFLYXhmaA) [44.1 KB] (Magic: SWF)
3: /goodness/1834996/earnest-fantastic-thorough-weave-protosque-forth-awaken-fountain -> text/html (earnest-fantastic-thorough-weave-protosque-forth-awaken-fountain) [20.0 B] (Magic: GZ)
4: /observation/enVjZd4cnpz -> application/octet-stream (enVjZd4cnpz) [350.0 KB] (Magic: BINARY)
5: /VOEH5Q.php7wxd4k7d4j06 -> text/html (VOEH5Q.php) [0.0 B]
6: /76N1Lm.php7wxd4k7d4j06 -> text/html (76N1Lm.php) [14.0 B] (Magic: TEXT)
7: /VOEH5Q.php7wxd4k7d4j06 -> text/html (VOEH5Q.php) [0.0 B]
8: /76N1Lm.php7wxd4k7d4j06 -> text/html (76N1Lm.php) [120.8 KB] (Magic: TEXT)
9: /VOEH5Q.php7wxd4k7d4j06 -> text/html (VOEH5Q.php) [0.0 B]
10: /76N1Lm.php7wxd4k7d4j06 -> text/html (76N1Lm.php) [0.0 B] (Magic: TEXT)
```

图 A-3 在 pcapr 上查看 DHCP 流量捕获

每次要查找某种确定类型的通信样例时，我都是首先在 pcapr 上搜索。如果你在自己的试验中创建了大量不同的捕获文件，不要犹豫，请将它们上传到 pcapr 社区分享。

## 8. NetworkMiner

NetworkMiner 是一款主要用于网络取证的工具，但我发现它在其他一些情形下也非常实用。虽然它也可以用来捕获数据包，但它的强项在于如何解析数据包。NetworkMiner 会检测 PCAP 文件中网络各端的操作系统类型，并将文件解析成主机间的会话。它甚至允许你直接从捕获记录中提取传输的文件。

## 9. Tcpreplay

每当有一堆数据包需要在线路上重传以观察设备如何响应它们时，我就用 Tcpreplay 来执行这个任务。Tcpreplay 专门设计用来重传 PCAP 文件里的数据包。

## 10. ngrep

如果你熟悉 Linux，毫无疑问，你肯定用过 grep 搜索数据。ngrep 与它非常相似，允许你在 PCAP 数据上执行特定搜索。当捕获和显示过滤器都无法实现我的目标或者实现太复杂时，我就使用 ngrep。

## 11. Libpcap

如果你计划开发一款应用程序，来进行一些确实高级的数据包解析，或是创建处理数据包，那么你要对 Libpcap 非常熟悉。简言之，Libpcap 是一个用于网络流量捕获的可移植的 C/C++ 库。Wireshark、Tcpdump，以及其他大部分数据包分析工具都在一定层次上依赖于 Libpcap。

## 12. Hping

Hping 是你武器库中应有的「瑞士军刀」之一。Hping 是一个命令行的数据包操纵和传输工具。它支持各种各样的协议，反应非常快且直观。

## 13. Domain Dossier

如果你需要查询域名或 IP 地址的注册信息，那么 Domain Dossier 正合你意。它快速、简单、有效。

## 14. Perl 和 Python

Perl 和 Python 虽然不是工具，但却是值得留意的脚本语言。当你熟练于数据包分析时，你会遇到没有自动化工具满足要求的情况。在那些情况下，首选 Perl 和 Python 语言编写工具，它们可以带你在数据包上做些有趣的事情。对于大部分应用程序，我通常使用 Python，但这只是个人选择。