# 概述

tcpdump命令是一款嗅探sniff工具，它可以打印所有经过网络接口的数据包的头信息，也可以使用-W选项将数据包保存到文件中，方便后续分析。

# 选项

# 实战

我们可以使用tcpdump抓包，然后使用fiddle或者wireshark分析数据包。

比如我们需要抓取10.47.181.1这台主机的br\_com网桥发往10.47.181.2主机8080端口的数据包，如下操作：

（1）抓包

tcpdump –i br\_com src 10.47.181.1 and dst 10.47.181.2 and port 8080 –w test.cap

（2）分析

转包后的文件用wireshark打开，点击对应的http包，然后点击追踪HTTP流，就可以看到整个发送包的内容。