Further Reading

Although the tool used primarily in this book is Wireshark there are a great deal of additional tools that will come in handy when you're performing packet analysis whether it be for general troubleshooting, slow networks, security issues, or wireless networks. This chapter is devoted in its entirety to noting some useful packet analysis tools and other packet analysis learning resources.

Tools

Tcpdump/Windump

Although Wireshark is very popular it is probably less widely used that tcpdump. Considered the de-facto packet capture and analysis utility by several crowds, tcpdump is entirely text based. Although it lacks the graphical features that Wireshark has it is great for sifting through large amounts of data as you can pipe its output to other commands such as sed and awk in Linux. As you delve further into packet analysis you will find use for both Wireshark and tcpdump. You can download tcpdump from http://www.tcpdump.org/.

Cain and Abel

Discussed in chapter two, Cain and Able is one of the better Windows tools for ARP cache poisoning. C&A is actually a very robust suite of tools and you will surely be able to find other uses for it as well. It is available at http://www.oxid.it/cain.html.

Scapy

Scapy is a very powerful Python wrapper that allows for the creation and manipulation of packets based upon command line scripts within its environment. Simply put, it's the most powerful and flexible packet crafting application available. You can read more about Scapy, download it, and view sample Scapy scripts at http://www.secdev.org/projects/scapy/.

Netdude

If you don't need something as advanced as Scapy then Netdude is a great Linux alternative. Although its limited in its ability, Netdude provides a GUI that is very easy to utilize for creating and modifying packets for research purposes. You can download Netdude from http://netdude.sourceforge.net/.

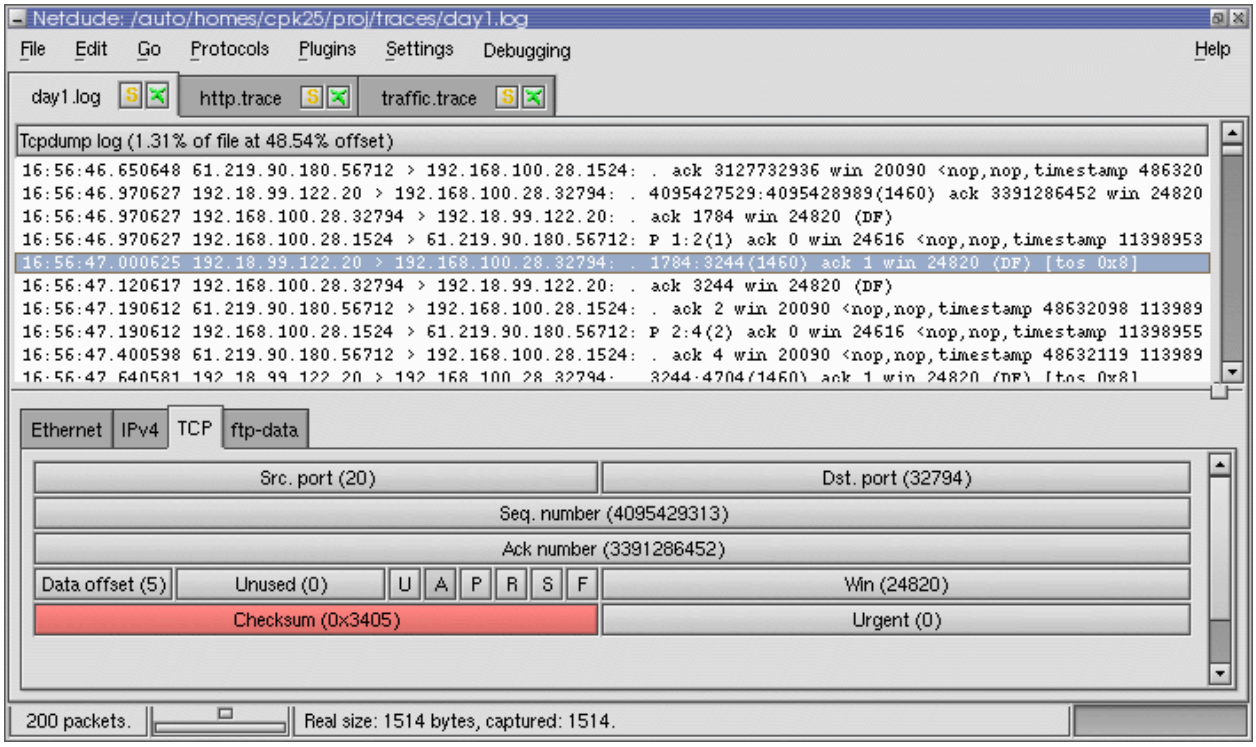

Figure 11-1: Modifying packets within Netdude

Colasoft Packet Builder

If you don't need something as advanced as Scapy and want to go the Windows route then Colasoft Packet Builder is an excellent free tool. Colasoft also provides a very easy to use GUI for packet creation and modification. You can download it at http://www.colasoft.com/packet_builder/.

CloudShark

As a writer and blogger CloudShark (developed by QA Café) has come to be one of my favorite online resources for sharing packet captures with others. It is a web site that displays network capture files inside your browser in a Wireshark-esque manner. This allows users to upload capture files and send the link to colleagues for shared analysis. My favorite thing about CloudShark is that it doesn't require registration and accepts direct linking via URL. This means that when I post a link to a PCAP file on my blog someone can just click it and see the packets without having to download the file and open it in Wireshark. CloudShark is accessible at http://www.cloudshark.org.

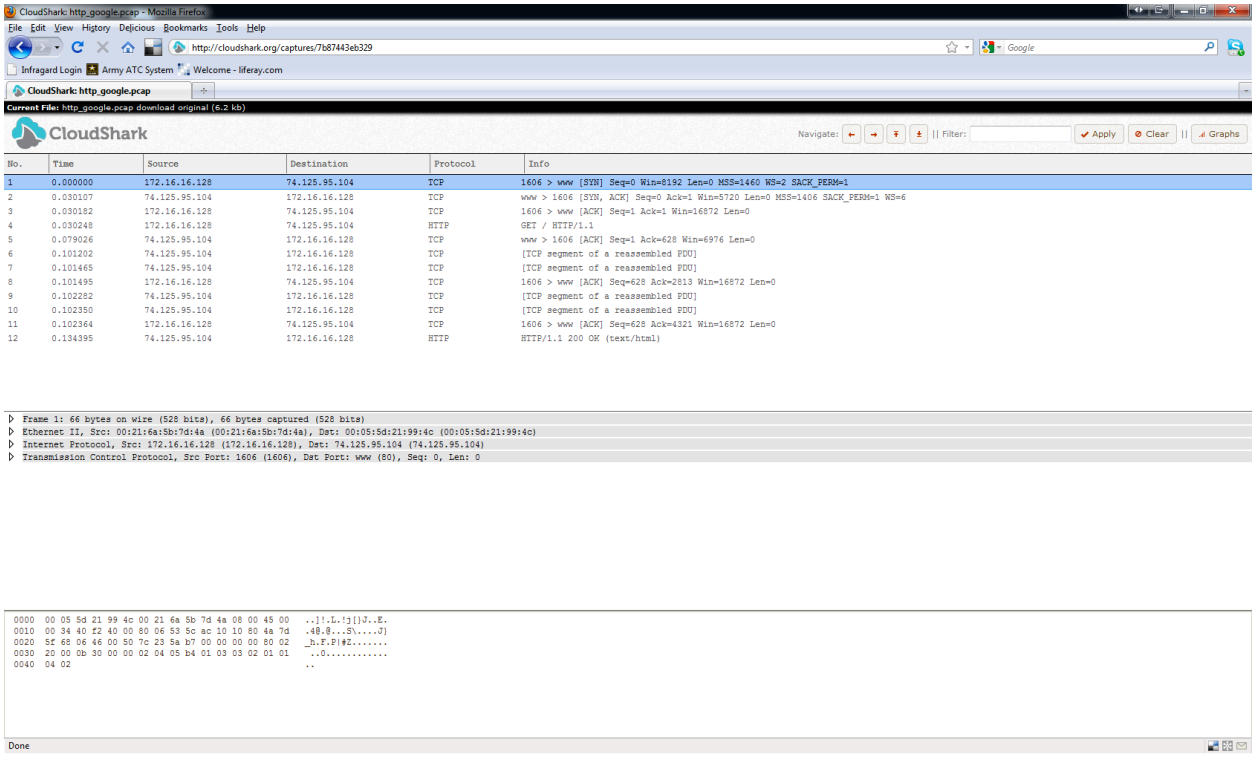

Figure 11-2: A sample capture file viewed with CloudShark

Network Miner

Network Miner is a tool primarily used for network forensics but I've found it useful in a variety of other situations as well. Although it can be used to capture packets, its real strength is how it parses PCAP files. Network Miner will take a PCAP file and break it down into the operating systems detected, the sessions between hosts, and even allows you to directly extract transferred files from the capture. Network Miner is a free download from http://networkminer.sourceforge.net/.

Tcpreplay

Whenever I have a set of packets that I need to retransmit over the wire to see how a device reacts to them I use Tcprelay to perform that. Tcprelay is designed specifically to take a PCAP file and retransmit the packets contained within it. You can download it at http://tcpreplay.synfin.net/.

Ngrep

If you are familiar with Linux that you've no doubt used the grep utility to search through data. Ngrep is very similar and allows you to perform very specific searches through PCAP data. I most commonly use ngrep when capture/display filters won't do the job or get too wildly complex. You can read more about ngrep at http://ngrep.sourceforge.net/.

Domain Dossier (http://centralops.net/co/DomainDossier.aspx)

If you need to look up the registration information for a domain or IP address then this is the place to do it. It's fast, it's simple, and it works.

Perl/Python

Perl and Python aren't tools, but rather, scripting languages that are well worth of a mention in this book. As you become proficient in packet analysis it is inevitable that you will encounter a situation for which you need to parse or manipulate data where no automated tool exists. In that case, Perl or Python are the languages of choice for making tools that can do interesting things with packets. Which one you choose is a matter of preference. I've always considered Perl an easier introductory language and the better choice for data parsing and while Python isn't much more difficult I use it for more advanced programs that go a bit beyond data parsing.

Learning Resources

Wireshark Homepage (http://www.wireshark.org)

The foremost resource for everything related to Wireshark is its homepage. The homepage includes the software documentation, a very helpful wiki that contains sample capture files, and sign up information for the Wireshark mailing-list.

SANS SEC 503 Course

As a SANS Mentor I'm slightly biased, but I don't think there is a better packet analysis course on the planet than SANS SEC 503. The course is entitled Intrusion Detection In-Depth and focuses on the security aspect of packet analysis. Even if you aren't focused on security, the first two days of the course provide the best introduction to packet analysis and tcpdump that I've ever seen. The course is taught by two of my packet analysis heroes Mike Poor and Judy Novak and is taught at live events several times throughout the year. If your travel budget is limited the course is also taught through an on-line and web based on demand format. You can read more about SEC 503 and other SANS courses at http://www.sans.org.

Chris Sanders Blog (http://www.chrissanders.org)

It's my book so of course I'm going to plug my own blog. I don't get around to posting nearly enough but I do occasionally write articles related to packet analysis and post them here. If nothing else, my blog serves as a portal that links to other articles/books I have written and provides information on how to get in touch with me.

Packetstan Blog (http://www.packetstan.com)

The blog of Mike Poor and Judy Novak is my favorite packet related blog out there at the moment. The site contains some great breakdowns of interesting traffic and every single piece of content on it is A+ material. Mike and Judy are two of the best at what they do and are a large inspiration for the things I do.

Wireshark University (http://www.wiresharktraining.com/)

Laura Chappell is one of the most prolific Wireshark evangelists you will find. Her site contains loads of Wireshark tips as well as information on her book, "Wireshark Network Analysis", and courses she teaches.

Pcapr (http://www.pcapr.net)

Pcapr is a very robust web 2.0 platform for sharing PCAP files created by the folks at Mu Dynamics. As of the writing of this book it currently contains nearly 3000 pcaps with examples of 421 different protocols. If I'm looking for an example of a certain type of communication I start by searching on Pcapr. If you find yourself creating a lot of different capture files in your own experimentation then don't hesitate to share them with the community by uploading them to Pcapr.

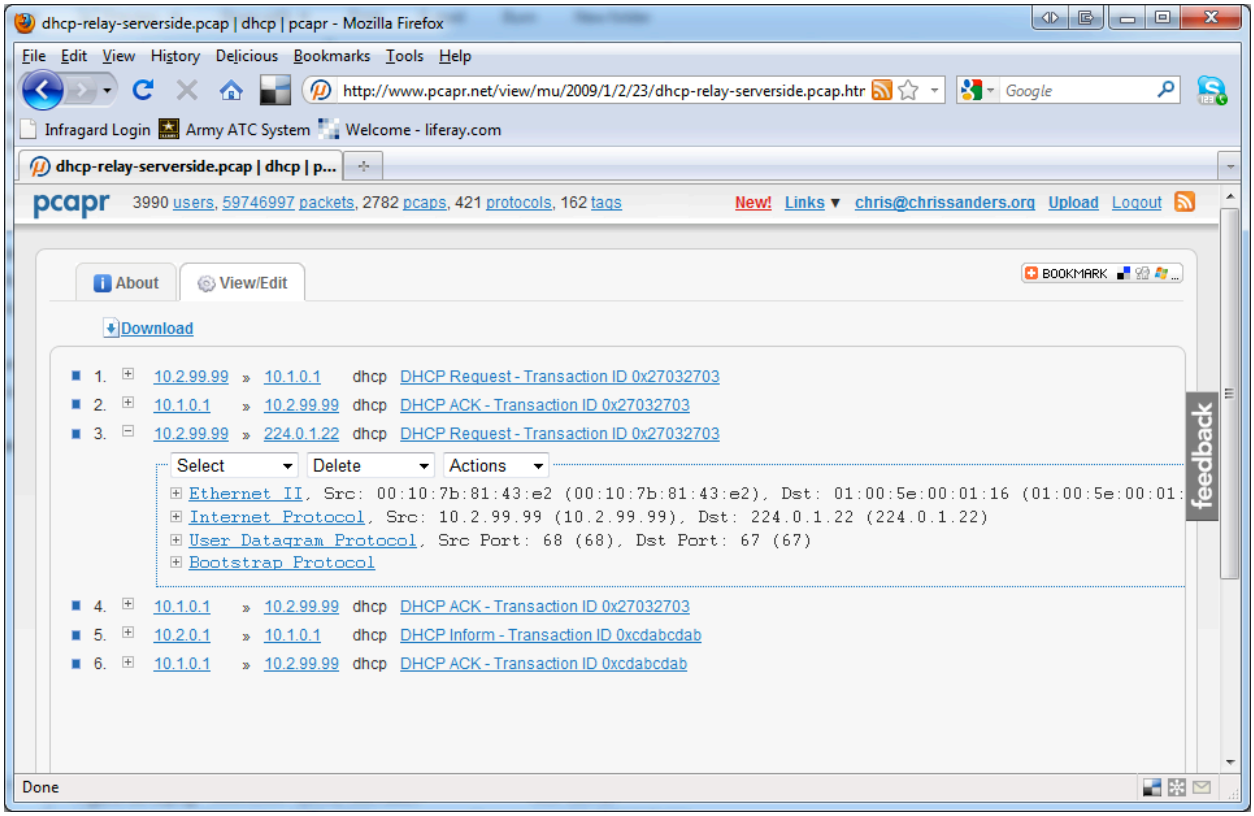

Figure 11-3: Viewing a DHCP traffic capture on Pcapr

IANA (http://www.iana.org)

The Internet Assigned Numbers Authority (IANA) oversees the allocation of IP addresses and protocol number assignments for North America. Its website offers some valuable reference tools, such as the ability to look up port numbers, view information related to top-level domain names, and browse companion sites to find and view RFCs.