Lab 7: Import a DNS/HTTP Errors Profile

Once you've created that fabulous profile that detects various types of HTTP or DNS problems perhaps, consider installing that profile on your other Wireshark systems. Since Wireshark bases profiles on text files, this is a simple process.

- Step 1:Visit www.wiresharkbook.com and download the sample profile
(httpdnsprofile101v2.zip). This new profile's directory and contents are zipped
into a single file.
- **Step 2**: Select **Help | About Wireshark | Folders**. Double-click on your personal configuration folder to examine the directory structure.
- **Step 3**: As mentioned earlier, Wireshark creates a *profiles* directory when you build your first custom profile (as you did in Lab 6). If you do not see a *profiles* directory at this point, you can manually create one or return to and complete Lab 6. Open the *profiles* directory.



- **Step 4**: Extract the *httpdnsprofile101v2.zip* file contents into this *profiles* directory. You should see a new directory called *HTTP-DNS_Errors*. Look inside this new directory to see the Wireshark configuration files included in this profile.
- **Step 5**: Return to Wireshark and click on the **Profile** column on the Status Bar. You should see the new profile listed. Click on the *HTTP-DNS_Errors* profile to examine this new profile.



86 Chapter 1 Skills: Work with Key Wireshark Elements

Step 6: Open *dns-nmap101.pcapng* while working in your *HTTP-DNS_Errors* profile. You should see some interesting colors in the trace file and two new buttons in the display filter area.

🛓 dns-nmap101.pcapng – 🗆 🗙							
<u>File</u>	lit <u>V</u> iew <u>G</u> o	<u>Capture</u> <u>Analyz</u>	e <u>S</u> tatistics Tel	ephony	<u>W</u> ireless <u>T</u> o	ools <u>H</u> elp	
		X G 9 @	***			H	
Apply a dsplay filter < Ctrl-/> Expression HTTP Errors DNS Errors							
No.	Time	Source	Destination	Protocol	Length	Info	
□ 1	0.000000	192.168.0	192.168.0	DNS	72	Standard query 0xa570 A www.nmap.org	
2	0.999676	192.168.0	192.168.0	DNS	72	Standard query 0xa570 A www.nmap.org	
3	1.999677	192.168.0	192.168.0	DNS	72	Standard guery 0x2570 A way amon ong	
4	3.999680	192.168.0	192.168.0	DNS	72	Standard query 0xa570 A www.nmap.org	
5	5.095538	192.168.0	192.168.0	DNS	7	Standard query response 0xa570 Server failure A www.	
6	5.095541	68.87.76	192.168.0	DNS	72	Standard query response 0xa570 Server failure A ww	
- 7	6.047552	192.168.0	192.168.0	DNS	72	Standard query response 0xa570 Server failure A ww	
8	6.047555	68.87.78	192.168.0	DNS	72	Standard query response 0xa570 Server failure A	
9	21.8254	192.168.0	192.168.0	DNS	76	and guery 0x8b73 A d.getdropbox.com	
10	21.8375	192.168.0	192.168.0	DNS	92	Standard query response 0x0075 A d.getdropbox.com	
11	43.1673	192.168.0	192.168.0	DNS	75	Standard query 0x66fd A mail.google.com	
12	43.2165	192.168.0	192.168.0	DNS	166	Standard query response 0x66fd A mail.google.com C	
13	44.0130	192.168.0	192.168.0	DNS	76	Standard query 0x654a A www.insecure.org	
14	45.0127	192.168.0	192.168.0	DNS	76	Standard query 0x654a A www.insecure.org	
15	46.0127	192.168.0	192.168.0	DNS	76	Standard query 0x654a A www.insecure.org	
16	48.0126	192.168.0	192.168.0	DNS	76	Standard query 0x654a A www.insecure.org	
17	49.0265	192.168.0	192.168.0	DNS	76	Standard query response 0x654a Server failure A ww	
18	49.0265	68.87.76	192.168.0	DNS	76	Standard query response 0x654a Server failure A www.	
19	49.0547	192.168.0	192.168.0	DNS	84	Stondard query 0x9cd0 A ratings-wrs.symanter	
0 2					Packets: 24 ·	Displayed: 24 (100.0%) · Load time: 0:0.1 Profile: HTTP-DNS_Errors	

Step 7:LAB CLEAN-UPClick the Profile column on the Status Bar and select yourwireshark101profile. You will continue to enhance the wireshark101profile inupcoming chapters of this book.

Remember that profiles are simply a collection of configuration text files. It is easy to move single elements of a profile or entire profiles to other machines. If you work with a troubleshooting team, consider creating common Wireshark profiles that the entire team can use.

🖲 TIP

Some configuration text files, such as the *recent* configuration file, contain directory paths. This may generate Wireshark startup errors when you move these types of configuration files to another system that does not have the same directory paths in place. You could either avoid moving these files to another system or edit the relevant configuration files to match the directory structure of the target system.