10 Cool Things You Should Know How to Do with Wireshark
June 16, 2010

Laura Chappell
Founder  |  Chappell University/Wireshark University

SHARKFEST ‘10
Stanford University
June 14-17, 2010
What’s Up These Days?

• Translations of Wireshark Network Analysis
• Wireshark Certified Network Analyst Exam Release
• Wireshark Certification Official Exam Prep Guide
• Wireshark Certification Bootcamps
• Oh yeah… and this little “Microsoft project”
Skills to Master

1. **Perform Local/Remote Capture Like a Pro**
   
   Locate most active interface
   Test your interfaces (see video at wiresharkbook.com)
   Use `rpcapd.exe` for remote capture

2. **WLAN Graphing (Get a Wi-Spy Adapter now... Just do it!)**
   
   Graphing 802.11 retries (`wlan.fc.retry == 1`)

3. **VoIP Playback**
   
   Look for jitter, packet loss and errors
Skills to Master

4. **Create Sexy Hot Profiles**
   - Free profiles online at wiresharkbook.com
   - Video on copying in profile info at wiresharkbook.com

5. **Recognize Malicious Traffic Patterns**
   - Have a baseline ready
   - Know scanning/discovery signs
   - Colorize questionable traffic

6. **Analyze an Application**
   - What is the process?
Skills to Master

6. Command-line statistical reporting
   Using Tshark effectively

7. Perform QoS Comparisons

8. Compare subnet performance
   Same as #7, but use subnet filters such as ip.addr==10.2.0.0/16
9. **Add Columns Fast!**

Available with version. 1.4.0rc1

Right click on any field and select **Apply as Column**

Right click column headings to align, rename and more (yes – you can left-align the No. column!)
Skills to Master

10. Build Your “Exclusion Filter of Death”

ip.addr==192.168.0.106 && !srvloc && !dns && !ip.addr==74.6.114.56 && !ip.addr==239.255.255.250 && !ip.addr==96.17.0.0/16 && !ip.addr==192.168.0.102 && !smb && !nbns && !ip.addr==192.168.0.103 && !ip.addr==64.74.80.187 && !ip.addr==83.150.67.33 && !ip.addr==67.217.0.0/16 && !ip.addr==66.102.7.101 && !ip.addr==216.115.0.0/16 && !ip.addr==216.219.0.0/16 && !ip.addr==69.90.30.72


See “Google over SSL” Analysis at www.wiresharkbook.com/coffee
Let’s Go Play with Wireshark

- Profile Stuff
- Application Analysis Stuff
- Advanced IO Graphing Stuff
- Whatever else comes to mind...
Remote Capture with Rpcapd.exe
Graphing WLAN Retries

(wlan.fc.retry==1) && (wlan.sa==00:24:b2:1f:27:f9)
Try Application Analysis Yourself!

- Launch First Instance of Wireshark
- Clear DNS and browsing cache (ipconfig /flushdns)
  - Start capture
  - http://sharepoint.microsoft.com/?wax=off
  - Stop capture
- Launch Second Instance of Wireshark
- Clear DNS and browsing cache (ipconfig /flushdns)
  - Start capture
  - http://sharepoint.microsoft.com/?wax=on
  - Stop capture

Capture on your local host while running Wireshark and connecting to the site.
### Compare Conversations (Time Values)

<table>
<thead>
<tr>
<th>Statistic</th>
<th>Optimize</th>
<th></th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Off</td>
<td>On</td>
<td></td>
</tr>
<tr>
<td>Time to Load Page Plus Links (secs)</td>
<td>6.91</td>
<td>5.33</td>
<td>24.30% faster launch</td>
</tr>
<tr>
<td>Packets to Load Page Plus Links</td>
<td>2,180</td>
<td>1,651</td>
<td>22.90% fewer packets</td>
</tr>
<tr>
<td>Bytes to Load Page Plus Links</td>
<td>1,779,036</td>
<td>1,468,861</td>
<td>17.44% fewer bytes</td>
</tr>
<tr>
<td>HTTP GET Requests</td>
<td>90</td>
<td>34</td>
<td>62.22% fewer GETs</td>
</tr>
</tbody>
</table>
VoIP Analysis and Playback

- Telephony | VoIP Calls | [select call] | Player | Decode [Check conversation(s)] | Play
Malicious Traffic Detection

- Baseline, baseline, baseline
## Tshark Command-Line Statistics

From Wireshark Network Analysis

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-z &lt;statistics&gt;</code> Examples</td>
<td>Display protocol hierarchy statistics as seen in Figure 36/7</td>
</tr>
<tr>
<td><code>tshark -qz io,phs</code></td>
<td>Display IO statistics for IP, UDP and TCP traffic at 10 second intervals</td>
</tr>
<tr>
<td><code>tshark -qz conv,eth -z conv,ip</code></td>
<td>Display Ethernet, IP and TCP conversation statistics</td>
</tr>
<tr>
<td><code>-z conv,tcp</code></td>
<td>Display Ethernet, IP and TCP conversation statistics</td>
</tr>
<tr>
<td><code>tshark -qz conv,eth -z conv,ip</code></td>
<td>Display IO statistics for IP, UDP and TCP traffic at 10 second intervals</td>
</tr>
<tr>
<td><code>-z conv,tcp</code></td>
<td>Display IO statistics for IP, UDP and TCP traffic at 10 second intervals</td>
</tr>
<tr>
<td><code>tshark -qz io,stat,10,ip,udp,tcp</code></td>
<td>Displays IO statistics for ICMP traffic at 5 second intervals—all traffic is saved to a trace file called allpkts.pcap (Note the filter used for ICMP is not applied to the traffic captured—to apply this filter to the traffic captured, use the <code>-f</code> parameter)</td>
</tr>
<tr>
<td><code>tshark -z io,stat,5,icmp</code></td>
<td>Displays IO statistics for ICMP traffic at 5 second intervals—all traffic is saved to a trace file called allpkts.pcap (Note the filter used for ICMP is not applied to the traffic captured—to apply this filter to the traffic captured, use the <code>-f</code> parameter)</td>
</tr>
</tbody>
</table>
Tshark Command-Line

• tshark -i 3 -qz conv,eth -z conv,ip -z conv,tcp

- i 3
  Capture on the 3rd interface listed by tshark -D

- qz conv,eth
  Don’t show packets (-q), but capture Ethernet conversation statistics

- z conv,ip
  Only use -q once. Capture IP conversation statistics

- z conv,tcp
  Only use -q once. Capture TCP conversation statistics
Keep Up with Me

- **Twitter** - www.twitter.com/laurachappell
- **Newsletter** (chappellU.com)
- **Wireshark Weekly Tips** (wiresharktraining.com)
- **Free Wireshark Webinars** (chappellU.com)
- **Microsoft Project** -
  [http://facebook.com/MVPress](http://facebook.com/MVPress) - Search for post “Laura Needs Your Help” and reply with your ideas and suggestions