Notes:

Wireshark Jumpstart: Wireshark 101

www.chappellseminars.com

Presenter: Laura Chappell, Founder of Chappell University and Wireshark University
laura@chappellu.com
Follow me: www.twitter.com/LauraChappell

The phone rings… multiple lines at one time… never a good sign. The users are complaining about network performance… again. They never call to say the network is doing great today – they don’t remember the numerous days when the network supported their every whim. No. They only call to complain. Being an IT support person is a thankless job.

In this live online seminar, Laura Chappell explains and demonstrates the key tasks using Wireshark, the world’s most popular network analyzer.
Notes:

I have lots of resources online:

- Follow me on Twitter (laurachappell)
- Check out the Wireshark Weekly Tips (www.wiresharktraining.com/tips.html)
- Watch some of the videos I uploaded to SecurityTube.net
- My blog is over at lcuportal.com
- The Laura’s Lab Kit v10 is over at lcuportal.com as well

Check out the other online seminars and keep learning... even if it is an hour at a time. The schedule is online at www.chappellu.com/schedule.html.
Notes:

These are the areas we will discuss in today’s seminar.

- What is Wireshark? I’ll show you a diagram of the elements of Wireshark.
- Placing the Analyzer. Do this right and save yourself loads of time.
- Capture and Display Filters. Focus on specific types of traffic.
- Spotting Problems. Let the Expert Info Composite window guide you.
- Basic Traffic Graphs: a picture is worth a thousand packets!
- Q & A. I’ll get to as many questions as time permits.

So let’s get started.
Notes:

Too often I am called onsite to troubleshoot a network after everyone has pulled their hair out. It boggles the mind. Why didn’t these people put an analyzer on the network and look at the traffic?

The packets never lie!

Wireshark is a FIRST RESPONDER tool. Network slow? Get the trace! Can’t connect? Get the trace! System behaving strangely? Get the trace!

Network analysis can always tell you WHERE the problem is, but it cannot always tell you WHY the problem is happening.
Notes:

These are some of the cool new features available in the Wireshark 1.4.0 version.

If you are an All Access Pass member, a video on these functions is available at lcuportal.com. If you need more information on the All Access Pass, visit lcuportal.com.

TIP:
My favorite simple addition to Wireshark v1.4.0 is the right click Apply As Column! Try it. Open a trace file containing a web browsing session. Expand a TCP header and right click on the Sequence Number field. Choose Apply As Column. You now have a Sequence Number column in the Packet List pane.
I often add a tcp.window_size column based on the TCP Window Size field (not visible in the first packet of the handshake currently) and TCP Sequence Number and Acknowledgment Number fields.
Notes:

When you are capturing traffic off the network using Wireshark, you are likely using one of three possible drivers.

**WinPcap driver**  
Used on Windows hosts running Wireshark.

**AirPcap driver**  
Used to capture WLAN traffic on a Windows host. The AirPcap adapter is available from CACE Technologies [www.cacetech.com](http://www.cacetech.com) – which was purchased by Riverbed in November 2010. I often run three AirPcap adapters on my system and set each to listen to a different WLAN channel. Capturing with the AirPcap aggregating driver allows me to capture on all these different channels at one time.

**Libpcap driver**  
Used to capture traffic on a *nix host.

The first filter applied is the Capture filter. If you apply a capture filter for all broadcast traffic, that is what will be passed up to the capture engine. You can’t go back and get packets that were filtered out from view using capture filters, so use these sparingly.
Notes:

You do not need WinPcap, AirPcap or Libpcap in order to open up trace files. Those drivers are used to capture traffic on the network.

When you open a trace file, you are using the wiretap library which supports numerous trace file formats including trace file formats used by Network General Sniffer, Wildpackets OmniPeek, Snoop and more.

Select File > Open and click the down arrow to the right of File Type to see the list of recognized file types.
Notes:

Dissectors, plugins and display filters are applied once the packets are passed up either by the capture engine or the wiretap library into the core engine.

Dissectors/plugins interpret the contents of the packet and are a key component of Wireshark enabling you to ‘read’ packets and see interpreted fields.

The display filters enable you to select which packets to view based on specific criteria that you define. Display filters do not affect the trace file itself – they only affect which packets you view.

The GIMP ToolKit (commonly referred to as GTK+) provides the graphical interface for Wireshark. GTK+ was initially developed for and used by GIMP, the GNU Image Manipulation Program. It is used by a large number of applications including the GNU project’s GNOME desktop.

Select Help > About Wireshark > Folders to find where the various Wireshark files are located. Starting in Wireshark v1.2, the locations listed are hyperlinked so you can quickly open folders.
Key Tasks

- Place the analyzer appropriately
- Create network baselines
- Filter on specific conversations or types of traffic
- Look for “hot” problems
- Create key graphs

Notes:

**Place the Analyzer Appropriately:** Switched networks can cause the analyst grief — blocking the traffic from easy view. We’ll go through four ways to capture wired network traffic and a few ways to capture WLAN traffic next. Hey — if you can’t see the packets, you are blind to the problem.

**Create Baselines:** Baselines are sample trace files of traffic when life was good... this will be on your ‘To Do’ list if not.

**Filter on Specific Conversations or Types of Traffic:** If Fred is complaining about his web browsing speeds you could start with a filter on just Fred’s HTTP/HTTPS traffic.

**Look for “Hot” Problems:** Pay attention to Wireshark’s Expert Info Composite information.

**Create Key Graphs:** A picture is worth a thousands words. In this case, an IO graph is worth a thousand packets.
Notes:

Unless you are the IT slave at an old school that still supports hubs, you are likely working in a switched environment.

Love ‘em or hate ‘em, switches are necessary network traffic cops. From the analyst’s perspective, however, they reduce visibility by limiting the forwarding traffic of traffic from unnecessary paths or segments.

Switches forward four types of packets by default:

- Broadcasts (MAC-layer broadcasts)
- Multicasts (MAC-layer multicasts) – if configured to do so
- Traffic to/from the connected host’s MAC address
- Traffic to unknown MAC addresses (I hope you never see this)

We’d be blind to Fred’s traffic to the server if we placed the analyzer off the switch as shown in the graphic.

So what can we do... what CAN we do?!
Notes:
The first thing we can do (although one of my least-desired options) is just run Wireshark off Fred’s machine.

Yeah... it’s an easy solution, but filled with risks... we typically don’t want to alter the system that is having problems. Network analysis is a passive, non-invasive process. I often compare it to an x-ray machine – “oh look... your foot is broken in two places... no more Dancing with the Stars for you!” Imagine if the x-ray machine was embedded in your foot to find the problem – ouch.

I also detest the idea of showing Fred that his system can run Wireshark. Fred is, after all, the “User from Hell” and in this case, ignorance is bliss... his ignorance is my bliss.

But... sometimes that is the only feasible option. Start Wireshark running in the background (maybe with a nice ring buffer – we’ll discuss that later in this class) and tell Fred to ‘do his stuff’ and show you what he’s experiencing.

Be sure to uninstall Wireshark afterwards!
Notes:

This option only works on half-duplex networks.

A stinkin’ old hub can save your hide!

*Hubs are stupid...* all they know are 1s and 0s and they forward every bit in every direction (except back they way the bits came in). By placing a hub along the path between Fred and the switch and plugging my analyzer into the hub, I get to see all Fred’s traffic.

Watch out for those 10/100/1000 hubs though. If you have a speed mismatch on the connecting devices that hub may act as a switch between the different speed devices.

Test this first before you need it. Connect two hosts and your analyzer to a hub. Make sure you can see the devices pinging each other. There are a lot of ‘hubs’ that are cross-dressers – they are actually switches. There’s no truth in advertising these days (especially in the tech world).
Notes:

If you are working on a full-duplex network, a hub ain’t gonna cut the mustard (aka “won’t work” for my international attendees). To tap into a full-duplex network, you’ll need a full-duplex tap. Simply connect it up just as you did the hub and away you go! Uh... except for one thing... There are many variations of full-duplex tap out there. The main differentiator is, of course, speed (10/100/1000) and port type (copper/fiber). Past that, you also have non-aggregating taps and aggregating taps.

Non-Aggregating Taps
These taps have two output ports and do not combine the full-duplex streams in each direction. You need to hang two analyzers off these taps to see bi-directional communication. Use File > Merge or the command-line mergecap utility to combine multiple trace files.

Aggregating Taps
Well worth the money. These taps combine the bi-directional data and forward it out one monitor port (or two if you have a regenerating that and want to place something else – maybe a Snort box – off the extra port).
Tapping in vs. Spanning Whitepaper

www.netoptics.com
Resources > Whitepapers

Hints for the Enterprise
Install multiple taps
Install your taps BEFORE you need them
Set up taps in front of your critical servers
Test the capture process

12/21/2011 (c) Chappell University 2011 chappellu.com

Notes:
This is the whitepaper that I refer to in the class – it’s very well written and helps differentiate between using a tap to capture your traffic or spanning a switch port.

Best Practices Guide
- Basic best practices
- Types of taps – aggregating, regenerating taps, link aggregation taps, etc.
- Advance best practices

Sites: lcuportal.com - chappellu.com - wiresharkbook.com - wiresharktraining.com
Notes:

Easy, eh?

Port A connects to the switch. Port B connects to the target. Port C connects to your analyzer.

There are a lot of variations possible when you’re looking for a tap.

Hmmm... but what’s the chance a company is going to let me disconnect their server from the network to install my full-duplex tap? Not likely... so that’s when I go the next route...
Notes:

Non-manageable switches are great for home networks – they DO NOT, however, belong on the corporate network.

All of your switches should have the ability to do port spanning (aka port mirroring). Port spanning enables you to have a copy of all network traffic flowing from another switch port down your switch port. It’s relatively passive, but not totally passive as you did reconfigure the switch – and... if the switch is the problem, such reconfiguration may ‘solve the problem’ or give the switch enough of a kick in the behind to get it working properly... most likely only until you have critical network traffic again – then it will fail again.

*DON’T GET ME STARTED* on ‘port sampling’. What good is it to see only a piece of an x-ray result? Aargh!

Make sure you test out your spanning commands and ensure your switch spans ports properly. Even the highest and mightiest of switch manufacturers seems to have stumbled from time to time in implementing this necessary feature.
Notes:

Ok… here’s the scoop. You can just select your wireless adapter to begin monitoring traffic – it most likely will let you see your traffic. But… uh… what about Fred’s traffic? Most NICs won’t go into full monitor mode and allow you to see other folk’s traffic.

This is where a Windows host has an advantage (amazing to hear myself say that...). Riverbed (who purchased CACE Technologies), where Gerald Combs, creator of Wireshark, and Loris Degioanni and Gianluca Varenni, creators of WinPcap, work, has AirPcap adapters.

These three AirPcap adapters should be connected to your system via USB hub most likely. With the AirPcap aggregating driver you can now see all the traffic on three channels simultaneously. Just too cool. Riverbed (who purchased CACE) also has WiFi Pilot. Megageek’s Wi-Spy adapter offers spread spectrum analysis (I demonstrate this adapter live in the “Top 10 Reasons Your Network is Slow” class – check it out).

TIP:
See the free video, Start the Day by Testing Your Network Adapter, at www.wiresharkbook.com/coffee. You’ll see me testing two WLAN adapters to see if they will work for capturing traffic. Your WLAN adapters should run in both promiscuous mode and monitor mode for best results.
Key Wireshark Functions

Choosing the Interface
Capture Filtering
Capturing to File Sets
Capturing with a Ring Buffer
Altering the Time Column
Display Filtering (new auto-complete)
Using the Expert Info Composite
Defining Profiles
Reassembling Streams

Notes:

These are the functions that I consider key when you are analyzing networks:

- Choosing the Interface
- Capture Filtering
- Capturing to File Sets
- Capturing with a Ring Buffer
- Altering the Time Column
- Display Filtering (new auto-complete)
- Using the Expert Info Composite
- Defining Profiles
- Reassembling Streams

I will cut down the time spent on slides so I can get into the demo process a.s.a.p. in this training.
Notes:

You have many options when starting your capture.

You could just capture a single file and (a) manually stop the capture or (b) set a stop trigger.

You could capture a file set that you (a) manually stop or (b) stops based on a trigger.

To control the number of trace files created you can use a ring buffer which is a FIFO (first in, first out) buffer.

**Triggers for Multiple Files**
Next file every x kilobytes, megabytes, gigabytes (careful of file size)
Next file every x seconds, minutes, hours, days (again... watch the size)
Ring buffer with x files
Stop capture after x files

**Stop Triggers**
... after x packets
... after x kilobytes, megabytes, gigabytes (you know the warning)
...after x seconds, minutes, hours, days (yup... same thing)
Notes:

Here are some of the things to know:

**Examining the Interfaces**
Select Capture > Interfaces to see the active interfaces and check out the interface details, start capturing right away or set up your capture options.

**Capture Filters**
Make a ‘Not Me’ capture filter to filter out your traffic from your trace files. You don’t want your email or web browsing session to be captured when you are working on Fred’s network problems. The syntax for a “Not Me” capture filter is `not ether host 00:21:97:40:74:d2` (with your MAC address).

**Set the Time Correctly**
Use Edit > Time Display Format > Seconds Since Previous Displayed Packet to see the delta time from the end of one packet to the end of the next. Now you can sort the time column to see large gaps in time!

**Listen to the Expert**
Select Analyze > Expert Info Composite to identify possible problems seen in the trace file. Expand the findings to locate specific packets in the trace.

**Check the IO Rate**
Select Statistics > IO Graph to note when the IO rate drops. Click anywhere on the IO graph to locate that area in the trace.
Notes:

Here are some of the things I’m going to demonstrate (continued):

**Measure Pain**
Learn to measure time between packets spread throughout the trace. Select the start point and right click. Choose Set Time Reference (toggle). You might be prompted for the time format change. Scroll down to the next time measurement and the time column now shows you the time from the Time Referenced packet to this one. You can set multiple Time Reference packets in the trace if desired.

**Right-Click Filtering**
In my example, I want to find out if the trace includes BOTH the original and the retransmitted TCP packet (find a retransmission packet). Inside the TCP header, I right clicked the TCP Sequence Number field and said Prepare as a Filter (just so I can look at the filter before it gets applied). When you apply the filter I will learn if I am upstream (before packet loss occurs) or downstream (after packet loss has occurred) on the network.

**Custom Columns**
Time permitting I also wanted to show you how to add a column for the TCP Window Size field value to Wireshark’s summary pane. Click the field to see the field name in the status bar at the bottom of the Wireshark window. This field is called tcp.window_size. I showed the right click Apply as Column feature!
## Your “To Do” List

1. C’mon... update to the current version of Wireshark! Try Wireshark version 1.7.x!
2. Test analyzer placement
3. Baseline your network traffic
4. Learn to filter (capture AND display)
5. Don’t ignore the Expert Info
6. Learn TCP/IP at packet level
7. Get the *Wireshark Network Analysis* book!
8. Study for the certification!

---

### Notes:

Now what?! Here’s a quick list of ‘to do’ items for you after this class.

1. C’mon... *try* the new version! Get to www.wireshark.org and update to the latest version of Wireshark.

2. Test analyzer placement: Make sure you feel comfortable with your capture options – hubbing out, tapping out, WLAN AirPcaps, spanning, etc.

3. Baseline your network traffic: Know what’s normal. Take baselines of host startup processes, connection to the key network devices, shutdown, etc.

4. Learn to filter (capture AND display): Work with both types of filters. Become a filter guru to save yourself loads of time when analyzing network problems.

5. Don’t ignore the Expert Info: Always give a nod to the Expert Info Composite findings – verify the alerts listed by looking at the trace in-depth.

6. Learn TCP/IP at packet level: Installing and configuring a TCP/IP network is entirely different from analyzing the traffic. Get to know TCP/IP inside and out – that includes ARP, IP, TCP, UDP, DHCP, ICMP, HTTP, POP, SMTP, etc. Check out the three trace analysis courses in the All Access Pass (lcuportal.com).


---

Sites: lcuportal.com - chappellu.com - wiresharkbook.com - wiresharktraining.com
Now we move on to live Q & A.

Remember to follow me on Twitter (laurachappell) and check out my blog at www.lcuportal.com.

Check out the other online seminars and keep learning... even if it is an hour at a time.

The All Access Pass includes trace file analysis training, Wireshark training and more. Here’s a partial list of courses online at lcuportal.com:

- AAP Event: Analyzing the Window Zero Condition
- Core 1: Wireshark Functionality and TCP/IP Analysis
- Core 2: Troubleshoot/Secure Networks with Wireshark
- CS42: Hacked Hosts
- CS43: Analyze and Improve Throughput
- CS44: Top 10 Reasons Your Network is Slow
- CS47 Nmap Network Scanning 101
- CS58: Packet Crafting to Test Firewalls
- CS61: Tshark Command-Line Capture
Thank You for Attending this Online Course

For sample trace files, videos and configuration files, visit wiresharkbook.com

(c) Chappell University 2011

Notes:

Well... thanks much for attending the online live seminar.

You can help us guide the content, length, pricing and format of these courses by sending your thoughts to me at laura@chappellU.com.

Now I ask a favor...

*Please* help us reach out to the IT community to let them know about these online seminars.