RUNAS RADIO

http://www.runasradio.com

RunAs Radio is a weekly Internet Audio Talk Show for IT Professionals working with Microsoft products. The full range of IT topics is covered from a Microsoft-centric viewpoint.

Text Transcript of Show #160
(Transcription services provided by PWOP Productions)

Laura Chappell Wires Sharks!
May 19, 2010

[Music]

Brandon Wenn: From runasradio.com, you're listening to RunAs Radio, the Internet audio talk show for IT professionals with Richard Campbell and Greg Hughes. This is Brandon Wenn, announcing show #160, with guest Laura Chappell, recorded Friday, May 14, 2010. RunAs Radio is produced each week by PWOP Productions, providing professional media and podcasting services online at pwop.com. You can follow the boys on Twitter at twitter.com/runasradio.

Richard Campbell: Thank you very much, Brandon. This is Richard Campbell and with me as always, my co-host, Greg Hughes.

Greg Hughes: Hey, Richard. What's going on?

Richard Campbell: Ah, you know spring is in the air. The barbeque is up and running and all the important things are happening.

Greg Hughes: Yeah. I mean, the last couple of days here have just been beautiful. It's like everything is just -- you know, you hit those first couple of days where you realize it's really and truly have come.

Richard Campbell: Yeah, finally the dark times are over and I feel dumb for working in my office all the time.

Greg Hughes: Yeah.

Richard Campbell: But I'm still virtualizing out my own rack bit-by-bit, shutting down all the old hardware and getting everything into a pair of big servers so that I can simplify my network.

Greg Hughes: Cool. Well, it seems to be the way of things.

Richard Campbell: Yes. Systems Center Virtual Machine Manager is my friend.

Greg Hughes: Well, cool. Very good.

Richard Campbell: Yeah, it's all good. Let us dive right in. We've got a funny show today, I'm really looking forward to it. Here, let me introduce our guest. Laura Chappell is the Founder of the Wireshark University and Chappell University and has been analyzing network traffic for 20 years now (yes, she has grey hairs!). She is a top rated speaker at numerous industry conferences including Microsoft's TechEd conference and various law enforcement conferences. She is a voting member of the IEEE and an active member of the High Technology Crime Investigation Association. In March, Laura released the ultimate 800-page book on network analysis using Wireshark and is finalizing the upcoming Wireshark Certified Network Analyst exam for release by the end of the second quarter of 2010. She has two teenage kids, can't cook without a fire extinguisher and is thankful that she can order in. Welcome, Laura.

Greg Hughes: Hey, Laura.

Laura Chappell: Well, thanks very much. It's great to join both you and Greg this morning.

Richard Campbell: Now I remember when Wireshark was ethereal.

Laura Chappell: You have gray hairs also then.

Richard Campbell: Yeah.

Laura Chappell: That's what they told me.

Richard Campbell: Yeah, yeah and I remember having to adjust the programming on switches to be able to use ethereal properly like to, oh boy, I get chills just thinking about that.

Laura Chappell: Yeah. You know, interestingly enough there are still folks working with those same switches and working as hard as they can. They've got the standing and the mirroring working right so they get the traffic. But you know, it's been a great place to be for the last 20 years. Analysis is never boring so hopefully I'll fill you in on some really cool stuff today.

Richard Campbell: So, we'd better take a step all the way back. For the folks that are out there that have not used Wireshark, what's it about?

Laura Chappell: Wireshark is, in the simplest terms, it's a sniffing tool. You load it on your own machine and you can sniff your own traffic. In that way you could see how applications are running. You might be able to see if you have some background traffic that might be a phone home, traffic from some application and you could see why your network communications might be slow. So in its very essence, it is a packet-the-thing tool and it's used primarily for troubleshooting, security, optimization by looking at the network. It's the X-ray machine for network communication.

Richard Campbell: Now the biggest problem I see most people have with this is that it's actually an over abundance of data that when you actually look at the raw stream coming out of the network, it's so much stuff. How do you sort it all out?

Laura Chappell: Ah. You know, that's the needle-in-the-haystack problem that we always talk about because people that are getting new into network analysis, they know they can go to wireshark.org and they can download this free open

source tool. They load it on their system, they fire up their machine, and then they log in, and then they web browse, and then they do this, then they do that, and then they look at the traffic and they throw up and decide I can't do this and they shut it down because it's just an overload. So much of that can be helped by realizing that when you're going to analyze communications, you need to separate it out. You need to really focus in one thing. So if you want to understand what your login process looks like, you begin the analysis process then you log in and then you stop the analysis process and you look at just that one section of your communications. When you're starting out just to sort of piecemeal it, you know, start Wireshark going and then browse to a website and then stop Wireshark, you'll be able to see exactly what it took to get to that website and then as you become more and more familiar with your typical communications from the types of things you do, you can look at a big, fat trace now with this huge spaghetti message of communication and you could really begin to separate it out by saying, "Oh, okay, I recognize that. That's my virus detection tool doing its update. I've seen that before. Oh, look, that's what it looks like when I log in. I recognize that. Oh, that's me going to this website." The other thing is when people are starting out, get used to the idea of running Wireshark on your own system and don't go into like the middle of the infrastructure and say "I want to capture all the traffic on the whole entire network, as much as I can feed into my system."

Greg Hughes: Sure.

Laura Chappell: You know, it's a typical thing people do because they're just, ah, their eyes are open, they want to see it all and so they start capturing it all and the next thing they've got, you know, 780 gigs of packets and they lost all their social life, they have no sense of humor. It's just awful and you just see them being so overwhelmed when it's really it's very logic -- communications are so logical, the best way to start is start grabbing your own traffic and just browse to a website. You'll see your TCP handshake, and then you'll see the get request, and then you'll see the response and it's just very logical but taking it piece-by-piece so you don't hit that big haystack issue is so important to keep going with this.

Richard Campbell: So doesn't Wireshark help you sort out these chunks of data as well understand certain fingerprints of certain applications?

Laura Chappell: You know, it does. It has dissectors in it where it can break up traffic but it also has capture filters that allow you to say, "You know, I don't want to capture everything. I'm only interested in looking at the broadcast traffic that's coming from my workstation or the broadcast traffic that's coming down the switch." So I can say in Wireshark I can start up to say, okay, let's just look at the broadcast traffic right now. Or I can start up and say I'm really only interested in looking at the DHCP communications right now, or I just want to look at web browsing traffic. We can apply filters. We can apply filters before we capture traffic or if we did go get the big spaghetti mess, and I'll use an example here of working on a SharePoint network. Whoa, you talk about the ultimate spaghetti, multicolored spaghetti. It's unbelievable to see all the different ports and applications that are part of the full SharePoint implementation and you capture all this. One beautiful thing I love to use in Wireshark when I'm working in the SharePoint environment is you've got so many different TCP connections in SharePoint. You've got so many conversations going on that you can look at a conversation in Wireshark and you can right mouse click and say I want to colorize that. Let's colorize that with this light purple color. Oh, look. Okay, that conversation is now very distinct in my Wireshark screen. Oh, but look, there's another connection that's established right after. Well, let's change that to sort of a peach color. So we take something like a very complex communication that's a spaghetti type of thing and we can colorize the conversations, we can pull out a single conversation out of the whole entire spaghetti message and say I only want to focus on that. We can do all sorts of things to pull apart the spaghetti strand bit-by-bit to figure out, okay, which spaghetti strand is it that I'm having a problem with? Which one is really showing that? And then like you said, there are things in Wireshark where it can help you figure out where there are problems. So it has an expert notification system in it. So if somebody goes and captures a bunch of traffic, in the bottom left-hand corner of Wireshark there's this little brown button, it's a colored coded button, and if you click that a window pops up that says, "Hey, these are the areas I think that might be a problem. You have an X amount of packet lost, you have duplicate acknowledgement, you've got some retransmissions, you've got some systems that are advertising this zero window site which means don't talk to me. So we can go through and tell you, hey, pay attention to some of these things when you're working, some of these things might be a problem. So it has a lot of capabilities to help the new analyst and the experienced analysts when they're working with a lot of traffic.

Richard Campbell: So you typically attach Wireshark to a given NIC?

Laura Chappell: What you do is let's say I'm loading it on a laptop and typically people do load Wireshark on a laptop because it's a mobile process. We like to move around the network because ideally when Fred complains, you know every network has Fred, the user from hell, and Fred is going to complain, "Oh, it's really slow when I'm working today. I don't like it." We like to be as close to Fred as possible when we capture our traffic. So what we do is we load it on our laptop and Wireshark will list on the main start page on the left-hand side, it will show

you all the interfaces that it recognizes on your laptop and you could click on any one of those interfaces to start capturing on those interfaces whether they're wired or wireless. Now what you can out of wireless really depends on the capability of the driver and the card that you have in the wireless environment, but over on the Wireshark book website I did a video on testing your adapters to see what can I get in traffic with these adapters. This is how you test an adapter. So as long as Wireshark can see the adapter, it can capture traffic from that adapter. Whatever that adapter passes up, Wireshark will handle.

Richard Campbell: Right.

Laura Chappell: So we typically say get as close to Fred as you can and if you have to use a full duplex tap to listen on full duplex communication, that's one way to do it. Another is just to stand a port off of that switch, copy step to and from Freds workstation down to yours.

Richard Campbell: So I'm thinking now in terms of what I could do for wireless with this as well because when I think about troubled networks I usually think about wireless. Does Wireshark get into some of the channel conflicts and that sort of stuff?

Laura Chappell: Absolutely. You know, poor wireless. It gets such a bad mouth on this.

Richard Campbell: Well, I think it's just abused by so many people especially in the enterprise or sort of the SMB market where you think you can just buy yourself a little Linksys WRT54G, throw it in there, and handle a hundred laptops and wonder why it breaks down. Those little home units just haven't got the guts.

Laura Chappell: Yeah. You know what, they're just not there as -- we sort of shipped in the wireless environment too. We're very excited about it, and all of a sudden it was like, "Oh, this is simple. Just plug it in and it will work and that thing would be great."

Richard Campbell: Right.

Laura Chappell: And you know, in wireless, just like in the wired environment where we're blind to what's going on. That's the beauty of packet analysis, it allows us to see what's going on. So in the wireless environment, let's say I'm sitting at my window and I've got a Windows 7 box sitting here. I'm running 64-bit Windows 7. I can load Wireshark on that machine and the first thing I do on a new machine when I get it and I run Wireshark is I go ahead and I say to Wireshark, "Well, let's just capture on the wireless interface, my native wireless interface. Tell me what you can see." Now, a lot of wireless cards out there will be able to go into promiscuous mode which means I can listen to traffic going to other hardware addresses and that's great and that's what we use at the wired department. But the wireless world is a little different. We want a network adapter that will go into what we call monitor mode.

Richard Campbell: Uh-hmm.

Laura Chappell: And monitor mode means that when my adapter is at monitor mode, it will not join any service set. It will not be part of any wireless network which means that that card can pick up traffic on everybody's wireless network that I can see. Any wireless packets that are within range will be picked up. So most cards out there though will go into monitor mode and they're one of the things where you can talk to the card manufacturer and say, "Come on. Let's get a monitor mode driver for your card. Can't you do that?" They don't see the monitor advantage of just doing that. So the guy who created Wireshark is Gerald Combs and he created originally of course this ethereal. He works at a company called CACE Technologies and that's spelled CACE, CACE Technologies, and they have put out an adapter that's specifically made to work on Windows systems. It's called an AirPcap Adapter. It does not join any service set and while you're in Wireshark you can move from channel to channel to channel with that one adapter and capture all the traffic. It goes in the monitor mode and it goes to the promiscuous mode. It's well worth it. I have three of them hanging off of my machine so I can simultaneously listen to three channels at one time.

Richard Campbell: Which doesn't sound like a normal thing to do at all, Laura. What are you up to?

Laura Chappell: Well, you know, the thing is here we go to so many wireless networks where they're following the rules. They're network is running on Channel 1, 6, 11.

Richard Campbell: Right.

Laura Chappell: They've got three channels running simultaneously. For me when I'm doing analysis in their network and they're complaining about performance, I don't want to have to listen in on one channel and be blind to the other.

Richard Campbell: Right.

Laura Chappell: And then walk the floor and listen to Channel 6 and be blind to 1 and 11 and then go to the left. So what I do is I have all three adapters hanging off the USB hub and I start up Wireshark and I choose. Automatically when you have these three adapters going, you have a new option saying the AirPcap aggregator and that means you're going to capture all three at the same time.

Richard Campbell: Right.

Laura Chappell: And then with that filtering capability that we talked about earlier, you can then go in and say, okay, I'm going to sit and focus only on everything that happen on Channel 6 first. Let's just look at the Channel 6 traffic and you know what? It just saves me so much time rather than do a single channel analysis at a time. There's another product from the folks at MetaGeek if you're familiar with them, metageek.net, they have a wi-spy adapter and I use that to look at the RF signals around me. Before you even get to packet level, I want to know RF signals around me. Do we have any interference? Do we have any noise?

Richard Campbell: Right. Yeah, this is exactly the product I was looking for when you're talking about this because the biggest one was the leaky microwave oven. Everybody's network connection fails when somebody heats up a cup of coffee.

Laura Chappell: Yup, and you know, we even on doing the Wireshark book, when I got to the wireless chapter, you cannot focus just on the packets in the wireless world like you really can in the wired world.

Richard Campbell: Right.

Laura Chappell: In the wireless world, you've got to look for everything else other than what we see as 802.11 packet. So I put in a piece in there about how these MetaGeek adapters do what they do and then on the website, on wiresharkbook.com, I actually put my recordings up there so people can see what my Xbox looks like when I turn it on, what does my Uniden phone looks like when I turn it on, what does this microwave looks like and we did a microwave cook off last December where we went, we bought a bunch of microwave ovens and we told this company we were designing a house, and we threw popcorn in each one of those, popcorn bags in each one and we pops the popcorn in each one one at a time and then walked up to 50 feet away from the microwave to see how bad is this interference and is this going to hit us on only Channel 1, is this going to hit us on Channel 6, what are each of these microwaves doing. The most expensive microwave which I absolutely love, it's a beautiful microwave, turned out to be the most hideous on the wireless network. It was just nailing the signal and it went across every single channel.

Richard Campbell: Wow.

Laura Chappell: Oh, my gosh. Because a lot of times microwaves will kind of stay around the lower frequencies so you know that your local access point power will automatically be moved up to 6 or 11 and you'll be just fine when people heat up their coffee, but this thing nailed every single channel and I walked -- I had this long cord that I can get up to 50 feet away and I did not see any difference by walking 50 feet away. The signal was just so strong and you knew that this poor company I was at when we were testing this was like, oh, sorry, your wireless network is down right now. But this is a really good test.

Richard Campbell: Well, the biggest one for me is two or three access points of different offices all on the same floor, all on the same channel.

Laura Chappell: Yup, exactly and that's so common.

Richard Campbell: Right.

Laura Chappell: Gosh, I get to go to Vegas this Sunday to do some wireless work in some casinos which is fascinating because of a lot of the casino machines now are getting their programming through a wireless communication.

Richard Campbell: Right.

Laura Chappell: You know, at the drop of a billion dollar, they should be able to swap over their stats really fast. But what they're finding is these machines are not being updated in a timely enough fashion and these casinos are losing a lot of money. Well, we'll see what's happening with their wireless communications that I know I've been to this casino just a few months ago just to do a little prep work and what I saw was that every single access point in the entire casino is on the same channel.

Richard Campbell: Right.

Laura Chappell: Yeah.

Richard Campbell: And they're all wrestling with each other.

Laura Chappell: It's just total saturation, yup. And it's with the food service information. They've got lots of interference from -- you know those exit signs you have for the emergency exit?

Richard Campbell: Yeah.

Laura Chappell: They've got a lot of these exit signs where as you walk under the exit sign, you get this huge amount of noise that's coming straight down at you. It doesn't go to the site, it doesn't sort of stand up and straight down.

Richard Campbell: Interesting.

Laura Chappell: So it's kind of interesting as signals are passing underneath those, they're getting mangled.

Richard Campbell: Well, and the terrible thing about the wireless situation is anybody can poison it. You can architect everything flawlessly and

somebody wonders in with a jacked up access point and takes that channel out.

Laura Chappell: Yeah. You know, still to this day I don't care what anybody says, there's no such thing as a secure wireless network whether it's a malicious person coming in and bringing in a jamming tool. You can get great jamming tools in Germany, you know.

Richard Campbell: Yeah.

Laura Chappell: It's totally illegal but somebody can come in and jam your network or somebody can simply walk in with a $10 Uniden phone from Target and turn that thing on and walk through your floor and nail everyone of the lower frequencies or like you said, a lousy poorly configured access point, one that is just set for signal strengths as high as it can be and it just screams bloody murder and destroys the network communications. When we look at the packet level, what we see is, yeah, we could see the stack with the MetaGeek tool. We can see, oh, we've got this thing that is just showing us and as we walk around we could see the signal get stronger so we can tell where it is, we can move close to it. But when we get to the packet level, what we see if we never looked at the signal, what we see at the packet level is we see this one bit set in the frame control field which is the retry bit. It's not a TCP retransmission. We're talking about a tool level retransmission and there's a single bit. So on Wireshark, when I'm running on a wireless environment, I set this coloring system up so that every time a packet has the retry bit set, it's this bad, ugly orange background color. Orange to me is the color that just makes me want to reach. So for me, those are my big, important packets that come up. I'm streaming, I'm watching all the stuff flying by and when I start walking to an area where the packets are getting mangled, all of a sudden my packets are flying by and they become orange and then I walk away and they go back to their other colorizations, to the protocol, and then I walk closer and it's orange, orange, orange, orange so I know that right here I've got something that's mangling the packets and we have these retransmissions.

Richard Campbell: It's interesting, yeah.

Laura Chappell: It's fascinating. You know what? It's playing a game. It's all like playing a game and it's just a matter of figuring out the solution.

Richard Campbell: And a great tip about that retry bit because it's so difficult at packet level to realize the network is actually struggling, that the error rate is up and then these are repeatedly sent packets.

Laura Chappell: Oh, you know what? If I were working in a wireless environment and people are complaining, if I have the MetaGeek products I'm going to run those first and foremost just to get the whole idea of, okay, what kind of interference have I got? What kind of overlapping have I got? I want to know that first, then I go over to the packet level environment. Now for me, I use the Air Pickup Adapters and I know they can pick up all the traffic on any channel I want and then I see this close to the user that's complaining in the wireless environment. Same thing I thing I did in the wired environment, I'm going to sit as close to Fred as possible. I want to feel the pain from Fred's perspective, not from 30 feet away.

Richard Campbell: Right.

Laura Chappell: Yeah, and I'm not going to jack up my system with a big antenna because what if it doesn't have that big antenna. So I'm going to sit as close to Fred as I can possibly stand it and then I'm going to tell Fred, okay, go ahead and start working on the network and let me see your screen when you say your performance is bad because a lot of times users will say, well, the network is very slow and you find that a web page is not loading all of its ads because the browser is set not to load, allow those, or we know we filtered out skankywebsite.com.

Richard Campbell: Right.

Laura Chappell: You know, I like to see what is Fred feeling about all these and then once I've got a bunch of this traffic I'm watching and he says, okay, this is what I mean by slowness, I look at my screen and the first thing I'm looking for is do I see any orange here?

Richard Campbell: Yeah.

Laura Chappell: Do I see any orange at all? It's amazing how many times I could start looking at Fred going, okay, right now I bet you're feeling slowed down. He's like, ha, how do you know? Okay, this is it. Now when I start seeing those retries, the minute I see those retry bits are all set to one at one point, I'm going to go back to my MetaGeek products and I'm going to say, "Okay, what is happening right now?" You can run the two simultaneously too. What is happening right now on this channel that we are on? What happened? Did we suddenly get a blast or something? Or sometimes you'll just see that everybody starts getting on the network at the same time and of course you've got contention going on.

Richard Campbell: You know, we don't see this much anymore in the wired network. I think gigabyte has really obviated saturated Ethernet. But I remember in the 10Base-T days when you could bury a network and we go in with ethereal and you can see that there was an 80% point where the whole collision detection avoidance thing starts taking over the bandwidth.

Laura Chappell: Yeah. It's really the biggest thing that I think changed our world in the Ethernet environment, CSMA/CD, was when we went from half duplex to full duplex.

Richard Campbell: Right.

Laura Chappell: We used to spend a week talking to people about, oh, collisions, collision domain at the back of the algorithm and all these things because we're living in this half duplex environment and then all of a sudden when we went to full duplex it was like, hey, collisions can happen in the back plane of the switch but that doesn't happen very often. So suddenly it's like, oh, we really did just completely change our architecture and the performance difference. Even if we went from 10 megabit half duplex or 10 megabit full duplex, it was a noticeable difference and true put along...

Richard Campbell: Sure.

Laura Chappell: Then of course we go to a hundred, then we go to thousand and it's like wow.

Richard Campbell: Yeah and now we're talking...

Laura Chappell: And then we say now let's do wireless.

Richard Campbell: Yeah and it's such a shock as do we get back to those old problems. The only place that I'm seeing switches really strained is ebsites where we're still getting into where you're actually using a significant portion of the total bandwidth of a switch and you finally see that stress again. But I find in regular workstation environments, it's just not an issue. The machine is slower than the network now.

Laura Chappell: Absolutely. You know what? That's what we're finding. We're finding that the local systems that have not been updated forever are sitting there and they're getting bugged down or they're got older applications on their system. They're not pulling data out of the buffer fast enough. Our networks are flying fast and it's the endpoint to the problem, and then at TechEd I've got a session where I'm going to be talking about the death of a network. It's all this death of series. I'm going to be really finger pointing at one of the things that a lot of companies have done which is to upgrade their infrastructure devices to the point that they have killed their network. You know, when you say a switch, it should be almost wire speed forwarding. I mean, those things are fast.

Richard Campbell: Yeah.

Laura Chappell: They're layer two boxes. But then you sit there and you go, ah, but I was told if I change it to layer 3 a cross dressing switch, now I can do layer 3 communications. Oh, and not only that. It's got ideas, capabilities built into it. It's got QoS built into it and as they've been improving the level of sophistication in their infrastructure, what we're seeing is the performance level from the endpoint is really thinking. At TechEd I'm going to go through this one nightmare situation that companies have no idea that this is taking place right now unless they're looking at the packets. They're just seeing that things are starting to feel like they're getting a little bit slower. What you're seeing is you're seeing the TCP/IP stack that's been enhanced to the endpoint so, you know, I'm sitting on a Windows 7, sitting with Vista you know, I've got some capabilities that are now turned on by default.

Richard Campbell: Right.

Laura Chappell: That is what TCP can do. Well, these infrastructures in the center are saying "No, no, no, no, no. I'm not going to let you take advantage of that because I don't understand it, or I'm not set to using it, or I have bugs on it so as you go through me I'm just going to turn that off."

Richard Campbell: You're talking about the sliding MTO, aren't you?

Laura Chappell: Oh, part of it is that, yeah.

Richard Campbell: That was one of the meanest things Microsoft ever did. When that first shipped in Vista, there were all kinds of network devices that just blew up because they were fixed at 1534.

Greg Hughes: That was on the pro.

Laura Chappell: Yeah. Well, you've got that and you've also got Windows scaling being enabled at the end devices and you've got infrastructure devices that literally during the handshake will remove that option.

Richard Campbell: Yeah.

Laura Chappell: You suddenly look at a packet from a client that come all the way through this lovely infrastructure, the billion dollar infrastructure, and you look at the TCP option and all you see is "null apps, null apps, null apps, null apps." It's all null, it's all filled with null and you know that that's impossible. TCP doesn't allow you to have all these no's in a row so what was it at the beginning? And you find that you've got your Windows 7 box that had sent this packet out that says I want to do Windows scaling and I want to do selective acknowledgement and you have an infrastructure device in the middle that says "No, no, no, no, no. I'm going to strip all that out." They actually pick up the packet, open -- I mean, not only the IP header but they go into the TCP header of the handshake and say, "Ah, it's a handshake. I don't like these options. I will strip them out. I will recalculate. TCP had to checksum. I will send it to

IPE and checksum." Then on to the next network or whatever it is with a new header and move it on. It's just unbelievable the effect that it's having and it's just hideous that it's literally taking our improvements in TCP that have taken place over the last 6 to 10 years and it's bringing us back to where we were. We might as well go to a 10-megabit per second network because when you start doing high-through but you lose a packet, without this functionality you might as well be at 10 megabits per second because you're going to nail the network with unnecessary communication. It's just how it makes me soft there.

Richard Campbell: But you know, the other side of this is the IP. If we're going to play in the layer 3, we really need to start thinking IPv6 anyway because all our new machines have this stuff turned on by default.

Laura Chappell: That's right and I still go to customers where they've got IPv6 traffic flowing all over their network just because at the endpoint it's enabled by default.

Richard Campbell: Right.

Laura Chappell: But in their infrastructures, they're not using it at all.

Richard Campbell: No.

Laura Chappell: They're not using it so what you need to do is you need to make a decision and say, you know what? It's like the old IPX and TCP/IP world.

Richard Campbell: Yes.

Laura Chappell: You can go to companies and you say, oh, you migrated to TCP/IP, how come all your printers are spitting out IPX and SAP and all this garbage? No, no, no. You make a conscious decision to work on one platform or one protocol stack or the other protocol stack and when you're in one protocol stack environment and you begin the migration, you begin it section-by-section through your network. You don't just throw the whole thing out there and go to lunch and hope it will all work. You have to be in control of your network. Don't let your network take control of it. Companies don't just really know what's slowing through their network. If they could see all the garbage that's slowing through their network, the junks that are unnecessary, cleaning that up really helps. You can control this money into all these infrastructure devices and upgrades and this and that. Yeah, just clean the garbage off of there.

Richard Campbell: I mean this is one of the things I think Wireshark would do outstandingly well. It's just recognizing how much IPv6 traffic you have going across your network that you're basically unaware of.

Laura Chappell: Oh yeah. Oh yeah, absolutely. The other thing is it's so easy to make an IPv6 color filter. So let's say you want to make that a purple color. So as you're moving around whether on the wireless network or the wired network, you want to know where your concentration is of IPv6 traffic. It just cruises around the network and you'd be able to see it when it all comes up in this purple color. I really believe in colorization to bring things up to people. It makes it so much easier to work and see things really easily.

Richard Campbell: It sounds like that's the main thing with Wireshark. So what do we -- for folks who want to get involved with Wireshark, how do they get started?

Laura Chappell: All right. Well, first of all, Wireshark is open source. You can download it. You just simply go to wireshark.org and you'll see the little download button at the upper right-hand corner. You know, go grab it. Just download it. If you're on a Windows system, it will automatically install WinPcap which is the Windows Packet Capture driver for you. The installation is simple, simple, simple standard installation and then just bring it up and look at the interfaces that's sitting, click on one and say, well, let's just start capturing something and then do something simple. You know, web browse but realize that when you look at your traffic, just because you're only web browsing does not mean that you don't have a ton of other communication happening in the background.

Richard Campbell: Right.

Laura Chappell: You know, your browser is going to be going out checking the validity of certain sites or you've got your virus detection updating or you've got another process in the background. So notice this simple system only bring a browser up and then just use something. Stop, look at that. And then over on the Wireshark book website, if they go to wiresharkbook.com, I've got a set of 6 videos out there that are really the starter videos for Wireshark. You know, what is analysis about? What can you do with analysis? Let's start capturing some traffic. Let me just take you through the process really quickly and what some of the gotchas might be encapturing, and then let's test your adapter. Let's create something called a profile so you can customize Wireshark. It's just really the basics and there's, I think, well over 300 trace files for them to play with, actual packet captures of this is an FTP session, this is an HTTP session, this is DNS when it went well, this is DNS when it didn't go so well. There are a lot of practice files for them to go grab if they don't want to just live on their own network environment and I should mention that before people start capturing traffic they should have the appropriate authorization to do so; so that they don't get in trouble at their company by listening in the traffic without

authorization which is one of the things that as an IT staff you just have to make sure that you're covered for that.

Richard Campbell: Yeah. Are there any legal issues around this? Can you actually grab stuff you really shouldn't be looking at?

Laura Chappell: Oh, absolutely. Absolutely. I mean, it is not legal to go and listen in to someone's traffic if there's an expected right to privacy there and in a number of companies they will have a corporate policy against this type of packet capture and they'll typically define it as wiretapping. You know, it's digital wiretapping. This is not allowed anywhere on the network. So you really need to make sure you cover yourself and you probably don't want to go up to some company and say, "Hey, you know what? I listened in on your wireless traffic while I was in the network in the parking lot and did you know that you've got all these unencrypted traffic." That's definitely going to get you some new friends in prison at some point.

Richard Campbell: You also get reminded of how much of internet traffic is all clear text. All that email, all those websites, like all that stuff is clear, anybody can look at it.

Laura Chappell: Yeah, that's right. There is an argument that let's say I do go down to a Starbucks coffee and they've got an open wireless network for people there. I'm listening in. Do they have an expected right to privacy? Well, not really because they're literally standing on a street corner and shouting their conversation with someone else.

Richard Campbell: Right.

Laura Chappell: I can't believe how many companies do not understand how many of their communications are clear text like you said. It's really surprising on the wired network as well as the wireless network. You know, it's shocking sometimes when a company says, "Well, let's see. Can you get our payroll information?" I'm like, "Well, let me listen." I'll listen for a little bit and say "No, I can't get your payroll information but I can get all the tax deduction amounts for everybody." So I give you a hint of everybody's payroll. The best way for security, the best way to know what's going on and whether somebody can listen in through your traffic and understand it, you listen in first. You better be the first one.

Richard Campbell: Right. Laura Chappell, I think we're about out of time.

Laura Chappell: Well, guys, it's been great talking to you. Richard and Greg, that was a lot of fun.

Richard Campbell: Well, thanks so much for coming on the show.

Laura Chappell: See you at TechEd too.

Richard Campbell: You bet. And we'll talk to you next week on RunAs Radio.