hello everyone. the society broadcast engineers is pleased to present today's webinar “Wireshark 2: Troubleshooting.”

We welcome all of you today. my name is Kathy Orosz and I will be your moderator. Please note the today's program is being recorded and a link will be sent to you within two business days after the webinar has been presented. if you experienced difficult listening today's presentation via streaming at any time please call the SBE office at three one seven eight four six nine thousand today's presentation will last about 90 minutes and throughout the webinar you can submit a question by typing it in the chat box at the bottom of your screen instructing today is Steven Poole market chief engineer for Crawford broadcasting in Birmingham Alabama in his role as market chief engineer for Crawford broadcasting Steven Cole maintains most of the company's servers being email in the web he has been certified instant electronic technician since the 1980s and were recently with the SBE as CBT CBRE and AMD has decades of experience with radio engineering computer embedded systems and networking and with that I'd like to welcome Steven blue I appreciate that I hope everyone's having a beautiful day I had to fly to get here but I'm glad to be here this is the second part we did the first part of course a few weeks ago on Wireshark I'm going to assume for this one that not only are you familiar with at least the basics of networking Ethernet networking and remember that includes Ethernet compatible Ethernet compatible networking basically if it has an rj45 and you can plug it into a normal usual network switch then you can consider it Ethernet compatible but a Wireshark is a packet analyzer it lets you actually look at the data and today I'd like to show you some ways that you can use Wireshark in your work to troubleshoot and look for common problems and of course there's where we talk about your encouraged view the webinar if you're not familiar with a Wireshark that would be the first one that we did help a few technical points some reminders Wireshark is a GUI actual packet capture engine the one I use is called pcap you may see some older versions that use when pcap other names but the important thing is to remember is that you do have a separate packet capture engine and then Wireshark is the graphical user interface that displays but the pcap or capture engine does we had somebody in the first webinar asked whether we should use display filters or capture filters and now I can give you a little bit better explanation for that get filters which I'll call capture filters are actually given to pcap now you can use that to winnow it out so that only your desired packets will be stored to a temporary file on disk and then Wireshark actually reads that temporary file and - you know display everything once you're done with the capture using a packet filter helps reduce the size of that disk file and besides it makes things run a little more quickly you're less likely to interfere with other networking that is going on on the computer that you're running Wireshark on display filters let you choose what you're going to view from the file that pcap captured and saved to disk. Another little brief quick review we saw this in the first webinar but you can see the main capture screen at the very top one after another you'll see the packets and I always love to remind people of this if you've never used Wireshark before especially if you've never used it on a really busy network I'd be astonished if the minute you click the capture button you don't see just what looks like a million packets scrolling through that top lenda that's one reason that if possible you need to think of a cap filter that will help limit it and of course once you stop the capture and want to start examining what you're looking at you'll use a display filter that's part of what I'm going to cover today here's an example from last time you can see I used up at the very top you can see we're looking at HTTP which of course that's your standard web pages and I've selected the top packet in the middle one you get to see the entire packet these are all the different fields Wireshark understands each of these they know the the frame at the very beginning what the Ethernet information is with stash your MAC addresses and then the Internet Protocol that's your IP addresses and then finally transmission control protocol destination port 80 down at the bottom you see the specified field and you'll see you could see up in the top line where I selected that it's a get command which is where I'm telling the web server what I want and you can see down at the very bottom it's highlighted it's an HTTP I can use version 1.1 so on and so on that's where I'm giving them on telling them the server my browser and what I'm looking for are getting into the nitty-gritty encapture filter primitives I hope everyone has had a chance to play with Wireshark like I told you in the first webinar you're really not going to hurt anything there's a possibility you could slow your computer down on a really busy network you could cause some missed packets but generally speaking you're not going to hurt anything just playing with Wireshark especially for example the way I taught myself to use it was a high installed Wireshark on a home computer and I just looked at my own stuff at my own web browsing email and and just slowly became familiar with it but these are the capture filters remember this is before you start this is what you're going to tell pcap what you want to let's reduce the size of the temporary file on the disk and it tends to make things a little quicker because obviously you're not trying to store every single packet that comes in or goes out first one of the filters is host that can be an IP address or a host name you can add the modifier source or destination tell it precisely which IP addresses you want that's useful for example if you were to go back and look at the web example and just showed you the HTTP you could tell it I only want to see stuff from server I don't need to see my requests well that's where you use your source and destination fields also got some logical commands and or not you can use those to combine commands or you use the not command to negate to tell it you don't want this and you see the example of there you don't want that particular host xxx for numbers these are you may remember the way I always remembered is the IP address is like the street address the port number is the name of the person you're trying to contact this you specify a port number that you want to watch you can also use common port names HTTP 4 port 80 that's webpages SMTP the Simple Mail Transfer Protocol that's on port 25 and so on and so on you can also specify a proto protocol you can say I want to see all TCP in port 25 that particular command will show you the email that that your computer is sending out all right here's some common capture filters of course like I said feel free to experiment and come up with your own and the nice thing is there is tons of documentation online including at the Wireshark website Wireshark dot-org that has all kinds of skeleton filters that you can fill in there also if you click on that capture bar you'll see that there is a you can hit the I believe it's a little green button and not looking at that right now but that will show you some of your most common commands and you simply pull them in there and then edit them to the correct IP address or port number here are some examples host 192 so on in dock 15 I'm going for that specific to ignore it not host one 92168 1.15 pacific port port 53 that's going to become important near the end of this webinar because that is the port that dns the domain name system that's the port that he lives on for example when you enter in your web browser you enter google.com it's going to query a DNS server and that DNS server will return the IP address that it wants you to use to go to Google and then combine filters with and and or TCP port 53 that means I'm looking for DNS and the source host what that means is I only want that IP address that's doing stuff for a DNS queries really limits the amount of capture and of course after doing the capture if it looks like you're not seeing everything that you want well you can go back and change your cap capture filter maybe make it a little bit less restrictive or the the main window is to the left here I showed you this last time yes it's a little green button next to the filter bar anyway you're going to choose an interface you see here I've selected fa0 or Ethernet port 0 I might put in a filter here I would say host IP address whatever and then I could hit the capture that I've circled kind of in the middle of the left screen like almost like a link you hit that and it will bring up the Box you see on the right the way you can get to that box more quickly is to click capture up in the menu select ops and you'll see this same box that appears on the right you see down near the bottom the little green button you can use to get hints and you see where you can enter a capture filter in the middle to top part of it that's where you're confirming which interface you won't sniff you don't want to sniff them all because whether you realize it or not there is a tremendous amount of network especially if you run something like Linux or UNIX is a lot of information actually going from one port to another inside your computer normally never know that you normally wouldn't see it but if you make the mistake of saying let me see absolutely everything going to see everything and it's going to absolutely fill that screen with packets I wanted to mention again about promiscuous mode we covered that in the first webinar remember that if you're using a good quality networks which by design that network switch is not going to let you see everything on the network since I mean he's trying that network switch is trying keep you from being overloaded there's no reason why you need to see your neighbor printing for example or another neighbor browsing the web there's no reason you need to see those packets sometimes you can put your network switch ports into promiscuous mode King from experience with Gigabit Ethernet it's not going to work well you've got so much data flowing through at such high speeds unless it's a very very small network things you're going to have missed packets and you're going to start getting complaints decides even if you can get it to work you're going to be swamped with data so you'll need to use a really long complex capture filter string something that just narrows in on what you want all right now I'll talk to you about the attorney the alternative is what's called a network tap decent you can think of it as an active Y adapter even though that's not totally accurate it you could think of it that way people say that you can make your own with basically just some cat five wire and some jacks I don't recommend that especially not weave gigabit ethernet it's probably not going to work well instead spend the money and get a good excuse me get a good active filter box or if it's not filtered tap box and you'll need a couple of short cat5 cables now the connection obviously is going to be down for a moment you move the wire over you see this is where we're going on the Left we plug into the network switch you're going to have to unplug device that you actually want to sniff or the sniffy you're going to have to actually unplug that plugging into the tap and then the tap at the bottom we see the wire that's running to your computer running Wireshark in my case is usually my laptop one good brand name that I've seen several times and I think I'm going to order one it's called shark tap you can just google at the Amazon eBay a lot of apparently a lot of people use shark down that's a little safer and the shark tap is ready if you get the correct one it's rated for Gigabit Ethernet it shouldn't but shouldn't do a lot of damage if you're sending a lot of data through there I those of us in broadcasting we have to think about that because if it's a busy link you're sending a lot of audio and/or video over that link you do want to be careful about possibly slowing the band width down or causing otherwise problems you know causing problems otherwise you want to be careful with that well the cheap alternative if you don't want to spend the 80 bucks on a shark tab to install Wireshark on a computer that will see those packets of god state the obvious here if you want to confirm that a server is sending data you need to install Wireshark on that server I would actually recommend it on the remote client because of the remote clients you're basically checking the path and you can see what you see there once again you can try promiscuous mode but you may not see all the packets or you'll be overwhelmed you could also cause slowdowns and drop packets on your network if you're not careful especially if it's gigabit okay having said all that what good is it well I'm about to show you here is the first thing write this one down have a hat made and wear this hat all over the building to get some benchmarks when things are working properly take Wireshark on and put it in various network paths in your facility just run a few captures look at the data play around with your filters because that's when you'll have time to experiment you're not going to have time if something is down or you're off air or there's a problem you're going to be under pressure that's not going to be the time to be trying to figure out what to do go ahead and save some captures of known good data you can save your capture to a file you see that on the right of this slide you see that's on my version Wireshark of course is just a good old file menu and then save as and you can adjust accept their default extension but give it a useful name like tie line very 13 20 20 you know give it a meaningful name so that if you come back to that file later and incidentally that same file menu you see open that's how you open a previously saved capture file and it's going to pop up in the windows and you know the package will show up in that top screen and everything will just pop right into place as though it's a fresh capture and you can use display filters to go through it it didn't specifically say this in any of the slides but by the way if you have a display filter that you think is too restrictive simply go up to the filter bar backspace it out once it gets blank that'll show you all the packets again here we go to poke around so that you get an idea of what things look right like this is an old old capture that I did after we installed our first HD radio transmitters here in the Birmingham market and it tickled the fire out of me this is the pad the program associated data we send you know and which will appear on an HD radios display screen and it's I got tickled the first time I ever saw this they use the id3 format the same format that CDs used to store title and artist that was interesting in this case it's not an artist this is just a station promo for what we were doing at that time you 101 and 1260 that was two of our stations here we had just changed formats on them if nothing else is kind of interesting to look at it and you can see that it's plain text and everything should look good to you obviously not going to understand the at dot XZ stuff because what that is is digital data the actual title and artist artist and title information is in plain text as you can see in the bottom here's another really good example it's helpful to get a capture in advance fact get several captures in this case I'm going to show you a capture I just happen to take this one while a commercial was playing or a station promo not a song so I can do another capture with some songs if you're running a talk format be sure to get several captures so that you get an idea of what things look like now this is the capture filter remember he uses a slightly different format from the display but I'm saying I only want to capture data to and from 94 which happens to be the transmitter or pardon me pardon me our streaming server on our internal network you say I pick next in that's what we call our internal network that's the name of it and here's the actual data once again don't be surprised it's plain text we can get their support people to help explain some of these fields to you actually a lot of it is just common sense okay it's a web rapport I couldn't remember if it was a promo or commercial it's a weather report but you can see all the information that we provide to sound exchange or uh you know for royalty reporting licensing take some captures of this and be sure good captures look at them then later on if you start having any problem with your reporting you can pull up the captures and compare them and hear by the way also as far as troubleshooting goes you're talking about the old principle of divide and conquer here took a sip of water the old principle of divide and conquer if you see this data leaving your server you don't see it on the streaming machine in that case you know the problem is somewhere between in our case we use what's called an audio server and it actually sends the information to the streaming machine if I'm running this on the streaming machine and I don't see it unwire shark on the audio server machine and I do see it that tells me the fault is that the packets are never actually arriving at the streaming machine if on the streaming machine Wireshark shows the packets that tells me that my streaming software a problem okay I think everybody follow me on that use some logic and the old divide-and-conquer principle on the server but not on the streaming machine you've got a problem somewhere in the path or perhaps at the streamer on the streaming machine and on your server you can see this data so you know it's making it to the streaming machine but yet it's not appearing in your logs or in the displays if we're talking HD radio or people who you know now playing on your webpage that tells you that the problem is in your configuration or in the software on the streaming machine here's another example years ago the HD radio standard that first pad that I showed you capture back whenever they were just sending out a simple UDP just firing out the data over UDP there really wasn't a whole lot to it now though it's kind of interesting to me you can't see it in this picture because I've only zoomed in on the data they're actually doing a full TCP connection now you know the syn acknowledged push a hand shaking and all that it's a full TCP connection now here you can see this is a tape this happens to be one of our stations it's a gospel music station and we are playing thank God I'm free by the happy Goodman family there you go that's what will appear on people's HD radios notice also though it's still using the id3 standard which you can go of Wikipedia or you can google it if you're curious about ID 3 it will tell you what all the fields in that are you would learn this from using Wireshark or you can learn it from looking at the standard very few applications use all of the fields either for the streaming sound exchange reporting I showed you a moment ago or for the pad with HD radio or whatever else very few of them use all the field you can see here that we're using the title to field and then we have the artists down here are a bunch of fields in there that are not even being used and you find that out too by using wireshark now in this minute ago there are plenty of cheat sheets displayed filters we are now on the display filter we're done with the capture for planning a cheat sheets and information online you see here I've chosen I'm using the TCP protocol on the flags which that's some of the things that tell you that tell your network what kind of TCP packet this is and then there's the push command which push usually means we're sending data you can see I've right clicked on that particular you see that I'm right-clicking on that particular packet I've snipped there in the middle I say I want to follow this stream look down at the bottom see that follow TCP stream that will immediately set it up to where you're following only kits that are associated with that particular connection very handy happen to have a bunch of different connections of showing up in your display you can choose just to follow one then only the packets from that one particular conversation will appear in the display be handy else excuse me of a thought experiment I actually don't recommend that you do this because uh there's just too much chance that you'll miss something and I don't mean you as in you I mean you as in plural as in all of us you're going to miss something it does the question does arise from time to time most recently suppose you have an older machine running Windows 7 remember Microsoft has tol dit its end-of-life now you're not going to be getting any more updates which means the longer you run that the more at risk you're going to be for vulnerability yes sometimes Microsoft will break out a patch for an old they just patched XP not too long ago and XP has been end-of-life for years but if you can't depend on that if it's way to do it as I'll show you in a minute is to set up a firewall and then only open that which you absolutely need and I do you see my little disclaimer there actually it's a big disclaimer you do the following at your own risk ideal is to place that computer with a newer version of Windows and then just bite the bullet and get some replacement software but I'm using this as a thought experiment suppose this is some software that you can't get a replacement for and you really really require it in your work alright you will need a dedicated firewall here's two more terms that you can google up online clear OS and pfSense i have used both of these firewalls both have their strengths and weaknesses pfsense seems to me a little bit better and it's more it's easier to block IP addresses you know like if you know you're getting a ton of spam from a certain IP address in bulgaria i'll show you how to do this in a few minutes you can actually try to find that entire network block of all the IP addresses that could be used coming from that place in bulgaria and then you can go into PF sense and say look block everything from this IP address to that IP address don't even let the May connection 0 s is a little bit better at filtering content filtering clearos can actually examine webpages and tell you if something is junk in it or they'll block you from websites that you probably shouldn't be going to so it's your choice I suggest when you get time download both of them and just play with them if you've never used them play with them and then see which one you like better we use to give you an idea we use clearos on our regular networks on our office networks we use pfSense on our mail server cause it is much better at blocking IP address groups because you know like I say I don't want to be getting spam from Bulgaria or Vietnam so I can just go in there and say look block everything from Vietnam and it does it here's how you'll do it now this picture does not specifically state this strongly implied this is your old PC running an old version of Windows with that special software that you either absolutely have to have or that you love to death and you can't get any new version of that software but there it is the old PC on the Left plug that into the dedicated firewall your firewall obviously is going to need to network cards you set when I'm up on a small network for that old PC and then your second one is the one that will go toward the Internet the second card and they want the both clear or less MPS sense both have pretty good installers that will ask you you know which they'll usually use terms like internal and external internet is external this old PC is internal by the way the big scary dangerous Internet you might be interested to know that picture that I chose to use to illustrate the internet that is an actual generated snapshot of everything that was happening on the internet in a particular day back in 2015 big big big nodes are of course the big internet distribution centers but you see why it's called the you see I just branches out and goes all over the place trying to figure out what that little little branch up there at the very top you know I guess that's going to Alaska or I'm tough in Arctic Canada or something that one's not very busy okay here's how I would do it and again we disclaim you only do this as a last resort and you only do this at your own risk I'm going to show you the way that I would do it and in fact I may end up doing it because I do have some old software on an old Windows 7 computer that I'm kind of loathe to replace you install Wireshark on your old Windows 7 PC set up your SEP this is that separate firewall now I am NOT talking about a firewall on the Windows machine is that separate clear OS pfSense or some other separate firewall machine open and it goes without saying once you decide to do this make sure your habits and your plans and if you can uninstall do not use that Windows 7 PC for anything except running that old software don't do email don't brownells the web don't even browse your local network just just use it for that software Ida limit things as much as possible now here's the clue software that wants to access the Internet uses DNS the domain name system in tune that earlier it's a it's a lot easier to type in google.com than one of their IP addresses for example Google's DNS servers which is one of the examples I use here are at 8.8.8.8 and 8.8.4.4 but it's a lot easier just to say google.com or in this case I forgot the names on this something like DNS one at Google and DNS two but yes as I mentioned earlier usually is is by default is exchanged over port 53 what we're going to be using is port 53 that's what I'm going to be capturing remember this is the capture filter this is before we start so that we can limit what we have to look at and what we're storing to that temporary file on disk I makes it a little more a little quicker and a little easier to deal with and then once we're done with the capture come up and notice I show IP destination host is my local machine the one that's running Windows through Windows seven that's the one end one 92168 1.72 that's my local into seven machine there's a bunch of music software that's what I use that machine for it home I use it to play around write music things like that prizing Lee anvil studio is going to be looked up because that's my my digital audio workstation software he's going to want to see if there's any upgrades sorry tart forgive me anvil studio is a little program I use for MIDI editing it magics the one I use for the doll we have Native Instruments they made my audio interface not sure who door event bus i/o is so we'll skip him edge Excel that's my doll software I use a Magic's amplitude is the one I like see it's returning the actual IP addresses if you're using pfsense you need to make sure those addresses are permitted if you're using clear or less you can use these domain names domain names are actually a little better simply because from time to time companies are going to change their IP addresses and you don't have to go through there in search and manually poke in all of these weird-looking numbers but we look at how many different things MAGIX does to the DNS server then one interesting one down here is at the very bottom while I was doing this capture when does I'm using the network time server you know set the time come to computer and while I was in the middle of that wind is decided to ping and check the current time so that one in there asked for the address of time windows.com now here's a super trick and you'll thank me for this one some software will try to access the Internet while you're starting your computer up so not necessarily during the initial boot because obviously you're not going to have a network connection until the boot has gone far enough to activate the network card and put in the drivers and all that but there is a lot going on on your computer and we'll just use this for the example two windows 7 computer by the time you see your desktop Windows 7 has already done several checks in the background it makes it look faster to you and you get to the desktop more quickly here we go let's look at what I did with this capture and how I did the capture is the interesting part he cut the computer off shut it down disconnect a network cable or your internet cable this is on the Windows 7 PC disconnect your network cable and then reboot the network disconnected because what it will do the operating system is going to put off of these checks and say oh I don't have internet right now I'd better try again in a few minutes nice way to make sure you can start Wireshark once you get to the desktop go ahead and start Wireshark or capture filter and then that's emit worded a little misleading there filter for DNS which is port 53 I say start Wireshark it would have been better if I had said start the capture and plug in your network cable and you might need to let it sit for awhile maybe 10 or even 15 minutes and give each of those programs that basically they're checking for updates in the background what you want to do is make sure you give each of those programs time to come around to the I'm going to retry now unsurprisingly let's go through through these I am on an 18 T is my highest ISP at home for some reason my computer that and is going let's talk AT&T the big one down you see this several times in the list is Microsoft MSFT in CSI there's a bunch of different things that we're getting to Microsoft he wants to probably looking for updates looking for information incidentally if you're not familiar with DNS records the a records the old four octet IP addresses ipv4 the ones you're familiar with look down here at the bottom of FileZilla the quad-a or the aaaa addresses that's your ipv6 that's the new super long IP addresses and I told you when we started we were going to pretty much stick with ipv4 because everything I'm showing you will still apply to ipv6 with a few little interesting twists find it interesting that I ran FileZilla in order to send that first capture for to the computer that I was using to make these slides and of course as soon as I started FileZilla you see what he did he wants to know where he can look up date at FileZilla - project so he can let me know if there's a new version and you've seen that before you start a software program and it comes up and says a new version is available and that now you know what's going on when you start the program he actually queries over the Internet he calls home and says hey I'm using version so-and-so do you have a new run and that server ways off somewhere else when the internet says hey yeah we got a new version and it'll bring up that little window says would you like to upgrade then finally down at the bottom we got somebody named maniac told I don't know who that is I don't know what it's for but there he is these are some more things can look up online these I use Linux as I've said in fact I use open suits if you're curious all of these commands are basically built in or are easily installed and you use them out of terminal at a command prompt looks up a host names IP address that's going to be useful in case you happen to remember that one of your Wireshark captors came up with Billy Bob calm but you can't remember what Billy Bob what his IP address is so you can do a host Billy Bob calm and it'll tell you let's look up you really need to look at the hell for that but that lets you look up all sorts of info and now that one is on or can be installed on Windows computers that's not just a that's a and also on Macintosh that's pretty wide or Macs that's pretty widespread available widespread availability on that command and we've got who is is extremely important when you see repeated attempts I don't know how closely you look at your spam nowadays if you're like me you try not to but sometimes you've got no choice but anyway let's say you're looking at your spam happen to notice that you'd they're coming in from different domains all of them with extremely farcical names you know like I've seen some like flashlights copper rice but E or something or another you know they're stupid names but yet the IP addresses all looks similar they have the same three octet or at least the first two octaves you know the first two to end that ipv4 address you can use who is look up that IP address and it will return the the entire net block that IP address is part of this case I bet a command that was host pardon me who is eight 8.8.8.8 in stresses that I'm just curious I want to see who actually ends that block even though I already knew and so I go who is 8.8.8.8 I did this out of command-line and I have heavily heavily edited what I got because of course it's going to give you everything it's going to give the addresses the various contacts if you're being abused who you contact and how I cut it down to what I'm going to want for my pfSense firewall tip this particular block is from 8.000 to 8.1 27 255 255 go into PF since that firewall and tell it I want to block I think pfSense likes the CIDR so I would block it and say I want you to block everything from 8.000 slash 9 that's that entire block which by the way don't do that you won't be able to Google anything this is just an example oh and there's at the bottom you see where it gives us the organization sure enough it's Google Google liability limited corporation or geo GL ok let's see were we there's couple of other little things I wanted to go back and briefly look at I guess we could always admire that good picture of the the entire internet anymore I want to mention again about these flags because BP or the transmission control protocol rides the top of tcp/ip the transmission control protocol as I said has a number of different things in it which you can examine the actual fields in Wireshark there are for example there's going to be our integrity information to verify that it was good got your different flags that tell you whether it is a sin an act a push a reset you could look at look just show me the TCP flag if you left off that word push you basically see all the packets and you'd see all the flags but by telling it I just won't push that means I'm only looking at the ones actually sending data and then I went down here like I said and I right-click don't follow and I could use that read up if you're curious and you want to know more about that read up on your TCP flags and you can see you know how you could possibly use that thing that you want to look for if you're constantly having trouble with a particular website a nice thing to do is if you've got Wireshark on that computer and you're trying to look at a website and this could be an internal website true like maybe one of your transmitters has one of those little built-in web browsers what you do is you bring it up you got Wireshark tell them I just want to look at this IP address then look for reset rst Flags that because a reset means a hard break of that connection server said I can't talk to you right now go away that happens you need you might if it's a remote server out on the Internet of course not much you can do servers just overloaded speaking from experience they may just need to install more RAM into their server machine but anyway the servers are related but if it's one of your internal devices you might want to look maybe someone logged into it and it's a really really low powered one of those little web servers on the stick and they mounted it inside the box and it's overloaded because a couple of other people in the building pulled it up and I've relieved left it running all the time I think that's really about all we needed to cover today and I do want to emphasize this not just be saying this you've only seen a very small portion of what Wireshark can actually do pay with it I can't emphasize that enough really put it on your laptop and carry that laptop around with you for the next week or so get up to different networks hook it up and from cases and just start wire sharking things get comfortable with it get familiar what they look like and then use Google if you see something you don't understand there is tons of assistance online for that you can see precisely who is trying to reach him that's an interesting one to me and I've done that before I showed showed you how to I showed you how to troubleshoot with this that if you see the data on the sending in but you don't seeing on the receiving end you've got a network issue if you do see the data on the sending and receiving ish end you have a software issue on the receiving end that in and of itself is going to be one of the most powerful uses for Wireshark because it will keep you from running in circles if you're trying to run down while you're RTS isn't being displayed or why of you know some other data that you you closed captioning or any other kind of data is not working correctly just a quick Wireshark will tell you where you probably need to start looking I'd love to take some questions if anybody has any or if I missed something let me know yeah a couple questions down here Stephen do you recommend a passive or active network tap what are the disadvantage of a passive app disadvantage to a passive tab the first one is electrical I mean by Ohm's law and all the other laws that we must think with help V was tube a if you have certain amount of voltage coming into that Y adapter and then you split it across two different connections you've cut the voltage in half and that member that's best case the other problem is once you get up to a hundred megabits or even up to especially up two gigabit you're going to have problems with a Haywired passive tab I'm sure you could get away with it on like a 10 megabit an old 10 megabit network you could probably get away with it just fine any higher speed network you're really going to want something like an active tab and by the way if you can find a gigabit hub no one that's a dumb hub that doesn't do any switching you could actually use that as your tapped as I did several Google searches nobody makes them that I could find old days 20 years ago you set up an oval network or your first Windows network about all you could find was hubs hubs basically are just electronic Y adapters that let everything squirt all over the place every port sees everyone else that's the difference between a switch and a hub to answer that question cans from bottom line if at all possible use an active tap another possible idea that I haven't done yet but I was thinking last night and I said hmm a raspberry pi Oh raspberry pi will run Wireshark wonderful raspberry pi with an extra Ethernet card wouldn't make a good inline man-in-the-middle tab I'm going to be looking into that and I encourage you to have fun with that little idea does that answer the question you you've answered the some switches have the ability to set up a port monitor port so you do attorney I can't see the questions here Oh audience questions duh Oh I really should not be allowed anywhere near this hey hey using a smile man you switch with port replication I tried if it works you're in you're in and Chris Stevens yes I've mentioned earlier in the bid that the one that seems a pretty good deal and that a lot of people recommend on the hacker sites not that I recommend you go to Accra sighs is the shark tap and in fact that's the one I'm getting ready to purchase able to do most of my troubleshooting just by carrying my laptop around and as needed put Wireshark on one end or the other but I see that in the future I'm going to want to tap use Wireshark with fiber links absolutely if you have a fiber link on the machine running Wireshark absolutely they make you can find fiber network taps as well I can't remember the brand I saw online but just google it pepper Network tap I like what websites do you prefer for premade filters the first one I try is Wireshark org and click the documentation link and the way I found them and I'm sorry I probably should have included some I didn't write them down just Google wireshark capture filters and you'll come up with a bunch of really nice pages I have a lot of information you use Wireshark with fiber links we just ask that besides do you prefer we just did that let's see which is have the ability to set up a port monitor that is true and we'll do it and I will say the same thing I did a moment ago try it I know the reason I say that is because I have had trouble once you start getting into gigabit and ten gigabit started we started losing some packets on our network and on an audio network what that meant was we had glicks glitches and pops in the audio one of those you're just going to have to try it and decide for yourself but I'm going to use a network tab I decided that while I was writing this series we have their phone number I can call for audio okay I can't help you with that we've active I think that's all the questions I have answered look at the very potent app tap would be helpful for looking at my data to exporter have it single cable most of the time did you answer that already very less how did I miss that one yes yes if you want to do is I can let me go back to that picture what are what you want to do with your tap always proof that I'm just a fiercely awesome your guy for all I know there's probably some quick way to get back to the one I want but see what you're doing is alright say the right here is your exporter which by the way I feel your pain I feel you man I know what you're talking about but anyway the right going from network switch to the right to the device being sniffed that's your current cable simply break the connection there plug the cable from exporter into this right jack and then take a little short jumper and plug that into the switch laws into the network switch into the same port and then the bottom Jack use a little short cable to run to your computer that has Wireshark because now Wireshark should be able to set your network card into promiscuous mode where he has trouble is trying to get your switched to go into promiscuous mode hope that answered requests but yes I would definitely recommend the tab replication we just got that just comment from Jeff pfsense have the ability to do packet captures based on interface and filters and can be analyzed in Wireshark you know that's a good point the truth of the matter is there are a number of programs that can do packet captures and if you look I couldn't possibly name them all off the top of my head but if you look in the help files for Wireshark or on the documentation on their webpage Pease point out that they can that Wireshark can pull in and read a number of different packet capture formats and he's absolutely right about that PF sense is a pretty sweet firewall the only reason we use clear or less on our office networks is because it's better at web filtering to meet personal opinion but you're right PF sense is a is a Ria's firewall that has it's got some serious chops you're right about that and remember you can even a capture that was made with some other program as long as it's a format the Wireshark recognizes you can just open that and then look at your screen hit the data go back and look at it and it will pull it up and it'll look just like that it'll look just like a fresh capture and this could be a capture file that you did and saved five years ago doing something completely different program there's some really nice tools associated with package sniffing now specifically mentioned this by the way but you notice that's in plain text here if you're feeling kind of puckish to do is if you could get a promiscuous connection on your network is just start looking for plain text and I promise you if anybody out there has got their stuff configured wrong and it's in it's not in using secure socket layer Zoar transport layer security you know SSL TLS and you see passwords flying around in plain text that's when you can take a screenshot and go tape it to their door and say dummy NAT - I got a mean streak in me okay any is there a fire but that that but I said as a fiber tap you know what oh no hold on the power of multitasking I'm going to google it as we speak do what I think of it that's a good point about PSS I want to hug that guy hadn't even thought about that ever network taps yes they're a bit more expensive one called the Hirshman spider for 130 bucks yes dance your questo and u.s. robotics makes one it's almost 600 but yes to answer your question you can get a fiber towel yeah I figured you could I couldn't see where somebody would make one but prices are still kind of high on them because they're not let's face it the most common debt were right now is still cat 5 or cat 6 from between rj45 jacks I mean you know it's just fiber still just not that common yet I mean when you know what I mean by common I've got fiber in my facility but talking about at large and the end the wild and my transmitter sites we've still got a bunch of copper okay well that looks like the questions Thank You Steven for a great presentation and if you do have any additional questions or comments you can send them to me I will forward them on to him know that each of you will receive an email with a link to a short evaluation form to complete about about today's program please take a moment to complete the evaluation and give us your feedback we count on your comments and suggestions the email will also include a PDF copy of Stephens presentation we will be sending a link to the archived version of the live webinar in this email like to welcome attendees who are not SPE members to learn more about the membership by logging on to WWSD org the SB hopes you enjoyed today's program and registration is now open for the Aoi P series module one IP networking for real-time media networks on February 25th RF 201 module nine TV combined combiners on March 12 and the Aoi P series module 2 Aoi P basics March 24th so go to the WSB org for details about these webinars as well as complete schedule of other upcoming webinars that concludes today's program and we thank you for attending may now disconnect