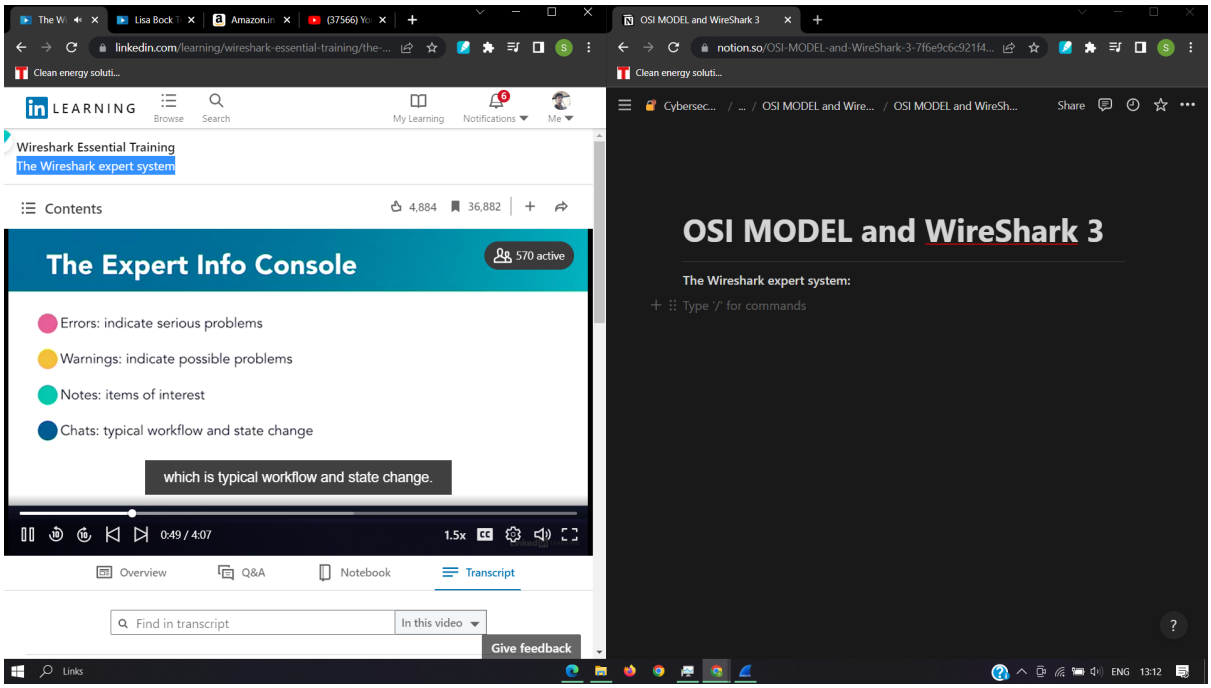
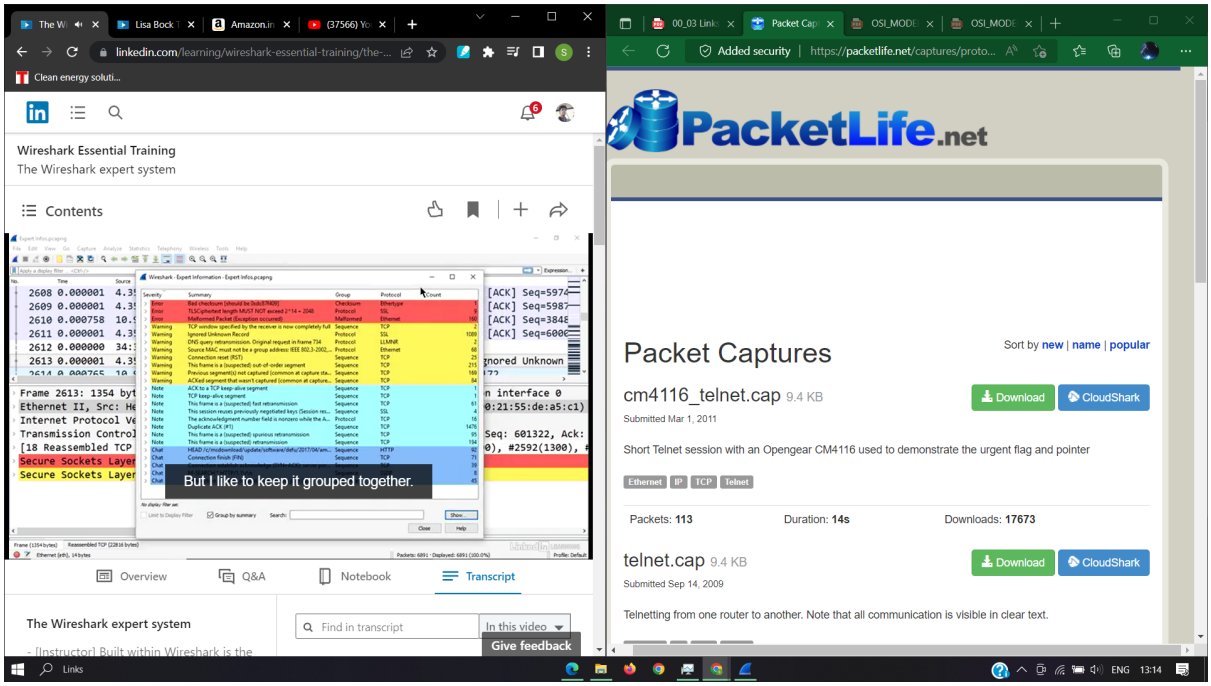
OSI MODEL and WireShark 3

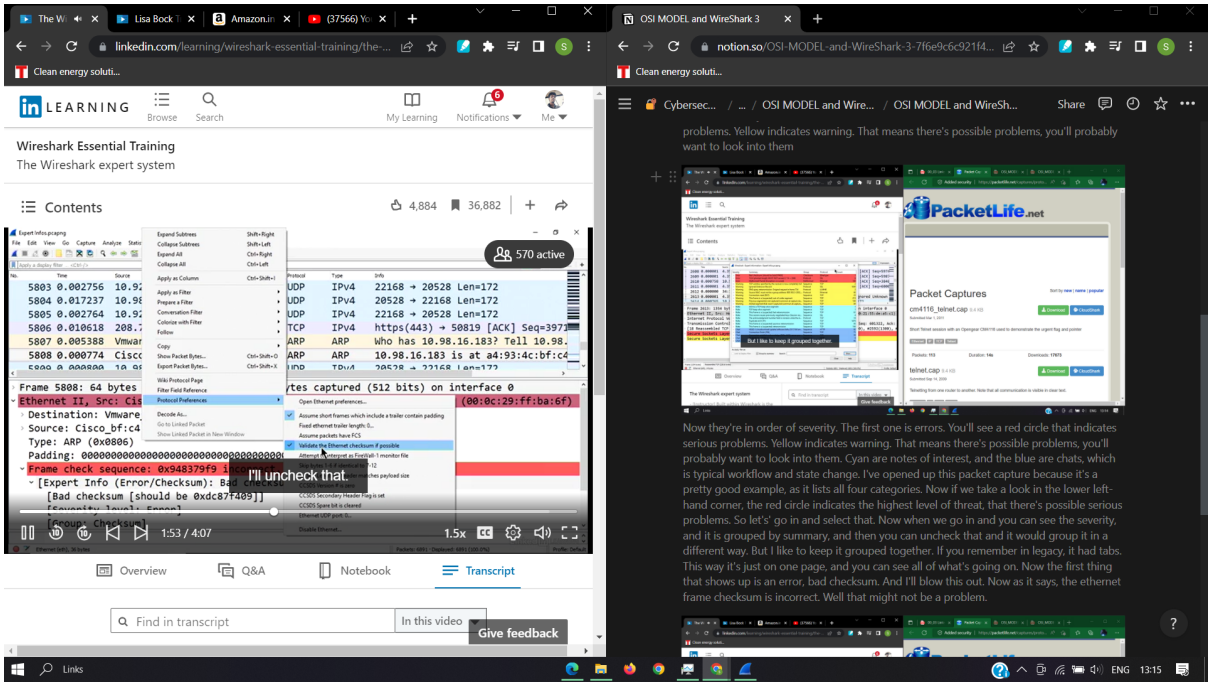
The Wireshark expert system:



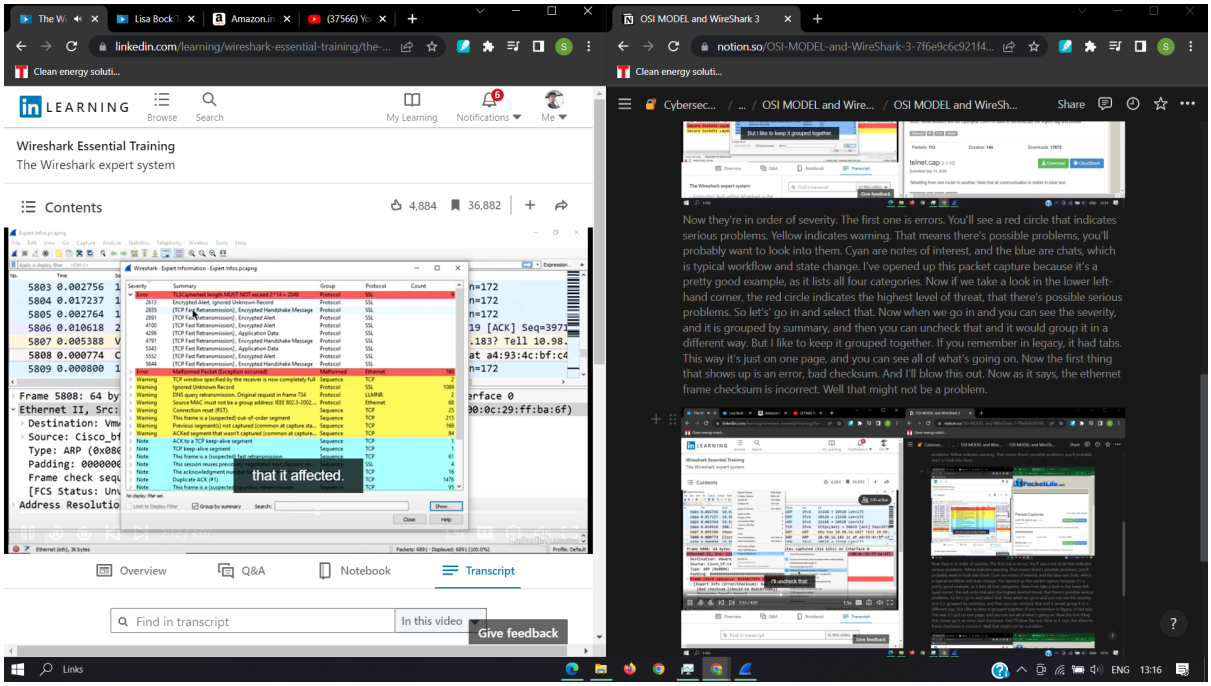
Built within Wireshark is the expert system. The expert system helps to alert the network administrator on possible issues once a capture's been made. Keep in mind, it's only a guide. Sometimes it really isn't a problem, such as a checksum incorrectly calculated. When we go into the Expert Info Console, you'll see four categories. I say expert info because that's how you might see it referenced if you go into the Wireshark wiki. Now they're in order of severity. The first one is errors. You'll see a red circle that indicates serious problems. Yellow indicates warning. That means there's possible problems, you'll probably want to look into them



Now they're in order of severity. The first one is errors. You'll see a red circle that indicates serious problems. Yellow indicates warning. That means there's possible problems, you'll probably want to look into them. Cyan are notes of interest, and the blue are chats, which is typical workflow and state change. I've opened up this packet capture because it's a pretty good example, as it lists all four categories. Now if we take a look in the lower left-hand corner, the red circle indicates the highest level of threat, that there's possible serious problems. So let's' go in and select that. Now when we go in and you can see the severity, and it is grouped by summary, and then you can uncheck that and it would group it in a different way. But I like to keep it grouped together. If you remember in legacy, it had tabs. This way it's just on one page, and you can see all of what's going on. Now the first thing that shows up is an error, bad checksum. And I'll blow this out. Now as it says, the ethernet frame checksum is incorrect. Well that might not be a problem.



Let's exit out of here, and then we'll go back over to the ethernet frame, any one, and right click. Go to protocol preferences, and here I say, validate the ethernet checksum if possible, I'll uncheck that. And now you see it won't be an error. And again, that's a common thing, it's not always an error, it's just incorrectly calculated. Now let's go into the expert infos again. Alright, now when we take a look at any of those categories, you can blow it out and see those packets that it affected.



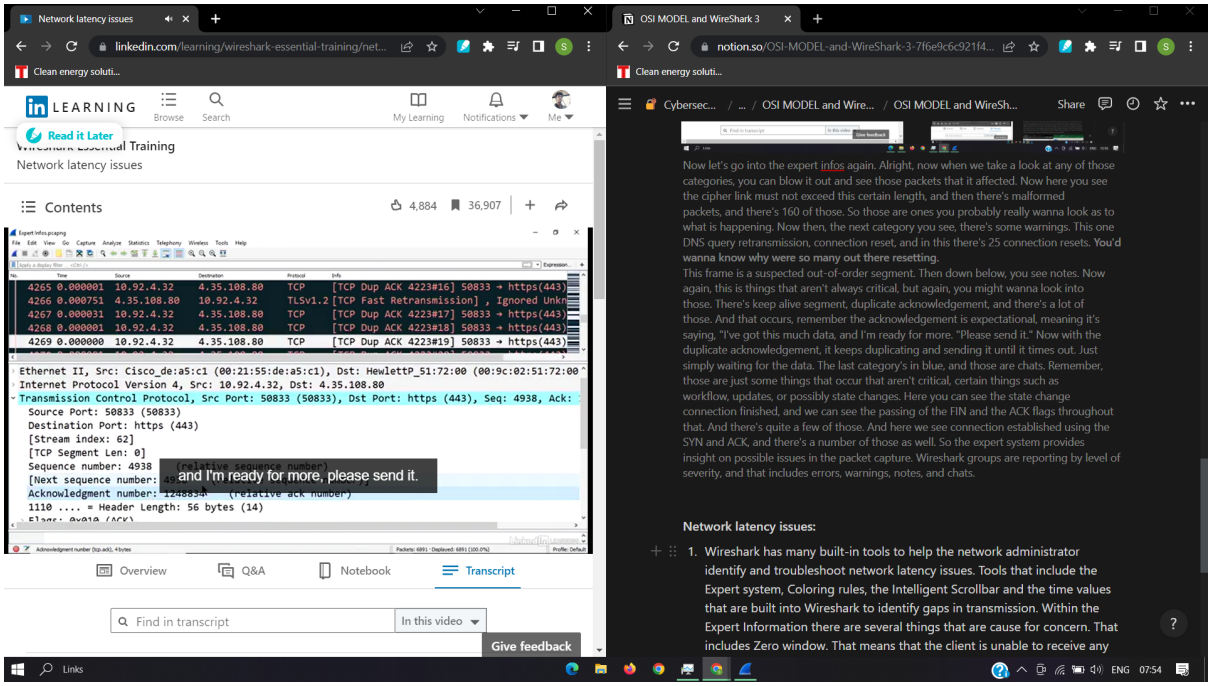
Now let's go into the expert infos again. Alright, now when we take a look at any of those categories, you can blow it out and see those packets that it affected. Now here you see the cipher link must not exceed this certain length, and then there's malformed packets, and there's 160 of those. So those are ones you probably really wanna look as to what is happening. Now then, the next category you see, there's some warnings. This one DNS query retransmission, connection reset, and in this there's 25 connection resets. **You'd wanna know why were so many out there resetting.**

This frame is a suspected out-of-order segment. Then down below, you see notes. Now again, this is things that aren't always critical, but again, you might wanna look into those. There's keep alive segment, duplicate acknowledgement, and there's a lot of those. And that occurs, remember the acknowledgement is expectational, meaning it's saying, "I've got this much data, and I'm ready for more. "Please send it." Now with the duplicate acknowledgement, it keeps duplicating and sending it until it times out. Just simply waiting for the data. The last category's in blue, and those are chats. Remember, those are just some things that occur that aren't critical, certain things such as workflow, updates, or possibly state changes. Here you can see the state change connection finished, and we can see the passing of the FIN and the ACK flags throughout that. And there's quite a few of those. And here we see connection established using the SYN and ACK, and there's a number of those as well. So the expert system provides insight on possible issues in the packet capture. Wireshark groups are reporting by level of severity, and that includes errors, warnings, notes, and chats.

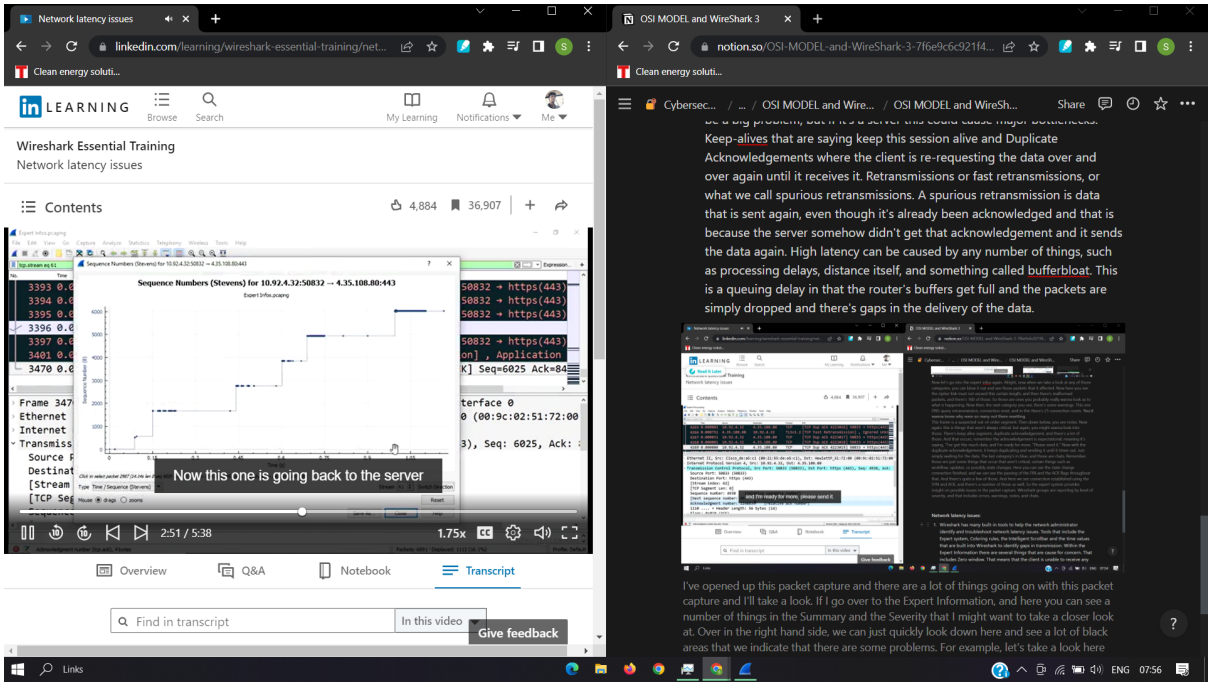
Network latency issues:

1. Wireshark has many built-in tools to help the network administrator identify and troubleshoot network latency issues. Tools that include the Expert system, Coloring rules, the Intelligent Scrollbar and the time values that are built into Wireshark to identify gaps in transmission. Within the Expert Information there

are several things that are cause for concern. That includes Zero window. That means that the client is unable to receive any more data because the buffer is full. Now on the client side that might not be a big problem, but if it's a server this could cause major bottlenecks. Keep-alives that are saying keep this session alive and Duplicate Acknowledgements where the client is re-requesting the data over and over again until it receives it. Retransmissions or fast retransmissions, or what we call spurious retransmissions. A spurious retransmission is data that is sent again, even though it's already been acknowledged and that is because the server somehow didn't get that acknowledgement and it sends the data again. High latency can be caused by any number of things, such as processing delays, distance itself, and something called bufferbloat. This is a queuing delay in that the router's buffers get full and the packets are simply dropped and there's gaps in the delivery of the data.

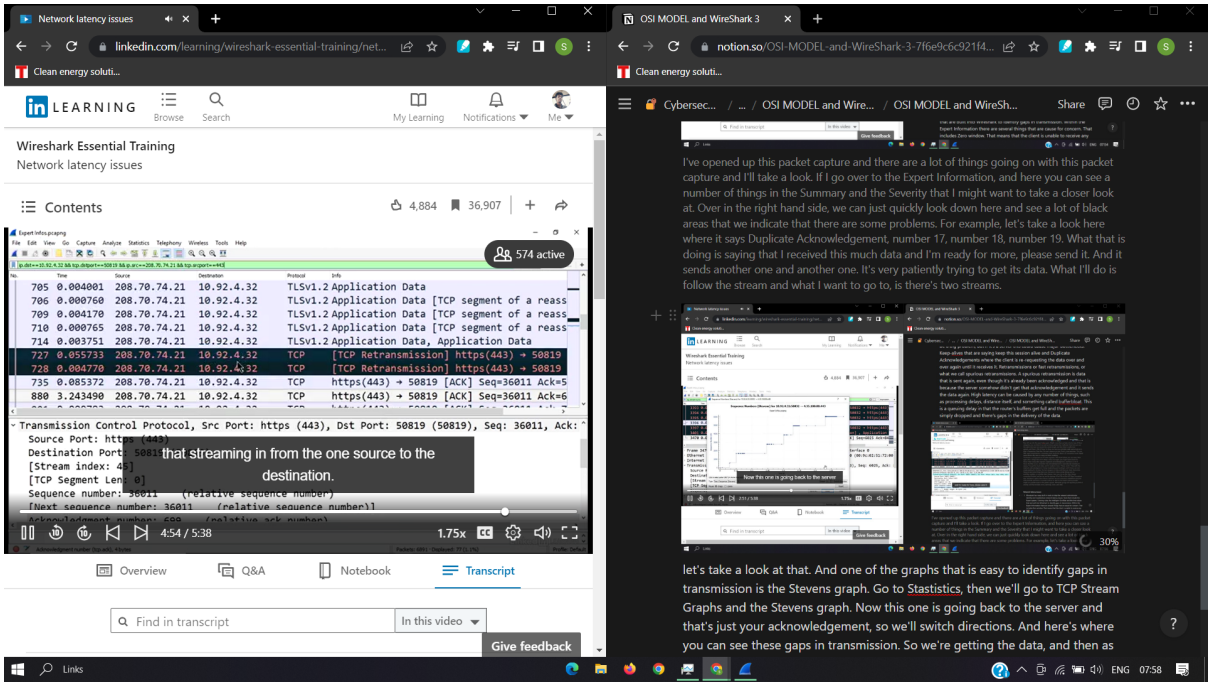


I've opened up this packet capture and there are a lot of things going on with this packet capture and I'll take a look. If I go over to the Expert Information, and here you can see a number of things in the Summary and the Severity that I might want to take a closer look at. Over in the right hand side, we can just quickly look down here and see a lot of black areas that we indicate that there are some problems. For example, let's take a look here where it says Duplicate Acknowledgement, number 17, number 18, number 19. What that is doing is saying that I received this much data and I'm ready for more, please send it. And it sends another one and another one. It's very patiently trying to get its data. What I'll do is follow the stream and what I want to go to, is there's two streams.



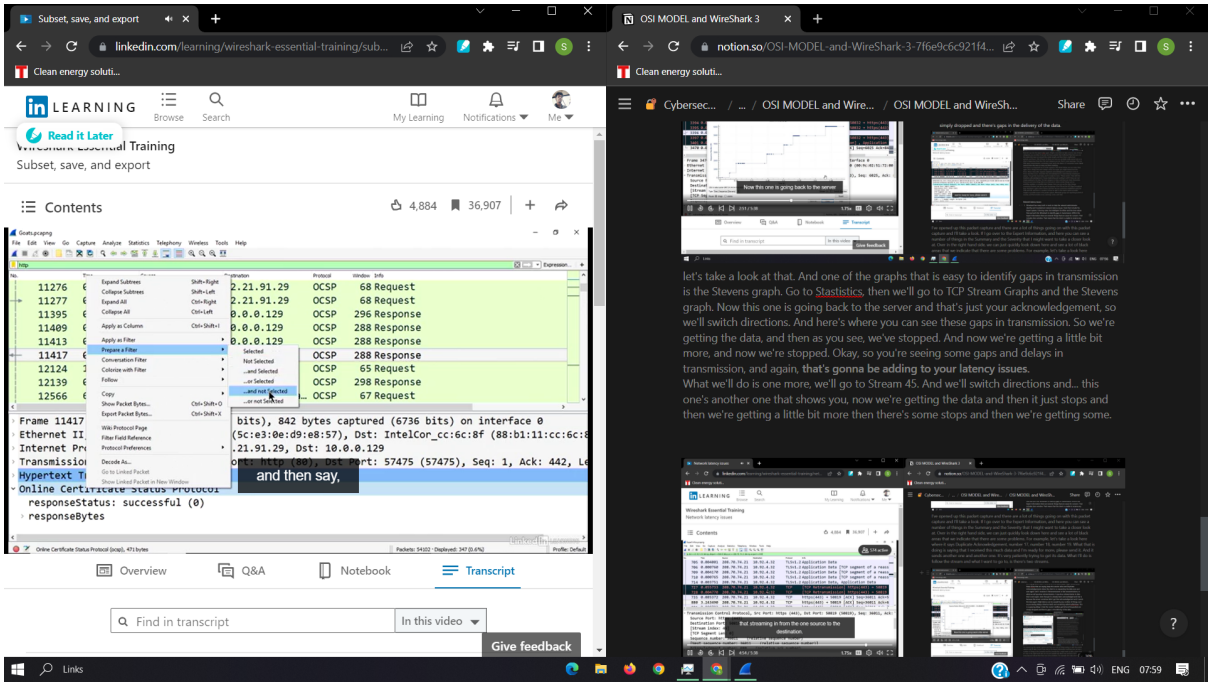
let's take a look at that. And one of the graphs that is easy to identify gaps in transmission is the Stevens graph. Go to Stastistics, then we'll go to TCP Stream Graphs and the Stevens graph. Now this one is going back to the server and that's just your acknowledgement, so we'll switch directions. And here's where you can see these gaps in transmission. So we're getting the data, and then as you see, we've stopped. And now we're getting a little bit more, and now we're stopped. Okay, so you're seeing some gaps and delays in transmission, and again, **that's gonna be adding to your latency issues.**

What we'll do is one more, we'll go to Stream 45. And we'll switch directions and... this one's another one that shows you, now we're getting the data and then it just stops and then we're getting a little bit more then there's some stops and then we're getting some.

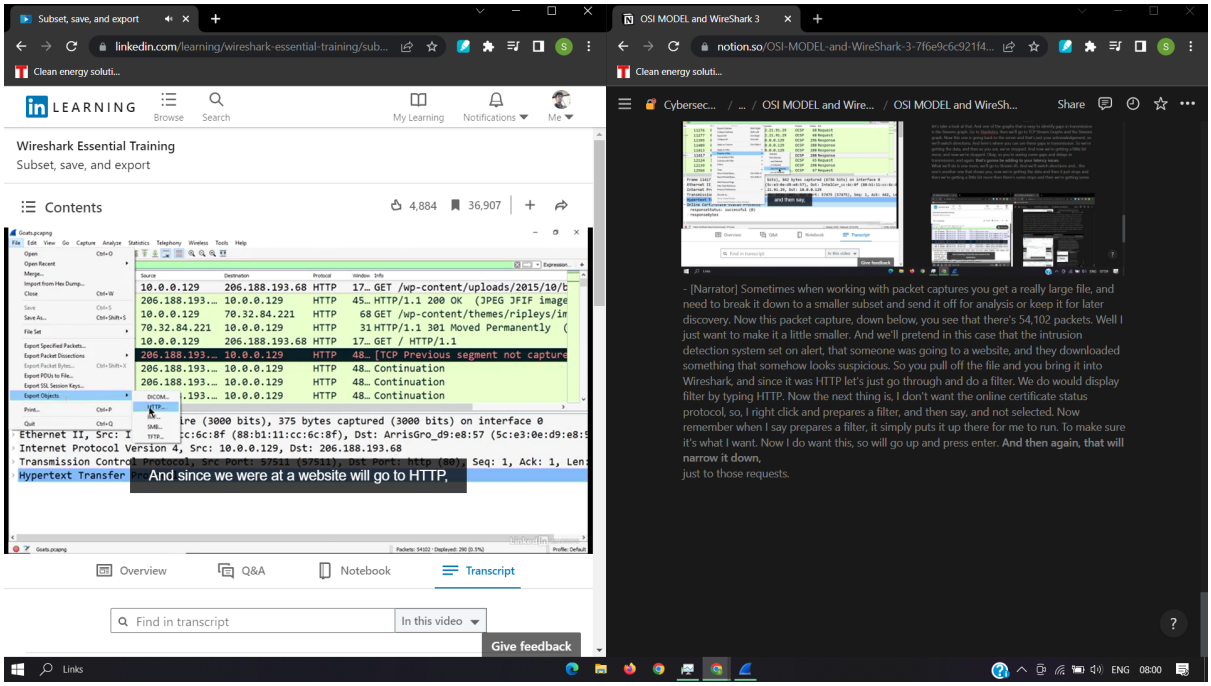


In addition to the Stevens graph, we can also use the time values to identify gaps in transmission. I'll have to find that Conversation. We'll first go to Statistics and then Conversations and then I'll have to filter down to that Conversation. As you see here, 208 is the IP address. When I right click, I Apply as a Filter but I want it to go from the server to the client and that would be B to A. Then I'll close that. And now what you wanna look at are the large gaps in between transmission, and when we first go in here we're gonna go to View, Time Display Format, and you wanna make sure that it's set correctly. In this case, it says Seconds Since Previously Displayed Packet and that's what I want because now you can see that streaming in from the one source to the destination. And here you can see that first gap right here in between this packet and this one is three seconds, and we did see that one. And then we'll go down below and this is the Stream 45 and there's another one. That's a one second. And here's one that's two seconds. So in addition to the Stevens graph, we can use the time values to identify gaps in transmission. **So, Wireshark can help the network administrator** identify and troubleshoot network latency issues but the next step is to be proactive and identify where the bottleneck is occurring so that you can keep the data flowing.

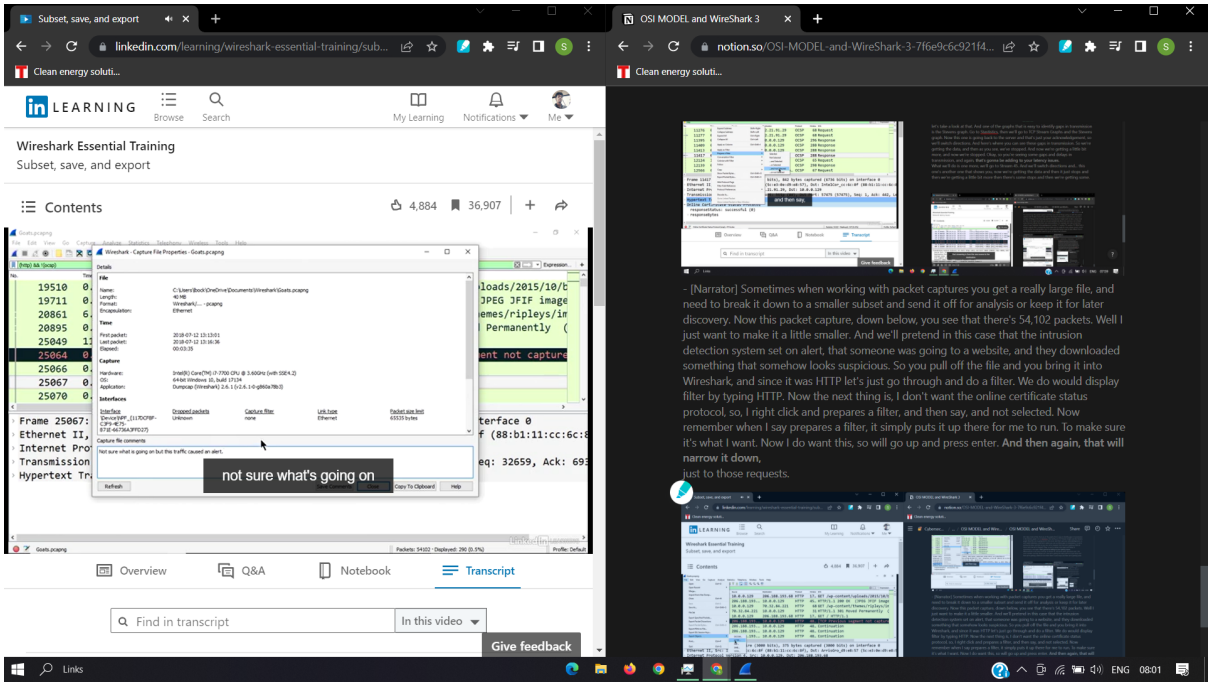
Subset, save, and export:



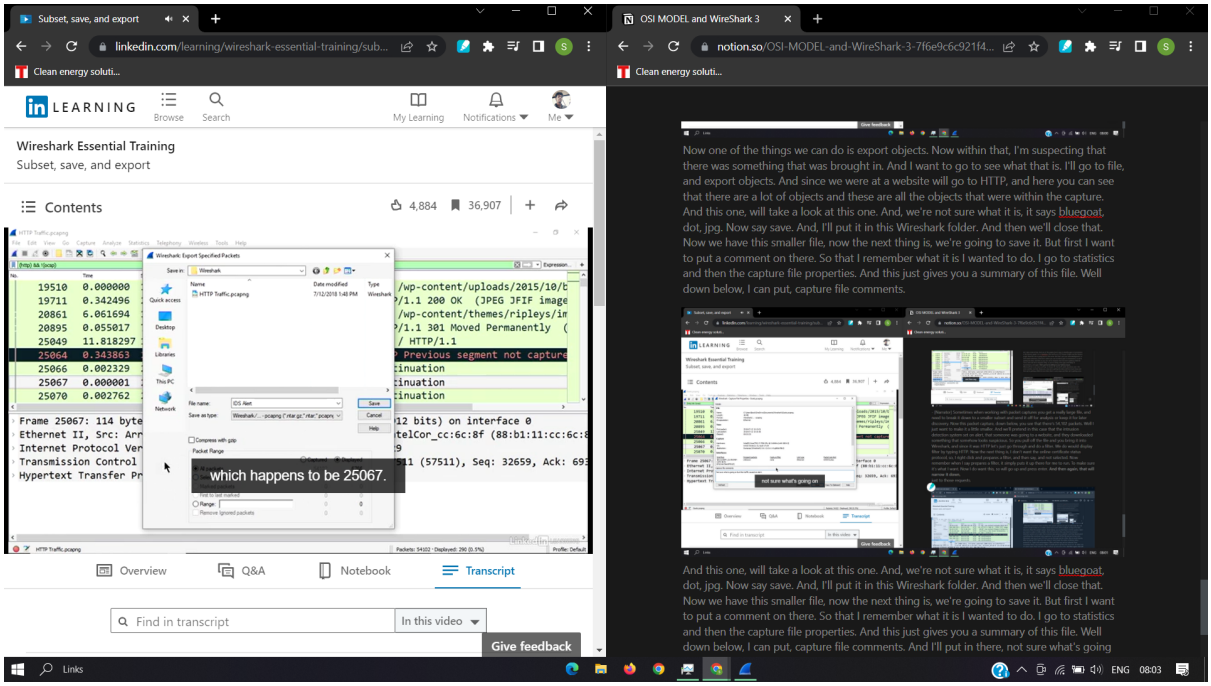
- [Narrator] Sometimes when working with packet captures you get a really large file, and need to break it down to a smaller subset and send it off for analysis or keep it for later discovery. Now this packet capture, down below, you see that there's 54,102 packets. Well I just want to make it a little smaller. And we'll pretend in this case that the intrusion detection system set on alert, that someone was going to a website, and they downloaded something that somehow looks suspicious. So you pull off the file and you bring it into Wireshark, and since it was HTTP let's just go through and do a filter. We do would display filter by typing HTTP. Now the next thing is, I don't want the online certificate status protocol, so, I right click and prepares a filter, and then say, and not selected. Now remember when I say prepares a filter, it simply puts it up there for me to run. To make sure it's what I want. Now I do want this, so will go up and press enter. **And then again, that will narrow it down,**
just to those requests.



Now one of the things we can do is export objects. Now within that, I'm suspecting that there was something that was brought in. And I want to go to see what that is. I'll go to file, and export objects. And since we were at a website will go to HTTP, and here you can see that there are a lot of objects and these are all the objects that were within the capture. And this one, will take a look at this one. And, we're not sure what it is, it says bluegoat, dot, jpg. Now say save. And, I'll put it in this Wireshark folder. And then we'll close that. Now we have this smaller file, now the next thing is, we're going to save it. But first I want to put a comment on there. So that I remember what it is I wanted to do. I go to statistics and then the capture file properties. And this just gives you a summary of this file. Well down below, I can put, capture file comments.

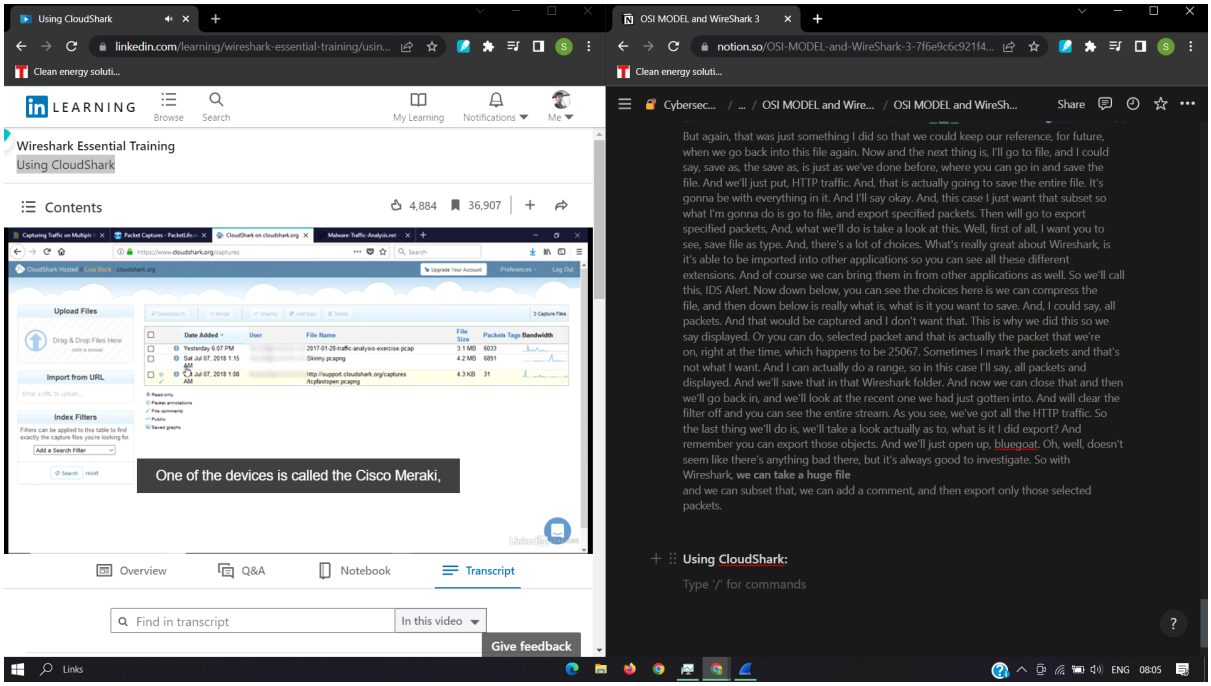


And this one, will take a look at this one. And, we're not sure what it is, it says bluegoat, dot, jpg. Now say save. And, I'll put it in this Wireshark folder. And then we'll close that. Now we have this smaller file, now the next thing is, we're going to save it. But first I want to put a comment on there. So that I remember what it is I wanted to do. I go to statistics and then the capture file properties. And this just gives you a summary of this file. Well down below, I can put, capture file comments. And I'll put in there, not sure what's going on but this traffic caused an alert. I'll say save the comments, and then we'll close it. Now, if you do notice that the file name has a little Asterix, once I save that, that will preserve the comments.

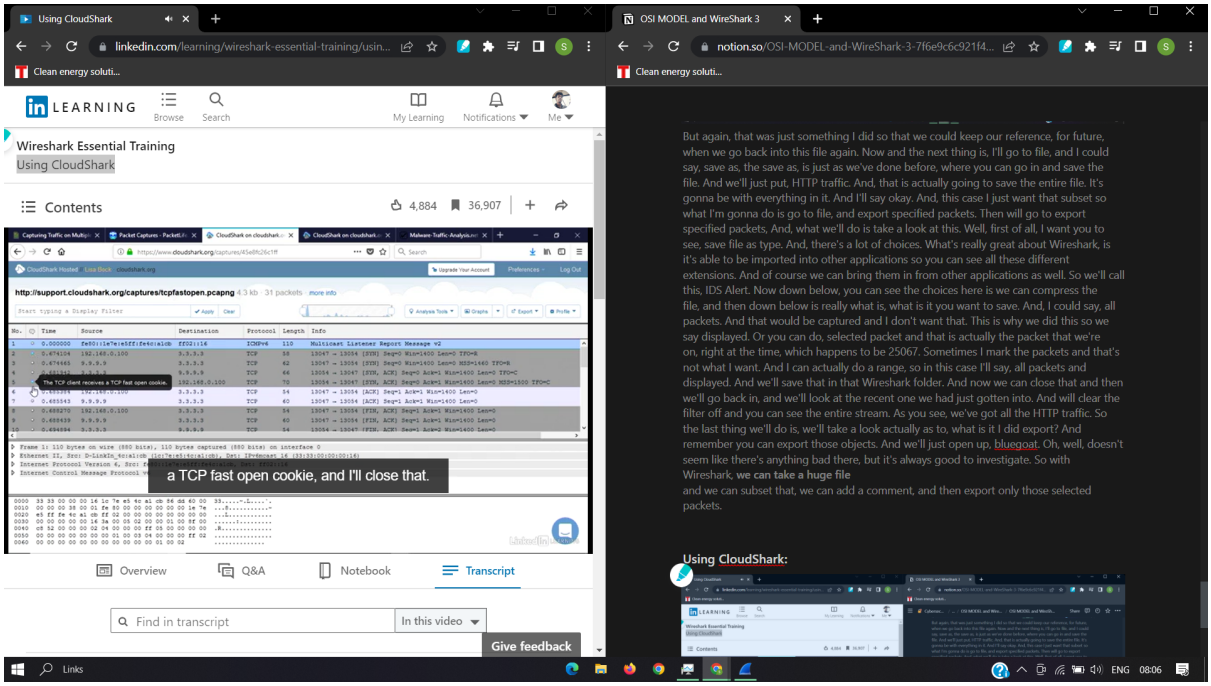


But again, that was just something I did so that we could keep our reference, for future, when we go back into this file again. Now and the next thing is, I'll go to file, and I could say, save as, the save as, is just as we've done before, where you can go in and save the file. And we'll just put, HTTP traffic. And, that is actually going to save the entire file. It's gonna be with everything in it. And I'll say okay. And, this case I just want that subset so what I'm gonna do is go to file, and export specified packets. Then will go to export specified packets, And, what we'll do is take a look at this. Well, first of all, I want you to see, save file as type. And, there's a lot of choices. What's really great about Wireshark, is it's able to be imported into other applications so you can see all these different extensions. And of course we can bring them in from other applications as well. So we'll call this, IDS Alert. Now down below, you can see the choices here is we can compress the file, and then down below is really what is, what is it you want to save. And, I could say, all packets. And that would be captured and I don't want that. This is why we did this so we say displayed. Or you can do, selected packet and that is actually the packet that we're on, right at the time, which happens to be 25067. Sometimes I mark the packets and that's not what I want. And I can actually do a range, so in this case I'll say, all packets and displayed. And we'll save that in that Wireshark folder. And now we can close that and then we'll go back in, and we'll look at the recent one we had just gotten into. And will clear the filter off and you can see the entire stream. As you see, we've got all the HTTP traffic. So the last thing we'll do is, we'll take a look actually as to, what is it I did export? And remember you can export those objects. And we'll just open up, bluegoat. Oh, well, doesn't seem like there's anything bad there, but it's always good to investigate. So with Wireshark, **we can take a huge file**
and we can subset that, we can add a comment, and then export only those selected packets.

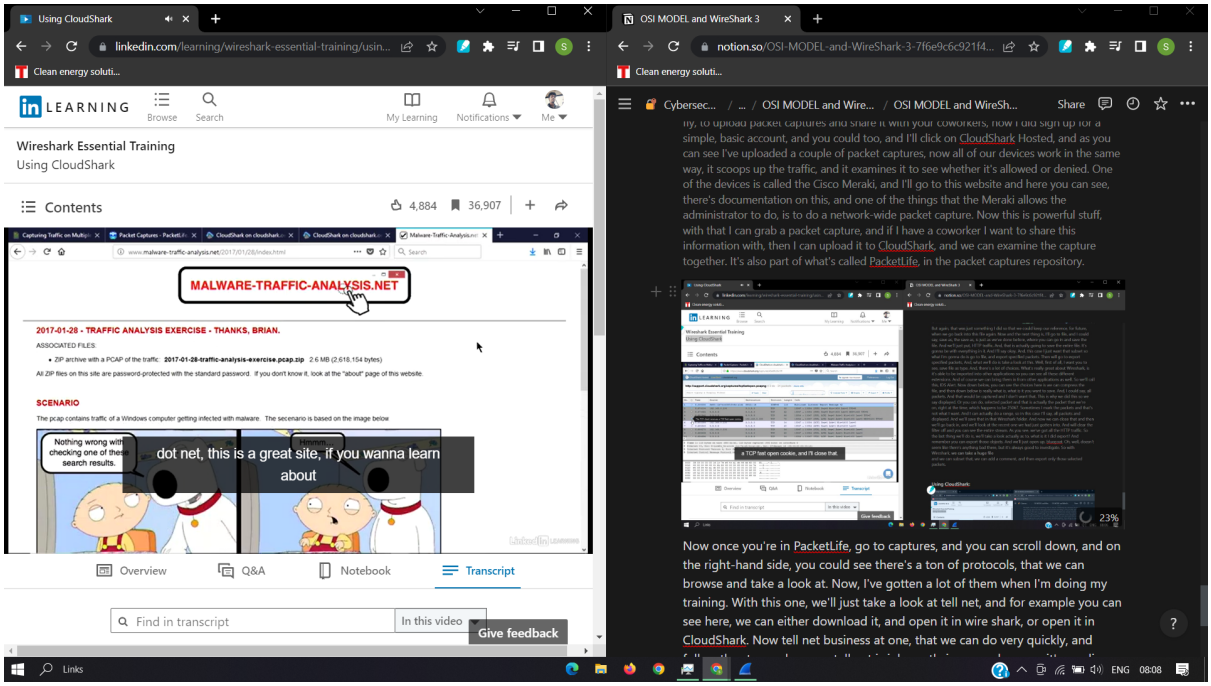
Using CloudShark:

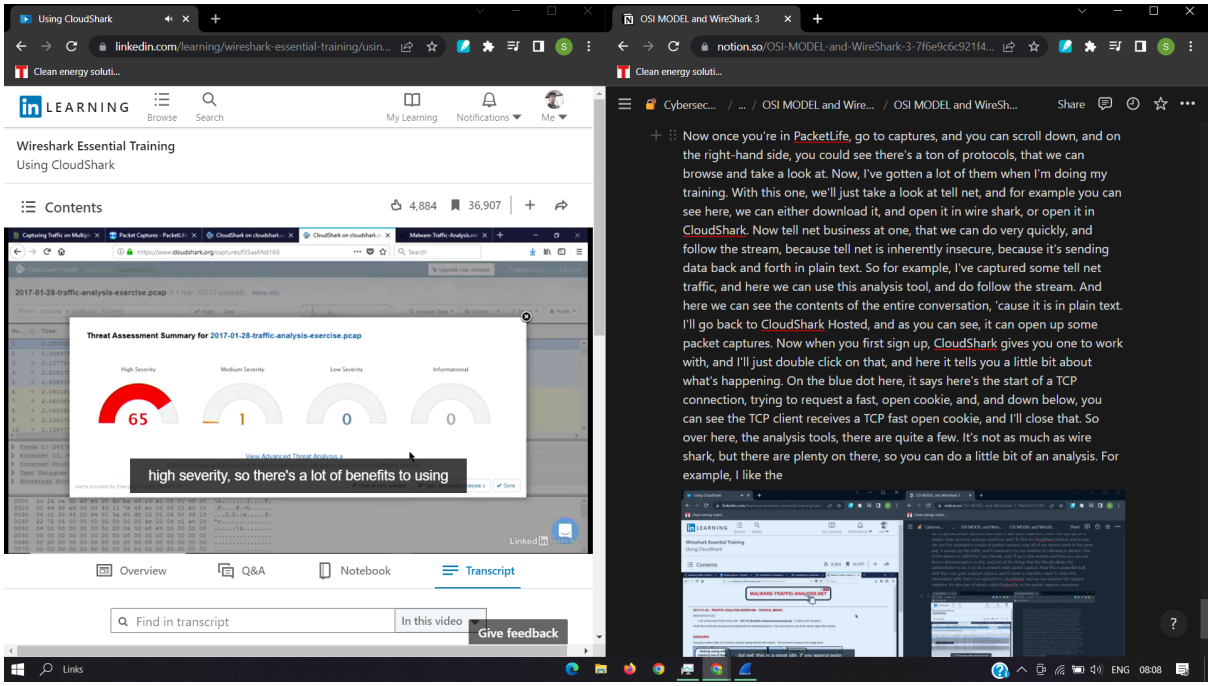


[Instructor] We all know that packet analysis is a valuable skill, that should be part of every network administrator's skillset. One site that makes it easy to learn about packet analysis, and share your packet captures, is CloudShark. This site helps you to do an analysis on the fly, to upload packet captures and share it with your coworkers, now I did sign up for a simple, basic account, and you could too, and I'll click on CloudShark Hosted, and as you can see I've uploaded a couple of packet captures, now all of our devices work in the same way, it scoops up the traffic, and it examines it to see whether it's allowed or denied. One of the devices is called the Cisco Meraki, and I'll go to this website and here you can see, there's documentation on this, and one of the things that the Meraki allows the administrator to do, is to do a network-wide packet capture. Now this is powerful stuff, with that I can grab a packet capture, and if I have a coworker I want to share this information with, then I can upload it to CloudShark, and we can examine the capture together. It's also part of what's called PacketLife, in the packet captures repository.



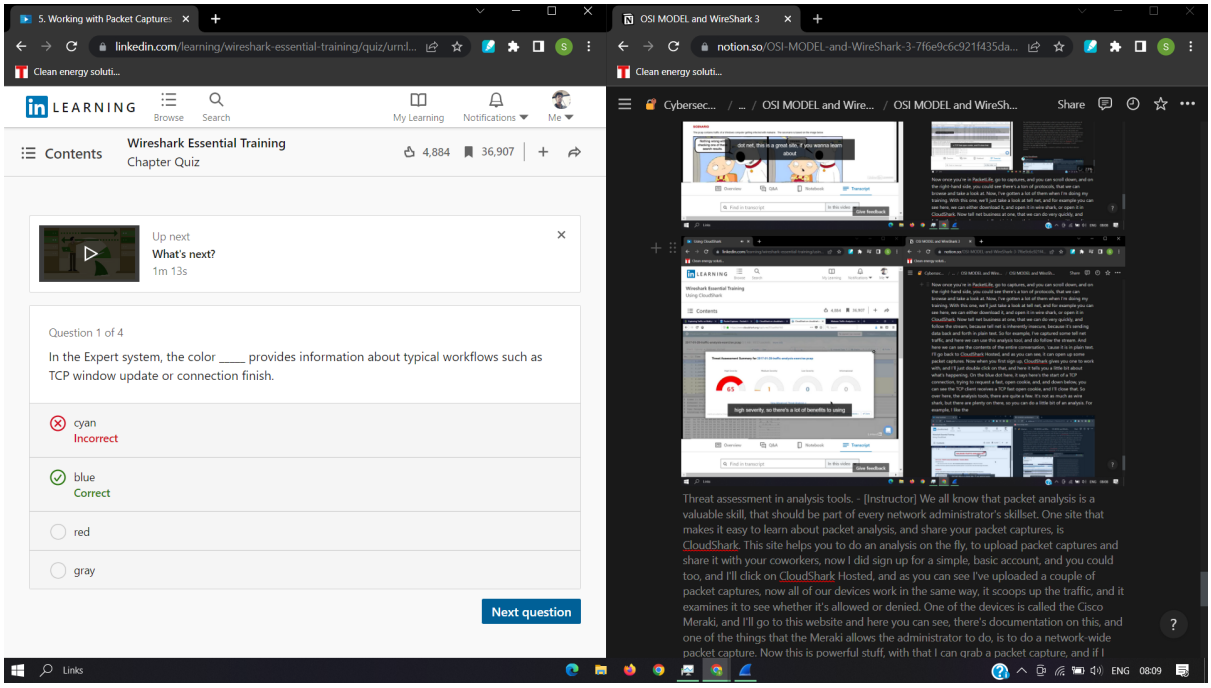
Now once you're in PacketLife, go to captures, and you can scroll down, and on the right-hand side, you could see there's a ton of protocols, that we can browse and take a look at. Now, I've gotten a lot of them when I'm doing my training. With this one, we'll just take a look at tell net, and for example you can see here, we can either download it, and open it in wire shark, or open it in CloudShark. Now tell net business at one, that we can do very quickly, and follow the stream, because tell net is inherently insecure, because it's sending data back and forth in plain text. So for example, I've captured some tell net traffic, and here we can use this analysis tool, and do follow the stream. And here we can see the contents of the entire conversation, 'cause it is in plain text. I'll go back to CloudShark Hosted, and as you can see, it can open up some packet captures. Now when you first sign up, CloudShark gives you one to work with, and I'll just double click on that, and here it tells you a little bit about what's happening. On the blue dot here, it says here's the start of a TCP connection, trying to request a fast, open cookie, and, and down below, you can see the TCP client receives a TCP fast open cookie, and I'll close that. So over here, the analysis tools, there are quite a few. It's not as much as wire shark, but there are plenty on there, so you can do a little bit of an analysis. For example, I like the

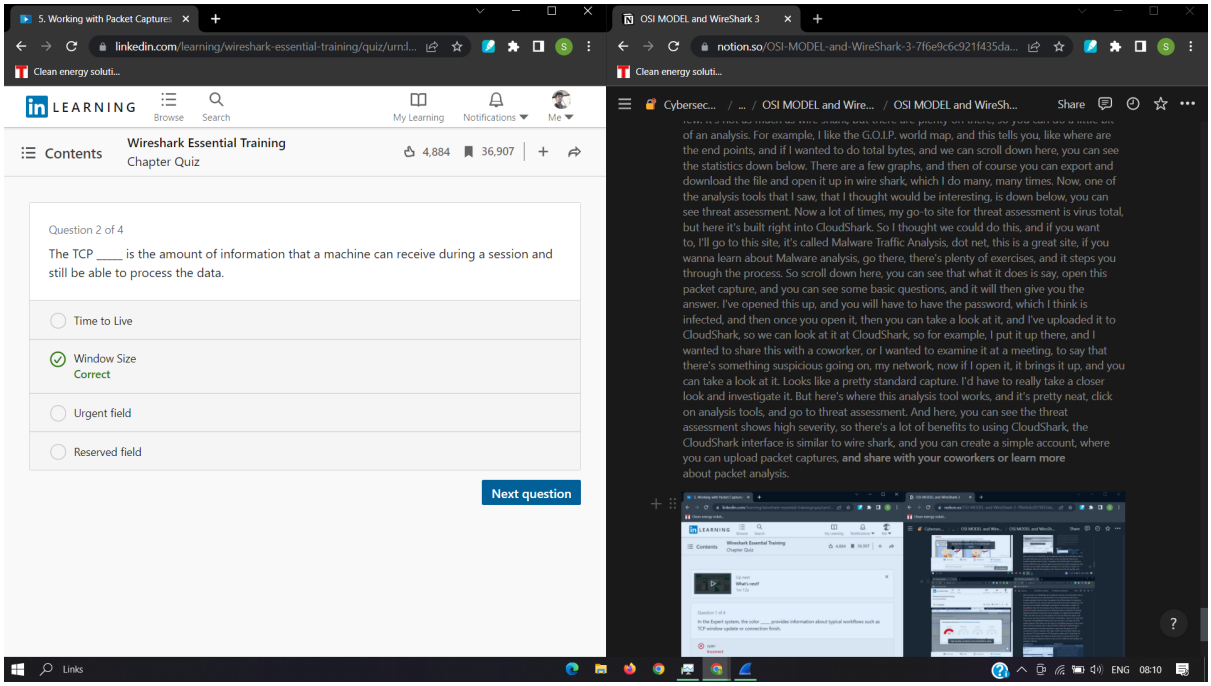

Using CloudShark
linkedin.com/learning/wireshark-essential-training/usin...
Clean energy soluti...
LEARNING
Browse
Search
My Learning
Notifications
Me
Wireshark Essential Training
Using CloudShark
Contents
4,884
36,907
MALWARE-TRAFFIC-ANALYSIS.NET
2017-01-28 - TRAFFIC ANALYSIS EXERCISE - THANKS, BRIAN.
ASSOCIATED FILES:
SCENARIO
dot net, this is a great site, if you wanna learn about
Overview
Q&A
Notebook
Transcript
Find in transcript
In this video
Give feedback
Links
OSI MODEL and WireShark 3
notion.so/OSI-MODEL-and-WireShark-3-7f6e9c6c921f4...
Clean energy soluti...
Cybersec...
OSI MODEL and Wire...
OSI MODEL and WireSh...
Share
Now once you're in PacketLife, go to captures, and you can scroll down, and on the right-hand side, you could see there's a ton of protocols, that we can browse and take a look at. Now, I've gotten a lot of them when I'm doing my training. With this one, we'll just take a look at tell net, and for example you can see here, we can either download it, and open it in wire shark, or open it in CloudShark. Now tell net business at one, that we can do very quickly, and
ENG
08:08

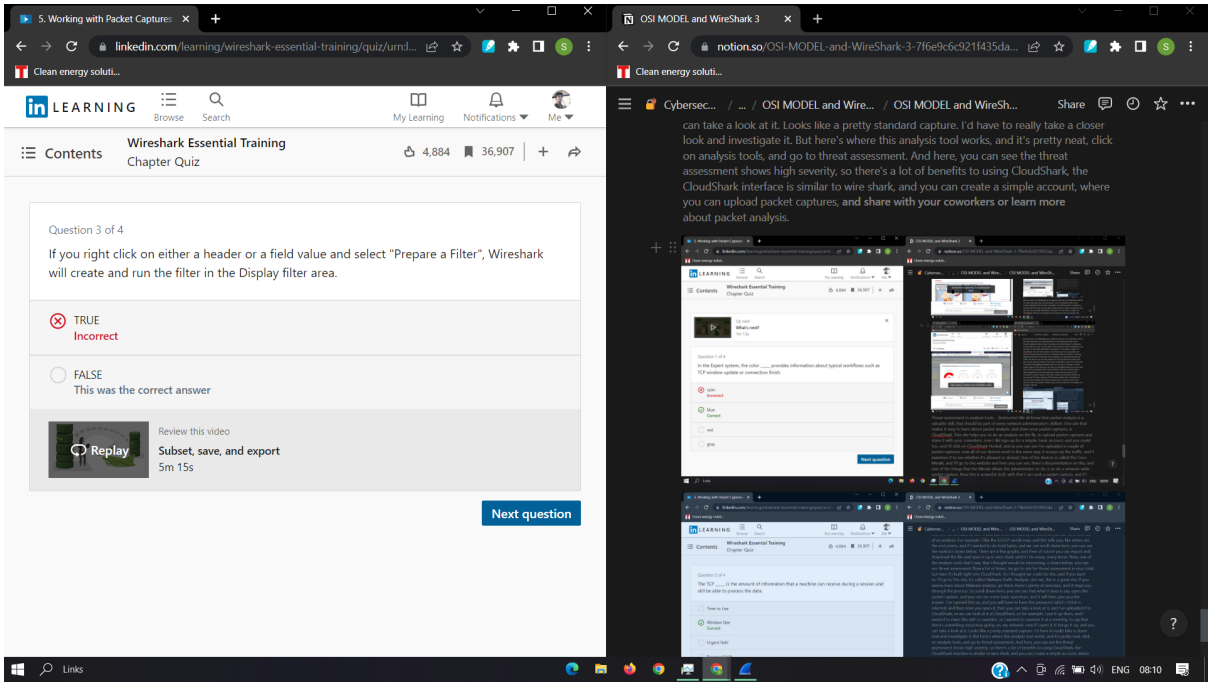


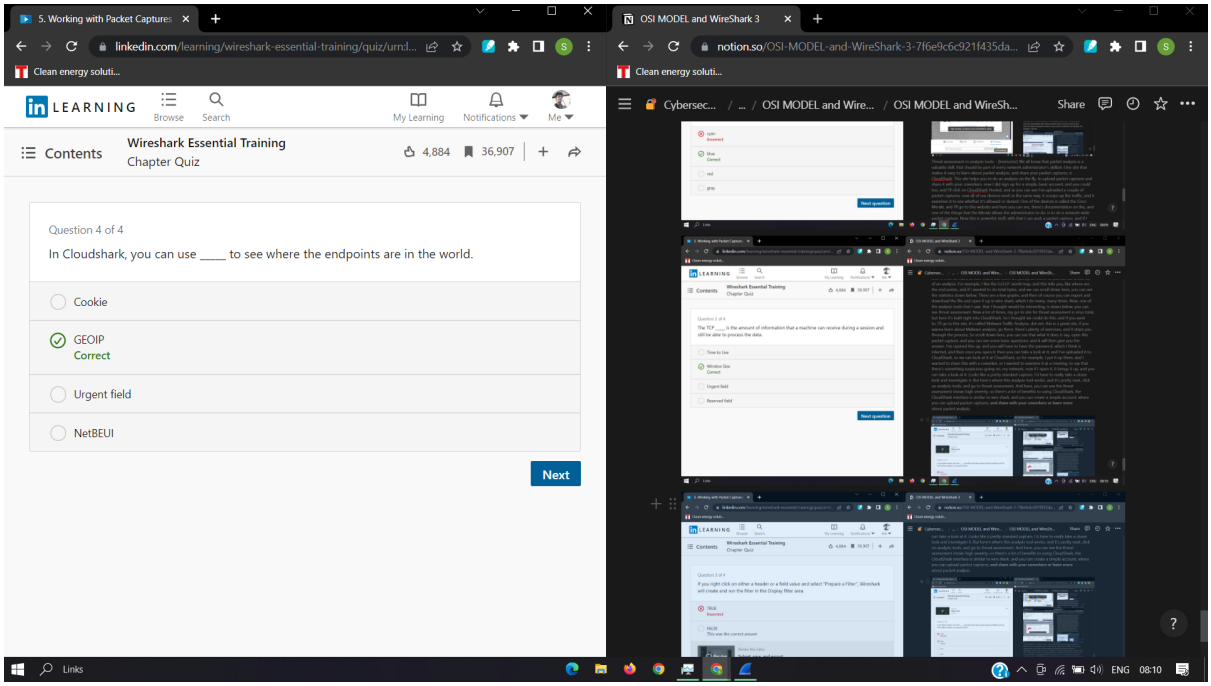
Threat assessment in analysis tools. - [Instructor] We all know that packet analysis is a valuable skill, that should be part of every network administrator's skillset. One site that makes it easy to learn about packet analysis, and share your packet captures, is CloudShark. This site helps you to do an analysis on the fly, to upload packet captures and share it with your coworkers, now I did sign up for a simple, basic account, and you could too, and I'll click on CloudShark Hosted, and as you can see I've uploaded a couple of packet captures, now all of our devices work in the same way, it scoops up the traffic, and it examines it to see whether it's allowed or denied. One of the devices is called the Cisco Meraki, and I'll go to this website and here you can see, there's documentation on this, and one of the things that the Meraki allows the administrator to do, is to do a network-wide packet capture. Now this is powerful stuff, with that I can grab a packet capture, and if I have a coworker I want to share this information with, then I can upload it to CloudShark, and we can examine the capture together. It's also part of what's called PacketLife, in the packet captures repository. Now once you're in PacketLife, go to captures, and you can scroll down, and on the right-hand side, you could see there's a ton of protocols, that we can browse and take a look at. Now, I've gotten a lot of them when I'm doing my training. With this one, we'll just take a look at tell net, and for example you can see here, we can either download it, and open it in wire shark, or open it in CloudShark. Now tell net business at one, that we can do very quickly, and follow the stream, because tell net is inherently insecure, because it's sending data back and forth in plain text. So for example, I've captured some tell net traffic, and here we can use this analysis tool, and do follow the stream. And here we can see the contents of the entire conversation, 'cause it is in plain text. I'll go back to CloudShark Hosted, and as you can see, it can open up some packet captures. Now when you first sign up, CloudShark gives you one to work with, and I'll just double click on that, and here it tells you a little bit about what's happening. On the blue dot here, it says here's the start of a TCP connection, trying to request a fast, open cookie, and, and down below, you can see the TCP client receives a TCP fast open cookie, and I'll close that. So over here, the analysis tools, there are quite a few. It's not as much as wire shark, but there are plenty on there, so you can do a little bit of an analysis. For example, I like the G.O.I.P. world map, and this tells you, like where are the end points, and if I wanted to do total bytes, and we can scroll down here, you can see the statistics down below. There are a few graphs, and then of course you can export and download the file and open it up in wire

shark, which I do many, many times. Now, one of the analysis tools that I saw, that I thought would be interesting, is down below, you can see threat assessment. Now a lot of times, my go-to site for threat assessment is virus total, but here it's built right into CloudShark. So I thought we could do this, and if you want to, I'll go to this site, it's called Malware Traffic Analysis, dot net, this is a great site, if you wanna learn about Malware analysis, go there, there's plenty of exercises, and it steps you through the process. So scroll down here, you can see that what it does is say, open this packet capture, and you can see some basic questions, and it will then give you the answer. I've opened this up, and you will have to have the password, which I think is infected, and then once you open it, then you can take a look at it, and I've uploaded it to CloudShark, so we can look at it at CloudShark, so for example, I put it up there, and I wanted to share this with a coworker, or I wanted to examine it at a meeting, to say that there's something suspicious going on, my network, now if I open it, it brings it up, and you can take a look at it. Looks like a pretty standard capture. I'd have to really take a closer look and investigate it. But here's where this analysis tool works, and it's pretty neat, click on analysis tools, and go to threat assessment. And here, you can see the threat assessment shows high severity, so there's a lot of benefits to using CloudShark, the CloudShark interface is similar to wire shark, and you can create a simple account, where you can upload packet captures, **and share with your coworkers or learn more**
about packet analysis.




5. Working with Packet Capture:
linkedin.com/learning/wireshark-essential-training/quiz/urn:l...
LEARNING
Browse
Search
My Learning
Notifications
Me
Contents
Wireshark Essential Training
Chapter Quiz
4,884
36,907
Question 2 of 4
The TCP ____ is the amount of information that a machine can receive during a session and still be able to process the data.
Time to Live
Window Size
Correct
Urgent field
Reserved field
Next question
OSI MODEL and WireShark 3
notion.so/OSI-MODEL-and-WireShark-3-7f6e9c6c921f435da...
Cybersec... / ... / OSI MODEL and Wire... / OSI MODEL and WireSh...
Share
of an analysis. For example, I like the G.O.I.P. world map, and this tells you, like where are the end points, and if I wanted to do total bytes, and we can scroll down here, you can see the statistics down below. There are a few graphs, and then of course you can export and download the file and open it up in wire shark, which I do many, many times. Now, one of the analysis tools that I saw, that I thought would be interesting, is down below, you can see threat assessment. Now a lot of times, my go-to site for threat assessment is virus total, but here it's built right into CloudShark. So I thought we could do this, and if you want to, I'll go to this site, it's called Malware Traffic Analysis, dot net, this is a great site, if you wanna learn about Malware analysis, go there, there's plenty of exercises, and it steps you through the process. So scroll down here, you can see that what it does is say, open this packet capture, and you can see some basic questions, and it will then give you the answer. I've opened this up, and you will have to have the password, which I think is infected, and then once you open it, then you can take a look at it, and I've uploaded it to CloudShark, so we can look at it at CloudShark, so for example, I put it up there, and I wanted to share this with a coworker, or I wanted to examine it at a meeting, to say that there's something suspicious going on, my network, now if I open it, it brings it up, and you can take a look at it. Looks like a pretty standard capture. I'd have to really take a closer look and investigate it. But here's where this analysis tool works, and it's pretty neat, click on analysis tools, and go to threat assessment. And here, you can see the threat assessment shows high severity, so there's a lot of benefits to using CloudShark, the CloudShark interface is similar to wire shark, and you can create a simple account, where you can upload packet captures, and share with your coworkers or learn more about packet analysis.
Links
ENG
08:10


5. Working with Packet Capture:
linkedin.com/learning/wireshark-essential-training/quiz/urn:l...
LEARNING
Browse
Search
My Learning
Notifications
Me
Contents
Wireshark Essential Training
Chapter Quiz
4,884
36,907
Question 3 of 4
If you right click on either a header or a field value and select "Prepare a Filter", Wireshark will create and run the filter in the Display filter area.
TRUE
Incorrect
FALSE
This was the correct answer
Replay
Review this video
Subset, save, and export
5m 15s
Next question
OSI MODEL and WireShark 3
notion.so/OSI-MODEL-and-WireShark-3-7f6e9c6c921f435da...
Cybersec... / ... / OSI MODEL and Wire... / OSI MODEL and WireSh...
Share
can take a look at it. Looks like a pretty standard capture. I'd have to really take a closer look and investigate it. But here's where this analysis tool works, and it's pretty neat, click on analysis tools, and go to threat assessment. And here, you can see the threat assessment shows high severity, so there's a lot of benefits to using CloudShark, the CloudShark interface is similar to wire shark, and you can create a simple account, where you can upload packet captures, and share with your coworkers or learn more about packet analysis.
Links
ENG
08:10


5. Working with Packet Capture:
linkedin.com/learning/wireshark-essential-training/quiz/urn:l...
Clean energy soluti...
LEARNING
Browse
Search
My Learning
Notifications
Me
Contents
Wireshark Essential Training
Chapter Quiz
4,884
36,907
Question 4 of 4
In Cloudshark, you can use ____ to see where the endpoints are in the world.
Cookie
GEOIP
Correct
Urgent field
NetBEUI
Next
Links
OSI MODEL and WireShark 3
notion.so/OSI-MODEL-and-WireShark-3-7f6e9c6c921f435da...
Clean energy soluti...
Cybersec...
OSI MODEL and Wire...
OSI MODEL and WireSh...
Share
ENG
08:10