Today I will talk about the free, downloadable network tool called Wire Shark. This is one of those tools that can do just about anything to inspect what is traveling in and out of your computer and your computer network but like the sound app audacity, and the video app that Barry showed recently, GIMP, it’s comprehensiveness and flexibility give it a steep learning curve.
All of us have heard about how Windows 10 is spying on what we do on our computers. It is. And if you read the 12,000 word usage agreement, you can find out exactly what information it gathers. You also know that by going into the privacy settings on W10, that you can limit that information gathering. But after all that is done, what is Microsoft still collecting? I will focus today on using Wire Shark to look at out going information from your computer and see if we can find out what this information is and maybe stop it.
By the way, this is a good article on the avast/avg website that you should read. A link to it will be given on Barry’s website. However, notice that they want to put cookies on your computer in order to use their website!
Here is an article from Forbes that talks about Windows spying. Links will be on Barry’s website.
And here is an article from ARS Technica. So the point is, W10 spying is happening. But what information is it gathering and how can we stop it?
Let’s get back to Wire Shark. This is how it looks when you first open it, without any scans running.
I have downloaded the most recent version of wire shark which is v2.6.4(v2.6.4-g29d48ec8)
Wire Shark

Note that you will also have to download and install WinPcap 4_1_3 which if you don’t have it installed, it will prompt you while you are doing the install.
Wire Shark will capture all network traffic going into and out of your computer. All of it! That is a huge amount of information that will overwhelm your attempts to understand what is happening. So the key is to filter what Wire Shark is capturing and then filter what it displays. Although there are several articles about capturing network traffic with WireShark, I don’t know how to do it, yet. All I can tell you about so far is capturing data from one or more of the network interface devices listed in the lower part of the screen.
But before we do that, let’s go down to the “interfaces” section, just below the “Capture” filter line, and turn off the interfaces that we don’t need to monitor. So here I have blown up that section of the WireShark screen that displays the “interfaces” or really, Network Interface Cards or NICs that I have on my laptop. There are 5 of them, 3 ethernet connections, a bluetooth connection and a Wifi connection. If you look close, only the wifi connection is active. (See the squiggly line).
So let’s turn off all the NICs except WiFi by going up to the menu – Capture – Options
That brings up this dialog box which again shows all the NICs that connect to your computer. Click the “Manage Interfaces” button in the lower RH corner.
Then this dialog box will come up showing all the interfaces. Turn off the ones you don’t need, i.e. all but wifi, by unchecking the boxes next to the NIC names.
Now when you go back to the main screen, all you will see is the one enabled interface.
The next thing we want to do is enter a capture filter. In the YouTube videos you will find extensive discussions on constructing strings of capture filter names. They may even say these are for capture filters. They are wrong. That is for display filters. You can only enter a few things for capture filters. As you type in the capture filter box it may turn red, that’s OK, as long as it is green when you finish typing your expression. If it remains red after you are done typing, then that is not a valid filter expression.
Pretty much the only thing you can do with this capture filter is to filter out the protocol. For our work today, we want to filter on TCP protocol. So if we do that, and start capturing, we only see TCP packets in our capture display. (Show that live.) This is still a lot of data, so now let us turn to the display filter.
We are now going to use the display filter, which is at the top of the WireShark screen, just under the menu bar, to focus in on the data that is being sent back to microsoft by W10. In particular, this is output data. This is where all the YouTube videos may be helpful. But wait, how do we know what data to look for? For this, we need to take a step back, out of WireShark, and go to one of our old standby networking tools, NetStat.
Bring up a command window and type in `NetStat -f`. The `-f` means that you will have “fully qualified” domain names for foreign addresses. i.e. you can see the name of who your computer is talking to. (go thru how by right clicking on the window and going to “properties”, you can change the command window from white text on black to black text on white making it easier to read)
<table>
<thead>
<tr>
<th>Real Networking Part 16</th>
</tr>
</thead>
</table>

**Microsoft IP Address Ranges:**

13.64.0.0 – 13.107.255.255  
52.145.0.0 – 52.141.255.255  

**NetStat**

What you are looking for are addresses in the range of 52.145.0.0 through 52.191.256.256. And for IP addresses in the range of 13.64.0.0 through 13.107.255.255. These are addresses that Microsoft owns and typically receive the data mined by Windows 10. Please write this down. If you don’t take anything else away from this presentation, take this.
If we look at the netstat results from my laptop at home we can see that it has established communication with one of those addresses on port 4023. Unfortunately, even a “fully qualified” address tells us nothing about the destination.
However, if we go to Whois.com and look up that address, we can see that it belongs to Microsoft. I would send out a link for this page but since the link is “Whois.com” I hope it isn’t necessary.
So going back to WireShark, let’s setup a capture filter for tcp and a display filter for outbound connections from the local computer and a destination of this MicroSoft ip. i.e. the display filter will read “ip.src == 10.54.1.32 && ip.dst == 52.173.28.179” and see what we get. (explain that it means a source IP address of my local computer, got this from netstat, AND (&&) destination address of the microsoft address).
After letting wireshark run this capture from my home laptop for about 20 minutes, we captured 3 relevant packets of information out of 9,469 total packets captured. Although this screen shot shows 6, 3 of them are Ack/Syn packets. They are all encrypted, I have no idea what information they contain. (When you do this live, expand the frames in the center to see if they give you any more information).
Using the advanced options on the Windows Firewall, we can set up an outbound rule to block port 4023. A link to this web page will be on Barry’s web page. (Go through this live if you have time)
Blocking Ports

In settings, go to “Update and Security”
Then click on “Windows Security”, you will see the shield for Windows Defender. Even if you don’t use windows defender for anti-virus, it controls your firewall, which you should be using.
Then click on “Firewall & Network Protection”, a dialog box for the firewall will pop up.
Blocking Ports

Click on “Advanced Settings”
Now you’ve done it. You’re into the heart of the windows firewall that filters everything going into and out of your computer. Note that there are inbound connection rules and outbound connection rules. We will be concerned today with outbound connection rules.
Note also that windows has defaults on the two types of connections: inbound connections must be explicitly allowed while outbound connections are allowed unless they are explicitly blocked. So let’s create an outbound rule blocking port 4023
First we click on “Outbound Rules” in the upper LH corner of the Windows Advanced Firewall dialog.
Holy guacamole! There are hundreds of rules already created. All of them allow connections to any port, any program, any local and any remote address. My computer is a literal fountainhead of outbound information. The only rule that blocks anything is the one that I already created on port 4023. Let’s duplicate that. Click on “New Rule” in the upper RH corner. Most of us also have a firewall on our routers and you may be able to block ports there as well. Since each router is different, I will concentrate on the common Windows firewall for now.
In the “New Outbound Rule Wizard”, click on “Port”, and then “Next”
In the “New Outbound Rule Wizard”, leave the “TCP” button selected and type “9368” or whatever port you find on your computer that is communicating within the range of IP addresses belonging to Microsoft that was on a previous slide. Click “Next”.
In the “New Outbound Rule Wizard”, leave the “Block the Connection” button selected. Click Next
In the “New Outbound Rule Wizard”, leave all the boxes checked on this screen. Click Next
In the “New Outbound Rule Wizard”, give the rule a name and brief description and click finish.
When you go back to the Windows firewall page, you will see your new rule at the top of the page.
If you run `netstat` again, you will see that communications on this port have ceased.
Windows responds by opening up a different port to communicate to the ip address 13.89.187.212. Now what? We should look at blocking the range of ip addresses in the earlier slide. I have not yet found a way to do this but this is a topic for future sessions. It has something to do with using Perl Regular Expressions in the display filter box but I have yet to find the syntax that works. Another possibility is to block the program or dll that is sending the data but that is also a future topic. Again, you may be able to block a range of ip addresses on your router’s firewall.
Here is what the firewall rules page looks like on my router. All unsolicited inputs are blocked unless specifically allowed here. All outputs are allowed unless specifically blocked here. There is a limited amount of things you can do. Again, I don’t see a way you can block a range of IP addresses.
That’s enough on WireShark for today. After the break, we will talk about AntiVirus programs.
Last week we had some discussions about AV tools and which was best. I will repeat part of a presentation I gave last April with some updates. I will use two basic references that I respect very much. One is a blog by Brian Krebs a former reporter on security topics for the Washington Post. The other is Bruce Schneier a respected writer on security topics. Both of them are not only knowledgeable, but they are eloquent. Both of which are essential in communication about highly technical subjects.
AV software is a fundamental part of what Mr. Schneier would call PET or Privacy Enhancing Technology. We have talked about this several times at this club and reviewed the ratings from several different sources. We have also noted the fact that most sites have some vested interest in the reviews because they get advertising from the AV companies.
I have belonged to consumers reports for many years and have great respect for their testing labs. Each year they rate AV programs and if you read their reviews, you will see that the ratings are very close. If you try and look behind the ratings, you will find almost no information about the specifics of how they do their testing. I was surprised to see that Avast was not on their recommended list. This was obviously before Avast bought AVG.
I was also surprised to see that Symantec and Kaspersky, two “Pay for” versions of AV s/w were listed as “Best Buy”. I wouldn’t recommend either. Symantec because it is so intrusive and Kaspersky because, well it’s Kaspersky.
So how have things changed since 2016? Here are the consumers reports reviews for 2018 products. In the category of pay for security suites, here are the ratings, BitDefender is at the top, followed by Norton Internet Security, and then Trend Micro and Kaspersky.
These top four are followed by these four, notice Avast is eighth.
And then these four, AVG is near the bottom. But notice, they are only separated by a total of 9 points between the top 11. All are recommended except the last, G-Data.
If we look at the stand-alone AV packages, the story is different. Here are the top four: Bitdefender, Avast, Avira and AVG.
These are followed by: Kaspersky, Microsoft W10 defender and Sophos. Here we see 14 points separating the top 6 packages. None of the last 3 are recommended.
There are two security experts that I respect very much. One of them is Brian Krebs.
In Mr. Krebs “Tools for a Safer PC” he says use any of these tools just keep it updated. If you buy an AV program, don’t renew it at the end of the subscription. Renewals are where the companies make most of their money. Buy the new version which will usually be on sale, especially at the end of the year.
when folks are buying tax programs.
In Bruce Schneier’s Book “Data and Goliath” in Chapter 15 “Solutions for the rest of us” and a sub section entitled “Avoid Surveillance” .....
he recommends what Barry has long been saying “You can use DuckDuckGo for internet searches”.

W10 will reset, change or add to your privacy settings after each update.
Open Settings.
Click on “Security & Updates”, then “Advanced Options” then “Privacy Settings”
Go through each of the settings on the left side of the screen and reset them to what you want.

Now as we go out into the world, love one another, keep your anti-virus definitions updated and do your back-ups.