East SIG Report July 2022

Neil Muller

Host Frank Maher opened the May meeting, again from home via Zoom. After welcoming members, Frank outlined the nights agenda shown below:

Presentation 1: Q&A with John Hall
Presentation 2: Best free VPN by Trevor Hudson
Presentation 3: Browser Finger Printing and other topics by Stewart Bedford

The first presentation of the night was by **John Hall** presenting Q&A in George Skarbek's absence.

Q. Over the last few days, the audio from YouTube videos is what I'd call very muddy or "bassy", and not very clear. I've looked at the Sound section in Windows Control Panel and the tests I've done show everything is working fine. I didn't want to do anything before the meeting, in case I had no sound, so I plan to test it further at a less time critical time, say on the weekend.

A. If you right click on the speaker icon on the Taskbar, a small menu will come up. Have a look and see if "Spatial sound" is turned off. That option counteracts the effect of playing sound in a large hall.
The sound on YouTube may be the fault. The volume control on a YouTube video operates independently to your computers system volume control. Adjust those and the sound may improve.
As we are only a day or so past Microsoft Patch Tuesday, I often find that Window updates are installing in the background without the user being aware. This can use up system resources and can affect Windows operations. After a reboot things often return to normal, so a reboot may help.

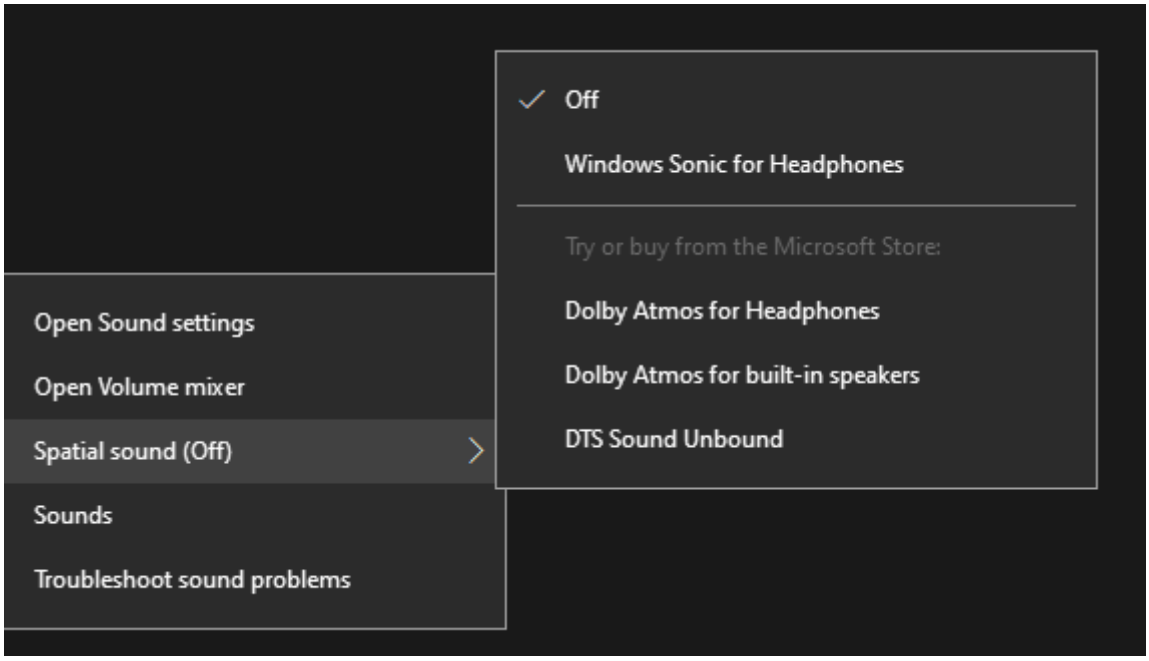

Figure 1 – Windows system sound menus & settings

Q. John, I notice that the lighting on your face is very clear and wonder what sort of lighting you use?

A. It's called a Hue light. I have one on each side and can adjust them from my phone. I purchased them from Amazon during a Prime day sale. They were still rather pricey though.

Figure 2 – Philips Hue light set

Q. For the last 6 months I've had two monitors connected to my computer. I find the setup very useful but have one annoyance that I've yet to overcome. Often, I'll only need to work with one monitor, so only turn the main monitor on. However, if I try to open a program that was last displayed and closed on the second monitor, nothing is displayed. At first I thought it was a fault but realised Windows was displaying the program out of view on the second monitor. I would then have to turn on the second monitor to be able to view the program. To overcome this annoyance, when I'm about to shut down my computer, I'll drag all the programs open on the second monitor onto the first and close them from there. This approach ensures that when I start my computer the next day, all programs will open from the main monitor. Is there an easier solution?

A. Right click on a blank area of your desktop and you will have the option to select Display settings. From there you can either extend your display over 2 screens or have 2 separate screens. If you change the way you have your screens setup, it may make life easier for you.

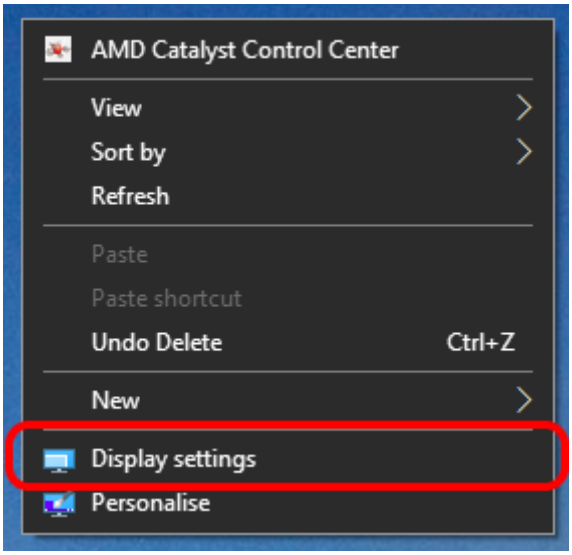

Figure 3 – Windows Display settings menu

[Stewart Gruneklee from iHelp answers] When the second monitor is turned off (in standby mode), use the shortcut Shift + Win Key + Arrow key to move the invisible but open program to the main monitor. You can use this shortcut to cycle the program between screens.

[Peter Carpenter replies] Because the second monitor is on standby, Windows still recognises its presence and that is why the program remains on the second monitor. If the power to the second monitor is turned off, Windows will acknowledge there are fewer screens. Windows will then automatically move the application that was previously shut down on the second screen, to the active screen.

Q. My living room faces north and it is very bright during the day. I was wondering about purchasing a computer screen with a large number of nits. Does anyone have any experience with screens with high nit ratings? People that work outdoors would need such screens so they must be available.

A. No one was able to answer this question.

Following Q&A, **Trevor Hudson** presented a new video he'd prepared and uploaded to his YouTube channel "PC Techtips", titled **"Best free VPN ProtonVPN".**

Figure 4 – YouTube graphic for “Best Free VPN ProtonVPN”

A VPN is a Virtual Private Network which provides privacy, by encrypting your online internet traffic through encrypted servers. It disguises your home location, so your real IP Address is untraceable. A user may use a VPN to access geo-blocked content from another country or to protect your identity on your computer at home or when using public or shared Wi-Fi. This ensures your data will be kept private when on the internet.

Proton VPN has been recommended as the best free VPN from review website TechRadar, by Kevin Stratvert and many other sites. Trevor’s video demonstrates how to obtain, install and run ProtonVPN. The free version gives servers in 3 countries (Japan, Netherlands and USA), medium VPN speed and one VPN connection. For those wishing to view content from the United Kingdom or other countries than the 3 offered by ProtonVPN, Trevor has listed other free VPNs in the description under the YouTube video. PrivadoVPN free at https://privadovpn.com/ is second on the list and has servers in the UK which Trevor uses to access the BBC TV and radio.

To test the effectiveness when connected to a VPN, Trevor recommends undertaking a leak test from sites http://ipleak.net/ and http://browserleaks.com/ip. An IP leak test is used to determine whether your real IP address is visible to others while connected to a VPN. This could occur when your computer unknowingly uses default servers rather than the anonymous VPN servers.

Trevor’s video can be found on YouTube by searching the title “Best free VPN ProtonVPN” or using the link https://tinyurl.com/2p8j9xut.

The main presentation was by **Stewart Bedford** on browser fingerprinting and a number of other internet security related topics**.**

Find your public IP address

An IP address or Internet Protocol address, is a series of numbers that identifies any device on a network. Computers use IP addresses to communicate with each other, both over the internet as well as on other networks. To quickly establish your public IP address, type the letters “IP” in your browser search bar. Most users would not be concerned with their IP address, however Stewart said he often refers to his. He’ll do this when using a VPN to determine where his data is coming from.

An IP address can be either dynamic or static. Most IP addresses are dynamic and you’ll find your ISP (Internet Service Provider) will change your IP address fairly frequently. A static IP address is not normally required by the average user, unless running a mail server or IP security cameras. Usually you have to pay extra for a static address.

You can get more information from dedicated sites like https://whatsmyip.com/ by logging on their site. The information obtained includes; your public IPv4 address, country, latitude & longitude, timezone, LAN, screen resolution, computer OS and your browser. The term used by websites such as WhatsMyIP.com to attain this information is called “browser fingerprinting”

Figure 5 – Whats My IP homepage

Browser fingerprinting

Browser fingerprinting is a powerful method that websites use to obtain information about your browser type and version, as well as your operating system, active plugins, time zone, language, screen resolution and various other active settings.

Stewart indicated, that although this information may appear generic, a recent analysis showed only one in 286,777 other browsers shared an identical fingerprint. This information is then used to track your browser activity and build a profile. Companies also collect fingerprints and on sell them.

Stewart alerted members to the website http://CoverYourTracks.eff.org , which has an excellent article on fingerprinting and how to combat it. The website results from Stewart's computer in Figure 6, showed he only had "some protection". This surprised Stewart as he'd spent some time locking down his security settings.

Figure 6 – CoverYourTrack.eff.org

Stewart mentioned the following tips to mitigate against browser fingerprinting

1. Use the Firefox browser and engage its privacy options. This is not a perfect solution but it does help.
2. Use the incognito mode of your browser, to reduce fingerprinting. Again, while it's not a perfect solution, it does reduce the amount of information shared with others.
3. Use the Tor browser. Tor is an extremely secure and private browser. It includes anti-fingerprinting features, such as cloaking your operating system and blocking revealing information like your time zone and language preferences. Without these details, it's much harder for your browser to be fingerprinted.
4. Use a VPN. A VPN doesn't prevent websites from using JavaScripts HTTP headers to collect browser fingerprints. It removes (hides) your address from the headers, but your fingerprint still might be unique.

The solution to stopping websites from collecting your fingerprint data, is to use a mixture of all the above tips, along with using a VPN.

Radio Apps on your phone

The next topic Stewart presented was on Radio apps you may have on your phone. When local radio stations 3AW and the ABC recently required Stewart to register their apps on his phone, he deleted both and installed Simple Radio instead. He could have used a false name and email address, but chose to delete both apps and install Simple Radio.

Simple Radio has 50,000 stations and no registration is required. The free version comes with ads, but there is a paid for, ad free version, which includes a sleep timer. Stewart uses the free version, with a separate free sleep timer from the Google Play store.

Simple Radio is available for Android and iPhones and gives access to FM Radio stations, AM Radio, Internet Radio Online and Free radio stations worldwide.

Figure 7 – Simple Radio

Free Encrypted Mail Client

From time-to-time Stewart uses an encrypted mail client for some of his personal emails. He uses the free version of Protonmail from an app on his phone, or via a web browser on his computer. Protonmail is the same Swiss company that Trevor mentioned in the previous presentation on ProtonVPN. Stewart uses Protonmail when he absolutely needs to ensure his email is secure and cannot be intercepted by others, such as when dealing with the government, tax department etc..

Protonmail is an end-to-end encrypted email service founded in Geneva, Switzerland. Protonmail uses client-side encryption to protect email content and user data **before** your emails are sent to Protonmail servers. Client-side encryption is more secure than other common email providers such as Gmail and Outlook, where emails are encrypted once they reach their servers.

Proton's policy is that your data belongs to you. That's why they use end-to-end encryption and zero-access encryption, to ensure that only you can read emails. Proton cannot read or give anyone else access to your emails. Their encryption happens automatically, with no special software or tech skills required.

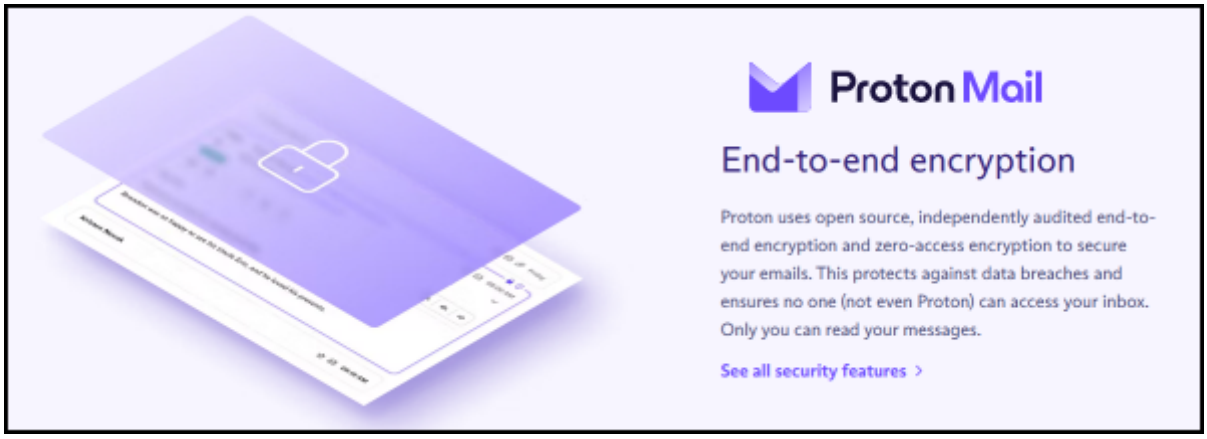

Figure 8 – Protonmail Android App

"Innocent" quizzes and challenges on Facebook

Many "innocent" quizzes and challenges on Facebook are designed to glean information about you, to build a marketing profile. Some have more sinister intent, being designed to gather personal information with fraud in mind.

Have you ever taken one of those ridiculous and inane quizzes on Facebook? If so, all your private information is likely being shared or sold.

Social media quizzes often ask the same questions your financial organisations use for security purposes, to verify your identity when you need to change your password or access your account without a

password. Some examples include the name of your hometown or the name of your first pet.

Other examples Stewart has seen are: “What was the first car you owned?”, “What is your mother’s maiden name?” or “What is the name of the street you grew up on?”. These are common security questions for insurance, banking and credit card accounts.

Downloading from YouTube (an update)

This is an update to a presentation Stewart gave to East SIG in September 2018, on downloading videos from YouTube. The meeting report of that presentation appeared in PCUpdate the following month, October 2018.

Watching videos on YouTube can be quite painful when the videos are plagued by the interruptions from advertisements. When Stewart finds something of interest that he wants to watch from YouTube, he’ll download the video and watch it ad free later. Many full movies are often available on YouTube, as he demonstrated in the example shown in Figure 9.

The technique Stuart uses involves working from the command line. In his previous presentation (September 2018) he used the command line downloader “youtube-dl”. This disappeared for a while and has now reappeared. However, Stewart now uses “yt-dlp” a fork of youtube-dl which works in Linux and Windows. Stuart proceeded to described how he uses “yt-dlp” in Windows.

Step 1 – For Windows users, download the executable file yt-dlp.exe 2022.06.22.1 (the current version at the time of his presentation) from https://www.videohelp.com/download/yt-dlp.exe). Although it has an .exe extension, the file can only be executed from a command line.

Step 2 – Move the file “yt-dlp.exe” in an existing folder or create a new one, and execute the exe file from there. The downloaded YouTube video files will be sent to that folder.

Step 3 – From the command prompt navigate to the folder, “YT” in Stewart’s example (Figure 9) and type “yt-dlp” and a space.

Step 4 – From YouTube copy the URL of the video you wish to download and paste it to the command line in step 3 and then press Enter.

Step 5 – After a short period, the file will be downloaded to the “YT” folder on the Desktop. It can then be watched on a phone, computer or TV without ads.

Stewart finds working from the command line is faster and has less system overheads. The process becomes second nature once completed a few times. (An annotated version shown in red in Figure 9 shows the process used.)

Figure 9 – Command Window using yt-dlp.exe

Recover and revive old black & white photos or negatives

If you have old black and white photos or even just the negatives, they can be recovered and revived with your smart phone. Prints can be scanned and “colorized” and negatives can be turned into positives and then “colorised”

To conclude his presentation, Stewart described how he took an old black & white negative and by shining a back light through the negative, took a photograph of the negative using the camera on his smart phone. Using the Android app “Photo negative scanner”, the resultant image was then colorised using a program called “Colorize Images”. Stewart then used Faststone Image Viewer to dial down the saturation, yielding

a very realistic result.

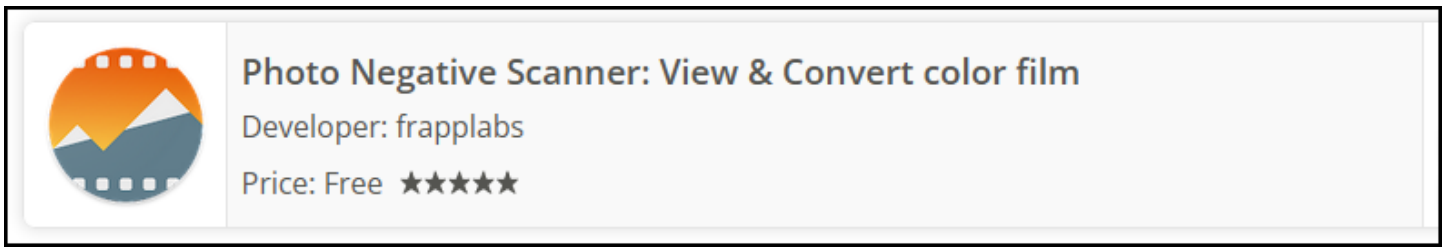

Figure10 – Photo Negative Scanner for Android

Figure11 – Colorize Images for Android

The meeting concluded with questions to Stewart on topics covered in his presentation, followed by informal discussions between audience members on a number of other topics.