East SIG Report – September 2023

After welcoming members to the September meeting of East SIG, host Dave Botherway outlined the nights agenda below:

Presentation 1: **Q&A** with George Skarbek Presentation 2: **Linux Mint Tutorials** by Trevor Hudson Presentation 3: **Tips and Tricks** by Peter Carpenter Presentation 4: **Cleansing a PC before handover** by George Skarbek

<u>Q&A</u> by George Skarbek.

Question 1: When I'm finished my computing for the day, I've been in the habit of using Sleep mode rather than shutting the computer down. I have 3 discs attached to my computer, but these are on a different power point, so obviously keep running. I was of the belief that the hard discs shouldn't be turned off regularly, so I've left them running. Have you got any advice on this procedure?

Answer 1: I would recommend you switch the discs off. Especially for rotating discs, as the bearings and head actuator have a finite life. I turn mine off simply to save wear and tear on the bearings rather than having then running over night unnecessarily. Turning the discs off will also save you a small amount of electricity over their 5-year life. If you're not using them, or running things in the background overnight, my recommendation is switch them off. It will prolong the life of your hard drive and save a little bit of money in the process.



Figure 1 – SATA Hard Drive internal components

Question 2: I have 3 discs inside my computer, comprising of 2 SSDs and a rotating hard drive. Would you advocate turning the PC off overnight or using Sleep mode?

Answer 2: The disc life with SSDs is quite different to rotating discs, as you don't have any wear and tear, but I would still recommend turning your PC off. I can't see what you gain from leaving

it on overnight. Leaving the PC in Sleep mode overnight only saves you a few seconds when you turn your computer on at startup. When your laptop is in sleep mode, the RAM retains information about open programs and data. If a hacker gained access to your laptop, they can use this retained information to their advantage in what is known as a "cold boot attack."

[During sleep mode, only your PC's RAM requires power to stay functional. Since other elements such as the screen, processor, and hard drive are turned off, your PC requires very little power to operate.]



Figure 2 – Sleep mode

Question 3: There is a school of thought that you should leave a computer on all the time, especially those with rotating hard drives, so the PC stays at the ambient temperature. Whereas if you turn it off, it cools down so when you turn it on the next day, it has to heat up again. The fluctuation in temperature is an argument for leaving a PC on. I turn mine off as I don't believe the argument, but what is your view?

Answer 3: I don't believe the ambient temperature argument either. When you're at home the ambient temperature shouldn't drop any more than 10 degrees at the most, so you're not going to get much differential heating in that range.

Question 4: A friend bought a laptop with an SSD and after about 17 months the SSD died. Although it was out of the 12-month warrantee, he complained to ASUS saying it would be expected that the warrantee for the SSD should be longer, as SSDs are more reliable. He asked for a new SSD, but ASUS refused, so he went out and bought a new one. What is the reasonable life of an SSD? There are no moving parts so what would break down?

Answer 4: The individual cells of an SSD have a finite life and are not like magnetic media that wears down slowly. The cell in an SSD gets charged one way then another, as it moves from a zero to one and back again. Doing that consistently causes the cells to wear. The Mean Time Between Failures (MTBF) is generally over a million hours. It doesn't mean the SSD will last that long, as that figure is an average, where some will die sooner others last longer. I believe the useful life for an SSD is around 8 years. Programs that are very aggressive with writing to an SSD is the main cause of cells wearing.

Question 5: I have Windows 11 on my machine and I've been looking to rationalise my apps. I have an app called "Windows Assessment and Deployment Get Windows 10". The app is 7 Gigabytes in size so do I need it?

Answer 5: My gut feeling is you don't want it. I have no intention to upgrade my Windows 10 to 11 personally. Windows 11 has a few extra nice features, but quite a few things require an extra one or two clicks and are buried.

[Dave Botherway] I would support deleting that app, particularly for anything that big. I'd copy it out and then back it up. I'd then delete the app from Windows 11 and see what happens.

Linux Mint Tutorials by Trevor Hudson

As a recent convert to Linux, Trevor Hudson presented two short videos he prepared to help new Linux users. These and other videos that he plans to add in the future can be found on his YouTube Channel "Linux Mint 1080 Tutorials".

The first video which is titled "Hide Linux Screen Icons", outlines how to hide screen icons and the Linux Mint watermark from the desktop. The video can be found at https://www.youtube.com/watch?v=tQjHbXAO9LQ

The second video is titled "Delete Linux Desktop Icons", outlines 2 methods to delete desktop icons in Linux Mint.

This video can be viewed at https://www.youtube.com/watch?v=PCBwT102vIA



Figure 3 – Linux Mint 1080 Tutorials

Tips and Tricks by Peter Carpenter

In this presentation, Peter Carpenter outlined how he extended the life of a keyboard and phone using clever low-cost solutions.

Peter's standard keyboard had a broken front leg, but even with the legs folded up, the keyboard rocked when used on an uneven surface. Peter felt if the forward-facing legs of the keyboard were soft legs, that might solve the problem of the keyboard rocking. To test his theory, Peter used adhesive to attach 2 square pieces of foam to the base of the keyboard as shown in figure 4. The foam raised the front of the keyboard and prevented the keyboard from rocking when used on an uneven surface. This trick extended the life of a perfectly good keyboard with this clever low-cost solution.



Figure 4 – Peter's computer keyboard repair.

When Peter's wife's iPhone 7 would only charge intermittently, Peter believed cleaning the charging socket on the iPhone might solve the problem. Using a bright light and tooth pick, Peter was able to carefully clear accumulated material from the charging socket on the iPhone. Then using some "Electrical Clean and Lube" on a fine flat artist's brush, he carefully cleaned the connectors within the charging socket.

When the charging cable was again connected to the iPhone, charging worked perfectly and was no longer intermittent. Peter used a brush to apply the "Electrical Clean and Lube", as it's unwise to spray isopropyl alcohol straight onto the socket. If the liquid had found its way inside and onto internal components it could have damage them.



Figure 5 – Peter's iPhone 7 cleaning utensils.

Peters' moral was if something fails, don't give up on it, try to repair it first.

<u>Cleansing a Windows computer before handover</u> by George Skarbek

In this presentation George Skarbek explains how to clean personnel information from a Windows computer before it's ready for donation or sale. The easiest solution to clean a Windows PC is to put it back to its factory settings. However, this option would wipe all data and any software installed, other than the Windows operating system. In his presentation however, George demonstrated how to remove all personal data, but retain existing software such as MS Office etc for use by the new owner, using only applications within Windows.

Pre cleaning issues

The owner of an ASUS laptop running Windows 10 had asked George if he could remove all personnel information from the computer, prior to it being donated. The PC had become so slow to respond to commands, it was unusable. George referred to it as almost "dead", as it was that slow.

Before cleaning of personnel data from the computer could commence, two problems had to be solved:

- 1. The Administer password was unknown and needed to be identified.
- 2. A rogue program had found its way onto the computer, slowing it to a crawl. This malware needed to be found and removed in order for the computer to be usable.

Identifying and removing the rogue malware

Initially George was unsure what was causing the computer to run slow. His first step was to open "Task Manager" and select the "Startup" tab, (Figure 6) where he disabled all programs except the virus checker. This procedure stopped programs loading into RAM unnecessarily, but did not delete them from the computer.

🙀 Task Manager					×
File Options View	\frown				
Processes Performance App history	Startup Users Details	Services			
			Last BIOS tim	e: 4.0 se	conds
Name	Publisher	Status	Startup impact		
Windows Security notificati	Microsoft Corporation	Enabled	Not measured		
Skype	Skype	Disabled	None		
Phone Link	Microsoft Corporation	Disabled	None		
PC App Store	Fast Corporate LTD.	Disabled	None		
PC App Store	Fast Corporate LTD.	Disabled	None		
S CCleaner	Piriform Software Ltd	Disabled	None		
💽 Microsoft Edge	Microsoft Corporation	Disabled	None		
Microsoft OneDrive	Microsoft Corporation	Disabled	None		
ManyDVD Application	SlySoft, Inc.	Disabled	None		
📥 Logitech Download Assistant	Logitech	Disabled	None		
SmartAudio CPL (32bit)	Conexant Systems, Inc.	Disabled	None		
File Association Helper	WinZip Computing, S.L.	Disabled	None		
WinZip Preloader	WinZip Computing	Disabled	None		
🗐 WinZip Update Notifier	Corel Corporation	Disabled	None		
🌋 Conexant High Definition A	Conexant Systems, Inc.	Disabled	None		
Fewer details				Disab	le

Figure 6 – Windows Startup

On rebooting the computer there was no change, and the computer was still running as slow as before. The malware was continuously paging data to the hard drive, causing the PC to slow to a crawl. This indicated the malware was not in startup.

The next step was to again open "Task Manager" and from the "Performance" tab, click the link on the bottom of that window to open the "Resource Monitor". (Figure 7)



Figure 7 – Windows Task Manager

In "Resource Monitor" George selected the "Overview" tab to view the "Disk" panel, to see what was writing to the disk. Here he clicked the "total bytes written" column, to see which apps were writing the most data to the hard drive. (Figure 8)

As that failed to identify the culprit, next view the "Memory" panel in "Resource Monitor" and the select the column header for "Hard Faults/sec". (Figure 8) This helped George identify the malware, as the app had a "Hard Faults/sec" reading over 100. Generally, a reading under 10 is the usual maximum found in that column.

Parourse Monitor											÷
File Monitor Help											~
Overview CPU Memory	Disk M	vetwork									
CPU		📕 4% CPU Usage			1	109% Maximum	Frequency		A 1	0	Views 🖛
Image	PID	Description	Status	T	reads	CPU Averag	e CPU		^	CPU	100% T
Zoom.exe	5576	Zoom Meetings	Running		278	1	1.94				
perfmon.exe	14036	Resource and Performance Monito	Running		21	0	0.60				
System interrupts	1200.00	Deferred Procedule Calls and inter	Running		1.	0	0.26				
dwm.exe	16804	Desktop Window Manager	Running		17	0	0.26				
C čsrss.exe	1592		Running		16	0	0.21				
System	4	NT Kernel & System	Running		320	0	0.18				
Taskerige.exe	3536	Task Manager	Running		23	0	0.17			60 Seconds	C %0
MsMpEng.exe	4328		Running		56	0	0.12			Disk	1 KB/sec
Claudiada and	.0100	Medana A. K. Daine Couch lost	• n		4	^	0.50		~		
Disk		555532 B/sec Dis	k VO			1% Highest Acti	ve Time		•		
Image PID File				Read (B/sec)	Write (B/sec)	Total (B/sec)	I/O Priority Re	sponse Time	^		
MsMpEng.exe 4328 C:\/	Program File	es\WinZip Smart Monitor\WinZip Sn	art Monitor S	216,704	0	216,704	Normal	0			
System 4 C:\\	Wordows (S)	stem32\LogFiles\WMI\NetCum.etl		0	131,072	131, 1 Int	al (B/sec): Average nur	mber of 0			
MsMpEng.exe 4328 C:\\	Program File	es (x86)\Common Files\Nuance\dgn	svc.exe	94,080	0	94,4 by	tes per second read from	m and 0			
System 4 C:\\	SLogFile (NI	(FS Volume Log)		0	85, 197	85, 100	tten to the file in the la	st minute		Network	1 Mbps
MsMpEng.exe 4328 C:\/	Program File	rs (x86)\Common Files (huance\log	erservice.exe	42,112	0	42,112	Normal	0			
System 4 C:\\	Users\Georg	e\AppData\Local\ConnectedDevice	Platform\2a2	0	40,141	40,141	Background	0			
System 4' C:\	ProgramDat	a/Microsoft/Search/Data/Applicatio	ns\Windows\	6	32,768	32,768	Normal	0			
Memory Co 2840 C:\	pagefile.sys	(Page File)		31,744	0	31,744	Normal	0	~		
Naturale Co	the density	11200 Khore Natur	ark 1/0	SCAR	-	1% Network Ibil	insting.	^			
Network		Ticos Kops Net	lork I/O			The retwork Util	12800h		~	Ma 100 Hz	ed Eaults/sec 7
image	PID	Address		Send (B/sec)	Receive (B/sec)	iotal (B/sec)				100110	a radita/sec
Zoom.exe	5576	168.138.18.199		1,731,438	234	1,731,667					
aakore.exe	4152	103.64.16.52		13,060	763	13,823					
aakore.exe	4152	AMD		0,219	5,494	13,433					t i i i i i i i i i i i i i i i i i i i
CyberProtectHomeOfficeMon	7114	AMD		9,4/1	2 684	3,331					
ockp_amgr.exe	6576	102 169 0.9		340	2,304	2,910					
ado, agent eve	5833	AMD		156	1 276	1,423					LO
monitoring-mini eve	6060	AMD		285	077	1 213					
indution y intrace	7160	4140		400	004				~		
Memory	_	Hard Faults/se				47% Used Physic	al Memory		•		
Image	PID	Hard Faults/sec Commit (K	Working Set (K	Shareable	(KB) Private ((KB)			^		
System	4	0 10 506 50	4 10.424.68	0. 2	268 10.422	412					
Zoomexe	\$576	0 787 15	0 502.36	8 00	308 403	960					
sychost eve (UnistackSwrGrou	n) 16148	0 482.62	0 32 38	4 22	916 9.	468					
McMnEng.eve	4328	10 420.70	4 278.28	8 62	404 215	884					
explorer.exe	15840	0 343.65	4 262.64	4 103	888 68	756					
aomhost64.exe	17940	0 230.40	4 36.46	0 23	576 12	884					
SearchApp.exe	17376	0 198.31	2 101.84	0 97	424 4	416					
dwm.exe	16804	0 151.96	8 97.10	4 47	856 49	248					
PowerToys PowerLauncher.ex	e 13220	0 147.36	0 25.80	8 13	440 12	368					
Searchindexer.exe	3476	0 130.58	4 77.00	0 19	312 57	688					
Zoom.exe	6784	0 100.41	2 63.59	6 57	.040 6	556					
Accelatere	12068	0 91.76	0 146.19	2 61	756 84	436					

Figure 8 – Windows Resource Monitor

Two instances of a program called DSOne.exe (the second with a similar name) were found to be running constantly, 100% of the time. The laptop had 4GB of memory and 3.9GB was used up paging data back and forth from the hard drive to RAM. This process occurs as programs can only run from memory.

George eventually removed the 2 apps using IObit Uninstaller, when the Windows uninstaller was unable to remove them.

Identifying the administrator password

Like many Window users, the original owner of the laptop set the computer to open without a password. This was achieved from the "Run" command and typing "control userpassword2" (Figure 9).

In the "User Accounts" window that opens, untick the box labelled "Users must enter a user name and password to use this computer". This now meant the computer loaded Windows on bootup, not needing a password to start. (Note: If the command "control userpassword2" is run when the box is unticked, George found the command doesn't run).

User Accounts		×
Users Advanced Use the list below to gran and to change password Users must enter a user name a	nt or deny users access to your computer, s and other settings. and password to use this computer.	
User Name	Group	
& dave_be2@hotmail.com & daveb@melbpc.org.au & db & HomeGroupUserS Margaret	HomeUsers HomeUsers HomeUsers; Administrators; Users HomeUsers HomeUsers: Administrators	
Password for Margaret To change your password.	dd <u>R</u> emove Pr <u>o</u> perties ord, press Ctrl-Alt-Del and select Change Reset <u>P</u> assword	
	OK Cancel Apply	1

Figure 9 – User Accounts

As the original owner didn't remember the password they used 6 years ago, George set about creating a new user with admin privileges. He did this by using the Password app from Hiren's BootCD, to remove the passwords and then created a new user.

How to boot up your system with Hiren's Boot CD In order to boot from the Hiren's Bootable USB stick, you need to set the USB as the first boot device from BIOS settings. Here are the steps:
 Power On your computer and then press "F1" or "F2" or "F10" or "DEL" to enter BIOS (CMOS) setup utility. (The method to enter into BIOS Settings depends on the computer manufacturer).
2. When you enter the BIOS menu, go to the "Advanced BIOS Features" menu and find the "Boot Order" setting.
3. In the "Boot Order" setting, set the USB-HDD as a first boot device.
4. Save and exit from BIOS settings.
The link to view a video that explains using Hiren's BootCD is at: <u>https://www.youtube.com/watch?v=p3l5aM2hPXI</u>

When creating a new user in Windows, you will be asked "Is it a family member"? Answer "No", then it will ask "Is it a friend"? When asked to put in the friend email address, answer "I don't know" or enter <u>no@thankyou.com</u> or <u>aa@bb.com</u>, the latter as suggested by audience members.

	-		×
Family & other users			
Your family			
Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.			
Sign in with a Microsoft account			
Other users			
Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.			
+ Add someone else to this PC			
Help from the web			
Creating a local user account			
Switching to a local account			
Setting screen time limits			
	 Family & other users Your family Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games. Sign in with a Microsoft account Image: Content of the set of your family to sign in with their own accounts. This won't add them to your family. Add someone else to this PC Help from the web Creating a local user account Setting screen time limits 	 Family & other users Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time inits, apps, and games. Sign in with a Microsoft account Sign in with a Microsoft account Other users Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family. Add someone else to this PC Help from the web Creating a local user account Switching to a local account Setting screen time limits 	 - □ Family & other users Your family Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games. Sign in with a Microsoft account Cother users Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family. Image: Add someone else to this PC Help from the web Creating a local user account Setting screen time limits

Figure 10 – Creating a New Administrator User

Eventually you will be given the option to create a new user and asked 3 questions. These questions could be "What city were you born in?", answer "a", then "What school did you go to?" answer "a" again, then "What was you first pets name?" and answer "a" again. Occasionally Windows may ask you to verify yourself. Answering with a lower case "a", makes it easier to remember. Once your new admin user is created you will be able to delete other users from the computer.



Figure 11 - New Administrator creation

Once the 2 major hurdles of removing the malware and creating a new user with Administrator privileges were overcome, the laptop became quite usable and George could proceed with the clean-up of the laptop.

Cleanup Procedure

George explained how, using only the software that comes with Windows to remove all personal data, while keeping existing software applications intact for the next user. Georges steps are underlined below.

- 1. <u>Delete all user docs and personal files</u> File Explorer can be used to delete data initially.
- Format all data drives. Do NOT use quick Format
 If data is kept on a separate drive or partition from the Windows operating system, format the
 drive. Make sure the "Quick Format" option is not selected as a full format is needed to
 ensure data cannot be retrieved. Figure 12.

Quick Format just wipes the directory and the File Allocation Table (FAT). All data remains on the hard drive and can be retrieved by someone using third-party Recovery software.

Format Data (D:)	×
Capacity:	
258 GB	~
File system	
NTFS (Default)	~
Allocation unit size	
4096 bytes	~
Data	
Format options	

Figure 12 – Format Data Drive

- 3. <u>Create a new Administrator user use a simple name such as User and password</u> This step is detailed above.
- 4. <u>Delete all mail account profiles via Control Panel, Mail</u> To delete other users mail accounts in this step requires a user with administrative privileges. Deleting Microsoft Outlook mail is fairly easy. From the "Control Panel" select "Mail (Microsoft Outlook)", which opens the "Mail Setup - Outlook" window. (Figure 13) Select "Email Accounts" to open the "Account Settings" window and delete all the accounts from the list.

The "Mail" icon will only appear in Control Panel if the user uses MS Outlook as their mail client.



Figure 13 – Mail Accounts - Outlook

- 5. <u>Delete all mail account databases such as *.pst and / or *.ost</u> Once all email accounts in step 4 have been deleted, select the "Data Files" button and delete all the data files from the list and select "Close"
- 6. Delete all other user accounts AND their data
- 7. <u>Delete all user accounts Control Panel, User Accounts and all their data</u> Open Control Panel and Select "User Accounts"
- <u>Delete all saved passwords & bookmarks in ALL browsers</u> In all browsers select "Settings" and look for Passwords. Again, you will need the Windows Administrator password (i.e. the password used to start the computer) to be able to look at everyone's browser passwords and delete them.

In Firefox you will need to look at Settings \rightarrow Privacy & Security \rightarrow Logins and Passwords.

User profiles for Thunderbird can be found in the Thunderbird Profile folder. The default location for profiles in Windows is: C:\Users\UserName\AppData\Roaming\Thunderbird\Profiles.

9. Delete all passwords in Credential Manager

Passwords are also stored in "Credential Manager". From "Control Panel" select "Credential Manager" and displayed are 2 lists of passwords for "Web Credentials" and "Windows Credentials". (Figure 14). As noted previously, these can be deleted but the Windows login password is required before this is possible.



Figure 14 - Credential Manager

- 10. Finally defrag all drives to reduce the very tiny chance of some data being recovered
- 11. Now the computer is ready to be donated