OPCUG

Users helping users

Alan German & Chris Taylor
Ottawa PC Users' Group

March 2, 2022

Share

ReasonLabs

The State of Consumer Cybersecurity 2022

- Some key findings for 2021
  - year of the miner—58% of all Trojans: crypto miners
  - sharp rise in cryptojacking and infostealing
  - phishing via documents/email still popular for distributing malware
  - one of most prevalent detections: *Adware Browser Modifiers*
    - adware that hijacks browser's search settings, new tabs and modifies expected behavior of your browser by injecting advertisements
- For 2022
  - shift in hackers' focus away from enterprises back to consumers
  - cryptojacking will continue to increase significantly
  - malware in cracks, games, cheats, increasing significantly
    - young consumers are most at risk

https://reasonlabs.com/research/cybersecurity-report

you have to provide a name and email, but fake info works

Finding keyloggers

- Most anti-virus (AV) programs will detect keyloggers
- How else can you make sure no keylogger is installed?
  - beyond looking for a suspicious processes under Task Manager…

Orion Clark

What is a keylogger?

- Records keystrokes, typically covertly
  - including passwords, credit card numbers…
- User unaware their keystrokes are being recorded
- Data retrieved by person operating logging program
- Keyloggers can be software or hardware

https://en.wikipedia.org/wiki/Keystroke_logging

A Hardware keylogger

- Inserted between keyboard and computer
- Records all keystrokes
- Attacker retrieves log later
  - ***or streamed over WiFi!***
- Defence: visual examination

Keystroke recorder benefits

Employers	Parents	Investigators
		
• Monitor acceptable internet usage • Monitor employee productivity • Detect unauthorized access attempts • Backup typed text • Collect computer usage statistics	• Monitor your family's computer activity • Protect your child from on-line hazards and predators • Observe WWW, E-mail, and chat usage • Save a copy of written documents	• Monitor remote computers • Retrieve unknown passwords, operating system independent • Collect computer related evidence • Detect unauthorized use of computer equipment

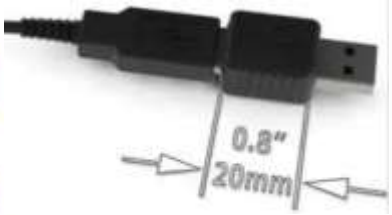
AirDrive Keylogger

Wireless. Innovative. Smart.

The **AirDrive Keylogger** is an innovative ultra-small USB hardware keylogger, only **0.8" (20 mm)** in length. It can be accessed with any Wi-Fi device such as a computer, laptop, tablet, or smartphone.

The **AirDrive Keylogger Pro** is an enhanced version of the AirDrive Keylogger, with additional connectivity options. It works both as a Wi-Fi hotspot, and as a Wi-Fi device, enabling features such as Email reports, time-stamping, and data streaming.

The **AirDrive Keylogger Max** is the most advanced keylogger in the AirDrive Keylogger family, with all the capabilities of the Pro version, enhanced with 16 GB internal memory available as a USB Hi-speed flash drive (480 Mbps).



Features

- Records keystrokes from **any USB keyboard**
- **16MB** internal flash memory
- 100% stealthy, **undetectable for security software**
- Supports over **40 national keyboard layouts**
- Compatible with **barcode readers**
- Works as a **Wi-Fi hotspot**
- Connect from any **computer**, **smartphone**, or **tablet**
- Access data from **web browser**, no software or app necessary
- Retrieve data remotely **without touching the device**
- Simple and clear **WWW interface**
- Supports **WEP**, **WPA**, and **WPA-2** network security
- Memory protected by **hardware encryption**

Pro and Max version:

- Works as a **Wi-Fi hotspot**, or as a **Wi-Fi device**
- **Sends Email reports** with recorded keystroke data
- Supports **time-stamping**
- Supports **live data streaming** over network

Max version:

- **16 gigabytes** of built-in memory
- Memory accessible as a **USB Hi-speed flash drive (480 Mbps)**

How to detect (software) keyloggers

- As Orion noted
  - most anti-virus (AV) programs can detect keyloggers
    - if they are known, that is…
    - most AV operates on a ***detect-if-known*** mode
- Question is
  - what can be done to detect keyloggers?
- Two ideas I can think of
  - second (3^{rd}, 4^{th}, 5^{th}?) AV program
    - no one AV program will detect all malicious software
  - Task Manager (as Orion noted)

Another anti-virus program

- Should only have one **on-access** AV program
  - constantly running watching for file accesses
  - when a file is accessed, on-access AV checks file first
  - if two on-access AV programs installed
    - fight for who accesses first
  - some specially-designed AV programs can operate on-access alongside another on-access program (e.g. MalwareBytes)
- Can have **on-demand** AV in addition to on-access AV
  - on-demand AV goes to open a file
  - on-access AV swoops in and scans the file first
  - once file deemed okay, passes to on-demand AV
  - on-demand AV scans it

Free on-demand anti-virus

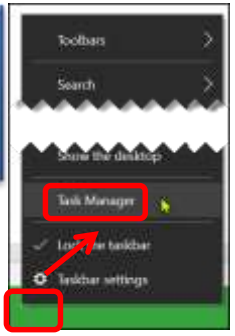
- **ESET**
  - https://www.eset.com/ca/home/online-scanner/
- **Trend HouseCall**
  - https://www.trendmicro.com/en_us/forHome/products/housecall.html
- **F-Secure**
  - https://www.f-secure.com/en/home/free-tools/online-scanner
- **Sophos Scan & Clean**
  - https://www.sophos.com/en-us/products/free-tools/virus-removal-tool/free-download
- **Microsoft Safety Scanner**
  - https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
- **Norton Power Eraser**
  - https://support.norton.com/sp/static/external/tools/npe.html
- **McAfee Stinger**
  - https://www.mcafee.com/enterprise/en-us/downloads/free-tools/stinger.html
- **MalwareBytes**
  - https://www.malwarebytes.com/premium
  - installs as premium with on-access capabilities. After 14-days, switches to on-demand-only
- **ClamWin**
  - https://sourceforge.net/projects/clamwin/
- **there are others…**

A Using Task Manager

The idea:
- find unknown / suspicious programs running and eliminate them

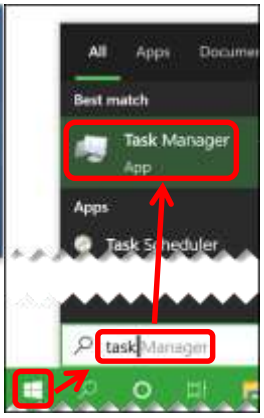
Press ***Ctrl-Shift-Esc***

Right-click blank area of Taskbar
Choose ***Task Manager***



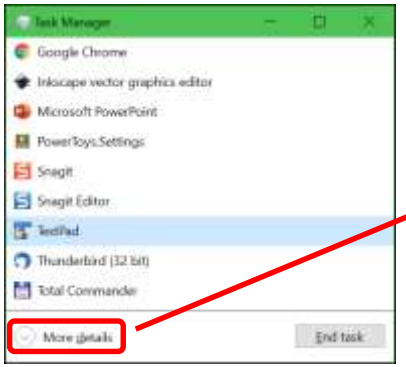
Press ***Ctrl-Alt-Del***
Choose ***Task Manager***

Press ***Start*** button
Start typing ***Task Manager***
Choose ***Task Manager***

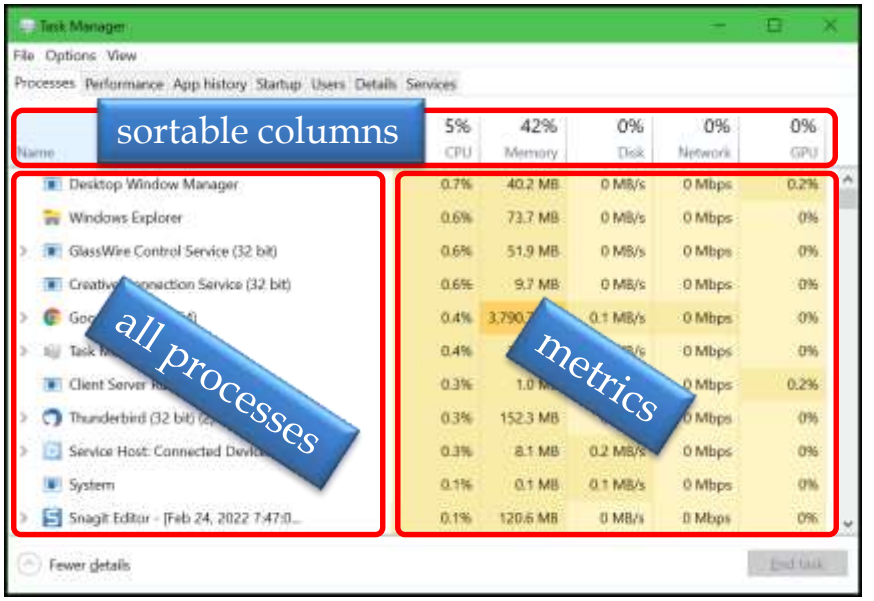


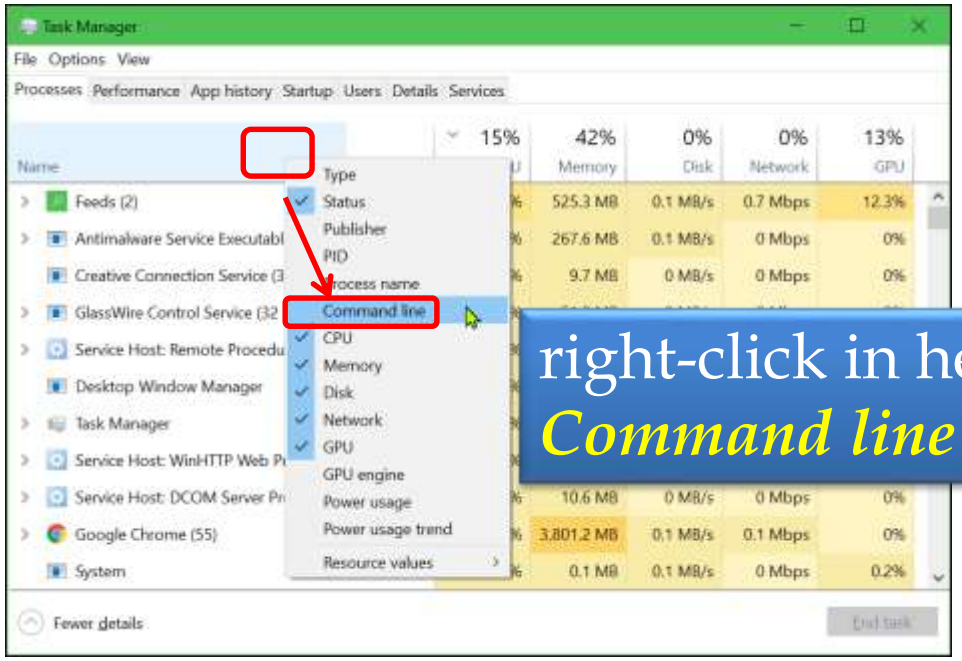
Configure Task Manager

Default shows only visible programs
Malware will never be a visible window!



click ***More details***



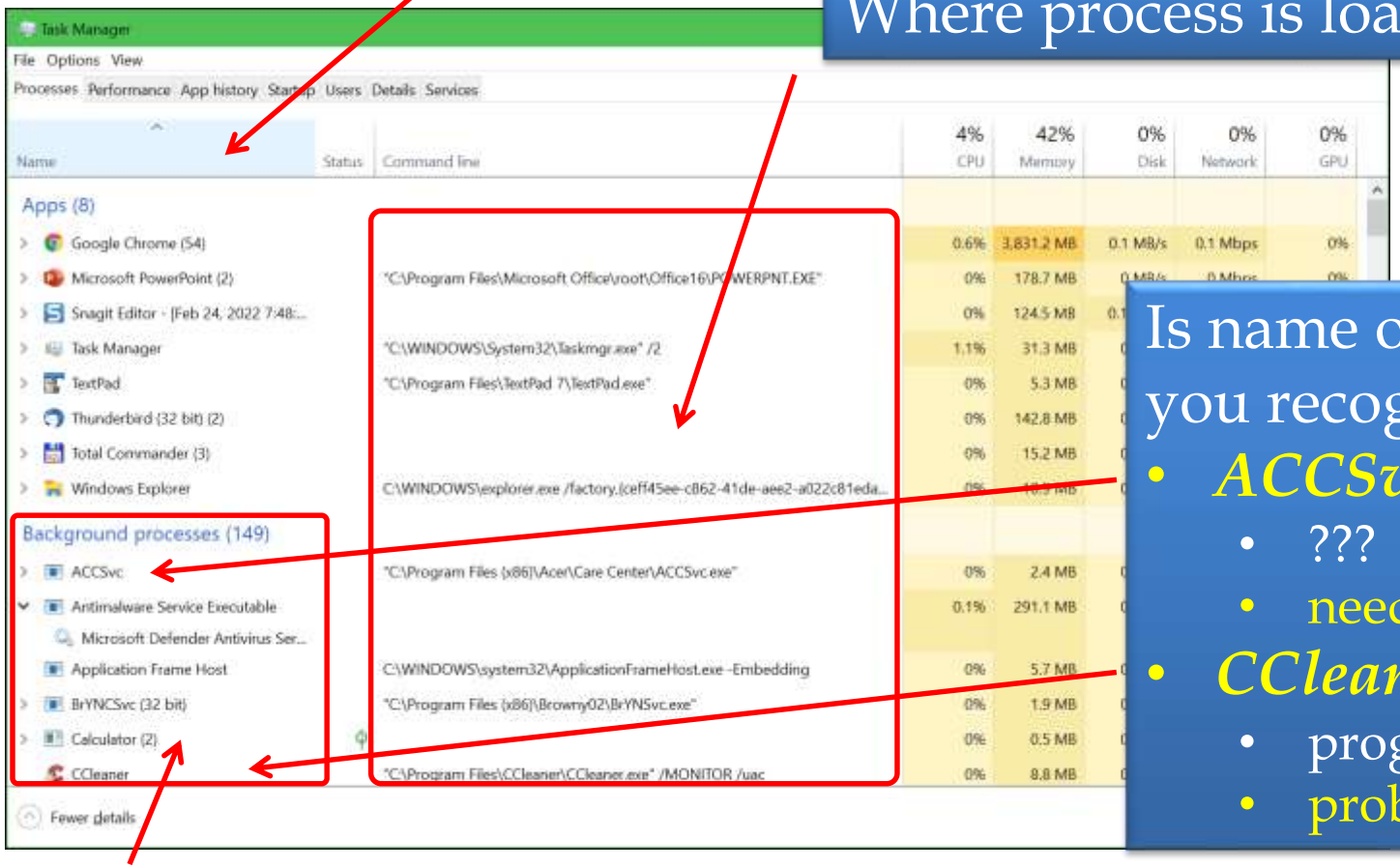


right-click in header & add
Command line

Task Manager details

click *Name* to sort

Where process is loading from

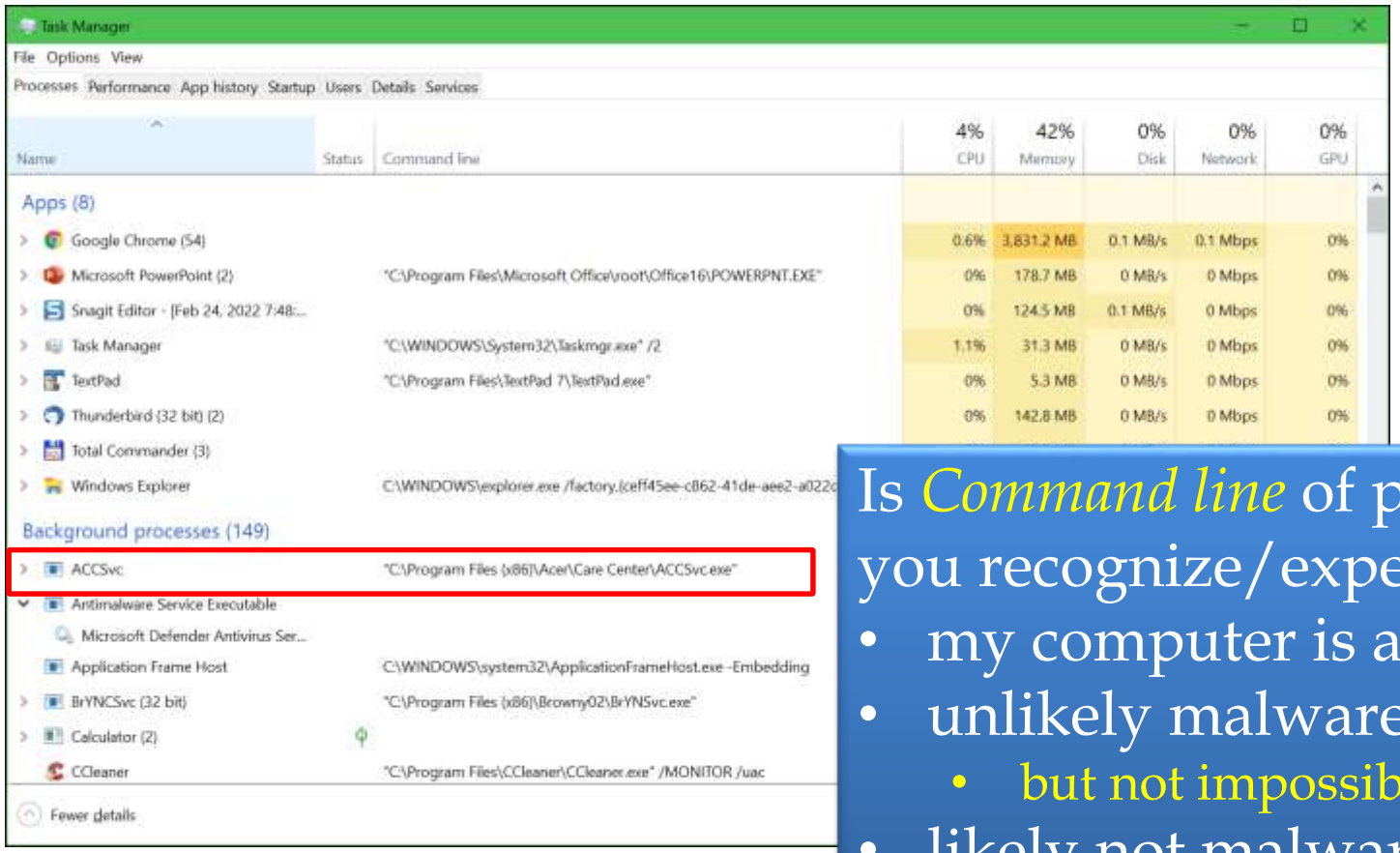


Is name of process something you recognize/expect?

- *ACCSvc*
  - ???
  - need to investigate further
- *CCleaner*
  - program I installed
  - probably ok

Concentrate on *Background processes*

Task Manager sleuthing



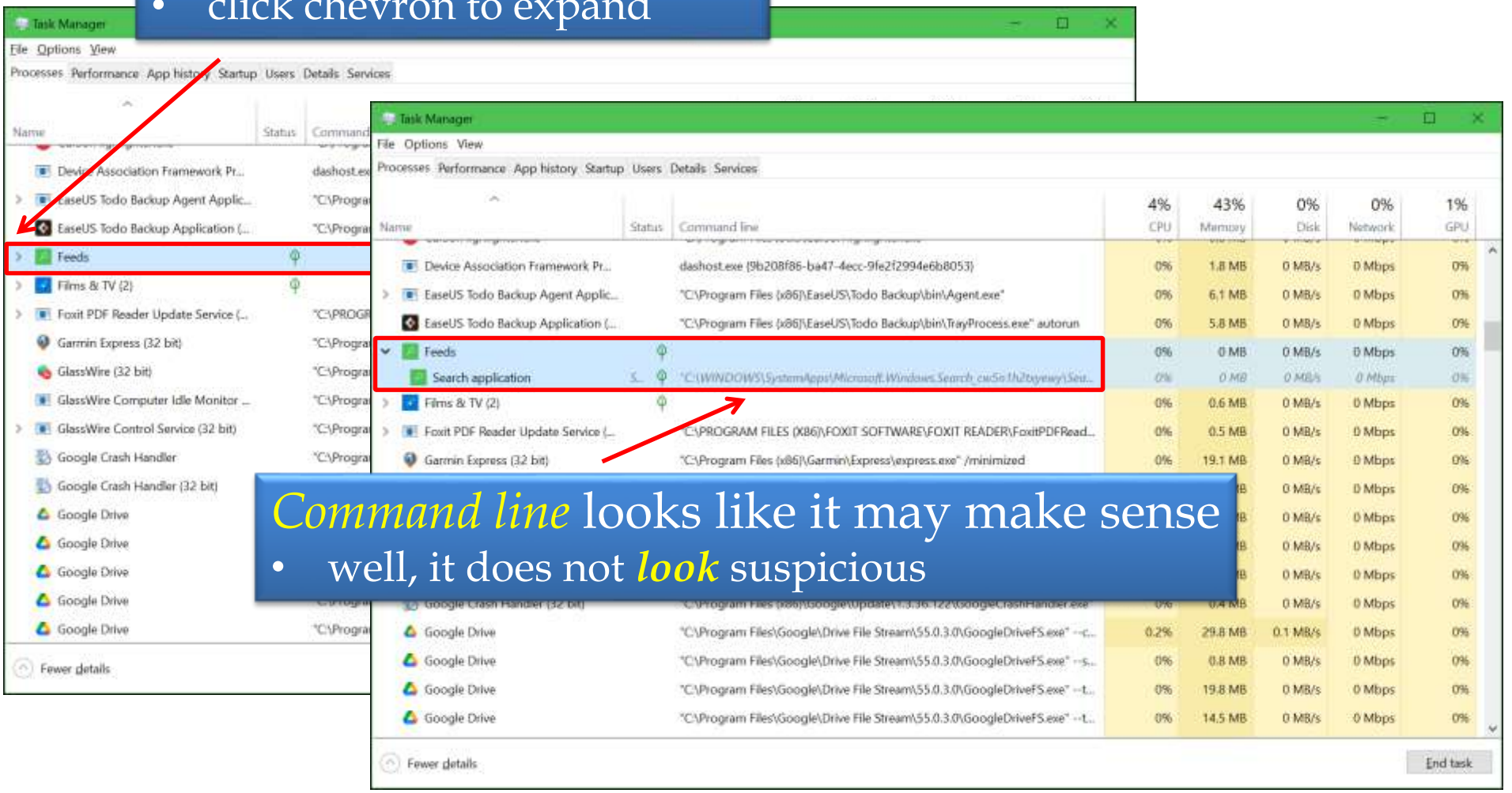
Is *Command line* of process something you recognize/expect?

- my computer is an Acer
- unlikely malware would end up here
  - but not impossible!
- likely not malware

Task Manager sleuthing

some entries have chevron

- click chevron to expand



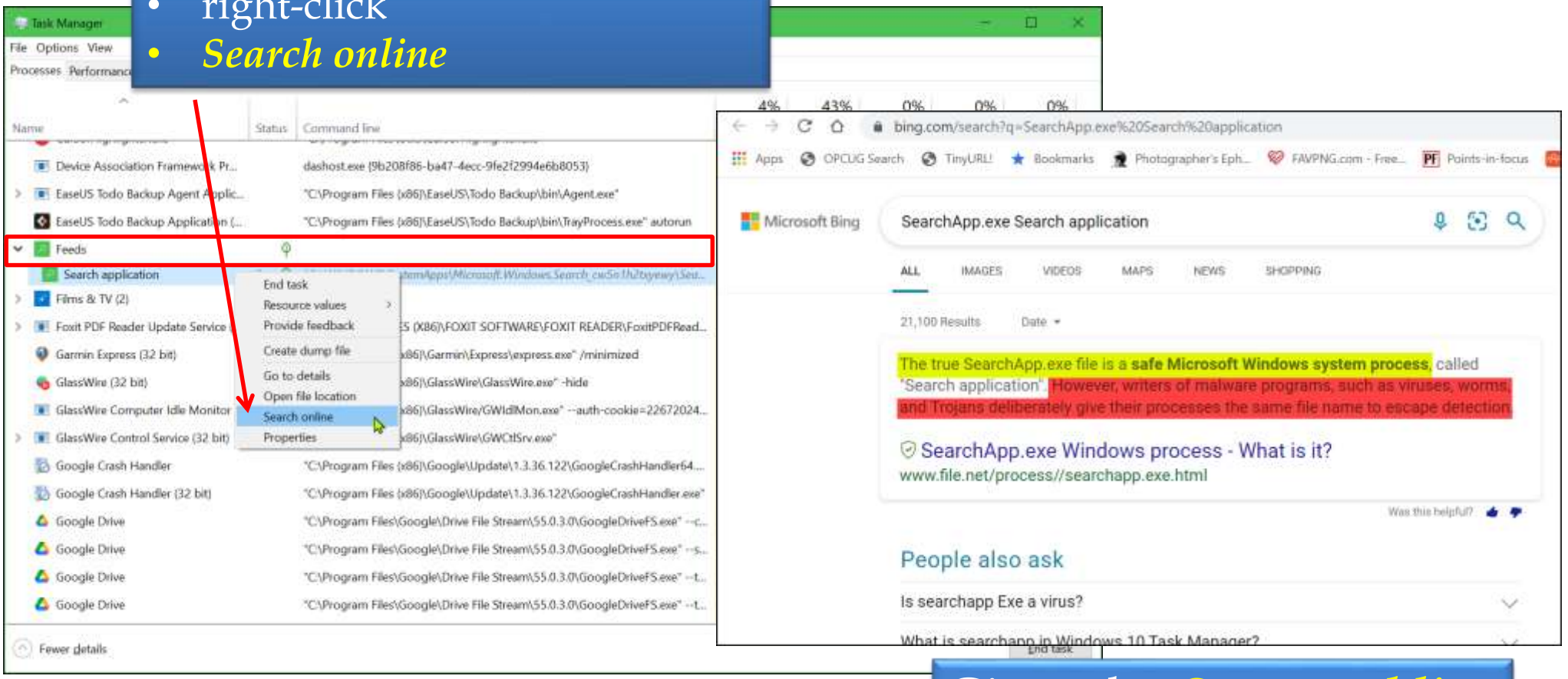
Command line looks like it may make sense

- well, it does not ***look*** suspicious

Sleuthing further

want to investigate further?

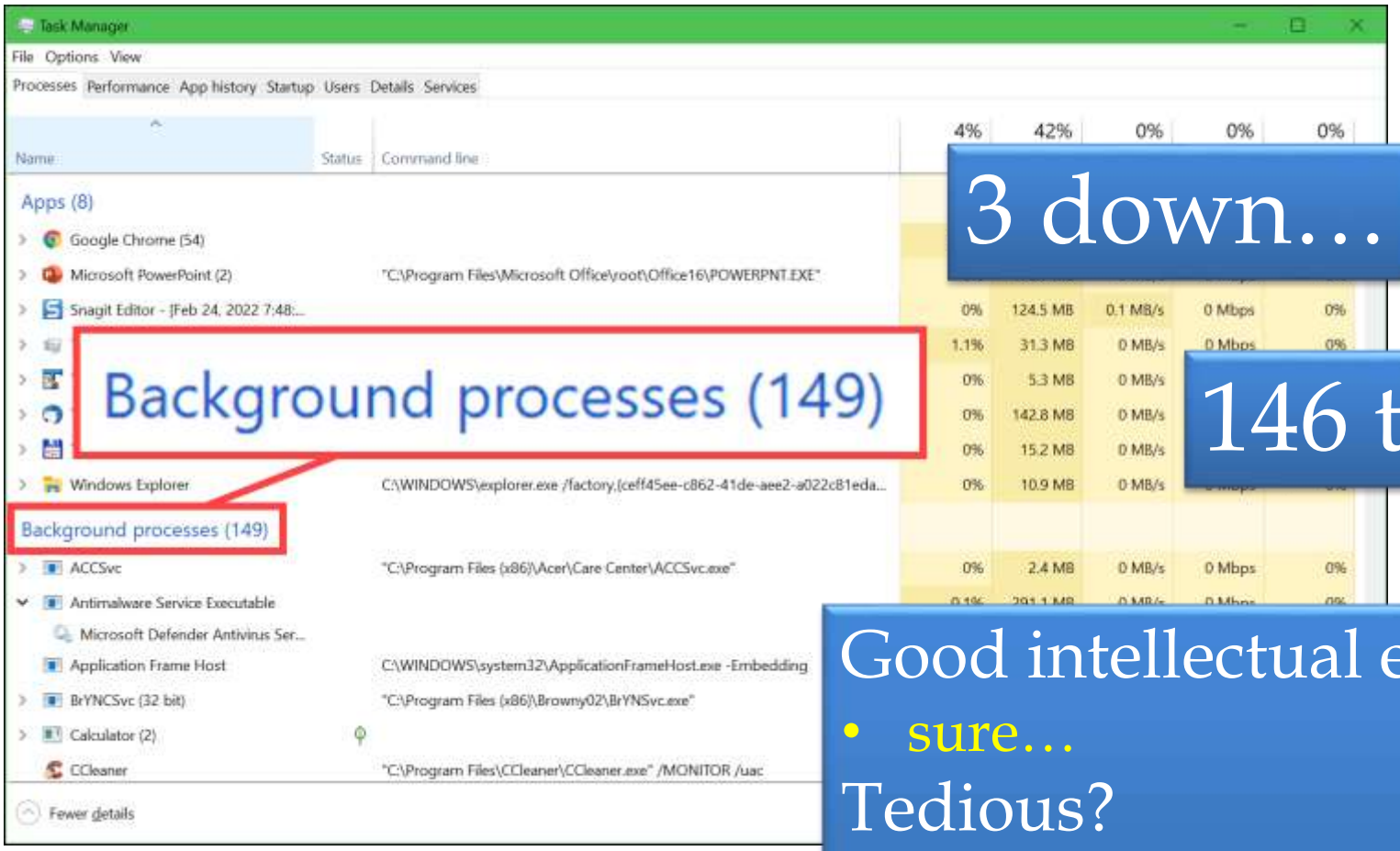
- right-click
- ***Search online***



Given the ***Command line***

- probably okay

A Rinse and repeat



3 down…

146 to go…

Good intellectual exercise?

- sure…

Tedious?

- definitely…

Likely to find a keylogger?

- maybe…

Tall Tales - Windows Update

- Once upon a time..
- Friend gave remote access to scammer
- Full disk image restored
- Image was from 2016 !
  (but it included installed
  copy of MS Office)

- Windows Update stopped at
  Version 1511 that is at end of service
- Downloaded *Windows10Upgrade28603.exe* to reach Version 1709
- Update then froze on KB4493440
- Troubleshooter said it fixed things - It didn't!

Tall Tales - Windows Update

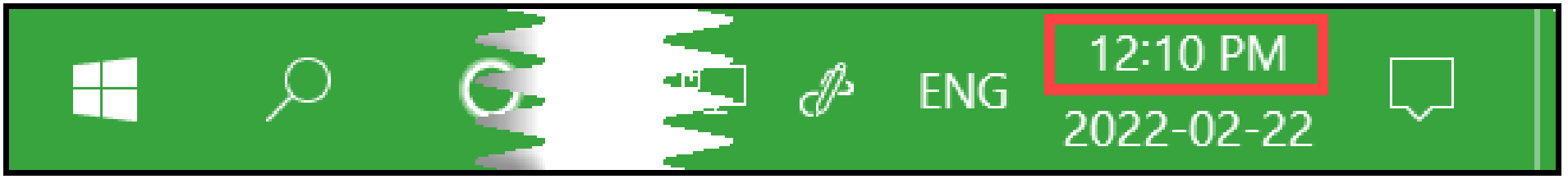
- Checked Chris's Q&A posting (27-Jan-2021)

- Ran Disk Cleanup on the System
- This took hours! (*What does this program do when it goes off to almost-never-never land?)*
- But, afterwards, Update got to Version 20H2
- And, on the next day, Update finally installed Version 21H2
- OS is up to date!
- The End

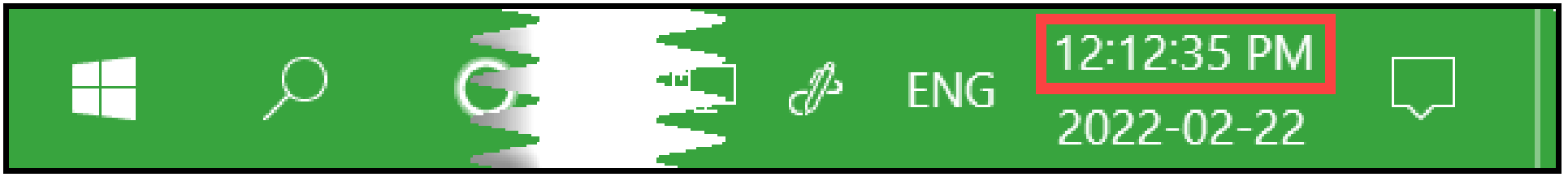
Share

Add seconds to taskbar clock

Windows displays hours/minutes in taskbar clock



Registry hack adds seconds

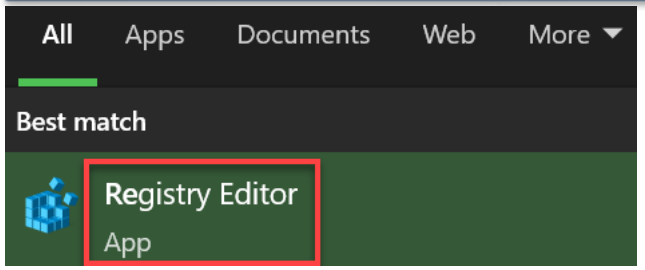


Share

Method 1: Registry Editor

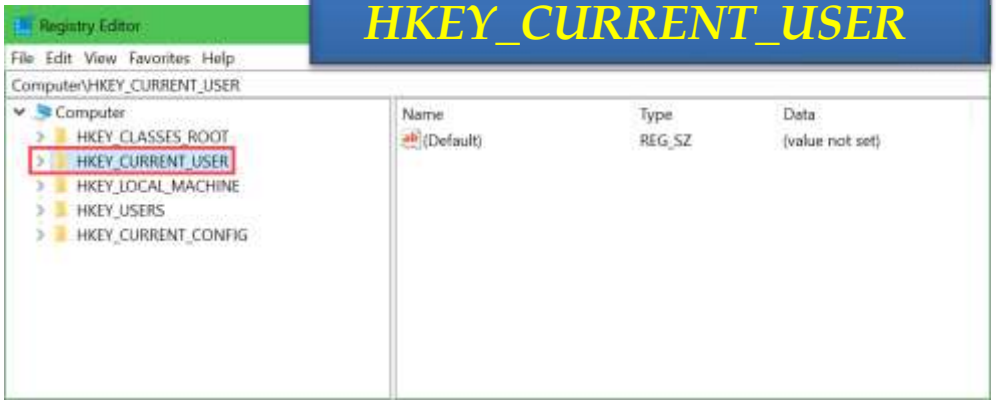
Step 1

Click *Start* button, type *regedit*, select *Registry Editor*



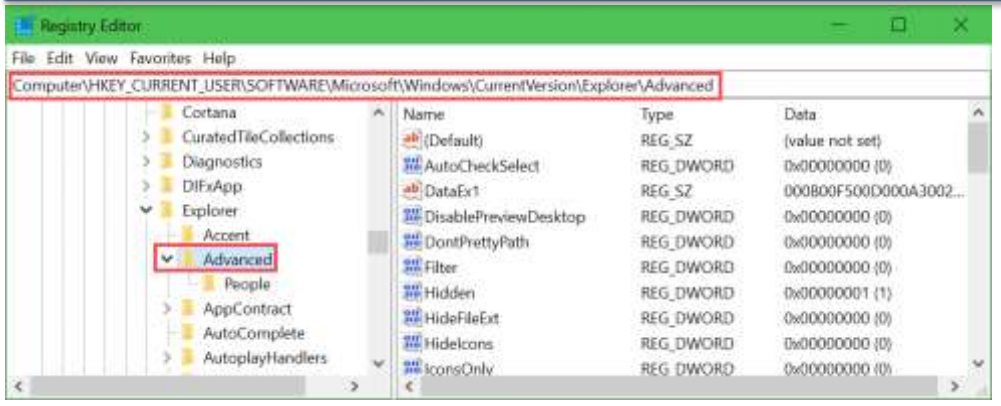
Step 2

Left pane
- click chevron to expand *HKEY_CURRENT_USER*



Step 3

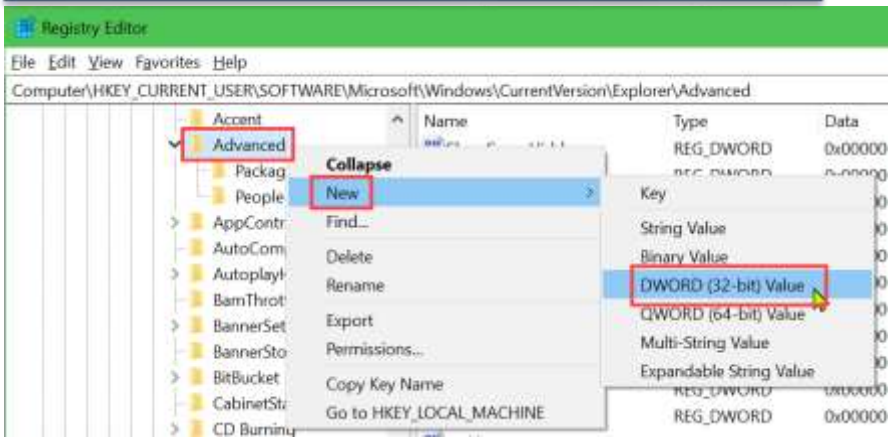
Continue expanding to
HKEY_CURRENT_USER\SOFTWARE\Microsoft\CurrentVersion\Explorer\Advanced



Share

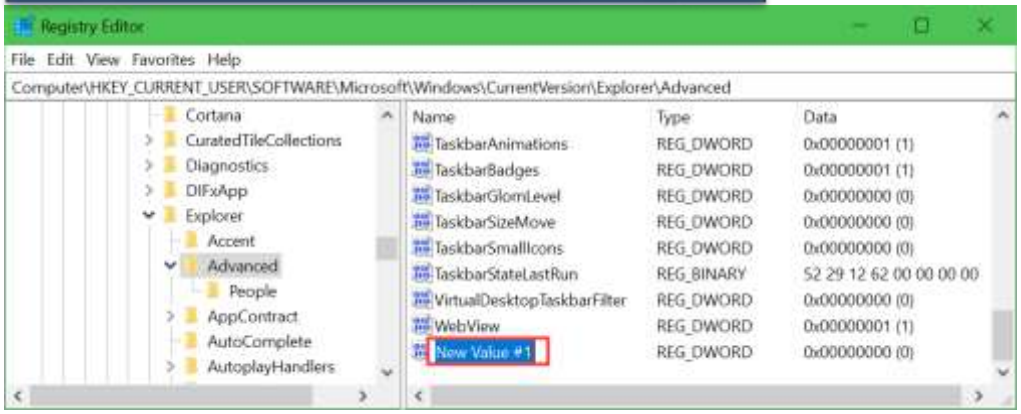
Step 4

Right-click on ***Advanced*** and choose ***New | DWORD (32-bit) value***



Step 5

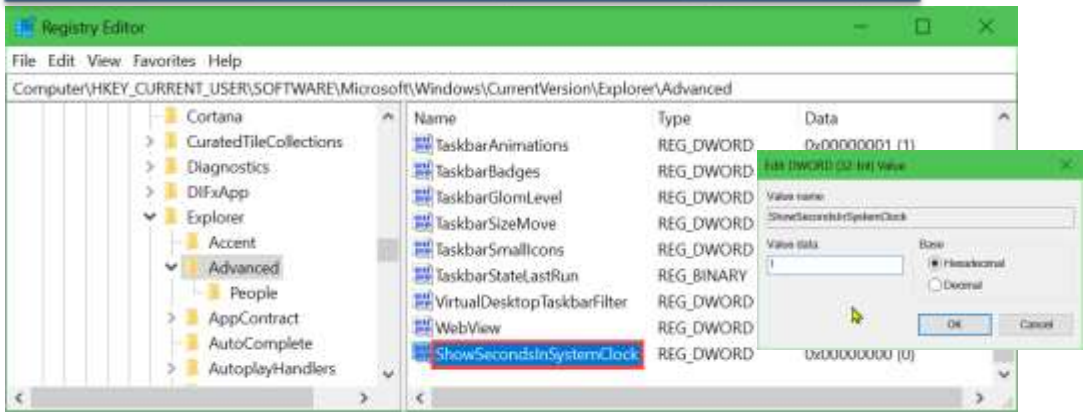
New Value #1 created
- overwrite name with new name
ShowSecondsInSystemClock



If you accidentally click off ***New Value #1***
- right-click it and choose ***Rename***

Step 6

Double-click the new value and set it to ***1***



Step 7

Click ***OK***
Sign out and sign in to Windows

Share

Method 2: Run a .reg file

.reg file - plain text file with "instructions" to the registry editor to import/change/delete information in the Windows registry

First line
Windows Registry Editor Version 5.00

Sections start with ***key*** to be modified, e.g.
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced]

Followed by one or more lines with the ***Value name*** to be added or modified with ***Value data***, e.g.
"ShowSecondsInSystemClock"=dword:00000001

Value name in quotes

Value type:Value data

Double-click a .reg file to have Registry editor make the changes in the registry

Share

.reg file to **add** seconds in Taskbar clock

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"ShowSecondsInSystemClock"=dword:00000001
```

.reg file to **remove** seconds in Taskbar clock

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"ShowSecondsInSystemClock"=dword:00000000
```

Share

We've saved you the typing!
Download
https://opcug.ca/downloads/TaskbarClockSeconds.zip

Unzip the file to any convenient location

ReadMe.txt
- short instruction file

ShowSecondsInTaskbarClock.reg
- double-click this file to show seconds in taskbar clock

HideSecondsInTaskbarClock.reg
- double-click this file to hide seconds in taskbar clock

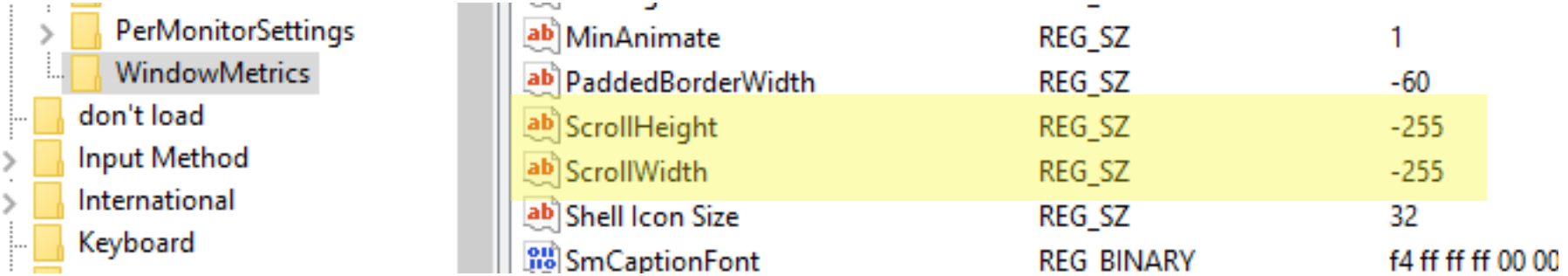
You must sign out of Windows and sign in for it to take effect

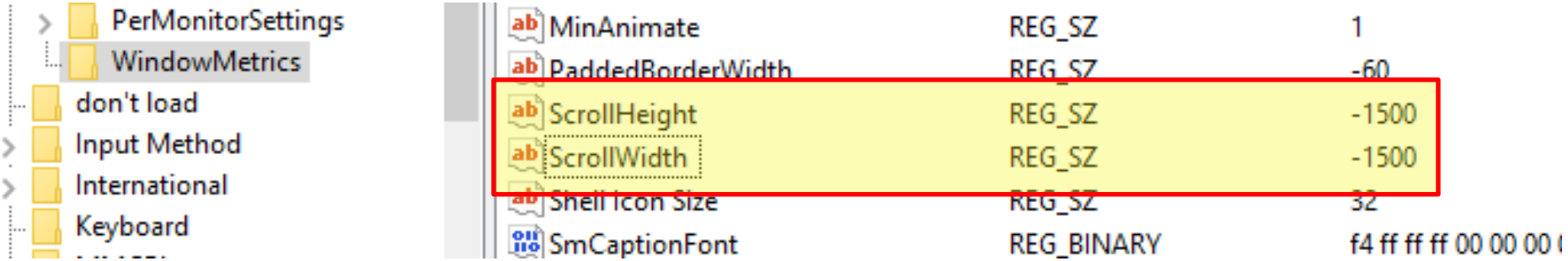
Follow-up

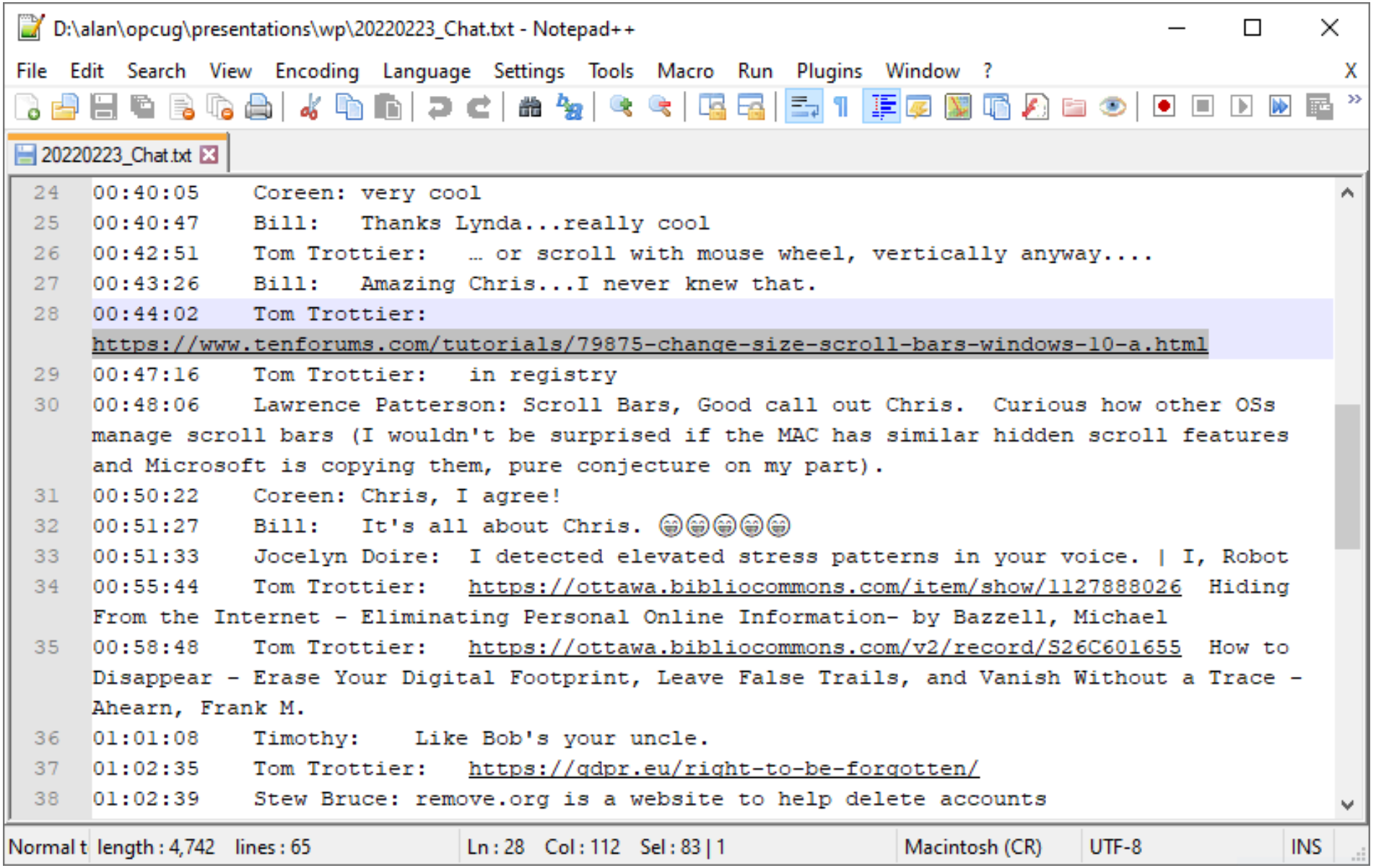
Change scroll bar size

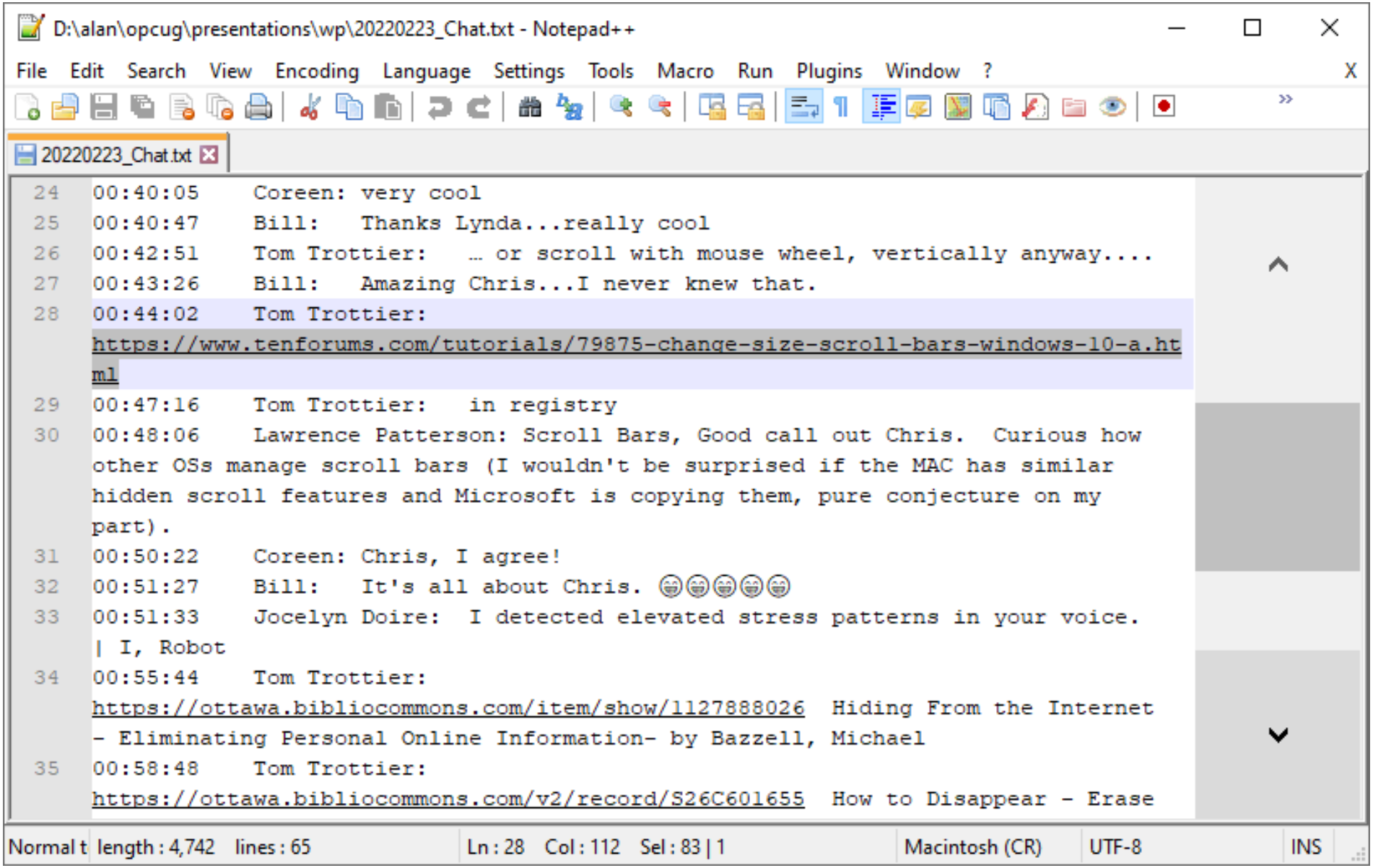
HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics

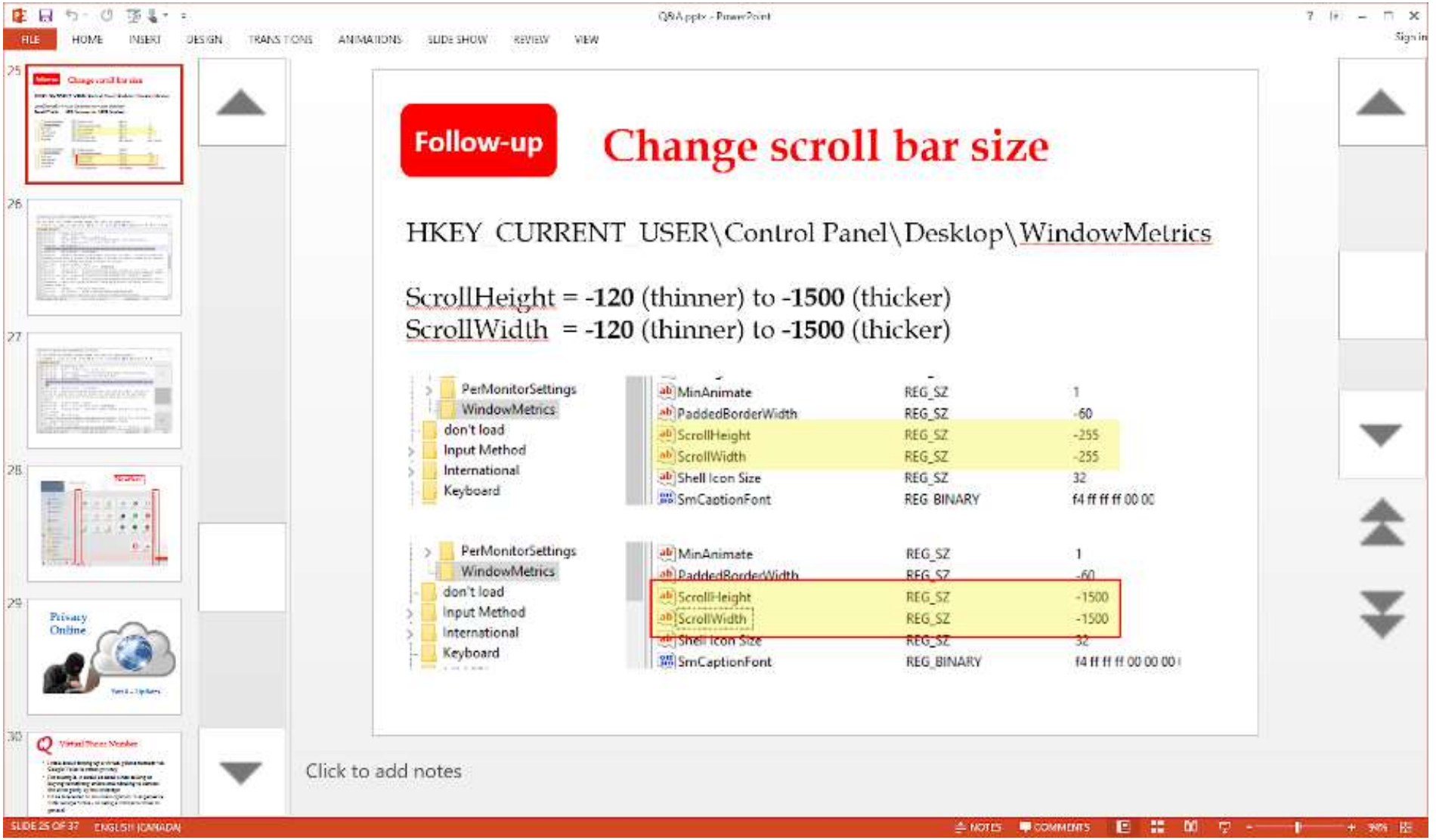
ScrollHeight = **-120** (thinner) to **-1500** (thicker)
ScrollWidth = **-120** (thinner) to **-1500** (thicker)



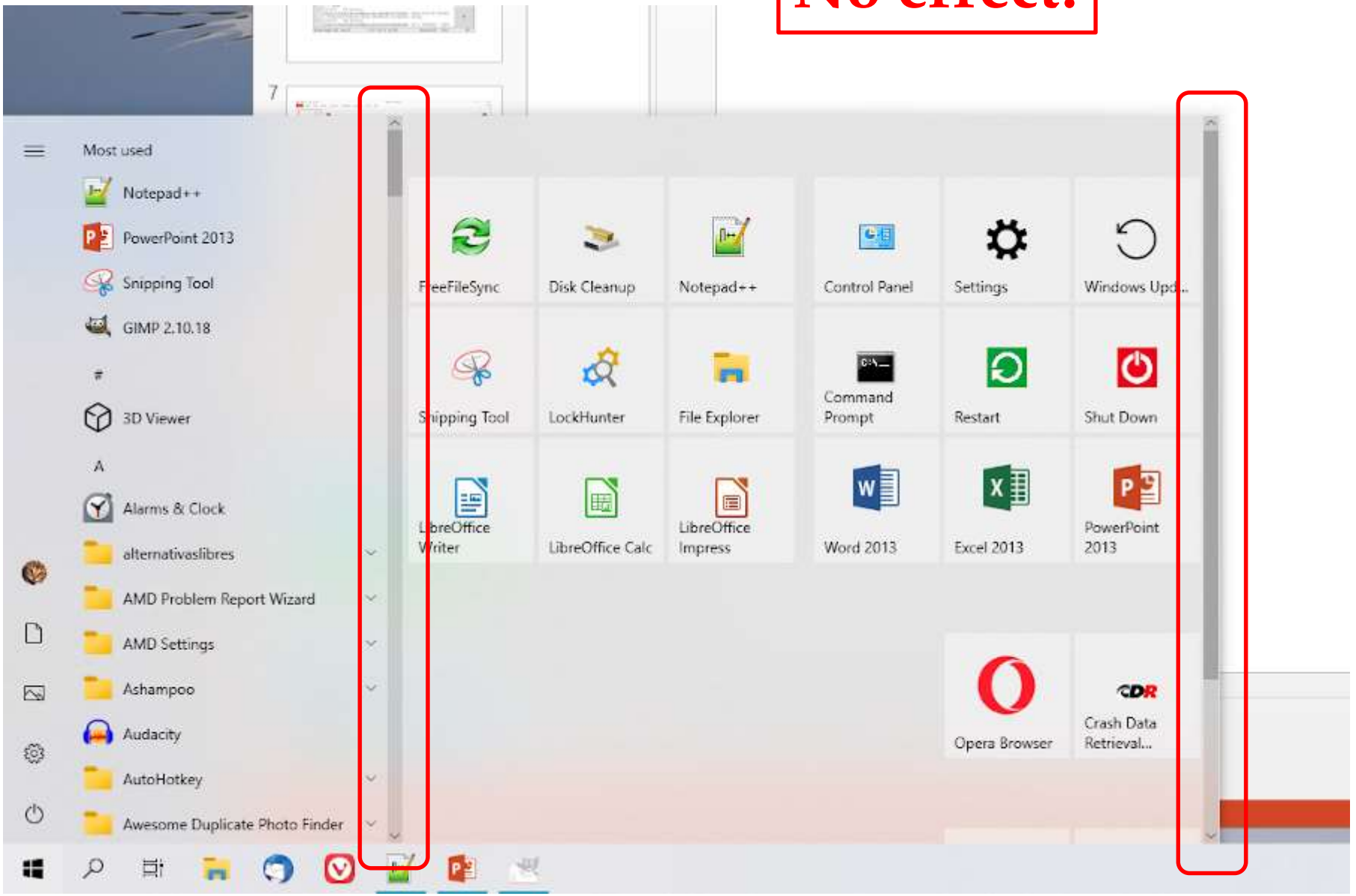



D:\alan\opcug\presentations\wp\20220223_Chat.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ? X
20220223_Chat.txt
24 00:40:05 Coreen: very cool
25 00:40:47 Bill: Thanks Lynda...really cool
26 00:42:51 Tom Trottier: … or scroll with mouse wheel, vertically anyway....
27 00:43:26 Bill: Amazing Chris...I never knew that.
28 00:44:02 Tom Trottier:
https://www.tenforums.com/tutorials/79875-change-size-scroll-bars-windows-10-a.html
29 00:47:16 Tom Trottier: in registry
30 00:48:06 Lawrence Patterson: Scroll Bars, Good call out Chris. Curious how other OSs manage scroll bars (I wouldn't be surprised if the MAC has similar hidden scroll features and Microsoft is copying them, pure conjecture on my part).
31 00:50:22 Coreen: Chris, I agree!
32 00:51:27 Bill: It's all about Chris.
33 00:51:33 Jocelyn Doire: I detected elevated stress patterns in your voice. | I, Robot
34 00:55:44 Tom Trottier: https://ottawa.bibliocommons.com/item/show/1127888026 Hiding From the Internet - Eliminating Personal Online Information- by Bazzell, Michael
35 00:58:48 Tom Trottier: https://ottawa.bibliocommons.com/v2/record/S26C601655 How to Disappear - Erase Your Digital Footprint, Leave False Trails, and Vanish Without a Trace - Ahearn, Frank M.
36 01:01:08 Timothy: Like Bob's your uncle.
37 01:02:35 Tom Trottier: https://gdpr.eu/right-to-be-forgotten/
38 01:02:39 Stew Bruce: remove.org is a website to help delete accounts
Normal t length : 4,742 lines : 65
Ln : 28 Col : 112 Sel : 83 | 1
Macintosh (CR)
UTF-8
INS


D:\alan\opcug\presentations\wp\20220223_Chat.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
20220223_Chat.txt
24 00:40:05 Coreen: very cool
25 00:40:47 Bill: Thanks Lynda...really cool
26 00:42:51 Tom Trottier: … or scroll with mouse wheel, vertically anyway....
27 00:43:26 Bill: Amazing Chris...I never knew that.
28 00:44:02 Tom Trottier:
https://www.tenforums.com/tutorials/79875-change-size-scroll-bars-windows-10-a.html
29 00:47:16 Tom Trottier: in registry
30 00:48:06 Lawrence Patterson: Scroll Bars, Good call out Chris. Curious how other OSs manage scroll bars (I wouldn't be surprised if the MAC has similar hidden scroll features and Microsoft is copying them, pure conjecture on my part).
31 00:50:22 Coreen: Chris, I agree!
32 00:51:27 Bill: It's all about Chris.
33 00:51:33 Jocelyn Doire: I detected elevated stress patterns in your voice. | I, Robot
34 00:55:44 Tom Trottier:
https://ottawa.bibliocommons.com/item/show/1127888026 Hiding From the Internet - Eliminating Personal Online Information- by Bazzell, Michael
35 00:58:48 Tom Trottier:
https://ottawa.bibliocommons.com/v2/record/S26C601655 How to Disappear - Erase
Normal t length : 4,742 lines : 65
Ln : 28 Col : 112 Sel : 83 | 1
Macintosh (CR)
UTF-8
INS


Follow-up
Change scroll bar size
HKEY_CURRENT_USER\Control Panel\Desktop\WindowMetrics
ScrollHeight = -120 (thinner) to -1500 (thicker)
ScrollWidth = -120 (thinner) to -1500 (thicker)
PerMonitorSettings
WindowMetrics
don't load
Input Method
International
Keyboard
MinAnimate REG_SZ 1
PaddedBorderWidth REG_SZ -60
ScrollHeight REG_SZ -255
ScrollWidth REG_SZ -255
Shell Icon Size REG_SZ 32
SmCaptionFont REG_BINARY f4 ff ff ff 00 00
ScrollHeight REG_SZ -1500
ScrollWidth REG_SZ -1500
Click to add notes

No effect!


Most used
Notepad++
PowerPoint 2013
Snipping Tool
GIMP 2.10.18
#
3D Viewer
A
Alarms & Clock
alternativaslibres
AMD Problem Report Wizard
AMD Settings
Ashampoo
Audacity
AutoHotkey
Awesome Duplicate Photo Finder
FreeFileSync
Disk Cleanup
Notepad++
Control Panel
Settings
Windows Upd...
Snipping Tool
LockHunter
File Explorer
Command Prompt
Restart
Shut Down
LibreOffice Writer
LibreOffice Calc
LibreOffice Impress
Word 2013
Excel 2013
PowerPoint 2013
Opera Browser
Crash Data Retrieval...

Privacy Online

Part 8 – Updates

Virtual Phone Number

- I read about setting up a virtual phone number via Google Voice to retain privacy
- For example, it could be used when selling or buying something online and needing to contact the other party by text message
- I'd be interested in anyone's opinion or experience with Google Voice - or using a virtual number in general

Fongo - Talk and Text Freely

- Local Canadian phone number
- Unlimited calling across Canada
- Unlimited incoming international calls
- Unlimited incoming SMS text messages
- Free outgoing calls and SMS to other Fongo users
- Regular outgoing SMS require subscription
- Outgoing international calls require calling credits (low rates, e.g. 2 cents/min)
- Travelling - call back to Canada for free
- Free premium features (e.g. caller ID, call waiting)
- VOIP call quality/stability not always reliable

Any other:

Questions

Comments

Shares?

March Meeting

OPCUG
Users helping users

Microsoft Teams – How Practical For Non-Corporate Users?

March 9, 2022
7:30 pm

Lawrence Patterson

Share

Virtual travel along the Danube

OPCUG
Users helping users

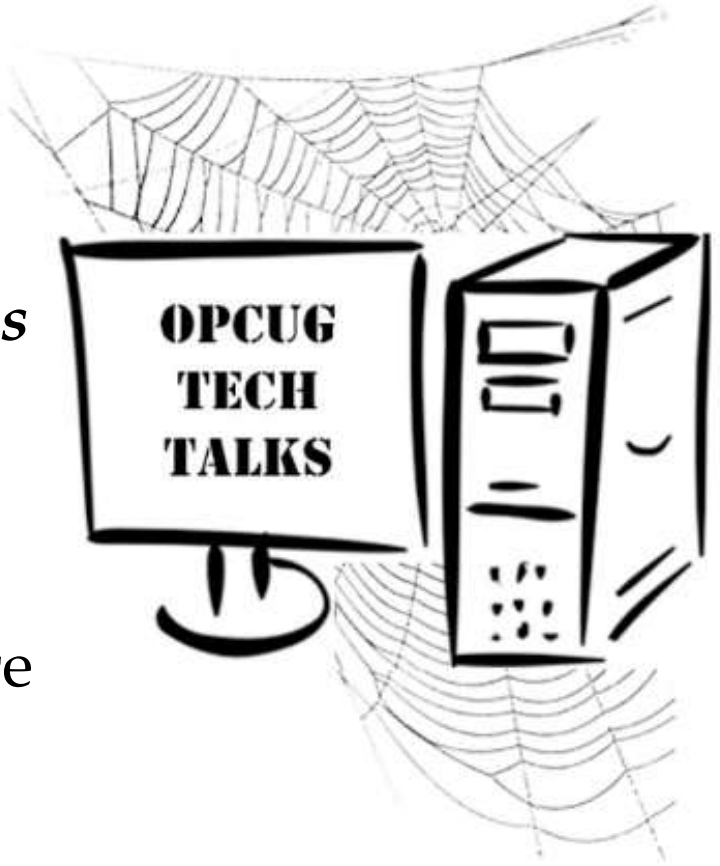
THROUGH THE LENS
A guide to digital photography for computer enthusiasts

- Join Lynda Buske for a virtual trip from Prague to Budapest.
- Tuesday, **March 15** at 7-8 pm EST
- Zoom link:
  https://us02web.zoom.us/j/89669560760?pwd=bjJCWDFETnRSM2ZUNHZFY1lzMjc3dz09

Any questions please email Lynda at **lbuske@sympatico.ca**

Spring Clean-up

April 4th, 7:00 pm



Ten tips to remove those digital cobwebs

1. Hard Disk Backup
2. Data File Synchronization
3. Security Settings
4. Double check your anti-virus software
5. Manage your Passwords
6. Software Updates
7. Remove Unused Software
8. Manage your E-mail
9. System Performance
10. Clean Up the Disk

Registration required

Free for OPCUG members

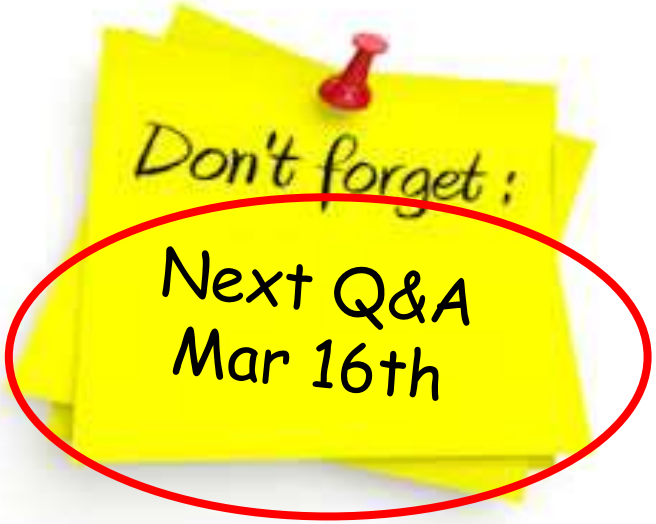
$20.00 for non-members

(including one-year membership)

Full details at:

https://opcug.ca/events/springcleanup/

No Q&A on
March 9
(Monthly Meeting)



Send your questions, answers, and topics you wish to share to:

SuggestionBox@opcug.ca