

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ "ЛЬВІВСЬКА ПОЛІТЕХНІКА"**

**Інститут ІКНІ
Кафедра ПЗ**

ЗВІТ

до лабораторної роботи № 1

На тему: *“Ознайомлення з процесами в ОС Windows.”*

З дисципліни: *“Операційні системи”*

Лектор:

ст. викладач ПЗ
Грицай О.Д.

Виконав:

ст. гр. ПЗ-11
Солтисюк Д.А.

Прийняв:

ст. викладач ПЗ
Грицай О.Д.

« ____ » _____ 2022 р.

Σ= ____ .

Тема роботи: Ознайомлення з процесами в ОС Windows.

Мета роботи: Ознайомитися з процесами та потоками в ОС Windows. Навчитися працювати із системними утилітами, що дають можливість отримувати інформацію про процеси, потоки, використовувану ними пам'ять, та іншу необхідну інформацію.

Теоретичні відомості

Операційна система - це сукупність програм, які призначені для керування ресурсами комп'ютера й обчислювальними процесами, а також для організації взаємодії користувача з апаратурою.

Перша функція ОС - керування ресурсами комп'ютера та їх розподіл. Ресурси - це логічні й фізичні компоненти комп'ютера: оперативна пам'ять, місце на диску, периферійні пристрої, процесорний час тощо.

Інша функція ОС - керування обчислювальними процесами. Обчислювальним процесом (або завданням) називається послідовність дій, яка задається програмою. У принципі, функції керування процесами можна було б передати кожній прикладній програмі, але тоді програми були б набагато більшими та складнішими. Тому зручніше мати на комп'ютері одну керуючу програму - операційну систему, послугами якої користуватимуться всі інші програми.

Для виконання третьої функції ОС - забезпечення взаємодії користувача з апаратурою - служить інтерфейс користувача ОС. До складу інтерфейсу користувача входить також набір сервісних програм - утиліт.

Утиліта - це невелика програма, що виконує конкретну сервісну функцію. Утиліти звільняють користувача від виконання рутинних і часом досить складних операцій.

Процес — одне з найважливіших понять у архітектурі операційних систем та програмуванні. Процес — об'єкт операційної системи, контейнер системних ресурсів, призначених для підтримки виконання програми.

Індивідуальне завдання

1. За допомогою утиліти «Диспетчер задач» та Process Explorer отримати повну інформацію про процеси: ідентифікатор процесу, завантаження ЦП (центрального процесора), час ЦП, базовий пріоритет, стан процесу, пам'ять-використання, пам'ять-зміни, пам'ять-максимум, помилок сторінки, об'єкти USER, код сеансу, об'єм віртуальної пам'яті, лічильник дескрипторів, лічильник потоків.
2. За допомогою утиліти Process Explorer отримати додаткову інформацію про процеси та їхні потоки.
3. Використовуючи «Диспетчер задач» та Process Explorer змінити пріоритет будь-якого процесу, від низького до «реального часу»; задати відповідність виконання процесів на окремих ядрах центрального процесора; виконати завершення процесу.
4. Використовуючи Process Explorer призупинити процес і відновити його роботу.
5. Скопіювати файл main.cpp представлений нижче і запустити виконуваний файл на різній кількості активних процесорів (ядер). Знайти для даної програми величини A , S , p при різних вхідних значеннях величини.
6. Дослідити вплив зміни відповідності ядру на швидкодію процесу. Виконати завдання згідно варіанту, що відповідає порядковому номеру у списку підгрупи (сканування деякої папки антивірусом).

Протокол роботи

За допомогою двох утиліт: Диспетчер завдань (Task Manager) та Process Explorer – отримав повну інформацію про процеси, змінив пріоритети процесів та задав відповідність виконання процесу на окремих ядрах ЦП, та завершив виконання процесу за допомогою даних утиліт.

На рис. 1 показаний перелік всіх процесів та їх властивостей стандартному Диспетчері завдань.

Name	PID	Status	User name	CPU	Memory (a...	Archite...	Description
AggregatorHost.exe	4200	Running	SYSTEM	00	748 K	ARM64	Microsoft (R) Aggregator Host
ApplicationFrameHo...	8600	Running	Dmytro	00	2,344 K	ARM64	Application Frame Host
blnsrv.exe	2728	Running	SYSTEM	00	32 K	ARM64	blnsrv
csrss.exe	520	Running	SYSTEM	00	788 K	ARM64	Client Server Runtime Process
csrss.exe	600	Running	SYSTEM	00	824 K	ARM64	Client Server Runtime Process
ctfmon.exe	6596	Running	Dmytro	00	2,384 K	ARM64	CTF Loader
dllhost.exe	6056	Running	Dmytro	00	2,924 K	ARM64	COM Surrogate
dllhost.exe	8340	Running	Dmytro	00	980 K	ARM64	COM Surrogate
dwm.exe	784	Running	DWM-1	02	52,528 K	ARM64	Desktop Window Manager
explorer.exe	4856	Running	Dmytro	01	46,740 K	ARM64	Windows Explorer
fontdrvhost.exe	920	Running	UMFD-0	00	104 K	ARM64	Usermode Font Driver Host
fontdrvhost.exe	912	Running	UMFD-1	00	1,992 K	ARM64	Usermode Font Driver Host
identity_helper.exe	1648	Running	Dmytro	00	3,944 K	ARM64	identity_helper
IpOverUsbSvc.exe	2172	Running	SYSTEM	00	1,648 K	x86	Windows IP Over USB PC Service
LockApp.exe	5276	Suspended	Dmytro	00	0 K	ARM64	LockApp.exe
lsass.exe	760	Running	SYSTEM	01	4,392 K	ARM64	Local Security Authority Process
MiniSearchHost.exe	8512	Suspended	Dmytro	00	0 K	ARM64	MiniSearchHost
msedge.exe	2336	Running	Dmytro	06	5,920 K	ARM64	Microsoft Edge
msedge.exe	620	Running	Dmytro	04	4,960 K	ARM64	Microsoft Edge
msedge.exe	3124	Running	Dmytro	02	4,684 K	ARM64	Microsoft Edge
msedge.exe	9180	Running	Dmytro	00	1,420 K	ARM64	Microsoft Edge
msedge.exe	8568	Running	Dmytro	26	20,620 K	ARM64	Microsoft Edge
msedgewebview2.exe	3504	Running	Dmytro	00	0 K	ARM64	Widgets - WebView2: Widgets
msedgewebview2.exe	8272	Running	Dmytro	00	9,536 K	ARM64	Microsoft Teams - WebView2 Manager
msedgewebview2.exe	8328	Running	Dmytro	00	256 K	ARM64	Microsoft Teams - Crashpad
msedgewebview2.exe	8560	Running	Dmytro	00	1,160 K	ARM64	Microsoft Teams - WebView2 GPU Process
msedgewebview2.exe	8572	Running	Dmytro	00	2,848 K	ARM64	Microsoft Teams - WebView2 Utility: Network Service
msedgewebview2.exe	8620	Running	Dmytro	00	1,188 K	ARM64	Microsoft Teams - WebView2 Utility: Storage Service
msedgewebview2.exe	8764	Running	Dmytro	00	13,292 K	ARM64	Microsoft Teams - WebView2: Microsoft Teams
msedgewebview2.exe	6848	Running	Dmytro	00	1,068 K	ARM64	Widgets - WebView2 Manager
msedgewebview2.exe	2360	Running	Dmytro	00	588 K	ARM64	Widgets - Crashpad
msedgewebview2.exe	1208	Running	Dmytro	00	156 K	ARM64	Widgets - WebView2 GPU Process
msedgewebview2.exe	4588	Running	Dmytro	00	0 K	ARM64	Widgets - WebView2 Utility: Network Service
msedgewebview2.exe	424	Running	Dmytro	00	0 K	ARM64	Widgets - WebView2 Utility: Storage Service
MsMpEng.exe	3248	Running	SYSTEM	11	106,400 K	ARM64	Antimalware Service Executable
msteam.exe	7636	Running	Dmytro	00	4,572 K	ARM64	Microsoft Teams
NisSrv.exe	6960	Running	LOCAL SE...	00	856 K	ARM64	Microsoft Network Realtime Inspection Service
OneDrive.exe	7196	Running	Dmytro	00	4,948 K	ARM64	Microsoft OneDrive
Registry	132	Running	SYSTEM	00	4,356 K	ARM64	NT Kernel & System
RuntimeBroker.exe	5540	Running	Dmytro	00	2,392 K	ARM64	Runtime Broker
RuntimeBroker.exe	5632	Running	Dmytro	00	4,540 K	ARM64	Runtime Broker

Рис. 1. Перелік процесів та їх властивості у Task Manager

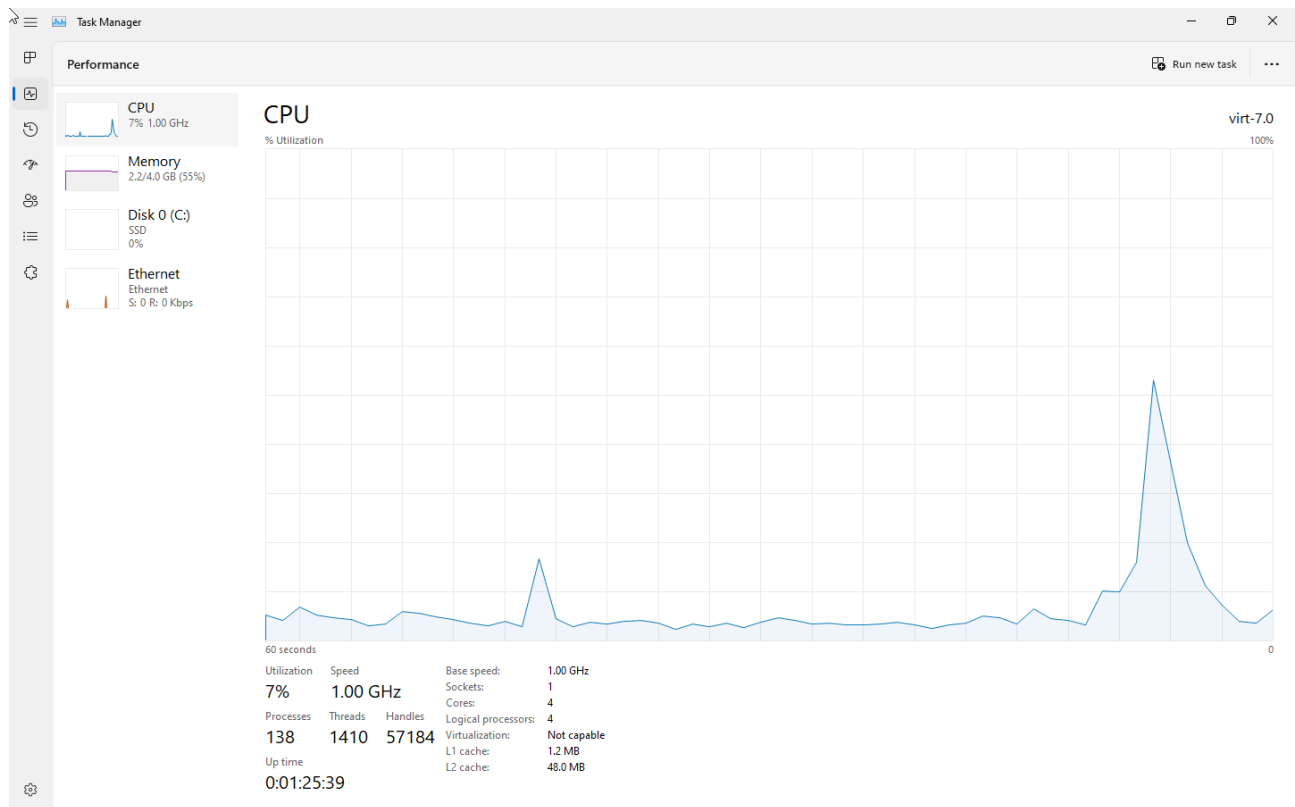


Рис. 2. Використання ресурсів комп'ютера

Process	CPU	PID	Session	CPU Time	Page Faults	Virtual Size	Peak Working Set	USER Objects	Shared Commit	Min Working Set	Max Working Set	Window Status	Private Bytes	Working
Registry	132	0	0	0:00:11.671	70,754	106,992 K	90,120 K	0	0 K	0 K	0 K	0 K	4,964 K	47.00
System Idle Process	98.11	0	0	12:22:58.812	9	4 K	8 K	0	0 K	0 K	0 K	0 K	56 K	
System	< 0.01	4	0	0:15:23.718	3,945	12,312 K	1,132 K	0	0 K	0 K	0 K	0 K	172 K	28
Interrupts	< 0.01	n/a	0	0:06:51.359	0	0 K	0 K	0	0 K	0 K	0 K	0 K	0 K	
smss.exe	400	0	0	0:00:00.859	1,301	2,151,720,596 K	1,524 K	0	0 K	0 K	0 K	0 K	1,688 K	1.17
Memory Compression	1820	0	0	0:01:44.968	175,860	167,808 K	166,288 K	0	0 K	0 K	0 K	0 K	4,936 K	146.20
csrss.exe	520	0	0	0:00:08.546	4,371	2,151,784,104 K	7,412 K	0	0 K	0 K	0 K	0 K	2,376 K	6.23
svchost.exe	592	0	0	0:00:00.796	2,755	2,151,761,976 K	8,624 K	0	0 K	0 K	0 K	0 K	1,744 K	7.34
services.exe	732	0	0	0:00:24.687	12,047	2,151,749,124 K	10,628 K	0	0 K	0 K	0 K	0 K	4,992 K	8.87
svchost.exe	876	0	0	0:01:20.187	61,616	2,151,869,376 K	32,080 K	0	0 K	0 K	0 K	0 K	10,804 K	30.22
SearchHost.exe	Susp...	5376	1	0:02:15.453	345,245	2,186,295,908 K	288,756 K	112	16,936 K	200 K	1,380 K	0 K	160,608 K	260.94
Widgets.exe	5384	1	0	0:00:32.750	34,207	2,168,784,052 K	51,852 K	24	3,792 K	200 K	1,380 K	0 K	9,800 K	46.79
msedgeview2.exe	6848	1	0	0:01:10.281	94,384	2,219,616,012 K	106,908 K	42	10,728 K	200 K	1,380 K	0 K	31,268 K	12.02
msedgeview.exe	2360	1	0	0:00:01.812	3,076	2,189,396,072 K	10,000 K	3	3,316 K	200 K	1,380 K	0 K	2,136 K	9.32
msedgeview.exe	1208	1	0	0:00:12.921	53,284	2,202,663,956 K	54,704 K	18	12,544 K	200 K	1,380 K	0 K	21,316 K	3.73
msedgeview.exe	4588	1	0	0:00:09.187	26,534	2,202,465,708 K	27,844 K	1	2,756 K	200 K	1,380 K	0 K	9,188 K	2.45
msedgeview.exe	424	1	0	0:00:01.609	12,302	2,202,416,488 K	18,688 K	1	2,396 K	200 K	1,380 K	0 K	7,228 K	2.01
msedgeview.exe	3504	1	0	0:00:22.343	85,549	3,347,654,700 K	77,696 K	0	3,764 K	200 K	1,380 K	0 K	22,944 K	2.06
StartMenuExperience.exe	5408	1	0	0:00:38.328	42,302	2,152,258,108 K	93,312 K	17	5,256 K	200 K	1,380 K	0 K	32,608 K	89.93
RuntimeBroker.exe	5540	1	0	0:00:10.640	16,441	2,151,903,388 K	31,520 K	4	2,688 K	200 K	1,380 K	0 K	6,676 K	28.40
RuntimeBroker.exe	5632	1	0	0:00:16.359	27,239	2,152,031,592 K	52,884 K	12	3,792 K	200 K	1,380 K	0 K	13,392 K	50.57
dllhost.exe	6056	1	0	0:00:06.765	17,605	2,151,892,336 K	22,964 K	3	2,480 K	200 K	1,380 K	0 K	6,484 K	19.70
lockApp.exe	Susp...	5276	1	0:00:01.312	15,575	2,152,114,752 K	55,552 K	22	3,616 K	200 K	1,380 K	0 K	12,820 K	46.64
RuntimeBroker.exe	6300	1	0	0:00:06.281	14,612	2,151,919,212 K	44,624 K	4	3,632 K	200 K	1,380 K	0 K	9,116 K	33.62
TextInputHost.exe	6728	1	0	0:00:55.281	77,648	2,186,050,580 K	178,780 K	85	5,276 K	200 K	1,380 K	Running	78,076 K	97.58
RuntimeBroker.exe	4420	1	0	0:00:01.859	4,402	2,151,903,880 K	15,460 K	1	2,644 K	200 K	1,380 K	0 K	2,472 K	13.44
WinSearchHost.exe	Susp...	8512	1	0:00:01.562	30,009	2,152,225,184 K	76,320 K	31	6,516 K	200 K	1,380 K	0 K	21,708 K	72.15
SystemSettings.exe	Susp...	4620	1	0:00:02.562	30,422	2,152,364,340 K	111,640 K	33	11,224 K	200 K	1,380 K	Running	35,816 K	4.59
ApplicationFrameHost.exe	8600	1	0	0:00:14.031	26,905	2,152,076,680 K	46,064 K	31	6,888 K	200 K	1,380 K	Running	13,956 K	44.07
UserOOBEBroker.exe	6532	1	0	0:00:00.812	3,418	2,151,799,992 K	12,144 K	1	2,360 K	200 K	1,380 K	0 K	2,292 K	11.36
ShellExperienceHost.exe	Susp...	6820	1	0:00:14.140	47,189	2,152,316,972 K	98,940 K	86	9,460 K	200 K	1,380 K	0 K	40,316 K	98.53
RuntimeBroker.exe	2220	1	0	0:00:08.125	18,546	2,151,956,892 K	38,480 K	15	3,648 K	200 K	1,380 K	0 K	8,304 K	35.94
dllhost.exe	8340	1	0	0:00:01.500	3,810	2,151,801,100 K	13,224 K	5	2,412 K	200 K	1,380 K	0 K	1,948 K	13.21
RuntimeBroker.exe	1016	1	0	0:00:02.515	10,879	2,151,873,332 K	31,672 K	4	2,740 K	200 K	1,380 K	0 K	8,268 K	25.81
SystemSettingsBroker.exe	7508	1	0	0:00:02.703	7,622	2,151,895,380 K	27,528 K	0	2,644 K	200 K	1,380 K	0 K	4,772 K	23.93
RecHealthUI.exe	Susp...	4632	1	0:00:15.656	32,470	2,152,178,804 K	84,700 K	21	8,252 K	200 K	1,380 K	Running	32,484 K	83.68
SecurityHealthHost.exe	1176	1	0	0:00:00.968	3,756	2,151,806,724 K	12,980 K	1	2,640 K	200 K	1,380 K	0 K	2,660 K	12.50
RuntimeBroker.exe	8256	1	0	0:00:00.306	6,023	2,151,823,500 K	19,084 K	1	2,656 K	200 K	1,380 K	0 K	2,692 K	16.28
svchost.exe	1004	0	0	0:00:59.218	29,071	2,151,782,704 K	16,076 K	0	0 K	0 K	0 K	0 K	7,972 K	15.50
svchost.exe	476	0	0	0:00:09.203	3,606	2,151,774,240 K	10,304 K	0	0 K	0 K	0 K	0 K	2,808 K	9.11
svchost.exe	1084	0	0	0:00:01.296	3,620	2,151,782,072 K	12,332 K	0	0 K	0 K	0 K	0 K	2,836 K	10.08
svchost.exe	1092	0	0	0:00:00.625	1,817	2,151,758,696 K	6,392 K	0	0 K	0 K	0 K	0 K	1,420 K	5.73
svchost.exe	1108	0	0	0:00:02.943	3,823	2,151,786,676 K	11,448 K	0	0 K	0 K	0 K	0 K	2,352 K	10.67
svchost.exe	1216	0	0	0:00:14.140	76,867	2,151,841,248 K	38,664 K	0	0 K	0 K	0 K	0 K	5,172 K	17.74
svchost.exe	1228	0	0	0:00:02.109	3,798	2,151,814,984 K	12,036 K	0	0 K	0 K	0 K	0 K	2,676 K	10.70
svchost.exe	1236	0	0	0:00:19.078	22,081	2,151,831,564 K	19,380 K	0	0 K	0 K	0 K	0 K	6,544 K	17.50
taskhost.exe	3940	1	0	0:00:16.187	12,021	2,151,904,880 K	22,080 K	6	3,792 K	200 K	1,380 K	0 K	6,676 K	21.09
taskhost.exe	9040	1	0	0:00:06.625	8,603	2,151,890,596 K	24,892 K	2	3,624 K	200 K	1,380 K	0 K	4,936 K	17.67

CPU Usage: 2.21% Commit Charge: 46.58%

Рис. 3. Перелік процесів та їх властивості у Process Explorer

За допомогою утиліти Process Explorer отримаємо додаткову інформацію про процеси та їхні потоки.

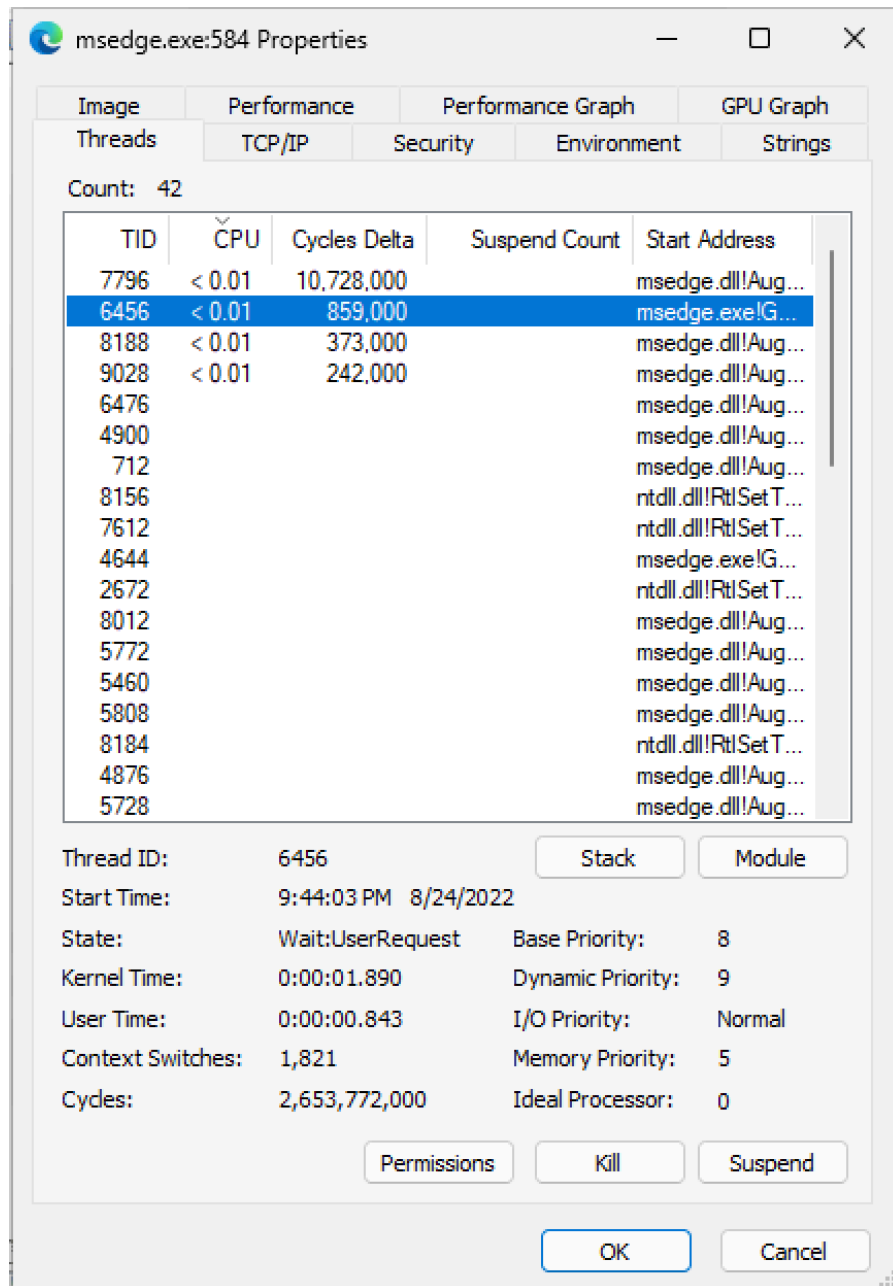


Рис. 4. Перелік параметрів обраного процесу в Process Explorer

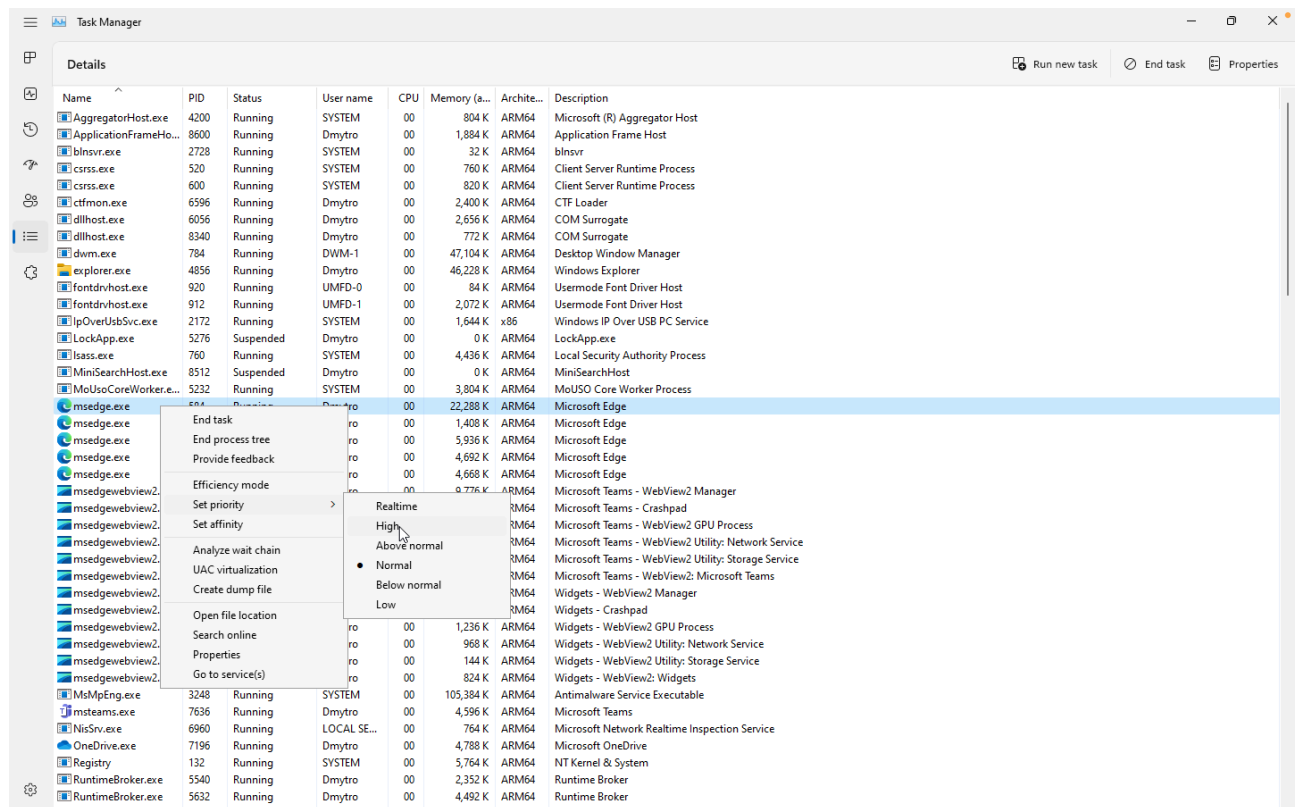


Рис. 5. Зміна пріоритетності процесу в Task Manager

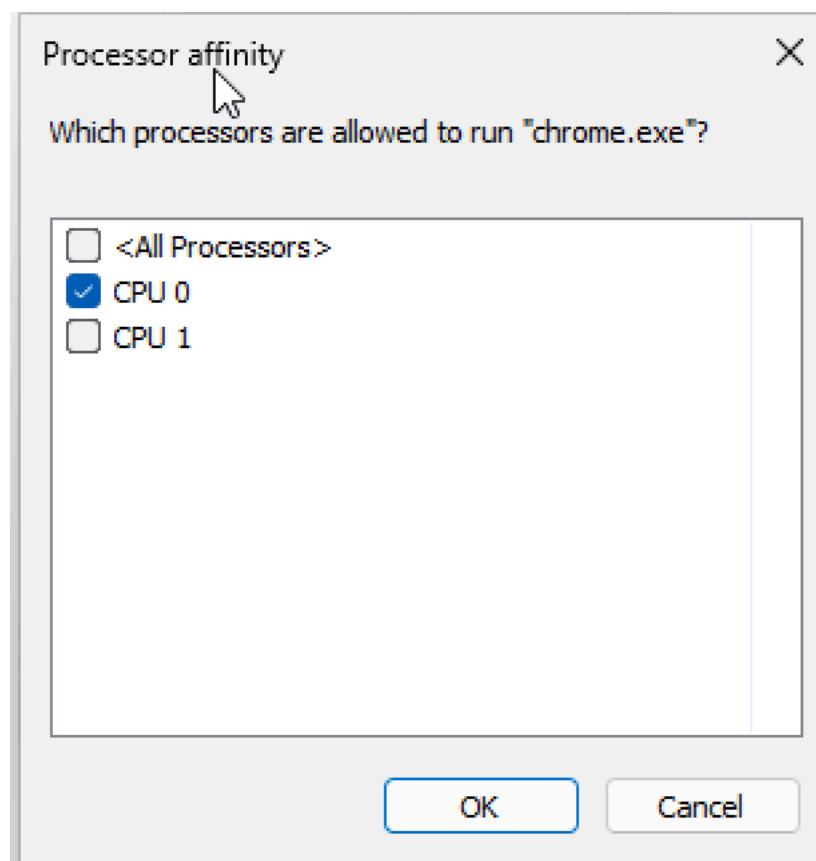


Рис. 6. Задання відповідності виконання процесу на окремих ядрах центрального процесора

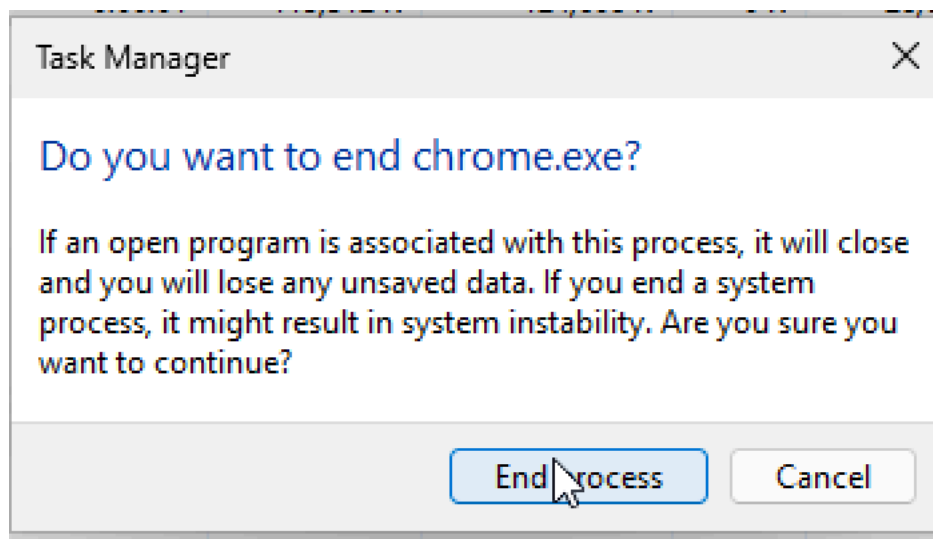


Рис. 7. Завершення процесу

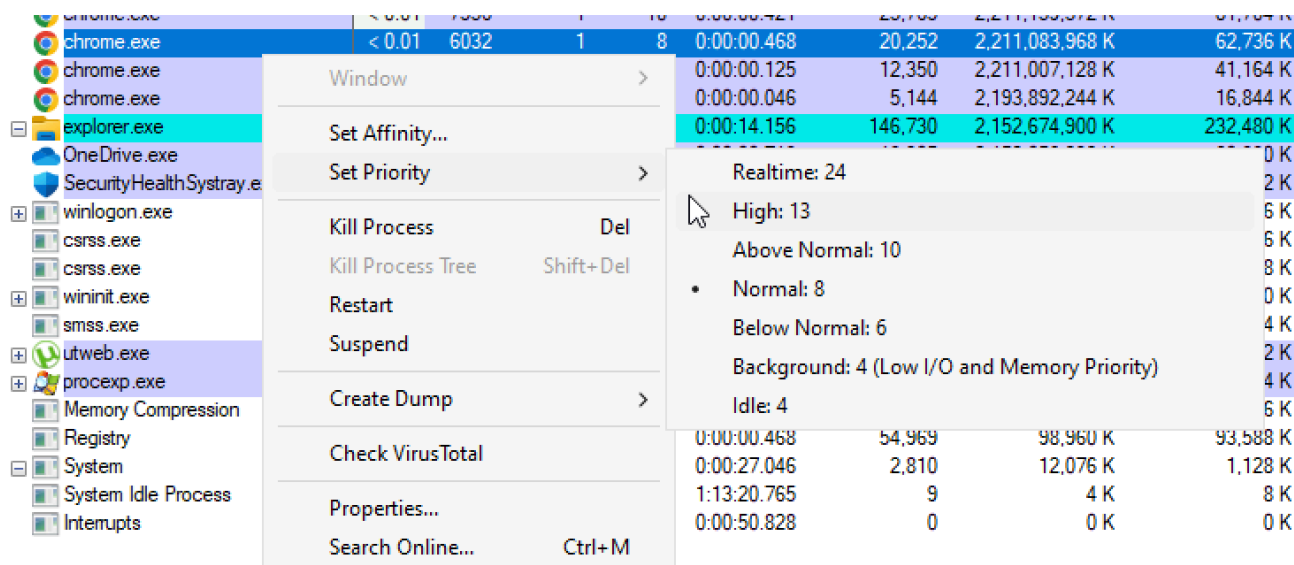


Рис. 8. Зміна пріоритету в Process Explorer

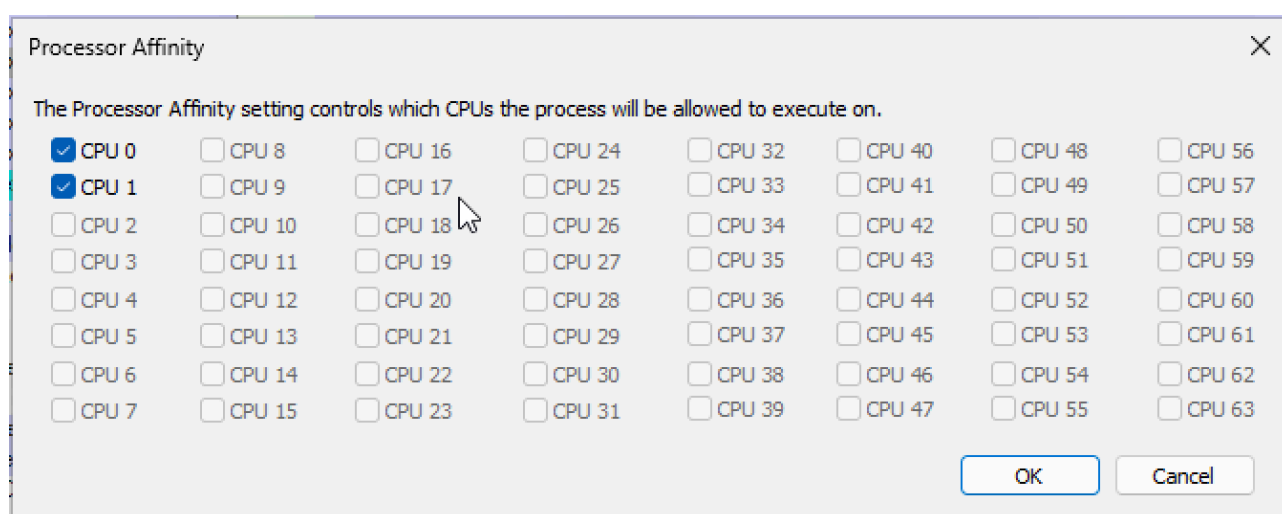


Рис. 9. Задання відповідності виконання процесу на окремих ядрах центрального процесора

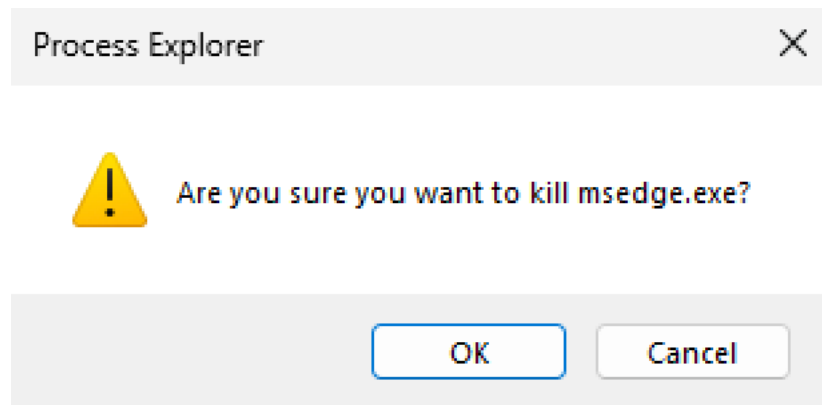


Рис. 10. Завершування процесу

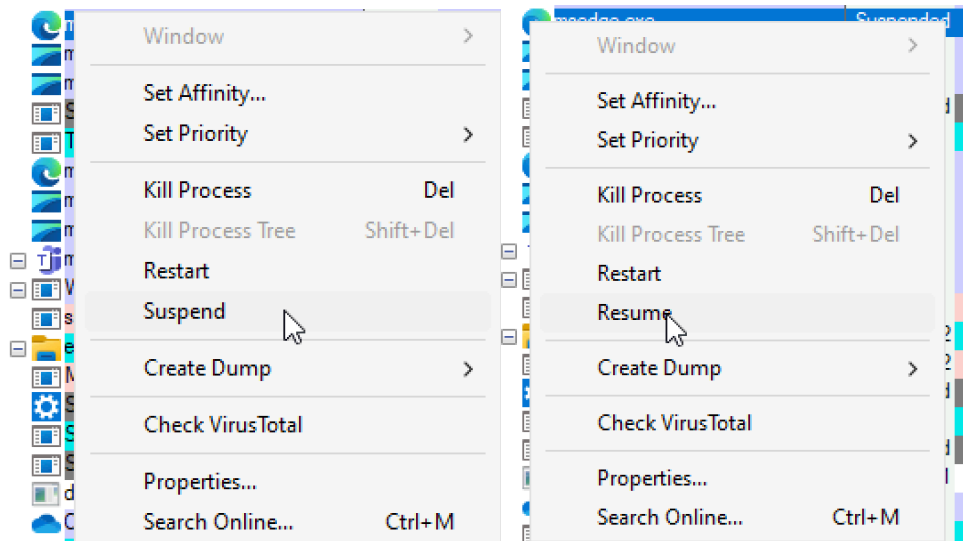


Рис. 11. Призупинка процесу і відновлення роботи в Process Explorer

$$p = \frac{\frac{n}{A} - 1}{n - 1}$$

$$n = 2,$$

$$A_2 = \frac{T_1}{T_2} = \frac{6719}{3582} = 1,88$$

$$S_2 = A_2 = 1.88$$

$$p_2 = \frac{2}{A_2} - 1 = \frac{2}{1.88} - 1 = 0.06$$

$$n = 3,$$

$$A_3 = \frac{T_1}{T_3} = \frac{6719}{2973} = 2.26$$

$$S_3 = A_3 = 2.26$$

$$p_3 = \frac{\frac{3}{A_3} - 1}{2} = \frac{\frac{3}{2.26} - 1}{2} = 0.16$$

$$n = 4,$$

$$A_4 = \frac{T_1}{T_4} = \frac{6719}{2548} = 2.63,$$

$$S_4 = A_4 = 2.63$$

$$p_4 = \frac{\frac{4}{A_4} - 1}{3} = \frac{\frac{4}{2.63} - 1}{3} = 0.17$$

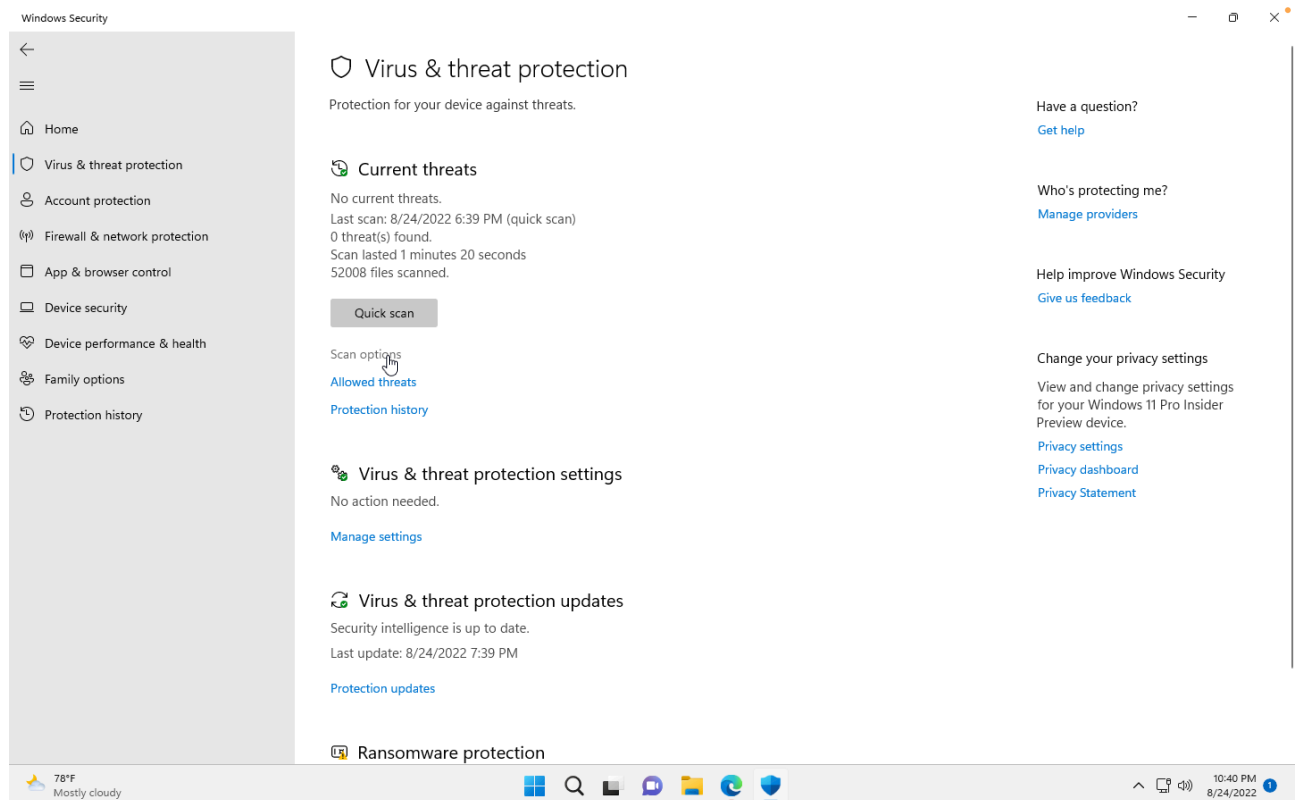


Рис. 12. Вибір опцій сканування для антивірусу в Windows Security для сканування папки

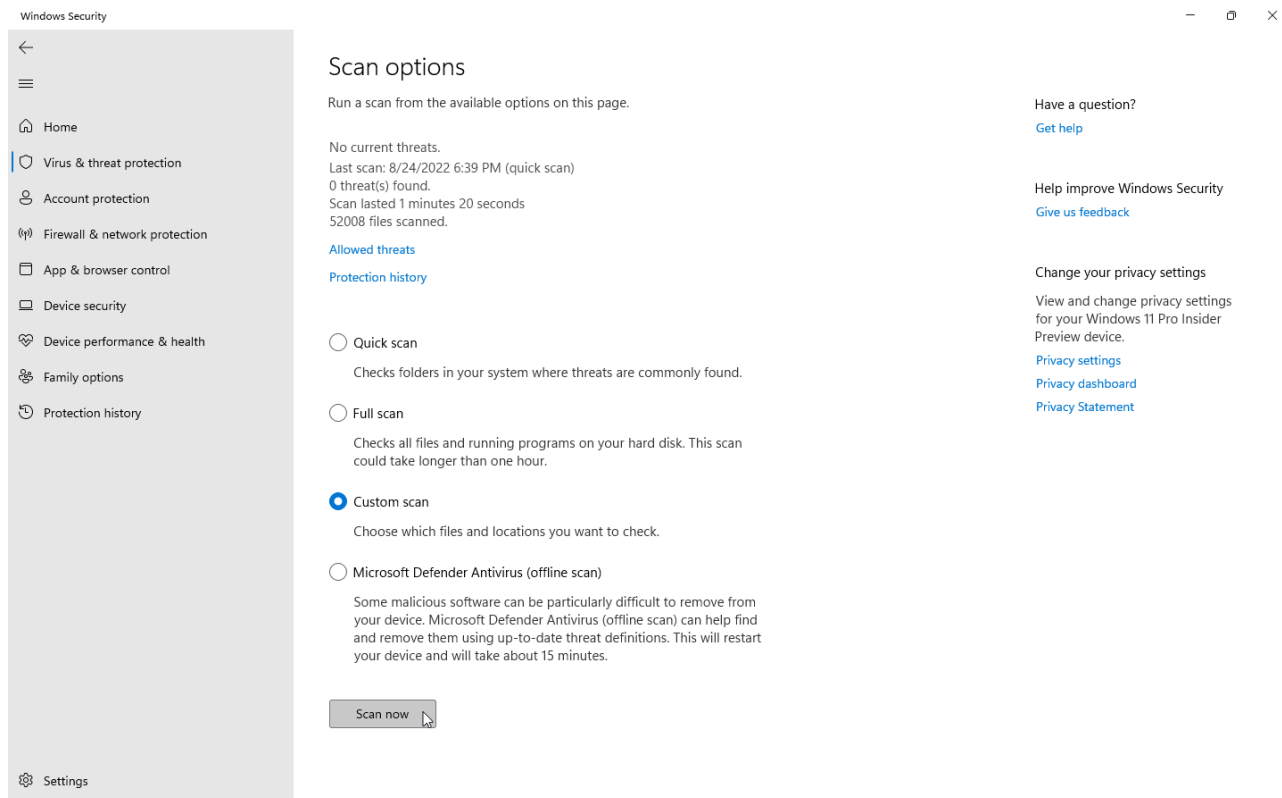


Рис. 13. Экран выбора опций для сканирования папки у Windows Security

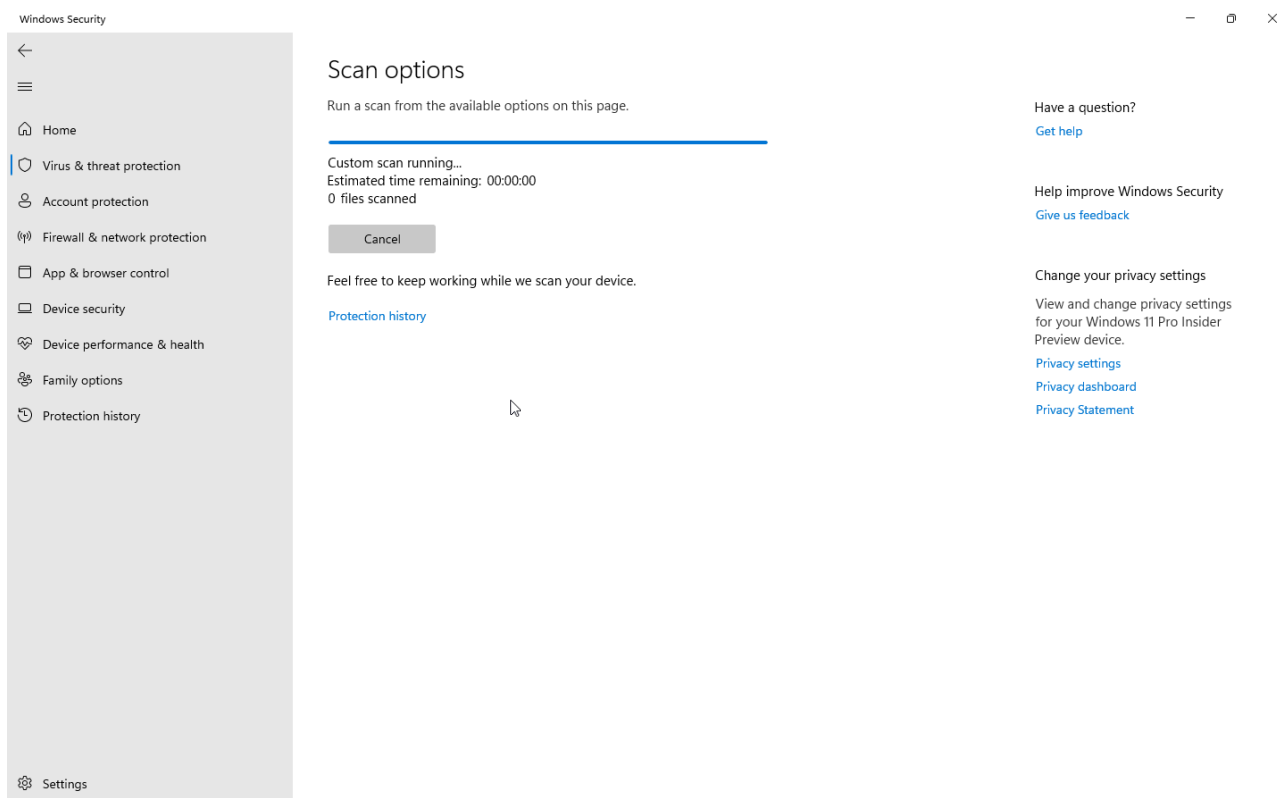


Рис. 14. Экран сканирования папки программой Windows Security

Scan options

Run a scan from the available options on this page.

No current threats.

Last scan: 8/24/2022 10:44 PM (custom scan)

0 threat(s) found.

Scan lasted 1 seconds

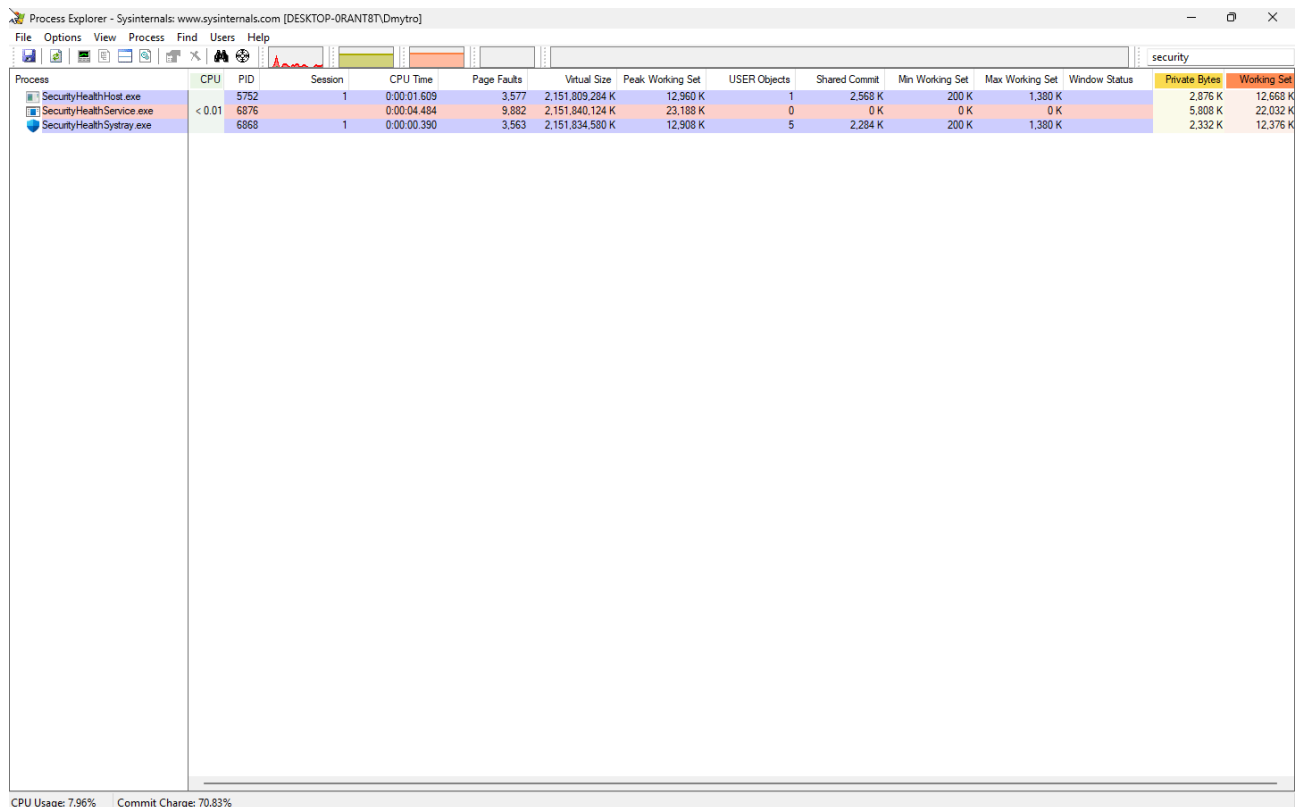
24 files scanned.

Quick scan

Allowed threats

Protection history

Рис. 15. Результати сканування Windows Security



The screenshot shows the Process Explorer window from Sysinternals. The title bar reads 'Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-ORANT8T\Dmytro]'. The menu bar includes File, Options, View, Process, Find, Users, and Help. The toolbar contains icons for file operations, process management, and system information. The main window displays a table of running processes. The table has columns for Process, CPU, PID, Session, CPU Time, Page Faults, Virtual Size, Peak Working Set, USER Objects, Shared Commit, Min Working Set, Max Working Set, Window Status, Private Bytes, and Working Set. Three processes are listed: SecurityHealthHost.exe (PID 5752), SecurityHealthService.exe (PID 6876), and SecurityHealthSystray.exe (PID 6868). The CPU usage for these processes is less than 0.01%. The status bar at the bottom shows 'CPU Usage: 7.96%' and 'Commit Charge: 70.83%'.

Process	CPU	PID	Session	CPU Time	Page Faults	Virtual Size	Peak Working Set	USER Objects	Shared Commit	Min Working Set	Max Working Set	Window Status	Private Bytes	Working Set
SecurityHealthHost.exe	< 0.01	5752	1	0:00:01.609	3,577	2,151,809,284 K	12,960 K	1	2,568 K	200 K	1,380 K		2,876 K	12,668 K
SecurityHealthService.exe		6876		0:00:04.484	9,882	2,151,840,124 K	23,188 K	0	0 K	0 K	0 K		5,808 K	22,032 K
SecurityHealthSystray.exe		6868	1	0:00:00.390	3,563	2,151,834,580 K	12,908 K	5	2,284 K	200 K	1,380 K		2,332 K	12,376 K

Рис. 16. Вплив сканування Windows Security без обмежень

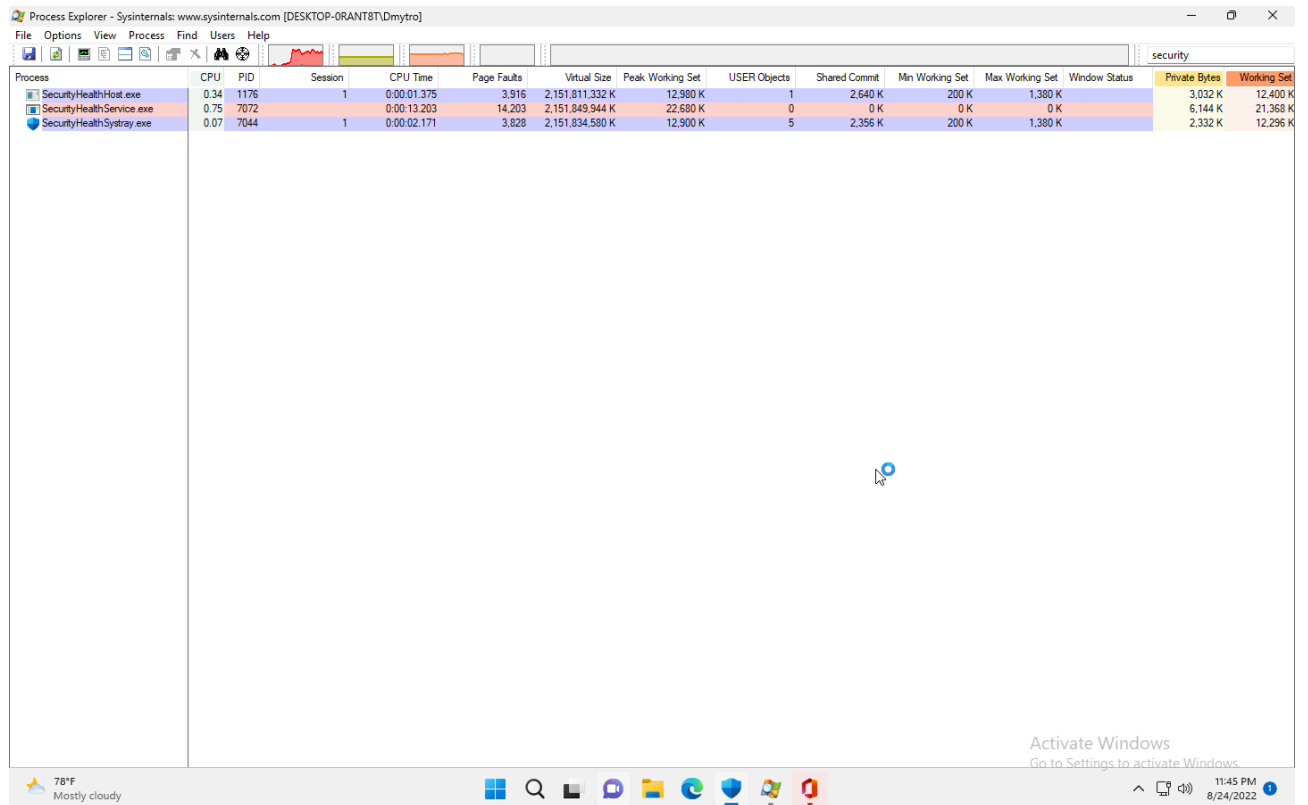


Рис. 17. Вплив сканування Windows Security з обмеженнями

Висновки

На лабораторній роботі я ознайомився з поняттями процес та потік та навчився проводити моніторинг, виставляти пріоритетність, завершувати процеси та керувати ними за допомогою системних утиліт: Диспетчер завдань (Task Manager) та Process Explorer.