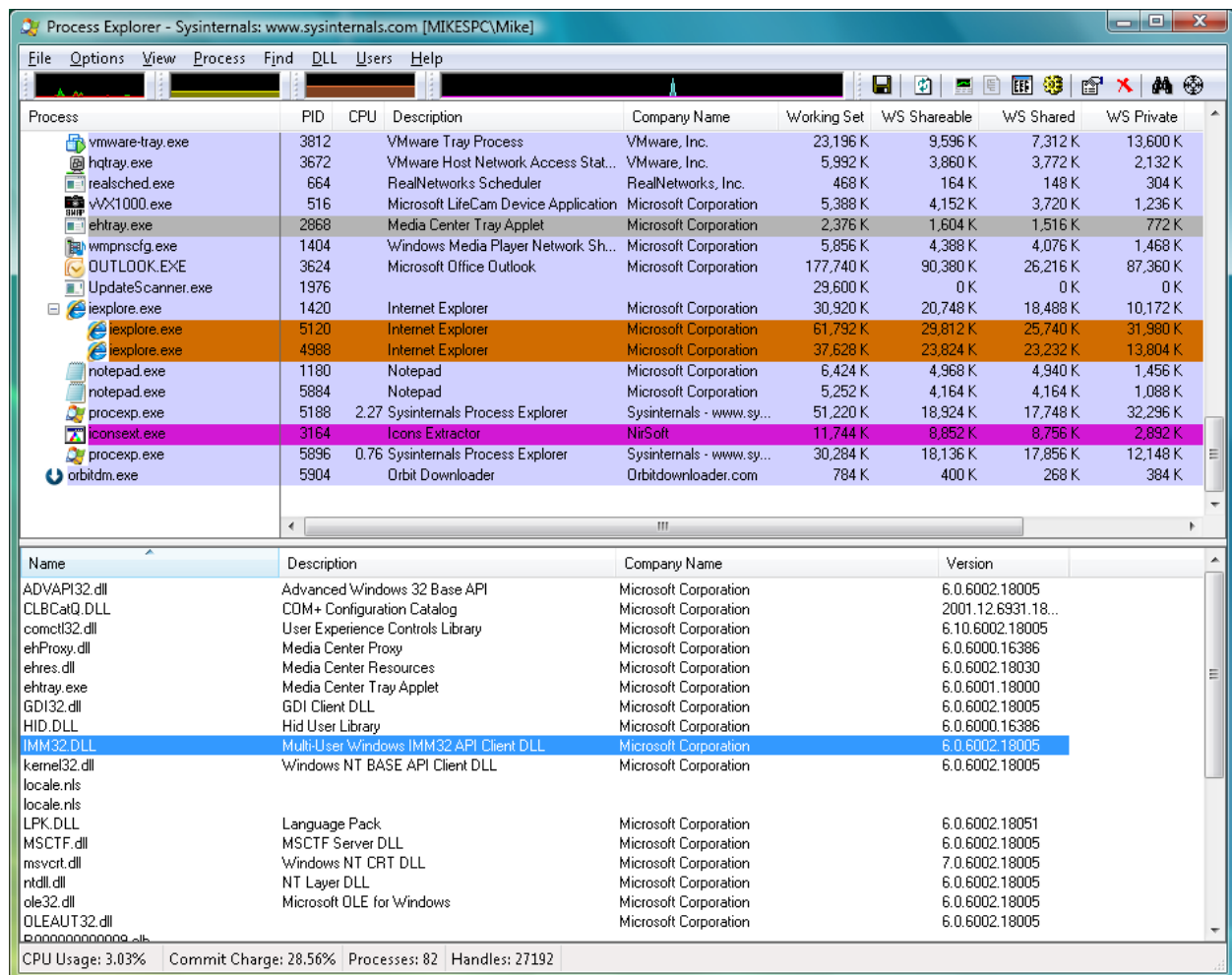


הדגמת Process Explorer

Process Explorer (סייר התהליכים procexp) הינה תוכנה מבית Sysinternals (חברה שנקנתה על ידי Microsoft) שנועדה להציג המון מידע על מערכת ההפעלה, ובמיוחד על התהליכים הרצים בה. התוכנה הינה חלק מה-Sysinternals Suite-אוסף תוכנות מאוד חזקות ושימושיות שמראות בצורה נוחה את רוב חלקיה של מערכת ההפעלה. ניתן להוריד את הכלים מהאתר של Microsoft בחינם (<https://docs.microsoft.com/he-il/sysinternals/downloads/sysinternals-suite>)

ניתן להוריד את התוכנות גם מאתר הקורס ב-google classroom. לאחר שנוריד את החבילה ונפתח אותה, נריץ את Procexp.exe (בהרשאות אדמיניסטרטור) ונראה מה הוא מציג.



The screenshot shows the Process Explorer window with the 'Process' tab selected. The table below lists the running processes, and the table below that lists the loaded DLLs.

Process	PID	CPU	Description	Company Name	Working Set	WS Shareable	WS Shared	WS Private
vmware-tray.exe	3812		VMware Tray Process	VMware, Inc.	23,196 K	9,596 K	7,312 K	13,600 K
hqtray.exe	3672		VMware Host Network Access Stat...	VMware, Inc.	5,992 K	3,860 K	3,772 K	2,132 K
realsched.exe	664		RealNetworks Scheduler	RealNetworks, Inc.	468 K	164 K	148 K	304 K
vx1000.exe	516		Microsoft LifeCam Device Application	Microsoft Corporation	5,388 K	4,152 K	3,720 K	1,236 K
ehtray.exe	2868		Media Center Tray Applet	Microsoft Corporation	2,376 K	1,604 K	1,516 K	772 K
wmprscfg.exe	1404		Windows Media Player Network Sh...	Microsoft Corporation	5,856 K	4,388 K	4,076 K	1,468 K
OUTLOOK.EXE	3624		Microsoft Office Outlook	Microsoft Corporation	177,740 K	90,380 K	26,216 K	87,360 K
UpdateScanner.exe	1976				29,600 K	0 K	0 K	0 K
ieexplore.exe	1420		Internet Explorer	Microsoft Corporation	30,920 K	20,748 K	18,488 K	10,172 K
ieexplore.exe	5120		Internet Explorer	Microsoft Corporation	61,792 K	29,812 K	25,740 K	31,960 K
ieexplore.exe	4988		Internet Explorer	Microsoft Corporation	37,628 K	23,824 K	23,232 K	13,804 K
notepad.exe	1180		Notepad	Microsoft Corporation	6,424 K	4,968 K	4,340 K	1,456 K
notepad.exe	5884		Notepad	Microsoft Corporation	5,252 K	4,164 K	4,164 K	1,088 K
procexp.exe	5188	2.27	Sysinternals Process Explorer	Sysinternals - www.sy...	51,220 K	18,924 K	17,748 K	32,296 K
iconsext.exe	3164		Icons Extractor	NirSoft	11,744 K	8,852 K	8,756 K	2,892 K
procexp.exe	5896	0.76	Sysinternals Process Explorer	Sysinternals - www.sy...	30,284 K	18,136 K	17,856 K	12,148 K
orbitdm.exe	5904		Orbit Downloader	Orbitdownloader.com	784 K	400 K	268 K	384 K

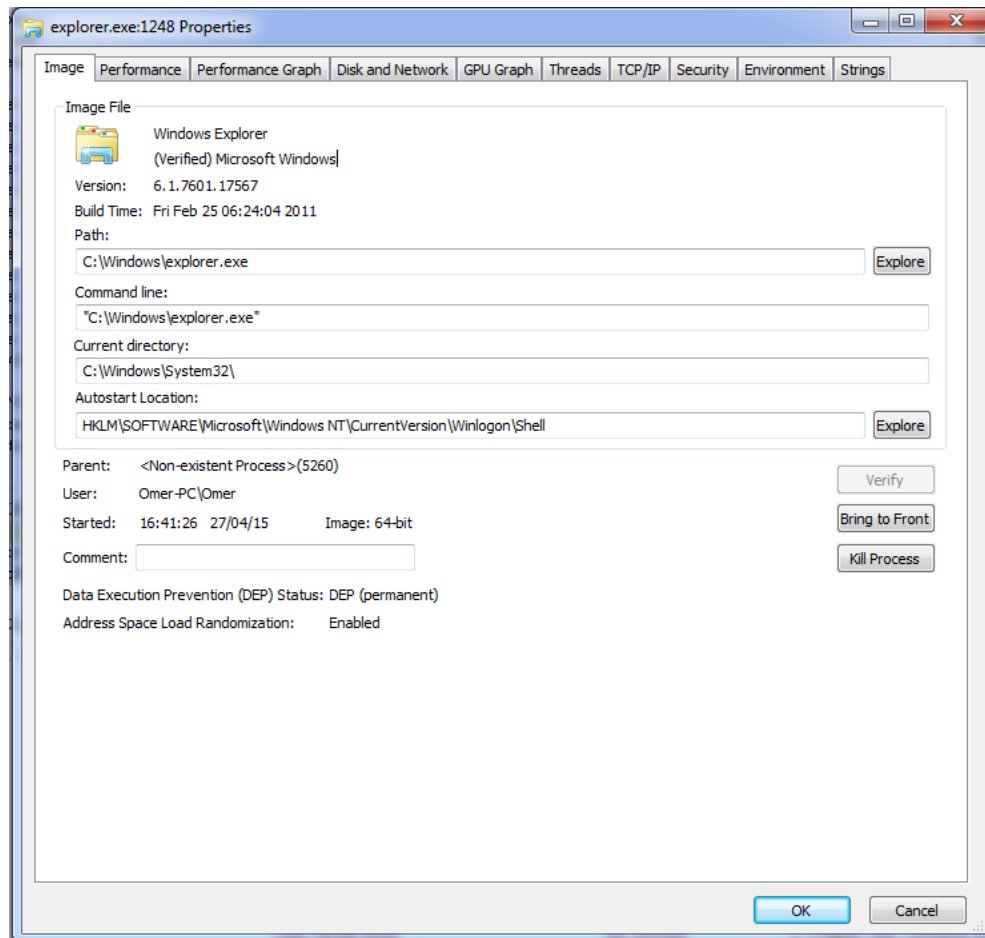
Name	Description	Company Name	Version
ADVAPI32.dll	Advanced Windows 32 Base API	Microsoft Corporation	6.0.6002.18005
CLBCatQ.DLL	COM+ Configuration Catalog	Microsoft Corporation	2001.12.6931.18...
comctl32.dll	User Experience Controls Library	Microsoft Corporation	6.10.6002.18005
ehProxy.dll	Media Center Proxy	Microsoft Corporation	6.0.6000.16386
ehres.dll	Media Center Resources	Microsoft Corporation	6.0.6002.18030
ehtray.exe	Media Center Tray Applet	Microsoft Corporation	6.0.6001.18000
GDI32.dll	GDI Client DLL	Microsoft Corporation	6.0.6002.18005
HID.DLL	Hid User Library	Microsoft Corporation	6.0.6000.16386
IMM32.DLL	Multi-User Windows IMM32 API Client DLL	Microsoft Corporation	6.0.6002.18005
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	6.0.6002.18005
locale.nls			
locale.nls			
LPK.DLL	Language Pack	Microsoft Corporation	6.0.6002.18051
MSCTF.dll	MSCTF Server DLL	Microsoft Corporation	6.0.6002.18005
msvcrt.dll	Windows NT CRT DLL	Microsoft Corporation	7.0.6002.18005
ntdll.dll	NT Layer DLL	Microsoft Corporation	6.0.6002.18005
ole32.dll	Microsoft OLE for Windows	Microsoft Corporation	6.0.6002.18005
OLEAUT32.dll		Microsoft Corporation	6.0.6002.18005

CPU Usage: 3.03% Commit Charge: 28.56% Processes: 82 Handles: 27192

נשים לב כי אנחנו רואים פה את כל התהליכים שראינו קודם במנהל המשימות: Explorer, winlogon, lsass, system. לפני שנתחיל להסתכל ממש עבור כל תהליך, נסתכל קצת על המידע המוצג במסך הראשי. ניתן להוסיף ולהוריד עמודות מידע בעזרת הלחצן הימני בשורה עם שמות העמודות. האם יש משהו שניתן לראות במנהל התהליכים ולא ניתן לראות כאן? על מנת לראות את החלון התחתון גשו ל-view->Shoe Lower Pane.

מידע על תהליך ספציפי

כעת נפתח ונראה את המידע המפורט הניתן לראות עבור כל תהליך.
משימה 1 : נפתח את המידע המוצג על explorer ונשווה אותו למידע שקיבלנו ממנהל המשימות (עימדו על התהליך, לחצו כפתור ימני ובחרו ב'פרטים...' – 'properties...').



אנו רואים פה גם דברים שראינו כבר בעבר Path , Command Line – וגם דברים חדשים שלא הכרנו:

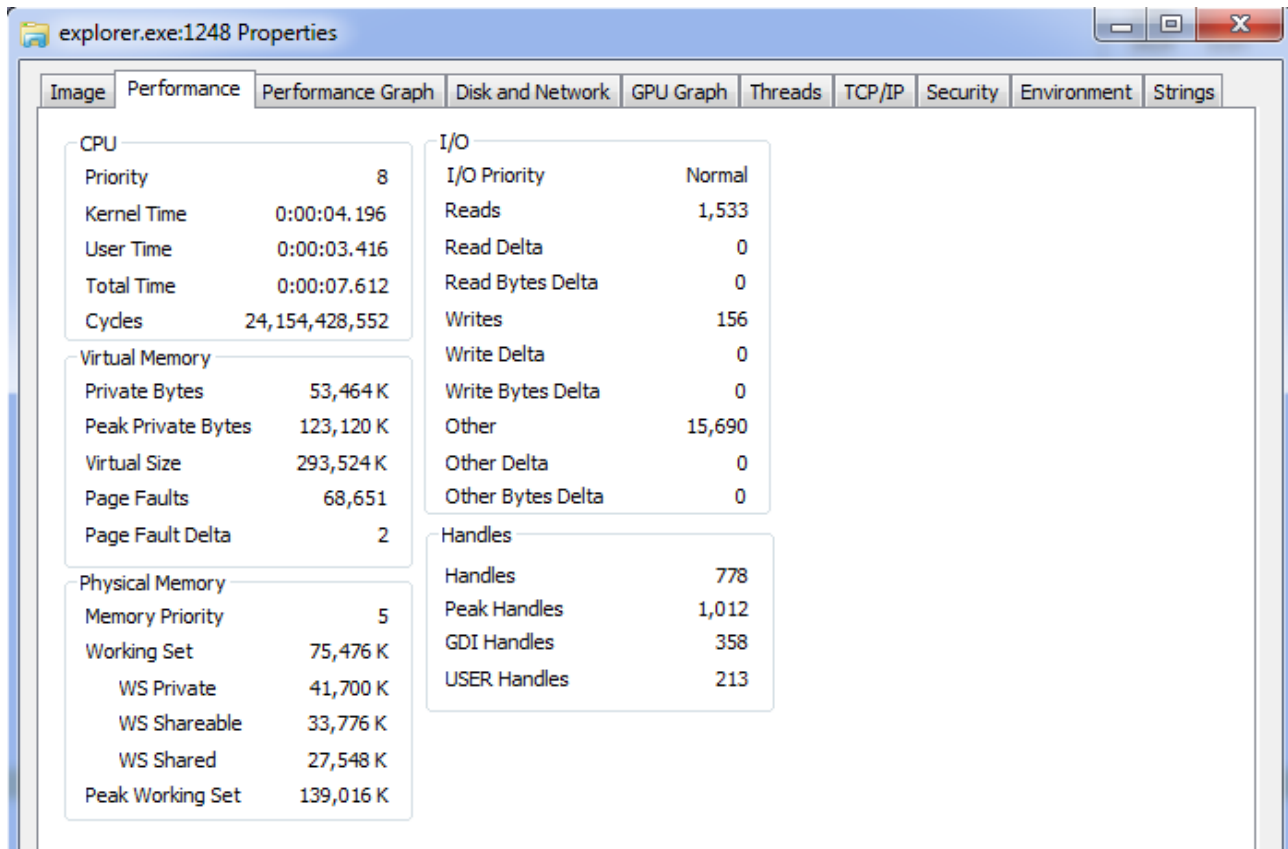
- Current Directory - התיקיה שמתוכה התהליך רץ כרגע.
- Parent - התהליך היוצר של התהליך הנוכחי (הסבירו לעצמכם מה קרה לתהליך האבא בתמונה הנ"ל).

ויש עוד הרבה מידע שכרגע לא מעניין אותנו. אנו רואים בחלקו העליון של המסך כי ישנם הרבה tabs- שונים המכילים הרבה מידע על התהליך. נעבור על החשובים שביניהם שהם Performance, Environment ו-Strings.

תרגיל: הסתכלו על ה tab של "TCP/IP" ושל "Performance Graph" ואמרו מה המידע המעניין המוכל בהם.

לשונית ה-Performance מפרטת מידע על הביצועים של התהליך. נסביר קצת על כל אחת מהקבוצות המופיעות:

- CPU - כמה זמן באמת התוכנה רצה ובאיזה חלק של מערכת ההפעלה (אם ב-User או ב-Kernel).
- Virtual Memory\Physical Memory - כרגע לא נסביר את ההבדל, אלה רק נשים לב שקיימים – 2 צורות עם ערכים שונים.
- I/O - קיצור ל-Input/Output, כמה התוכנה קוראת וכותבת. אין פה המון מידע שימושי, כדאי להשוות את זה אל מול Disk and Network.



משימה 2:

- פתחו חלון CMD חדש והריצו בתוכו Python. מצאו את התהליך שלו ב-Process Explorer.
- הסבירו לעצמכם למה זמן ה-CPU לא עולה כל עוד אתם לא כותבים בו פקודות.
- כתבו את השורות הבאות ב-python והסבירו את השינוי בזמן ה-CPU:

```
>>> i = 2
>>> for i in range(1000000):
...     i *= 8
```

- כתבו את השורות הבאות והסבירו את השינויים שאתם רואים בזמן ובצריכת הזיכרון אחרי כל שורה:

```
>>> b = []
>>> for i in range(1000000):
...     b.append(i)
```

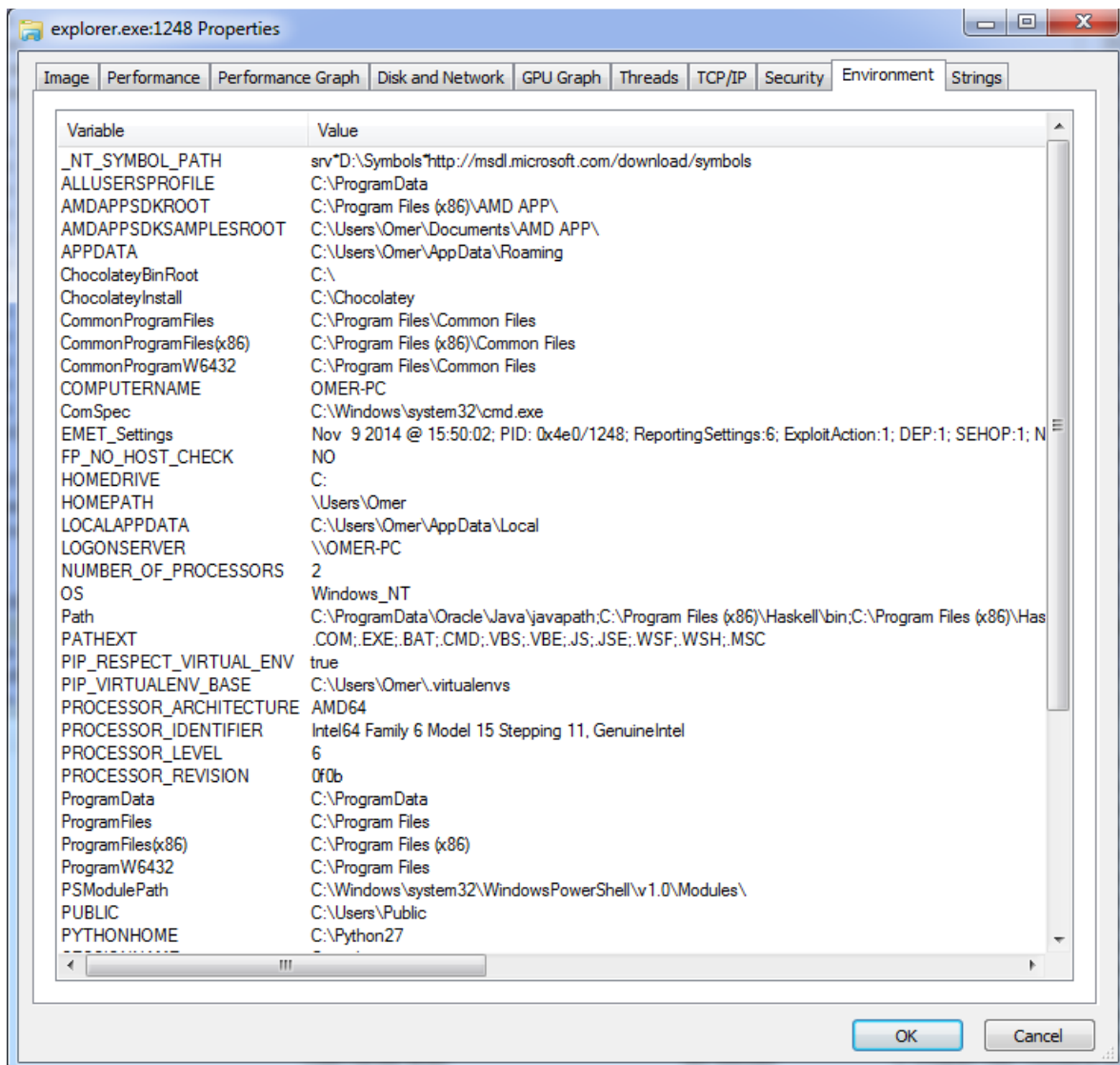
- כתבו את השורות הבאות והסבירו את השינויים שאתם רואים בזמן ובצריכת הזיכרון אחרי כל שורה:

```
>>> del(b)
```

- כתבו את השורות הבאות, ומצאו כמה תהליכים, נוצרו, מי יצר כל תהליך והסבירו זאת:
- ```
>>> import os
>>> os.system("python")
```

(**ההסבר** הוא שהפקודה system יוצרת cmd חדש, ואנחנו מתוכה יוצרים את ה-python החדש)

**לשונית ה-Environment** מכילה טבלת-Variable (משתנים) עם Value (ערך) לכל אחד. אלו הם "משתני הסביבה" של התהליך. משתנים אלו נועדו לעזור להגדיר פרמטרים לתוכנות דרך שורת הפקודה. הרעיון ישן, עוד מלפני שמחשבים היו דבר אישי עם הגרפיקה היפה של היום ואז לא הייתה דרך טובה יותר – להעביר הגדרות לתוכנה (השיטה השנייה הנפוצה הייתה לשנות את ה-assembly של התוכנה שאת ההגדרות שלה רצית לשנות).



למעשה יש שימוש מאוד נרחב במשתני סביבה גם היום. רוב המערכות העובדות בשורת הפקודה (והרבה תוכנות עם ממשק גרפי מודרני) עדיין מקבלות ועובדות עם פרמטרים אלו, וכן הם משמשים להגדרות כלליות של מערכת ההפעלה העוברות לכלל התוכנות.

**משימה 3 :** כעת נעשה תרגיל המדגים איך עובדים עם משתני סביבה, ונכיר קצת יותר טוב את שורת הפקודה של Windows.

**הערה** אומנם אנחנו לומדים על-Windows וספציפית שורת הפקודה של Windows, אך צורת העבודה עם משתני סביבה די זהה כמעט בכל מערכות ההפעלה

- פתחו את שורת הפקודה (WinKey ולאחר מכן הקלידו `cmd`)
- הריצו בשורת הפקודה את הפקודה `set` וראו מה הפלט שלה. השוו פלט זה אל מול הפלט של מסך ה-Environment של התהליך של שורת הפקודה שממנו הרצתם את הפקודה.
- הריצו את הפקודה `"set USERNAME"`. מה פקודה זו מראה לכם ששונה מפקודת `set` הרגילה? נסו גם את פקודת `"set PROCESSOR"`. נסו להציג ערך של משתנה סביבה שלא קיים בעזרת הפקודה `set`.

- נסו לשחק עם פקודת echo. פקודה זו מדפיסה בחזרה את הפרמטרים שהיא קיבלה. הריצו גם את הפקודה "echo %USERNAME%".
- כעת נבצע בדיקה ארוכה יותר, שתלמד אותנו יותר על איך משתני סביבה עובדים:
  - חשבו על שם מקורי למשתנה סביבה וודאו כי אינו קיים על המחשב.
  - בצעו את הפקודה הבאה "set YOUR\_CHOSEN\_NAME=Value". וודאו כי הוא אכן קיבל את הערך שציפיתם (החליפו את YOUR\_CHOSEN\_NAME ואת Value בשם ובערך שבחרתם).
  - מתוך שורת הפקודה, פתחו שורת פקודה חדשה (הריצו את הפקודה "start cmd". ודאו כי אכן מתוך שורת הפקודה נוצר תהליך חדש (בעזרת Process Explorer).
  - מתוך שורת הפקודה החדשה, בדקו את הערך של המשתנה שהגדרתם.
  - שנו את הערך של משתנה הסביבה שלכם (עדיין מתוך שורת הפקודה החדשה).
  - מתוך שורת הפקודה המקורית, בדקו את הערך של משתנה הסביבה שהגדרתם.
  - בדקו את הערך של המשתנה בשני החלונות בעזרת ה-process Explorer.
  - **שאלה:** מה ניתן ללמוד מכך על דרך הפעולה של משתני סביבה?

**תשובה:** ניתן ללמוד מכך כמה דברים. תחילה, ניתן לראות כי משתני סביבה "מורשים" (מלשון הורשה) מתהליך אבא לתהליך בן. בנוסף, ניתן ללמוד כי לכל תהליך יש עותק משלו למשתני הסביבה, וכי לאחר היצירה אין קשר בין משתני הסביבה של האבא למשתני הסביבה של הבן.

### לשונית ה-Strings

לשונית זו טובה למחקר מהיר של קבצים בלתי מוכרים. לשונית זו מציגה את כל המחרוזות הקיימות בקובץ של התהליך. הרבה פעמים, כבר מהמחרוזות ניתן לזהות דברים מעניינים למשל קבצים שהתוכנה צריכה, כל מיני הודעות של שגיאות, וכו'. לשם בדיקה, פתחו תוכנה כלשהי ובדקו כמה אתם יכולים ללמוד על התוכנה רק מלעבור על המחרוזות בקובץ. אזהרה את המחרוזות מזהים באופן היוריסטי. יכול להיות שיהיו מחרוזות שיתפספו ומחרוזות אחרות שהן "זבל" שבמקרה זוהה כמחרוזת.

## הצגת קבצים ו-DLL-ים במסך הראשי

The screenshot displays the Process Explorer interface. The top pane shows the loaded DLLs for the selected process (explorer.exe). The bottom pane shows the file system structure of the loaded DLLs.

| Name                                   | Description                                     | Company Name                 | Path                                                                |
|----------------------------------------|-------------------------------------------------|------------------------------|---------------------------------------------------------------------|
| ThgShell64.dll                         | TortoiseHg Shell Extension                      | TortoiseHg Project           | D:\Program Files\TortoiseHg\ThgShell64.dll                          |
| TortoiseOverlays.dll                   | TortoiseSVN overlay handler shim                | http://tortoisesvn.net       | C:\Program Files\Common Files\TortoiseOverlays\TortoiseOverlays.dll |
| libaprutil_tsvn.dll                    | Apache Portable Runtime Utility Library         | Apache Software Foundat...   | C:\Program Files\TortoiseSVN\bin\libaprutil_tsvn.dll                |
| libapr_tsvn.dll                        | Apache Portable Runtime Library                 | Apache Software Foundat...   | C:\Program Files\TortoiseSVN\bin\libapr_tsvn.dll                    |
| TortoiseSVN.dll                        | TortoiseSVN shell extension client              | http://tortoisesvn.net       | C:\Program Files\TortoiseSVN\bin\TortoiseSVN.dll                    |
| TortoiseStub.dll                       | TortoiseSVN shell extension client              | http://tortoisesvn.net       | C:\Program Files\TortoiseSVN\bin\TortoiseStub.dll                   |
| libsvn_tsvn.dll                        | Subversion library dll built for TortoiseSVN    | http://subversion.apache.... | C:\Program Files\TortoiseSVN\bin\libsvn_tsvn.dll                    |
| libsvn.dll                             | Subversion library dll built for TortoiseSVN    | http://subversion.apache.... | C:\Program Files\TortoiseSVN\bin\libsvn.dll                         |
| intl3_tsvn.dll                         | LGPLed libintl for Windows NT/2000/XP and Wi... | Free Software Foundation     | C:\Program Files\TortoiseSVN\bin\intl3_tsvn.dll                     |
| TortoiseGit.dll                        | TortoiseGit shell extension client              | http://tortoisegit.org/      | C:\Program Files\TortoiseGit\bin\TortoiseGit.dll                    |
| TortoiseGitStub.dll                    | TortoiseGit shell extension client              | http://tortoisegit.org/      | C:\Program Files\TortoiseGit\bin\TortoiseGitStub.dll                |
| gitdll.dll                             | libgit2 - the Git linkable library              | http://tortoisegit.org/      | C:\Program Files\TortoiseGit\bin\gitdll.dll                         |
| libgit2_tgit.dll                       | libgit2 - the Git linkable library              | http://tortoisegit.org/      | C:\Program Files\TortoiseGit\bin\libgit2_tgit.dll                   |
| crashhdl.dll                           | Crash handler library                           | Idol Software                | C:\Program Files\TortoiseGit\bin\crashhdl.dll                       |
| zlib1_tgit.dll                         | zlib data compression library                   | Idol Software                | C:\Program Files\TortoiseGit\bin\zlib1_tgit.dll                     |
| imageres.dll                           | Windows Image Resource                          | Microsoft Corporation        | C:\Windows\System32\imageres.dll                                    |
| secur32.dll                            | Security Support Provider Interface             | Microsoft Corporation        | C:\Windows\System32\secur32.dll                                     |
| sxs.dll                                | Fusion 2.5                                      | Microsoft Corporation        | C:\Windows\System32\sxs.dll                                         |
| profapi.dll                            | User Profile Basic API                          | Microsoft Corporation        | C:\Windows\System32\profapi.dll                                     |
| msasn1.dll                             | ASN.1 Runtime APIs                              | Microsoft Corporation        | C:\Windows\System32\msasn1.dll                                      |
| api-ms-win-downlevel-ole32-1-1-0.dll   | ApiSet Stub DLL                                 | Microsoft Corporation        | C:\Windows\System32\api-ms-win-downlevel-ole32-1-1-0.dll            |
| api-ms-win-downlevel-shlwapi-1-1-0.dll | ApiSet Stub DLL                                 | Microsoft Corporation        | C:\Windows\System32\api-ms-win-downlevel-shlwapi-1-1-0.dll          |
| wintrust.dll                           | Microsoft Trust Verification APIs               | Microsoft Corporation        | C:\Windows\System32\wintrust.dll                                    |
| crypt32.dll                            | Crypto API32                                    | Microsoft Corporation        | C:\Windows\System32\crypt32.dll                                     |

CPU Usage: 53.22% | Commit Charge: 35.01% | Processes: 83 | Physical Usage: 58.54%

| Type | Name                                                                                                                    |
|------|-------------------------------------------------------------------------------------------------------------------------|
| File | C:\Users\Omer\AppData\Local\Microsoft\Windows\Burn                                                                      |
| File | C:\Users\Omer\AppData\Local\Microsoft\Windows\Burn                                                                      |
| File | C:\Users\Omer\AppData\Local\Microsoft\Windows\Temporary Internet Files\counters.dat                                     |
| File | C:\Users\Omer\AppData\Local\Microsoft\Windows\WER\ReportArchive                                                         |
| File | C:\Users\Omer\AppData\Local\Temp\FXSAPI\DebugLogFile.txt                                                                |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned                                      |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned                                      |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Libraries                                                               |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Libraries                                                               |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Printer Shortcuts                                                       |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Printer Shortcuts                                                       |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Start Menu                                                              |
| File | C:\Users\Omer\AppData\Roaming\Microsoft\Windows\Start Menu                                                              |
| File | C:\Users\Omer\Desktop                                                                                                   |
| File | C:\Users\Omer\Desktop                                                                                                   |
| File | C:\Users\Public\Desktop                                                                                                 |
| File | C:\Users\Public\Desktop                                                                                                 |
| File | C:\Windows\Fonts\StaticCache.dat                                                                                        |
| File | C:\Windows\System32                                                                                                     |
| File | C:\Windows\System32\en-US\ActionCenter.dll.mui                                                                          |
| File | C:\Windows\System32\en-US\bthprops.cpl.mui                                                                              |
| File | C:\Windows\System32\en-US\KernelBase.dll.mui                                                                            |
| File | C:\Windows\System32\en-US\urlmon.dll.mui                                                                                |
| File | C:\Windows\winsxs\amd64_microsoft.windows.c...controls.resources_6595b64144ccf1df_6.0.7600.16385_en-us_106f9be843a9b4e3 |

CPU Usage: 58.03% | Commit Charge: 34.13% | Processes: 82 | Physical Usage: 57.16%

שתי יכולות מאוד שימושיות של Process Explorer הן להראות אילו משאבי מערכת מוחזקים על ידי תהליך ואילו מודולים טעונים על ידי התהליך. ניתן להראות את משאבי המערכת המוחזקים על ידי תהליך החלקו התחתון של חלון ה-process Explorer. ניתן לעבור בין תצוגה של מודולים (DLL) לתצוגה של משאבים ע"י View->Lower Pane View.

כרגע לא נמשיך לדבר עוד על מודולים נדבר עליהם בהרחבה בהמשך הקורס. לכן, נתמקד עכשיו במשאבי מערכת.

מסך זה מציג את כל ה-Handle-ים הפתוחים על ידי התהליך. Handle זהו אובייקט של Windows שבעזרתו ה-Kernel חושף לתהליכים משאבים בצורה אחידה (כך למשל, ניתן להציג את כל המידע במסך הזה בפשטות יחסית). נראה כי עבור כל משאב יש טיפוס ושם (ניתן להוסיף עוד פרמטרים, אך

הם אינם מעניינים אותנו כרגע). הטיפוס המעניין אותנו כרגע הוא File. טיפוס המייצג קובץ (ולמעשה עוד דברים כמו תיקיות ואפילו עוד).

**משימה 4 :** פתחו תהליך חדש של python, ומאחוריו החזיקו פתוח את Process Explorer כאשר אתם רואים את מסך ה-Handle-ים הפתוחים שלו ברקע.

- פתחו קובץ חדש ב-python לכתובה (לדוגמא `f = open('C:\\temp\\tester.bin', 'w')`).
- נסו דרך הממשק הגרפי של מערכת ההפעלה למחוק את הקובץ שפתחתם כרגע. הסבירו מדוע לדעתכם המחיקה נכשלה.
- ב-Process Explorer, זהו את ה-Handle הרלוונטי עבור הקובץ שפתחתם וסגרו אותו (בעזרת המקש הימני) **[אזהרה לסגור-Handle-ים אקראיים לתהליכים שאתם לא מכירים עלול להיות מסוכן מאוד - הדבר עלול לגרום בקלות לקריסת המחשב].**
- כעת, נסו שוב למחוק את הקובץ דרך ממשק מערכת ההפעלה. מדוע הפעם המחיקה הצליחה?

קרדיט

עומר ברק

תומר אלון