

בדיקות ביצועים במערכת ההפעלה

מערכת הפעלה אמינה נבחנת בביצועים שלה ובאופן ההתאוששות שלה מתקלות, יש חשיבות לנטר את ביצועי המערכת ולבצע אופטימיזציה במידת הצורך. נסקור כלים שיאפשרו לנו לבדוק את ביצועי המערכת בזמן אמת, וכמו כן סקירה של אירועים שעברו במערכת. נלמד להשתמש בכלים שיאפשרו לנו ליצור נקודת מוצא לביצועי המערכת שנוכל להשוות אליה בכל רגע נתון על מנת להחליט אם ביצועי המערכת נמוכים.

בעיות היכולות להשפיע על אמינות המערכת:

- מערכות קבצים שלא מאורגנות היטב
- תוכנות הצורכות משאבים רבים
- תוכנות רבות מידי העולות בשלב הפעלת המחשב
- דרייברים לא מתאימים
- וירוסים
- תוכנות שלא מותאמות למערכת ההפעלה

בעיות הקשורות לביצועי המערכת:

ביצועים נמדדים במהירות בה מערכת ההפעלה מסיימת משימה מוגדרת או הפעלת תוכנה, בעיות בביצועים יכולות להיגרם בכל פעם שמשאבי החומרה מנוצלים או נמצאים בחוסר.

ישנם ארבעה רכיבי חומרה שנרצה לנטר

- מעבד – ככל שהמעבד מהיר יותר או בעל יותר ליבות כך המחשב יוכל לבצע משימות הדורשות יותר משאבי חישוב
- דיסק קשיח – דיסקים מאחסנים מידע, ככל שהדיסק יהיה מהיר יותר כך שליפת המידע או כתיבתו אל הדיסק תבוצע ביעילות ומהירות יעלו ביצועי המחשב
- זיכרון – תוכנות טוענות את המידע מהדיסק אל הזיכרון, זיכרון גדול משמעו יותר תוכנות שיכולות לעבוד בזמנית
- רשת – כאשר רוב המידע המעובד מגיע מן הרשת נרצה ביצועי רשת מהירים ומתקדמים, עלינו לזכור שרוחב הפס מתחלק בין יתר העמדות המחוברות לאותה רשת.

כאשר אנו באים לבדוק ביצועי מחשב אנו יכולים למדוד מדדי ביצועים בזמן אמת, או בנק' זמן כלשהי

וכמו כן נרצה לעבור על אירועים שקרו בעבר על מנת להבין לעומק את המצב הנוכחי.

מע' ההפעלה מספקת מגוון רב של כלים מובנים על מנת לקבל תמונת מצב של המחשב ואנו נסקור אותם בפרק זה כמו כן נעבור על מס' כלים חיצוניים המסופקים לנו על ידי מייקרוסופט על מנת לקבל תמונה רחבה יותר.

מושגים הקשורים לבדיקות ביצועים :

ככל שנכיר את מע' ההפעלה ודרך הפעולה שלה נוכל לאתר חריגות ולגלות פעילות בלתי מורשית.

Processes and Threads and Jobs

למרות שתוכנות ותהליכים נראים על פניו זהים, הם שונים לגמרי.

תוכנה היא אוסף סטטי של הוראות לביצוע בעוד שתהליך הוא יחידה לוגית הכוללת בתוכה אוסף של משאבים הנדרשים להפעלת תוכנה. תוכנה אחת בשם **winword** יכולה ליצור 4 תהליכים שונים אם נערוך בו זמנית 4 מסמכים.

ברמה הבסיסית ביותר תהליך מכיל את המאפיינים הבאים :

-מזהה ייחודי הנקרא **process ID(PID)**

-לפחות **thread** (נים) אחד , לכל **thread** בתהליך יש גישה מלאה לכלל המשאבים שהתהליך מכיל, **thread** בעברית תהליכון מייצג רצף של פקודות שמבצעות משימה אחת בתהליך

-מרחב זיכרון וירטואלי פרטי (**private virtual address space**) – אוסף כתובות בזיכרון בהן התהליך יכול לאחסן נתונים וקוד

-אפליקציה פעילה שמגדירה את הקוד ההרצה והנתונים ומקושרת למרחב הזיכרון הוירטואלי של התהליך

-רשימה של כל ההפניות הפעילות למשאבי מערכת (**handles**) – היות והתהליך לא יכול לגשת ישירות למשאב מערכת או אובייקט של מע' הפעלה לדוגמא פתיחת קובץ , הוא עושה זאת דרך אובייקט שנקרא **handle** , כל תהליך מנהל טבלה של כל ה-**handles** שזמינים עבורו

- **access token** - מרכיב אבטחה המכיל מזהה של המשתמש הקבוצה הרשאות **UAC** וכו.

Process	Thread
מקבל משאבים (זיכרון וכו') ממערכת ההפעלה	יורש משאבים מה-Process
לא משתף משאבים עם Process אחרים	משתף משאבים עם Thread אחרים תחת אותו Process
אין לו קוד שרץ, חייב לפתוח Thread	מריץ קוד
יכול להכיל כמה Thread	חייב שיהיה לו Process אחד שייצור אותו

Jobs – ווינדוס מרחיבה את המודל של שימוש בתהליכים ומגדירה ג'וב (עבודה) , זהו אובייקט שמטרתו העיקרית היא לאפשר ניהול וביצוע שינויים לקבוצה של תהליכים כיחידה אחת. **JOB** מאפשר ניהול מאפיינים מסויימים של מס' תהליכים וכמו כן רישום מידע משותף עבורם.

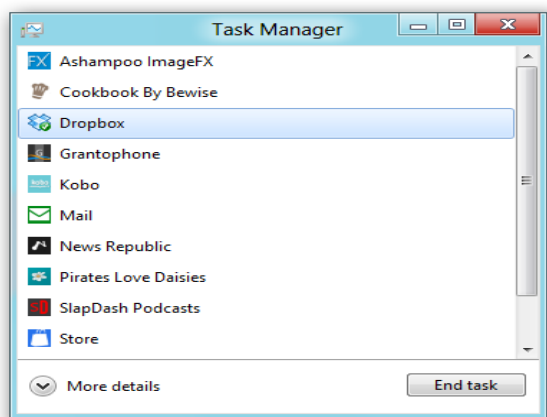
מה זה SERVICE ?

שירותי מע' הינם סוג מיוחד של תהליכים המופעלים אוט' ע"י מע' ההפעלה ומנוהלים על ידיה , כמו כן אין להם ממשק משתמש .

שירותים מע' פועלים כל הזמן ברקע לדוגמא שירות ההדפסה , שירות חיבור לרשת ועוד...

אם נרשום בתפריט RUN – services.msc נוכל לראות את שירותי המע' ולקבל מידע עליהם.

סקירת כלים מובנים במע' ההפעלה לבדיקות ביצועים :



Task Manager

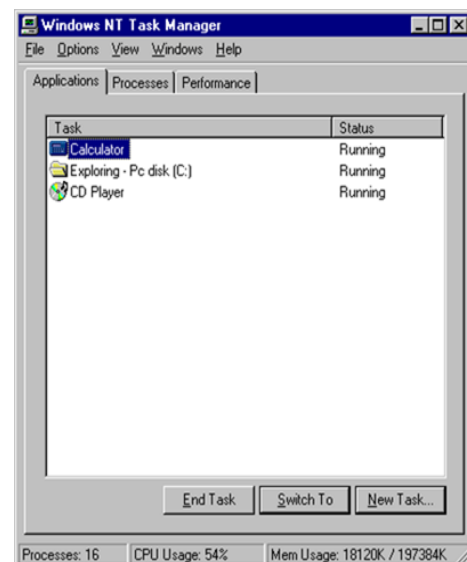
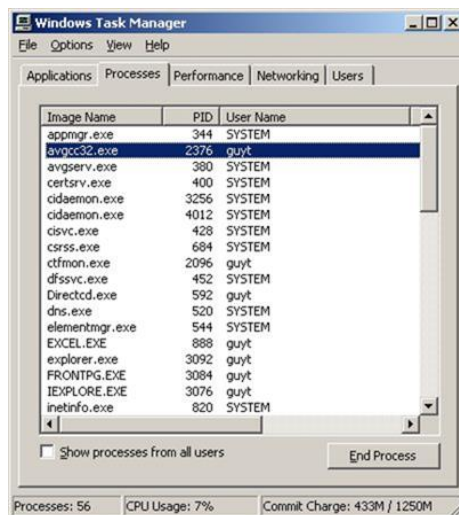
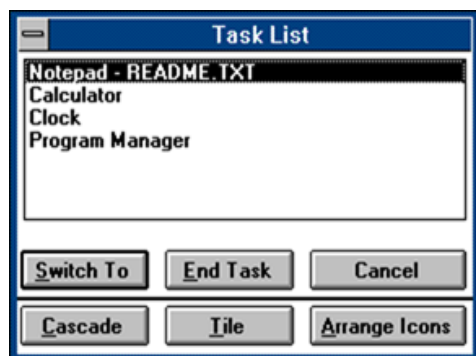
למראית עין יציג לנו רק את התוכנות הפועלות כרגע במחשב אך אם נלחץ על : **More details**

נגלה שיפור משמעותי ביחס לגרסה הקודמת של מע' ההפעלה .

בתצורתו המורחב של מנהל המשימות ניתן להבחין במידע הרב אותו יכול לקבל המשתמש.

כל תהליכים הפועלים כעת במערכת ההפעלה על פי חלוקה לאפליקציות , תהליכים ברקע או תהליכים בחלונות במידה ומדובר בשירותי מערכת ההפעלה .

ביחס לכל אחד מאלו יכול המשתמש לקבל פירוט נרחב על השימוש שעושה כל אפליקציה, שירות ברקע או שירות של מערכת בכוח המעבד, הזיכרון, הכונן הקשיח או רוחב הפס של חיבור הרשת.

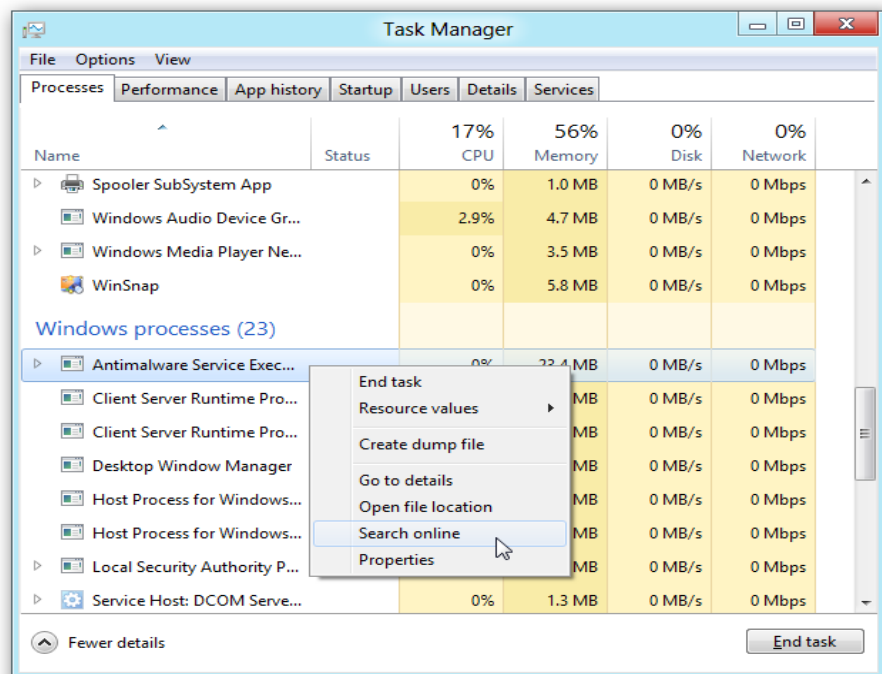


בתמונה למעלה סקירה של התפתחות ה-TASK MANAGER במע' ההפעלה השונות (מ- Win 3.00 ועד Win XP)

לשונית Process :

תספק לנו מידע על המשאבים הנצרכים על ידי התוכנות יחד עם התהליכים הרצים ברקע ותהליכים של מערכת ההפעלה.

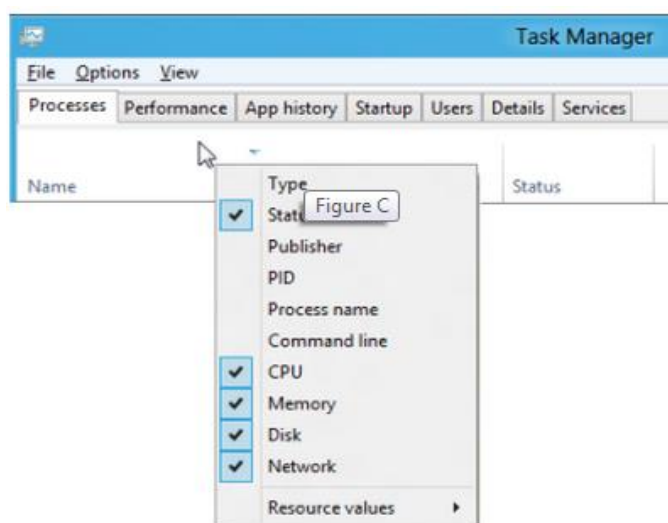
לחיצה על המשולש הקטן ליד כל תהליך תציג את כלל החלונות של התהליך במערכת ההפעלה.



לחיצה על כפתור ימני תאפשר לנו לבצע מס' פעולות לגבי כל תוכנה או תהליך

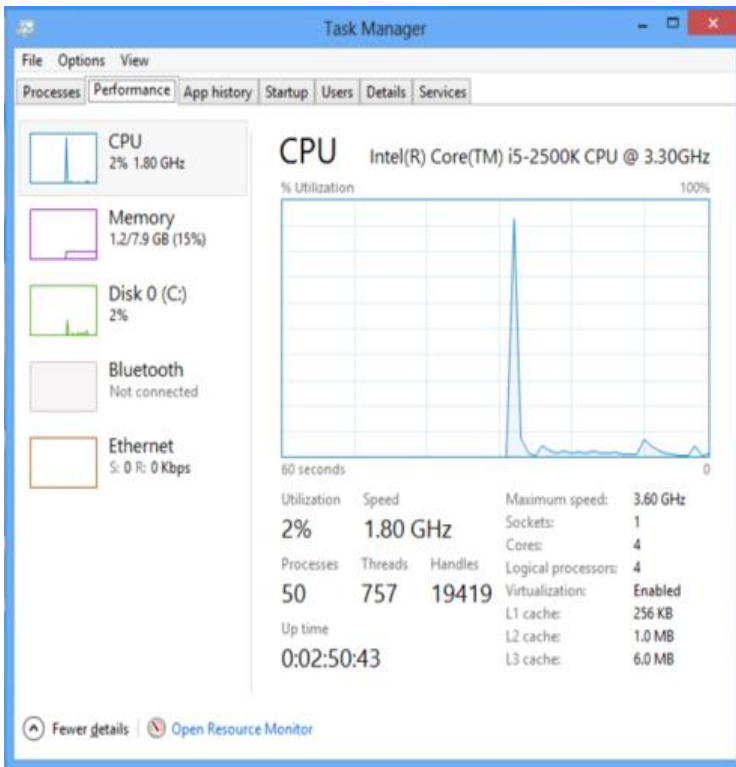
- **End Task** - סגירת התהליך
- **Resource values** - שינוי המדדים המוצגים למשתמש ביחס לביצוע התוכנה.
- **Create dump file** - יצירת קובץ Dump לתוכנה ספציפית ומעקב אחר קריסתה.
- **Go to Details** - יציג מסך פרטים מפורט (בדומה למסך המידע שהיה בגרסה הקודמת)
- **Open file location** - פתיחת התיקייה בה נמצא קובץ ההפעלה של התהליך.
- **Search online** - חיפוש שם התהליך במנוע החיפוש המוגדר כברירת מחדל במידה ואינם מזהים תהליך
- **Properties** - הצגת המאפיינים של קובץ ההפעלה של התהליך

לחיצה על הכפתור הימני בעכבר באזור העליון תאפשר לנו להציג משתנים נוספים שאותם נוכל לנטר באמצעות כלי זה.



לשונית Performance :

בלשונית זו תציג המערכת את ביצועי המערכת ואחוז השימוש הכולל במעבד, זיכרון, כונן קשיח וחיבור הרשת. המערכת תציג סקירה מפורטת של השימוש בהתקן בעבור כל התקן ברגע בו נבחר ברשימה ותמחיש זאת באמצעות גרף מתאים.



לשונית App history

זוהי אפשרות חדשה שמוצגת בגרסה הזו , לשונית זו תציג עבורכם סקירה של כל האפליקציות והתוכנות בהן אתם עושים שימוש ותסקור באופן מרוכז כמה זמן פעלה האפליקציה ומה היו דרישותיה מרכיבי החומרה השונים. במידה ותמצאו לאפס את הרשימה כל שעליהם לעשות הוא ללחוץ על כפתור מחק היסטוריית שימוש בחלק העליון

Resource usage since 1/4/2013 for current user account.
[Delete usage history](#)

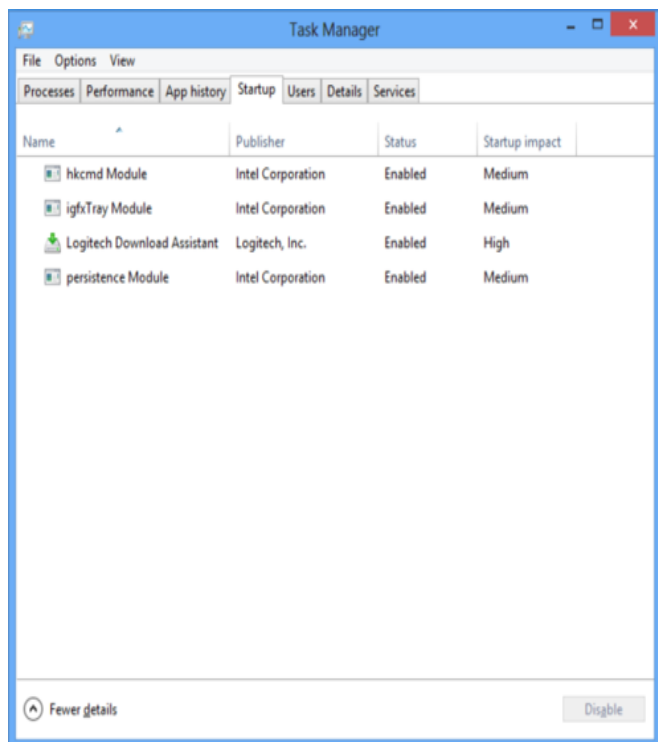
Name	CPU time	Network	Metered network	Tile updates
Bing	0:00:00	0.1 MB	0 MB	0.1 MB
Camera	0:00:00	0 MB	0 MB	0 MB
Finance	0:00:00	0.1 MB	0 MB	0.1 MB
Games	0:00:00	0 MB	0 MB	0 MB
Internet Explorer	0:00:00	0 MB	0 MB	0 MB
Mail, Calendar, People, a...	0:00:00	0 MB	0 MB	0 MB
Maps	0:00:00	0 MB	0 MB	0 MB
Music	0:00:00	0 MB	0 MB	0 MB
News	0:00:00	0.1 MB	0 MB	0.1 MB
Photos	0:00:00	0 MB	0 MB	0 MB
Reader	0:00:00	0 MB	0 MB	0 MB
SkyDrive	0:00:00	0 MB	0 MB	0 MB
Sports	0:00:00	0.1 MB	0 MB	0.1 MB

[Fewer details](#)

לשונית Startup

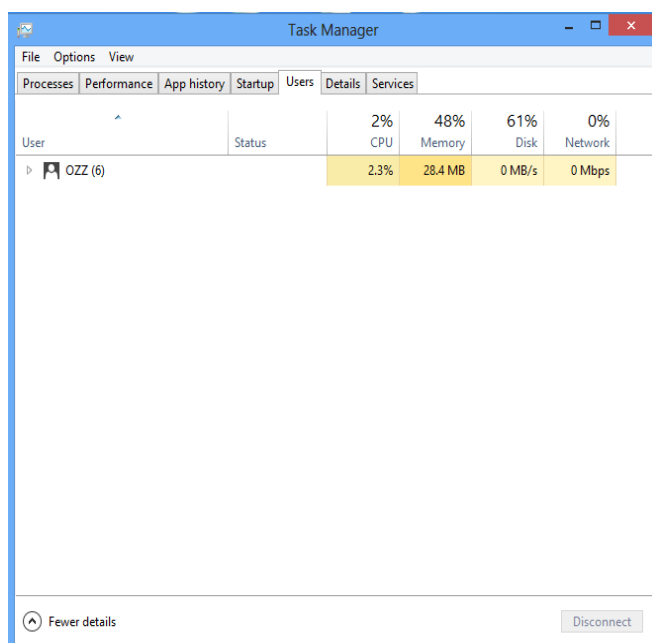
לשונית זו תציג לנו את כל התוכניות שעולות עם הפעלת מערכת ההפעלה

בלשונית אתחול תוכלו לנהל בקלות אילו תוכנות יעלו עם מערכת ההפעלה שלכם. כל שעליכם לעשות כדי לבטל את עליית התוכנות כל שעליכם לעשות הוא ללחוץ כפתור הפוך ללא זמין או הפוך לזמין על פי רצונכם.

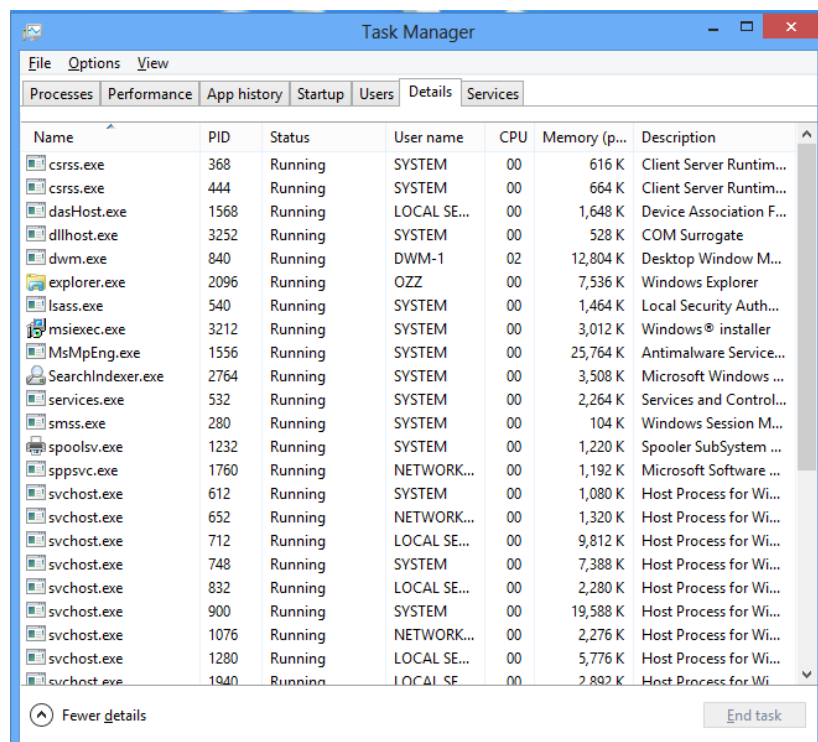


לשונית Users

בלשונית משתמש נוכל לבחון כל משתמש באופן נפרד. המערכת תציג לפנינו את המשתמשים השונים במערכת ואת אחוז השימוש שלכם ביכולות החומרה של המערכת. במידה ונהיה מעוניינים להציג פירוט של התוכנות השונות הפועלות באותו המשתמש עליכם ללחוץ על סמל החץ הקטן המופיע ליד שם המשתמש.

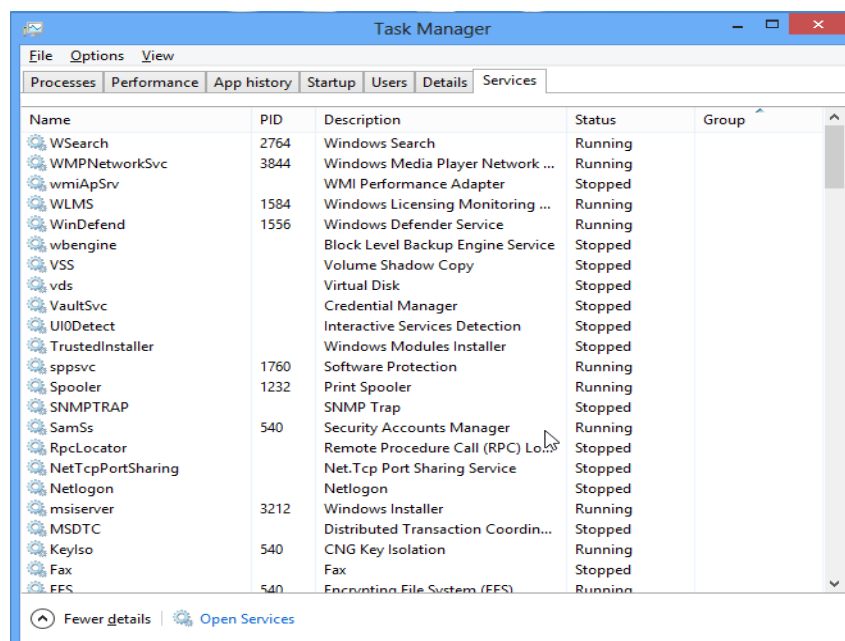


לשונית Details



בלשונית פרטים נוכל לראות תצוגה מעט מסורבלת יותר של כל התהליכים הפועלים כעת במערכת ההפעלה. תצוגה זו זהה כמעט לחלוטין לתצוגה במנהל המשימות הקודם. גם כאן תוכלו לחצות מקש ימני על כל אחד מהתהליכים ותפגשו באפשרויות הבסיסיות. אך, בתפריט זה תוכלו לפגוש גם בכמה אפשרויות מתקדמות יותר

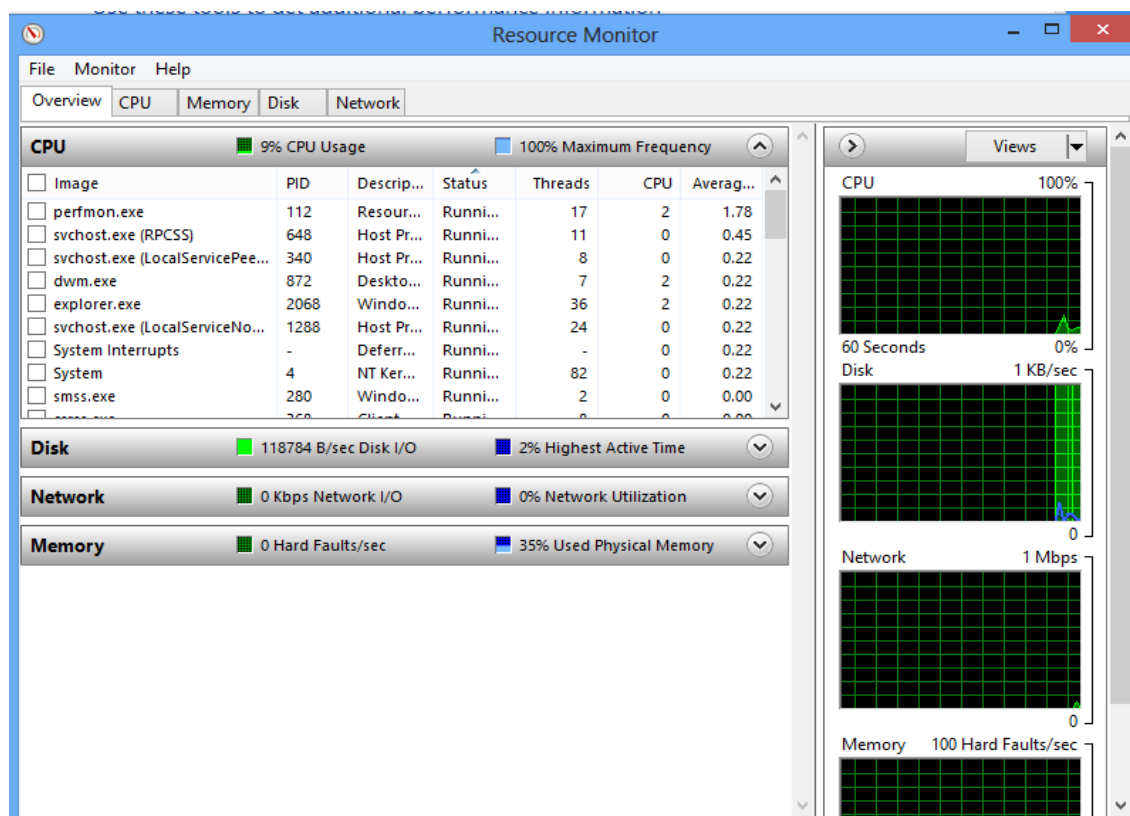
לשונית Services



לשונית שירותים היא הלשונית האחרונה המציגה למעשה את השירותים השונים של מערכת ההפעלה בדומה לחלון שירותי המערכת המוכר לנו ממערכות קודמות. בלחיצה של מקש ימני על אחד מהשירותים ויאפשר לכם להפעיל או להפסיק את השירות. בנוסף במידה ואינכם מכירים שירות כלשהו תוכלו לבצע חיפוש מקוון אודותיו.

חידוש נוסף הוא האפשרות לבצע **RESTART** ל-
Service

במידה ואתם מעוניינים להגיע אל חלון השירותים הישן תוכלו לחצות על כפתור פתח שירותים המופיע בחלק התחתון

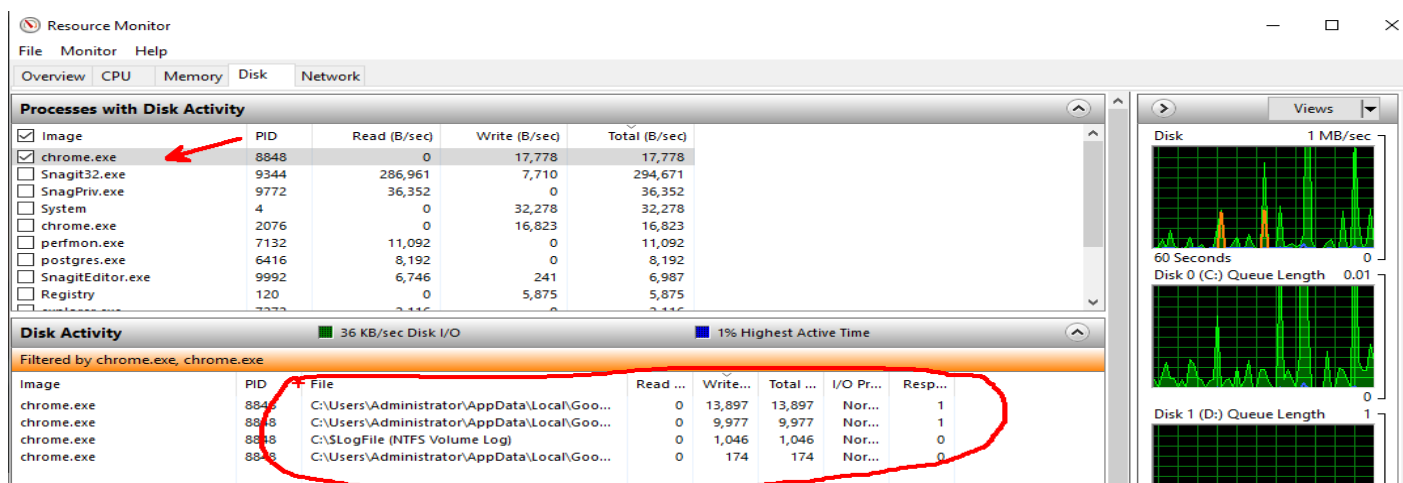


ניתן להפעיל משורת ה- `run` על ידי : `perfmon /res`

כלי זה יציג לנו בזמן אמת ניצול משאבי המערכת (מעבד, זיכרון, דיסק ורשת).

היתרון של כלי זה הוא בפירוט התוכנות והתהליכים המשתמשים במשאבים, מה שיאפשר לנו להבין בדיוק אילו תוכנות או שירותי מערכת גוזלים משאבים ונוכל לאתר תקלות המאטות את המחשב בזמן אמת.

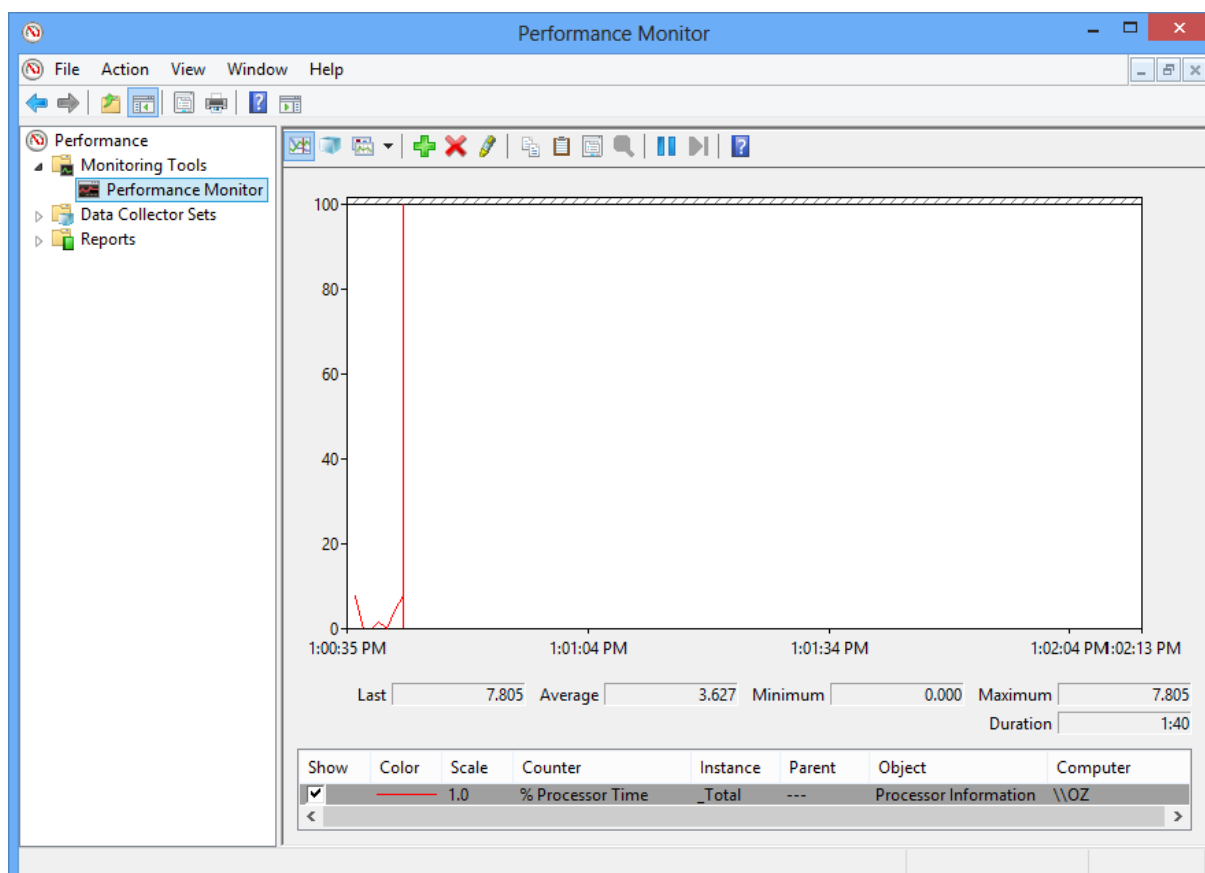
כמו כן נוכל לסמן אפליקציה היא תופיע ראשונה ברשימה ובך נוכל לבצע עליה מעקב לגבי כלל המדדים.



בתמונה למעלה אנו רואים את התהליך של כרום מבחינת ביצועי הדיסק ונוכל אף לראות את הקבצים אליהם הכרום כותב

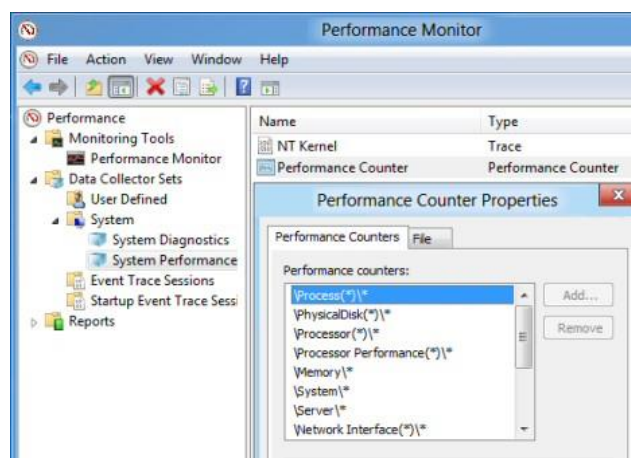
Performance Monitor

תפקידו של ה- **Performance monitor** הוא לספק מידע לגבי מצב מערכת העדכני, הוא מחולק לשלושה מרכיבים :
Monitoring Tool – נותן תצוגה גרפית לגבי מצב המערכת, ניתן להוסיף מדדי בדיקה לגבי כל רכיב ומאפיין במערכת.



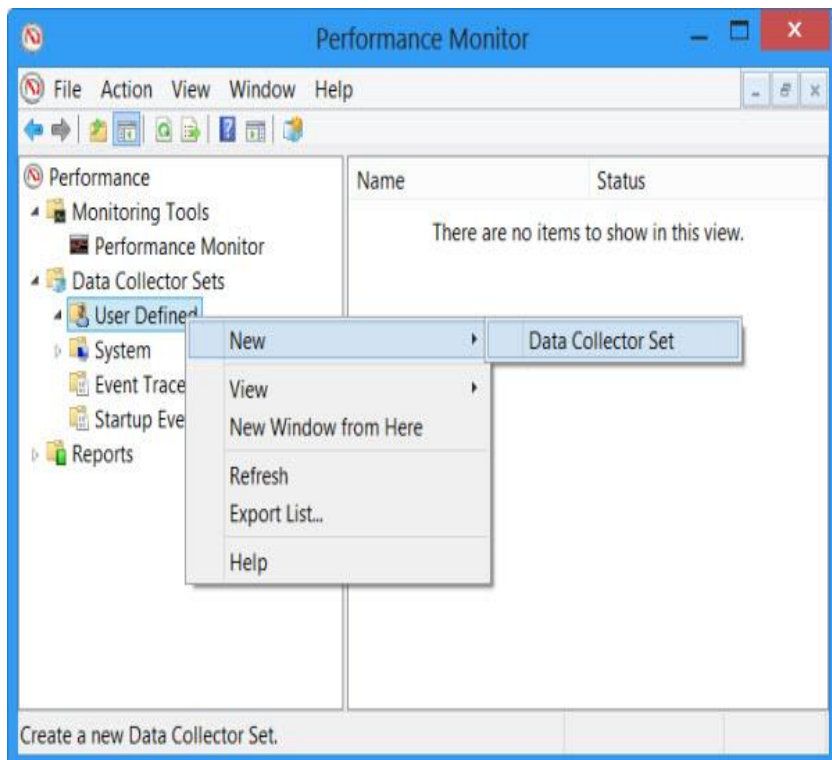
תוכל לבחור אילו מדדים לבדוק בזמן אמת מתוך רשימה של עשרות מדדי בדיקה אפשריים
ניתן להריץ כלי זה ישירות דרך תפריט **run** על ידי הקלדה של:

perfmon.exe



Data Collector sets

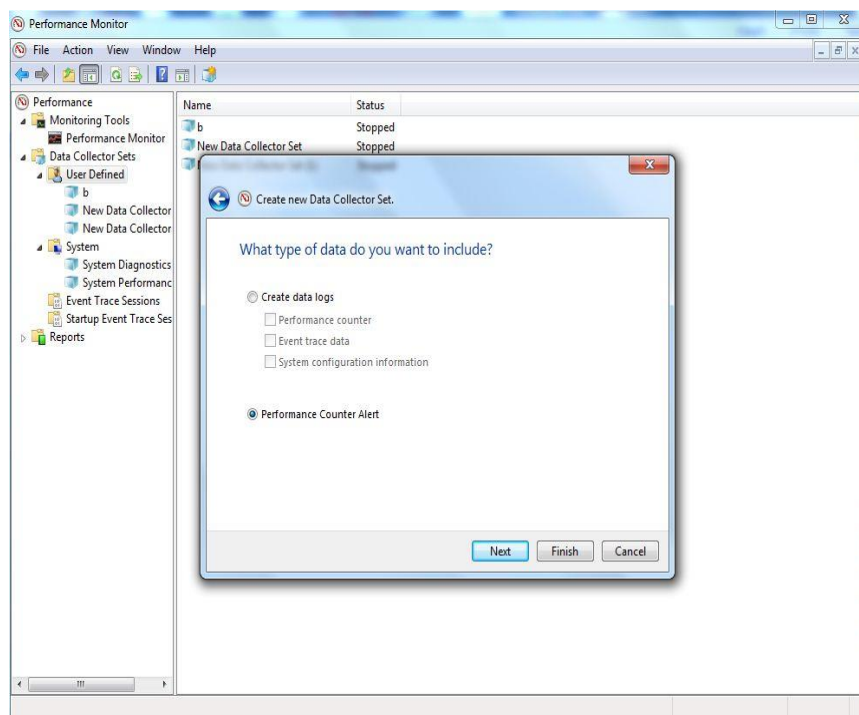
משמש לאסוף מידע מוגדר על ידי המשתמש. ניתן לשמור את המידע כקבצים ולבדוק את התוצאות של המידע שנאסף. ישנה אפשרות להריץ בזמן שנקבע מראש. ישנם **Templates** מוכנים מראש על מנת לאסוף מידע רלבנטי לתקינות המערכת. הקבצים נשמרים בתיקיית **C:\Perflogs** או ניתן לראות דוחות ישירות לאחר סיום איסוף המידע בעזרת **Reports**.



בעזרת ה- **Data Collector Sets** ניתן ליצור **ALERTS**, כלומר להגדיר למערכת שתודיע כאשר נתון מסוים במערכת עובר את הסף אשר הגדרתם עבורו. יש לבחור את רמת הסף שמעליה או מתחתיה המערכת תיתן אזהרה. ההודעה על החריגה תתרחש בכמה דרכים:

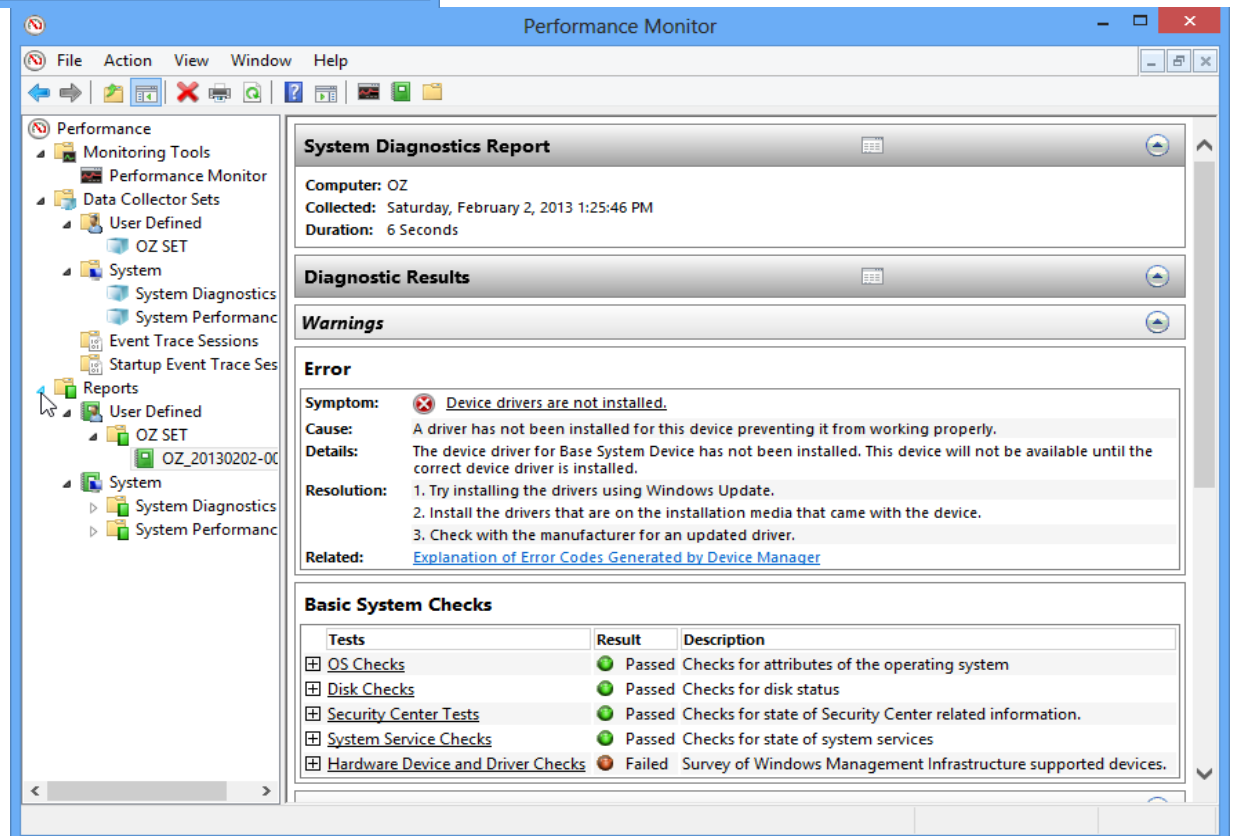
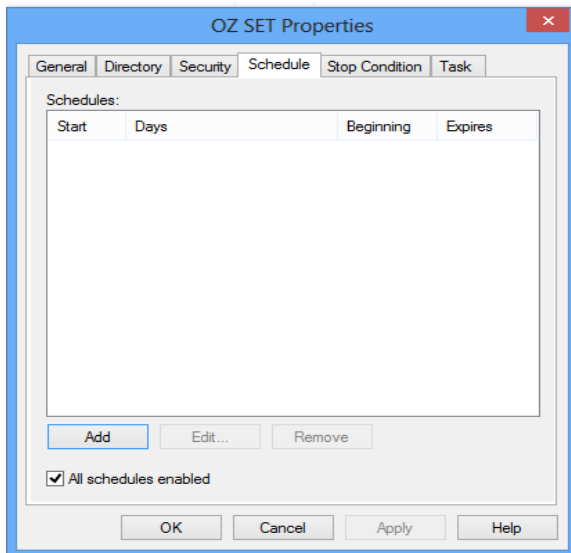
א. תופיע כ- **Event** ב- **Event Viewer** תחת **Application**.

ב. הרצת פקודה על פי בחירת המשתמש.



נוכל לתזמן את זמן פעילות איסוף הנתונים שהגדרנו :

את התוצאות של האיסוף נוכל למצוא ב- Reports



שם המדד	שימוש
LogicalDisk\% Free Space	מדד זה בודק את אחוז המקום הפנוי בדיסק, אם המדד יורד אל מתחת ל-15%, ישנו סיכון שמע' ההפעלה לא תוכל לשמור קבצים קריטיים ותהיה ירידה משמעותית בביצועים – הפתרון להוסיף דיסק או להגדיל את נפח הדיסק הקיים במידת האפשר.
PhysicalDisk\% Idle Time	המדד בודק את הזמן שבו הדיסק היה במצב אידיאלי כלומר ללא עבודה, אם המדד יורד מ-20%, הדיסק נמצא בבילאי מתקדם, נרצה לבדוק את הסיבה לכך וייתכן שנרצה לשקול החלפת דיסק.
PhysicalDisk\Avg. Disk Sec/Read	המדד מודד את הזמן הממוצע בשניות לקריאת מידע מהדיסק אם זמן זה עולה על 25ms הדבר מעיד על איטיות בזמן שליפת מידע מהדיסק
PhysicalDisk\Avg. Disk Sec/Write	כמו המדד מעליו הפעם מודד בדיקת ביצועי כתיבה
PhysicalDisk\Avg. Disk Queue Length	מדד זה בודק כמה פעולות קריאה/כתיבה (I/O) מחכות לביצוע, אם המספר גדול משמעותית נרצה לבדוק את מדדי הקריאה והכתיבה על מנת להחליט מהיכן הבעיה
Memory\Cache Bytes	מונה זה מציין את כמות הזיכרון המטמון בה מערכת הקבצים משתמשת. אם ערך זה גדול מ-300 מגה-בייט (MB) ייתכן צוואר בקבוק.
Memory\% Committed Bytes in Use	ערך זה בודק את אחוז השימוש בזיכרון הוירטואלי, אם המספר גדול מ-80% הדבר מעיד על מחסור בזיכרון RAM
Memory\Available Mbytes	המדד מעיד על כמות הזיכרון הפיזי הפנוי, אם מספר זה קטן מ-5% מכמות הזיכרון הפיזי המותקן המשמעות מחסור בזיכרון פיזי ועומס על הזיכרון הוירטואלי
Memory\Free System Page Table Entries	המדד מעיד על כמות הטבלאות בשימוש הזיכרון אם המספר קטן מ-5000 ייתכן דליפת זיכרון
Memory\Pool Non-Paged Bytes	מדד זה מודד את השימוש בזיכרון עבור אפליקציות שחייבות להשתמש בזיכרון פיזי לאורך זמן הפעילות שלהם, אם ערך זה גדול מ-175 מגה בייט תיתכן דליפת זיכרון
Memory\Pool Paged Bytes	המדד בודק את האובייקטים שכותבים לזיכרון הוירטואלי בזמן העבודה, אם הערך גדול מ-250 מגה בייט תיתכן דליפת זיכרון
Memory\Pages per Second	המדד בודק את הקצב בו הדפים נכתבים או נקראים מהדיסק אל הזיכרון, ערך גדול מ-1000 יכול להעיד על דליפת זיכרון
Processor\% Processor Time	המדד מודד את כמות הזמן באחוזים בו המעבד מבצע חישובים, ערך גדול מ-85 מעיד על עומס על המעבד ויש צורך להגדיל משאבי עיבוד
Processor\% User Time	ערך זה מודד את הביצועי המעבד עבור אפליקציות שהפעיל המשתמש, ערך גבוה מעיד על פעילות מעבד גבוהה ושימוש רב באפליקציות
Processor\% Interrupt Time	המדד מודד את כמות הפעמים בהם המעבד הופרע על ידי בקשות חומרה, ערך מעל 15% יכול להעיד על תקלות בחומרה
System\Processor Queue Length	המדד בודק את כמות הנימים שממתינים בתור למעבד, למעבד לא תמיד יש את המשאבים לטפל בכל הנימים, ערך גבוה לזמן ממושך יעיד על עומס למעבד
Network Interface\Bytes Total/Sec	המדד מודד את הקצב בו הנתונים נשלחים ומתקבלים על ידי כל כרטיס רשת, 70% ומעלה מעיד על עומס ברשת
Network Interface\Output Queue Length	המדד מודד את האורך של הפאקטות הממתינות למשלוח, מעל 2 מעיד על עומס
Process\Handle Count	המדד בודק את כמות ה-HANDLES שכל תהליך עושה בהם שימוש, מעל 10000 יעיד על תקלה
Process\Thread Count	מודד את כמות הנימים הפעילים לתהליך, אם יש פער של 500 בין המינימום למקסימום שנמדדו ייתכן שיש תקלה
Process\Private Bytes	מודד את כמות הזיכרון השמורה לכל תהליך אם הפער בין המקסימום למינימום הוא מעל 250 תיתכן דליפת זיכרון

יצירת בסיס השוואה למדדי ביצועים (BASELINE)

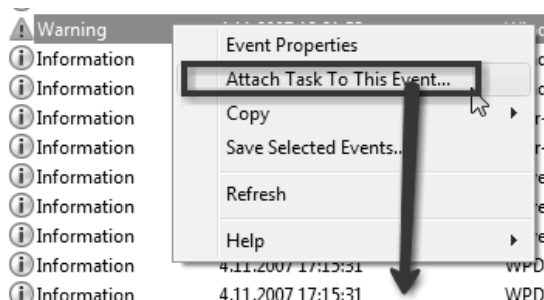
על ידי ניטור ביצועים והשוואתם לנק' כלשהי בעבר נוכל לבדוק אם חל שיפור או הידרדרות במצבו של המחשב
ניטור ביצועים בנק' זמן ייתן לנו מידע רק על נק' הזמן הנמדדת אבל ללא בסיס להשוואה לא נוכל לקבל את כל
התמונה .

כאשר ישנה תקלה נוכל להשוות את מדדי הביצועים אל הנק' בעבר ולנסות לזהות את מוקד הבעיה.
ע"י שימוש ביכולת איסוף והתזמון של **PERFMON** נוכל ליצור מדדי איסוף ולתזמן אותם לזמנים שונים ולבצע השוואה
בקלות באמצעות הדוחות שנקבל.
לכל מחשב נצור נק' השוואה משלו היות ולכל מחשב ישנה תצורה שונה ואפליקציות שונות .

לסיכום : כלי זה יכול לתת לנו נתונים בזמן אמת על ביצועי המחשב באמצעות מדידה של עשרות נתונים שונים , כלי
זה רב עוצמה זה מאפשר לנו לנטר כמעט כל פעילות במחשב ולתעד אותה באמצעות דו"חות על מנת ליצור בסיס
להשוואה עתידית.

כמו כן יש באפשרותנו לתזמן בדיקה ולבחור את הפרמטרים ואת הזמן שהבדיקה תבוצע וכמו כן להגדיר פעולות
שהמחשב יבצע בהתאם לתוצאות המתקבלות .

Event Viewer



מציג האירועים החדש כולל ממשק חדש ומפורט יותר. חידוש מרכזי מאפשר לשייך משימה שתבצע אוטומטית במקרה שיחול אירוע מסוים. משימה יכולה להיות הרצת תוכנית מסוימת או אפילו משלוח הודעת דוא"ל לנמען כלשהו (למשל ל- Administrator)

ההודעות נשמרות בשלושה סוגי log files: System, Application או Security.

להפעלת Event Viewer: Start ← Administrative Tools ← Event Viewer ← Windows logs

סוגי קבצי Log:

System (מערכת) עוקב אחרי תקלות/הודעות של מערכת ההפעלה בנושאים כמו חומרה או services.

Application (יישום) עוקב אחרי תקלות/הודעות של התוכנות המותקנות במחשב.

Security (אבטחה) עוקב אחרי פעולות חוקיות/לא חוקיות שביצעו משתמשים. כברירת

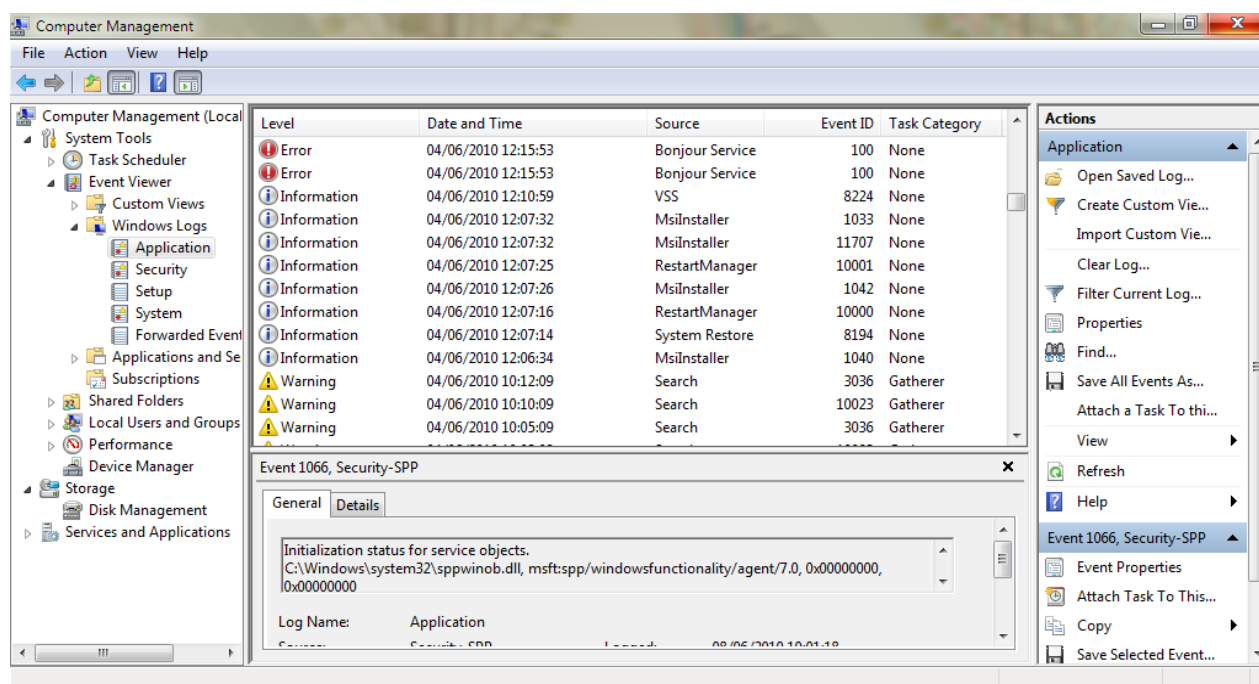
מחדל קובץ Log זה אינו פעיל, יש צורך להפעיל אופציית "מעקב" במידה ונרצה לראות הודעות.

ה-Event Viewer מציג הודעות מכמה סוגים:

Information (מידע) דיווח פשוט על אירוע שהתבצע.

Warning (אזהרה) המערכת גילתה משהו לא תקין, ומציעה לבדוק את הבעיה.

Error (שגיאה) המערכת זיהתה תקלה, ומציעה הסבר מרבי מה כדאי לבצע.



אתגר : האם תוכלו באמצעות כלי זה לבדוק כמה זמן לקח למחשב לעלות וכמה זמן לקח לו להתכבות?

הפעלה ע"י : **Maintenance, View reliability history** --> **Action Center** --> **Control Panel** או דרך החיפוש נרשום בקיצור RELI

חלון צג המהימנות המוצג לפניכם מחולק לכמה חלקים פשוטים :

מדד היציבות – צג המהימנות מציג את רמת היציבות של המערכת במדד הנע בין 1 ל-10. מדד זה נקבע לאור האירועים שהתרחשו במערכת באותו היום או השבוע. בחלק זה ניתן לבחור בין תצוגת ימים לתצוגת שבועות .

סימון כשלים – צג המהימנות מציג אילו כשלים התרחשו ביחס לכל יום ספציפי בחלוקה לכשלים של תוכנות שונות, כשלים של מערכת ההפעלה, כשלים אחרים כדוגמת כשל חומרתי , אזהרות על אירועים שונים או מידע על פעולה מסויימת שבוצע

פרטי האירוע – בחלק התחתון יוצג המידע על פי היום

הנבחר. בחלק זה נוכל לראות את פרטי האירוע וללחוץ על מנת לקבל מידע נוסף.

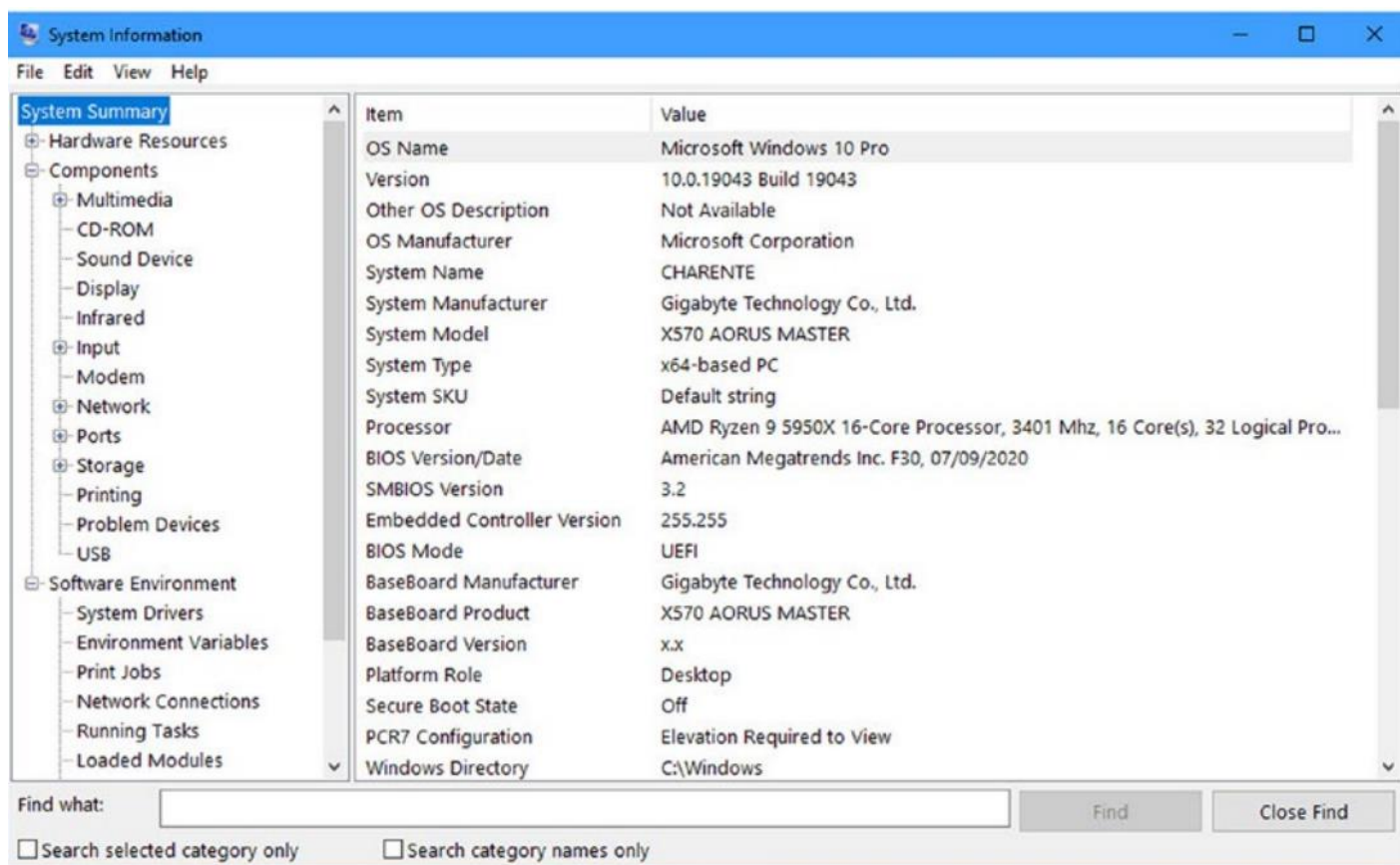
אפשרויות נוספות – תחת האפשרות להצגת פרטי האירוע יוצגו לפנינו אפשרויות נוספות כמו שמירת היסטוריית דוחות התקלות במערכת והאפשרות לחיפוש פיתרון לכל אחד מהבעיות .



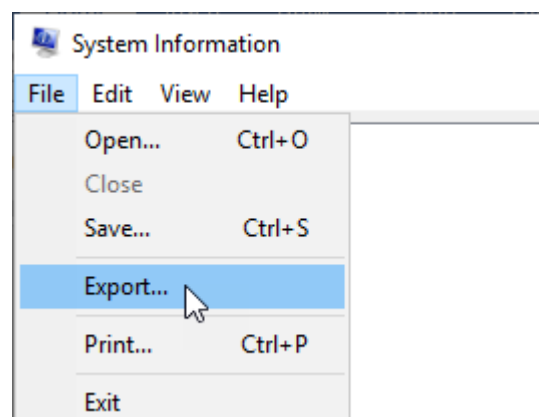
System Information

אם נרצה לקבל סקירה מקיפה על החומרה המותקנת במחשב, סוג הלוח היצרן וכו'. נוכל להשתמש בכלי הזה ונקבל את כל המידע שנצטרך על המחשב שלנו. את הכלי נוכל למצוא דרך החיפוש או לוח הבקרה או להריץ בתפריט RUN

Msinfo32.exe

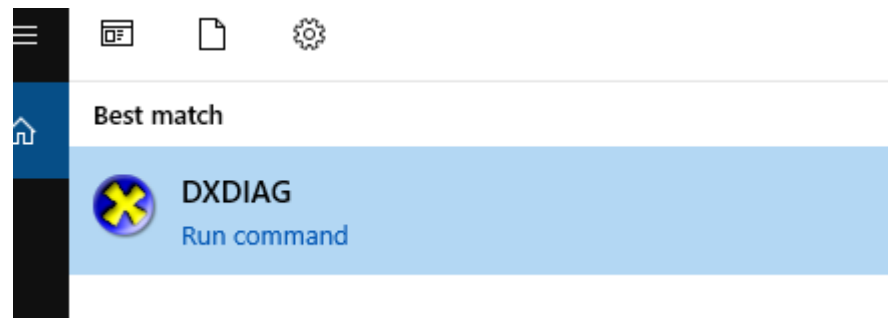


ניתן להשתמש בחיפוש על מנת לייעל את המהירות בה נגיע למידע הרצוי. נוכל אף לשמור את המידע לקובץ טקסט באמצעות היכולת לייצא בתפריט FILE > EXPORT

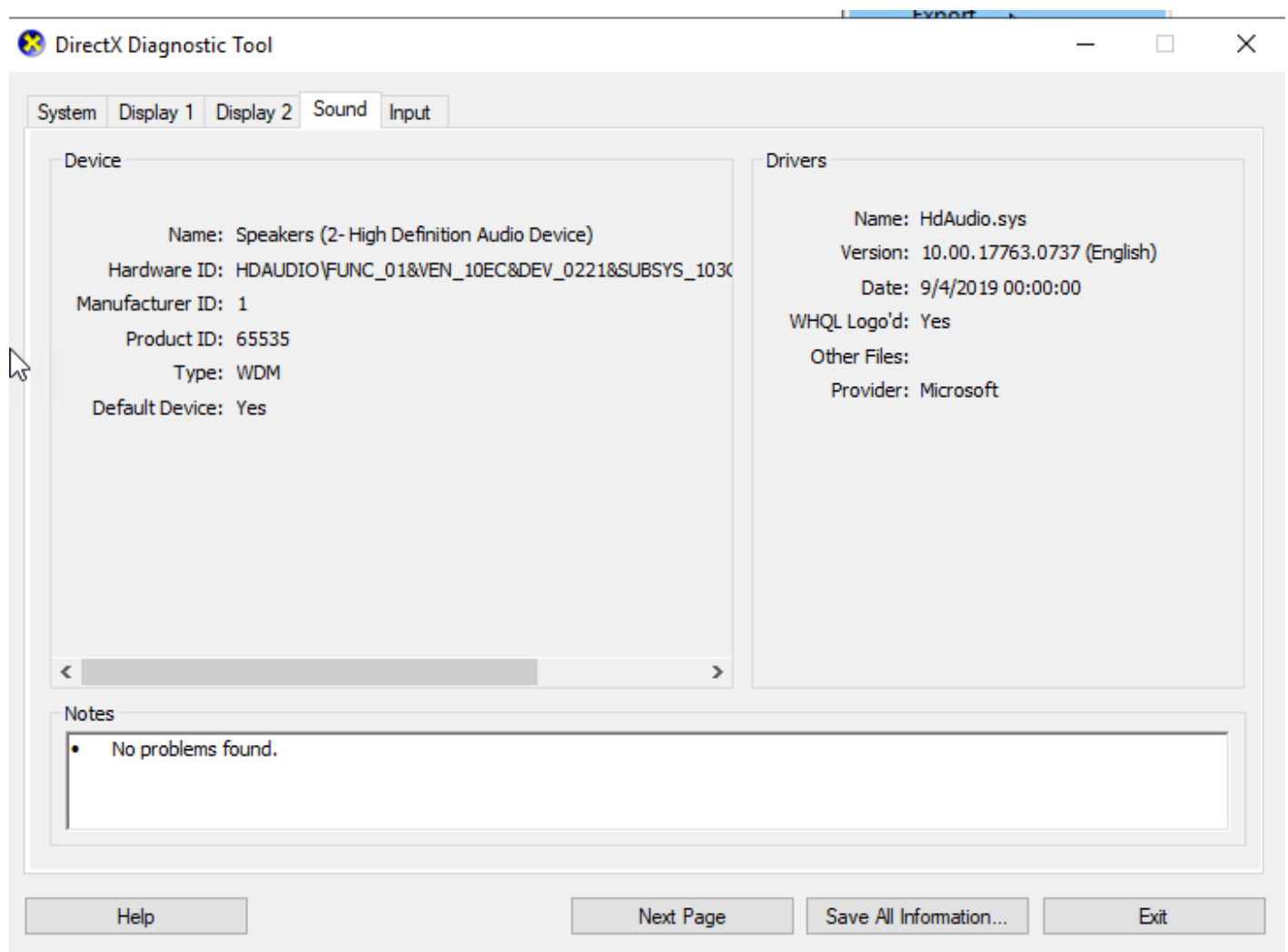


נוכל גם להתחבר למחשב מרוחק ברשת שלנו במידה והאפשרות הזו מאופשרת בעמדה המרוחקת.

אם אנו חושדים שיש לנו בעיה בוידאו או בכרטיס הקול נוכל להשתמש בכלי הדיאגנוסטיקה של DirectX, נבחר להריץ בתפריט RUN או בחיפוש



נקבל מידע מפורט על התקני הגרפיקה והקול וכמו כן סקירה לתקלות אם יש, את המידע ניתן לייצא ולשמור כקובץ טקסט.



מערכת הרישום של ווינדוס (REGISTRY)

הרישום הוא מסד נתונים גדול שבתוכו רשומות הגדרות מערכת ההפעלה, התוכנות, החומרה והמשתמשים. גדלו יכול לעשרות אלפי ערכים. בעזרת שינוי הגדרות הרגיסטרי בצורה נכונה ניתן לפתור תקלות לבצע התאמה אישית של מערכת ההפעלה והאפליקציות

השונות וכן לחשוף מאפיינים נסתרים במערכת ההפעלה.

הרגיסטרי מכיל מידע על כל פרט במערכת ההפעלה והתוכנות המותקנות בה סל המיחזור ועד גירסת הווינדוס המותקנת.

למרות הפוטנציאל הגדול לגרימת נזק למערכת ההפעלה הרגיסטרי נחשב לחסין יחסית ולא קיימים הרבה ערכים שיגרמו לקריסת המחשב אם נשנה אותם בצורה לא נכונה. בכל אופן חובה לגבות את הרגיסטרי לפני עריכת שינויים בו.

מידע ברגיסטרי נשמר במקטעים הנקראים 'ערכים' . values – 'לכל ערך יש שם והוא יכול להכיל מספר סוגי מידע . הערכים מאורגנים בתוך' מפתחות keys – 'הנראים כתיקיות והם מהווים את בסיס ההיררכיה של הרגיסטרי.

כל תכנה שמותקנת במחשב, רושמת את עצמה לתוך הרישום באופן הבא:

כאשר תוכנה מותקנת במחשב מתבצעים מספר תהליכים:

1. נוצרות תיקיות עבור התוכנה וקבצים מועתקים

2. נרשמים פרטים ברישום.

3. נוצרים קיצורי דרך.

בהתאם, כאשר תוכנה מוסרת מהמחשב באופן מסודר:

1. נמחקים קבצים ותיקיות של התוכנה.

2. נמחקים פרטי התוכנה מהרישום.

3. נמחקים קיצורי דרך.

לכן, הסרה של תוכנה צריכה להתבצע תמיד דרך add/remove בלוח הבקרה או על-ידי קובץ uninstall של התכנה. במקרים בעייתיים ניתן להשתמש בתוכנת צד-שלישי.

כיצד מתעדכן הרישום?

במחשב קיימים גיבויים לרישום על מנת לשחזרם במקרה של תקלה. קבצי הגיבוי של הרישום מתעדכנים אוטומטית בכל כיבוי מסודר של המחשב ובכל הדלקה מוצלחת של המחשב.

בעת הדלקת המחשב נטענים קבצי הרישום האחרונים שאיתם עבדה המערכת, הם נבדקים ולאחר שנמצאו תקינים הם מסומנים בהתאם.

היכן הרישום נשמר?

הרישום נשמר בקובץ **System** שבתיקיית `x:\windows\system32\config` (כאשר x הוא הכונן בו מותקנת Windows).

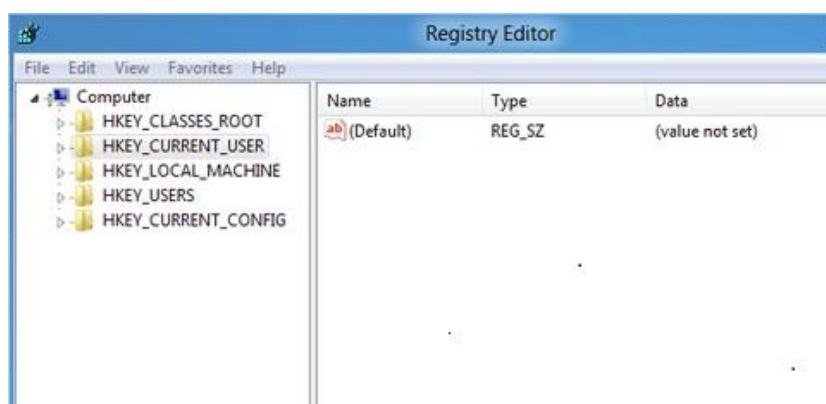
גיבוי של העותק הראשון של הרישום נשמר ב- `C:\Windows\System32\config\RegBack` במקרה שקובץ הרישום נפגם, ישנה אפשרות לחזור לעותק הראשון, אשר אינו מכיל את כל

עורך הרישום

ההגדרות שברישום הן למעשה הפניות קבצים הניתנות לעריכה במקרה הצורך, אך לא ניתן לערוך את הקובץ System ישירות, אלא רק מתוך "עורך הרישום" (Registry Editor): הקש

+  R ← **ורשום** ← **Regedit**.

עורך הרישום מציג את הרישום כשהוא בנוי מענפים עיקריים, אשר כל אחד מהם מתפצל לתת-ענפים:



הענפים הראשיים בעורך הרישום :

Hkey_Local_Machine

כל הגדרות תצורת המחשב: חומרה, תוכנות, הגדרות רשת, אבטחה ברשת ועוד. הגדרות אלו תופסות לגבי המחשב ולא לגבי משתמשים על גבי המחשב.

Hkey_Classes_Root

ענף זה מציג חלק מהענף הקודם בנפרד. למעשה, תוכן ענף זה זהה לתוכן תת-הענף `HKLM\Software\Classes`, רק שהוא מוצג כאן בשם אחר. בחלק זה נרשמים סוגי הקבצים לפי סיומות, בנוסף להגדרות שונות שקשורות לתוכנות.

Hkey_Current_Config

הגדרות החומרה הנוכחית. ענף זה בשימוש במידה ועובדים עם פרופילי חומרה.

Hkey_Users

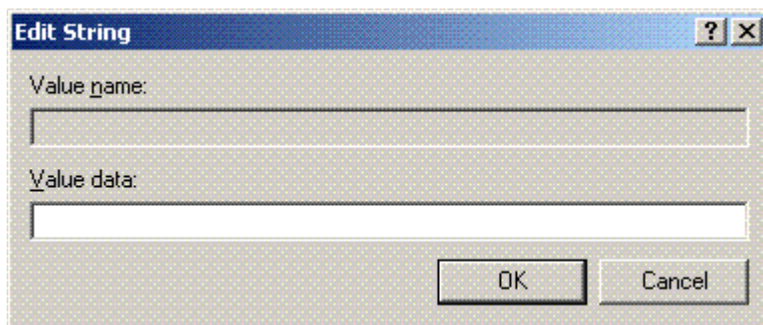
מכיל את הגדרות המשתמשים השונים כאשר עובדים עם פרופילי משתמש. כאשר לא עובדים עם פרופילי משתמש, יהיה שימוש במפתח Default.

Hkey_Current_User

מפתח רישום זה מכיל את הגדרות המשתמש הפעיל על המחשב (זה שביצע logon).

בתוך כל אחד ממפתחות אלו ישנם ערכים מסוגים שונים, שניתן לערוך, למחוק או להוסיף: **Binary Value**, **DWORD Value**, **String Value**, **Multi-String Value** ו-**Expandable String Value**.

סוג נוסף אשר לא ניתן להוסיפה הוא: **Full Resource Descriptor Value**, המשמש לרישום חומרה.



String values (REG_SZ) - String values מכילים 'מחרוזות' של תווים בד"כ טקסט. קיימים מספר סוגי מחרוזות:

String array value (REG_MULTI_SZ) מכיל מספר מחרוזות המודבקות יחד ובניהם ערכי null – אפסים. ניתן לערוך אותם אך לא ליצור אותם ידנית.

Expanded string value (REG_EXPAND_SZ) מכיל משתנים מיוחדים המתווספים ע"י מערכת ההפעלה.

Binary values (REG_BINARY) מכילים קוד הקסדצימאלי בממשק הנקרא hex editor – מומלץ לשנות ערכים אילו רק אם הנכם מבינים את משמעות הערכים הללו.

DWORD values (REG_DWORD) כעקרון **DWORD** – הינו מספר הקסדצימאלי. בד"כ 0 מייצג 'כן' ואילו 1 מייצג 'לא' ניתן להשתמש גם בערכים מספריים לציון מהירות או זמן (שניות).

יבוא\יצוא של הרגיסטרי

עורך הרגיסטרי תומך ביצוא של מפתחות ענפים בודדים או חלקים של הרגיסטרי לצורך גיבוי. פעולת export תיצור קובץ בעל סיומת REG אשר בלחיצת עכבר ניתן לשחזר את המידע שבהם אל הרגיסטרי. כדי לבצע יצוא יש להאיר את המפתח אותו רוצים לגבות ואז לבחור file>export. המפתח וכל תת הענפים שלו ישמרו. קבצי reg בנויים בצורה דומה לקובצי ini. וניתן לפתוח אותם בעזרת תוכנת notepad.

לחיצה כפולה על הקובץ תמזג את הערכים שבו חזרה אל תוך הרגיסטרי.

ניתן להשתמש בפקודת REG בממשק ה-CMD כדי לבצע מיזוג' שקט' של הקובץ לרגיסטרי.

ישנן פקודות PS המיועדות לעבודה עם רגיסטרי

חיוני לגבות את הרישום לפני שמשנים אותו

כל דבר שתזינו בקובץ הרישום יישמר מיידית ולצמיתות כולל שגיאות. החדשות הטובות הן שלא-

צריך לזכור ללחוץ Save. החדשות האיזמות הן שאי אפשר לעשות Undo -

לגיבוי קובץ הרישום מתוך Regedit, יש לבחור קובץ, ייצוא, ולבחור בכפתור המסומן ב"הכל".

עדכוני מערכת בווינדוס 11

עדכוני מערכת מספקים לנו תיקון לבעיות במע' ההפעלה היכולות להיות קשורות לתכונות או לבעיות אבטחה, כמו כן עדכונים מוסיפים תכונות חדשות למערכת. בתור ברירת מחדל עדכוני המע' מבוצעים בצורה אוט' ומותקנים ברגע שהמערכת מזהה עדכון ומורידה אותו ממיקרוסופט.

בעבר מיקרוסופט הייתה משחררת גרסה חדשה של מע' ההפעלה כל מספר שנים, עבור ארגונים היה הדבר כרוך בהכשרת משתמשים, הגירה למע' חדשה התאמה של תוכנות ועוד...

התפיסה הנוכחית היא היום של ווינדוס כשירות – כלומר מע' ההפעלה מתעדכנת בתכונות חדשות אך שומרת על תאימות לאחור. העדכונים היום מגיעים כחבילת עדכונים ולא כמו בעבר כל עדכון מגיע כקובץ נפרד ולנו יש שליטה מה להתקין

ישנם מספר סוגי עדכונים אותם נוכל לקבל:

עדכונים מצטברים (Cumulative updates) – מכונים גם quality updates – מכילים בד"כ תיקוני אבטחה, תיקוני באגים ושינויים קטנים בצורת הפעולה של המע'

שינויי גרסה – (feature updates) – מכילים תכונות חדשות של המע' ולמעשה מעבירים אותנו מהגרסה הנוכחית לגרסה מתקדמת יותר של ווינדוס 11.

עדכוני תצורה ל DEFENDER ולכלי הסרת רוגלות – עדכוני האבטחה מעדכנים את בסיס הנתונים של התוכנות להגנה מוירוסים ורוגלות על מנת שהמערכת תוכל להתמודד עם סיכוני האבטחה העדכניים.

עדכוני דרייברים – במידה ויש עדכון דרייברים עבור החומרה המותקנת אצלנו יבוצע עדכון

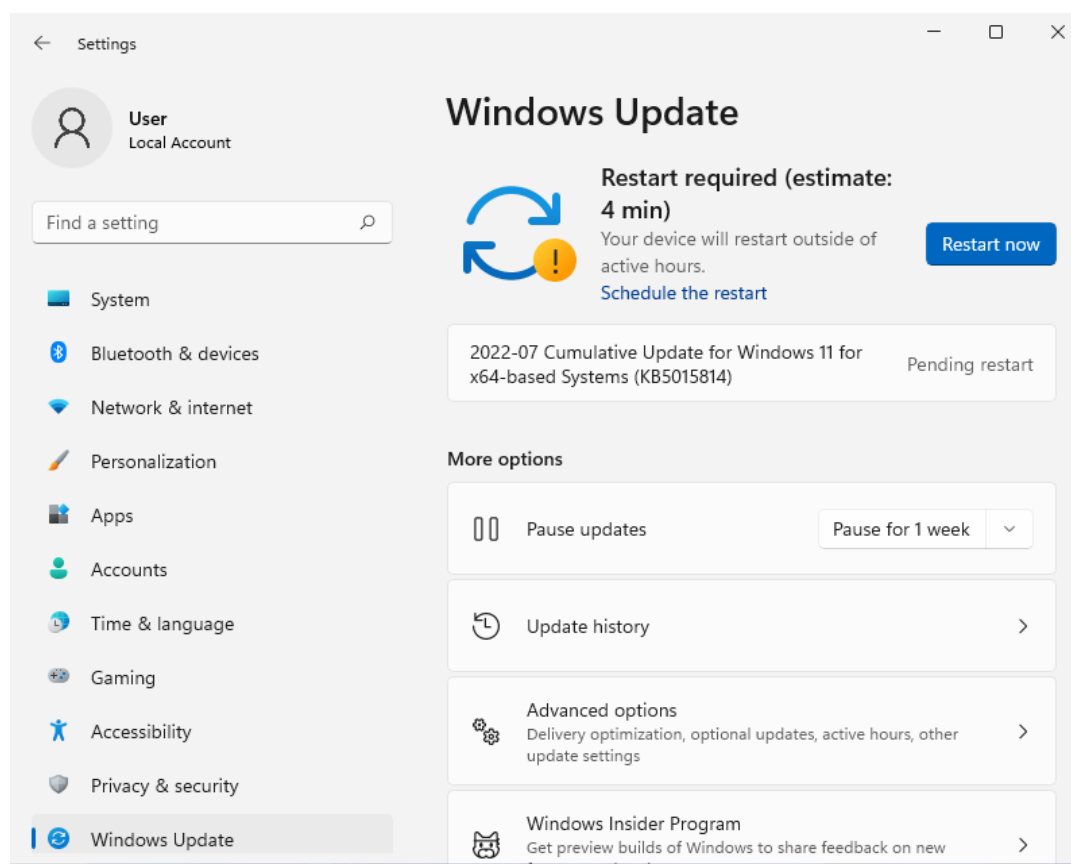
ישנם מספר ערוצים בהם מבוצע העדכון, כל ערוץ קובע למעשה את התדירות וסוג העדכונים אותם נקבל.

General Availability Channel - עדכונים במסלול זה יוצאים לאחר שנבדקו, תכונות חדשות יגיעו כל שנה בד"כ – זהו המסלול הרגיל למשתמשים ביתיים, משתמשים ארגוניים יכולים לבחור לדחות תכונות חדשות לאיזה פרק זמן שיבחרו.

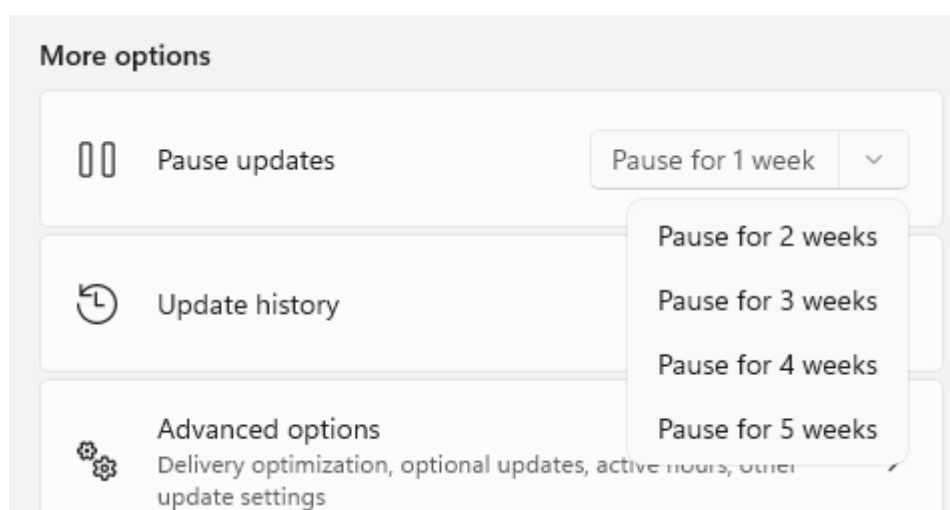
Long-Term Servicing Channel (LTSC) – ערוץ זה מתאים לגירסאות אנטרפרייז, מכיל גרסה יציבה של ווינדוס שמקבלת עדכוני אבטחה אך לא תכונות חדשות, גרסה זו מבחינת מייקרוסופט מיועדת למע' שמפעילות ציוד רפואי, כספומטים וכו'.

Windows Insider Program – אם אתם רוצים לבדוק את התכונות הכי חדשות עוד בטרם יצאו לציבור הרחב תוכלו להירשם לתוכנית זו ולקבל עדכונים שוטפים וגירסאות בטא של תכונות על מנת לדווח למיקרוסופט לגבי באגים במידה ונתקלתם בהם. רצוי מאוד שזו לא תהיה מע' ההפעלה בה אתם עובדים בצורה שוטפת כי תיתכן גם חוסר יציבות.

העדכונים מבוצעים אוט' אך נוכל לשלוט על מספר הגדרות, ניכנס אל תפריט ההגדרות Win+I, בחיפוש נרשום UPDATE



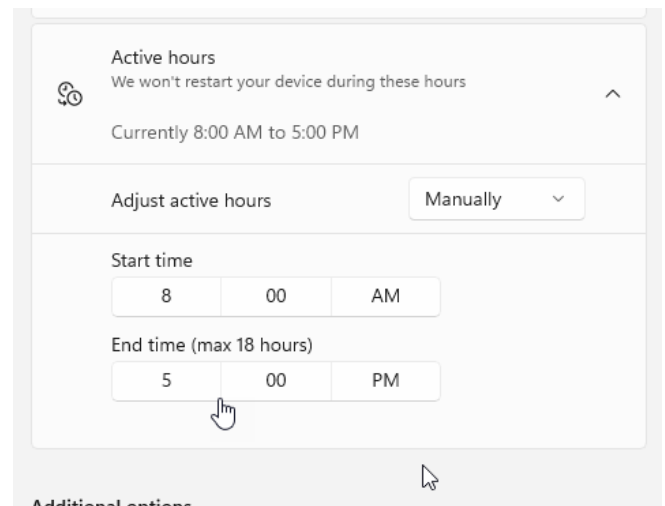
נוכל לראות את העדכונים שממתינים להתקנה ואת מספר KB שלהם על מנת לחפש ולקרוא מה מכיל העדכון
נוכל לדחות עדכונים לתקופה של עד חמישה שבועות



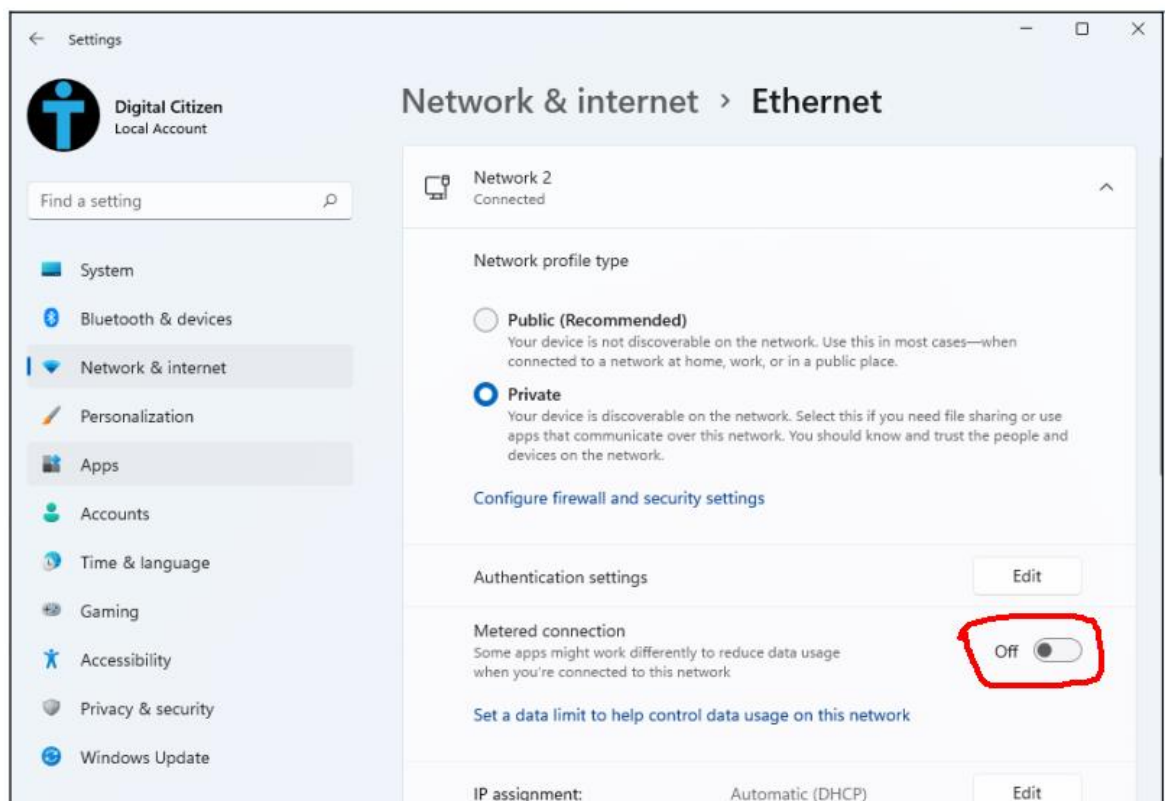
נוכל לראות עדכונים שהותקנו בתפריט Update History

נוכל להיכנס להגדרות מתקדמות ולהגדיר שם לקבל עדכונים עבור מוצרי מיקרוסופט אחרים מעבר למע' ההפעלה (אופיס, TEAMS וכו...)

נוכל לבחור את השעות בהן לא יבוצע אתחול לאחר הורדת עדכון באפשרות Active hours נבחר להגדיר את השעות ידנית ונציין את טווח הזמן



בוינדוס 11 אין לנו דרך לעצור עדכונים אך יש טריק שמאפשר לנו לבצע זאת, אנו יכולים להגדיר את הרשת שלנו כרשת בתשלום ואז לא יבוצעו עדכונים כל עוד נהיה מחוברים לרשת הזו. כדי לבצע זאת ניכנס להגדרות הרשת ונציין שהרשת היא רשת בתשלום



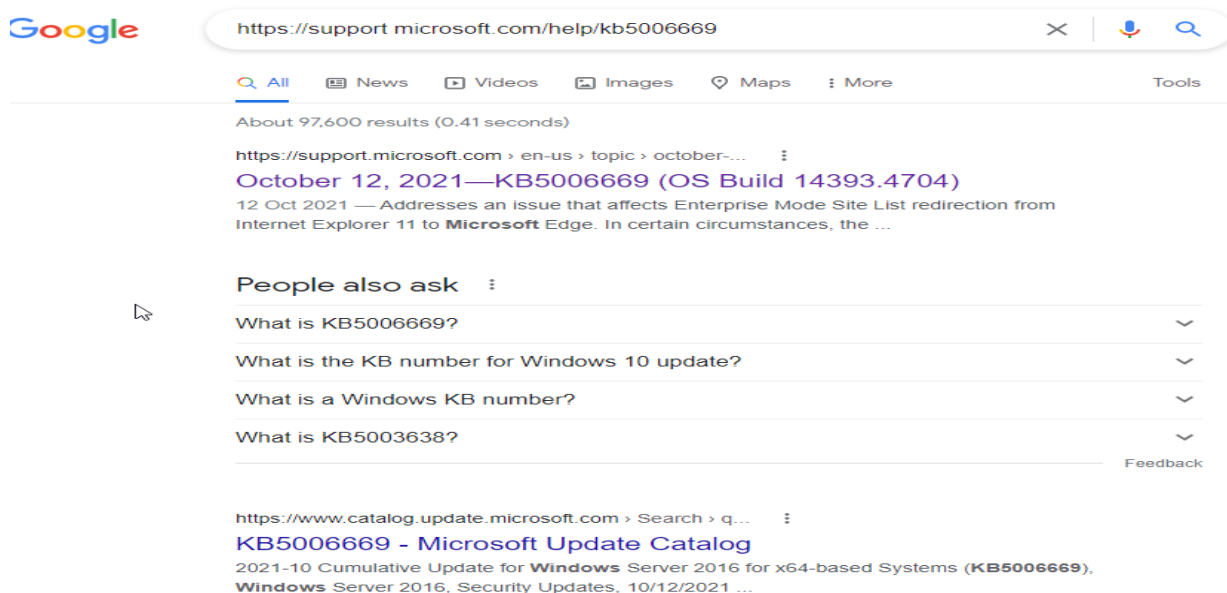
כעת לא יבוצעו עדכונים עד שלא נחזיר את הרשת למצב לא מנוטר כלומר לא בתשלום או שנעדכן בצורה ידנית

טיפול בתקלות עדכונים :

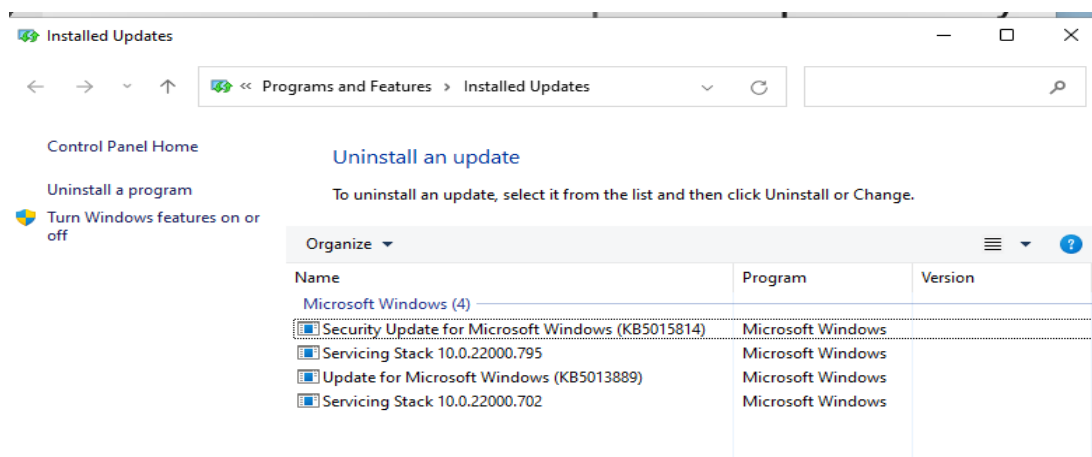
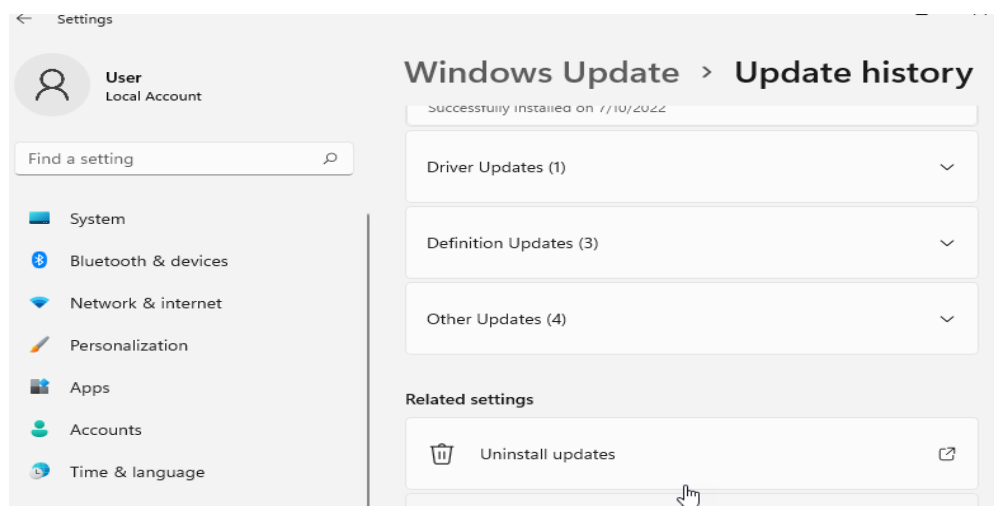
אם נרצה מידע על עדכון מסויים נוכל לגשת לכתובת הבאה :

<https://support.microsoft.com/help/nnnnnnnn/>

במקום חחח נרשום : KB והמספר של העדכון לדוגמא :



נוכל להסיר עדכון דרך
ההגדרות, ניגש להיסטוריית
העדכונים ונבחר להסיר עדכון



יפתח לנו ממשק של
לוח הבקרה דרכו נבחר
את העדכון הבעייתי

הבעיה בהסרת עדכון היא שהעדכון יותקן שנית בנקודה זו או אחרת, אם נרצה לחסום עדכון ספציפי מלהיות מותקן שנית, נוכל להשתמש בכלי הזה שנמצא ב GITHUB ופותח על ידי מתכנת עצמאי:

<https://github.com/DavidXanatos/wumgr/releases>

לעיתים התקנת עדכון יכולה להיתקע ובכך לגרום לנו להיכנס למעגל אין סופי שבו בכל פעם נצטרך לבצע אתחול והתקנה של העדכון, כדי לטפל בזה מיקרוסופט מספקת עזרה מפורטת בנושא בקישור הבא:

<https://docs.microsoft.com/en-us/windows/deployment/update/windows-update-resources>

כמו כן היא מספקת כלי דיאגנוסטיקה להורדה ישירה בקישור הבא:

<https://aka.ms/wudiag>

שימוש בכלים בדיקות ביצועים חיצוניים של מיקרוסופט

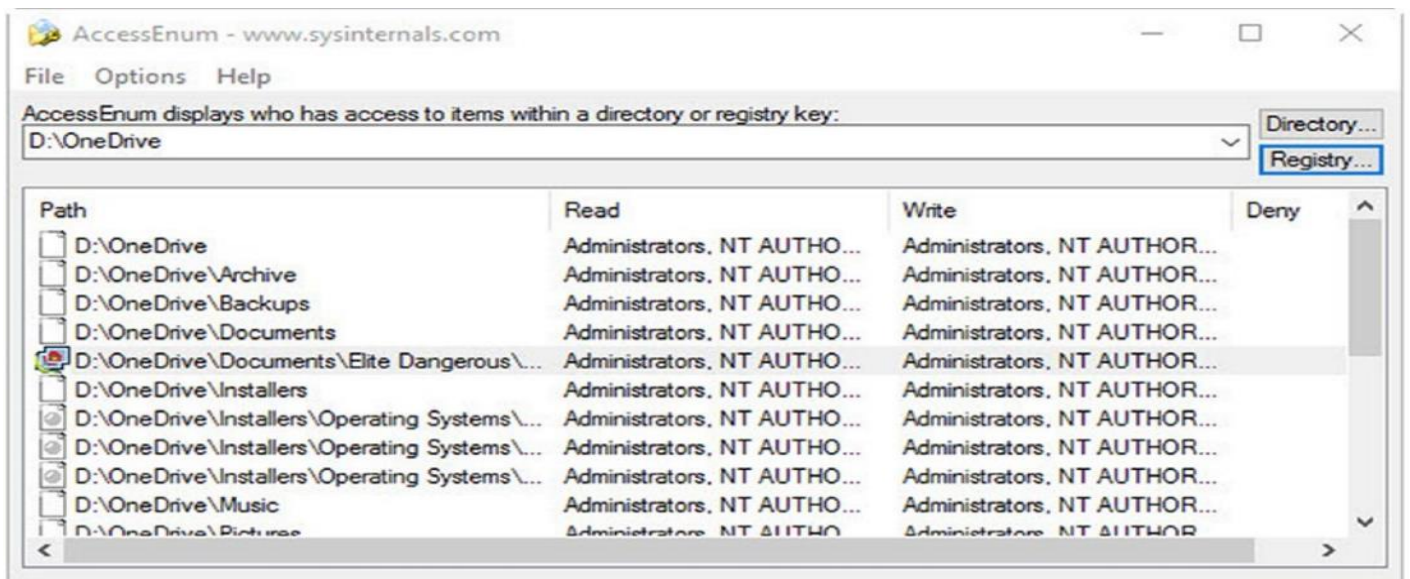
למיקרוסופט ישנה חבילת כלים יעודיים לתמיכה במע' ווינדוס בשם Sysinternals, כלים אילו פותחו ע"י מרק רוזינוביץ' וברייס קוגסוול בשנת 1996, מאוחר יותר נקנתה החברה ע"י מיקרוסופט והכלים נשארו חנימיים לשימוש הציבור.

ניתן להוריד את הכלים באתר בקישור הבא : <https://docs.microsoft.com/sysinternals>

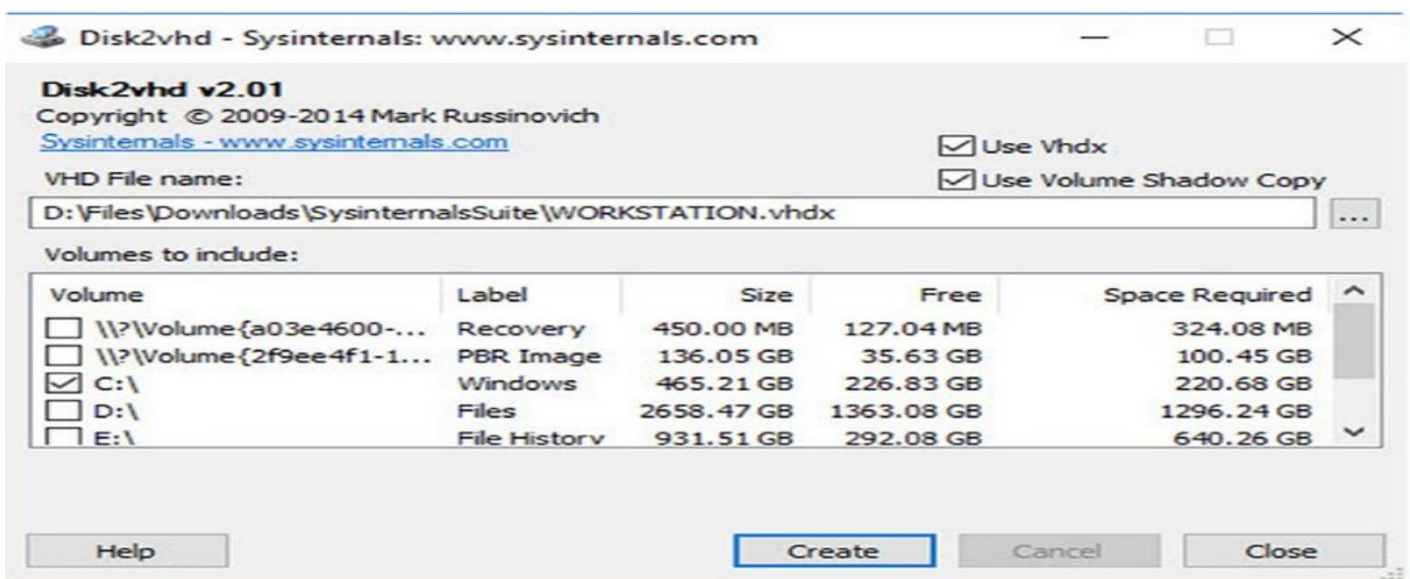
ישנו גם פורום פעיל בו נוכל לקבל מידע רב על הכלים. חלק מהכלים עובד בממשק CLI וחלק בממשק הגרפי, רובם עובדים בשני הממשקים וגם ב-32 ו-64 ביט. נוכל למצוא כלים לניהול הרשאות קבצים, בדיקה של הדיסק, תהליכים ועוד...

נסקור מספר כלים שימושיים :

AccessEnum - הכלי הזה יאפשר לנו לקבל מידע על הרשאות גישה לתיקייה, לייצא את המידע וגם להשוות אותו לקובץ קודם.



Disk2Vhd – התוכנה מאפשרת לנו להפוך דיסק פיזי לקובץ וירטואלי ובכך נקבל את האפשרות לבצע בחינה מעמיקה ובדיקות על הדיסק בסביבה וירטואלית



DiskMon – כלי דיאגנוסטיקה מעמיק, נוכל לקבל מידע על כל פעולה שבוצעה בדיסק, נוכל לדוגמא פעילות חריגה של כתיבה בדיסק אם אנו חושדים בפעילות חריגה של רוגלה או לראות אם תוכנה ניסתה לכתוב למקום פגום בדיסק.


```
C:\sys\SysinternalsSuite>du C:

DU v1.62 - Directory disk usage reporter
Copyright (C) 2005-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

Files:          163
Directories:    1
Size:           105,708,776 bytes
Size on disk:   106,037,248 bytes
```

DU – כלי CLI ייתן לנו מידע על השימוש בדיסק נוכל לשלב מספר פרמטרים ואף לייצא את המידע לקובץ CSV

```
C:\sys\SysinternalsSuite>ntfsinfo.exe C:

NtfsInfo v1.2 - NTFS Information Dump
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Volume Size
-----
Volume size           : 487285 MB
Total sectors         : 997960351
Total clusters        : 124745043
Free clusters         : 36555186
Free space            : 142793 MB (29% of drive)

Allocation Size
-----
Bytes per sector      : 512
Bytes per cluster     : 4096
Bytes per MFT record  : 0
Clusters per MFT record: 0

MFT Information
-----
MFT size              : 945 MB (0% of drive)
MFT start cluster     : 786432
MFT zone clusters     : 44270336 - 44295552
MFT zone size         : 98 MB (0% of drive)
MFT mirror start      : 16

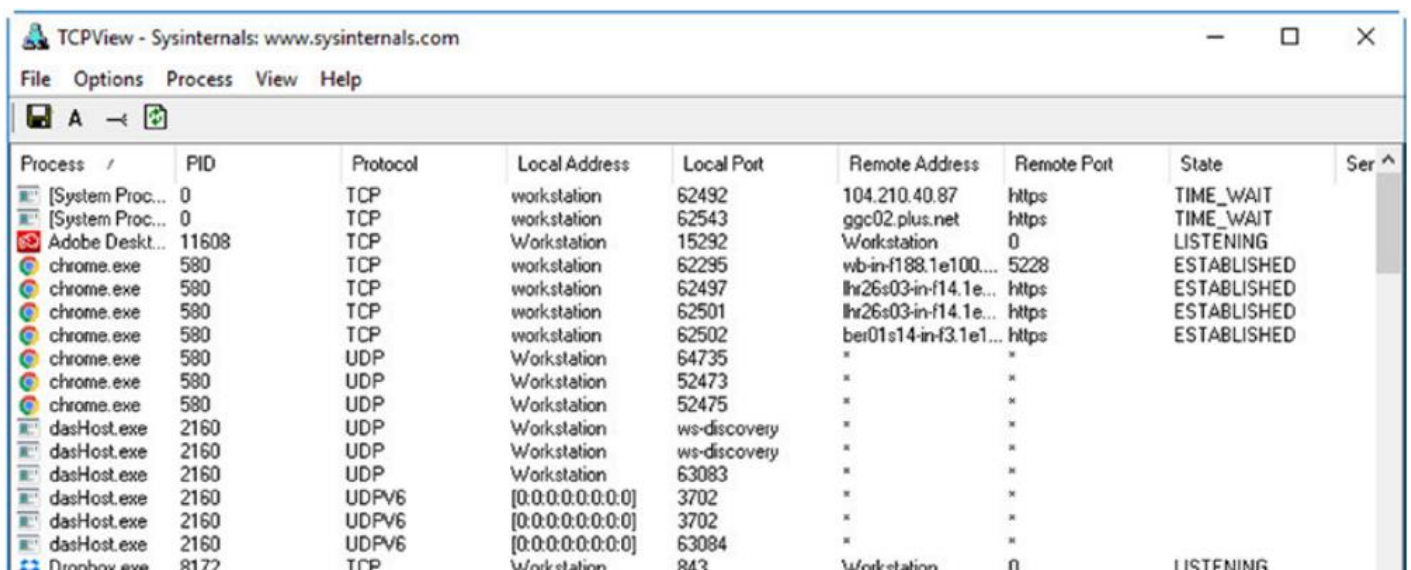
Meta-Data files
-----
```

NTFSINFO – נקבל מידע על מע' הקבצים NTFS

SDELETE – תוכנה שימושית שתאפשר לנו לבצע WIPE עבור קובץ ספציפי נוכל להגדיר את מספר הפעמים שהקובץ "יידרס", קובץ שנמחק בצורה זו לא יהיה אפשר לשחזר באמצעות תוכנות שחזור.

ShareEnum – תוכנה זו תתן לנו מידע על כל התיקיות המשותפות במחשב.

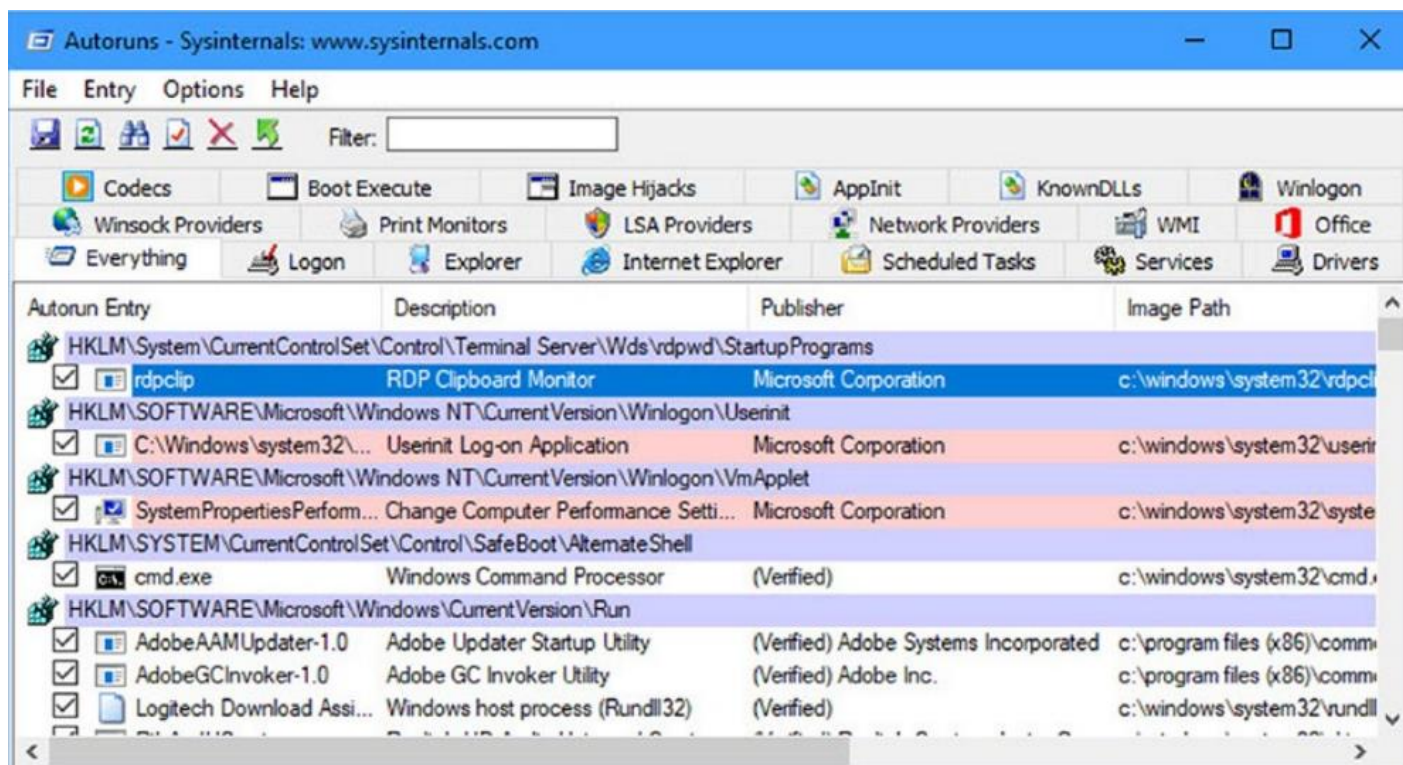
TCPVIEW – תתן לנו מידע על כל חיבורי הרשת שלנו, אילו תוכנות ואילו פורטים עושים שימוש ברשת



TCPView - Sysinternals: www.sysinternals.com

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	workstation	62492	104.210.40.87	https	TIME_WAIT
[System Proc...	0	TCP	workstation	62543	ggc02.plus.net	https	TIME_WAIT
Adobe Desk...	11608	TCP	Workstation	15292	Workstation	0	LISTENING
chrome.exe	580	TCP	workstation	62295	wb-in-f188.1e100...	5228	ESTABLISHED
chrome.exe	580	TCP	workstation	62497	lhr26s03-in-f14.1e...	https	ESTABLISHED
chrome.exe	580	TCP	workstation	62501	lhr26s03-in-f14.1e...	https	ESTABLISHED
chrome.exe	580	TCP	workstation	62502	ber01s14-in-f3.1e1...	https	ESTABLISHED
chrome.exe	580	UDP	Workstation	64735	*	*	
chrome.exe	580	UDP	Workstation	52473	*	*	
chrome.exe	580	UDP	Workstation	52475	*	*	
dasHost.exe	2160	UDP	Workstation	ws-discovery	*	*	
dasHost.exe	2160	UDP	Workstation	ws-discovery	*	*	
dasHost.exe	2160	UDP	Workstation	63083	*	*	
dasHost.exe	2160	UDPv6	[0:0:0:0:0:0:0:0]	3702	*	*	
dasHost.exe	2160	UDPv6	[0:0:0:0:0:0:0:0]	3702	*	*	
dasHost.exe	2160	UDPv6	[0:0:0:0:0:0:0:0]	63084	*	*	
Drobox.exe	8172	TCP	Workstation	843	Workstation	0	LISTENING

AutoRuns – אחת התוכנות השימושיות בחבילה, מאפשרת לנו לראות את כל התוכנות, שירותי המע' והתוספים שעולים עם עליית המחשב ולנטרל אותם וכמו כן לראות את ההגדרות ברגיסטרי



ListDlls – באמצעות הפקודה נוכל לראות את כל התהליכים הרצים כרגע במע' ואת קבצי ה-DLL שהם עושים בהם שימוש, יעיל מאוד אם נרצה לנטר פעילות של תוכנה חשודה. ניתן לראות פעילות של תהליך אחד אם נציין את שמו

```
PS C:\sys\SysinternalsSuite> .\Listdlls.exe notepad
```

```
Listdlls v3.2 - Listdlls
Copyright (C) 1997-2016 Mark Russinovich
Sysinternals

-----
notepad.exe pid: 8388
Command line: "C:\Windows\system32\notepad.exe"

Base                Size                Path
0x000000005c8d0000  0x43000             C:\Windows\system32\notepad.exe
0x00000000f1380000  0x1ed000            C:\Windows\SYSTEM32\ntdll.dll
0x00000000ee6f0000  0xb3000             C:\Windows\System32\KERNEL32.DLL
0x00000000ed420000  0x29a000            C:\Windows\System32\KERNELBASE.dll
0x00000000ee870000  0xa7000             C:\Windows\System32\ADVAPI32.dll
0x00000000ee9d0000  0x9e000             C:\Windows\System32\msvcrt.dll
0x00000000f0420000  0x9f000             C:\Windows\System32\sechost.dll
0x00000000f1160000  0x11d000            C:\Windows\System32\RPCRT4.dll
0x00000000ee840000  0x29000             C:\Windows\System32\GDI32.dll
0x00000000ed6c0000  0x19c000            C:\Windows\System32\gdi32full.dll
0x00000000ee380000  0xa0000             C:\Windows\System32\msvcrt_win.dll
```

Process Explorer - אחד מכלי בדיקות הביצועים החזק ביותר בחבילה, יכול להחליף גם את Task Manager הכלי ייתן לנו מידע מפורט לגבי כל תהליך שרץ במחשב. נוכל להחליט להשתמש בו במקום TASK MANAGER, במידה ונרצה להתחרט ולחזור למנהל המשימות הרגיל נקליד את הפקודה הבאה ע"מ לאפס את ערכי הרגיסטרי:

```
reg delete "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options\taskmgr.exe" /v Debugger.
```

The screenshot displays three windows from Windows Task Manager:

- Process Explorer:** Shows a list of running processes. Key processes include:
 - chrome.exe:** Multiple instances, using significant memory (up to 193,864 K).
 - WINWORD.EXE:** Microsoft Word, PID 16912, using 263,496 K of working set.
 - cmd.exe:** Windows Command Processor, PID 16108.
 - processp64.exe:** Sysinternals Process Explorer, PID 15856.
- System Information:** Shows system details under the 'Summary' tab:
 - I/O:** 311.7 KB
 - Network:** 461 B
 - Disk:** 40.0 KB
 - Summary Table:**

I/O		Network		Disk	
Read Delta	1,405	Receive Delta	2	Read Delta	0
Read Bytes Delta	85 KB	Receive Bytes Delta	0 KB	Read Bytes Delta	0 KB
Write Delta	1,273	Send Delta	1	Write Delta	5
Write Bytes Delta	85 KB	Send Bytes Delta	0 KB	Write Bytes Delta	40 KB
- WINWORD.EXE: 16912 Properties:** A window showing user information (User: WORKSTATION\Mike Halsey, SID: S-1-5-21-1297367860-1966104762-633137142-1001) and a list of privileges:
 - Privilege:** SeChangeNotifyPrivilege, SeIncreaseWorkingSetPrivilege, SeShutdownPrivilege, SeTimeZonePrivilege, SeUndockPrivilege.
 - Flags:** Default Enabled, Disabled, Disabled, Disabled, Disabled.

בתמונה פירוט של המידע על התהליך WinWord.

Process Monitor – כלי זה יאפשר לנו הבנה מעמיקה של הפונקציות אותן מריץ התהליך, במידה ויש לנו תוכנה חשודה שאיננו יודעים אילו פעולות היא מבצעת במע' ההפעלה, נוכל לבצע סקירה מעמיקה ולראות את הבקשות שהיא מבצעת מול ליבת המערכת. לדוגמא: הורדנו תוכנה חנימית מהאינטרנט, נוכל לגלות בקלות שבין יתר הפעולות שהיא עושה היא מבצעת שליחת מידע לאתר כלשהו...

Time	Process Name	PID	Operation	Path	Result	Detail
12:13:...	snagiteditor.exe	4764	NotifyChangeDi...	C:\		Filter: FILE_NOTIF...
12:13:...	SearchIndexer....	12556	ReadFile	C:\Windows\System32\vmssrch.dll	SUCCESS	Offset: 2,074,112, ...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,424,832, ...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,392,064, ...
12:13:...	SearchIndexer....	12556	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:13:...	SearchIndexer....	12556	FileSystemControlC:		SUCCESS	Control: FSCTL_R...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,367,488, ...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,351,104, ...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,238,464, ...
12:13:...	Explorer.EXE	5592	ReadFile	C:\Windows\explorer.exe	SUCCESS	Offset: 2,213,888, ...
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:13:...	Explorer.EXE	5592	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
12:13:...	Explorer.EXE	5592	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: HandleTag...
12:13:...	Explorer.EXE	5592	RegQueryKey	HKCU\Software\Classes	SUCCESS	Query: Name
12:13:...	Explorer.EXE	5592	RegOpenKey	HKCU\Software\Classes\Applications\...	NAME NOT FOUND	Desired Access: R...
12:13:...	Explorer.EXE	5592	RegOpenKey	HKCR\Applications\Procmon64.exe	NAME NOT FOUND	Desired Access: R...
12:13:...	Explorer.EXE	5592	CreateFile	C:\Users\Mike Halsey\AppData\Local\...	SUCCESS	Desired Access: R...
12:13:...	Explorer.EXE	5592	QueryBasicInfor...	C:\Users\Mike Halsey\AppData\Local\...	SUCCESS	CreationTime: 01/0...
12:13:...	Explorer.EXE	5592	CloseFile	C:\Users\Mike Halsey\AppData\Local\...	SUCCESS	

Showing 44,028 of 66,567 events (66%) Backed by virtual memory

Process: chrome.exe PID: 1628					
Committed:	65,636 K				
Private Bytes:	1,736 K				
Working Set:	7,556 K				

Type	Size	Committed	Private	Total WS
Total	2,185,394,744 K	65,636 K	1,736 K	7,556 K
Free	135,253,558,784 K			
Heap	1,488 K	324 K	260 K	264 K
Image	26,904 K	26,904 K	816 K	6,144 K
Managed Heap				
Mapped File	5,340 K	5,340 K		128 K
Page Table	120 K	120 K	120 K	120 K
Private Data	37,783,832 K	356 K	356 K	320 K
Shareable	2,147,509,964 K	32,408 K		492 K
Stack	65,536 K	184 K	184 K	88 K
Unusable	1,560 K			

Address	Type	Size	Committed	Private	Total WS	Private
000000007FFE0000	Private Data	4 K	4 K	4 K	4 K	
000000007FFE0000	Private Data	4 K	4 K	4 K	4 K	
000000C6CDE00000	Private Data	2,048 K	68 K	68 K	68 K	6
000000C6CE000000	Thread Stack	8,192 K	28 K	28 K	28 K	16
000000C6CE800000	Thread Stack	8,192 K	24 K	24 K	24 K	12
000000C6D0000000	Thread Stack	8,192 K	20 K	20 K	20 K	8
000000C6D0800000	Thread Stack	8,192 K	32 K	32 K	20 K	2

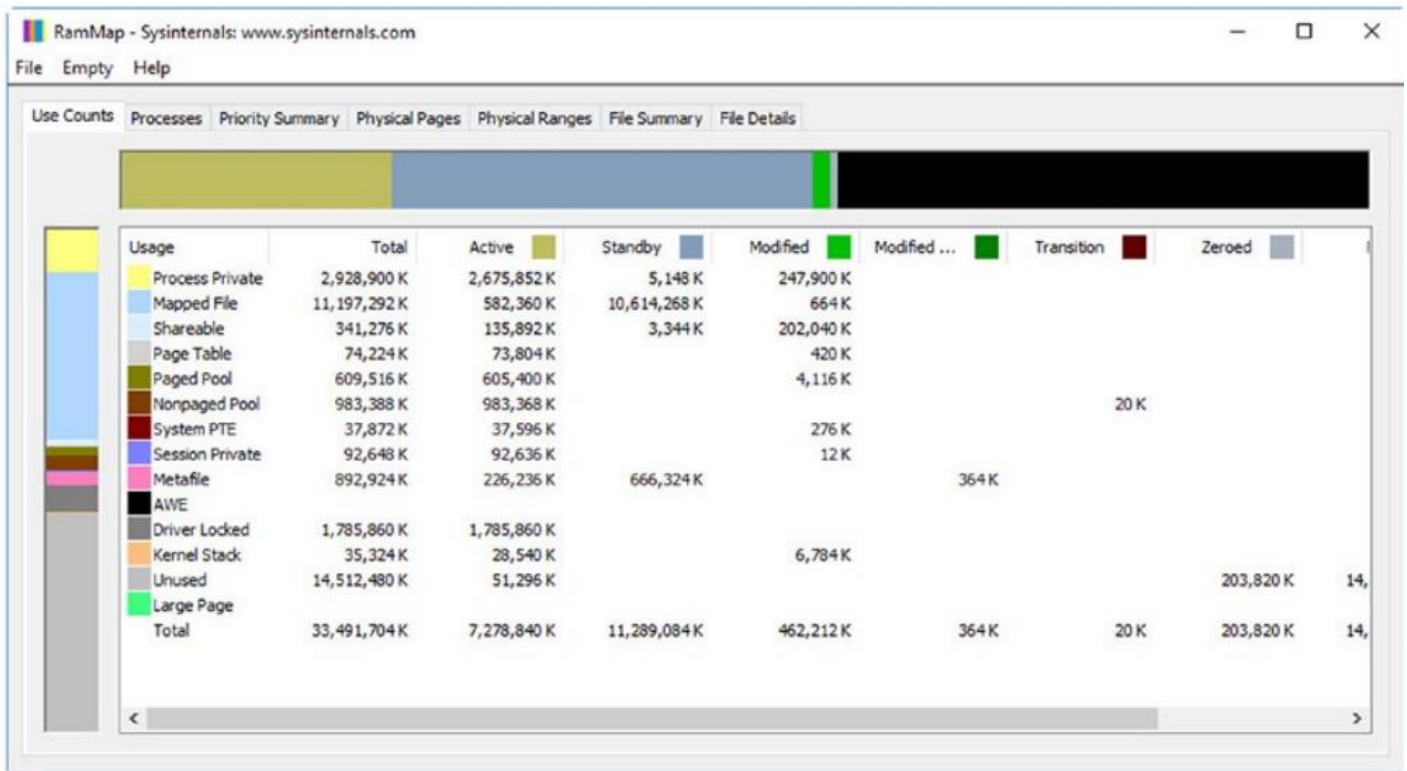
Timeline... Heap Allocations... Call Tree... Trace...

VMMap - תאפשר לנו לקבל מידע מעמיק על השימוש בזיכרון הוירטואלי והזיכרון הפיזי עבור תהליך ספציפי
נקבל מידע לגבי הגודל והכתובות בהן נעשה שימוש

LogonSessions – נוכל לקבל מידע על כל המשתמשים המחוברים , כמו כן נוכל לקבל מידע באילו הרשאות חיבור תהליכים מסויימים רצים .

Sysmon – התוכנה תאפשר התקנה של שירות מערכת ודרייבר לשלבי האתחול המתקדמים על מנת שנוכל לקבל מידע ב EVENT VIEWER לגבי תקלות או רגולות שרצות במחשב.

RAMMAP - כלי גרפי שיציג לנו את השימוש בזיכרון RAM לגבי כל אפליקציה ותהליך



לסיכום ישנם כלים רבים בחבילה , חלק גדול לא סקרנו , מומלץ להיכנס לאתר ולעבור על הכלים והמידע הרב שמיקרוסופט מספקת עבורם.