

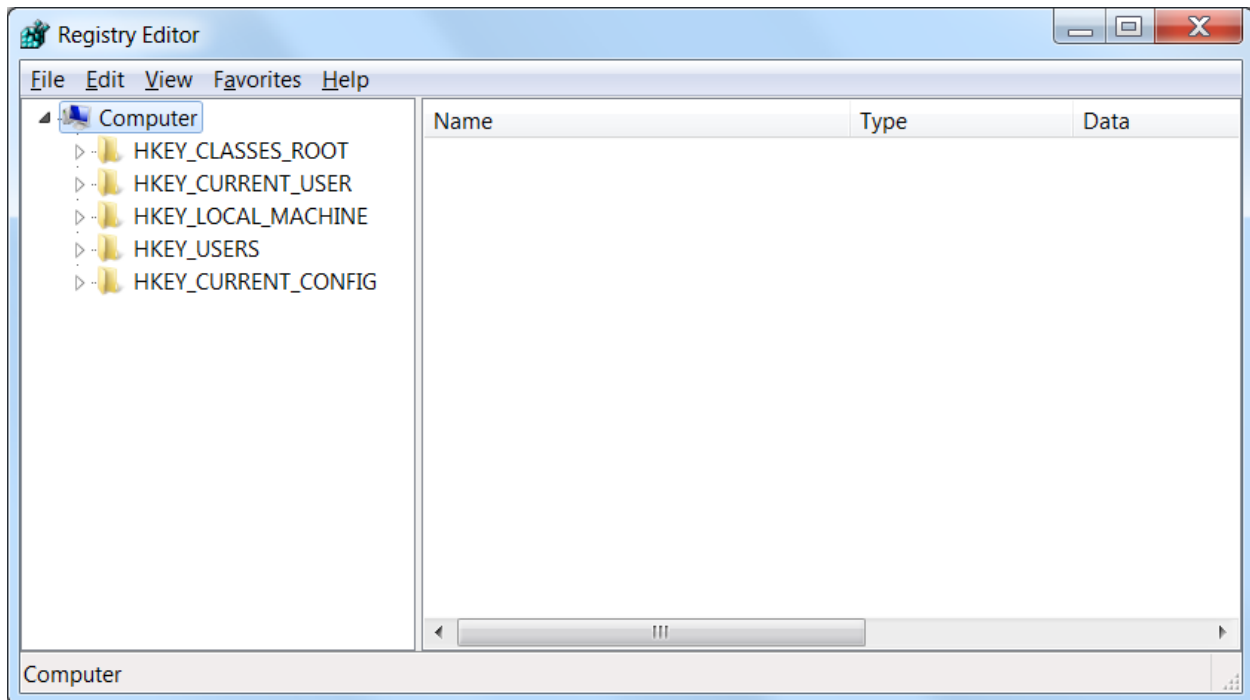
הדגמת RegEdit ותרגיל

בשיעור למדנו על מנגנון ניהול ההגדרות ב Windows. על מנת להקל את העבודה של משתמשים עם מאגר ההגדרות העצום – נוצר כלי בשם RegEdit, המגיע עם מערכת ההפעלה, ומאפשר דרך GUI פשוט לצפות ולערוך ערכים.

אנו נעזר בכלי זה כדי ללמוד קצת על מבנה ה Registry וגם נתנסה בביצוע שינויי הגדרות למחשב.

אזהרה: שינוי ערכים שאינכם יודעים מה משמעותם עלולה לפגוע בפעולה התקינה של המחשב. מומלץ, אם ניתן, לבצע "מחקרים" רק מעל מכונה וירטואלית.

נתחיל בפתיחת הכלי. הדרך הכי פשוטה – הקשה על צירוף המקשים WinKey + R לפתיחת שורת ההרצה ולאחר מכן הקלדת regedit. כעת יפתח לכם החלון הבא:



נשים לב כי ישנם מספר "תיקיות" בבסיס העץ (למעשה, המינוח הנכון הוא "מפתחות" – אבל לשם נוחות נתייחס בשם מפתח רק לאלו המופיעים בחלון הימני, בתוך ה"תיקיות"). נתחיל בתיקיית האב הראשונה: **HKEY_CLASSES_ROOT**. נפרוש את עץ התיקיות (לוחצים על החץ הקטן ליד שם התיקייה) ונראה רשימה ארוכה מאוד של תיקיות.

משימה 1: חפשו את התיקייה *txt*. והסתכלו אילו תיקיות יש בתוכה. אחת התיקיות הינה *ShellNew* – הביטו במפתחות שבה ובערכים שלהם. מה מצאתם? מה לדעתכם משמעות הגדרות אלה?

HKEY_CLASSES_ROOT מכיל בין השאר את ההגדרות המשייכות סיומת קובץ – לתוכנה שפותחת אותו.

2. כעת חפשו את התיקייה *doc*. ובתוכה את *ShellEx* – היכנסו לאחת התיקיות בתוכה ושימו לב למפתח בשם (Default) ולערך "המוזר" בתוכו. ערך מהצורה {A1C140-AE5C-4CD2-B1C9-3DFA2AE118FE91} נקרא GUID (Globally Unique Identifier) ומשמש כמזהה ייחודי.

3. ה GUID הזה למעשה מקשר אותנו למפתח Registry הנמצא במקום אחר! המטרה העיקרית היא לאפשר לעשות סדר באיפה נמצא כל דבר, ולמנוע שכפול – בתיקיה אחת יש את התוכנות השונות המשמשות לפתיחת הקבצים, בתיקיה אחרת יש את הקישורים בין סיומות לתוכנות וכו'. נרצה לחפש את הערך הזה – שמופיע כתיקייה במקום אחר בתוך ה Registry. לשם כך – נשתמש פשוט בחיפוש (CTRL+F) לשם הערך שמצאנו ב- (2).

פתחו את התיקייה שמצאתם ב 3 – מה יש בתוכנה? איזו תוכנה פותחת את הקובץ?

לפני שנמשיך הלאה – נדבר על משהו משמח: קיצורים!

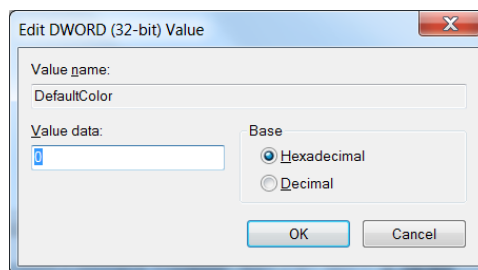
על מנת להקל על הגישה לתיקיות הבסיס ב- Registry תוכלו למצוא בהרבה מקומות שימוש בקיצורים הבאים:

- HKEY_LOCAL_MACHINE – HKLM -
- HKEY_CLASSES_ROOT - HKCR -
- HKEY_CURRENT_USER - HKCU -
- HKEY_USERS – HKU -
- HKEY_CURRENT_CONFIG – HKCC -

זכרו זאת להמשך!

המפתח **HKEY_CURRENT_USER** מכיל הגדרות הרלוונטיות למשתמש המחובר כרגע למחשב. למעשה, המידע המופיע תחת מפתח זה נמצא גם תחת אחת התיקיות הנמצאות ב **HKEY_USERS** (נסו לזהות איזה מהתיקיות ב HKU היא זו של המשתמש שלכם שכרגע מחובר!)

משימה 2: היכנסו לערך הבא: **HKEY_CURRENT_USER\Software\Microsoft\Command Processor** וערכו את המפתח **DefaultColor** על ידי לחיצה כפולה עליו – שימו לב לסמן תחת הגדרת בסיס ההצגה (Base) את האפשרות להצגה כ- HEX. כעת הכניסו את הערך ההקסדצימלי DF ולחצו על כפתור האישור.



פתחו את חלון ה CMD השחור והאהוב (פתחו חלון חדש). מה קרה? (התשובה בעמוד הבא). ננצל את ההזדמנות לעשות שימוש קצר ופשוט בפקודת *Reg* : הריצו בחלון שנפתח את הפקודה:
reg Query "HKEY_CURRENT_USER\Software\Microsoft\Command Processor"

מה קיבלנו?



כעת החזירו את הערך ל 0, (או לכל ערך שתרצו בין 00 ל FF, כאשר התו הראשון מסמל את צבע הרקע והשני את צבע הטקסט – כך שמומלץ לא להשתמש בערכים כמו 33 או DD שכן תאלצו לכתוב על עיוור... ©)

המפתח **HKEY_LOCAL_MACHINE** (HKLM) מכיל את מרבית ההגדרות של מערכת ההפעלה ומחולק למספק קטגוריות בתוכו. תחת מפתח זה מופיעות רוב ההגדרות של מערכת ההפעלה, הגדרות רשת, הגדרות של תוכנות שונות שאינן תלויות משתמש (אחרת הן ימצאו ב HKCU).

משימה 3: הריצו (WinKey+R) את האפליקציה msconfig. תחת הקטגוריה Startup ישנה רשימה של התוכנות אשר עולות עם עליית המחשב (ב- Windows 8 ומעלה תמצאו שם הפניה לעמוד Startup שב- Task Manager). אפשר עכשיו לעשות Enable / Disable לתוכניות שכבר ברשימה, אבל הבאסה היא שלא ניתן להוסיף לשם ערכים ☹️. אך... אל חשש! אחרי שלמדנו קצת איך ההגדרות של Windows עובדות – אנחנו יודעים לפתור זאת. התוכנות השונות ברשימה נלקחות או מתיקיה ספציפית במחשב, או ממספר מפתחות רג'יסטרי. אתם כבר יכולים לנחש באיזו דרך נבחר... (נסו לראות כיצד ניתן להבדיל בין תוכנות ברשימה שהגיעו מהתיקיה לבין תוכנות שהגיעו מהרג'יסטרי. למשתמשי Windows 8 ומעלה – שימו לב שניתן להוסיף אם צריך עמודות לטבלאות ב- Task Manager שאינן מופיעות בברירת המחדל).

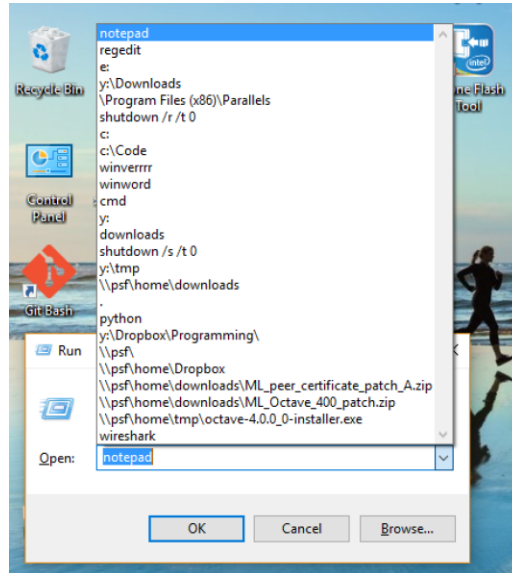
רשימה זו נמצאת תחת המפתחות:

XXX\Software\Microsoft\Windows\CurrentVersion\Run

(כאשר XXX יכול להיות HKLM או לחלופין HKCU. בדקו שאתם זוכרים מהו ההבדל).

הסתכלו על תצורת הערכים ברשימה והוסיפו גם את notepad שיעלה עם עליית המחשב תחת אחד מהמפתחות. (מומלץ לא לגעת בשאר הערכים שכן, כרגיל, הדבר עלול לפגוע בפעילות התקינה של המחשב).
[אתם יכולים בשלב זה לנסות לבצע אתחול למחשב ולראות אם Notepad עלה. ייתכן כי בשל תצורת המחשבים בכיתה זה לא יעבוד – חשבו מדוע. בכל אופן, ודאו לאחר מכן כי הורדתם את Notepad מהרשימה, בכדי לחסוך למשתמשי המחשב הבאים את ההנאה מ Notepad שנפתח לאחר עליית המחשב...]

משימה 4: פתחו שוב את חלון ה-Run (WinKey+R). שימו לב שחלון זה שומר את היסטוריית הפקודות שהורצו באמצעותו, וניתן לצפות בה באמצעות לחיצה על החץ הקטן:



באופן מפתיע, ההיסטוריה הזאת נשמרת ב-Registry, תחת המפתח:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU

1. כתבו תוכנית בפייתון אשר מדפיסה למסך את כל ההיסטוריה של חלון ה-Run. לצורך כך, קראו על המודול `_winreg` בפייתון, והתמקדו בפונקציות `OpenKey`, `QueryInfoKey`, `EnumValue`.
2. הוסיפו לתכנית אפשרות למחיקת ערכים מההיסטוריה.
3. הוסיפו לתכנית אפשרות לשתילת ערכים בהיסטוריה.