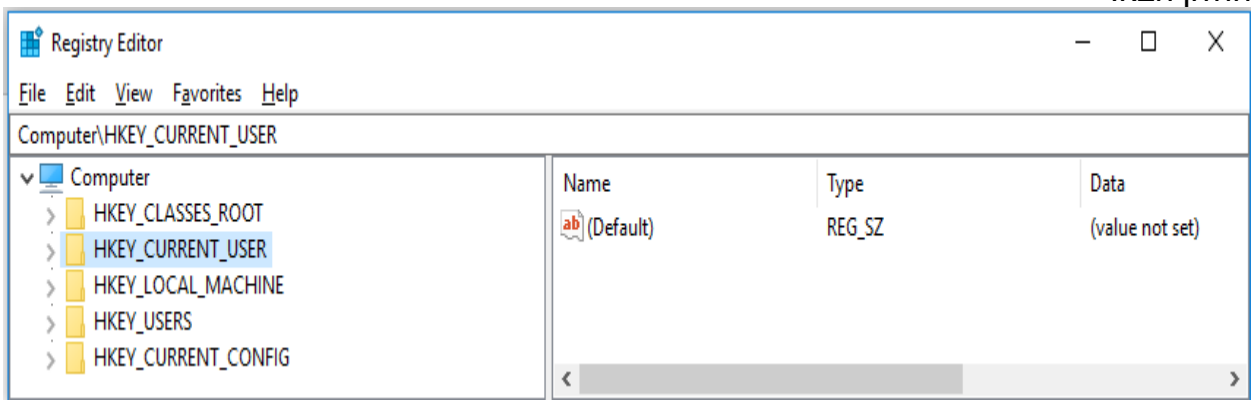
REGISTRY

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 ה – WinKey וכתיבת 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 :

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.

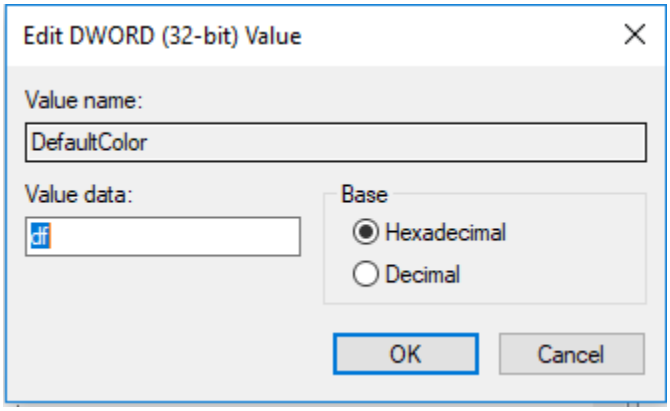
2. כעת חפשו את התיקייה *doc.* ובתוכה את *ShellEx* היכנסו לאחת התיקיות בתוכה ושימו לב למפתח שם(Default) ולערך "המוזר" בתוכו. ערך מהצורה
{84F66100-FF7C-4fb4-B0C0-02CD7FB668FE}
נקרא (Globally Unique Identifier) ומשמש כמזהה ייחודי.
3. ה GUID הזה למעשה מקשר אותנו למפתח Registry הנמצא במקום אחר! המטרה העיקרית 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?

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

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

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.



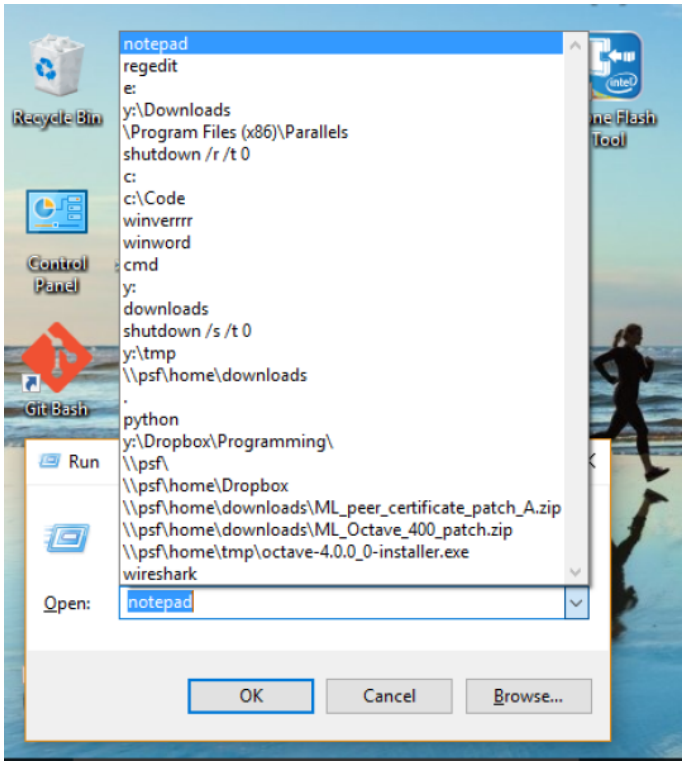
פתחו את חלון ה CMD השחור והאהוב (פתחו חלון חדש). מה קרה? (התשובה בעמוד הבא). ננצל את ההזדמנות
לעשות שימוש קצר ופשוט בפקודת : *Reg* הריצו בחלון שנפתח את הפקודה:
reg Query "HKEY_CURRENT_USER\Software\Microsoft\Command Processor"

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

משימה 3 : הריצו את ה- Task Manager. תחת הלשונית Startup ישנה רשימה של התוכנות אשר עולות עם עליית המחשב. הבאסה היא שלא ניתן להוסיף לשם ערכים. נסו לאתר את המקום אשר בו מוגדרות התוכנות ב registry והשוו הין הרשימות.

משימה 4 : פתחו את חלון ה-(WinKey+R) Run והריצו notepad.
פתחו שוב את החלון והריצו winword.
פתחו שוב את החלון ולחצו על החץ הקטן בצד, 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 תכנית בpython אשר מדפיסה למסך את כל ההיסטוריה של חלון ה-Run. לצורך כך, קראו על המודול winreg_ בpython, והתמקדו בפונקציות OpenKey, QueryInfoKey, EnumValue.
2. הוסיפו לתכנית אפשרות למחיקת ערכים מההיסטוריה.
3. הוסיפו לתכנית אפשרות לשתילת ערכים בהיסטוריה.

קרדיט
תומר גלון
עומר ברק