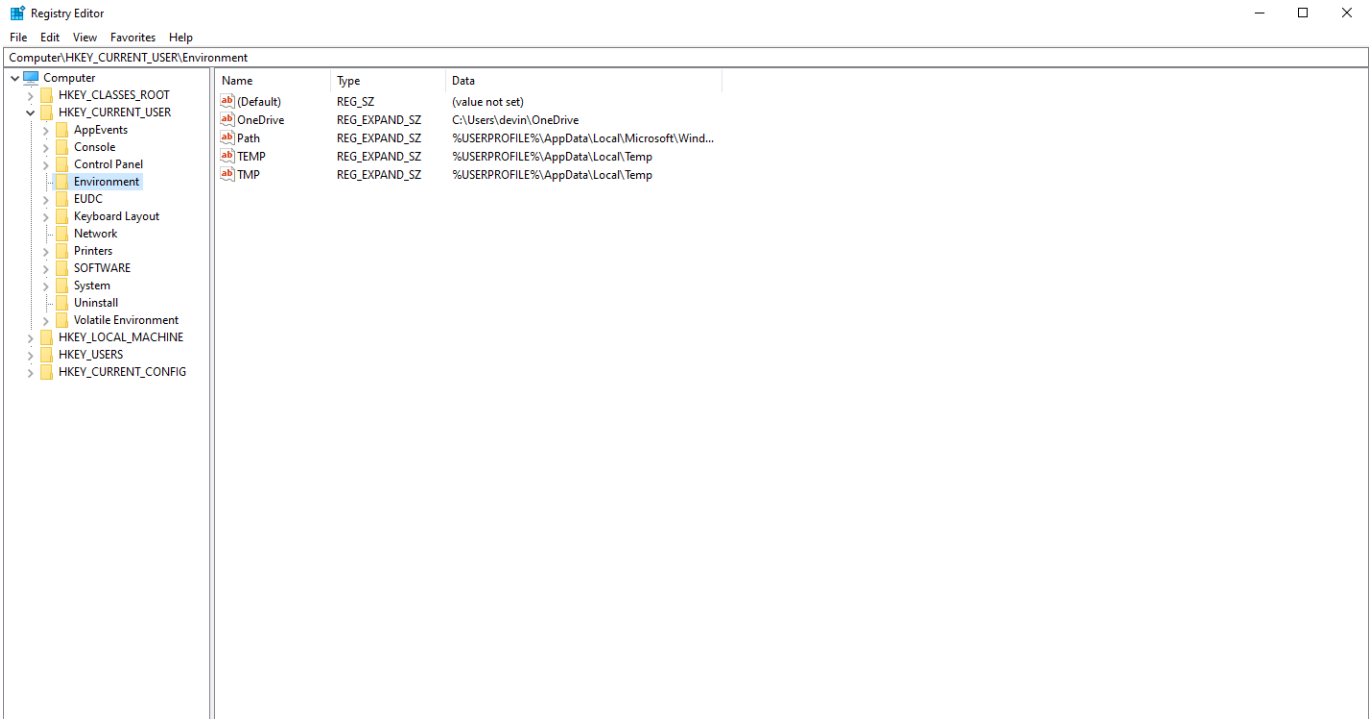
– Devin Rankin

Registry Key



- For this assignment I'll be using the Environment key.
- This key stores `REG_SZ` and `REG_EXPAND_SZ`. `REG_SZ` is a simple data string and `REG_EXPAND_SZ` is an expandable data string.
- Data strings cannot perform *string interpolation*, which is the act of embedding simple variable references (for example, `$var`), and expressions, whereas expandable data strings can.

Extracting the Key

- I used `reg_export` to successfully extract the key into my `Documents` folder.

```
C:¥Windows¥system32>reg export HKCU¥Environment C:¥Users¥devin¥Documents¥reg_export.txt
The operation completed successfully.
```

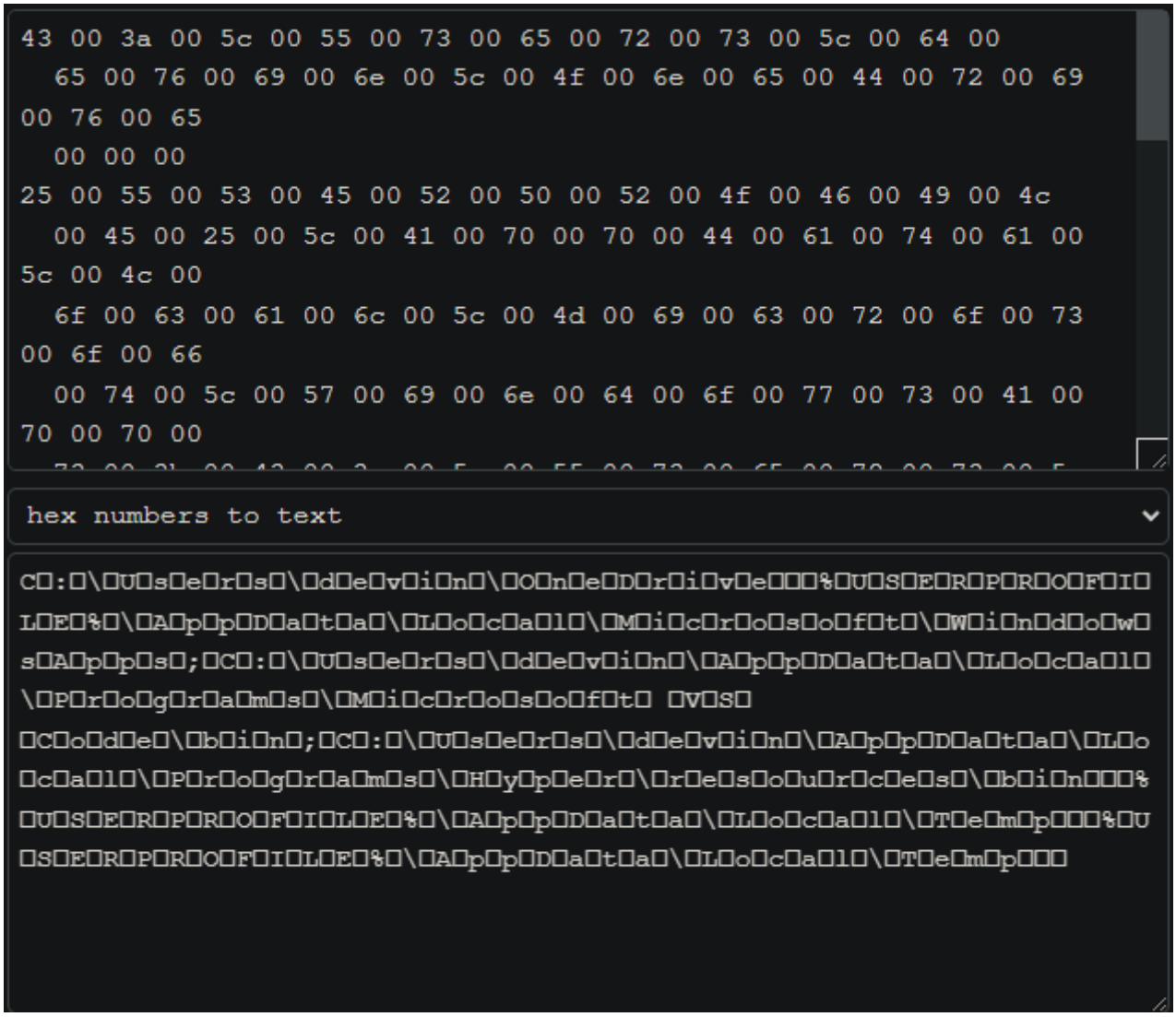
- I checked the data from the key extraction:

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Environment]
"OneDrive"=hex(2):43,00,3a,00,5c,00,55,00,73,00,65,00,72,00,73,00,5c,00,64,00,\
  65,00,76,00,69,00,6e,00,5c,00,4f,00,6e,00,65,00,44,00,72,00,69,00,76,00,65,\
  00,00,00
"Path"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,\
  00,45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,\
  6f,00,63,00,61,00,6c,00,5c,00,4d,00,69,00,63,00,72,00,6f,00,73,00,6f,00,66,\
  00,74,00,5c,00,57,00,69,00,6e,00,64,00,6f,00,77,00,73,00,41,00,70,00,70,00,\
  73,00,3b,00,43,00,3a,00,5c,00,55,00,73,00,65,00,72,00,73,00,5c,00,64,00,65,\
  00,76,00,69,00,6e,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,\
  4c,00,6f,00,63,00,61,00,6c,00,5c,00,50,00,72,00,6f,00,67,00,72,00,61,00,6d,\
  00,73,00,5c,00,4d,00,69,00,63,00,72,00,6f,00,73,00,6f,00,66,00,74,00,20,00,\
  56,00,53,00,20,00,43,00,6f,00,64,00,65,00,5c,00,62,00,69,00,6e,00,3b,00,43,\
  00,3a,00,5c,00,55,00,73,00,65,00,72,00,73,00,5c,00,64,00,65,00,76,00,69,00,\
  6e,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,6f,00,63,\
  00,61,00,6c,00,5c,00,50,00,72,00,6f,00,67,00,72,00,61,00,6d,00,73,00,5c,00,\
  48,00,79,00,70,00,65,00,72,00,5c,00,72,00,65,00,73,00,6f,00,75,00,72,00,63,\
  00,65,00,73,00,5c,00,62,00,69,00,6e,00,00,00
"TEMP"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,\
  00,45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,\
  6f,00,63,00,61,00,6c,00,5c,00,54,00,65,00,6d,00,70,00,00,00
"TMP"=hex(2):25,00,55,00,53,00,45,00,52,00,50,00,52,00,4f,00,46,00,49,00,4c,00,\
  45,00,25,00,5c,00,41,00,70,00,70,00,44,00,61,00,74,00,61,00,5c,00,4c,00,6f,\
  00,63,00,61,00,6c,00,5c,00,54,00,65,00,6d,00,70,00,00,00
```

Decoding the Data

- When decoding the data, I got these weird boxes between each character.



- However after pasting the data into `notepad++`, the strings appeared normally.

```
C:\Users\devin\OneDrive%USERPROFILE%\AppData\Local\Microsoft\WindowsApps
C:\Users\devin\AppData\Local\Programs\Microsoft VS Code\bin
C:\Users\devin\AppData\Local\Programs\Hyper\resources\bin
%USERPROFILE%\AppData\Local\Temp
%USERPROFILE%\AppData\Local\Temp
```

- The data converted is understandable because the `Environment` key holds absolute paths to specific variables such as `OneDrive`, `bin folders`, etc.