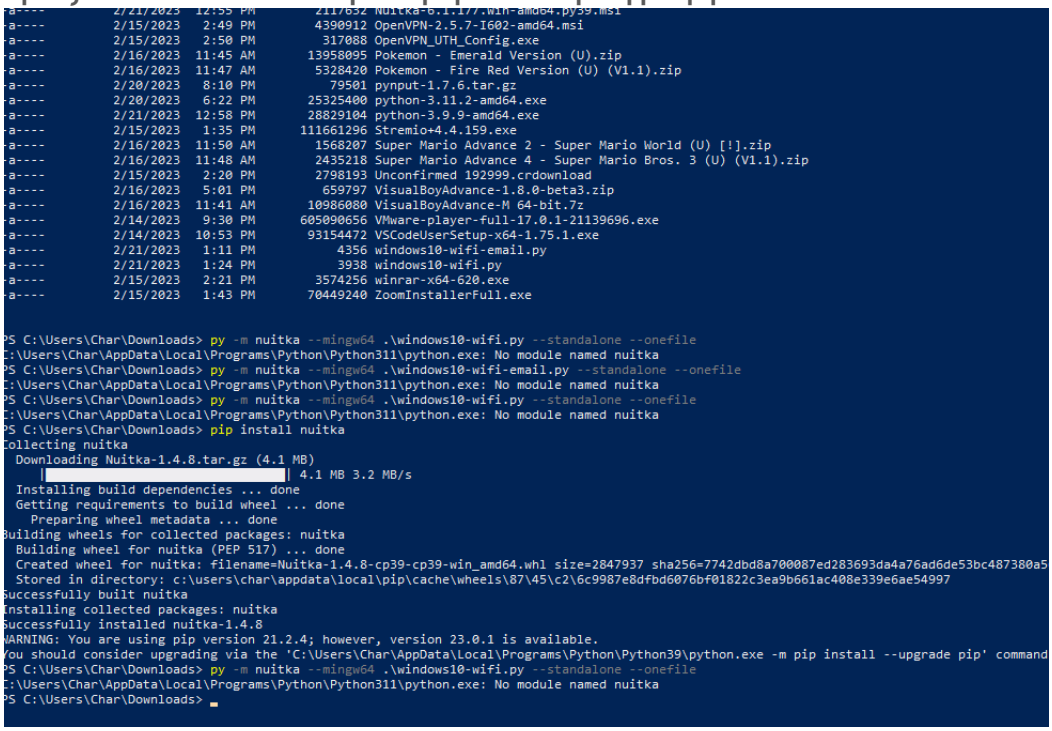
Κατασκευή Keylogger

- Προσπάθησα να το κάνω με **χρήση C#** όπως στα βίντεο:
  - How to Create a Keylogger that Sends Emails (C# 2021) | Simple Explanation + Demo
  - https://www.youtube.com/watch?v=4k2IQCQV9Kc&t=6s
- Μετά λόγω ευκολίας κώδικα αποφάσισα να το υλοποιήσω με **Python**.
- Έγραψα τον πρώτο κώδικα όπως το βίντεο: https://youtu.be/yvHrNlAF0Y0
- **Αποθήκευσα το αρχείο ως .pym και όχι ως .py για μεγαλύτερη προσβασιμότητα του προγράμματος στον υπολογιστή**.
- Με το που τελείωσα την σύνταξη του κώδικα το Windows Security ανάγνωρισε κατευθείαν το αρχείο ως ιό και το διέγραψε αυτόματα. Επομένως για αποφευχθεί αυτό κατά τη σύνταξη κώδικα αποφάσισα να απενεργοποιώ κάθε φορά το antivirus και να το ανεβάζω στο google drive για να μένει ασφαλής ο κώδικας.
- Άλλα παραδείγματα keylogger σε Python:
  - https://youtu.be/XKoTwepEzPI
  - https://youtu.be/8BiOPBsXh0g
  - https://www.youtube.com/watch?v=LBM3EzBXhdY&t=82s

- **Για να είναι εφαρμόσιμο το keylogger και σε υπολογιστές που δεν έχουν κατεβασμένη την Python αλλά και για να μην αναγνωρίζεται από το Windows Security χρειάζεται το αρχείο να γίνει executable.**
- Για να πετύχω αυτό τον σκοπό προσπάθησα να το κάνω compile μέσω **Nuitka** όπως το βίντεο: https://www.youtube.com/watch?v=qaZ-IbssPDI&t=749s (10:22

– 13:51). Υπήρξε όμως θέμα με την αναγνώριση του module παρόλο που ήταν κατεβασμένο στα downloads ενώ είχα στα windows κατεβασμένα την Python 9.9 που συνίσταται για να τρέξει σωστά το συγκεκριμένο πρόγραμμα.

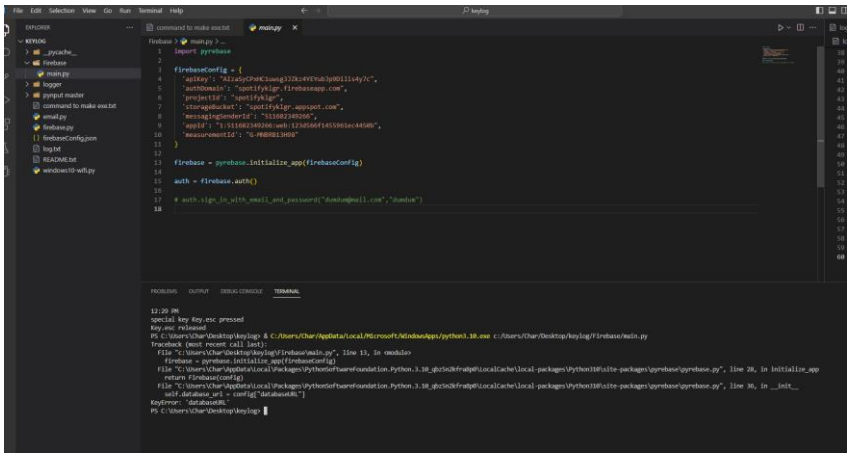


- **Προσπάθησα να γράψω κώδικα που στέλνει το αρχείο με το output του keylogger σε gmail** με τη βοήθεια κυρίως του chat gpt αλλά εμφανιζόντουσαν διάφορα errors τα οποία εκάναν δύσκολη τη σωστή χρήση των gmail libraries.
- Κώδικας για απόκτηση δεδομένων wifi: https://github.com/davidbombal/red-python-scripts/blob/main/windows10-wifi.py
- Μία άλλη μέθοδος για compile είναι η χρήση του **auto-py-to-exe** (https://youtu.be/Y0HN9tdLuJo), το οποίο κατάφερε στην αρχή να κάνει τον κώδικα με το wifi executable αλλά είχε θέμα με τα υπόλοιπα δύο αρχεία (keyboard input, email) και μάλιστα στο πρώτο αρχείο μου έβγαζε error για βιβλιοθήκη που δεν υπάρχει καθόλου στον κώδικα παρά στον κώδικα του email.
- Τελικά το πρόβλημα λύθηκε με τη χρήση του PyInstaller για compile χρησιμοποιώντας την εξής μέθοδο:

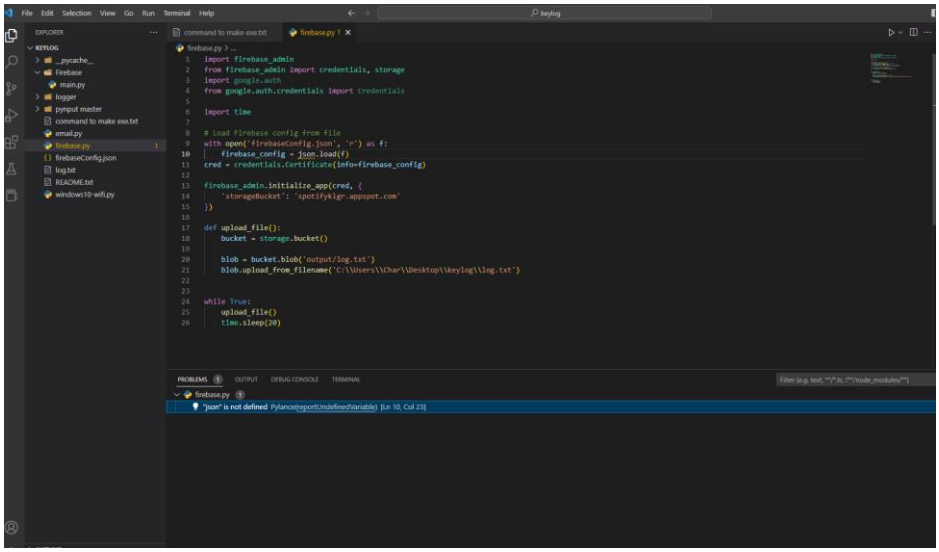
command to make exe.txt

```
1   Go inside python folder
2   Write cmd in the address bar
3   Use this command
4   PyInstaller --onefile --windowed --icon=app.ico logger.py
5   Exe file is located in the dist folder
```

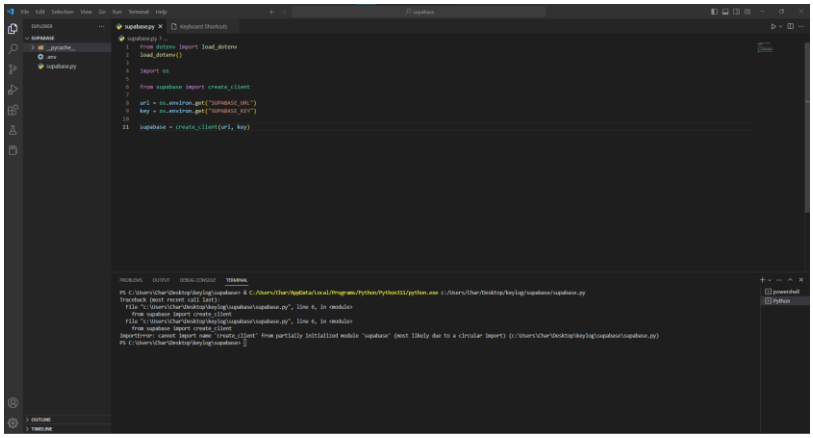
- Για την μεταφορά των δεδομένων από τον χρήστη σε μένα αποφάσισα να αφήσω τη χρήση του gmail και να χρησιμοποιήσω το **Firebase**. Για αυτό είδα τα βίντεο:
- https://youtu.be/mNMv3WNgp0c
- https://youtu.be/s-Ga8c3toVY
- Ωστόσο, υπήρξαν πάλι θέμα με την αναγνώριση των βιβλιοθηκών pyrebase, το οποίο λύθηκε με την διαγραφή της python 9.9 και upgrade της 10.10, η οποία ήταν ήδη κατεβασμένη, αλλά και της βιβλιοθήκης. Παρόλα αυτά, τα errors συνέχιζαν να εμφανίζονται παρόλο που κατέβασα το upgraded version (pyrebase4) και ακολούθησα τα βήματα του δεύτερου βίντεο.



- Με τη βοήθεια του chatgpt έφτιαξα έναν άλλον κώδικα, ο οποίος όμως έχει το θέμα ότι δεν αναγνωρίζεται η βιβλιοθήκη google.auth παρόλο που είναι κανονικά κατεβασμένη και updated.



- Αποφάσισα ως βάση δεδομένων να χρησιμοποιήσω το supabase και για αυτό είδα το βίντεο: https://www.youtube.com/watch?v=M6cfT2pgpSc&list=WL&index=62&t=4s
- Υπήρχε ένα bug στην αναγνώριση της βιβλιοθήκης dotenv το οποίο **λύθηκε με την αλλαγή του Python Interperter από το VS Code.**
- Ωστόσο τρέχοντας το αρχείο δημιουργήθηκε άλλο θέμα στην αναγνώριση της βιβλιοθήκης create_client όπως δείχνει η εικόνα:



- Τελικά δεν υπήρχε θέμα με την εκδοχή της python που χρησιμοποιώ (python 3.11) αλλά με **το όνομα του αρχείου που είναι ίδιο με το όνομα της βιβλιοθήκης, γι' αυτό και το circular import**.

- ‘Εφτιαξα κώδικα που ανεβάζει κάθε 15 δευερόλεπτα ένα txt αρχείο στο supabase (συγκεκριμένα για το log.txt) αλλά λόγω σφαλμάτων που εμφανίζονται άμα τον προσθέσω ως ξεχωριστό κώδικα το άφησα σαν δεύτερο επιπλέον αρχείο που θα λειτουργεί παράλληλα με το κύριο μέρος του keylogger.
- Το πρόγραμμα upload λειτουργεί κανονικά αν δεν υπάρχει ήδη στο supabase bucket αρχείο “log.txt” αλλιώς εμφανίζει error (**refresh error**).

Για βελτίωση του keylogger:

1) Το αρχείο upload να μπορεί να προσθεθεί στο logger χωρίς errors.
2) Φτιάξε το “refresh error” που αναφέρεις προηγουμένως.
3) Χρήση trojan horse. (https://youtu.be/eiT7mslA63c)
4) Να παίρνει δεδομένα του ποντικού.
5) Να παίρνει δεδομένα από κάμερα.
6) Αλλαγή των χαρακτήρων αναλόγως με τα special keys που πατιούνται.
7) Απόκρυψη των βοηθητικών αρχείων (πχ “.env”,”log.txt”).