

# Tudor-Gabriel VÎJIALĂ (78284) - Keylogger cu buton de rewind

Autorul poate fi contactat la adresa: **Login pentru adresa**

## Introducere

Un keylogger este un dispozitiv care se conectează între tastatură și calculator, cu rolul de a înregistra ce s-a tastat. Dispozitivul înregistrează parole de autentificare, detalii de carduri de credit, conversații private și alte detalii confidențiale etc.

Pentru proiectul la PM implementez un keylogger care funcționează pe interfața PS/2 și reține într-un buffer circular o secvență cu caracterele tastate de victimă.

## Descriere generală



Keylogger-ul va dispune de două mufe PS/2: una de intrare și una de ieșire. În modul normal de funcționare, acesta va repeta valorile pinilor de intrare, la ieșire, repetând semnalul. Keylogger-ul va memora ultimele câteva sute de caractere în memoria sa internă, fiind capabil să le retrimită prin mufa de ieșire la apăsarea butonului BTN din placa de bază.

## Hardware Design

### Lista de piese

Nu am nevoie de prea multe piese adiționale: voi lega pinii mufei PS/2 la GPIO, microcontrollerul având rol de repetor.

- placa de bază
- 2 conectori PS/2 (6 pini) - [Conex Electronic - CONECTOR MINI DIN MAMA PCB 6 PINI](#)
- convertor PS/2 → USB - [conectica.ro - Adaptor PS/2 la USB pentru tastatura](#)
- convertor USB → PS/2 - [conectica.ro - Adaptor USB la 2 X PS/2](#)
- tastatură PS/2 - [olx.ro](#)
- tastatură USB - [olx.ro](#)

## Schema electrică



Nimic mai simplu.

## Despre PS/2

Din conectorul PS/2 ne interesează două fire: DATA și CLK.

Comunicația este serială, sincronă și bidirecțională. Tastatura generează semnalul de ceas, iar calculatorul oprește comunicarea trăgând linia de ceas la masă.

Frecvența uzuală de ceas este 12.5khz.

## Despre cablaj

Am conectat mufele PS/2 folosind jumper-e legate direct la placa de bază. Toate sârmele sunt legate folosind alte sârme de găurile de suport ale plăcii de bază.

## Software Design

Dezvoltarea s-a realizat pe linux. La editarea codului sursă s-a folosit editorul vim, singura alegere corectă.

Pentru conducerea celor 2 mufe PS/2 se folosesc 4 pini de GPIO: un DATA și un CLK pe intrare, plus alți doi pini pentru ieșire.

În mare, microcontrollerul trebuie să:

- primească pe la intrare scan code-uriile PS/2 și să le stocheze într-un buffer
- citească caracterele noi din buffer și să le transmită prin mufa de ieșire
- rescrie buffer-ul la ieșire la apăsarea butonului BTN

## Scrierea datelor pe mufa PS/2

Pentru scriere, am folosit ca inspirație [acest articol](#) care se bazează pe delay-uri pentru a comuta atât ceasul cât și linia de date.

Pentru aplicația dată, am considerat că este satisfăcătoare o soluție care scrie la PS/2 folosind ca sincronizare delay-uri.

## Citirea datelor de pe mufa PS/2

Pentru citirea datelor de la mufa PS/2 am pornit de la [acest ghid de pe internet](#). Am folosit aceeași logică și eu, declanșată pe întreruperea PCINT a pinului de CLK.

## Redarea caracterelor stocate în RAM

Microcontrollerul trebuie să memoreze semnalele primite la intrare în ultima vreme într-un buffer intern, pentru a putea reda o secvență de caractere din nou la ieșire.

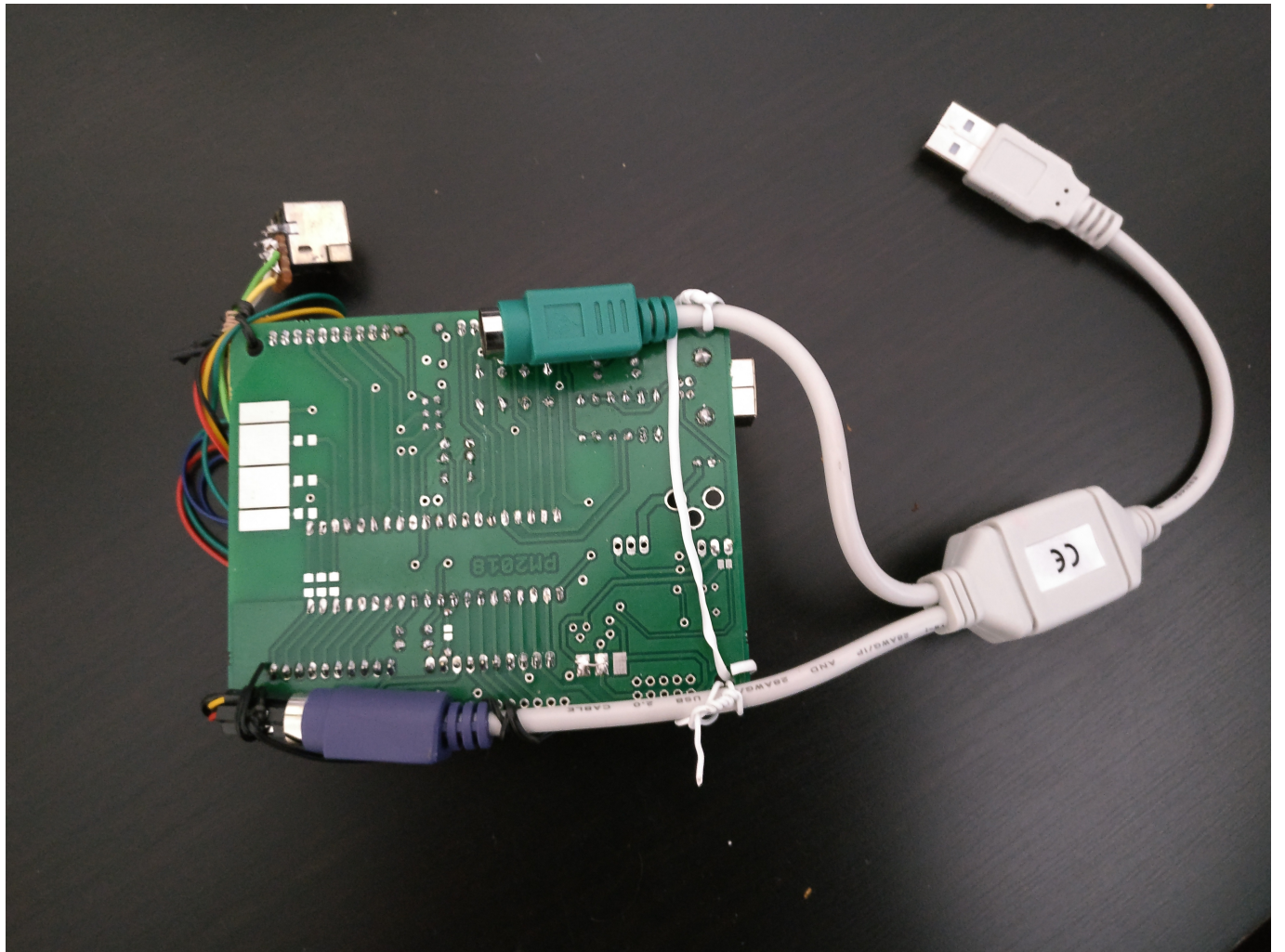
Pentru asta folosesc un buffer circular de 1kb, declarat ca memorie globală.

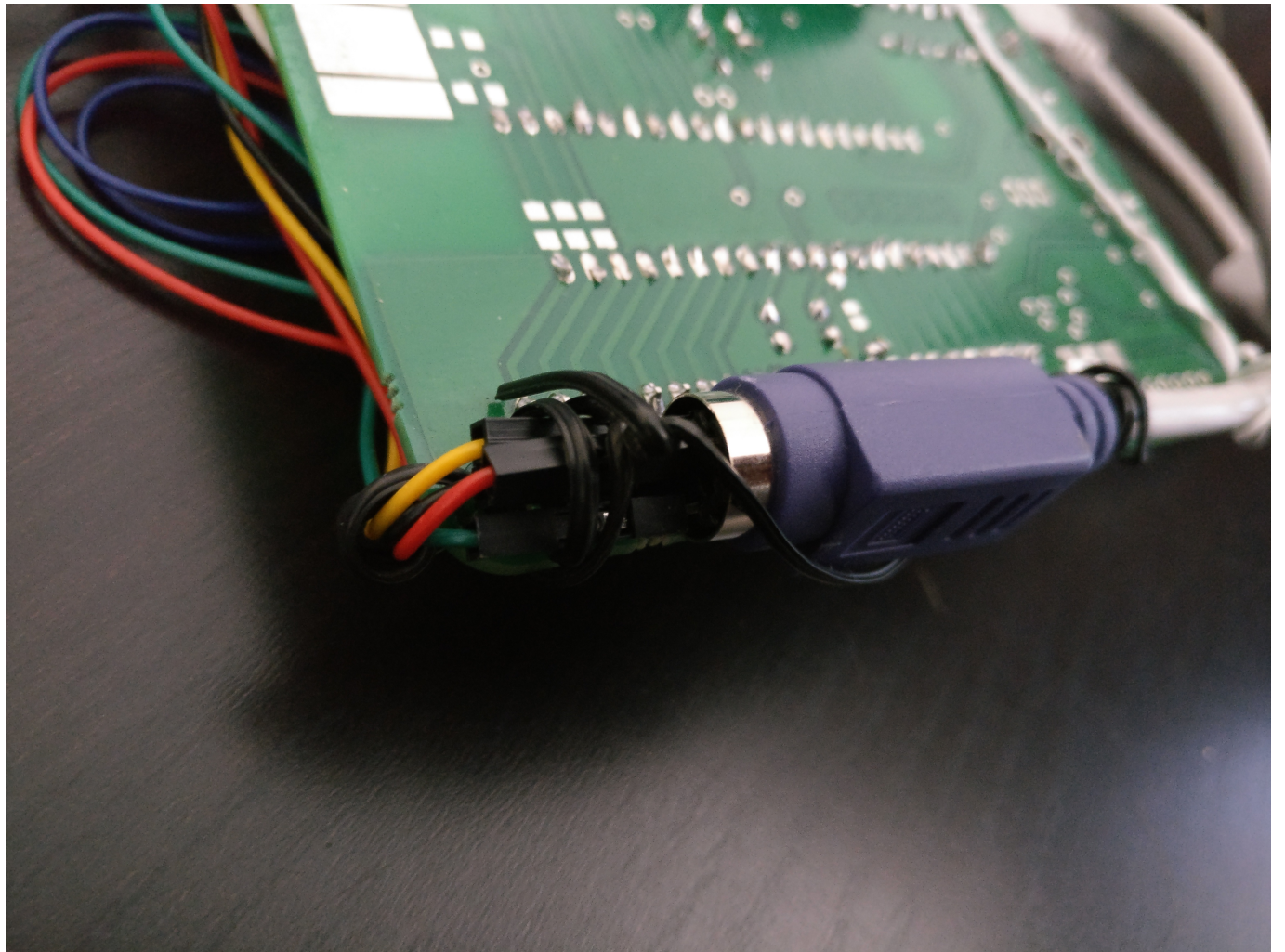
## Rezultate Obținute

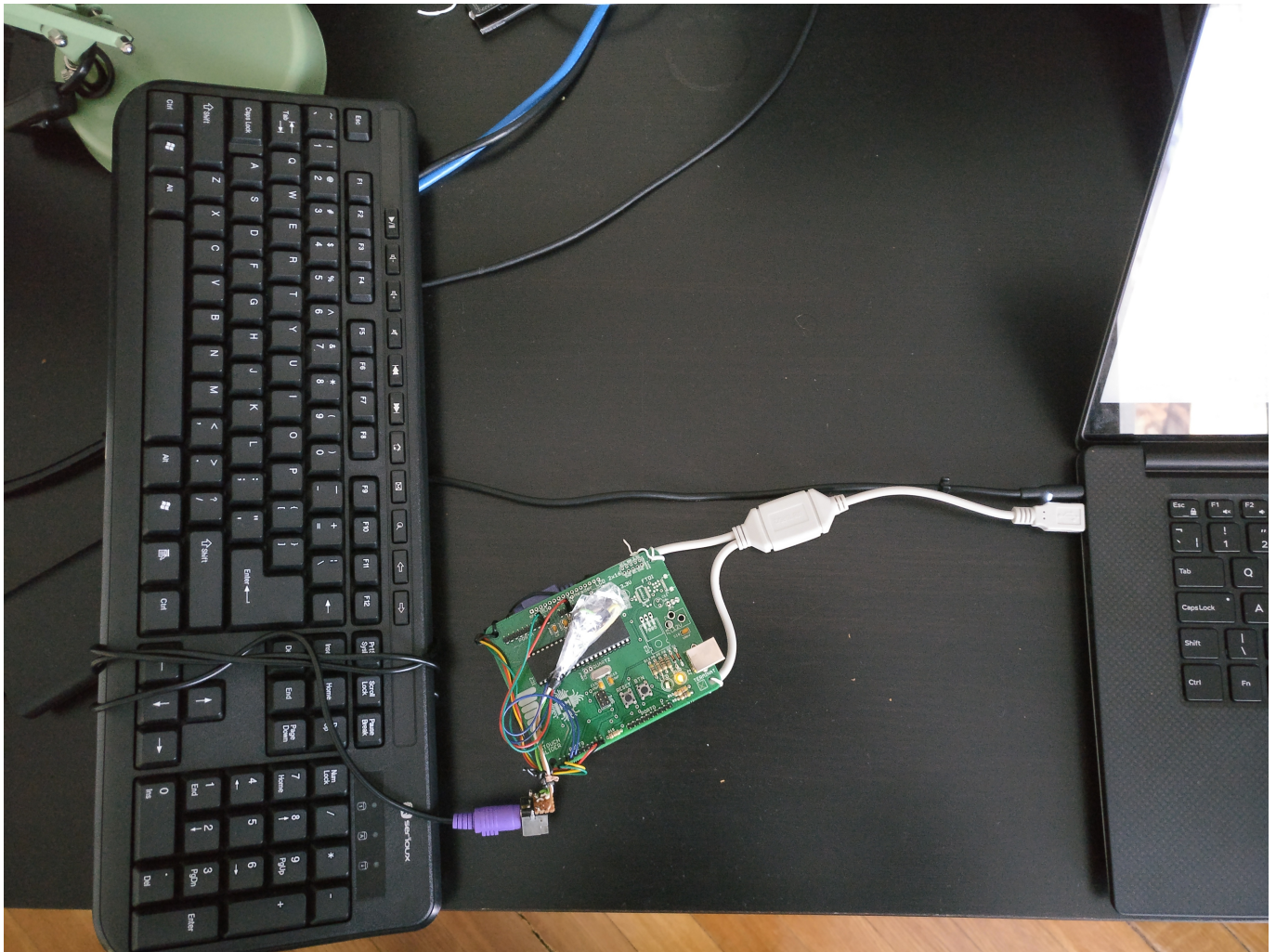
Am reușit să scriu o propoziție la tastatură, să apăs pe buton, și să o văd scrisă din nou pe ecran.

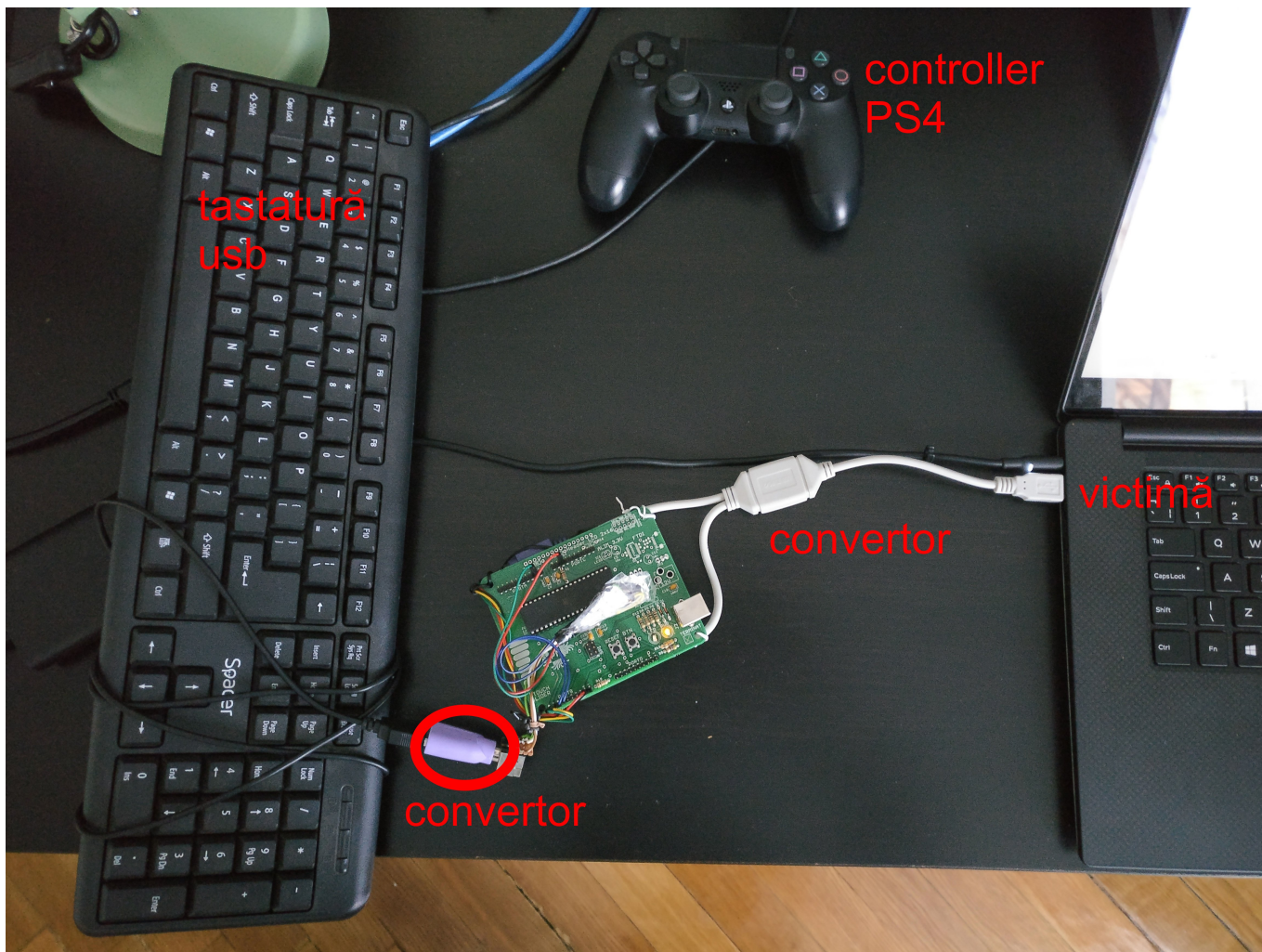
## Fotografii











## Concluzii

În concluzie, reamintim următoarele:

Deținerea sau confecționarea, fără drept, de mijloace specifice de interceptare ori de înregistrare a comunicațiilor se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.

-- Codul Penal, Art. 302, Alin. 6

Interceptarea, fără drept, a unei convorbiri sau a unei comunicări efectuate prin telefon sau prin orice mijloc electronic de comunicații se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă.

-- Codul Penal, Art. 302, Alin. 2

## Download

Descărcați arhiva proiectului de [aici](#).

Proiectul poate fi accesat pe [GitHub](#). Arhiva cu toate resursele este disponibilă [aici](#).

## Jurnal

- aprilie - început pagina de wiki
- 3 mai - cumpărat piesele
- 6 mai - schemă electrică
- 23 mai - finalizare proiect

## Bibliografie/Resurse

- [Explicații despre protocolul PS/2](#)
- [Ghid despre scrierea caracterelor la interfața PS/2](#)
- [Ghid despre citirea caracterelor de pe interfața PS/2](#)
- [Inspirație: proiect PM Raluca-Ștefania TROFIN, 2017](#)
- Documentația în format [PDF](#)

From:

<http://ocw.cs.pub.ro/courses/> - **CS Open CourseWare**

Permanent link:

<http://ocw.cs.pub.ro/courses/pm/prj2018/astatulat/tudor.vijiala>



Last update: **2021/04/14 15:07**