ABEL

Il sistema di build della nuova CAINE

Andrea Lazzarotto — andrealazzarotto.com

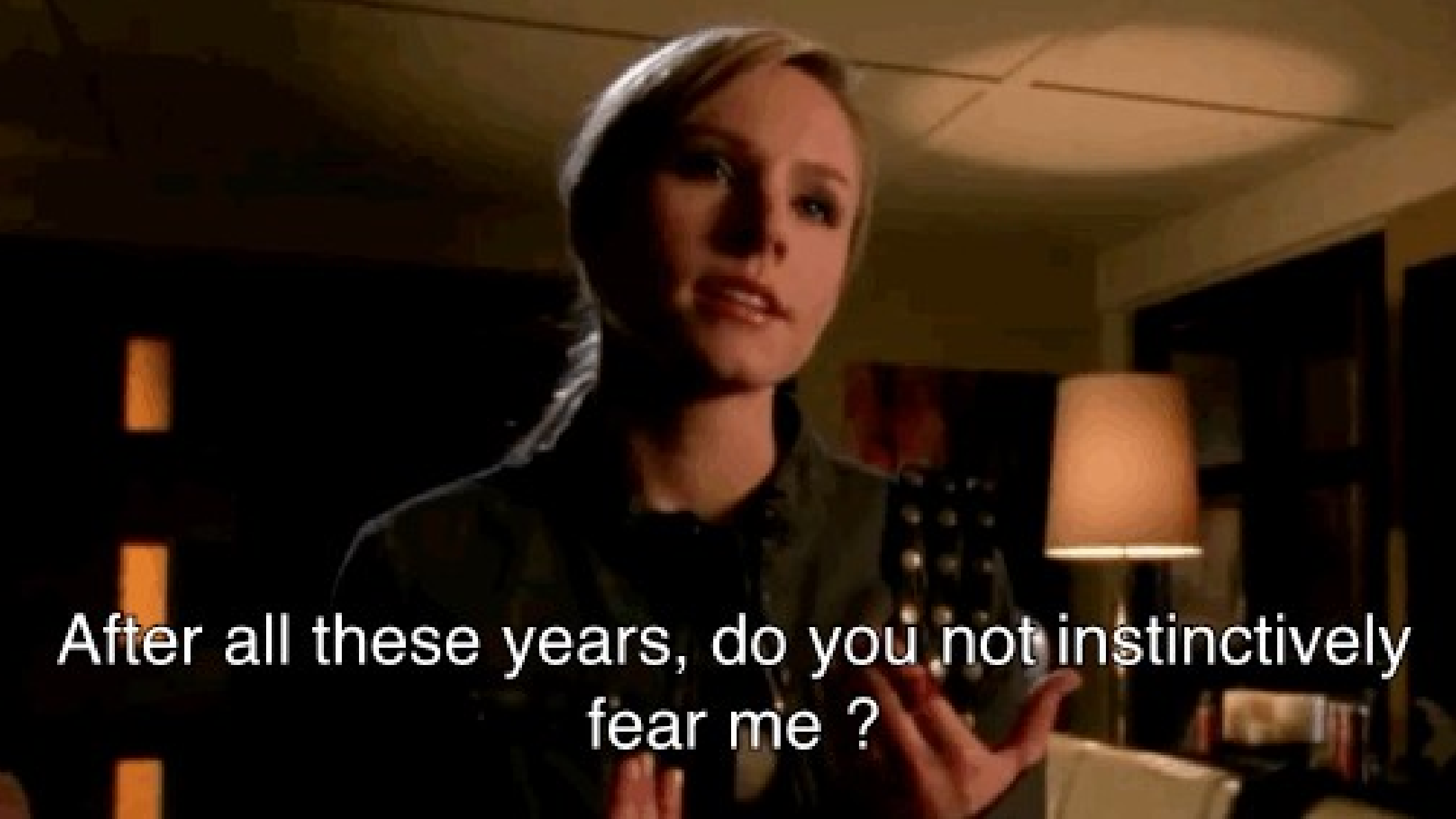
MI OCCUPO DI

- Informatica forense
- Sviluppo software
- RecuperaBit, Carbon14, CAINE

CAINE

- **2008:** Nata come tesi di laurea
- **2009:** Nanni Bassetti diventa maintainer
- **2017:** Esce la versione 9, contando ormai utenti e recensioni da tutto il mondo

Idea iniziale di Giancarlo Giustini


After all these years, do you not instinctively fear me ?

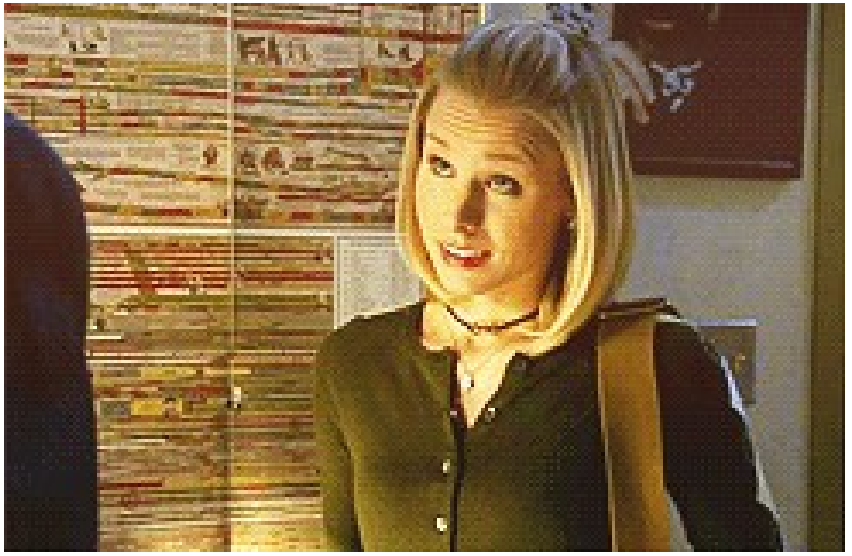
CAINE è uno strumento completo che comprende decine di tool e applicazioni forensi

Grazie a rbfstab e Mounter tutti i dispositivi sono bloccati in scrittura

Strumenti basati sul lavoro di John Lehr

Ci sono inoltre delle patch agli script di avvio per evitare montaggi

Alcune modifiche suggerite da Suhanov Maxim

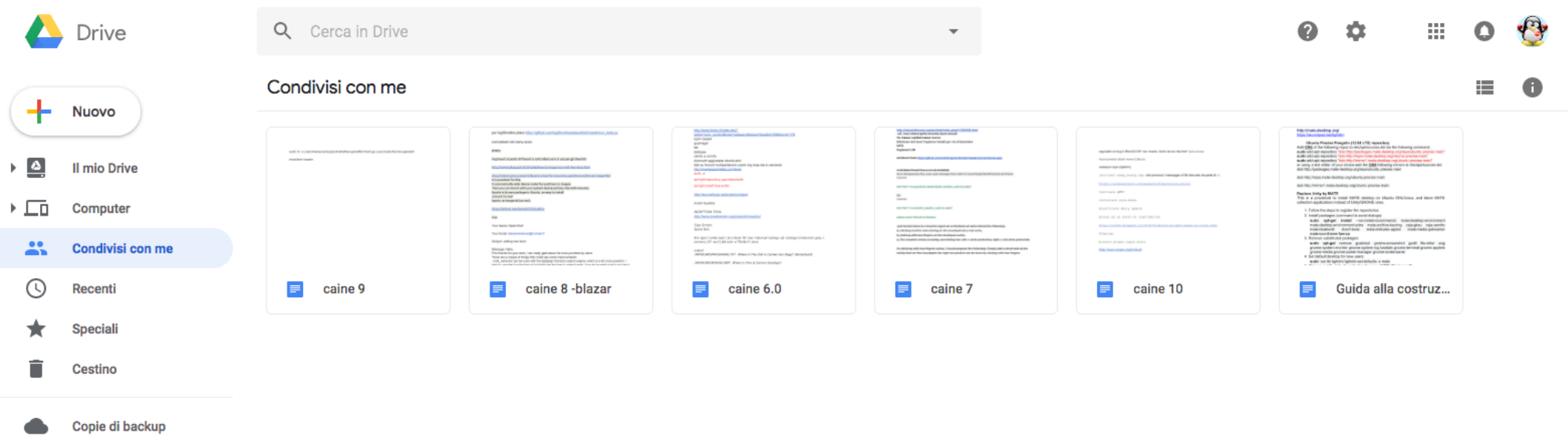


Purtroppo finora la distro è stata fatta a mano

… con Systemback

SVANTAGGI

Questo approccio è poco ordinato ed è facile commettere errori



Diventa difficile tenere traccia delle modifiche

Non si può suddividere lo sviluppo

Per non parlare di eventuali bug report,
che vengono **inviati per email** a Nanni


Down, boy. Relax, I've got it covered.

IDEA

Ho pensato di automatizzare e rendere tracciabile tutto il processo.

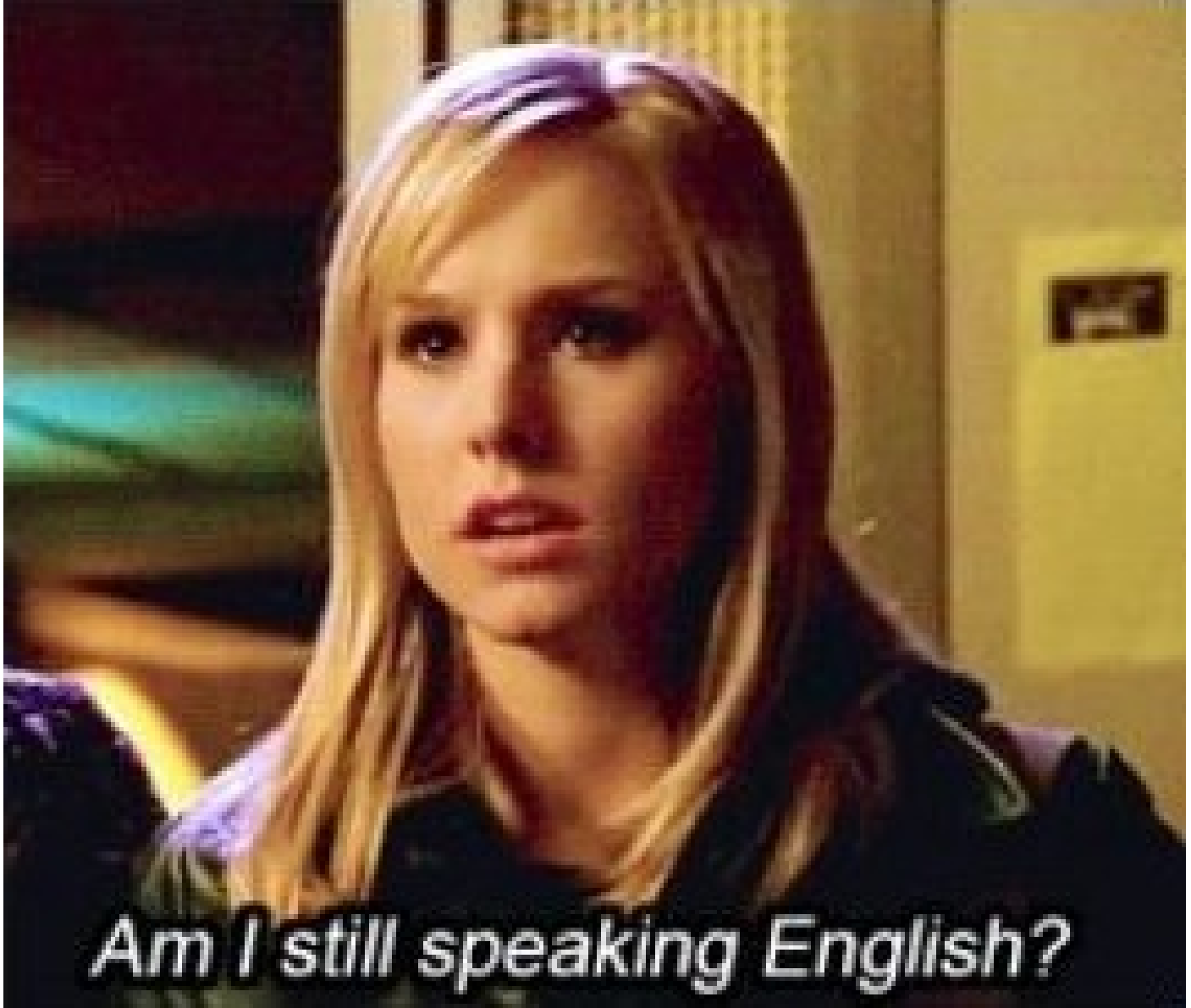
L'ispirazione è stata una parola molto brutta, e la sto per dire…

DevOps

(scusatemi per l’imprecazione)

PROPOSTO AL TEAM DI DEFT

- Bla bla… e quindi avresti tutto tracciato.
- Bello! Però boh abbiamo sempre fatto così…
- Ma avete sempre il problema che uno fa tutto.
- Vero, boh… sento gli altri, ti so dire…


Am I still speaking English?

POI AL TEAM DI CAINE

- A maggio nasce la prima bozza di Abel (*Automated Build Environment Lab*)
- Basato su Vagrant per racchiudere l'ambiente dentro a **una VM conosciuta e riproducibile**
- Utilizza Customizer su Ubuntu 16.04

La prima demo di Abel aggiornava tutti i pacchetti con APT

STRUTTURA DI ABEL

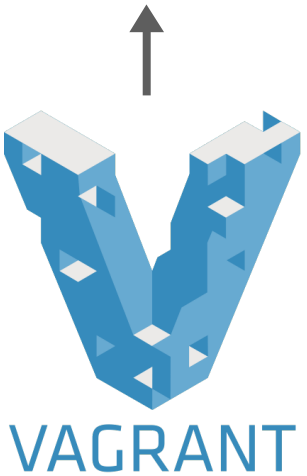
bin / abel

environment /

- base.iso
- branding.sh
- customizer.conf
- hook.sh
- **launchers /** generate.py
- Makefile
- overlay.sh
- **scripts /** ...

Vagrantfile

Processo di build automatizzato con Makefile e cartella script



Provision tramite Vagrantfile (Ubuntu 16.04 + Customizer)

MAKEFILE

Il comando abel esegue un Makefile

```
all: extract hook rebuild clean

extract:
    sudo customizer --extract

hook:
    /environment/overlay.sh
    sudo customizer --hook

rebuild:
    sudo /environment/branding.sh
    sudo customizer --rebuild
    sudo mv /home/*.iso /environment

clean:
    # More runs could be needed because it fails sometimes
    while true; do if sudo customizer --clean; then break; fi; done

chroot:
    sudo customizer --chroot
```


TA-DA!


THIS FACE
RIGHT HERE:
MY OVER-
THE-MOON
FACE

FINCHÉ NON SI È ROTTO TUTTO

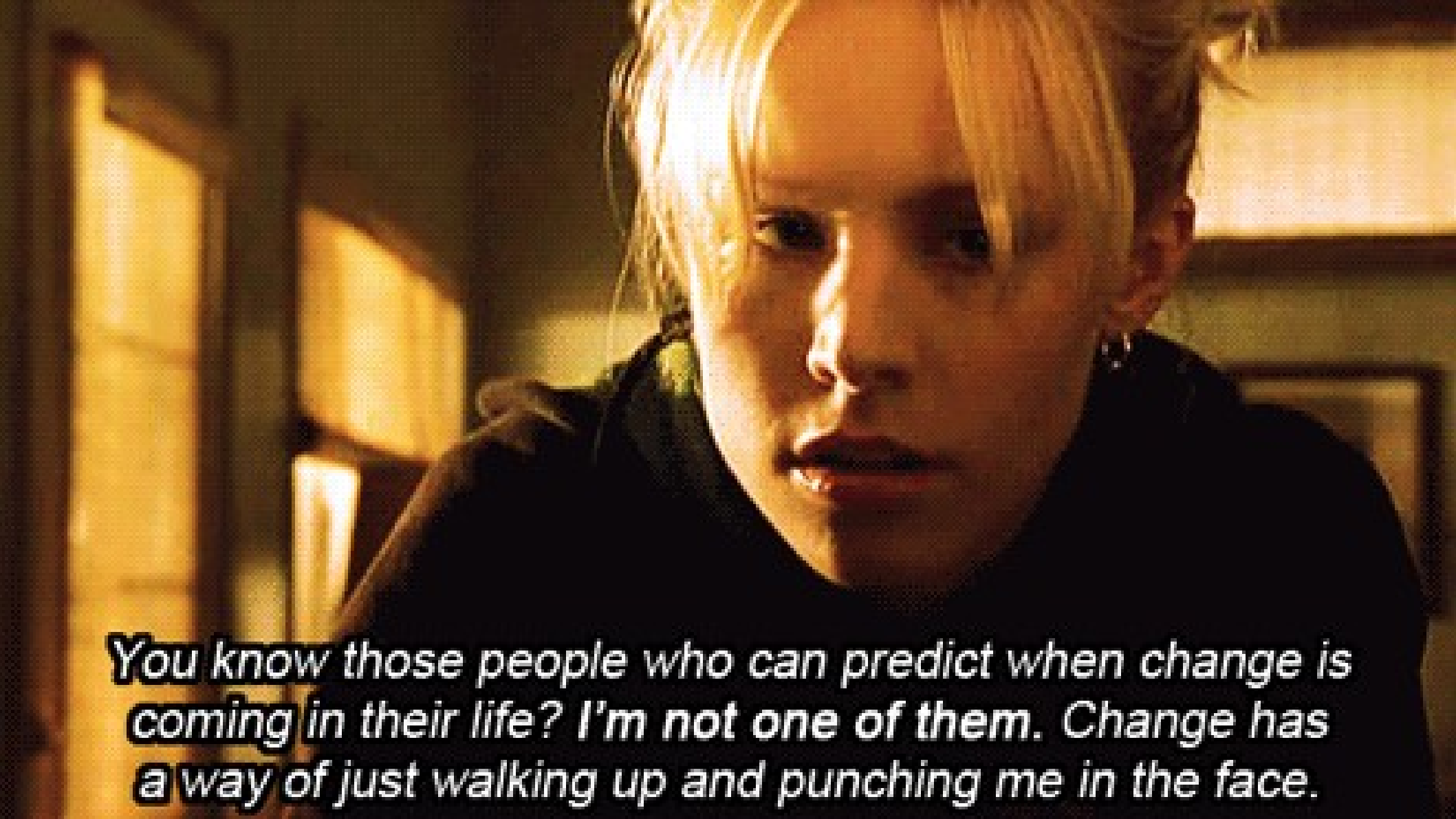
Un bel giorno la build ha smesso di funzionare…

Ubuntu ha rilasciato un kernel che usa una compressione diversa dai precedenti!


WHY DO
YOU INSIST
ON
PISSING
ME OFF?

MORALE

- Reinstallare il kernel (nella ISO non è completo) e fissarlo con apt-mark
- **Usare sempre versioni fisse** dei programmi che non sono nei repository
- Testare, testare, testare


You know those people who can predict when change is coming in their life? I'm not one of them. Change has a way of just walking up and punching me in the face.

PERSONALIZZAZIONI

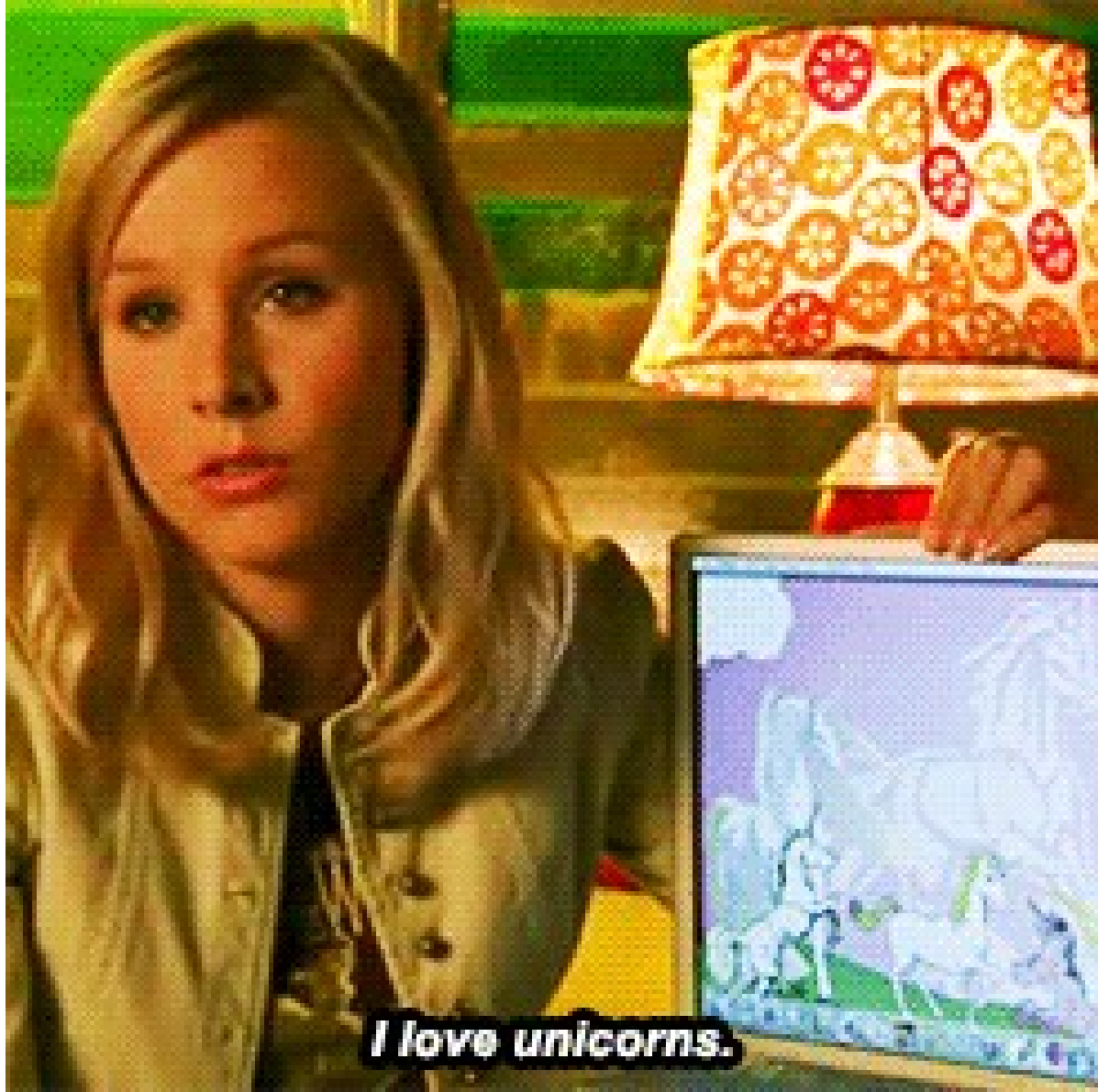
Tramite gli script possiamo installare tutti i pacchetti desiderati

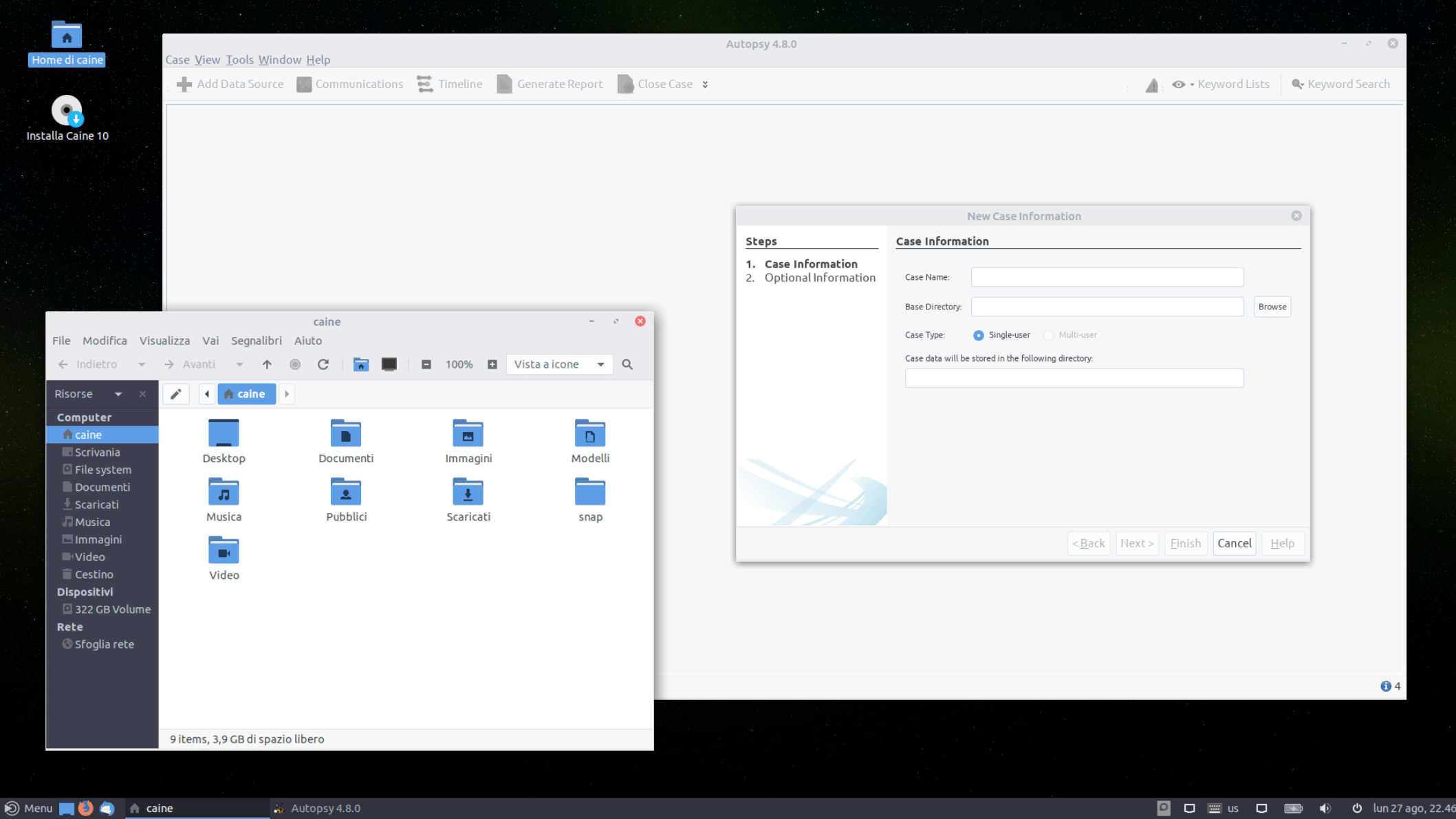
Scarichiamo e incorporariamo programmi già compilati come Autopsy

Applichiamo le patch forensi alla ISO

Creiamo i lanciatori (icone nel menu) con un pratico script Python

Cambiamo tema, sfondo e icone in /etc/skel




Home di caine
Installa Caine 10
Autopsy 4.8.0
Case View Tools Window Help
Add Data Source
Communications
Timeline
Generate Report
Close Case
Keyword Lists
Keyword Search
caine
File Modifica Visualizza Vai Segnalibri Aiuto
Indietro
Avanti
100%
Vista a icone
Risorse
caine
Computer
caine
Scrivania
File system
Documenti
Scaricati
Musica
Immagini
Video
Cestino
Dispositivi
322 GB Volume
Rete
Sfoglia rete
Desktop
Documenti
Immagini
Modelli
Musica
Pubblici
Scaricati
snap
Video
9 items, 3,9 GB di spazio libero
New Case Information
Steps
1. Case Information
2. Optional Information
Case Information
Case Name:
Base Directory:
Browse
Case Type:
Single-user
Multi-user
Case data will be stored in the following directory:
< Back
Next >
Finish
Cancel
Help
Menu
caine
Autopsy 4.8.0
us
lun 27 ago, 22.46

VANTAGGI

- La ISO viene prodotta in modo totalmente automatizzato, tracciabile e *peer-reviewed*
- Più persone possono lavorare allo sviluppo
- I miglioramenti si fanno con gli script

```
vagrant up
vagrant ssh
abel
```