GIUGNO 2023

Progetto ELSA - Efficient and Lightweight System Analyzer

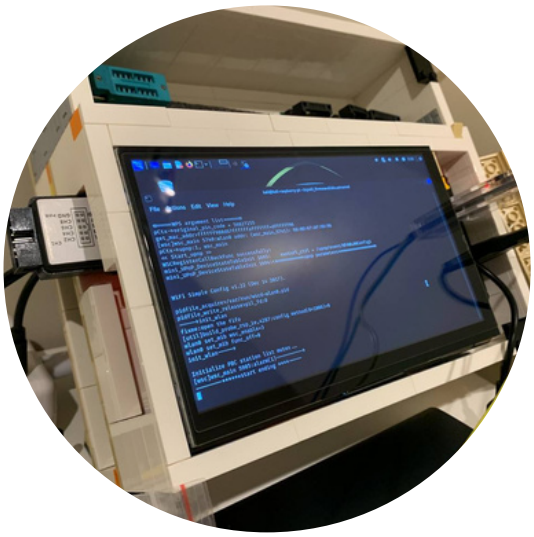
PROPOSTO DA

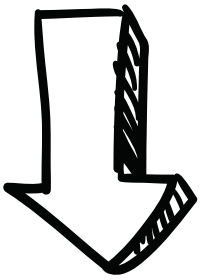
Giuseppe Compare

HARDWARE BOX TESTING STATION

PROGETTO

Questo progetto mira alla realizzazione di una box All-In-One portatile per effettuare Penetration Test Hardware/Software. In questo modo, con una semplice valigetta, è possibile viaggiare con la massima comodità ed avere sempre tutto a portata di mano.





CICLO DEL PROGETTO

01

RACCOLTA INFORMAZIONI

In una prima fase sono state raccolte tutte le informazioni inerenti i tool principali utilizzati da un penetration tester (hardware/software)

02

REALIZZAZIONE PROTOTIPO

Tramite l'utilizzo dei Lego è stato possibile iniziare a creare un primo prototipo funzionante in modo da testare direttamente il prodotto e applicare i dovuti miglioramenti ove previsto

03

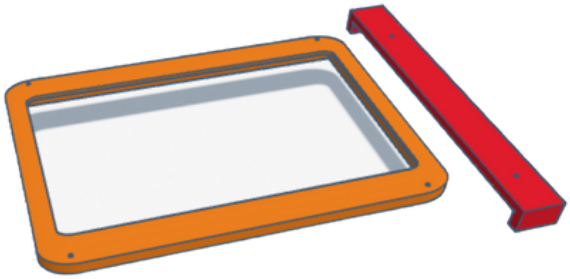
DISEGNO 3D

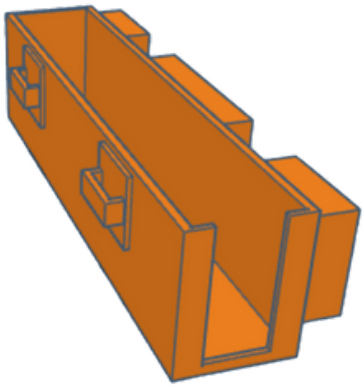
Sviluppo e messa in opera del progetto 3D per la realizzazione di un modello operativo

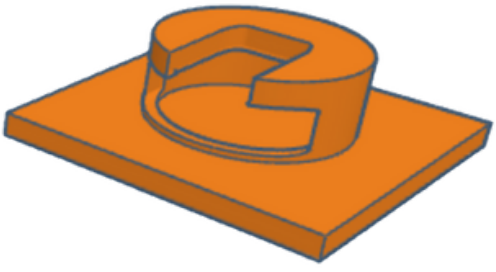
04

SVILUPPO CONTINUO

Miglioramenti continui del prodotto







TOOL UTILIZZATI

01

SISTEMA OPERATIVO

Kali Linux

02

SOFTWARE PENTEST

Tutti gli strumenti messi a disposizione di Kali Linux.

03

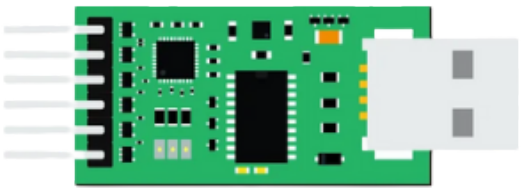
HARDWARE PENTEST

FT232RL (per analizzare la UART), CH341A (per analizzare SPI), Bruschetta Board (All-in-One analisi hardware made by Luca Bongiorni), Multimetro, Saldatore, filo di stagno, filo di rame, Pogo Pins (per interagire con la board), supporto magnetico, punte aggiuntive saldatore, cavi di collegamento, adattatori vari

04

SOFTWARE AGGIUNTIVO

Python GUI interface per agevolare i test. Una semplice ed intuitiva interfaccia grafica per accedere ai tool più utilizzati per l'hardware penetration test.



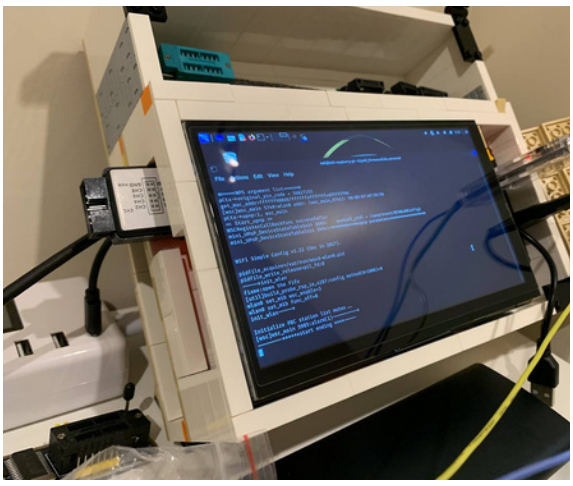
PRIMO PROTOTIPO

PROTOTIPO LEGO

Il primo prototipo prodotto mi ha consentito di verificare quali fossero le migliori soluzioni per una corretta progettazione. Grazie a questa tipologia di approccio mi è stato possibile sperimentare direttamente sul campo, senza perdite di tempo, il prodotto finale. Infatti tutto il "case" e le strutture di supporto sono state progettate utilizzando i lego. Quando una parte della struttura non era utilizzabile o presentava rischi strutturali veniva semplicemente sostituita. Utilizzare direttamente il modello 3D avrebbe richiesto molto più tempo in quanto i tempi di stampa sarebbero stati molto più lunghi. Ad esempio per un case grande con determinate caratteristiche ci sarebbe voluto almeno 1 giorno di stampa, oltre al fatto che ogni eventuale modifica avrebbe richiesto una ristampa di tutto il prototipo.

Il prototipo prevedeva l'utilizzo di una raspberry pi 3B+. La modalità del prototipo era pensata per uno sviluppo stile "tablet". Sotto lo schermo veniva posta la Raspberry Pi ed il logic analyzer che fuoriusciva dal lato frontale

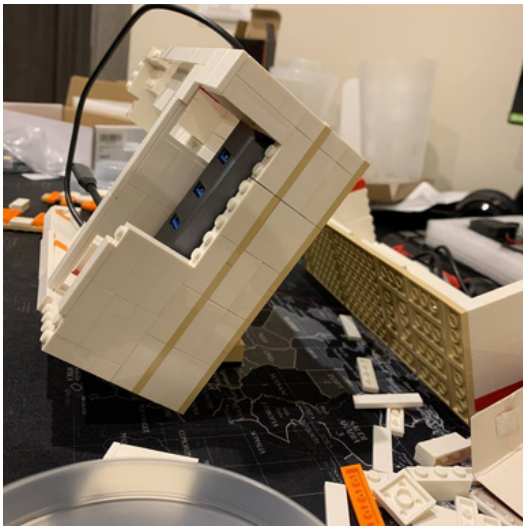
Nella parte posteriore erano presenti, in un vano, tutti gli accessori e adattatori principali: Multimetro, adattatori SPI, UART. Sulla destra, in un altro vano, erano presenti tutte le porte USB per poter utilizzare i vari tool. In una fase successiva il Logic Analyzer è stato spostato sulla sinistra per praticità

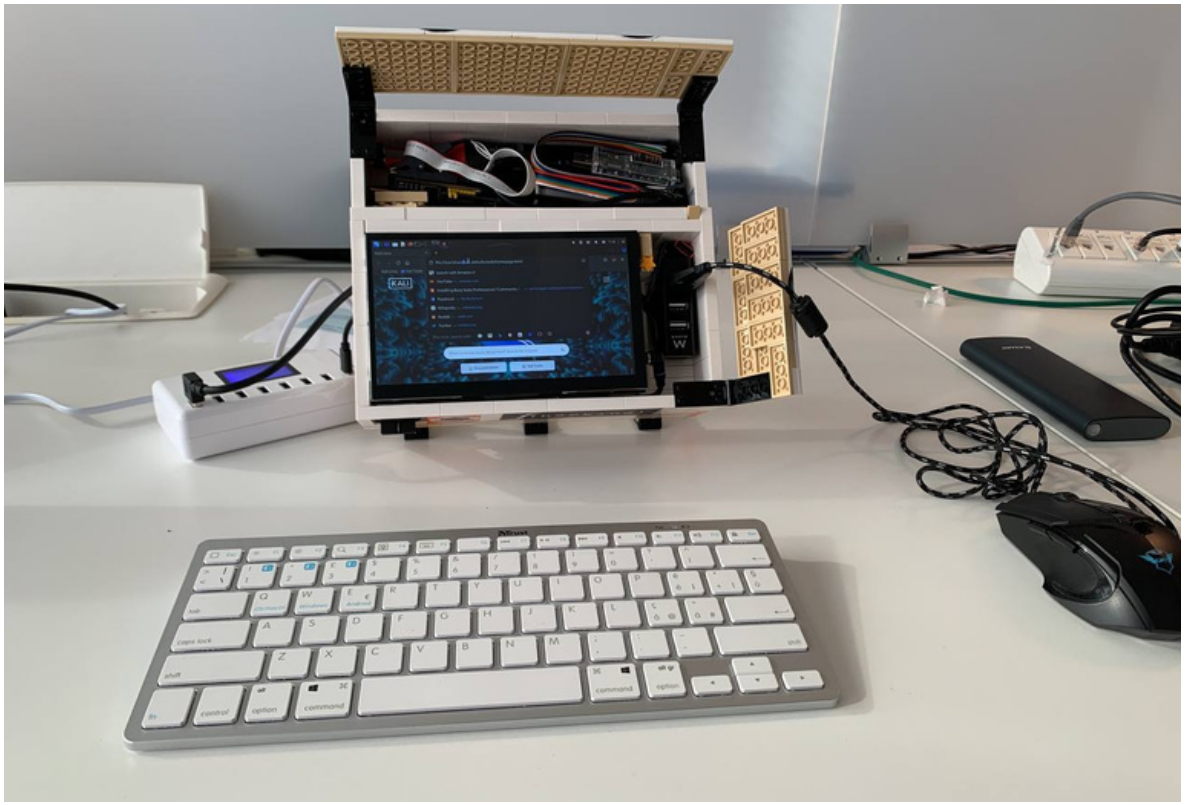


PRIMO PROTOTIPO

Il primo prototipo non permetteva il corretto inserimento di una tastiera e di una base magnetica per fissare i device da testare. Sotto al raspberry pi era presente una batteria portatile che consentiva l'utilizzo del prodotto in qualsiasi situazione

Per poterlo utilizzare al meglio è stato inserito un supporto sul retro del prodotto in modo da poterlo utilizzare anche in modalità "PC". Al primo prototipo mancava quindi: la base magnetica per fissare i device, il saldatore, la tastiera, il mouse. Questo ha portato alla realizzazione di un secondo prototipo in grado di raccogliere tutte queste informazioni





SECONDO PROTOTIPO

Il secondo prototipo è stato pensato come un mini pc completamente funzionante e completo. Oltre ad aggiungere le caratteristiche mancanti del primo prototipo, ha permesso l'inserimento anche di un kit completo di cacciaviti magnetici di precisione

Inoltre è stato possibile aggiungere un kit All-In-One per l'hardware penetration test sviluppato da Luca Bongiorni (whid.ninja). Questo tool è in grado di analizzare UART a diversi voltaggi (1.8V-5V), JTag, SPI, I2C. Inoltre ci sono dei jumper che consentono l'utilizzo della board in alcune situazioni particolari. La board al momento della stesura di questo documento non è ancora in commercio

SECONDO PROTOTIPO

Prodotti Utilizzati

Il prodotto principale utilizzato per realizzare questo prototipo è sicuramente la BOX. Le misure sono 27x24,5x13. Le misure sono perfette da permettere l'inserimento della base magnetica, del saldatore e di tutti i tool necessari per effettuare i test Hardware

Il kit completo di cacciaviti magnetici posto sul lato sinistro della Box, consente, tramite un carrellino estraibile, l'utilizzo di qualsiasi forma per poter interagire con i vari target. Ad esempio per estrarre la scheda da una cover, per svitare supporti che nascondono punti cruciali della scheda e tanto altro

La Bruschetta Board, creata da Luca Bongiorni, è una All-In-One board, creata per poter analizzare correttamente SPI, UART, I2C, JTAG. Uno strumento davvero utile in quanto evita di dover utilizzare più schede e tool per effettuare hardware test

La tastiera pieghevole con il mouse integrato consente di avere sempre a disposizione tutto l'occorrente per utilizzare il sistema operativo senza intoppi. La tastiera è ricaricabile ed utilizza la connessione bluetooth

SECONDO PROTOTIPO

Prodotti Acquistati

Le fascette di diversa lunghezza consentono il corretto inserimento di alcuni componenti e la facilità di rimozione degli stessi. Vengono utilizzati sia internamente, per i vari tool, sia esternamente per batteria e tastiera

La mini scheda wireless fornisce il giusto supporto wifi in caso di problemi di compatibilità tra sistema operativo e single board computer utilizzato per la Box. Ha una capacità media ottima per il tipo di applicazione. Nel dettaglio è Dual-Band 600Mbps

La cavetteria ruotabile consente un corretto inserimento di cavi senza creare punti di rottura evitando quindi interruzioni improvvise. Infatti questo tipo di cavi si adattano bene alla box e agli spazi stretti che si creano all'interno

I pesetti sono stati utilizzati per bilanciare la BOX quando tutti i tool vengono rimossi dal suo interno, dato che, nella parte superiore, è presente uno schermo che la rende più pesante e potrebbe farla cadere

SECONDO PROTOTIPO

Prodotti Acquistati

La batteria da 65W e 20000 mAh consente di alimentare non sono il single board computer ma anche il monitor ed il touch screen. Consente un utilizzo prolungato della box in assenza di corrente.

Il cavo di ricarica a Molla a Spirale, 12V 5A è importante per collegare il single board computer alla batteria in modo da consentire la corretta alimentazione dello stesso.

L'adattatore HDMI ad angolo sinistro e ad angolo retto con connettore HDMI 2.1 consente il corretto collegamento del monitor con il single board computer, senza creare rotture o piegamenti del cavo

L'hub USB a 4 porte, viene utilizzato per collegare i vari dispositivi per effettuare i test hardware. La porta collocata nella parte superiore viene utilizzata per il collegamento della mini pendrive wifi

SECONDO PROTOTIPO

Prodotti Acquistati

Lo schermo utilizzato è uno schermo touch-screen da 7" IPS HD. Grazie alla luminosità e alla qualità di questo schermo è possibile utilizzare il PC anche se non si dispone di uno schermo più grande

Il Single Board prescelto è stato il NiPoGi Mini PC Stick con 8 GB di ram DDR4, processore Intel Celeron N4000 e con Windows 10 Pro preinstallato, 128 GB di ROM e supporto 4K HDMI, Bluetooth e Dual band WiFi. Su questo dispositivo è stata installata una distro Kali Linux

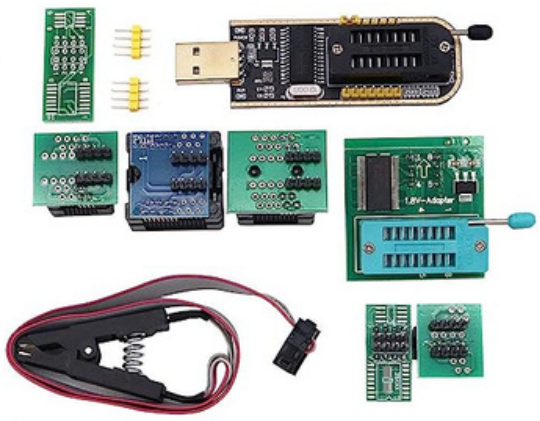
Gli adesivi 3M VHB hanno permesso la corretta adesione dei pezzi stampati con la stampante 3D all'interno del BOX. In alcuni casi si è reso necessario l'utilizzo di alcune viti aggiuntive per supportare meglio la struttura. In particolare il supporto batteria necessità l'utilizzo di viti per evitare lo scollamento della stessa a causa del peso eccessivo

SECONDO PROTOTIPO

Prodotti Acquistati

Tutti i supporti aggiuntivi sono stati stampati utilizzando un PLA+ di colore nero della Sunlu. Questo PLA è molto resistente e si adatta bene alla BOX. La stampante utilizzata con questo prodotto è la Anycubic Kobra Neo. Solitamente si usano 72 gradi per il piatto e 220 per l'estrusore

DSD TECH SH-U09C5 convertitore UART, da USB a TTL con supporto per chip FTDI 5V 3.3V 2.5V 1.8V. Questo dispositivo consente di interagire con la UART, debug interface, a diversi voltaggi



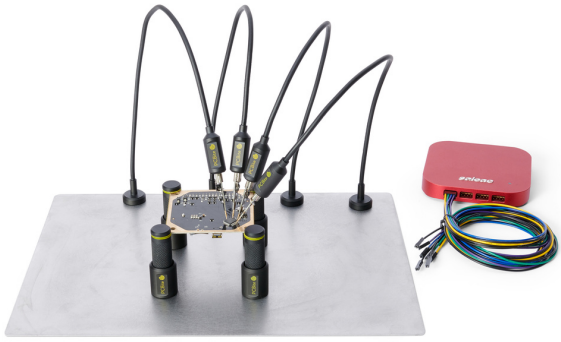
Il CH341A con kit incluso, consente di analizzare l'SPI e le memorie grazie anche a diversi adattatori, a seconda della grandezza di memoria da analizzare. In questo Kit è presente anche un supporto per le SPI che funzionano ad 1.8V. Il cavetto aggiuntivo consente anche l'utilizzo di una clip senza dissaldare l'SPI.

SECONDO PROTOTIPO

Prodotti Acquistati

Il kit di Saldatura consente di fissare e/o rimuovere componenti sulla board per poterli analizzare separatamente. Ad esempio per la rimozione dell'SPI e, dopo averla analizzata, per risaldarla. Consente anche la rimozione di componenti che limitano l'utilizzo della scheda stessa

Il multimetro portatile a "penna" consente di analizzare la continuità e i vari voltaggi presenti sulla scheda. Oltre ad avere tutte le funzionalità di un multimetro dispone di una modalità automatica che consente di ottenere informazioni a seconda dei pin che vengono toccati



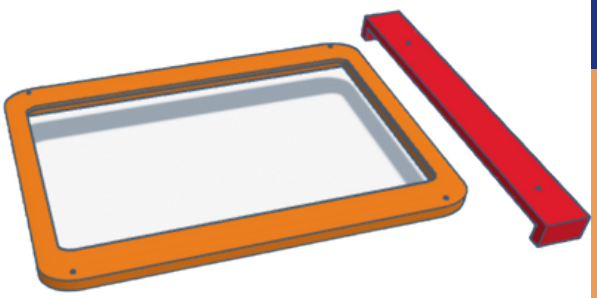
Il Kit PCBite consente di avere un supporto magnetico per fissare le board da analizzare ed utilizzare i Pogo Pins per interagire direttamente con la scheda. La misura non troppo grande consente anche di migliorare la portabilità del prodotto. Ovviamente si ricorda di rimuovere le punte durante il trasporto per evitarne la rottura

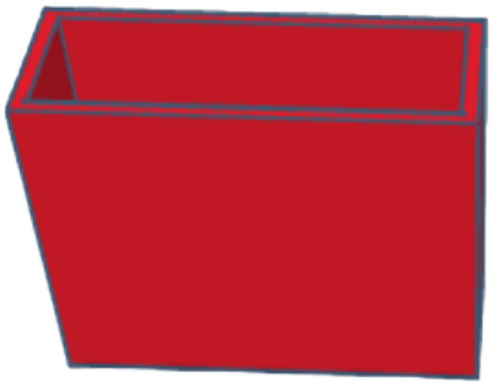
SECONDO PROTOTIPO

Stampe 3D

Tutti i supporti aggiuntivi sono stati stampati utilizzando un PLA+ di colore nero della Sunlu. Questo PLA è molto resistente e si adatta bene alla BOX. La stampante utilizzata con questo prodotto è la Anycubic Kobra Neo. Solitamente si usano 72 gradi per il piatto e 220 per l'estrusore

Supporto stampato con il PLA+ per lo schermo. Sono stati aggiunti due supporti (di colore rosso) per avvicinare lo schermo all'utente e non incastrarlo nella BOX. In arancione la cornice dello schermo





Il porta cavi è situato all'interno della Box e consente di trasportare cavetti di rame utilizzati per le operazioni con UART/JTAG e per interagire direttamente col dispositivo. Si trova all'interno sulla parte sinistra, fissato con l'adesivo 3M

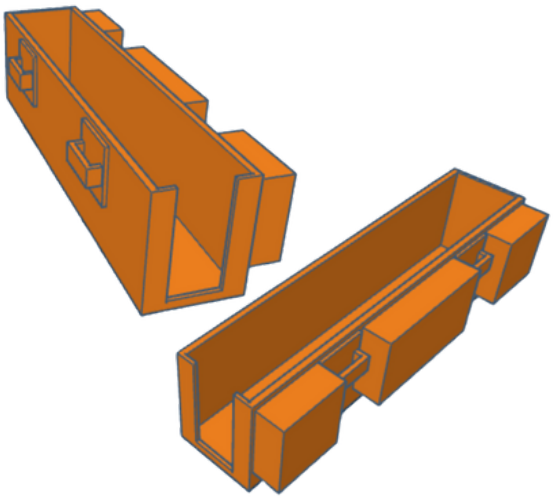
Il supporto per il velcro si è rilevato utile in fase di "fissaggio" temporaneo dei vari tool presenti nella BOX e per la tastiera e la batteria presenti esternamente

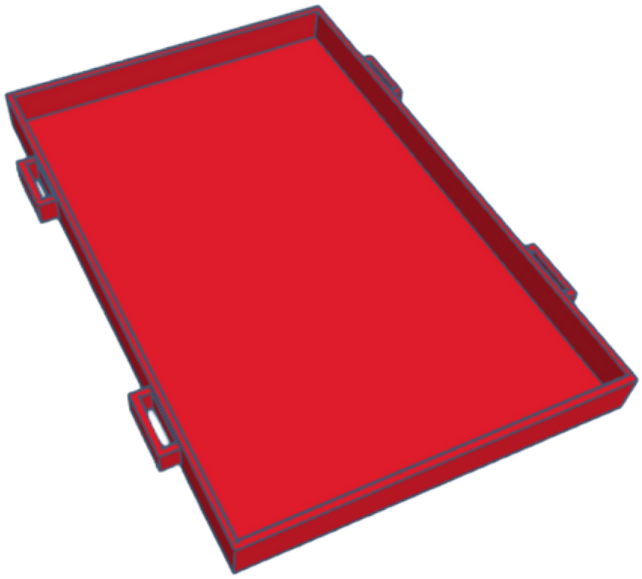
SECONDO PROTOTIPO

Stampe 3D

Il supporto per i magneti è utile per fissare il kit PCbite. In questo modo è possibile posizionare il kit a testa in giù lasciando la parte magnetica rivolta verso l'alto in modo tale da poter appoggiare la board magnetica del Kit

Il supporto per la batteria deve avere uno spessore per evitare di rendere l'estrazione e l'inserimento difficoltosi. Al supporto è stata aggiunta la possibilità di utilizzare il velcro per rendere il tutto più sicuro e facilmente removibile





Il supporto per la tastiera pieghevole è stato aggiunto esternamente sulla parte alta della BOX. Il fissaggio è con un adesivo 3M, mentre la tastiera viene appoggiata all'interno del vano e fissata con il velcro, in modo tale da rimuoverla e inserirla in maniera rapida e veloce.

SECONDO PROTOTIPO

Foto Finali del prodotto

Foto del prodotto esterno

Kit Cacciaviti Magnetici Estraibile

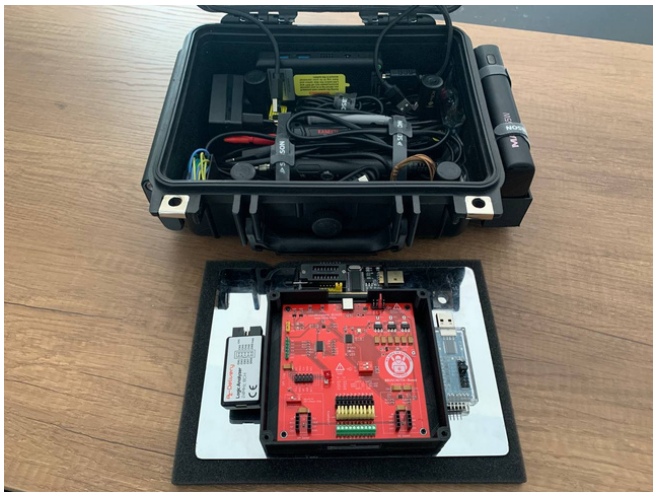
Tastiera Pieghevole

SECONDO PROTOTIPO

Foto Finali del prodotto

Foto del prodotto interno

Board Magnetica



Kit completo Interno

SECONDO PROTOTIPO

Foto Finali del prodotto

Tools

Interno Box

Monitor e Hub

SECONDO PROTOTIPO

Foto Finali del prodotto