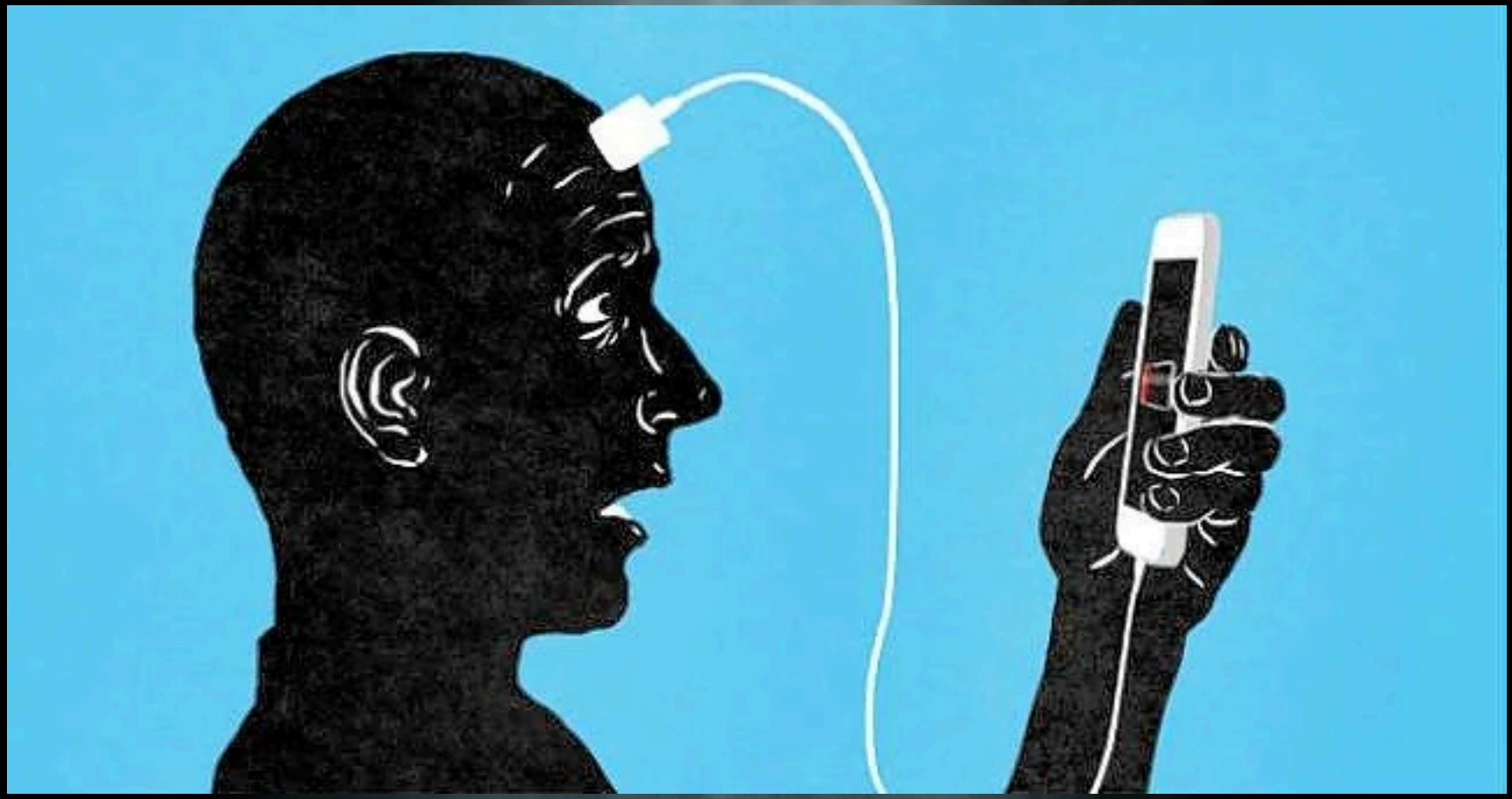
Ordine degli ingegneri

Napoli, 8 marzo 2019

Elementi di intelligence e analisi investigativa

La “persona” che vi conosce meglio al mondo sono i server di Google in North Carolina e di Apple in California.

Dal 2007 ad oggi, con la diffusione di internet mobile e di telefoni con sempre più funzionalità, abbiamo lentamente ma inesorabilmente iniziato a riversare prima, tutte le nostre comunicazioni, poi noi stessi in questi strumenti.

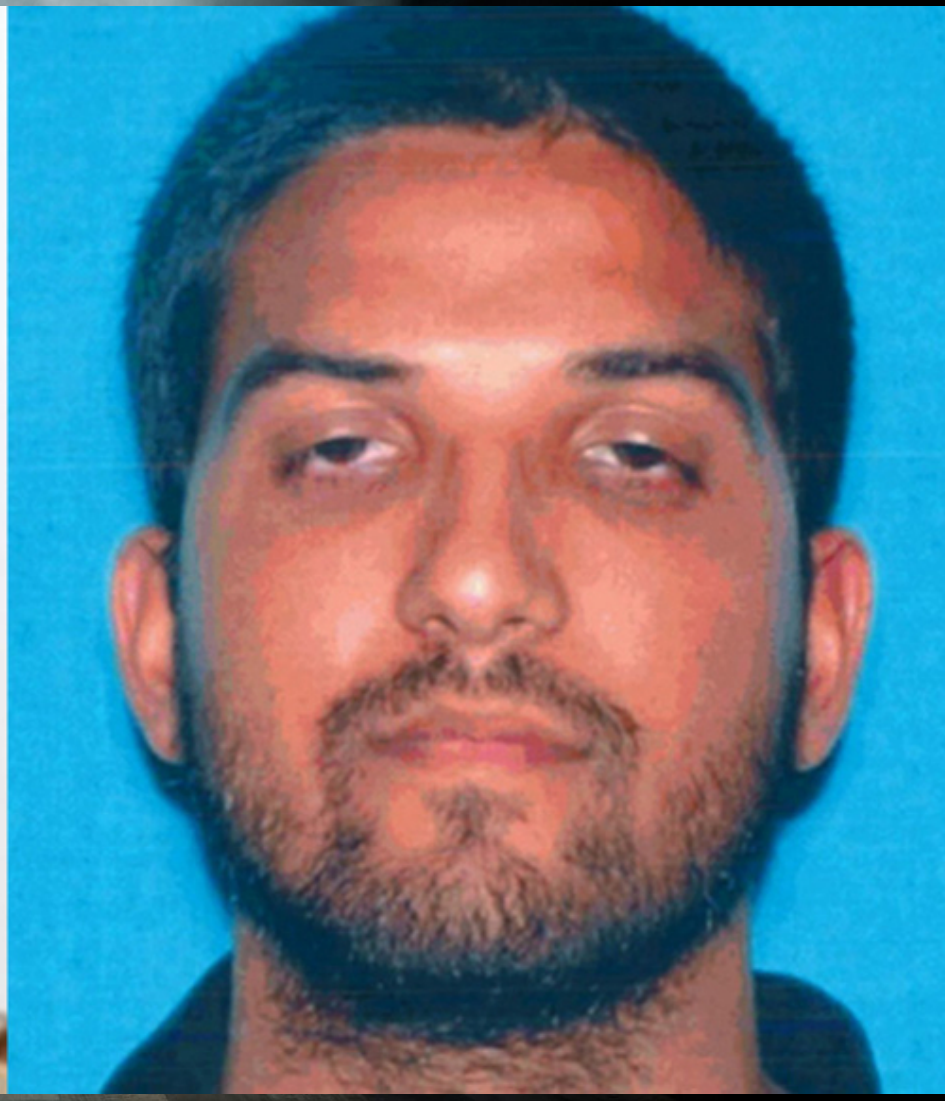


Oggi, il nostro telefono è quanto di più simile, abbiamo mai inventato, a una estensione artificiale del nostro cervello.

La presenza di questi oggetti, oracoli di noi stessi, ha cambiato drasticamente il modo in cui le forze dell'ordine possono accedere alle informazioni personali.

Tashfeen Malik

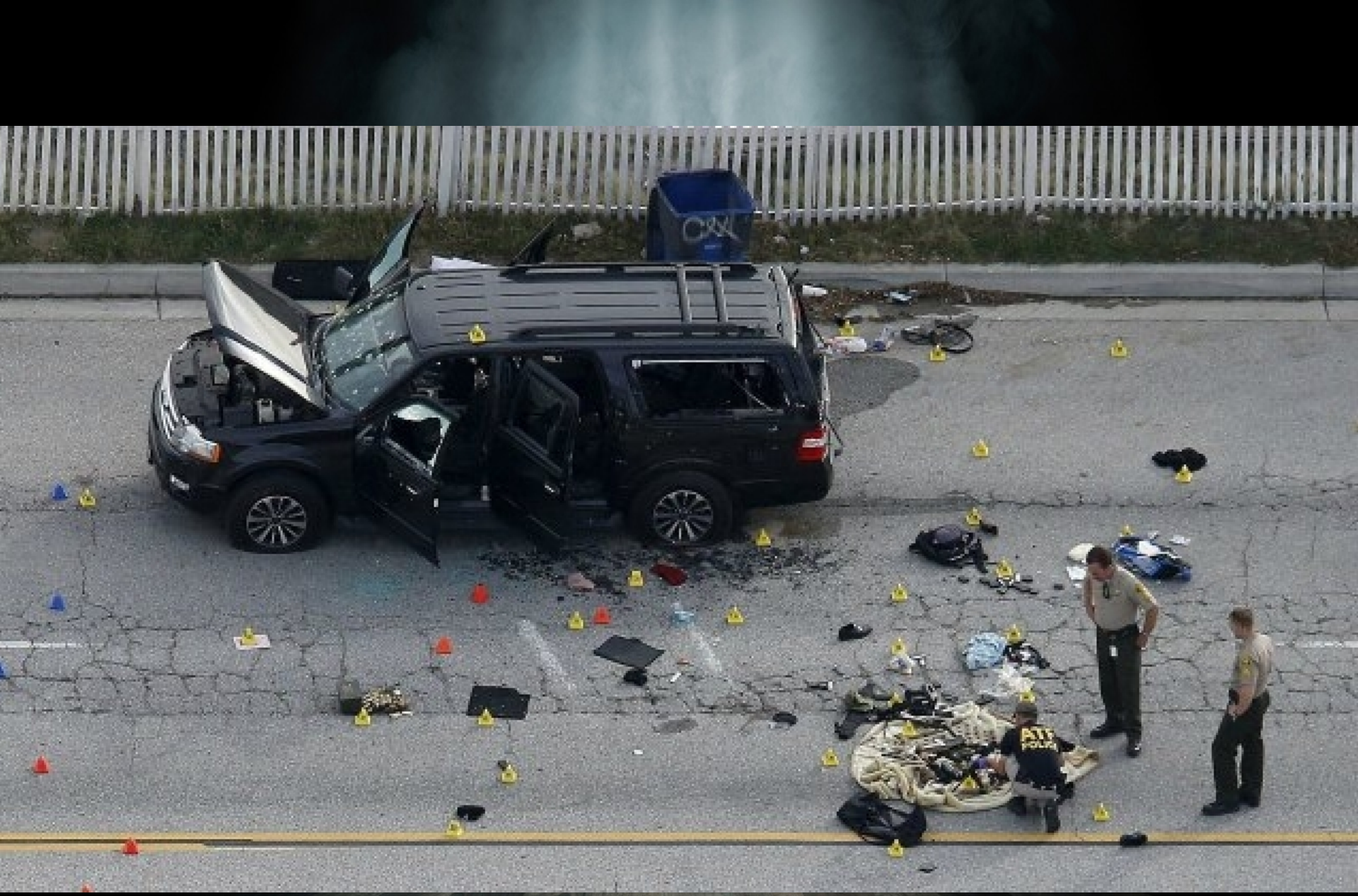
Syed Farook



2 dicembre 2015

The 14 victims killed in a mass shooting in **San Bernardino**

2 dicembre 2015



2 dicembre 2015

FBI ingiunge a Apple di sbloccare il telefono, adducendo una motivazione apparentemente invincibile:

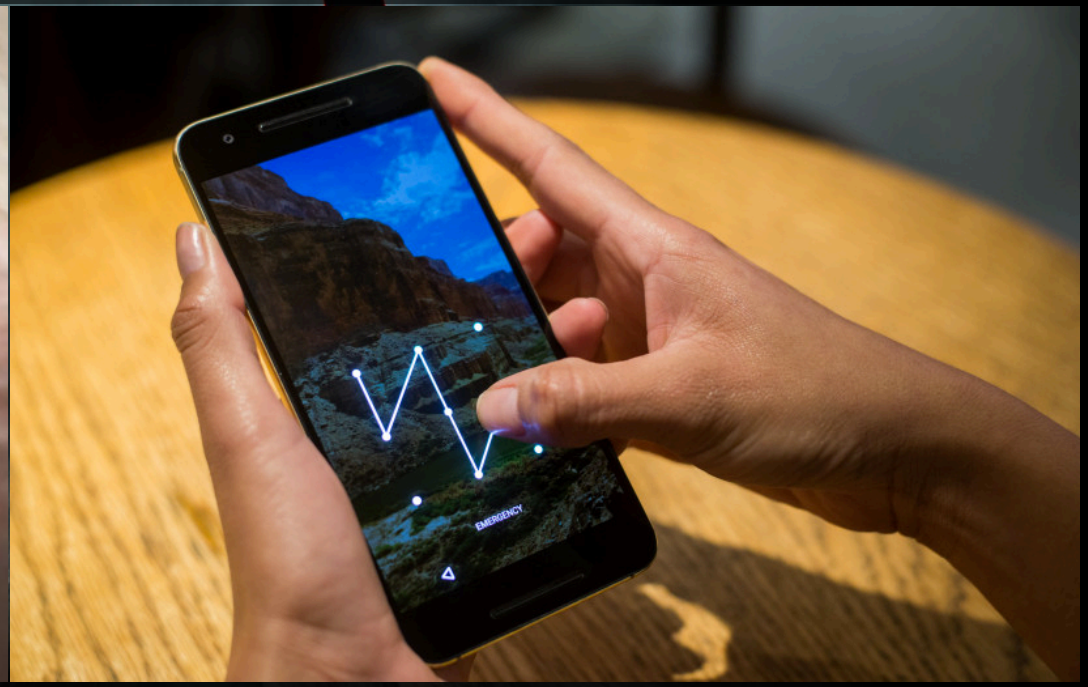
la sicurezza nazionale.

Apple si oppone

Iphone 5C

alla fine l’FBI riesce a sbloccare il telefono con metodi propri.

Ma il vero obiettivo dell'FBI, nel caso di San Bernardino, era quello di creare un vero precedente che giustificasse il bypass delle misure di sicurezza di Apple e Google.

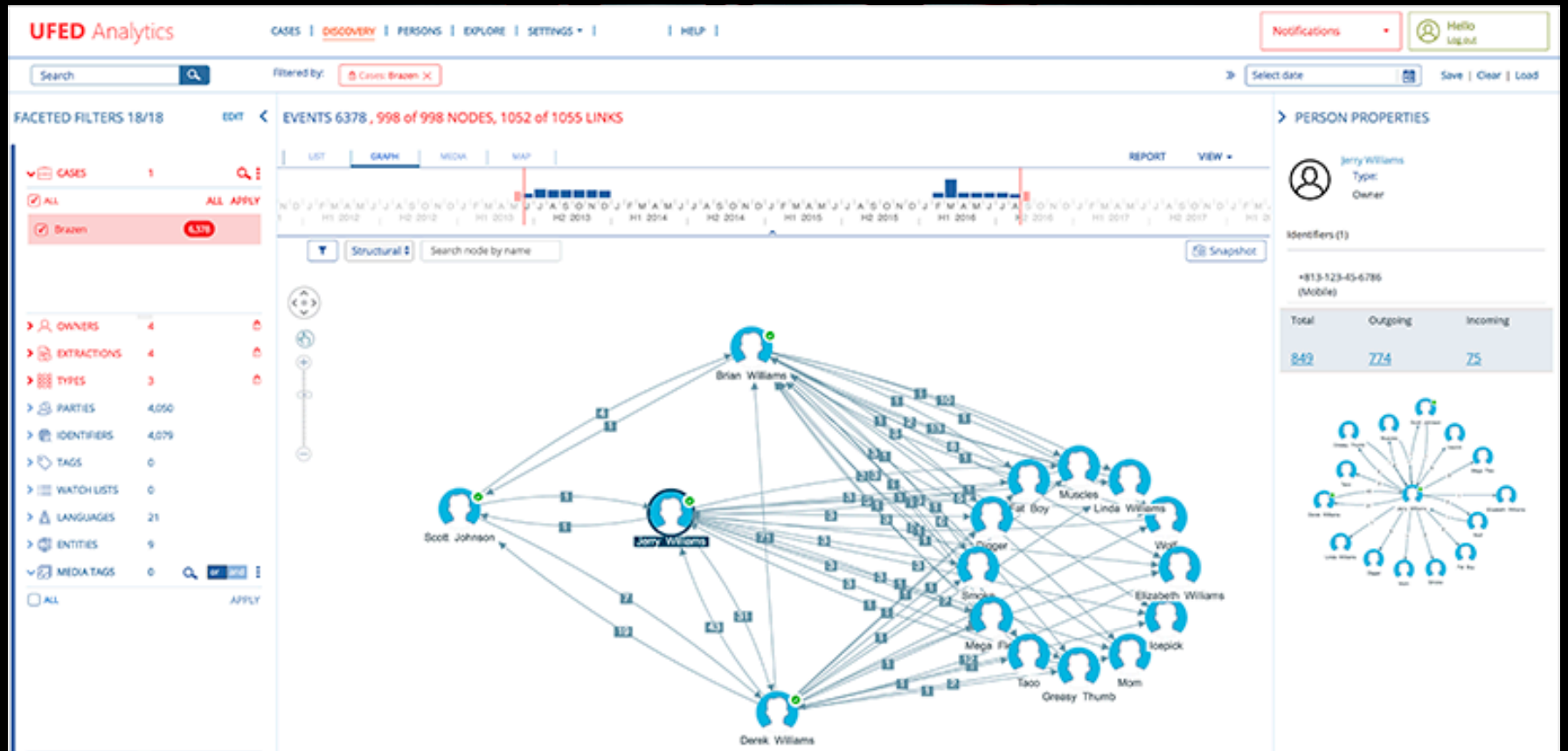


L’azienda con cui l’FBI si è interfacciata per accedere ai dati contenuti nell’iPhone:

Attiva nel settore dal 2007, all’inizio della diffusione esplosiva degli smartphone, vanta tra i propri clienti varie forze armate di tutto il mondo nonché l’Europol.

Cellebrite controlla una parte sostanziale del mercato della estrazione dei dati, in pratica quello che possono fare gli uffici di polizia del mondo, è quello che Cellebrite permette loro di fare.

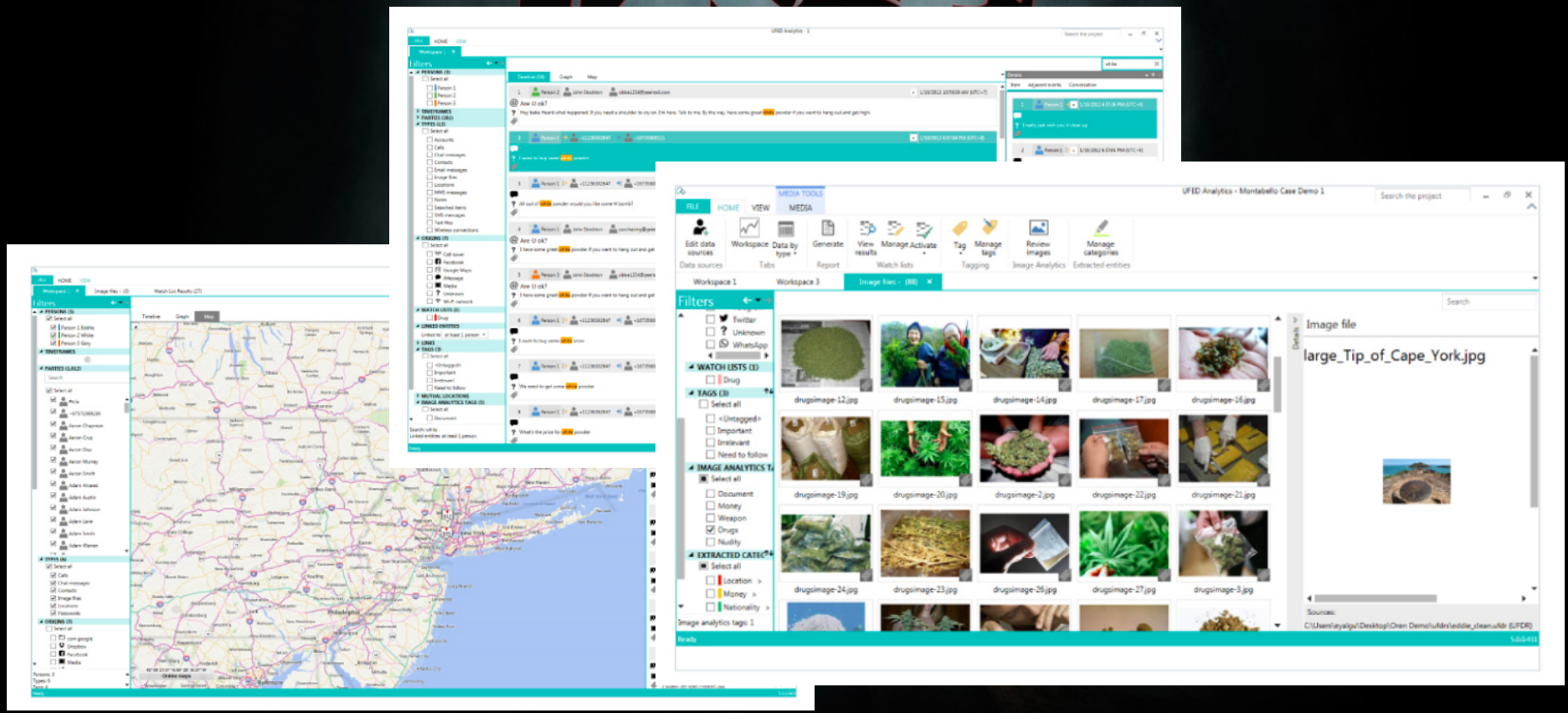
Cellebrite da poco ha presentato UFED Analytics, un programma di analisi e investigazione che permette agli utenti di navigare all'interno di un database contenente tutti i dati raccolti dai telefoni di sospettati e da "servizi collegati" ai loro proprietari nonchè di vittime e di vicini di casa coinvolti.



«Tutti i dati raccolti»

è anche una dichiarazione estremamente vaga…

Edward Snowden ci ha insegnato che ogni carattere battuto su ogni tastiera è accessibile alle grandi agenzie di intelligence internazionali



Cosa succede a un telefono nelle mani delle forze di polizia?

ANDROID

bypassa il codice di sicurezza e procede all'estrazione dati completa fino a Android 8.0

APPLE

estrae e decripta dati su telefoni con versioni di iOS precedenti alla 10.

...e le nuove versioni?

Advanced Unlocking

Cellebrite Advanced Unlocking Services is the industry's only solution for overcoming many types of complex locks on market-leading devices. This can determine or disable the PIN, pattern, password screen locks or passcodes on the latest Apple iOS and Google Android devices.

This exclusive paid Advanced Unlocking Service is available to law enforcement agencies globally for lawfully authorized examinations. Law enforcement agencies are then empowered to perform the device extraction themselves or take advantage of Cellebrite Advanced Extraction Services to retrieve more data from the most complex devices as part of the same submission process.

Advanced Extraction

Even if an unlocked device is recovered or a consent search is granted, being able to perform a complete physical extraction or full file system extraction of the latest Apple iOS and Google Android devices may not be possible through conventional means due to full disk encryption and a highly intertwined relationship between the secure processor and flash memory.

Cellebrite makes the world's first and only decrypted physical extraction capability possible for leading Apple iOS and Google Android devices. These new capabilities enable forensic practitioners to retrieve the full file system to recover downloaded emails, third-party application data, geolocation data and system logs, without needing to jailbreak or root the device. This eliminates any risk in compromising data integrity and the forensic soundness of the process. This enables access to more and richer digital data for the investigative team.

Advanced Unlocking and Extraction Services are available for the latest Apple iOS devices including all iPhone models (iPhone 4S to iPhone X), iPad, iPad mini, iPad Pro and iPod touch, running iOS 5 to iOS 11.

Unlocking and decrypted physical extraction of Samsung Galaxy S6, S6 edge, S6 edge+, S6 active, A5, A7, A8, J1, J7, Note 5, S7, S7 edge, S7 edge, S7 active.

Unlocking and decrypted physical extraction of most Samsung devices including: Galaxy S6/S7/S8, A5/A7/A8, J1/J3/J5/J7, Note 5/Note 8

- Decrypted Physical extractions available for most models
- Decrypted contents of Samsung SecureFolder available
- Limitations may apply based on iOS/Android version and Security patch level
- Some models must be submitted to Cellebrite lab location for extended processing times

This list of supported products is continuously updated so you should contact Cellebrite for specific requests.

UFED estrae la rubrica dei contatti, SMS e MMS, email, calendari, lo storico delle chiamate, e tutti i dati non criptati di tutte le app installate. Inoltre, è in grado di decriptare il database locale di WhatsApp

Il limite principale di questo strumento è l'impossibilità di accedere a telefoni completamente criptati.

Domanda

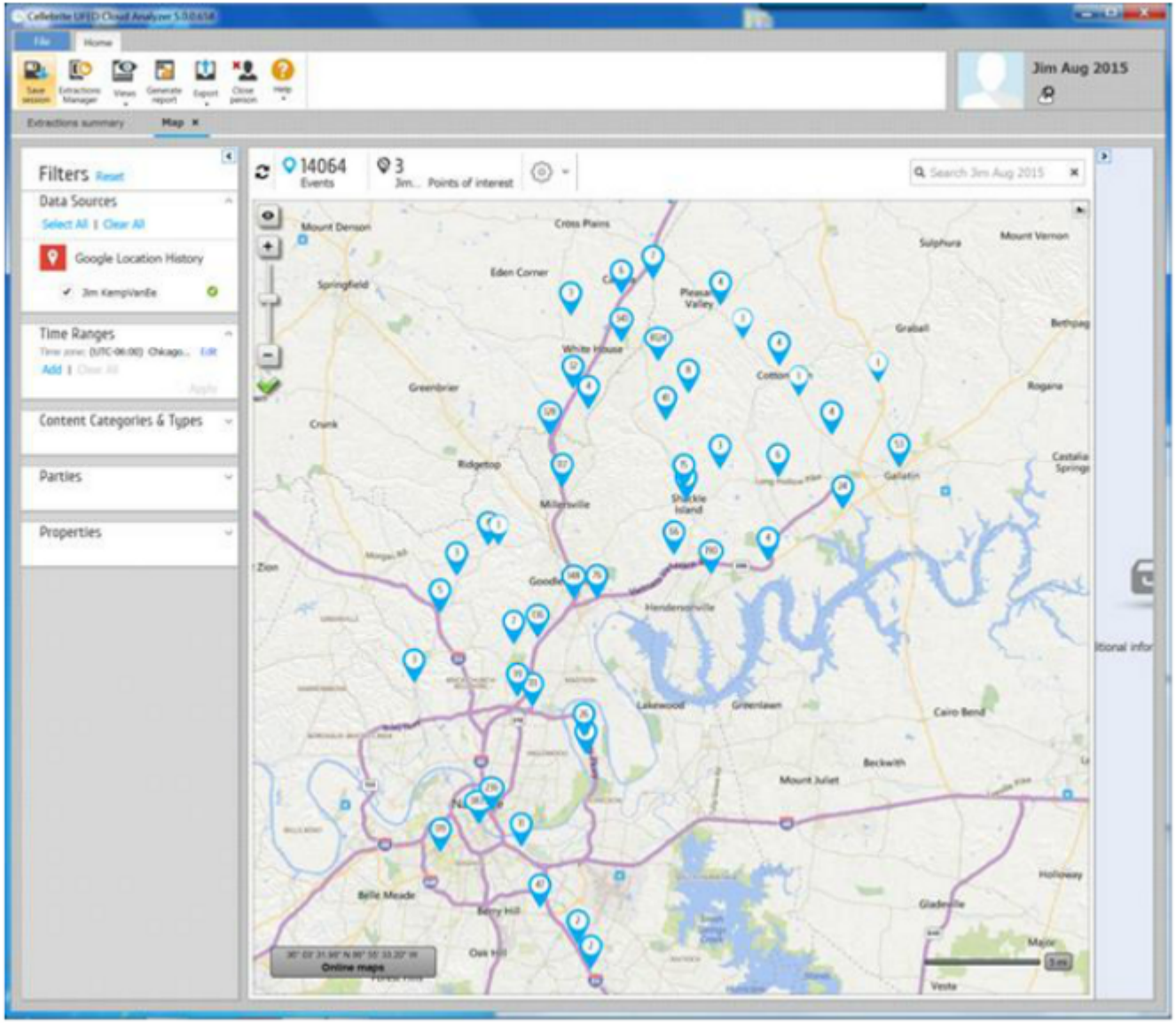
Al giorno d'oggi, tutti i dati stanno fisicamente sul cellulare?

UFED Cloud Analyzer

Attraverso Cloud Analyzer le forze di polizia possono accedere a tutti i servizi web collegati a un cellulare cioè tutti i dati da social network, mail, e simili anche senza password solo se si è in possesso di una copia completa del file system del telefono, il software può usare i dati sul telefono per accedere direttamente a tutti i servizi collegati.

Il software è in grado di estrarre tutti i dati dalla Location History di Google in mezz'ora, e offre agli investigatori un anno di dati, a differenza dei quattro mesi condivisi dalla società di Mountain View.

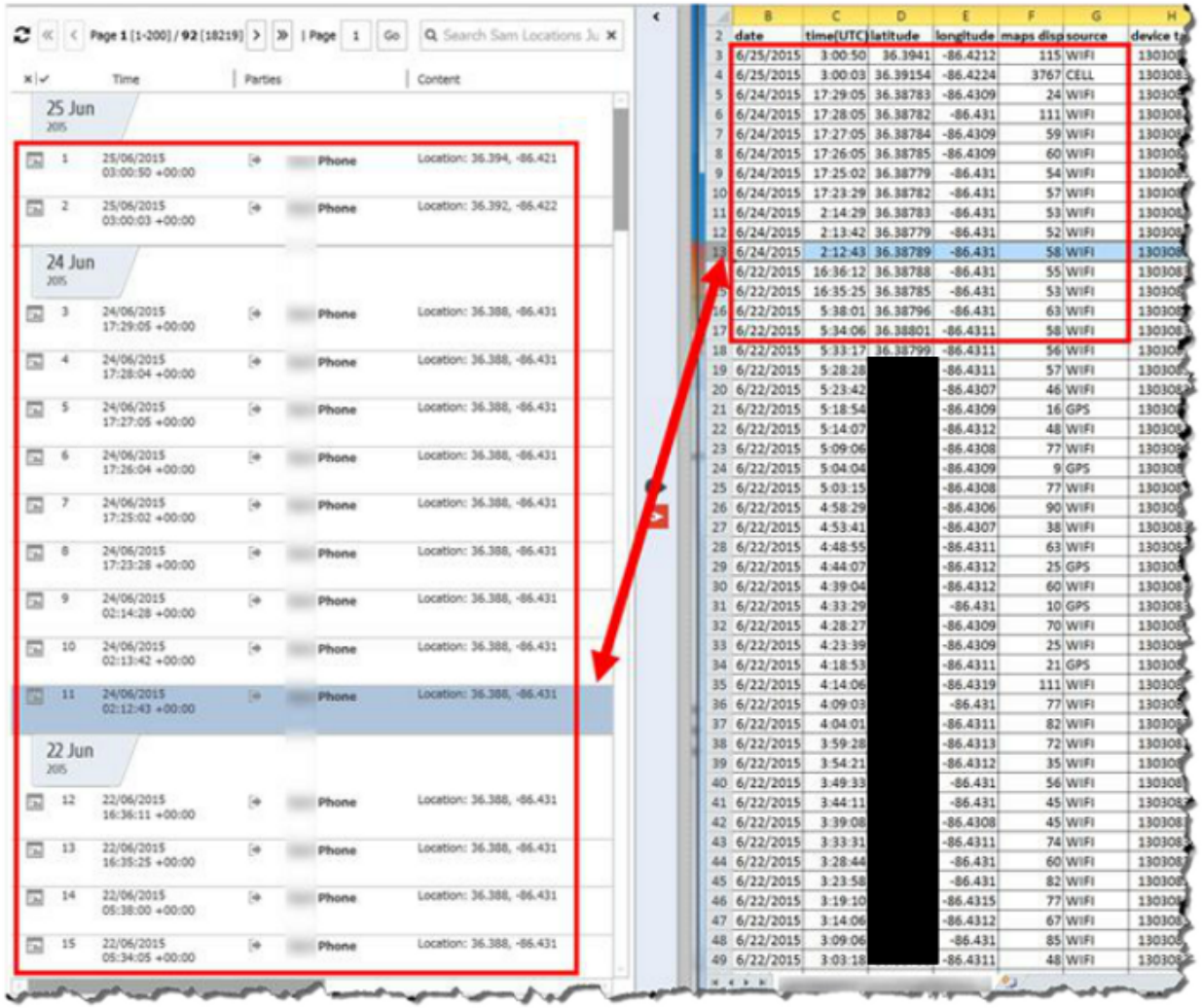
EXAMPLE - CLOUD ANALYZER MAP



cellebrite
delivering mobile expertise

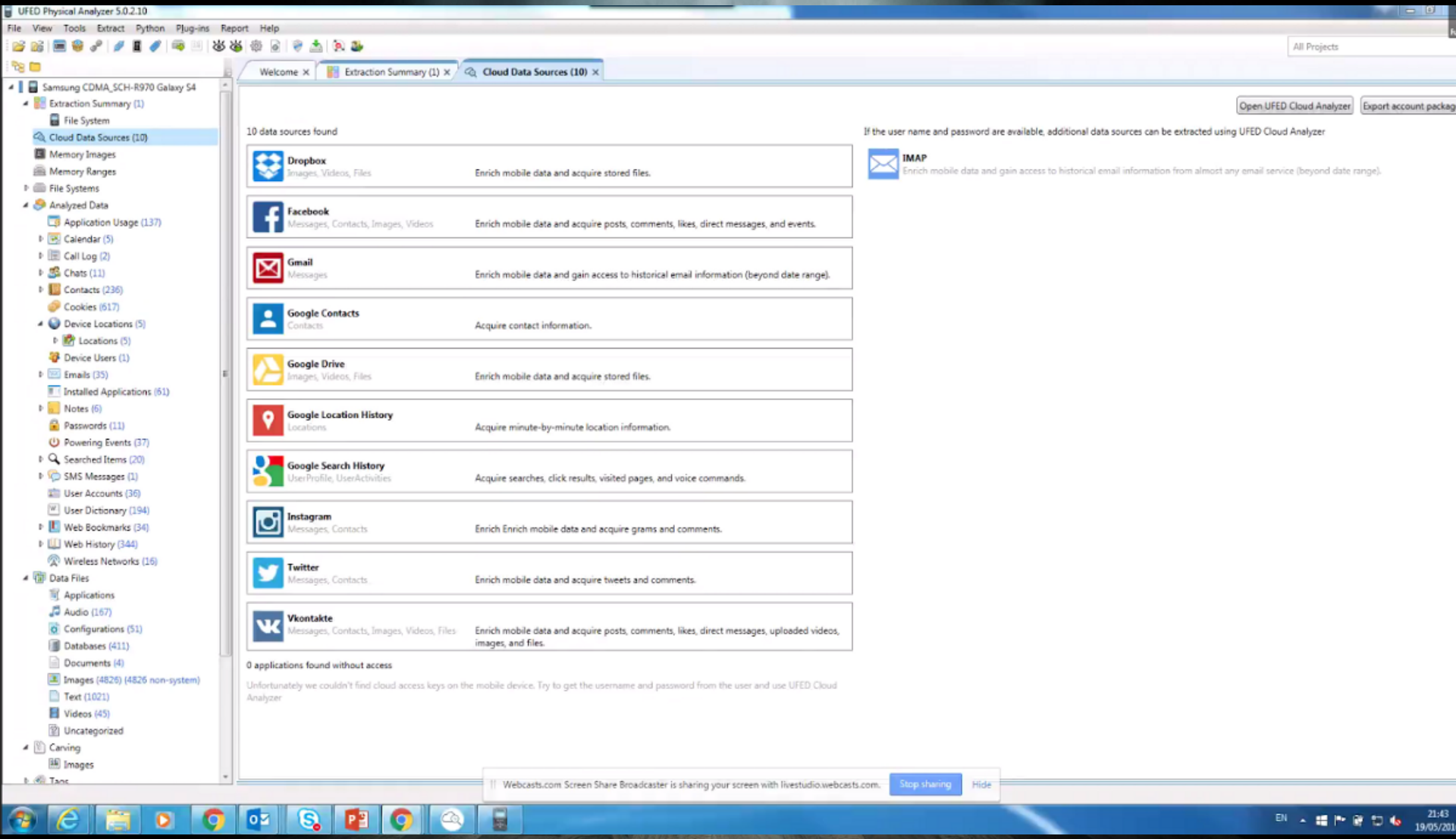
CLOUD ANALYZER COLLECTION VALIDATED

Cloud Analyzer Collection



Google "Official" Records

cellebrite
delivering mobile expertise

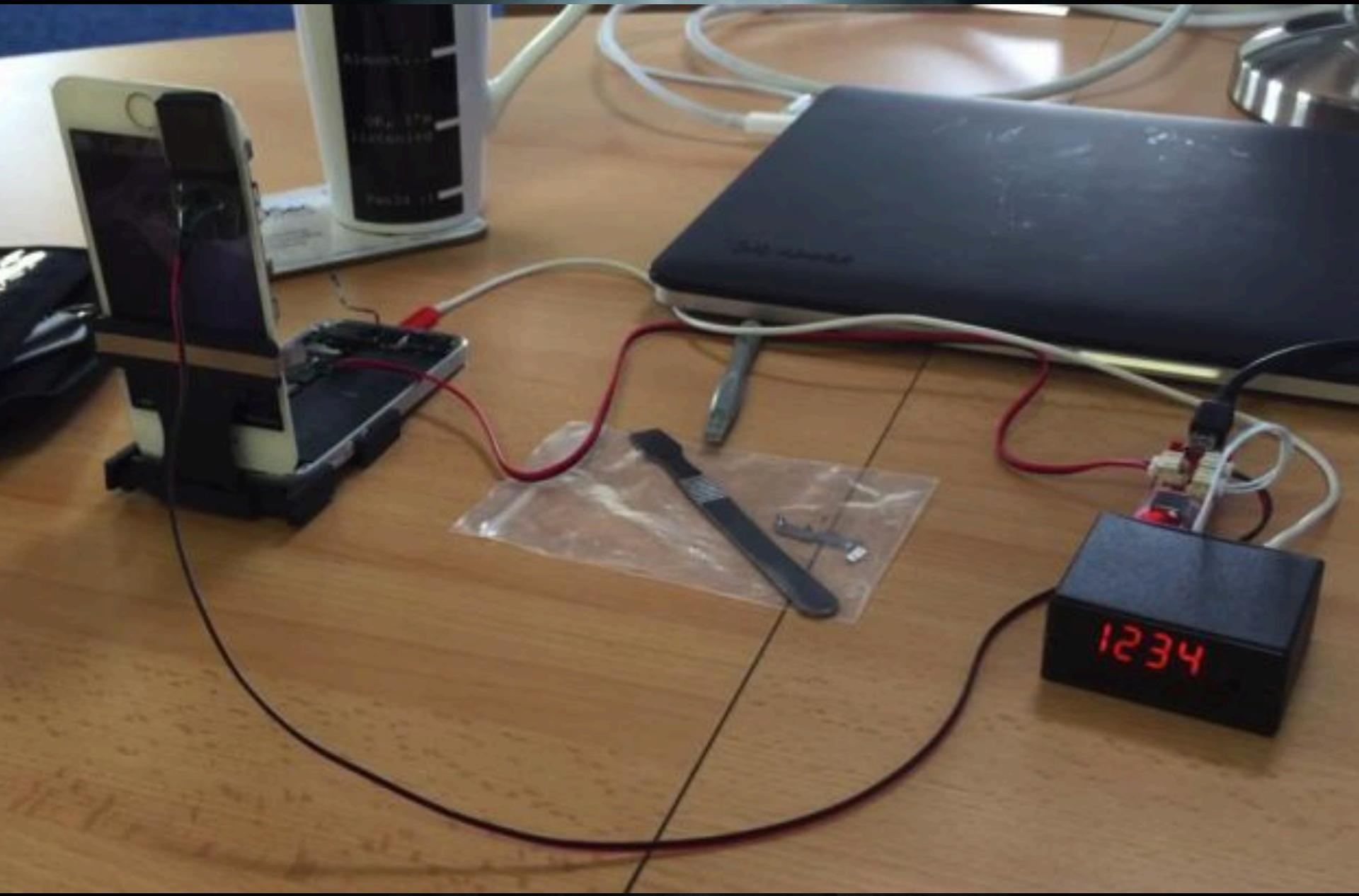

UFED Physical Analyzer 5.0.2.10
File View Tools Extract Python Plug-ins Report Help
All Projects
Welcome
Extraction Summary (1)
Cloud Data Sources (10)
Samsung CDMA_SCH-R970 Galaxy S4
Extraction Summary (1)
File System
Cloud Data Sources (10)
Memory Images
Memory Ranges
File Systems
Analyzed Data
Application Usage (137)
Calendar (5)
Call Log (2)
Chats (11)
Contacts (236)
Cookies (617)
Device Locations (5)
Locations (5)
Device Users (1)
Emails (35)
Installed Applications (61)
Notes (6)
Passwords (11)
Powering Events (37)
Searched Items (20)
SMS Messages (1)
User Accounts (36)
User Dictionary (194)
Web Bookmarks (34)
Web History (344)
Wireless Networks (16)
Data Files
Applications
Audio (167)
Configurations (51)
Databases (411)
Documents (4)
Images (4826) (4826 non-system)
Text (1021)
Videos (45)
Uncategorized
Carving
Images
Tags
Open UFED Cloud Analyzer
Export account packag
10 data sources found
If the user name and password are available, additional data sources can be extracted using UFED Cloud Analyzer
Dropbox
Images, Videos, Files
Enrich mobile data and acquire stored files.
IMAP
Enrich mobile data and gain access to historical email information from almost any email service (beyond date range).
Facebook
Messages, Contacts, Images, Videos
Enrich mobile data and acquire posts, comments, likes, direct messages, and events.
Gmail
Messages
Enrich mobile data and gain access to historical email information (beyond date range).
Google Contacts
Contacts
Acquire contact information.
Google Drive
Images, Videos, Files
Enrich mobile data and acquire stored files.
Google Location History
Locations
Acquire minute-by-minute location information.
Google Search History
UserProfile, UserActivities
Acquire searches, click results, visited pages, and voice commands.
Instagram
Messages, Contacts
Enrich Enrich mobile data and acquire grams and comments.
Twitter
Messages, Contacts
Enrich mobile data and acquire tweets and comments.
Vkontakte
Messages, Contacts, Images, Videos, Files
Enrich mobile data and acquire posts, comments, likes, direct messages, uploaded videos, images, and files.
0 applications found without access
Unfortunately we couldn't find cloud access keys on the mobile device. Try to get the username and password from the user and use UFED Cloud Analyzer
Webcasts.com Screen Share Broadcaster is sharing your screen with livestudio.webcasts.com.
Stop sharing
Hide
EN
21:43
19/05/201

UFED Cloud Analyzer è un programma ed è possibile chiedere una demo gratuita di 30 giorni.

http://go.cellebrite.com/CATrialInquiry

L'uso è consentito solo sul proprio dispositivo, non è legale utilizzarlo su altri dispositivi.

ip box


1234


Verizon
Enter Passcode
Your passcode is required
to enable Face ID
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0
Emergency
Cancel
Status

GrayKey box

fine dei giochi da iOS 12

Etico sbloccare uno smartphone con il dito di

.....

un morto?

Ma se il telefono non è ancora nelle mani delle forze di polizia?

Le intercettazioni telematiche

captare il flusso telematico di dati, permette l'acquisizione di informazioni e contenuti rilevanti in ambito investigativo.

Art. 266 bis Codice di Procedura Penale

Nei procedimenti relativi ai reati indicati nell'articolo 266 del codice penale nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.

Mettendo da parte le intercettazioni telefoniche, le classiche intercettazioni del traffico dati su linea non forniscono più informazioni e dati di interesse, in quanto la maggior parte del traffico passante risulta cifrato.

Per questo motivo sono state sviluppate, tecnologie in grado di intercettare le informazioni nei punti in cui sono in chiaro, cioè direttamente all'interno dei dispositivi.

Tali tecniche vengono generalmente denominate “intercettazioni attive”, presupponendo non più solo un ascolto passivo, ma un’attività di cattura dell’informazione.

In sostanza, l’attività di captazione si sposta all’interno del dispositivo, trasformandosi da “intercettazione” in “cattura” del dato presente nel computer (o nello smartphone), rimanendo nella copertura normativa dell’intercettazione prevista dagli art. 266 e seguenti del c.p.p.

Questi sistemi di decodifica dell'informazione sono estremamente funzionali ma al tempo stesso generano la necessità di essere gestiti in maniera corretta e calibrata sotto il profilo investigativo.

In particolare, si possono verificare casi di ambiguità nella fase installativa degli agenti tecnici (captatori informatici):

un esempio è dato dall'intercettazione di un pc pubblico: in questo caso risulta fondamentale poter intercettare esclusivamente il traffico generato dalla persona indagata e non tutto il traffico generato dal sistema.

Un altro caso è quello di un'installazione su un sistema telematico del quale non sia chiara la struttura di rete interna: in questo caso l'individuazione del dispositivo (sistema informatico) da intercettare risulta alquanto difficile e potrebbe accadere che venga monitorato un dispositivo non di interesse investigativo.

Nell’ambito dei servizi di telefonia mobile la polizia giudiziaria sfrutta da tempo le molteplici informazioni custodite dai gestori. In particolare possiamo distinguere i dati utili, acquisiti dai gestori, nei seguenti:

traffico fonia, chiamate e messaggistica SMS (24 mesi);

traffico dati (12 mesi);

chiamate non risposte (30 giorni);

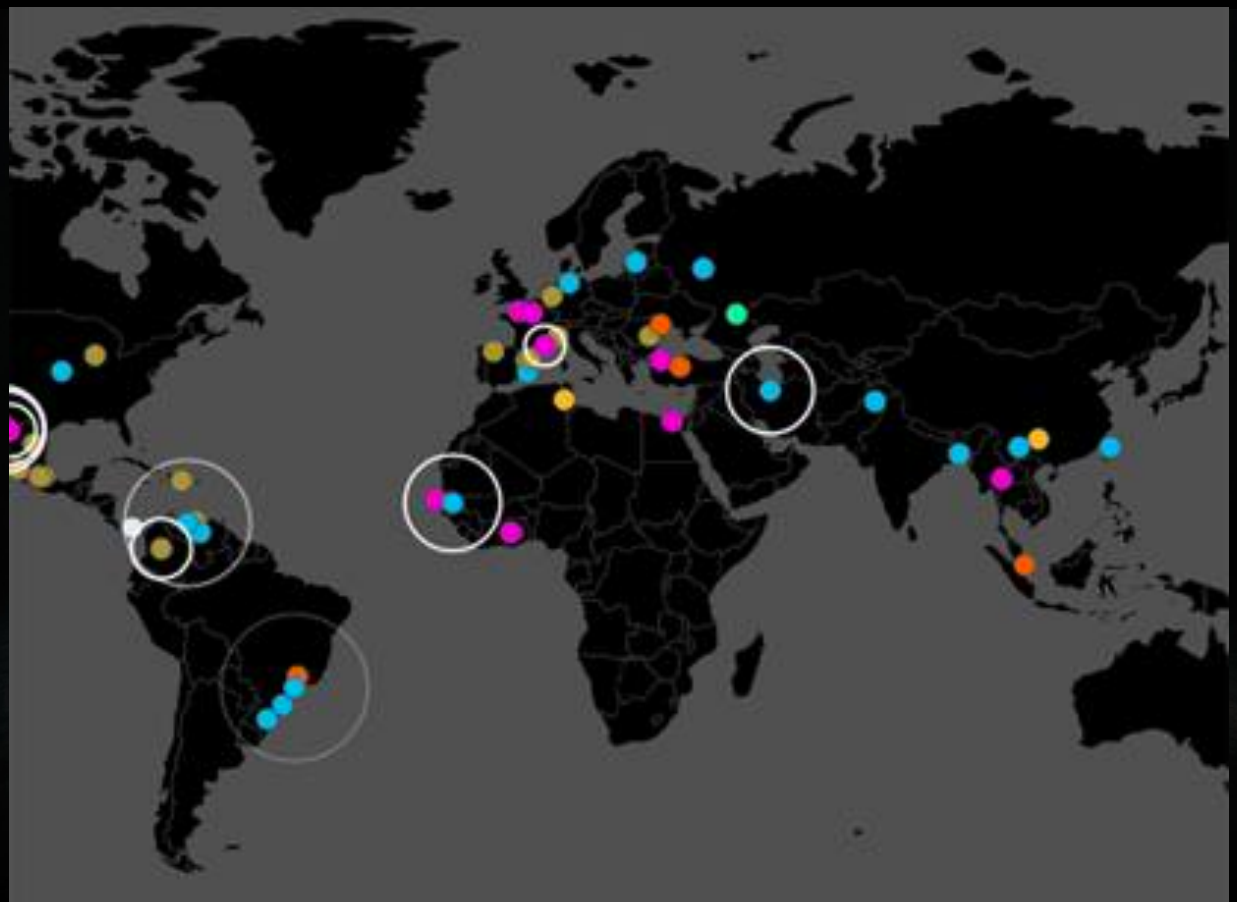
anagrafiche utenti (senza scadenza);

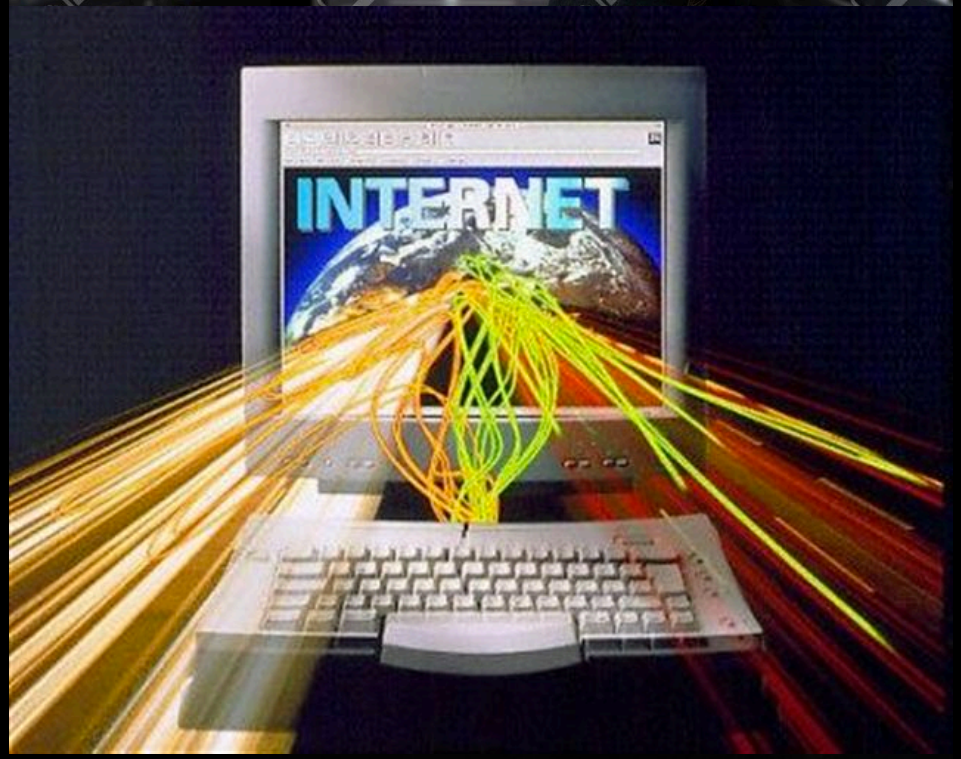
elenco delle stazioni radiobase (aggiornamenti mensili).

Le caratteristiche di transnazionalità e immaterialità della rete rendono i reati commessi attraverso Internet più difficili da perseguire.

A differenza dei reati comuni, che sono consumati nel luogo in cui si trova l'autore del reato e hanno per oggetto persone o beni individuabili nella realtà fisica, i reati informatici sono realizzati in uno spazio virtuale in cui gli oggetti del reato sono spesso intangibili.

Rispetto al criminale comune, il soggetto di un reato informatico ha il vantaggio di poter essere un cittadino straniero, realizzare la propria condotta per mezzo di un terminale all'estero, usare un flusso dati che passa in reti estere.





In questi casi le autorità devono ottenere permessi e affrontare diverse problematiche processuali. Inoltre le legislazioni in materia dei vari stati sono disomogenee, e risulta pertanto necessario individuare con esattezza il luogo in cui l'azione viene consumata.

23 novembre 2001

dal Consiglio d'Europa sulla criminalità informatica

Convenzione di Budapest

Tale Convenzione sul cybercrime ha imposto, a tutti gli Stati membri dell'Unione Europea e non membri, di adottare misure legislative rivolte alla repressione penale dei nuovi crimini informatici, armonizzando, in questo modo, i diversi ordinamenti giuridici interni e coordinando forme di collaborazione per quanto concerne la raccolta di prove da parte delle autorità.

La situazione nel 2019 vede un totale di **62** Stati che hanno aderito alla Convenzione.

Hanno firmato la Convezione ma non hanno ratificato:
Irlanda, Svezia, San Marino, Sud Africa.

In ordine di tempo, gli ultimi ad aver ratificato la Convenzione al 2018 sono il Tonga, Sri Lanka, Senegal, Paraguay, Marocco, Filippine, Costa Rica, Cile, Capo Verde, Argentina, Polonia, Turchia, Monaco, Lussemburgo, Liechtenstein, Grecia, Andorra.

Ad Aprile 2019 il Ghana ratificherà la convenzione.

<u>Non</u> hanno firmato la convenzione.
Russia, Messico, Nigeria, Tunisia, Perù, Colombia.

Per quanto riguarda gli Stati Uniti d'America, hanno presenziato e firmato la Convenzione nel 2001, l'adesione si è concretizzata con la ratifica il 29-09-2006, ed entrata in vigore nel 2007.

L'Italia ha firmato il 23-11-2001, ratificato il 05-06-2008 ed entrata in vigore il 01-10-2008 con la legge n.48 del 2008.


WhatsApp
Gmail
Microsoft®
Hotmail®
Skype
YAHOO!
amazon
facebook

https://www.facebook.com/records

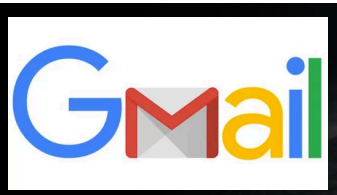
whatsapplec@zwillgen.com

ie-legalpoc@yahoo-inc.com

lealert@microsoft.com

richieste-polizia@amazon.it

lerm@skype.net

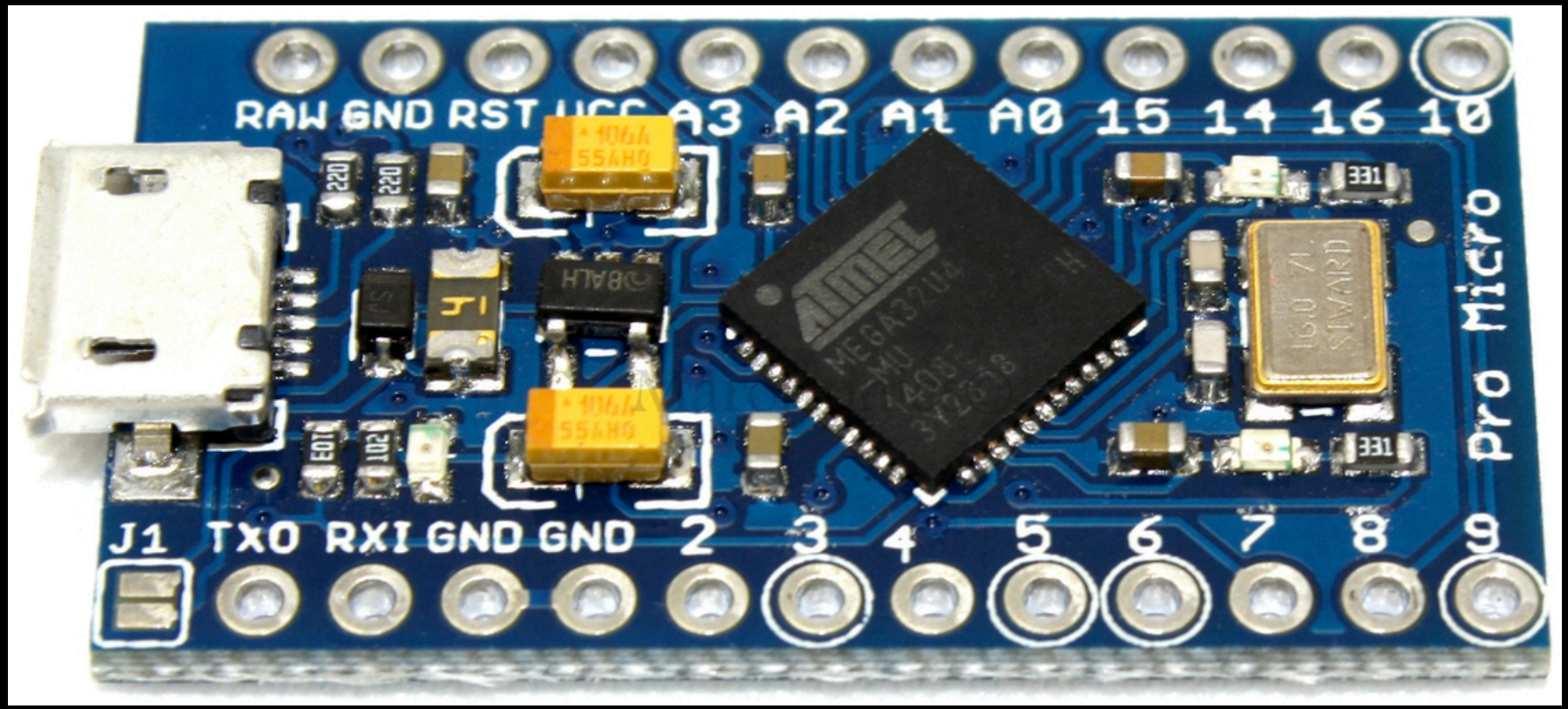


lis-global@google.com

lawenforcement@support.youtube.com

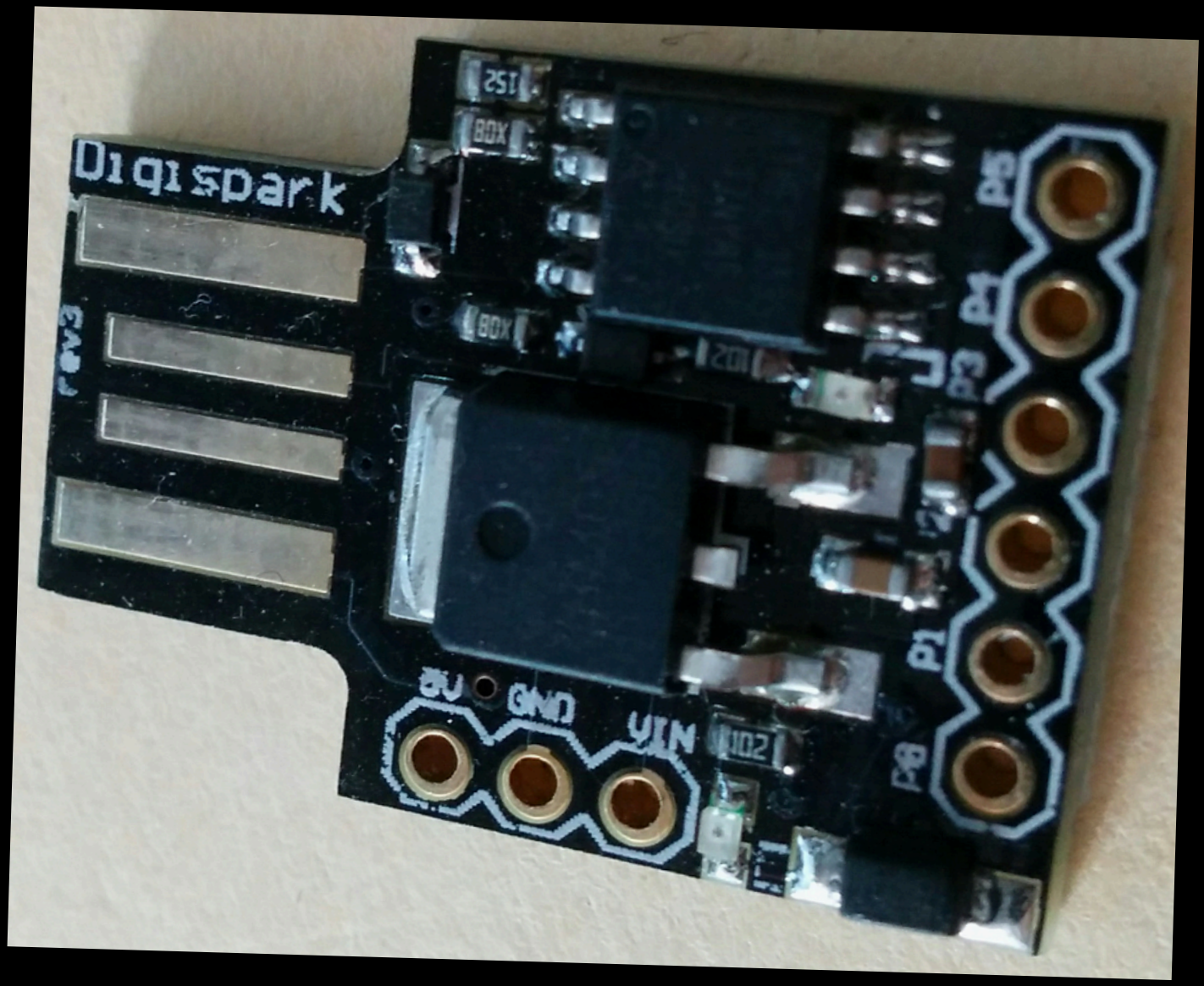

yubico
blackhat®

Arduino

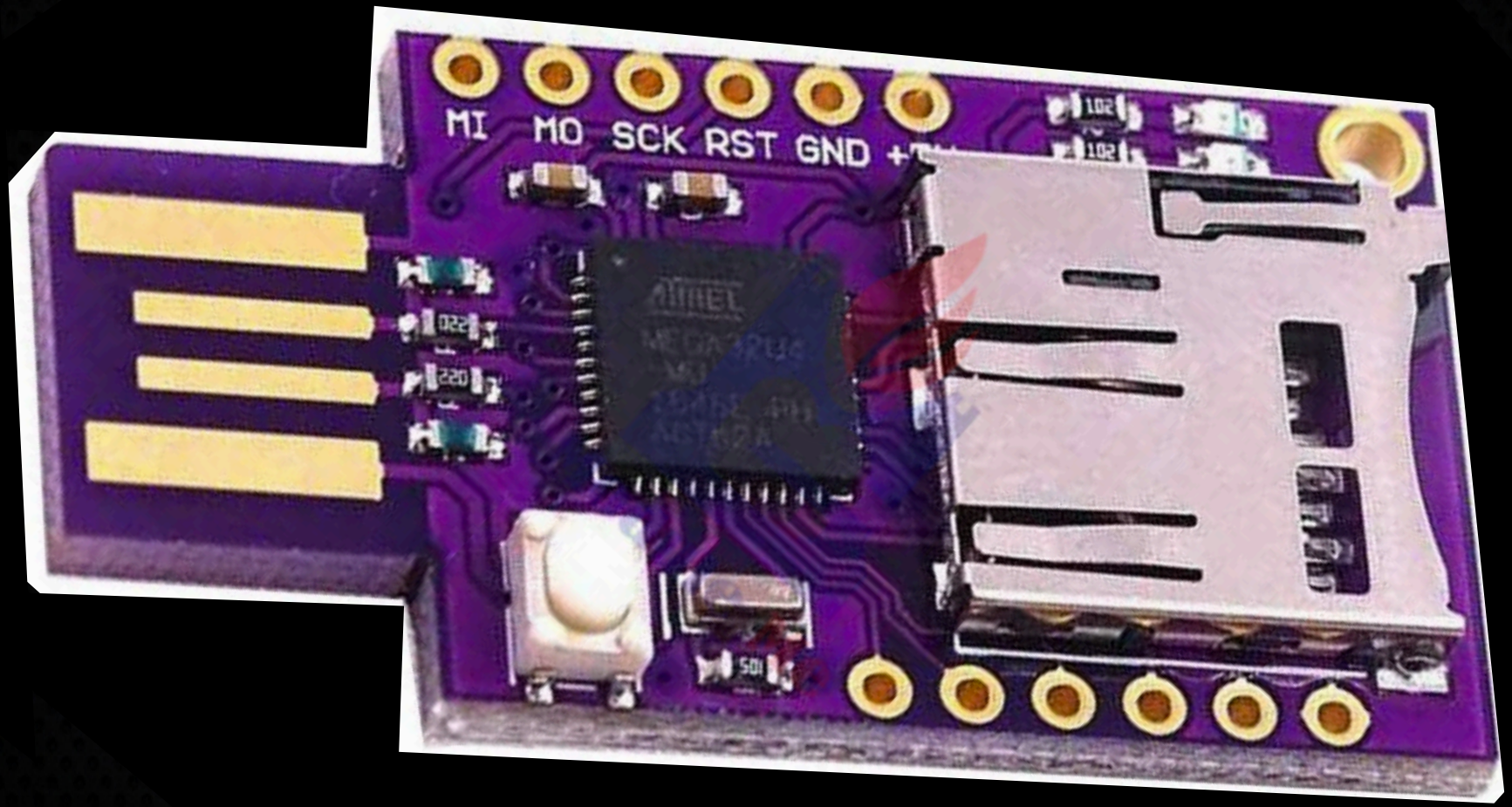

RAW GND RST VCC A3 A2 A1 A0 15 14 16 10
J1 TXO RXI GND GND 2 3 4 5 6 7 8 9
Pro Micro
ATMEL

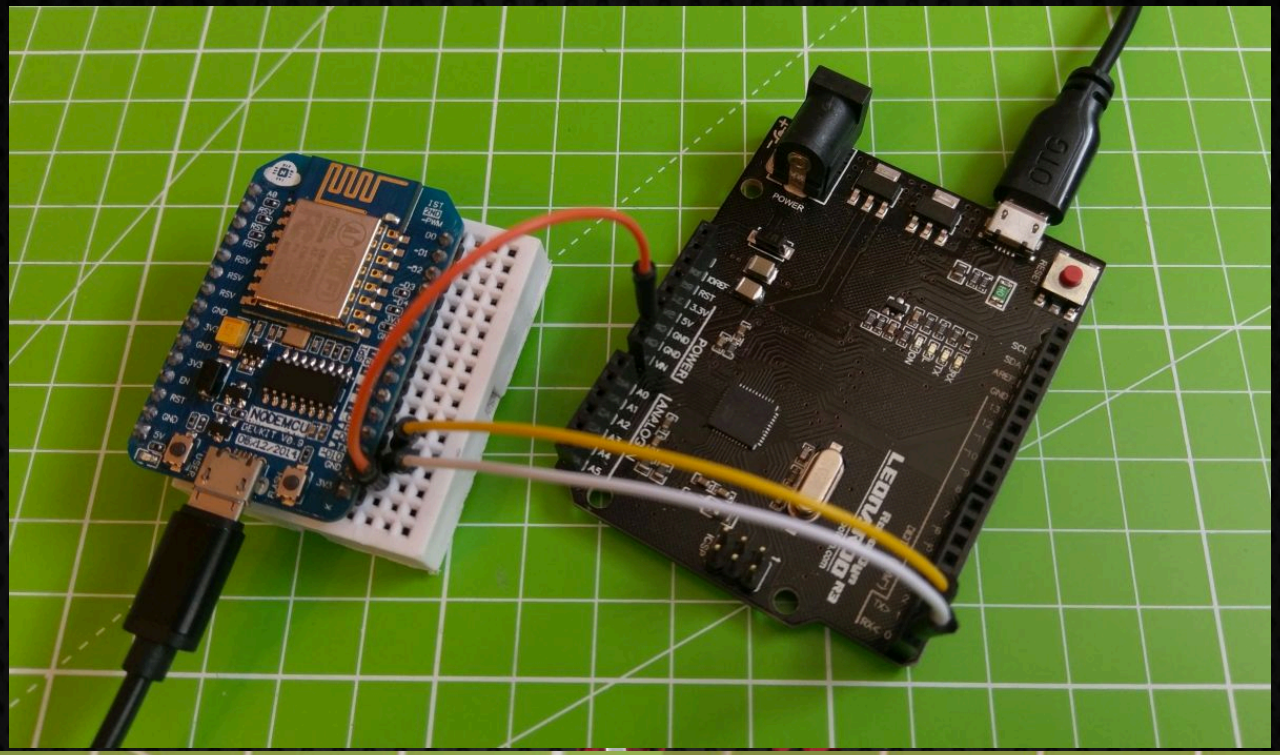
Attracco HID: Human Interface Device

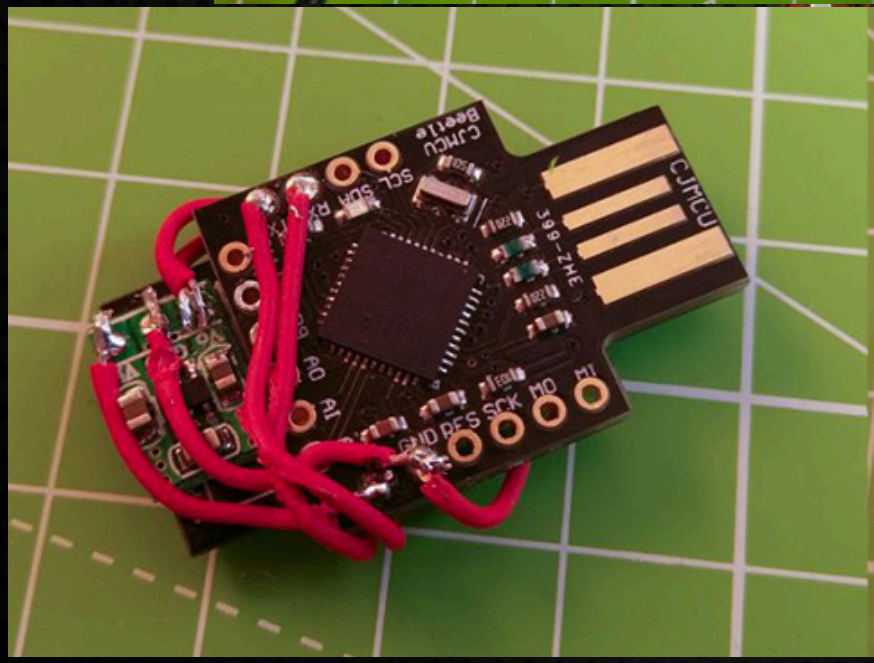
Attracco HID: Human Interface Device

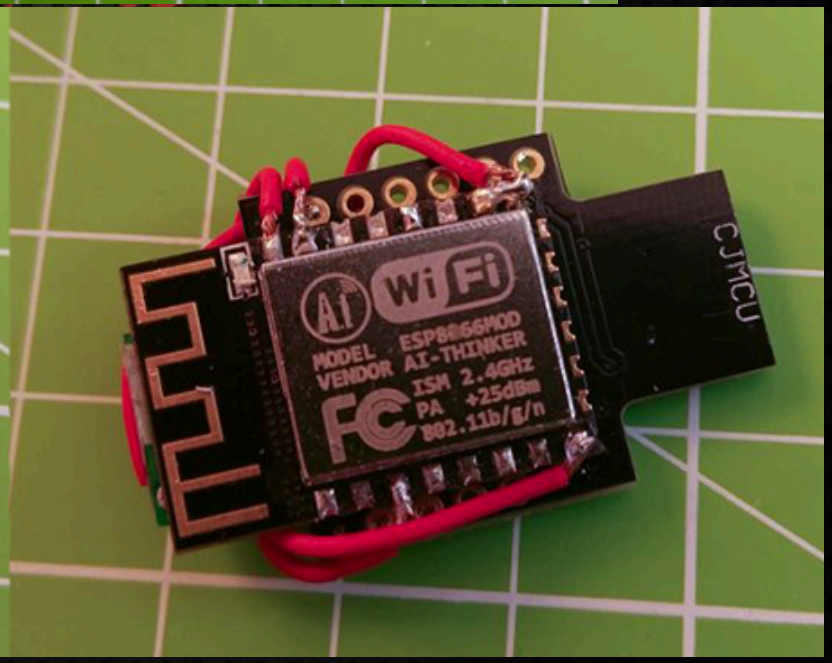


Attracco HID: Human Interface Device

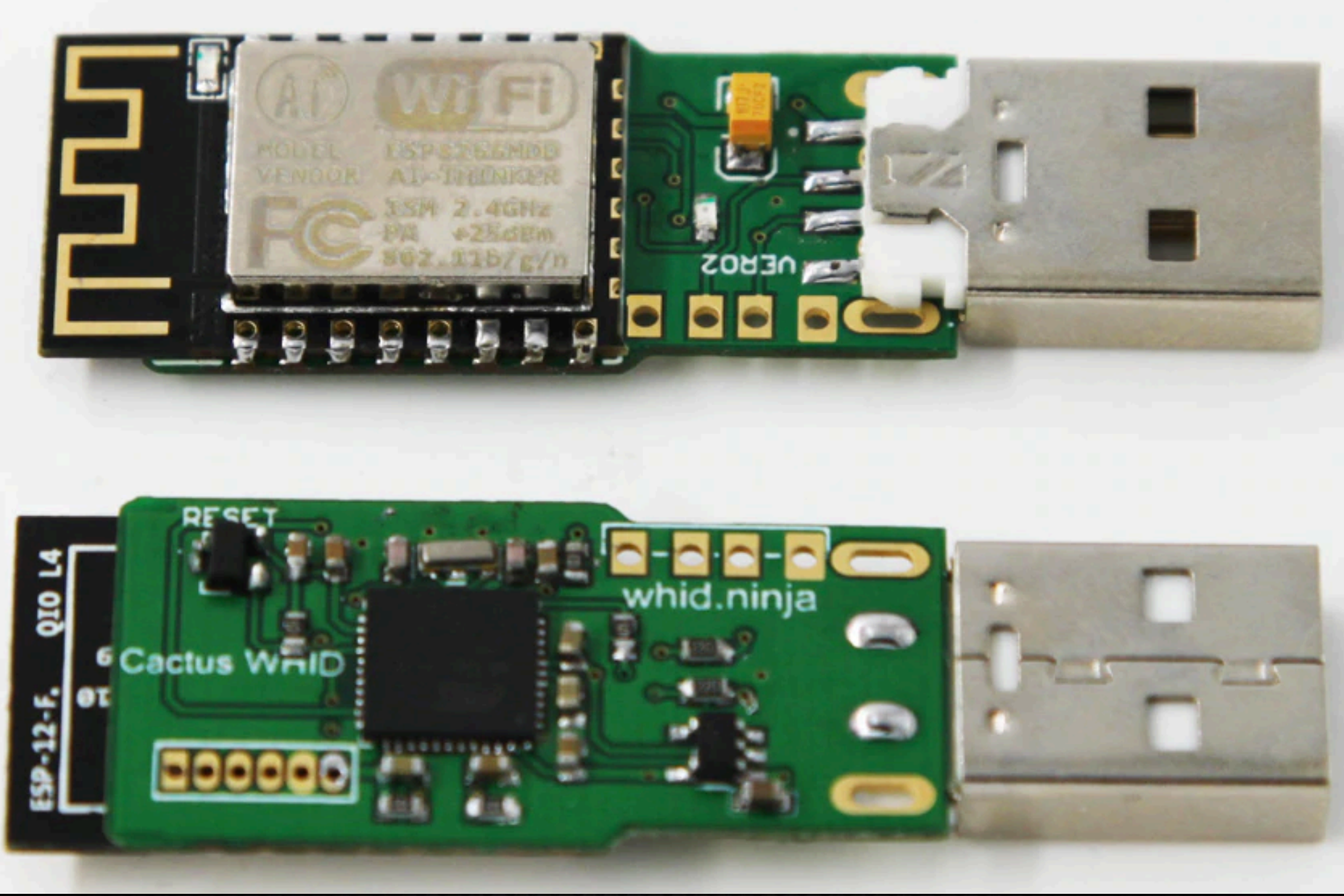



POWER
OTG


CJMCU
SCL SDA RX TX
GND RES SCK MO MI

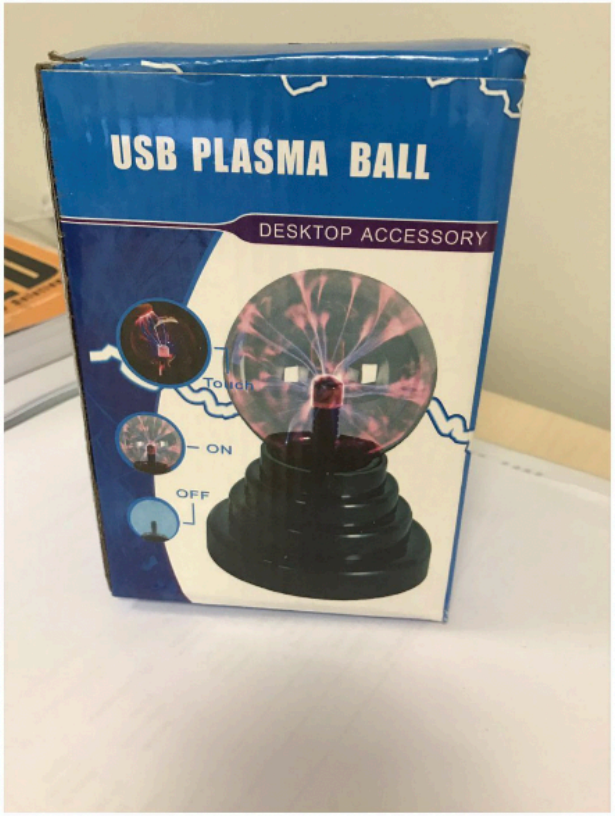

Ai WiFi
MODEL ESP8266MOD
VENDOR AI-THINKER
ISM 2.4GHz
PA +25dBm
802.11b/g/n
CJMCU

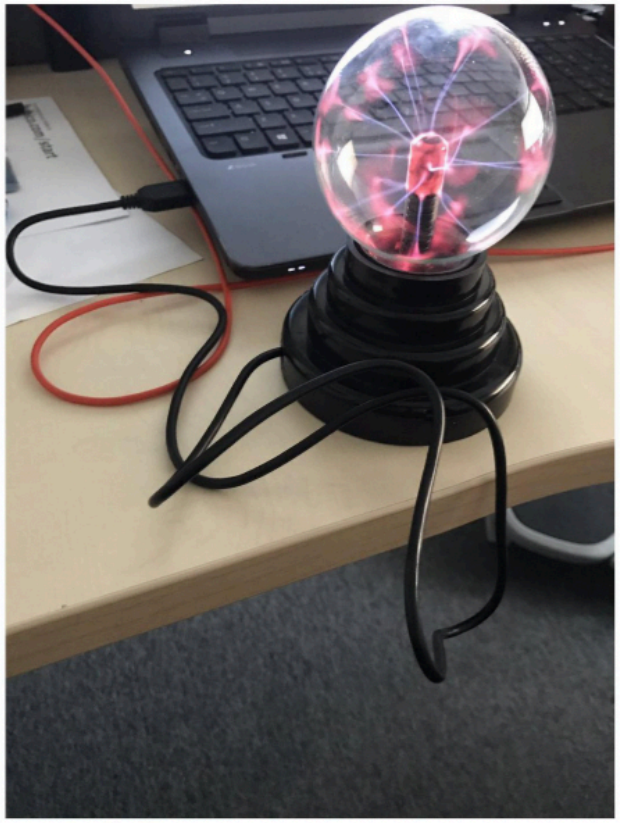
Cactus WHID



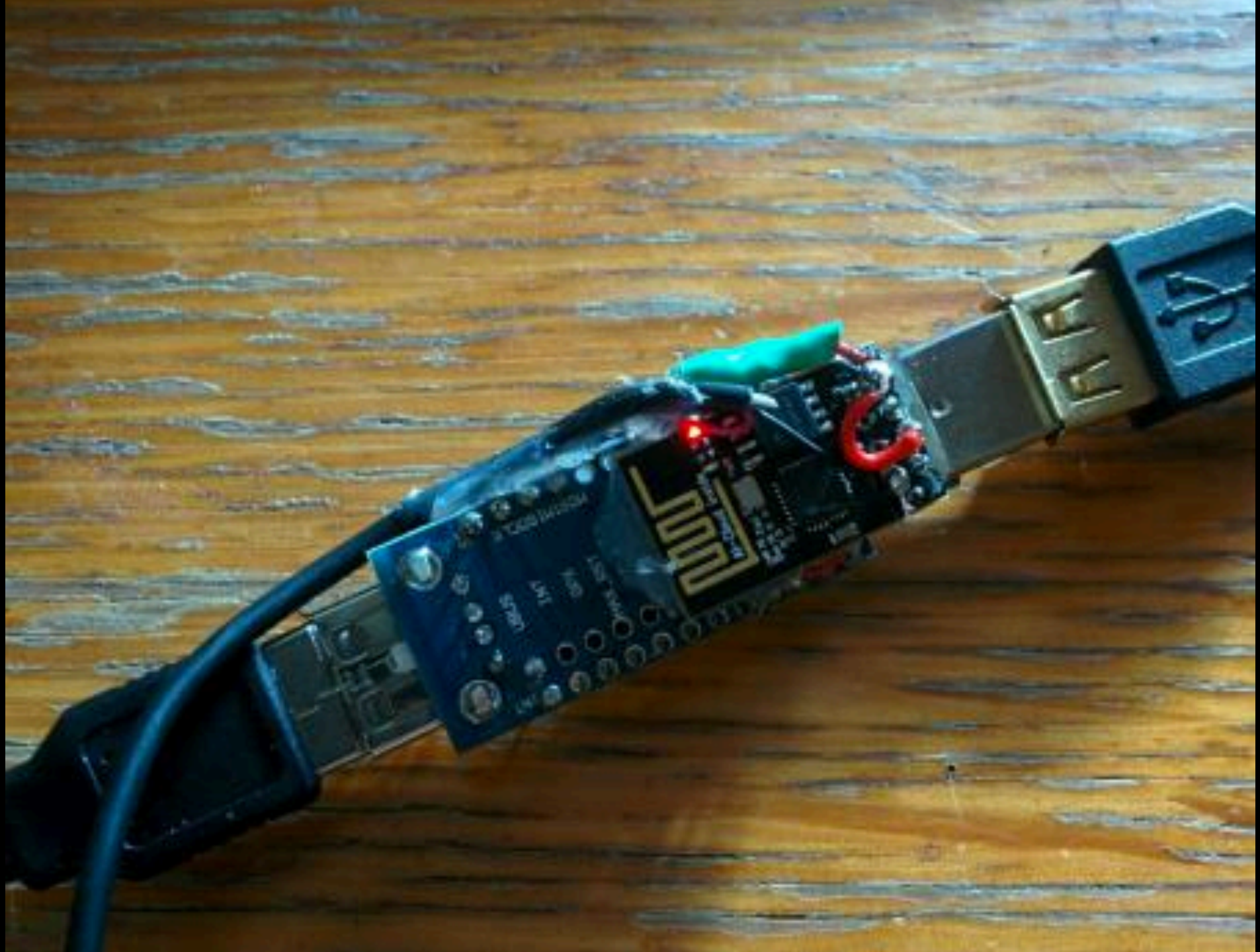
Cactus WHID

Cactus WHID



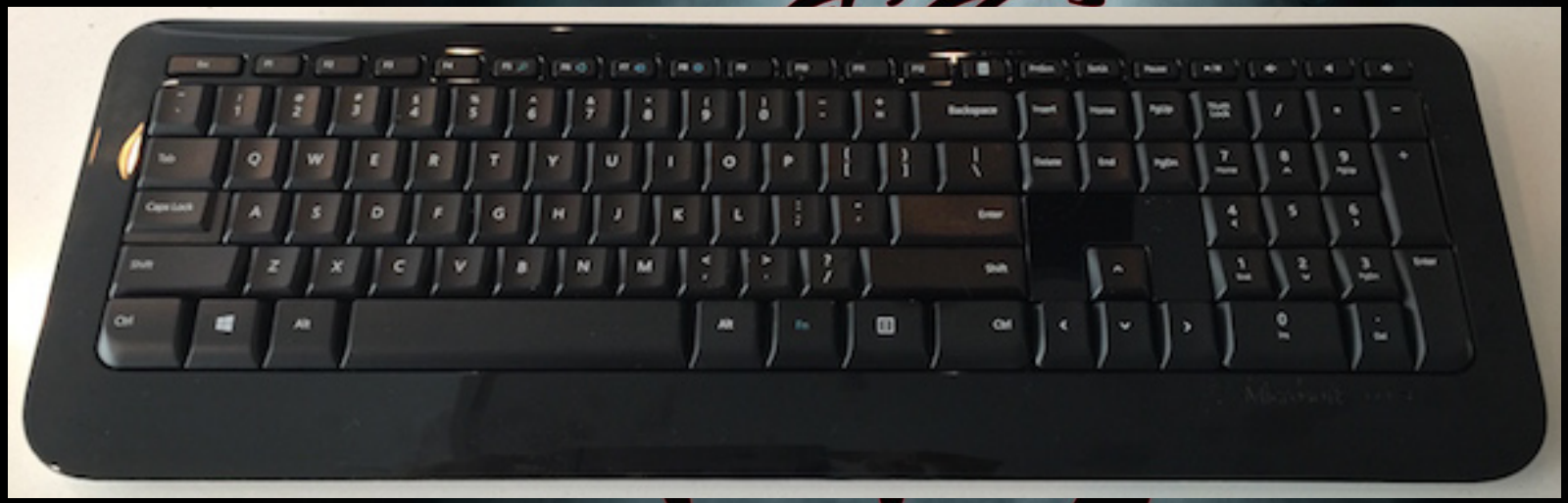


Cactus WHID

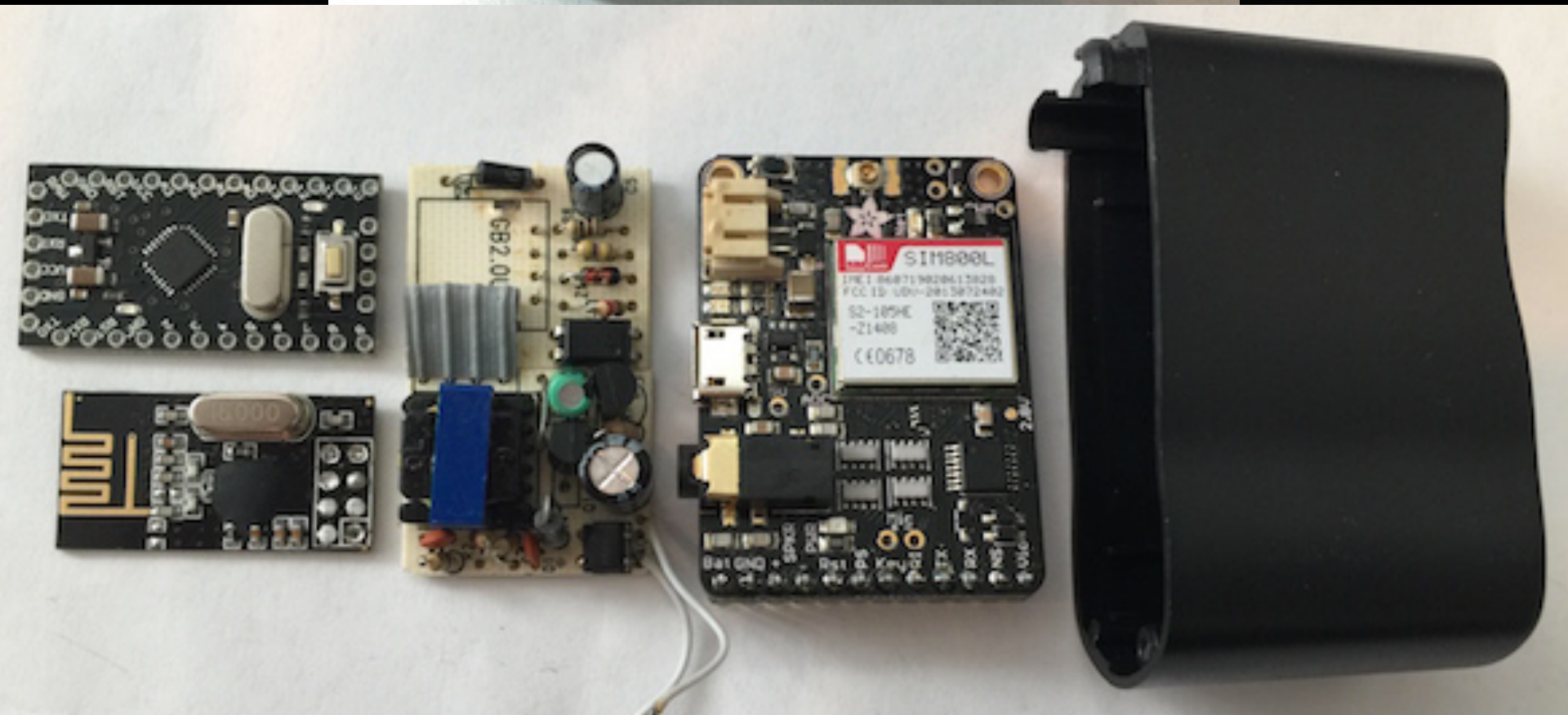



Keylogger

KeySweeper



è un dispositivo basato su Arduino, camuffato come un caricatore da muro USB funzionante, che sniffa in modalità wireless, decodifica, registra e riporta tutte le battute di una tastiera Microsoft wireless (che utilizza un protocollo RF proprietario da 2,4 GHz).


SIM800L

Le sequenze di tasti vengono trasmesse tramite un chip GSM, possono essere archiviate localmente o consegnate in modalità wireless nel raggio di trasmissione.

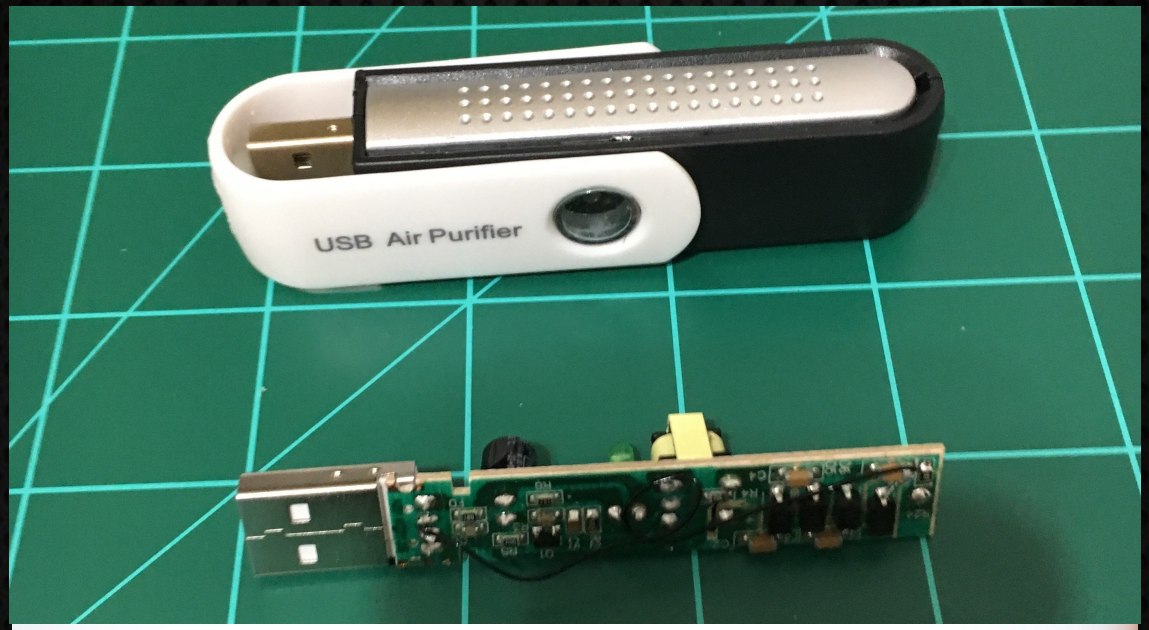
Se viene rimosso dalla presa di corrente, pur sembrando spento, il dispositivo continua a funzionare in modo nascosto utilizzando una batteria interna che viene ricaricata automaticamente.

VI RACCOMANDO

di non accettate mai caramelle dagli sconosciuti….

nemmeno USB

USB Killer



Il mondo tecnologico è talmente vasto ed in continua evoluzione che vale sempre la storica frase:

CHI SI FERMA E' PERDUTO

Grazie per l'attenzione

domande?