Informatica forense

Massimo Carnevali

Massimo Carnevali
posta@massimocarnevali.com
https://it.linkedin.com/in/massimocarnevali

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

Informatica forense

- Digital Forensics

..

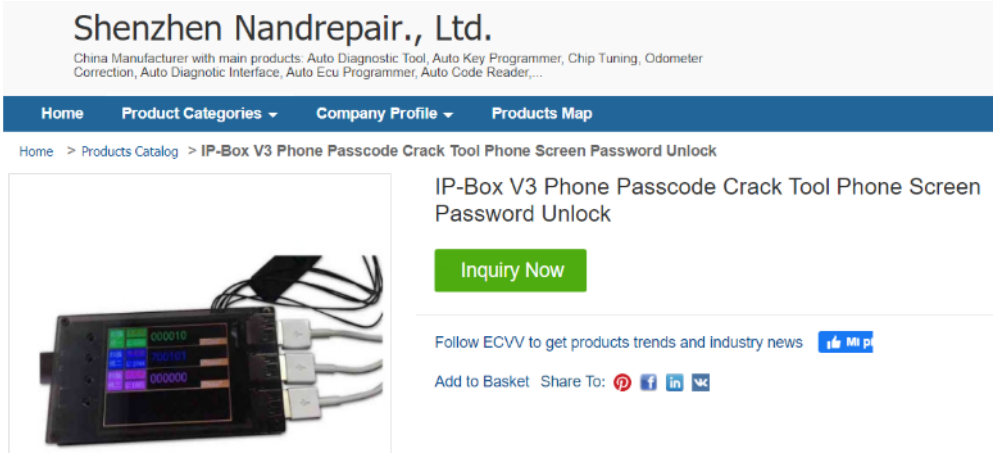
Digital Forensics

http://en.wikipedia.org/wiki/Digital_forensics

L'anatomo patologo del mondo digitale.
Fondamentale per avere delle prove valide in un processo per un crimine informatico.
Non bisogna contaminare la scena del crimine (ad esempio non spegnere uno smartphone ma metterlo in modalità “aereo” http://www.bbc.com/news/technology-29464889 per evitare brutte sorprese).
Garantire autenticità e affidabilità dei dati recuperati dai dispositivi (ove possibile con riproducibilità delle operazioni). Scientificità in tutte le fasi di gestione dell'«evidenza». Conoscere le debolezze della tecnologia su cui si sta operando e scegliere la migliore soluzione caso per caso.

Digital Forensics

Magari non mi presento da un giudice con dei dati estratti da un iPhone con un dispositivo da 230€ cinese comperato online ...



https://www.ecvv.com/product/4859099.html

Cosa può aver fatto ai dati del mio telefono quel dispositivo non è dato a sapere per cui la prova, a livello legale, non è più valida (ma le informazioni se mi servono ce le ho …).
Nota: **AL MOMENTO** il dispositivo **disponibile in rete** non funziona con gli ultimissimi iPhone.

Digital Forensics

Ma si trovano anche rivenditori ufficiali.

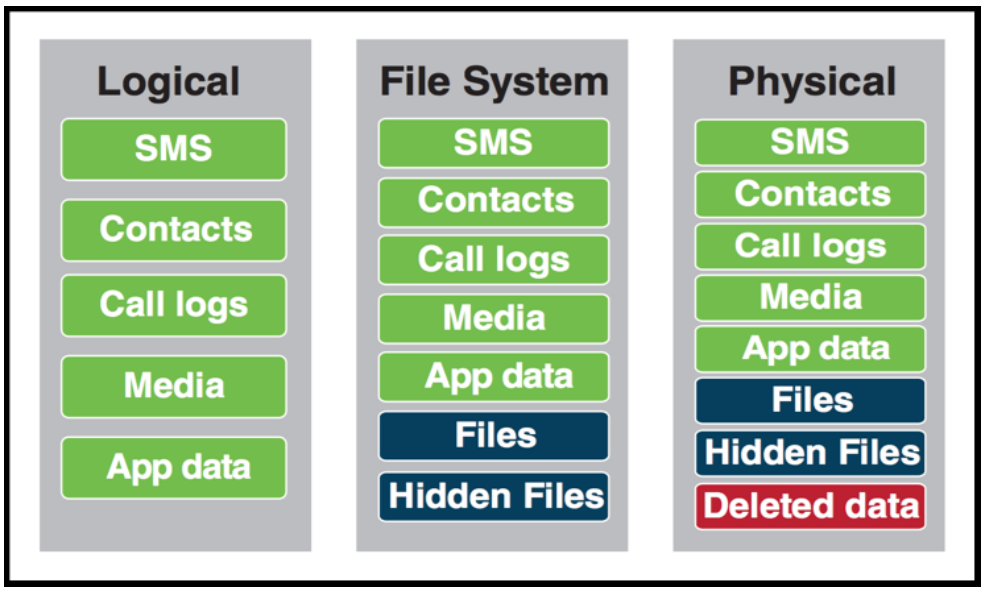
Cellebrite Rugged PRO

Ad esempio i prodotti Cellebrite
https://www.cellebrite.com/en/platforms/
Nuovo 6000$, c'è chi l'ha trovato usato e pieno di dati su E-bay per 100$
https://www.forbes.com/sites/thomasbrewster/2019/02/27/the-feds-favorite-iphone-hacking-tool-is-selling-on-ebay-for-100and-its-leaking-data/#5a2f732f5dd4
Israeliani ma sponsorizzati dagli USA
https://www.forbes.com/sites/thomasbrewster/2017/04/13/post-trump-order-us-immigration-goes-on-mobile-hacking-spending-spree/#365793b0a1fc

CELLEBRITE SAYS IT CAN UNLOCK ANY IPHONE FOR COPS
https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android/

Digital Forensics

Diversi livelli di estrazione dei dati da telefono



 6

Livello logico, sistema operativo

https://privacyinternational.org/long-read/3256/technical-look-phone-extraction

Digital Forensics

La storia curiosa di una indagine, parlando di gatti, macchine e telefoni:
The Koobface malware gang – exposed!

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Digital Forensics

Command&control srv → statistiche → file corposo → backup → sorgenti →

- Numeri di telefono → Russia
- Immagine → exif → San Pietroburgo
- Nickname → annunci online
  - Gatti → email e nickname
  - Auto → numero di targa

email+nickname → Facebook (profilo bloccato e nome fittizio ma c'è la fotografia, e gli amici, non bloccati, la moglie) → immagini della macchina corrente, della casa, del luogo di lavoro → nome dell'azienda → sede a San Pietroburgo → ricerca sui social dei dipendenti → immagine corrisponde → abbiamo nome, faccia, telefono, mail ecc.

La prossima ricerca potresti essere tu ...

https://nakedsecurity.sophos.com/koobface/
Koobface=importante attacco Malware con un meccanismo di Command e Control

Semplificazione dei passaggi, per il dettaglio con tutti gli screenshot vedi documento sophos_koobface_article.pdf