Computer forensics

Łukasz Dzwoniarek

Computer forensics

Celem jest zbadanie cyfrowych nośników informacji, w celu identyfikacji, zachowania, odzyskania i analizy informacji na nich zawartych

Wykorzystywana w sporach z kodeksu karnego i cywilnego

Metody są często zbliżone do technik odzyskiwania danych, posiadają jednak dodatkowe procedury związane z niepodważalnością dowodów w sądzie.

Komputery osobiste

Co Windows pamięta ?

- ID podłączanych urządzeń USB
- Link files - lista otwartych plików (z czasem)
- BagMRU - klucz rejestru pokazującego aktywność danego użytkownika
- Jump lists - “ostatnio otwarte” dla danego programu
- wyczyszczenie historii stron często nie wystarcza: strony przechowują wiele dodatkowych informacji na komputerze

Unix

Logi systemowe

Czas ostatniego odczytu

Kali Linux - dystrybucja dostosowana do potrzeb informatyki śledczej i badania podatności systemów

Autopsy - oprogramowanie do analizy zawartości dysków twardych, potrafi automatycznie analizować metadane plików, rozpakowywać archiwa, oraz tworzyć raporty na podstawie zgromadzonych danych

Defcon 21 - Forensic Fails - *Shift + Delete Won't Help You Here*

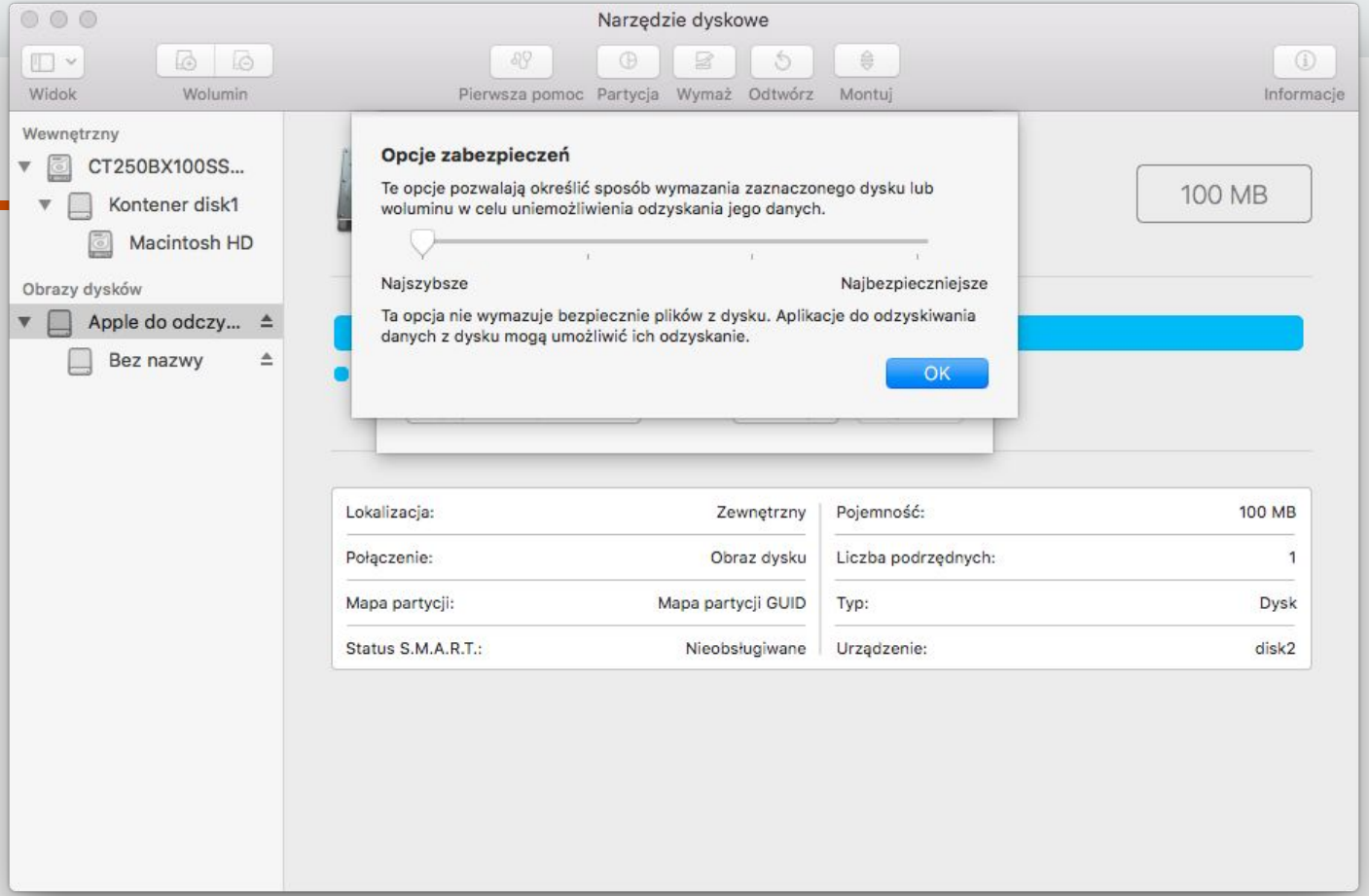
- skasowane pliki to pierwsza rzecz poddawana dokładnej analizie
- zapisywanie wzorcem np. “f**k” nie jest dobrym pomysłem, ale bez tego prawie zawsze da się wykryć zamazywanie danych
- zmiana rozszerzenia nie pomaga np. MP3 o rozmiarze 300MB
    - File Signature Analysis
- Outlook.PST - uszkodzenie pliku uruchamia mechanizm odzyskiwania, który odzyskuje skasowane pliki

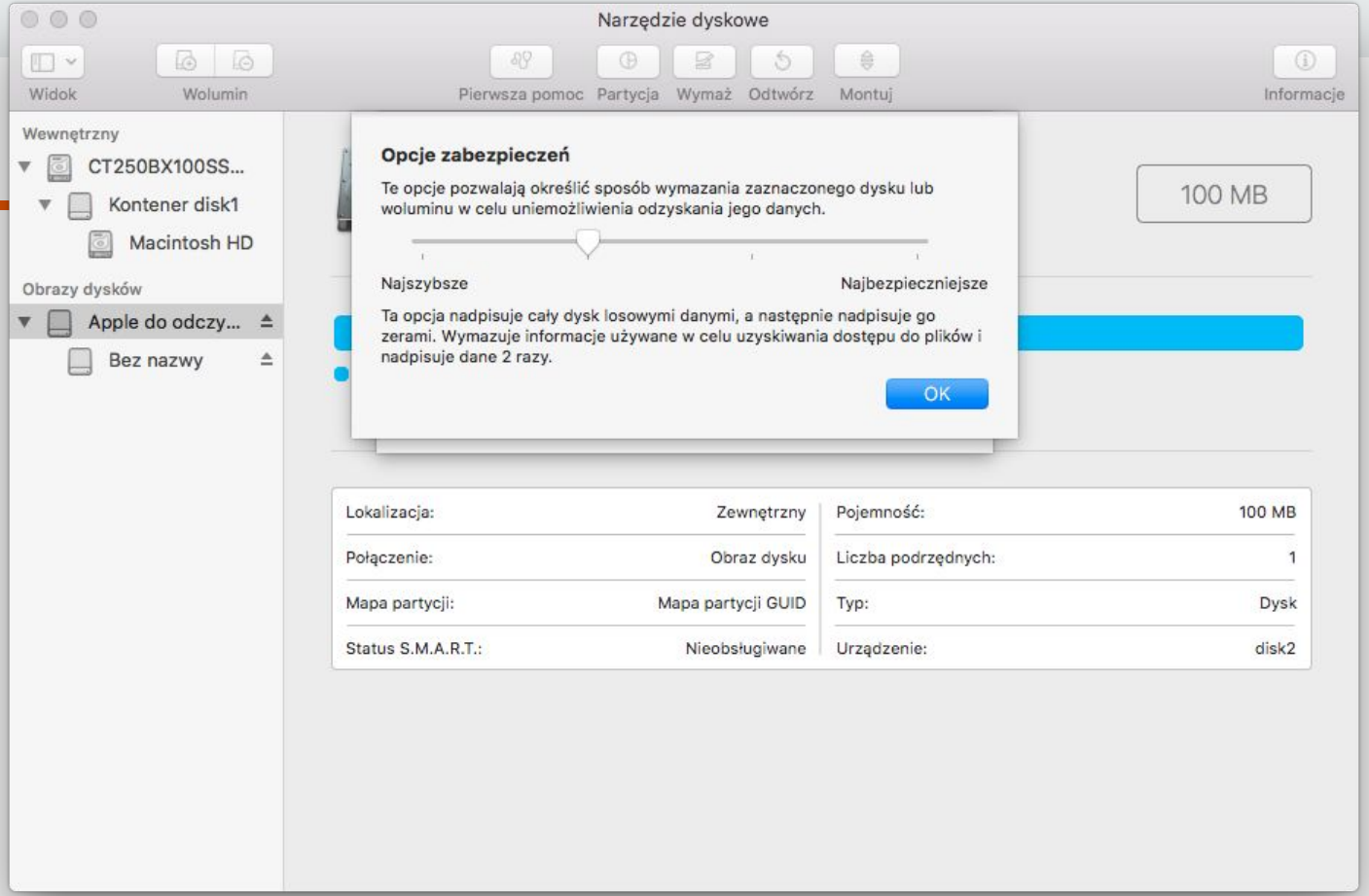
Odzyskiwanie danych z dysków HDD

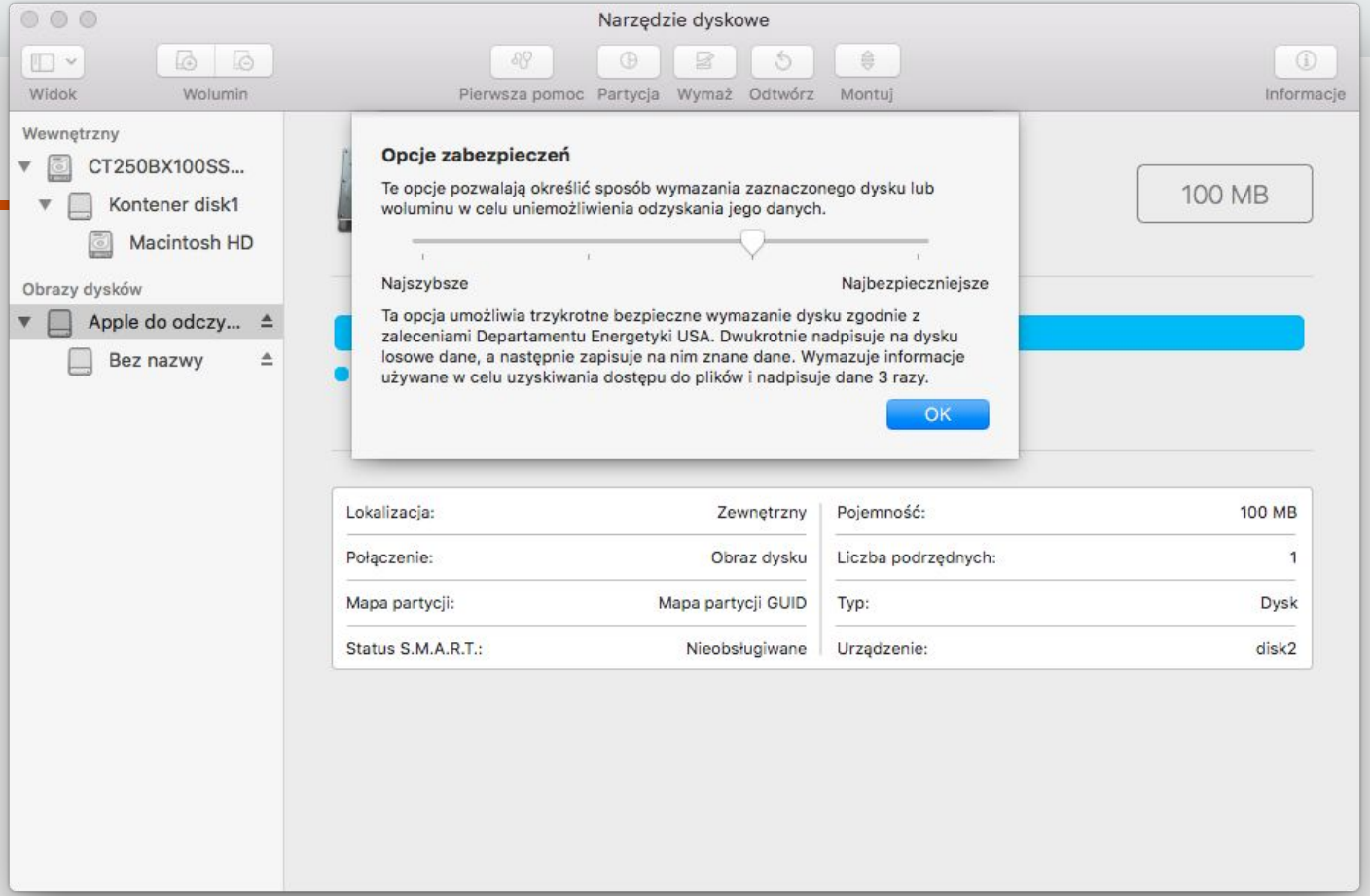
- *Kurs: Odzyskiwanie danych* - Tomasz Wierzbicki
- Popularne formaty obsługują dzienniki aktywności dyskowej
  - NTFS
  - ext4
  - HFS Plus
- Przydatne programy
  - Windows: Acronis Disk Suite
  - Linux: testdisk, tsk, ntfs3g, photorec, ntfsundelete
  - Mac: Disk Drill

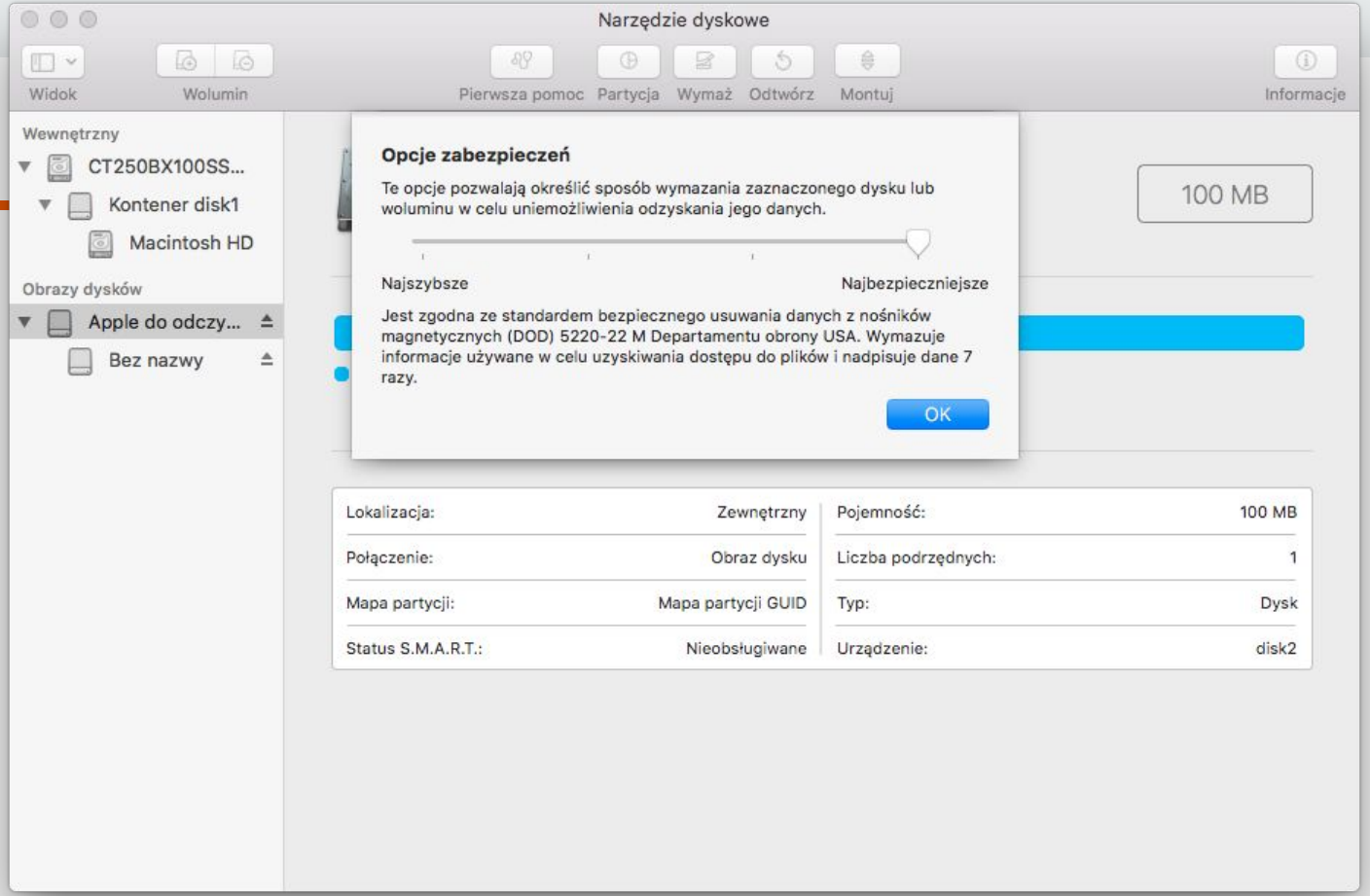
Afera Watergate

- Nieudana próba zainstalowania podsłuchu w siedzibie sztabu wyborczego amerykańskiej Partii Demokratycznej w Waszyngtonie.
- 17 czerwca 1972 przyłapano na gorącym uczynku pięć osób biorących udział w tej operacji.
- Zniknięcie 18 minut nagrania z kluczowej taśmy, co było fałszywie usprawiedliwiane przez Biały Dom pomyłką sekretarki.


Narzędzie dyskowe
Widok
Wolumin
Pierwsza pomoc
Partycja
Wymaż
Odtwórz
Montuj
Informacje
Wewnętrzny
CT250BX100SS...
Kontener disk1
Macintosh HD
Obrazy dysków
Apple do odczy...
Bez nazwy
Opcje zabezpieczeń
Te opcje pozwalają określić sposób wymazania zaznaczonego dysku lub woluminu w celu uniemożliwienia odzyskania jego danych.
Najszybsze
Najbezpieczniejsze
Ta opcja nie wymazuje bezpiecznie plików z dysku. Aplikacje do odzyskiwania danych z dysku mogą umożliwić ich odzyskanie.
OK
100 MB
Lokalizacja: Zewnętrzny
Połączenie: Obraz dysku
Mapa partycji: Mapa partycji GUID
Status S.M.A.R.T.: Nieobsługiwane
Pojemność: 100 MB
Liczba podrzędnych: 1
Typ: Dysk
Urządzenie: disk2

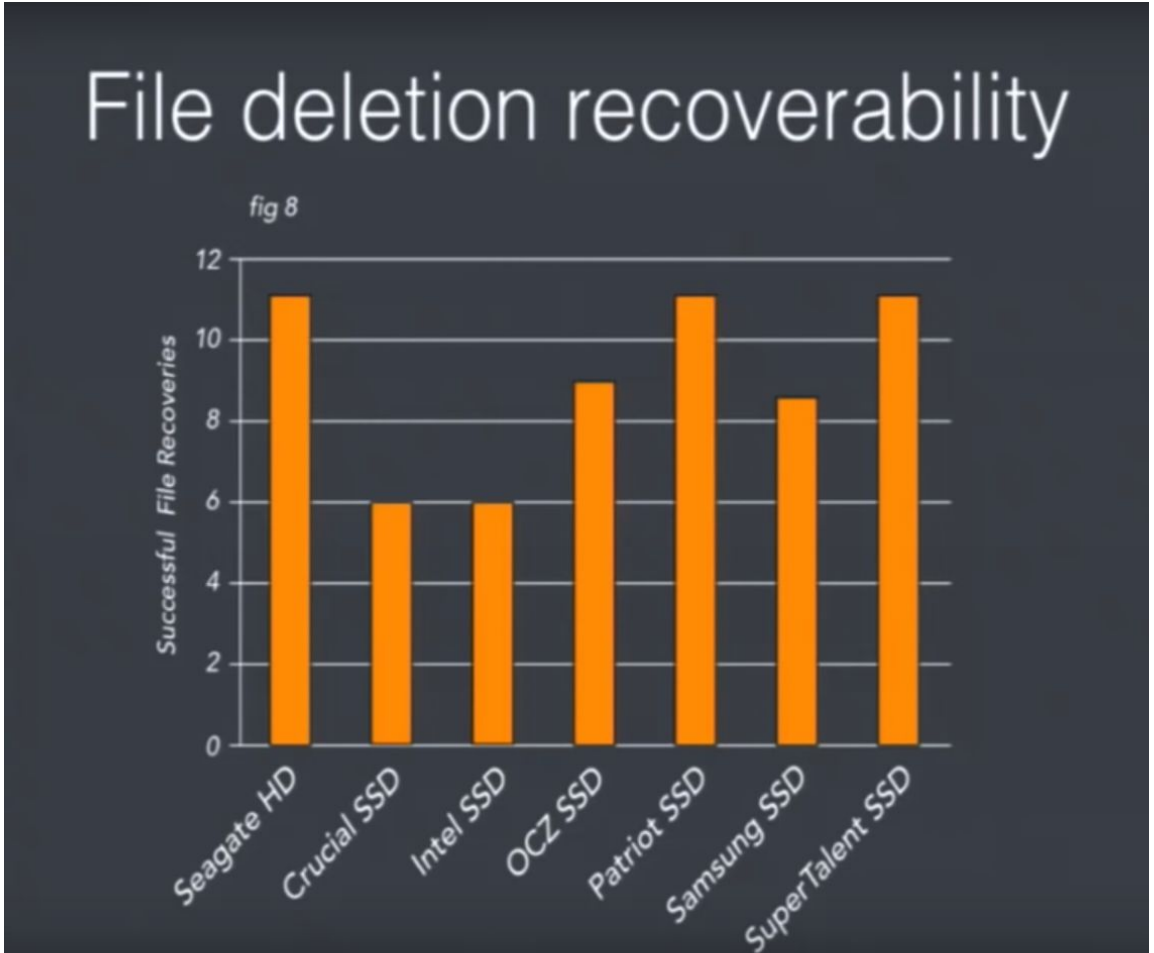

Narzędzie dyskowe
Widok
Wolumin
Pierwsza pomoc
Partycja
Wymaż
Odtwórz
Montuj
Informacje
Wewnętrzny
CT250BX100SS...
Kontener disk1
Macintosh HD
Obrazy dysków
Apple do odczy...
Bez nazwy
100 MB
Opcje zabezpieczeń
Te opcje pozwalają określić sposób wymazania zaznaczonego dysku lub woluminu w celu uniemożliwienia odzyskania jego danych.
Najszybsze
Najbezpieczniejsze
Ta opcja nadpisuje cały dysk losowymi danymi, a następnie nadpisuje go zerami. Wymazuje informacje używane w celu uzyskiwania dostępu do plików i nadpisuje dane 2 razy.
OK
Lokalizacja: Zewnętrzny
Połączenie: Obraz dysku
Mapa partycji: Mapa partycji GUID
Status S.M.A.R.T.: Nieobsługiwane
Pojemność: 100 MB
Liczba podrzędnych: 1
Typ: Dysk
Urządzenie: disk2

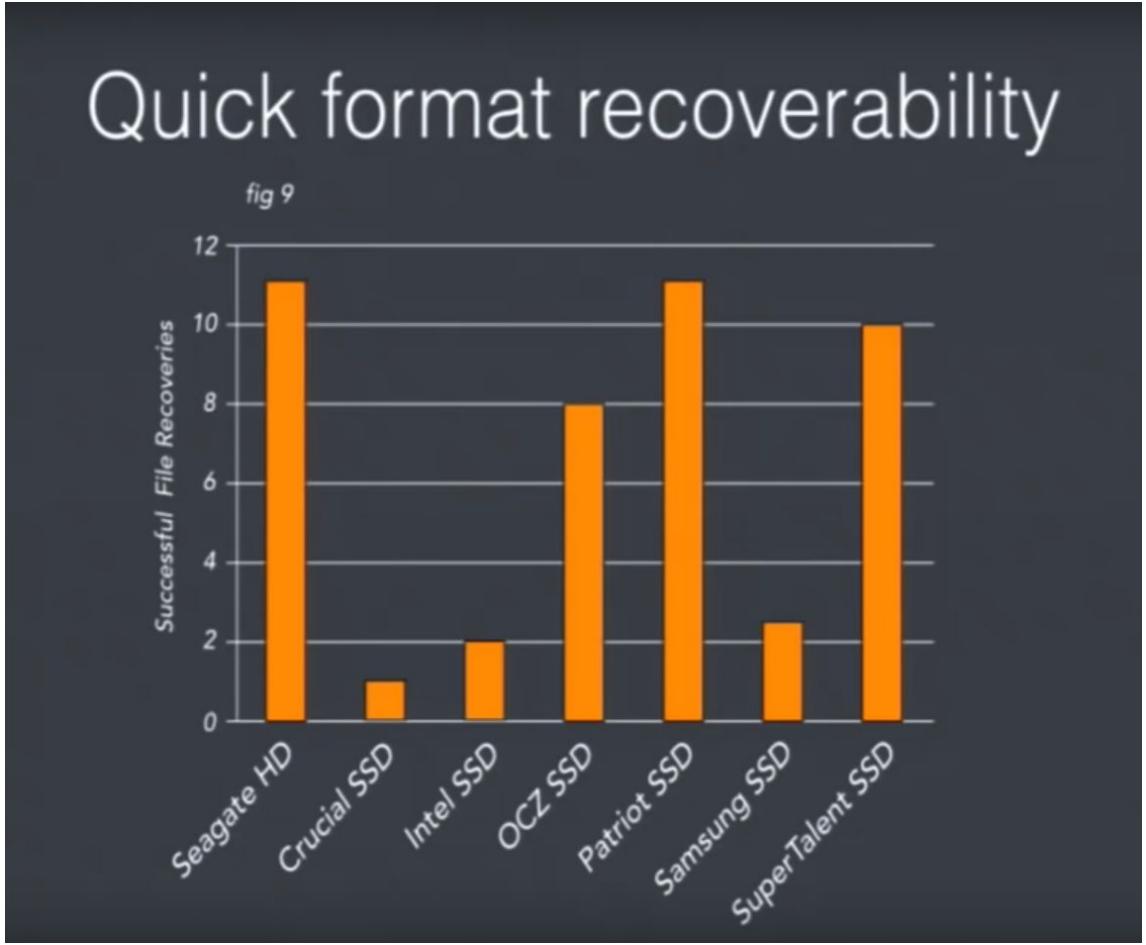

Narzędzie dyskowe
Widok
Wolumin
Pierwsza pomoc
Partycja
Wymaż
Odtwórz
Montuj
Informacje
Wewnętrzny
CT250BX100SS...
Kontener disk1
Macintosh HD
Obrazy dysków
Apple do odczy...
Bez nazwy
100 MB
Opcje zabezpieczeń
Te opcje pozwalają określić sposób wymazania zaznaczonego dysku lub woluminu w celu uniemożliwienia odzyskania jego danych.
Najszybsze
Najbezpieczniejsze
Ta opcja umożliwia trzykrotne bezpieczne wymazanie dysku zgodnie z zaleceniami Departamentu Energetyki USA. Dwukrotnie nadpisuje na dysku losowe dane, a następnie zapisuje na nim znane dane. Wymazuje informacje używane w celu uzyskiwania dostępu do plików i nadpisuje dane 3 razy.
OK
Lokalizacja: Zewnętrzny
Połączenie: Obraz dysku
Mapa partycji: Mapa partycji GUID
Status S.M.A.R.T.: Nieobsługiwane
Pojemność: 100 MB
Liczba podrzędnych: 1
Typ: Dysk
Urządzenie: disk2


Narzędzie dyskowe
Widok
Wolumin
Pierwsza pomoc
Partycja
Wymaż
Odtwórz
Montuj
Informacje
Wewnętrzny
CT250BX100SS...
Kontener disk1
Macintosh HD
Obrazy dysków
Apple do odczy...
Bez nazwy
Opcje zabezpieczeń
Te opcje pozwalają określić sposób wymazania zaznaczonego dysku lub woluminu w celu uniemożliwienia odzyskania jego danych.
Najszybsze
Najbezpieczniejsze
Jest zgodna ze standardem bezpiecznego usuwania danych z nośników magnetycznych (DOD) 5220-22 M Departamentu obrony USA. Wymazuje informacje używane w celu uzyskiwania dostępu do plików i nadpisuje dane 7 razy.
OK
100 MB
Lokalizacja: Zewnętrzny
Połączenie: Obraz dysku
Mapa partycji: Mapa partycji GUID
Status S.M.A.R.T.: Nieobsługiwane
Pojemność: 100 MB
Liczba podrzędnych: 1
Typ: Dysk
Urządzenie: disk2

Do SSDs Have a Mind of Their Own?

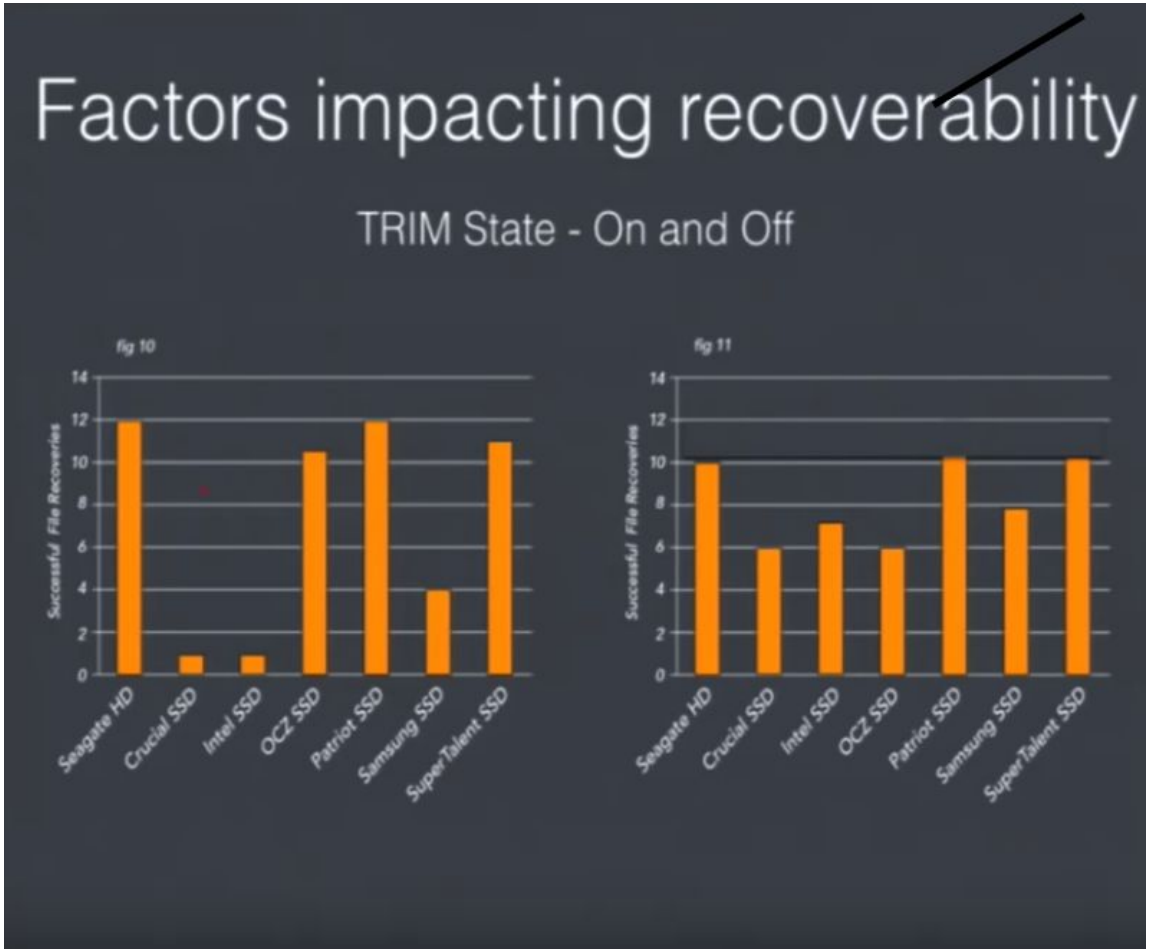
- DEF CON 24 - Tom Kopchak - *Sentient Storage: Do SSDs Have a Mind of Their Own*
- Dyski SSD zachowują się inaczej od SSD
- Szanse na odzyskanie plików zależą od
  - producenta 1-12%
  - TRIM 1-12% vs 6-12%
- Problem z obliczaniem sumy kontrolnej


File deletion recoverability
fig 8
Successful File Recoveries
12
10
8
6
4
2
0
Seagate HD
Crucial SSD
Intel SSD
OCZ SSD
Patriot SSD
Samsung SSD
SuperTalent SSD


Quick format recoverability
fig 9
Successful File Recoveries
12
10
8
6
4
2
0
Seagate HD
Crucial SSD
Intel SSD
OCZ SSD
Patriot SSD
Samsung SSD
SuperTalent SSD

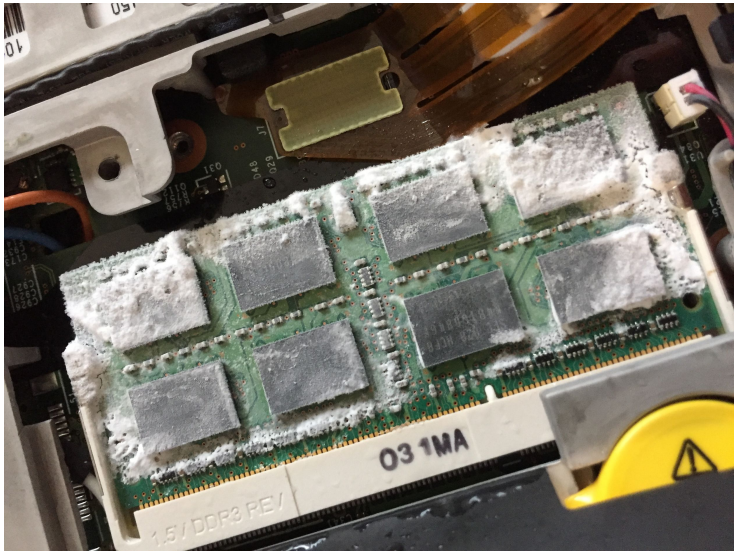
Factors impacting recoverability

TRIM State - On and Off

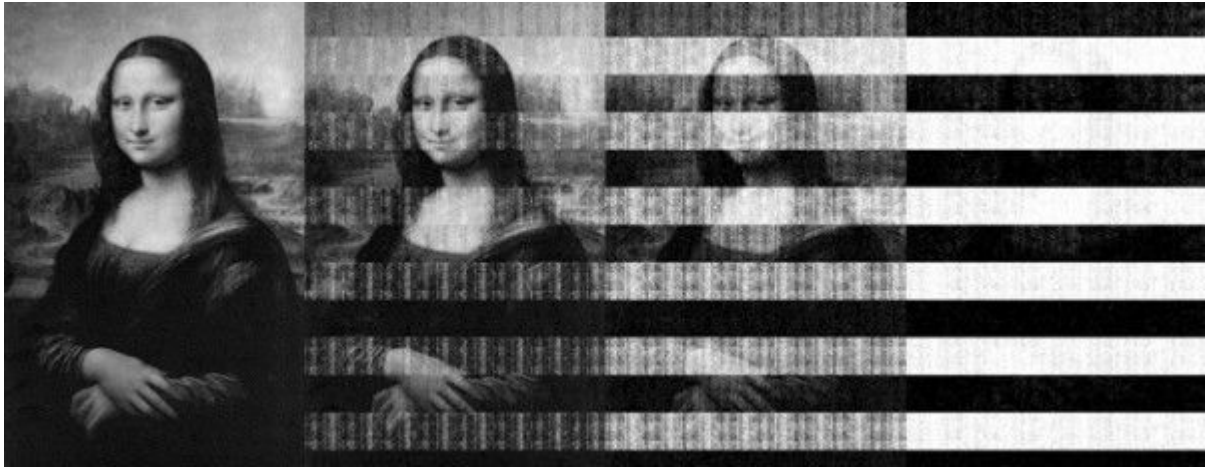


Szyfrowanie dysku nie zawsze wystarczy

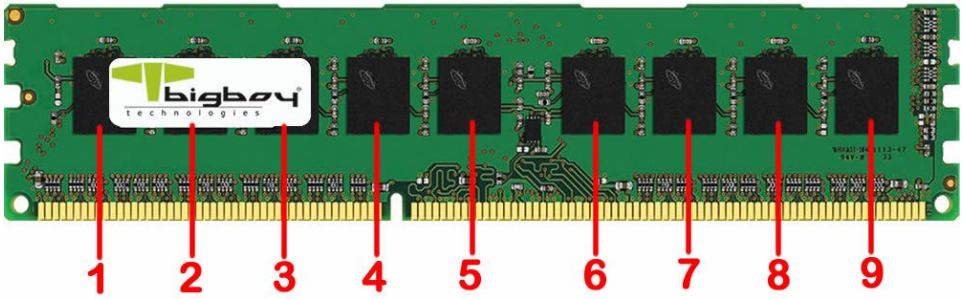
Marko Schuba
nullcon Goa 2015
Cold Boot Attack on DDR2 and DDR3 RAM

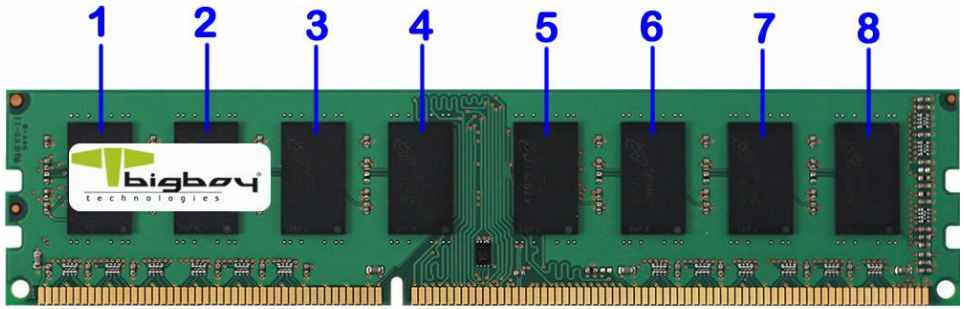


Odczyt z pamięci po 30 sekundach, 60 sekundach i 5 minutach:



ECC RAM





Non-ECC RAM

Nie-progrmistyczne metody “usuwania” danych

DEF CON 23
Zoz
And That's How I Lost My Other Eye...Explorations in Data Destruction

https://www.youtube.com/watch?v=-bpX8YvNg6Y&feature=youtu.be&t=3

Chemiczne metody destrukcji

Mechaniczne metody destrukcji

Urządzenia mobilne

Analiza telefonów komórkowych

- W przeciwieństwie do komputerów telefon podczas badania jest cały czas włączony
- Kluczowe znaczenie ma jednak jego izolacja od sieci GSM
- Popularne usługi typu FindMyiPhone czy Find My Android mogą umożliwić właścicielowi zdalne kasowanie danych
    - Wi-Fi vs security

Karta SIM

- Ma ograniczoną pojemność.
- Telefon decyduje jakie informacje będą na niej zapisywane
    - Możemy znaleźć kontakty wraz z numerami telefonów, wiadomości tekstowe oraz rejestr ostatnio wykonanych połączeń (bez informacji o dacie połączenia i czasie trwania)
- Trzeba wykonać jej kopię

Pamięć telefonu

- informacje o połączeniach,
- wiadomości tekstowe SMS,
- historia rozmów w komunikatorach (np. Signal, WhatsApp)
- kontakty
- kalendarz,
- notatki,
- zdjęcia,
- pliki multimedialne,
- historia odwiedzonych stron internetowych,
- szereg innych danych, w zależności od systemu operacyjnego i wykorzystywanych aplikacji

Pamięć telefonu

Telefony komórkowe starszej generacji w większości nie posiadają złącz typu USB, w związku z powyższym podłączenia dokonuje się za pomocą tzw. boxów serwisowych podłączanych kablami do pól ulokowanych m.in bezpośrednio pod baterią.

W nowych modelach smartfonów podłączenie boxów serwisowych do odpowiednich punktów serwisowych (JTAG – ang. Joint Test Action Group)

Szczególnym aspektem analizy, jest to, że każdy producent telefonów w różny sposób definiuje zapis danych w pamięci telefonu. Bardzo często zdarza się, że model implementacji danych u danego producenta zmienia się zależnie od modelu.

FBI vs Apple

- FBI jest w posiadaniu iPhona 5C terrorysty (model A1532 z chipem A6 pracujący pod kontrolą systemu operacyjnego iOS 9 — gdyby był to iOS w wersji poniżej wersji 8, problemu z dostępem do danych nie byłoby żadnego).
- Telefon jest zablokowany, ale nie hasłem alfanumerycznym a maksymalnie 6 cyfrowym PIN-em.
- Ten model iPhona nie posiada czytnika linii papilarnych, więc nie można go odblokować przykładając doń palec martwego terrorysty.
- FBI musi więc odgadnąć PIN, ale ma tylko 10 prób, ponieważ na urządzeniu włączone jest zabezpieczenie polegające na kasowaniu danych po 10 błędnie wprowadzonych PIN-ach.
- Pamięć iPhona jest zaszyfrowana sprzętowym kluczem skojarzonym z tym konkretnym urządzeniem i nieznanym przez Apple, więc wykonanie tzw. chip-off (wylutowanie chipa i podpięcie do innego urządzenia) nic nie da.

FBI: attack vector

- iCloud - na kilka tygodni przed zamachem, terrorysta wyłączył backup do chmury
  - FBI już w dzień po pozyskaniu telefonu zwróciło się do jego właściciela — i tu niespodzianka, nie był nim terrorysta, a rządowa organizacja, w której pracował — o to, aby pracodawca terrorysty zresetował hasło do konta iCloud skojarzonego z telefonem.
  - Analiza metodą decappingu
- Metoda 3: klucze parujące pozyskane z komputera

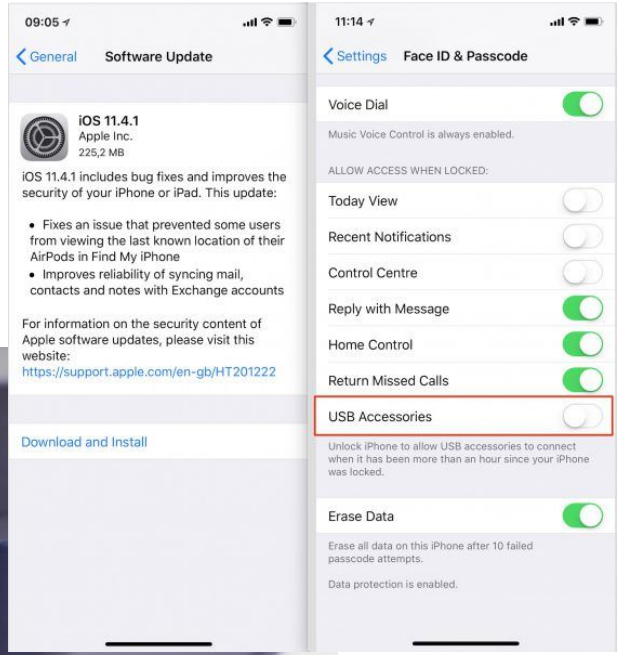
  terrorysta poza służbową, pozyskaną przez FBI komórką, posiadał także prywatny telefon, to odpowiadam — tak, ale go zniszczył przed zamachem. Podobnie jak zniszczył dysk twardy swojego komputera

iOS USB Restricted Mode

GreyKey

od Greyshift

za 15 000 USD



Greyshift

Obecna rekomendacja dla służb i informatyków śledczych jest następująca:

1. Po zarekwirowaniu iPhone podłącz go pod przejściówkę Lightning-do-USB

2. Pod port USB przejściówki podepnij battery packa.

3. Umieść całość w torbie Faradaya

iOS “panic button”

W iOS 11 pięciokrotne naciśnięcie przycisku “Sleep/Power” powodowało natychmiastową blokadę Touch ID.

iOS Device Dashboard

	iOS v1.0 -> v3.1	iOS v4	iOS v5	iOS v6	iOS v7	iOS v8	iOS v9
iPhone							
iPhone 3g							
iPhone 3gs							
iPhone 4							
iPad							
iPhone 4s							
iPhone 5							
iPhone 5c							
iPad 2							
iPad 3							
iPad 4							
iPad Mini							
iPhone 5s							
iPhone 6							
iPhone 6+							
iPad Air							
iPad Air 2							
iPad Mini 2							
iPad Mini 3							
iPad Mini 4							
iPad Pro							
iPhone 6s							
iPhone 6s+							

Reference Key	
	Commercial solutions available (XWays, Cellebrite, Lantern, etc)
	Unallocated space may be carved from
	File level encryption
$	Cellebrite Advanced Investigative Services
	Pairing File from synced computer may be used to bypass lock
	Pairing File from synced computer may be used to bypass lock providi
	iCloud backup may contain snapshots
	Law Enforcement/Legal Process options available
	Lock bypass solutions available: Celebrite Unlock Tool IP
	Apple Inc. may assist in unlocking of device with proper legal authorit

Google może zdalnie wyłączyć blokadę ekranu na Androidzie

Firma może na niektórych typach urządzeń z systemem Android zdalnie wyłączyć konieczność podania kodu do odblokowania urządzenia. Dzięki temu specjaliści z zakresu informatyki śledczej mogą uzyskać dostęp do danych użytkownika.

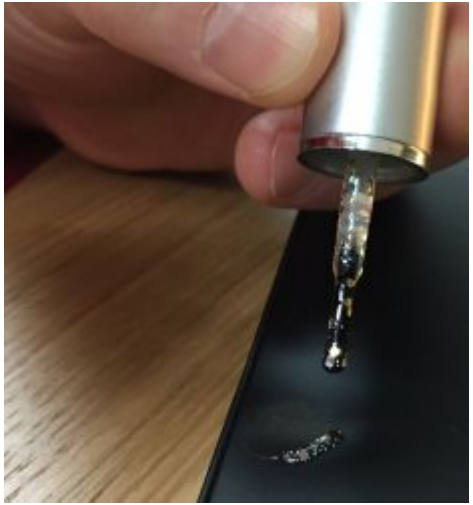
There are a larger variety of Android devices than Apple devices. Forensic examiners are able to bypass passcodes on some of those devices using a variety of forensic techniques. For some other types of Android devices, Google can reset the passcodes when served with a search warrant and an order instructing them to assist law enforcement to extract data from the device. This process can be done by Google remotely and allows forensic examiners to view the contents of a device.

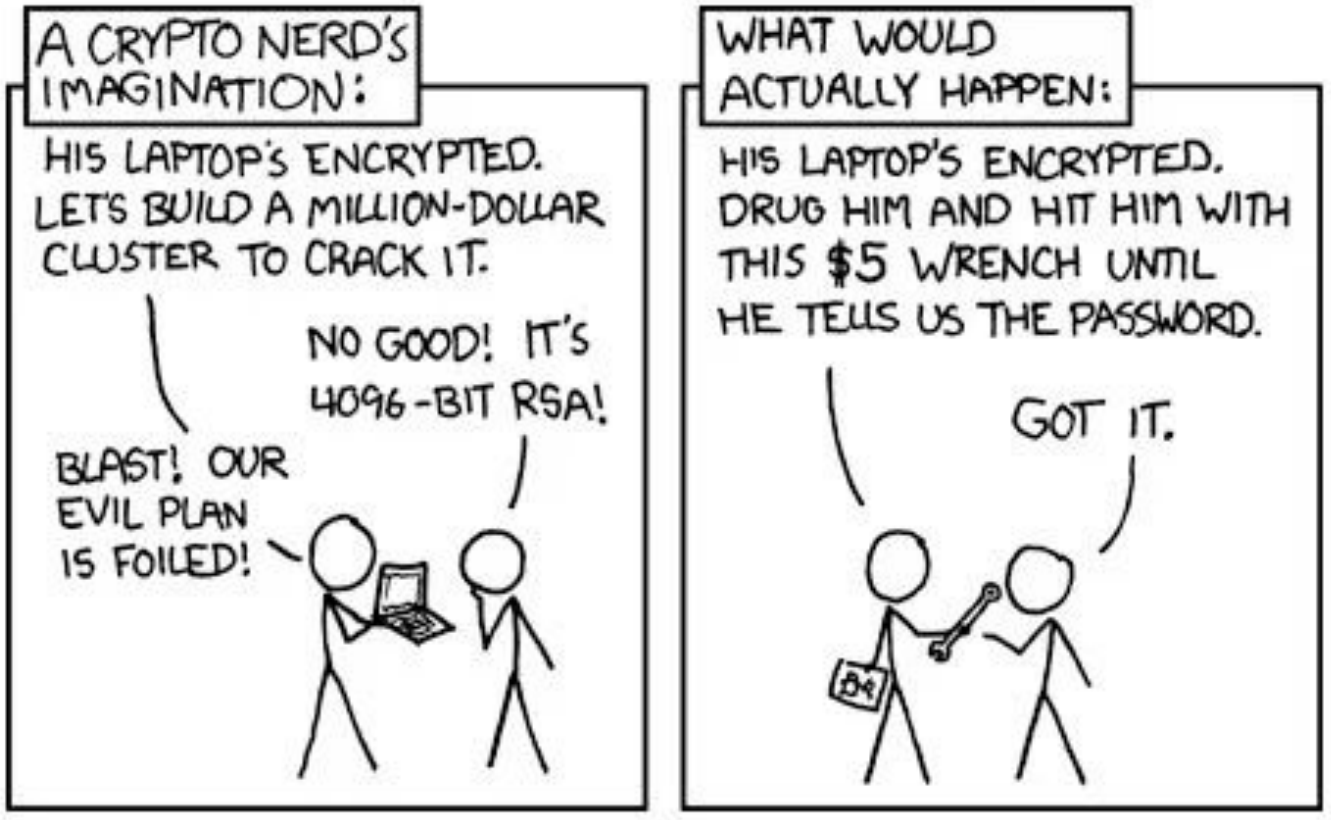
Jak się zabezpieczyć

- Korzystaj z hasła blokady ekranu a nie TouchID.
- Złamanie 6 cyfrowego kodu blokady ekranu na iPhonie zajmuje 22 godziny (pomiędzy próbami wymuszane jest opóźnienie 80 milisekund). Wystarczy jednak mieć 11 cyfrowy kod blokady ekranu, aby sprawdzenie wszystkich możliwych kombinacji zajęło 127 lat.
- Włącz opcję “Erase Data”, czyli kasowania danych z telefonu po 10 błędnie wprowadzonym haśle blokady.
- Wyłącz opcję “Notification view”, dzięki czemu nikt nie uzyska dostępu do historycznych powiadomień przy zablokowanym telefonie
- Wyłącz obsługę iClouda.
- Jeśli chęć odzyskania telefonu po jego zgubieniu ma dla Ciebie wyższy priorytet niż ochrona przed służbami (czyli nie jesteś terrorystą ani nie śpisz w czapeczce z folii aluminiowej na głowie), to rozważ włączenie FindMyiPhone.

Podsumowanie

Przetnij kable, zamaluj śruby




A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Czas na demo

Bibliografia

- https://niebezpiecznik.pl/post/wyjazd-do-rosji-na-co-uwazac-mundial/
- https://niebezpiecznik.pl/post/nowe-zabezpieczenie-iphona-przed-atakiem-zgadywania-hasla-mozna-obejsc-podpieciem-dowolnej-przejsciowki/
- https://niebezpiecznik.pl/post/iphone-bruteforce-pin-haslo-blokady-ekranu-obejscie/
- https://niebezpiecznik.pl/post/face-id-nowy-iphone-x-bedzie-odblokowywany-twarza-wlasciciela-czy-to-grozne/
- Defcon 21 - Forensic Fails - Shift + Delete Won't Help You Here
- https://niebezpiecznik.pl/post/3-sposoby-fbi-na-zhackowanie-zablokowanego-iphona/
-