When Encryption Baffles the Police: A Collection of Cases

This is a collection of cases where the police tried to decrypt encrypted computer data used by criminal suspects. In most (but not all) cases the authorities were not successful. Here's my RSA Conference Talk about this topic.

For German speaking readers: Wenn die Polizei gegenüber der Verschlüsselungstechnik kapitulieren muss

1. Daniel Dantas

Brazil, 2008

Suspected crime: financial offense

Daniel Dantas is a Brazilian banker and suspected financial criminal). Wikipedia writes: "In July 2008, several TrueCrypt-Encrypted hard drives were seized from Daniel Dantas, who was suspected of financial crimes. The Brazilian National Institute of Criminology (INC) tried for five months (without success) to obtain access to TrueCrypt-protected disks owned by the banker, after which they enlisted the help of the FBI. The FBI used dictionary attacks against Dantas' disks for over 12 months, but were still unable to decrypt them."

https://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/
https://en.wikipedia.org/wiki/Daniel_Dantas_%28entrepreneur%29

Encryption product used: TrueCrypt

Breaking of encryption successful: no

Case status: Dantas was convicted to ten years imprisonment

2. Sebastien Nussbaumer

Germany/Switzerland, 2012

Suspected crime: murder

Nussbaumer was arrested in Germany in 2012. The police can't decrypt his files.

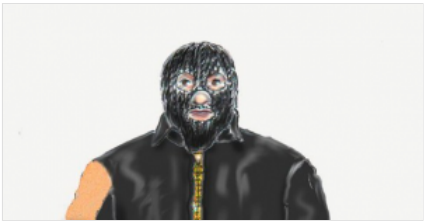
https://www.20min.ch/ausland/news/story/12293022
https://www.20min.ch/schweiz/news/story/12546537

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Nussbaumer was convicted to 12 years imprisonment

3. Martin Ney



Germany, 2012

Suspected crime: murder

Martin Ney (aka the Mask Man) is a children murderer. The police found several encrypted storage media in his possession but could not decrypt them.

https://www.focus.de/panorama/welt/verschluesselt-und-nicht-knackbar-polizei-scheitert-an-festplatten-des-maskenmanns_aid_705621.html

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Ney was convicted to life in prison

5. Oliver Drage

UK, 2010

Suspected crime: child porn

Suspected childporn dealer Oliver Drage from UK was convicted to a prison sentence because he did not reveal the password he had used to encrypt his hard drive.

https://blog.zdf.de/hyperland/2010/11/ab_in_den_knast_fur_verschluss/
https://www.theregister.co.uk/2010/10/06/jail_password_ripa/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Drage from UK was convicted to a prison sentence because he did not reveal his password

6. Ramona Ficosu

Colorado, 2012

Suspected crime: financial offense

Ramona Ficosu, a Colorado woman, was ordered to unlock her computer for investigators. However, she is saying she can't remember her password.

https://gizmodo.com/5882811/defendant-ordered-to-decrypt-hard-drive-says-she-forgot-her-password
https://www.forbes.com/sites/andygreenberg/2012/02/24/two-cases-lessons-if-cops-dont-know-what-you-encrypted-they-cant-make-you-decrypt-it/

Encryption product used: Symantec PGP Desktop

Breaking of encryption successful: no

Case status: plea bargain

7. Ross Ulbricht

USA, 2013

Suspected crime: drug offense

After the FBI arrested Ross Ulbricht, the alleged person behind the online drug marketplace Silk Road, it could not decrypt Ulbricht's personal Bitcoin stash.

https://www.networkworld.com/news/2013/100713-fbi-silk-road-274563.html

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Ulbricht was convicted to life in prison

8. Wisconsin childporn case

Wisconsin, 2013

Suspected crime: child porn

A federal magistrate ordered a Wisconsin man suspected of possessing child pornography to decrypt hard drives the authorities seized from his residence.

https://www.wilderssecurity.com/showthread.php?t=347853, https://www.wilderssecurity.com/showthread.php?t=347853
https://www.wired.com/2013/05/decryption-order/
https://www.wired.com/2013/08/forced-decryption-legal-battle/

Encryption product used: Maxtor BlackArmor / MyBook

Breaking of encryption successful: no

Case status: unknown

9. Christopher Nixon (aka John Doe)

USA, 2012

Suspected crime: child porn

John Doe is the name used for an anonymous person in the US suspected of trading child pornography. The court ruled that Doe wasn't required to reveal the password to an encrypted hard drive that might contain incriminating information. Forcing him to to so, the judge argued, would violate Doe's fifth amendment rights to not offer testimony that incriminates himself.

https://www.forbes.com/sites/andygreenberg/2012/02/24/two-cases-lessons-if-cops-dont-know-what-you-encrypted-they-cant-make-you-decrypt-it/

Encryption product used: TrueCrypt

Breaking of encryption successful: no

Case status: Nixon was convicted to 17.5 years imprisonment

10. James DeSilva

Arizona, 2014

Suspected crime: child porn

In 2014, IT department employee James DeSilva was arrested on charges of sexual exploitation of a minor through the sharing of explicit images over the Internet. His computer, encrypted with TrueCrypt, was seized. DeSilva refused to reveal the password. The police were unable to gain access to his stored files.

https://blogs.phoenixnewtimes.com/valleyfever/2014/02/true_crypt_software_that_hides.php

Encryption product used: TrueCrypt

Breaking of encryption successful: no

Case status: DeSilva was convicted to five years imprisonment

11. Red Brigade

Italy, 2003

Suspected crime: terrorism

In 2003 the Italian police could not decrypt PGP-encrypted data stored on seized Psion PDAs belonging to members of the Red Brigade.

https://www.computerworld.com/s/article/81486/Red_Brigades_PDAs_highlight_encryption_controversy

Encryption product used: PGP

Breaking of encryption successful: no

Case status: PDAs could not be connected to a particular crime

12. Sebastien Boucher

Vermont, 2006

Suspected crime: child porn

In December 2006 US customs agents seized a laptop PC that allegedly contained PGP-encrypted child pornography. Obviously, the encryption could not be broken. Vermont where a child pornography suspect, Sebastien Boucher, had a file on his computer clearly labelled as graphic child pornography. The fact that the file was encrypted didn't help him–the mere title of the file was enough to bypass his fifth amendment argument against handing over the password.

https://news.cnet.com/8301-13578_3-10172866-38.html
https://en.wikipedia.org/wiki/In_re_Boucher

Encryption product used: PGP

Breaking of encryption successful: no

Case status: Boucher was convicted to three years imprisonment

13. JFL

UK, 2009

Suspected crime: terrorism

In 2009 a British citizen was convicted and jailed for nine months for refusing to provide the police with keys to PGP-encrypted files.

https://www.theregister.co.uk/2009/11/24/ripa_jfl

Encryption product used: PGP

Breaking of encryption successful: no

Case status: JFL was convicted to nine months imprisonment

14. Thomas Kirschner

Michigan, 2010

Suspected crime: child porn

In March 2010, a federal judge in Michigan ruled that Thomas Kirschner, facing charges of receiving child pornography, would not have to give up his password.

https://docs.justia.com/cases/federal/district-courts/michigan/miedce/2:2009mc50872/241276/4/0.pdf

Encryption product used: unknown

Breaking of encryption successful: no

Case status: unknown

15. Animal Rights Activists

UK, 2007

Suspected crime: terrorism

Activists attacked animal testing labs.

https://news.bbc.co.uk/2/hi/technology/7102180.stm

Encryption product used: PGP

Breaking of encryption successful: no

Case status: unknown

16. Suspected Terrorist

unknown

Suspected crime: terrorism

A suspected terrorist was apprehended with his laptop open and turned on with the TrueCrypt Mount window displayed on screen. Part of the passphrase
for a 1 GB TrueCrypt volume had been typed into the TrueCrypt Mount window. The screen contents and partial passphrase were noted by the police before the laptop was
seized, imaged and examined. The suspect was asked in interview for the full passphrase but he refused until an order was obtained from the High Court requiring him to
disclose the passphrase. However, the passphrase he provided did not work. In court, the suspect stated that he believed that that was the correct passphrase, but it was
months since he had even seen his computer and he may not be remembering correctly. Based on this situation, the judge held that there was no case to answer.

https://www.sciencedirect.com/science/article/pii/S1742287611000727

Encryption product used: TrueCrypt

Breaking of encryption successful: partially

Case status: unknown

17. Albert Gonzalez

USA, 2009

Suspected crime: hacking

Albert Gonzalez and his associates, convicted in 2009 for a string of intrusions including TJX CorpandHeartlandPaymentSystems, widely employed FDE and encrypted containers. Because of the expectation that encrypted storage was prevalent, the pre-raid preparations and on-scene search strategies were crafted to maximize the opportunity to gain access to running systems and the datathey contained. As a result of this careful planning and the ability to gain access to an FDE system at one of the first crime scenes that digital investigators processed during acoordinated series of searches led by the US Secret Service, critical information was exposed that paved the way forthe recovery of a much larger trove of evidence – and eventually to successful prosecution of the organization.

“The growing impact of full disk encryption on digital forensics”: https://www.sciencedirect.com/science/article/pii/S1742287611000727

Encryption product used: unknown

Breaking of encryption successful: partially

Case status: Gonzales was convicted to 20 years imprisonment

18. Anna Chapman

DC, 2010

Suspected crime: espionage

As part of the recent situation involving a US-based Russian spy ring, the Federal Bureau of Investigation (FBI) successfully circumvented full disk encryption utilized by the Russian agents. The FBI was able to access and analyze their acquired forensic images of the encrypted devices because during their searches they recovered pieces of paper containing the necessary passphrases. It begs the questions of what would have happened had the Russian agents not written them down (U.S. v. Anna Chapman and Mikhail Semenko).

“The growing impact of full disk encryption on digital forensics”: https://www.sciencedirect.com/science/article/pii/S1742287611000727

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: Chapman was arrested and exchanged

19. Max Butler

USA, 2007

Suspected crime: hacking

In the Max Ray Butler (Iceman) case, the digital investigators expected to encounter encryption and the on-scene search was planned accordingly to maximize the opportunity to gain access to running systems, whether they were locked or not. Gaining access to cryptographic data during the search permitted the subsequent decryption of his FDE systems and an assortment of encrypted containers on external drives. This greatly added to initial evidence of the sale of encoding data for several thousand credit cards, leading to Butler’s eventual conviction for the theft of data for nearly 2 million unique payment cards. It also gave investigators access to artifacts
from more than a hundred intrusions over several years.

“The growing impact of full disk encryption on digital forensics”: https://www.sciencedirect.com/science/article/pii/S1742287611000727

Encryption product used: unknown

Breaking of encryption successful: partially

Case status: Butler was convicted to 13 years imprisonment

20. John Craig Zimmerman

Texas, 2007

Suspected crime: child porn

Government investigators were able to easily break the ZIP file encryption Zimmerman used to conceal illegal images.

https://www.cnet.com/news/child-porn-defendant-locked-up-after-zip-file-encryption-broken/

Encryption product used: ZipKey 5.5

Breaking of encryption successful: yes

Case status: solved

21. Joseph Edward Duncan

Idaho, 2005

Suspected crime: murder

Joseph Edward Duncan (born 1963) is an American convicted serial killer and sex offender who is on death row in federal prison in conjunction with kidnappings and murders. Before his arrest he kept a blog named “The Fifth Nail”. In this blog he wrote: “I am working on an encrypted journal that is hundreds of times more frank than this blog could ever be (that’s why I keep it encrypted). I figure in 30 years or more we will have the technology to easily crack the encryption (currently very un-crackable, PGP) and then the world will know who I really was, and what I really did, and what I really thought.” Police never was successful in decrypting the journal.

https://www.webpronews.com/inside-the-mind-of-a-sexual-psychopath-blogger-2005-07
https://www.schneier.com/blog/archives/2005/08/cryptographical.html

Encryption product used: PGP

Breaking of encryption successful: no

Case status: Duncan was convicted to life in prison

22. Dan Ring

Washington State, 2004

Suspected crime: several

Sheriff Detective Dan Ring was arrested in January 2004. He was accused of several crimes. His laptop was found by investigators to have a section encrypted by a program so secure the manufacturer said it is virtually impossible to crack.

https://www.seattlepi.com/news/article/Ring-case-spurs-review-expert-will-try-to-crack-1180256.php
https://www.seattlepi.com/news/article/Secrets-locked-away-in-encrypted-files-1179734.php

Encryption product used: Safehouse

Breaking of encryption successful: no

Case status: solved

23. Susan Powell

Utah, 2009

Suspected crime: murder

Susan Powell disappeared in 2009. Her husband and her brother-in-law were suspected of having killed her. Both committed suicide. Investigators found hard drives containing e-mails between the brothers, which occurred around the time Susan Powell vanished. However, police have been unable to decipher them.

https://www.sltrib.com/sltrib/news/58161806-78/maxwell-josh-police-susan.html.csp
https://scienceblogs.de/klausis-krypto-kolumne/2014/08/05/vermissten-fall-powell-polizei-beisst-sich-an-verschluesselten-e-mails-die-zaehne-aus/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: unsolved

24. Jihadists

Paris, France, 2014

Suspected crime: terrorism

https://www.leparisien.fr/faits-divers/les-cibles-du-jihadiste-la-tour-eiffel-le-louvre-les-festivals-09-07-2014-3987713.php
https://scienceblogs.de/klausis-krypto-kolumne/2014/07/18/franzoesische-polizei-codeknacker-verhindern-anschlag-auf-eiffelturm/

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: unknown

25. Christopher Wilson

UK, 2014

Suspected crime: hacking offence

Computer science student Christopher Wilson was accused of hacking offences. He was jailed for failing to hand over his encryption passwords.

https://www.theregister.co.uk/2014/07/08/christopher_wilson_students_refusal_to_give_up_crypto_keys_jail_sentence_ripa/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Wilson was convicted

26. Leon Gelfgatt

Massachusetts, 2014

Suspected crime: financial offense

Massachusetts' top court ruled that a criminal suspect can be ordered to decrypt his seized computer.

https://arstechnica.com/tech-policy/2014/06/massachusetts-high-court-orders-suspect-to-decrypt-his-computers/

Encryption product used: DriveCrypt Plus

Breaking of encryption successful: no

Case status: unknown

27. Robert Eugene Revay

Florida, 2013

Suspected crime: child porn

Robert Eugene Revay was arrested in 2013 after police conducted an investigation into an online chat group, whose members traveled to engage in sex with young boys, and produced and distributed child pornography.

https://www.local10.com/news/elderly-man-sentenced-for-conspiring-to-produce-child-pornography/26998138

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: Revay was convicted to 15 years imprisonment

28. Kim Dotcom

New Zealand, 2012

Suspected crime: copyright violation

In 2012, New Zealand police seized computer drives belonging to Kim Dotcom, copies of which were unlawfully given to the FBI. Dotcom wants access to the seized content but the drives are encrypted. A judge has now ruled that even if the Megaupload founder supplies the passwords, they cannot subsequently be forwarded to the FBI.

https://torrentfreak.com/dotcom-encryption-keys-cant-be-given-to-fbi-court-rules-140702/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: pending

29. YouTube User

Minnesota, 2012

Suspected crime: child porn

Law enforcement officials investigated a person using a YouTube account whom the Government suspected of sharing explicit materials. During the course of the investigation, police obtained several IP addresses from which the account accessed the internet. Three of these IP addresses were then traced to hotels, which hotels' guest registries revealed the sole common hotel registrant during the relevant times was defendant. The Government believed that data existed on the still-encrypted parts of the hard drive and "introduced an exhibit with nonsensical characters and numbers, which it argued revealed the encrypted form of data." Further, the Government's forensic expert conceded that, although encrypted, it was possible the volumes contained nothing.

https://mntech.typepad.com/msba/2012/02/eleventh-circuit-rules-defendant-cannot-be-compelled-to-divulge-encryption-password.html

Encryption product used: unknown

Breaking of encryption successful: no

Case status: unknown

30. J.E.M

Minnesota, 2012

Suspected crime: child porn

"J.E.M.", a seventeen-year-old resident of Minneapolis, appealed his delinquency adjudication of possession of pornographic work.

https://cyb3rcrim3.blogspot.de/2012/05/ubuntu-truecrypt-and-child-pornography.html

Encryption product used: TrueCrypt

Breaking of encryption successful: no

Case status: Revay was convicted to 15 months imprisonment

31. Markus R.

Germany, 2014

Suspected crime: espionage

Markus R. was a BND employee who is accused of spying for the CIA. On his laptop he used a “highly professional” encryption solution the German authorities have not been able to break so far.

https://www.spiegel.de/netzwelt/netzpolitik/cia-bnd-ermittler-koennen-spionage-laptop-nicht-knacken-a-991472.html

Encryption product used: unknown

Breaking of encryption successful: no

Case status: pending, Markus R. has confessed

32. Jimmy Cournoyer

New York City, 2014

Suspected crime: drug smuggling

Jimmy Cournoyer is a convicted drug smuggler. He and his associates used encrypted Blackberry devices to communicate. They were unaware that police in both the U.S. and Canada were able to break these communications.

https://www.theglobeandmail.com/news/national/king-jimmy-the-rise-and-fall-of-a-quebec-born-monarch-of-marijuana/article19888433/

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: Jimmy Cournoyer was convicted

33. Australian Biker Gang

Australia, 2014

Suspected crime: murder

Australian law enforcement try to solve a number of murders. Suspects apparently used encrypted phones.

https://betabeat.com/2014/03/australian-biker-gang-allegedly-used-super-encrypted-phone-to-kill-hells-angels/
https://www.smh.com.au/digital-life/mobiles/bikies-blackberrys-beat-law-20110206-1ahmo.html

Encryption product used: Blackberry

Breaking of encryption successful: no

Case status: solved

34. David Miranda

UK, 2013

Suspected crime: espionage

In 2013 David Miranda, partner of journalist Glenn Greenwald, was arrested at London’s Heathrow Airport while en route to Rio de Janeiro from Berlin. He was carrying with him an external hard drive said to be containing sensitive documents pertaining to the 2013 global surveillance disclosures sparked by Edward Snowden. Contents of the drive were encrypted with TrueCrypt. A police detective said that the hard drive contained around 60 gigabytes of data, of which only 20 have been accessed to date.

https://www.webcitation.org/6PxzwlLK3

Encryption product used: TrueCrypt

Breaking of encryption successful: partially

Case status: solved

35. John Cockroft

UK, 2014

Suspected crime: child porn

Cockroft’s had stored childporn material on his computers. On one of his laptops, police found two encrypted files they could not crack.

https://www.theboltonnews.co.uk/news/11540727.Pervert_scout_assistant_caught_with_pre_teen_sex_book_when_group_leader_looked_at_his_Kindle/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Cockroft was convicted to a three-year community service order

36. Brittney Mills

Louisiana, 2015

Suspected crime: murder

Brittney Mills was murdered. The police tried to access her iPhone in order to check her calls, messages, and contacts. However, they could not compromise the built-in encryption of the iPhone operating system.

https://theadvocate.com/news/acadiana/13069594-123/moore-cell-phone-encryption-is
https://www.nola.com/crime/baton-rouge/index.ssf/2015/07/brittney_mills_locked_iphone.html

Encryption product used: iPhone

Breaking of encryption successful: no

Case status: unsolved

37. Justin Gerard Gryba

Canada, 2012

Suspected crime: child porn

Saskatchewan police after 2½ years of trying managed to crack an encrypted device containing child pornography and have made an arrest.

https://www.cbc.ca/news/canada/saskatchewan/after-2-years-of-trying-police-crack-encrypted-child-porn-cache-1.2770717

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: Gryba was convicted to a two year imprisonment

38. Secunder Kermani

India, 2015

Suspected crime: espionage

Police have seized the laptop of a young Newsnight journalist in a case that has shocked BBC colleagues and alarmed freedom of speech campaigners. Officers obtained an order from a judge that was served on the BBC and Secunder Kermani, who joined the flagship BBC2 news show early last year and has produced a series of reports on British-born jihadis.

https://timesofindia.indiatimes.com/world/uk/Police-use-terror-powers-to-seize-BBC-Newsnight-journalists-laptop/articleshow/49579295.cms

Encryption product used: unknown

Breaking of encryption successful: unknown

Case status: unknown

39. Blackburn Teenager

UK, 2015

Suspected crime: terrorism

A British boy of 14 sent thousands of online encrypted messages as he plotted the beheading of police officers in a terrorist outrage on the other side of the world.

https://www.policeprofessional.com/news.aspx?id=24515

Encryption product used: unknown

Breaking of encryption successful: no

Case status: solved

40. Christopher Glenn

Florida, 2015

Suspected crime: espionage

Christopher Glenn, 35, violated national security. U.S. He was sentenced to 10 years in federal prison.

https://www.sun-sentinel.com/news/fl-christopher-glenn-sentenced-20150731-story.html
https://www.techdirt.com/blog/?tag=truecrypt

Encryption product used: TrueCrypt

Breaking of encryption successful: yes

Case status: Glenn was sentenced to 10 years in federal prison

41. Ray C. Owens

Illinois, 2015

Suspected crime: murder

Owens was shot dead in Evanston, Ill. The police found two smartphones alongside the body of the deceased: an iPhone 6 and a Samsung Galaxy S6 Edge. Both devices were passcode protected.

https://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0

Encryption product used: iPhone + Android

Breaking of encryption successful: no

Case status: unsolved

42. Ottawa Student (child porn suspect)

Ottawa, 2015

Suspected crime: child porn

An Ontario judge has granted Ottawa police another 12 months to try to crack the password on the hard drive of a college student's laptop.

https://www.lawtimesnews.com/news/general/police-granted-extra-12-months-to-try-to-crack-suspects-computer-encryption/261673

Encryption product used: unknown

Breaking of encryption successful: no

Case status: unknown

43. Michael Cascioli

Pennsylvania, 2013

Suspected crime: drug dealing

After arresting their suspect, Michael Cascioli, in the hallway outside his 18th floor apartment, policemen alledgedly took Cascioli back inside. Although they lacked a search warrant, the cops searched Cascioli's rooms anyway. The officers alledgedly "repeatedly assaulted and threatened [Cascioli] during the search to obtain information about the location of money, drugs, and drug suppliers."

https://arstechnica.com/tech-policy/2015/04/drug-dealer-cops-leaned-me-over-18th-floor-balcony-to-get-my-password/

Encryption product used: Palm Pilot

Breaking of encryption successful: no

Case status: pending

44. Lauri Love

UK, 2013

Suspected crime: hacking offense

Love, an alleged British hacker who has criminal charges pending in three American federal districts petitioned a court to compel the National Crime Agency (NCA) to return his encrypted seized computers and storage devices.

https://arstechnica.com/tech-policy/2015/02/accused-british-hacker-wanted-for-crimes-in-us-wont-give-up-crypto-keys/

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Love was arrested

45. Ben Beaudoin

Massachusetts, 2014

Suspected crime: child porn

Beaudoin was charged with three counts of knowingly purchasing or possessing visual material of child depicted in sexual conduct. A police computer expert was able to break the encryption placed on the several files on Beaudoin's computer. The computer was taken to a forensic lab, where technicians were able to view 116 videos and 85 images of child pornography.

https://www.newburyportnews.com/news/local_news/w-newbury-man-charged-with-child-porn/article_8310e834-2cfd-5caa-b490-ecb71a0ba65e.html

Encryption product used: unknown

Breaking of encryption successful: yes

Case status: solved

46. Paul Taylor

UK, 2013

Suspected crime: child porn

Paul Taylor was found with child pornography on his work laptop. Analysis of the laptop was delayed when the police were given the wrong password for TrueCrypt. A search of the laptop found 69 indecent images in a temporary file in the laptop's C Drive.

https://www.getreading.co.uk/news/local-news/worker-denies-viewing-child-pornography-6378432

Encryption product used: TrueCrypt

Breaking of encryption successful: no

Case status: Taylor received a cmmunity sentence

47. Al-Qaida

Germany, 2012

Suspected crime: terrorism

Dokumente mit entsprechenden Planungsdetails waren offenbar verschlüsselt und in einem Porno-Video versteckt.

https://www.cruisetricks.de/al-qaida-plaene-fuer-entfuehrung-eines-kreuzfahrtschiffs/

Encryption product used: TrueCrypt

Breaking of encryption successful: yes

Case status: solved

48. Robert Hanssen

Virgina, 2001

Suspected crime: espionage

Used PDA with encrypted contents.

https://en.wikipedia.org/wiki/Robert_Hanssen

Encryption product used: Palm III

Breaking of encryption successful: yes

Case status: Hanssen was convicted to life in prison

49. Wolfgang Prikopil

Vienna, 2006

Suspected crime: kidnapping

Wolfgang Prikopil took porn pictures of his kidnapping vitim and offered them for sale in the Vienna sado-maso scene.

https://www.rp-online.de/panorama/ausland/verkaufte-priklopil-nataschas-bilder-in-die-sado-maso-szene-aid-1.2039015

Encryption product used: unknown

Breaking of encryption successful: no

Case status: Prikopil has committed suicide, case is solved

50. Syed Farook

California, 2015

Suspected crime: terrorism

Syed Farook was one the San Bernardino shooters. Police could not decrypt his iPhone and asked Apple for help.

https://www.theguardian.com/us-news/2016/feb/17/apple-ordered-to-hack-iphone-of-san-bernardino-shooter-for-fbi

Encryption product used: iPhone

Breaking of encryption successful: no

Case status: Farook was killed at the shooting

51. Volkswagen

Germany, 2015

Suspected crime: deception

As part of the VW diesel scandal, police investigated 1500 laptops. Many of them were secured with encryption software, and investigators had great difficulty obtaining the passwords.

https://www.welt.de/wirtschaft/article154523222/Hunderte-VW-Aufklaerer-scheitern-an-Codewoertern.html

Encryption product used: unknown

Breaking of encryption successful: partially

Case status: ongoing

52. Hunter Drexler and Justin Staton

Arkansas, 2015

Suspected crime: deception

Derexler and Staton murdered Arkansas couple.

https://www.arkansasonline.com/news/2016/mar/30/fbi-agrees-unlock-iphone-arkansas-teens-murder-cas/

Encryption product used: iPhone, iPad

Breaking of encryption successful: unknown

Case status: Drexler and Staton are convicted

53. Robert Capancioni

Ontario, 2015

Suspected crime: child pornography

Capancioni was accused of distributing child pronography.

https://www.sootoday.com/local-news/police-30000-software-couldnt-crack-hard-drive-187746

Encryption product used: unknown

Breaking of encryption successful: unknown

Case status: Capancioni is convicted

54. Jun Feng

New York, 2016

Suspected crime: drug dealing

Jun Feng was accused of distributing distribute methamphetamine.

https://arstechnica.com/tech-policy/2016/02/apple-prevails-in-forced-iphone-unlock-case-in-new-york-court/

Encryption product used: iPhone

Breaking of encryption successful: yes

Case status: unknown

55. Hussein Khavari

Freiburg, 2016

Suspected crime: murder

Khavari murdered 19-year-old student Maria Ladenburger.

https://www.welt.de/vermischtes/article172287105/Mordprozess-Hussein-K-Die-Version-vom-Handeln-im-Affekt-ist-mit-dem-heutigen-Tag-obsolet.html

Breaking of encryption successful: yes

Case status: Khavari was convicted to life in prison.

TBD

https://www.aclu.org/court-documents-related-all-writs-act-orders-technical-assistance
https://www.aclu.org/legal-document/1-16-mj-02006
https://truthvoice.com/2016/02/the-feds-lied-all-along-demand-apple-to-decrypt-12-more-iphones/
https://assets.documentcloud.org/documents/2718214/Apple-Allwrits-List.pdf

> Suspect who won't decrypt hard drives jailed indefinitely