Digitalna forenzika

Andrej Brodnik

Digitalna forenzika

- predavanja: dr. Andrej Brodnik
- vaje: Aleks Huč, dr. Gašper Fele-Žorž
- e-viri: učilnica

Opis predmeta

- Literatura:
  - ***Eoghan Casey: Digital Evidence and Computer Crime (third edition)***
  - DFRWS (Digital Forensics Research Conference): http://www.dfrws.org/
  - Digital Investigation – Elsevier: http://www.journals.elsevier.com/digital-investigation/
  - SSDDFJ (Small Scale Digital Device Forensics Journal): http://www.ssddfj.org/
  - IFIP Working Group 11.9 Digital Forensics: http://www.ifip119.org/
  - IJDCF (International Journal of Digital Crime and Forensics): http://www.igi-global.com/Bookstore/TitleDetails.aspx?TitleId=1112

Opis predmeta – nadalj.

- predavanja: vključno z vsaj dvema vabljenima predavanjima
- domače naloge (DN):
  - štiri domače naloge iz vsebine predavanj (!), vaj in knjige
  - *za pozitivno: vsaka naloga vsaj 20% in povprečje vsaj 40%*
  - DNo in DNn
- laboratorijski nalogi (LN):
  - dve praktični laboratorijski nalogi
  - nalogi postavljeni v učilnici, kamor se tudi oddaja rezultate
  - *za pozitivno: vsaka vsaj 20% in povprečje vsaj 50%*

Opis predmeta – nadalj.

- seminarska naloga (SN):
  - Skupina (do trije) bo morala prebrati: znanstveni članek izkonference ali revije, knjige, orodja ali podobno
  - predstavitev (20 minut) in pisni izdelek, ki ga kolegi recenzirajo ter na koncu dokončni izdelek
  - časovni razpored:
    - do 27.2. izbira skupine; do 6. 3. vsaka skupina odda predlog teme svoje seminarske naloge, ki se jo potrdi oziroma zavrne vendar najkasneje do 13. 3. potrdi;
    - do 18.5. oddana predstavitev; do 8.5. oddana seminarska; do 22.5. recenzija; do 30.5. dokončno besedilo;
    - v maju in juniju predstavitve seminarskih nalog
  - *za pozitivno: oddani vsi izdelki in vsaj 40% iz predstavitve ter 40% iz končnega pisnega izdelka ter vsaj 50% iz skupne ocene seminarske naloge*

Opis predmeta – nadalj.

- pisni izpit (PI):
  - samo en pisni izpit in to sredi leta (predvidoma 5. 5.)
  - *za pozitivno: vsaj 50%*

- skupna ocen predmeta:

1/3 * PI + 1/3 * SN + 1/3 * (½ * LN + ½ * DN)

Okvirni program

- Uvod in osnove
- Računalniki – strojna oprema
- Operacijski sistemi (MS Windows, Unix/Linux)
- Računalniška omrežja
- Mobilne naprave
- Digitalna forenzika slik
- Zbiranje informacij odprtega tipa in cloveski vektorji napada
- Izvajanje digitalne preiskave
- Varstvo pravice do zasebnosti v kazenskem postopku

slike na prosojnicah so iz knjige © 2011: ***Eoghan Casey: Digital Evidence and Computer Crime (third edition)***

Okvirni program – nadlj.

- vabljena predavanja:
  - Digitalna forenzika v detektivski agenciji
  - Digitalna forenzika omrežij (SI-CERT)

Razpored predavanj in vaj

	teden	predavanja		E. Casey: Digital Evidence and Computer Crime
1	14.02.22	Uvod in osnove	Introduction and basics	1, 2, 3, 4, 5
2	21.02.22	Računalnik, operacijski sistem MS Windows	Computer and operating system MS Windows	15, 17
3	28.02.22	Operacijski sistem Unix	Operating system Unix	18
4	07.03.22	Računalniška omrežja	Computer networks	21
5	14.03.22	Mobilne naprave	Mobile devices	20
6	21.03.22	Digitalna forenzika slik	Digital forenscis of images	
7	28.03.22	Zbiranje informacij odprtega tipa in človeški vektorji napada	Open source intelligence gathering (OSINT) and human attack vectors	
8	04.04.22	Varstvo pravice do zasebnosti v kazenskem postopku	Protection of the right to privacy in criminal procedure	
9	11.04.22	Izvajanje digitalne preiskave	Execution of a digital investigation	6, 7
10	18.04.22	**praznik**	**Holiday**	
11	25.04.22	Vabljeno predavanje / Digitalna forenzika mrežnih napadov	Invited lecture	
12	02.05.22	***izpit***	***exam***	
13	09.05.22	Vabljeno predavanje / Preiskovalno delo zasebenega detektiva in digitalna forenzika	Invited lecture	
14	16.05.22	predstavitve seminarskih nalog	presentation of seminars	
15	23.05.22			
16	30.05.22			

Razpored predavanj in vaj

	teden	vaje	DN
1	14.02.22		1
2	21.02.22	Predstavitev predmeta, 1. laboratorijska.	
3	28.02.22	Osnovni ukazi (ls, grep, mount, ps, md5sum)	
4	07.03.22	Iso, hdd dump, dostop do particij, LVM, RAID, Fsck, fuse, mkisofs,	
5	14.03.22	Analiza metapodatkov v slikah	2
6	21.03.22	Windows registry, ReactOS	
7	28.03.22	Windows kraja ključev	
8	04.04.22	Syslog, linux init sistemi, keyloger	
9	11.04.22	Sqlite, Zgodovina v brskalnikih, cache, db	3
10	18.04.22	*prazniki*	
11	25.04.22	Podatki na mobitelu – android	
12	02.05.22	Buffer overflow 1	
13	09.05.22	Metasploit	4
14	16.05.22	Analiza podakov v pomnilniku	
15	23.05.22	Steganografija	
16	30.05.22		

Razpored predavanj in vaj

	teden	laboratorij	seminarske	
2	21.02.22		27.02.22	izbira skupine
3	28.02.22		06.03.22	predizbira teme
4	07.03.22		13.03.22	izbira teme
5	14.03.22			
6	21.03.22			
7	28.03.22			
8	04.04.22	LAB1		
9	11.04.22			
10	18.04.22			
11	25.04.22			
12	02.05.22		08.05.22	seminarska
13	09.05.22			
14	16.05.22		18.05.22	predstavitev
15	23.05.22	LAB2	22.05.22	recenziji
16	30.05.22	LAB3	30.05.22	končni izdelek

Uvod in osnove

poglavja 1 – 5

Osnove digitalne forenzike

poglavje 1

- Kaj je digitalni dokaz?
  - Digitalni dokaz je katerikoli digitalni podatek, ki je shranjen ali prenešen in omogoča dokaz ali zanikanje [kriminalnega] dejanja.
- Kaj je to računalniški sistem?
  - odprti računalniški sistemi
  - komunikacijski sistemi
  - vgrajeni sistemi

Osnove digitalne forenzike

- za izvajanje forenzične preiskave ni dovolj znanje, ampak se zahteva certificiranost osebja, organizacije, laboratorija, ...

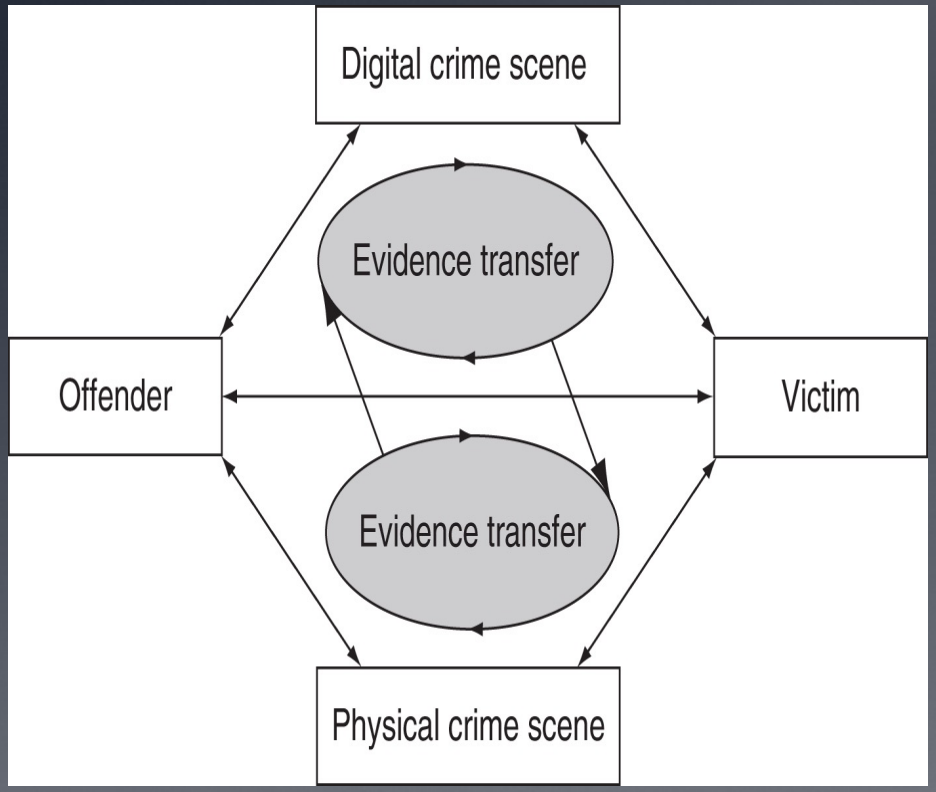
Principi digitalne forenzike

- uporaba znanosti za potrebe prava
- pomen razlikovanja gotovosti in verjetnosti:

Neobstoj dokaza ni dokaz o neobstoju!

- priprava in hranjenje gradiva za morebitni sodni spor

Izmenjava dokaza



- prstni odtisi (na tipkovnici)
- e-pošta in zabeležke
- zabeležke o obiskovanih straneh
- komunikacijske sledi
- ...

Izmenjava dokaznega gradiva med žrtvijo in storilcem (ali prizoriščem)

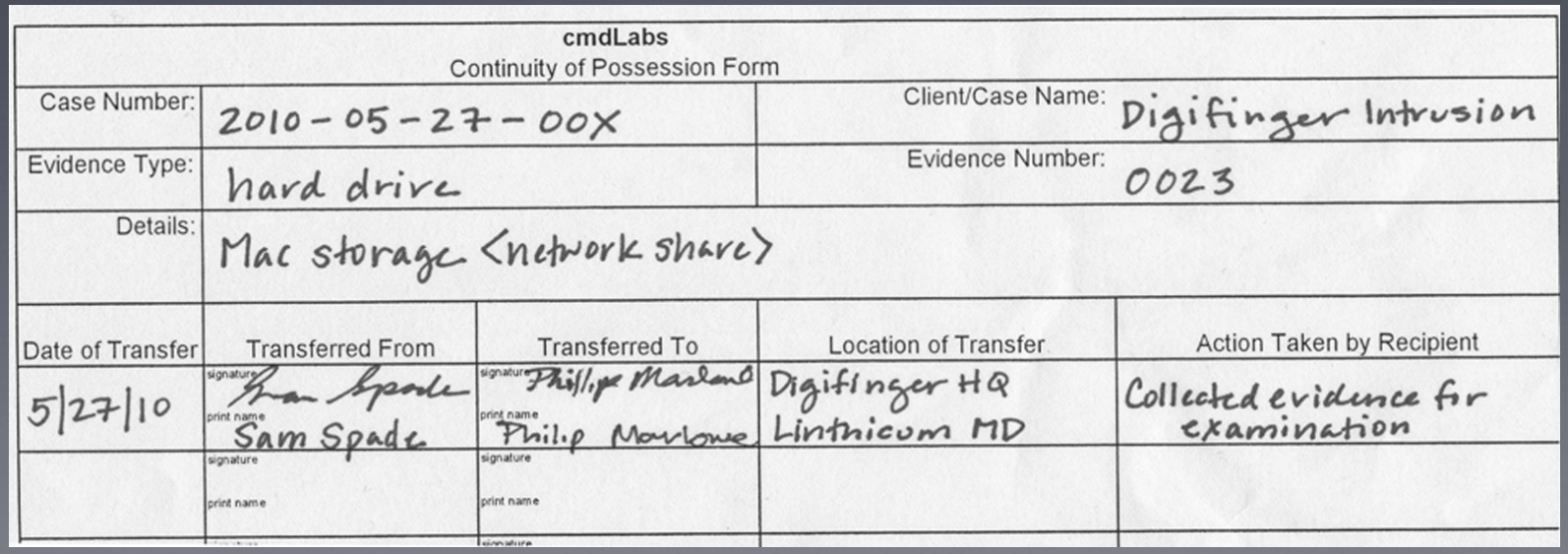
Locardov princip izmenjave

Dokazi

- dokazi imajo skupne lastnosti (vsi programi te vrste) in posebne lastnosti (konkretne nastavite)
- da je digitalni dokaz sprejemljiv na sodišču:
  - mora biti pravilno obdelan (zajet) in
  - mora biti hranjen na forenzično pravilen način
- zato je potrebno beležiti vse akcije na prizorišču

Dokazi

- zagotavljanje avtentičnosti:
  1. vsebina mora biti nespremenjena
  2. vsebina mora izvirati s prizorišča (beleženje vrstnega reda posedovanja dokaza – dokazna veriga)
  3. dodatne informacije o rokovanju z dokazi



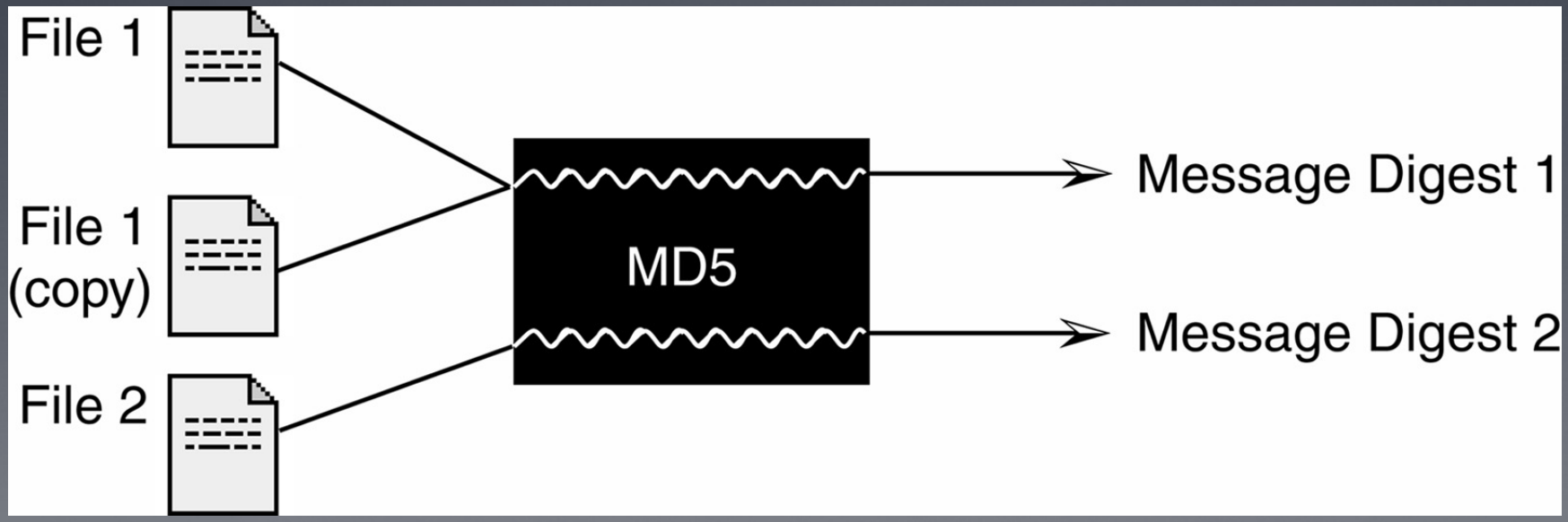
cmdLabs
Continuity of Possession Form

Case Number:	2010-05-27-00X	Client/Case Name:	Digifinger Intrusion
Evidence Type:	hard drive	Evidence Number:	0023
Details:	Mac storage <network share>		

Date of Transfer	Transferred From	Transferred To	Location of Transfer	Action Taken by Recipient
5/27/10	signature: Sam Spade print name: Sam Spade	signature: Phillip Marlowe print name: Phil.p Marlowe	Digifinger HQ Linthicum MD	Collected evidence for examination
	signature print name	signature print name		

Celovitost dokaza

- sprejeta oblika zagotavljanja celovitosti dokaza je podpisovanje z razpršilno funkcijo
  - MD5, SHA-1, ...



Ravnanje z dokazi

- objektivnost dokaza
  - vsebuje interpretacijo in predstavitev dokaza
- ponovljivost analize dokaza

Izzivi rokovanja z digitalnimi dokazi

- ostanki ali rekonstrukcija ni isto kot celotno gradivo:
  - rekonstruirana datoteka, ki je bila izbrisana, ni isto kot delčki le-te
  - ostanki poslane e-pošte ni isto kot celotna e-pošta
- povezava med (digitalnim) dokazom in storilcem ni vedno očitna
- podatki niso večni
  - podatki o prometu na omrežju

Izzivi rokovanja z digitalnimi dokazi

- dokazi niso nujno brez napak
  - administrator je že bil poskušal rešiti pobrisano datoteko
  - sistemski administrator je spremenil vsebino, da bi zavaroval sistem
  - prišlo je do napake pri zajemu podatkov (nestandardni postopek)
  - pri zajemu podatkov je bil uporabljen okužen medij
  - medij s shranjenimi podatki se je poškodoval
  - ...

Digitalni svet ni ločen od realnega

- primer: kupec je preko eBay kupil dobrino
  - *case example: Auction Fraud, 2000*; str. 29
- podatki lahko pridejo iz povsem nepričakovanih mest

Razvoj jezika raziskave računalniških zločinov

poglavje 2

- na začetku ni bilo računalnikov in zakon je ščitil samo materialne dokaze
- digitalni dokazi vključujejo:
  - računalniška (datotečna) forenzika
  - omrežna forenzika
  - mobilna forenzika
  - slabogramje (*malware*) forenzika
- pomembna razlika med preiskovanjem in analizo podatkov
  - preiskovanje vključuje zajem, organizacijo, ...
  - analiza predstavlja dejansko obravnavo dokazov

Vloga računalnika

Po Parkerju, 1976, 1983, 1998:

1. predmet (objekt) zločina
   - kraja računalnika ali uničenje
2. osebek (subjekt) zločina – zločin je bil narejen nad računalnikom
   - okužba računalnika
3. orodje za pripravo in/ali izvedbo zločina
   - kopiranje dokumentov
4. uporaba po svojih lastnostih v zločinu (*symbol*)
   - ponujanje storitev ali zmožnosti računalniških storitev: dobitki na borzi, ...

- vir podatkov(!!) – ostanki datotek, e-pošte, ...

Vloga računalnika

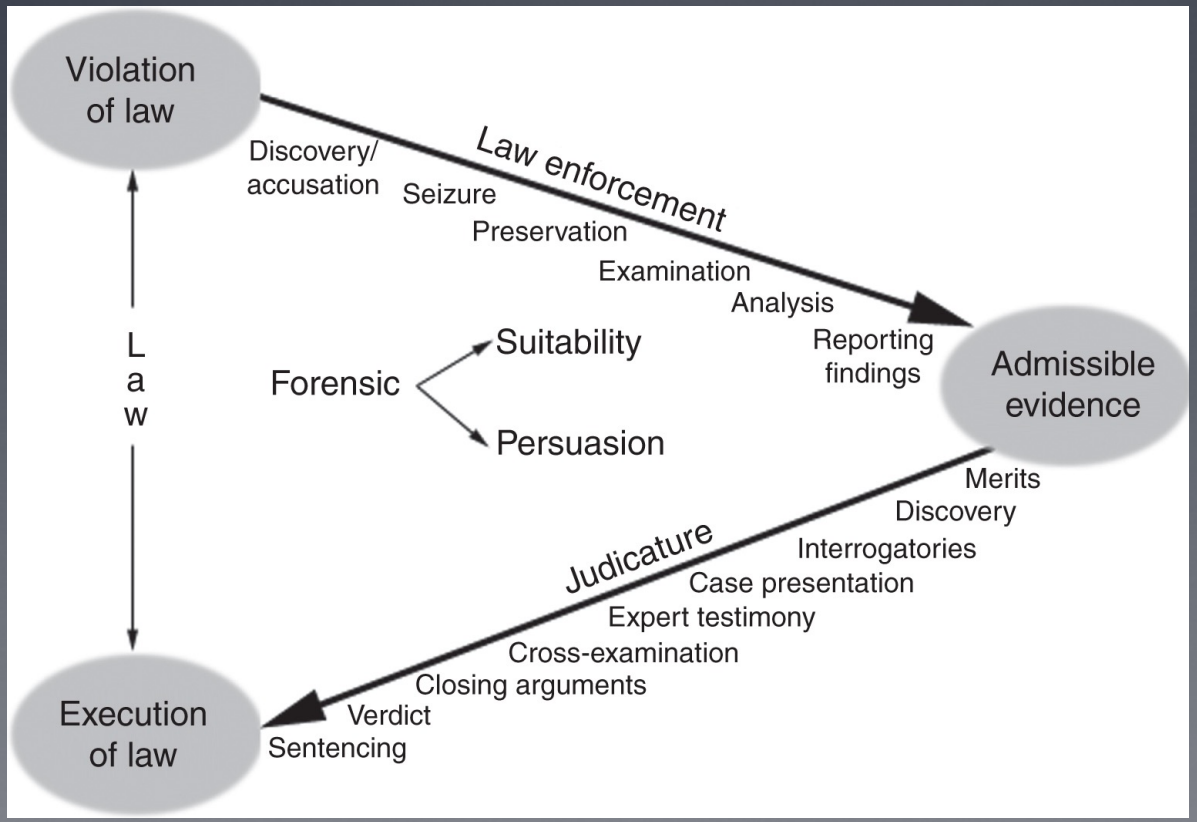
USDOJ (*US Department of Justice*), 1994, 1998:

- strojna oprema kot predmet ali rezultat zločina
- strojna oprema kot instrument
- strojna oprema kot dokaz
- informacija kot predmet ali rezultat zločina
- informacija kot instrument
- informacija kot dokaz

Digitalni dokaz na sodišču

poglavje 3

digitalni dokaz na sodišču



Naloge izvedenca

- predstavitev dokaznega gradiva:
  - ne podleči vplivom
  - odklanjati prezgodaj postavljanje teorije
  - raba znanstvene resnice za potrebe pravnega procesa
- ACM Code of ethics
- IEEE Code of ethics

Sprejemljivost gradiva

- pet osnovnih pravil:
  1. relevantnost gradiva za primer
  2. avtentičnost gradiva *(zajem, sledljivost, …)*
  3. niso govorice *(dokaz sam niso govorice, če ni govorec prisoten)*
  4. najboljši možen dokaz *(original in kopija)*
  5. dokazno gradivo brez potrebe ne napeljuje na zaključke
- nalog za preiskavo

Stopnje zanesljivosti

- v beležkah imamo zapis:

```
2009-04-03 02:28:10 W3SVC1 10.10.10.50 GET
   /images/snakeoil13.jpg-80-192.168.1.1
   Mozilla/4.0+(compatible;+MSIE+6.0;Windows+NT+5.1) 200
   0 0
```

- kaj sklepamo iz njega?
- stopnje zanesljivosti:
  - (1) skoraj zagotovo; (2) zelo verjetno; (3) verjetno; (4) zelo možno; (5) možno
  - statistična verjetnost

Računalniška zakonodaja

poglavje 4

- zakonodaja ZDA
  - 50 zakonodaj
  - zakonodaja Washingon DC
  - zvezna zakonodaja

Računalniška zakonodaja

poglavje 5

- zakonodaja ES (*EU*)
  - Irska (in Velika Britanija) ločen sistem – *common law*
  - preostale države – *civil law*
- skupna zakonodaja:
  - parlament EU
  - Konvencija o računalniških zločinih (*Convention on Cybercrime*), 1. julij 2004
    - nista ratificirali Irska (in Velika Britanija)
  - Protokol o dejanjih rasizma in ksenofobije, 1. marec 2006
  - GDPR, 2019

Zločini nad integriteto računalnika

- Dostop do računalnika ni dovoljen, če nam tega ne dovoli lastnik
- Primeri:
  - hekerji
  - kraja podatkov
  - prestrezanje podatkov
  - vplivanje na podatke in/ali sisteme (DOS, virusi)
  - ››napačna‹‹ ali nenamenska uporaba enote/naprave

Zločini s pomočjo računalnika

- ponarejanje
- goljufija
- zloraba

Zločini povezani z vsebino podatkov

- Zločini, ki zadevajo vsebino podatkov
  - otroška pornografija
  - spletno zapeljevanje
  - rasizem in ksenofobija

Ostali zločini

- kršenje avtorskih pravic
- računalniško izsiljevanje
- ...