University of Maribor
Faculty of Electrical Engineering and Computer Science
FERI

IT and electronic evidence

Boštjan Kežmah

Data retention

- How do you store electronic evidence in the case file?
  - Do you have an electronic case file system?
- In paper-based case file systems
  - Printouts
  - Various data media
    - CD, DVD, Blue-Ray
    - USB Keys
    - Hard drives

Evidence conversion

- Usually from paper to electronic form
  - Scanners
  - Document cameras
- Easy to do, no technical issues – really?
  - How many colors?
  - DPI?
  - Forensic analysis – there is no information about the paper, paper defects (dents, pressure etc.)

Massive conversion

- Numerous documents
- Stapled documents
  - Many documents, stapled differently
  - Many sizes of documents
  - Single/double sided
- Extensive documents
  - Many pages resulting in large size of files

Evidence conversion

- Electronic to paper form – even easier?
  - Perception based on „button-click“ printing
  - What information will be lost because of printing?
    - Electronic signatures?
    - Information not visible on printed document?
  - What information will be changed because of printing?
    - Self-changing fields in documents
    - Use of different software/version for printing

Data transmission

- How to transfer and store large quantity of electronic data?
  - Communications throughput
  - Storage capacity
    - Electronic case file
    - Data media – CD, DVD, …?

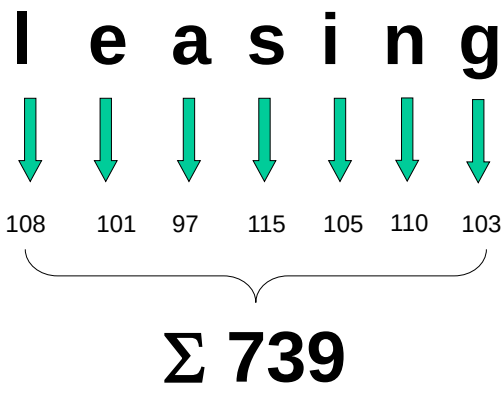
Data security

- How do you prove that the electronic evidence has not changed since it was put in the case file?
  - Why is this different than with the evidence in the paper form?
    - Don‘t we trust the court already?
    - Properties of the paper as a medium for preservation of authenticity is quite different than properties of electronic media!

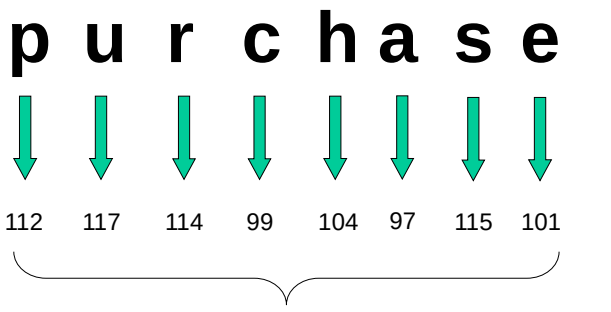
HASH

- Is basic technology for protecting integrity of information
- Examples
  - Fiscal number, social security number
- Cryptographic hash function
  - More sensitive to changes in information
  - MD4, SHA-1, SHA-256, SHA-512

Hash/electronic signature



Hash/electronic signature



Hash security

- Free collision
  - Looking for any kind of information (any data) with the same hash
    - May even be audio/video file, image or even a number of bits without a meaning
  - Possible with weak hash algorithms
- Tied collision
  - Looking for a document with specific content with the same hash
    - Almost impossible to achieve

11

HASH

- Sample for SHA-512
- 13ed241e5d2c6ba17b2bd3cdc031b772cc9
  2bfc9ab42123e7f8183e5ee2bc3f0dc75c79
  0e4d1c8d0afe8f4b0cf2dde70eee3e479f90d
  65e1dda643aad30b8430
  - Large hexadecimal number

12

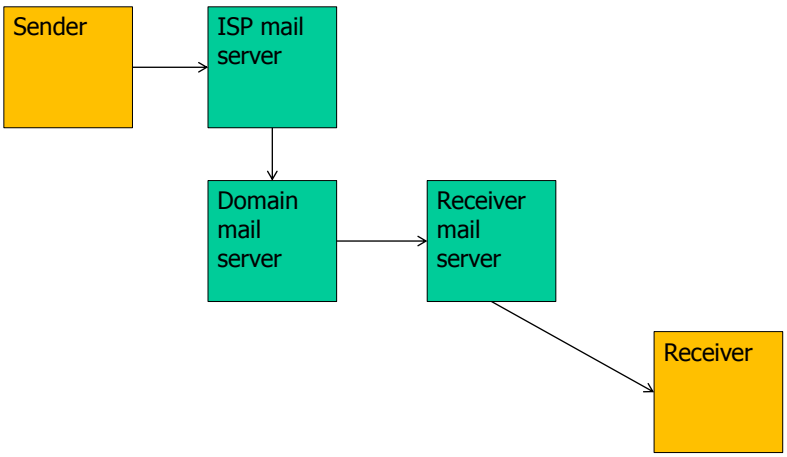
Why not printouts

- Usually printouts lack information for further thorough examination of evidence (judicial experts?)
  - Printed electronic photo does not contain EXIF information (time, date, GPS, exposure information, device information)
  - Printed electronic document does not contain information about date/time created, last changed, time edited etc.

Electronic mail

- Can be used as evidence – usually stored for prolonged periods
  - Use COMPLETE email not just text of the message
- Forging
  - It is very easy to forge electronic mail
- Eavesdropping
  - Messages are not encrypted by default
- Web clients
  - Gmail (Google)
  - Outlook.com (Microsoft)

Exchange of electronic messages



Connections not using encryption

15

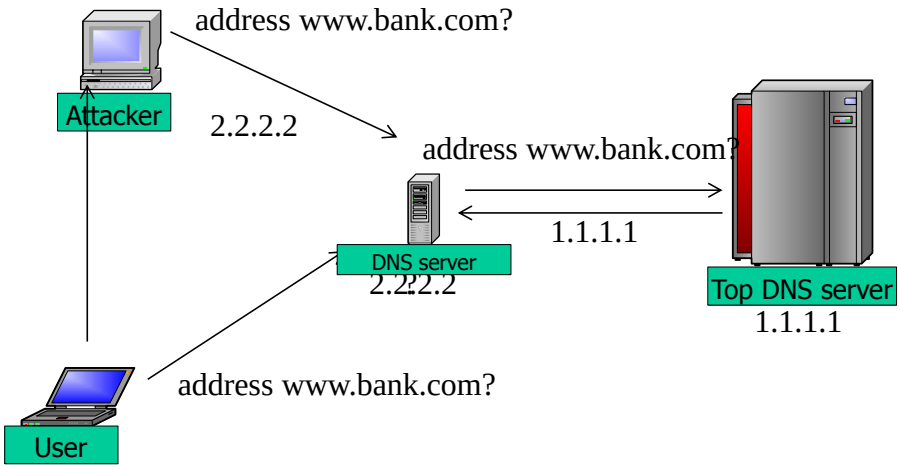
Email header sample

Return-Path: <rok@ledmarketing.si>
Received: from out-2.mail.amis.net ([212.18.32.14])
by win3.slohosting.com
with hMailServer ; Tue, 16 Apr 2013 12:32:19 +0200
Received: from in-3.mail.amis.net (in-3.mail.amis.net [IPv6:2001:15c0:ffff:f::22])
by out-2.mail.amis.net (Postfix) with ESMTP id B117C8132F;
Tue, 16 Apr 2013 12:32:13 +0200 (CEST)
Received: from in-3.mail.amis.net (localhost [127.0.0.1])
by in-3.mail.amis.net (Postfix) with ESMTP id 83A2EC94A8;
Tue, 16 Apr 2013 12:32:13 +0200 (CEST)
Received: from in-3.mail.amis.net ([127.0.0.1])
by in-3.mail.amis.net (in-3.mail.amis.net [127.0.0.1]) (amavisd-new, port 10024)
with ESMTP id vtdk4DX4__HF; Tue, 16 Apr 2013 12:32:10 +0200 (CEST)
Received: from smtp1.amis.net (smtp1.amis.net [IPv6:2001:15c0:ffff:f::41])
by in-3.mail.amis.net (Postfix) with ESMTP id CD322C948B;
Tue, 16 Apr 2013 12:32:09 +0200 (CEST)
Received: from uporabni26db9f (cpe-92-37-118-18.dynamic.amis.net [92.37.118.18])
by smtp1.amis.net (Postfix) with SMTP id 67F11C2DDD;
Tue, 16 Apr 2013 12:32:07 +0200 (CEST)
Message-ID: <19B46BFEAF574DD6B7765259A1FF19D3@uporabni26db9f>

Technical view on identity

- DNS
  - Domain Name System
  - Translates human readable names of computers into IP addresses
  - IP addresses can change over time
  - One can not reliably connect IP address with physical location

DNS spoofing

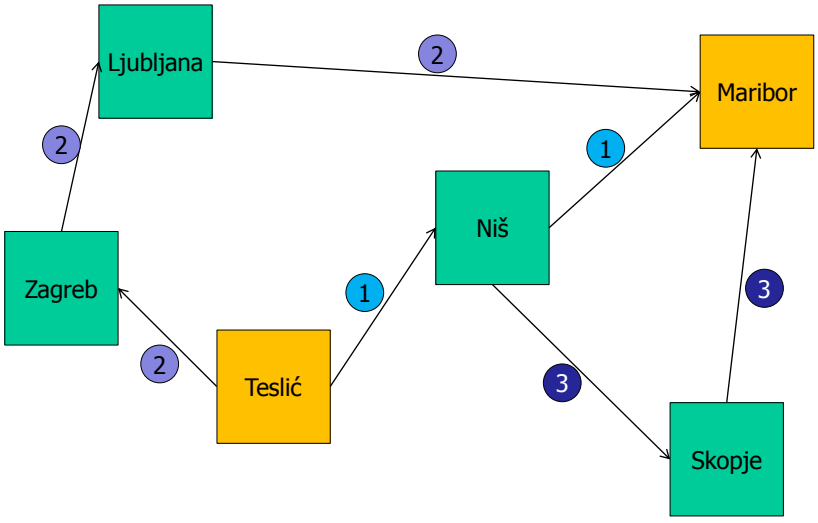


18

Privacy

- Can we avoid using personal data in videoconference hearings?
  - Identification of the witness, judge, …
  - Content of the hearing
  - Content of evidence transmitted during the hearing
- Can we risk transmitting personal data over unsecure communication channel?
  - Who will „filter out“ personal data?

Geographic path vs electronic path



20

Let‘s put in some bureaucracy

- DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
- Article 17
  - controller must, where processing is carried out on his behalf, **choose a processor providing sufficient guarantees** in respect of the **technical security measures and organizational measures** governing the processing to be carried out, and must ensure compliance with those measures.

Guarantees in Slovenia

- In written form
- General terms not acceptable
  - Processor will provide service according to Directive…
- Specific measures should be clearly specified in the terms
  - Using encryption AES-256
  - Using Lampertz cell with physical security based on biometric key lock

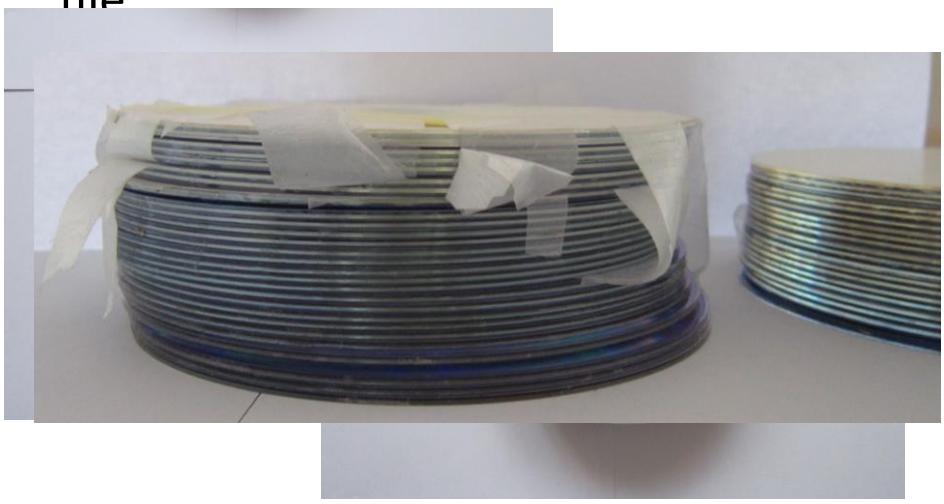
Export to 3rd countries

- Are you sure you are not exporting personal data to 3rd countries?
- How about Skype?
  - May be supported by your videoconference system, but should you use it?
    - All communications are using about 20.000 Microsoft's servers
    - Clear evidence of support for foreign governance agencies eavesdropping (e.g. US, China)

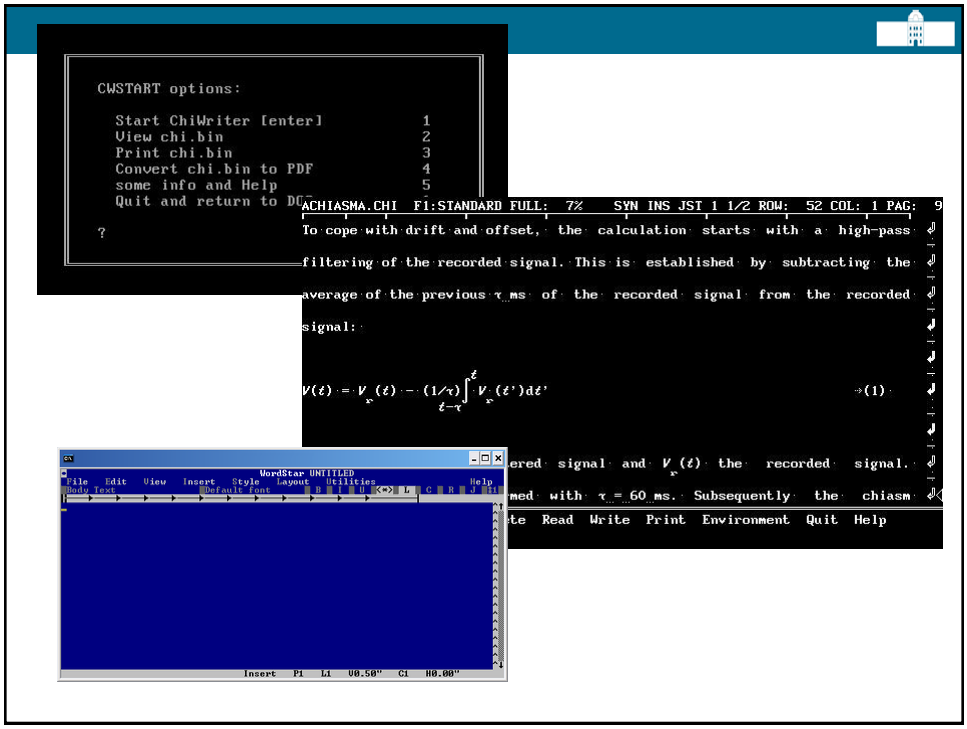
Electronic evidence availability

- Last but not least
- How long will electronic evidence last?
  - Physical deterioration of data media
  - Outdated software
  - Outdated hardware

Large quantity of CDs in physical case file



25


CWSTART options:
Start ChiWriter [enter] 1
View chi.bin 2
Print chi.bin 3
Convert chi.bin to PDF 4
some info and Help 5
Quit and return to DOS
?
ACHIASMA.CHI F1:STANDARD FULL: 7% SYN INS JST 1 1/2 ROW: 52 COL: 1 PAG: 9
To cope with drift and offset, the calculation starts with a high-pass
filtering of the recorded signal. This is established by subtracting the
average of the previous τ ms of the recorded signal from the recorded
signal:
V(t) = V_r(t) − (1/τ) ∫_{t−τ}^{t} V_r(t')dt' →(1)
ered signal and V_r(t) the recorded signal.
med with τ = 60 ms. Subsequently the chiasm
te Read Write Print Environment Quit Help
WordStar UNTITLED
File Edit View Insert Style Layout Utilities Help
Body Text Default Font
Insert P1 L1 V0.50" C1 H0.00"


Verizon 3G 1:23 PM


SAMSUNG
12:45 PM
Google


Start


commodore 64

What do we do about it?

- Protection of Documents and Archives and Archival Institutions Act
  - Uniform Technical Requirements based on Moreq2
- Detailed organisational and technical requirements for long term preservation of records
  - Yes, that includes case files!

Retention process

- Devices/software, formats, procedures for:
  - Capture material
  - Store material
  - Search and access material
    - Control and audit access to material
  - Destroy Material

Enforce usage of the Act

- Public entities
  - Should use accredited
    - Hardware
    - Software
    - Internal rules
- Is there a consequence for using other (unaccredited) equipment and procedures?

Internal rules

- There is a consequence at least for internal rules
  - Accredited internal rules and entity operating as required by internal rules
    - Every unit is equal to original by the law
  - Unaccredited internal rules and entity operating as required by internal rules
    - Every unit is equal to original if internal rules meet requirements for accreditation
  - No internal rules / not following internal rules
    - Equality determined for every unit of material in question

Solution?

- Standardization!

Faculty of Electrical Engineering
and Computer Science

Discussion

bostjan.kezmah@uni-mb.si

37