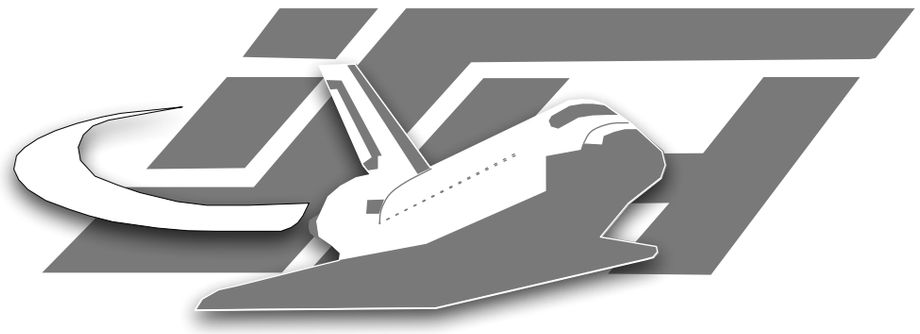
Far More Than You Ever Wanted To Tell

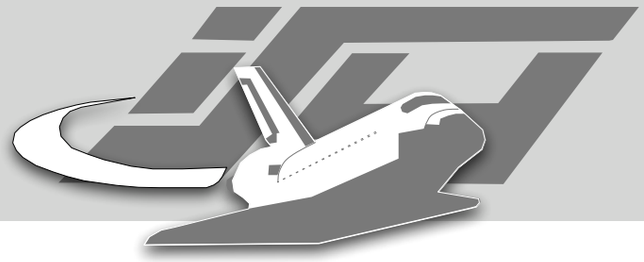
Hidden Data In Document Formats

Maximillian Dornseif
at Defcon 2004, Las Vegas



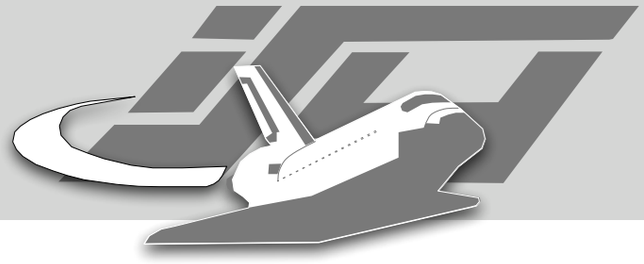
RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

Laboratory for Dependable Distributed Systems • RWTH Aachen University



Warning

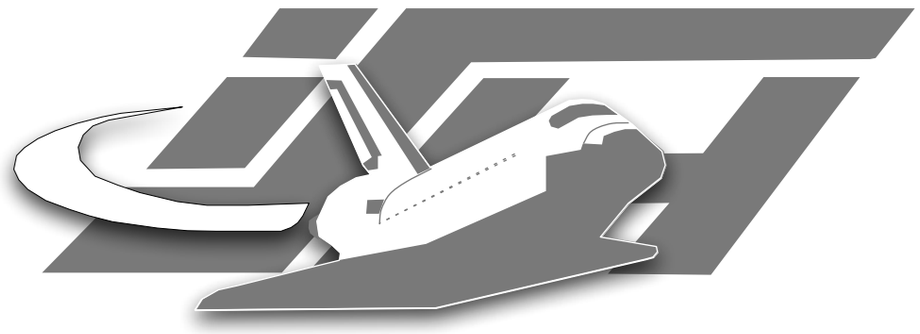
- When you read this this slides are probably outdated.
- Get the slides used in the presentation at http://md.hudora.de/presentations/#hiddendata-dc
- The PDF version has no demos. Go for the Quicktime version,



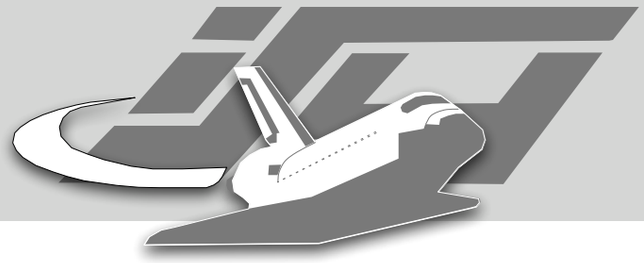
The Problem

- Complex Dataformats
  - We are not supposed to understand
  - or we are not willing to understand
- Covert channels everywhere!

Examples




RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN

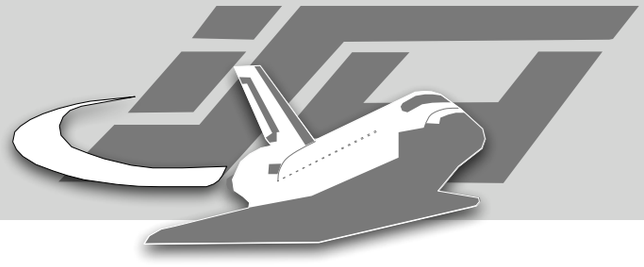


Mail- & News-Headers

- RfC 822 and friends are well known in the techie community but a mystery to everybody else.
- Data in there possibly include: OS, IP, server, software and their versions, organisation, time, customer number at isp / telephone number (!), etc.

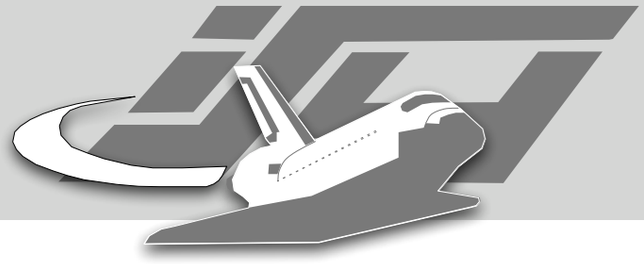
Incidents

- T-Online



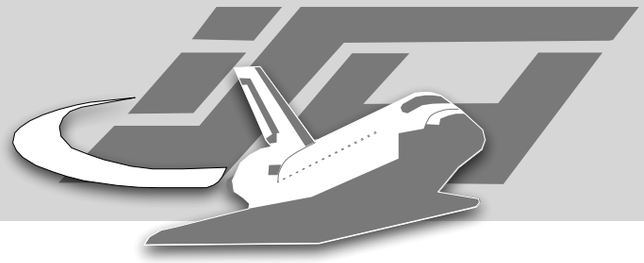
Config Files

- Config files which are not well understood are a security issue...
- ... but also can result in disclosure of information which is not to be disclosed



Incidents

- Apache
- BitchX



HTML

- Complex programs generate complex HTML
- Most obvious:
  - META generator
  - Paths to local files

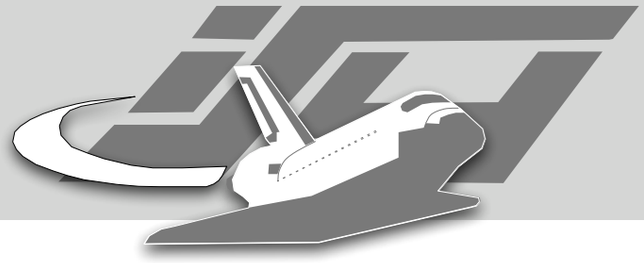
Incidents

- Defaced web pages (attrition.org)

```
<img src=”c:\...\Jon Doe\My Documents\coolpix.jpg”>
```

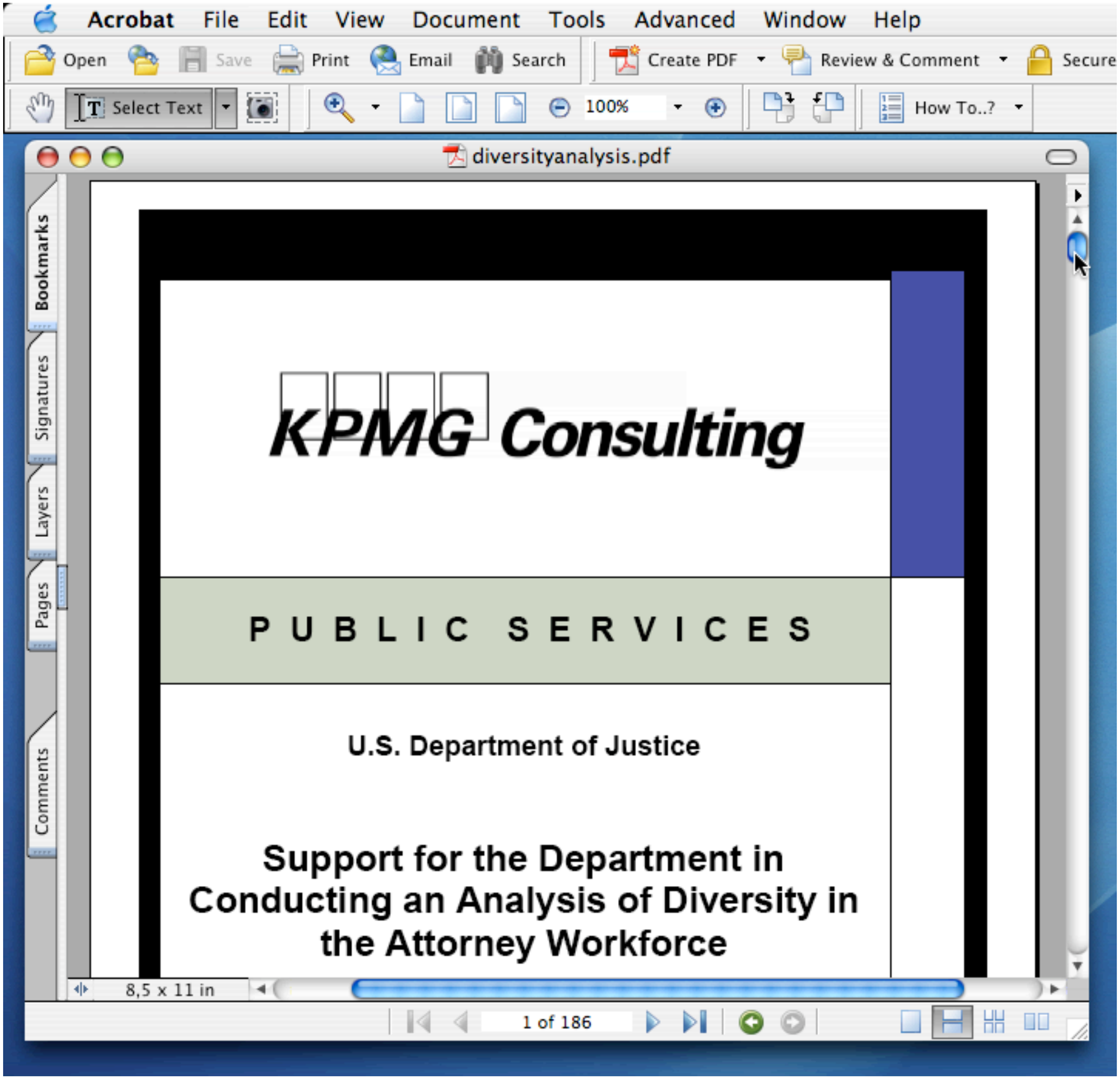
PDF

- Looks like an “open standard” ...
- ... but very hard to decode in depth
- The Problem of [redacted] / redaction.



Exploiting hidden data

- Copy black text on black ground
- Copy underlying graphics


Acrobat File Edit View Document Tools Advanced Window Help
Open Save Print Email Search Create PDF Review & Comment Secure
Select Text 100% How To..?
diversityanalysis.pdf
Bookmarks
Signatures
Layers
Pages
Comments
KPMG Consulting
PUBLIC SERVICES
U.S. Department of Justice
Support for the Department in Conducting an Analysis of Diversity in the Attorney Workforce
8,5 x 11 in
1 of 186

Acrobat File Edit View Document Tools Advanced Window Help

Open Save Print Email Search Create PDF Review & Comment Secure

Select Text 125% How To..?

washpost_sniperletter.pdf

Bookmarks Signatures Layers Pages Comments

Sniper instructs authorities to transfer $10 million into a Visa credit card account. The account belongs to a woman who reported the card stolen in California. The card was later used in Tacoma, Wash.

Pg 2.

more important than catching us.... now, then you will accept our demand which are non-negotiable

(i) You will place ten million dollar in Bank of america account no. [redacted]

Pin no. [redacted]

activation date [redacted]

Exp. date [redacted]

Name: [redacted]

member since [redacted]

Platinum Visa Account,

We will have unlimited withdrawal at any atm world-wide.

You will activate the bank...

Pg - 3

(ARLINGTON, VA)

Bodacious Buffet

6:00 am Sunda

You have until Monday morning transaction. Try to catch at least you will body bags.

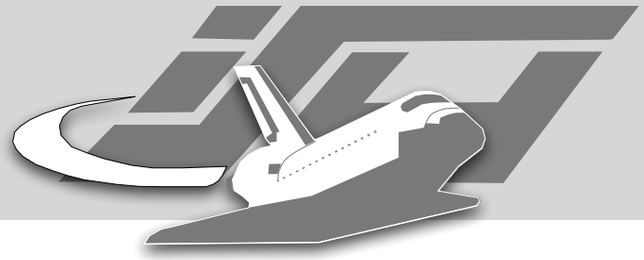
(BUT)

(ii) If trying to c more important you body bags. If we give that is what t "Word is Bond"

P.S. your childre

11 x 17 in

1 of 1

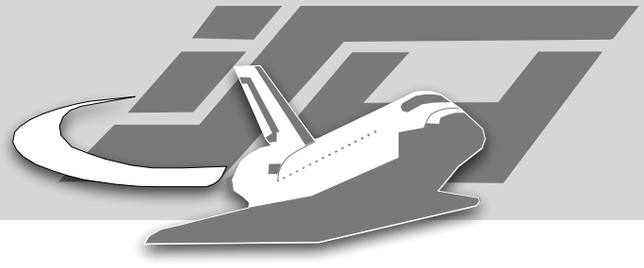


Incidents

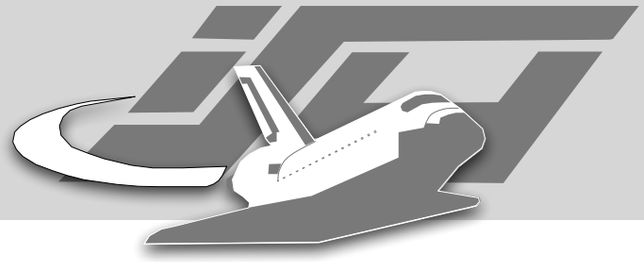
- Sniper Letter
- The Justice Dept's Attorney Workforce Diversity Study
- "Secrets of History: The C.I.A. in Iran"

MS Office

- The MS Office document format is incredibly complex, undocumented and ever changing

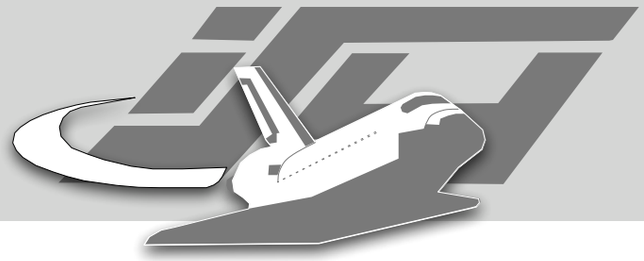


- Documented incidents include:
  - Text from a completely unrelated document edited before appears in the file.
  - Data deleted from the document or overwritten is appears in the file.



Incidents

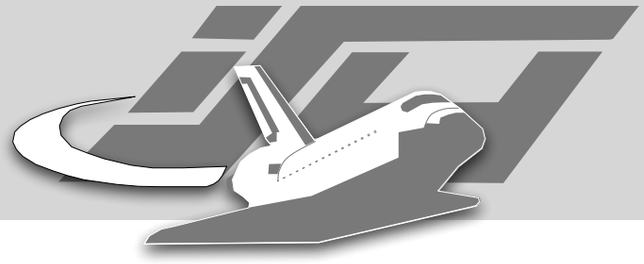
- UK Irak Dossier
- Transrapid / Rheinbraun / Managment / Machbarkeitsstudie
- Melissa



JPEG/EXIF

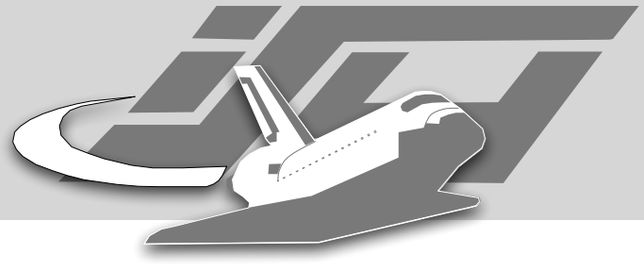
- Many image formats contain comment fields which might disclose unwanted data.
- JPEG has the extensible EXIF format for meta data.
- There was a remarkable incident with EXIF thumbnails


File name:
Open
Files of type:
All Formats
Cancel



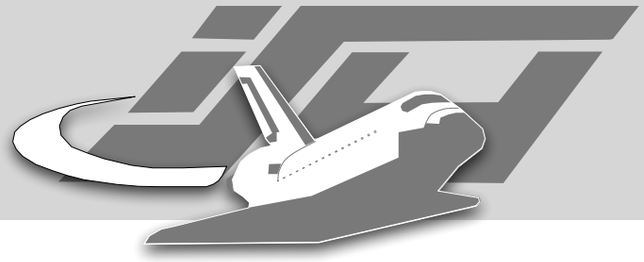
Misc

- Starr Report
- Embedded Serials / GUIDS
- unregistered marks
- ...



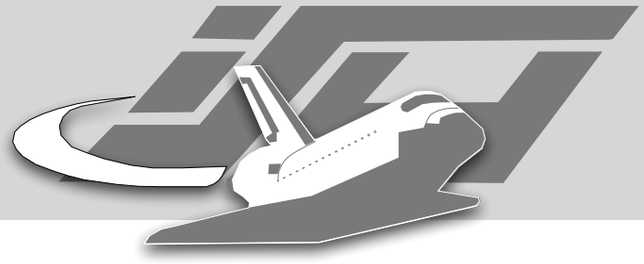
An Experiment

- Idea
  - Crawl the Web
  - Download Documents
  - Find the ones with hidden data.
- Problem:
  - How to detect hidden data?



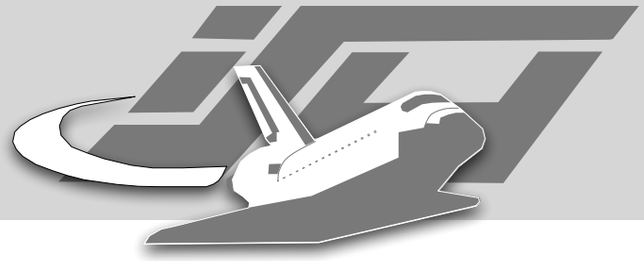
The Byers Experiment

- Scalable Exploitation of, and Responses to Information Leakage Through Hidden Data in Published Documents, Simon Byers, IEEE Security & Privacy pp. 23-27, March / April 2004



Our Experiment

- Technical details and demo



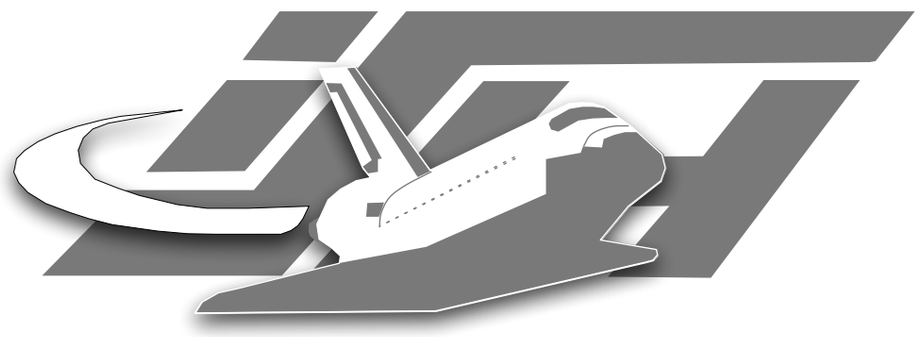
Conclusions

- You never know what properitary formats carry
- Open formats are only part of a solution
- Spider the web and enjoy

Thank You!

Maximillian Dornseif <dornseif@informatik.rwth-aachen.de>

Slides at http://md.hudora.de/presentations/#hiddendata-dc



RWTH AACHEN
RHEINISCH-WESTFÄLISCHE TECHNISCHE HOCHSCHULE AACHEN