Mittuniversitetet
MID SWEDEN UNIVERSITY

A TALK ABOUT INCREASED USE OF FORENSIC TOOLS IN ARCHIVAL PRACTICE, TEACHING, AND RESEARCH

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

MY SPEAK WILL COVER

- Something more about my self
- Forensic tools and their usage in archival domain
  - In Records management
  - In Archival management
- The teacher role & Learning perspective
- The hunt for “the silver bullet”
- The run from the werewolf
- Hybrid records

Mittuniversitetet
MID SWEDEN UNIVERSITY

MY BIO

- Police officer for 20 years 1991-2010
- Not a forensic specialist
- However a basic general forensic experience related to evidentiality and authentictity
- PhD Computer and system science 2008, Associate professor 2012
- Research within the field of crisis management
  - Researcher within RCR Risk & Crisis Research Center

MODERN ARCHIVAL EDUCATION

- Since early 1990s problem related to digital records have been on the agenda

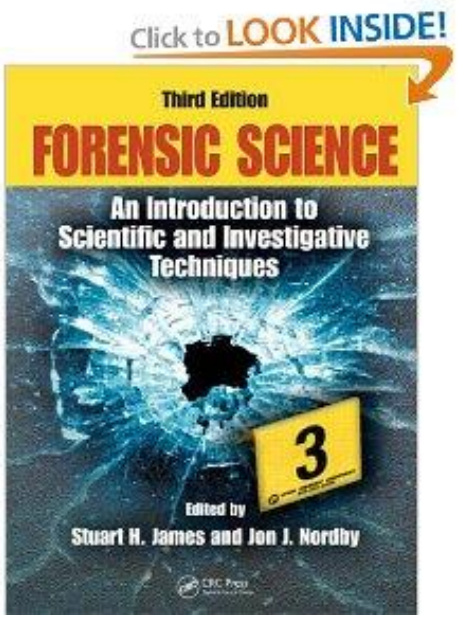
COMPETENCES THAT SUDDENLY WAS NEEDED

- IT-related competence
  - Databases
  - Modelling
  - Software engineering
  - XML
  - System development
  - Emulation
  - Migration
  - Process analysis
  - Etc

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

THE HUNT FOR EVIDENCE

The archivist is an forensic scientist (Diamond, 1994)



Mittuniversitetet
MID SWEDEN UNIVERSITY

FORENSIC

- Sciences and technologies aimed aimed to find evidence (most often criminal law) But also exist in civil law
- Criminal investigations use forensic technologies to investigate a crime scene
- Many refer to what a forensic scientist do as what is presented in e.g. CSI
- Forensic science consists of many subdivisions
- Digital forensic / Computer forensic maybe the most commonly known

DIGITAL FORENSIC

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

Gary Palmer, A Road Map for Digital Forensic Research.Technical Report DTR- T0010-01, DFRWS, November 2001. Report from the First Digital Forensic Research Workshop (DFRWS): 16, http://www.dfrws.org/2001/dfrws-rm-final.pdf

DIGITAL FORENSIC TOOLS

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

- I am not an Computer Forensic expert
- But these are examples of forensic tools and what they can do
  - Software that can boot a suspect system into a trusted state
  - Data acquisition to be able to capture data from suspect systems (dead or live)
  - Software to determine file structure, partition labels, disk labels etc
  - Software to analyze content of a file, on application level
  - Software for network analysis, packages and trafic
  - Software for analyzing memories
  - Software for disk imaging of live and dead systems

SILVER BULLET ?

Of all the monsters that fill the nightmares of our folklore, none terrify more than werewolves, because they transform unexpectedly from the familiar into horrors. For these, one seeks bullets of silver that can magically lay them to rest.

/…/

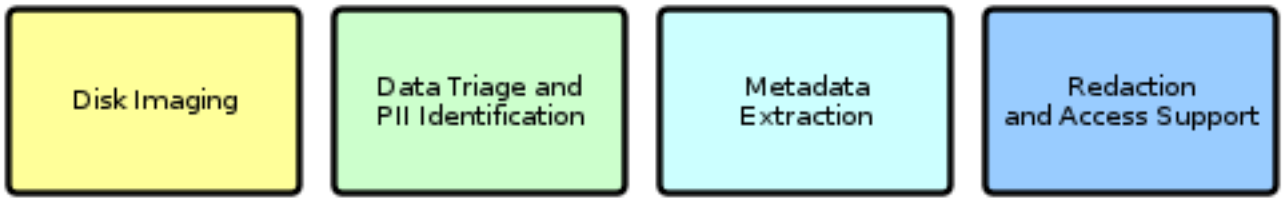
But, as we look to the horizon af a decade hence, we see no silver bullet.

No Silver Bullet: Essence and Accidents of Software Engineering” article (Brooks Jr., 1987)

SOME AREAS WHERE WE USE FORENSIC TOOLS

- In digital curation
- E-archives
- Document/records workflows
- Together with authentication techniques the tools can be used to find errors, security issues

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

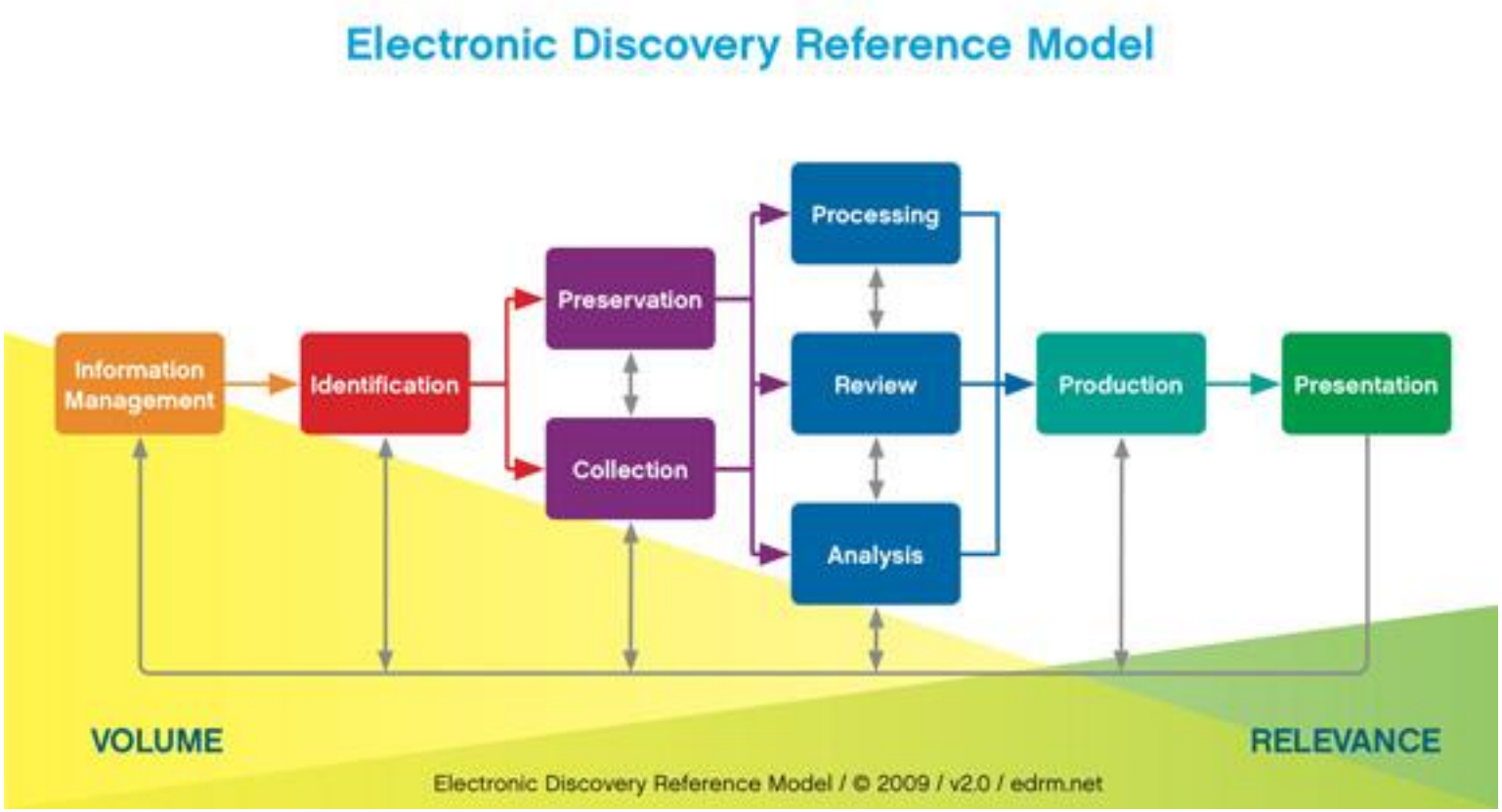


Mittuniversitetet
MID SWEDEN UNIVERSITY

AUTHENTICITY

- Archivists have been working with the term authenticity for long
- Authenticity is necessary for the evidential value of records
- Forensic tools help us in dealing with authenticity
- Evidential value is about authenticity

E-DISCOVERY AN EXAMPLE



BASIC STEPS IN COMPUTER FORENSIC EXAMINATION

1. Policy and Procedure Development
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination
5. Documenting and Reporting

(NIJ Report, Apr 04)

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

OR IS IT A WEREWOLF?

Mittuniversitetet
MID SWEDEN UNIVERSITY

A FORENSIC SCIENCE….

- The rapid development and introduction of forensic tools results in new challenges
- We need more research on use of forensic tools in archival domain

LIKE A CHICKEN RACE?

- Many think: “Everyone use them, I need to act and use them as well”
  - Do everyone understand what the tools can do? And what the tools can be used for?

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

MANY PROBLEMS?

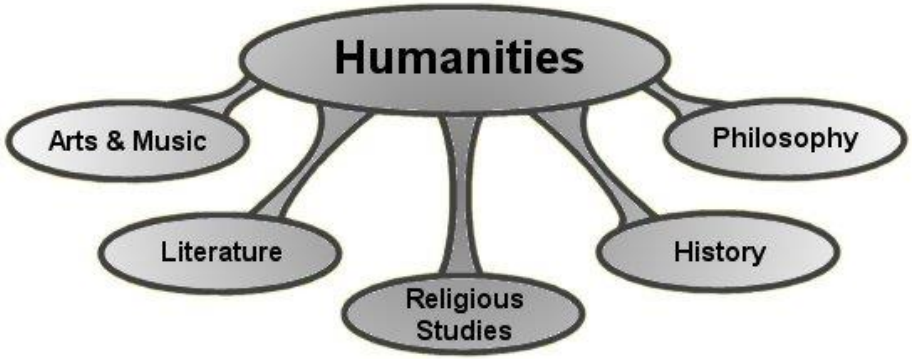
- When should we use the Forensic tools?
- Why should we use them?
- Who should use them?
- Few know the tools and the few that does becomes experts

Mittuniversitetet
MID SWEDEN UNIVERSITY

EDUCATIONAL CHALLENGES

- Archival science and records management in Scandinavia has its roots in history and cultural science
- Still majority of our students have found their archival interest from those domains

A Challenge to meet expectations from student whilst we need to prepare them for reality



STUDENT BACKGROUND

Art and music

History

Archeology

Museology

Library

….

Few with a IT background

HOW TO TEACH HIGH TECH?

- The students learn to be users of
- At Mid Sweden University, we call it IT-lab
- Exercises where they use software of which some is forensic tools

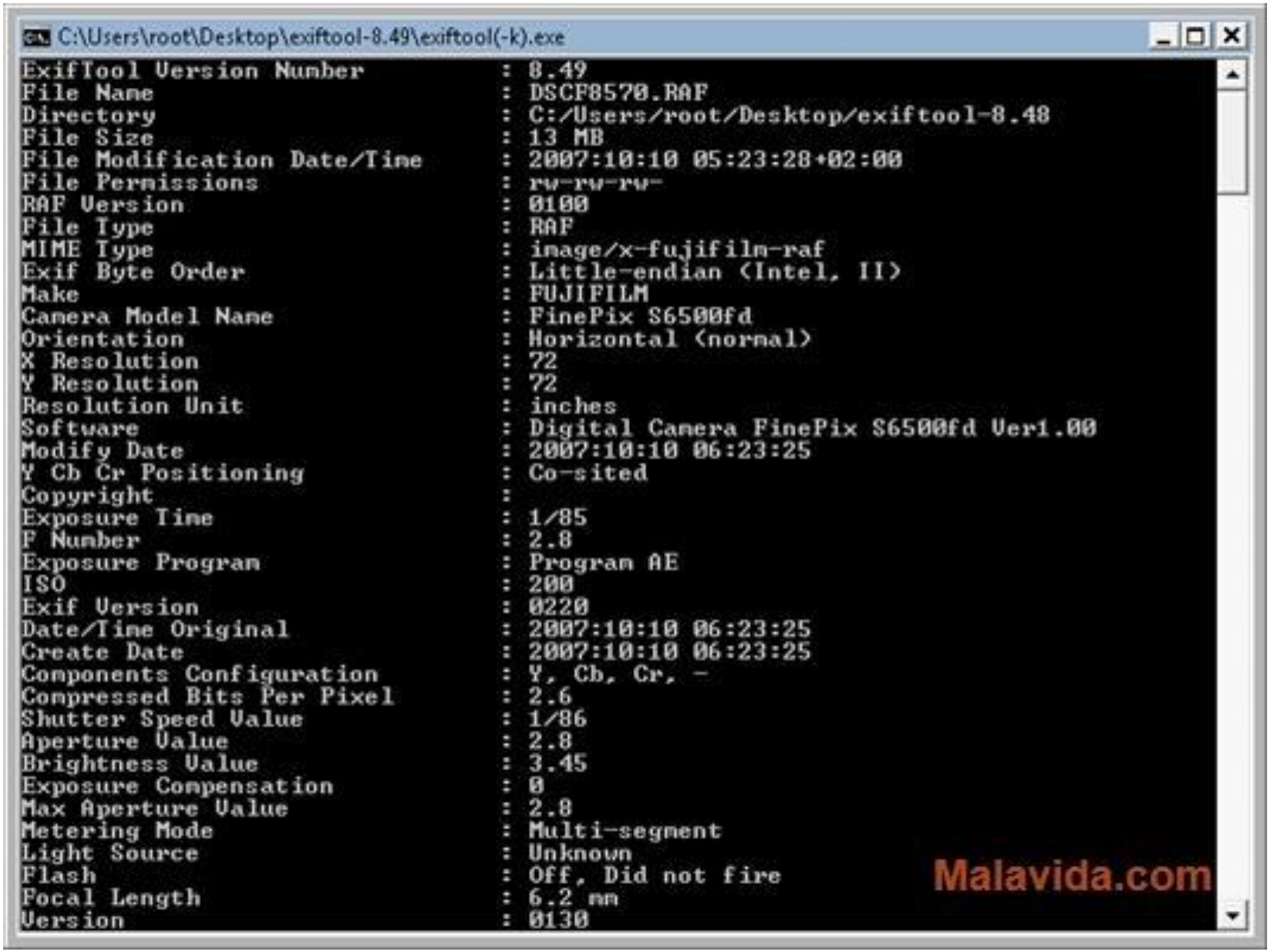
EXAMPLE IT-LAB

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

Meta data analysis with exiftool

```
======== /home1/photo-main07/photos-test/exiftool/select/e7506-5816.jpg
File Name                       : e7506-5816.jpg
File Size                       : 123 kB
Camera Model Name               : FinePix E550
Date/Time Original              : 2007:05:06 11:45:41
Image Size                      : 640x480
Quality                         : FINE
Focal Length                    : 28.8mm
Shutter Speed                   : 1/350
Aperture                        : 5.6
ISO                             : 100
White Balance                   : Auto
Flash                           : Off
======== /home1/photo-main07/photos-test/exiftool/select/e7406-5357.jpg
File Name                       : e7406-5357.jpg
File Size                       : 4 MB
Camera Model Name               : FinePix E550
Date/Time Original              : 2007:04:06 08:38:21
Image Size                      : 4048x3040
Quality                         : FINE
Focal Length                    : 28.8mm
Shutter Speed                   : 1/320
Aperture                        : 5.6
ISO                             : 100
White Balance                   : Auto
Flash                           : Off
    1 directories scanned
    2 image files read
```

Mittuniversitetet
MID SWEDEN UNIVERSITY


C:\Users\root\Desktop\exiftool-8.49\exiftool(-k).exe
ExifTool Version Number : 8.49
File Name : DSCF8570.RAF
Directory : C:/Users/root/Desktop/exiftool-8.48
File Size : 13 MB
File Modification Date/Time : 2007:10:10 05:23:28+02:00
File Permissions : rw-rw-rw-
RAF Version : 0100
File Type : RAF
MIME Type : image/x-fujifilm-raf
Exif Byte Order : Little-endian (Intel, II)
Make : FUJIFILM
Camera Model Name : FinePix S6500fd
Orientation : Horizontal (normal)
X Resolution : 72
Y Resolution : 72
Resolution Unit : inches
Software : Digital Camera FinePix S6500fd Ver1.00
Modify Date : 2007:10:10 06:23:25
Y Cb Cr Positioning : Co-sited
Copyright :
Exposure Time : 1/85
F Number : 2.8
Exposure Progran : Progran AE
ISO : 200
Exif Version : 0220
Date/Time Original : 2007:10:10 06:23:25
Create Date : 2007:10:10 06:23:25
Components Configuration : Y, Cb, Cr, -
Compressed Bits Per Pixel : 2.6
Shutter Speed Value : 1/86
Aperture Value : 2.8
Brightness Value : 3.45
Exposure Compensation : 0
Max Aperture Value : 2.8
Metering Mode : Multi-segment
Light Source : Unknown
Flash : Off, Did not fire
Focal Length : 6.2 mm
Version : 0130
Malavida.com

NOT HIGH TECH BUT

- The students use a simple forensic tool
- They need to discuss what they see,
  - what information is imbedded in the file
  - What do the information tell us?
  - What can we do with the information?
  - I.e. bring focus down to archival issues

THIS IS JUST ONE WEREWOLF ASPECT

- Modern archives and records management adopt new technologies
- But modern archives and records management also adapt existing tools for our own purposes
- My believe is that we do not need to be the forensic experts
- But we must be as skilled user so we can adapt the tools to our purposes

ADOPT OR ADAPT

- I believe we need to adopt new technologies
- We need to dare to test the new technologies
- We should also adapt the technologies for our pursposes
- We might face new potential silver bullets around the corner that we must adopt, and after a while adapt.

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

NEED FOR ADAPTION

A presentation of research where adopted forensic tools can help us to solve part of the challenges.

Mittuniversitetet
MID SWEDEN UNIVERSITY

NEW WAYS OF IT-USE

- We interact in new ways with technology
- The Digital natives are terms that have been presented
- Digital natives are however not the best tool for understanding the new IT-use

ABOUT THE AGENCY

- Information systems research have been trying to understand IT in organizations
- Structuration theory and Actor Network Theory are popular theoretical departures
- Both these can see technology as an actor

BUT

- Both these separate the user from technology

THE HYBRIDS AS E.G. A LAPTOPER

- When using ANT and structuration theory (often used in IS research) the technology are separated from the users
- Mike Michael (2000, 2006) create the hybrid, where technology not are separated from the user
- Lindroth (forthcoming) create the laptoper
- This approach is also supported by e.g. Wanda Orlikowski (2007) “*all* practices are always and everywhere sociomaterial “

CHARACTERISTICS OF THE HYBRID

- The hybrid is the actor that is using information technology in a way that makes the IT almost as a part of the actor.
- The young people using their mobile telephone as “glued” to their hand is another example
  - “One can not go to sleep until the contact list on MSN have turned all red”
  - You sleep with your phone
    - Its never turned off

LET US APPLY THE HYBRID PERSPECTIVE

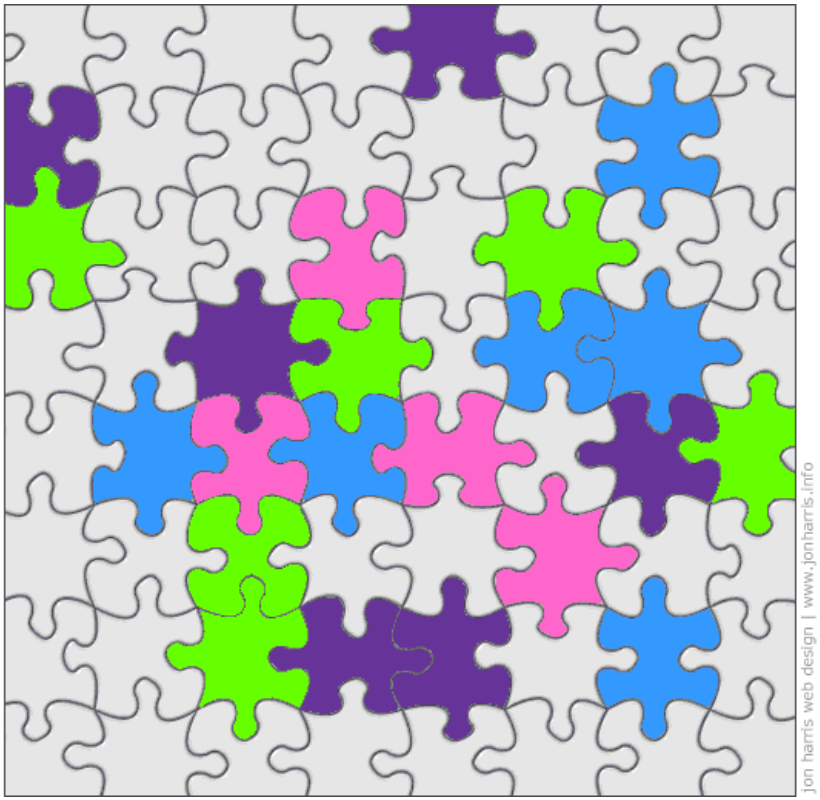
- There is no real boundaries between digital and non digital world.
  - There are only one “world”
- A hybrid is not a boundary spanner or a broker (i.e. a person moving between communities)
- The hybrid is acting in “the world”
- The hybrid leaves digital and non digital traces of activities
  - Digital and non digital evidence of activities
  - Digital and non digital records

THE PIMP

- The “pimp” characterize an individual that act as hybrids, i.e. acting with technology
  - Leaving traces of action in digital and non digital environments
  - The criminal act seamless without boundaries (narrative 1)
  - The crime is a chain of activities and is taking place in digital and non digital environment (narrative 1)

THE CHALLENGES

- Records are recorded information…. and are evidence over action, and activities
- When applying the hybrid approach a set of problems occur
- The full extent of activities can not be understood because records captured are either digital or non digital
- The full puzzle can be difficult to achieve



CHALLENGES CONTINUE

- Current records capture techniques do not help us to capture hybrid records
- With current records capture techniques the full evidence of the activities will not be captured
- It will be yet another puzzle
  - Digital records
  - Non digital records
  - Needs to be put together, and forming new records

- I have argued that modern activites take place in a hybrid environment
- If the current heritage should be captured, new techniques for records capture needs to be identified
- The technology aspect is not the big issue,
  - now the issue is about what level of details we want to preserve activities for the future

- Notice the hybrid is more than a car ☺

FORENSIC APPROACH

- The hybrid is challenging because evidence is born in both digital and non digital environment
- By applying a full forensic approach it could help us to understand and capture evidential values of the full hybrid records.

BACK TO BASIC?

- But if the archivist is a forensic scientist
- Do we really need to rely on the forensic tools?
- Can we not just see that the forensic tools are yet another tools for helping us in dealing with authenticity?

THE END….

- There are other potential werewolves
  - Big data
  - Open data
  - The cloud
- The modern archive and records management can not be solved by one single silver bullet.!

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

QUESTIONS?

Erik Borglund
erik.borglund@miun.se

Mittuniversitetet
MID SWEDEN UNIVERSITY