
# ARE THE FORENSIC TOOLS A SILVER BULLET FOR MODERN ELECTRONIC RECORDS MANAGEMENT? OR YET ANOTHER WEREWOLF?

Dr Erik Borglund, @ACAUBC Symposium 2013

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

# AGENDA

Comments to my bio

Forensic tools

Examples of how forensic tools are used

The ”silver bullet” aspect

The ”werewolf” aspect

Challenges and Problems

Educational aspects

Mittuniversitetet
MID SWEDEN UNIVERSITY

# COMMENTS ON MY BIO

Police officer for 20 years

Not a forensic specialist

However a basic general forensic experience related to evidentiality and authentictity

# SOME TRENDS

- The work for archivists and records manager tend to be more complex than ever
- It begun to be less easy when records started to become digital on broad mass
- A simple solution or a magic wand is often wanted
- The IT it self made the upcoming solutions, tools not understandable for every one
- One of many trends have been Forensics

# 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 and apopted in our community

- Digitalization increase the need for evidence hunt in digital environments
- E-discovery, white collar crime
- Fight against terror
- Business intelligence (not necessary the legal one)
- Computer Forensics or digital forensics is the subdivision that are most applied amongst the archival community.

# 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

- 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)

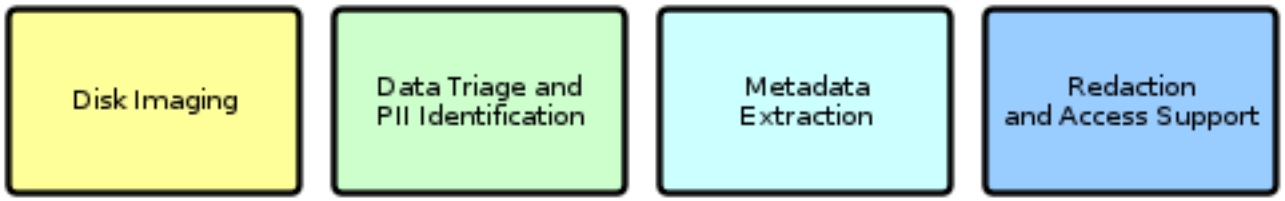
# SOME AREAS WHERE WE USE FORENSIC TOOLS

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

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

E.g.


BitCurator
Visit the main page


Disk Imaging
Data Triage and PII Identification
Metadata Extraction
Redaction and Access Support

# 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
- Archivists are as forensic scientists.

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

# BUT MY PRESENTATION WILL NOT FOCUS ON WHERE THE TOOLS ARE USED

Mittuniversitetet
MID SWEDEN UNIVERSITY

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

# ANOTHER WEREWOLF?

Mittuniversitetet
MID SWEDEN UNIVERSITY

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

# 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?
- “better start using some forensic tools”
- Forensic tools is da shit!

Mittuniversitetet
MID SWEDEN UNIVERSITY

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
- Not only valid for forensic tools
  - We do not stand still and analyze the current need and the current situation

Mittuniversitetet
MID SWEDEN UNIVERSITY

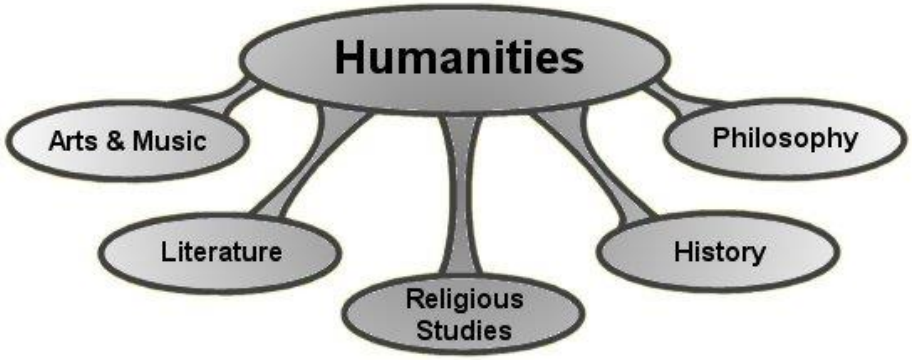
# EDUCATIONAL CHALLENGES

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

- But as educator it is an challenge to meet the upcoming requirements
- Educate for what is needed or educate for what is wanted?
- 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

Mittuniversitetet
MID SWEDEN UNIVERSITY

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




MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

# STUDENT BACKGROUND

Art and music

History

Archeology

Museology

Library

….

Few with a IT background

Mittuniversitetet
MID SWEDEN UNIVERSITY

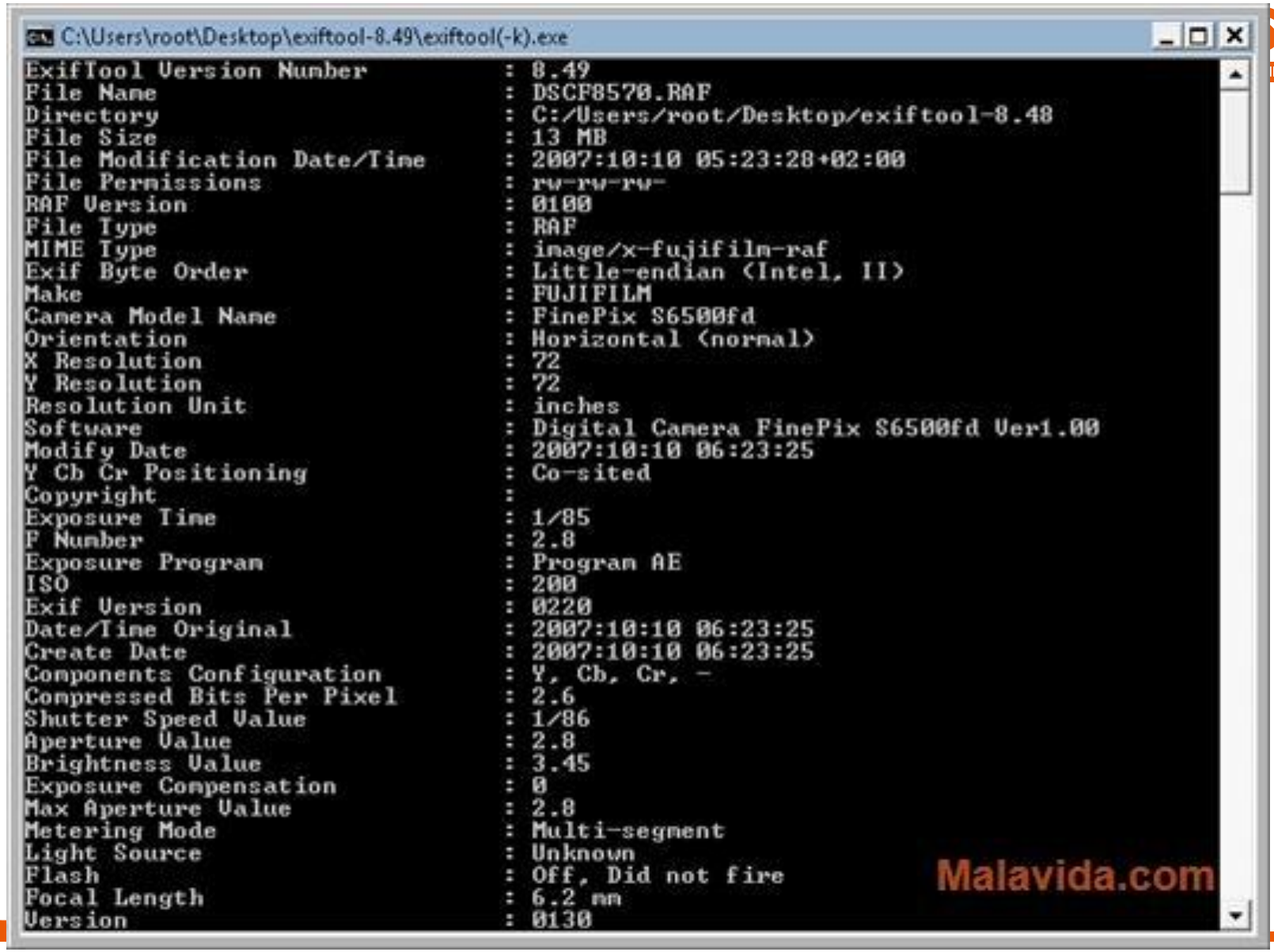
# HOW TO TEACH HIGH TECH?

MIUN.SE
UPPTÄCK DINA MÖJLIGHETER

- 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

Mittuniversitetet
MID SWEDEN UNIVERSITY

```
======== /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
```


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

# FORENSIC TOOLS

- They are challenging because they require new skills
- They can help us
- But
- They are not solely the solution for e.g. dealing with authenticity.

# WHAT IS NEEDED?

- Forensic tools do not capture the context
- Authenticity is dependent upon the context in which the records are born

# THE FIRST END…

- What I really propose is the need to understand the current society
- There have come many tools since Migration was presented as an important tool
- You need to understand what constitutes the record
  - Today records can be more complex than ever,
    - Many systems
    - Digital / Non digital
- How many have practically worked with forensic tools?
- How many will actually use them?
- Unfortunately there is a “hype” warning for the use of forensic tools

# THE SECOND 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