



## About Me

I am:

- Eivind Utnes, M.Sc.



I work for:

- Watchcom Security Group AS

I work as:

- Information Security Consultant
  - Security Audits
  - Digital Forensics / Incident Response
  - Education



## Outline

- Incident Management
- Digital Forensics
- Finding Evidence

# Digital Forensics in Incident Management

SECURITY // **ATTACKS & BREACHES**

---

**NEWS**  
5/5/2011  
12:27 PM

## Sony Brings In Forensic Experts On Data Breaches



Data Forte, Guidance Software, and ProTiviti will investigate who hacked into Sony's servers and how they cracked the company's defenses.

Informationweek.com, 05.05.2011

---

**MILITARY & DEFENSE** More: Associated Press Edward Snowden NSA

## The NSA Has No Idea How Much Data Edward Snowden Took Because He Covered His Digital Tracks

Businessinsider.com, 25.08.2013

---

04.03.2014 Watchcom Security Group AS 4



Incident Response

04.03.2014 Watchcom Security Group AS 5

**Incident Management**

- Incident Response Policy
- Incident Response Team

04.03.2014 Watchcom Security Group AS 6

Proactive measures:

Employee training - Awareness

SIEM (System information and Event Management) implemented to monitor the system.

## Incident Response Policy

- **Responsibility**
  - Who makes the decisions?
- **Asset Priority**
  - Which systems can be taken offline?
  - Which systems can absolutely not be taken offline?
- **Outside Experts and Agencies**
  - Who do we call?
  - At what point is Law Enforcement involved?

## Incident Response Policy

- As an employee, if I discover an incident, what do I do?
- The policy must include information on
  - Chain of escalation
  - How to prevent further damage
  - How to preserve evidence until the Response Team can take over



## Incident Response Team

- Permanent
- Virtual
- Hybrid

04.03.2014 Watchcom Security Group AS 9

Permanent team:

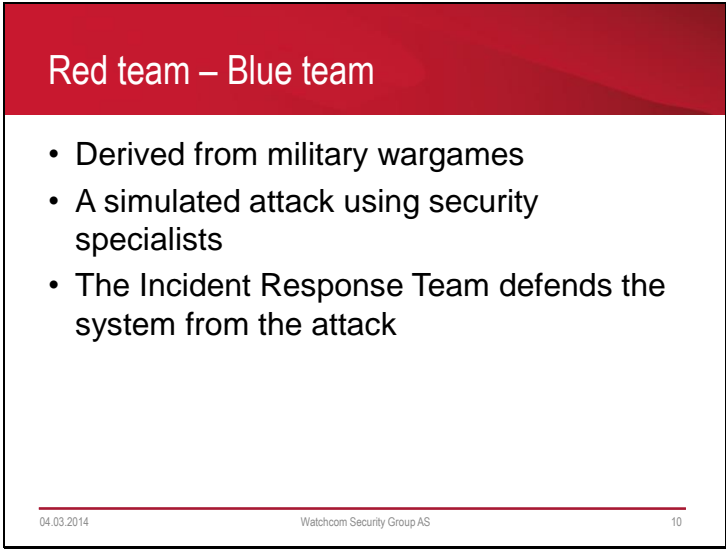
Each member of the team works there full time

Virtual team:

Each member have a “day job” in the organization, but is expected to drop it when an incident occurs

Hybrid:

Some members from each group.

A presentation slide with a red header and a white body. The header contains the title "Red team – Blue team". The body contains a bulleted list of three points. At the bottom, there is a thin red horizontal line, and below it, the date "04.03.2014", the company name "Watchcom Security Group AS", and the page number "10".

## Red team – Blue team

- Derived from military wargames
- A simulated attack using security specialists
- The Incident Response Team defends the system from the attack

04.03.2014 Watchcom Security Group AS 10

Used to train the Incident Response Team and test the Incident Response Policy

## Incident Response Procedures

- Triage
- Investigation
- Containment
- Analysis
- Tracking
- Recovery

04.03.2014 Watchcom Security Group AS 11

Some of these procedures can be done in parallel.

The slide features a red header with the word 'Triage' in white. Below the header, a white box contains a bulleted list of four items. The first item is 'Weed out false positives'. The second item is 'Categorize the event', which is followed by four sub-bullets: 'Type of incident', 'Source of incident', 'Growth of incident', and 'Damage potential of incident'. At the bottom of the slide, there is a thin red horizontal line, and below it, the date '04.03.2014', the company name 'Watchcom Security Group AS', and the slide number '12' are displayed.

## Triage

- Weed out false positives
- Categorize the event
  - Type of incident
  - Source of incident
  - Growth of incident
  - Damage potential of incident

04.03.2014 Watchcom Security Group AS 12

Triage is similar to how medics treat injured people - Who needs medical attention first?

The type - What is happening? Is it a virus infection, a denial of service attack, or an active hacker in the network?

The source - Is it internal or external?

The growth - How fast is the virus spreading? What has the attacker gained access to?

The damage potential - How bad is it? Which servers are compromised? How much is this costing us in lost sales/labor?

**Investigation and Containment**

- Collect data
- Mitigate the damage

04.03.2014 Watchcom Security Group AS 13

These stages can be done in parallel

Data collected in this stage will be used in the analysis stage

What is the best response? Disconnecting the server from the internet might stop an attacker, but is the downtime worth it?

The slide features a red header with the title 'Analysis and Tracking' in white. Below the header, on a white background, is a bulleted list of two main questions. The first question has four sub-points. At the bottom of the slide, there is a thin red horizontal line, and below it, the date '04.03.2014', the company name 'Watchcom Security Group AS', and the slide number '14' are displayed.

## Analysis and Tracking

- What is the root cause of the incident?
  - Who
  - How
  - When
  - Why
- Do we need to involve Law Enforcement?

04.03.2014 Watchcom Security Group AS 14

These stages can be done in parallel  
Including law enforcement can lead to losing control of the situation  
Secrecy is not promised  
Seized evidence can be unavailable for a long time

## Follow-up (Postmortem)

- Fix the problem
- Can we improve the Incident Response Policy?
- Disclosure

04.03.2014 Watchcom Security Group AS 15

Fix the problem:

- Deactivating or patching vulnerable services
- Cleaning infected systems
- Restoring backups

Deactivating vulnerable services can be as easy as blocking certain ports, or it can require that the entire system is upgraded.

Never trust a compromised system, unless it is absolutely critical; "burn it to the ground" and reinstall the system from backups.

- An attacker can have changed the system in subtle ways and added backdoors.

Disclosure:

How is the incident explained to the media and customers?

How is it explained to shareholders?



Digital Forensics

04.03.2014

Watchcom Security Group AS 16



## Digital Forensics in Court

- **The BTK Killer**
  - Metadata in Word file led to arrest after 30 years
- **Krenar Lusha**
  - Search of laptop led to discovery of bomb-making equipment
- **Matt Baker**
  - Suicide of wife ruled murder after incriminating google searches is discovered 4 years later
- **Sharon Lopatka**
  - Emails on her computer led to her killer
- **Corcoran Group**
  - Evidence that data had been deleted led to conviction

The slide features a red header with the title 'Digital Forensics' in white. Below the header, a white area contains a bulleted list of terms. At the bottom, a thin red line separates the content from the footer, which includes the date '04.03.2014', the company name 'Watchcom Security Group AS', and the slide number '18'.

## Digital Forensics

- Known by many names
  - Computer forensics
  - Network Forensics
  - Electronic Data Discovery
  - Cyberforensics
  - Forensic Computing

04.03.2014 Watchcom Security Group AS 18

There is a large difference between handling of evidence in Criminal and Corporate cases. Sometimes a corporate case can become a criminal case - always err on the side of caution.

## What is Digital Evidence?

- Any digital data that contains reliable information that supports or refutes a hypothesis about an incident

The Forensic Investigation Process

- Identification
- Preservation
- Collection
- Examination
- Analysis
- Presentation

04.03.2014 Watchcom Security Group AS 20

#### Identification

Discovering the incident

«My computer is acting weird»

«Someone just posted our entire database on wikileaks»

#### Preservation

Make sure that the evidence is not destroyed - «Do not turn that off»

#### Collection

Gathering all the potential evidence in a forensic manner - Volatile data first - RAM, then disks - Use write blockers, create multiple images, one image is kept as «master»

#### Examination

Find and extract hidden and deleted files and partitions

#### Analysis

Use two tools to verify results – the steps MUST be repeatable

Create timelines of events

#### Presentation

Presenting the evidence to the court

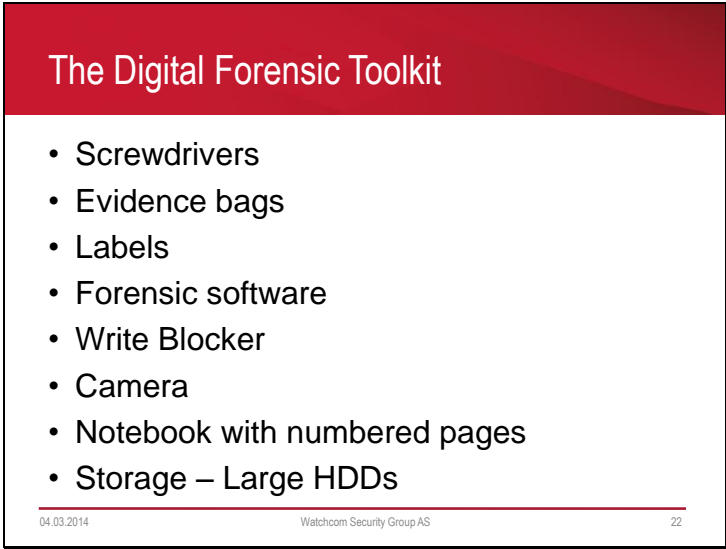
## At the Crime Scene

- Document the crime scene
  - Document who has access
  - Document any contamination
- Photograph everything
  - Especially the screen
- Locate the media
  - Follow cables
  - Search for WiFi
- If the computer is running, dump the RAM

---

04.03.2014 Watchcom Security Group AS 21

Note: Dumping the RAM is necessary, but document the process. Dumping the RAM changes the RAM.



The Digital Forensic Toolkit

- Screwdrivers
- Evidence bags
- Labels
- Forensic software
- Write Blocker
- Camera
- Notebook with numbered pages
- Storage – Large HDDs

04.03.2014 Watchcom Security Group AS 22

Evidence bags that works as faraday cages are available, always use these when dealing with cell phones and other «always connected» devices.  
This is to avoid remote wipes.

## Basic Scientific Principles

1. Best evidence
2. Minimal Intrusion
3. Minimal Force
4. Minimal Interruption
5. Transparency
6. Chain of Custody
7. Primacy of the Mission
8. Impartiality
9. Documentation

04.03.2014 Watchcom Security Group AS 23

- Obtain the best possible evidence. Preferably, the original, if not, then a clone and so on.
- Only seize what is necessary, only keep for as long as necessary
- Do not use excessive force to gain access to the evidence
- Who has had access to the evidence
- Do not interrupt the business unnecessarily
- All the evidence is revealed to the court, no steps taken are secret
- Focus on the mission, despite interesting sidetracks. Note them and move back if necessary
- The do not evaluate evidence with the focus of proving one or the other. Let it speak for itself
- Document everything. When, what, why. Both to provide to the court, and to remember. Often a long time between operation and trial.

Where is the Evidence?

- Network analysis
- Media analysis
- Software analysis
- Hardware analysis

04.03.2014 Watchcom Security Group AS 24

Network analysis:  
Communication analysis  
Log analysis  
Path analysis

Media analysis:  
Disk drives  
Metadata  
Slack Space  
Content

Software analysis:  
Reverse Engineering  
Malware analysis

Hardware analysis:  
Firmware analysis  
Embedded operating systems (Cars, SCADA systems, Roombas)



The slide features a red header with the title 'When Dealing with Evidence' in white text. Below the header, a white box contains a bulleted list of options under the heading 'R-OCITE'. At the bottom of the slide, there is a thin red horizontal line with the date '04.03.2014' on the left, the company name 'Watchcom Security Group AS' in the center, and the slide number '25' on the right.

**When Dealing with Evidence**

- R-OCITE
  - Return
- Or seize
  - Original
  - Clone
  - Image
  - Targeted copy
  - Extensive copy

04.03.2014 Watchcom Security Group AS 25

Return – if the media does not contain evidence, return to the company

Seizing original – Best evidence, access to the media during the whole process, but minimal force rule is not respected and the interruption of operations is unavoidable

ALWAYS seize if possessing the data is illegal or the media is stolen

Seizing a clone – Second best evidence (equal to image), have access to all of the data, but need to have cloning equipment and the interruption of operations is unavoidable

Seizing an image – Second best evidence, possible to restore and boot from, does not need to provide an identical device, but lose access to the original and must have imaging hardware available

Seizing a targeted copy – Minimum intrusion, but can miss evidence on the original and the validity of the evidence rest on the software used to copy

Seizing an extensive copy – Minimum intrusion, takes less time than cloning or imaging, but takes more time than targeted copy, deleted files and hidden files not necessarily copied

## Is the Evidence admissable?

- How was it gathered?
- How was it treated?
- Who handled it?
- How reliable is it?
- Is the Chain of Custody complete?

## Evidence categories

- **Conclusive Evidence**
  - This is fact
- **Best Evidence**
  - This is it
- **Secondary Evidence**
  - This how it looks
- **Direct Evidence**
  - This is what I saw

## Evidence categories

- **Corroborative Evidence**
  - That happened, because of this
- **Circumstantial Evidence**
  - That could have happened, because of this
- **Opinion Evidence**
  - I'm an expert, this is what happened
- **Hearsay Evidence**
  - I heard this about that

## Digital Evidence

- Digital evidence is considered hearsay
- Unless an expert vouches for it



Finding Evidence

04.03.2014

Watchcom Security Group AS 30

**Finding Evidence**

- Many ways to hide evidence
- Many ways to find evidence

04.03.2014 Watchcom Security Group AS 31

Some examples – hidden files, innocent names, file slack, hidden partitions, encryption  
Always ask the suspect, many hours can be saved

## Hidden files

- Setting the “hidden” flag on the file
- Placing illicit materials in folders named “Tax Stuff” or “Guest Lectures”



## Locating hidden files

- We ignore the “hidden” flag by default
- Forensic software can be set to show the whole drive as a “flat” drive, ignoring all folders

## Changing File Extensions

- When opening the file, the system returns an error message
- “Oh, I guess it is corrupted. Too bad.”

## Discovering changed File Extensions

- Some forensic software will point out files with mismatched extensions
- File signatures tells us what kind of file it is
  - Also called “Magic Numbers”

## File signatures

- A hexadecimal code in the file

Examples:

25 50 44 46	= %PDF	= PDF
49 44 33	= ID3	= MP3
FF D8 FF	= ÿØÿà	= JPEG
42 4D	= BM	= BMP
4D 5A	= MZ	= EXE, COM, DLL

04.03.2014 Watchcom Security Group AS 36

Hexadecimal numbers are made up of the numbers 0-9 and the letters A-F, totaling 16 numbers, 0-15

Examples: 7 = 7, A = 10, F = 15.

## Example signature: JPEG

Offset	0	1	2	3	4	5	6	7	8	
00000000	FF	D8	FF	E1	15	FE	45	78	69	ÿøÿá þExi
00000009	66	00	00	49	49	2A	00	08	00	f II*
00000018	00	00	09	00	0F	01	02	00	06	
00000027	00	00	00	7A	00	00	00	10	01	z
00000036	02	00	14	00	00	00	80	00	00	!
00000045	00	12	01	03	00	01	00	00	00	
00000054	01	00	00	00	1A	01	05	00	01	
00000063	00	00	00	94	00	00	00	1B	01	!
00000072	05	00	01	00	00	00	9C	00	00	!
00000081	00	28	01	03	00	01	00	00	00	(

## Obscure filenames

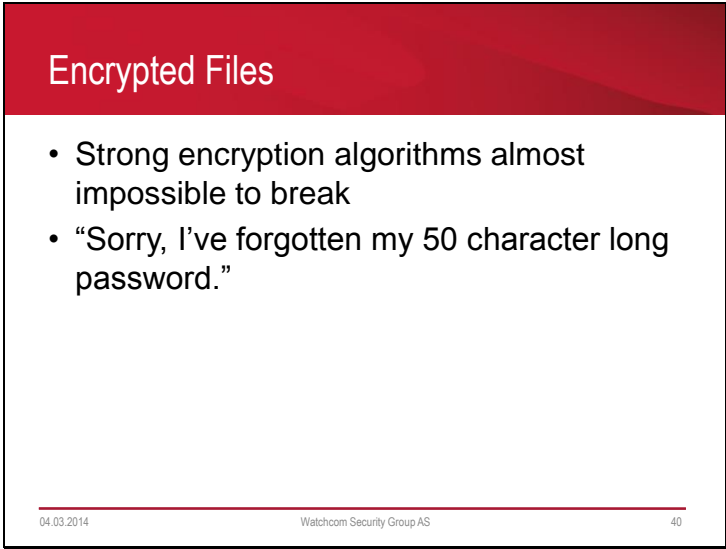
- Hide files by giving them innocent sounding names
- “Blueprints\_iPhone7.jpeg” becomes “Florida vacation 001.jpeg”

## Filenames not always necessary

- We use hashing algorithms to quickly look for known files, and either note or ignore them
  - Hash lists recognize known illicit files
  - Other lists recognize known good files
  - We can create our own

04.03.2014 Watchcom Security Group AS 39

A hashing algorithm is a mathematical function that takes an input and creates a “hash” representing that file. The hashing process is one way, and the hash is unique for each file. Two identical file hashes mean that these two files are identical. The file hashes ignore filenames, only look at the content of the file. MD5 and SHA1 is the most used hashing algorithms, and both are often used in forensics.



The slide features a red header with the title "Encrypted Files" in white. Below the header, there are two bullet points on a white background. At the bottom, a thin red line separates the footer from the main content. The footer contains the date "04.03.2014", the company name "Watchcom Security Group AS", and the slide number "40".

## Encrypted Files

- Strong encryption algorithms almost impossible to break
- “Sorry, I’ve forgotten my 50 character long password.”

04.03.2014 Watchcom Security Group AS 40

You can encrypt everything, from a few words to a whole drive



The slide features a red header with the title "Breaking" Encryption. Below the header is a white area containing a bulleted list. At the bottom of the slide, there is a thin red horizontal line, and below it, the date "04.03.2014", the company name "Watchcom Security Group AS", and the slide number "41".

## "Breaking" Encryption

- Recovering key from RAM
- Brute force
- Exploiting weaknesses in the software or the algorithm used
- Some countries have laws that compel the suspect to give up keys

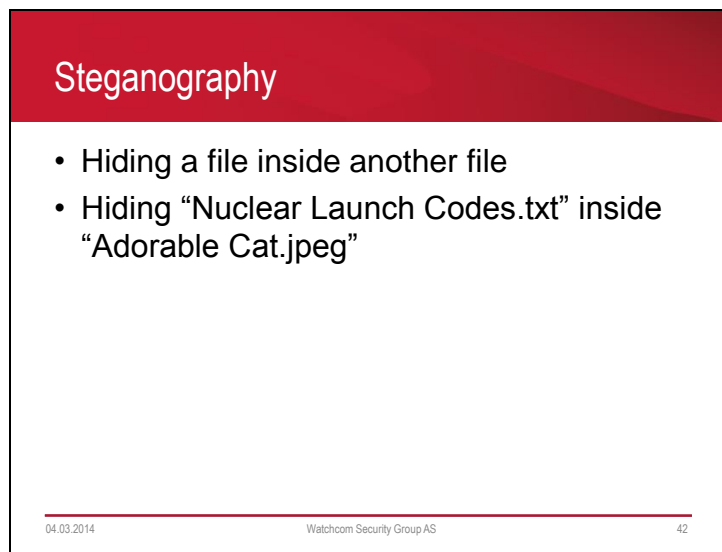
04.03.2014 Watchcom Security Group AS 41

Recovering the key is only possible if the computer is currently on and decrypted. The key is stored in RAM and used to write to and read from the drive.

Some organizations have a "master key" that can decrypt all of their computers

Countries that might force you to give up your keys:

Canada, Finland, France (3-5 years in jail for resisting), India (7 years for resisting), United Kingdom (up to 2 years) [[http://en.wikipedia.org/wiki/Key\\_disclosure\\_law](http://en.wikipedia.org/wiki/Key_disclosure_law), 04.03.2014]



The slide features a red header with the title 'Steganography' in white. Below the header, a white area contains a bulleted list. At the bottom, a thin red line separates the content from the footer, which includes the date '04.03.2014', the company name 'Watchcom Security Group AS', and the slide number '42'.

## Steganography

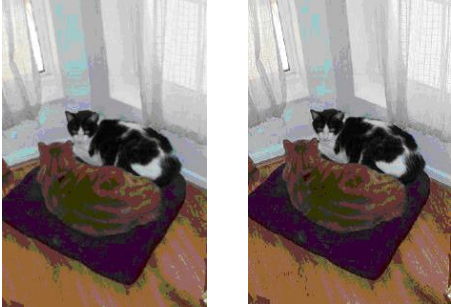
- Hiding a file inside another file
- Hiding “Nuclear Launch Codes.txt” inside “Adorable Cat.jpeg”

04.03.2014 Watchcom Security Group AS 42

Commonly hidden inside image files and music files.

There is little difference between the colour “4333” and “4322”, and static in music files not easy to notice

## Steganography example



Inside one of these files the text "This is a test. This is only a test." is hidden.

[symantec.com](http://symantec.com), 02.11.2010

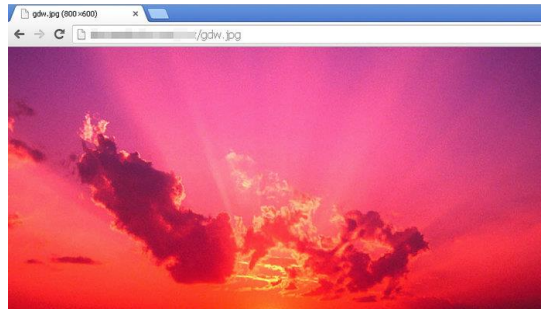
---

04.03.2014

Watchcom Security Group AS

43

## Steganography example



The ZeusVM malware uses image files to hide configuration files

digi.no, 19.02.2014

## Discovering Steganography

- Hard to determine, unless you are looking for it
- Can be discovered by noticing steganography software on the suspects computer

## Deleting Files

- Deleting the files from the computer before law enforcement claims it
- “You can’t prove anything, there is nothing there.”

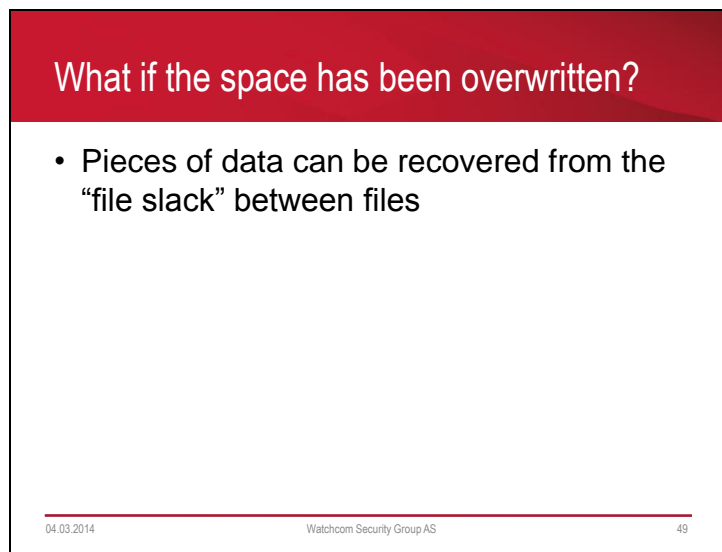
## How does the System delete Files?

- Deleting a file does not actually remove it
- In Windows, the file is renamed
  - CorporateSecrets.txt
  - ~orporateSecrets.txt
- This tells the system that the space is available

## How to reclaim it?

- Simplest way: Renaming!
  - ~orporateSecrets.txt
  - CorporateSecrets.txt
- The system no longer considers the space available



A presentation slide with a red header and a white body. The header contains the question "What if the space has been overwritten?". The body contains a single bullet point: "• Pieces of data can be recovered from the 'file slack' between files". At the bottom, there is a thin red horizontal line, and below it, the date "04.03.2014", the company name "Watchcom Security Group AS", and the slide number "49".

**What if the space has been overwritten?**

- Pieces of data can be recovered from the "file slack" between files

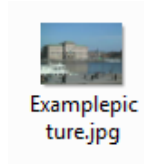
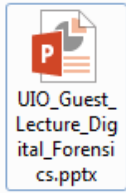
---

04.03.2014 Watchcom Security Group AS 49

This is a complex topic, can be discussed in class if there is time.

## Metadata

- What if we only have a file?



## Using Metadata

- Data about the file
  - When was the file last used?
  - When was the file created?
  - Who opened it?
  - Where was it created?
- Can prove who had access to the file

---

04.03.2014 Watchcom Security Group AS 51

Many new cameras and cell phones “geotags” pictures with latitude and longitude. Excellent if you want to share where you’ve been. Not so good if you want to hide it.

## Metadata Example

