Digital Forensics – UiO

About Me

I am:

- Eivind Utnes, M.Sc.

I work for:

- Watchcom Security Group AS

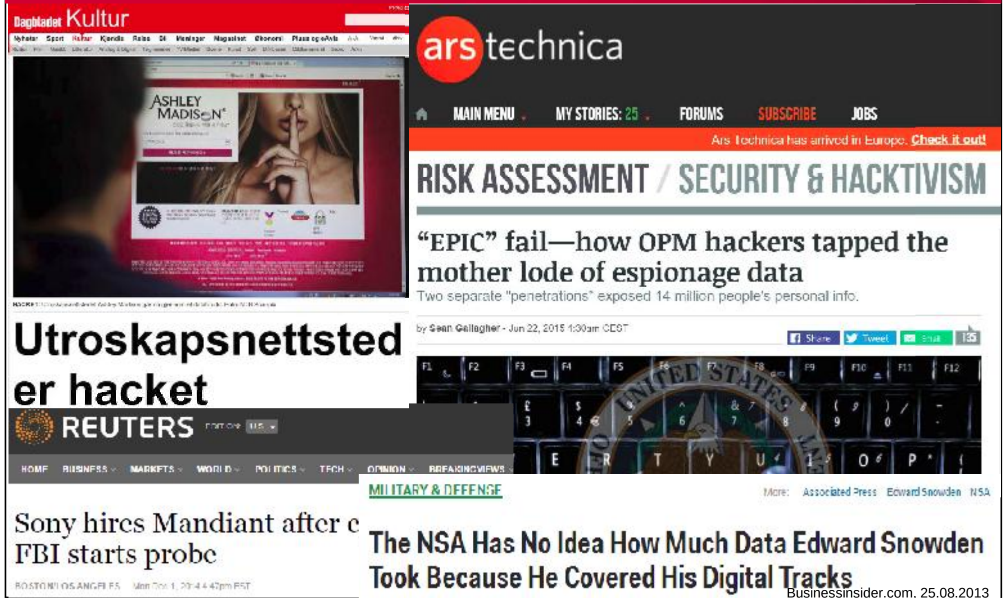
I work as:

- Head of Security
- Senior Information Security Consultant
  - Security Audits
  - Digital Forensics / Incident Response
  - Education

Outline

- Incident Response
- Digital Forensics
- Finding Evidence

Digital Forensics in Incident Response



Utroskapsnettsted er hacket

Ars Technica has arrived in Europe. Check it out!

RISK ASSESSMENT / SECURITY & HACKTIVISM

"EPIC" fail—how OPM hackers tapped the mother lode of espionage data

Two separate "penetrations" exposed 14 million people's personal info.

by Sean Gallagher - Jun 22, 2015 1:30am CEST

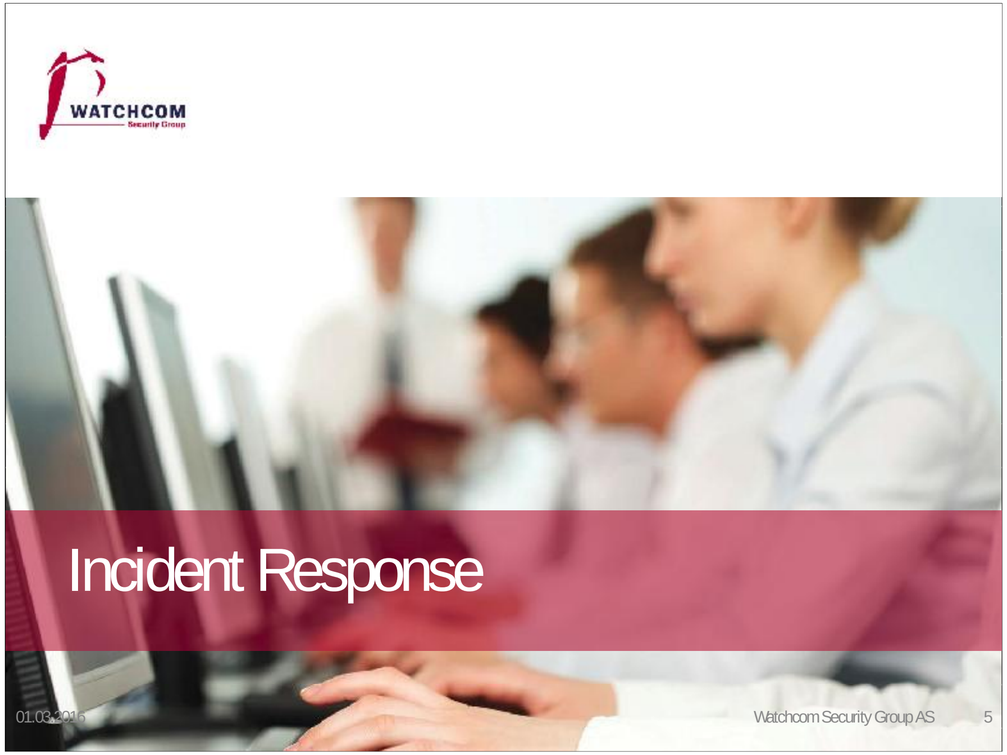
Sony hires Mandiant after c FBI starts probe

MILITARY & DEFENSE

More: Associated Press Edward Snowden NSA

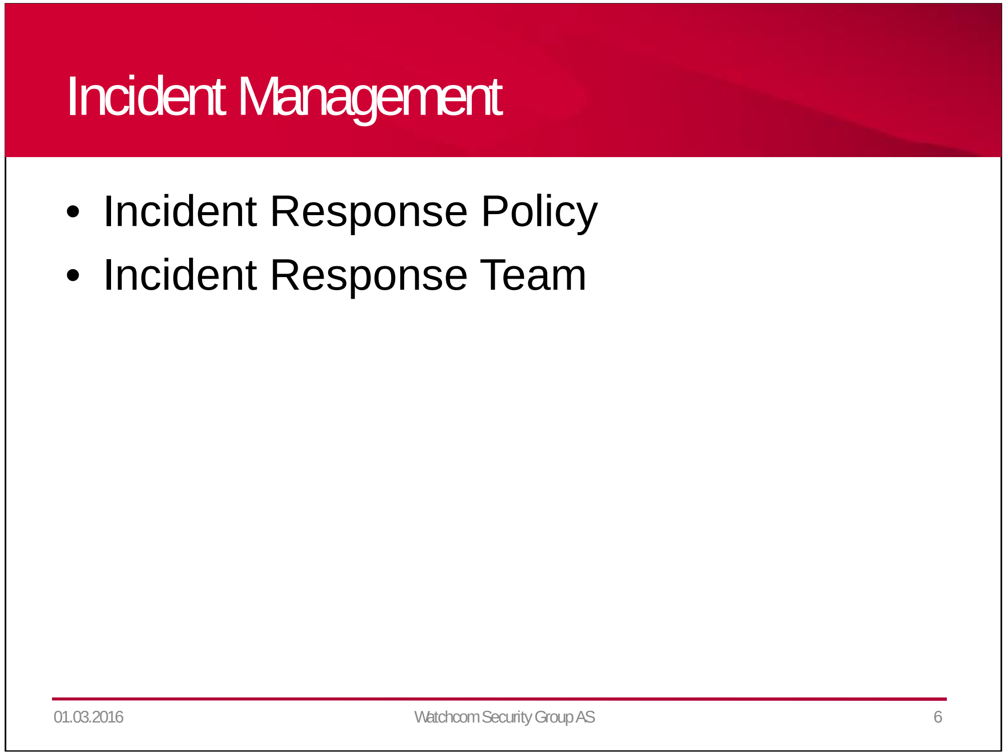
The NSA Has No Idea How Much Data Edward Snowden Took Because He Covered His Digital Tracks

Businessinsider.com, 25.08.2013



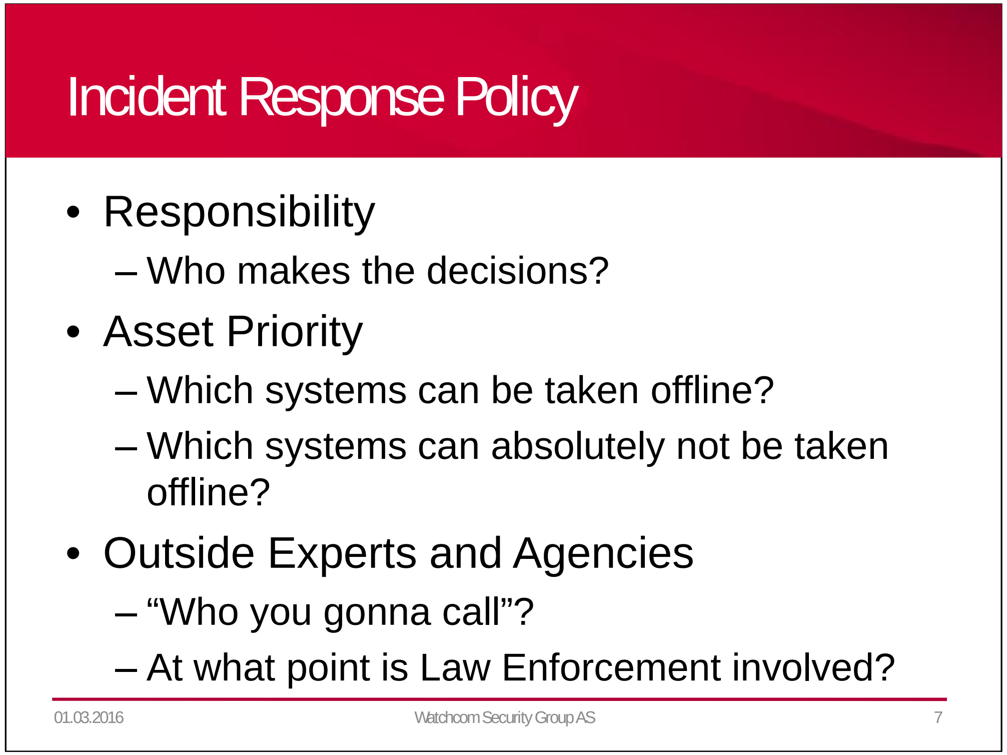
WATCHCOM Security Group

Incident Response



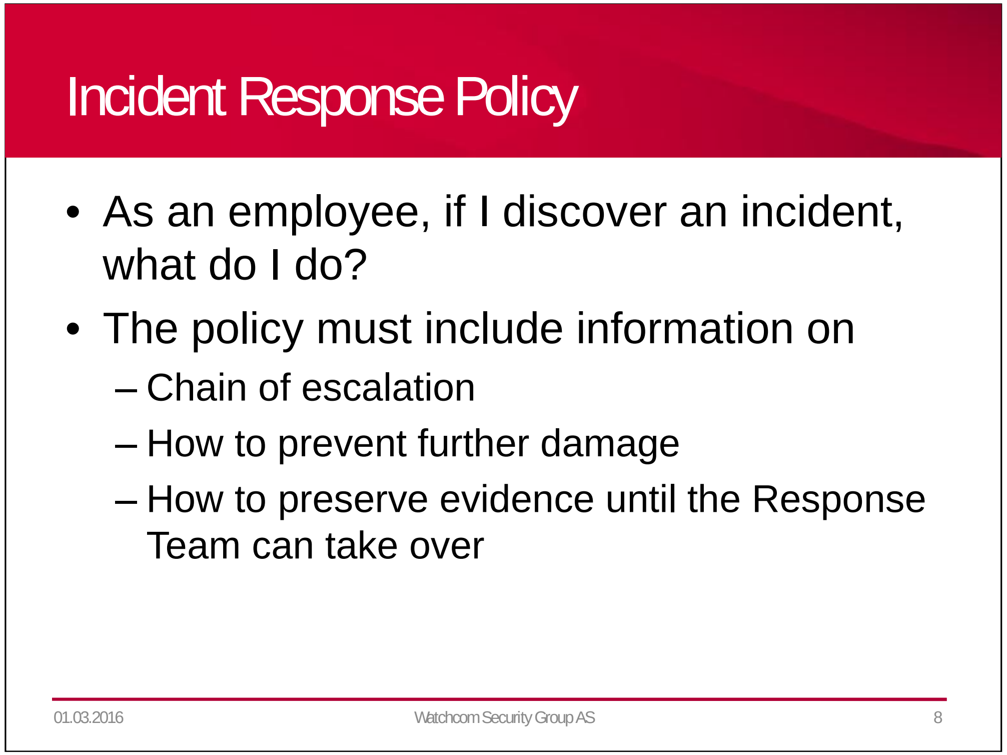
Incident Management

- Incident Response Policy
- Incident Response Team



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 you gonna 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

Red team – Blue team

- Derived from military wargames
- Simulates an actual attack against the company
- The Incident Response Team defends the system from the attack

Pearl Harbor Red Team

Incident Response Procedures

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

Triage

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

Investigation and Containment

- Collect data
- Mitigate the damage

Analysis and Tracking

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

Follow-up (Postmortem)

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

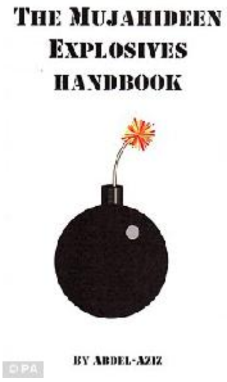
Digital Forensics

Digital Forensics in Court

- The BTK Killer – Dennis Rader
  - Metadata in Word file led to arrest after 30 years

Digital Forensics in Court

- Krenar Lusha
  - Search of laptop led to discovery of bomb-making equipment



THE MUJAHIDEEN EXPLOSIVES HANDBOOK

BY ABDEL-AZIZ

Digital Forensics in Court

- Matt Baker
  - Suicide of wife ruled murder after incriminating google searches is discovered 4 years later

Digital Forensics in Court

- Sharon Lopatka
  - Emails on her computer led to her killer
- Corcoran Group
  - Evidence that data had been deleted led to conviction

Digital Forensics

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

What is Digital Evidence?

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

What is Digital Evidence?

What is Digital Evidence?

The Forensic Investigation Process

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

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

The Digital Forensic Toolkit

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

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

Where is the Evidence?

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

When Dealing with Evidence

- R-OCITE
  - Return

  Or seize
  - Original
  - Clone
  - Image
  - Targeted copy
  - Extensive copy

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

WATCHCOM Security Group

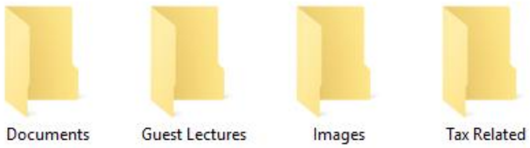
Finding Evidence

Finding Evidence

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

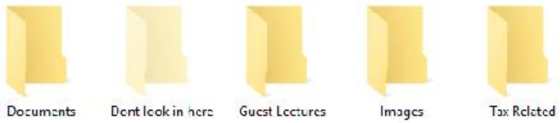
Hidden files

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



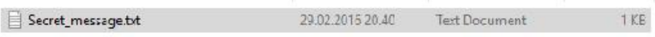
Locating hidden files

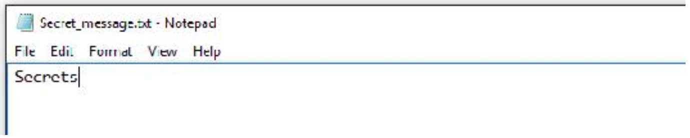
- We ignore the “hidden” flag by default
- Forensic software can be set to show the whole drive as a “flat” drive, ignoring all folders



Changing File Extensions

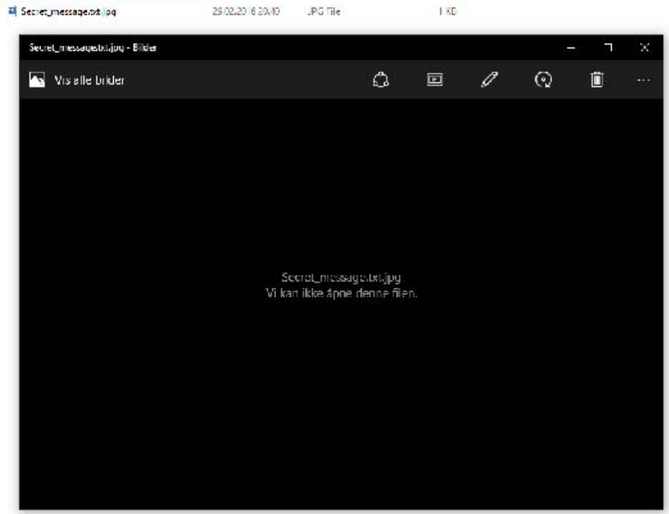
- When opening the file, the system returns an error message
- “Oh, I guess it is corrupted. Too bad.”


Secret_message.txt 29.02.2015 20.40 Text Document 1 KB


Secret_message.txt - Notepad

Secrets

Changing File Extensions



Secret_message.txt.jpg 29.02.2016 20:40 JPG File 1 KB

Secret_message.txt.jpg - Bilder

Secret_message.txt.jpg
Vi kan ikke åpne denne filen.

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”

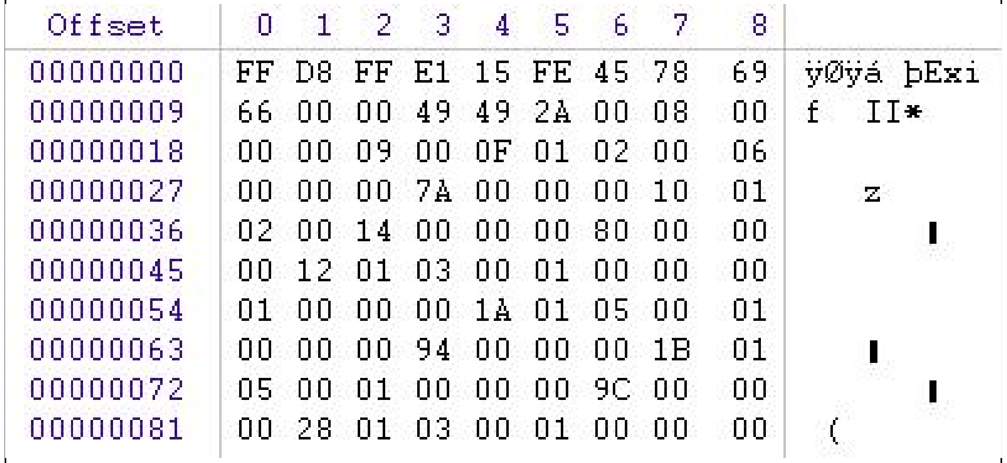
File signatures

- 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

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

Encrypted Files

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

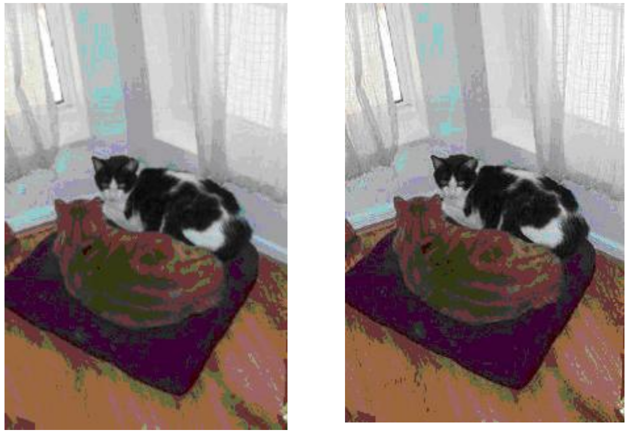
“Breaking” Encryption

- Recovering key from RAM
- Brute force
- Exploiting weaknesses in the software or the algorithm used (Cryptanalysis)
- Some countries have laws that compel the suspect to give up keys
- Less ethical methods
  - Rubber-hose cryptanalysis
  - Black-bag cryptanalysis

Steganography

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

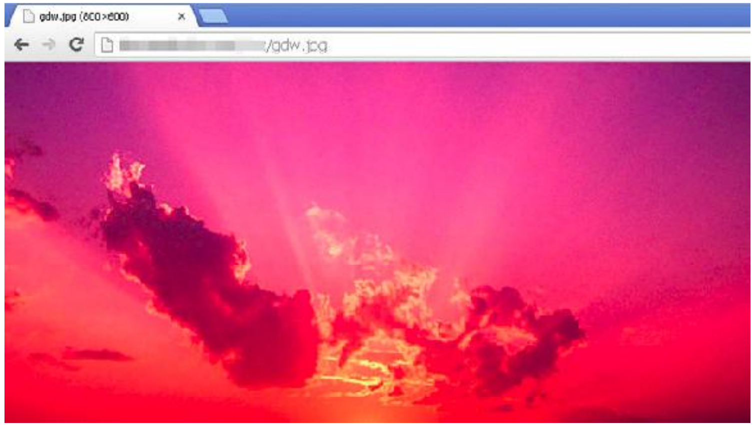
Steganography example



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

symantec.com, 02.11.2010

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
- Steganography software on the suspects computer is a strong indicator

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?

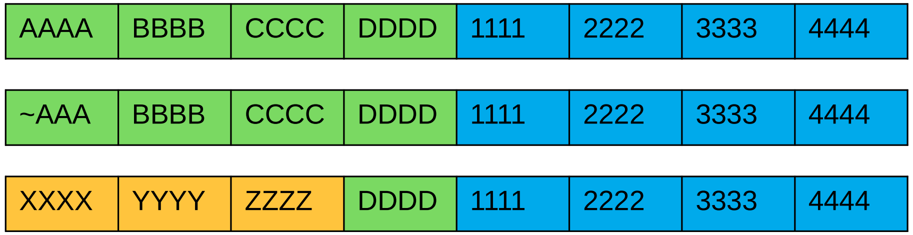
- Deleting a file does not actually remove it
- In Windows, the file is renamed
  - CorporateSecrets.txt
  - ~orporateSecrets.txt
- This tells the system that the space is available

How to reclaim it?

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

What if the space has been overwritten?

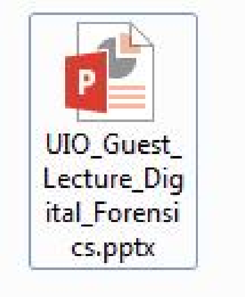
- Pieces of data can be recovered from the “file slack” between files



AAAA	BBBB	CCCC	DDDD	1111	2222	3333	4444
~AAA	BBBB	CCCC	DDDD	1111	2222	3333	4444
XXXX	YYYY	ZZZZ	DDDD	1111	2222	3333	4444

Metadata

- What if we only have a file?



UIO_Guest_Lecture_Digital_Forensics.pptx

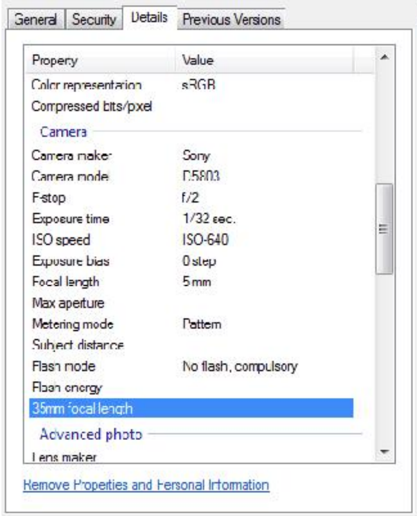
DSC_0024.JPG

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

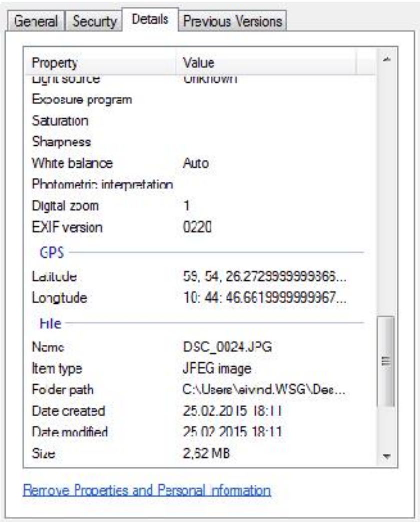
Metadata Example

Metadata Example



Property	Value
Color representation	sRGB
Compressed bits/pxel	
Camera	
Camera maker	Sony
Camera model	D5803
F-stop	f/2
Exposure time	1/32 sec.
ISO speed	ISO-640
Exposure bias	0 step
Focal length	5 mm
Max aperture	
Metering mode	Pattern
Subject distance	
Flash mode	No flash, compulsory
Flash energy	
35mm focal length	
Advanced photo	
Lens maker	

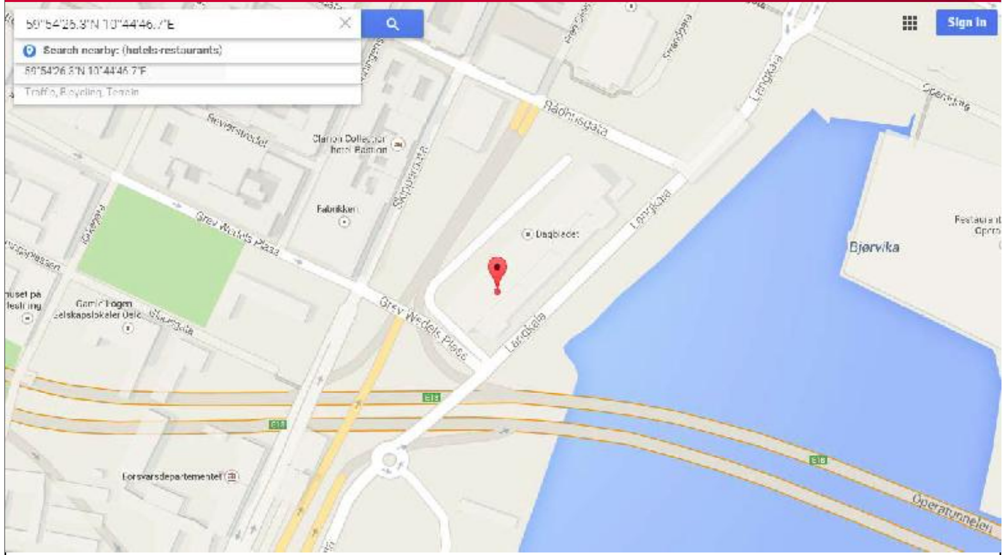
Remove Properties and Personal Information



Property	Value
Light source	Unknown
Exposure program	
Saturation	
Sharpness	
White balance	Auto
Photometric interpretation	
Digital zoom	1
EXIF version	0220
GPS	
Latitude	59; 54; 26.2729999999366...
Longitude	10; 44; 46.6619999999967...
File	
Name	DSC_0024.JPG
Item type	JPEG image
Folder path	C:\Users\eivind.WSG\Des...
Date created	25.02.2015 18:11
Date modified	25.02.2015 18:11
Size	2,52 MB

Remove Properties and Personal Information

Metadata Example



59°54'26.3"N 10°44'46.7"E

Search nearby: (hotels-restaurants)

59°54'26.3"N 10°44'46.7"E

Traffic, Bicycling, Terrain

EOL

- Questions?