9. ders belgemiz

[Belge alt konu başlığı]

zdf

Tablo : cihazlar tablosu

9. ders belgemiz

[Belge alt konu başlığı]

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

Örnek satır

**Çizilmiş metin kutusu**

Metin Kutusu : örnek açıklama

Örnek metin kutusu örnek başlık

[Kenar çubukları, metninizdeki önemli noktaları belirtmek veya hızlı başvuru amacıyla ek bilgiler yerleştirmek (zamanlama gibi) için çok kullanışlıdır.

Genellikle sayfanın soluna, sağına, üstüne veya altına yerleştirilirler. Ancak istediğiniz bir konuma kolayca sürükleyebilirsiniz.

İçeriğinizi eklemeye hazır olduğunuzda, buraya tıklayarak yazmaya başlayabilirsiniz.]

Örnek satır

Metin Kutusu 1’de gösterildiği üzere

9. ders belgemiz

[Belge alt konu başlığı]

Özel başlık

# Başlık 1dsad

Furkan Gözükara

sdff

## Başlık 2

# Furkan Gözükara

Furkan.gozukara2@toros.edu.tr

dd

## 15 Aralık 2020 Salı

9. ders belgemiz

[Belge alt konu başlığı]

Örnek satır

Örnek satır

Örnek satır

Örnek satır

Örnek satır

Örnek satır

Örnek satır

1. Örnek 1
2. Örnek 2
3. Örnek 3
   1. Örnek 3 a

Örnek 3’de gözüktüğü üzere ,

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| sdfsdfsd |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| sdf |  |  |  |  |  |  |
|  |  |  | sf |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

gfdgfdgdfgdfgdfgdf



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | ~ 15 ~ |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | 1 | 15 |  |  |  |  |  |
|  |  | 2 |  |  |  |  |  |  |
|  |  | 3 |  |  |  |  |  |  |
|  |  | 4 |  |  |  |  |  |  |
|  |  | 5 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |







Tablo : gelirler tablosu

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Şekil : metinler grafiği

Şekil : a d c

### Başlık deneme 3

*Kaynak: File:Computer Retro.svg -* [*https://en.wikipedia.org*](https://commons.wikimedia.org/wiki/File:Computer_Retro.svg)

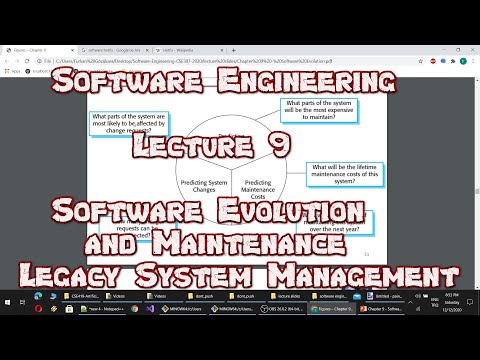
"Legal requirements for the licensing or certification of professional software engineers vary around the world. In the UK, there is no licensing or legal requirement to assume or use the job title Software Engineer. In some areas of Canada, such as Alberta, British Columbia, Ontario, and Quebec, software engineers can hold the Professional Engineer (P.Eng) designation and/or the Information Systems Professional (I.S.P.) designation. In Europe, Software Engineers can obtain the European Engineer (EUR ING) professional title."

*Kaynak: Software engineering -* [*https://en.wikipedia.org*](https://en.wikipedia.org/wiki/special:search/Software%20engineering)





😝

[](https://www.youtube.com/watch?v=ahr9l4TEIk4)

[secourses](https://www.youtube.com/watch?v=YUlyJ8UrrCw)

Tablo : giderler tablosu

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Furkan.gozukara2@toros.edu.tr

üst

b

## 0 Başlık 2

# Furkan Gözükara

Furkan.gozukara2@toros.edu.tr

dd

Şekil 2’de gösterildiği üzere

Tablo 3’de gösterildiği şekilde

Program; deneme; bilgisayar becerileri

B

ir başka metin

**Word art örnek metin**



12:56:03 ÖÖ

16.12.2020 00:56:10



CSE413 –Security of Information

Systems 2020

PhD Furkan Gözükara, Toros University

*https://github.com/FurkanGozukara/Security-of-Information-Systems-CSE413-2020*

# Lecture 7

Digital Forensics and Incident

Response

*Composed from Christian August Holm Hansen*

*@UIO 05.03.18*

Source : https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/



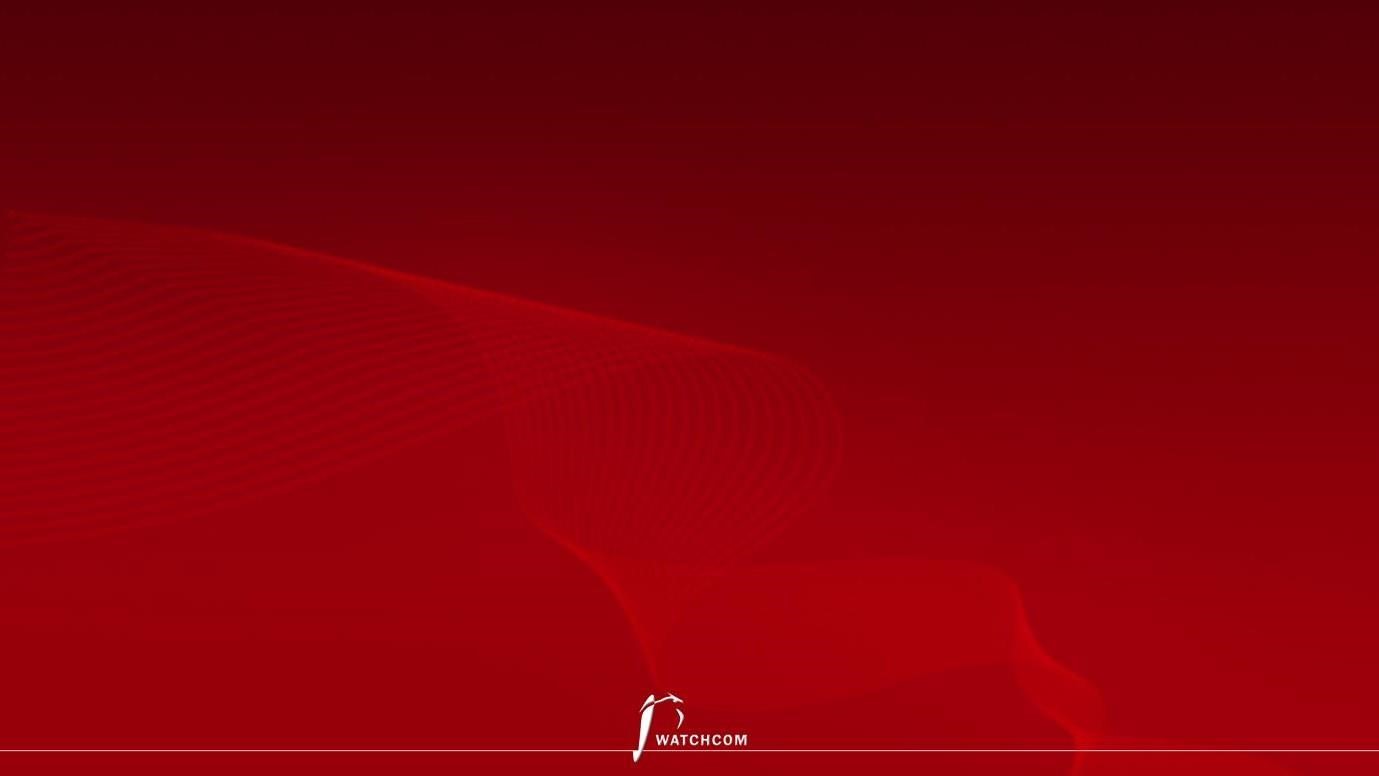
## Outline

* Incident Response
* Digital Forensics
* Finding Evidence
* Demos

Who does this?

Digital forensics is often part of an incident responder’s job - “DFIR”

* Law enforcement
* CERTs (Government/industry specific/company specific)
* In Norway: NorCERT, KraftCert, TelenorCert, FinansCert, UIOCert++
* Company IRTs
* In Norway: DNB IRT, Statoil CSIRT++
* SysAdmins
* Consultants
* In Norway: Watchcom Security Group, Mnemonic IRT++
* And others…



Incident

Response

### Incident Management

* Incident Response Policy
* Incident Response Team

## 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?

## 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

## Team

* Many names and definitions – the same principles apply to all of them (IMO)
* IRT, SIRT, CERT, CSIRT... (Response Team being the key)
* Permanent
* Virtual
* Hybrid

## Red Team – Blue Team

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

### Incident Response Procedures

* Detect
* Respond
* Recover

Source: Ross McRae, Microsoft (@HollisticInfoSec)

### Detect

Know your assets

* If you don’t know your assets, you cannot defend them

Triage

* Weed out false positives
* Categorize events
* Type of incident
* Source
* Growth
* Damage potential Source: Ross McRae, Microsoft (@HollisticInfoSec)

### Respond

* Collect data
* Mitigate damage
* Isolate systems

Source: Ross McRae, Microsoft (@HollisticInfoSec)

### Respond (2)

* Analyze and track adversary
* What is the root cause of the incident?
* Who, how, when, why
* Law enforcement
* Is it necessary?

Source: Ross McRae, Microsoft (@HollisticInfoSec)

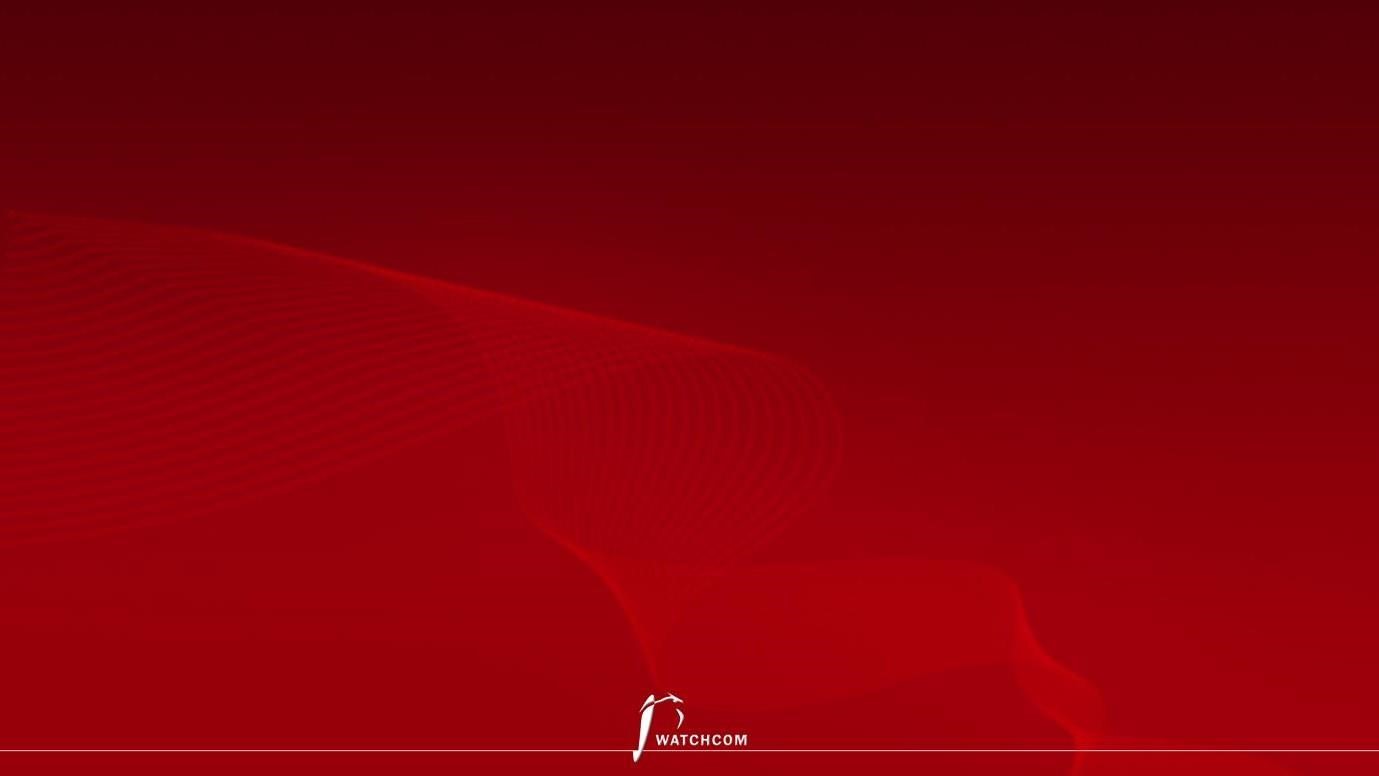
### Recover

* Fix the problem
* Improve Incident Response

Policy

* Disclosure

Source: Ross McRae, Microsoft (@HollisticInfoSec)



Digital

Forensics

### Digital Forensics in Court

The Dennis Lynn Rader (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

### Digital Forensics

It’s all the same…

* Digital forensics, computer forensics, network forensics, electronic data discovery, cyberforensics, forensic computing…

Big difference in the handing of evidence

* Law enforcement
* Corporate incidents

What is digital evidence?

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

### 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
* All digital devices may contain digital evidence If the computer is running, dump the RAM

### 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

### Evidence Location

* Network analysis • Media analysis
* Software analysis
* Hardware analysis

### Dealing with Evidence

R-OCITE

* **R**eturn

Or seize...

* **O**riginal
* **C**lone
* **I**mage
* **T**argeted copy
* **E**xtensive copy

### Admissible Evidence

* 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

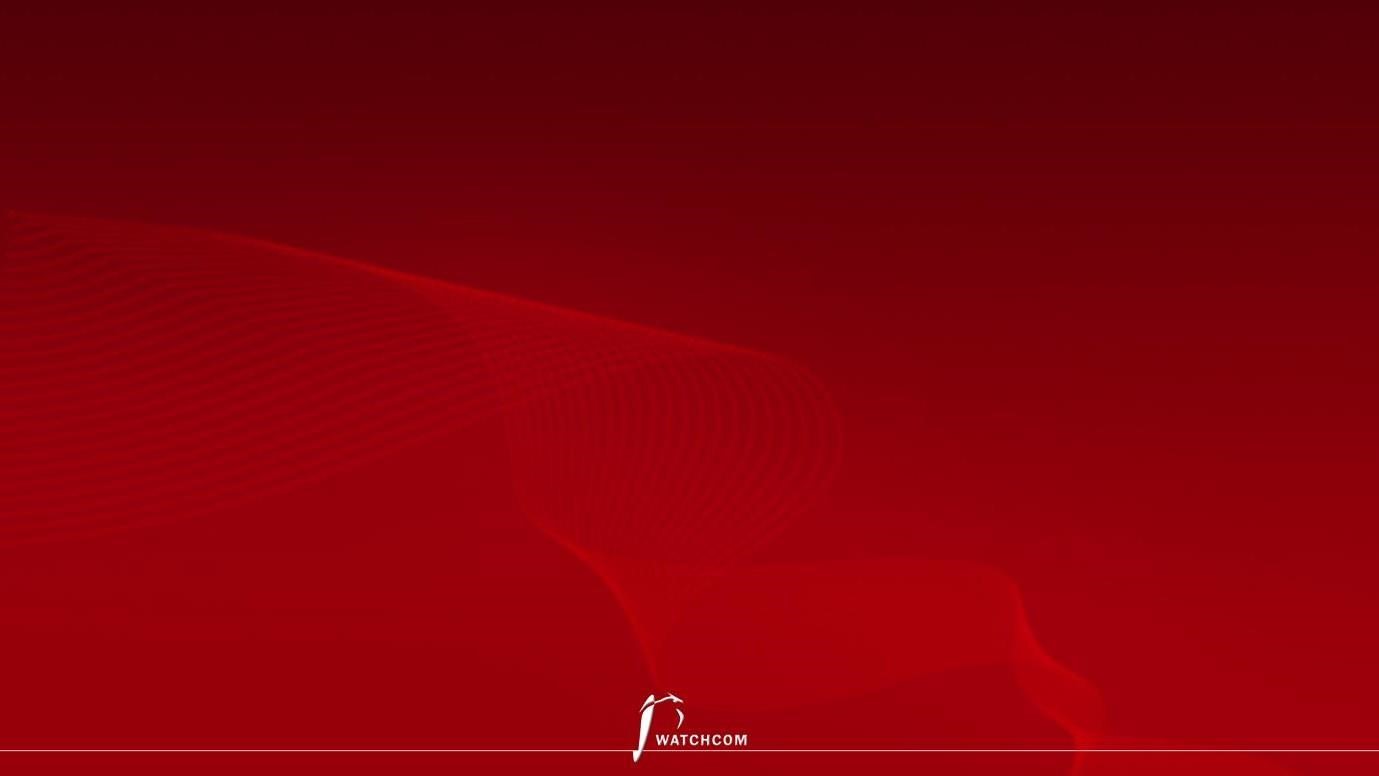
* This is what I saw

### 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 is considered hearsay unless an expert vouches for it



Finding

Evidence

### Finding Evidence

* Many ways to hide
* Many ways to find

## Hidden Files

* Setting the “hidden” flag on the file
* Different for Windows and \*nix
* Inconspicuous folder names

### Locating Hidden Files

* The “hidden” flag is ignored by default
* Forensic software can be set to show the drive as a ”flat” drive
* Ignoring folder hierarchy

### 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, also called file “headers” and “footers” 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 |

### Obscure File Names

* Hiding files by giving them inconspicuous file names
* “Blueprints\_iPhone8.jpeg” becomes “Florida vacation 001.jpeg”

## File Names not an Issue

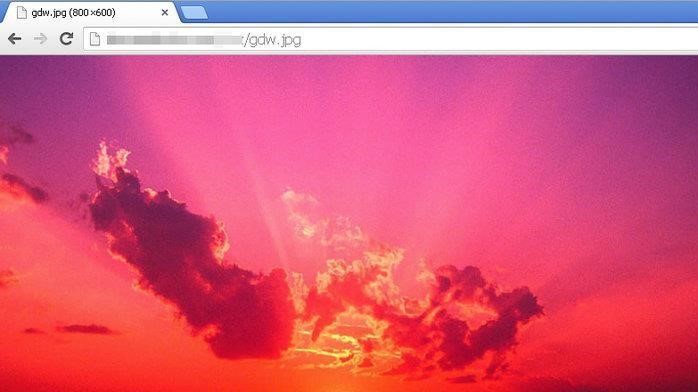
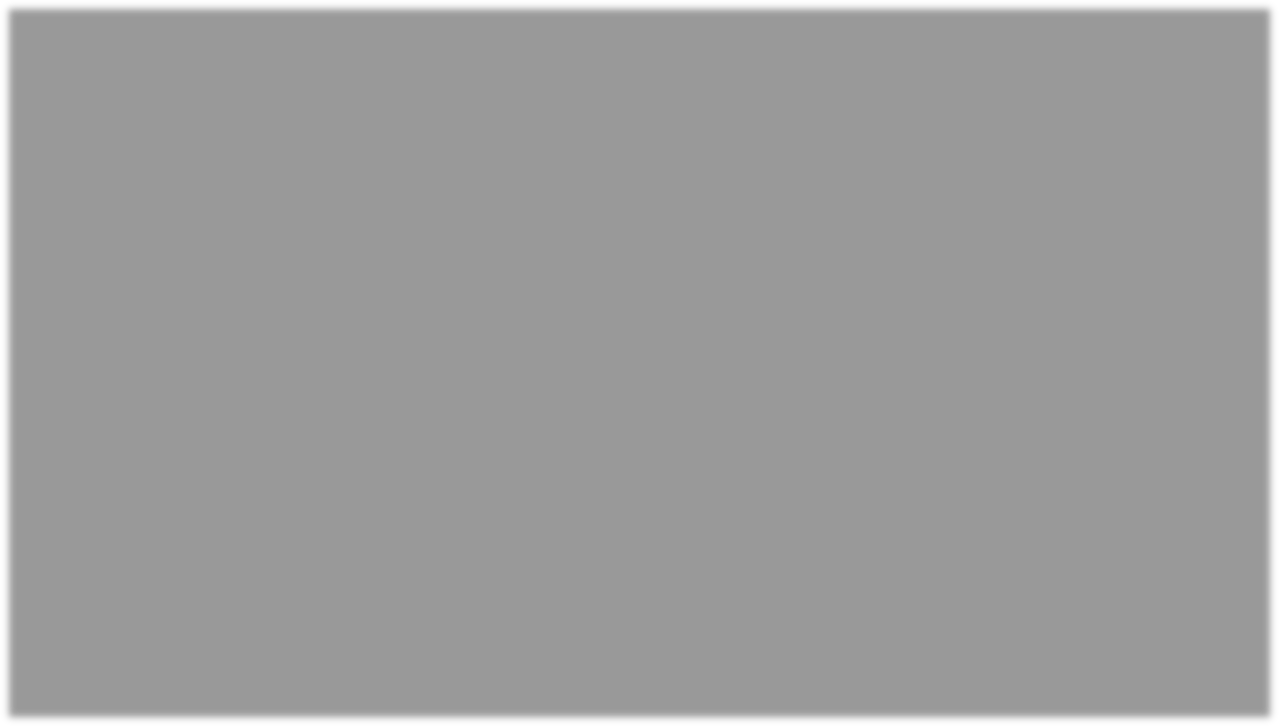
* Hash functions to look for known files
* Lists of hash sums recognize known illicit files
* Lists of hash sums recognize known ”good” files
* We can create our own lists

## Steganography

* Hiding a file inside another file
* Hiding “Nuclear Launch Codes.txt” inside “Adorable Cat.jpeg”
* Not very common

### Steganography Example

* Command & Control traffic in images



* Known sites - imgur, Dropbox, Instagram etc.
* ZeusVM botnet malware used image files to hide configuration files

### Discovering Steganography

* Hard to determine unless you are looking for it
* Steganography software on suspect’s computer a strong indicator
* File type signatures to the rescue
* Linux tools: binwalk, file

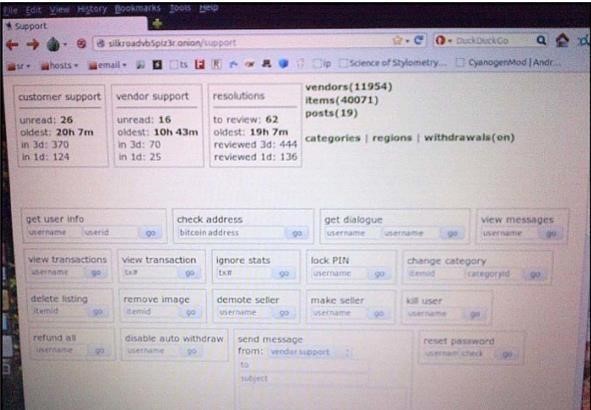
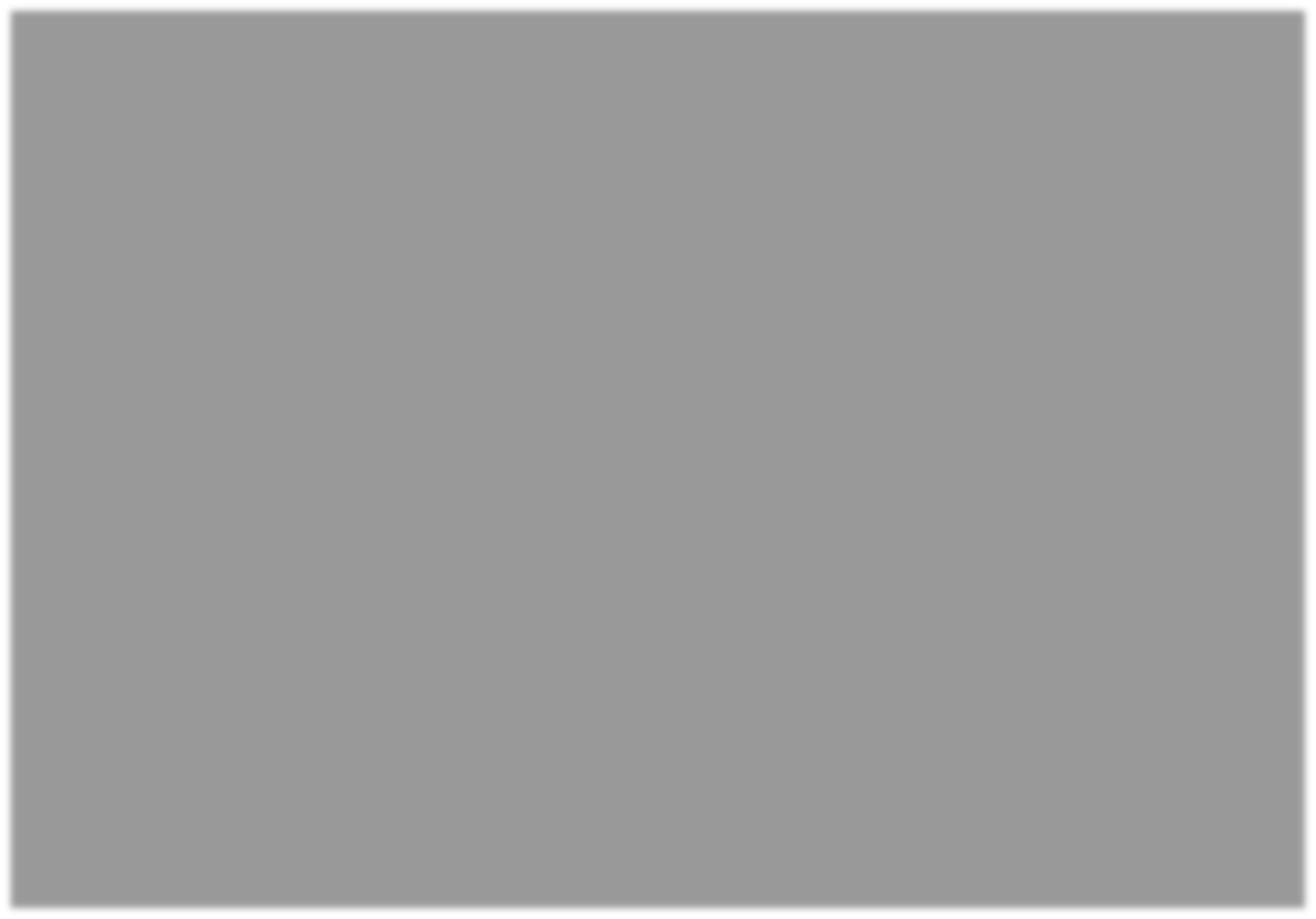
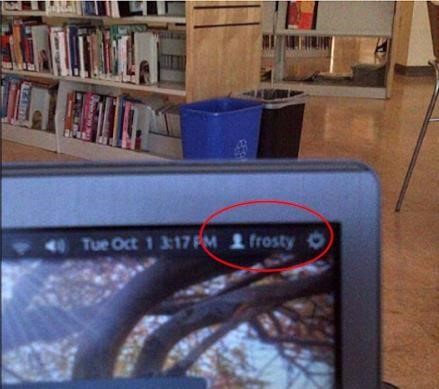
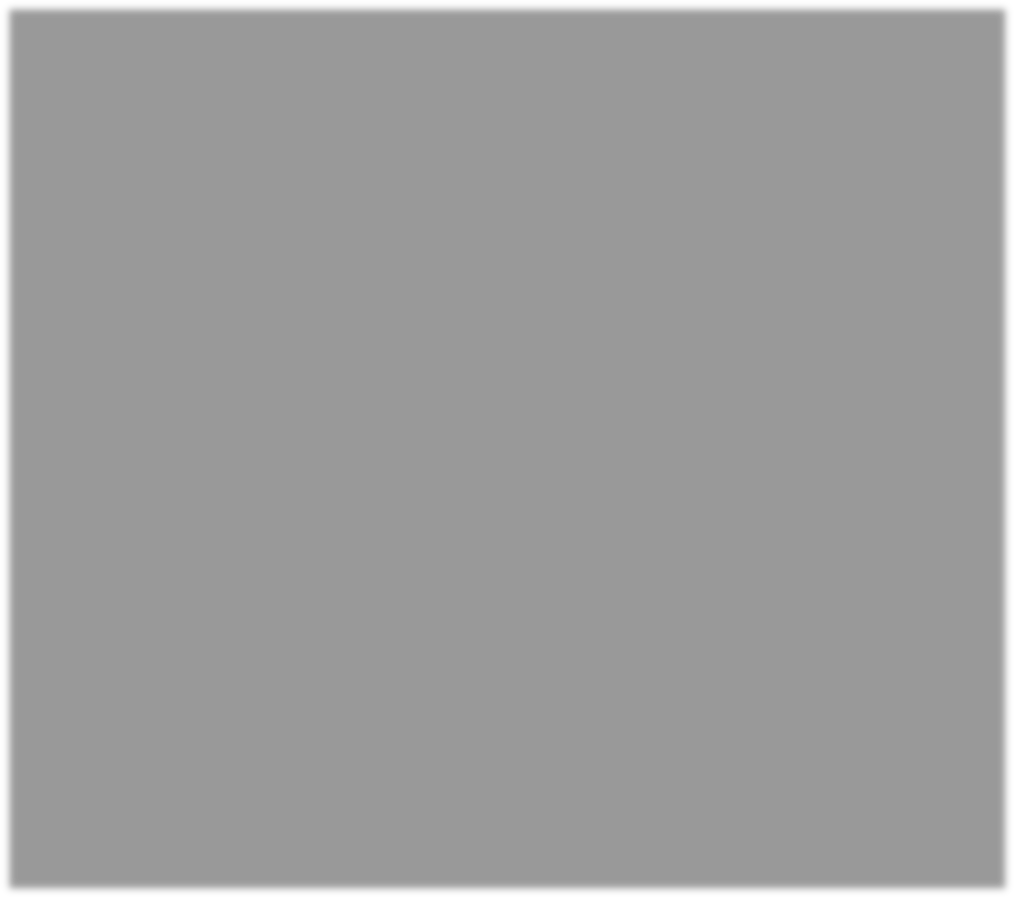
### Encrypted Files

* This is where the problems start for the investigator
* Strong encryption algorithms almost impossible to break
* “Sorry, I’ve forgotten my 50 character long password.”

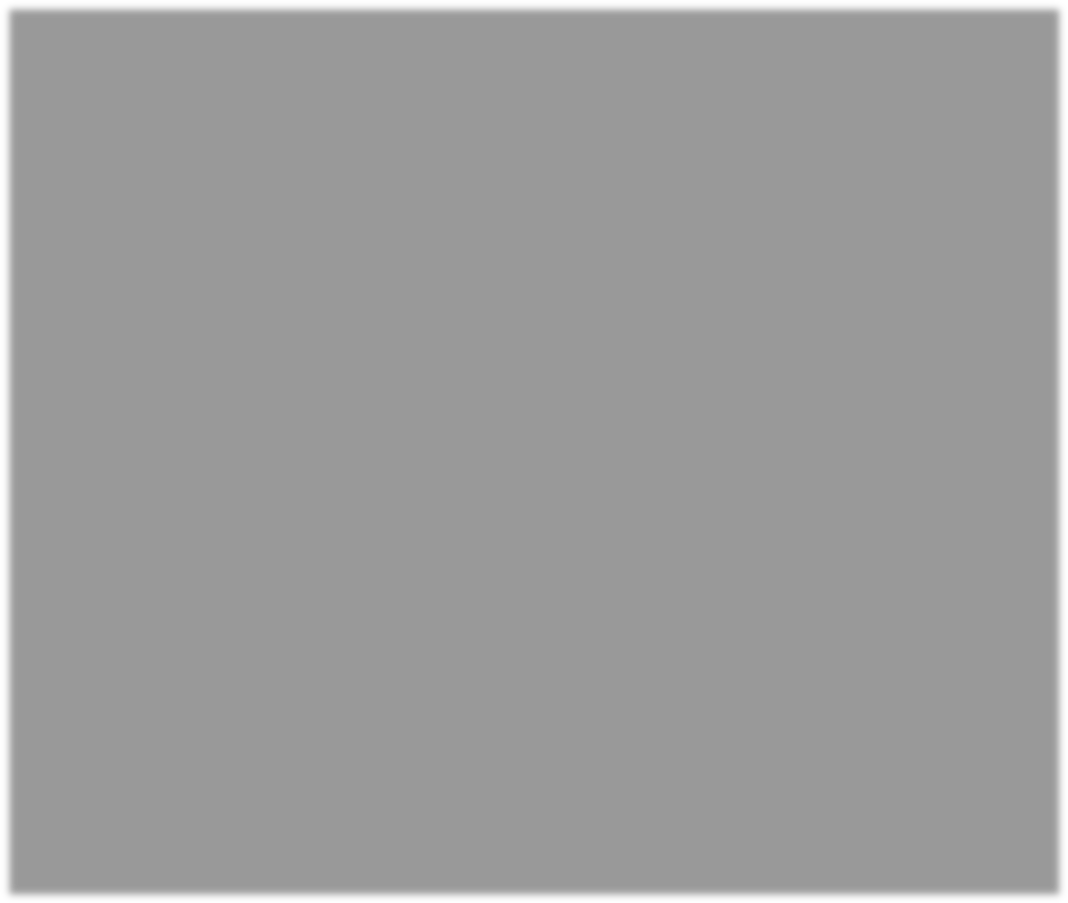
### “Breaking” Encryption

* Get access to data while unencrypted
* Recovering key from RAM
* Mimikatz
* Brute force
* Exploiting weaknesses in the software or the algorithm used (Cryptanalysis)
* Some countries have laws that compel the suspect to give up keys

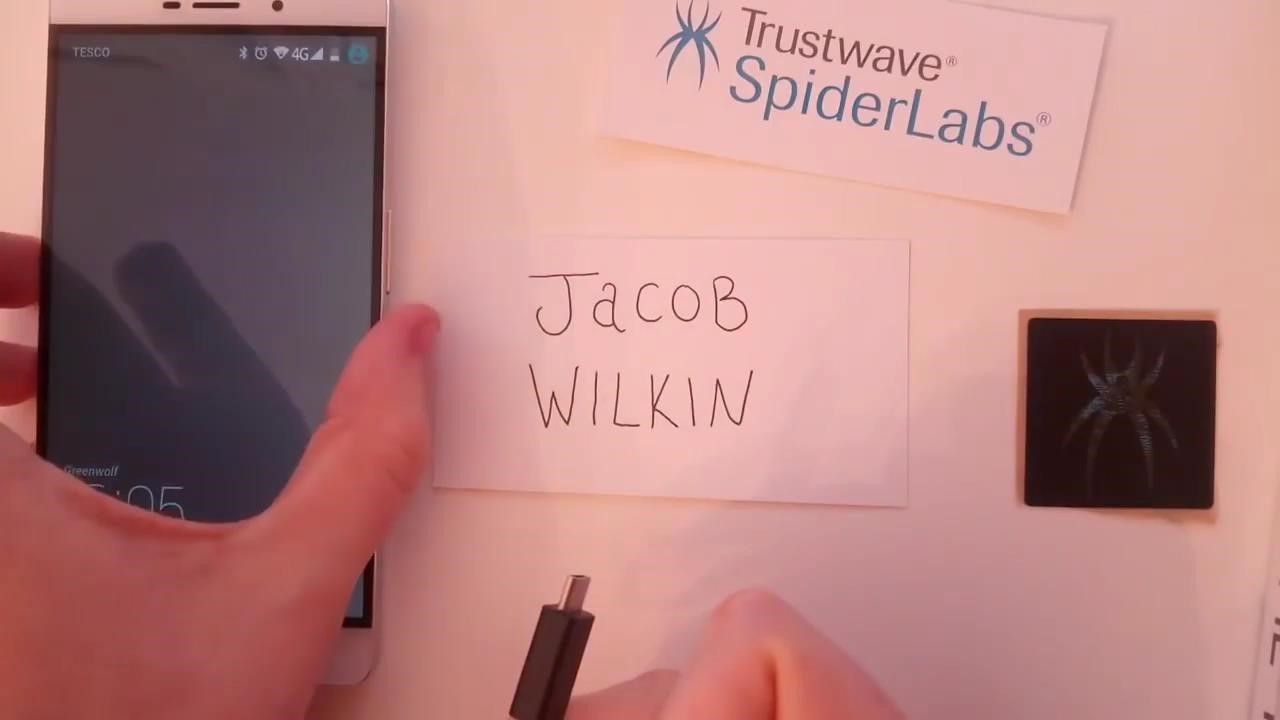
### Unencrypted data – the arrest of Ross Ulbricht



### Brute force (?) – San Bernadino case



### Exploit weaknesses



### 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 to be overwritten in the future

### Reclaiming Deleted Files

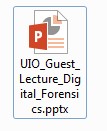
* Data carving
* Ignore file system – extract file directly from the media
* Renaming the file

### Reclaiming Overwritten Files

* Pieces of data can be recovered from “slack space”
* File slack, RAM slack, drive slack
* Forensics software can often recover files or parts of files from slack space
* People encrypt their drives nowadays

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

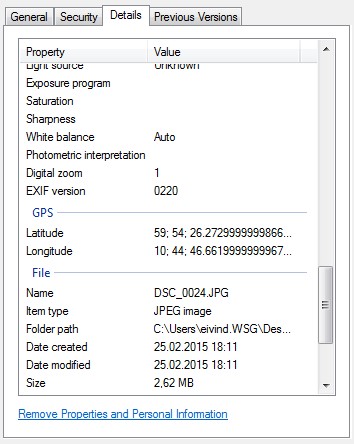
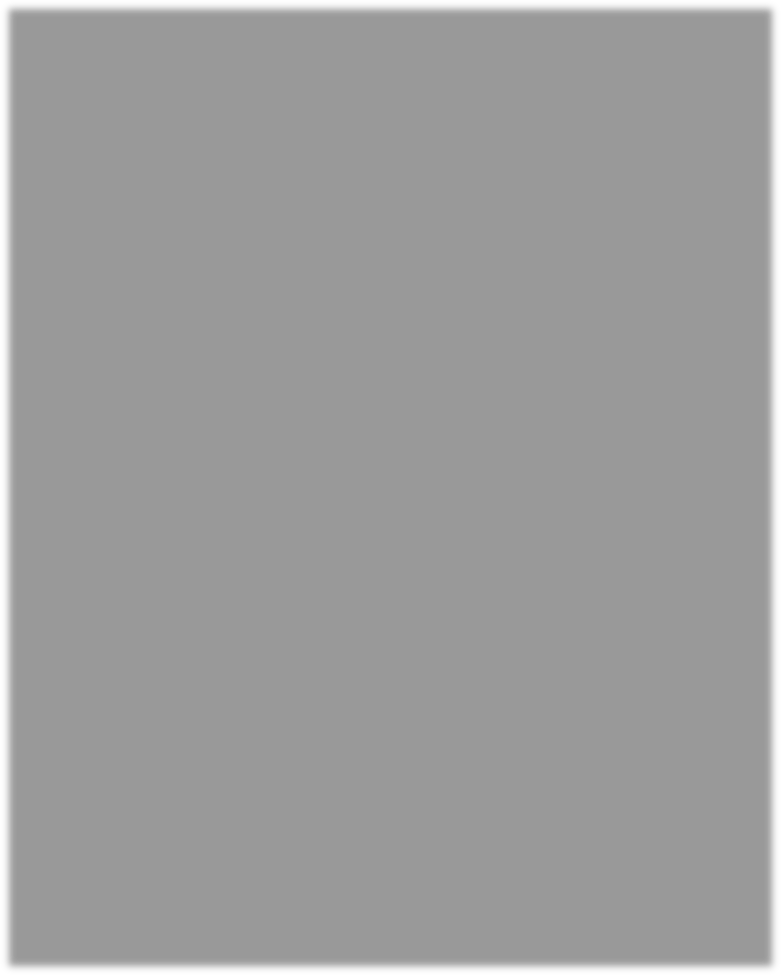
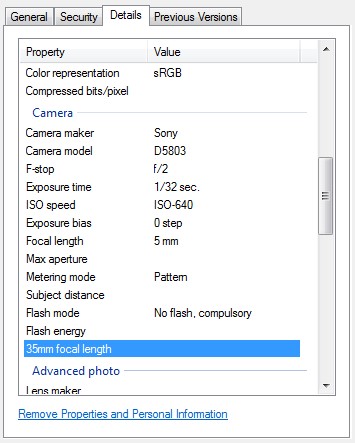
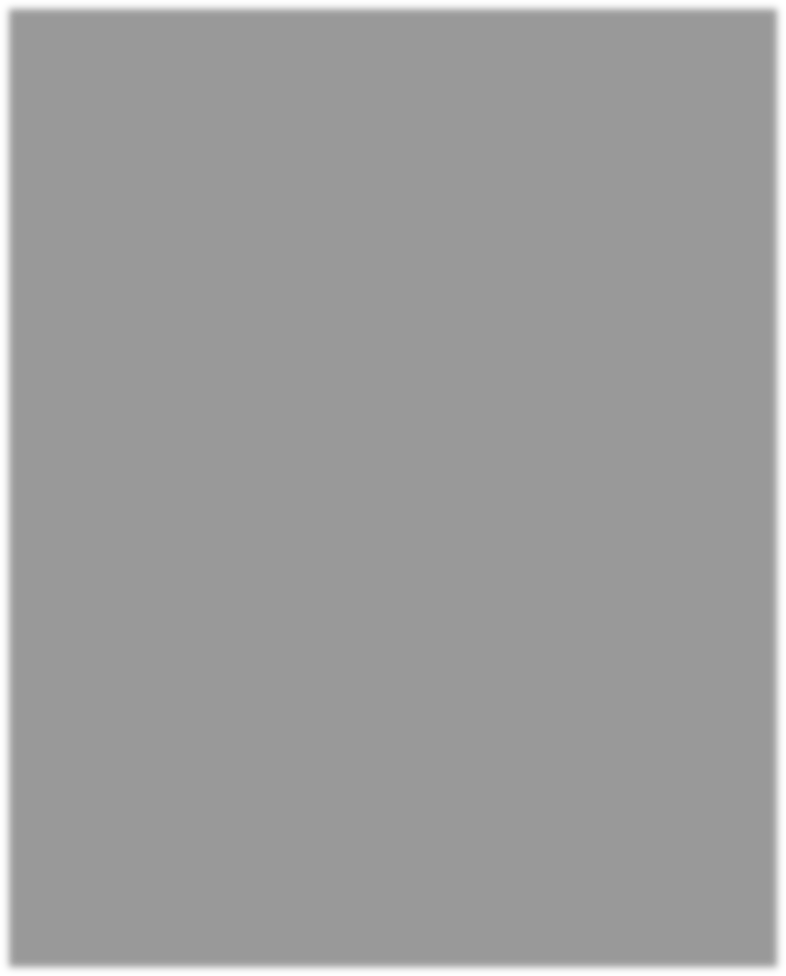
* What if we only have a file, and not the source media?

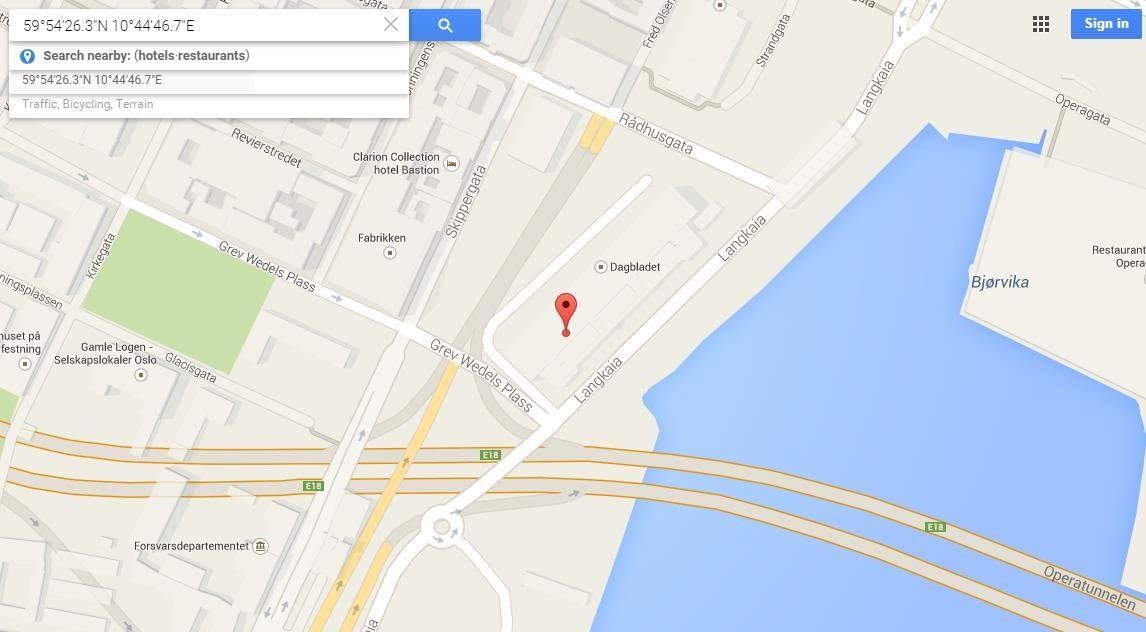


### Using Metadata

* 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 2

• Red Star OS – Appends unique system identifier to all media files



### It’s not all theory – if you want to learn more…

CTFs Courses (e.g. SANS SEC504/FOR572)

Forums (e.g. /r/forensics, /r/netsec)

Virtual machines, tools & wargames •

* Sans DBIR
* Redline
* Volatility
* Sandboxed malware (be careful…)
* Books
* Course contents are public. UseGoogle to learn the goals!

Conferences (DEFCON, DerbyCon, CCC, Paranoia)

* Videos are often published online, freely available
* Paranoia is held in Oslo Spektrum on the 29th and 30th ofMay
* Books

### /> whoami

Christian August Holm Hansen:

* M.Sc. NTNU/Eurécom
* Senior Information Security Consultant
* Pentester, advisor, incident responder
* All opinions in this presentation are my own and all facts are based on open sources

Questions?

#### [christian.hansen@watchcom.no](mailto:christian.hansen@watchcom.no)

🏛🕸