DIGITAL FORENSICS AND INCIDENT RESPONSE

Emil Taylor Bye
@UiO 2018-09-25

WATCHCOM
A COMBITECH COMPANY

~$ whoami

Emil Taylor Bye

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

WATCHCOM
A COMBITECH COMPANY

OUTLINE

- Incident Response
- Digital Forensics
- Finding Evidence
- Demo time

WATCHCOM
A COMBITECH COMPANY

SECURITY // ATTACKS & BREACHES

NEWS

5/5/2011
12:27 PM

Sony Brings In Forensic Experts Data Breaches

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

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

Change your passwords… again: another Yahoo data breach affecte million accounts

Chris Smith @chris_writes
March 2nd, 2017 at 6:50 AM

Share

SECURITY / LEER EN ESPAÑOL

Exactis said to have exposed 340 million records, more than Equifax breach

We hadn't heard of the firm either, but it had data on hundreds of millions of Americans and businesses and leaked it, according to Wired.

BY ABRAR AL-HEETI / JUNE 28, 2018 10:14 AM PDT

WATCHCOM
A COMBITECH COMPANY

WHO DOES THIS?

Digital forensics is often part of an incident responder's job

- **Law enforcements**
- **Computer Emergency Response Teams (CERTs)**
  - **In Norway: NorCert, Nordic Financial CERT, KraftCERT, Telenor CERT, Uninett CERT+++**
- **Company Incident Response Teams**
- **Sysadmins**
- **Consultants**
  - **Watchcom Security Group, mnemonic, +++**
- **+++**

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE

INCIDENT MANAGEMENT

- **Incident Response Policy**
- **Incident Response Team**

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE POLICY

- Responsibility
  - Who makes the decisions?
- Asset priority
  - What is essential
- Who?
  - Who you gonna call?
  - At what point should we/do we have to involve Law Enforcement, other agencies

INCIDENT RESPONSE POLICY

- As an employee, what do I do when I discover an incident?
  - Chain of escalation
  - How to minimize further damage
  - How to preserve evidence

INCIDENT RESPONSE TEAM

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

WATCHCOM
A COMBITECH COMPANY

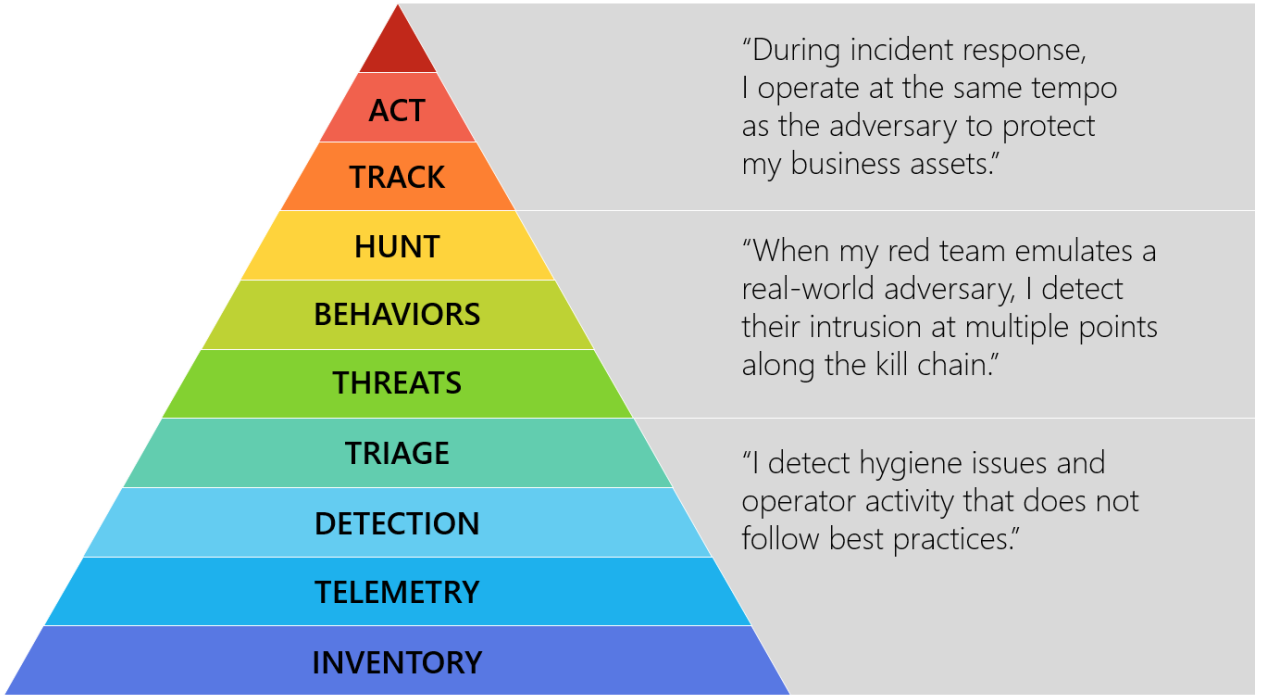
RED TEAM – BLUE TEAM

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

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE PROCEDURE

- **Detect**
- **Respond**
- **Recover**



Source: Russ McRee, Microsoft (@holisticinfosec)

WATCHCOM
A COMBITECH COMPANY

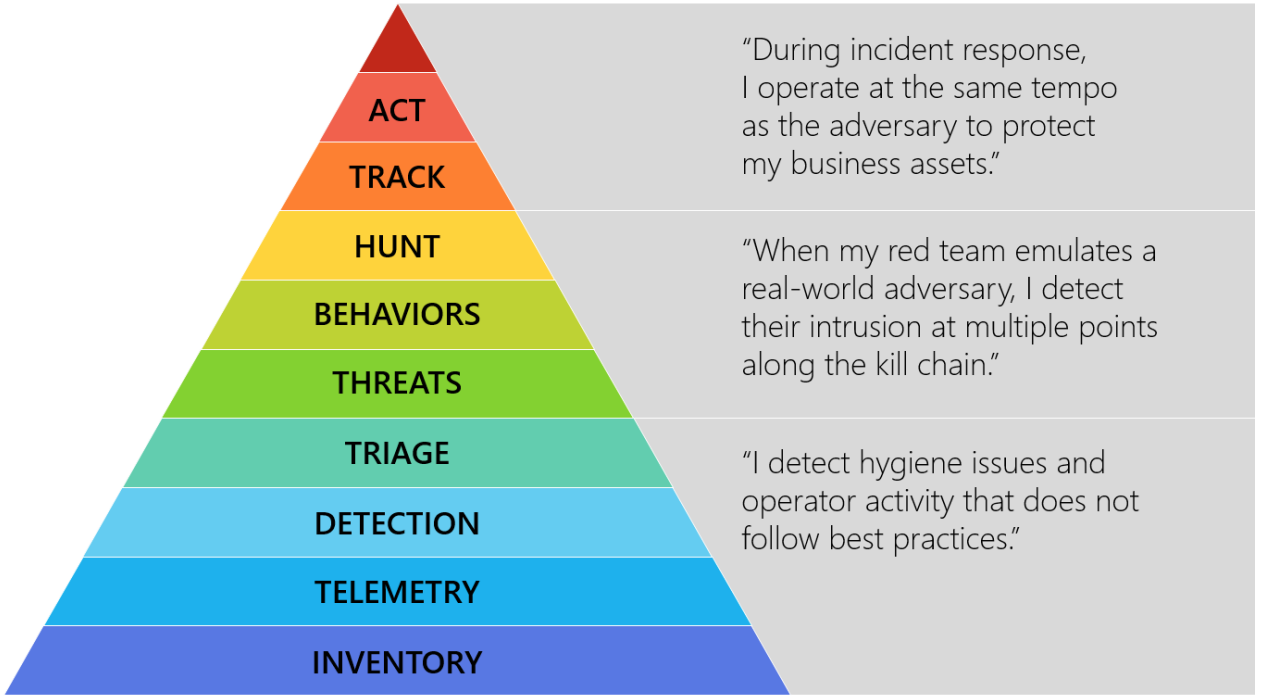
INCIDENT RESPONSE PROCEDURE

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**
  - **Spread**
  - **Damage potential**



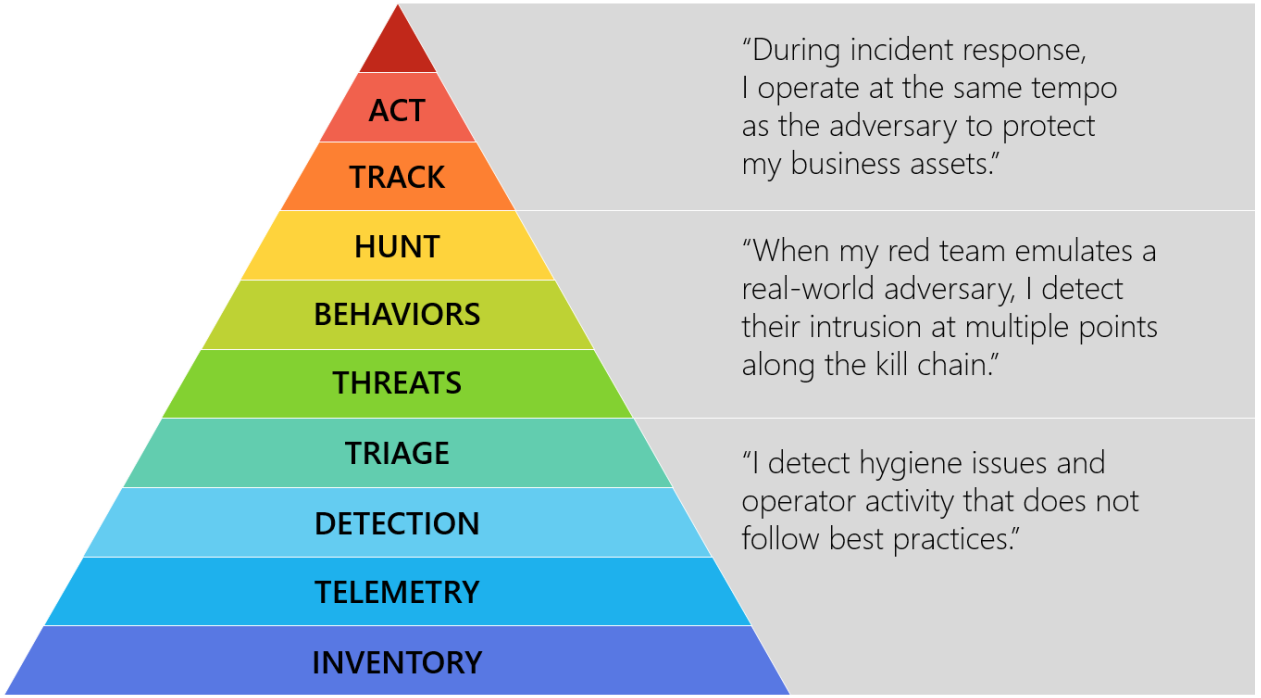
Source: Russ McRee, Microsoft (@holisticinfosec)

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE PROCEDURE

Respond

- **Collect data**
- **Mitigate damage**
- **Isolate systems**



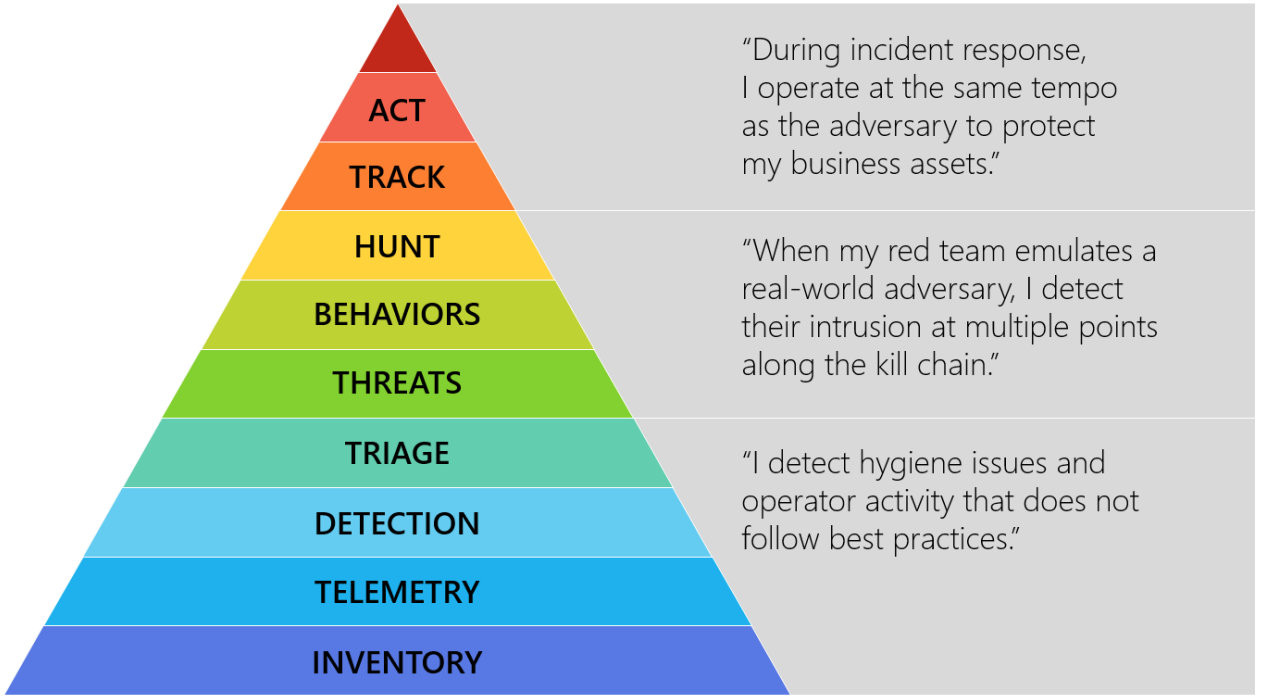
Source: Russ McRee, Microsoft (@holisticinfosec)

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE PROCEDURE

Respond (2)

- **Analyze**
  - **Root cause**
  - **How, when, why. Who?**
- **Involve others**
  - **(Law enforcement?)**



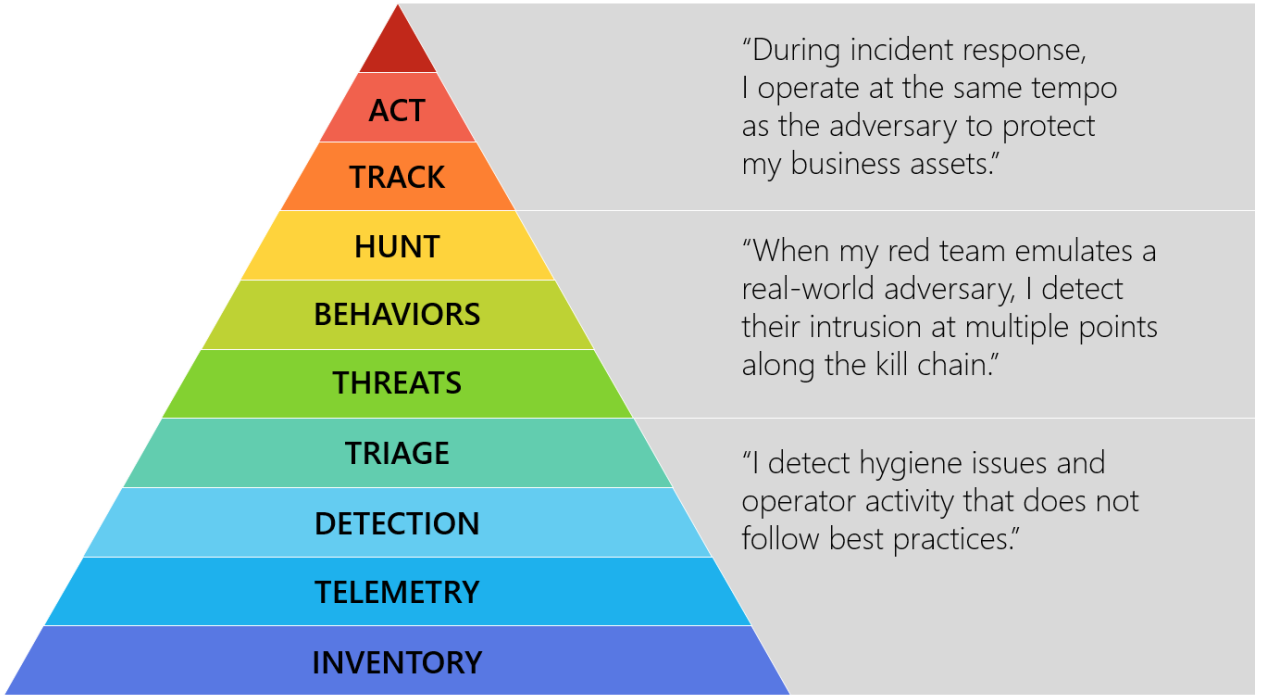
Source: Russ McRee, Microsoft (@holisticinfosec)

WATCHCOM
A COMBITECH COMPANY

INCIDENT RESPONSE PROCEDURE

Recover

- **Fix the problem(s)**
- **Disclose**
- **Analyze, improve**



Source: Russ McRee, Microsoft (@holisticinfosec)

WATCHCOM
A COMBITECH COMPANY

DIGITAL FORENSICS

WATCHCOM
A COMBITECH COMPANY

DIGITAL FORENSICS

- «BTK» Serial Killer
  - Metadata on a deleted word file on a floppy disk
- Corcoran Group
  - Evidence in deleted e-mails
- 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

WATCHCOM
A COMBITECH COMPANY

DIGITAL FORENSICS

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

- Often differences in handling of the evidence
  - Law enforcement
  - Corporate incidents

DIGITAL EVIDENCE

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

WATCHCOM
A COMBITECH COMPANY

INVESTIGATION PROCESS

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

WATCHCOM
A COMBITECH COMPANY

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

AT THE CRIME SCENE

The toolkit

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

WATCHCOM
A COMBITECH COMPANY

BASIC FORENSIC 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 ON DEVICES

- Live acquisition
  - Collect from a running system
  - Easier in some cases – such as an encrypted storage medium
- Post mortem acquisition
  - Better preservation of integrity
  - No chance of influencing the data
  - Chance of loss of volatile data

DEALING WITH EVIDENCE

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

WATCHCOM
A COMBITECH COMPANY

ADMISSIBILITY

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

EVIDENCE CATEGORIES

- Corroborative Evidence
  - This happened because of this
- Circumstantial Evidence
  - Because of this, that happened
- Opinion Evidence
  - This is what I believe happened
- Hearsay Evidence
  - I heard this about that

In general, digital evidence is considered hearsay unless an expert vouches for it

FINDING EVIDENCE

WATCHCOM
A COMBITECH COMPANY

EVIDENCE

- Many ways to hide
- Many ways to find

WATCHCOM
A COMBITECH COMPANY

HIDDEN FILES

- Hiding the file by setting the «hidden» flag
- Hide in plain sight

- «Hidden» files are typically not very hard to find
- Forensic software can be set to show the drive as a ”flat” drive
  - No folder hierarchy

CHANGING FILE EXTENSIONS

- Typically will return an error message when the user tries to open the file
  - "I guess it is corrupted, oh well, too bad"
- Can in many cases be defeated by fingerprinting the file contents
- Mismatch between file extension and file contents should be a red flag for forensic software
- Many file formats use "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

OBSCURING FILE NAMES

- Hiding files by giving them inconspicuous file names
- “Blueprints_iPhone8.jpeg” becomes “Florida vacation 001.jpeg”

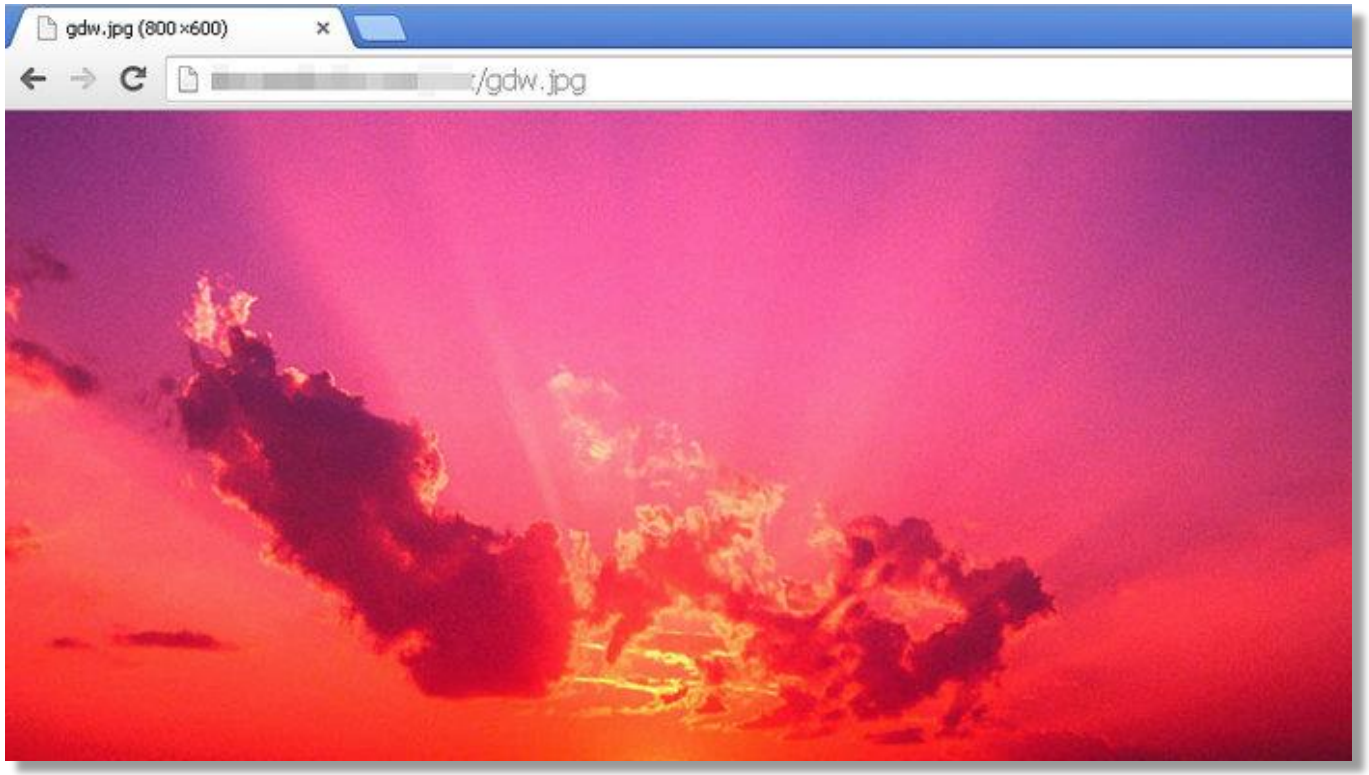
- Hash functions to look for known files
  - Lists of hash sums recognize known illicit files
  - Lists of hash sums recognize known ”good” files
  - We can create our own lists

STEGANOGRAPHY

- Hiding a file inside another file
- Hiding “Nuclear Launch Codes.txt” inside “Cute_Cat2.jpeg”

STEGANOGRAPHY EXAMPLE

- Command & Control traffic in images
  - Known sites - imgur, Dropbox, Instagram etc.
- ZeusVM botnet malware used image files to hide configuration files



WATCHCOM
A COMBITECH COMPANY

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

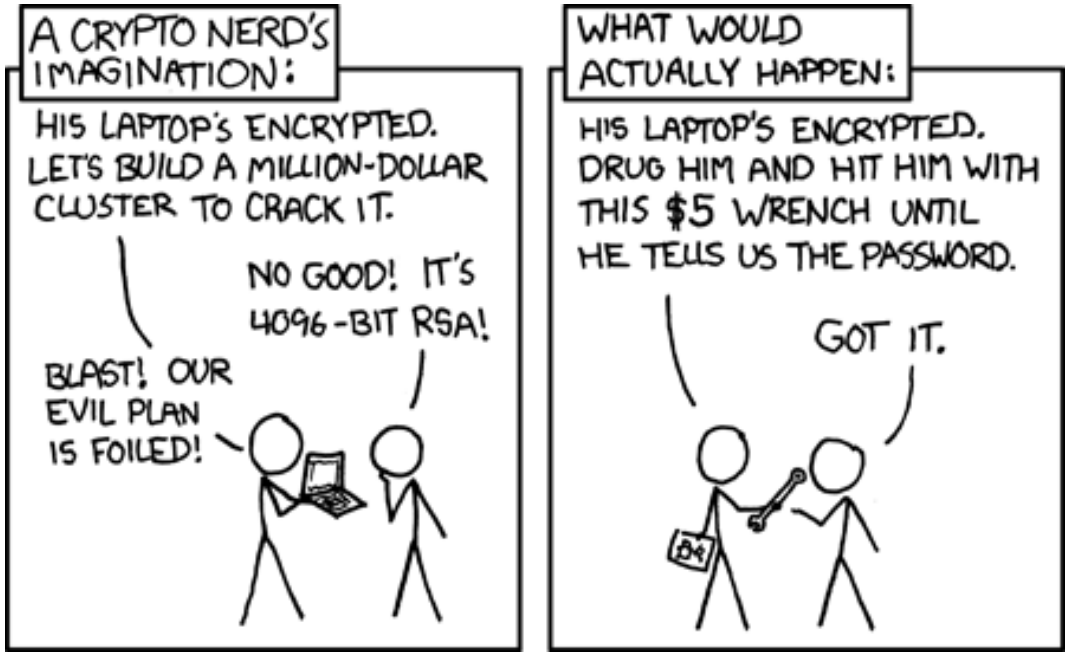
ENCRYPTED FILES

- 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

- 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

“BREAKING” ENCRYPTION



xkcd.com/538

The Intercept_

BRITISH HACKER WINS COURT BATTLE OVER ENCRYPTION KEYS

Ryan Gallagher

May 10 2016, 5:42 p.m.

WATCHCOM
A COMBITECH COMPANY

DELETING FILES

- Deleting files before they can be found
- If there are no signs at all of deleted files, it is as if they never were there

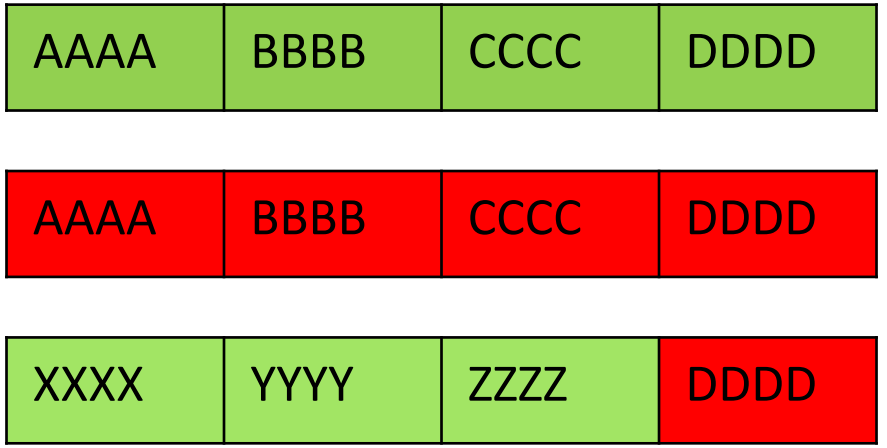
- Deleted files are generally not deleted
  - Set a “deleted” flag to let the system know that the space is available and can be overwritten

RECLAIMING DELETED FILES

- Data Carving
  - Ignore file systems, extract data directly from the medium
- “Unset” deleted flag

RECLAIMING DELETED FILES

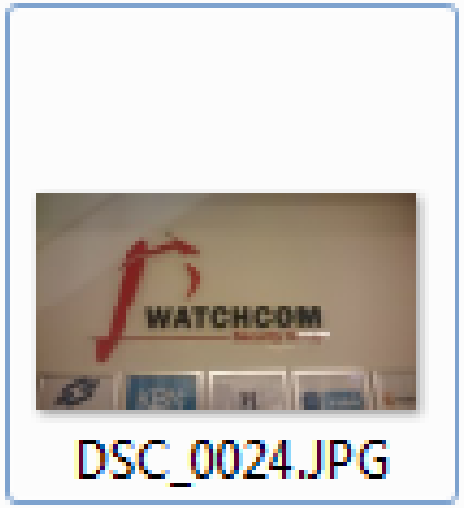
- Pieces of data can be recovered from “slack space”
- File slack, RAM slack, drive slack
- Forensics software can often recover files or parts of files from slack space



WATCHCOM
A COMBITECH COMPANY

METADATA

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



WATCHCOM
A COMBITECH COMPANY

USING METADATA

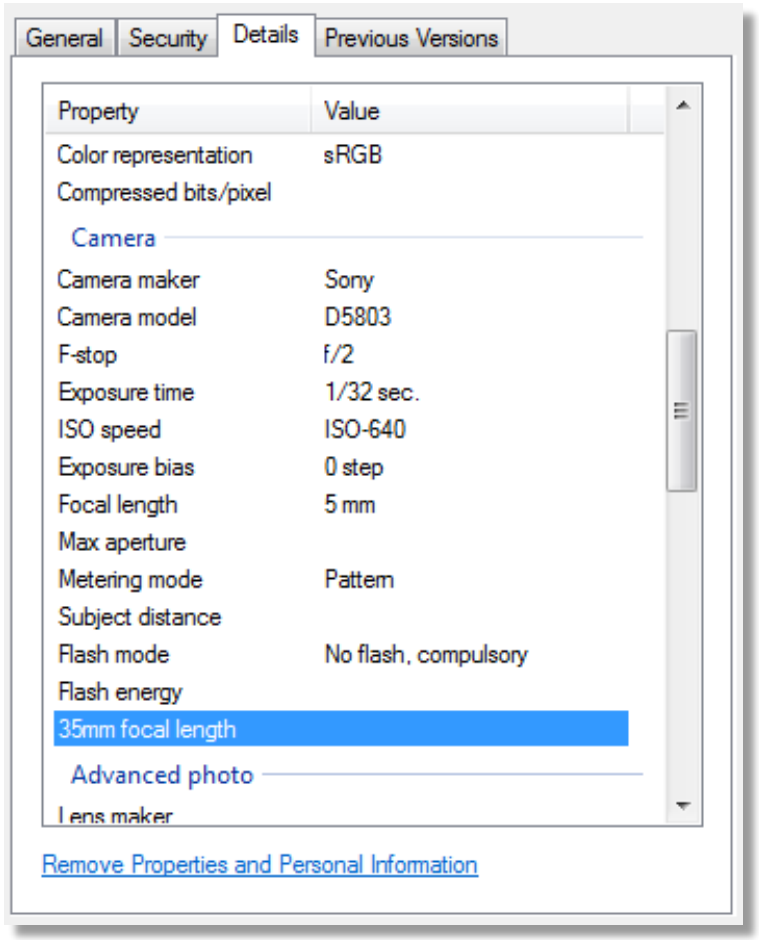
- Data about the file
  - When was the file last used?
  - When was the file created?
  - Who opened it?
  - Where was it created?
- Can prove who had access to the file

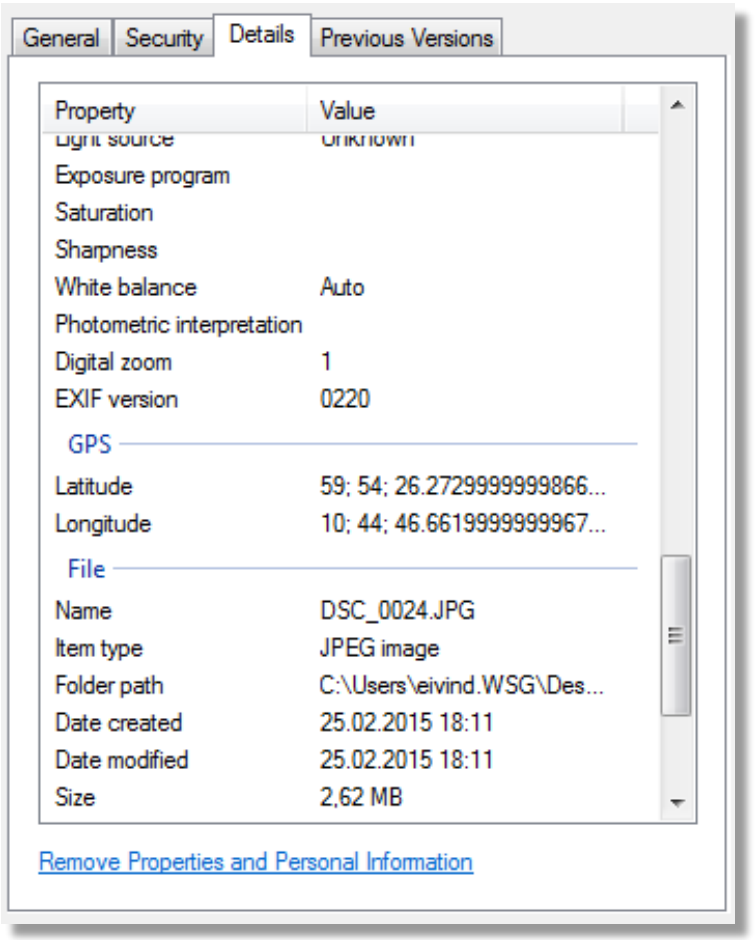
WATCHCOM
A COMBITECH COMPANY

METADATA EXAMPLE

WATCHCOM
A COMBITECH COMPANY

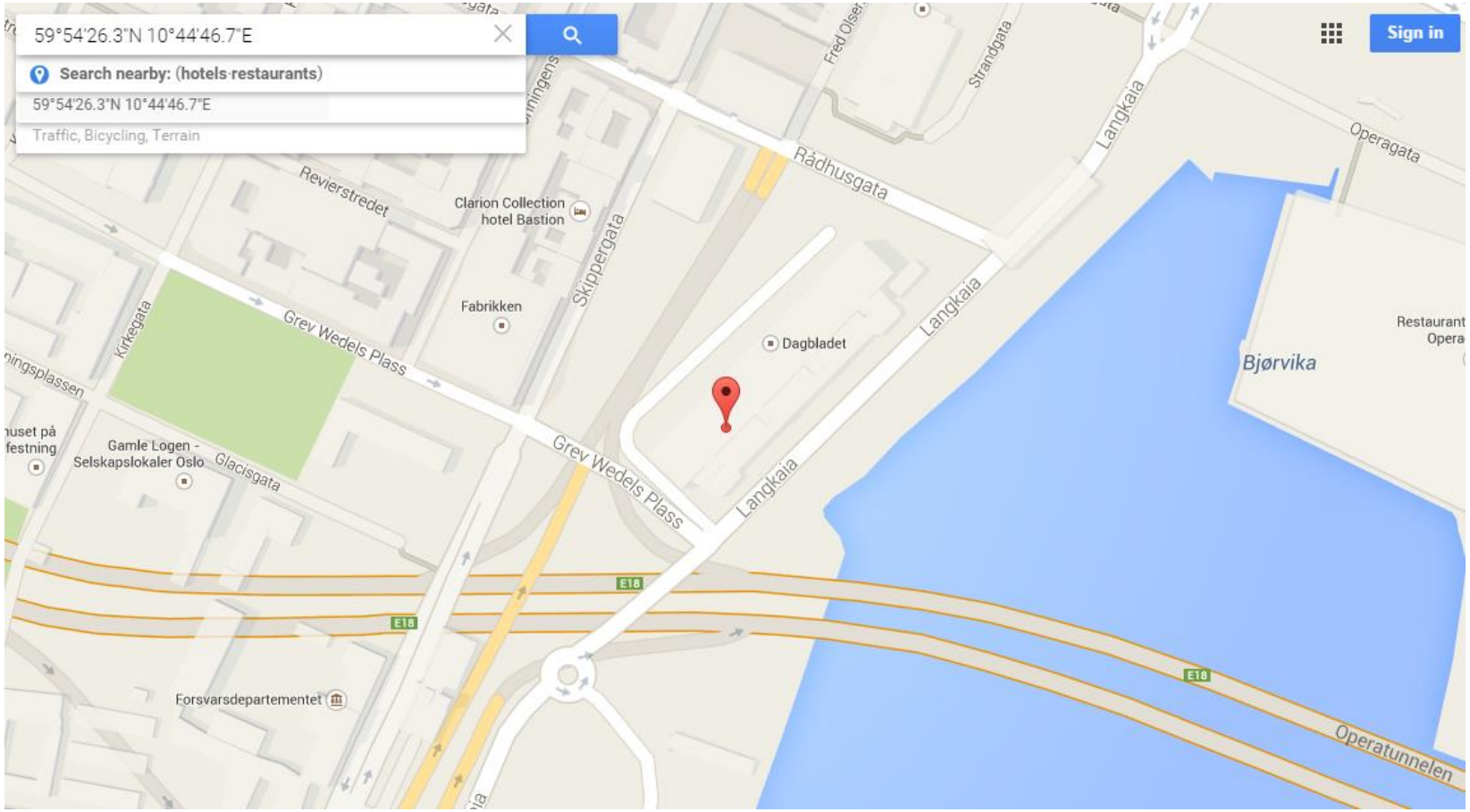
METADATA EXAMPLE





WATCHCOM
A COMBITECH COMPANY

METADATA EXAMPLE



WATCHCOM
A COMBITECH COMPANY

METADATA EXAMPLE 2

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

WANT TO TRY?

- CTFs
- Forums (/r/forensics, /r/netsec)
- Virtual machines, tools & wargames
  - Sans DBIR
  - Redline
  - Volatility
  - Sandboxed malware (be careful…)
- Books

- Courses (e.g. SANS SEC504)
  - Course contents are public. Use Google to learn the goals!
- Conferences (DEFCON, Black Hat, BSides, Paranoia)
  - Videos are often published online, freely available
  - Paranoia is held in Oslo Spektrum on the 21st and 22nd of May
- Books

QUESTIONS?

- **emil.bye@watchcom.no**

WATCHCOM
A COMBITECH COMPANY

DEMO TIME

- What do you want to see?
  - Red Star OS
  - Gaudox Botnet
    - Redline Forensics Utility
  - I want to go home