Detica Forensics

REVEALING DIGITAL EVIDENCE

From Gamekeeping to Poaching - Information Forensics and Associated Challenges

Andy Clark

Eurocrypt 2008, Istanbul

14 April 2008

Detica

INFORMATION INTELLIGENCE

Disclaimer

- The contents of this presentation are the personal views of the presenter and do not represent any opinion or statement of Detica plc or any of its subsidiaries or operating companies

Contents

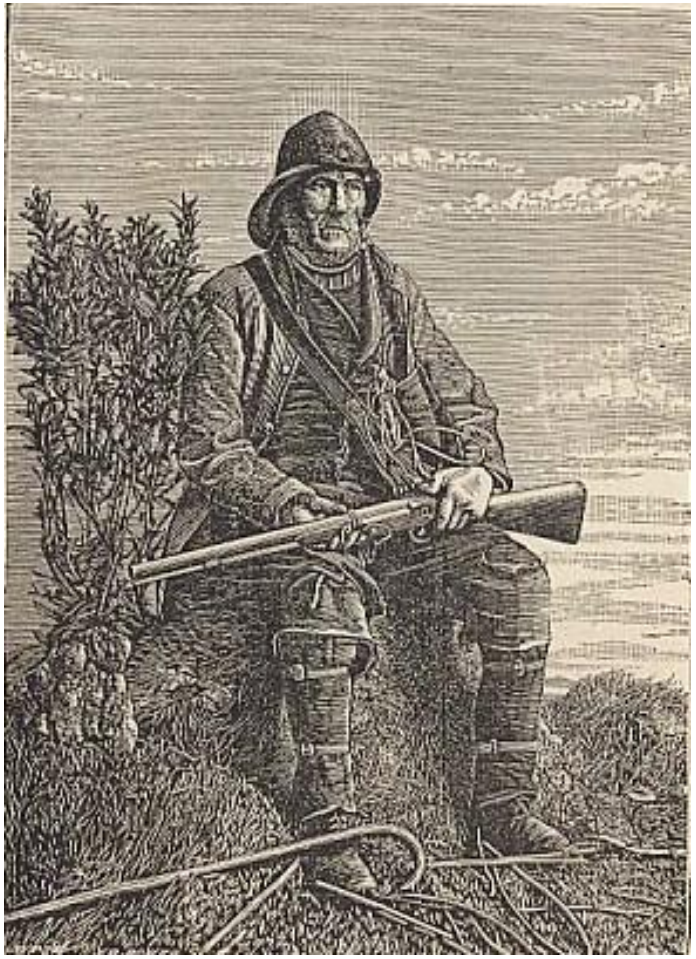
- What's a Gamekeeper and a Poacher
- Historical context – lessons learned 1984
- Information forensics – history and current relevance
- Computer forensic investigations – phases and challenges
  - The elephant in the room – encrypted data
- Dead or alive?
- Case studies
- Lessons learned 2008

Gamekeeping and Poaching explained …

- Gamekeeper
  - Looks after an area of countryside to make sure there is enough game for hunting and fish for angling
  - Actively manages areas of woodland, waterway, farmland etc for game birds/animals
  - Typically employed by the owner of the land to prevent loss of the fish, birds and animals by specialist thieves known as poachers

Gamekeeping and Poaching explained …

- Poacher
  - Someone who steals the fish, game birds and animals from a landowner
  - Normally works alone and frequently leaves hidden traps to catch wildlife
  - Tries to evade detection by taking only small quantities of wildlife at any one time



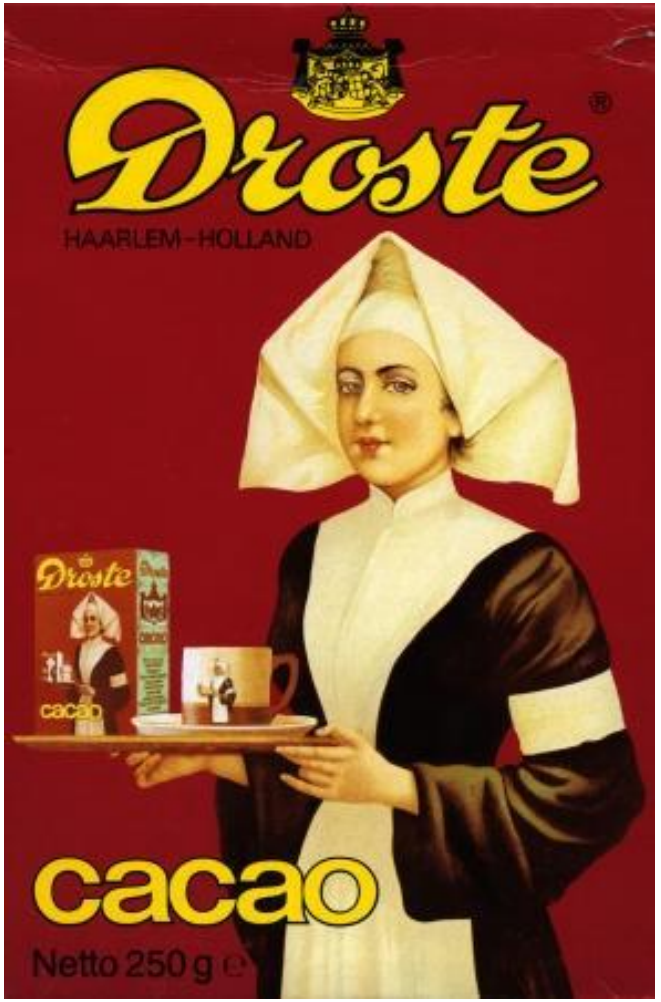
In Information Security terms …

- A Gamekeeper might be the designer of a secured information system to protect a set of assets against compromise, such as loss of:
  - Confidentiality
  - Integrity
  - Availability
  - Auditability
- They would be likely to use cryptographic methods to implement some of their protection methods

- A Poacher might be an adversary attempting to compromise a set of assets through a variety of means
- If the Poacher wishes to conceal their plans, cover their tracks and make sure they protect their stolen property they too may use cryptographic methods
  - So the Poacher becomes a Gamekeeper
  - And anyone attempting to catch them becomes a Poacher

Everything clear?

- In our field we might loosely map the roles to those of the cryptographer and the cryptanalyst
- So my introduction into this industry was as an engineer implementing cryptographic systems through hardware devices
- And that was a long time ago …



When I was a student ...

- Phone preaking had a cult following in the 70's where figures like Steve Wozniak and Steve Jobs had fun with phone networks
- The advent of the (new) PC provided a platform for software blue box development
- Some time later, organised crime took advantage of the techniques and the levels of theft of service to the telcos became significant
- The early years of computer assisted crime

Blue Box

The early years

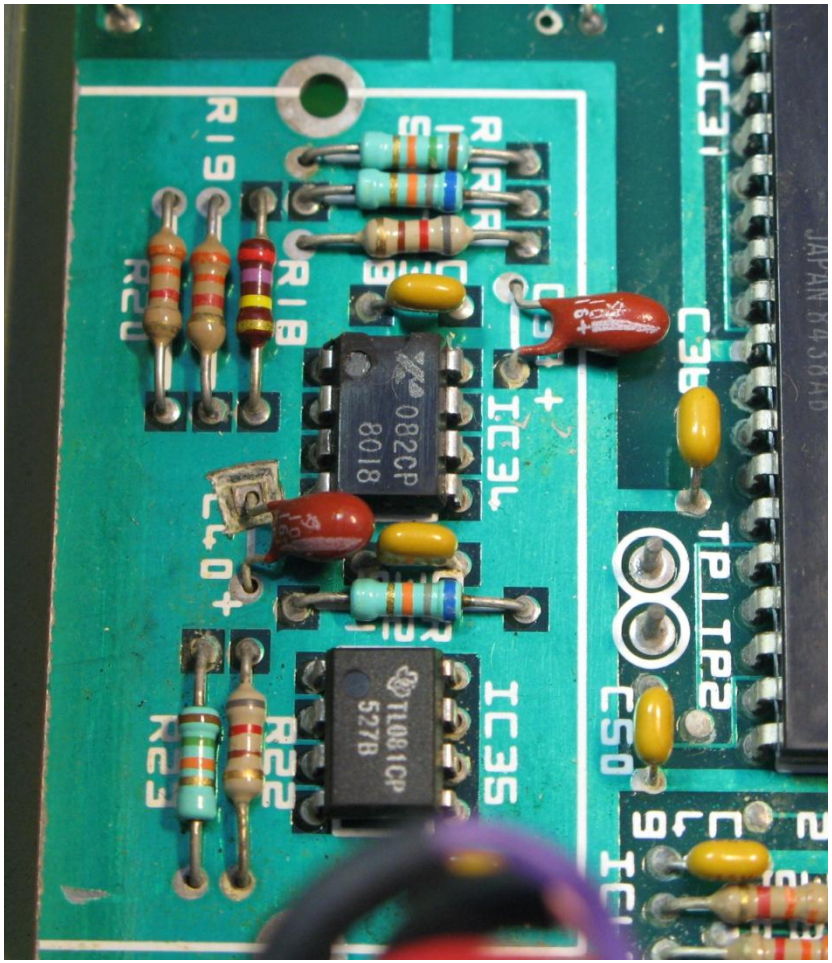
- “Hacking” was about to be popularised
- The film WarGames was released in 1983
  - It introduced “war dialling” when the main character used a dial up modem to search for computer systems
  - It highlighted the use of “default” passwords that had not been changed
  - It had a bizarre ending that with hindsight we might consider to be an early denial of service attack

The early years

- 1984 – hardware crypto design and manufacture
- Commercial clients
  - Banking and finance
  - DES
  - Emerging use of RSA for key transport
  - Data integrity mandatory but data privacy “optional”
- Little commercial use of encryption outside finance
- No real standards for hardware construction outside government
  - ~10 years before FIPS 140-1
- Z80 CPU running at 4-6MHz

Things that concerned us

- Making RSA run faster!
  - Paul Barrett, Crypto ’86 - Implementing RSA on a Standard Digital Signal Processor
- Tamper resistance
  - Andy Clark, Eurocrypt ’87 – Physical protection of cryptographic devices
  - Hardware random number generation
  - Active overwriting of RAM
  - Active alarm detection
  - Shielding etc.



Typical (perceived) threat to banking

- Interception of communications involving electronic funds transfer
  - Leading to replay attacks or manipulation of legitimate messages
- Insider attacks
  - Introduction of illegitimate messages into EFT systems
- The adversary may be technically capable, but there were few of them
- Most networks were “private”

It was a golden age

Lessons we learned …

- Crypto algorithms may be strong, (enough) but the implementation may be weak
  - Leaving key material unprotected is not good practice
- System level key management design issues can lead to compromise, e.g.
  - Same manufacturers top level (symmetric) KEK in all devices
  - Limited tamper resistance, can afford to destroy 1 or 2 devices

Lessons we learned …

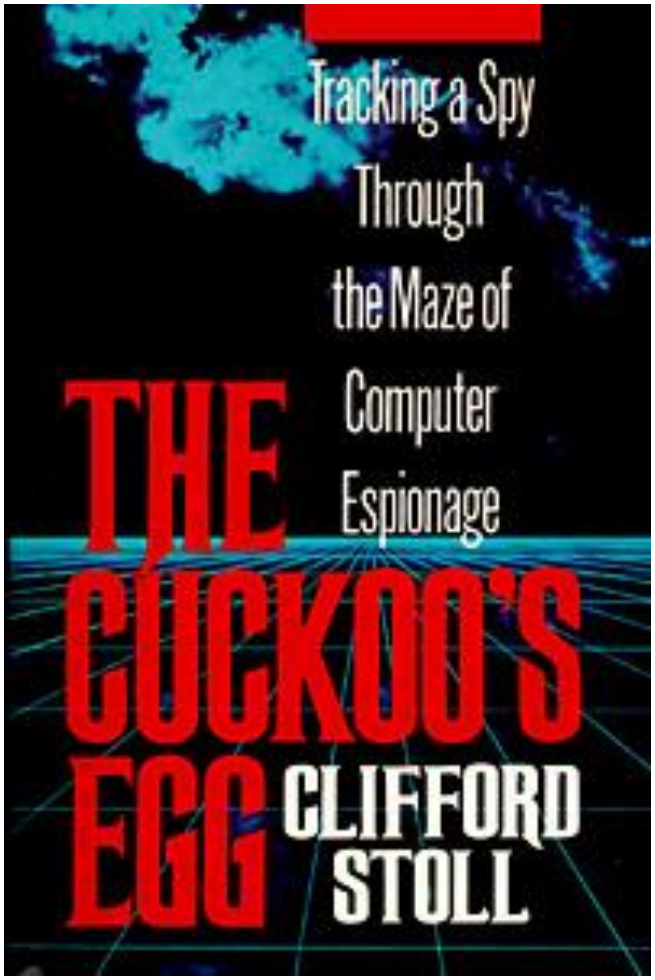
- People do not tend to be security minded – especially if it involves their creating strong passwords
- Most people prefer to use just one password for everything
- If people have to create and remember several passwords they are likely to use:
  - Familiar items as prompts or aides memoire
  - Derivations from a common source
  - Common formats

Key research/products

- Personal authentication
- Linking individuals with electronic activity
- Lots of Biometrics studies
- Token based authenticators
- “Smart brick”
- RSA accelerators
- A few people were considering the production of software based crypto

And amateurs got results

- 1986 Cliff Stoll started tracking what lay behind a 75c accounting discrepancy
- He spent ten months hunting for a computer hacker who broke into a computer at the Lawrence Berkeley National Laboratory
- It was a methodical piece of network investigation that led to the trial and conviction of Markus Hess – published 1990



The changing landscape

- 80’s
  - The Hackers Handbook
  - Computer Fraud & Abuse Act (US)
  - Christmas Tree Worm
  - Morris Worm
- 90’s
  - PGP
  - Legion of Doom – credit card and wire fraud
  - Kevin Poulsen wins a Porsche
  - DEF CON
  - www
  - MP3 sharing
  - CDC Back Orifice
- 00’s
  - ILOVEYOU
  - EU Cybercrime Treaty
  - Ddos attacks
  - Web defacement
  - Bots
  - P2P

Computer based/assisted crime

- The law was not well placed to deal specifically with computer assisted or computer based crime
- In the UK courts in 1985, *R v Gold & Schifreen*, Robert Schifreen and Stephen Gold were prosecuted under section 1 of the Forgery and Counterfeiting Act 1981, for defrauding BT by manufacturing a "false instrument“
  - they were convicted on specimen charges and fined
- They subsequently appealed their conviction successfully and that appeal was tested in 1988 when the prosecution appealed to the House of Lords who affirmed the appeal
- This led to the UK’s introduction of the Computer Misuse Act in 1990 specifically designed to deal with criminal activities associated computer systems
- This led to a need for proper computer forensic investigation

Forensics

Detica

So what's this forensics stuff then?

- The historical root of the word 'Forensics' is legal rather than technical. The word itself is derived from the Latin word 'forensis', which is derived from the Latin word for (Roman) forum, the place where legal disputes would be settled.
- Forensics as we know them today began with Alphonse Bertillon, who developed one of the first scientific systems of personal identification in Paris in the late 1800s

So what's this forensics stuff then?

- Bertillon also proved to be an inspiration for several generations of his students, one of whom, Dr. Edmond Locard, is widely cited as the founding father of modern discipline of forensic science
- Of particular importance is his "Locard Exchange Principle"
  - Every contact leaves a trace

Locard Exchange Principle

- Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value.

Locard in the digital age

- Every time we engage with a digital system we leave some trace of our activities
- The level of “digital detritus” varies from system to system and is of particular interest to information forensics investigators
  - Assuming we can get it
- It must be properly collected, preserved and interpreted to be suitable for presentation as evidence in court proceedings

Investigation phases

- **Identification**
  - Of the subject of the investigation, normally through intelligence gathering
- **Preservation**
  - Isolation, securing and preserving digital evidence
- **Collection**
  - Either the making of forensic copies of the digital evidence, or:
  - Live capture of digital evidence while equipment is still operating
- **Examination**
  - Focused searching using a variety of dedicated tools
- **Analysis**
  - Establishing the relevance of each item of evidence and determining linkages between items to build as complete a picture as possible
- **Presentation**
  - Providing a full expert report on the findings of the investigation and presenting it in the appropriate forum – typically a tribunal or court
  - In a way that can be understood
- **Decision**
  - Made by people independent of the case who decide based on the weight of the evidence presented to them

Identification

Detica

Data Driven Investigation/Identification

- Forensics professionals can often assist by helping identify critical data that may be relied on in court and advising on how it may be preserved and collected
- For example, the scenario that follows describes mechanisms to support the identification of key individuals who are believed be prolific “seeders” of peer-to-peer file sharing networks and are sharing movie copyright material illegally

Defining entities and documents

- BitTorrent tracker entity

- Person entity

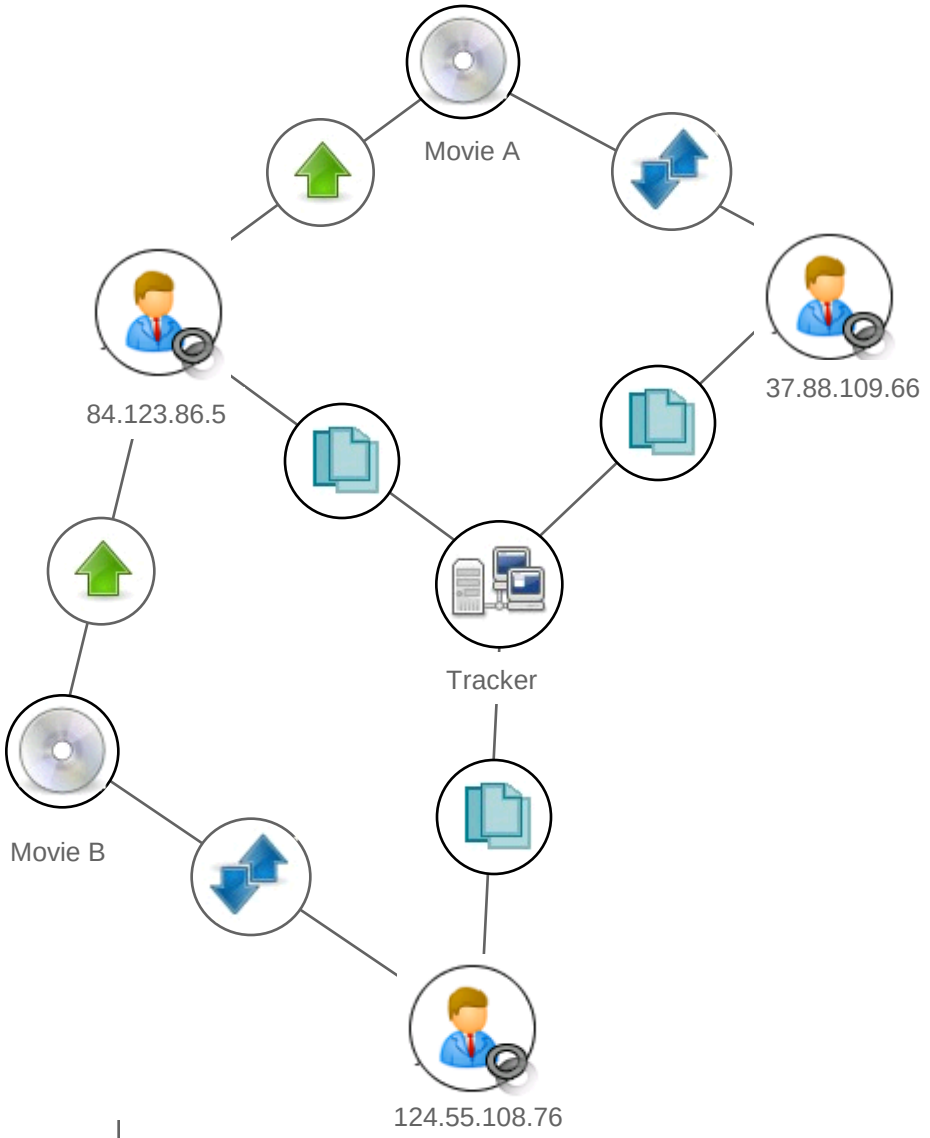
- Movie (media) entity

- Seeder document (linking a person seeding a movie)

- Download document (linking a person downloading a movie)

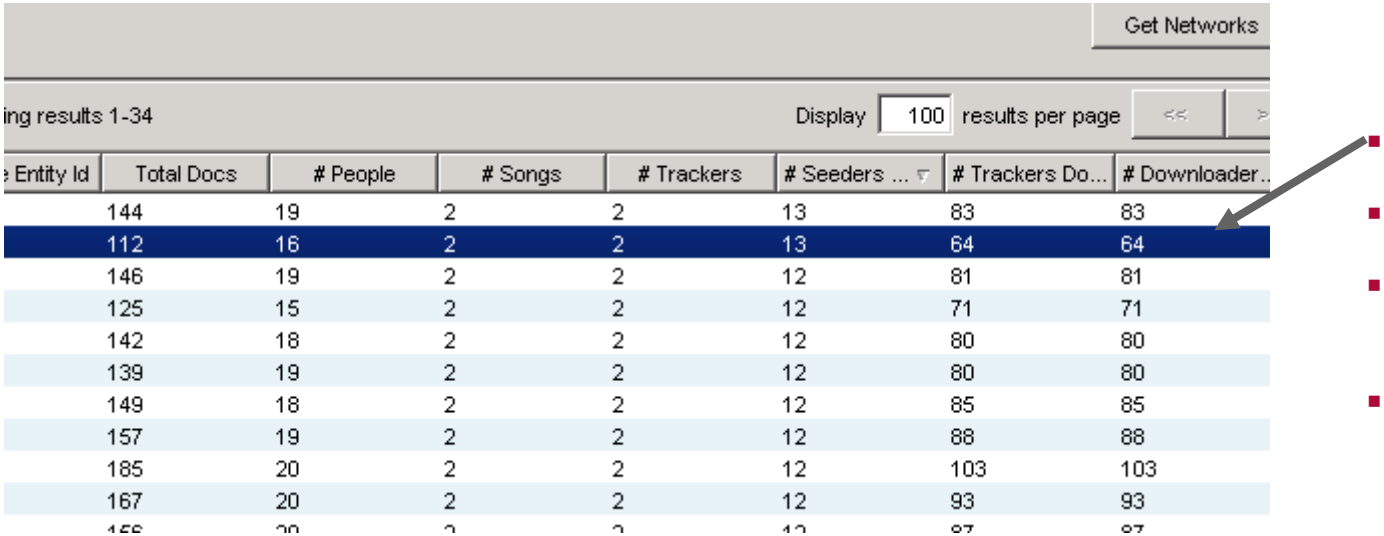
- Tracker document (indicating an interaction with a tracker)

Overview of the network visualisation



- People are linked to trackers and movie(s) that they have downloaded. The movies that a person downloads are visualised independently of the tracker
  - Information about which movies a tracker is responsible for is not visualised.
- Seeder / Downloader information is shown as links (documents) between entities

Network Dossier View 1



Get Networks

ing results 1-34 Display 100 results per page << >

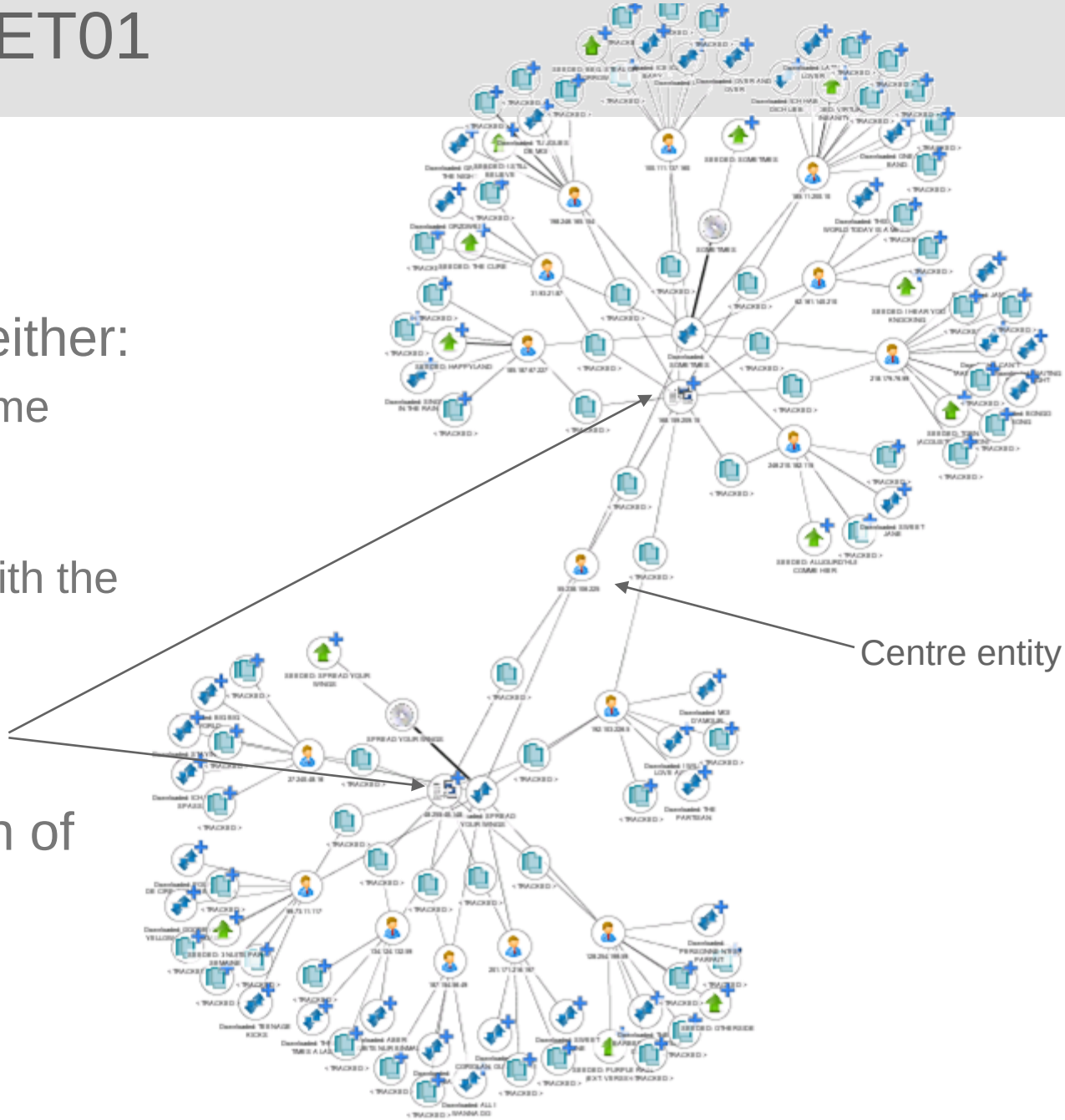
Entity Id	Total Docs	# People	# Songs	# Trackers	# Seeders ...	# Trackers Do...	# Downloader...
	144	19	2	2	13	83	83
	112	16	2	2	13	64	64
	146	19	2	2	12	81	81
	125	15	2	2	12	71	71
	142	18	2	2	12	80	80
	139	19	2	2	12	80	80
	149	18	2	2	12	85	85
	157	19	2	2	12	88	88
	185	20	2	2	12	103	103
	167	20	2	2	12	93	93

- Total Docs: small
- Seeder Docs: high
- Number of Trackers: small
- Investigate this network (NET01)

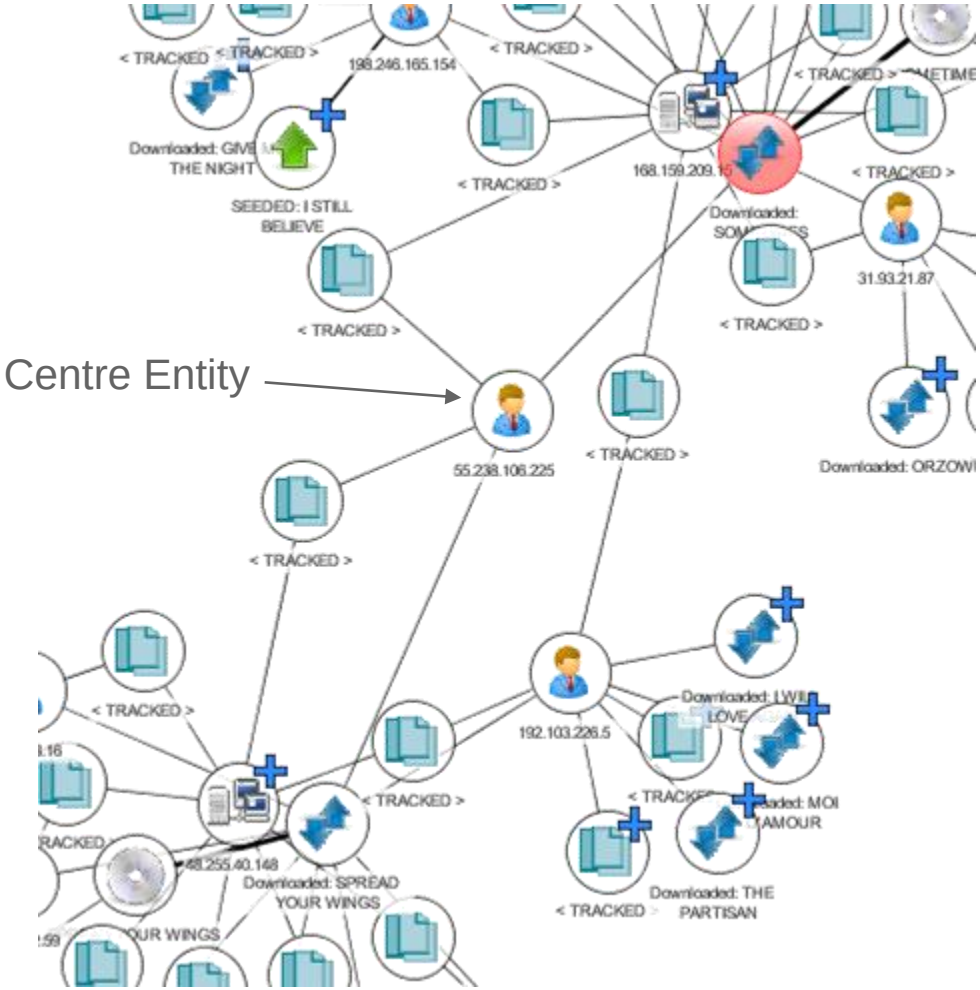
- Information in dossier view helps to identify networks of interest
- Networks with a high number of ‘Total Docs’ may be indicative of prolific behaviour
- Networks with a large number of Seeder documents relative to the number of people are indicative of prolific uploaders

Investigate NET01

- All the person entities are connected by either:
  - using the same tracker
  - having an interaction with the same movie
- Two trackers
- High proportion of seeders

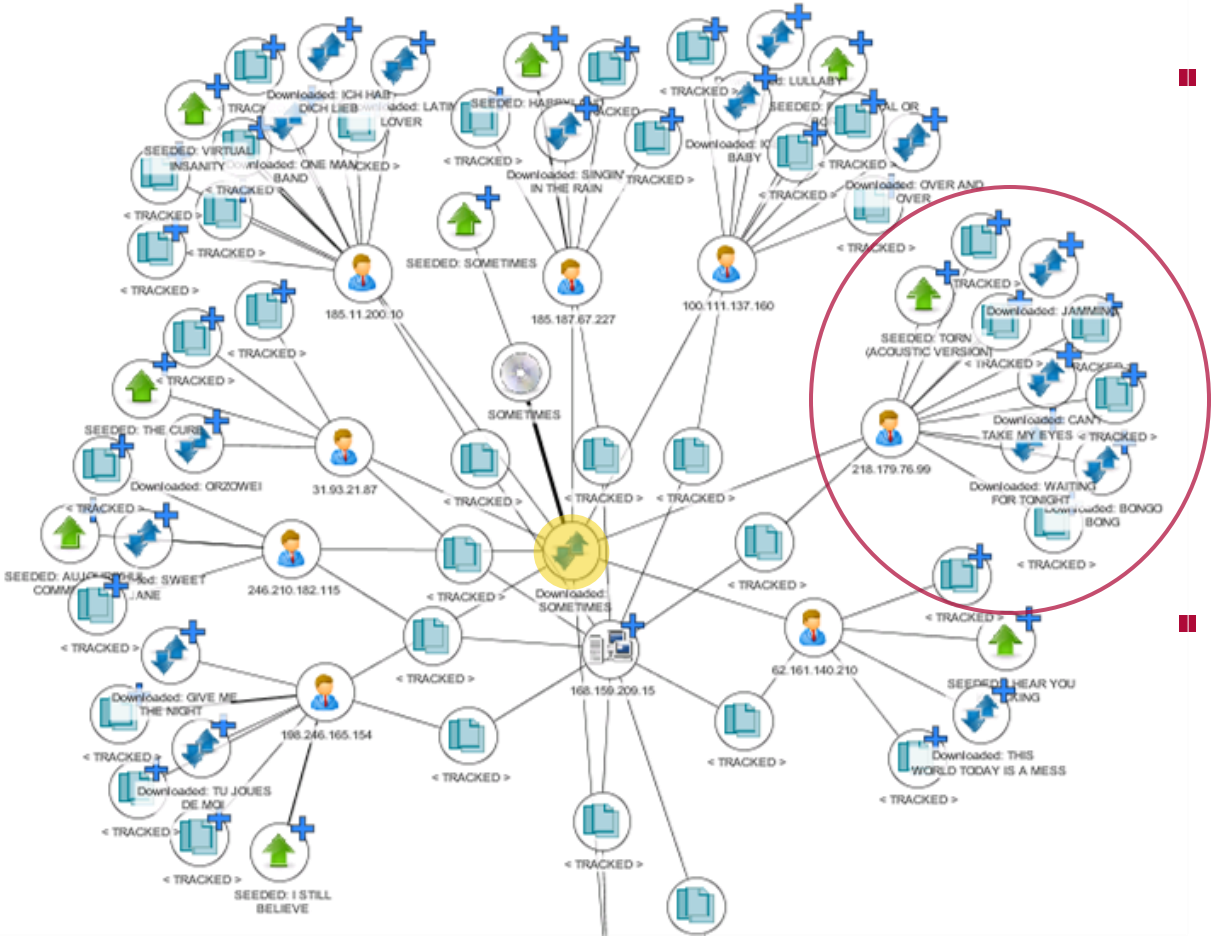


Investigation of NET01: central person



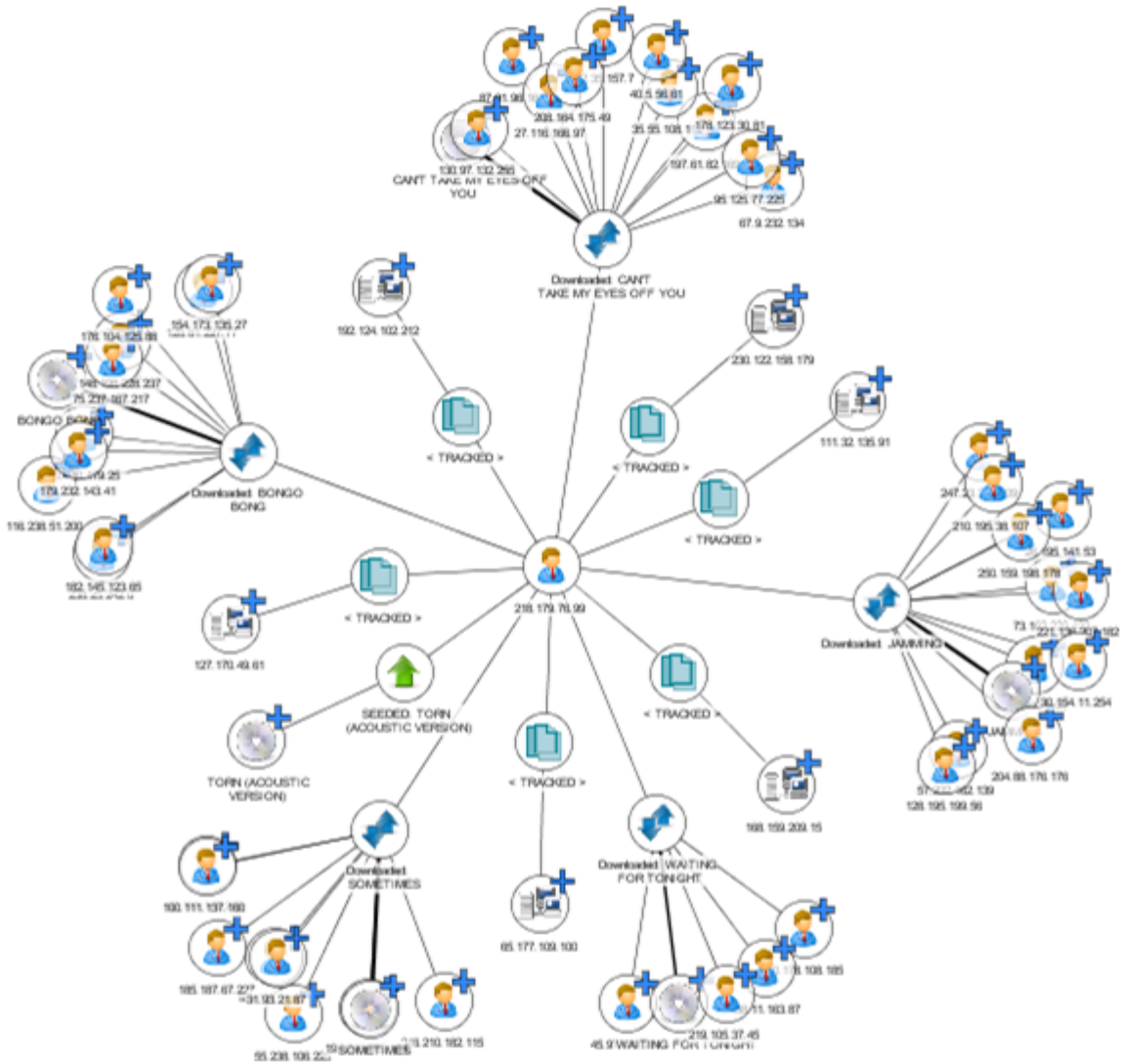
- Centre entity downloaded two movies using two trackers
  - NOT prolific behaviour, entity not of interest
- Investigate activity around trackers instead

Investigation of NET01: tracker



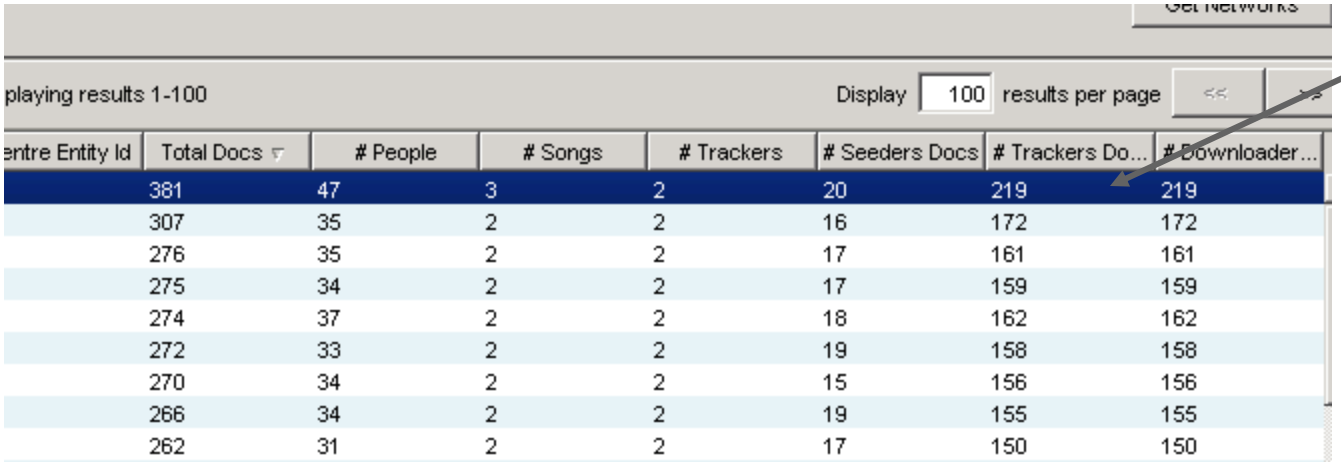
- Active tracker
- Many people downloaded the highlighted movie. However, cross-linking of the same movies between different people doesn't occur.
  - Probably a public tracker
- Some individuals are prolific (circled red – 218.xxx.xx.xx > open in new dossier)

Investigation of NET01: person [218.xxx.xx.xx]



- Downloaded 5 movies
- Seeded 1 movie
- Used 6 trackers
- One of the first downloaders for five movies
- Seeds other networks?

Network Dossier View 2



playing results 1-100 Display 100 results per page

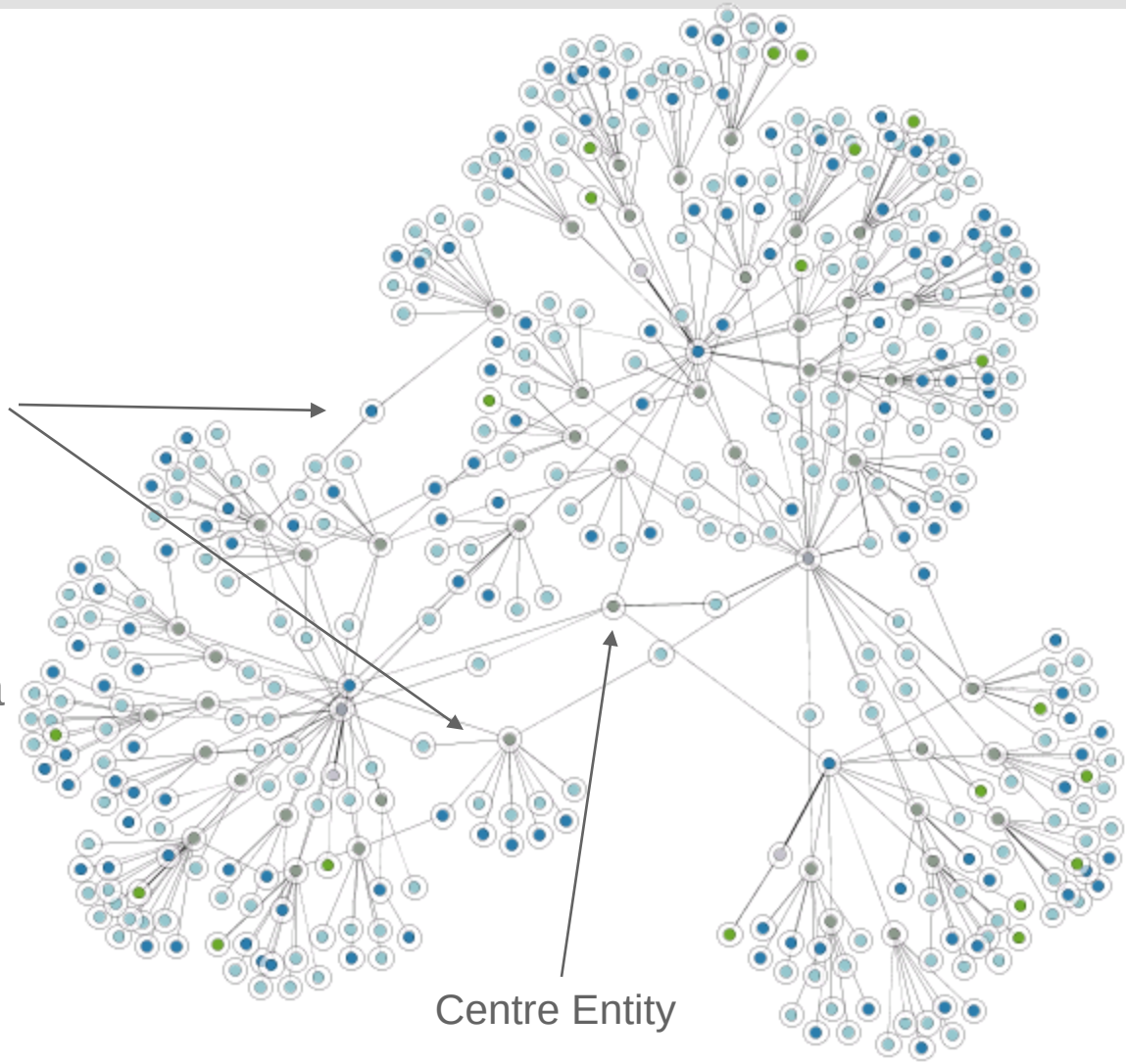
entre Entity Id	Total Docs	# People	# Songs	# Trackers	# Seeders Docs	# Trackers Do...	# Downloader...
	381	47	3	2	20	219	219
	307	35	2	2	16	172	172
	276	35	2	2	17	161	161
	275	34	2	2	17	159	159
	274	37	2	2	18	162	162
	272	33	2	2	19	158	158
	270	34	2	2	15	156	156
	266	34	2	2	19	155	155
	262	31	2	2	17	150	150

- Total Docs: high
- Number of Trackers: small
- Investigate this Network (NET02)

- Choose a network with a large number of documents but a small number of trackers
- This would indicate a higher proportion of cross-linking (people who regularly use a tracker and download the same movies)

Investigate NET02

- More chaotic schema. Central person downloaded 3 movies
- Ring patterns can be seen indicating connections between people
- Remove tracker documents to reveal a less cluttered picture

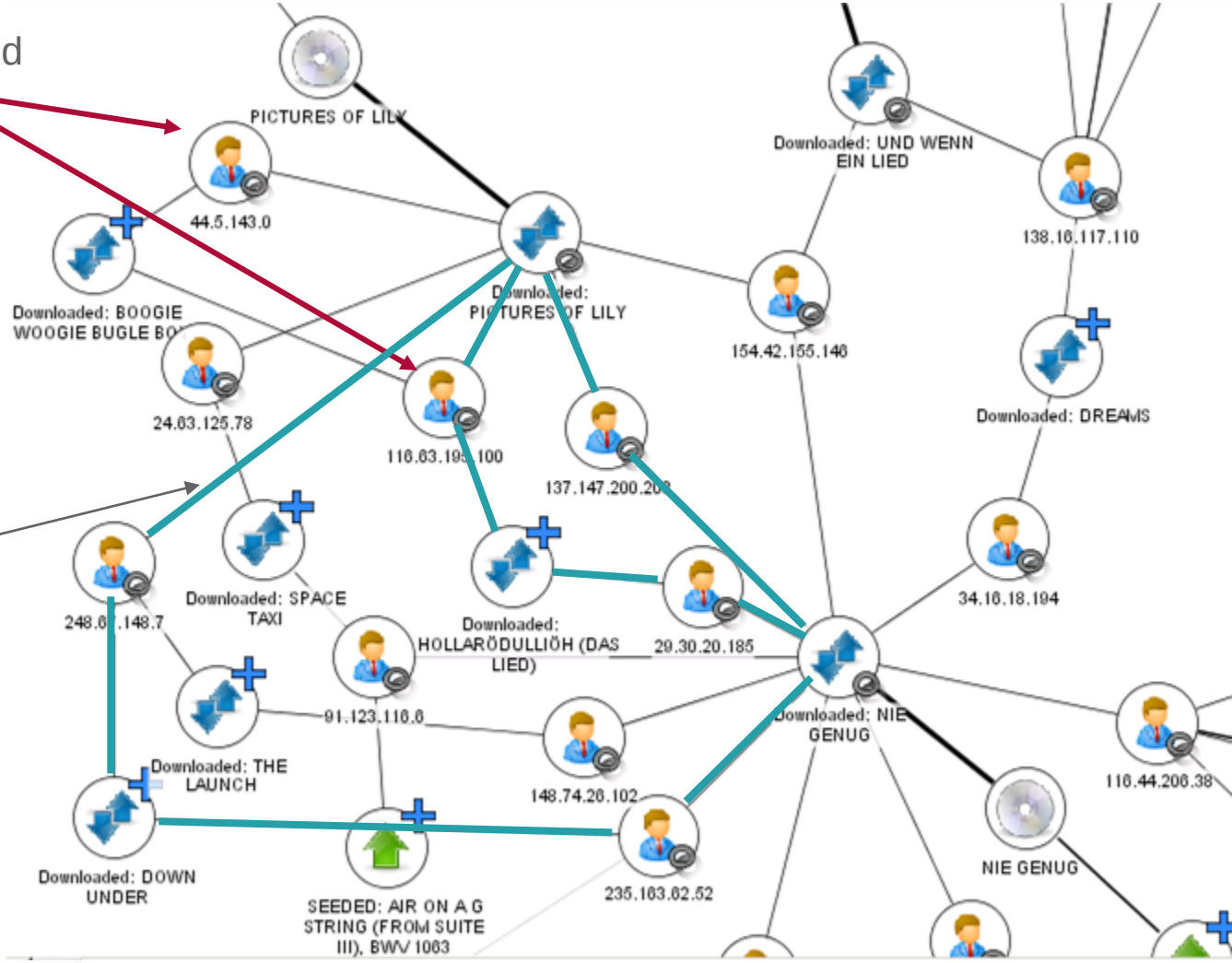


Investigation of NET02: filtered tracker documents

These two people downloaded the same two movies

Not all the people in this view have downloaded the same movie; but they can be linked back to each other through the movies that they have downloaded (highlighted by the BLUE ring)

Since there are only two trackers in this network, this could be indicative of a private tracker system



- **This Network was heavily filtered to show only links between people who all been connected to each other through their download patterns**

Example data of evidential value

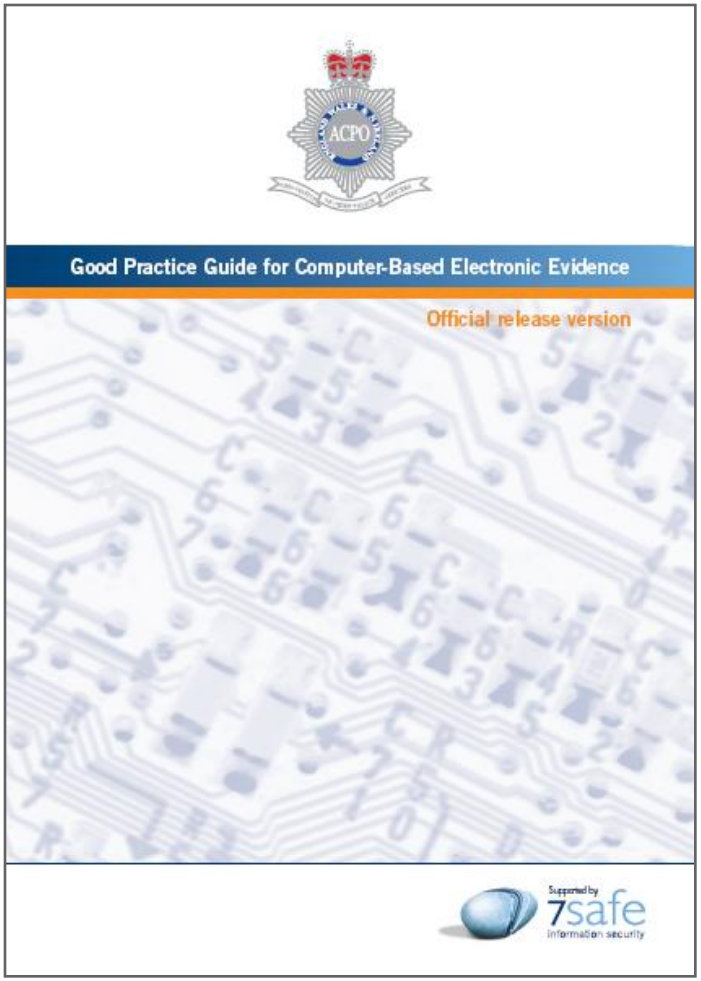
- Network addresses
- Dates and times of network access
- Traffic protocols/ports in use
- Client software variants in use
- File names and types – both at the individual end points and at the tracker sites
- Hashes of shared files (from tracker and download client)

Preservation

Detica

Preservation

- The proper preservation of computer based evidence is one area where “good practice” has been established
- Generally the principles established in documents like the ACPO Guidelines are accepted by law enforcement in many jurisdictions



Preservation

- *With ever-increasing numbers of digital seizures and constantly developing technology, these guidelines are essential to informing the collection and preservation of this most fragile form of evidence. Previous versions of this document have set vital standards for law enforcement and corporate investigators alike, a position I would like to see continue with this and future revisions of the document. The continuing fast paced evolution of both hardware and software makes it essential to develop best practice in line with the technical challenges which we face when capturing digital evidence, in order to prevent its contamination or loss. This latest revision has been not only timely, but also essential, in order that our practices are fit for purpose when considering recent and upcoming advances in every day technology.*
- Sue Wilkinson. Commander, Metropolitan Police Service, Chair of the ACPO E-Crime Working Group

Contents of ACPO Guidelines

- The principles of computer-based electronic evidence
- Overview of computer-based electronic investigations
- Crime scenes
- Home networks & wireless technology
- Network forensics & volatile data
- Investigating personnel
- Evidence recovery
- Welfare in the workplace
- Control of paedophile images
- External consulting witnesses & forensic contractors
- Disclosure
- Retrieval of video & CCTV evidence
- Guide for mobile phone seizure & examination
- Initial contact with victims: suggested questions
- Glossary and explanation of terms
- Legislation

Already taking account of the use of crypto

be lost by removing the power supply e.g. running processes and information about the state of network ports at that time. Ensure that for actions performed, changes made to the system are understood and recorded. See section on Network forensics and volatile data.

- Consider advice from the owner/user of the computer but make sure this information is treated with caution.
- Allow any printers to finish printing.
- If no specialist advice is available, remove the power supply from the back of the computer without closing down any programs. When removing the power supply cable, always remove the end attached to the computer and not that attached to the socket. This will avoid any data being written to the hard drive if an uninterruptible power protection device is fitted.
- Remove all other connection cables leading from the computer to other wall or floor sockets or devices.
- Routers.
- Digital cameras.
- Floppy disks.
- Back up tapes.
- Jaz/Zip cartridges.
- CDs.
- DVDs.
- PCMCIA cards (see glossary).
- Memory sticks, memory cards and all USB/firewire connected devices.
- N.B. Always label the bags containing these items, not the items themselves.

If the power is removed from a running system, any evidence stored in encrypted volumes will be lost, unless the relevant key is obtained. Also, note that potentially valuable live data could be lost, leading to damage claims, e.g. corporate data.

ACPO Principles

1. No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court

2. In circumstances where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions

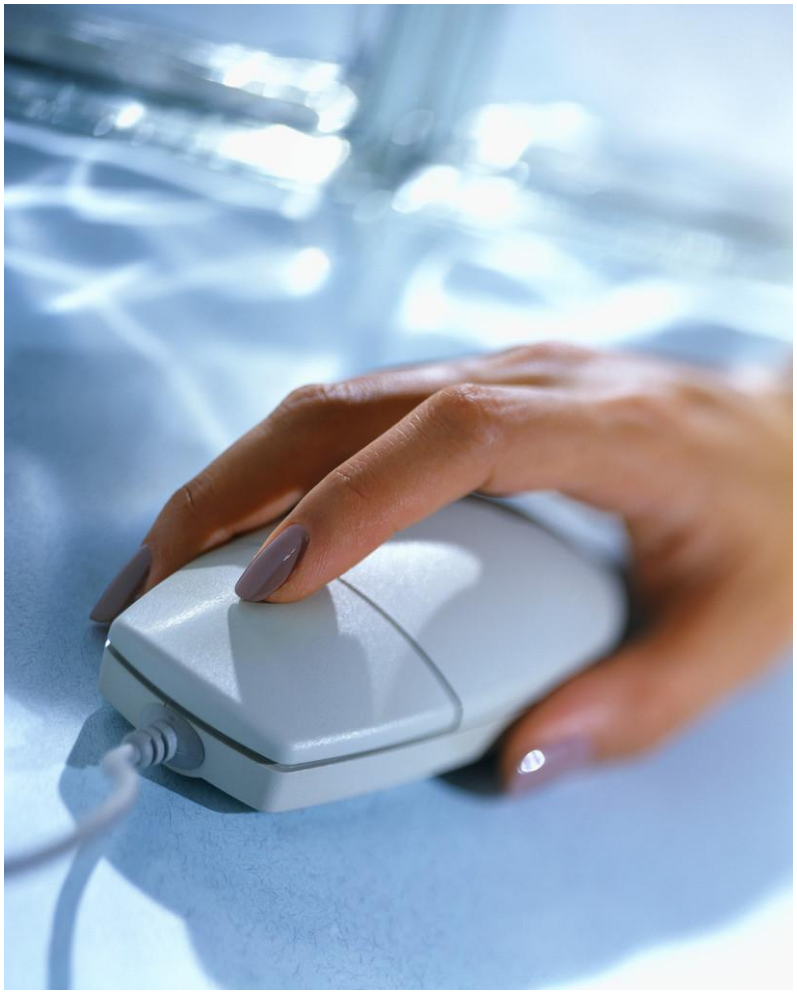
ACPO Principles

3. An audit trail or other record of all processes applied to computer-based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result

4. The person in charge of the investigation (the case officer) has overall responsibility for ensuring that the law and these principles are adhered to

Preservation

- Sometimes the simplest things can make sure that you preserve evidence
  - Digital cameras
  - “mouse duty”



Collection

Detica

The elephant in the room

- “We are approaching a world of cryptographic abundance” (Berson)
  - IACR distinguished lecture at AsiaCrypt in Kyoto, 2000 entitled “Cryptography everywhere”
  - “Cryptographic Abundance” in the MIT Technology Review January/February 2002
- It makes things harder … but not always impossible

Collection

- Once upon a time it was easy ...
- Targets were typically hard drives and all you needed was a good write-blocker
  - SCSI
  - IDE (PATA)
  - SATA

Collection

- Now data storage is prolific, and not always easy to locate and process ...
- In the slides that follow, consider
  - Is this a computer in its own right? (Advice to follow)
  - Could there be data of evidential value?
  - Can I collect it in an evidentially sound way?

What is a computer?

- A machine that manipulates data according to a list of instructions (Wikipedia)
- A machine comprising as minimum Arithmetic Logic Unit, Memory, Input and output channels (R. v. Squance, 1996)

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

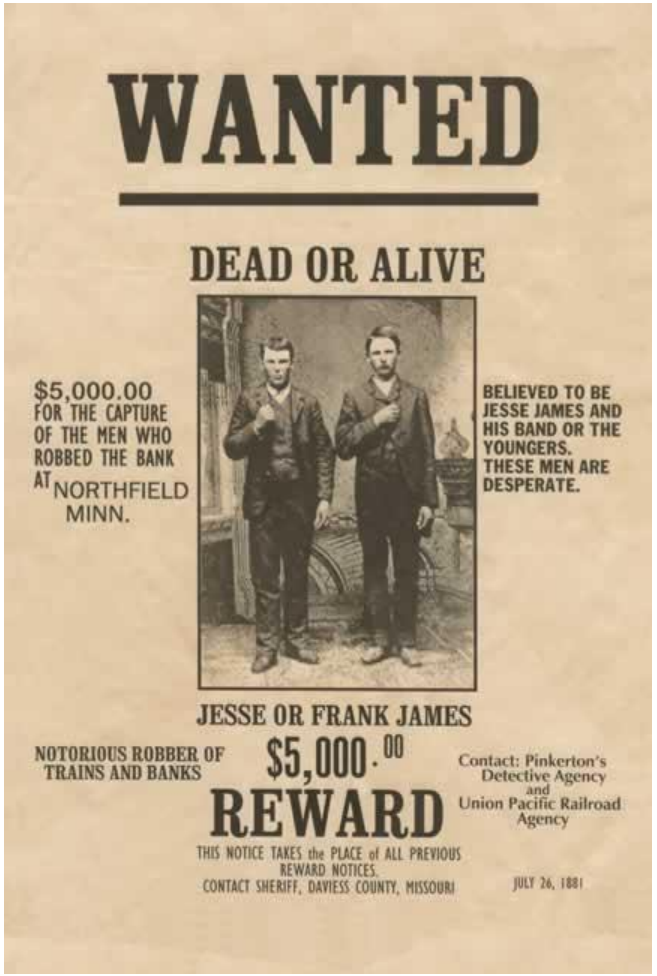
What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

What is it? / Can we get Evidence?

Collection

- Early decision needed on whether or not collection needs to be done on live machines
  - Data protected by strong crypto
  - Need to prove linkage between an individual and a remote machine
- It's challenging but becoming more common



Static data collection

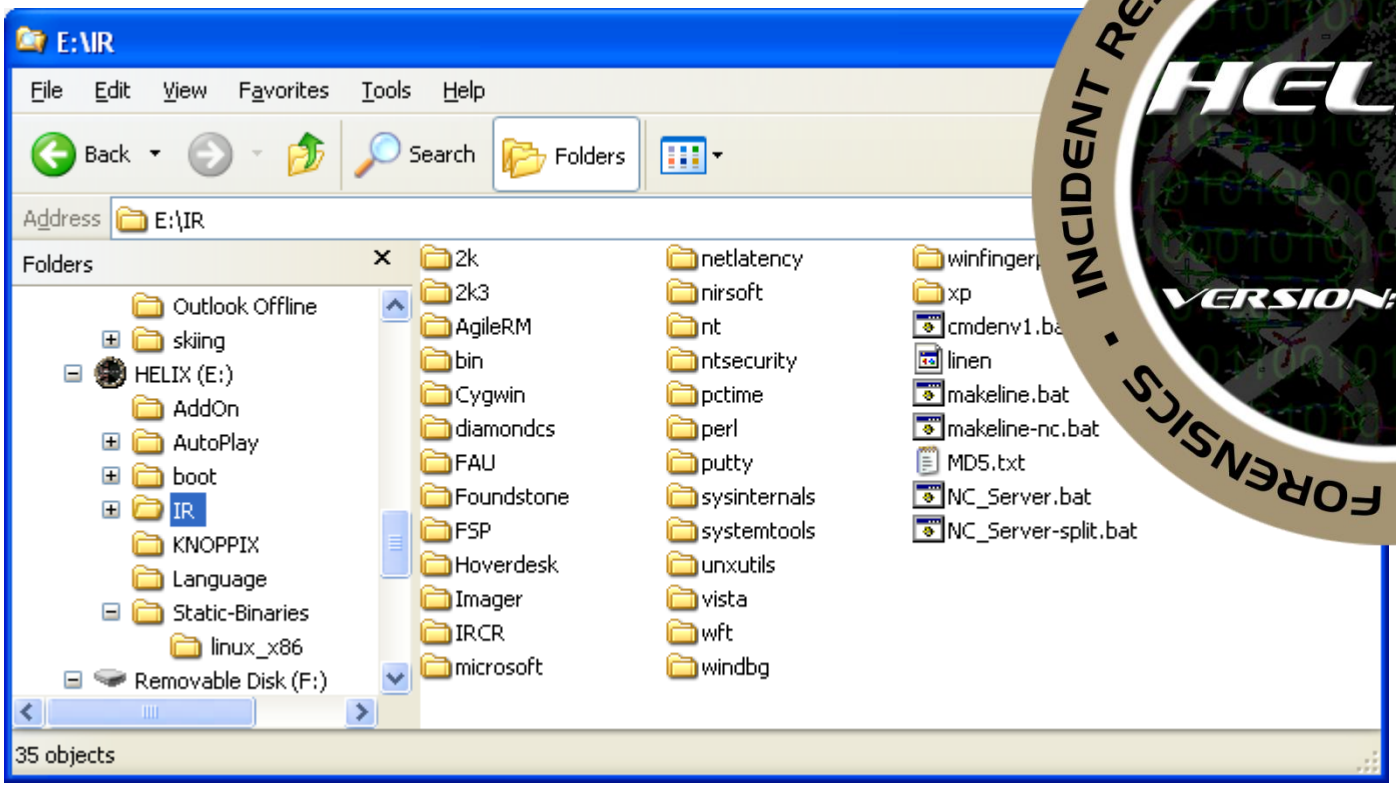
- Use accredited forensic tools and systems
- Every file collected is stored together with a hash of its contents
  - To enable auditing that the file has not been changed subsequently and evidence altered
  - Allows elimination of known files (OS etc.) from investigation set
- Hash calculated across the whole acquisition
  - To enable auditing that evidence has not been added
- Most forensic practitioners acquire using two separate tools and cross check results

Live data challenges

- Need to collect data from the target but we must minimise use of target resources
  - “no change”
- Need to capture volatile data to assist in reconstruction of what was running, keys etc.
- Best to use simple but effective tools
  - NetCat the Swiss Army Knife of Networking tools (minimum footprint to get a channel)
  - DD to capture data ranging from memory to full disk image

Live forensics tools

- Limited success ...



Examination & Analysis

Detica

What do we have to look for?

- Information forensic evidence is rarely the only evidence to be relied upon in a case
- The ideal would be to identify a “smoking gun” piece of evidence from digital storage (and that does happen) for example:
  - Email trails
  - Document metadata
  - Chat logs
  - File transfer logs
- Generally, we need to link individuals with specific events

It’s not all about forensic tools

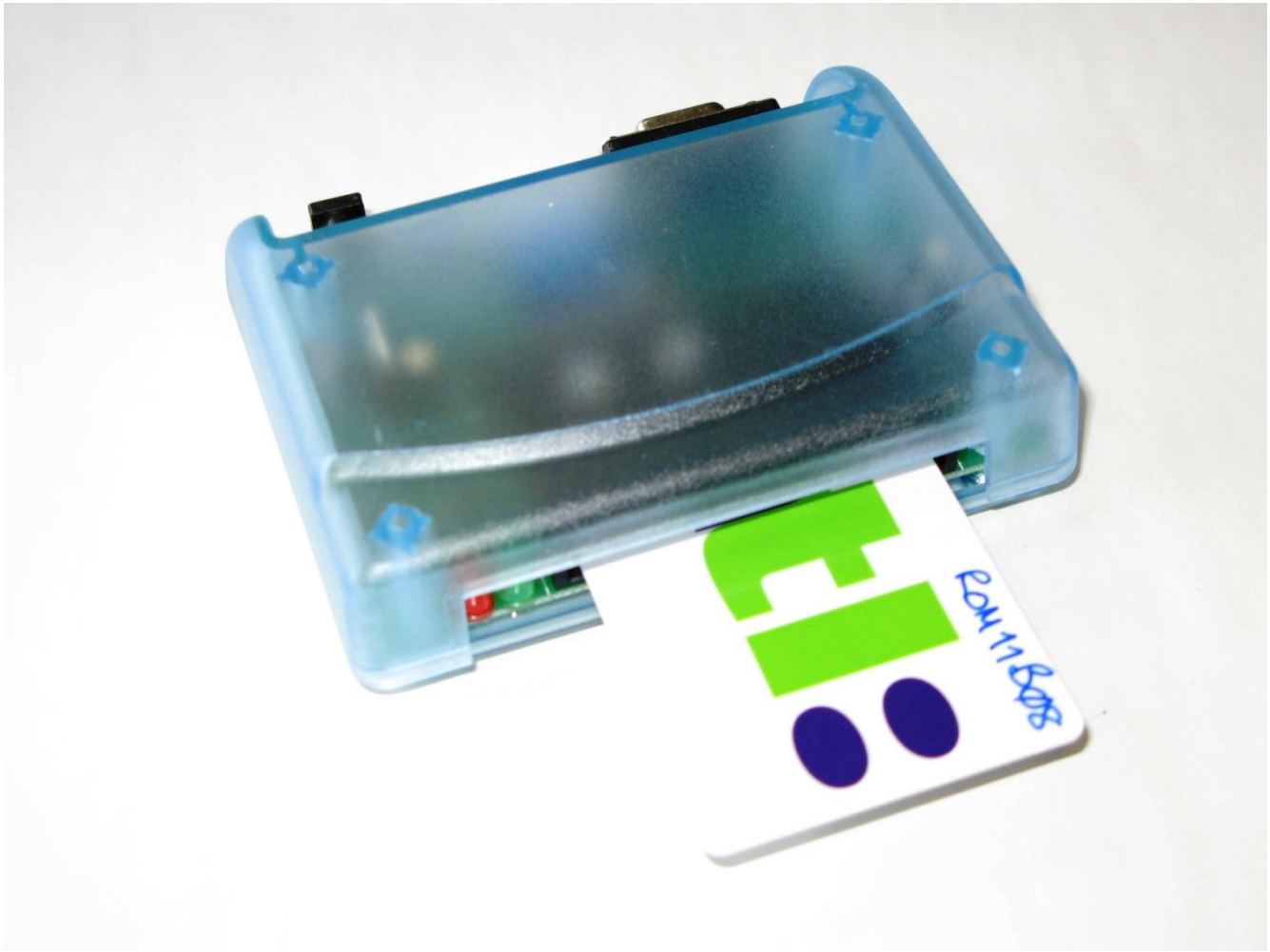
- Tools can help with the formatting of complex data into a way that is easy to understand
- They are frequently optimised to provide fast searching of large volumes of data
- They are not a silver bullet alternative to detailed examination of low-level data where necessary

There are several barriers to examination

- The volumes of data being recovered can be overwhelming
- Weak crypto still needs recovery
- Linking individuals to actions at a particular time can be difficult
  - Trusted time is easy to say and harder to achieve

You need (access to) a range of skills

You need (access to) a range of skills



And a lot of time

- You will have to eliminate a substantial amount of irrelevant data
- What's left will take time to analyse and present in a format that a jury of non-technical people can understand!

A real case study or three ...

Detica

And finally ...

Detica

Lessons in 2008

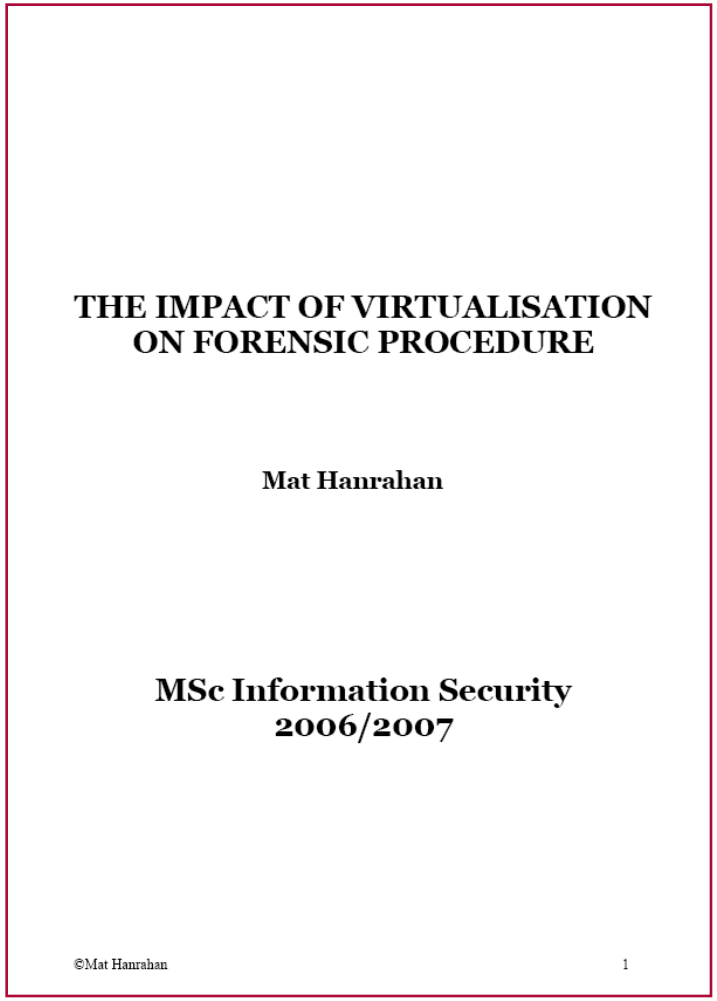
- Crypto algorithms may be strong, (enough) but the implementation may be weak
- System level key management design issues can lead to compromise
- People do not tend to be security minded – especially if it involves their creating strong passwords
- Most people prefer to use just one password for everything

Lessons in 2008

- If people have to create and remember several passwords they are likely to use:
  - Familiar items as prompts or aides memoire
  - Derivations from a common source
  - Common formats
  - Post-It notes

Credits and thanks

- Thanks to Mat Hanrahan for allowing me to use and quote from his MSc thesis (RHUL 2007) on the history of forensics
- Thanks to the Program Committee of Eurocrypt 2008 for inviting me
- And thanks to you for listening
  - And for making my job so much harder year by year



THE IMPACT OF VIRTUALISATION ON FORENSIC PROCEDURE

Mat Hanrahan

MSc Information Security 2006/2007

©Mat Hanrahan 1

Questions