First Principles

Definitions
First Principles
The Growth of Digital Forensics

Dr Harjinder Singh Lallie
Director of the Accredited Centre of Excellence in Cyber Security Education
Discipline group leader (cyber security)
HL@warwick.ac.uk

1

1

Definitions

Digital forensics, evidence, and admissibility

2

Definition: Digital Forensics

- The systematic application of scientific methods to investigate digital devices and reveal and present admissible evidence relating to incidents and/or events
- From: *forensic/fora* – the courts, the forum
- The term encompasses computer forensics, computational forensics, network forensics, cyber forensics, e-forensics, eDiscovery. However, network forensics and eDiscovery have very specific applications
- Other branches include: Forensic Psychology/Psychiatry, Forensic Anthropology, Forensic Pathology, Forensic Chemistry/Toxicology, Forensic Engineering, Forensic Accounting

Dr. Harjinder Singh Lallie 3

3

Definition: Digital Forensics

Although you might never investigate a criminal case, it is important that as a cyber security practitioner, you are fully aware of how cases should be investigated

Dr. Harjinder Singh Lallie 4

4

Definition: Digital Evidence

- The outcome of an investigation is a set of evidence that supports one or more assertions
- Evidence is only evidence if it proves a given conclusion, otherwise it is only 'data' or artefacts
- "…information stored or transmitted in binary form that may be relied on in court"[1] "…information and data of value to an investigation that is stored on, received or transmitted by an electronic device. This evidence can be acquired when electronic devices are seized and secured for examination"[2] "…any probative information stored or transmitted in digital form that a party to a court case may use at trial"[3]

[1] National Institute of Justice, 2016 | [2] National Forensic Science Technology Center, 2016 | [3] Wikipedia

Definition: Digital Evidence

- The outcome of an investigation is a set of evidence that supports one or more assertions
- Evidence is only evidence if it proves a given con
only 'data' or artefacts
- "…information stored or transmitted in binary fo
in court"[1] "…information and data of value to an
on, received or transmitted by an electronic dev
acquired when electronic devices are seized and
examination"[2] "…any probative information stored or transmitted in digital form that a party to a court case may use at trial"[3]

A challenge faced by digital forensics students is to understand the difference between 'evidence of' and just 'useful data'

[1] National Institute of Justice, 2016 | [2] National Forensic Science Technology Center, 2016 | [3] Wikipedia

Digital Forensics and Forensic Science

Unfortunately, digital forensics is unlike other forensic sciences such as DNA analysis or chemical analysis, where the result produced by an analysis tool is a conclusion in and of itself. Tools used for digital analysis are more similar to the use of a chemical compound to reveal latent bloodstains at a physical crime scene; they make evidence visible but do not interpret how it was created or how the evidence relates to the surrounding environment. Consequently, digital forensic analysis has two distinct processes that must be able to satisfy Daubert; the software processes that render data for viewing, and the interpretive process performed by the analyst. Even more significantly, the interpretive process must also fulfill the second prong of Rule 702; "the expert must apply the principles and methods reliably to the facts of the case." Daubert/ 702 does not allow testimony by an expert to address the reliability issue as easily as applying Rule 901, which is why a structured model for the interpretive process is important

Andrew, M.W., 2007, April. Defining a process model for forensic analysis of digital devices and storage media. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)* (pp. 16-30). IEEE.

7

Types of Evidence

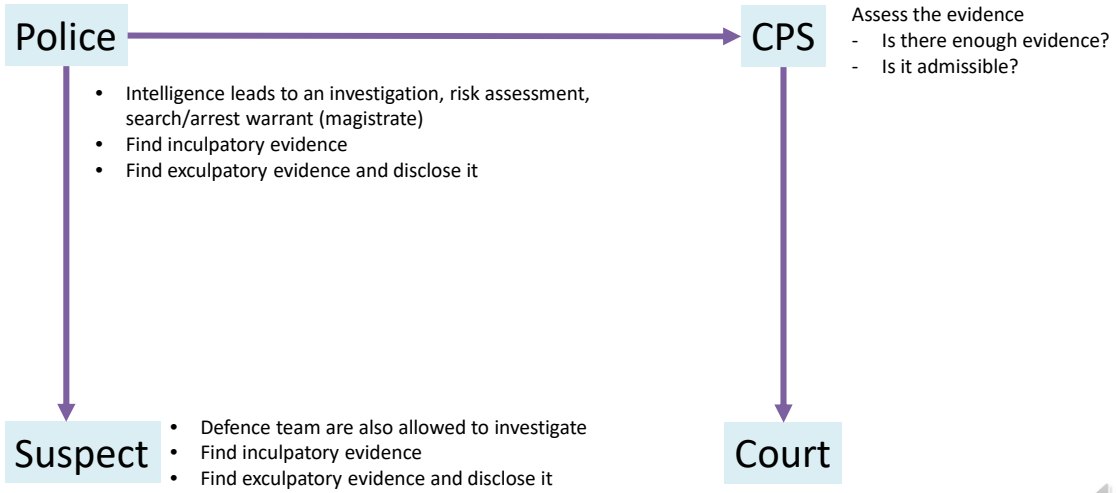
Inculpatory *Supports a given theory*	Employee is accused of harassment (sending abusive/ harassing emails to a colleague). Case relies on 13 emails sent from the machine of the accused (evidenced by MAC addresses coupled with static IP addresses and corroborated with email logs)
Exculpatory *Contradicts a given theory, could introduce reasonable doubt*[1]	In the same case however, the accused claims that he was on annual leave during the time that the emails were sent, somebody else must have logged onto the machine and sent the emails. This is exculpatory evidence that the individual was not at the machine when the emails were sent.
Direct Evidence *Supports the truth of an assertion directly, without an intervening inference*	Witness(es) saw employee type out the email and press the send button.
Circumstantial *Shows circumstances that logically lead to a conclusion of fact*	An inference is required to connect it to a conclusion of fact, judgements can be based entirely on circumstantial evidence. Witness(es) heard suspect say he hates victim.

8

Legal overview of an investigation

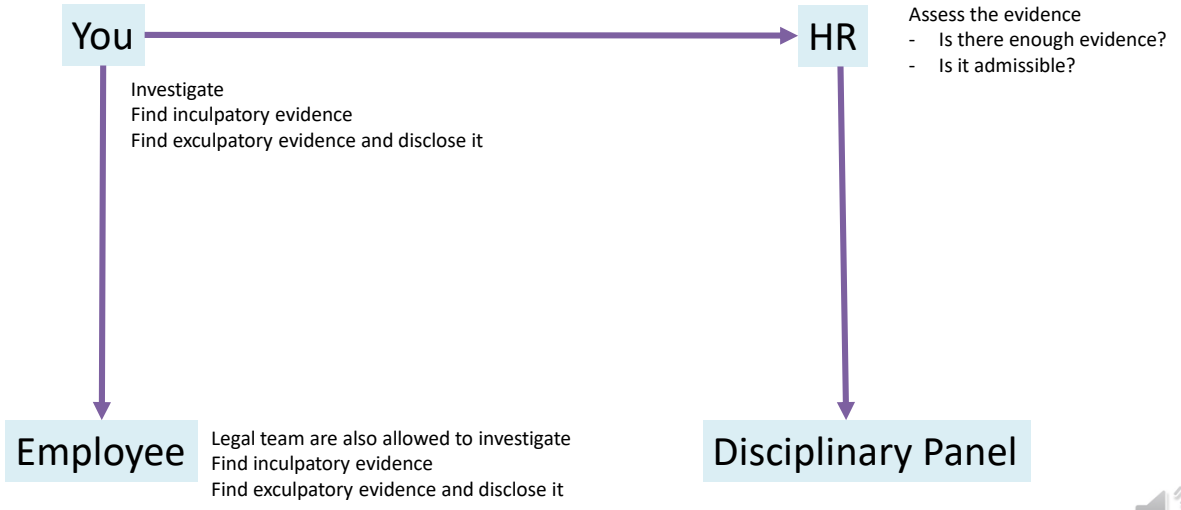
9

Criminal incident



10

Corporate incident



11

Exculpatory evidence

12

Numerous cases where the failure to reveal exculpatory evidence has led to case dismissal, miscarriage of injustice, and associated distress for the defendant/others

CPS and police 'routinely failing' to disclose evidence

Attorney general calls for zero tolerance of any failures to hand over relevant material

Geoffrey Cox: 'For too long, disclosure has been seen as an administrative add-on rather than fundamental pillar of our justice system.' Photograph: Dinendra Haria/Rex/Shutterstock

Prosecutors and police are routinely failing in their duties to disclose crucial evidence leading to cases being pursued that should have been dropped, a review by the attorney general has found.

The report, presented by Geoffrey Cox, calls for a culture of zero tolerance in the Crown Prosecution Service (CPS) and police forces of any failures to hand over relevant material obtained during investigations.

13

The Metropolitan Police and the Crown Prosecution Service have apologised to Liam Allan after a rape case against him collapsed following the discovery of crucial text message evidence that had not been disclosed to his legal team.

The 22-year-old was cleared after lawyers were handed a mobile phone download containing previously undisclosed text messages which cast doubt on the claim the sex was non-consensual.

14

"a diary which supported his case was uncovered … Judge Jonathan Black heard the diary "tips the balance" in favour of the defendant...
Prosecutor Sarah Lindop said it contained previously unseen evidence which was "not of assistance to the prosecution".

15

Is it criminal to withhold exculpatory evidence?

Not if it was negligence. Deliberately withholding can lead to reputational/career damage

As an expert witness your duty to the Court comes above your duty to any of the parties, you cannot withhold evidence of any description and breaching that can lead to contempt of court proceedings

16

Further Reading

Home > Literature > Disclosure Failures in Criminal Trials

Date updated: Thursday 13th May 2021

More than 900 criminal cases were dropped in England and Wales last year due to a failure by police or prosecutors to disclose evidence, it has been reported. According to the BBC, this marked a 70% increase in the number of collapsed cases over the course of two years. The corporation said figures obtained under freedom of information revealed 916 people had charges dropped last year due to a failure to disclose evidence – up from 537 in 2014-15 and 732 the following year.

Most of us would expect the police to want to catch the criminals. The people that have done it. The guilty ones. And that is exactly what most police officers, perhaps understandably, think is their job as well. But you and they would be wrong, profoundly wrong, and it is this basic, fundamental error that lies at the heart of the problem.

Because who decides who's guilty? The job of the police is to investigate whether or by whom an offence has been committed. They have a legal duty to investigate all reasonable lines of enquiry, whether they point towards the guilt or innocence of a particular suspect. It sounds simple, but if you are a suspect in a criminal case you need to understand that this isn't how it works. This isn't a story of a few rogue cops gone bad, or a crumbling, underfunded criminal justice system overwhelmed by national austerity (though both get blamed daily in courts and the press to cover a wider, more difficult truth). This is a story of a state funded system designed with political ends in mind to convict those accused of crime, because once a person is charged they must be guilty, if only the Crown can prove it. Inconvenient evidence that would undermine a prosecution or assist a suspect doesn't achieve either of those aims, so it doesn't have

Further reading: Disclosure Failures in Criminal Trials (Stone King): https://www.stoneking.co.uk/literature/e-bulletins/disclosure-failures-in-criminal-trials

17

‘evidence to the contrary’ is important in your thesis

“A more convincing account of the non-supported hypotheses could be provided here. Why was effort expectancy a non-significant predictor of intention to use in this population?”

18

Admissibility

19

Admissibility

- The evidence must have been revealed legally, properly and fairly.
- The rules concerning admissibility generally state that the evidence must be:
  - Probative. The evidence is relevant to the case, it is credible, it has value to the case, it does not waste court time.
  - Not prejudicial. The evidence is factual, it is impartial.
  - Relevant. Helps to prove the guilt or innocence of the defendant.
  - Accurate. The evidence can be shown not to have been altered or tampered.
  - Coherent. The court can understand it, evidence is presented in chronological order, the court does not need to call in an expert
  - Provable. The results can be repeated. If a non standard tool was used, a fundamental method of reproducing the results can be used to prove the results. The system that stored the evidence was secure throughout the item's lifetime
- Consequently, evidence might become inadmissible if it was seized without appropriate authority, was 'changed', chain of custody cannot be proven…
- There must be full disclosure of both inculpatory and exculpatory evidence.

See: Criminal Justice Act 2003 and the Police and Criminal Evidence Act 1984, specifically, "Evidence in Criminal Investigations", Home Office, (2020), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/919630/evidence-in-criminal-investigations-v5.0.pdf

20

Further Reading

Admissibility: Acceptable Tools

- The tools we use must be rigorous and proven. More work needs to be done in arriving at acceptable tool testing methodologies. Please consider reading:

- Horsman, G., 2018. *"I couldn't find it your honour, it mustn't be there!"– Tool errors, tool limitations and user error in digital forensics.* Science & Justice, 58(6), pp.433-440.
- Flandrin, F., Buchanan, W.J., Macfarlane, R., Ramsay, B. and Smales, A., 2014, September. Evaluating digital forensic tools (DFTs). In 7th International Conference: Cybercrime Forensics Education & Training (pp. 1-16).

Further Reading

Bando vs Gates (1996), available from: https://cyber.harvard.edu/digitaldiscovery/library/preservation/gates.html

Metropolitan Police Authority vs PS Virdi (2001), available from: http://www.policeauthority.org/Metropolitan/downloads/scrutinites/virdi/virdi-report-01a.pdf

Definition: Incident

Category	Description	Example	Typical mode of trial
Class 1 - Crime	Criminal offences and law enforcement	Kidnap, rape, murder	Judge/jury
Class 2 - Internal	Internal investigations	Disciplinary or audit investigations	Internal panel/CEO
Class 3 - External	External attack	Cyber-attack	Internal panel/CEO/-CISO
Class 4 Civil Dispute	Civil disputes	Contractual disputes	Tribunal chair
Class 5 Regulatory Compliance	information is to be provided in compliance with a regulatory requirement	Freedom of Information Act requests, potential GDPR failures	Statutory body - e.g. ICO

Communications-electronics Security Group (CESG 2015)

23

2

First Principles

What are the ACPO principles and how do they apply to non criminal investigations?
What type of investigations might one be involved with?

24

ACPO – 4 principles

- Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

25

Three Core Principles (AIR)

- *Accountability.* An investigation answers to two entities, the 'head' of the investigation and the 'court' that decides on the weight of the evidence
- *Integrity.* Scientific processes have to be applied to the investigation. These processes have to be reliable. The evidence must not have been altered in any way, if it is altered, a satisfactory explanation must be provided.
- *Repeatability.* The investigative process must be conducted in a manner – with suitable logs in place to enable someone else to repeat the process and arrive at the same conclusion

26

Accountability

- The *accountability* principle requires that investigators:
  - Are accountable to two entities, the entity that requested the investigation and the entity that will determine the validity of the evidence
  - Must have the authority to do the investigation
- **Criminal** matters 'automatically' require police investigation
  - A criminal case is 'prosecuted'. It has a prosecution and defence
  - A judge/Jury decides on the weight of evidence which has to be proven *beyond reasonable doubt*. Prosecution bears the burden of proof
- In a **civil case** A tribunal chair typically decides on the weight of evidence which has to be proven by clear and convincing evidence
- In a **corporate investigation**, executives, managers, sometimes chairs of a panel typically decide on the weight of evidence
  - Police get involved if ordered to by a judge
  - Incident response, disciplinary, IP theft
- Who is an investigator professionally accountable to?

Category	Typical mode of trial
Class 1 - Crime	Judge/jury
Class 2 - Internal	Internal panel/CEO
Class 3 - External	Internal panel/CEO/CISO
Class 4 Civil Dispute	Civil court, district/circuit judge
Class 5 Regulatory Compliance	Statutory body - e.g. ICO

Integrity

- Scientific processes have to be applied to the investigation. These processes have to be reliable. The evidence must not have been altered in any way, if it is altered, a satisfactory explanation must be provided.
  - Scientific processes and tools
  - Control.
    - Chain of custody
    - What about cloud?
    - Evidence is not altered. What about live and network forensics?

What four observations can you make about the following clip that might be pertinent to the present module?

Dr. Harjinder Singh Lallie 29

29

6th July, 2008. Colleton Company, The, Clyde Phillips Productions, John Goldwyn Productions. Dexter, Series 2, Episode 1.
This recording is to be used only for educational and non-commercial purposes under the terms of the ERA Licence

30

Answers

- Roles on a forensic scene
- First responder analysis
- Protecting/securing the crime scene
- The problem of contaminating the crime scene

31

32

3

Changing States: how is evidence created?

33

Changing States

"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 fibers 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."

Professor Edmond Locard (1877-1966)

Every time a computing device is turned on, whenever a user accesses a file, runs a program, inserts a USB stick etc, 'evidence' is created

Generally, a digital transaction must have been conducted resulting in a change of state for a file.

We search for the relevant transactions to find the evidence

34

Changing States

A user installs an email client, which three places might we look for evidence of

A: evidence of installation

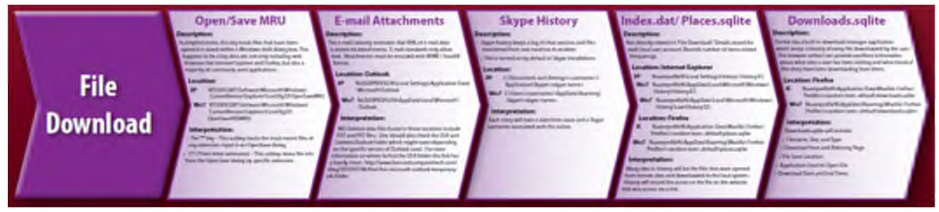
i. Registry
ii. File system: system metadata and application metadata
iii. App list
iv. Configuration files

B:received emails

i. Web client
ii. Within the app
iii. Auto file attachment locations

35

Further Reading



Source: https://blogs.sans.org/computer-forensics/files/2012/06/SANS-Digital-Forensics-and-Incident-Response-Poster-2012.pdf

36

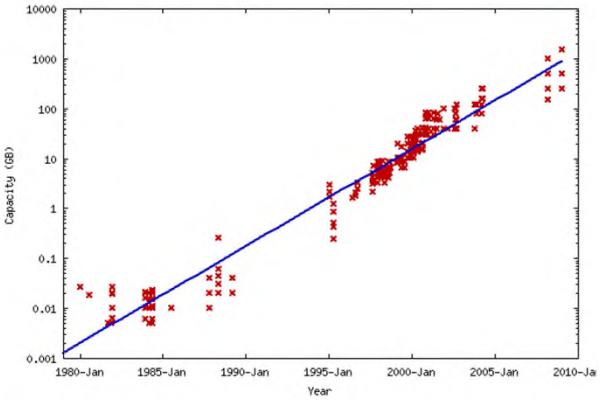
4

The Growth of Digital Forensics

What are the factors involved in the growth of the industry?
What is the impact of that growth?

The rise… and rise of digital investigation

- There are numerous reasons for the increased work in this area largely driven by Moore's law and Nathan's law:
  - Memory capacities
  - Array of digital devices
- Terror threat
- International growth, countries which are developing expertise



source: Wikimedia (https://upload.wikimedia.org/wikipedia/commons/a/a1/Hard_drive_capacity_over_time.png)

Growth of the Academic Discipline

In September 2005, UK Universities alone offered **3** cyber security/digital forensics related degree courses. By 2011, it became **75**, by 2012 **84** degree courses comprising **39** Cyber Security degree courses, **25** Digital Forensics degree courses and **20** Information Security and Digital Forensics degree courses

LALLIE, H., SINCLAIR, J., JOY, M., JANICKE, H., PRICE, B. & HOWLEY, R. 2014. *Pedagogic Challenges in Teaching Cyber Security: A UK perspective*, Elsevier.

39

Growth of the Academic Discipline

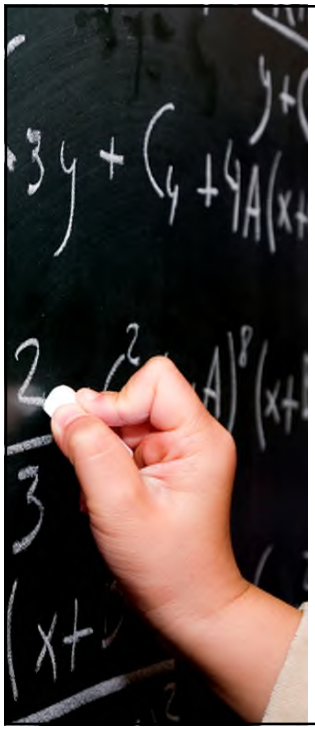
Year	2007	2008	2009	2010	2011	2012	2013
No. of Forensic Examinations	4634	4524	6016	6564	7629	8566	7273
Terabytes of Data Processed	1228	1756	2334	3086	4263	5986	5973
Terabyte per Forensic Examination	0.26	0.39	0.39	0.47	0.56	0.7	0.82

Total number of Forensic Investigations by the FBI between 2007 to 2013

Source: U. S. Department of Justice, 2007, U. S. Department of Justice, 2008, U. S. Department of Justice, 2009, U. S. Department of Justice, 2010, U. S. Department of Justice, 2011, U. S. Department of Justice, 2012, U. S. Department of Justice, 2013

See also: Irons, A., & Lallie, H. (2014). Digital Forensics to Intelligent Forensics. Future Internet. Retrieved from http://www.mdpi.com/1999-5903/6/3/584/htm

40



Why Does This Matter?

- Digital forensics is a new discipline
- Russell group /Redbricks only started teaching this recently (Warwick 2011, Oxford 2016)
- One *world class* journal, a second *decent* journal, no really reputable conferences
- No accepted standards in terms of professional accreditation, methods of representing evidence

Opportunities

- Good opportunities to establish oneself
- So much to discover

41

Moodle quiz

42

1

Creating and managing a Case

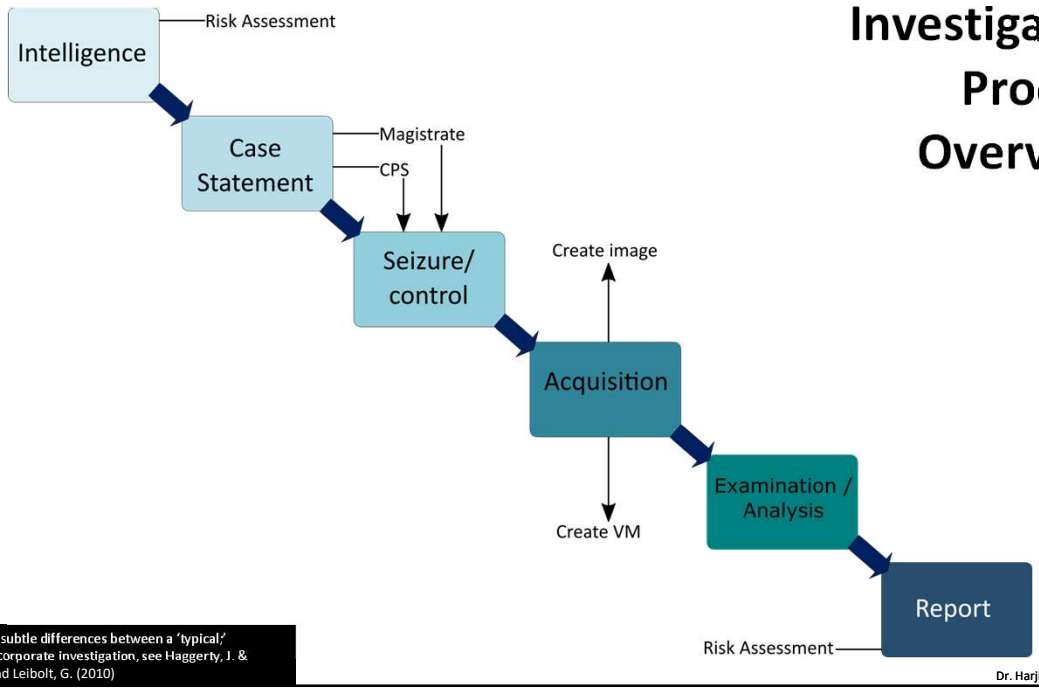
```
animal.E01
TrashedDisk.E01
```

Dr Harjinder Singh Lallie
Director of the Accredited Centre of Excellence in Cyber Security Education
Discipline group leader (cyber security)
HL@warwick.ac.uk

RATE MY PROFESSORS Linked in facebook

1

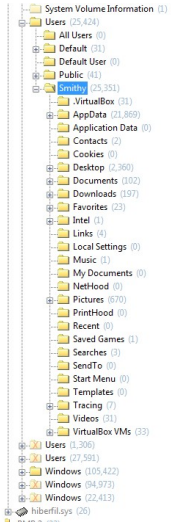
Investigative Process Overview



For more about the subtle differences between a 'typical' investigation and a corporate investigation, see Haggerty, J. & Taylor, M. (2006) and Leibolt, G. (2010)

2

VMs as an alternative way of presenting 'complex' evidence

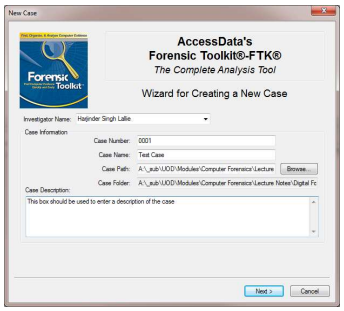


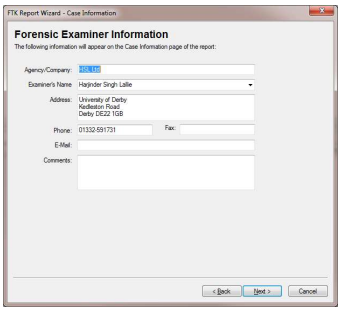
Proprietary software – not seen or understood by the jury, encrypted volumes, other complex software/configuration can be presented as a walk-through using a VM

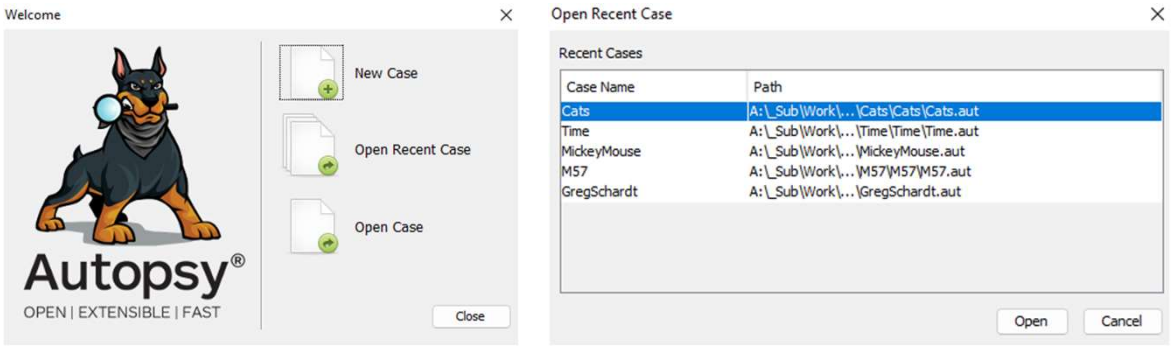
Creating a Case

The term 'case' means different things at various contexts.

- In Autopsy/EnCase/FTK, this is a project file which contains multiple items of evidence
- To the 'case manager' this is the overall case which includes management of multiple entities, people and forensic processes
- The case can be shared, over a network, or by copying the case directory (with some possible modifications to the .aut file)

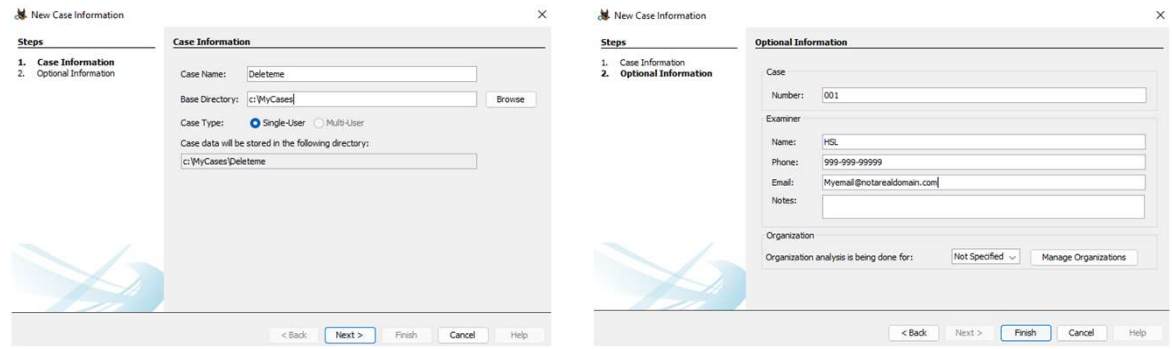






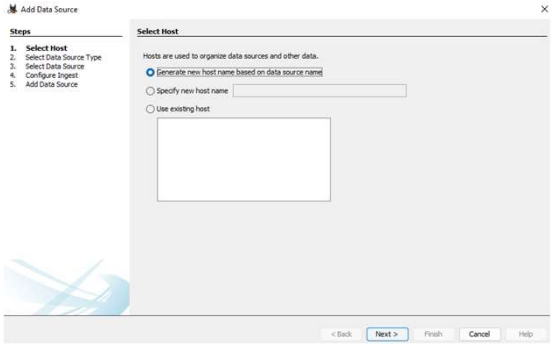
Dr. Harjinder Singh Lallie 5

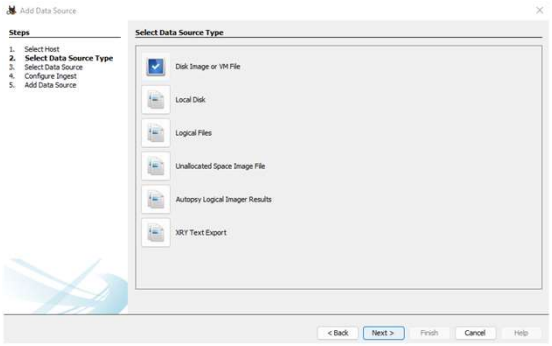
5



Dr. Harjinder Singh Lallie 6

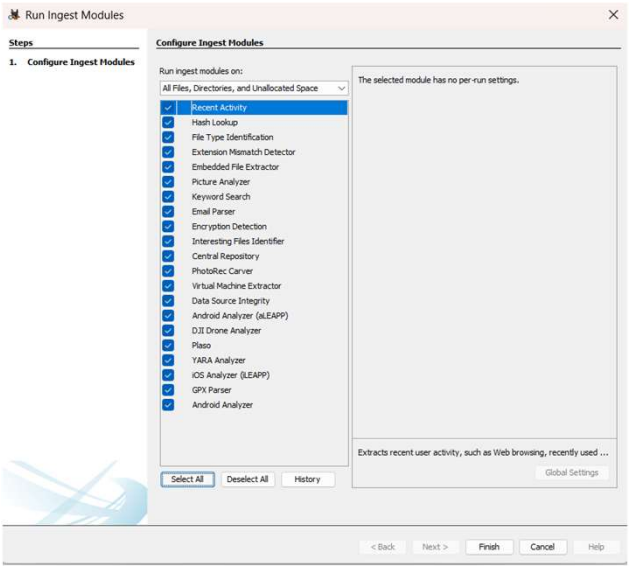
6



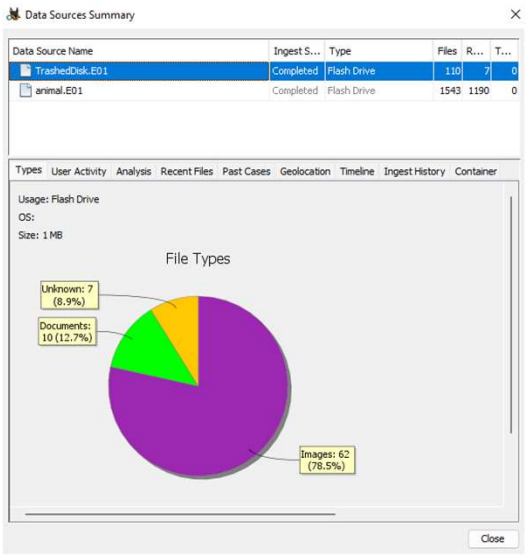


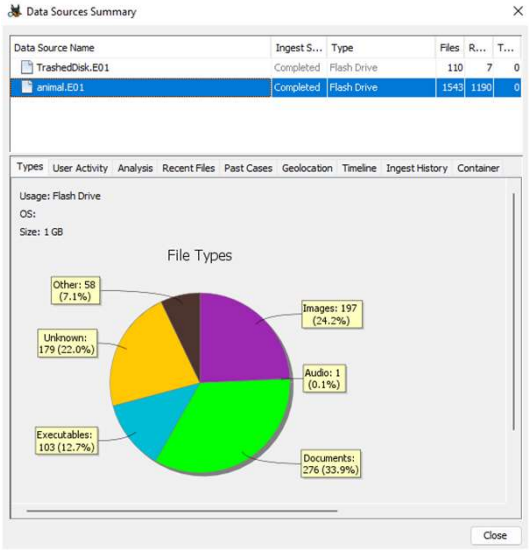
7

Always let ingest modules finish, otherwise you will have incorrect / inaccurate / incomplete results



8





9

Ten Asians named in 21-strong tax crime gang jailed

The final defendant of a twenty-one strong crime gang was sentenced this week for his part in a £37.5 million tax fraud. In total all twenty-one were jailed for a total of seventy-four years.

Harbans Singh Kohli, 47, from Ealing, London, was sentenced to two years and six months, following two re-trials, for laundering just over £1 million in associated 'missing trader' fraud. He was disqualified from being a company director for 10 years. He was originally sentenced in 2007 but released by the Court of Appeal.

The sentencing which ended one of the most complex investigations undertaken by HM Revenue & Customs (HMRC) came at the end of seven trials and retrials. Investigations began in

HMRC said the fraud related to the dishonest manipulation of the VAT system through the import and export of computer processing units (CPUs).

The fraud involved importing CPUs from Ireland VAT-free and then selling them on with VAT added, together with sham invoices, HMRC said. Once the goods had been sold on a number of times, they were exported back to the EU, and the exporter claimed a VAT credit from HMRC for VAT paid on the purchase of the goods, HMRC added.

The gang divided laundered the profits through 12 bank accounts. Account holders withdrew the cash, receiving commission, while the money is believed to have been invested in third of a tonne of gold bullion, property in Dubai and a luxury flat near Harrods.

in seven interlinked trials and easy profits at the added, through a chain of bulk of the cash. They defendants from

The 'Shape' of Data

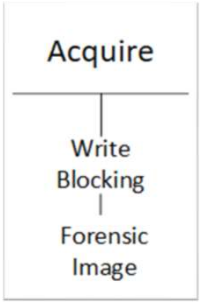
Investigation of invoices, PDFs, JPGs, some are 'OCR'able, others are not, proprietary accounting software…

https://citywire.com/funds-insider/news/37m-tax-crime-gang-jailed/a402119

10

See: https://www.digitalforensics.com/blog/how-to-make-the-forensic-image-of-the-hard-drive/

Acquire



- Make a digital forensic image* of all the DSS**
- A digital forensic image is an identical bit for bit copy of the DSS, for instance for a DSS, this is a copy of every sector and track of the hard disk including the data contained in 'blank' sectors and sectors which are marked as 'deleted' in the file allocation table (FAT)
- Forensic Image/Copy: bit for bit copy of all or portions of the original medium
- .E01, RAW, .DD, AFF, AD1
- 'Mirror copy': Complete copy of all the 'visible' elements of the original medium (backup)
- 'Bit copy': AKA Sector by sector copying resulting in a bootable medium

- A hash confirms the validity of the image. The hash travels with the image
- Investigations are conducted on the forensic image and never on the original DSS other than in exceptional circumstances such as network forensics, or other 'live' attacks

* Not the same as Hard Drive Cloning, Ghost imaging, Mirror Image, however, the term forensic copy 'does' mean the same
** digital storage system

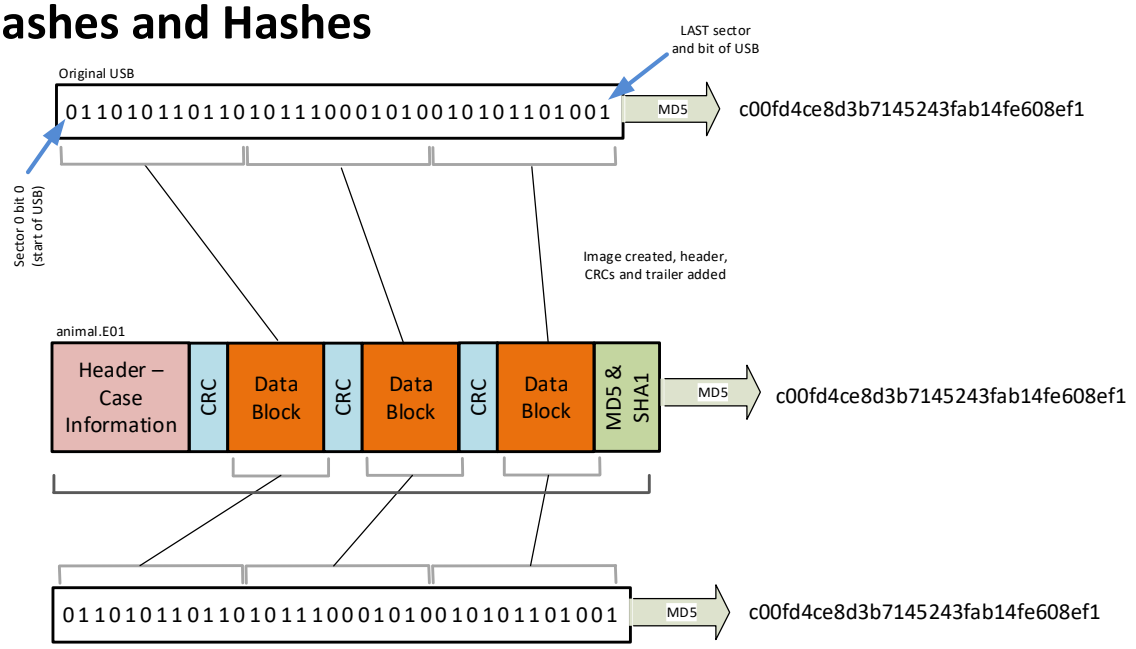
13

Digital Forensic Image

- Forensic Workstation:
  - Check for viruses (say you did it in the report!)
  - Ensure it is not connected to network/internet
- Write blocker
  - Write blockers prevent the operating system from writing anything to the hard disk
  - Capture commands that request the hard disk to overwrite sectors from the operating system
  - Two techniques:
    - Deny all writes to the disk and report as successful(not popular)
    - Cache Based: Use on-board memory to cache writes for the duration of the session
    - Cache based blockers present the appearance to the operating system that the drive is writable, uses memory to ensure that the operating system sees changes to the individual disk sectors it attempted to overwrite.
- Perform a hash of the original drive and compare with the forensic copy to make sure you have a bit-for-bit copy
  - Encase and FTK have provision for this to happen 'automatically'

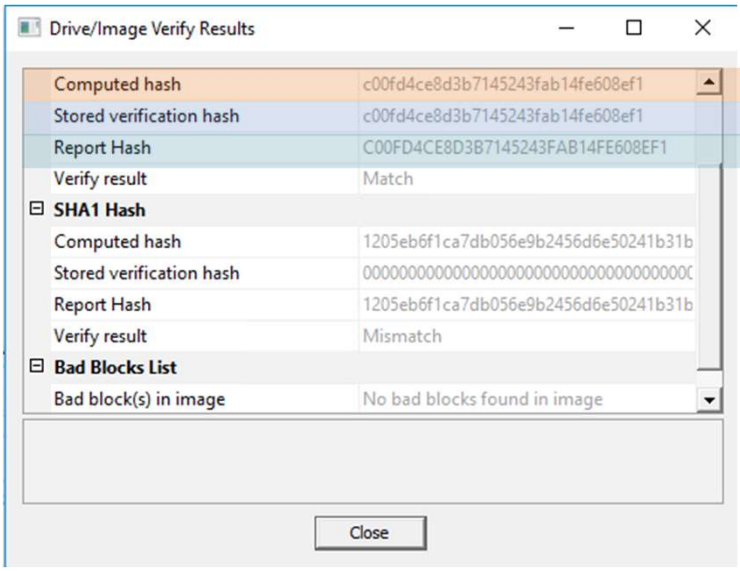
14

Hashes and Hashes



15

DFI hashes



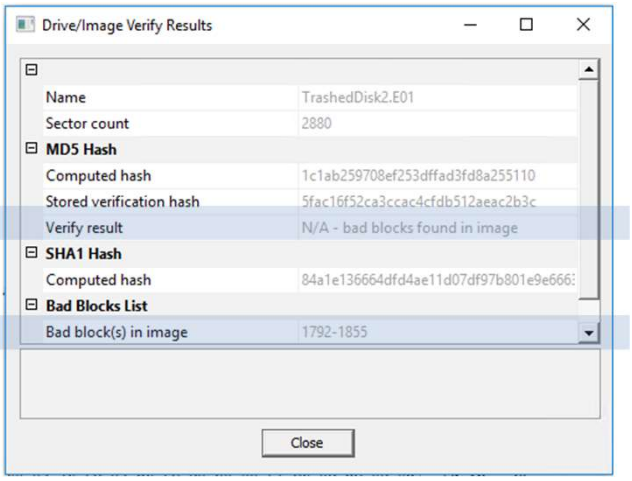
Calculated just now on the data blocks in E01

Calculated on original DSS and stored in E01

Stored in accompanying text tile

16

Is this a problem?



Do the bad blocks impact the evidence you have found (are photos visible?) No? Continue and report

Are parts of evidence not visible, possibly because of bad blocks, report that evidence with caution

Reimage the original and try to understand why the SVH and CH are different

17

Forensic Workstation

HyperStation FRX-R - Digital Forensics Analysis Workstation

Built upon Intel's Xeon Scalable platform the HyperStation FRX-R is powered by dual Xeon Gold 5118 CPU's, providing 96 PCI-E lanes for increased I/O bandwidth, and support for up to 2TB of DDR4 ECC memory, this system delivers outstanding performance for heavily threaded, CPU intensive workloads.

A standard feature amongst all of our forensic workstation is the inclusion of a Tableau Forensic Universal Bridge, and integrated write-blocker that allows forensic acquisitions via SATA, USB 3.0, PCIe, SAS, FireWire 800, and IDE. Built-in HDD docking bays, plus hot-swap bays for both 2.5" and 3.5" drives make it easy to swap disks in and out regularly.

- 2x Intel Xeon Gold 5118 2.30GHz (3.20GHz Turbo) 12 Core Processors
- NVIDIA RTX 2080TI 11GB GDDR6 Graphics
- 96GB ECC DDR4 2400MHz Memory
- Dual Gigabit LAN
- Tableau Universal Forensic Bridge

18

Further Reading

2.3.1 Known Hashes

Materials

The following few steps will be done in your own time and will not be covered in the class.

The National Software Reference Library (NSRL), downloadable for Android, IOS. and Windows files from: `https://sourceforge.net/projects/autopsy/files/NSRL/`, is a database of known files. The library has collected software from various sources and incorporates file profiles from popular software.

This library can be added to Autopsy, and Autopsy told to 'ignore' these files in its' analysis. This saves time in an investigation.

31. Download the latest Windows library from: `https://sourceforge.net/projects/autopsy/files/NSRL/` (Figure 14)
32. Unzip the library
33. right click on the DFI and select `Run Ingest Modules`

Figure 14: National Software Reference Library (NSRL)

NIST's NSRL

19

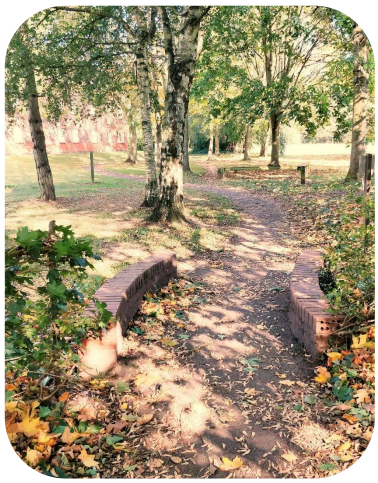
Static vs Live Acquisition

Acquisition 'generally' takes place 'offline', however on occasion it is necessary to do a live acquisition – for example with RAM, networks, systems that can't be turned off (because they are encrypted or central to an organization functioning)

20

Basic Forensic hygiene

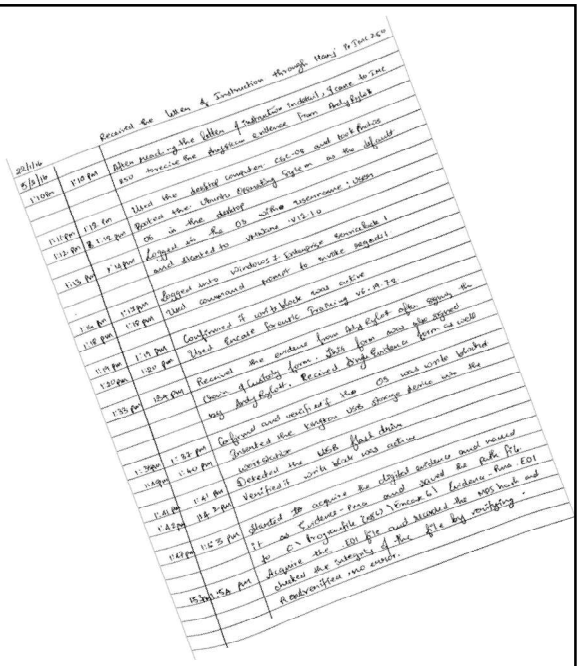
- Did you virus check the forensic workstation?
- Did you virus check the image?
- Did you hash check, what was the result?
- What was the software and machine you used?



Documentation

Documentation helps to prove control and can act as evidence

- General case intake form*
- Chain of custody form**
- Crime/Incident scene notes
  - Sketches, diaries, passwords, post-its
- Labelling
  - leads→ports, description, make/model/serial number, MAC/IP addresses (if still on), operating System/service pack (if still on, time on the machines (for benchmarking) (if still on)
- The log
- Report***
  - Encase report, your report, case officers report...



Anywhere Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: _____ Offense: _____
Submitting Officer: (Name/ID#) _____
Victim: _____
Suspect: _____
Date/Time Seized: _____Location of Seizure: _____

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

APD_Form_#PE003_v.1 (12/2012) Page 1 of 2 pages (See back)

Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location

Final Disposal Authority

Authorization for Disposal

Item(s) #: _____ on this document pertaining to (suspect): _____
is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)
☐ Return to Owner ☐ Auction/Destroy/Divert
Name & ID# of Authorizing Officer: _____ Signature: _____Date: _____

Witness to Destruction of Evidence

Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ID#:____
in my presence on (date) _____.
Name & ID# of Witness to destruction: _____ Signature: _____Date: _____

Release to Lawful Owner

Item(s) #: _____ on this document was/were released by Evidence Custodian
_____ID#:_____ to
Name _____
Address: _____ City: _____State: _____ Zip Code: _____
Telephone Number: (____)_____
Under penalty of law, I certify that I am the lawful owner of the above item(s).

Signature: _____ Date: _____

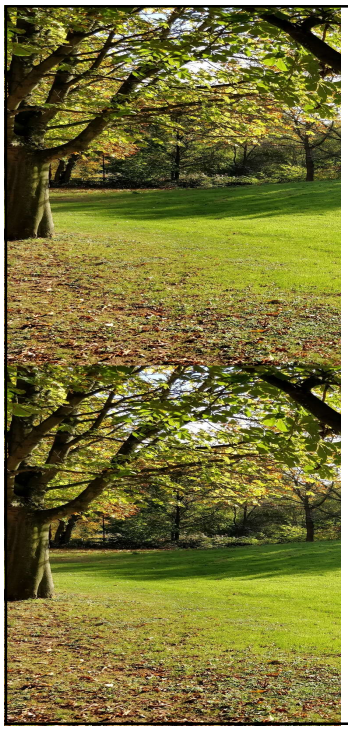
Copy of Government-issued photo identification is attached. ☐ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.

APD_Form_#PE003_v.1 (12/2012) Page 2 of 2 pages (See front)

Chain of Custody Form

23



Seize

Seizure is *the search for, recognition of, collection of, and documentation of electronic evidence* (NIJ, 2001)

- The key goals here are to: (a) bring potential evidence into your control (b) not taint the evidence in the process
- 'Governed' by guidelines such as the ACPO "Good practice Guide for Computer based Electronic Evidence" (2014) and "NIJ, Electronic Crime Scene Investigation, A Guide for First Responders 2e (2008)", Scientific Working Group on Digital Evidence (SWGDE, 2013)
- CESG identify six significant factors that can cause loss or degradation of evidence at a crime/incident scene, for example, suspect is at the scene; attacks in progress on live ICT systems; system users inadvertently destroying or corrupting evidence; system administrators inadvertently destroying or corrupting evidence; power loss and environmental issues; information management and access

24

Managing the Crime/Incident Scene

The crime/incident scene has to be carefully managed and controlled so as to minimise/reduce the likelihood of tainting or corrupting the evidence.

This means: someone is **in charge**, some form of **quarantine** is in place, CSIs are aware of **what to seize**, adequate **documentation** is being kept

College of Policing guidelines: CSIs and managers | identifying scenes | securing the scene | cross-contamination | preserving the scene | managing the media | searching and examining the scene | releasing the scene

Dr. Harjinder Singh Lallie 25

25

Question

What's are the 6 problems with the following 'seizure'

Dr. Harjinder Singh Lallie 26

26

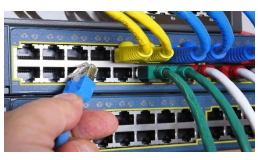
27

28

You've just been employed in a small firm (200 people) and have been alerted to an incident involving potential IP Theft. What is the **FIRST** thing you should do?

Is there a policy?

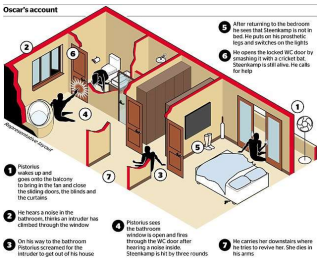
31

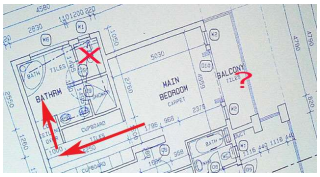


The Crime/Incident Scene

CSIs **'know' the crime/incident scene**, are capable of handling **powered up/down/hibernated** machines, are able to make decisions on whether to **capture data** on the scene or away from it, can deal with **networked** connections and data transfers

32





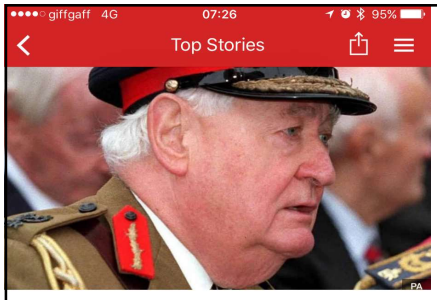
Recording the Crime/Incident Scene

It is good practice to video/photo record and/or sketch the scene. This includes a record of how devices were connected and running programmes/processes

In addition, the CSI takes notes of the scene and the actions taken

Record the configuration/connection of network points, access points, external devices such as hard drives

33



Lord Bramall 'receives Met Police apology' over abuse claims

1 hour ago | UK

Lord Bramall, the former chief of the defence staff, has said he has received an apology from the Metropolitan Police over its investigation of historical child abuse allegations against him.

The 92-year-old told the BBC the apology came from Met commissioner Sir Bernard Hogan-Howe.

He says Sir Bernard told him the force had been wrong to delay informing him that no further action would be taken.

Seizure

ACPO proposes that a level of 'proportionality' be applied so that CSIs don't seize items simply because 'they are there' and 'the person in charge of the search must have reasonable grounds to remove property and there must be justifiable reasons for doing so.'

Some items cannot be 'seized easily' (servers)

Items must be handled correctly (cooling, tagging, transportation, storage)

Police and Criminal Evidence Act 1984c. 60:
S19: General Powers of Seizure
S20: Extension of Powers of Seizure to Computerised Information
S21: Access and Copying

34

Triage

An LEA enter a suspect's home and discover more than 40 laptop devices. The full investigation of all devices is likely to take up to 9 months

- The process of assessing an items' priority in an investigation – which are the most important devices?
- Pre-configured to include specific search parameters, including keywords and hash values
- Moves away from the 'seize everything' mantra but contradicts the 'change nothing' mantra because the USB 'makes changes' to the system.

35

Further reading

- *NIST Sample Chain of Custody form* (APD_Form_#PE003_v.1 (12/2012)) available from: https://www.nist.gov/document/sample-chain-custody-formdocxcalib
- *Forensic Examination of Digital Technology*, ENFSI Working Group (2016), available from: https://enfsi.eu/wp-content/uploads/2016/09/1._forensic_examination_of_digital_technology_0.pdf
- *Computer Security Incident Handling Guide*, NIST, *(2012)*, available from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
- *Search powers, and obtaining and executing search warrants,* College of Policing (2013) available from: https://www.college.police.uk/app/investigation/investigative-strategies/search-powers-and-obtaining-and-executing-search-warrants
- Hitchcock, M., Gillespie, B., Crilly, J. and Chaboyer, W., 2014. Triage: an investigation of the process and potential vulnerabilities. Journal of advanced nursing, 70(7), pp.1532-1541.
- Jusas, V., Birvinskas, D. and Gahramanov, E., 2017. Methods and tools of digital triage in forensic context: Survey and future directions. Symmetry, 9(4), p.49.

36

2

Seizure
Understanding the Environment

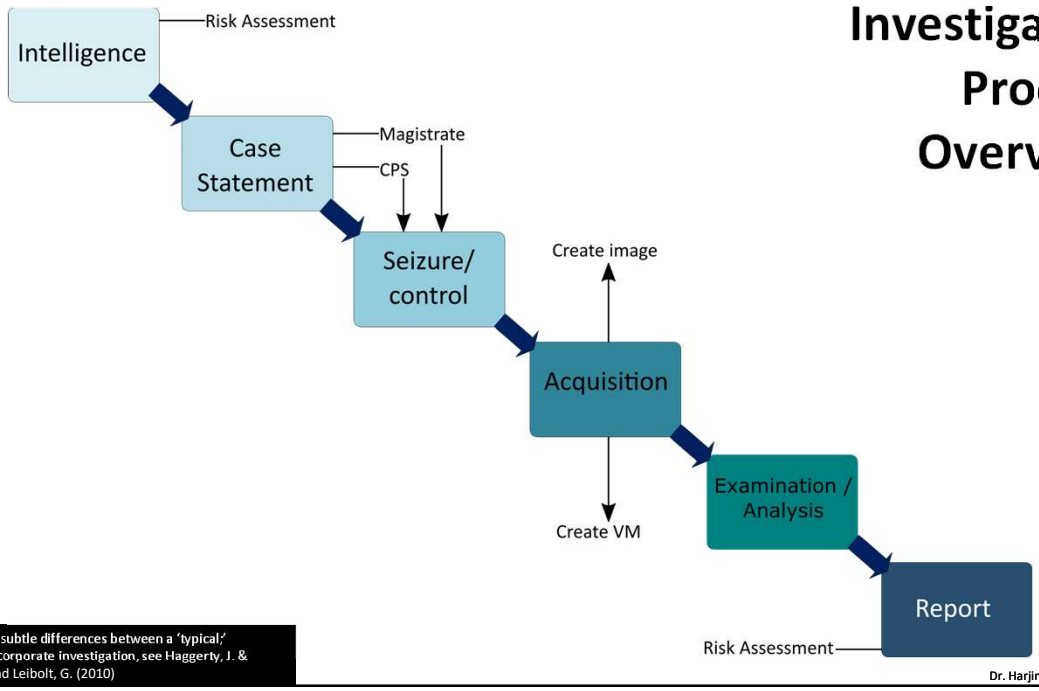
Stanley.E01

Dr Harjinder Singh Lallie
Director of the Accredited Centre of Excellence in Cyber Security Education
Discipline group leader (cyber security)
HL@warwick.ac.uk

RATE MY PROFESSORS LinkedIn facebook

37

Investigative Process Overview



For more about the subtle differences between a 'typical' investigation and a corporate investigation, see Haggerty, J. & Taylor, M. (2006) and Leibolt, G. (2010)

38

TutorialHandbook[181022].pdf

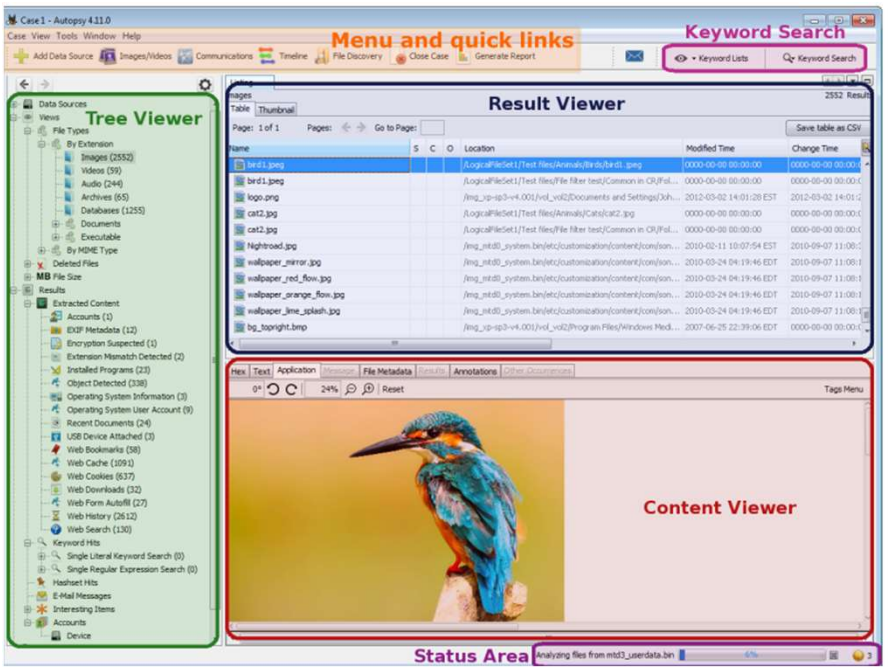
ForensicWorkstation121022.ova

↓

Snapshot

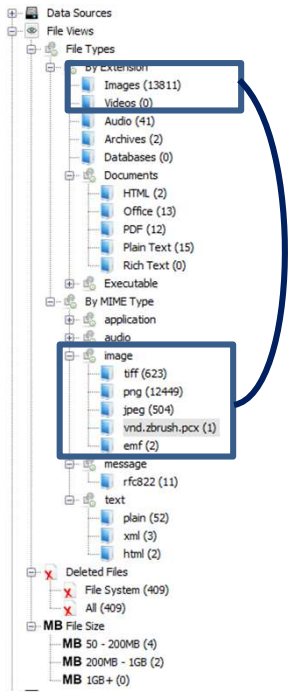
39

The Environment



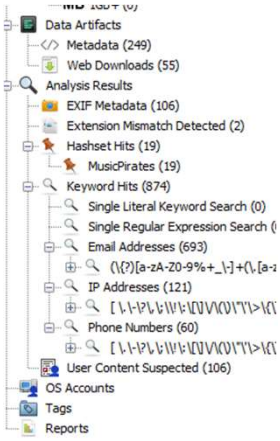
40

Tree view



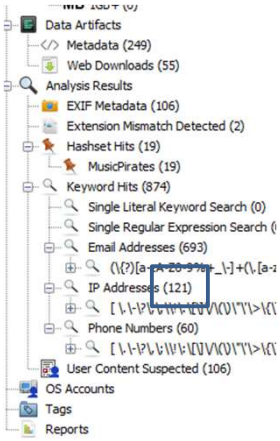
- There are multiple ways in which data is presented. Understand what is different about them
- The numbers don't always seem to add up – explore why

Tree view



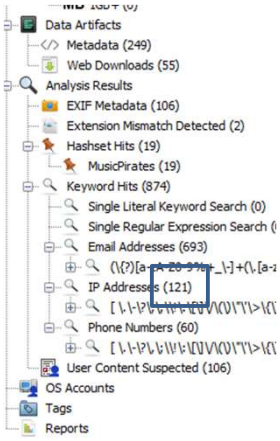
- There are multiple ways in which data is presented
- The numbers don't always seem to add up – explore why
- Results of searches and ingest presented in the tree
- Tags and bookmarks also presented here

Tree view



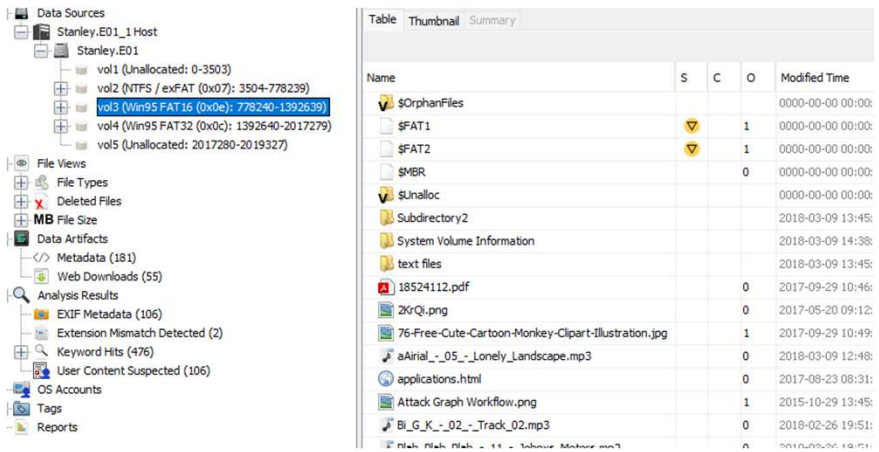
Don’t save search result unless happy with it, each search enumerates the count

Tree view



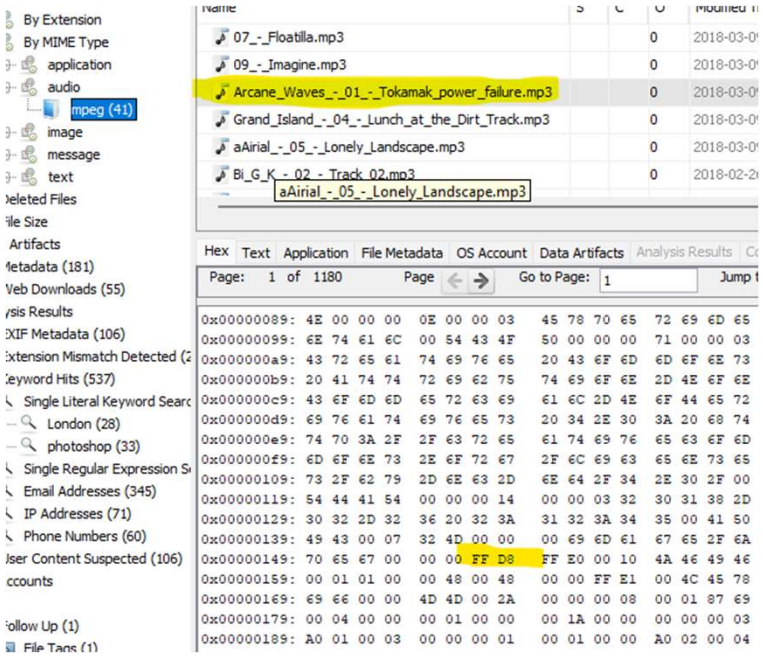
There might be lots of false positives. Autopsy just does as its told

Result view changes to reflect tree selection



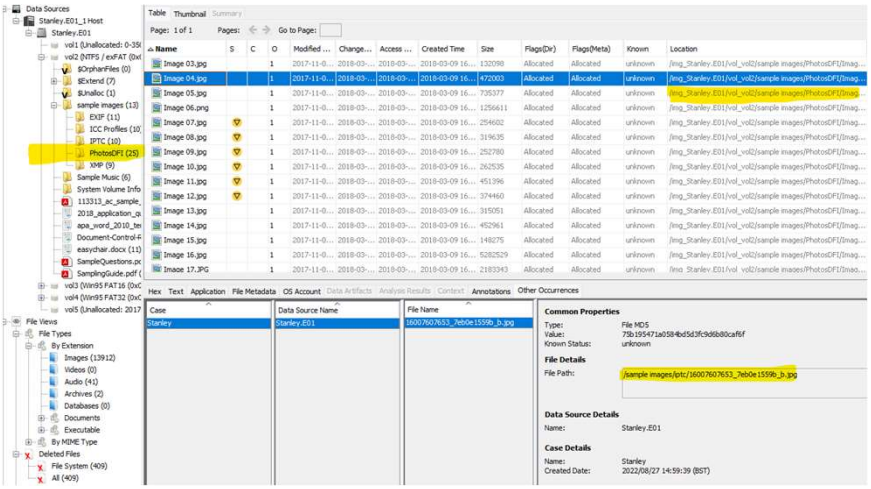
45

Content view changes to reflect what is selected in result view



46

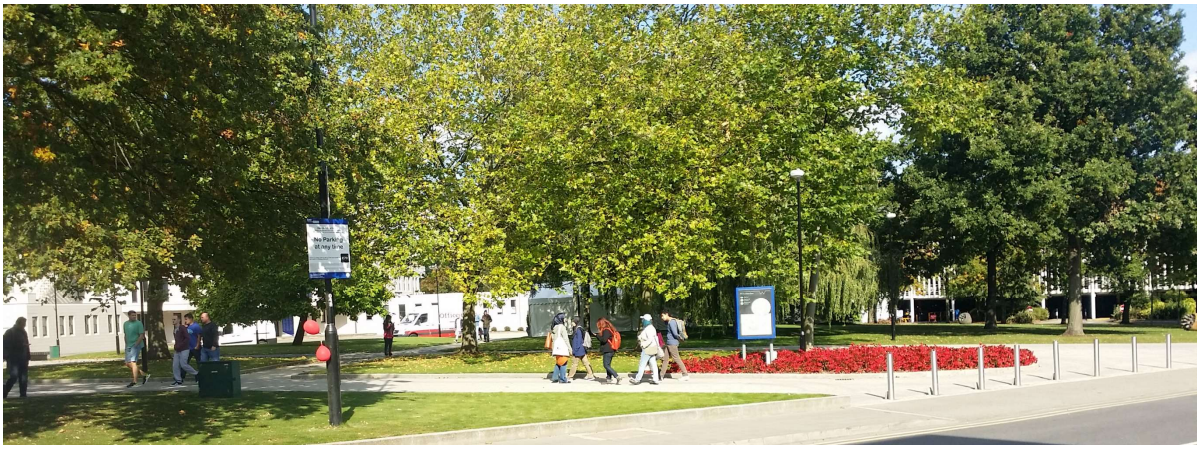
There are multiple *content viewer tabs*



47

120min

Complete Section 3



48

Examination and Analysis

What is examination and Analysis?
What might we look for?
What are (examples of) legal tests we have to meet?
Can technology help us to become more efficient?

Harjinder Singh Lallie
Associate Professor
HL@warwick.ac.uk

RATE MY PROFESSORS LinkedIn facebook

1

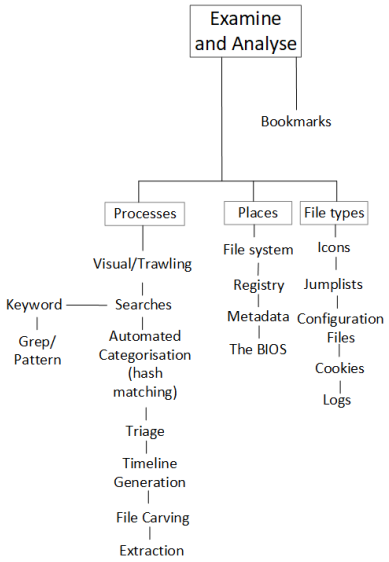
1

What is examination and Analysis?

2

Examine and Analyse

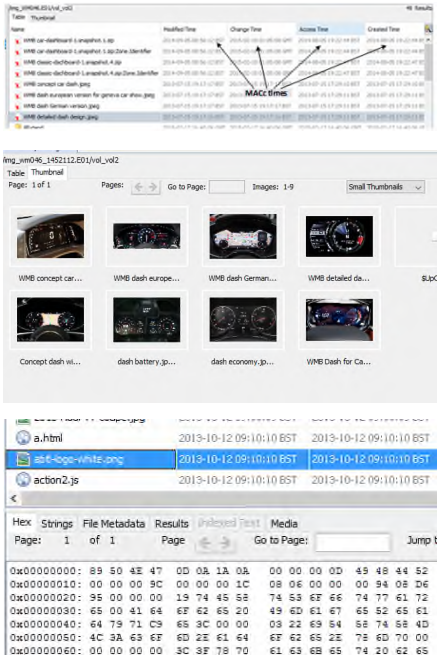
- The **examiner** reveals the presence of data that may be evidence in the case, and explaining the origins and significance
- Bookmarks important evidence (not data)
- The **analyst** analyses the results (bookmarks) of the examination and determining the significance and probative value to the case



3

Examination modus operandi

- Look through the results of ingest for low hanging fruits. Is the evidence obvious?
- Prepare searches
- Intrusive analysis



4

2

What might we look for?

5

Case types, and types of evidence

- Fraud
- Illegal images
- Drugs
- IP Exfiltration

6

Case types, and types of evidence

- Fraud
- Drugs
- IP Exfiltration
- Illegal images

Documents, PDFs, JPEGs

Enron
Kohli & Co
Serenity Travel & Serenity Community Transport Ltd

George Bush (left) Kenneth Lay (Right)

https://www.youtube.com/watch?v=e5qC1YGRMKI
https://citywire.com/funds-insider/news/37m-tax-crime-gang-jailed/a402119
https://www.cps.gov.uk/cps/news/three-fraudsters-convicted-scamming-taxpayer-over-ps1-million-pay-their-lavish-lifestyles

7

Case types, and types of evidence

- Fraud
- Drugs
- IP Exfiltration
- Illegal images

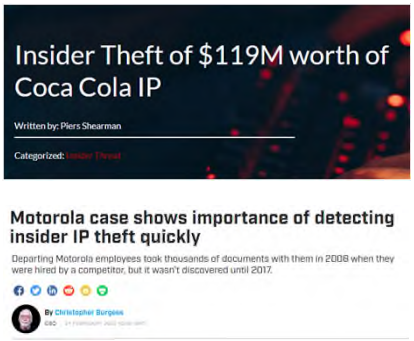
Comms (Email, Social Media)
Some photos

Olsi Beheluli posing with around £250,000 in cash
https://www.mirror.co.uk/news/uk-news/drug-dealer-who-posed-picture-5448945

8

Case types, and types of evidence

- Fraud
- Drugs
- IP Exfiltration
  - Email
  - Some photos (some on phone)
  - PDFs
  - USB activity
  - Cloud storage
  - Phone photos
- Illegal images



https://www.vestigeltd.com/thought-leadership/ip-theft-case-studies/

3

What are the legal tests we have to meet?

Illegal images

- Majority of E-Forensic department investigations in the UK involve illegal images
- To be tried, the photos must be:
  - Indecent
  - photographs or pseudo-photographs of
  - A child (A child is a person under 18 (s.7(6) of the PCA)

29 SEPTEMBER 2014, THE TABLET

More than 100,000 child porn files found on Wesolowski computer

by Liz Dodd , CNS

More than 100,000 indecent images and videos of children have been found on the computer of the laicised former papal ambassador Archbishop Jozef Wesolowski.

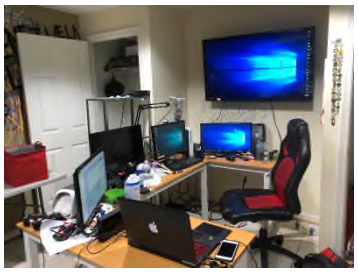
EssexLive

Essex crime: Epping man who sexually abused child had 100,000 indecent images

Law enforcement deal with 10,000s images per case

Illegal images

- Majority of E-Forensic department investigations in the UK involve illegal images
- To be tried, the photos must be:
  - Indecent
  - photographs or pseudo-photographs of
  - A child (A child is a person under 18 (s.7(6) of the PCA)



And often dozens of devices

We respond to the Defence

- Legitimate Reason: researcher.
- 'Lack of Awareness
  - I must have been hacked
  - It must have been a virus
  - It was someone else (shared computer)
  - It's not my computer
- Marriage and other relationships

Brooklyn 99, 2013, Universal Television

13

We prove the offence

We examine for three offences: possession, distribution, & creation

Sentencing is guided by what we find

	Possession	Distribution	Production
Category A	**Starting point** 1 year's custody	**Starting point** 3 years' custody	**Starting point** 6 years' custody
	Category range 26 weeks' – 3 years' custody	**Category range** 2 – 5 years' custody	**Category range** 4 – 9 years' custody
Category B	**Starting point** 26 weeks' custody	**Starting point** 1 year's custody	**Starting point** 2 years' custody
	Category range High level community order – 18 months' custody	**Category range** 26 weeks' – 2 years' custody	**Category range** 1 – 4 years' custody
Category C	**Starting point** High level community order	**Starting point** 13 weeks' custody	**Starting point** 18 months' custody
	Category range Medium level community order – 26 weeks' custody	**Category range** High level community order – 26 weeks' custody	**Category range** 1 – 3 years' custody

14

Possession

We look to show whether:

- Images are there or not.
- The suspect knew about them.
- We may be able to explain how they got there

	Possession	Distribution	Production
Category A	**Starting point** 1 year's custody	**Starting point** 3 years' custody	**Starting point** 6 years' custody
	Category range 26 weeks' – 3 years' custody	**Category range** 2 – 5 years' custody	**Category range** 4 – 9 years' custody
Category B	**Starting point** 26 weeks' custody	**Starting point** 1 year's custody	**Starting point** 2 years' custody
	Category range High level community order – 18 months' custody	**Category range** 26 weeks' – 2 years' custody	**Category range** 1 – 4 years' custody
Category C	**Starting point** High level community order	**Starting point** 13 weeks' custody	**Starting point** 18 months' custody
	Category range Medium level community order – 26 weeks' custody	**Category range** High level community order – 26 weeks' custody	**Category range** 1 – 3 years' custody

15

Distribution

There is evidence of suspect offering to/ actually sharing them with others

Emails, chat logs

	Possession	Distribution	Production
Category A	**Starting point** 1 year's custody	**Starting point** 3 years' custody	**Starting point** 6 years' custody
	Category range 26 weeks' – 3 years' custody	**Category range** 2 – 5 years' custody	**Category range** 4 – 9 years' custody
Category B	**Starting point** 26 weeks' custody	**Starting point** 1 year's custody	**Starting point** 2 years' custody
	Category range High level community order – 18 months' custody	**Category range** 26 weeks' – 2 years' custody	**Category range** 1 – 4 years' custody
Category C	**Starting point** High level community order	**Starting point** 13 weeks' custody	**Starting point** 18 months' custody
	Category range Medium level community order – 26 weeks' custody	**Category range** High level community order – 26 weeks' custody	**Category range** 1 – 3 years' custody

16

Production

Metadata in photos linked to cameras we have seized

Suspect's house

Suspect is present, must have been involved with production

	Possession	Distribution	Production
Category A	**Starting point** 1 year's custody	**Starting point** 3 years' custody	**Starting point** 6 years' custody
	Category range 26 weeks' – 3 years' custody	**Category range** 2 – 5 years' custody	**Category range** 4 – 9 years' custody
Category B	**Starting point** 26 weeks' custody	**Starting point** 1 year's custody	**Starting point** 2 years' custody
	Category range High level community order – 18 months' custody	**Category range** 26 weeks' – 2 years' custody	**Category range** 1 – 4 years' custody
Category C	**Starting point** High level community order	**Starting point** 13 weeks' custody	**Starting point** 18 months' custody
	Category range Medium level community order – 26 weeks' custody	**Category range** High level community order – 26 weeks' custody	**Category range** 1 – 3 years' custody

17

Categorisation

We have to categorise each image

This is traumatic, time consuming, subjective

	Possession	Distribution*	Production**
Category A	Possession of images involving penetrative sexual activity. Possession of images involving sexual activity with an animal or sadism.	Sharing images involving penetrative sexual activity. Sharing images involving sexual activity with an animal or sadism.	Creating images involving penetrative sexual activity. Creating images involving sexual activity with an animal or sadism.
Category B	Possession of images involving non-penetrative sexual activity.	Sharing of images involving non-penetrative sexual activity.	Creating images involving non-penetrative sexual activity.
Category C	Possession of other indecent images not falling within categories A or B.	Sharing of other indecent images not falling within categories A or B.	Creating other indecent images not falling within categories A or B.

18

Manual grading

We must ensure each image captures a child (<18)

This is traumatic, time consuming, subjective

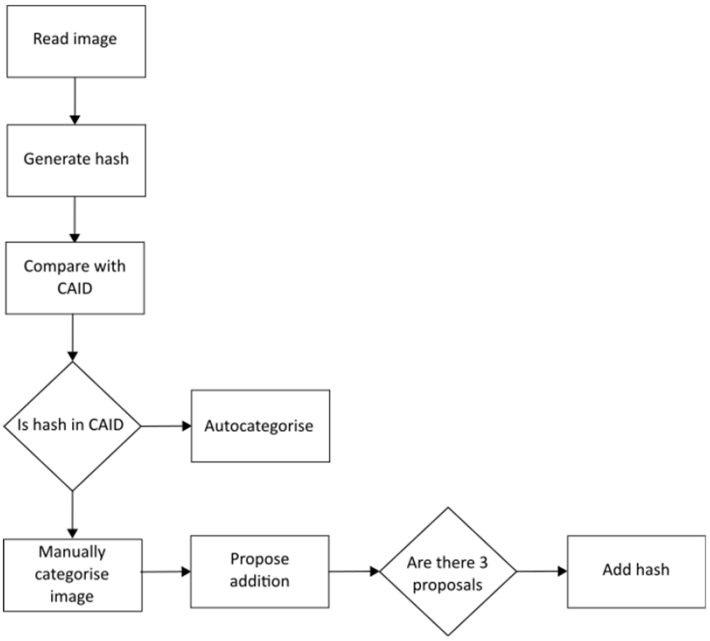
Grey area of actual age, so we set a threshold of <=14 and we aim for higher than 250, grade A or B or C (so we aim for higher)

19

4

Can technology help us conduct more efficient investigations?

20



21

When to stop

Mode of Trial

The aim of the investigation is (generally) to find 'enough' evidence to convict. It serves little interest to go beyond this point.

The case manager determines when 'enough evidence has been found' to secure a conviction. This might happen in stages (enough to get a plea, enough to convince CPS, enough to convince a Jury).

22

When to stop?

Mode of Trial

"The thresholds are: 250 Category A (the most serious) or 1000 Category A-C."

"When a case is listed for trial and the prosecution form the view that the appropriate course is to accept a plea before the proceedings commence or continue, or to offer no evidence on the indictment or any part of it, the prosecution should whenever practicable speak to the victim or the victim's family"*

*https://www.gov.uk/guidance/the-acceptance-of-pleas-and-the-prosecutors-role-in-the-sentencing-exercise

23

When is 'enough'

Police officer 1: "The aim of the investigation is (generally) to find 'enough' evidence to convict. It serves little interest to go beyond this point"

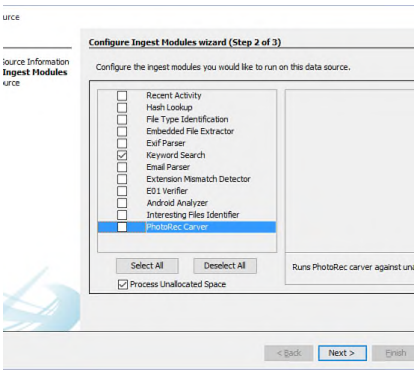
- Resource
- No effect on sentence

Police officer 2: "We investigate every system and identify all illegal images, the tax payer is expecting us to be thorough"

- Let's contribute to CAID
- Maybe we can identify more victims?
- We might find 'other stuff'

24

Pre-searching/Ingest



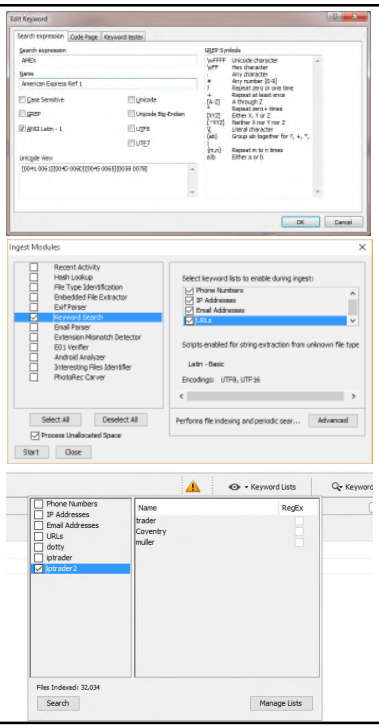
- Algorithms which reveal file/data patterns e.g., hash matches, mismatched extensions, URLs, email addresses
- Front-loads some of the search work
- However, these algorithms need improvement and generally work on file header
- There's too much reliance on manual methods and not enough research into automated/intelligent methods to aid the investigation, for instance in automating/correlating event analysis, applying confidence measures to causality/data

27

Where and how might a user have attempted to hide files in a file system?

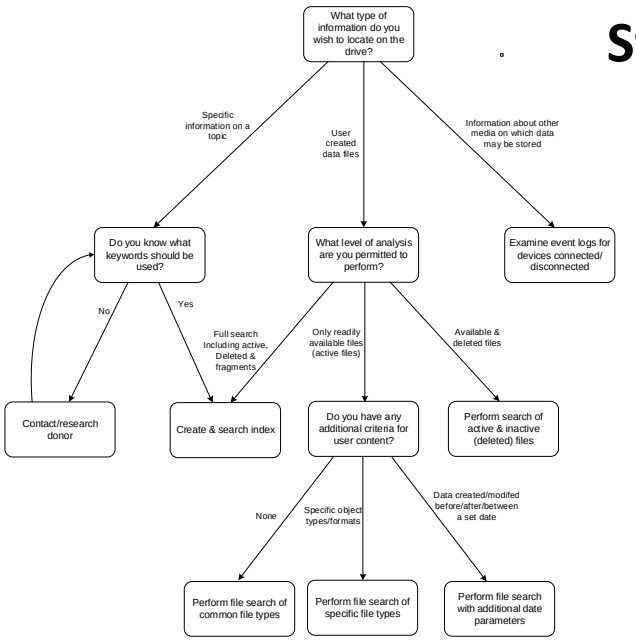
- Hidden files/directories (attributes changed)
- Files/folders/partitions are deleted
- Extensions changed
- Files 'hidden' in deep nested/unusual directories
- Steganography
- Use slack space
- Use registry space
- Encrypt
- Hide inside a VM – encrypt the VM

29



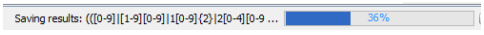
Keyword searches

- More focused/specific/literal searching for specific terms, names and places
- Generally led by case intelligence/remit
- Searches can be saved and then retrieved for future cases
  - Cases involving drugs, search files will contain common terms
  - Dictionaries of terms can be used as part of a case (Drugs: Cocaine, coke, stuff, s**t, etc)



Strategising the Search

- Searches take a long time and have to be 'planned'
  - Common to set up searches and then run them overnight
- Certain valid terms will yield too many results
  - US → "it was all of US"; "I mUSt see him tomorrow"



Based on a flow chart by Lindsay Ould (KCL)

Strategising the Search

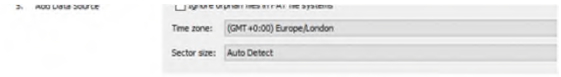
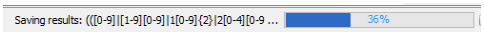


Figure 8: Import the image (created by author)

3) **For the keyword search [cat]**, there are a total of 42871 results. H
these were system files, configuration information and some other file

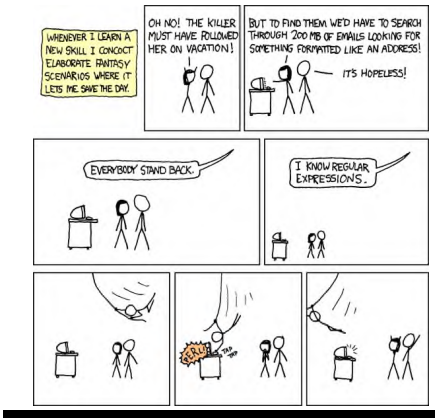
- Searches take a long time and have to be 'planned'
  - Common to set up searches and then run them overnight
- Certain valid terms will yield too many results
  - US → "it was all of US"; "I mUSt see him tomorrow"



Based on a flow chart by Lindsay Ould (KCL)

32

Regular Expression Based Searches*



https://www.princeton.edu/~mlovett/reference/Regular-Expressions.pdf

- A 'tool' used in Linux/Unix to format expressions, can be used to build powerful search patterns for instance:

```
\b[A-Z0-9._%+-]+@[A-Z0-9.-]+\.[A-Z]{2,4}\b
```

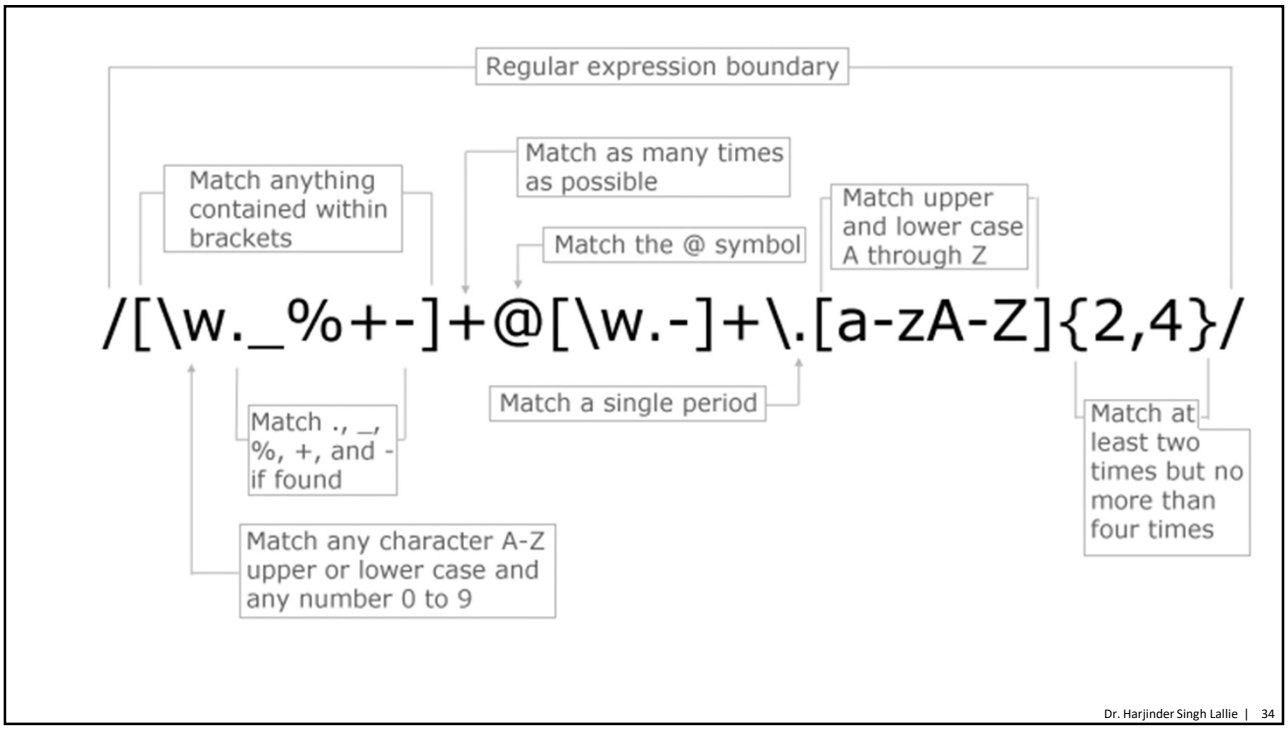
- Would give you email addresses

```
\(^\|[^0-9]\)\{1\}\([345]\{1\}[0-9]\{3\}\|6011\)\{1\}[-
]\?[0-9]\{4\}[-]\?\ [0-9]\{2\}[-]\?[0-9]\{2\}-\?[0-
9]\{1,4\}\($\|[^0-9]\)\{1\}
```

- Would give credit card numbers
- Regular expressions for the most commonly sought data are available online….

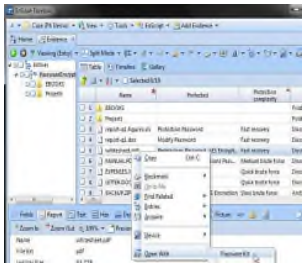
*GREP is a linux utility stands for globally search a regular expression and print

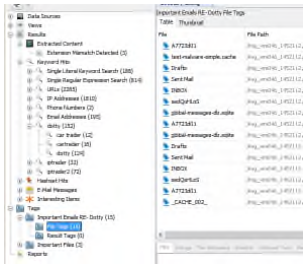
33



34

Bookmarking





- When a search returns data that 'may' be useful evidence, it is bookmarked for consideration later on
- Files, directory structures, photos, deleted documents/text etc can be bookmarked
- Bookmarks are important as they contain the bulk of the information required in the report
- Allows for important items to be saved and categorised
- Balance between 'over' and 'under' bookmarking (too much or not enough for the analyst)
- Common to do a bookmark review
- Begin bookmarking at the outset rather than doing an analysis and then having to return to bookmark 'important' data

35

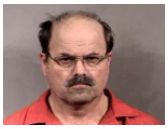
Metadata

Harjinder Singh Lallie
Associate Professor
HL@warwick.ac.uk

RATE MY PROFESSORS LinkedIn facebook

1

The BTK Killer



- 1974 to 1991 a series of murders took place in which the victims were bound, tortured and killed (BTK) by Dennis Lynn Rader
- Killer communicated with police confessing to the murders through regular letters
- Police had DNA samples of the killer and knew that he drove a black Jeep Cherokee
- 2004: Rader won the confidence of the police and he asked them if it was possible to trace a file to his computer, they said no. Rader sends a word document as part of the continued communication.
- Word document metadata points to a man called Dennis at the 'Lutheran Church'. They were able to identify Dennis Lynn Rader (president of Christ Lutheran Church) and found a black Cherokee parked outside his house.
- This was all circumstantial evidence (common sense!) until they matched his DNA with the DNA from the crime scenes.

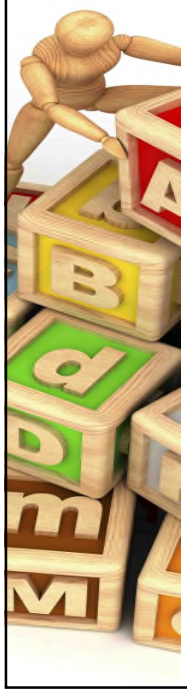
See also: State v. Guthrie *627 N.W.2d 401 (2001);* Williams v. Sprint/United Management. Co., 230 F.R.D. 640 (2005); United States v. Hamilton, 413 F.3d 1138 (2005) (https://caselaw.findlaw.com/us-10th-circuit/1479501.html)

2

1

Metadata Fundamentals

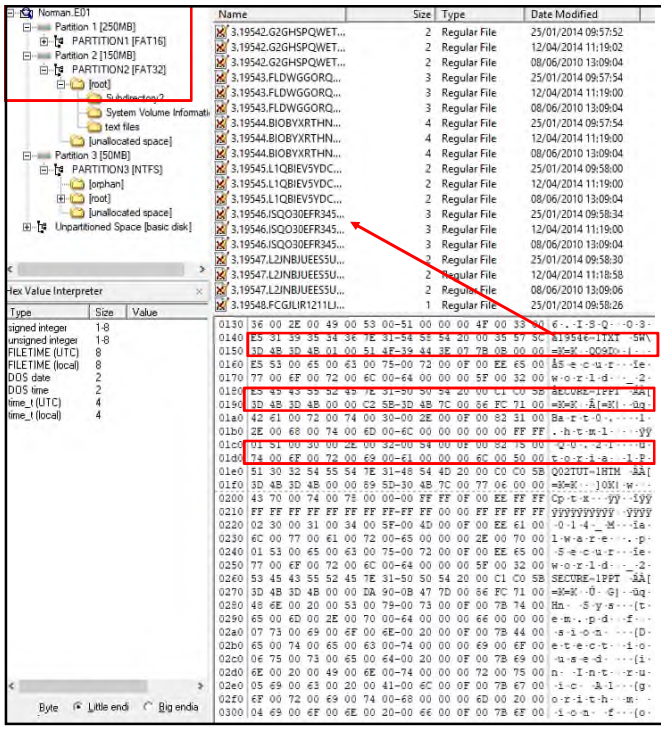
3



What is (μετά)Metadata?

- Printouts: You see everything, digital files contain “information about information”, “data about data”
- Metadata can be the following:
  - The date and time the file was created, accessed, modified, printed
  - The name of the author
  - Organisation name
  - File Size
  - Document version
- Generally, there are two types of metadata: System Metadata and Application metadata

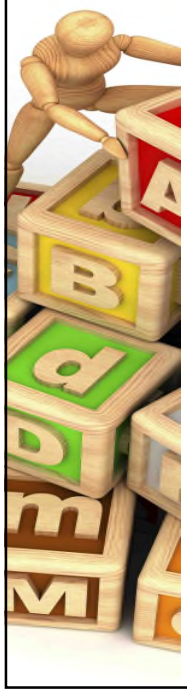
4



System Metadata

- Available to the operating system – stored in the directory table entry
- Meta information automatically created by the file system, when a file is created or copied/moved to a new location of the system or automatically updated by the system when edited to the existing location.
- Holds name, size, creation, modification and usage

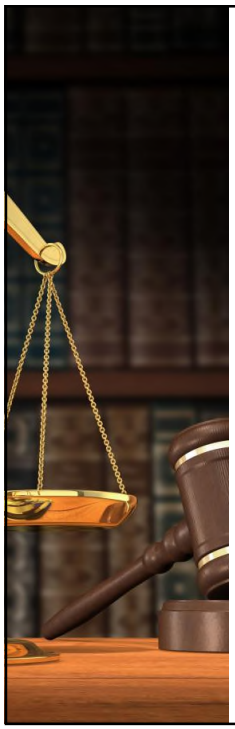
6



Application Metadata

- Available to applications that can read it
- Further information that describes the file and is embedded in the specific file
- Moves with the file when the file is moved or copied to a new location
- Holds information about the file such as tracked changes, document author, document version (if is a document file) macros, e-mail “to”, “from”, “subject” etc.

7

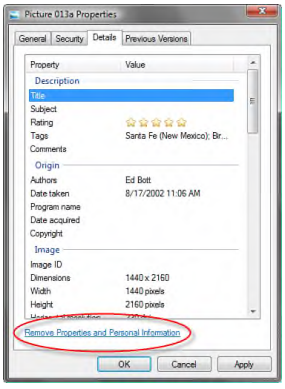


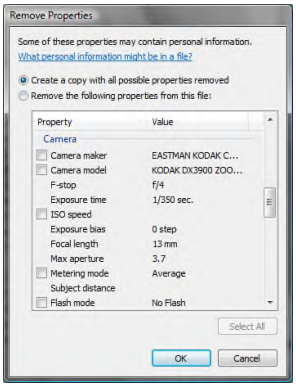
The problem with Metadata…

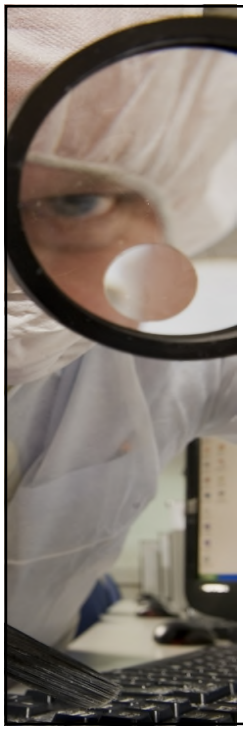
- Metadata does not tell us how and where files have come from
  - Dynamic routing of data in the cloud – how do we know where data was stored, is stored?
- Metadata can be forged easily
  - So… metadata is generally used as circumstantial evidence

Metadata Anti-Forensics

- Common Sense should be used when relying on metadata as a source of evidence
- Timestamps and other metadata can be easily 'forged' and even completely removed (Timestomp: http://www.offensive-security.com/metasploit-unleashed/TimeStomp)
- Tools
  - Windows Vista onwards incorporates a metadata removal utility
  - iScrub, Metadata Assistant, Workshare protect, Doc Scrubber, 3BClean etc are all freeware metadata modification tools







Challenging the Reliability of iPhone Geo-tags

"Geo-positional systems have gained in technological prominence over previous years. T…vhich, in some…e such applicat…on of an imag…r, this study, sh…ty of this dat…phic coord…efore …d (2012)

In this paper we showed that metadata can be altered beyond trace and therefore mustn't be relied upon as the sole source of evidence. In any case, no investigator should rely on a single source of evidence and the metadata should form part of the corroborating evidence

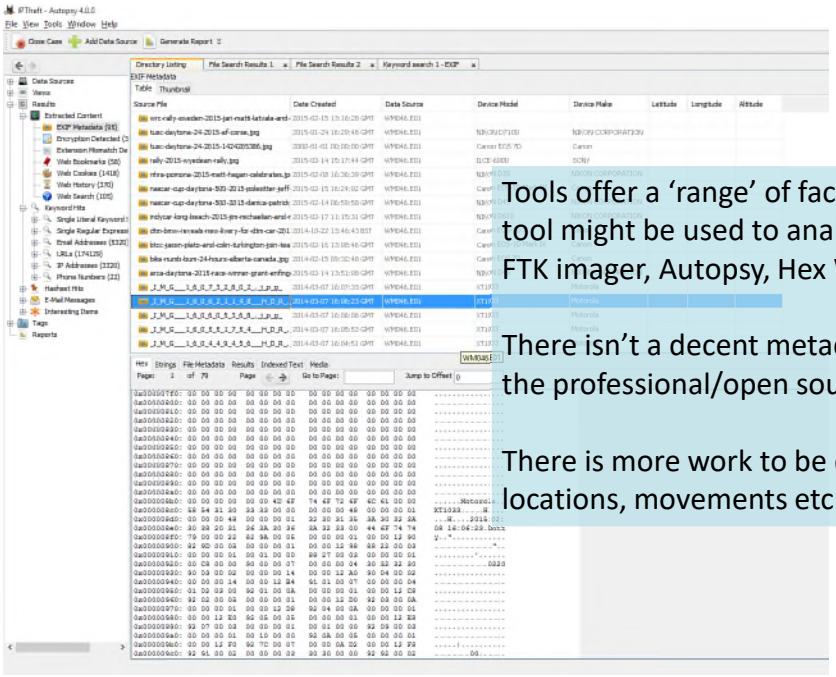
11

2

Accessing Metadata

2.1 Third party access
2.2 Forensic tool access
2.3 File system access

12

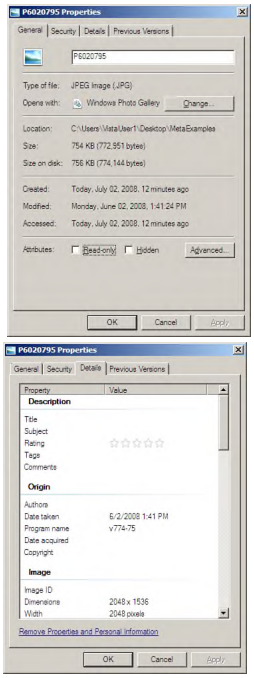


Forensic Tools and Metadata

Tools offer a 'range' of facilities and more than one tool might be used to analyse metadata including: FTK imager, Autopsy, Hex Workshop, Exif Pro.

There isn't a decent metadata forensic tool (none of the professional/open source tools are good enough)

There is more work to be done in terms of analysing locations, movements etc



3.1 Third party tool based access

- DESCRIPTION: title, subject, rating, tags, comments
- ORIGIN: Authors, Date Taken, program name, date acquired, copyright
- IMAGE: Image ID, Dimensions, width, height, horizontal resolution, vertical resolution, bit depth, compression, resolution unit, colour representation, compressed bit/pixels
- CAMERA: camera maker, camera model, F-stop, exposure time, ISO speed, exposure bias, focal length, max aperture, metering mode, subject distance, flash mode, flash energy, 35mm focal length
- ADVANCED PHOTO: lens maker, lens model, flash maker, flash model, camera serial number, contrast, brightness, light source, program mode, saturation, sharpness, white balance, photometric interpretation, digital zoom, EXIF version
- FILE: name, type, folder path, date created, date modified, size, attributes, offline availability, offline status, shared with, owner, and computer.

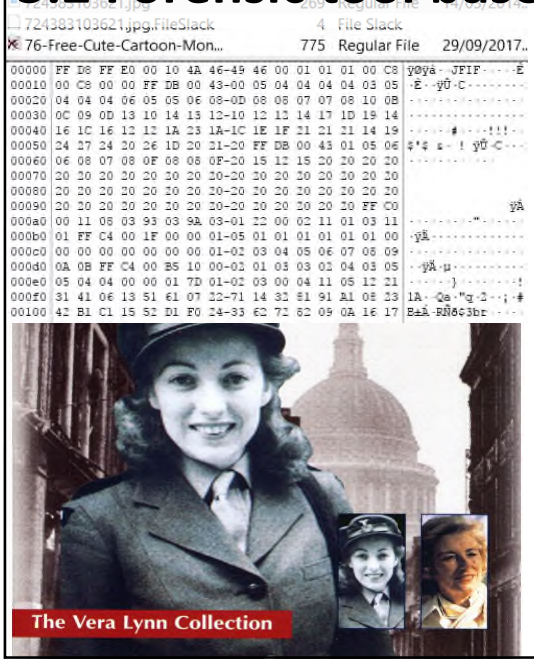
3.1 Third party tool based access

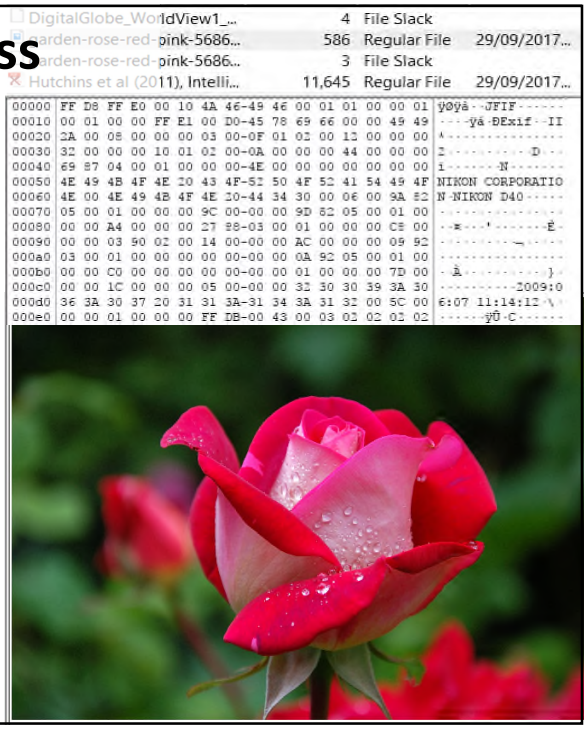
- MAIN INFORMATION: ImageDescription, Make, Model, Orientation, XResolution, YResolution, ResolutionUnit, Software, Date Time, YCbCrPositioning, ExifInfoOffset, PrintIM IFD
- PRINT IMAGE MATCHING INFO: Version, Unknown (0001, 0002. 0003, 0007, 0008, 000E, 0100, 0101, 0102, 0103, 0104, 0105, 0106, 0107, 0110) , contrast, Brightness, Saturation, Sharpness
- SUB INFORMATION: Exposure Time, FNumber, ExposureProgram, ISOSpeed Ratings, ExifVersion, DateTime Original, ExifTime Digitized, ComponentConfiguration, CompressedBitsPerPixel, ExposureBiasValue, MaxApertureValue, MeteringValue, LightSource, Flash
- FOCALLENGTH: MakerNote, UserComment, FlashPixVesrion, ColorSpace, ExifImageWidth, ExifImageHeight, ExifInteroperabilityOffset, FileSource, Scene Type, Custom Rendered, ExposureMode, WhiteBalance, DigitalZoomRatio, SceneCapture Type, GainControl, Contrast, Saturation, Sharpness
- VENDOR ORIGINAL INFORMATION: mode, quality, Macro Mode, digital Tele, Software Version, PicInfo, CameraID, One Touch WB
- EXIFR98: ExifR, Version, THUNMBAIN INFORMATION, compression, Xresolution, YResolution, ResolutionUnit, JPGEInterchangeFormat, JPEGInterchangeFormatLenght

http://www.takenet.or.jp/~ryuuji/minisoft/exifread/english/

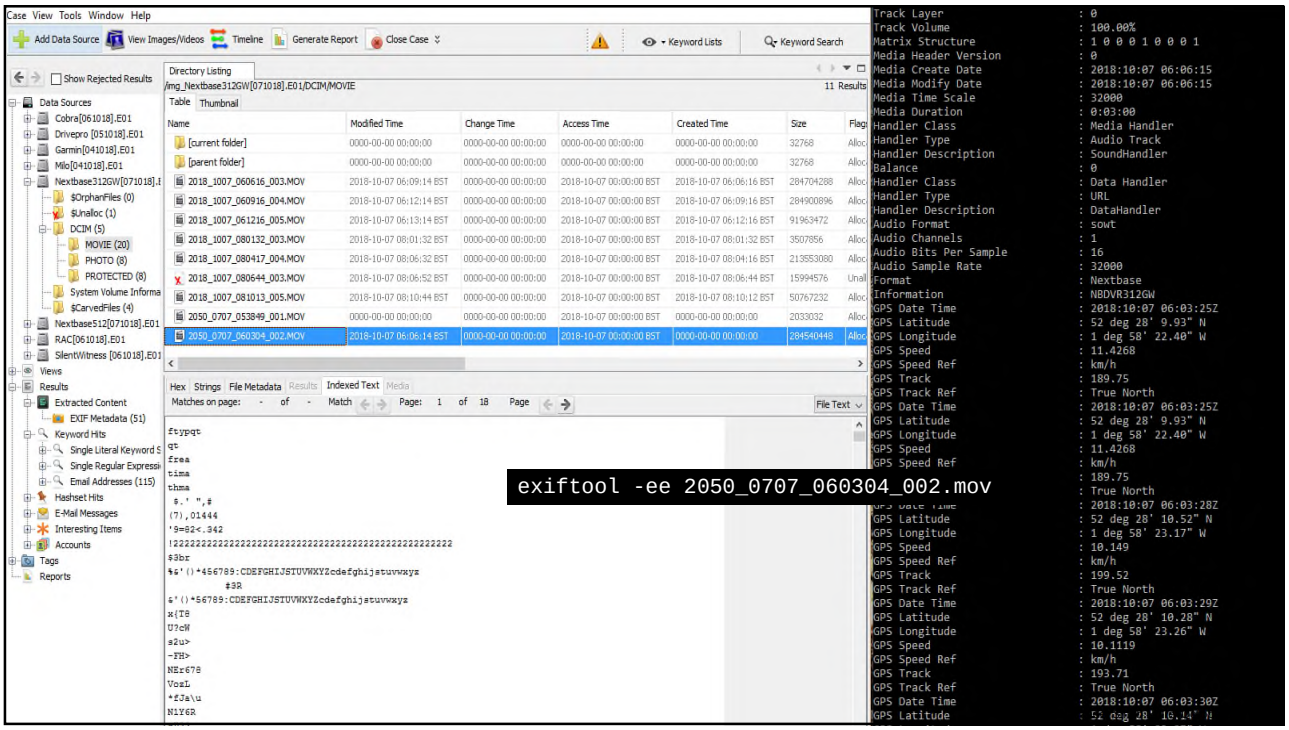
18

3.2 Forensic tool based access



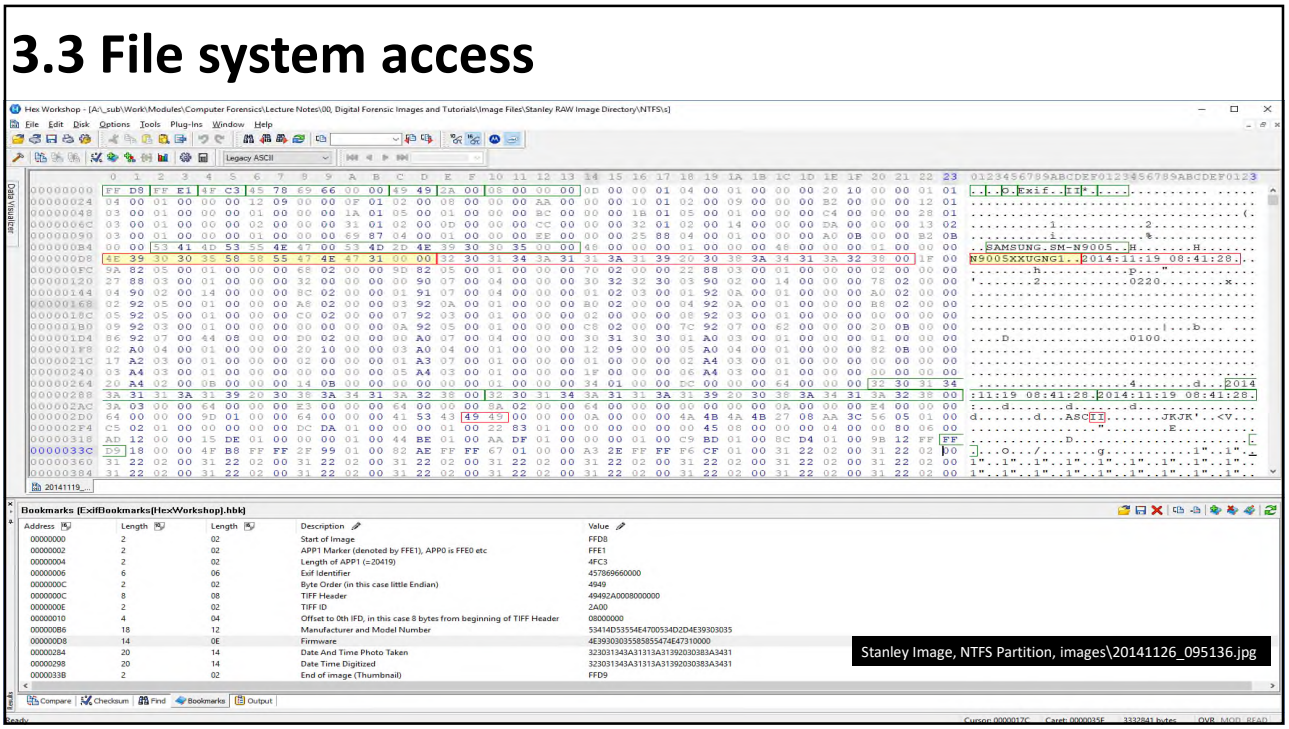


19



20

3.3 File system access



25

Further Reading

F. Buchholz and E. Spafford, "On the role of file system metadata in digital forensics," Digital Investigation, vol. 1, pp. 298-309, 2004.

Lallie, H.S., and Benford, D., (2011), 'Challenging the Reliability of iPhone Geo-Tags', The International Journal of Forensic Computer Science, 6 (1), 59-67.

A. Ames, C. Maltzahn, N. Bobb, E. L. Miller, S. A. Brandt, A. Neeman, et al., "Richer file system metadata using links and attributes," in Mass Storage Systems and Technologies, 2005. Proceedings. 22nd IEEE/13th NASA Goddard Conference on, 2005, pp. 49-60.

Buchholz and Spafford, (2004), *On the role of file system metadata in digital forensics, Digital Investigation, vol 1*

Agrawal et al., (2007), *A five-year study of file-system metadata, ACM Transactions on Storage, Volume 3 , Issue 3*

Garfinkel L. S., (2007), *Anti-Forensics: Techniques, detection and countermeasures, 2nd International Conference on i-Warfare and Security, Naval Postgraduate School*

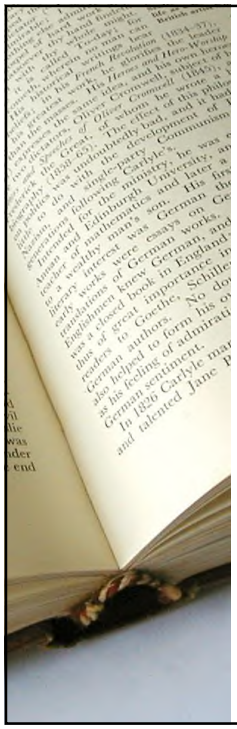
Ball C., (2005) *Beyond Data about Data: The Litigator's Guide to METADATA*, American Bar Association, available from: http://www.craigball.com/metadata.pdf

The Registry

Dr Harjinder Singh Lallie
Director of the Accredited Centre of Excellence in Cyber Security Education
Discipline group leader (cyber security)
HL@warwick.ac.uk

RATE MY PROFESSORS LinkedIn facebook

1



Lecture Goals

- What is the registry?
- How is it organised?
- How do we access the registry?
- How do we extract it for investigation?
- What are the common items of interest from a forensic viewpoint?

2

1

What is the registry, and how is it organised?

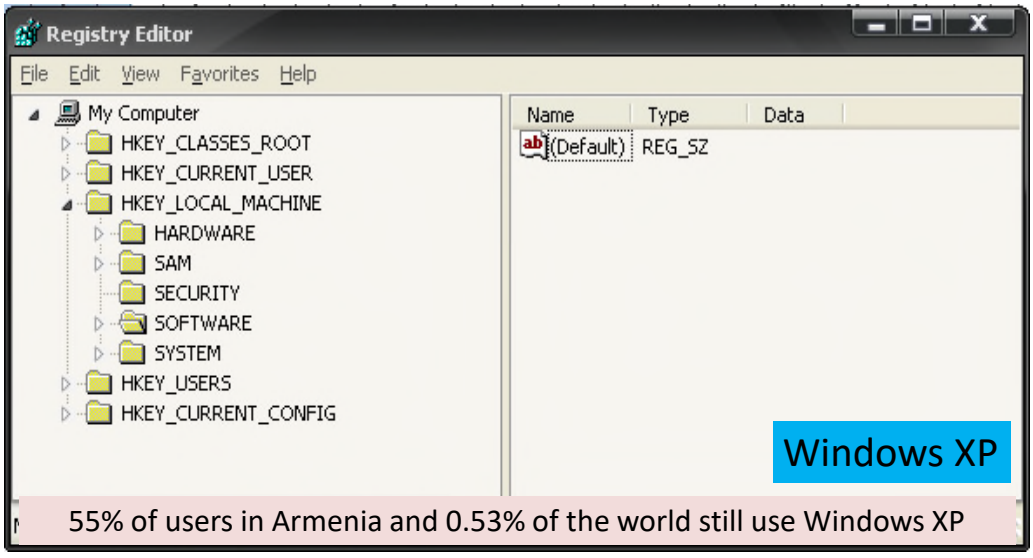
Introduction

"A central hierarchical database used in Microsoft Windows… to store information that is necessary to configure the system for one or more users, applications and hardware devices"

Microsoft, *Microsoft Computer Dictionary 5th Ed* (2002)

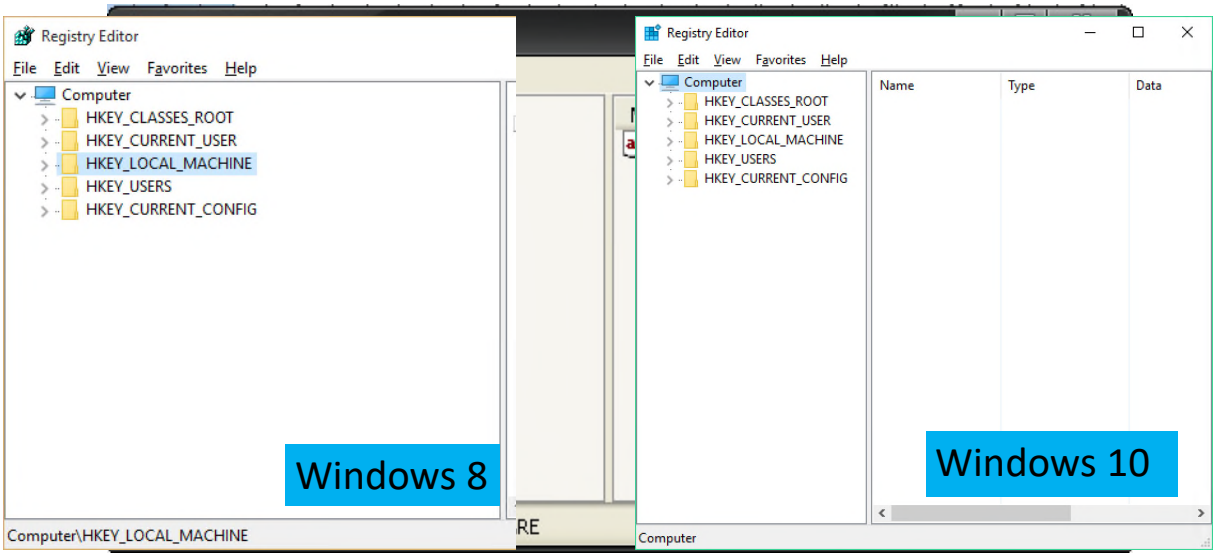
Contains: information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

Not much has changed in the registry



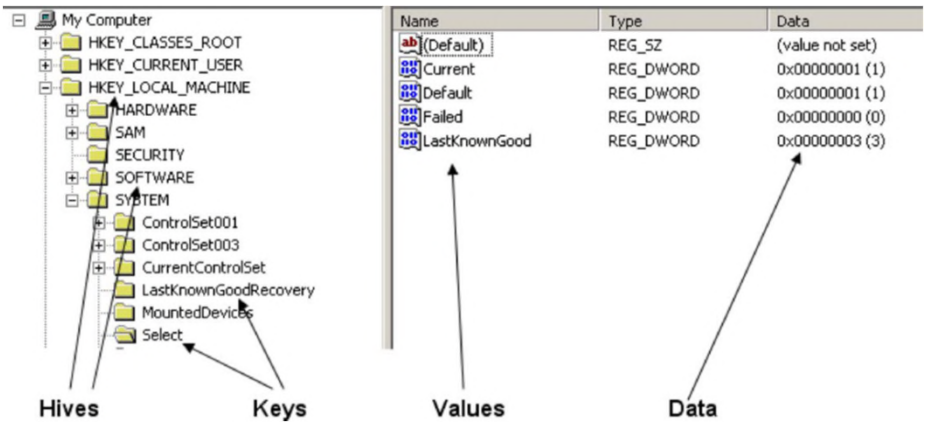
55% of users in Armenia and 0.53% of the world still use Windows XP

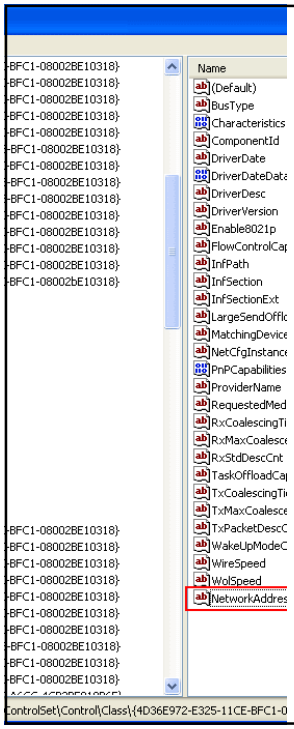
Not much has changed in the registry



The structure of the registry is quite complex, it is subdivided into what might be suggested to be illogical sections, furthermore, each hive is then saved in a backup file. Nobody really knows why Microsoft did it this way and what advantage it gives, but we have learned to live with it……

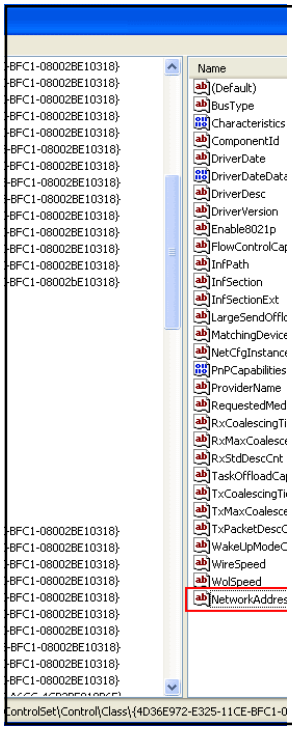
Structure





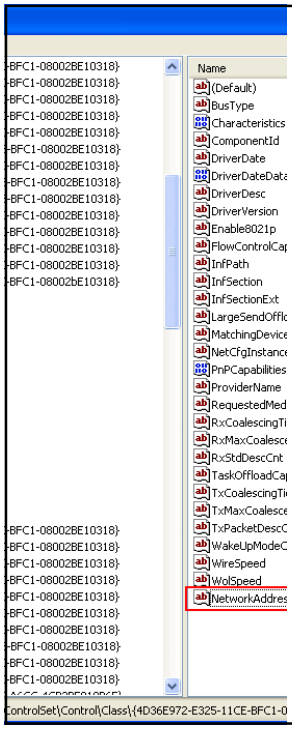
HKEY_CLASSES_ROOT (HKCR)

- This is used to manage object linking and embedding ensuring that the ‘correct’ application opens the file when selected
- E.g. an mp3 file, a pointer will be registered to the file as a windows sound object which can be handled by windows media player



Why is HKEY_CLASSES_ROOT important to an investigator?

- What app was the suspect using to create the {jpeg,pdf,other} files?
- What evidence is there of apps that might have been used, but now appear deleted?



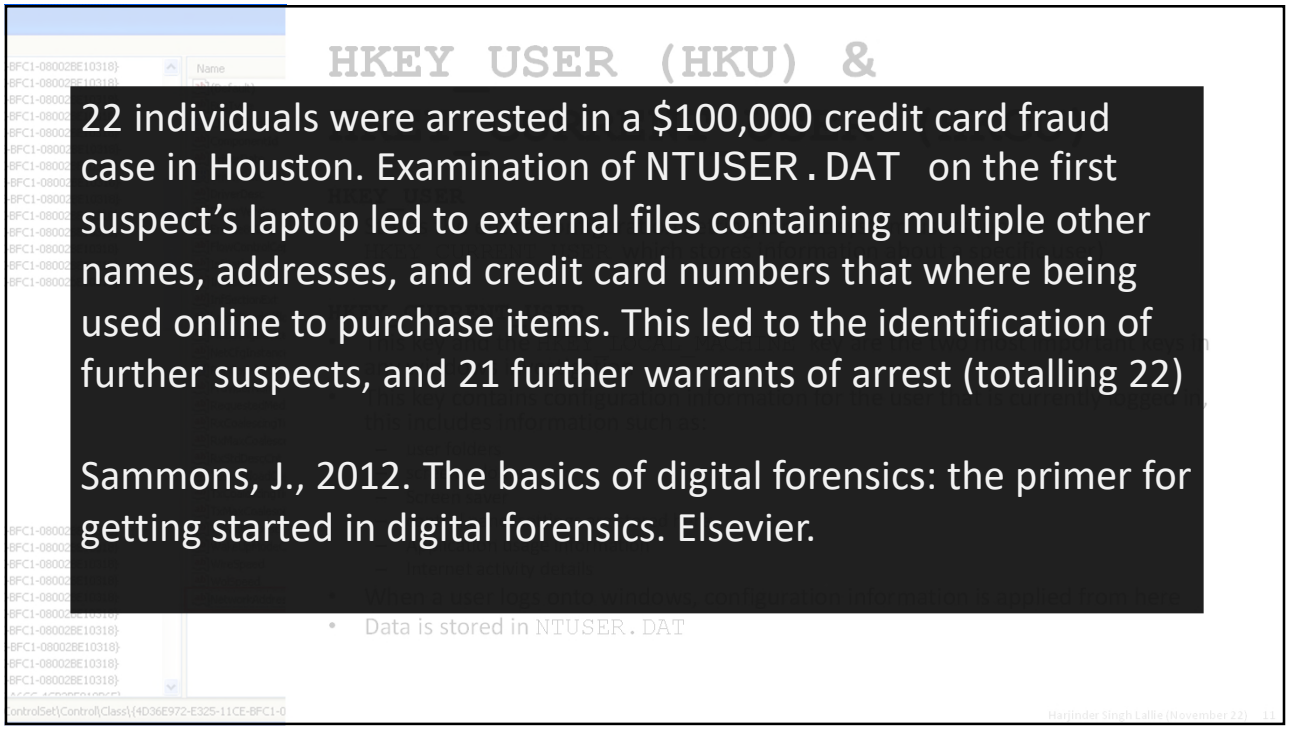
HKEY_USER (HKU) & HKEY_CURRENT_USER (HKCU)

HKEY_USER

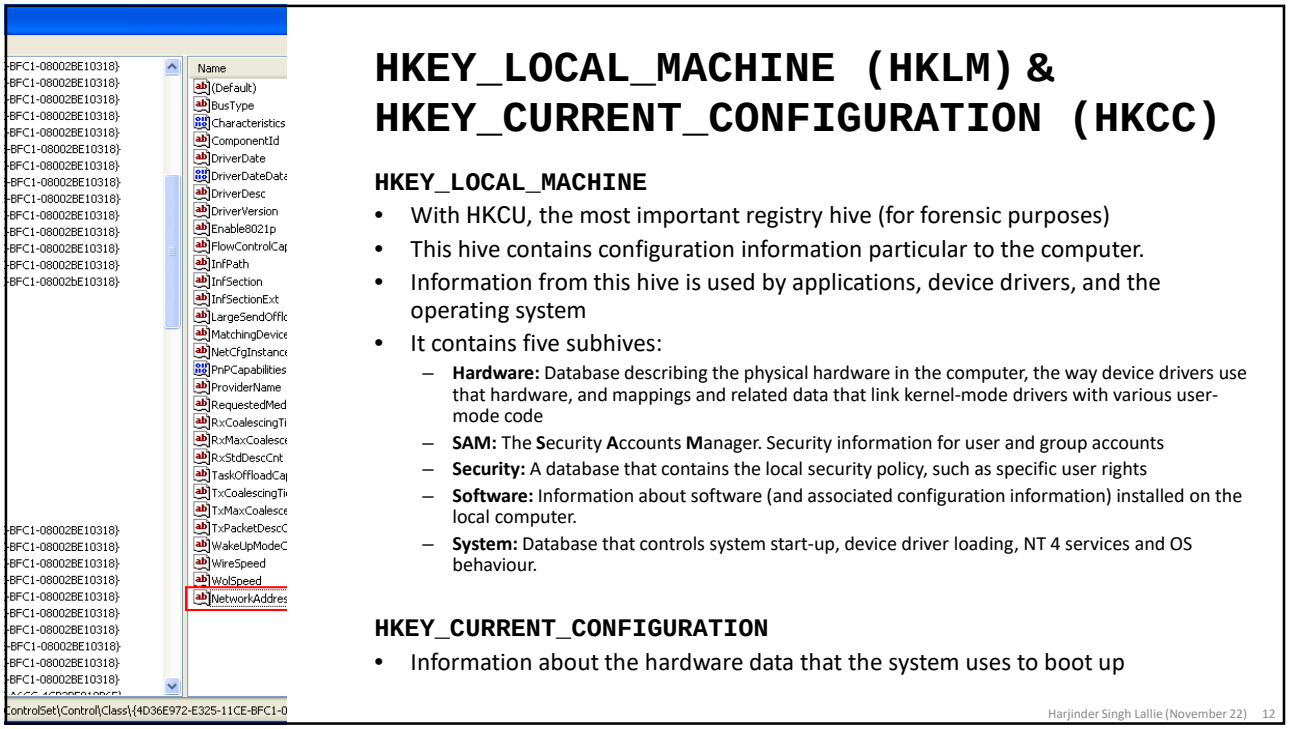
- Stores the entire configuration setting for ALL system users (unlike HKEY_CURRENT_USER which stores information about a specific user)

HKEY_CURRENT_USER

- This hive and the HKEY_LOCAL_MACHINE key are the two most important hives in any windows investigation
- This hive contains configuration information for the user that is currently logged in, this includes information such as:
  - user folders
  - screen colours
  - Screen saver
  - control panel settings are stored here
  - Application usage information
  - Internet activity details
- When a user logs onto windows, configuration information is applied from here
- Data is stored in NTUSER.DAT


HKEY USER (HKU) &
22 individuals were arrested in a $100,000 credit card fraud case in Houston. Examination of NTUSER.DAT on the first suspect's laptop led to external files containing multiple other names, addresses, and credit card numbers that where being used online to purchase items. This led to the identification of further suspects, and 21 further warrants of arrest (totalling 22)
Sammons, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.
Internet activity details
When a user logs onto windows, configuration information is applied from here
Data is stored in NTUSER.DAT

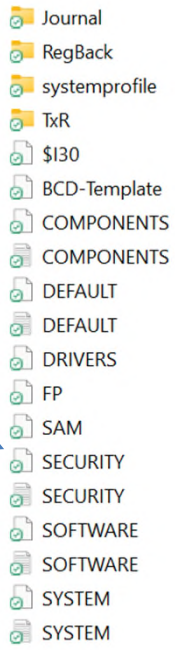
11


HKEY_LOCAL_MACHINE (HKLM) & HKEY_CURRENT_CONFIGURATION (HKCC)
HKEY_LOCAL_MACHINE
With HKCU, the most important registry hive (for forensic purposes)
This hive contains configuration information particular to the computer.
Information from this hive is used by applications, device drivers, and the operating system
It contains five subhives:
Hardware: Database describing the physical hardware in the computer, the way device drivers use that hardware, and mappings and related data that link kernel-mode drivers with various user-mode code
SAM: The Security Accounts Manager. Security information for user and group accounts
Security: A database that contains the local security policy, such as specific user rights
Software: Information about software (and associated configuration information) installed on the local computer.
System: Database that controls system start-up, device driver loading, NT 4 services and OS behaviour.
HKEY_CURRENT_CONFIGURATION
Information about the hardware data that the system uses to boot up
Harjinder Singh Lallie (November 22) 12

12

Two methods of accessing the registry

- Live : `regedit.exe`
- Offline
  - `DEFAULT (HKEY_USERS\DEFAULT)`
  - `SAM (HKEY_LOCAL_MACHINE\SAM)`
  - `SECURITY (HKEY_LOCAL_MACHINE\Security)`
  - `SOFTWARE (HKEY_LOCAL_MACHINE\Software)`
  - `SYSTEM (HKEY_LOCAL_MACHINE\System)`



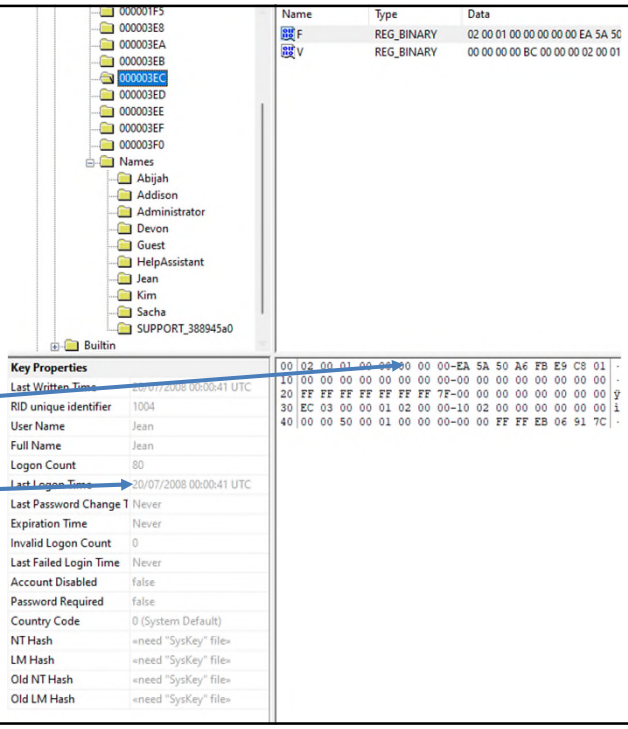
Tools

Tools

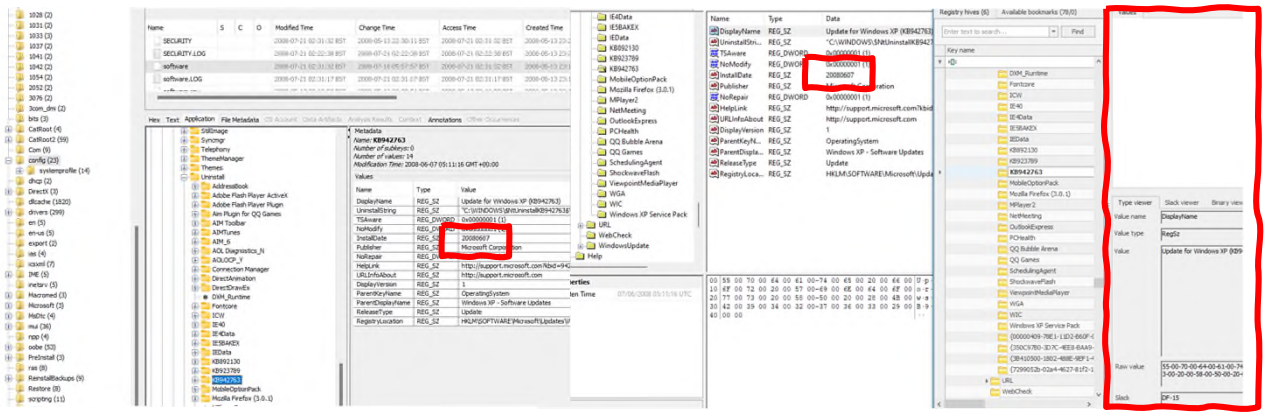
- Autopsy 4.19.3
- Accessdata Registry Viewer
- Registry Explorer
- KAPE

The tools convert the binary into something you can comprehend

Not all the tools present all the data in the same way.



Not all the tools present all the data in the same way.



Autopsy 14.19.3 | Accessdata Registry Viewer | Registry Explorer 2.0

Where can I find the (most important from a forensic viewpoint) registry files?

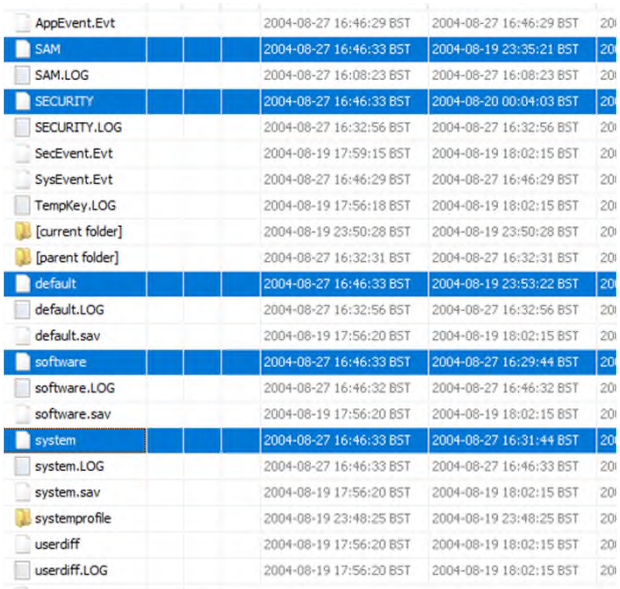
Registry Hive	Location	Files
HKLM\SAM	`windows\system32\config\sam`	Sam, sam.log, sam.sav
HKLM\Security	`windows\system32\config\security`	Security, security.log, security.sav
HKLM\Software	`windows\system32\config\software`	Software, software.log, software.sav
HKLM\System	`windows\system32\config\system`	System, system.alt, system.log, system.sav
HKCU	`\Users\Username*`	System, system.alt, system.log,system.sav, NTuser.dat, NTuser.dat.log
HKU\Default	`windows\system32\config\default`	Default, default.log, default.sav

`* C:\Documents and Settings\{username}` Windows XP

This is not the entire registry, some files are not included in my list. Furthermore, some hives are volatile, they are created when Windows is operating, removed when shutdown

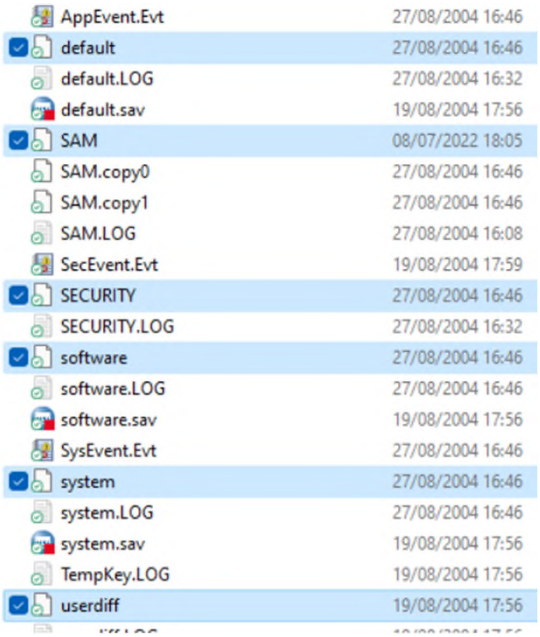
Task 1: extracting the registry

1. Create a directory called **`GregSchardtRegistries`**
2. Open the `GregSchardt` image in FTK imager
3. Navigate to **`Partition1\noname[NTFS]\root\Windows\system32\config`**
4. Select the files highlighted in the image opposite, select Export Files
5. Save to the **`GregSchardtRegistries`** directory
6. Now go to each user directory in **`\Documents and Settings`**. Save each **`NTUSER.DAT`** into a directory with a corresponding name. i.e. the MrEvil **`NTUSER.DAT`** into a directory within the directory above called `MrEvil`.



Task 2: Opening the registry files in RegExplorer

1. Open *Registry Explorer*
2. Select File→Load Hive
3. Point to the **`GregSchardtRegistries`** directory
4. Open all the files in this directory
5. Save the project as **`GregSchardt`**



2

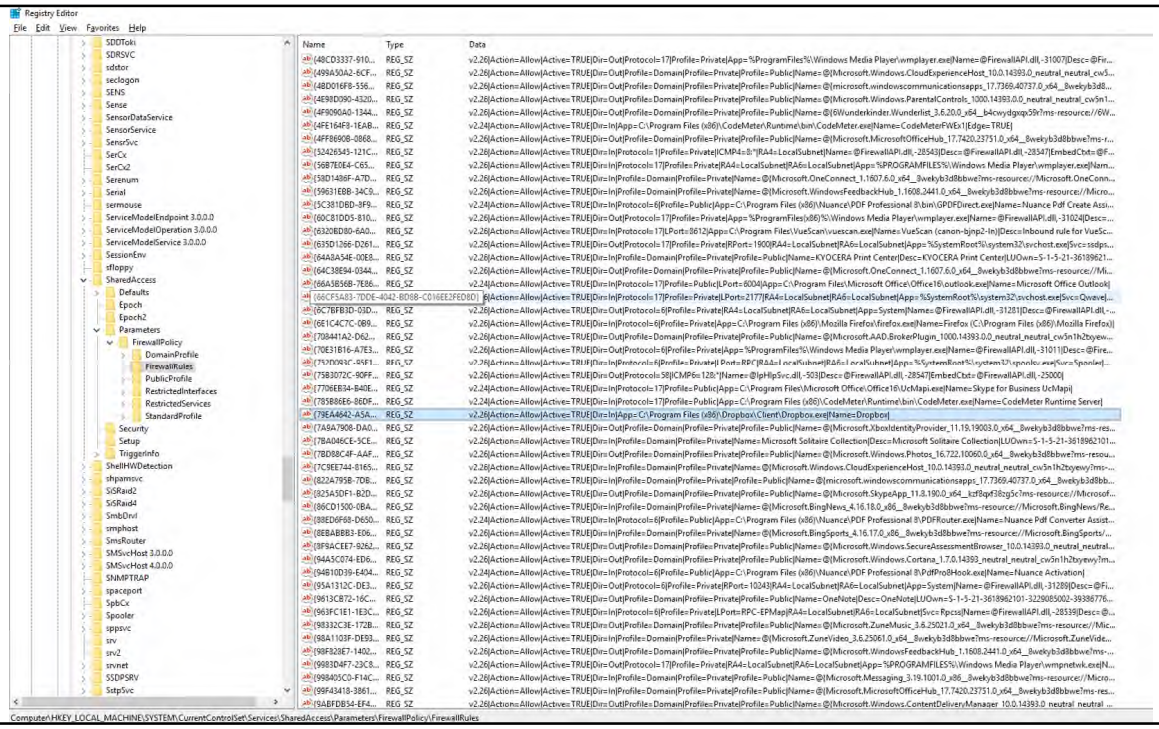
What are the common items of interest from a forensic viewpoint?

The 12 most important registry items of forensic interest

1. Operating System
   a. What is the operating system (inc build)?
   b. When was the operating system installed?
   c. Who (which user) installed it?
2. Names and Accounts
   a. What is the name of the computer
   b. Who (appears to have) has an account on this system?
   c. When did they last log in?
   d. When did each of them last shutdown the computer?
3. What was the timezone the computer was set to?
4. What USB devices have been accessed on this system?
5. What WiFi networks have been accessed on this system?
6. What programmes have been installed on this system? Is there evidence of programmes having been uninstalled (see my paper)?
7. Recent activity
   a. What were the most recently accessed files, programmes, and sites?

Other items of forensic interest

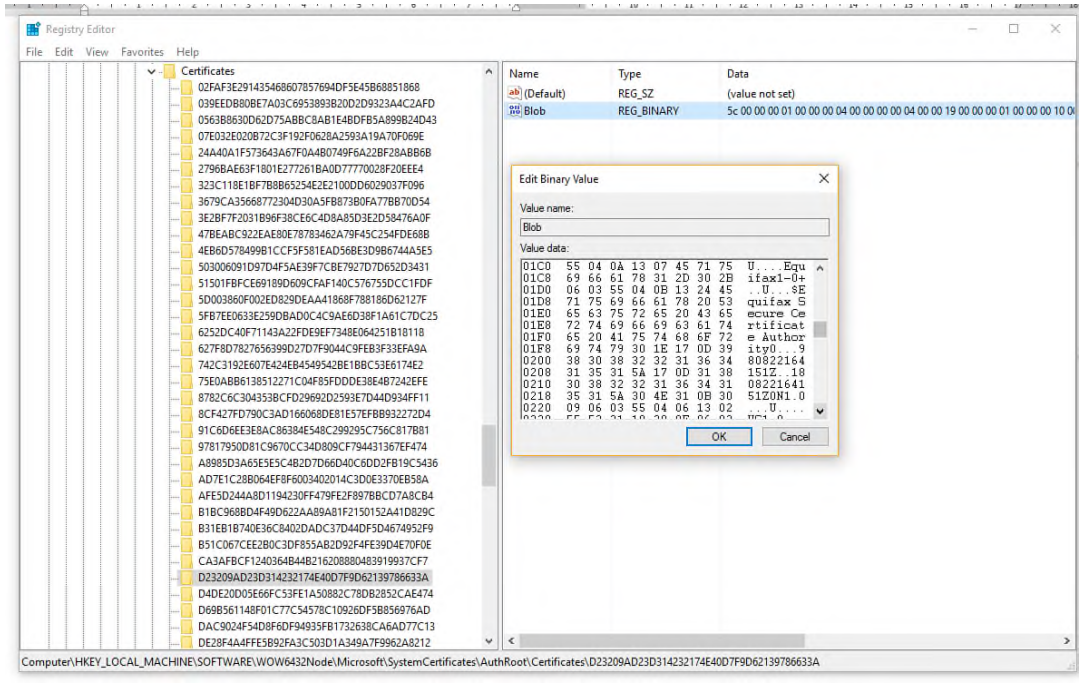
Item	Forensic Significance
Firewall and Virus Protection	For systems using Windows “Security Center” there are Registry settings which can indicate whether any of the firewall or anti-virus protection has been switched off. This includes the ability to check which ports may have been deliberately opened to incoming network traffic. Other security application vendors (e.g. Symantec) also use the Registry but employ their own key structures.
Installed software	There is a SOFTWARE key containing various subkeys defining different aspects of installed applications. There is also a useful Uninstall key which can identify applications **even after they have been de-installed** and the code overwritten. This can therefore provide evidence that an application was installed on the machine at a point in the past.
IP Addresses	In the case of machines which use DHCP, it is possible to determine what IP addresses have been used in order to carry out network analyses. For example, it might be useful to know if the current machine had a specific IP address at a particular time.
Logged-in User History	User account details of **the last logged-in user** can be obtained. This can be useful in determining the identity of users accessing the machine.
Remote Desktop	It may be useful to know whether intruders could have had access to the current machine using the Remote Desktop facility. There is a Registry entry under a “Terminal Server” subkey which can be used for this purpose.
Security Identifiers	Security Identifiers for Windows users and groups are found in various parts of the Registry. For example, under the HKEY_LOCAL_MACHINE Hive, there are records corresponding to each interactive login providing clues as to who may have accessed the machine. As shown in Section 3 later, there are also details of user accounts and groups present under the SAM and SECURITY subkeys.
Terms of Use	Anson and Bunting (2007) point out that if “**terms of use**” are accepted by a user at login then this could provide information implying a level of user consent which could be useful in court. Typically, this type of feature is controlled through a banner window which needs to be acknowledged by the user clicking on an “I Accept” button or similar. The Registry can contain details of the presence of this type of feature.



Other items of forensic interest

Item	Forensic Significance
Storage Devices	There are a number of registry entries associated with storage devices. This includes currently mounted disks, and media which may have been connected to the machine in the past. For example, it is possible to determine whether a USB stick of a particular type was connected to the machine.
Email	Certain information related to user email can be found, such as the email application currently set for the user, and number of unread emails.
Executed Software	There are various Registry locations which provide details of recently executed applications. This is a source from which to determine whether programs have been run or, if a program has been de-installed and the Registry cleaned up (see “Installed software” Item in HKEY_LOCAL_MACHINE), it can be used to show that an application must have been present in the past.
Documents Recently Accessed	There are keys which provide lists of files recently accessed, especially through Microsoft applications such as Word. This includes files which may have been deleted since their last access.
Web Sites Visited	A list of recently visited URLs can be obtained, for example, by inspecting keys related to a browser application such as Internet Explorer. These values can however usually be removed from the Registry using the standard Internet Explorer deletion options.

23



24

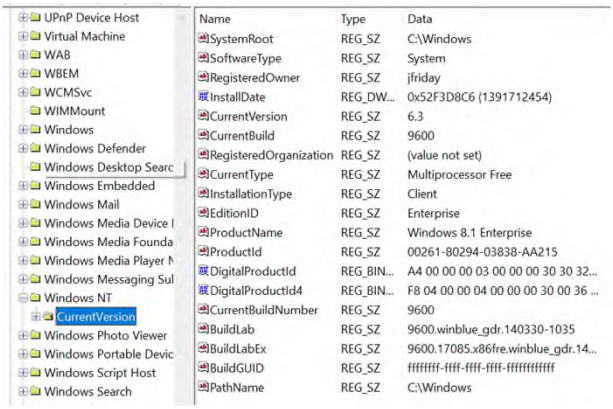
Operating System

Employee returns corporate laptop after quitting role. Laptop has been 'wiped clean', "I've lost all the recent corporate designs". Laptop investigated to reveal employee had installed a (nearly) fresh install of Windows 10, most likely removed sensitive files before hand with an intention not to return them.

Windows update did it, https://www.tetradefense.com/digital-forensics-services/forensic-case-files-windows-update-did-it/

Operating System

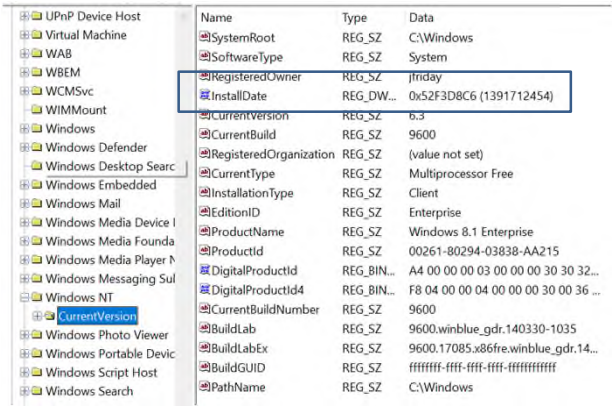
1. What is the operating system
2. Which build?
3. When was it installed?
4. Who is the registered owner?



SOFTWARE\Microsoft\Windows NT\CurrentVersion

When was the operating system installed?

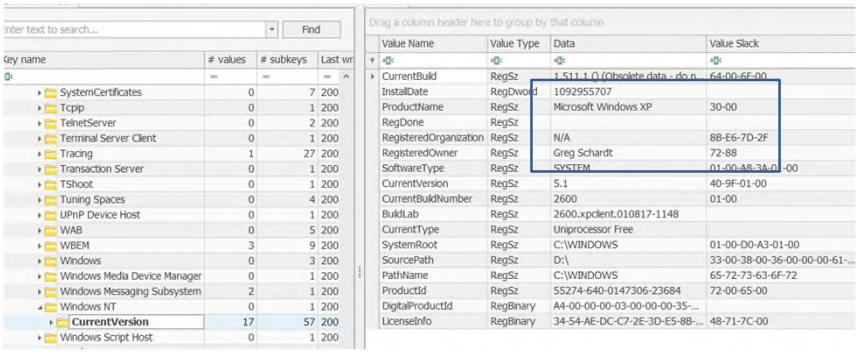
- A Unix timestamp - a way to track time as a running total of seconds from the Unix Epoch on January 1st, 1970 at UTC
- 1391712454 can be converted to give Thu, 06 Feb 2014 18:47:34 GMT



https://www.rapidtables.com/convert/number/hex-to-decimal.html
https://www.onlineconversion.com/unix_time.htm

- What is Mr Evil's operating system, when was it installed, who is the registered owner?
- The date (1092955707) can be converted to Thu, 19 Aug 2004 22:48:27 GMT

Task

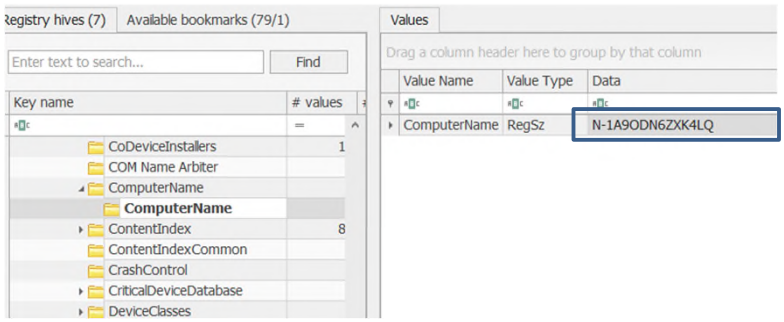


https://www.onlineconversion.com/unix_time.htm

Computer Name

What is the name of this computer?

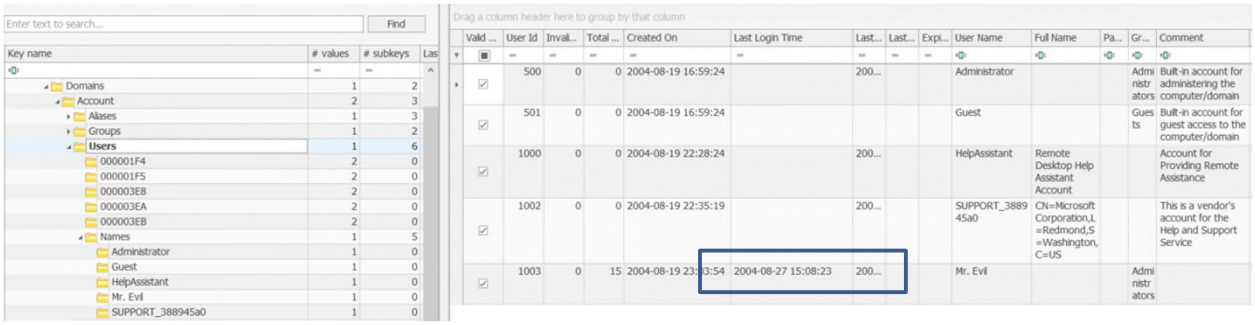
The computer name is the name by which it is recognised on the network and in communications



`HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ComputerName` (Windows XP+)

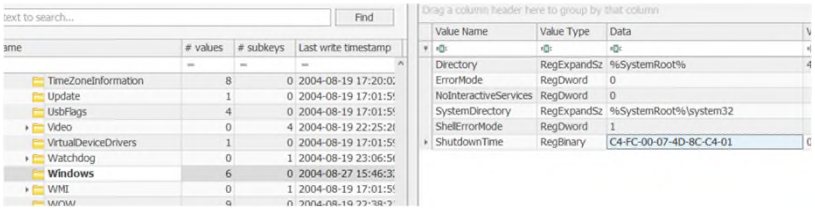
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ComputerName\ActiveComputerName` (Windows 7+)

When did a user last log in?

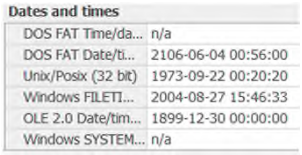


SAM/Domains/Account/Users/Names/

When was this system shutdown?



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows

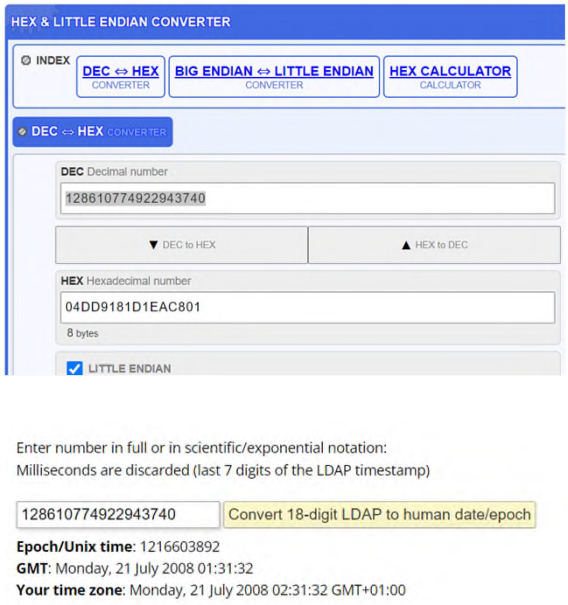


https://www.save-editor.com/tools/wse_hex.html
https://www.epochconverter.com/ldap

When was this system shutdown?

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows

Convert the Unix timestamp (hex) to decimal, 04DD9181D1EAC801 = 128610774922943740

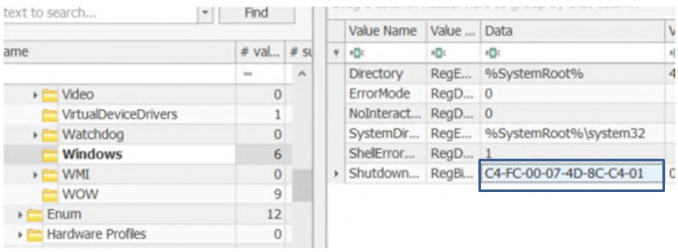


https://www.save-editor.com/tools/wse_hex.html
https://www.epochconverter.com/ldap

Task

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows

When was Mr. Evil's system shutdown?



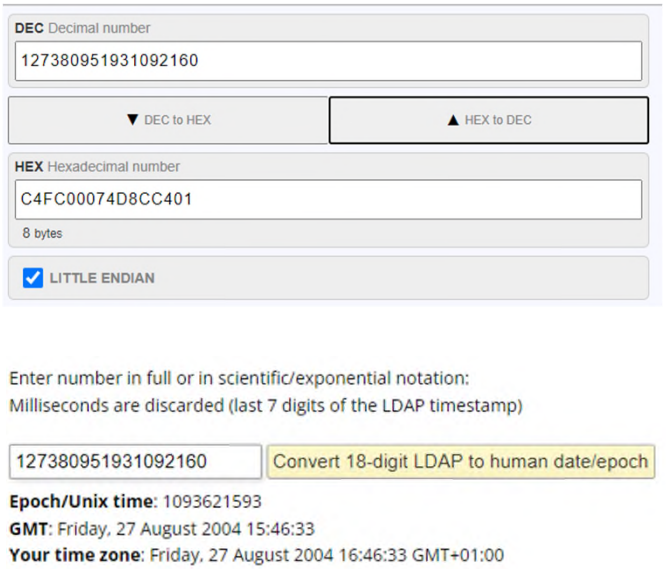
https://www.save-editor.com/tools/wse_hex.html
https://www.epochconverter.com/ldap

Task

When was Mr. Evil's system shutdown?

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows

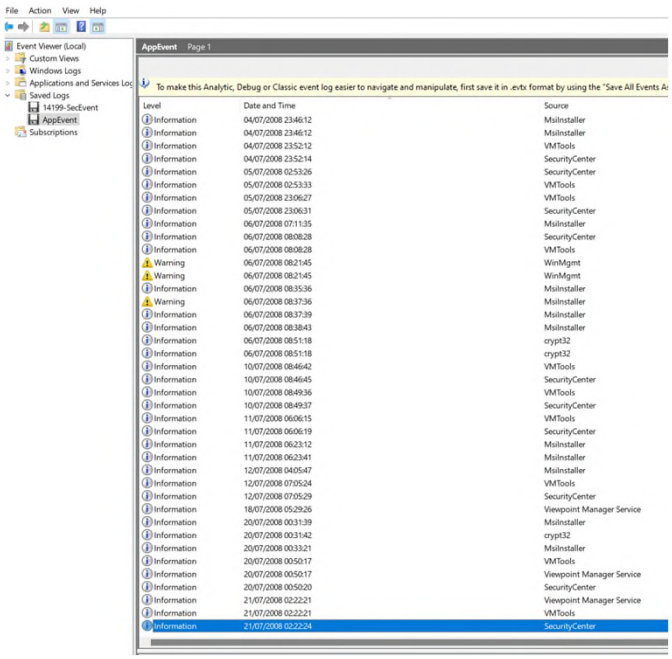
Convert the Unix timestamp (hex) to decimal, C4FC00074D8CC401 = 127380951931092160



https://www.save-editor.com/tools/wse_hex.html
https://www.epochconverter.com/ldap

Last known operated time?

- Appevent, open in windows event viewer.
- Last date in the Appevent is the last possible saved event. This could be newer than the last shutdown because the shutdown is graceful, this is not.



Lastwrite

- Additionally, each registry entry has a ‘lastwrite’ value associated with it. This value is 10,000 times the number of seconds from 00:00 January 1st 1601 till the date and time the value was last modified. This is of course dependant upon the system clock on the PC. This of course can be of great importance as it can identify the last time a particular programme or file was accessed to a very precise time. Any offset caused by discrepancies between the actual date and time and the date and time according to the computer must of course be taken into account.

Programs

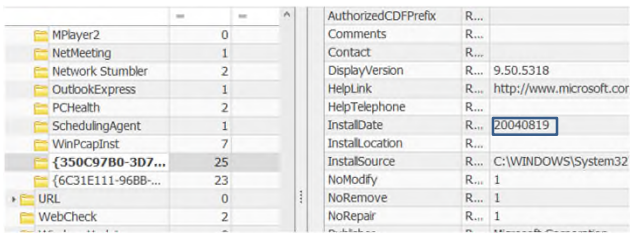
Programs

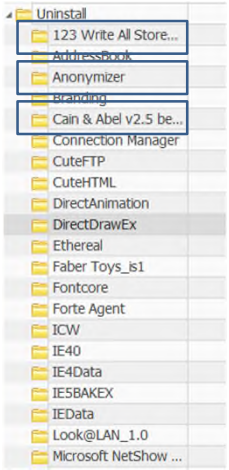
- What programs have been installed on this system?
- What programs were recently run?
- When were they run?
- Is there evidence of programs having been uninstalled?

What is installed?

SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

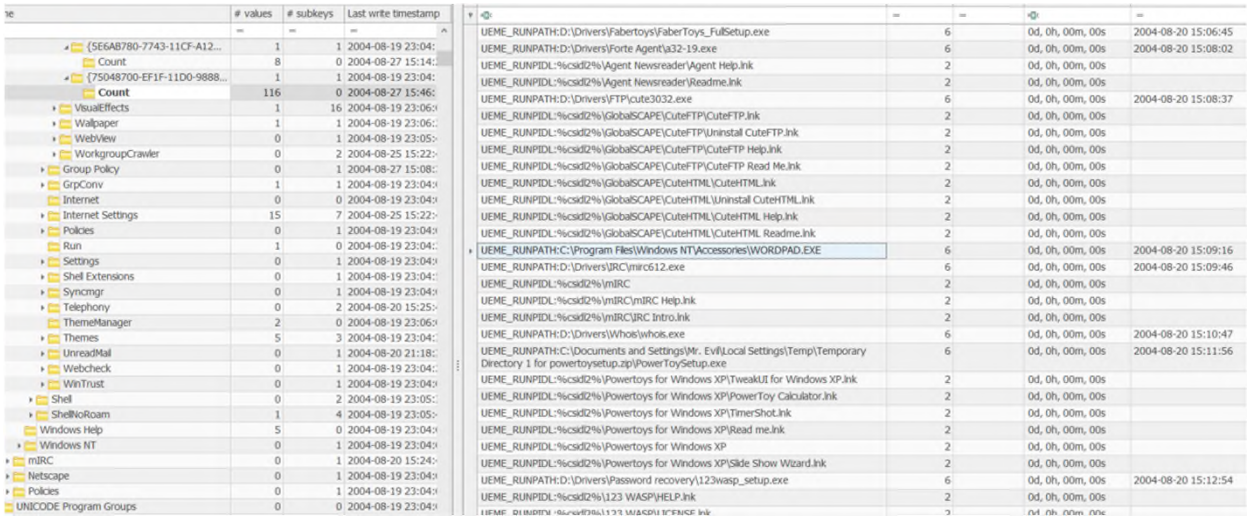
- **Task:** Mr. Evil has been accused of stealing passwords at cafes, are there any tools installed which might help with this?
- **Task:** When was: {350C97B0-3D7C-4EE8-BAA9-00BCB3D54227} installed?





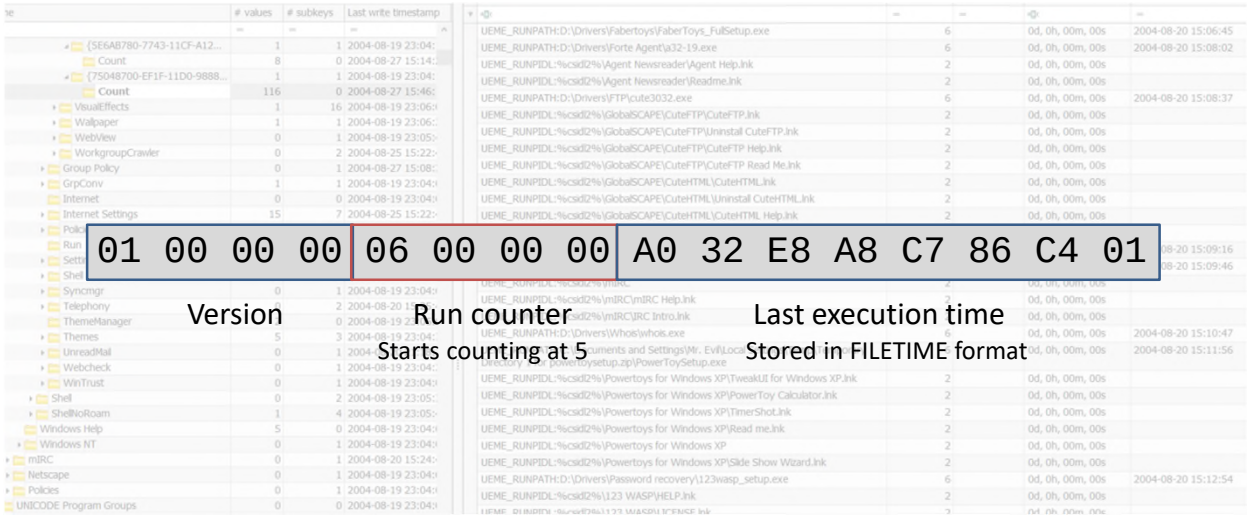
What programs have been run and when?

NTUSER.DAT: Software\Microsoft\ Windows\CurrentVersion\Explorer\UserAssist



What programs have been run and when?

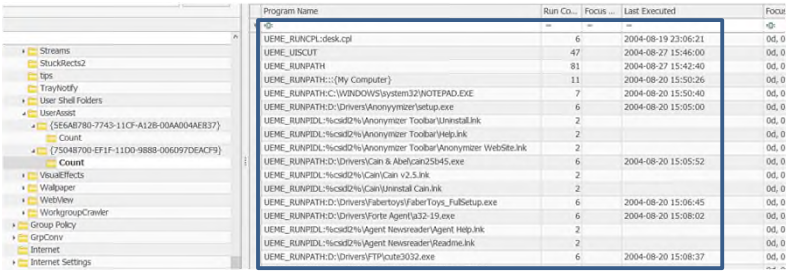
NTUSER.DAT: Software\Microsoft\ Windows\CurrentVersion\Explorer\UserAssist



What programs have been run and when?

NTUSER.DAT: Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

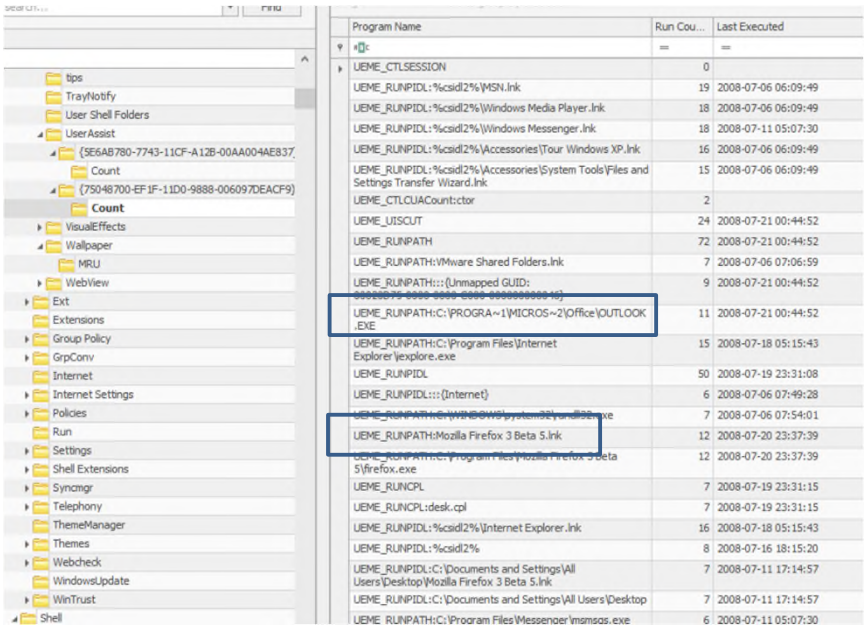
Task: Did Mr. Evil execute any of the programs identified earlier? If so when, how many times?



Program Name	Run Co...	Focus ...	Last Executed	Focus
UEME_RUNCPL:desk.cpl	6		2004-08-19 23:06:21	0d, 0
UEME_UISCUT	47		2004-08-27 15:46:00	0d, 0
UEME_RUNPATH	81		2004-08-27 15:42:40	0d, 0
UEME_RUNPATH:::{My Computer}	11		2004-08-20 15:50:26	0d, 0
UEME_RUNPATH:C:\WINDOWS\system32\NOTEPAD.EXE	7		2004-08-20 15:50:40	0d, 0
UEME_RUNPATH:D:\Drivers\Anonymizer\setup.exe	6		2004-08-20 15:05:00	0d, 0
UEME_RUNPIDL:%csidl2%\Anonymizer Toolbar\Uninstall.lnk	2			0d, 0
UEME_RUNPIDL:%csidl2%\Anonymizer Toolbar\Help.lnk	2			0d, 0
UEME_RUNPIDL:%csidl2%\Anonymizer Toolbar\Anonymizer WebSite.lnk	2			0d, 0
UEME_RUNPATH:D:\Drivers\Cain & Abel\cain25b45.exe	6		2004-08-20 15:05:52	0d, 0
UEME_RUNPIDL:%csidl2%\Cain\Cain v2.5.lnk	2			0d, 0
UEME_RUNPIDL:%csidl2%\Cain\Uninstall Cain.lnk	2			0d, 0
UEME_RUNPATH:D:\Drivers\Fabertoys\FaberToys_FullSetup.exe	6		2004-08-20 15:06:45	0d, 0
UEME_RUNPATH:D:\Drivers\Forte Agent\a32-19.exe	6		2004-08-20 15:08:02	0d, 0
UEME_RUNPIDL:%csidl2%\Agent Newsreader\Agent Help.lnk	2			0d, 0
UEME_RUNPIDL:%csidl2%\Agent Newsreader\Readme.lnk	2			0d, 0
UEME_RUNPATH:D:\Drivers\FTP\cute3032.exe	6		2004-08-20 15:08:37	0d, 0

What programs have been run and when?

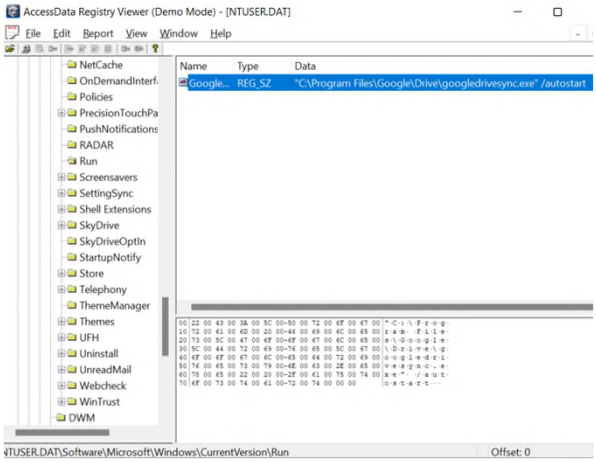
- {5E6AB780-7743-11CF-A12B-00AA004AE837} is for Microsoft's Internet toolbar
- and {75048700-EF1F-11D0-9888-006097DEACF9} is the Active Desktop.



Program Name	Run Cou...	Last Executed
UEME_CTLSESSION	0	
UEME_RUNPIDL:%csidl2%\MSN.lnk	19	2008-07-06 06:09:49
UEME_RUNPIDL:%csidl2%\Windows Media Player.lnk	18	2008-07-06 06:09:49
UEME_RUNPIDL:%csidl2%\Windows Messenger.lnk	18	2008-07-11 05:07:30
UEME_RUNPIDL:%csidl2%\Accessories\Tour Windows XP.lnk	16	2008-07-06 06:09:49
UEME_RUNPIDL:%csidl2%\Accessories\System Tools\Files and Settings Transfer Wizard.lnk	15	2008-07-06 06:09:49
UEME_CTLCUACount:ctor	2	
UEME_UISCUT	24	2008-07-21 00:44:52
UEME_RUNPATH	72	2008-07-21 00:44:52
UEME_RUNPATH:VMware Shared Folders.lnk	7	2008-07-06 07:06:59
UEME_RUNPATH:::{Unmapped GUID:	9	2008-07-21 00:44:52
UEME_RUNPATH:C:\PROGRA~1\MICROS~2\Office\OUTLOOK.EXE	11	2008-07-21 00:44:52
UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe	15	2008-07-18 05:15:43
UEME_RUNPIDL	50	2008-07-19 23:31:08
UEME_RUNPIDL:::{Internet}	6	2008-07-06 07:49:28
	7	2008-07-06 07:54:01
UEME_RUNPATH:Mozilla Firefox 3 Beta 5.lnk	12	2008-07-20 23:37:39
	12	2008-07-20 23:37:39
UEME_RUNCPL	7	2008-07-19 23:31:15
UEME_RUNCPL:desk.cpl	7	2008-07-19 23:31:15
UEME_RUNPIDL:%csidl2%\Internet Explorer.lnk	16	2008-07-18 05:15:43
UEME_RUNPIDL:%csidl2%	8	2008-07-16 18:15:20
UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop\Mozilla Firefox 3 Beta 5.lnk	7	2008-07-11 17:14:57
UEME_RUNPIDL:C:\Documents and Settings\All Users\Desktop	7	2008-07-11 17:14:57
UEME_RUNPATH:C:\Program Files\Messenger\msmsgs.exe	6	2008-07-11 05:07:30

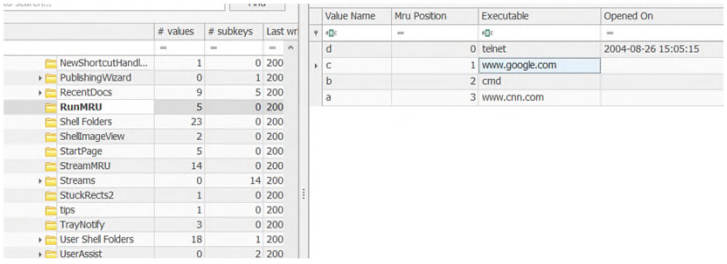
What programs have been set to autorun

- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run**
- **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run**
- **SOFTWARE\Microsoft\Windows\CurrentVersion\Run**



MRU (Most Recently Used List)

- The list of commands executed using the `Start→Run` function in Windows
- Found in: **HKEY_CURRENT_USER\software\microsoft\windows\currentVersion\explorer\RunMRU**
- **TASK:** What were the last few, if any, most recently used applications/website through the Start→Run function in Mr Evil's computer?

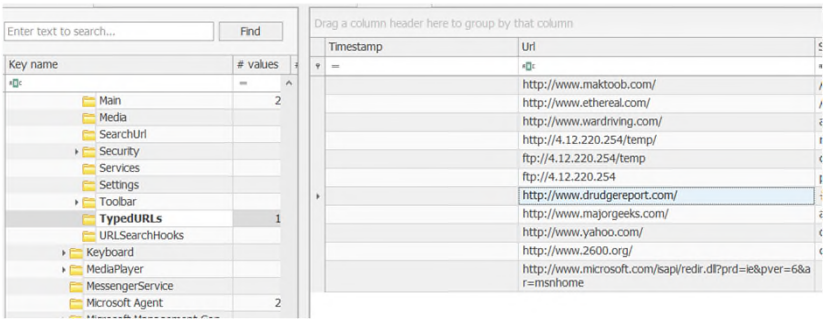


Trucker smuggling 3,300 pounds of marijuana questioned and arrested after weight of truck inconsistent with bill of lading. Bill of lading ticket found to be forged by software recently deleted from hard disk.

US v Diaz https://infosecusa.com/us-v-diaz-marijuana-possession-new-mexico

Internet Explorer

Internet explorer: information related to use of internet explorer are stored, URL last accessed are stored in the following key:



HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\typedURLs

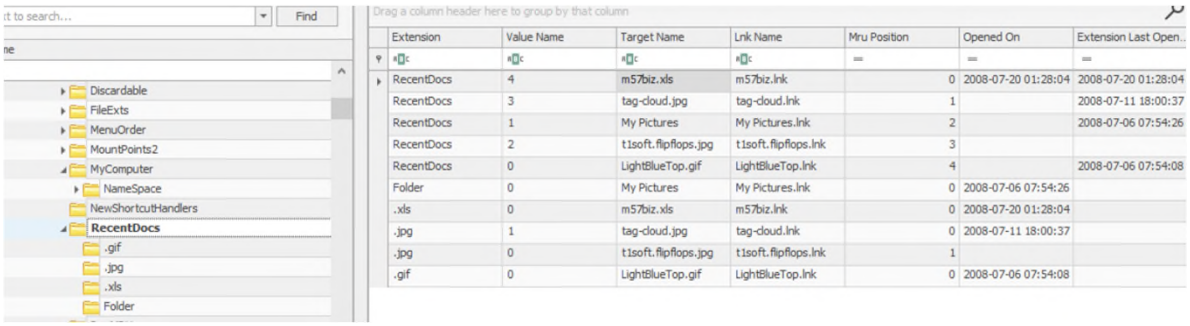
Other MRU places of interest*

Search Files	`Software\Microsoft\Search Assistant\ACMru\5603`
Internet Search Assistant	`Software\Microsoft\Search Assistant\ACMru\5001`
Printers, Computers and People	`Software\Microsoft\Search Assistant\ACMru\5647`
XP Start Menu - Recent	`Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`
R. Desktop - Connect	`Software\Microsoft\Terminal Server Client\Default [MRUnumber]`

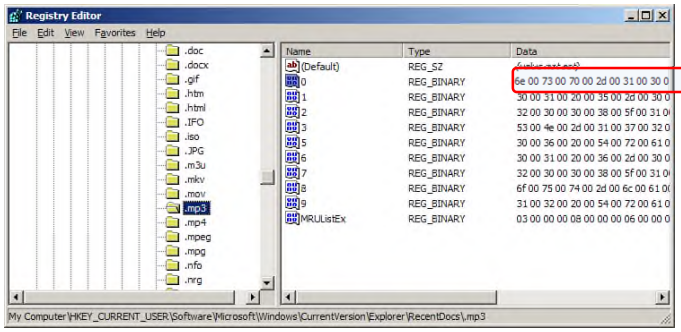
*Some are created when used.

What documents have been opened

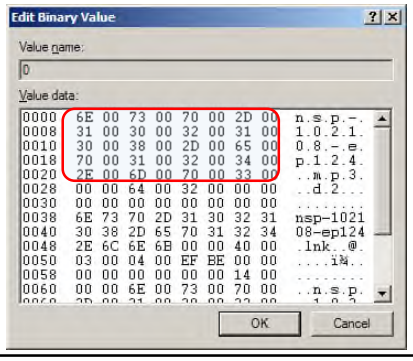
`Jean\NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs`



Connecting registry evidence, an example



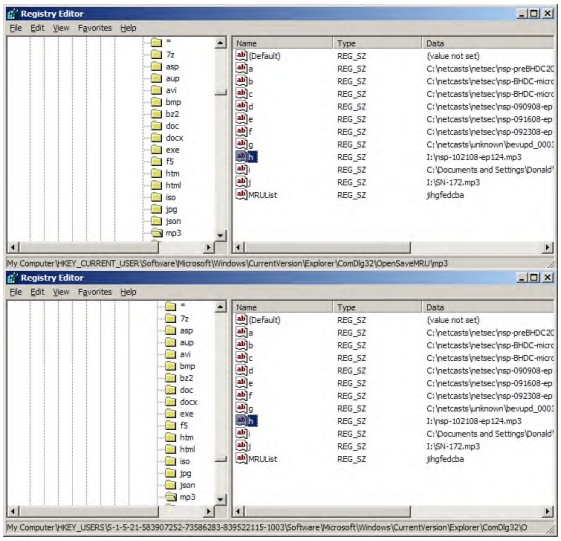
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.mp3



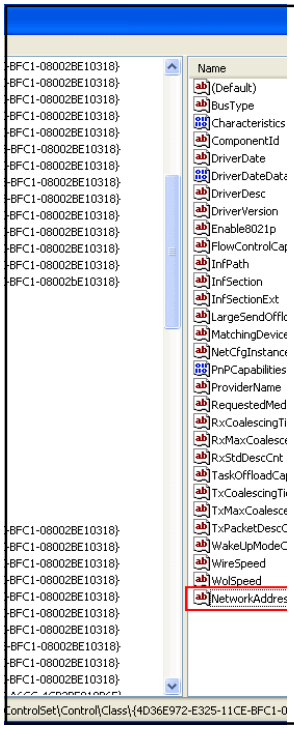
MRU Example

- Often we need to connect evidence together to get a bigger picture.
- This registry location shows a recently accessed mp3 file
- The second figure shows the hexadecimal data with its ascii equivalent. From this it can be seen that the user has listened to an MP3 titled ‘nsp-102108-ep124.mp3’. A quick search on the internet reveals that this MP3 file is a netcast called “network security podcast”.

MRU Example



If the file identified was one that the investigator had an interest in, then searching for the file on the drive would identify its location, however, searching for the string 'nsp-102108' within the registry turns up 2 results.



MRU Example

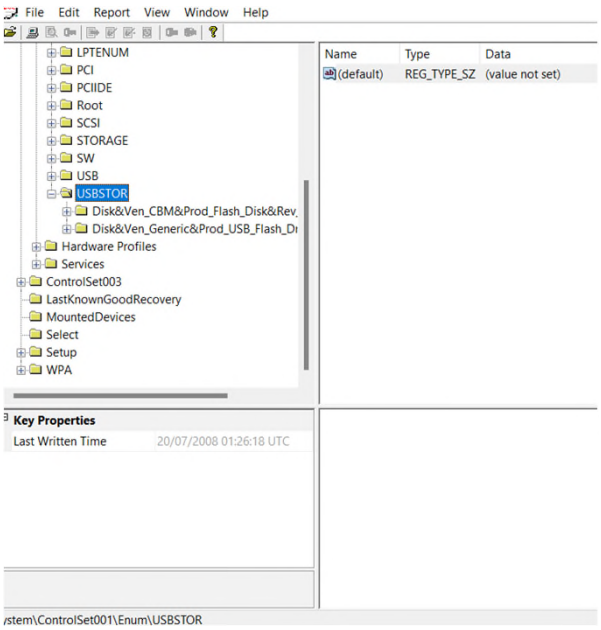
- It is a good job that the search was performed within the registry in this case, as the drive letter 'I' refers to a removable USB drive which is currently not attached to the system. This information can be found in the registry in other locations.
- The two results show the same list of MP3 files recently played. The difference between these two lists is that one comes from the 'Current User' branch of the registry, whilst the other comes from a 'User' branch of the registry. As can be seen, the two lists are identical, indicating that whilst there may be more than one user account on the system, either one is rarely used or the other user does not play any MP3 files.
- The MRUList at the bottom of the right hand pane in the diagrams above, shows the order in which these last 10 MP3s were played. Thus the file nsp-102108-ep124.mp3 was the third from last file played on this system

What USB devices have been accessed on this system?

- **SOFTWARE\Microsoft\Windows Portable Devices\Devices**
- **HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\ENUM\USBSTOR**

<Windows 7+ :

- **System\ControlSet001\Enum\USB**



What USB devices have

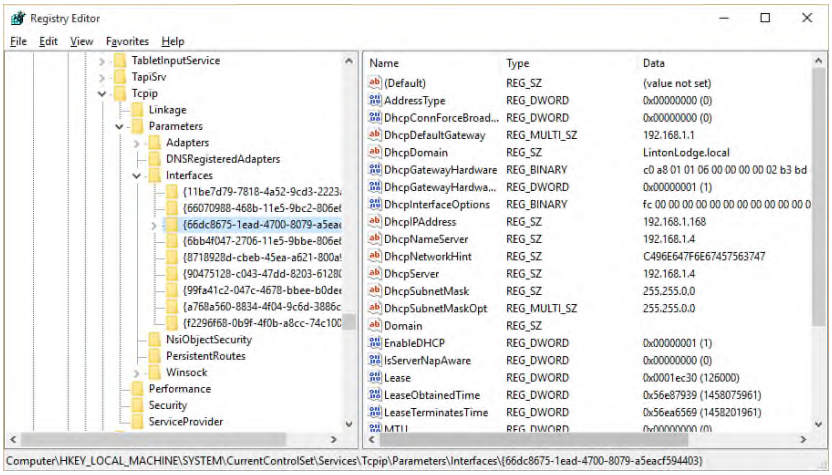
Illegal images of children. A laptop and two hard disks recovered following a raid on a hotel. Two suspects arrested. In interview, suspect A claims laptop is his, but the offending hard disks containing illegal images are not his and have never been connected to laptop. Registry analysis (USBSTOR) showed hard disks had been connected to the laptop.

Sammons, J., 2012. The basics of digital forensics: the primer for getting started in digital forensics. Elsevier.

Wireless SSIDs

Which WiFi networks has this device connected with?

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters\Interfaces



Encrypting sensitive data in the registry

- In recognising that there may be some ‘sensitive’ data in the registry, Microsoft used a version of the Caesar Cipher known as ROT-13 to protect the sensitive data.
- Unfortunately this is easy to decipher as each letter is rotated around the wheel of the alphabet by 13 places and is therefore very easy to decipher.
- To expedite the process, free programmes such as the one found at www.rot13.com are available
- Other more complex forms of encryption are used to protect more sensitive data, such as saved passwords for internet explorer and outlook express. In this case, the website addresses are listed in plaintext, but the passwords are encrypted
- Again, there are utilities available to easily decrypt these passwords (e.g. RockXP)

Hiding empty registry space

- Morgan, T.D., 2008 identified that by defragmenting the registry, hidden data can be removed
- Registry gets fragmented over time
- Tools can be used to 'fix' the registry. These tools can hide evidence.
  - Auslogics registry defrag
- Process:

1. Repair the registry.
2. Clean the registry.
3. Defragment the registry.
4. Fill the free space with many keys and small values, preferably over a period of time

(Morgan, T.D., 2008, Recovering deleted data from the Windows Registry. *Digital Investigations*, 5, pp.33-41)

Further Reading

- Lallie H., Briggs P., (2010), Windows 7 Registry Forensic Evidence Created by Three Popular BitTorrent Clients, The International Journal of Digital Forensics & Incident Response (March 2011)
- Wong, L.W., Edith Cowan University, 2006, Forensic Analysis Of The Windows Registry [Online]. http://www.forensicfocus.com/downloads/forensic-analysis-windows-registry.pdf
- Morgan, T.D., 2008, Recovering deleted data from the Windows Registry. *Digital Investigations*, 5, pp.33-41
- Assignment submission by Lawrence Maxwell (2009)

Logs

- C:\windows\system32\config\sam.log might have log1, log2

- Backupfile
- C:\windows\system32\config\regback

Dashcam Forensics

Lallie, H.S., 2020. Dashcam forensics: a preliminary analysis of 7 dashcam devices. *Forensic Science International: Digital Investigation*, *33*, p.200910.

1

2

1

Dashcams in court

3

Background

- Dashcam usage increasing rapidly in the UK.
  - 2015, 9% of drivers were using dashcams
  - 2016: 15%
  - 2017: 17%
  - 2018: 27%
  - ~2026, may become a standard fixture
- Nottingham Police recorded 211,598 dashcam records over a three year period leading up to 2017.

Method of accepting Evidence	**Police constabulary**
Nextbase site	Warwickshire, West Mercia, West Midlands, Wiltshire
Police site	Avon and Somerset, Cheshire, Dyfed-Powys, Essex, Gwent, Hampshire, Metropolitan Police Service, Norfolk, North Wales, South Wales, Suffolk, Surrey, Sussex, Thames Valley
Intention to activate	Bedfordshire, Cambridgeshire, City of London, Cleveland, Derbyshire, Devon and Cornwall, Durham, Greater Manchester, Hertfordshire, Humberside, Lincolnshire, Merseyside, Northamptonshire, Northumbria, Nottinghamshire, South Yorkshire, Staffordshire
Not accepting online submission	Cumbria, Dorset, Gloucestershire, Kent, Lancashire, North Yorkshire, West Yorkshire

4

Dashcam evidence is appearing in an increasing number of court cases

There are no tools or guidelines on how to investigate, rendering the risk of miscarriage

Case, court and date	Summary
Scott vs Harris, 2010, United States Supreme Court [18]	Deputy Scott accused of using excessive force to stop claimants car after a car chase. Dashcam footage upheld Deputy Scott's case
Regina vs Luke Whitchard, 2015 [65]	Third party dashcam captures Whitchard dangerously overtaking cars on a bend.
Regina Vs Stocks, 2015, Mold and Caernarfon Crown Court [63]	Dashcam footage captures James Stocks recklessly overtaking other drivers - closely missing a van driver which is forced off the road
Regina v Collins 2017/05113/A2 113 EWCA, 2018 Old Bailey [70]	Patrick Collin's dashcam captures Collins knocking over and killing Selwyn Clarke and a conversation admitting the accident moments later
German supreme court, 2018 [53]	Plaintiff argues video footage of him crossing a red light breaches privacy laws. Supreme court rules against the plaintiff.
Regina vs Marc Hyland, 2018, Northallerton Magistrates [44]	Marc Hayland overtakes a series of vehicles waiting to turn
Regina vs Ryan Haffenden, 2017, Brighton Magistrates Court [24]	Haffenden overtakes vehicles on a single carriageway - narrowly missing a pedestrian and avoiding collision with oncoming traffic.
Regina vs Andrew Williams EWCA Crim 1886 WL 03777362 (Court of Appeal Criminal Division), 2018, Nottingham Magistrates Court [42]	Andrew Williams was drunk and driving in speeds in excess of 120mph Vehicle veered onto the hard shoulder and almost crashed into a motorcyclist.
Regina v Lewes Marcin Dariusz Purlis, EWCA Crim 1134, 2017, (Criminal Division) [15]	Purlis convicted of robbery. Dashcam footage captured by a third party was instrumental as was the evidence by a facial mapping expert
Gajdamowicz v First Glasgow Ltd, 2017, All Scotland Sheriff Court [52]	Cyclist - Gajdamowicz knocked over by a bus attempting to overtake. Bus camera shows Gajdamowicz wearing headphones and not indicating prior to moving into the path of the bus. Case ruled in favour of First Glasgow.
Shane Mullen and Gez Bennett, 2015, Warwick Crown Court [8]	Assailants carjacked a car and were captured in the car's dashcam admitting the theft.
Regina v Welsby (Ian), 2017, Hull Crown Court [19]	Third party dashcam shows Ian Welsby clipping a motorcyclist Colin Walker as he (Ian) cut a corner as he turned into a side street.
McIntosh v Harman [2018] EWHC 726 (QB), 2018, Queen's Bench Division [61]	Police dashcam records PC Susan McIntosh knocked down by Barry Harman as she (Susan) was interviewing members of the public.
Regina v Thompson (Chloe May) EWCA Crim 1291 Court of Appeal [23], 2017, Maidstone Crown Court	Chloe Thompson crashed into the back of a vehicle at 80-88mph killing a grandmother. Dashcam footage captured on a car travelling in the same direction.
Harvey Schofield, 2018, Chester Magistrates' Court, [12]	Harvey Schofield undertook a tipper truck and pulled out into the path of a vehicle causing him to slam his brakes.

The term *third party* is used in the table to refer to a person or persons not directly involved in the incident.

5

Guardian, the (2021), *Wayne Couzens timeline: footage shows movements before murdering Sarah Everard*, available at: https://www.theguardian.com/uk-news/2021/sep/29/wayne-couzens-timeline-footage-shows-movements-before-murdering-sarah-everard [14-11-22]

6

Geospatial data in well known cases

Guardian, the (2021), Wayne Couzens timeline: footage shows movements before murdering Sarah Everard https://www.theguardian.com/uk-news/2021/sep/29/wayne-couzens-timeline-footage-shows-movements-before-murdering-sarah-everard [14-11-22]

7

2

What evidence can we find?

8

Surrey Police (2022), Burglar caught admitting crimes on dashcam footage, available at: https://www.surrey.police.uk/news/surrey/news/2022/06/burglar-caught-admitting-crimes-on-dashcam-footage/ [14-11-22]

9

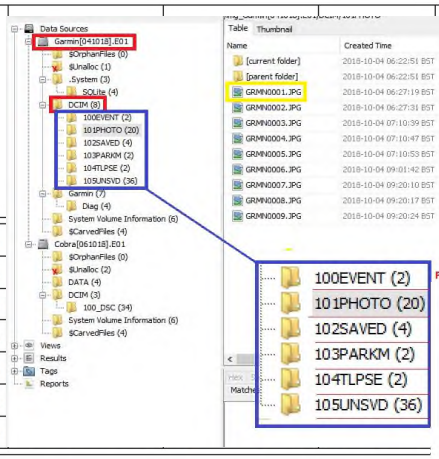
10

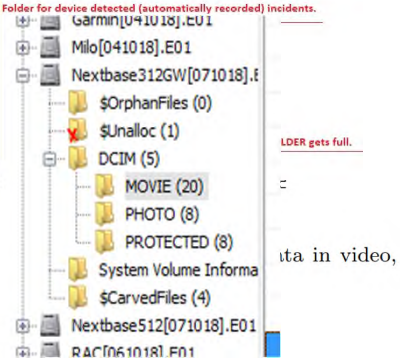
Make	Emergency recording			Parking mode				GPS				Speed			License plate	Time						
Cobra	⊗	f	p	⊗	f	⊗	⊗	§	§	§	§	e	n	w	⊗	⊗	⊗	⊗	f	⊗	w
Nextbase 312GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w	e	n	w	w	⊗	⊗	e	f	n	w
Nextbase 512GW	d	⊗	p	d	⊗	⊗	p	⊗	e	n	w	e	n	w	w	⊗	⊗	e	f	n	w
SilentWitness[1]	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	e	⊗	⊗	e	⊗	w	w	⊗	⊗	⊗	f	⊗	w
MiVue	d	f	p	d	f	n	⊗	a	e	n	w	e	n	w	⊗	a	⊗	e	f	⊗	w
Garmin	⊗	⊗	⊗	d	⊗	⊗	p	⊗	e	n	w	e	n	w	⊗	⊗	c	e	⊗	n	w
RAC[1]	⊗	f	p	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	⊗	w

Key: [1]does not have a native video player *a*=NMEA file, *c*=configuration file, *d*=directory structure, *e*=EXIF data in video, *f*=filename, *n*=native video player, *p*=write protection, *w*=watermark
§ Optional extra, not included in the system analysed in this research
⊗ not available

11

Make	Emergency recording		
Cobra	⊗	f	p
Nextbase 312GW	d	⊗	p
Nextbase 512GW	d	⊗	p
SilentWitness[1]	⊗	⊗	⊗
MiVue	d	f	p
Garmin	⊗	⊗	⊗
RAC[1]	⊗	f	p





Key: [1]does not have a native video player *a*=NMEA file, *c*=configuration file, *d*=dir ıta in video, *f*=filename, *n*=native video player, *p*=write protection, *w*=watermark
§ Optional extra, not included in the system analysed in this research
⊗ not available

12

3

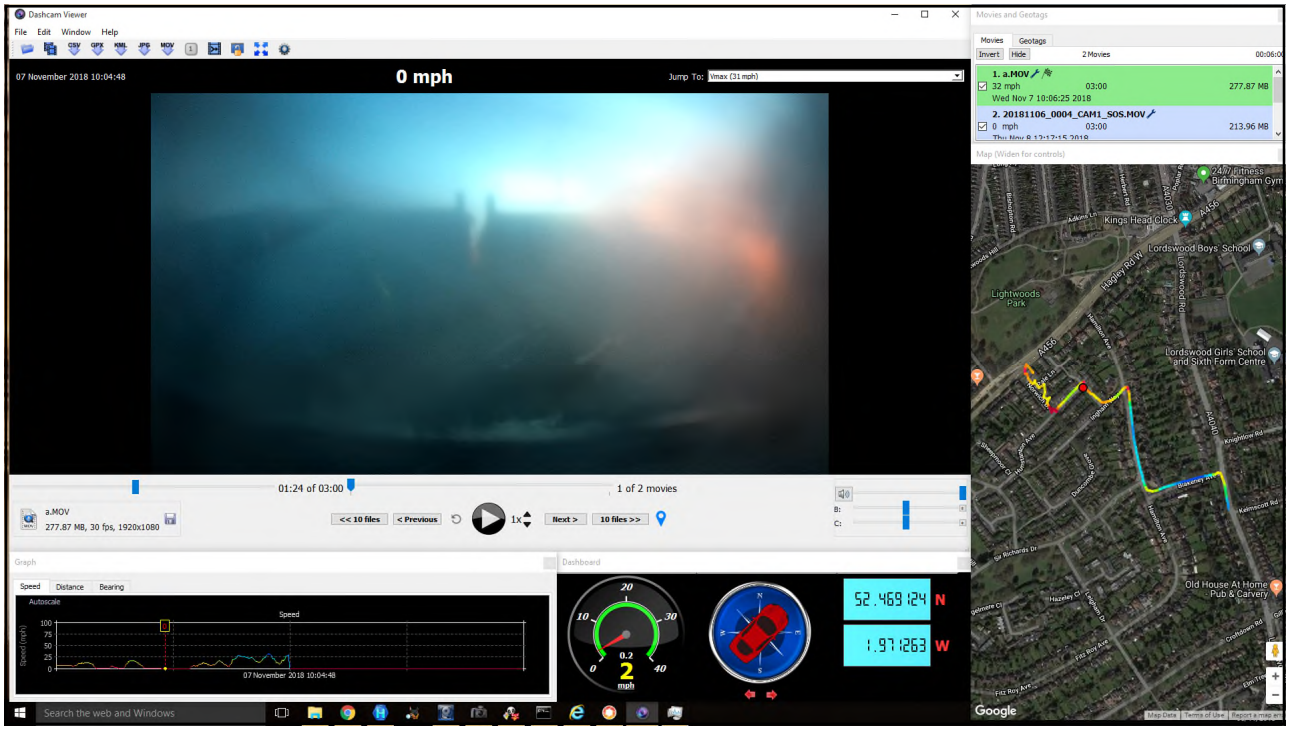
How to extract the evidence

19

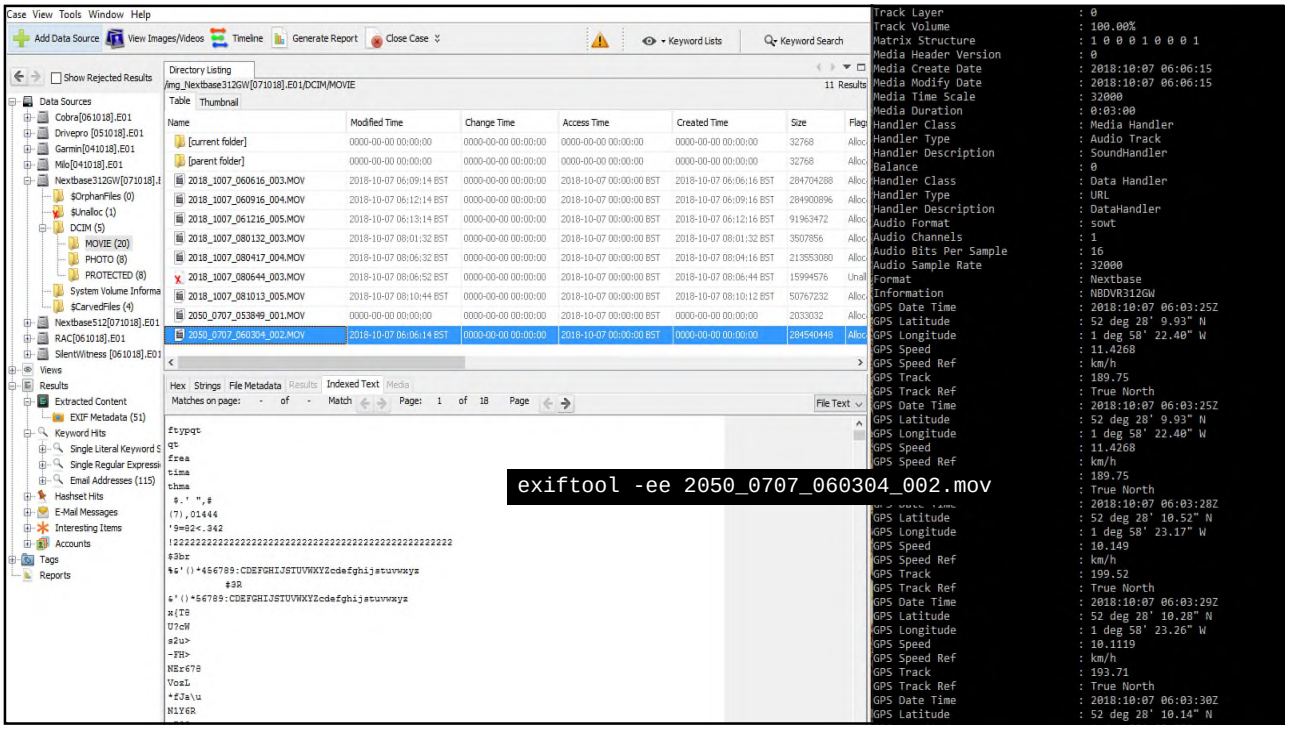
Investigation Steps

1. • Data Gathering & Pre – checks
2. • Data Extraction
3. • Data Transformation
4. • Data Mapping

20


Dashcam Viewer
File Edit Window Help
07 November 2018 10:04:48
0 mph
Jump To: Vmax (31 mph)
01:24 of 03:00
1 of 2 movies
a.MOV
277.87 MB, 30 fps, 1920x1080
<< 10 files
< Previous
Next >
10 files >>
Graph
Speed
Distance
Bearing
Autoscale
Speed
Dashboard
52.469124 N
1.971263 W
Movies and Geotags
Movies
Geotags
Invert
Hide
2 Movies
1. a.MOV
32 mph
03:00
277.87 MB
Wed Nov 7 10:06:25 2018
2. 20181106_0004_CAM1_SOS.MOV
0 mph
03:00
213.96 MB
Map (Widen for controls)
Kings Head Clock
Lordswood Boys' School
Lightwoods Park
Lordswood Girls' School and Sixth Form Centre
Old House At Home Pub & Carvery
Google

21


Case View Tools Window Help
Add Data Source
View Images/Videos
Timeline
Generate Report
Close Case
Keyword Lists
Keyword Search
Show Rejected Results
Directory Listing
/img_Nextbase312GW[071018].E01/DCIM/MOVIE
11 Results
Table
Thumbnail
Name
Modified Time
Change Time
Access Time
Created Time
Size
[current folder]
[parent folder]
2018_1007_060616_003.MOV
2018_1007_060916_004.MOV
2018_1007_061216_005.MOV
2018_1007_080132_003.MOV
2018_1007_080417_004.MOV
2018_1007_080644_003.MOV
2018_1007_081013_005.MOV
2050_0707_053849_001.MOV
2050_0707_060304_002.MOV
Hex
Strings
File Metadata
Indexed Text
Media
exiftool -ee 2050_0707_060304_002.mov
Track Layer : 0
Track Volume : 100.00%
Matrix Structure : 1 0 0 0 1 0 0 0 1
Media Header Version : 0
Media Create Date : 2018:10:07 06:06:15
Media Modify Date : 2018:10:07 06:06:15
Media Time Scale : 32000
Media Duration : 0:03:00
Handler Class : Media Handler
Handler Type : Audio Track
Handler Description : SoundHandler
Balance : 0
Handler Class : Data Handler
Handler Type : URL
Handler Description : DataHandler
Audio Format : sowt
Audio Channels : 1
Audio Bits Per Sample : 16
Audio Sample Rate : 32000
Format : Nextbase
Information : NBDVR312GW
GPS Date Time : 2018:10:07 06:03:25Z
GPS Latitude : 52 deg 28' 9.93" N
GPS Longitude : 1 deg 58' 22.40" W
GPS Speed : 11.4268
GPS Speed Ref : km/h
GPS Track : 189.75
GPS Track Ref : True North
GPS Date Time : 2018:10:07 06:03:25Z
GPS Latitude : 52 deg 28' 9.93" N
GPS Longitude : 1 deg 58' 22.40" W
GPS Speed : 11.4268
GPS Speed Ref : km/h
GPS Track : 189.75
GPS Track Ref : True North
GPS Latitude : 52 deg 28' 10.52" N
GPS Longitude : 1 deg 58' 23.17" W
GPS Speed : 10.149
GPS Speed Ref : km/h
GPS Track : 199.52
GPS Track Ref : True North
GPS Date Time : 2018:10:07 06:03:29Z
GPS Latitude : 52 deg 28' 10.28" N
GPS Longitude : 1 deg 58' 23.26" W
GPS Speed : 10.1119
GPS Speed Ref : km/h
GPS Track : 193.71
GPS Track Ref : True North
GPS Date Time : 2018:10:07 06:03:30Z
GPS Latitude : 52 deg 28' 10.14" N

22

ExifTool Commands Example

- GPS Speed and Datetime are extracted for deriving the Speed Chart:

```
exiftool -c "%.6f" -d "'%Y-%m-%d %H:%M:%S" -p
$GPSDatetime,$GPSLatitude,$GPSLongitude,$GPSSpeed -
ee "D:\ Dashcamproject Extracted files\*" >>
"D:\PMA\IMA Output\output.csv"

exiftool -p "D:\Dashcamproject Output
GPXSee\gpx.fmt" -ee -ext MP4 -w
"D:\\DashcamprojectOutput GPXSee\\MapFiles\\%f.gpx"
"D:\Dashcamproject Extracted files\*.MP4”
```

23

Open-Source Mapping System Solutions

QGIS

Digital maps on your computer.

Create customized maps.

Data format accepted

GeoPackage, GeoTIFF, GRASS, ArcInfo binary and ASCII grids, ERDAS Imagine SDTS, WMS, WCS, PostgreSQL/PostGIS

GpxSee

Import option available

View waypoint lists with their longitude and latitude

Data format accepted

GPX, TCX, FIT, KML, NMEA, IGC, CUP, SIGMA SLF,SML, LOC, Garmin GPI&CSV, TomTom OV2&ITN, ONmove OMD/GHP

GeoDa

Insights from data

Modeling spatial patterns

Data format accepted

.csv, .dbf, .xls, .ods

ArcGIS

Online is cloud-based mapping.

Promotes sharing and collaboration.

Data format accepted

.sh, .shx, .dbf

Example of tools used for investigation along with mapping system:

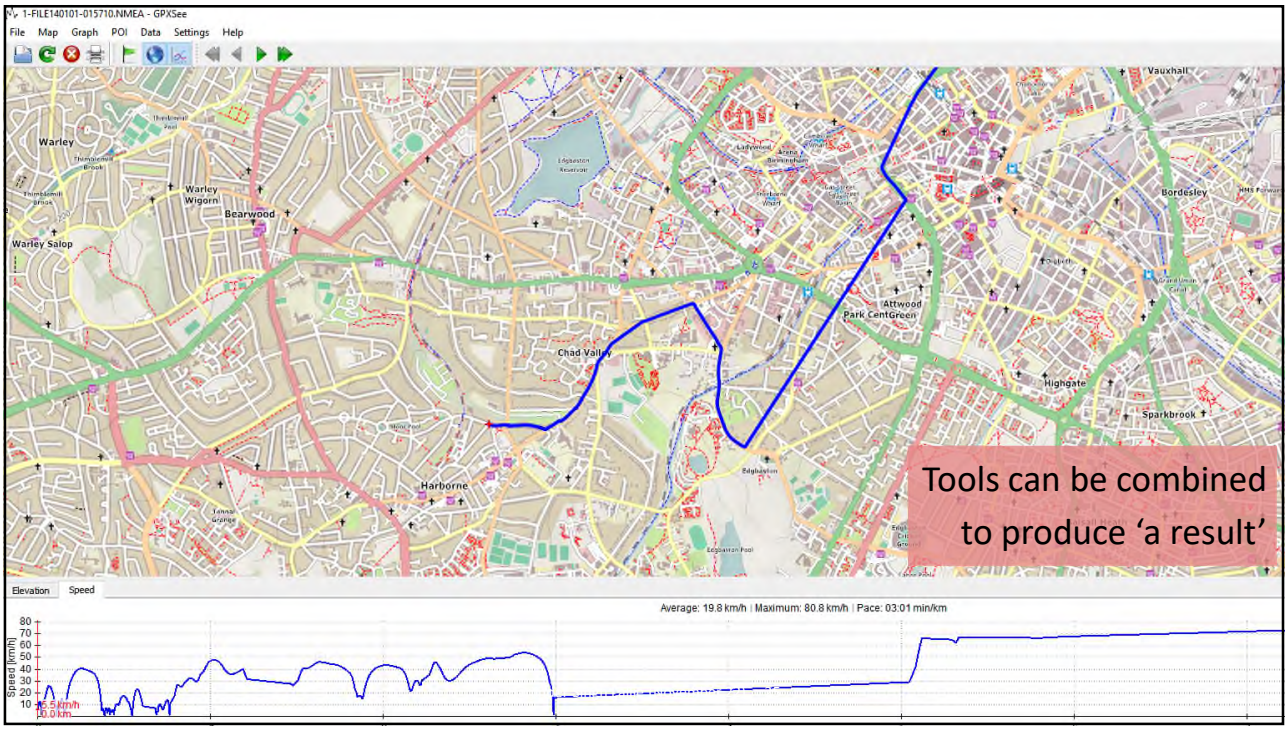
Autopsy

Microsoft Excel

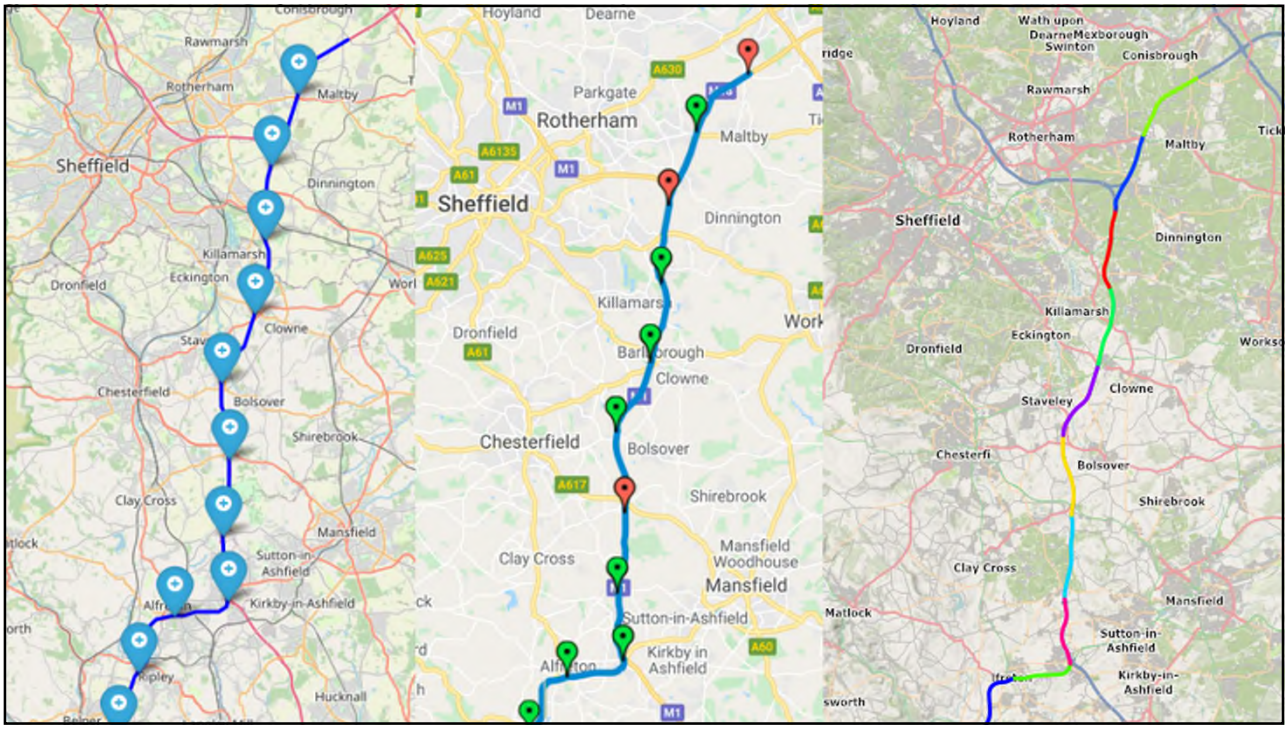
ExifTool

My Nextbase

24


1-FILE140101-015710.NMEA - GPXSee
File Map Graph POI Data Settings Help
Warley
Warley Wigorn
Bearwood
Warley Salop
Harborne
Chad Valley
Attwood Park CentGreen
Highgate
Sparkbrook
Bordesley
Vauxhall
Tools can be combined to produce ‘a result’
Elevation
Speed
Average: 19.8 km/h | Maximum: 80.8 km/h | Pace: 03:01 min/km
Speed [km/h]

25


Rawmarsh
Rotherham
Maltby
Sheffield
Dinnington
Killamarsh
Eckington
Dronfield
Clowne
Chesterfield
Bolsover
Shirebrook
Clay Cross
Mansfield
Sutton-in-Ashfield
Kirkby-in-Ashfield
Hucknall
Parkgate
Rotherham
Maltby
Sheffield
Dinnington
Killamarsh
Dronfield
Clowne
Chesterfield
Bolsover
Shirebrook
Clay Cross
Mansfield Woodhouse
Mansfield
Sutton-in-Ashfield
Kirkby in Ashfield
Hoyland
Wath upon Dearne
Mexborough
Swinton
Conisbrough
Rawmarsh
Rotherham
Maltby
Sheffield
Dinnington
Killamarsh
Eckington
Dronfield
Staveley
Clowne
Bolsover
Shirebrook
Clay Cross
Mansfield
Matlock
Sutton-in-Ashfield
Kirkby-in-Ashfield

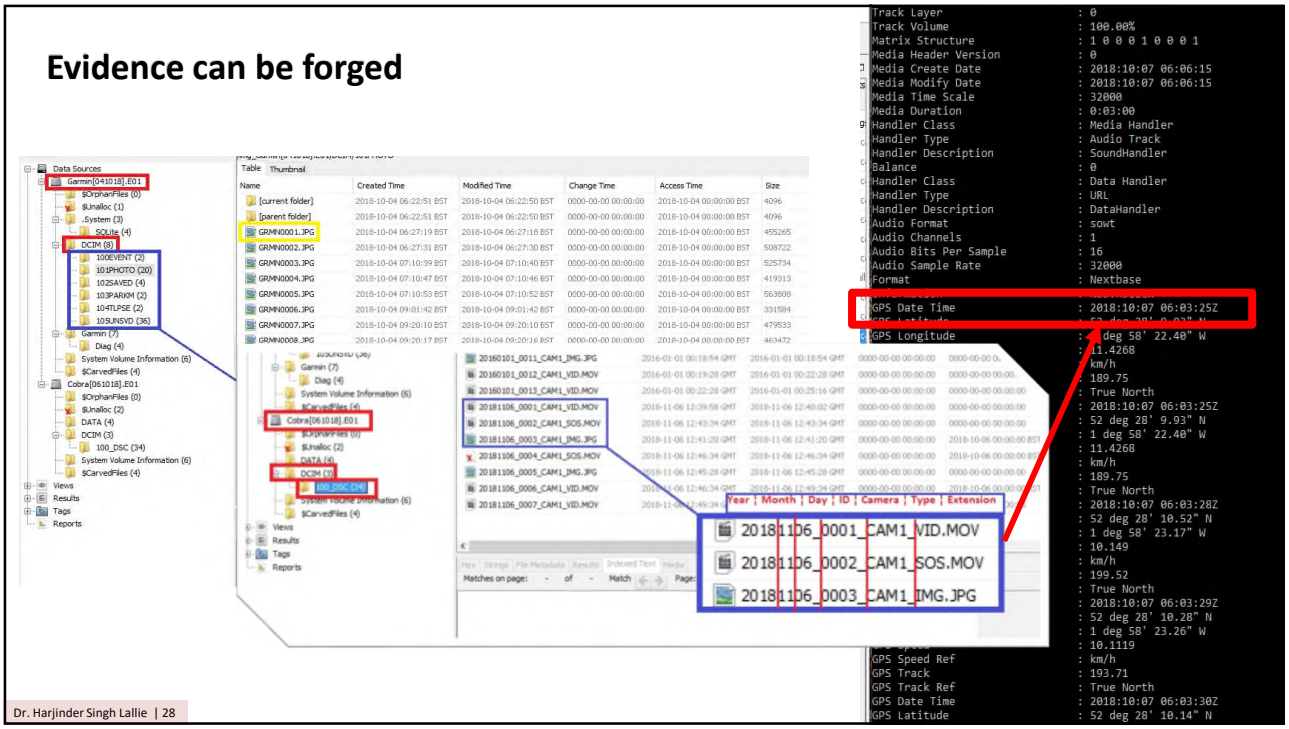
26

4

How to forge the evidence

27

Evidence can be forged



28

Case study

Scenario:

John Dooe is the subject of multiple court orders **(a)** a restraining order preventing entry within a 1.5 mile radius of his ex-wife's workplace (situated in CV4 7AL); **(b)** a restraining order granted under Section 5, of the Protection from Harassment Act (PHA 1997) which places a curfew on travel. The curfew restricts the suspect to only travelling between the hours of 10:00 and 16:00 **(c)** a court order which requires the suspect to have a fully functioning speed limiter on his vehicle. The speed limiter prevents the vehicle from travelling in excess of 40mph.

Task: Is there any evidence to suspect that the suspect may have **(a)** contravened any of the orders, **(b)** altered/tampered with the date/time on the dashcam device, or in any other way attempt to obfuscate his actions/movements?

Exhibits: You are provided with a selection of dashcam videos.

Drone forensics

AKA unmanned aerial vehicles (UAV)

Dr Harjinder Singh Lallie
Director of the Academic Centre of Excellence in Cyber Security Education
Discipline group leader (cyber security)
HL@warwick.ac.uk

1

Introduction

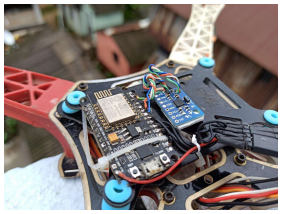
Videos

- Live drone reports: https://www.dedrone.com/resources/incidents/all
- Use of drones to smuggle contraband into prison: https://www.youtube.com/watch?v=3zXq7ywyCnY
- Use of drones in forensic investigations: https://youtu.be/IpN6ee-D6HY
- Battling with the problem of drones: https://www.youtube.com/watch?v=rah_i7FFGRw

Case studies

- Drug, mobile phone, gun/weaponry, other object smuggling into prisons/schools
- A tool to conduct terrorism by planting explosives into stadiums and other public venues
- Corporate/government espionage, monitoring and intelligence gathering
- Voyeurism and invasion of people's privacy by trespassing on private property, stalking, harassment, and invasion of privacy by paparazzi or unethical journalists and reporters
- Disrupting the workflow of airports and distracting air traffic
- International espionage and unauthorised trans-border supervision
- Warfare: launching aerial missile attacks
- Physical attacks, vandalism
- Violation of no-fly zones

Investigating drones, data storage



WISP DRONE
CLOUD

Investigating drones, data storage

- There can be up five (or more) file systems
- Drone data can be reset remotely
- There are no forensic tools…

2

Questions for an investigator

Questions (what can we find?)

- What happened
  - Where did the flight begin and end?
  - What was the altitude?
  - What was the speed?
    What was the route?
  - What other routes has this drone taken?
- The drone
  - What software firmware?
  - What are the battery levels?
  - What is the make, model, serial number?
  - Networks/radio: Wifi, SSID, MAC, IP, MAC, IMEI, IMSI, Bluetooth, 3G/4G connectivity status

Questions (what can we find

- Other
  - Payload weights
  - Paired devices
  - Atmospheric conditions
  - Temporal data
  - geospatial data
  - Controller ID
  - EXIF metadata
  - GPS status during flight
  - Pilot control input
  - Pilot-configured settings
  - File system data
  - Registry entries

9

2

Where and How can we find it?

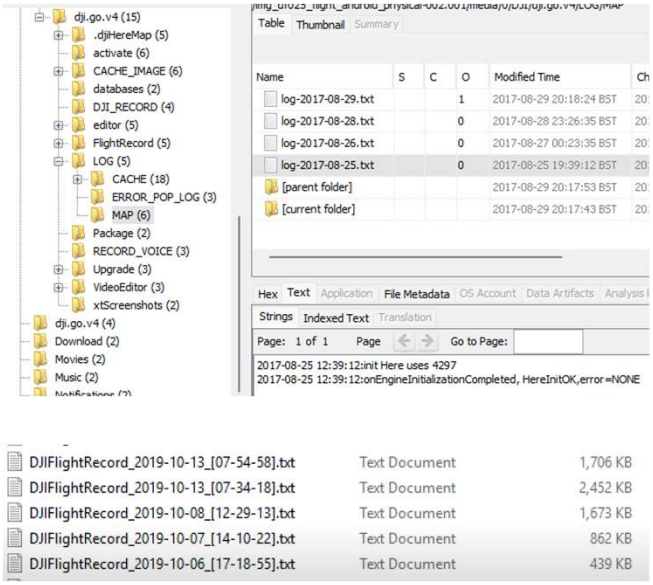
10

What/where?

- Phone
  - Flight records
  - Supplementary flight records (telemetry)
  - Videos/photos
- Drone
  - Second / backup flight record, must be exported using specialist tools.

Log files

- Configuration, usage, update, and flight logs: `.dat`, `.csv`, `.txt`
- Often encrypted
- Often in `dji.go.v4/Flightrecord`, but may just have to search for `.txt` and/or `.dat` and/or `.csv`



CUSTOM.d	CUSTOM.	OSD.flyTi	OSD.flyTi	OSD.latiti	OSD.long	OSD.heig	OSD.heig	OSD.vpsH	OSD.altiti	OSD.mile	OSD.hSpe	OSD.hSpe	OSD.xSpe	OSD.xSpe	OSD.ySpe	OSD.ySpe	OSD.zSpe	OSD.zSpe	OSD.pitch	OSD.roll	OSD.yaw	OSD.yaw	OSD.flycS	OSD.flycC	OSD.fligh	OSD.gpsN	OSD.gpsL	OSD.isGP	OSD.non(
8/29/2017	18:05.9	9m 3.3s	543.3	39.9612	-106.216	0	0	0.7	8128	0	0	0	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Starting M	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:06.0	9m 3.4s	543.4	39.9612	-106.216	0	0	0.7	8128	0	0	0	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Starting M	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:06.1	9m 3.5s	543.5	39.9612	-106.216	0	0	0.7	8128	0	0	0	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Starting M	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:06.5	9m 3.9s	543.9	39.9612	-106.216	0	0	0.7	8128	0	0.1	0.1	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:06.6	9m 4.0s	544	39.9612	-106.216	0	0	0.7	8128	0.1	0.1	0.1	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:06.7	9m 4.1s	544.1	39.9612	-106.216	0	0	0.7	8128	0.1	0.2	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.0	9m 4.2s	544.2	39.9612	-106.216	0	0	0.7	8128	0.1	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.3	9m 4.3s	544.3	39.9612	-106.216	0	0	0.7	8128	0.1	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.4	9m 4.4s	544.4	39.9612	-106.216	0	0	0.7	8128	0.1	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.5	9m 4.5s	544.5	39.9612	-106.216	0	0	0.7	8128	0.1	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.8	9m 4.6s	544.6	39.9612	-106.216	0	0	0.7	8128	0.1	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:07.9	9m 4.8s	544.8	39.9612	-106.216	0	0	0.7	8128	0.2	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.0	9m 4.9s	544.9	39.9612	-106.216	0	0	0.7	8128	0.2	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.2	9m 5.1s	545.1	39.9612	-106.216	0	0	0.7	8128	0.2	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.3	9m 5.2s	545.2	39.9612	-106.216	0	0	0.7	8128	0.2	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.4	9m 5.3s	545.3	39.9612	-106.216	0	0	0.7	8128	0.2	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.5	9m 5.4s	545.4	39.9612	-106.216	0	0	0.7	8128	0.2	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.6	9m 5.5s	545.5	39.9612	-106.216	0	0	0.7	8128	0.2	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.8	9m 5.6s	545.6	39.9612	-106.216	0	0	0.7	8128	0.2	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:08.9	9m 5.7s	545.7	39.9612	-106.216	0	0	0.7	8128	0.2	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.2	292.8	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.0	9m 5.8s	545.8	39.9612	-106.216	0	0	0.7	8128	0.3	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.1	9m 6.0s	546	39.9612	-106.216	0	0	0.7	8128	0.3	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.2	9m 6.2s	546.2	39.9612	-106.216	0	0	0.7	8128	0.3	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.5	9m 6.4s	546.4	39.9612	-106.216	0	0	0.7	8128	0.3	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.6	9m 6.5s	546.5	39.9612	-106.216	0	0	0.7	8128	0.3	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.7	9m 6.6s	546.6	39.9612	-106.216	0	0	0.7	8128	0.3	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.8	9m 6.7s	546.7	39.9612	-106.216	0	0	0.7	8128	0.3	0.1	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:09.9	9m 6.8s	546.8	39.9612	-106.216	0	0	0.7	8128	0.3	0.1	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.1	9m 6.9s	546.9	39.9612	-106.216	0	0	0.7	8128	0.4	0.1	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.2	9m 7.1s	547.1	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.4	9m 7.2s	547.2	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-1	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.5	9m 7.4s	547.4	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.6	9m 7.5s	547.5	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.7	9m 7.6s	547.6	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-0.9	-2.8	-67.3	292.7	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:10.9	9m 7.7s	547.7	39.9612	-106.216	0	0	0.7	8128	0.4	0	0.2	0	0	0	0	0	0	-0.9	-2.7	-67.4	292.6	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:11.0	9m 7.8s	547.8	39.9612	-106.216	0	0	0.7	8128	0.4	0.1	0.2	0	0	0	0	0	0	-1	-2.3	-67.5	292.5	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:11.1	9m 7.9s	547.9	39.96119	-106.216	0	0	0.7	8128	0.4	0.1	0.2	0	0	0	0	-0.2	0	-1.2	-1.1	-67.6	292.4	Manual Ta	Auto Fly	Takeoff (R	16	5	TRUE	
8/29/2017	18:11.2	9m 8.0s	548	39.96119	-106.216	0	0	0.7	8128	0.4	0.1	0.2	0	0	0	0	-0.7	0	-1.3	-0.4	-67.8	292.2	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:11.3	9m 8.1s	548.1	39.9612	-106.216	0	0	1	8128	0.5	0.1	0.2	0.2	0.2	0	0	-1.3	0	-1.1	0	-67.8	292.2	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:11.5	9m 8.2s	548.2	39.9612	-106.216	0.3	0.3	1.3	8128	0.5	0.2	0.2	0.2	0.2	0	0	-2	0	-1.1	-0.4	-67.8	292.2	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:11.7	9m 8.3s	548.3	39.9612	-106.216	0.7	0.7	1.6	8129	0.6	0.5	0.5	0.5	0.5	0	0	-2.9	0	-1.1	-1.1	-67.7	292.3	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:11.9	9m 8.5s	548.5	39.9612	-106.216	2	2	3	8130	0.9	0.9	0.9	0.7	0.7	0	0	-4.7	0	-1.1	-2.3	-67.7	292.3	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:12.1	9m 8.6s	548.6	39.9612	-106.216	2.6	2.6	3.3	8131	1	0.9	0.9	0.7	0.7	0	0	-5.6	0	-0.9	-3.1	-67.7	292.3	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:12.3	9m 8.8s	548.8	39.9612	-106.216	4.6	4.6	5.2	8133	1.3	1	1	0.5	0.7	0	0	-7.8	0	-0.9	-3.6	-67.7	292.3	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:12.5	9m 8.9s	548.9	39.9612	-106.216	5.9	5.9	6.2	8134	1.5	1.1	1.1	0.5	0.7	0	0	-9	0	-0.9	-3.8	-67.6	292.4	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:12.8	9m 9.0s	549	39.9612	-106.216	7.2	7.2	7.5	8135	1.6	0.8	1.1	0.5	0.7	0	0	-9.8	0	-0.7	-4	-67.6	292.4	P-GPS	Auto Fly		16	5	TRUE	
8/29/2017	18:13.0	9m 9.1s	549.1	39.9612	-106.216	8.9	8.9	9.2	8137	1.8	0.9	1.1	0.2	0.7	0	0	-10.5	0	-0.2	-4.2	-67.6	292.4	P-GPS	Auto Fly		16	5	TRUE	

There are no accepted drone forensic tools

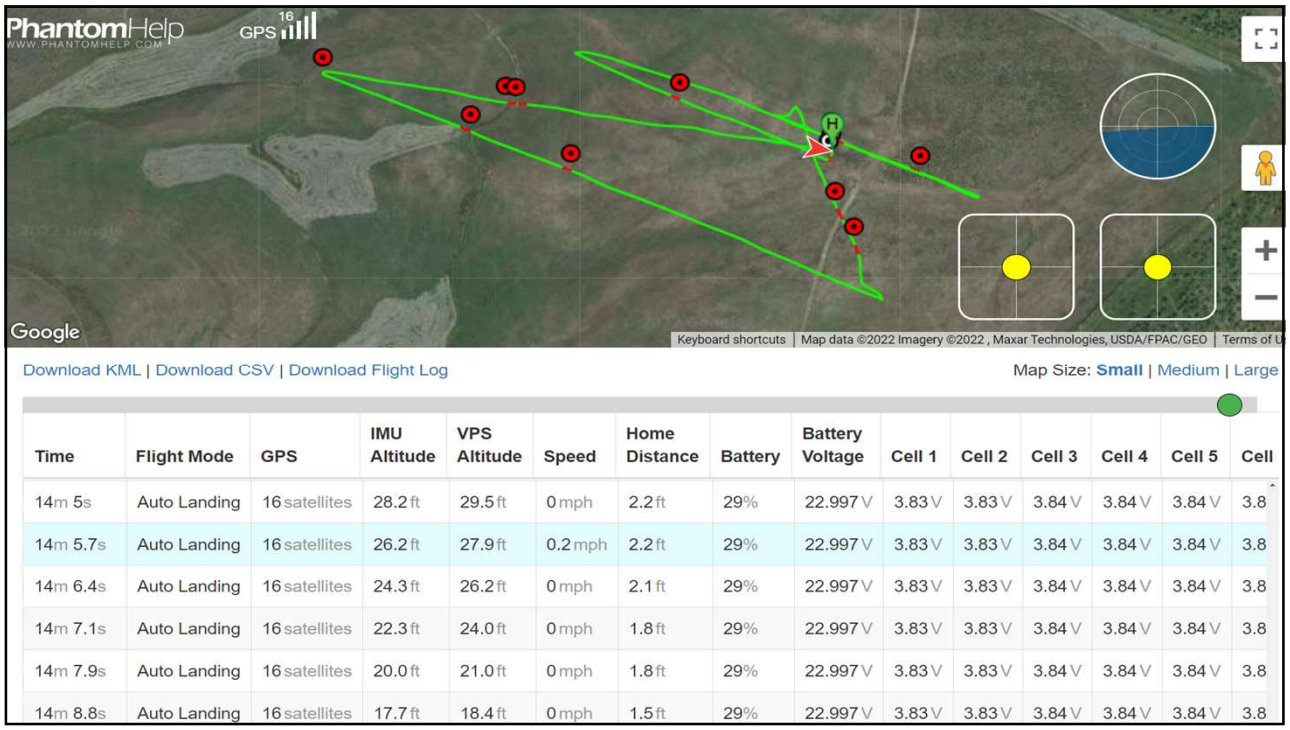
However, we can use

1. Phantom Help Log Viewer[1]
2. AirData uav[2]
3. CsvView[3]
4. DatCon[4]

[1]https://www.phantomhelp.com/LogViewer
[2]https://airdata.com
[3]https://datfile.net/
[4]https://datfile.net/

15

16

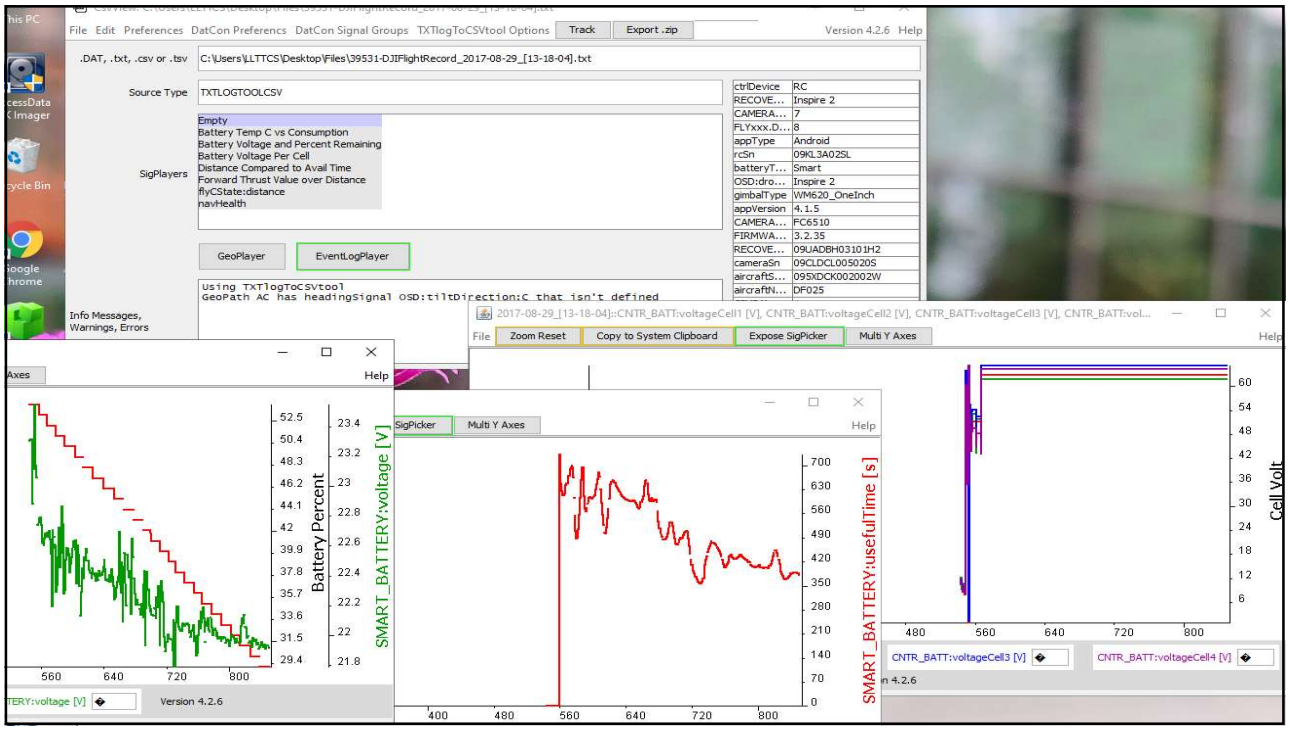


Download KML | Download CSV | Download Flight Log

Map Size: **Small** | Medium | Large

Time	Flight Mode	GPS	IMU Altitude	VPS Altitude	Speed	Home Distance	Battery	Battery Voltage	Cell 1	Cell 2	Cell 3	Cell 4	Cell 5	Cell
14m 5s	Auto Landing	16 satellites	28.2 ft	29.5 ft	0 mph	2.2 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8
14m 5.7s	Auto Landing	16 satellites	26.2 ft	27.9 ft	0.2 mph	2.2 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8
14m 6.4s	Auto Landing	16 satellites	24.3 ft	26.2 ft	0 mph	2.1 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8
14m 7.1s	Auto Landing	16 satellites	22.3 ft	24.0 ft	0 mph	1.8 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8
14m 7.9s	Auto Landing	16 satellites	20.0 ft	21.0 ft	0 mph	1.8 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8
14m 8.8s	Auto Landing	16 satellites	17.7 ft	18.4 ft	0 mph	1.5 ft	29%	22.997 V	3.83 V	3.83 V	3.84 V	3.84 V	3.84 V	3.8

17

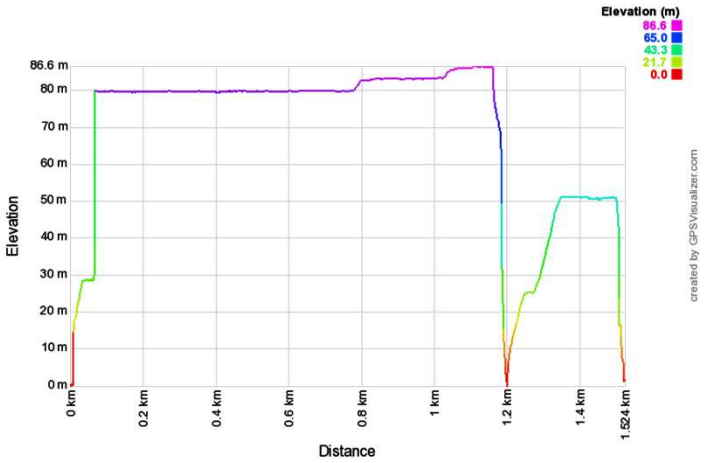


18

Telemetry data

Contained within the flightlog, sometimes separated into an CSV

Convert to GPX[1], then convert to a graph[2]



[1]http://www.gpsvisualizer.com/convert_input?convert_format=gpx
[2]http://www.gpsvisualizer.com/profile?output_home

Firmware

Firmware – no universal location, search for 'firmware'

Home

```
2017-08-29 13:17:43:mbCoordianteCali = true
2017-08-29 13:17:45:addHomeMarker: wsg=lat/lng:
(39.96120292202613,-106.21639890802577)
altitude=0.0 accuracy=0.0, gcj=lat/lng:
(39.961203,-106.216399)
2017-08-29 13:18:24:mbCoordianteCali = true
2017-08-29 13:18:24:mbCoordianteCali = true
```

The home coordinate is a failsafe mechanism which enables the drone to return to a pre-configured home location when the battery is low, there are mechanical problems, or communication is lost with the remote controller