Digital Forensics

What is it, and how can I get involved?

Phil Cobley

Training Development Lead for MSAB

What we shall look to cover…

- Who am I?
- What is Digital Forensics?
- Some basic (but core) Digital Forensic principles
- Take a look at some Digital Forensics in action!
- Things to consider if you wish to enter the field of Digital Forensics

Who am I?

- Over 11 years experience in the Police as an Officer
- Managed & Developed Digital Forensics in Bedfordshire Police
- Regional Cyber Crime Unit Secondment – Regional Cyber Protect Coordinator
- Certified in various Information Security & Digital Forensics disciplines
- Currently studying an MSc in Information Security and Digital Forensics (part time)
  - Undergraduate Studies were in "Computing & IT: Software Development"
- Guest Lecturer, Trainer and Advisor
- Member of:
  - British Computing Society (MBCS)
  - BCS Bedford Branch Committee
  - High Tech Crime Consortium (HTCC)
- Sat on the National ISO 17025 Standards Expert Network
- Joined MSAB as a Digital Forensics Technical Trainer in 2016
- MSAB Training Development Lead in June 2017

BEDFORDSHIRE POLICE

Eastern Region Special Operations Unit

Regional Organised Crime Unit

MSAB

Ecosystem of Mobile Forensics

What is Digital Forensics?

…actually…what is Forensics?

"Forensic science is application of science to matters of law."

(Higher Education Academy, 2010)

So what is Forensic Science?

- Making order out of chaos by providing explanations for what we see around us.
- The scientific method can be broken down into:
  - Make an observation
  - Give a provisional hypothesis
  - Derive a method to test that hypothesis
  - Test it!
  - Analyse the results and evaluate against hypothesis
  - Report on what you have found and observed
- The important things to note are:
  - Transparency
  - Universality
  - Repeatability
  - Nothing can be proven in absolute terms – good until proven false!
  - ***Humility, patience, and lots of tea are critical!***

What is Digital Forensics?

- Cybercrime forensics is the forensic examination of ***digital media*** with a view to ***securely collecting, preserving and analysing*** computer data in such a way that the results can be ***admissible as evidence*** in a tribunal or court of law.

-College of Policing 2014

What type of digital media?

Desktop Computers

Laptop / Notebooks

Smart TVs

Mobile Phones

Tablet Devices

Games Consoles

Removable Storage

Servers

IoT Devices / Digital Cameras

Routers & Network Devices

Printers & Photocopiers

Vehicle Forensics

How does Digital Forensics work?

- The 5-step process (simplified):

1. **Identification** – Identify potential sources of information

2. **Preservation** – Protecting a scene, environment, physical data nodes

3. **Collection** – Removing drives, imaging devices, data extraction, etc

4. **Analysis** – Examining the collected data and drawing conclusions

5. **Reporting** – Producing forensic reports and providing contemporaneous notes of the entire examination/investigation process

So, what do you need to "do" digital forensics?

Correct Attitude

Environment

Equipment & Tools

Professional Network

Training & Competence

Legislation Awareness

Policies & Procedures

Accreditations & Vetting

Legislation

- What are the main pieces of legislation and/or guidance that could be relevant to criminal cases involving digital forensics?
  - ACPO Principles of Digital Evidence
  - Data Protection Act 1998 (DPA)
  - Freedom of Information Act 2000 (FOIA)
  - Computer Misuse Act 1990 as updated by the Police and Justice Act 2006 (CMA)
  - Electronic Communications Act 2000 (ECA)
  - Human Rights Act 1998 (HRA)
  - Regulation of Investigatory Powers Act 2000 (RIPA)
  - Malicious Communications Act 1988 (MCA)
  - Police and Criminal Evidence Act 1984 (PACE)

ACPO Principles of Digital Evidence

- ***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.

  - ***Don't use or access any data***

ACPO Principles of Digital Evidence

- ***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.

  - ***If you have to use or access it, ensure you're trained to do so***

ACPO Principles of Digital Evidence

- ***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.

  - ***If you have used it then document what you've done (audit trail)***

ACPO Principles of Digital Evidence

- ***Principle 4:***

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

  - ***Ultimately, the person/Officer in charge of investigating the case (OIC) is responsible***

ACPO Principles of Digital Evidence

- ***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.

ACPO Principles of Digital Evidence

So, simply put…

- Don't change any data

  unless

- You're trained & competent to do so

  either way

- Keep notes of what you do

  however

- The buck stops at the OIC

So let us now have some fun…

We shall now try to do the following…

- Acquire a forensic image of a USB thumb drive of data
- Review the thumb drive data
- Look at some python and see the links to Digital Forensics

And if we have time…

- Review an acquired Windows operating system

…all with free tools you can download today!

Equipment – Forensic Tools

MSAB

MAGNET FORENSICS

AccessData

BlackBag TECHNOLOGIES

V-F-C MD5

GRIFFEYE

GUIDANCE SOFTWARE

cellebrite delivering mobile expertise

**Not an exhaustive list – Endless Open Source tools also available!*

Training & Competence

- Need to have a formalised, structured development roadmap or framework
- Beware the certification trap!
  - Courses are expensive – Choose them wisely!
  - Many can repeat and cover the same material or be too generic
  - Research Carefully - Certificates do not equate to knowledge or expertise!
  - Expert Witness Status – Decided by each individual Court, not you!
- Fast moving industry – difficult to keep up to speed – Be prepared!
- Workshops, conferences and industry updates are essential
- Share knowledge and experience across the DF community

Training & Competence

- NCSC-certified degrees
  - www.ncsc.gov.uk/information/ncsc-certified-degrees
- Pluralsight
  - www.pluralsight.com
- Coursera
  - www.coursera.org
- Open University – OpenLearn (Free)
  - https://bit.ly/2XlqSNY
- SANS DFIR
  - www.sans.org
- Vendor Specific Certifications
  - MSAB / EnCase / Magnet / UFED / AccessData / NUIX / Blackbag

Accreditations

- Pulling it all together…
  - ISO 17025
    - Validation and Verification of processes and techniques within the laboratory environment
    - Based around a Quality Management System
    - Scientific process – verification of results with repeatable, evidenced processes

  - ISO 27001
    - Information Security Management System
    - Looking at identification of information assets, risk assessments, vulnerability and threat identification, appropriate controls and risk treatment plans

Any Questions?

Phil Cobley

Training Development Lead

Training Department

MSAB

phil.cobley@msab.com

phil.cobley@hotmail.co.uk