CREATING AND INTEGRATING A FLOSS PRODUCT INTO UK LAW ENFORCEMENT

Joseph Williams

joseph.williams@canterbury.ac.uk

Canterbury Christ Church University

INTRODUCTION

- This talk will focus on
  - how law enforcement in the UK conduct open source research (OSR)
  - OSIRT – Open Source Internet Research Tool
  - a case-study surrounding OSIRT's integration into a police force
  - my anecdotal experience… Can you relate? Can you see where I've gone wrong?

ASIDE…

- I will try to use the following terms:
    - Open Source Research (OSR)
    - FLOSS
- Sorry, as hard as I try ‘open source’ may slip out in relation to either mean OSR or FLOSS.

OPEN SOURCE RESEARCH?

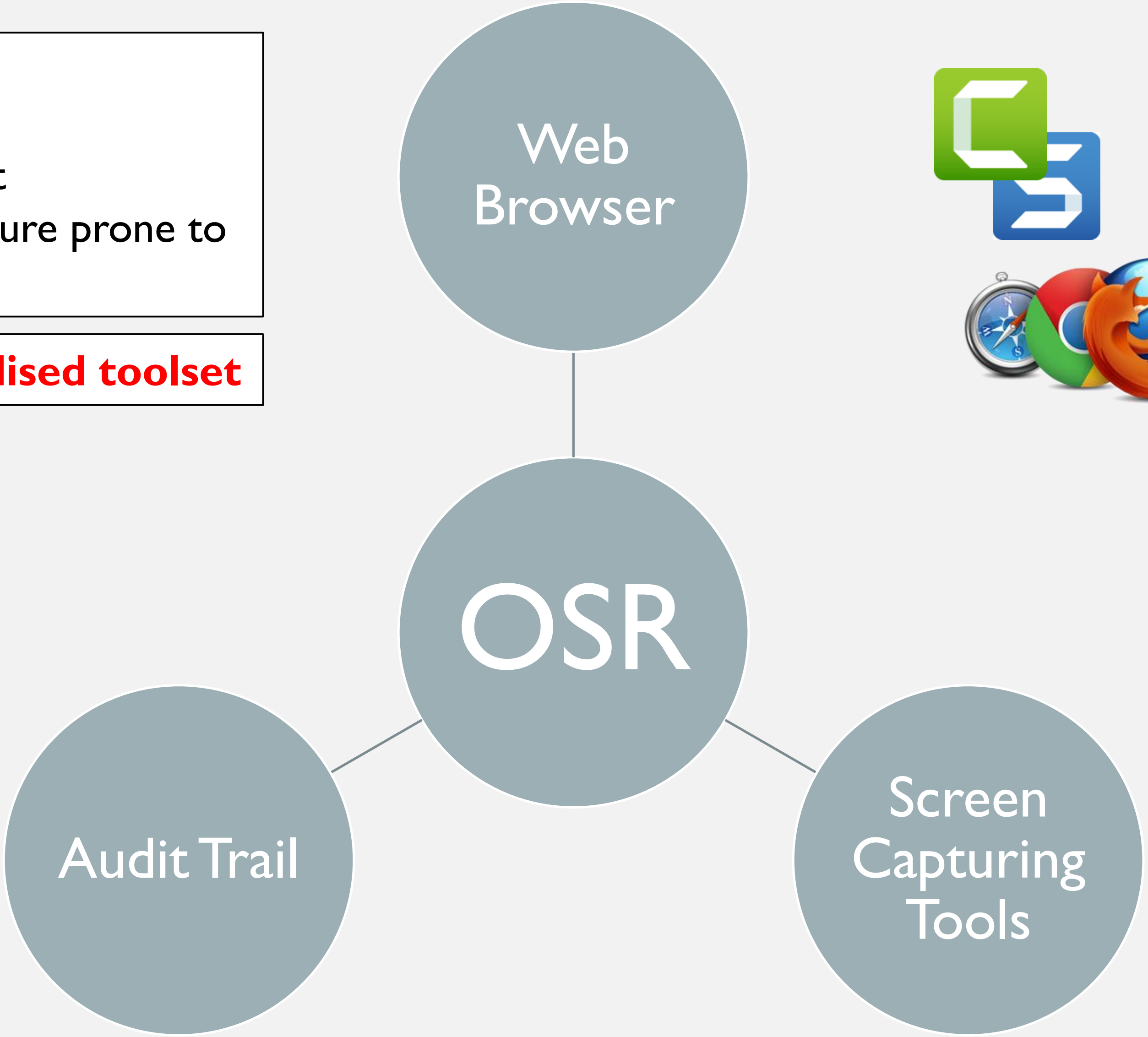
"The collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence within investigations."

-Association of Chief Police Officers, 2012

HOW OSR IS CONDUCTED

- Cost
- Training
- Time spent
- Manual nature prone to error

No standardised toolset



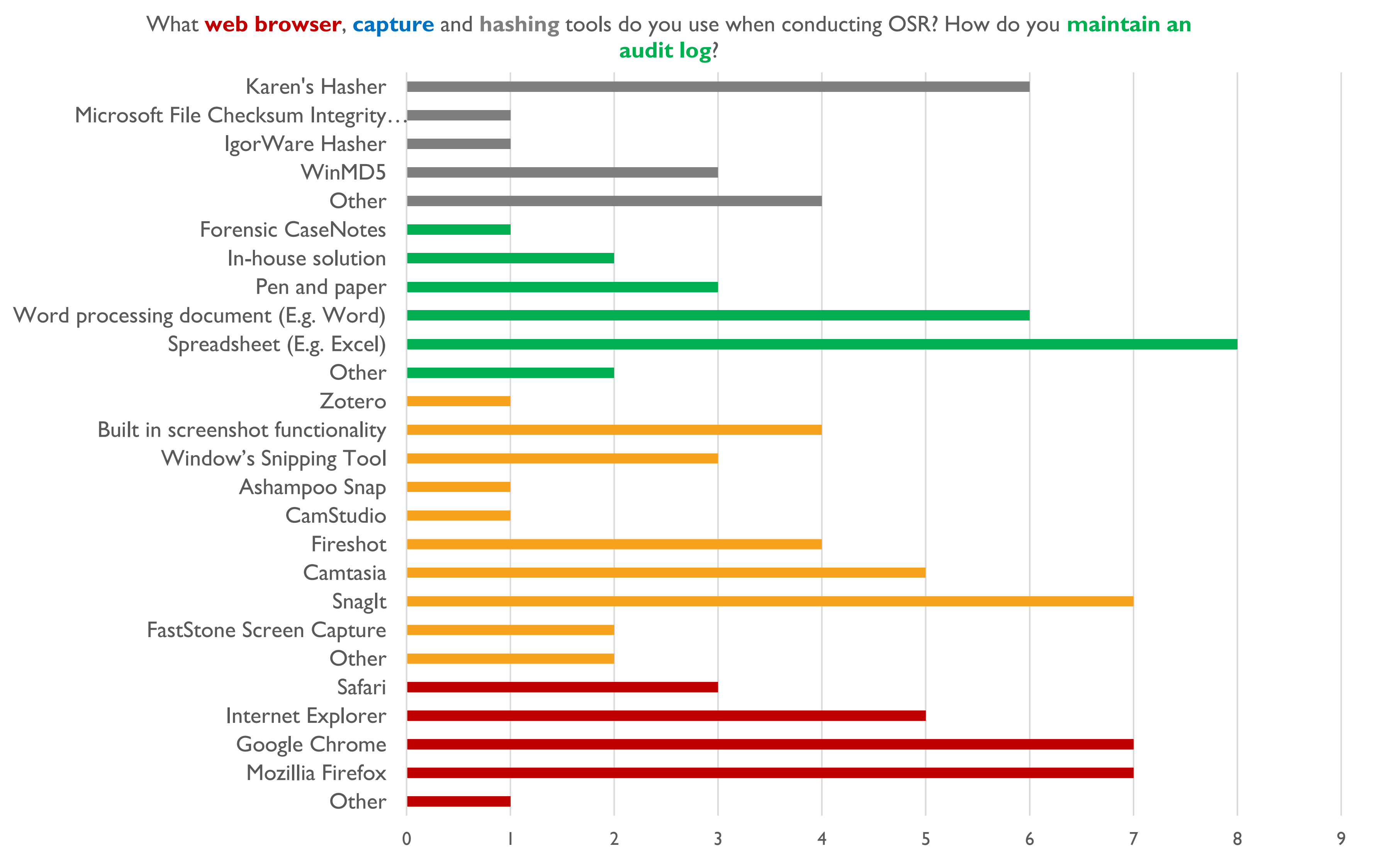
Web Browser

OSR

Audit Trail

Screen Capturing Tools

TOOL USAGE



- 20 responses. 12 constabularies
- Could select more than one response, hence total >20

COLLEGE OF POLICING SPEC

- **Essential requirements:**
  - Ability to set default homepage (e.g. www.google.co.uk)
  - Ability to enter username and password in protected sites
  - Ability to create, save and load a case with any number of different cases to a location of user's choice.
  - Must record every URL visited in sequence with date and time URL is visited.
  - Ability to screen capture whole web pages, parts of web pages, videos and downloaded documents.
  - Ability to add notes when capturing screenshots/ videos.
  - Must be able to automatically hash the screen captures (Still and moving) and documents.
  - Must be able to store screen captures, audit log in a case container/folder
  - Must be able to produce a report showing audit log with screen capture file names and hash values.
  - Cheap licence (e.g. £30 a licence)

- **Desirable requirements:**
  - Ability to capture a video screenshot
  - Ability to download a video
  - Ability to attach Constabulary icon to reports as a default

PROTOTYPE

- Prototype created in 2015
- Contained everything from within the spec
- Feedback, observations, interviews and SUS results highlighted the need for a tool like OSIRT
  - It wasn't designed with extensibility and maintainability in mind
- Closed source…

OSIRT

Open **S**ource **I**nternet **R**esearch **T**ool

Canterbury Christ Church University

College of Policing

OSIRT IS HERE BECAUSE OF FLOSS

CEF

CEFSharp

SQLite

DotNetZip

ExifLib

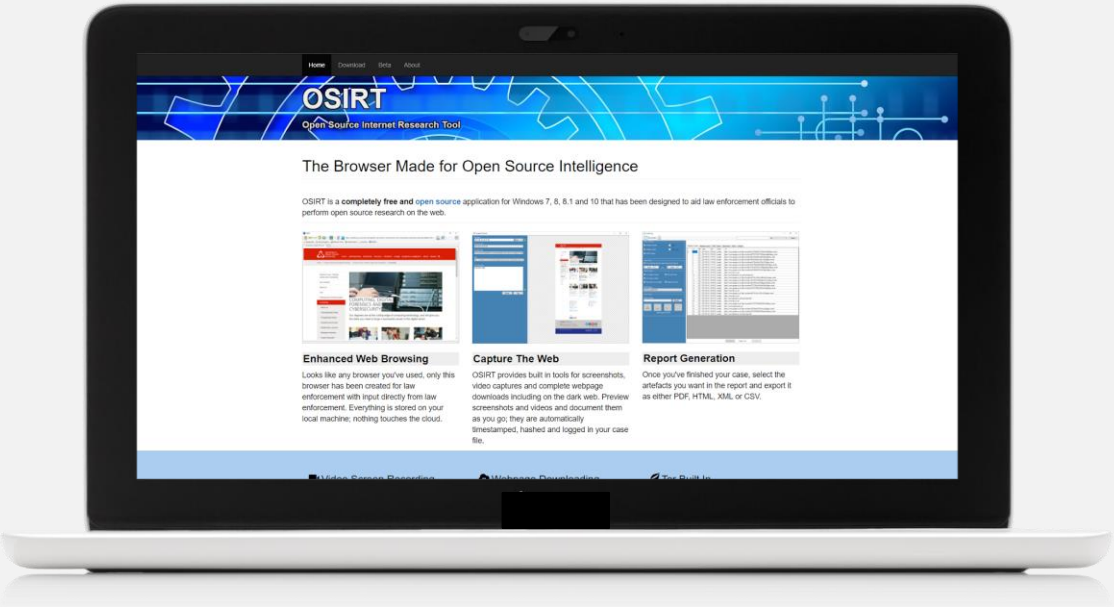
ImageMagick

WK<html>TOpdf

Tor

OSIRT

- Full and partial screen captures
- Webpage downloading
- Tor built in
- Reporting
- Logging
- Lots of other little helpful tools



The Browser Made for Open Source Intelligence

OSIRT is a **completely free and** open source application for Windows 7, 8, 8.1 and 10 that has been designed to aid law enforcement officials to perform open source research on the web.

Enhanced Web Browsing

Looks like any browser you've used, only this browser has been created for law enforcement with input directly from law enforcement. Everything is stored on your local machine; nothing touches the cloud.

Capture The Web

OSIRT provides built in tools for screenshots, video captures and complete webpage downloads including on the dark web. Preview screenshots and videos and document them as you go; they are automatically timestamped, hashed and logged in your case file.

Report Generation

Once you've finished your case, select the artefacts you want in the report and export it as either PDF, HTML, XML or CSV.

http://osirtbrowser.com/

ABOUT OSIRT

- Thousands individual downloads from osirtbrowser.com
- Used by police forces and law enforcement across the globe
- Trained at the College of Policing
  - Core component of the RITES course
- Has been used to capture artefacts for an array of investigations
  - E.g. Murder, CSE, anti-terrorism
- Been used with international policing collaboration
- Integrated into private OSINT training packages
- Strong interest from ECTEG (European Cybercrime Training and Education Group)
  - Particularly, SC3 (Swedish Cybercrime Centre) looking to support OSIRT long-term for 5-7,000 users.

FLOSS INTEGRATION INTO UK PUBLIC SERVICE

- Been several pushes by the government to see the integration of FLOSS into public service
- However, it was acknowledged in 2012 that it is not "widely used in government IT" [2]
  - Yet, in 2004, FLOSS should be "actively and fairly considered" [3]
- More recently, in 2017, the government pushed for FLOSS to "to improve transparency, flexibility and accountability" [4]
- Those departments with a "degree of autonomy" may be more willing to integrate FLOSS [5]
- Police are offered a great deal of autonomy in decision making, but there is little data surrounding hat software police use for what purpose

WHY A SLOW UPTAKE OF FLOSS?

- Negative perceptions surrounding FLOSS?
- It's not unusual to receive e-mails querying OSIRT's provenance
  - "Where has this come from, and why is it free!?"
- Typically, questions fall into five categories
  - **Security**
  - **Maintenance**
  - **Technical support**
  - **Cost**
  - **Training**
- These five areas will form the focus of the case study

METHOD

- **Semi-structured interviews**
  - Inspector, DC and IT Administrator
    - Manager, daily user and ‘the integrator’
  - Look at OSIRT’s integration into a police force
  - Police force has “about 40” active OSIRT users

INTERVIEWS

TRUST AND SECURITY

- All three participants noted being able to trust software as important factor of usage
- “We trust OSIRT because we’ve spoken to you, we can contact you.” – Inspector
    - Highlights importance of having a point of contact
- OSIRT being FLOSS made it “easier” to trust, and the thought of having the source code available offered “peace of mind.” - IT administrator
- Understandable that it’s hard to trust a product made by an individual.
    - OSIRT is FLOSS to abate those concerns
    - OSIRT is linked to both a University and has collaborative links with the College of Policing

MAINTENANCE

- Lone developer issue
- There were some initial concerns from the IT administrator
  - Again, being able to talk to the developer helped
- The DC focused on the technological shift
  - "It feels like my work changes on a yearly basis"
- Inspector was pragmatic, and looked within the police force itself to drive updates with "cyber specials"
  - Shows they are thinking about the issues around the lone developer

TECHNICAL SUPPORT

- In the DC's opinion of FLOSS, technical support is "scarce"
  - They felt that with paid-for tools, there is a contract where technical assistance is part of the cost. Not always the case with FLOSS.
    - "had my fingers burnt"
- Inspector agreed that it was "crucial" to be able to reach out for assistance
- IT administrator knows the risk of using FLOSS ("par-for-the-course"), and expectations of support should be lowered

- Aside, OSIRT is fortunate in that it has an online community on POLKA (a closed police forum where knowledge is shared)

COST

- Unsurprisingly, OSIRT’s cost was a driving factor in its integration
- The inspector said they had looked at several tools, but the cost was “too high” with some costing “£60-£150 a user per year”.
- “Money does not necessarily mean better quality”, notes the IT administrator
- DC was the least cost-averse and stressed the importance of software quality to deliver the “best service”

TRAINING

- Inspector saw training as a cost/benefit trade-off.
  - "Of course you get the software for free, but we have things in place already and replacing software means training, it means time, and we have to trade-off the cost of licenses versus the cost of training"
- DC saw the integration of new software to cause potential "resent[ment]" as officers may be in their "comfort zone" with their present workflow.

SUMMARY

- Very much appreciate this small case study is not representative
- However, it does display thought processes and issues faced by those making decisions when integrating software.
- Interviews also align we the numerous, anecdotal, conversations had with police forces.

FUTURE

- It has been incredibly challenging being an independent developer
- There have been some business offers, but I absolutely want OSIRT to remain FLOSS
- How do you keep your FLOSS project going?