Creating and Integrating a FLOSS Product into UK Law Enforcement

Joseph Williams

Creating and Integrating a FLOSS Product into UK Law Enforcement

Joseph Williams

Canterbury Christ Church University. Department of Computing, Digital Forensics and Cybersecurity. North Holmes Road, Canterbury, Kent. CT1 1QU. UK.

joseph.williams@canterbury.ac.uk

Abstract. Open Source Internet Research Tool (OSIRT) is a free and open source software tool that enables law enforcement officials to conduct online research and obtain artefacts in an evidential and lawful manner. Over the past three years, OSIRT has seen growth from a handful of users within UK law enforcement, to a reach that extends to countries across the globe which also sees usage outside of law enforcement and beyond its original scope.

This paper will reflect upon OSIRT's development, and discusses issues surrounding the development of a FLOSS product for UK law enforcement. With cuts to budgets being made to law enforcement services, FLOSS software like OSIRT has an opportunity to flourish in this sector. To establish OSIRT's and FLOSS' integration into UK law enforcement, interviews, a small case study and questionnaires were conducted with serving police officers, police trainers and an IT administrator; all have experience with OSIRT.

Keywords: Open Source Research, Open Source Intelligence, Internet Investigations, Law Enforcement, Open Source Software

1 Introduction

With cuts to policing budgets in the UK expected to hit £700m by 2020 [1], police services are finding themselves needing to reduce expenditure. One of the areas law enforcement can save is by integrating FLOSS. With an ever-increasing rise in cybercrime, policing is now seeing itself requiring a shift from 'traditional' roles to a digital, online presence with a need for officers to be capable of conducting online investigations.

The Internet plays host to a variety of artefacts law enforcement can also use for intelligence purposes, further extending the need for officers to be able to obtain information using technology. To aid law enforcement in conducting research online, OSIRT, a FLOSS product, was created in collaboration with the UK's College of Policing.

This paper looks at OSIRT's integration and usage within UK law enforcement by looking at, often closed-sourced, tools that were previously used when conducting

open source research and why this plethora of different tools was standardised with OSIRT. To support this, views and experiences of law enforcement officials (LEOs) are considered by means of a case study, interviews and questionnaires.

2 Background

This section will review how police conduct open source investigations in the UK, including technical limitations and the need for software standardisation. This section will also look at how the UK government are encouraging public services to adopt FLOSS.

2.1 Open Source Research

As part of their daily investigative routines, LEOs across the United Kingdom conduct Open Source Research (OSR), which the Association of Chief Police Officers (ACPO) define as "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" [2].

Given a typical OSR workflow, LEOs must manually log any action they have taken. For example, every website visited must be logged with a date and time stamp. If anything tangible is obtained from that website, such as a screenshot or download, it must be hashed using a suitable hashing algorithm and logged with a date and time stamp in tandem with the originating URL. Any artefacts obtained (e.g. screenshots) are then placed into a suitable directory structure, or directly onto the note taking application of choice to complete the audit log. Any extra annotations the investigator wishes to make are also then added.

This only tells part of the story, however, in order to obtain these artefacts, LEOs have to use an exhaustive variety of different tools. These tools differ in quality, usability, and price and will often vary from constabulary to constabulary. Largely, they amount to a web browser, static and dynamic screen capturing tools, a hashing tool and a note taking application for manually maintaining an audit log.

2.2 Toolkit Standardisation

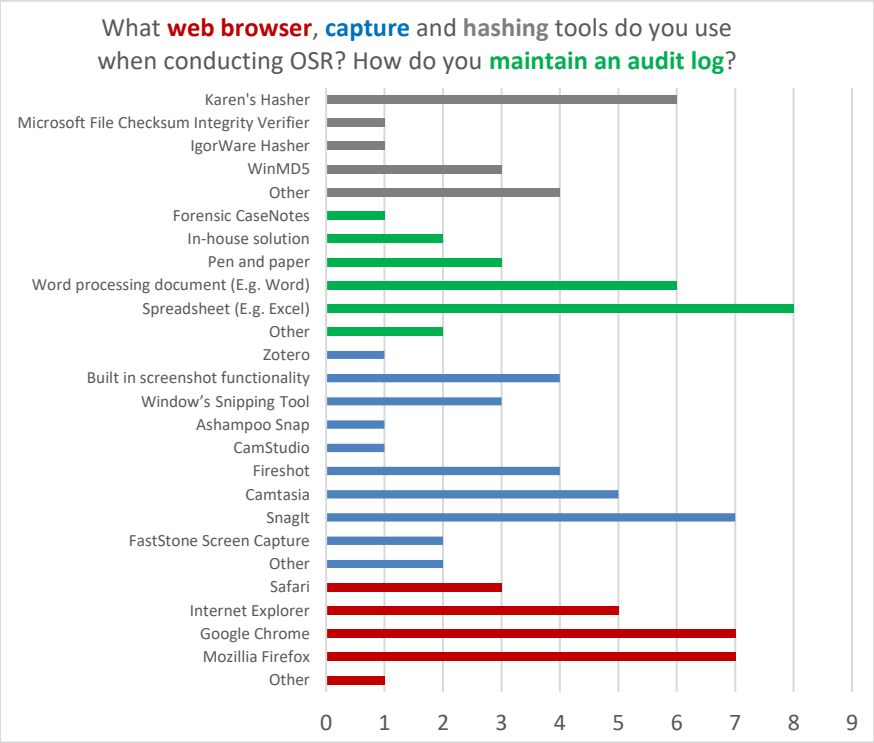
To aid digital investigators in conducting OSR, and to help standardise procedures, the UK's College of Policing runs a Researching Identifying and Tracing the Electronic Suspect (RITES) course[1]. The RITES course is a week-long training package aimed at LEOs of all skill levels, with a strong focus around conducting open source investigations and research. As part of this course, trainers provide a standard toolset. However, trainers noted that the introduction of too many tools, and manual audit log entry, overloaded the students.

[1] http://www.college.police.uk/What-we-do/Learning/Professional-Training/digital-and-cyber-crime/Pages/Researching-Identifying-Tracing-Electronic-Suspect.aspx (Last accessed: January 14th 2018)

To establish current practices and tool usage in the working environment, a short questionnaire was distributed to LEOs within the UK who have a range of experience of conducting OSR. The levels of experience ranged from less than one year, to over six years with the participants ranked from Police Constables to Inspectors. Twenty responses were received from twelve constabularies. In addition to establishing current tool usage, an exploratory question asked what LEOs would like to see from an all-in-one OSR tool. Figure 1 shows the tool usage results from the questionnaire.

Respondents were also asked “Does the cost of some tools prohibit you from being able to use them?”, 13 responded “yes”. A question then asked, “I am more inclined to use a tool if it is free of charge.”, 12 responded “yes”.

Fig. 1. Tool usage when conducting OSR



Additionally, audit log maintenance was time consuming and prone to unintentional mistakes; such as a digital investigator forgetting to log when action was taken. Given the nature of the potential evidence being obtained, such oversight may compromise a case, and contravenes principle 3 of ACPO guidelines stating the requirement for an audit trail [3]. The trainers at the College of Policing identified these shortcomings, and issued a specification requesting a means to encapsulate the func-

tionality required into a single tool; this prompted the creation of Open Source Internet Research Tool (OSIRT).

2.3 OSIRT

OSIRT is a free and open source C# application available under the MIT license for Windows 7, 8, 8.1 and 10 with a repository available on GitHub at https://github.com/joe-williams-cccu/OSIRTv2. Portable and installable builds are available at http://osirtbrowser.com/get-osirt/, where feedback is highly encouraged by the developer.

OSIRT is a web-browser and investigative tool that is designed to aid LEOs of all skill-levels to conduct OSR. OSIRT automatically logs all websites visited, allows the capture of full-page and partial screenshots in addition to video capturing, along with a plethora of other tools for the digital investigator to effectively conduct OSR while adhering to the law and procedural policies. Gathered intelligence is automatically logged within an evidential container, hashed, then date and time stamped with a report then generated for dissemination.

OSIRT's overall goal is to provide an accessible piece of software for all LEOs to conduct OSR on both the surface and deep web.

OSIRT's development was split into two phases. Firstly, a prototype was rapidly created that implemented much of the core functionality from the initial requirements. This prototype allowed for garnering feedback, which ensured OSIRT was the tool LEOs required to conduct OSR. Secondly, a 'release' version was generated based on the prototype, and this version is the basis of this paper.

As the RITES course runs throughout the year, it offers an opportunity for continuous feedback from users; allowing features to be dynamically implemented, giving maximum flexibility. As an incremental approach provides users with a "core product" [4] additions to OSIRT can be made as a result of law enforcement evaluation and response.

2.4 FLOSS Integration into UK Public Services

In 2012, the UK Government released a report acknowledging FLOSS "is not widely used in Government IT" [5]. This is contrary to previously issued guidance, as early as 2004, that pushed for more governmental agencies to make use of FLOSS. Current policy sees that FLOSS should be "actively and fairly consider[ed]" over its proprietary counterpart [6]. During the UK Government's re-push for FLOSS integration, they released alongside their 2012 report a list of FLOSS alternatives to well-known proprietary systems [5]. In November 2017, the UK Government once again stressed the use of open source "to improve transparency, flexibility and accountability" [7] and provided a 15-point guide to evaluating the use of open source software.

Waring and Maddocks [8] also highlighted that FLOSS was seldom used in the public sector, perhaps due to skills shortages, but those with a "degree of autonomy" may be more able and willing to integrate FLOSS. Law enforcement within the UK are allowed some choice, in which IT decisions, depending upon an officer's skill set, can

be made on an individual level. That said, there is little data surrounding what software law enforcement are using and for what purpose.
The potential reason for the slow uptake of FLOSS is that it may bring with it negative perceptions. From personal experience, it is not unusual to receive communications surrounding OSIRT's provenance and why the software is free-of-charge. Questions typically fall in to one of five categories: security, maintenance, technical support, cost and training. These are five points will form the focus of the case study surrounding OSIRT as a FLOSS product.

3 Methodology

3.1 Interviews

Two sets of interviews were conducted, the first were sixteen semi-structured interviews held with LEOs taking the RITES course, along with two interviews from the RITES course trainers and four interviews by officers from UK constabularies. All officers interviewed had experience conducting OSR, and had been in a policing role ranging from 6 to 22 years. These interviews covered their experience of using OSIRT over the RITES course, along with general questions involving their experience conducting OSR and what existing tools they used.

The second batch of interviews looked at OSIRT's integration and the impact of FLOSS into a police force with three participants being interviewed; an Inspector, Detective Constable and IT Administrator. The police service in this case-study has approximately 40 active OSIRT users. The three participants were chosen as they all have a different perspective when integrating or using software. Questions to these participants looked closer at OSIRT's integration as a FLOSS product and how it can make an impact. These questions looked at five key areas: Trust, maintenance, technical support, cost and training.

All interviews lasted from 15 to 45 minutes

3.2 General Questionnaires

OSIRT is used extensively during the RITES course, performing a central role where LEOs use it to conduct an open source investigation, capturing evidence for a fabricated case; a task performed throughout the five days of the course. This fictitious investigation provides a robust scenario in which OSIRT can be thoroughly tested by the very users it is intended for. Additionally, each increment of OSIRT is beta tested on the RITES course before general release, and by several LEOs in a live environment. Feedback is sent directly to the author from the LEO, or collated by the lead trainer and passed back.

This study used an opportunity sample to distribute questionnaires to 42 attendees of the RITES course over five courses. The questionnaire focused on OSR, existing tool usage, FLOSS and OSIRT.

4 Results and Discussion

4.1 Case Study Interviews

Trust and Security. A common question received in one form or another is "How can I trust this software?" this is an important question any user should be asking when using software, but it is particularly important on sensitive systems such as policing where evidential artefacts are being obtained. All three interviewees highlighted being able to trust software as being an important factor of usage. The Inspector said "We trust OSIRT because we've spoken to you, and we can contact you. If this was some software made by 'who-knows' then it would be a different story". The IT administrator also highlighted the fact OSIRT being open-source made trusting "easier" and although they are "not an advanced programmer" just the thought of the source code being available provides peace of mind.

Without being a large software distributor, it is, understandably, hard for those to trust a product made by an individual, making OSIRT open source was an attempt to assuage those concerns. OSIRT is both linked to a university and has collaborative links with the College of Policing, aiding in abating trust issues.

Maintenance. Updating is a challenge that is faced by any development team, but as a lone developer working on an FLOSS project, this concern feels amplified by potential consumers. The IT administrator highlighted this initial concern surrounding OSIRT, "We need to ensure our systems are water-tight, so updates are important." The Detective Constable highlighted the dynamic nature of their work and the importance of keeping abreast of current technological advances as a key driver for updates "It feels the nature of my work changes on a yearly basis, who knows what I'll be working on next year, so having a tool that keeps on top of that, like OSIRT has been, is important to me".

The Inspector also noted that updates were "important" but spoke about skills within the police service that may aid in development. Some police services within the UK are adopting 'cyber-specials', a volunteer group with exceptional skills in areas of cybersecurity. The Inspector said that "Given that OSIRT is available [open-source] means we can look at giving the [cyber] specials tasks in updating OSIRT". OSIRT, presently, has no developer community beyond the author so an opportunity to work with volunteers in policing roles provides a good opportunity to extend and maintain OSIRT.

Technical Support. While closely linked to 'maintenance' the ability to provide support and help if needed was an issue raised by all participants. The Detective Constable, who is a daily OSIRT user, highlighted the need to be able to reach out and how "scarce" technical support is, particularly for free tools. "The thing with paid for tools is that, as part of the contract, technical assistance is part of the cost, so we can reach out". This officer felt that was not always the case with free tools, where there is no contact available. "I've had my fingers burnt before where I used some open source tool and it stopped working with an error message, but I had no way of con-

tacting the developer". The Inspector echoed this sentiment, also adding the ability to reach out and get support if needed was "crucial".

The IT administrator agreed with this, too, but said that this is "par-for-the-course" using FLOSS and that expectations of support should be lowered. "To me, this is the sole trade-off. You lower the initial costs, but may face larger ones supporting free software".

Cost. Unsurprisingly, the cost of OSIRT was a driving factor in its implementation within this police services' system. The Inspector said that they had looked at "a couple of other tools", however, the cost of these tools was "too high" with some of the tools being "£60-£150 a user per year." The Inspector also highlighted that buying licenses could be better spent, "If I wanted to roll that out, that would cost me thousands but I have OSIRT for free which means that budget can be spent on other things.".

The IT administrator also noted cost and said "money does not necessarily mean better quality". While the administrator said that where proprietary software was used, they were in a position to look at FLOSS alternatives if needed. The administrator said that some forces "may not have this flexibility [to introduce FLOSS] due to policy, but things are changing.".

The Detective Constable was, seemingly, least averse to cost and instead highlighted the importance quality software was to deliver the "best service" whether the best software was free "shouldn't decide what's best for the best results, luckily OSIRT for me is the best tool for the job", but they "understood" why management would be forced to look at free alternatives.

Software where there is no immediate charge may invoke a 'try before you buy' response as there is not a commitment to integrate the product if it does not work out.

Monetary costs are not the only considerations to any implementation of, or change to alternative, software. Further considerations include costs in time, deployment and training

Training. One issue surrounding the use of more FLOSS products was the need to provide training on the new technology. This is not particularly a FLOSS issue, as any piece of software will require famarliarisation. The Detective Constable spoke about the "comfort zone" and changing an officer's workflow may cause them to "resent" the new software; highlighting the need for a robust training plan to abate those concerns.

The Inspector highlighted additional 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".

OSIRT is fortunate in that it is used as the tool on the RITES course, providing officer's hands-on use over the five-days as part of a wider training package. Additionally, as part of OSIRT's development, usability tests have been conducted by means of observations, SUS questionnaires [9] and cognitive walkthroughs [10]. Conducting

these usability tests, arguably, enhance OSIRT's ease-of-use which may then lead to require less training for OSIRT itself.

Summary. While this short case-study is not necessarily, nor does it claim to be, representative it does highlight experiences, thought-processes and issues faced by those using and making decisions when integrating software into systems. These interviews are reflective of the conversations had with several police services within the past, and while anecdotal in nature, does support the need for, and successful implementation of, OSIRT in law enforcement systems.

4.2 OSIRT Interviews and Questionnaires

This section looks at the 22 interviews and 42 questionnaires conducted with various LEOs and trainers. The topics covered OSIRT and how, if applicable, the participants conduct OSR.

OSIRT as part of LEO Training. Interviews and discussions with the lead trainer for the RITES course have shown that OSIRT has had a positive impact. The lead trainer noted that before OSIRT, the audit log was all maintained within a spreadsheet. "[Spreadsheets] were so time consuming, and you've noticed on the course we have people with different skill bases, so if you add the complexity of trying to operate a spreadsheet, trying to fit an image inside a cell on top of all the tools they have to use, you can imagine how complex that is. OSIRT pulled that all together, and streamlined the process".

Since OSIRT has been introduced on the course, there has been a "large increase" in the number of students who fully complete the 'live' open source investigation, where previously auditing and reporting were identified as issues.

OSIRT Integration into Workflow. Respondents were asked in the general questionnaire "Can you see OSIRT being integrated into your current role?" thirty-six out of forty-two responded "Yes". During the interviews, participants from the RITES course were asked about how they could see OSIRT's integration into their roles, with thirteen participants making positive comments that it would be "simple" or "easy" to do so. A response from a Detective Sergeant noted "It's quite a simple sort of transition to move away from our current system, which is to use pen and paper to record things, and straight into using OSIRT", another noted that their procedure involved a spreadsheet and a notebook, and while they would not stop hand writing notes, OSIRT's automated logging of actions was "a God send". Those that could not see OSIRT being integrated either said their current IT infrastructure makes it too burdensome (two), or that OSIRT could not integrate into their role at all (one).

The four officers interviewed from the constabularies, who have been using OSIRT as part of their investigations, all noted OSIRT has saved them time. "Its [OSIRT] at least halved, probably more actually, how long it takes me to conduct [open source] research", noted one interviewee.

Automated Logging and Reporting. The end product after an investigation is crucial for LEOs with all respondents noting the report output by OSIRT was in their top three features. An interviewee noted that reporting "[…] can be a complete pain, so anything that can do it for me is fantastic", a sentiment largely echoed by nine other interviewees. While the report generation was popular amongst respondents, seven interviewees did mention that the report could do with some cosmetic changes.

The automated logging of actions was another popular choice, with thirteen LEOs acknowledging during the interviews that logging every minute action as not possible. An interviewee noted that "Seeing my audit in OSIRT surprised me, […] I performed a lot of actions that I wouldn't really think twice about. Opening Google, performing a search and clicking a link are actually three [actions], but I've always considered [it] just one". The majority of interviewees all explicitly mentioned how the automated log was a time saver.

Respondents to the questionnaire shed some light as to why the automated logging and reporting is an ideal feature, as when asked in the questionnaire "How do you maintain an audit log when conducting OSR?" all respondents used some manual means for logging. Table 1 summarises their results. Multiple answers were selectable; hence the responses exceeding 42.

Table 1. How LEOs maintain their audit log

How do you maintain and audit log when conducting OSR? (Select all that are relevant)	
Spreadsheet (E.g. Excel)	26
Word processing document (E.g. Word)	17
Pen and paper	10
In-house solution	4
Zotero (or other bookmarking app)	2
Web browser's inbuilt bookmarking functionality	8
Forensic CaseNotes	3
Notepad/++	2
I don't maintain an audit log	0
Other	4

OSIRT's automated logging and report generation were very popular amongst interviewees and questionnaire respondents. It was not unusual to hear an officer criticise the monotony of having to manually maintain an audit log, and how an automated system is better not only to save time but to also ensure guidelines and policies are enforced.

Screen Capturing. The ability to capture screenshots and screen recordings was also favourable among respondents. Interviewees frequently commented that having this functionality for free is good, as they do not necessarily have the budget to afford the

licenses for some tools. “Screen recording tools can be very expensive, or have an upper limit of how much you can record if they are free. The inbuilt video capture in OSIRT does not impose limits, plus it’s free.”. One interviewee said, when asked about what screen capturing tools they use, “Anything I can find and is free. I used to use *FastStone Capture* but the free trial run out, and I cannot obtain a license.” A similar story was raised by six other interviewees.

Ten interviewees commented that being able to take full-page screenshots of large pages, such as Facebook, was beneficial to them. An interviewee noted “We have to take small screenshots, then stitch them back together. So OSIRT is going to be extremely useful.”

5 Reflection

Developing OSIRT has been a highly rewarding experience and has provided opportunities to deliver a useful tool for law enforcement. OSIRT’s growth has seen it shift from a simple training tool to use across the globe, with a userbase ranging from Barbados to Israel. While OSIRT’s growth is exciting, it has brought with it additional challenges. OSIRT was written only with UK law enforcement in mind, and as such is British-centric in its design. Obviously, the nature of the Internet makes nothing localised and purposeful software will disseminate to wherever it finds a use, and this brings with it a need for internationalisation.

Being an academic, sometimes it is easy to forget that software must be shipped and that people are going to be using it, and will need support. Thankfully, OSIRT is buoyed in the policing community with many questions answered before being contacted. That said, if OSIRT did not have that internal support it would be considerably harder to manage as an individual.

6 Conclusion

Over the past three years, OSIRT has gone from a prototype used on the College of Policing’s RITES training course to a fully-fledged piece of software used by various law enforcement agencies and individuals across the globe. OSIRT has been well received, with responses pointing to its rich feature integration and time saving through automation as a significant reason for this positive reaction.

Feedback is continually given and encouraged, with this avenue providing feedback which enhances OSIRT’s trust and offers an opportunity for growth. The case-study highlighted the balance OSIRT must straddle with being FLOSS, and the importance that trust, support, maintenance, cost and training have. There is a conscious need to ensure pros of the software outweigh both the imagined and potential cons. Only by being aware of and managing those expectations can FLOSS flourish.

By receiving both positive responses and suggestions for improvement, OSIRT is perpetually evolving along a path dictated by the very people who comprise its target audience. Having such direction will be crucial in OSIRT’s continued development.

7 References

1. Dodd, V.: Britain's police budgets to lose £700m by 2020, amid rising crime, http://www.theguardian.com/uk-news/2017/nov/09/britains-police-budgets-to-lose-700m-by-2020-amid-rising, (2017).
2. Association of Chief Police Officers: Online Research and Investigation, http://library.college.police.uk/docs/appref/online-research-and-investigation-guidance.pdf, (2013).
3. Association of Chief Police Officers: ACPO Good Practice Guide for Digital Evidence, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, (2012).
4. Pressman, R.S.: Software Engineering: A Practitioner's Approach. McGraw-Hill Higher Education, New York, NY (2014).
5. Cabinet Office, Home Office: Open Source Software Options for Government. (2012).
6. Cabinet Office, Home Office: All About Open Source - An Introduction to Open Source Software for Government IT. (2012).
7. UK Government Digital Service: Be open and use open source - GOV.UK, https://www.gov.uk/guidance/be-open-and-use-open-source.
8. Waring, T., Maddocks, P.: Open Source Software implementation in the UK public sector: Evidence from the field and implications for the future. Int. J. Inf. Manag. 25, 411–428 (2005).
9. Brooke, J.: SUS-A quick and dirty usability scale. Usability Eval. Ind. 189, 4–7 (1996).
10. Wharton, C., Rieman, J., Lewis, C., Polson, P.: Usability Inspection Methods. John Wiley & Sons, Inc., New York, NY, USA (1994).