




Apr 25th, 8:30 AM

SiMPLE - Rethinking the Monolithic Approach to Digital Forensic Software

Craig Valli

Edith Cowan University, Perth, Western Australia, c.valli@ecu.edu.au

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Valli, Craig, "SiMPLE - Rethinking the Monolithic Approach to Digital Forensic Software" (2008). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 7.
<https://commons.erau.edu/adfsl/2008/friday/7>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



SiMPLE - Rethinking the Monolithic Approach to Digital Forensic Software

Dr Craig Valli

Edith Cowan University

Perth, Western Australia

Phone +61-8-93706013 Email c.valli@ecu.edu.au

ABSTRACT

This paper outlines a collaborative project nearing completion between the *sec.au* Security Research Group at Edith Cowan University and Western Australian Police Computer Crime Squad. The primary goal of this project is to create a software tool for use by non-technical law enforcement officers during the initial investigation and assessment of an electronic crime scene.

This tool will be designed as an initial response tool, to quickly and easily find, view and export any relevant files stored on a computer, establishing if further expert investigation of that computer is warranted. When fully developed, the tool will allow investigators unprecedented real time, on site access to electronic evidence whilst maintaining complete forensic soundness.

Keywords forensic, triage, images, project, police, case study

1. INTRODUCTION

The primary goal of this project is to create a software tool for use by non-technical law enforcement officers during the initial forensic investigation and assessment of an electronic crime scene. This project is being conducted by the *sec.au* Security Research Group at Edith Cowan University in conjunction with the Western Australian Police Computer Crime Squad.

This tool will be designed as an initial response tool, to quickly and easily find, view and export any relevant files stored on a computer, establishing if further expert investigation of that computer is warranted. When fully developed, the tool will allow investigators unprecedented real time, on site access to electronic evidence whilst maintaining complete forensic soundness. This tool is customer focused and should provide an efficient, effective and reliable response to electronic crime. It is anticipated that this will significantly benefit evidence discovery by

- Improved service delivery
- Facilitate at scene interview of suspects
- Enable at scene comparisons of images to environment (Children at Risk)
- Significantly reduce property seizure
- Reduce demand for specialist forensic examination by enabling immediate and local resolution of issues

It is anticipated that the software tool will, in combination with the development of training and protocols for its use, allow law enforcement investigators to collect electronic evidence that can be introduced into the scrutiny of a judicial process. This project has incorporated extensive testing to an international standard which will be used to prove the developed tool is fit for purpose.

The Computer Crime Squad (CCS) is responsible for providing the Western Australia Police (WAPS) with expert services in the investigation, identification, preservation, interpretation and articulation of electronic evidence. The ubiquitous nature of computers, the Internet, mobile telephones, computer networks and other electronic devices in society today has resulted in new and complex challenges for

law enforcement. Australians are avid consumers of technology having one of the highest adoption rates in the world. For law enforcement this translates into more offenders using technology to commit crimes, and electronic devices being a potential source of evidence for all crimes.

To add further complexity to policing within Western Australia the state is geographically sparse with a land area of 1 million square miles. Some crime scenes are located over 3000 kilometres from the main office of the computer crime squad in Perth. This means that personnel and equipment must be transported at considerable expense to these remote locations for on-site triage and for the presentation of evidence in court.

2. ONE SIZE DOES NOT FIT ALL

One of the major issues facing police is the ability to respond to electronically initiated crime. Much of the existing response capability is based around the use of solutions that have a significant investment in training of staff to a level where they become proficient enough to analyse and present electronic evidence in a court of law. The software and hardware solutions whilst in of themselves are very powerful forensic analysis tools in the hands of suitably qualified experts are in some regards a self deprecating loop. The deprecating loop is as a result of increasingly high levels of specialisation and training required for the expert use of these increasingly complex “forensic” tools even for simple tasks. So it logically and legally follows that use of these expert tools by other than suitably acquitted staff may rightfully produce polemic evidence or outcomes. Therefore, instead of having a simple purpose built tool or process that can be used by individuals with minimal training to affect a simple profiling exercise, organisations are increasingly compelled to use complex and expensive software driven by well-trained, niche specialists to undertake even simple preliminary investigations. A further effect is that of a positive feedback loop for the investigation of incidents, which overtime, regardless of magnitude, size and seriousness, will require increasingly higher levels of expertise and equipment.

This feedback loop is the equivalent of using a large laser level guided 30 tonne bulldozer to dig a 20cm x 20cm x 20 cm deep hole in free flowing sand. Although technically feasible, the particulars of a task can be accomplished far more easily, efficiently and effectively with a purpose built trenching shovel. This is the argument underpinning fundamental principle of design used in this project and that is that less is more.

Currently, there are a multitude of security and forensics related bootable CDs available for download on the Internet or distributed restrictively by police forces that are potentially suitable for use by experienced and expert users for forensic analysis. There are however, several serious forensic problems and quality issues with the use of these CDs as “baseline” systems on which to build systems. Firstly, the author challenges any user of either KNOPPIX STD (Cumming, 2008) Helix (e-fense, 2008) or any similar monolithic bootable CDs to describe the purpose and function of all security related binaries on these systems. It is possible to by using these CDs to produce polemic outcomes for a prosecuting party. For instance, Helix contains known malware and penetration testing tools none of which should have a place on a system that is being used for initial examination of a suspect’s computer or device, yet some investigators persist in using Helix for initial examinations and acquisition.

The issues of binary abundances aside there are basic and fundamental forensic operational issues with these CD systems. A stark example is a default installation of KNOPPIX STD by default mounts any swap spaces on the hard disks that are present in the computer. This is not an ideal outcome when the only evidence that may be of any use in a prosecution now resides in a contaminated swap file as result of the use of the CD by a forensic novice.

Due to the large number of binaries in existence on these CDs the subsequent menus are extensive, complex and require significant understanding. Each binary not required for a particular purpose relating to the forensic process being undertaken potentially also introduces another compounding

variable into the forensic integrity equation. Furthermore, this large monolithic approach is similar to the bulldozer example above. Take a simple task such as cleaning media and then imaging and validating the subsequent image. Why do you need to use something as complex as Helix, Knoppix or even monolithic commercial tools to do this. It would be smarter, less contentious and more prudent to use a small purpose built and tested CD containing the operating system and only the required specialist binaries. In this case a validated bootable CD with dd or other suitable imaging program and requisite utilities to produce hashes of the acquired images and requisite system logs would be sufficient.

Furthermore, a problem with the multi-purpose security or forensics CD is that many of them will start various additional services some of which may compromise the forensic integrity of the computer under investigation. In addition, this mode of operation causes often unnecessary use of computer resources in terms of processor and memory, which can be better utilised in performing the required forensic task at hand.

One of the advantages of the bootable LINUX environments is that they can be fully customised to suit a specific need or requirement. For experienced users this is a relatively simple task to accomplish and normally requires a CD burner and a PC with sufficient RAM and hard disk space for decompression and recompression of the resultant CD image. This well established process allows for the production of highly customised, highly specific niche CDs to be produced for use in variety of ways. For this reason the system under development has utilised a Linux bootable CD environment for its development.

Fitness to task

As mentioned previously one of the major problems is the availability of solutions that will allow a non digital forensic specialist or private investigator the ability to preview evidence at scene in a forensically sound manner. While EnCase (Software 2008), Forensic Tool Kit (AccessData 2008), Helix or KNOPPIX STD etc are all competent tools they are not suited for use by the mainstream police or private investigators for the same could be contentious at best in a court of law.

One of the major issues faced by most computer crime teams globally is the possession and distribution of offensive or illegal images via the Internet. These images are typically sexual in nature and normally relate to paedophilia, bestiality, rape and other criminal acts. One of the advantages for the offender in remote Australia is that the accessibility of the Internet has made it easier for them to acquire images of an illicit or illegal nature. The potential offender's machines are often located in remote locations and normally are in regions where specialist crime facilities are scant and reduced in size. This has a serious implication for policing as seizure or on-site triage of such equipment requires specialist skills or expert status not normally found in these rural and remote locations. Excluding remote areas, there is strong evidence to suggest that the possession of illegal or illicit images is increasingly becoming the volume crime of the digital crime area with successful campaigns netting a wide range of offenders in geographical locations and societal strata (Scoop, 2008; McAuliffe, 2001).

This current status quo scenario has precipitated the need for a validated tool for use by mainstream police to enable them to undertake sound digital forensic examination of topical images found on a computer. From this scenario several design considerations are mandatory for the tool/CD and should:

- Be able to be used with a minimum of computer knowledge or training to extract images
- Be forensically valid and minimise polemy in its *modus operandii* and construction
- Allow for easy extraction of evidence and duplication to forensically clean media.
- Allow for subsequent presentation of evidence from the media.
- Use validated and tested tools in its production

3. THE SIMPLE APPROACH

The approach by the development team has been the production of a single purpose, specialised tool to use for profiling of a suspects computer that has a simple to use interface. Unlike other similar CD projects the startup of the CD and subsequently the program is treated as a first part of a atomic and complete process that concludes with successful output of the suspect images to DVD in a readily readable format. All means of input other than that which is required has been trapped or disabled, reducing the ability for someone to subvert or pervert the process.

The SiMPLE approach is to search only for topically found files i.e no file carving or overtly forensic process is used to locate candidate files for examination. This does limit the search capabilities of the tool but the law enforcement advisers believe this to be the least contentious approach. The law enforcement experience has been also that offender's motivation in viewing this type of material is one of quick access and viewing for gratification which is counter to the use of erasure and encryption processes.

The project has had staged development and testing throughout and has been so far broken into four distinct but coupled phases. Each phase has been subject to extensive and rigorous testing. These stages are the production of base operating system, production of image indexing, production of image viewer and output of results.

Base Operating System

The underlying kernel is a Gentoo kernel that is monolithic containing all possible drivers relevant to the preview and output of suspect material. The team determined that the ad-hoc loading of kernel modules would increase the complexity of verification and potentially lead to possible complications with evidence and the expert ability of the user. The kernel although monolithic with respect to drivers needed for display and output of images does have a reduction or elimination of unnecessary drivers. The kernel itself is stripped for example of all network drivers and the SiMPLE CD is incapable of initiating a network session. This reduction removes the contention that the investigating machine was compromised by a network borne Trojan, virus or RPC malware during preview of the images. It also disallows the loading of network file shares and other network based services that may introduce issues into the preview.

Furthermore, all unnecessary binaries from a default install have been removed. The design tenet is if it does not have a purpose in the indexing, preview and output it does not have a place on the CD. This tenet further reduces dispute about the CD eliminating the possibilities for misuse or misapplication unlike the typical monolithic security/forensics CD such as Helix or KNOPPIX STD that contain hundreds of unnecessary binaries. The system is also designed to operate on a Pentium 3 standard PC with 256Mbytes of RAM.

Image indexing

This process currently spawns as a series of scripts that search the hard drive for topically stored images or movies. The resultant topical files found are indexed, hashed and their location stored in a database structure. This database structure is then used to retrieve details about the located files for use by other parts of the program or process for example final output of the results to DVD media.

Image viewer

The image viewer is a simple to use application that allows an officer or investigator to preview the located files visually. It creates an initial thumbnail view of all the located files, the user is then able to select a larger view of the file (in the case of a graphic) or allow the viewing of a video file by clicking on it with the mouse. Then, if the investigator wishes they can select the image for later output to the DVD by selection via simple check box.

Output of results

The final process is the output of results to sterile media, in this case a blank DVD. USB memory sticks were considered initially but issues with management and handling with respect to continuity (chain of evidence) were thought to be unnecessarily complex. A USB-based DVD burner is connected to the suspect computer allowing for the export of material of interest. In addition to exportation of the selected images and files, the program also outputs a full forensic log of all activity undertaken during the process. In addition, to the program activity logs, all the relevant system based logs are also written to the DVD. All of the data stored on the DVD is in readily accessible HTML format, which allows viewing of the suspect's material on a wide range of platforms. Contained in the output is the file hash, file location (full path), file size and other relevant information.

Other relevant design features

The system also has some operational exception handling incorporated. The system will halt for particular instances for example if encrypted volumes or non Windows based partitions are located on the machine. These exceptions could possibly indicate obfuscation attempts by the person of interest and require higher grade of examination/scrutiny for resolution.

4. CONCLUSION

The SiMPLE project is nearing its first official beta and represents almost 4000 hours of effort from initial idea, to proof of concept and now release beta. The tool has already generated significant interest with the Australian Law Enforcement community with its simple, single task orientation.

Already the outcomes of this project have sparked the production and development of another application to extract registry keys and ownership identifiers from laptops proffered for sale on the second hand market or in the possession of a person of interest. The Laptop Inspection and Recovery System (LIARS) will be using the same base kernel and development approach of SiMPLE.

Operationally for police a tool like this, has significant potential to impact workloads and clear-up rates of digital enabled crime. This impact is that it allows non-forensically trained police officers to undertake profiling of a suspect's computer in-situ and immediately.

Finally, SiMPLE is about equipping police and investigators after a minimal amount of training with easy to use tools and techniques to recover rudimentary digital evidence. We can no longer rely on a monolithic and wholly expert approach to digital evidence collection if we are to combat crime. The systems have to be easy to use and have much of the expert knowledge embedded in the tool and its modus operandii. In the same way the most existing police are trained and able to take fingerprint evidence from the scene, SiMPLE is a tool aimed at enabling the digital equivalent.

REFERENCES

- AccessData. (2008). "AccessData - Forensic Toolkit® 2.0.",
<http://www.accessdata.com/Products/ftk2test.aspx>
- Cumming, M. (2008). "Knoppix STD." <http://www.knoppix-std.org/>
- e-fense. (2008). "Helix - Incident Response & Computer Forensics Live CD by e-fense", Inc."
<http://www.e-fense.com/helix/>
- McAuliffe, Wendy (2001). "Commercial child porn ring bust leads to 100 arrests",
<http://news.zdnet.co.uk/internet/0,1000000097,2092866,00.htm>

Scoop, (2008) "NZ tip uncovers international child porn ring",
<http://www.scoop.co.nz/stories/PO0803/S00050.htm>

Software, G. (2008). Encase. Pasadena, California, Guidance Software, Inc.