

LIARS – Laptop Inspector and Recovery System

Andrew Woodward
School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
a.woodward@ecu.edu.au

Abstract

Of the many notebook computers which are stolen, a large number are subsequently recovered. However, if the device is password protected, and the serial number has been removed, then it is difficult for police or other authorities to trace the legitimate owner. The squad dedicated to computer related crime do not have sufficient resources to conduct a thorough forensic examination of every laptop in order to determine its rightful owner. This project aims to produce a tool which can be used by virtually any police officer, or other person, which does not alter the hard drive in any fashion. This tool will be used to identify the original owner of a laptop with a view to having it returned to them. This paper outlines the various phases of the project and the testing methods that will be used to validate the tool.

Keywords

Forensic tools, software validation, linux, chntpw

INTRODUCTION

Laptop theft is of major concern for both individuals and business. For an individual, it represents the loss of a personal asset that they may not be able to replace easily, if at all. For a government agency or a corporation, it can represent much more: the loss of corporate IP or trade secrets. There are numerous statistics which attest to the fact that laptop theft is an on-going problem. Costs of laptop theft have two components: the hardware and the claimed value of the data on the stolen device. The most recent Australian report on computer crime, produced by AUSCERT, the 2006 Australian computer crime and Security survey, indicated that of those organisations surveyed, 58% reported theft of a laptop (AUSCERT 2006). This was up from 53% the previous year, but the year before that was also 58% (AUSCERT 2006). They also reported that 69% of organisations suffered financial loss as a result of laptop theft. No information was provided in terms of what proportion of the loss was due to the device itself, or any information contained on it. However, a value of 2.267 million dollars was attributed to laptop theft alone (AUSCERT 2006). Considering that there were only 126 respondents, when extrapolated to the whole of the Australian financial sector, this represents a significant loss. These figures also represent just organisations: they do not take into account theft of laptops from individuals.

The Western Australian Police have indicated that they recover a large number of laptops as a result of their inquiries. However, most of these laptops are erased and sent to auction, as there are not sufficient resources to enable identification of the legitimate owner. The volume of recovered laptops far exceeds the amount of staff available, meaning that unless the laptop can easily be accessed in order to identify the owner in terms of the information contained within it, then no further identification is attempted. This lack identification of recovered laptops creates two problems. The first is in the increased cost to both businesses and to consumers in terms of a rise in insurance premiums. Whilst a number of these devices are found, if their legitimate owners are not able to be found, then effectively, the device at least in the eyes of insurance companies, has not been recovered. The second problem has two aspects to it. The problem itself is in relation to the information contained on the laptop. If the device is not returned to the original owner then they have effectively lost all of the information on it. The other issue is that if the original owner cannot be identified, then the hard drive will be erased, and the information contained on it is again lost.

There have been some third party software vendors selling products which aim to aid in the recovery of stolen laptops (Absolute Protect 2006; BSS 2006; Computrace 2006). These programs work by placing a piece of code on the hard drive of the device, possibly in a hidden partition on the hard drive. This code communicates with the manufacturer whenever it is connected to the Internet. In the event that the laptop is stolen, the manufacturer attempts to track the laptop, presumably based on its IP address. When queried, the WA Police Force indicated that they rarely see such a system in use, suggesting that uptake by individuals and organisations is low (Duncan 2006).

This demonstrates the need for a basic tool which can be used by anyone with minimal training to allow for identification of the recovered laptops. This will allow for several important outcomes. The first, and most important for the legitimate owner, is the recovery of their laptop. Both the device itself and information contained in it will be important to them. To the police, identification of the original owners will allow for an increase in the so-called clear up rate, an aspect which is of importance to them. Thirdly, the insurance companies, who are ultimately responsible for paying for the replacement cost of the laptop, are also an interested party.

There are several aims and different stages of implementation for this project. The first phase is to develop a stable live CD environment, based on a linux distribution, which has been tested to ensure that it is forensically sound. The primary goal is to produce a tool which would enable someone with minimal knowledge of computers or forensic methods to identify the registered owner of a Windows XP based laptop. This will be done at a topical level, meaning that if the operating system has been formatted, then no information is likely to be found. Subsequent phases will see the drive examined at a level which will allow for owner registration data to be recovered from a formatted drive. When complete, the tool and underlying live CD system will be tested using established testing standards, such that its operation does not compromise the forensic integrity of the laptop.

PHASES OF THE LIARS PROJECT

There will be several distinct phases in the LIARS project. Initial phases will allow for simple data extraction, with subsequent versions allowing for recovery from formatted drives, and a final version which will have some preventative or reactive measures built.

Phase I

The aim of the first, as stated above, will be to produce a forensically sound CD which extracts basic information from a recovered laptop. It will be a simple process of making sure that the BIOS is set to boot from a CD, inserting the disk, having the application extract any user information (where available) and displaying it on screen. Other than checking the BIOS settings, no other user intervention is required or even possible. The tool will have been previously validated to ensure that it does not alter any information on the drive itself. At this point the assumption is made is that the drive does contain some data. If it has been erased subsequent to its theft then obviously no identifiable information will remain, or at least that is recoverable by the tool at this stage of its development.

Phase II

The second phase will be to expand upon the basic module, and look at deleted data. In the event that a laptop has been formatted, no data will be available to an investigator at a topical level. At this point, it will be necessary to examine the drive using a forensic analysis tool in order to attempt to recover information. This functionality will be added to the basic application, but user intervention, and thus training, will be kept to a minimum. As with Phase I, this phase will also be built upon the forensically validated Live CD, with the application itself also undergoing thorough testing.

Phase III

This is not really an extension to the LIARS investigation CD, but it is still related to increasing the rate of laptop recovery. In an attempt to cut down on laptop theft, this third phase will implement a proactive system where the

device is able to report to a central authority in the event that it is stolen. A hidden partition on the drive is used to facilitate this, with information allowing the device to connect to a reporting server somewhere to announce that it has been stolen. Whereas the first two phases allow for identification after the recovery of the device, this phase may also aid in its discovery. It is hoped that a large government department whose staff are issued with laptops would be used as a trial for this phase of the project.

DESIGN OF THE TOOL FOR PHASE I

There are three main components to the LIARS system: the underlying Live CD, the tool itself, and testing. All three are equally as important, but the Live CD needs to be established firstly, as the tool requires it to run. Testing will be very important, because although the information may not be used in a legal proceeding, there is the chance that it will, and therefore it needs to meet established forensic standards.

Assumptions

There is one main assumption or decision that has been made for this project and it relates to the operating system. This project will work from the assumption that the majority of laptops are running Windows XP as their primary operating system. This is a reasonably safe assumption, as Windows XP was released in 2001, and although Windows Vista is due for release shortly, it is not yet available other than in beta form. This assumption will cause some issues later on, particularly with Windows Vista being made available shortly. However, as with Windows XP, it is likely that it will be some time before Windows Vista achieves widespread adoption. It is estimate by the Western Australian police force that it took windows XP approximately 2 years to achieve majority use (Taylor 2006).

The Live CD

The premise of the LIARS is that it is able to be run on virtually any laptop, and that it does so without affecting the native hard drive. To achieve this, a live CD will be built, based on a linux distribution. This disc is effectively an operating system on a CD, which uses RAM for its data storage, and does not write any information to the hard drive. The process will start with a current bootable linux distribution, with any excess programs and processes stripped from the operating system. It is then recompiled and tested for functionality.

A Live CD is a customised version of a publicly available Linux distribution which has had any unwanted parts removed so that it will fit into the 640MB of space on a standard CD. The first of these was the Knoppix Live CD, upon which most other live CDs are built (Knoppix 2006). The Live CD is effectively an operating system on a disc, which can be booted on virtually any computer, be it a laptop or desktop. The original idea was to have access to a standard desktop or suite of applications wherever a user may be. This concept has been altered to produce standard utility disks, such as Helix, which contains is designed specifically for forensic incident response (Helix 2006). The LIARS project will take the concept a step further, and customise the operating system such that its only functionality is to contain enough drivers to boot the target computer, and run one customised application. No other functionality will be include on the disk, and there will be no means to access any other applications, should any be still contained in the files on the CD.

There are some other forensic tools available which aim to provide this sort of functionality, such as the previously mentioned Helix project, and the system preview and disk acquisition project (SPADA), but they have some serious limitations. The problem is that they are effectively a full Knoppix CD with specific forensic tools added. Another issue is that there is limited or no forensic validation, meaning that if the information was taken to court, it could be easily challenged. The greatest limitation, however, is that the user needs to have a high degree of knowledge of computers and of the Live CD itself. This makes such tools unsuitable, as the current problem of not being able to identify recovered laptops is lack of suitably trained staff. The LIARS tool needs to be able to be used by someone with limited or no skills, hence the need for a fully customised Live CD platform.

The Application - chntpw

The application to be developed for use will need to be able to extract information from the Windows registry, as user and owner data for Windows XP systems is stored in the registry hives.

One of the advantages of using a linux distribution is that it is covered by the GPL, meaning that source code of all programs is available. It also means that the software is available without any financial commitment. Although there are programs such as Registry Viewer available, this is proprietary software, which requires both licensing fees and the use of a dongle for its operation (AccessData 2006). Also, it will only run in a Windows environment, making it unsuitable for this project.

This project will use the chntpw utility, a program designed to change administrator passwords on Windows computers (Hagen 2004). Although designed for locating passwords in the SAM (security account manager) registry hive and resetting them, this program also has registry viewing and editing functionality. It is this aspect of the chntpw utility which is desirable, as much information relating to legitimate owner and any organisational registration information can be found in the registry. This software is also open source, which provides several advantages. The first advantage is that the code can be examined to make sure that there are no unexpected features or pieces of code which may affect the host system in an unwanted manner. The second is that as we have the source code, it can be altered or changed to suit our purposes, saving a lot of development time. The third is that there is no financial cost, as long as the original author is acknowledged.

Location of Information on the hard drive

When a Windows XP operating system is installed, the user is prompted to enter both their name, and that of the company, if applicable. This may or may not happen where the laptop is bought from a local supplier, but it is highly likely that this will be done where a corporate or standard operating environment (SOE) image is used. A search of an ECU laptop with an SOE image reveals many registry keys where the word "ECU" is found. In addition, there are numerous other applications which also store user information in the registry hives. Information is also stored about other applications, such as messenger clients and email programs (AccessData 2005). Table 1 contains a list of common user information and its location in the registry. Most of this information is stored in the NTUSER.DAT file. In addition to the information contained in the table, there are other locations and applications which store information about the user or registered organisation / owner of the laptop.

There are registry keys created by Office 2003, Office XP, Office 2000, Outlook Express and Outlook. In addition, virtually any software package that installs itself correctly will also create registry information which will contain the user's details. For example, the Adobe family of products contains this information. This is very useful, as virtually every computer has a copy of the freely available Adobe Reader in order to read PDF files (Adobe 2006).

Table 1: Information about the registered user, company, and other software variables and their respective location in the registry hive.

| Identifier | Key | Value |
|----------------------------|--|------------------------|
| Office XP Company name | HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\< GUID> | RegCompany |
| Windows XP User name | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion | RegisteredOwner |
| Windows XP Company name | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion | RegisteredOrganization |
| Windows XP User name | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\<GUID>\Products\<ID>\InstallProperties | RegOwner |
| Windows XP Company name | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\<GUID>\Products\<ID>\InstallProperties | RegCompany |
| MSN | \Software\Microsoft\MessengerService\Listcachce\NETMessen | |

| | | |
|--------------------|--------------|-----------|
| Messenger | gerService* | |
| Yahoo Messenger | | Last User |

FORENSIC VALIDATION

Both the underlying live CD and the developed applications and script will be tested to make sure that no alteration of the host system occurs. To this end, testing will be performed according to ISO 17025 (ISO 2006) and NIST standards (NIST 2006). Testing will also ensure that no unwanted application behaviour can occur as a result of random or unexpected key strokes.

The live CD

The following outlines the testing regime that will be used to validate the Live CD to be used for the application:

Forensic Soundness

Testing whether the file system has been mounted read only:

- Inspect mount points to verify all partitions are mounted
- Check System Logs to verify if mount status
- Use Linux utilities to verify mount status
- Attempt to manually write to partitions
- Attempt to change permissions on partitions

No changes are made to the storage device:

- Generate hard drive hashes (MD5 & Tiger) before and after use of the LiveCD, Compare to verify no changes have been made to the drive.

Accountability

All actions/ background process are logged:

- Execute predefined commands, check log files to ensure commands have been recorded correctly and check correct timestamp was appended.

Evidence Preview

Identify the hardware's, partition and storage devices:

- Ensure system and partition log files exist
- Check the integrity of the log files:
 - Compare the log files with existing information (system specifications should be noted before every test).

Ability to identify any errors or failures:

- Ensure the system generates an error message on the detection of an unsupported file system.
 - Use unsupported file system.
 - Use corrupted file systems.
 - Use encrypted file systems.
- Ensure the system generates an error message on the detection of an unsupported hardware's and doesn't meet the minimum requirements.

- Use unsupported hardware's.
- Use hardware's below the minimum requirements.
- Any other failures discovered while testing.

Security Testing

The following procedures are to ensure that there is no possibility of the user being able to enter an unauthorised mode and that there is no back-door into the system. It also ensures that no outside connections are possible.

Ensure no network connectivity exists:

- Check system information logs to verify network interface has not been detected
- Check network card driver is not loaded
- Check Ethernet Interface has not been activated

Tamper proofing

- Use predefined set of key commands in an attempt to close or bypass the GUI
- Attempt to enter interactive mode while cd is booting
- Attempt to open a system terminal
- Attempt to halt, reboot or crash the livecd product.

The Application

For the first phase, application testing will be fairly simple and will ensure that the hard drive is not altered, and that it is not possible for the user to interact with the subject laptop in any fashion. To this end, testing will mostly mirror that of the live CD.

CONCLUSION

The aim of the LIARS project is to develop a tool that can be used by a police officer, or other investigator, with little knowledge of computers. The tool will be produced and subsequently tested to determine its forensic validity with an appropriate framework. The Live CD which will be used as the base for the examination tool is currently undergoing testing. It is hoped that when the application has been successfully developed, that it will be used by the WA Police force in the field, and that its use will result in a significant increase in return of laptops to the official owner.

Future phases will add additional functionality to the LIARS system, with the ultimate aim to incorporate "phone home" ability. Future research will look at examining Windows installations for other sources of identifying information, in addition to those being used now. Searching of email for user details is a potential avenue which will be explored. With the impending release of Windows Vista, it will also be necessary to examine the tools functionality in relation to its ability to locate the same information.

REFERENCES

- AccessData (2005). Registry quick find chart, URL http://www.accessdata.com/media/en_us/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf accessed 18 September 2006
- AccessData (2006). AccessData Registry Viewer, URL <http://www.accessdata.com/products/rv/> accessed 18 September 2006
- Adobe (2006). Adobe Reader, URL <http://www.adobe.com/products/acrobat/readermain.html> accessed 19 October 2006

- AUSCERT (2006). 2006 Australian computer crime and Security survey, URL <http://www.auscert.org.au/images/ACCSS2006.pdf> accessed 10 October 2006
- Business Security Systems (2006). Stoptrack, URL <http://www.bsys.com.au/products/stoppremium.html> accessed 30 August 2006
- Computrace (2006). LoJack for Laptops, URL <http://www.lojackforlaptops.com/learn-more-lojack-for-laptops.asp>, accessed 30 August 2006
- Hagen, P.N. (2004) The Offline NT Password & Registry Editor, URL <http://home.eunet.no/pnordahl/ntpasswd/> accessed 19 October 2006
- Helix (2006). The Helix Live CD page, URL <http://www.e-fense.com/helix/> accessed 20 October 2006
- ISO (2005) General requirements for the competence of testing and calibration laboratories, URL <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39883> accessed 15 October 2006
- Knoppix (2006). Knoppix, URL <http://www.knoppix.org/> accessed 15 October 2006
- NIST (2006). Computer security division – computer security resource centre, URL <http://csrc.nist.gov/> accessed 15 October 2006
- Taylor, D. (2006). Personal Communication.

COPYRIGHT

Andrew Woodward ©2006. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors