Edith Cowan University
Research Online

Australian Digital Forensics Conference | Security Research Institute Conferences

2007

A Proof-of-Concept Project for Utilizing U3 Technology in Incident Response

Marwan Al-Zarouni
Edith Cowan University

Haitham Al-Hajri
Edith Cowan University

Originally published in the Proceedings of the 5th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, December 3rd 2007.
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/adf/15

A Proof-of-Concept Project for Utilizing U3 Technology in Incident Response

Marwan Al-Zarouni
Haitham Al-Hajri
School of Computer and Information Science
Edith Cowan University
usb@marwan.com
Haitham@MySecured.com

Abstract

This paper discusses the importance of live forensics and the use of an automated USB based smart data gathering technology to be used in incident response. The paper introduces the technology and its application in incidence response as well as highlight how it works. It also explains the tools that it uses to gather the live data from target systems. The paper also highlights some of the advantages and disadvantages of the technology as will as its limitations. The paper concludes with mentioning the importance of testing the tool and ways it can be developed and taken further.

Keywords

U3, Live Forensics, Incident Response, Computer Forensics, Network Forensics, Forensics Tools, Automation.

INTRODUCTION

Computer forensics is traditionally looked at as "dead" forensics. This means that the target system analysed is unplugged from the power source. Although dead forensics has less of a chance to modify data on the disk of the target system, it most defiantly loses "live" volatile data from the target system forever.

Live forensics which is more commonly known as "Incident Response" is an important aspect of digital forensics especially when it comes to cases involving network forensics or hacking which are incidents where live volatile data is of upmost importance. The aim of live forensics is to collect volatile data before unplugging the target system and to collect and preserve memory, process, and network information that would be otherwise lost with traditional forensics.

As the name implies, incidence response requires timely access to the target system and live data collection from it directly. This is considered by many as an intrusive way to collect data from the target system because it involves modifying and affecting the target system by using it to perform the live acquisition. Therefore, extensive expertise and knowledge when it comes to the target operating system (OS) must be possessed by live forensic investigators at the scene of the crime. This is because actions taken by them can and will alter the content on the target system. Therefore, the goal is to minimize impacts to the integrity of the system as much as possible while capturing volatile data from the system.

It is not always possible to have a live forensics expert at every incident and therefore there is a need for a basic tool which can be used by anyone with minimal training to allow for live capture of volatile data from target systems with the least interaction with the system as possible.

USB BASED INCIDENT RESPONSE

The purpose of this paper is to introduce a basic proof-of-concept USB-based tool that collects volatile data from target systems automatically and with little interference from the user of the device. This USB device can be used for live forensic data collection in remote areas or in areas where live forensic investigators cannot reach in person or in a reasonable amount of time or if there was a need to satisfy urgent investigation requirements.

Police Forces Operating in Remote Areas

The device targets police forces that operate in a wide geographical area and have limited staff when it comes to live digital forensics. This includes police forces such as Western Australian Police Force (WA Police) which operates the world's largest single police jurisdiction, an area covering 2.5 million square kilometres with a structure comprising three regions, 14 districts and 163 police stations (WAPolice 2007). The USB tool addresses areas that live CDs cannot address. It collects live volatile data and network and traffic related data that will be or may be lost in an event of a re-boot which is required by live CDs.

INTRODUCTION TO U3 TECHNOLOGY

U3 technology was developed to allow users to take their data and portable applications with them to any Windows XP based computer and to launch them automatically once the device is inserted in a USB port. Applications written for U3 smart drives were meant to be easy to install and provided users with portability without violating any copyright laws or end-user licences.

U3 Features

One of the most important features of U3 technology is the seamless launch of applications within the USB drive. This is done by fooling the OS into thinking that the USB drive is in fact two pieces of hardware rather than one. The operating system in this case thinks that the U3 device is a CDROM device and a USB storage device both inserted into the USB port at the same time.

The U3 in fact has two parts within it. The first part is a small part portion of the flash memory drive space containing an ISO image. The second large part is the remainder of the flash memory space which is used to store the actual applications and user data. An ISO image is basically a file with an extension of (.iso). This specifically means that it is compliant with the ISO 9660 standard which defines a file system for CDROM media. Generally speaking though, the term refers to any optical disk image. An ISO image contains both data and metadata such as boot code, structures, and attributes of files. In U3 devices though, the ISO containing portion of the U3 device appears to the computer as an actual CDROM disk within a CDROM drive which is contains an autorun.inf file which is used to automatically launch the U3 application. Figure 1 shows how Windows XP sees the U3 device.

Figure 1: The two devices under device manager and as Removable Disk (F:) and CD Drive (E:)

U3'S APPLICATION IN LIVE FORENSICS

As highlighted above, there are two features of U3 smart USB technology that distinguish it from normal USB drives. These features are:

- The ability to Auto-run once inserted into the USB port of a Windows XP system.
- Having a read-only ISO based portion

These features can be utilized in the forensic tool as follows:

- The auto-run feature can be used to execute a batch file that in turn runs the forensic tools contained in the read-only part to the USB drive (the CD ROM portion) and store the output from the tools into the re-writable portion of the USB drive.
- Having a read-only the (CD ROM) portion means that the tools can be stored in a tamper proof area which cannot be modified by the target OS thus insuring the forensic integrity of the tools.

THE AIM OF THE PROJECT

There are several aims and different stages of implementation for this project. However, this paper will focus on the first phase of the project which is a basic proof of concept device that contains the following:

- A Read-only virtual CD ROM portion of the U3 USB device which contains a basic set of too tools
- A Flash disk portion of the USB which is re-writable and will be used to store the collected evidence

The tool also features verification of the collected data via the use of hashing algorithms. The primary goal of the project is to demonstrate the capabilities of U3 technology the application of such technology to the area of live digital forensics.

CREATING AND UPLOADING THE ISO IMAGE

The U3 forensic tool works by auto executing a batch file which in turn executes other command line utilities in a consecutive order. These command line utilities and the batch file itself are placed in the CDROM portion of the U3 drive. This is done by first creating an ISO file containing the batch file and the utilities. MagicISO is the program that can be used for this purpose (MagicISO 2007). The ISO image is then renamed to cruzer-autorun.iso and placed in the same folder as the SanDisk's update utility "LPInstaller.exe". The update utility is then executed and what it simply does is replace the ISO image on the U3 drive with the one it finds in its folder.

Figure 2: Contents of installation folder:

The update utility "LPInstaller.exe" and

the cruzer-autorun.iso file.

PHASE 1 FOCUS AND LIMITATIONS

The first phase of the project will focus on one operating system (OS) namely Windows XP. The reason for that is that the CDROM auto-run feature is enabled by default in the Windows XP which makes it an ideal candidate for the U3 based forensic tool. Moreover, Microsoft tools can be obtained directly from Microsoft and can be used to capture volatile data from its operating system therefore ensuring that the source of the tools is trustable.

Because the auto-run feature can be disabled in Windows XP, it can be a limitation of the automation of the U3 tool. This can be easily overcome by manually double-clicking on the CDROM icon of the CDROM portion of the U3 device once the device is inserted in the USB port.

PHASE 1 TOOL SET

Phase 1 of the project focuses on using a small selection of utilities to collect some basic volatile information from the target system. The tools used are divided in steps based on the degree of volatility of data collected. Most volatile data is collected first. The steps are as follows:

- Pre Data Collection Step

1. Collection of Memory Related Data
2. Collection of Network Related Data
3. Collection of System Related Data
4. Collection of Log Files

The following section of the paper explains each of the above steps in detail. It discusses the data collected and displayed in the evidence data file. The U3 tool uses a batch file to execute each of the commands in the order mentioned from step 1 to step 4.

PRE DATA COLLECTION STEP

Before starting the actual collection of data, the batch file first determines the target drive letter where the information from the tools must be saved. This is because drive letter has to be the one associated with the re-writable portion of the U3 USB device. This is simply done by the process of basically finding the drive with a pre-determined folder in its root. This has to be a unique folder name, for example, a folder by the name of

"data_dump121123787238" or any other unique name. This path is then set by the batch file for the tools to dump their contents in. Then the batch file executes the data collection steps.

STEP ONE: COLLECTION OF MEMORY RELATED DATA

In this step, the tool will start by collection the memory related data such as, the loaded programs in the memory. The tool used to perform this operation is ***mem.exe***, it is an external command line tool, which can be downloaded from Microsoft's web site, and this tool has a number of extended operations (Microsoft 2007d). In addition to the ability to display the loaded programs in memory, it also can show the status of the programs along with the overall memory usage of the computer. Finally the last extension that will be used in this script is the option classify, where this extension will summarize, the overall memory utilization, along with the available free memory blocks.

STEP TWO: COLLECTION OF NETWORK RELATED DATA

This step is dedicated to the collection of network related data. In this step, a number of tools are used to collect network related volatile data:

Display Network Configurations

Using the tool ***ipconfig.exe*** displays the settings of the network along with other relevant information such as host MAC address, current network host, current IP address used by the host, the gateway IP address and additional network related data. Ipconfig is a standard Windows tool that is available in most of windows platforms but it can also be downloaded from Microsoft's web site (Microsoft 2007e).

Display Network Statistics

Netstat.exe is another tool from Microsoft, this tool displays the TCP/IP protocol connections on the host machine, in addition to the state of each of those connections, whether they are in lessening, established or in a time wait mood (Microsoft 2007b).

Display Network Settings

This is achieved by using the ***net.exe*** command which is an external command line tool from Microsoft (MSDN 2007a). This tool enables the forensic examiner to view the host network, and the network settings. This tool has many extensions with different data outcomes for each extension. Using the command ***net start*** displays the started windows services. This information can aid the forensic examiner in defining what the starting services on the host machine are. The second extension is the ***net session*** command which displays all the connected sessions to the host computer. The third command is the ***net share*** which displays the shared files on the network. This information can alert the examiner to the possibility of exploring different network shred folders. The forth extension of the net command is the ***net group*** which displays the network domain groups members, which the host machine is a member of. The fifth extension of the net command used in the U3 Forensic USB script is the ***net use*** which displays the remotely opened folders on the host machine. The sixth command extension for the net tool is the ***net user*** which displays a list of the user accounts within the host machine. The seventh extension command of the net tool is the ***net accounts*** which displays the accounts policy of the host machine. Finally the last extension of the net command is the ***net view*** which displays a list of the computers within the current domain. This option enables the forensic examiner to identify what computers are connected in this domain.

Display Routing Table

The command ***route.exe*** is a command line tool that is available in most of windows platforms and also can be downloaded from Microsoft's website (MSDN 2007b). This tool displays the information regarding the routing table including IP address, default gateway, and network mask. This information produces better understanding of the network configuration and therefore it will help the forensic examiner in his investigation.

Display Address Resolution Protocol (ARP) Table

Address resolution protocol, is a wide topic, especially when it comes to the digital forensics from the security point of view. Due to the fact that ARP is involved in many of the security issues. Address resolution protocol could be used in many forums of attacks, such as man in the middle, ARP poisoning, and ARP password sniffing (Bryner 2006). ***arp.exe*** is a command line based tool, from Microsoft, its available on most of windows platforms and could be downloaded from Microsoft web site. This tool displays the ARP table with the current

connections add IP address. The obtained information from the ARP table will provide the forensic examiner a better understanding of the network state.

STEP 3: COLLECTION OF SYSTEM RELATED DATA

This step is devoted towards the collection of relevant information regarding the host machine. The information gathered can be used as a verification of the host machine, in addition to other data that help the forensic examiner to identify any malicious activities on the host machine. The tools used in the step are as follows:

Display System Information

Systeminfo.exe is a command line tool, developed by Microsoft. This tool is available in Windows XP and can also be downloaded from the Microsoft website. This tool illustrates to the forensic examiner all the system information from the security level, configuration of the host machine operating system to the hardware system such as network cards, hard disks and other hardware devices (Microsoft 2007c).

Display Current User

A small utility program form Microsoft is used for this purpose and it is called ***whoami.exe*** which can be used to determine the current logged in user to the host machine (Microsoft 2007j).

Display MAC address

This tool, ***getmac.exe*** is a command based tool, that display the media access control of the host machine, this tool is ideal for quick retrieval of the host MAC address (Microsoft 2007j).

Display Log Events

The ***psloggedon.exe*** is command line tool is a part of PStools which are hosted under sysintermainls.com, and is available to download from the Windows website. This tool can identify who have logged into the machine locally (Microsoft 2007f).

Display a List of Open Ports

fport.exe is a freeware tool developed by FoundStone. It is a command line tool that displaces all TCP/IP and UDP connections and relates it all to their host application in addition to displaying the open ports on the host system (Foundstone 2007).

Display a List of the Current Running Process

pslist.exe is a command line tool that displays a list of the current running process in the system , this allows the forensic examine to verify which process is running, in addition it aids the discovery of malicious processes in the system. Moreover this tool has an extension command to display the process in a tree format which makes it easy to the forensic examiner navigate throw the process, this tool is hosted under Microsoft's SysInternals website (SysInternals 2007).

Show Process Services

psservice.exe is a command line tool that views the process services of the host machine, also it shows the configuration of the system and any running stopped process (Microsoft 2007g).

Schedule Process Using AT

At is a scheduling tool that enables the user to preset a task to be carried on in a specific time, this tool displays and schedules process on a host machine. Using this tool will assist the forensic examiner to determining any scheduled processes, or any malicious process on the target machine. This tool is available to download on the Microsoft's website (Microsoft 2007a).

Collect Server Uptime History

Uptime is a command line tool devolved by Microsoft which enables the forensic examiner to collect the uptime statistics of the host machine (Microsoft 2007i).

STEP 4: COLLECTION OF LOG FILES

Selected tools have been added to the USB toolset to collect log files from the target system. A list of the tools and a brief description of them follows:

Event Log

psloglist.exe is a tool that can view and save a list of the local and remote log events that accrued on the host system. If used without a switch it retrieves more information about the host system. If the tool is used with an extension such as system ***psloglist-s system***, it shows the system event log. ***psloglist-s application*** displays all the log events for the applications on the host system. This in turn allows the forensic examiner to trace the events of those applications. Finally the command ***psloglist-s security*** allows the forensic examiner to view the security event log. This tool is a command line based tool that can bee downloaded from Microsoft (Microsoft 2007h).

Internet Explorer History File

The ***iehv.exe*** tool allows the forensic examiner to view a list of the URL address that has been visited on the host machine, this tool can be used as GUI or in a command line. This tool has been developed by NirSoft. The tool is useful when the forensic investigator intends to get a copy of the URL address list from the host machine (NirSoft 2007a).

Display USB connections list

USBDeview.exe is a tool to list the USB devices that are currently connected and any USB that have been used on the machine before, the tool records sufficient information regarding the USB devices that been connected in the host machine (NirSoft 2007b).

This concludes the data collection steps and the tool pops up a dialog box to the user instructing them to remove the USB drive from the target system.

ADVANTAGES OF THE U3 DRIVE FORENSIC TOOL

One of the main advantages of this tool is that it requires no expertise from the officer at the crime scene. It also requires little action by the officer at the crime scene which means fewer things can go wrong in the investigation. Also, having both read only and read and write portions means that the evidence-containing U3 drive can be shipped to the forensic experts for evaluation. Another advantage of the U3 forensic device is that the re-writable portion of the USB drive can be forensically wiped and sanitized again for re-use in other live forensic cases.

DISADVANTAGES OF THE U3 DRIVE FORENSIC TOOL

One of the disadvantages of U3 drive forensic tool is cost when compared to the low cost of Live CD based solutions. A 4 Giga Byte U3 enabled USB stick costs between: 50-100 Australia Dollars which can be considered high when compared to Live CDs which cost under 1 Australian dollar. Capacity limitation is another issue and limitation that has to be taken into consideration when selecting tools to be placed into the ISO image and the amount of data collected from the target machine. Another limitation that has to be considered by the users of the U3 USB tool is the Limit of re-writes on Flash media and its limitations.

PHASE 2 AND BEYOND

Phase 2 of this project will be based on testing the U3 USB forensics tool using established testing standards, to determine its effects on the forensic integrity of the of the target system. Further testing of the U3 forensics tool in regards to compatibility with anti-virus and anti-hacking software should also be tested in the second phase. Even though the tools are saved in the CDROM portion of the USB drive and cannot be deleted by the programs on the target OS, they can still be stopped from execution on the target system which can hinder the investigation.

Further development of the tool can see the introduction of a new set of tools with more data gathering capabilities and further standardized testing at each phase of the project.

CONCLUSION AND FURTHER WORK

U3 technology has great potential when applied in field of live forensics as demonstrated in this paper. Further development of the project could see the formation of a USB-based framework for live data acquisition. Such a framework can then become the basis on which other forensic tools can be modified and adapted to work with U3 technology. This could then be used to develop truly portable forensic applications fully utilizing U3 technology.

REFERENCES:

Bryner, J. (2006) Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks, URL https://www2.sans.org/reading_room/whitepapers/threats/474.php?portal=6e96e71bd547149c4b10c3c7a5ce70f0, Accessed 2 November 2007

Foundstone (2007) Foundstone Network Security Free Tools, URL http://www.foundstone.com/us/resources-free-tools.asp, Accessed 2 November 2007

MagicISO (2007) MagicISO, URL http://www.magiciso.com/, Accessed 13 November 2007

Microsoft (2007a) HOW TO: Use the At.exe Command to Schedule a Backup in Windows NT, URL http://support.microsoft.com/kb/313289, Accessed 2 November 2007

Microsoft (2007b) Microsoft Windows XP - Netstat, URL http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/netstat.mspx?mfr=true, Accessed 2 November 2007

Microsoft (2007c) Microsoft Windows XP - Systeminfo, URL http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/systeminfo.mspx?mfr=true, Accessed 2 November 2007

Microsoft (2007d) MS-DOS 5.0 Internal and External Commands, URL http://support.microsoft.com/kb/71986, Accessed 12 November 2007

Microsoft (2007e) Options for Ipconfig.exe in Windows 2000, URL http://support.microsoft.com/kb/223413 Accessed 2 November 2007

Microsoft (2007f) PsLoggedOn v1.33, URL http://www.microsoft.com/technet/sysinternals/Security/PsLoggedOn.mspx, Accessed 2 November 2007

Microsoft (2007g) PsService v2.21, URL http://www.microsoft.com/technet/sysinternals/utilities/psservice.mspx, Accessed 2 November 2007

Microsoft (2007h) PsTools v2.43, URL http://www.microsoft.com/technet/sysinternals/SystemInformation/PsTools.mspx, Accessed 2 November 2007

Microsoft (2007i) Uptime.exe Tool Allows You to Estimate Server Availability with Windows NT 4.0 SP4 or Higher, URL http://support.microsoft.com/kb/232243, Accessed 2 November 2007

Microsoft (2007j) Windows 2000 Resource Kit Tools for administrative tasks, URL http://support.microsoft.com/kb/927229, Accessed 2 November 2007

MSDN (2007a) Net.exe Utility, URL http://msdn2.microsoft.com/en-us/library/Aa939914.aspx, Accessed 2 November 2007

MSDN (2007b) TCP/IP Utilities, URL http://msdn2.microsoft.com/en-us/library/Aa940250.aspx, Accessed 2 November 2007

NirSoft (2007a) IE HistoryView: Freeware Internet Explorer History Viewer, URL http://www.nirsoft.net/utils/iehv.html, Accessed 2 November 2007

NirSoft (2007b) USBDeview - View all installed/connected USB devices on your system, URL http://www.nirsoft.net/utils/usb_devices_view.html, Accessed 2 November 2007

SysInternals (2007) PsTools: Please READ Before POSTING, URL http://forum.sysinternals.com/printer_friendly_posts.asp?TID=3748, Accessed 2 November 2007

WAPolice (2007) Western Australia Police - About Us, URL http://www.police.wa.gov.au/ABOUTUS/tabid/893/Default.aspx, Accessed 12 October 2007

COPYRIGHT

Marwan Al-Zarouni, Haitham Al-Hajri ©2007. The authors assign 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. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. The authors also grant a non-exclusive license to ECU to publish this document in full in the Conference Proceedings. Any other usage is prohibited without the express permission of the authors.