

REPORT DOCUMENTATION PAGE			Form Approved OMB NO. 0704-0188		
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 28-08-2012		2. REPORT TYPE Related Material		3. DATES COVERED (From - To) -	
4. TITLE AND SUBTITLE A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis			5a. CONTRACT NUMBER W911NF-11-1-0174		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER 206022		
6. AUTHORS Jose de la Cruz, Dr. Jeff Duffany (Advisor)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Polytechnic University of Puerto Rico 377 Ponce De Leon Hato Rey San Juan, PR 00918 -			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211			10. SPONSOR/MONITOR'S ACRONYM(S) ARO		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S) 58924-CS-REP.16		
12. DISTRIBUTION AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.					
14. ABSTRACT Collecting a forensically sound memory image from a "live" system increases the effectiveness of the forensic investigation by providing analysts with enhanced data and context to extend the knowledge obtained from					
15. SUBJECT TERMS Digital forensics; Brute-force methods; Windows Memory Analysis					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Alfredo Cruz
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU			19b. TELEPHONE NUMBER 787-622-8000

Report Title

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

ABSTRACT

Collecting a forensically sound memory image from a “live” system increases the effectiveness of the forensic investigation by providing analysts with enhanced data and context to extend the knowledge obtained from long term storage devices.

? More, and better, data will most likely deliver better and more robust conclusions.

? Enhanced understanding leads to better policy development and application.

Why is it important?

? Capability to inspect disks protected by whole disk encryption

? Recover passwords for files, folders, etc. without incurring in “brute-force” methods

? Obtain “up-to-date” data on active processes

? Provide analysts with the capability to extract more information from the system by providing context to the “swap” disk area

? Obtain active (and “closing”) network connections

Project Proposal

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

April 20, 2012

José R. De la Cruz

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

Digital Forensics, or the application of forensic science and procedures to computers, has been defined by the Committee on National Security Systems, in CNSS Instruction No. 4009, as “*the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.*” Digital Forensics Analysts have dedicated most of their efforts to gather evidence from long term storage devices. The new “era” of robust and effective forensic analysis now includes the “live” portion of the target system; i.e. the data contained in memory.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Memory contents:
 - Page tables
 - Indexes
 - Passwords
 - Encryption keys
 - Network connections
 - Active processes
 - Clipboard contents
 - IM (Instant Messaging) information

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Memory contents (continued)
 - System time
 - Logged-on users
 - Open files and folders
 - Open port list
 - Port to process mapping
 - OS processes running in background
 - Hardware process data (drivers)

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Why is it important?
 - Capability to inspect disks protected by whole disk encryption
 - Recover passwords for files, folders, etc. without incurring in “brute-force” methods
 - Obtain “up-to-date” data on active processes
 - Provide analysts with the capability to extract more information from the system by providing context to the “swap” disk area
 - Obtain active (and “closing”) network connections

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- In summary, collecting a forensically sound memory image from a “live” system increases the effectiveness of the forensic investigation by providing analysts with enhanced data and context to extend the knowledge obtained from long term storage devices.
- More, and better, data will most likely deliver better and more robust conclusions.
- Enhanced understanding leads to better policy development and application.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Problems
 - Locard's Exchange Principle:
 - When two object's come in contact there is a transfer of materials between them
 - Changes will always occur on idle systems
 - Asking the system for information changes the state
 - Inability to create an accurate “bit-by-bit” memory image, or forensic copy.
 - Acquisition “speed” can render “outdated” memory contents, especially on very active systems.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Problems (continued)
 - In CNSS Instruction No. 4009, forensic copy is “*an accurate bit-for-bit reproduction of the information contained on an electronic device or associated media, whose validity and integrity has been verified using an accepted algorithm.*”
 - This definition is the main “problem” affecting the use of memory images for forensic analysis.
 - Because compliance with *forensic copy* cannot be validated, evidence derived from it can be refuted in court.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Project Goals
 - Conform to CNSS Instruction No. 4009 definition for forensic copy by “validating” a memory image to be correct and integral.
 - Determine, or map, Windows OS use of memory real estate in order to discard some areas of the memory or label them as unimportant.
 - Develop a protocol which ensures that data used from acquired image is indeed verifiable and its integrity can be proved.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Proposed Project Plan
 - Build Body of Knowledge that will support the development of the project.
 - Understand how Windows OS “uses” memory (physical).
 - Single out background and maintenance processes that do not include forensically relevant information.
 - Read and analyze methods or procedures suggested by others, and annotate weaknesses and strengths.
 - Collect, examine, and analyze current memory image acquisition tools and annotate weaknesses and strengths.
 - From previous two steps, develop initial protocol.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Proposed Project Plan (continued)
 - Select specific target system to be used in empirical testing scenario.
 - Develop test procedure.
 - Use initial protocol to acquire memory images at different time instances.
 - Compare the different memory images in order to single out the differences between them.
 - Analyze the differences so as to discard irrelevant data.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Proposed Project Plan (continued)
 - Develop initial “memory map”.
 - Use some “accepted” forensic analysis application to extract “evidence” from all memory images, and analyze the differences.
 - Refine protocol to account for errors or other actions that hinder the *forensic copy* acquisition.
 - Finally, publish results of protocol in a publication or Web site and invite others to test the protocol and submit reviews.

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Some Important Questions
 - Is it possible to develop such protocol?
 - Can the protocol be extended to other versions of Windows OS's?
 - Can the protocol be extended to other operating systems?
 - Is the protocol specific to a hardware & software set or does it apply to many other combinations?
 - Has the “*verified using an accepted algorithm*” requirement been met?

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

- Further Research Extensions
 - Can the same protocol be used in mobile devices?
 - Can the protocol be extended to other computer system related devices, such as routers, switches, printers, etc.?
 - Is there a need for the development and deployment of a specific tool set?
 - Would there be a “market” for such tool set?

A Forensically Robust Memory Image Acquisition Protocol Based on Windows Memory Analysis

