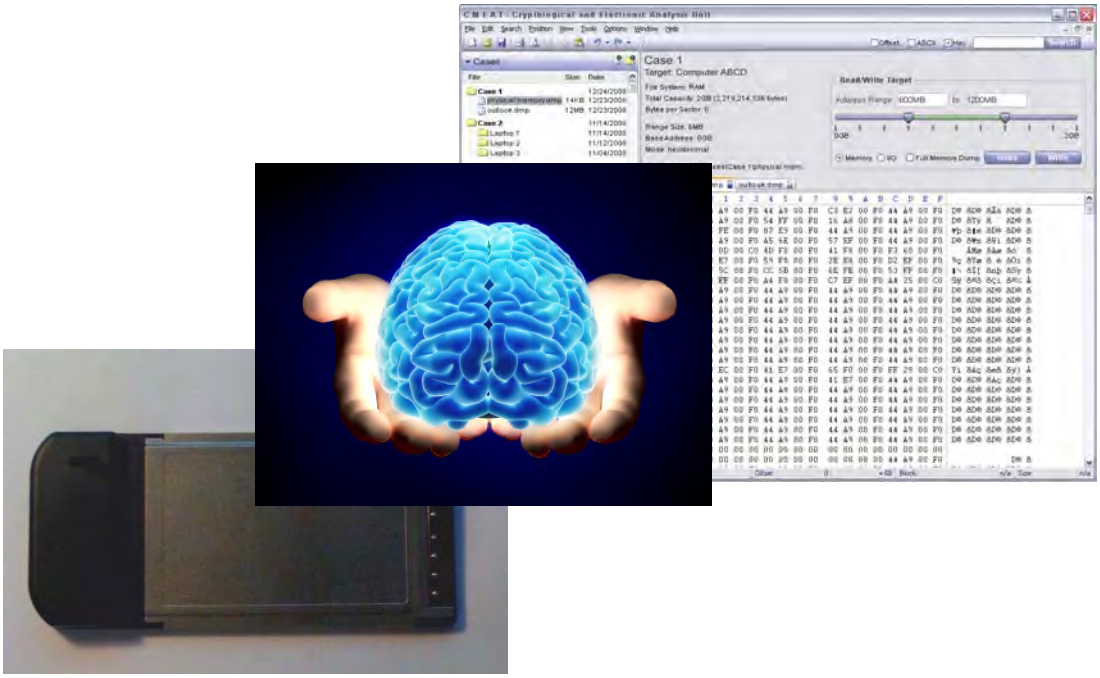
Memory Grabber

Computer Forensic Volatile Memory Acquisition and Analysis System

White Paper

6 May 2010



Prepared By:

Jim Costabile
Systems Research and Applications Corporation
8830 Stanford Blvd., Suite 205
Columbia, MD 21045
jim_costabile@sra.com
443-656-7247

Table of Contents

Table of Exhibits

1 INTRODUCTION

1.1 Purpose

The purpose of this paper is to describe the SRA Memory Grabber system, which provides memory access to a running and password protected laptop through the use of a small PC Card inserted into the PCMCIA slot of the laptop. The Memory Grabber device shown in the figure below is operating system agnostic; working on Microsoft Windows, Linux, and MacOS and is available today as a production unit for use with Express Card and Card Bus laptop systems.

Figure 1: Memory Grabber Device

2 OPERATIONAL NEED

2.1 Problem Description

Currently, when law enforcement agents or Special Operations personnel seize a running laptop that is password protected, they have no way of capturing the potential valuable information resident in memory. Typically, they will power down the laptop and take it back to lab to perform forensic analysis on the hard drive losing all information associated with the current state of the machine (e.g. partially constructed documents or emails, web history, or any other information that gets permanently deleted upon power down). Law enforcement agents and Special Operations personnel need a tool that provides memory access to a running laptop in the field enabling the timely capture of volatile information.

3 OUR SOLUTION

3.1 Solution Overview

The Memory Grabber system provides direct memory access to a running laptop via a small PC card (i.e. Memory Grabber device) that can be inserted into the external PCMCIA slot, similar to commercially-available external broadband network cards. The target laptop can be screen-locked and password-protected. The Memory Grabber system can be used in either tethered or un-tethered modes (see Figure 1), and supports both Express Card and Card Bus laptop interfaces. The system can be used to acquire data from laptops running various versions of Microsoft Windows, Linux and MacOS, and supports both 32 bit and 64 bit operating systems.

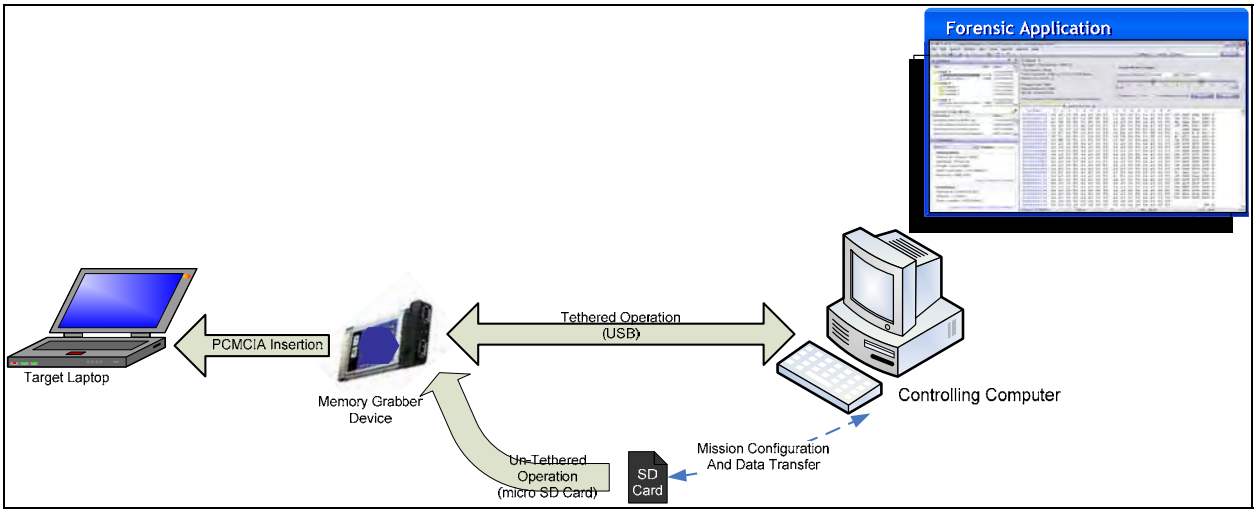


Figure 2: Memory Grabber Operational Context

In tethered mode, the Memory Grabber device is connected to a controlling computer via USB. Tethered mode provides the ability to perform highly user-interactive analysis. For example, the Memory Grabber system can be used in a laboratory to provide dynamic analysis of the state of the machine in debugging software applications or analyzing malware.

The un-tethered mode is intended for field use, providing a highly portable and less interactive mode of operation. In un-tethered mode, data in memory is acquired and written to a micro SD memory card embedded within the device. A full memory snapshot or targeted memory areas can be captured and saved for detailed analysis later in the lab. For forensic applications, the on-board processing resources provide the ability to compress and encrypt the captured data, as well as ensure data integrity (e.g. through the use of digital signatures or a hash function).

A forensic application running on a controlling computer provides memory forensic analysis, as well as device control and configuration, communications management and data transfer capabilities. The forensic application is constructed in a modular fashion, allowing the use of other COTS or custom tools such as hex editors, or data analysis systems.

3.2 System Details

The Memory Grabber system is a volatile memory forensic analysis tool that provides memory access to a laptop in a power-on state and possibly password protected via the external PCMCIA interface. The system consists of a specialized hardware device (Memory Grabber device) that provides a bridge between the target laptop and a controlling computer, and a forensic application running on the controlling computer that provides analysis of the captured memory as well as device control and configuration, communications management and data transfer capabilities. The system hardware and software architectures are depicted in the following diagram:

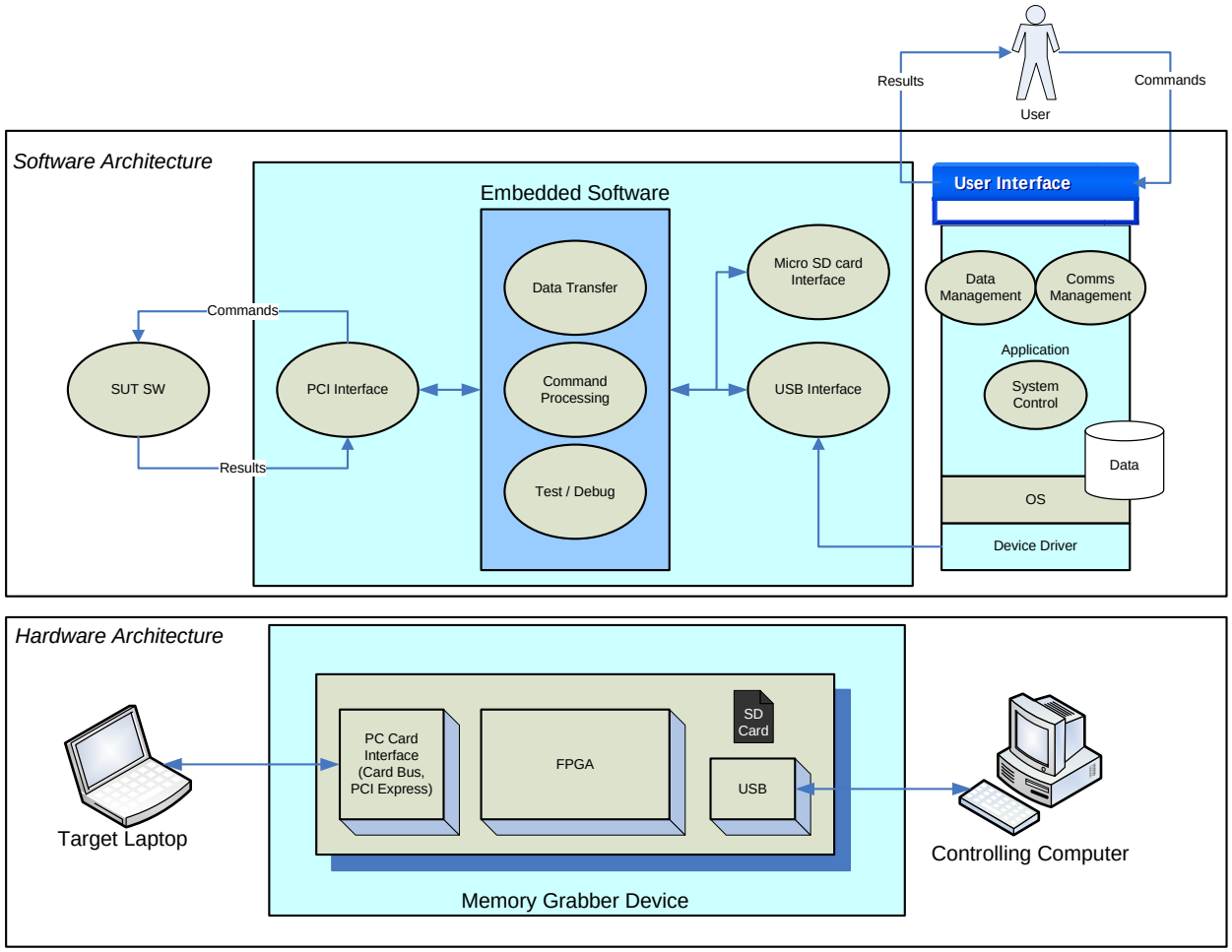


Figure 3: System Architecture

The specialized hardware platform is an FPGA based embedded system that provides the capability to implement the target laptop interface (ExpressCard or CardBus) as well as the controlling computer interface (USB, micro SD card). The FPGA also provides the capability to process information and bit streams and can be configured for unique operational scenarios very quickly due to the reprogrammable nature of FPGAs. The hardware platform has been designed in a modular fashion providing the capability to easily modify for other customer required interfaces.

The embedded software / firmware running on the device implements the external interfaces to the target computer and controlling computer, as well as provides the ability to perform processing on the captured data (e.g. data compression, or encryption). The embedded software also provides the ability to handle vendor-specific implementations of the external interfaces (e.g. Card Bus and Express Card) internally without the need for user interaction. This enables the system to be compatible across a wider range of laptops. As a part of our rigorous compatibility testing, we have verified the operation of the Memory Grabber device on a wide variety of laptops from different manufacturers running various operating systems including 32 bit and 64 bit versions of Windows, Linux and MacOS.

The forensic application running on the controlling computer provides basic memory access functionality and memory capture, as well as basic device command and control. The forensic application is written in JAVA to allow portability across multiple-platforms as required. Currently, it is running on Windows based controlling computers. The modular nature of our application design facilitates the ability to leverage COTS or custom analytic tools such as hex editors, display tools and debuggers.

3.3 System Specification

Table 1: Memory Grabber Specifications

Parameter	Express Card	Card Bus
Target Laptop OS	Windows Linux Mac OS (32 bit and 64 bit versions)	Windows Linux Mac OS (32 bit and 64 bit versions)
Operational Mode	Tethered (USB) Un-Tethered (micro SD card)	Tethered (USB)
Data Integrity Available	Yes	Yes
Data Acquisition Speed (nominal)	8 Mbytes per sec	2 Mbytes per sec

4 SUMMARY

The Memory Grabber system provides access to critical information resident in volatile memory even if the laptop is screen locked and password protected. The system can also be used to provide dynamic analysis of running systems allowing engineers to analyze and view active memory while a system is running. One example of this would be the analysis of malware to understand the program's memory footprint and how it affects the host system.

The Memory Grabber system is commercially available today, and has a defined roadmap to include new features and system extensions. The system has been designed in a modular fashion allowing easy customization and refinement based on the customer's unique operational needs. For more information, to schedule a demonstration or to discuss unique requirements and customization options, please contact us using the contact information on the title page of this document.