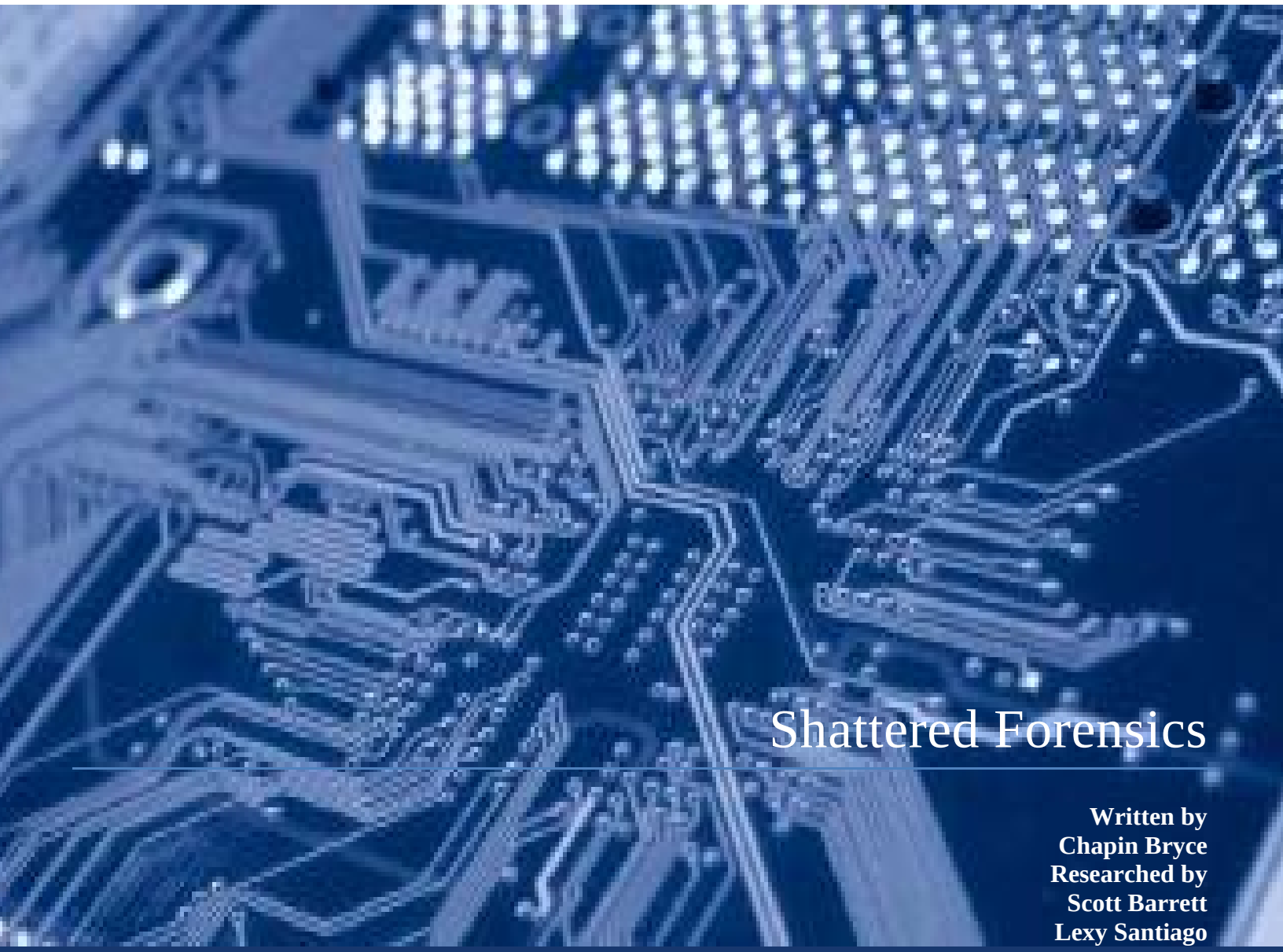
CHAMPLAIN COLLEGE | LCDI Leahy Center for Digital Investigation



Shattered Forensics

Written by
Chapin Bryce
Researched by
Scott Barrett
Lexy Santiago

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

5/7/14

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Shattered is an open source, Google Glass-specific Android acquisition tool that automates the process of gathering and processing artifacts on mobile devices such as Glass. The goal of this project is to provide a tool set to forensic examiners that is capable of effective analysis of android wearable devices.

Background:

Shattered was a product of the necessity to gather data for research on Google Glass at the LCDI. With such a potential value, it branched into a separate project focused on the development and improvement of the tool for the forensics community. With the expansions of modules and libraries, Shattered has grown to support the parsing of data in addition to the acquisition.

Purpose and Scope:

This tool provides a reliable method of acquisition of artifacts from Android devices, such as Google Glass. Though it assists the Leahy Center at Champlain College with research and development of new devices, it is also available to help those in the forensic community. Since other mobile forensic tools in the industry have not developed options for acquiring Google Glass or other wearable Android devices yet, Shattered provides a cutting edge service in android acquisition and artifact parsing.

Research Questions:

This forensic tool ensures that acquiring artifacts from wearable devices is a repeatable and defined process. This removes the human element of error for the repeatable process of acquiring information from both the Glass file system and from the live system. In addition, the automation allows for examiners to focus on analysis and spend less time acquiring every artifact on the device.

Terminology:

Python – A cross platform scripting language
Android Debug Bridge (ADB) - a tool used to transfer data between Android-based devices and a host machine.

Methodology and Methods

Scripts will be designed around generated data to support other projects at the LCDI. Built in a modular environment, Shattered is designed to expand and add more features, as Google Glass is an ever-changing device. These scripts are hosted on Google Code (http://code.google.com/p/shattered) and available for download by anyone with an internet connection. The LCDI internally tests the script suite on current research, and then publishes the working scripts for the public to use.

Equipment Used

Google Glass running XE12, the latest version of the eXplorer Edition of Google Glass, was used in creating the test image to generate modules from.

Data Collection:

Shattered v. 1.3 was used to collect data from the Google Glass. This version of Shattered does not provide any processing that newer versions offer, but instead acquires the data off the device. The newer versions restructured v. 1.3 to optimize performance and affectivity of the code.

Analysis

Data was generated by Google Glass, using a variety of Glassware applications, directions, local events, messaging, social media, and other features. This ensured the Google Glass was equipped with a large data set so that the full features of Glass could be tested and parsed by Shattered. Based on other research projects at the LCDI, we looked into artifacts identified and began to parse them with a module-based system. The current modules include sqlite, event log, and logcat parser.

1.1 Logcat Parser

This was the first module written and was designed to simplify reading the logcat entries from Android. The logcat tool exports the data into a text file that can be read by any text editor. The difficulty in reading it comes from the formatting, in which the time metadata is located on a different line than the actual data. In addition, there are a series of undefined data columns, which are consistent in every entry. The logcat parser takes each line and formats them into these columns. It organizes the dates and times into a format that can be sortable and filterable. In addition, it places the warning level into its own column that allows it to be another sortable and filterable feature. Overall, converting the logcat output to CSV makes it easier to read and analyze by the examiner.

1.2 Event Log Parser

The event log parser is similar to the logcat parser and provides the ability to look closely at the many event logs within the event logs on Glass. The event logs are saved in multiple text files and with this module are coordinated and sorted into one document that is easier for examiners to view.

1.3 SQLite Parser

This parser focuses on the many SQLite databases within the code and can be parsed into csv-formatted documents for easier viewing and comparison by the examiner. This includes the timeline.db, entity.db, and homemenuitems.db databases. For each database file, the tables within the databases are written to their own csv file with column headers specific to the table. There is only support for 6 databases at the moment, though more is expected to be developed in the future.

1.4 Private Cache Parser

The private cache contains cached data from the timeline on Google Glass. This includes png, text, and html files that can be used to rebuild the cards, as seen on Glass. This parser sorts these files by type into contextual directories and assigns the proper file extensions to each so that it can be viewed and interpreted correctly.

Results

While conducting the development, the results were varied since the Google Glass operating system continued to update and modify how and where certain artifacts were stored. Several parsers were not developed due to the data no longer existing, or being simplified so that it did not require parsing. This does not mean that there is

an inability to add additional parsers to the Shattered project since there is plenty of data to examine and analyze.

Conclusion

The goals of this project were to create a repeatable automated solution to provide examiners with a reliable and efficient system to save time and to increase accuracy of analysis of wearable devices such as Google Glass. Overall, the acquisition script provides a detailed capture of Google Glass at the specific point in time and zips into a container to prevent modification and ease transferring the output. In addition, the parser script calls to the libraries and begins to analyze case data from an acquisition.

Further Work

Additional Parsers can be built to analyze more SQLite databases, look into the sorted cache files, and export EXIF information about media files on the device. With the increased interest of Google to expand its Android Wearable Technologies, Shattered could be used as the system to acquire and parse this data, staying ahead of the curve of other industry mobile device tools.