Whitepaper – High Tech Crime Institute, Inc.

High Tech Crime Institute, Inc.
7935 114th Ave N
Largo, Florida 33773
813.343.0766
http://www.gohtci.com
A Service-Disabled, Veteran-Owned Business

Using Physical Collection of Cell Phone Data as an Enhancement to Logical Collection

Author
Stephen Pearson
Managing Partner
High Tech Crime Institute Incorporated
stephen@gohtci.com

4 January 2011

Introduction

Today's complex Cell Phones are providing operator/agents ever increasing challenges in the collection of intelligence or evidence. With the storage structures growing in size and the uses of the Cell Phone changing daily the collection of data from these devices is becoming increasingly more challenging. New devices such as IPhone, Android and Blackberry cell phones provide the user with full connectivity to cloud environment allowing the collection of email and connecting to the corporate network. Cell Phones have become portal devices with direct connection to social networks like Facebook and linkedIn. Text and SMS messages have become the new communication standard for many users.
All of these new uses bring with them their own storage containers unique or specific to the applications being used. Newer methods have to be developed to take advantage of these new storage containers that may contain orphaned or deleted data fragments. One of these methods for the enhanced collection of data from the Cell Phone is the physical acquisition methodology. The physical collection acts more like the traditional forensic acquisition tool in that it gathers data at the byte level from the storage container. This allows the operator/agent the ability to gather data that may not be available using the traditional logical collection method. This paper is an attempt to provide an analysis of those investigators that are using the newer physical method. The goal is to understand if physical collection is useful to the operator/agent performing triage analysis and attempt to define where in the collection process the use of physical analysis should be conducted.

This whitepaper is based on a non-scientific survey commissioned by the High Tech Crime Institute (HTCI). Its sole purpose was to gather information on the use of the physical collection methodology from the cell phone. HTCI felt it was important in the information gathering process that we did not gather information about any specific devices or turn the survey into a product specific survey. Questions were asked to investigators that participate on the High Tech Crime Consortium (HTCC) forum. These investigators are from the Law Enforcement and Corporate Security community and have the most expertise in the use of physical collection methods.

The following questions asked are as follows:

1. How often are you finding a device that is susceptible to a physical dump?
2. The length of time needed to then convert the dump to a format understandable by others or is there a time penalty associated with a physical extraction?
3. Have you actually found evidence or intelligence that was not found in the logical dump?

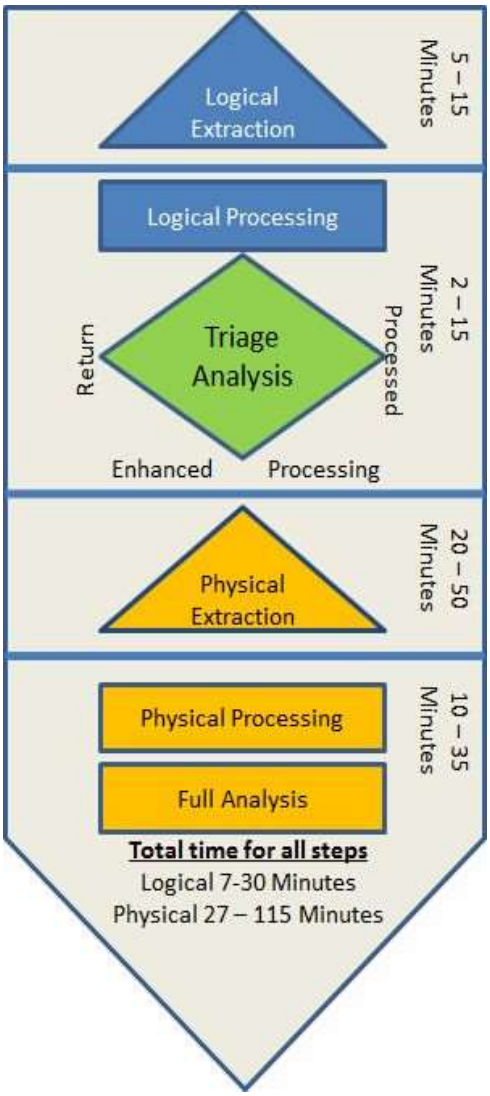
HTCI feels that these three questions have furnished enough feedback to be able to make a clear analysis for the use of the physical dump methodology by operators/investigators in the battlefield environment. After the collection of data was obtained the principal of Digital Triage Forensics (DTF) was applied to the results. This is the additional parameters of safety and time.

Analysis

- Question 1 - How often are you finding a device that is susceptible to a physical dump?

- Analysis of feedback - 40% of the respondents stated that they were able to use the physical dump on a cell phone after the logical dump had been conducted. The one interesting fact that came from this is that 100% of all respondents used the logical dump first to gather the initial data.
- It was noted that the respondents that were able to gather physical dumps were using cell phones that were between 0 and 3 years old.
- Smart phones such as the Android, Blackberry and the current IPhone were not able to be successfully gathered by examiners.
- Other tools were used on the Android and IPhone that allowed collection of data using backup files.

- Question 2 - The length of time needed to then convert the dump to a format understandable by others or is there a time penalty associated with a physical extraction?
  - Analysis of feedback - 100% of the examiners stated that a time penalty was incurred when using the physical dump method. The average time penalty that was experienced by examiners was between 25 and 40 minutes depending on the size of the data container used by the cellphone.
  - This is an issue when applying the time parameter to the collection of cellphones by operator/agents. The operator/agent has a very limited time frame to accurately collect and triage data.
  - In the training of triage processing operator/agents are looking for indicators or probable cause to maintain a person. The quick interpretation can be obtained using the logical collection of the cellphone. If the cellphone can be processed physically then it is an enhancement to run the physical collection after the logical collection.
  - As can be seen in the diagram (see figure 1) the logical analysis will be conducted every time as it is the most reliable capture method for Cellphones. After the logical dump has been accomplished then the operator/agent will reacquire the cellphone using the physical extraction method. (different cables are normally required for this as well doubling the number of cables that would need to be maintained) As can be seen there is a time penalty with each new process that is conducted.



- Question 3 - Have you actually found evidence or intelligence that was not found in

the logical dump?

- Analysis of feedback – 10% of the respondents stated that they had been able to recover data that was not gathered with the logical method. One investigator was able to recover emails that had been deleted that were not gathered in the logical process. This investigator stated that the logical capture provided enough data to make the investigator continue on with the physical examination.
- The remaining investigators stated that they always use the logical process first which normally yields the information desired. It was noted that all investigator procedures included the logical method first, followed by the physical process. No investigators indicated that they would use the Physical process first.

Conclusion

With the growth of the collection and analysis of cellular devices it is becoming more and more important to be able to use multiple methods to gather all the data from the cellular device.
Physical collection is a methodology that needs to be included in the toolkit, but at the appropriate collection layer. With this in mind the question becomes at what layer does a physical acquisition make sense? The time penalty that is involved to conduct the physical examination alone takes it out of the realm of the triage analysis. The operator/agent is not going to take the time that is required to process the cellphone for a second time to gather potential intelligence at the collection point. This secondary analysis will be done at the FOB or higher possibly by another entity.
The amount of data that is collected outside of the logical collection was not impressive and leads to the question of return on investment. It was found while researching vendor websites that the physical collection of cell phones can be applied to about 600 cell phones. This does not include smartphones that prevent the collection by physical methods. This is less than a 1/3 of the cell phones that can be processed logically. It was also noted during the research of websites that most vendors charge a premium rate for the additional physical acquisition capability. This includes additional cables that are required to be able to conduct the physical acquisition increasing the size of the operator/agents collection kits. This cost does not include the increased training cost required to train operator/agents in the secondary procedure to gather and interpret data.
HTCI finds that based on the results that the logical method is currently the most effective method for operators/agents to be able to collect actionable intelligence to influence tactical questioning.

To help determine the use of physical acquisition by a unit a set of questions has been developed to ask vendors:

1. How many TESTED phones does the software acquire as opposed to the logical collection?
2. What time penalty will be added to the acquisition?
3. What data will it parse and how does it parse the data (Known data sets, Headers, etc).

4. When newer headers are found can the software be changed by the operator to include the new header formats?
5. What units do you have in inventory that can already perform the physical extraction and is there any cost benefit to change to the newer software?

About the Author

Stephen Pearson combines more than twenty-nine years of law-enforcement experience with in-depth expertise in today's most pervasive Internet and computer technologies.

During his tenure in federal and civilian law-enforcement agencies, Stephen has had the opportunity to see all facets of Computer Crime Investigations. In 1994, he began developing tools and training for the investigation of computer crime investigation when he was assigned to the United States Army Military Police School at Ft McClellan, Alabama.

In 2003, Stephen retired from the Military Police Corps as the Non-Commissioned Officer in Charge of the Advanced Technology Criminal Investigation Courses. Afterward, he pursued his career in the computer crime investigations world by becoming an investigator with the Pulaski County Sheriff's Office. During his tenure at the Sheriff's office, Stephen used his technology skills on numerous cases, one of which led to the safe recovery of an abducted child during a joint FBI and Sheriffs department investigation. Most recently, Stephen has been directly involved in the development and implementation of Computer Crime and Forensics training for our Armed Forces in Iraq and Afghanistan.

Stephen is recognized by the Federal government as an expert witness in DOS file structures and has been consulted on numerous high profile investigations. He developed the ground-breaking Cyber Squire Internet child safety program for the United States Army at Ft Leonard Wood which has become a standard program for the local school system for child internet safety. In addition, he is the co-author of the book *Digital Triage Forensics: A Battlefield Guide to Digital Forensic Collection* (ISBN: 978-1-59749-596-7).

Mr. Pearson has been awarded numerous decorations, including the Meritorious Service Medal, Army Commendation Medal, and Army Achievement Medal. In September 2002, he was awarded the Military Police Corps Order of the Marechaussee (Bronze) – the highest peace time Military Police award – for his superior performance and dedication to training excellence.

Stephen holds a Bachelor of Science degree in Computer Information Science (Summa Cum Laude) and Associate Degrees in Administration of Justice and Computer Information Science. Currently, he is in the process of completing a Master of Business Administration degree from Webster University. Stephen holds the Microsoft Certified System Engineer Certificate (+ Internet) and is also a US Army Master Instructor.