COMPUTER EVIDENCE RECOVERY, INC.

Canada's Premier Computer Investigation Agency
Suite 300, 160 Quarry Park Blvd SE, Calgary, Alberta, Canada T2C 3G3 www.computerpi.com
Tel: (403) 703-4846 Toll Free: (866) 703-4846 Fax: (403) 770-8158 kevin@computerpi.com

CASE PROFILE

INTAKE DATE: February 10, 2017

CLIENT: Commission of Inquiry Respecting the Death of Donald Dunphy

CLIENT FILE #: Unknown

CONTACT'S NAME: Sandra R. Chaytor, Q.C

PHONE NO.: 709 [redacted] 329

TYPE OF INVESTIGATION: Forensic Data Analysis

CIRCUMSTANCES: Our agency was tasked by the client to conduct an analysis of data extracted from a Blackberry 9100 Pearl utilized by Cst. Joseph Smyth, limited to the time period of April 1, 2015 – April 30, 2015.

CONFIDENTIAL REPORT

THIS IS A WORKING REPORT. IT HAS BEEN PREPARED BASED ON PROVIDED INFORMATION AND ASSUMPTIONS. IT IS SUBJECT TO CHANGE AS ADDITIONAL INFORMATION BECOMES AVAILABLE OR IS CLARIFIED.

DATED: March 3, 2017

I thank you for the opportunity to provide these findings pursuant to our conversations on this case.

I am the Computer Forensics Coordinator for Computer Evidence Recovery, Inc. (hereinafter referred to as CER), an investigation agency licensed, bonded, insured, and headquartered in the Province of Alberta. I have held this position since 1999. CER conducts forensic examinations of computers and other digital media evidence at our head office in Calgary, AB, and in on site situations as circumstances dictate. I also assist other forensics companies, law firms, and various Police Services as requested. In my current position, I am responsible for supervising and conducting on site and static operations, as well as the development of CER procedures and practices as they relate to the forensic examination of computer evidence. I am knowledgeable in Macintosh and IBM Compatible platforms, as well as Symbian, CE, and analysis of Cellular Telephones, SIM cards, and Personal Digital Assistants. I have completed forensic examiner training. As a Forensic Examiner. I

have performed more than one thousand computer forensic examinations and assisted or supervised numerous others.

My duties include assisting with subpoenas, ensuring proper search and seizure of all computer-related equipment, forensics analysis of all computer data storage mediums, examination of all computer hardware, and assisting in computer-related civil and criminal investigations.

My computer specific training is as follows:

- Computer Security and Configuration Specialist – I have taught this course to investigators and law enforcement across North America.
- Forensic Data Recovery Specialist
- Microsoft Windows Advanced Forensics Data Specialist
- Internet Investigation Specialist – I have taught this course to investigators and law enforcement across North America.
- Email Tracing Specialist – I have taught this course to investigators and law enforcement across North America.
- Ongoing continuing education and upgrading.
- EnCase Certified Examiner
- Advanced Lab Data Recovery Specialist
- Windows Vista Forensics
- Hacking Exploits Investigation Specialist
- Certified Data Recovery Professional
- Certified Ethical Hacker
- Level 3 Cellular Repair Technician
- SANS Information Security (SEC301) – I teach this course for The SANS Institute.
- GIAC Information Security Fundamentals Certification (GISF)
- SANS Security Essentials (SEC401) – I teach this course for The SANS Institute.
- GIAC Security Essentials Certification (GSEC)
- SANS Digital Forensics (FOR408) – I teach this course for The SANS Institute.
- SANS Advanced Digital Forensics (FOR508)
- SANS Securing the Human (MGT 433)
- GIAC Certified Forensic Analyst (GCFA)
- SANS ICS/SCADA Security Essentials (ISC410)
- SANS Certified Forensic Examiner (GCFE)

I obtained passing grades in both written and practical examinations where applicable in each of the above-mentioned courses.

Acquisition Methodology Common to This Case

Not applicable in this case, as I was provided with an acquired dataset from the Client.

ANALYSIS

During the course of my investigation, my mandate was to fulfill the following tasks:

1. Identify any relevant data not previously extracted by the RCMP;
2. Retrieve relevant deleted data;
3. Determine dates on which data was deleted;
4. Provide explanations as to any anomalies on dates.

After a thorough and exhaustive review of the pertinent portions of the dataset provided by the Client, I note that pursuant to task #1, I did not identify any relevant data that was not already previously extracted by the RCMP.

I note that pursuant to task #2, I did not identify any relevant deleted data that had not already been extracted by the RCMP.

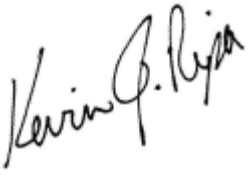
I note that pursuant to task #3, I was unable to determine dates on which data was deleted, owing to the make and model of the device in question. This is not uncommon with cellular devices.

I note that pursuant to task #4, I am unable to provide a explanation for the time anomaly identified by the client, without first performing a complete analysis of the entire dataset from scratch using both the Cellebrite software version that the RCMP used, and an updated version, then creating a report from the findings, and then comparing it to the reports provided by the RCMP. Even so, there is no guarantee that I may be able to answer the question definitively. Without performing this task, I can only opine at the most likely explanations. Those being a mistake in the review of the dataset, or an undesired and unexpected performance of the specific version of Cellebrite that was used in the examination. In either case, it would appear by the data and report provided to me by the Client, that this anomaly had been corrected.

CONCLUSION

If you have any questions regarding this investigation, please do not hesitate to conduct the undersigned. I would like to take this opportunity to thank you for allowing us to be of service.

Sincerely,



Kevin J. Ripa
PI, EnCE, GISF, GSEC, GCFE, GCFA, BAI, CDRP
Director of Investigations
Alberta Department of Justice W010876