

Digital Forensic Analysis Report

Data Recovery Project

For

Local 305 Postal Carriers Union

FDI-2016-0043

By

Seltek, Inc.

May 31, 2016

Prepared by:

Patrick Logan, CCE

Table of Contents

Table of Contents.....	2
Background:	3
Processing:	3
File Recovery:	3
Conclusions:	4

Initial Report

Background:

Leslie Hamlett from the Local 305 Postal Carriers Union (L305) contacted Seltek Technology Services on March 10, 2016 referencing the need to examine four computers and attempt recovery of deleted data from these computers. Mr. Hamlett delivered these computers to the Seltek office on March 18, 2016. The data recovery process began on March 21, 2016.

Processing:

On March 21, 2016, Seltek Technology Services began the processing the hard drives in an attempt to recover deleted data from them. The following computers were provided to Seltek for processing

Description	User	Serial Number
Lenovo Laptop	John Dudley	CB13358036
Black Raidmax case	Ed Evans	N/A
Black & white Raidmax case	Derrick Carr & Kevin Fletcher	N/A
Green Corsair case	Yan Cardin	015813527803

This process involved analyzing the contents of the hard drives using several different file recovery software programs in an attempt to recover any data that had been deleted from the hard drives.

File Recovery:

Once the processing had completed, we began the recovery process. The recovery process involved copying any data that was found during the recovery processing phase to a folder labeled for each computer on a Seagate 1TB USB hard drive. During the recovery process it was discovered that someone had run a file wiping utility on the Lenovo laptop and green Corsair computer to permanently wipe data from the hard drive. Normally, when files are deleted from a computer, the data still resides on the computer hard drive until new data being stored on the hard drive overwrites the deleted data. In most cases, deleted data can be recovered, if the original data has not been overwritten. When wiping utilities are run on a computer hard drive, they actually overwrite the deleted data with random characters which make recovery impossible. On both the Lenovo laptop and the green Corsair computer we

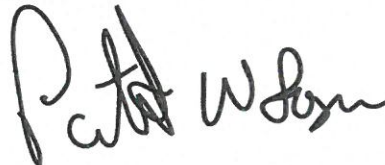
found the existence of .zzz files, which are left behind when the wiping feature of the program CCleaner is run on a hard drive. On both of these computers, we were unable to recover any of the data that had been wiped. All other recovered data was provided to the client on the Seagate 1TB USB hard drive for review on April 08, 2016.

Conclusions:

During the recovery process we found that many files had been deleted from the four computers we processed for file recovery. While Seltek was able to recover some of the deleted data, it is unknown whether all data that had been deleted was recovered. Seltek also determined that someone had deliberately run a data wiping program on the Lenovo Laptop and the Corsair computer to permanently delete any of the wiped data. This wiping process made it impossible to recover any of the deleted data from these computers that had been wiped.

This report was reviewed and executed on May 31, 2016 in Richmond, VA.

Examiner

A handwritten signature in black ink, appearing to read "Patrick Logan". The signature is stylized and cursive.

Patrick Logan, CCE
Seltek Technology Solutions