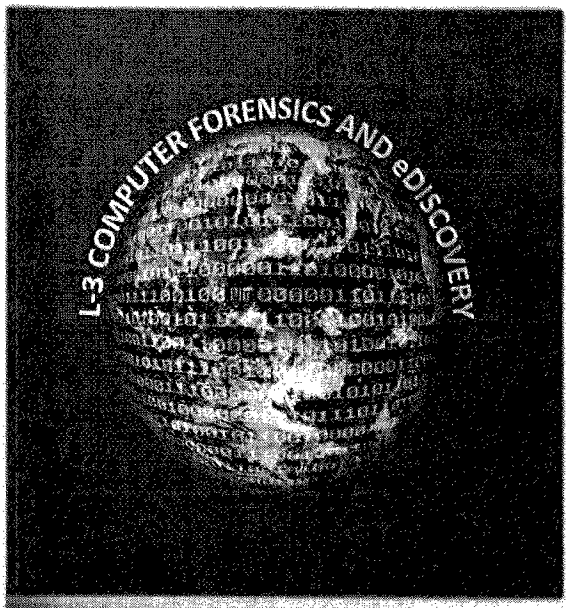
# EXHIBIT B

# PART 1




# Lower Merion School District Forensics Analysis

## Initial LANrev System Findings

**L-3 Services, Inc.**
455 Business Center Drive, Suite 200
Horsham, PA 19044
Phone: 215-674-0200
Fax: 215-443-0474
Web: l-3com.com

**Prepared for:**
**Ballard Spahr**

**May 2010**

Ballard Spahr

# Confidentiality Statement

This document is confidential and is intended for review by Ballard Spahr and those entities deemed by Ballard Spahr to have a need-to-know. The contents of this document constitute an attorney work product, are protected by the attorney/client privilege, and may otherwise be protected against public disclosure.

# Table of Contents

# List of Tables



# List of Figures

# 1 Background

In the fall of 2008, the Lower Merion School District (LMSD) provided every high school student at Harriton High School with Mac Book® laptops in what is referred to as the "1-to-1" initiative. This initiative allowed students to use these laptops both in and out of school throughout the school year. LMSD utilized the software product, "LANrev," developed by Pole Position Software, to manage the student laptops and other LMSD computing assets. LANrev is an asset management technology capable of tracking computing assets, remotely installing software, accounting for software licenses and automating the remote installation of vendor patches. In addition to the remote management of computers, LANrev also provides a feature to assist in the investigation and recovery of laptops, called "TheftTrack." When this feature is activated by a LANrev Information Technology (IT) administrator through the LANrev Administration Console, the managed assets (e.g., student laptops) communicate back to the LANrev server on a periodic basis and send a combination of screenshots (pictures showing what is on the laptop's screen) and images taken using the integrated web camera (webcam), installed on all Mac Book® laptops. In addition to these pictures, technical information [redacted]

The LMSD purchased LANrev in 2007. LANrev was acquired from Pole Position Software by Absolute Software in December 2009, and rebranded the product, "Absolute Manage."

On February 16, 2010, Michael E. and Holly S. Robbins, on behalf of Blake J. Robbins (i.e., Plaintiff), filed a civil lawsuit against the LMSD, the Board of Directors of the LMSD and Christopher W. McGinley, LMSD Superintendent, (i.e., Defendants), seeking to recover damages caused by the Defendants' alleged invasion of privacy, theft of Plaintiff's private information and unlawful interception and access to acquired and exported data and other stored electronic communications through the use of the LANrev software.

The LMSD School Board hired Ballard Spahr a law firm with offices in the Philadelphia area, to represent the LMSD School Board. On February 21, 2010, Ballard Spahr contracted with L-3 Communications (L-3), a global information technology firm, to determine the facts surrounding the allegations filed by the Plaintiff. The objective of L-3's computer forensics support in this case is to:

- Determine when, how, and which LMSD personnel utilized the LANrev "TheftTrack" feature of the LMSD LANrev IT management software application
- Identify any reasonably accessible/recoverable LANrev pictures from the various sources of Electronically Stored Information (ESI) collected and preserved from the LMSD computing assets
- Identify LMSD email communications referencing the activation, ongoing monitoring, and deactivation of the LANrev "TheftTrack" feature
- Present the results within the timeline defined by the court

This report provides a current summary of the analysis, observations and findings of L-3's efforts to reconstruct a historical timeline of all LANrev "TheftTrack" activities that occurred at the LMSD.

While the forensic effort is ongoing, the analysis performed to-date and documented in this report provides information towards gaining an understanding of the goals and scope of this investigation. Continued forensic processing and analysis may introduce additional data relevant to the scope of this investigation. Although computer forensics is a technical subject, every effort has been made to ensure that this report can be interpreted by individuals from a technical and non-technical background.

## 2 Methodology

In support of stated project objectives, L-3 utilized proven and vetted best practices for performing computer forensic investigations. The methodology, tools and processes employed are designed to be consistent and repeatable. At a high level, our approach consisted of a four-phased process for performing computer forensics activities. These phases included the following:

- **Collection:** identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.
- **Examination**: forensically processing collected data using a combination of automated and manual methods, extracting and assessing data of particular interest, while preserving the integrity of the data.
- **Analysis**: analyzing the results of the examination to derive useful information that addresses the questions that were the impetus for performing the collection and examination.
- **Reporting**: documenting the results of the computer forensics engagement in a manner that can be understood and acted upon.

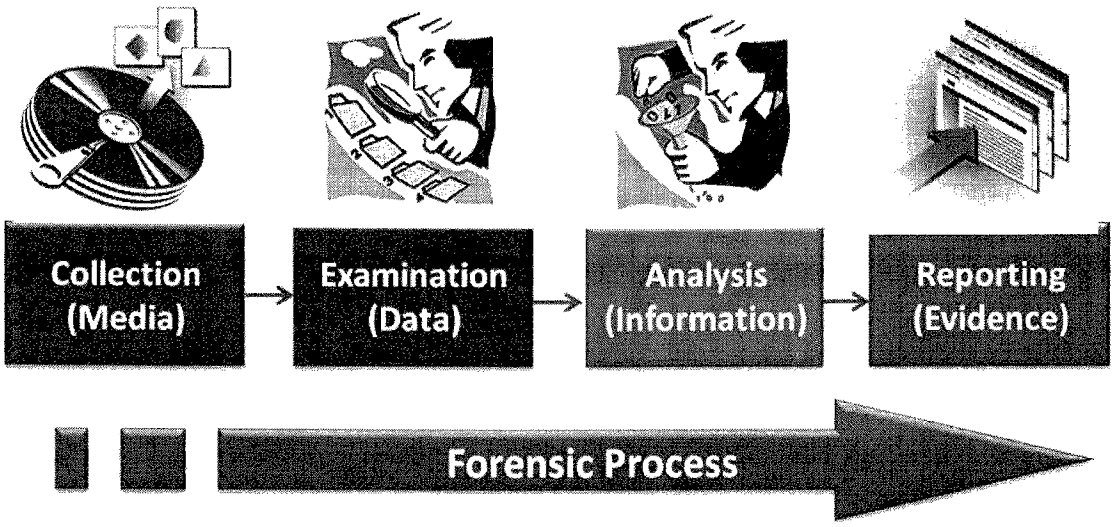



Figure 1. Four-Phased Forensic Process

Throughout this project, L-3 personnel used a variety of computer forensics tools and applications as required and appropriate.

# 3 Forensic Approach

This section documents tasks performed within each phase of the computer forensics engagement.

## 3.1 Phase 1 - Collection

Prior to the acquisition and forensic imaging of LMSD computing assets, L-3 personnel gained an understanding of the LMSD networks, systems and applications with a focus on their relationships to the LANrev system, in order to identify potentially relevant repositories of electronic data. L-3 personnel reviewed Microsoft Visio diagrams of LMSD networks and systems, and conducted interviews with pertinent LMSD IT personnel. LMSD systems identified as pertinent to the case, and subsequently acquired, include:

- LANrev servers
- Laptops/Desktops from various LMSD personnel
- File Servers
- Directory Servers
- Security/Authentication Control Devices
- Log Servers
- Email Servers

The goal in the collection phase was to preserve any relevant data, and to the extent possible, minimize any operational impact on LMSD day-to-day operations. L-3 personnel obtained custody of relevant workstations and laptops for transportation to its Horsham, PA, forensics lab to create the forensic copies, or image files. LMSD production systems, such as email, were forensically copied onsite and then transported to L-3's forensic lab for examination. Acquired images were hashed and validated to the original source's hash created to ensure its integrity. Hashing refers to the process of generating a unique mathematical value based on file contents and are used to prove that a copy/image has not been altered from its original state. In total, approximately 19 Terabytes (TB) of data was acquired from the LMSD for examination. The systems acquired included Windows and Mac OS operating systems, and were obtained from both physical and virtual environments.

## 3.2 Phase 2 - Examination

Working copies of the original images were created and examinations were then performed on the working copies. Multiple forensic software applications, such as Forensic ToolKit, Linux utilities, and scripting tools were used to identify and extract data of interest for analysis, while preserving the integrity of the data. Additionally, specialized tools for specific functions were utilized. All of the tools utilized are industry accepted and vetted.

## 3.3 Phase 3 - Analysis

To accomplish the primary goals established by Ballard Spahr, the Analysis Phase focused on three primary areas: the LANrev system, email communications, and LANrev web camera pictures and screenshots.

- LANrev System – acquire all LANrev related data supporting the development of a historical LANrev TheftTrack timeline

- LMSD Email Analysis – identify and correlate emails between and amongst LMSD personnel supporting activation, ongoing monitoring, and knowledge of LANrev TheftTrack activity
- LANrev Web Camera Pictures and Screenshots – identify and correlate recovered images associated with LANrev TheftTrack activity.

These areas were analyzed to develop a timeline of LANrev TheftTrack activities. Each of the three primary areas is described in further detail below.

### 3.3.1 LANrev System

LANrev is an IT asset management platform originally developed by Pole Position Software. The LMSD purchased LANrev in 2007 and was used to manage technology assets, including student laptops.

The LANrev system, as deployed by the LMSD on or about February 22, 2010, is depicted in Figure 2 below. There are three components to the LANrev deployment at the LMSD:

- LANrev Agent
- LANrev Servers (Inventory Server and Software Server)
- LANrev Administration Console

The LANrev agents are deployed on managed assets such as student laptops. The LANrev Administration Console is installed on select LMSD IT staff workstations and servers. The LANrev Administration Console is a LANrev application component that acts as the user interface with the LANrev Servers.

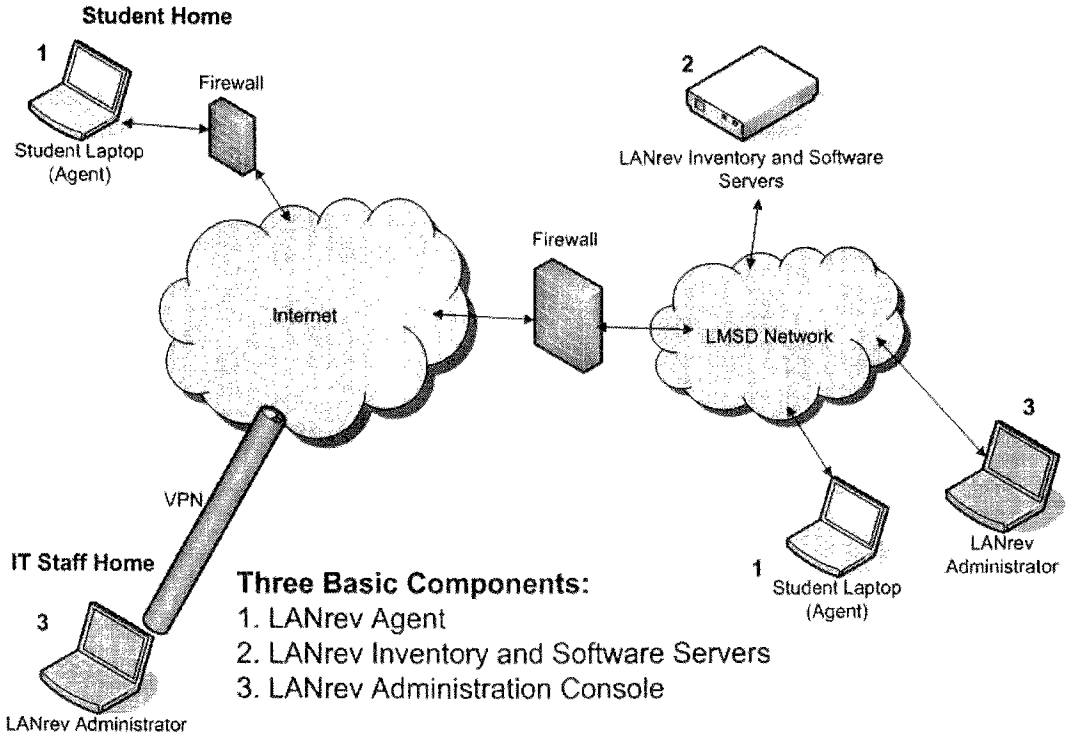



Figure 2. High-Level LANrev Network Overview

The LANrev Agent (1) installed on the student laptops continuously attempts to communicate with the LANrev Servers (2); this communication is known as the "heartbeat." This heartbeat communication between the LANrev Agent and LANrev Servers occur whether the laptop is connected to the LMSD network or a non-LMSD network. [redacted] Management of the LANrev Servers and execution of the features it provides is done through the LANrev Administration Console (3) that is installed on an LMSD IT Administrator's workstations (desktop/laptop).

#### 3.3.1.1 Development of LANrev Test Environment

To gain an understanding of the architecture, data structure, configuration and system-specific capabilities of LANrev as deployed by LMSD, a LANrev test environment was established. The test environment was built using:

- LANrev software installation packages recovered from LMSD systems acquired in the collection phase
- Student laptop (i.e., MacBook, Mac OS) clones created from acquired hardware
- L-3 MacBook Pro laptops and server hardware

The LANrev test environment was used to become familiar with LANrev system specific features such as:

- Default configuration settings and options
- Logging capabilities
- Communication protocols
- Security features
- LANrev TheftTrack initiation and setting options
- Database and table structures

Use of the LANrev test system supported the prioritization and selection of specific acquired systems for analysis to be responsive to the court's timeline. Additionally, the test lab environment was used to continually communicate our forensic approach and project activities with the case stakeholders (LMSD School Board, Ballard Spahr, Plaintiff's counsel, USAO, etc.).

Although not the focus of our forensics support, cursory research was conducted on the activation of the "green light" of the built-in iSight camera on the Apple MacBook laptops. After a limited review of the green light activation, to-date, we have not identified any means by which the green LED would illuminate without software (i.e., any software) interacting with the iSight camera. While testing the LANrev TheftTrack feature, LANrev activations produced a single flash for each picture taken after activation.

### 3.3.1.2 LMSD's LANrev System Specifications

The hardware specifications and operating systems for LMSD's LANrev server are included in Table I below:

Table I. Hardware/Operating System Specifications

| | |
|---|---|
| Hardware | Apple Xserve 1u appliance x 2: [redacted] |
| Operating System | Mac OS Server 10.4.11 [redacted] |

Since its initial purchase by the LMSD in 2007, the LANrev software went through numerous revisions and build numbers. These revisions and build numbers, as represented in the LMSD LANrev server logs, are documented in Table II below. The software versions are important from two perspectives: ensuring that the test environment utilized the same software versions in use by LMSD, and from a logging perspective. LANrev software versions prior to version 5.0 do not log (i.e., not seen within the data reviewed) the 1022 command, the command identifier that signifies the initiation and deactivation of the TheftTrack feature.

Table II. LMSD LANrev Software Revisions and Build Numbers

| Date | LANrev Version |
|---|---|
| 11-12-2007 | LANrev Server 4.5.1 (v963) |
| 11-29-2007 | LANrev Server 4.6 (v1040) |
| 03-28-2008 | LANrev Server 4.6.2 (v1084) |
| 08-06-2008 | LANrev Server 4.6.4 (v1159) |
| 10-31-2008 | LANrev Server 5.0 (v1375) |
| 11-07-2008 | LANrev Server 5.0 (v1377) |
| 03-06-2009 | LANrev Server 5.0.1 (v1390) |
| 03-28-2009 | LANrev Server 5.1 (v1474) |

### 3.3.1.3 LANrev Backups

LMSD did not employ a process for backing up the LANrev servers to tape or disk; however, the LANrev system was configured to maintain an eight-day rotating backup cycle where the databases are backed up during nightly processes.

### 3.3.1.4 LANrev TheftTrack Feature Overview

One of the features of the LANrev IT asset management platform is the TheftTrack feature. This feature, which is no longer available on current versions of Absolute Manage, has the capability to capture information relating to IT assets which it manages. When this feature is enabled, the LANrev Administrator has the option to capture screenshots, pictures, or both. These options are accessed via the "Computer Tracking" command (Figure 3) listed in the agent menu and are defined below:

- Take screenshots – If this option is checked, the tracked computers take screenshots and transmit them to the LANrev Server whenever they send a "heartbeat"
- Take pictures with camera – If this option is checked, the tracked computers take pictures of their immediate surroundings with their built-in cameras and transmit them to the LANrev Server whenever they send a "heartbeat"

In the test environment, it was observed that other events triggered a screenshot and picture in shorter intervals than the configured heartbeat value. For example, it was observed in some cases that TheftTrack activations with screenshots and pictures occurred a minute apart for several activations even though the heartbeat value was configured for 15 minutes. After some additional review, it was observed that the picture and screenshot activation also occurs when the network connection is changed, when a user logs in or out, or when the computer is woken up. Otherwise, regular heartbeat intervals continued.

The following sequence of screenshots illustrates the activation of the TheftTracking feature:

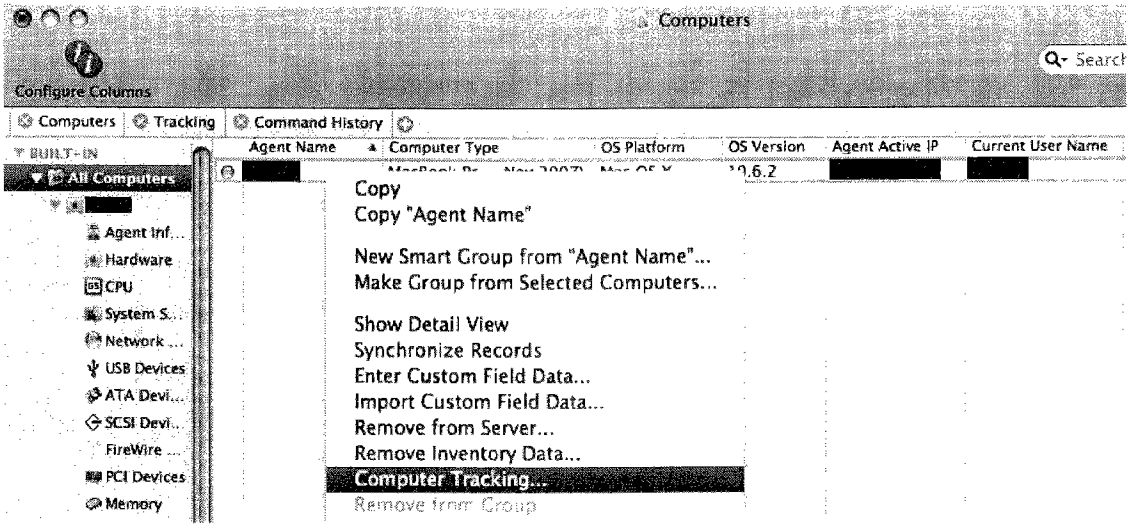



Figure 3. Enable Computer Tracking

By default, Computer Tracking is not enabled. When enabling computer tracking, the LANrev Administrator must activate each option via a checkbox, as shown in Figure 4 below. Once activated, the computer tracking option will stay active until the LANrev Administrator turns it off.

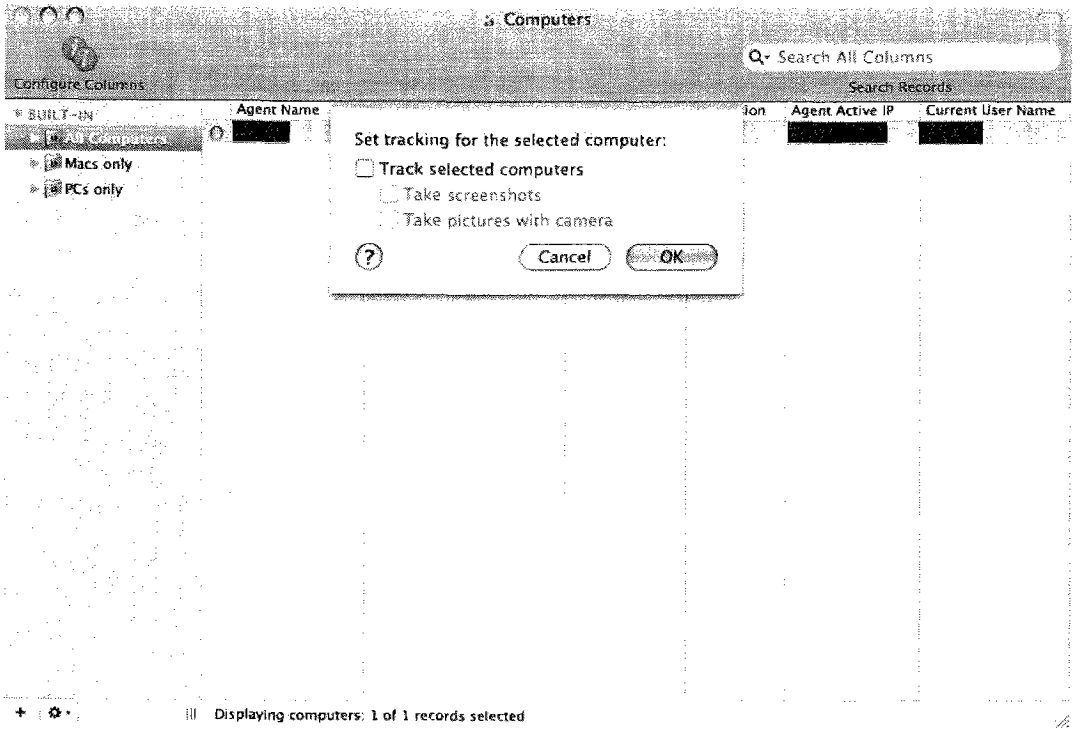



Figure 4. Default Computer Tracking Settings

When enabled, the following information can be tracked using the "TheftTrack" feature:

- Agent Name – The name assigned to a computer on which the LANrev Agent is installed.
- Tracked Computer Time Stamp – The date and time (according to the LANrev server's clock) of the last contact with the tracked computer.
- Tracked Computer Address – The IP address that the tracked computer currently has in the local network in which it is located.
- Tracked Computer Router Address – The IP address of the router that the tracked computer is currently using.
- Tracked Computer Public Address – The IP address that the tracked computer currently is assigned.
- Tracked Computer GMT Delta – The current time difference between the tracked computer's internal clock and universal time (GMT).
- Tracked Computer Current User Name – The name of the current user who is active on the tracked computer.
- Tracked Computer Current User Account – The full name of the account that is currently active on the tracked computer.
- [redacted]

- [redacted]
- [redacted]

When an LMSD IT administrator is notified to activate the LANrev "TheftTrack" feature, they must activate each option via a checkbox available in the Computer Tracking dialog box as shown in Figure 5 below.

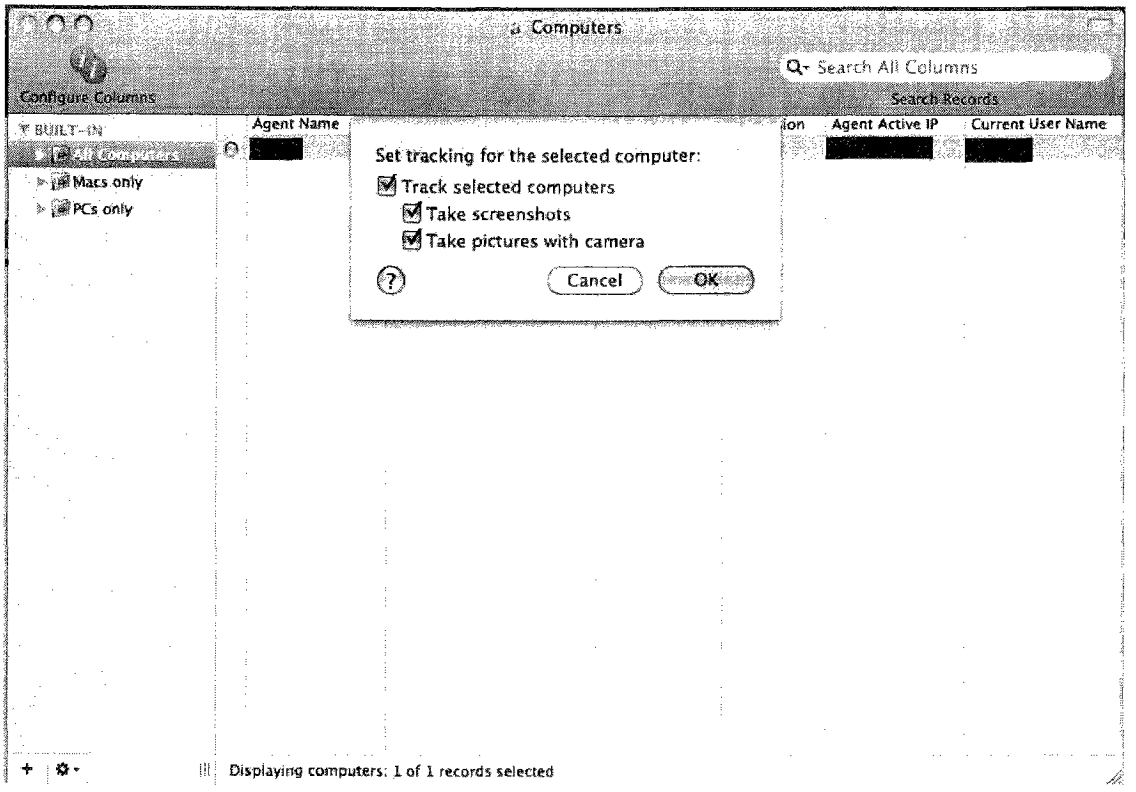



Figure 5. Computer Tracking Settings Enabled

Once enabled, the selected agent will begin capturing screenshots and pictures which will then be sent back to the LANrev Server. The interval for capturing information from a tracked asset is determined by the "heartbeat" setting. By default, LANrev Agents will issue a "heartbeat"[1] every 15 minutes, but this can be configured via Agent Settings and can be adjusted down as low as one minute intervals. The setting to adjust intervals is shown in Figure 6 below.

[1] *Heartbeat Interval*: The interval in which the agents are to contact the server to let it know that they are still available.

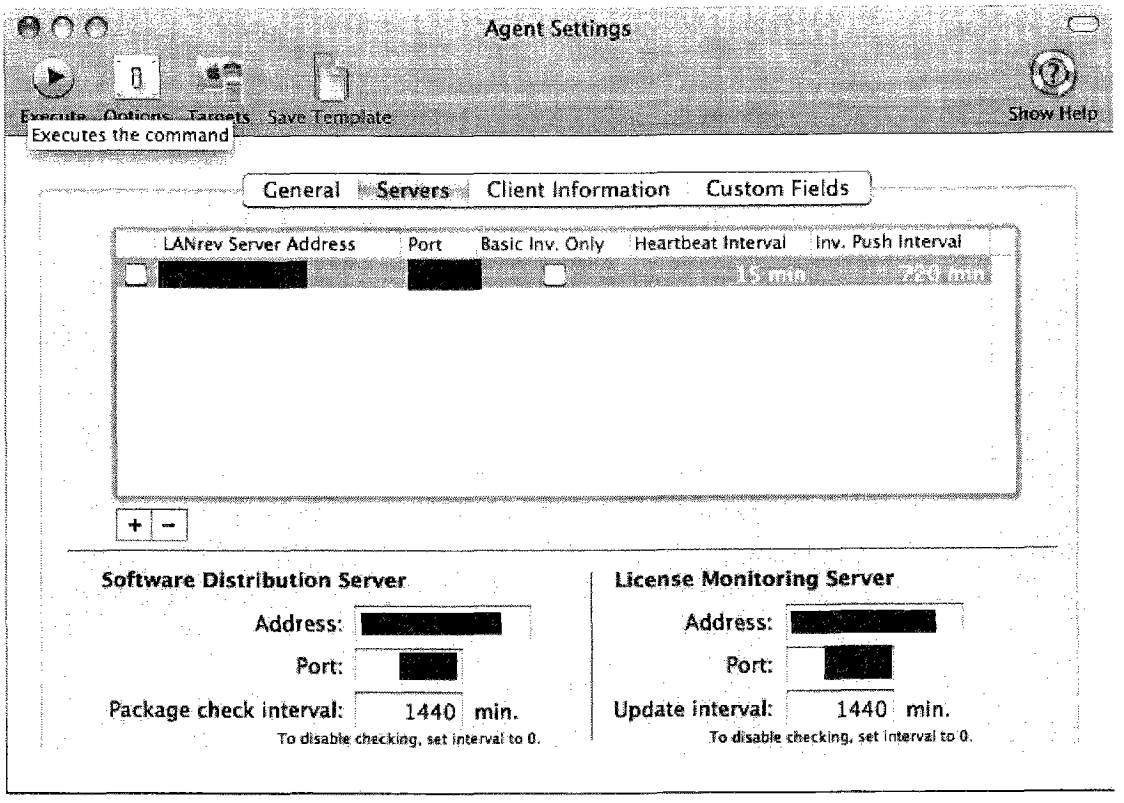



Figure 6. Default Heartbeat Interval

As previously shown in Figure 2, "High-Level LANrev Network Overview," the LANrev Administration Console can be used while on the LMSD Network as well as when connected through the LMSD Virtual Private Network (VPN). Remote access exists for IT personnel to logon to a [redacted] The logon is sufficient to provide administrators with remote access to LANrev.

### 3.3.1.5 LANrev Administrators

Sustaining the operations of the LMSD includes a support staff of more than 500 people. Within these 500 support staff personnel includes an IT staff of over 21 people which maintain the network infrastructure, information systems, servers and computers throughout the LMSD.

There are various permissions that are assigned to each LMSD LANrev administrator. The Table below contrasts the roles and permissions for LANrev Administrators for the periods of March 8, 2009, February 17, 2010 and February 20, 2010. The table maps each of the LMSD LANrev Administrators against a subset of LANrev permissions pertinent to the use of the TheftTrack feature. Cells within the table with the value of "1" have this permission turned on; those with "0" do not have the permission. Cells within the table with no value shown did not have an account at that time. As shown in this table, Michael Perbix and Carol Cafiero were the only LMSD LANrev Administrators with permissions to initiate or stop tracking of LMSD LANrev agents using the TheftTrack feature. The permissions of Michael Perbix and Carol Cafiero were revoked on February 19, 2010, and a LANrev account was created for Dr. Christopher McGinley, LMSD's superintendent.

Table III. Roles and Permissions for LANrev Administrators

| LANrev Database Date | Is Super Admin | Can Login | Allow Change Computer Tracking | Allow Remove Commands From History | Allow Change History Options | Allow Remove Computer Records | Allow Remove Inventory Data | Allow Change Agent General Settings | Allow Change Agent Server Settings | Allow Change Agent Client Info Settings | Allow View Commands Window | Allow View Computer Tracking Data | Allow View Computer Tracking Camera Picture | Allow View Computer Tracking Screenshot | Allow Change Computer Tracking Screenshot | Allow Change Computer Tracking Camera Picture | Can See All Records | Allow Remote Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Michael Perbix** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| February 17, 2010 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| March 8, 2009 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **Carol Cafiero** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| February 17, 2010 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| March 8, 2009 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **Jeremy [redacted]** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| February 17, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| March 8, 2009 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **Brad [redacted]** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| February 17, 2010 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| March 8, 2009 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **Amanda [redacted]** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| February 17, 2010 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| March 8, 2009 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **Kyle [redacted]** | | | | | | | | | | | | | | | | | | |
| February 20, 2010 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| February 17, 2010 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| March 8, 2009 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |

Table III. Roles and Permissions for LANrev Administrators (Continued)

| LANrev Database Date | Is Super Admin | Can Login | Allow Change Computer Tracking | Allow Remove Commands From History | Allow Change History Options | Allow Remove Computer Records | Allow Remove Inventory Data | Allow Change Agent General Settings | Allow Change Agent Server Settings | Allow Change Agent Client Info Settings | Allow View Commands Window | Allow View Computer Tracking Data | Allow View Computer Tracking Camera Picture | Allow View Computer Tracking Screenshot | Allow Change Computer Tracking Screenshot | Allow Change Computer Tracking Camera Picture | Can See All Records | Allow Remote Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Dave [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Matthew [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Jim [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Neil [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Tom [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Jessica [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |

Table III. Roles and Permissions for LANrev Administrators (Continued)

| LANrev Database Date | Is Super Admin | Can Login | Allow Change Computer Tracking | Allow Remove Commands From History | Allow Change History Options | Allow Remove Computer Records | Allow Remove Inventory Data | Allow Change Agent General Settings | Allow Change Agent Server Settings | Allow Change Agent Client Info Settings | Allow View Commands Window | Allow View Computer Tracking Data | Allow View Computer Tracking Camera Picture | Allow View Computer Tracking Screenshot | Allow Change Computer Tracking Screenshot | Allow Change Computer Tracking Camera Picture | Can See All Records | Allow Remote Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Matt [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Jason [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |
| **LANrev User** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Jason [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 0 | 1 |
| **March 8, 2009** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 1 |
| **Andrew [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **March 8, 2009** | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| **James [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **March 8, 2009** | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |

Table III. Roles and Permissions for LANrev Administrators (Continued)

| LANrev Database Date | Is Super Admin | Can Login | Allow Change Computer Tracking | Allow Remove Commands From History | Allow Change History Options | Allow Remove Computer Records | Allow Remove Inventory Data | Allow Change Agent General Settings | Allow Change Agent Server Settings | Allow Change Agent Client Info Settings | Allow View Commands Window | Allow View Computer Tracking Data | Allow View Computer Tracking Camera Picture | Allow View Computer Tracking Screenshot | Allow Change Computer Tracking Screenshot | Allow Change Computer Tracking Camera Picture | Can See All Records | Allow Remote Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Charles [redacted]** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| **February 17, 2010** | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| **March 8, 2009** | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| **Christopher McGinley** | | | | | | | | | | | | | | | | | | |
| **February 20, 2010** | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| **February 17, 2010** | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| **March 8, 2009** | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |

### 3.3.1.6 LANrev Databases

The LANrev system stores the information it collects and the commands issued against LANrev agents in multiple SQLite databases, each of which contain multiple tables. There are three key databases within LANrev which provide insight into the historical use of the TheftTrack feature. These databases are:

- "ServerCommands.db"
- "ServerDatabase.db"
- "AdminDatabase.db"

***ServerCommands Database***

The ServerCommands database contains three primary tables of interest: Commands, CommandQueue and CommandQueue_History. These tables show which LANrev Administrators executed specific commands through the LANrev Administration Console, such as activating the TheftTrack feature and the date this was executed. Commands are actions taken by a LANrev Administrator against assets managed by LANrev. There are 38 commands; each assigned a unique ID that can be issued against an agent by a LANrev Administrator. Examples of LANrev commands include:

Table IV. LANrev Commands

| Command ID | Command Description |
|---|---|
| 1006 | Appoint Administrators |
| 1018 | Remove Inventory Data |
| 1022 | TheftTrack |
| 2039 | Reinstall computer |
| 2050 | Power management settings |

Of specific interest is the "1022" command which is the TheftTrack activation command. The TheftTrack activation command catalogs when, who, what agent, and whether pictures and/or screenshots were activated when an asset was tracked using the LANrev TheftTrack feature. A separate 1022 command entry is created when TheftTrack on a LANrev agent is stopped.

***ServerDatabase***

One of the relevant tables in the ServerDatabase is the "machine_tracking_info" table. This table contains the tracking records reported back by LANrev agents, such as public IP addresses, logged-on user, etc. Additionally, pictures and screenshots (if chosen) are stored in Screenshot and CameraPicture fields in a blob (binary large object data type) column in the machine_tracking_info table.

***AdminDatabase***

The AdminDatabase (AdminDatabase.db) resides within an IT staff member's home directory on LMSD systems that have the LANrev Administration Console installed, and contains all the aforementioned

tables ("Command," "CommandQueue," "CommandQueue_History," and "machine_tracking_info"). The AdminDatabase synchronizes with the LANrev server when used, and stores LANrev data in the aforementioned tables.

#### 3.3.1.7 LANrev Database Analysis

The LANrev databases contain detailed information regarding the objective of reconstructing a history of all recoverable LMSD LANrev TheftTrack activity, including screenshots and pictures. However, no single LANrev database recovered contained a comprehensive listing of who executed LANrev commands, what command was executed, which student laptop it was executed on and when it was executed.

It was stated during interviews with LMSD IT staff that it was common practice for the LMSD LANrev Administrators to routinely execute a "Remove Inventory Data" command on an agent once a laptop is recovered or found and the TheftTrack feature is turned off. This action removes the tracking information, including the pictures and screenshots from the machine_tracking_info table for that agent.

IT staff also stated during interviews that LANrev databases were purged at various periods, citing performance considerations. Analysis confirmed that databases were in fact purged at various periods, usually prior to the school year, thereby deleting all of the activity from the previous year off the server. Additionally, the LANrev servers were not included in a backup process. This factor posed challenges for identifying TheftTrack activations and related data such as pictures returned to the server as a result of activation. However, several other sources of LANrev databases were recovered. Specifically, several ad hoc copies of LANrev databases were found on the LANrev server. These copies appear to have been made during troubleshooting periods. For example, it was clear from the directory names where these databases reside (e.g., troubleshooting) that Administrators copied the databases during troubleshooting efforts. Databases for March 2009 were recovered in this manner.

AdminDatabases were also recovered from LMSD IT Administrator workstations that had the LANrev Administration Console installed. These databases synchronized data from the LANrev server (e.g., Commands, CommandQueue_History, CommandQueue and machine_tracking_info). Several of the AdminDatabases recovered were launched at different time periods; thereby synchronizing at different dates and retaining the LANrev data synchronized on those dates.

In addition to the databases found residing on the LANrev servers and workstations with the LANrev Administration Console, a number of partial databases were also carved from unallocated space on the LANrev server.

Upon identification of all recoverable LANrev databases and tables, relevant data was imported from all of the databases into an aggregated SQLite database, inserting unique records from each source database. Using custom perl scripts, it was possible to import to and query from the aggregated database to analyze the data collected. Data imported into the aggregated database included commands issued to LANrev, as well as the data contained in the machine_tracking_info tables (i.e., data returned from agents upon TheftTrack activations). Some of the data is discussed below.

***LANrev February 18, 2010 Record Deletion***

On February 18, 2010, the day the civil case was made public, LMSD personnel turned off TheftTrack on tracked laptops. Additionally, it was observed that tracking records (e.g., pictures) were deleted from LANrev. This fact was validated by reviewing LANrev databases where the "Remove Inventory Data" commands were seen and also observed by a decrease in file size from the February 18th and 19th "ServerDatabase" databases.

On February 20th, 2010, Mr. Perbix logged onto the LANrev server and created an archive file of the entire directory containing the LANrev server databases; effectively, preserving the current LANrev server databases along with their eight-day rotating backups. This is evident by reviewing one of Mr. Perbix's systems where step-by-step screenshots depicting the creation of the archive file were saved to his workstation. The following screenshot (Figure 7) is one of multiple screenshots showing the archive creation process as stored on Mr. Perbix's system.

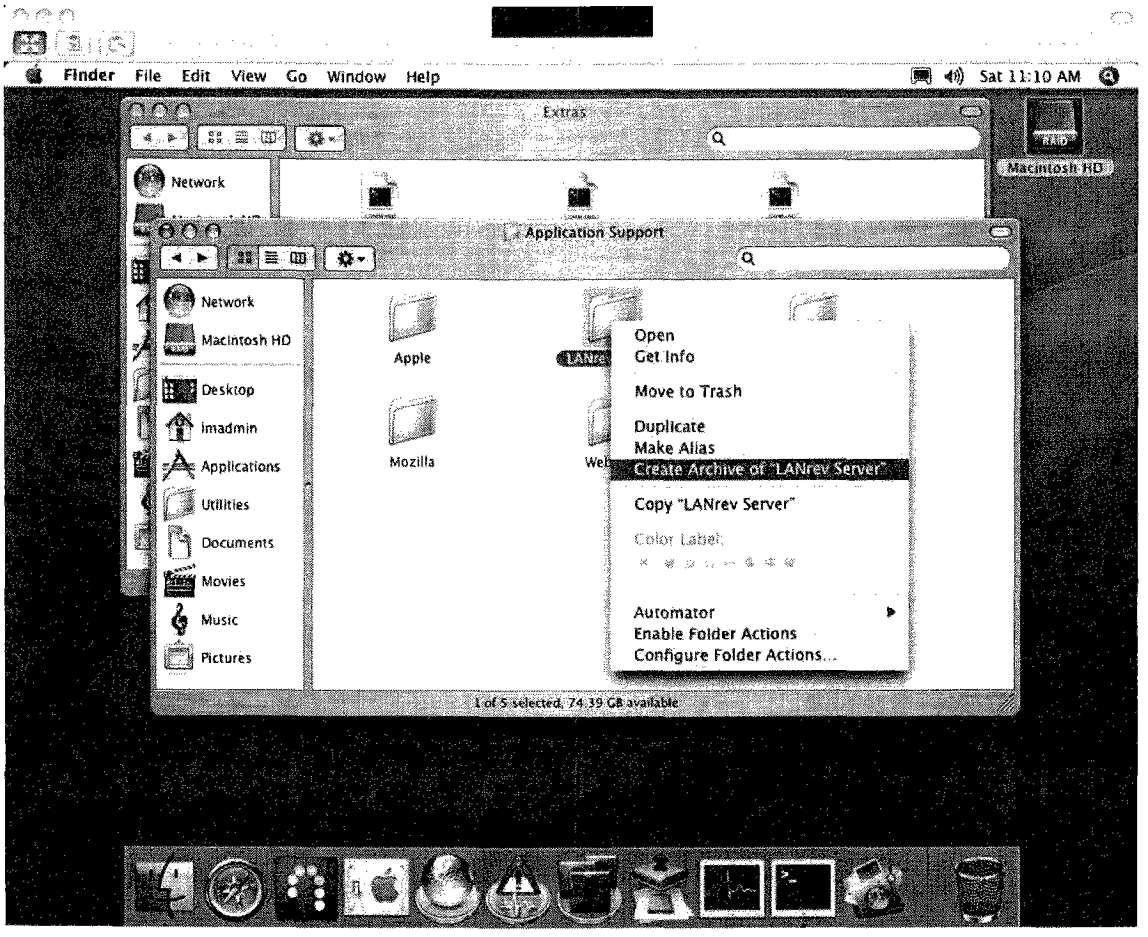



Figure 7. LANrev Server Archive Creation Process

### *LANrev Commands Analysis*

Initial analysis on the LANrev aggregated database focused on LANrev command data. Perl scripts were written to extract all LANrev command data out of the aggregated database. The resulting data output was further pared down to identify three artifacts of the command data: the sequential ID Number (Primary Key), Command Creation Time, and the LANrev Command ID. This dataset was manipulated and arranged to determine what command sequences had been recovered, and what command data was not recovered. The resulting dataset in Table V is shown below.

Table V. Three Facets of the LANrev Command Data

| ID | Command Creation Time | Command ID |
|---|---|---|
| 1 through | 2008-08-07T00:33:19Z | 2036 |
| 14 | 2008-08-12T15:20:23Z | 2019 |
| Missing Commands #15 & 16 | | |
| 17 through | 2008-08-14T09:44:08Z | 2047 |
| 36 | 2008-09-03T15:10:23Z | 2000 |
| Missing Command #37 | | |
| 38 through | 2008-09-03T16:03:55Z | 2000 |
| 59 | 2008-09-25T17:32:12Z | 2000 |
| Missing Command #60 through 65 | | |
| 66 through | 2008-09-26T00:02:05Z | 2047 |
| 69 | 2008-09-26T01:46:25Z | 2047 |
| Missing Command #70 | | |
| 71 through | 2008-09-26T01:47:51Z | 2047 |
| 73 | 2008-09-26T02:03:54Z | 2047 |
| Missing Command #74 & 75 | | |
| 76 through | 2008-09-26T02:12:46Z | 2047 |
| 100 | 2008-09-26T13:21:34Z | 2019 |
| Missing Command #101 | | |
| 102 through | 2008-09-26T13:44:42Z | 2015 |
| 145 | 2008-10-03T00:58:37Z | 2015 |
| Missing Command #146 | | |
| 147 through | 2008-10-03T16:47:13Z | 2000 |
| 1056 | 2009-05-27T13:56:36Z | 2900 |
| Missing Command #1057 through 1119 | | |
| 1120 through | 2009-06-11T14:53:49Z | 1022 |
| Missing Command #1121 through 1574 | | |
| 1575 | 2009-07-20T16:40:48Z | 1005 |
| Missing Command #1576 through 3357 | | |
| 3358 through | 2009-09-07T01:27:17Z | 2047 |
| 3539 | 2009-09-17T12:52:07Z | 2047 |
| Missing Commands #3540 through 3546 | | |
| 3547 through | 2009-09-17T13:01:38Z | 2047 |
| 3630 | 2009-09-25T12:36:29Z | 2019 |
| Missing Commands #3631 through 3633 | | |
| 3634 through | 2009-09-25T14:05:39Z | 2900 |
| 3647 | 2009-09-25T18:15:28Z | 2000 |

| ID | Command Creation Time | Command ID |
|---|---|---|
| Missing Command #3648 | | |
| 3649 through | 2009-09-25T18:19:45Z | 2047 |
| 3651 | 2009-09-25T18:22:14Z | 2047 |
| Missing Commands #3652 & 3653 | | |
| 3654 through | 2009-09-25T18:34:26Z | 2047 |
| 4865 | 2010-02-19T14:54:48Z | 2000 |
| Missing Command #4866 | | |
| 4867 through | 2010-02-22T17:04:05Z | 2000 |
| 4881 | 2010-02-22T17:36:23Z | 2000 |

Each LANrev command issued against a LANrev agent(s) was assigned a unique, sequential identification number (identified in Column 1). This number corresponds to the primary key or "ID" field in the commands table and does appear to synchronize across recovered databases. This assertion is made by also reviewing the sequencing of Command Creation Time (Column 2) as the second artifact. For each LANrev Command, a Command Creation Time is identified with the corresponding Command ID issued (Column 3). Over the period of August 7, 2008 through February 22, 2010, there were 4,881 LANrev commands issued against LANrev agents, with the first recovered LANrev Command issued on August 7, 2008, and the last command issued on February 22, 2010. The first command found corresponds with the upgrade to LANrev Server 4.6.4 (v1159).

The analysis of the Commands recovered reveals gaps in the Sequential ID numbers. For example, Commands #1-14 were recovered; however, Commands #15 and #16 were not recovered, as shown above in Table V.

When analyzed over time, several observations of the command data (shown in Figure 8 below) can be made:

- For the 2008/2009 school year (from August 7, 2008 to May 27, 2009), approximately 98% of LANrev Commands were recovered
- For the 2009/2010 school year (from September 7, 2009 to February 22, 2010), approximately 99% of LANrev Commands were recovered
- Of the commands not recovered starting from August 7, 2008, approximately 98% were between the dates of May 28, 2009 and September 6, 2009