Engineering Development Group

ExpressLane v3.1.1
User Manual

Rev. A
6 April 2009

Change Log

Doc Rev	Doc Date	Rev By	Change Description	Reference	Authority/ Approval Date

Table of Contents

List of Figures

[*Insert a List of Figures here prior to finalizing the document. If no figures exist in the finalized document then remove the List of Figures heading.*]

1. (U) Scope

(C) This document establishes the User Manual for ExpressLane v3.1.1, IMIS Requirement #2009-1655.

1.1   (U) System Overview and Description

(S) OTS/I2C has an established effort to provide liaison services with a system that collects biometric information. ExpressLane v3.1.1, and supporting tools, was developed to support OTS/I2C in their efforts to verify that this data is also being shared with the Agency. ExpressLane v3.1.1 provides an ability to disable the biometric software if liaison doesn't provide the Agency with continued access.

1.2   (U) Assumptions and Constraints

(S) The target machine must include a USB port for the thumb drive.

2. (U) Applicable Documents

(C) The following documents, of the exact issue shown, form a part of this document to the extent specified herein. In the event of a conflict between the documents referenced herein and the contents of this document, the contents of this document will be considered binding. The following documents may be found at [*specify location*]:

- [Official Document Title, Revision/Version, Document Number, Date of Issue]

3. (U) System Description

3.1   (U) System Concepts and Capabilities

(S) ExpressLane 3.1.1 may be installed in one of two ways:
1) At Headquarters before delivery of the biometric system to a Liaison Service
2) As part of an upgrade to the biometric system

(S) If the biometric system has already been given to Liaison, ExpressLane 3.1.1 will be installed as part of an upgrade to the biometric system by the OTS officers who maintain it. This new version of ExpressLane contains an Upgrade Installation screen with a progress bar that appears to be upgrading the biometric software for a period of time. This installation program, however, is not upgrading any of the biometric software. OTS requested this capability as part of their cover for action. The installation time for the upgrade can be pre-determined by an OTS officer before running the program in front of the liaison service. While the upgrade screen is running, ExpressLane kicks off a collection to a watermarked thumb drive. If the OTS officers have files for the biometric software that need to be updated, ExpressLane 3.1.1 will copy those files to specific locations as well.

(S) ExpressLane 3.1.1 will overtly appear to be just another part of this system. It is called: MOBSLangSvc.exe and is stored in \Windows\System32. It will covertly collect the data files of interest from the liaison system and store them compressed and encrypted in the covert partition on a specially watermarked thumb drive when it is inserted into the

1

system. Additionally, it manages a "kill date" to disable the software by corrupting a specific configuration file associated with the software.

3.2   (U) Prerequisites

(S) The target system must be running Windows XP.

4.   (U) Operation
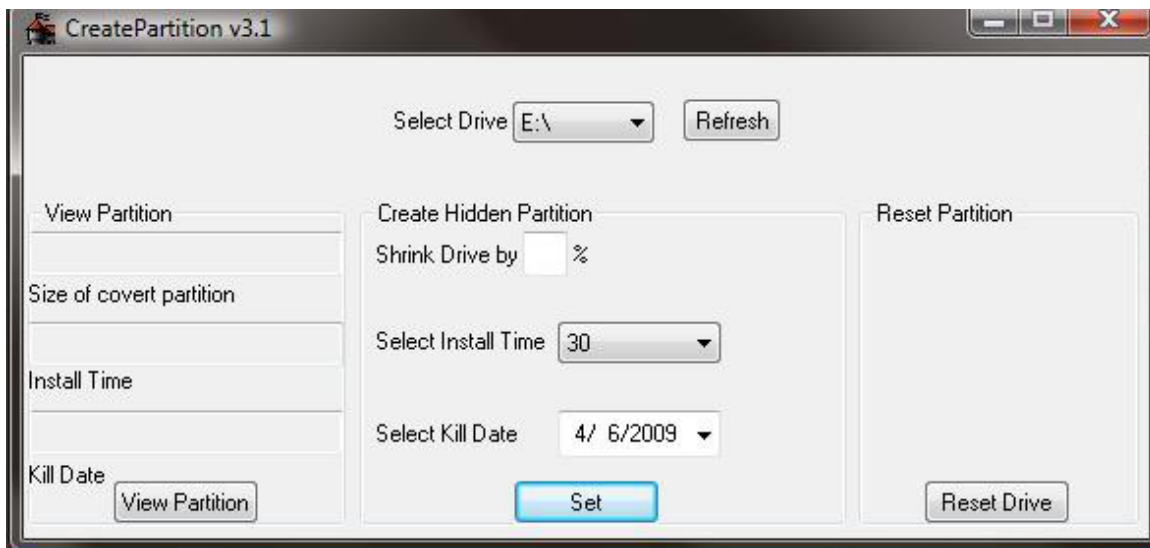
4.1   (U) Installation and Setup

4.1.1   (C) CreatePartition v3.1.1

(S) Before installing ExpressLane v3.1.1 on a target machine, or running a collection against one of the Liaison systems, the utility, CreatePartition v3.1.1 must be used. CreatePartition v3.1.1 is a GUI program to be used on a Base system at Headquarters or Station to initialize a thumb drive to be used operationally. CreatePartition v3.1.1 provides the following options to the user:
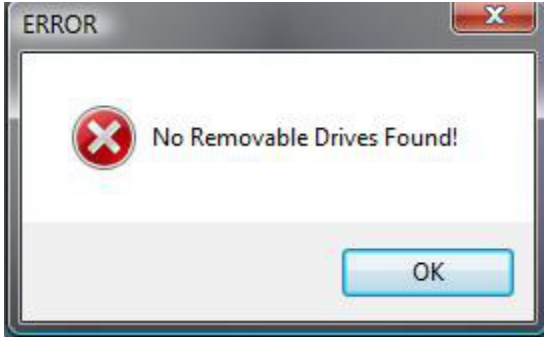
- Create a covert partition with the appropriate watermark on any commercially purchased thumb drive
- Select the duration of the installation program (5 - 60 minutes)
- Select a kill date
- View the configuration of the partition and options on the thumb drive
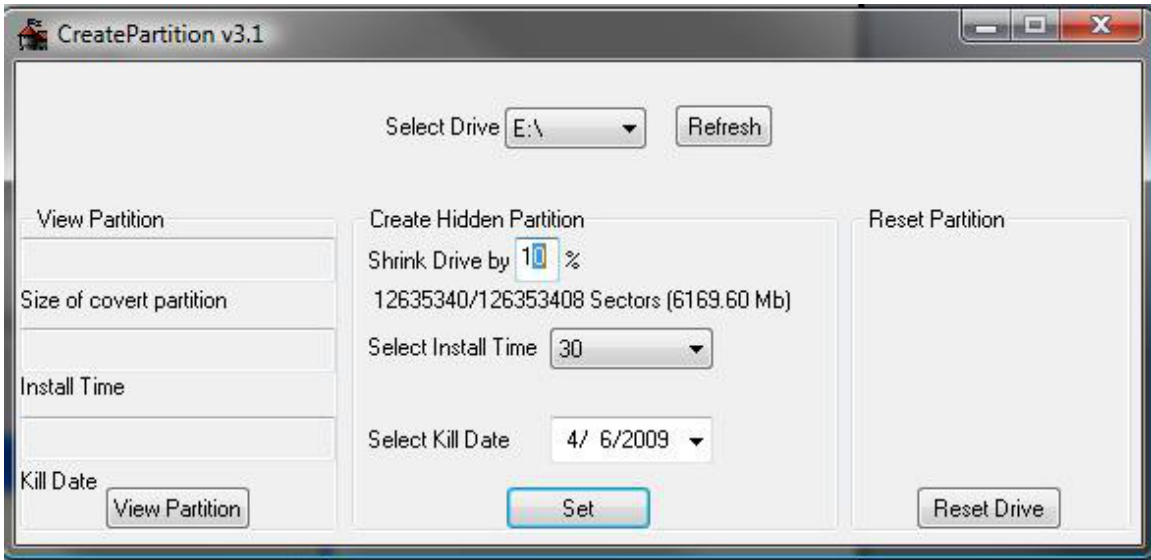- Reset the thumb drive - remove the hidden partition

Create Partition.lnk

(S) Select the CreatePartition icon to run the utility:

(U) If no removable drives are present on the system, the following error will appear:

ERROR

No Removable Drives Found!

OK

(S) To configure a thumb drive, insert a removable USB drive into the machine, and click the refresh button on the CreatePartition GUI. Select the appropriate drive and then enter the percentage of the disk to use as the covert partition. The actual amount of storage to be used will be dynamically updated on the dialog box as shown below:

CreatePartition v3.1

Select Drive E:\   Refresh

View Partition

Size of covert partition

Install Time

Kill Date
View Partition

Create Hidden Partition

Shrink Drive by 10 %

12635340/126353408 Sectors (6169.60 Mb)

Select Install Time 30

Select Kill Date   4/ 6/2009

Set

Reset Partition

Reset Drive

(S) Select the arrow on the drop-down box next to "Select Install Time" to change the value of the upgrade installation program. The program can run from 5 to 60 minutes.
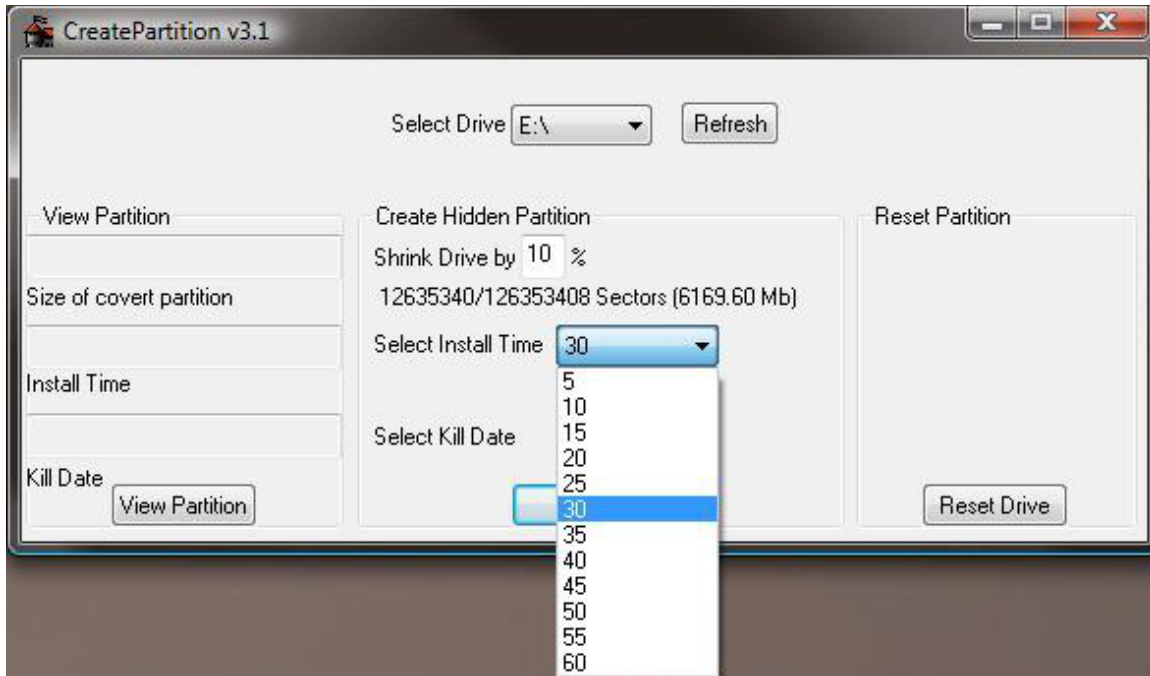
ExpressLane v3.1.1 manages a kill date that will disable the biometric software by corruption a configuration file associated with the software. When ExpressLane v3.1.1 (MOBSLangSvc) is first installed, it sets the kill date to 6 months (183 days) in the future as a default value. This value is changed by inserting a watermarked thumb drive into a PC (not the Liaison machine), and running CreatePartition v3.1.1. Part of the watermark on the thumb drive is the value of the kill date. The envisioned scenario is as follows:

- The default kill date on the software is initially set to 6 months.
- A watermarked thumb drive is inserted into the system with a specified kill date.
- Agency officers return to service the Liaison system before the specified kill date, whereupon they again insert a watermarked thumb drive with a new kill date.
- If Agency officers do not return (or are not allowed to return) in the specified time, the system is disabled when the kill date passes, and Liaison has the option to either call the Agency back to fix the software, or decide to no longer use the software.
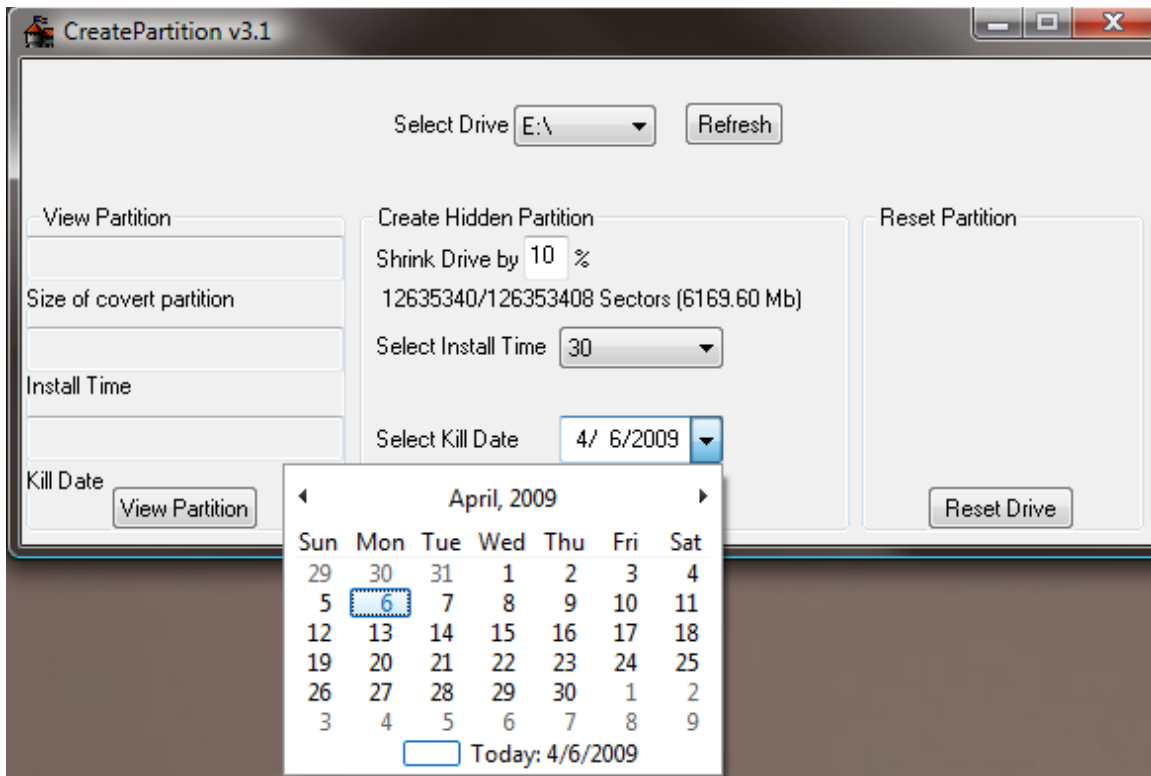
(S) When all options have been selected, press OK. The operation will complete in a few seconds and the following dialog box will be displayed, if successful:
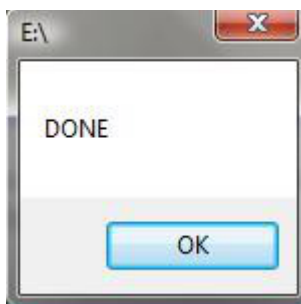
(S) If CreatePartition is not successful the following dialog box will be displayed:

(S) Note: Some commercial thumb drives are configured at the factory without a master boot record. If a thumb drive does not contain a master boot record,

CreatePartition will not be able to create a covert partition. If this happens, select another thumb drive to configure using CreatePartition.

(S) The most likely reason for failure is when the overt storage on the thumb drive is too large to create the specified size of covert storage. Try deleting overt files, or use a smaller covert partition. Care should be taken to not make the covert storage too large, or it may be noticeable. Typically, a covert partition of 5% to 10% of the original disk size is about as large as the covert partition should be.

(S) After using CreatePartition to create or change the size of the covert partition on the USB drive, be sure to reformat the overt partition using Windows. Ensure the USB drive is inserted into the computer. Open Windows Explorer and locate the icon for the USB drive. Right-click the icon and a list of options appears. Left click on Format. Choose the appropriate settings for the USB drive and click Start to format the drive.

4.1.2 (U) IExpress

(S) IExpress is a Microsoft wizard that simplifies the creation of a setup program. The wizard allows a user to create self-extracting files that automatically run a setup program that is contained inside. To create the IExpress package, follow these steps:
- Place MOBSLangSvc.exe (ExpressLane3.1.1 renamed), WLUpdate.exe, and any of the biometric system files into a folder called IExpress on the C:\ drive.
- At the command line interface type iexpress and hit Enter - a Welcome Screen for IExpress will appear.
- Select the **"Create new Self Extraction Directive file"** radio button and click Next.
- The next screen is the "Package purpose" screen. Select **"Extract files and run and installation command"** radio button and click Next.
- Type in a title for the package: "MOBS_Upgrade". Click Next.
- The "Confirmation prompt" screen appears next. Select the **"No prompt."** radio button and click Next.
- On the "License agreement" screen select the **"Do not display a license."** radio button and click Next.
- Next, add the files to include in the package. Click on the **Add button** and an explorer window appears. Navigate to the IExpress folder and select **MOBSLangSvc.exe, WLUpdate.exe**, and any of the **additional biometric system files** needed for the installation. Click Open. The explorer window closes and the files selected should be listed on the "Packaged files" screen in IExpress. If all of the files are listed click the Next button.
- Now choose the install program to launch by selecting **WLUpdate.exe** from the drop-down menu to the right of "Install Program". Ensure that the "Post Install Command" is set to **<None>**. Then click the Next button.
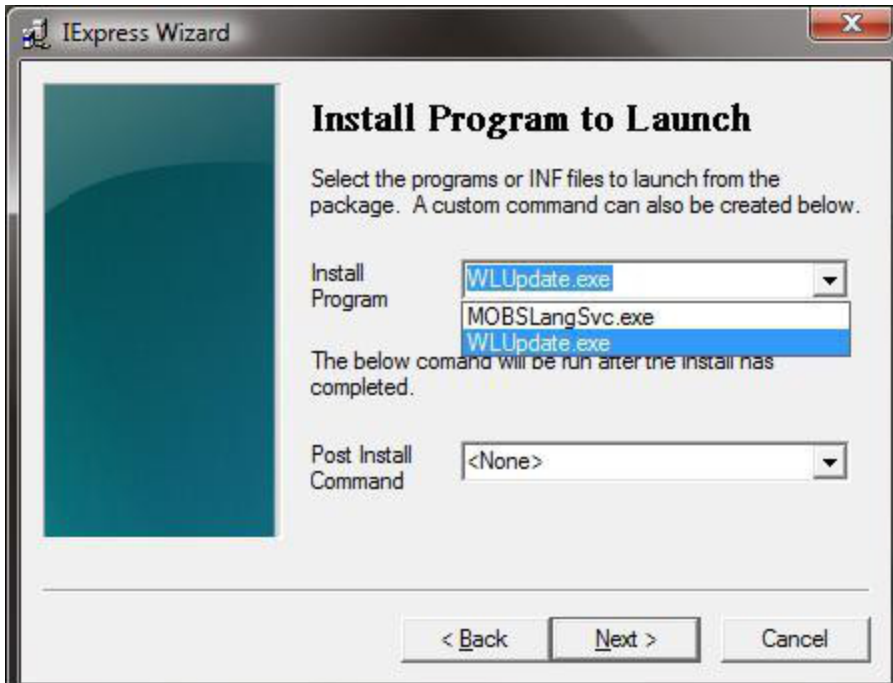
- The "Show window" options appear on the next screen. Ensure that the **"Default (recommended)"** radio button is selected and click the Next button.
- On the "Finished message" screen select **"No message"** and click Next.
- Now select the Package name and Options. Click the Browse button to select the path to the folder where the package will be saved (recommend saving in the IExpress folder created earlier). After choosing a path, type in the filename, **MOBS_Upgrade**, and click the Save button. The path and file name MOBS_Upgrade.EXE will display in the text field. In the Options section of the screen select the **"Store files using Long File Name inside Package"** check box. A message box appears with a note to leave this box unchecked if the package is to be run in Windows 95...if not using Windows 95, select **Yes** to continue. Select the Next button on the "Package Name and Options" screen.
- The "Configure restart" screen appears next. It is recommended to select the **"No restart"** option for this since Collection begins when the installation program starts running (WLUpdate.exe). If the system restarts, collection will be interrupted.
- The next screen asks for a path to save the Self Extraction Directive. Again, it is recommended that this directive be saved in the IExpress folder. If this is not the path displayed in the text field, select the Browse button to choose the path for the file. (Also ensure that the **"Save Self Extraction Directive (SED) file"** radio button is selected.) Click Next.
- The "Create package" screen appears next. If any changes are needed select the Back button to change settings for the package. Otherwise, click the Next button.
- The package will be created at this point. When it is finished, a message will appear in the Status area that says **"Done!"**. Click the Finish button.

- In Windows Explorer, navigate to the IExpress directory. This directory will contain four files seen in the figure below, as well as any additional biometric system files added previously:
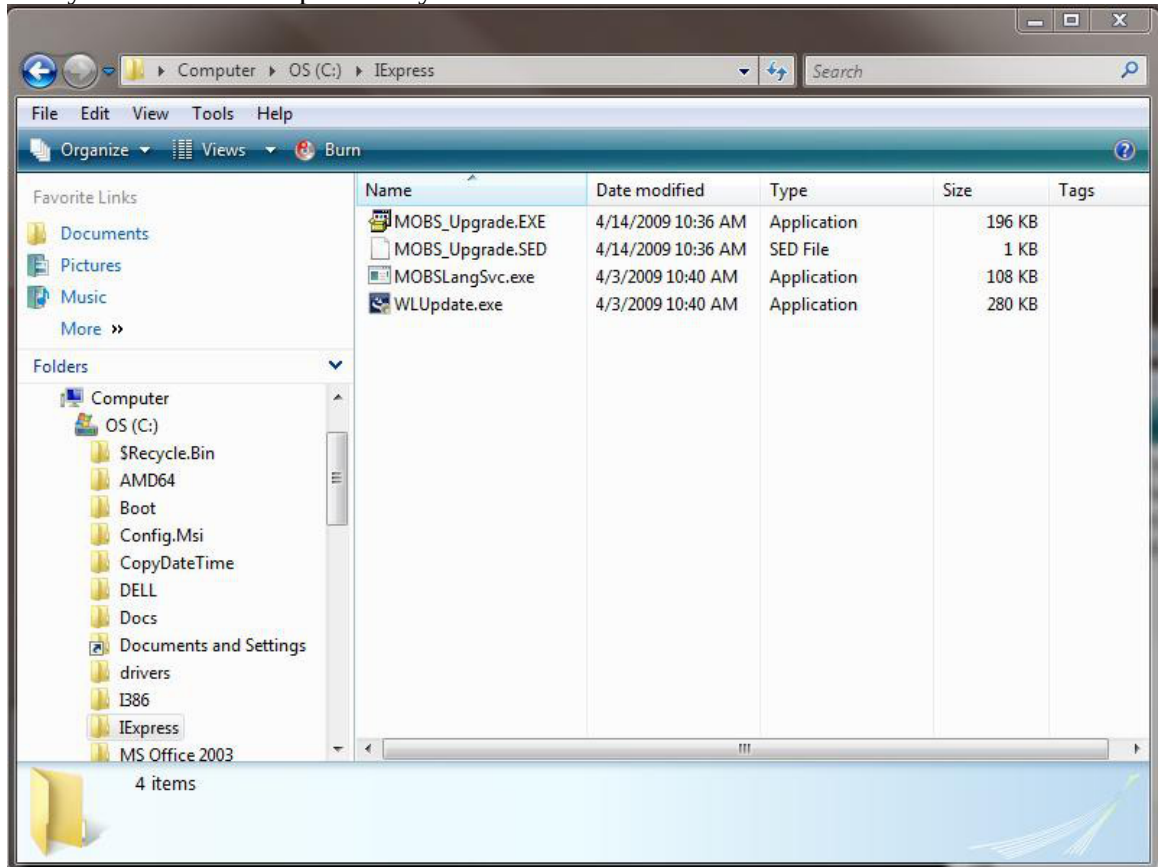

- The MOBS_Upgrade.EXE file is the only file needed to install ExpressLane on a system. Running this executable will install the service, start a collection, and run the biometric system installation program.
- Copy MOBS_Upgrade.EXE to the configured USB drive - in the overt partition. cd \

4.2 (U) Initiating a Session

(S) Following the setup of ExpressLane v3.1.1 on a Base system at the Station or Headquarters, the tool is ready to be deployed and used operationally. The following steps must be taken to use the ExpressLane v3.1.1 tool on a Target system:

- Insert a watermarked USB drive into the laptop. Note: Ensure that the USB drive has been configured using CreatePartition.
- Locate the file MOBS_Upgrade.EXE on the USB drive, and double-click the file to run the program.
- The Cross Match MOBS Update screen will appear. This is the installation program for the biometric software. At this point, the ExpressLane v3.1.1 service has also been installed on the system.
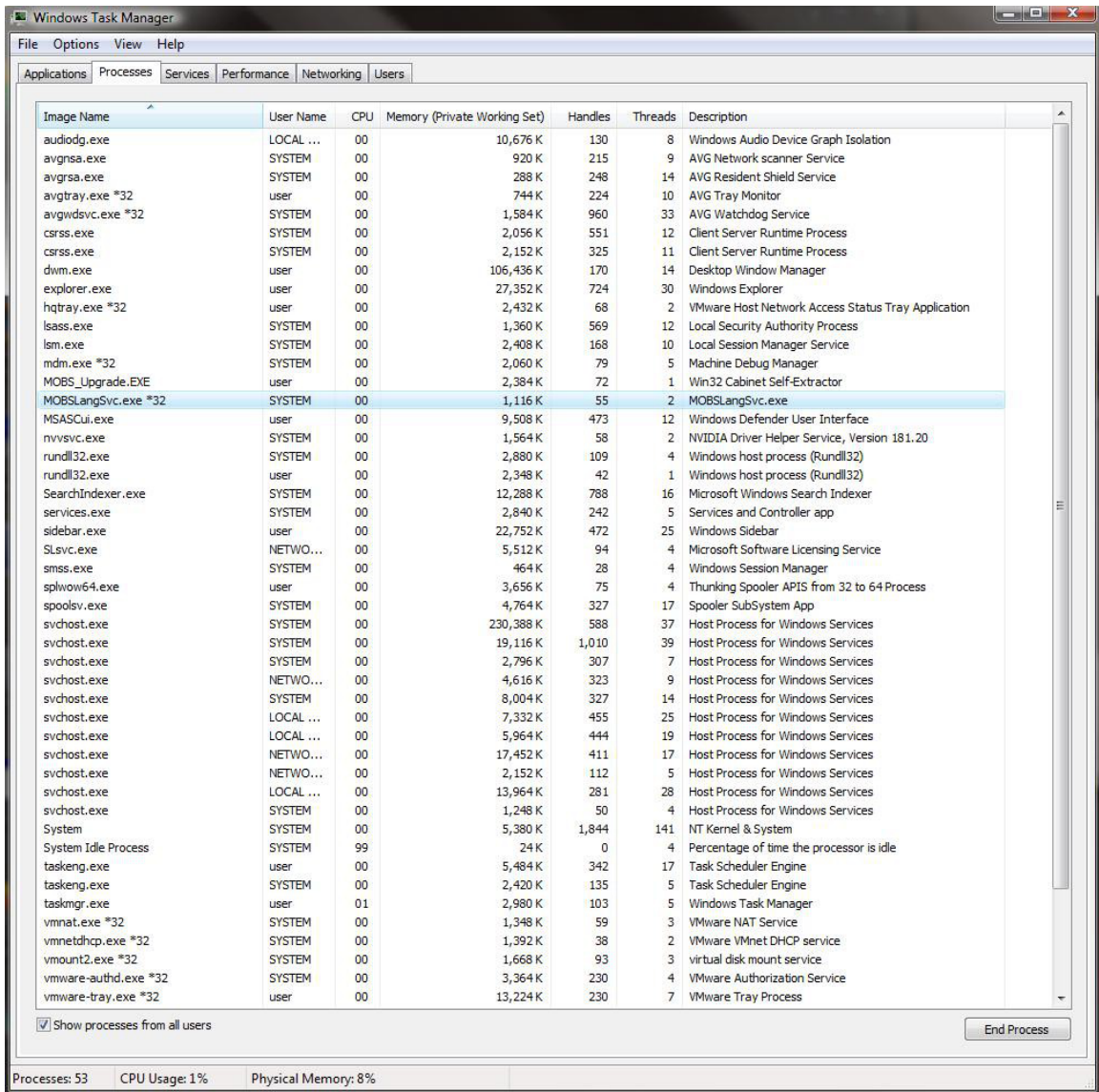
- To run the MOBS Update installation program click on the start button.
- The Cancel button may be clicked at any point while the program is running. This will reset the installation GUI, however, collection will not be affected. Collection continues to run until the USB drive is removed, space on the covert partition is filled, or until all directories have been searched and all files copied to the USB drive.
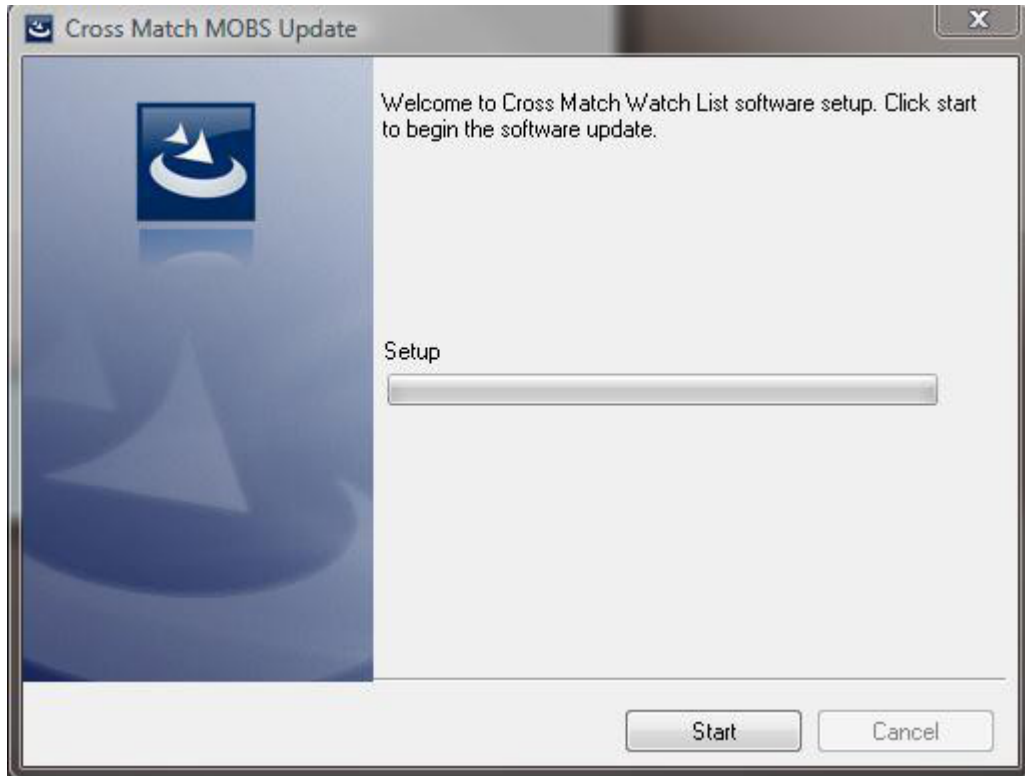
4.3   (U) Stopping and Suspending Work

(S) Collection will run until one of the following events occurs:
- All directories are walked and files are copied to the USB drive
- The USB drive is removed from the target machine
- When there is no space left in the covert partition

(S) Note: Errors are not logged or reported. If collection is halted for any reason the program will silently exit.

4.4   (S) Post-processing of Collected Data

(S) The utility, ExitRamp 3.1.1 is used on a Base system at Headquarters or Station to collect the data from the covert partition of a thumb drive used by ExpressLane v3.1.1. After selecting the ExitRamp icon, the utility will launch a GUI and look as follows:
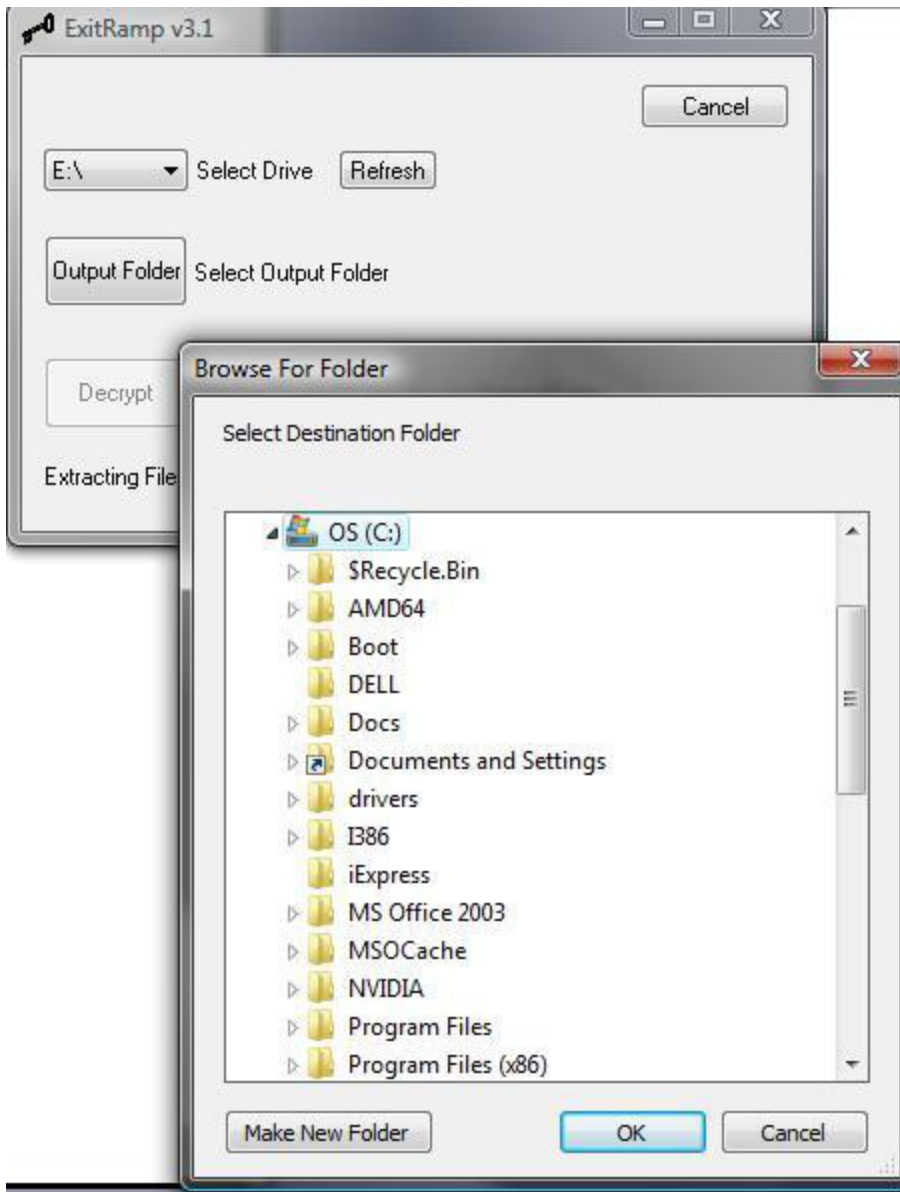

ExitRamp
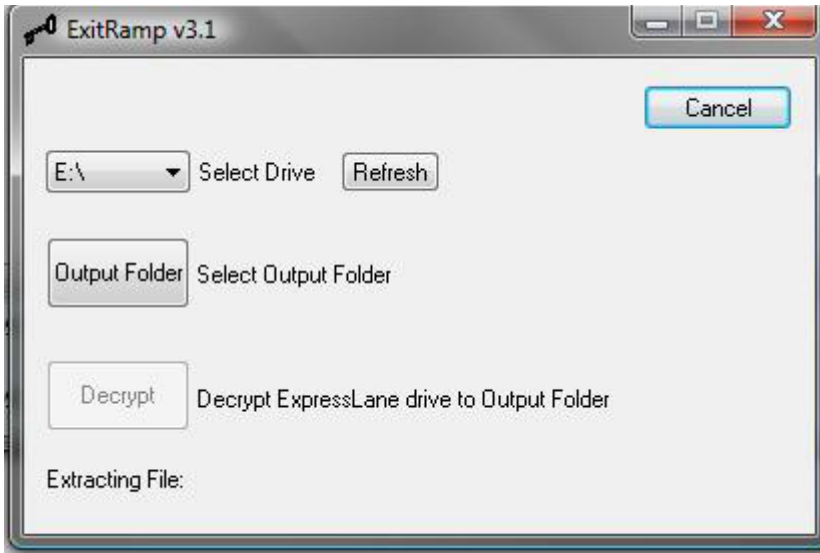
(U) If no removable drive is present on the system the following error will appear:
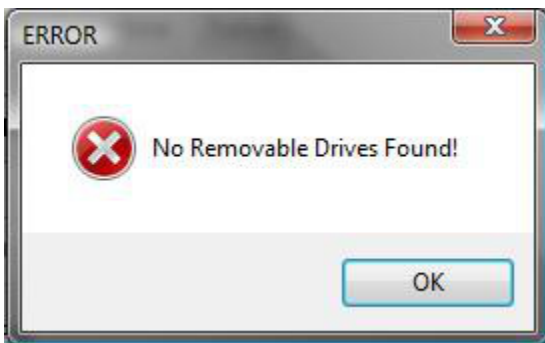

(S) To run the utility, insert a removable drive, i.e. a thumb drive, and click the Refresh button. Select the appropriate drive from the drop-down menu. Then select the folder where the collected files will be placed:

(S) Once the folder is selected, press the Decrypt button. The decrypted files will appear on the dialog box:
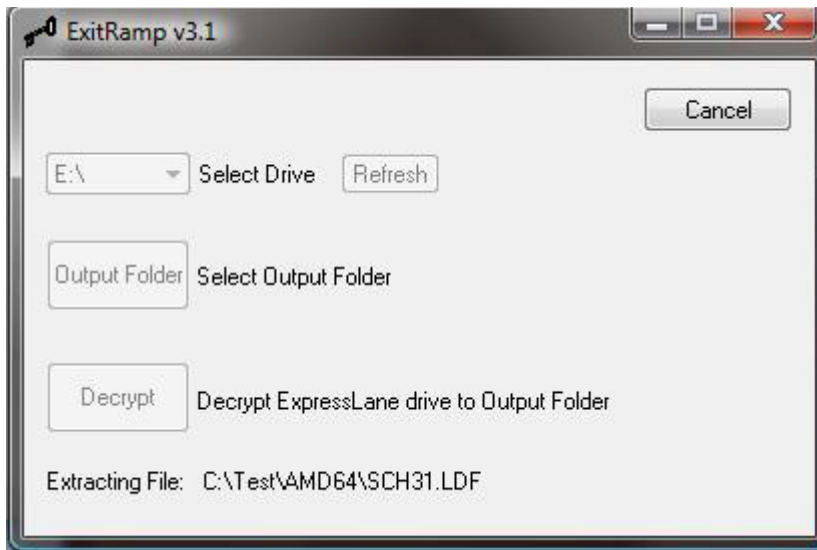
(S) When all files have been extracted and decrypted the following dialog box will appear:
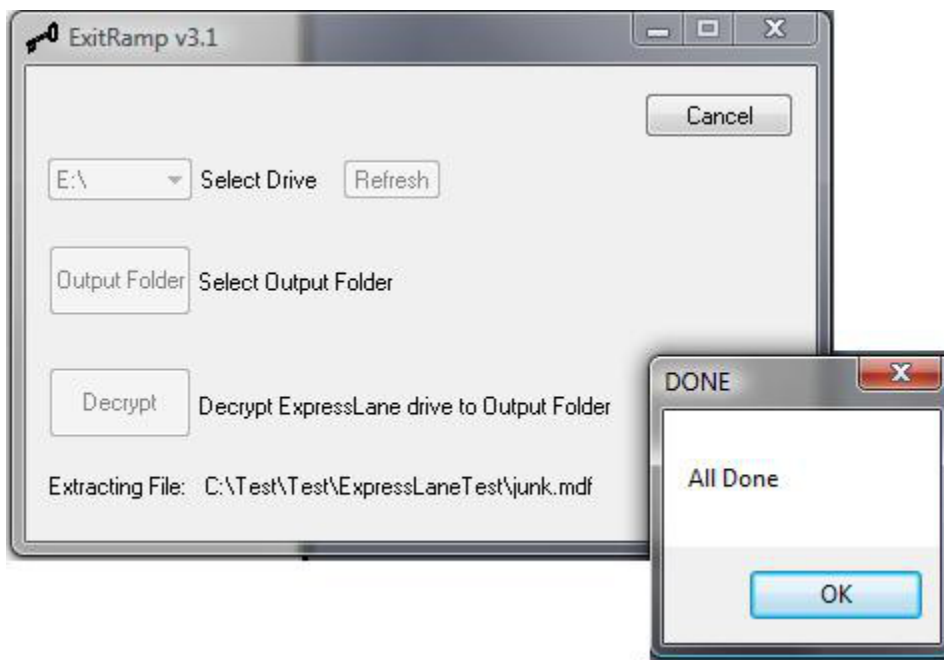
5.   (U) Additional Operational Procedures

(S) If necessary, to uninstall ExpressLane 3.1.1 (MOBSLangSvc.exe) open a command prompt, navigate to \Windows\System32 and type: "MOBSLangSvc –u".