AccessData

MOBILE PHONE EXAMINER
PLUS

MPE+
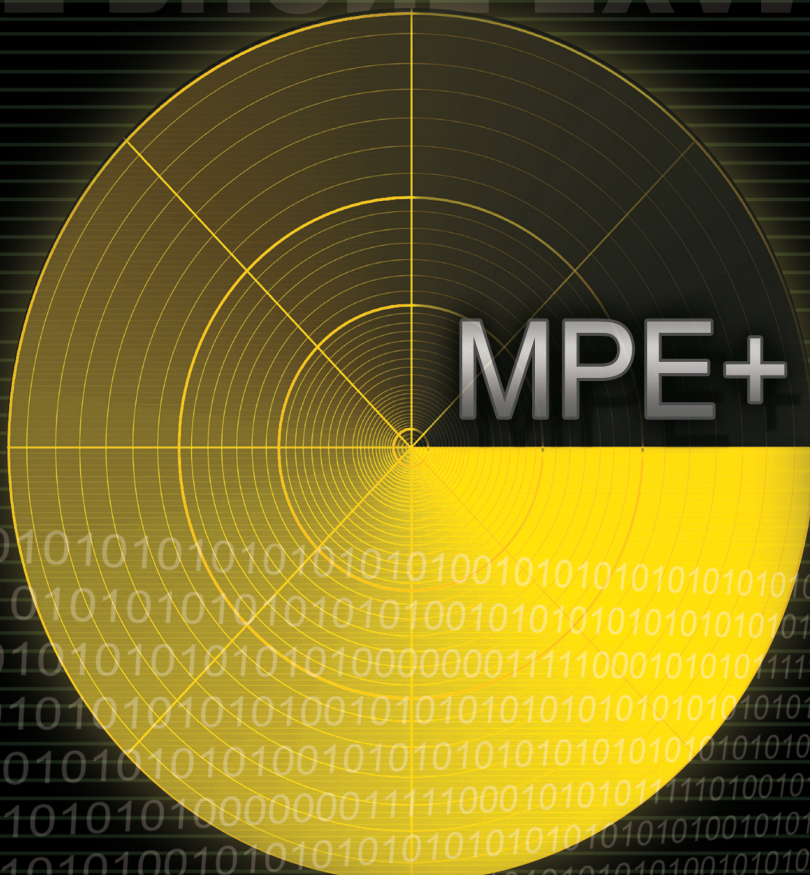
AccessData Legal and Contact Information

Document date: January 10, 2014

Legal Information

AccessData Group, LLC.
588 West 400 South
Suite 350
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, LLC.
- Distributed Network Attack® is a registered trademark of AccessData Group, LLC.
- DNA® is a registered trademark of AccessData Group, LLC.
- Forensic Toolkit® is a registered trademark of AccessData Group, LLC.
- FTK® is a registered trademark of AccessData Group, LLC.
- Password Recovery Toolkit® is a registered trademark of AccessData Group, LLC.
- PRTK® is a registered trademark of AccessData Group, LLC.

- Registry Viewer® is a registered trademark of AccessData Group, LLC.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Third party acknowledgements:

- FreeBSD ® Copyright 1992-2011. The FreeBSD Project.
- AFF® and AFFLIB® Copyright® 2005, 2006, 2007, 2008 Simson L. Garfinkel and Basis Technology Corp. All rights reserved.
- Copyright © 2005 - 2009 Ayende Rahien

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [$variable\_data$] format. Steps that required the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData web site.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData Group, LLC. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AD Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, LLC. 384 South 400 West Suite 200 Lindon, UT 84042 USA *Voice*: 801.377.5410 *Fax*: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales:	*Voice*: 800.574.5199, option 1 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Federal Sales:	*Voice*: 800.574.5199, option 2 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Corporate Sales:	*Voice*: 801.377.5410, option 3 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Training:	*Voice*: 801.377.5410, option 6 *Fax*: 801.765.4370 *Email*: Training@AccessData.com
Accounting:	*Voice*: 801.377.5410, option 4

Technical Support

Free technical support is available on all currently licensed AccessData products.

You can contact AccessData Customer and Technical Support in the following ways:

AD Customer & Technical Support Contact Information

Standard Support:	Monday through Friday, 5:00 AM – 6:00 PM (MST), except corporate holidays. *Voice*: 801.377.5410, option 5 *Voice*: 800.658.5199 (Toll-free North America) *Email*: Support@AccessData.com
After Hours Phone Support:	Monday through Friday 6:00 PM to 1:00 AM (MST), except corporate holidays. *Voice*: 801.377.5410, option 5

AD Customer & Technical Support Contact Information (Continued)

After Hours Email-only Support:	Monday through Friday 1:00 AM to 5:00 AM (MST), except corporate holidays.
	Email: afterhours@accessdata.com
Standard Support:	Monday through Friday, 8:00 AM – 5:00 PM (UK-London), except corporate holidays.
	Voice: +44 207 160 2017 (United Kingdom)
	Email: emeasupport@accessdata.com
After Hours Support:	Monday through Friday, 5:00 PM to 1:00 AM (UK/London), except corporate holidays.
	Voice: 801.377.5410 Option 5*.
After Hours Email-only Support:	Monday through Friday, 1:00 AM to 5:00 AM (UK/London), except corporate holidays.
	Email: afterhours@accessdata.com
Web Site:	http://www.AccessData.com/Support
	The Support web site allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your "trouble tickets", and in-depth contact information.
AD SUMMATION	Americas/Asia-Pacific:
	800.786.2778 (North America).
	415.659.0105.
	Email: support@summation.com
Standard Support:	Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays.
After Hours Support:	Monday through Friday by calling 415.659.0105.
After Hours Email-only Support:	Between 12am and 4am (PST) Product Support is available only by email at afterhours@accessdata.com.
AD Summation CaseVault	866.278.2858
	Email: support@casevault.com
	Monday through Friday, 8:00 AM – 6:00 PM (EST), except corporate holidays.
AD Summation Discovery Cracker	866.833.5377
	Email: dcsupport@accessdata.com
Support Hours:	Monday through Friday, 7:00 AM – 7:00 PM (EST, except corporate holidays.

Note: All support inquiries are typically responded to within one business day. If there is an urgent need for support, contact AccessData by phone during normal business hours.

Documentation

Please email AccessData regarding any typos, inaccuracies, or other problems you find with the documentation: *documentation@accessdata.com*

Professional Services

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK, FTK Pro, Enterprise, eDiscovery, and Lab. They can help you resolve any questions or problems you may have regarding these products

Contact Information for Professional Services

Contact AccessData Professional Services in the following ways:

AccessData Professional Services Contact Information

Phone	Washington DC: 410.703.9237
	North America: 801.377.5410
	North America Toll Free: 800-489-5199, option 7
	International: +1.801.377.5410
Email	*adservices@accessdata.com*

Table of Contents

Chapter 1
Introduction

AccessData (AD) Mobile Phone Examiner Plus (MPE+) VELOCITOR is an appliance used to extract mobile device data from Chinese chipsets for forensic review. MPE+ VELOCITOR is used in conjunction with AccessData (AD) Mobile Phone Examiner Plus (MPE+) as part of a mobile field unit or in the lab. MPE+ VELOCITOR can extract physical NOR/NAND images and extract information such as phone and address book data, media files, call logs, SMS and MMS messages, and file system data stored in the memory of a mobile device.

Audience

The MPE+ VELOCITOR manual and the MPE+ manual are written for law enforcement and corporate security professionals with the following competencies:

- Basic knowledge of and training in forensic policies and procedures
- Basic knowledge of and experience with personal computers, mobile phones, enhanced PDAs, and SmartPhones
- Familiarity with the fundamentals of collecting digital evidence from mobile devices
- Understanding of forensic data images and how to acquire forensically sound images
- Experience with case studies and reports
- Basic competency with MPE+
- Familiarity with the Microsoft Windows environment

Scope

This manual documents the available tools, functions, and other features built into the MPE+ VELOCITOR appliance. For more infomation about the functions and features of MPE+, please see the MPE+ User Guide. For information on proper mobile device forensics and data analysis practices, you should register for one of AccessData's beginner, intermediate, and / or specialized mobile forensics workshops.

Chapter 2
Getting Started

This chapter contains all the information you need to get started with MPE+ VELOCITOR, including the requirements needed to run MPE+ VELOCITOR, as well as information on connecting devices to your computer through the MPE+ VELOCITOR appliance. Once you have completed the tasks covered in this chapter, MPE+ VELOCITOR will be ready to extract and save data.

Licensing

MPE+ VELOCITOR requires the following to operate correctly:

- A copy of MPE+.
- MPE+ License, which is required to launch the application.
- Installation of CodeMeter software. The version of CodeMeter that runs depends upon the license that you've purchased.
- A valid MPE+ VELOCITOR License.

See *Managing Security Devices and Licenses* in the MPE+ User Guide for more information on licensing.

Installing Drivers

Before the MPE+ appliance and the device can be connected, you need to launch MPE+ and install device drivers before to begin extracting data.

To install drivers

1. Launch MPE+.
2. Under *Product Information*, click the *Driver Management* tab.
3. Locate and expand **International** drivers.
4. Click **Download** for the following drivers:
   - MTK
   - FTDI
   - Spreadtrum
   - M-STAR
5. Once the drivers download, click **Install.**

Connecting MPE+ VELOCITOR

MPE+ VELOCITOR is an appliance that connects to both the device from which you are extracting data and the system that you are using to analyze the data. Before extracting data from the device, verify that MPE+ VELOCITOR is properly connected to both the device and the system.

To connect MPE+ VELOCITOR for extracting data

1. Plug the USB cable provided into the USB port on the MPE+ VELOCITOR box.
   MPE+ VELOCITOR is powered through the USB port.
2. Plug the other end of the USB cord into your system.
3. There is a 26 pin cable that is included with MPE+ VELOCITOR. Plug the end of the cable that does not have the power clip leads into the appliance. This is the male end of the cable.

MPE+ VELOCITOR Cable
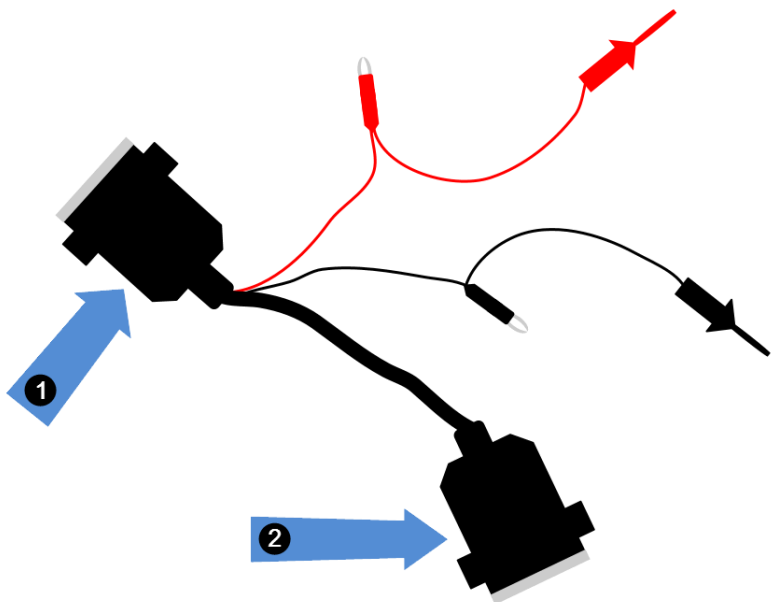
MPE+ VELOCITOR Cable

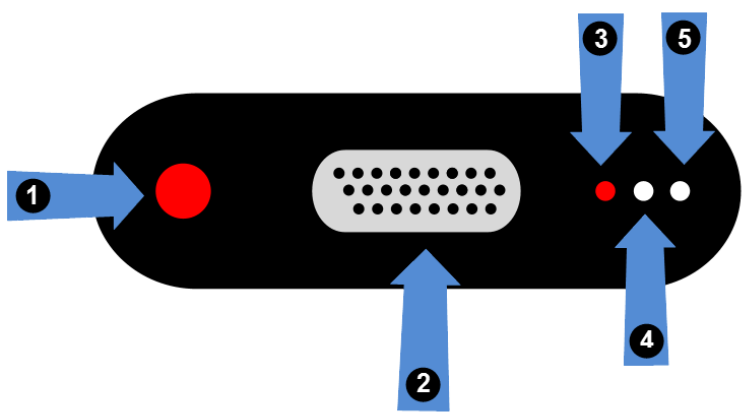| Number	Item
1	Device end
2	VELOCITOR end

MPE+ VELOCITOR - Cable Port Side

MPE+ VELOCITOR - Cable Port SIde

Number	Item
1	9 volt to 5 volt power switch
2	26 PIN adaptor
3	Box power
4	Phone power
5	Transmit/Receive

4. Plug the device end of the 26 pin cable into your system. This should be the female end of the cable with the power leads attached.

5. The red button on the appliance should be in the up, or USB, position.

6. If the appliance is receiving power, the red Box Power light will be lit.

To connect a mobile device

1. Remove the device's battery.

2. Attach the red positive power clip lead to the device's positive pole and the black negative power clip lead to the device's negative pole. Use the smaller power clips that are at the end of the leads if the battery has the clips. If the battery poles are the blades, use the larger alligator clips that are on the leads. Using the alligator clips for anything other than the blade type poles can damage the battery pins and make the device inoperable.

> **Note:** Having the poles reversed does not adversely affect the device. However, the device will not communicate with the appliance until the leads are properly connected.

Chapter 3

Extracting Data with MPE+ VELOCITOR

Once the device is properly attached to the VELOCITOR appliance, you can start extracting data.

Extraction Dialog

You can access the extraction dialog as follows:

- After opening MPE+, click the **Select VELOCITOR Device** button in the *Main* tab view.

Extraction Dialog Options

Element	Description
Auto Detect Chipset	With this box selected, MPE+ VELOCITOR will attempt to identify the chipset. Unselected allows the selection of the chipset to be examined.
Connect	Click to connect the device to MPE+.
Interface	COM should be selected when extracting data. If connection does not occur with the device, select USB. By selecting USB, MPE+ VELOCITOR will begin the installation of the USB drivers for the connected phone. Wait for the drivers to install to continue with the extraction.
Detected Manufacturer	Once MPE+ VELOCITOR determines the device's manufacturer, the manufacturer will be visible here.
Detected Chipset	Once MPE+ VELOCITOR determines the device's chipset, the chipset will be visible here.
Status Message	This window updates as the appliance detects the chipset, loads the bootloader, and reads the flash.
Reset	If you need to terminate the extraction at any time, click **Reset.**
Cancel	Pressing **Cancel** resets the extraction and returns to the MPE+ main user interface.

Extracting Data

To extract data

1. Click **Select VELOCITOR Device** in MPE+.

2. Verify that **Auto Detect Chipset** is selected and that **Interface** is set to COM. Click **Connect**.

   ● The phone power indicator light on the VELOCITOR appliance will not light until you click **Connect** in the dialog box.

3. When the red **Hold Power Button** displays, depress the power button on the acquired device until the **Hold Power Button** disappears.

   ● You may be prompted at least two different times to hold the power button during the device's connection, and possibly several more times during the extraction process.

   ● If MPE+ VELOCITOR fails to determine the manufacturer and chipset after a period of time, See Troubleshooting on page 16.

4. Once MPE+ VELOCITOR detects the manufacturer and chipset, MPE+ can search for the correct boot loader for the device if **Auto Detect Boot** is checked. A boot loader is a program that loads the main operating system. Verify that **Auto Detect Boot** is selected to start this process. You also can uncheck Auto Detect Boot and manually select a boot loader.

   Note: MPE+ VELOCITOR cycles through various boot loaders in order to determine the correct boot loader for the device. This process may make several attempts before the correct boot loader is determined.

5. Click **Extract Data**. MPE+ VELOCITOR extracts the data located on the device. If the red **Hold Power Button** appears in the dialog box, depress the power button on the acquired device until the **Hold Power Button** disappears.

6. Once the data is extracted, MPE+ VELOCITOR saves the image file and parses the data. When parsing is complete, MPE+ automatically makes the data available for viewing. You can now examine and carve the data.

   ● To learn more about parsing, carving, and reviewing data, see the MPE+ User Guide.

   ● If you have any trouble with extracting data, See Troubleshooting on page 16.

Chapter 4
Troubleshooting

This section deals with common problems that may occur when using the MPE+ VELOCITOR appliance.

Failed to Connect

If you can't connect to the device while holding the power button when prompted, try to connect again without holding the power button. Spreadtrum and M-STAR devices do not need the power button held down for connection.

Failed to Detect COM Port

If the COM port has not been detected by MPE+ VELOCITOR, it could be:

- The correct driver may not be installed. Verify that the FTDI, MTK, M-STAR, and Spreadtrum drivers are installed. See on page 13.
- MPE+ VELOCITOR may not be connected. Verify that all cables are securely connected. See See Managing Security Devices and Licenses in the MPE+ User Guide for more information on licensing. on page 10.
- The MPE+ VELOCITOR appliance or the USB cable may be faulty. Contact your AccessData representative if you suspect a faulty device or cable.

Failed to Detect Chipset

If the chipset has not been detected by MPE+ VELOCITOR, it could be:

- The power leads connecting the device to the MPE+ appliance may be reversed. Reverse the power leads on the device and try to extract the data again. See See Managing Security Devices and Licenses in the MPE+ User Guide for more information on licensing. on page 10.
- You need to press the power button on the device to get the device to communicate with the appliance.

- MPE+ cannot auto detect the chipset. Click **Reset**, unselect the **Auto Detect Chipset** box, and select the chipset from the options in the menu for the Chipset Manufacturer. After choosing a chipset manufacturer, click **Connect**.

- The device may need a UART connection to communicate with the appliance. This is an advanced technique. To learn how to create a UART connection, please attend AccessData's training on MPE+ VELOCITOR. For more information on attending this training, please contact your AccessData representative.

- The device is not supported. MPE+ VELOCITOR was created to extract data from Chinese devices. Other types of devices are not recognized.

Failed to Advance

If MPE+ VELOCITOR fails to advance in the extraction process, it may be:

- MPE+ VELOCITOR may take up to several minutes to acquire the correct boot loader. This is the correct operating procedure. See Extracting Data with MPE+ VELOCITOR on page 14.

- Some chipsets, particularly MTK, require the power button to be pressed on the device before it can transmit data. If MPE+ VELOCITOR seems to stop at a particular boot loader and fail to advance, you can force the appliance to examine the next boot loader in the sequence by releasing the power button on the acquired device and pressing the power button again.

- MPE+ VELOCITOR has stopped functioning. To correct this, unplug MPE+ VELOCITOR from both your system and the device. Next, reattach MPE+ to both your system and the device. Click **Reset** in the dialog box and click **Connect**.