MAGNET ACQUIRE

COMMUNITY EDITION

GETTING STARTED

CONTENTS

OVERVIEW

As the usage of mobile devices continues to increase, it's important that you be able to efficiently acquire as much information as possible from these devices. Magnet ACQUIRE offers a new approach to the acquisition of smartphone images, an approach designed to deal with issues introduced by enhanced security on iOS and Android. By using several different methods of extraction, Magnet ACQUIRE is able to retrieve as much data as possible, given the constraints of a modern smartphones. Magnet ACQUIRE is also able to capture images from common storage drives, including HDD, SSD, SD and USB flash, and other external devices.

In this guide, you'll learn how to:

- Set up a mobile device for imaging
- Acquire Android, iOS, and drive images
- Open the image in Magnet IEF

SYSTEM REQUIREMENTS

To get the best performance from Magnet ACQUIRE, ensure that your computer fulfills the following requirements:

- Operating system: Windows 7 or later
- File system: NTFS
- Memory: 4GB RAM minimum
- Microsoft .Net 4.5
- Available disk space for acquired images
- Latest version of iTunes (required for acquiring iOS images).

Note: Running Magnet ACQUIRE through a virtual machine is not currently supported.

IMAGE TYPES

The type of image that you choose depends on your time restraints and the type of data that you're looking for.

DRIVE IMAGE TYPES

For drives, there are three types of images:

- The **Entire contents of the drive** option represents a physical image of the drive. During this type of acquisition, Magnet ACQUIRE copies the entire contents of the drive into a single file (by default, a raw image file).
- The **All files and folders** option represents a logical image that contains all files and folders. During this type of acquisition, Magnet ACQUIRE copies all files and folders into a single, compressed file. This does not include deleted files and/or content.
- The **Targeted acquisition** option represents a logical image that contains important files for forensic analysis. During this type of acquisition, Magnet ACQUIRE copies files such as system files, user profiles, and more into a single, compressed file. The locations that Magnet ACQUIRE targets are typically the ones that are most likely to contain evidence.

MOBILE IMAGE TYPES

For mobile, there are two types of images:

- A **quick** image is a comprehensive logical image that contains both user data and some native application data. Magnet ACQUIRE uses multiple acquisition methods to get you as much information from the device as quickly as possible so that you can start examining the evidence right away.
- A **full** image is a physical or file-system logical image. During this type of acquisition, Magnet ACQUIRE copies the entire contents of a drive into a single file (either a .raw file or a .zip file, depending on the target).

SUPPORTED DEVICES

Magnet ACQUIRE supports a number of different types of drives and mobile devices.

DRIVES

Magnet ACQUIRE can obtain images from HDDs, SSDs, USB and SD flash drives, and other external drives. Windows, OS X, and Linux are all supported.

IMAGE TYPE	OS	EVIDENCE
Entire contents of the drive	Windows, Linux, OS X	A physical image of the entire drive.
All files and folders	Windows, Linux, OS X	A full, logical file system image that includes all files and folders. This does not include deleted files and/or content.
Targeted acquisition	Windows	Pagefile, Hibernation File, Master File Table, USN Journal, Event Logs, Setup API Logs, Windows Registry Hives, LNK Files, User Profiles, Prefetch Files
	Linux	System logs, home, sleep images, tmp, etc, and usr.
	OS X	System logs, home, sleep images, tmp, etc, and usr.

ANDROID DEVICES

Magnet ACQUIRE can obtain a quick image from any Android device (2.1 and later) and a full image from any rooted Android device.

For full images, if an Android device is not rooted, Magnet ACQUIRE attempts to gain privileged access to the device using tested rooting methods. Magnet ACQUIRE creates a log file documenting the process, and indicates which roots are tried and whether any are successful.

Quick images are formatted as .raw files and full images as .zip files.

IMAGE TYPE	OS	METHODS	EVIDENCE
Quick	2.1 to 3.2.6	Android Debug Bridge (ADB) pull command	Contents of any external storage (i.e. SD card).
	2.1 to 3.2.6	Agent application	Call logs, SMS/MMS, browser history, and user dictionary.
Quick	OS 4+	ADB Backup / Agent application	Third-party application user data Some native device data including SMS/MMS, browser history, calendar, call logs, BT devices, WiFi hot spots, user accounts, and user dictionary. Contents of any external storage (i.e. SD card).
Full	OS 2.1 to 5 Requires a rooted device. Magnet ACQUIRE will root select devices.	Linux DD command	Recover a full physical image of the device's flash memory. Evidence collected will include all files, folders, user data, native data and unallocated space.

iOS DEVICES

Magnet ACQUIRE can obtain a quick image from any iOS device (5.0 and later) and full images from any jailbroken iOS device.

Both full and quick images are formatted as .zip files.

IMAGE TYPE	OS	METHODS	EVIDENCE
Quick	5.X to 8.X	iTunes backup process	Third-party application user data Some native device data including SMS/MMS and iMessage, calendar and call logs
	5.X to 8.X	Apple File Conduit	Camera pictures, ringtones and iTunes books

IMAGE TYPE	OS	METHODS	EVIDENCE
	Below 8	File relay	Some native device data including complete photo album, SMS/MMS and iMessage, address book, typing cache, geolocation cache, application screenshots, WiFi hot spots, voicemail and native email metadata.
Full	5.X to 8.3 Requires a jailbroken device	Apple File Conduit 2	For jailbroken iOS devices Magnet ACQUIRE will recover a full logical file system dump which includes all of the files, folders, user data and native data.

ACQUIRE A DRIVE IMAGE

1. Connect a drive to your computer using USB.
2. Start Magnet ACQUIRE. Details about the drive appear automatically.

3. Select the drive that you want to acquire and click **NEXT**.
4. Choose the type of image that you want to acquire and click **NEXT**.
5. Provide details about the image, such as the folder name and destination, the examiner name, and evidence number.
6. Click **ACQUIRE**.

When imaging is complete, the **SUMMARY** screen displays information about the time required to create the image, the image size, and its location. You can also open the folder containing the image.

ACQUIRE A MOBILE IMAGE

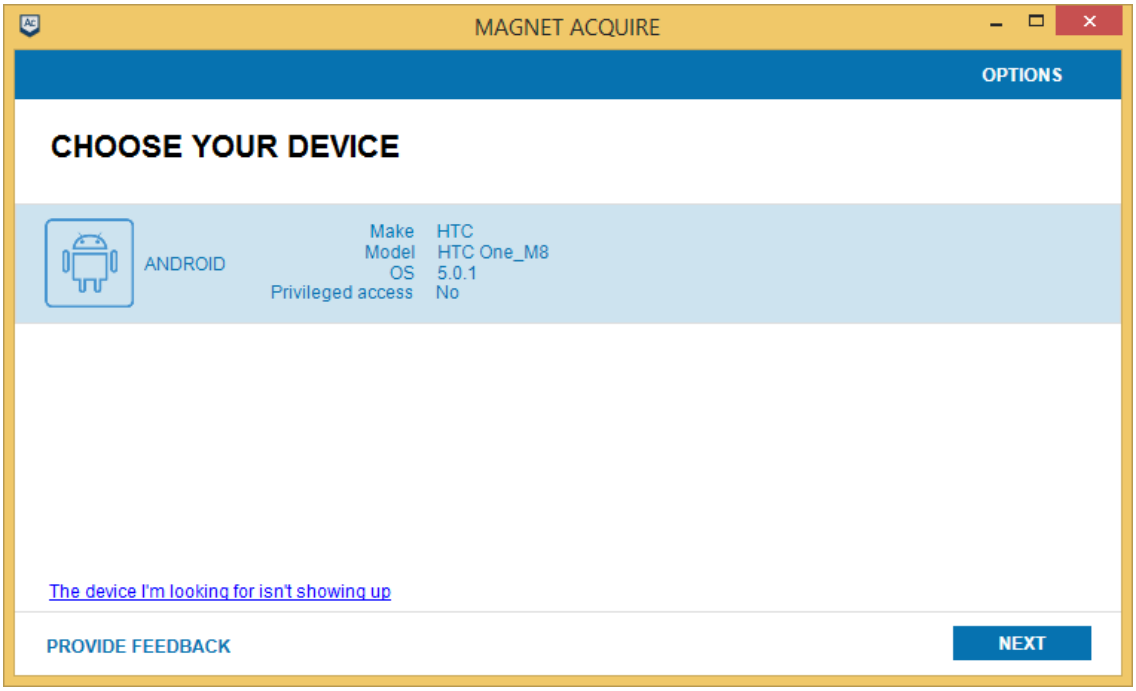
Before you begin: See MOBILE DEVICE CONFIGURATION to learn how to configure a device correctly.

1. Connect the mobile device to your computer with a USB cable.
2. Start Magnet ACQUIRE.
3. On the **CHOOSE YOUR DEVICE** screen, do one of the following actions:
4. If the device you want to image doesn't appear in the list, you might need to install the drivers for that device. Click **The device I'm looking for is not showing up**.
5. Select a device type and click **NEXT**.

6. Do one of the following:
   - For iOS, you must install Apple iTunes before you can proceed. After you install iTunes, click **NEXT** to restart the Apple Mobile Device Service. After the service restarts, the device appears on the **CHOOSE YOUR DEVICE** screen.

- For Android, follow the instructions on the screen to disconnect and reconnect the device. Depending on the version of Windows that you use, Magnet ACQUIRE might have to download the drivers over the Internet. If you're not currently connected to the Internet, Magnet ACQUIRE provides a URL for where you can download the drivers separately. After you install the drivers, the device appears on the **CHOOSE YOUR DEVICE** screen.

7. If the device you want to image appears in the list, select the device and click **NEXT**.

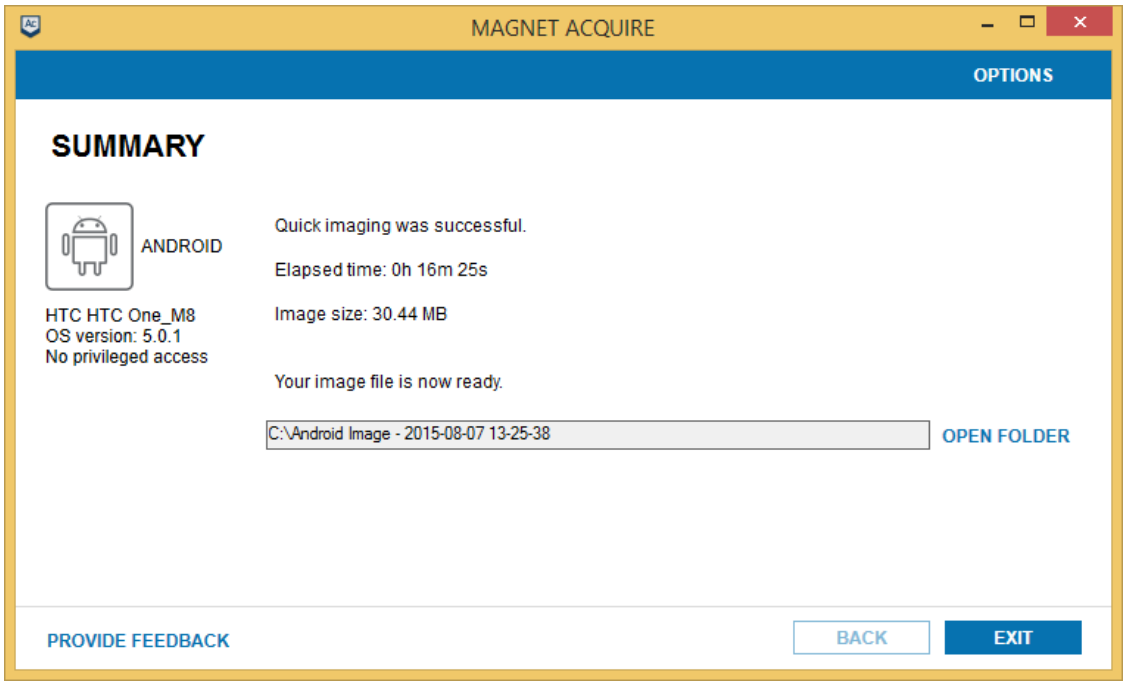


8. On the **SELECT IMAGE TYPE** screen select either **Quick** or **Full**. Click **NEXT**.

9. On the **CREATE EVIDENCE FOLDER** screen, enter information about the image. The folder name and destination are required fields. Click **ACQUIRE**.

10. Follow any instructions that Magnet ACQUIRE presents to you during the imaging process.

When imaging is complete, the **SUMMARY** screen displays information about the time required to create the image, the image size, and its location. You can also open the folder containing the image.



MOBILE DEVICE CONFIGURATION

When you connect a device to your computer using a USB cable, Magnet ACQUIRE should recognize the device automatically. In instances where Magnet ACQUIRE doesn't recognize the device, you should verify the following:

- The device is powered on.
- The device is properly connected to your computer with a USB cable.
- Airplane mode is turned on (not necessarily required, but is a best practice).
- Lock screen is disabled and the screen is set to stay awake/never turn off.
- If you know the password for the device, disable the password lock.
- The device must trust the computer it's connected to. When you connect the device to your computer, follow the device's on-screen instructions to trust the computer. For Android devices, you must enable USB debugging before you receive a prompt to trust a computer.
    - For Android, you can revoke the trust setting in the Developer Options menu, using the **Revoke USB Authorizations** option.

- For iOS, there is no way to revoke the trust of a computer.

- For iOS devices:
  - The device must be running iOS 5 or later (earlier versions are not supported)
  - The computer must have latest version of iTunes installed.
- For Android devices:
  - The device must be running Android 2.1 or later (earlier versions are not supported)

> The device must NOT have MTP / Mass storage enabled. Having this setting enabled might cause the device to unmount the SD card, resulting in less data being acquired during a quick image.

  - The device must have USB debugging enabled (developer mode). How to enable USB debugging varies from device to device, but you can usually enable it by pressing the build number multiple times in the device's Settings menu. Here's where you can find the Settings menu for a few popular devices:

Android 2.x+	Settings > Applications > Development Tap the **Enable USB Debugging option**.
Android 4.2+	Settings > About phone Tap the **Build Number** field approximately 7 times until the message "You are now a Developer" displays on screen.
HTC One (M7/M8/M9)	Settings > About > Software information > More > Build number Tap the **Build Number** field approximately 7 times until the message "You are now a Developer" displays on screen.
LG G2/G3 Samsung Galaxy	Settings > About phone > Software information > Build number Tap the **Build Number** field approximately 7 times until the message "You are now a Developer" displays on screen.
Stock Android	Settings > About phone Tap the **Build Number** field approximately 7 times until the message "You are now a Developer" displays on screen.

- The computer must also have mobile device drivers installed. You can obtain the latest drivers through Windows Update or from the device manufacturers' websites. For example:
  - HTC - http://www.htc.com/us/software/htc-sync-manager
  - LG - http://www.lg.com/us/support/software-manuals
  - Motorola - https://motorola-global-portal.custhelp.com/app/answers/detail/a_id/88481
  - Nexus - http://developer.android.com/sdk/win-usb.html
  - Samsung - http://www.samsung.com/us/support/downloads
- To ensure that Magnet ACQUIRE is pulling as much data as possible from Android devices, use the following device settings (the wording of the settings may vary depending on the device manufacturer):
  - Disable **Verify apps over USB or Verify apps: Block or warn before installing apps that may cause harm**
  - Enable **Unknown Sources: Allow installation of apps from sources other than the Play Store**
  - Enable **Apps from unknown sources**

- For more information about Android devices, visit the Android developer page: http://developer.android.com/tools/extras/oem-usb.html

OPEN THE IMAGE IN MAGNET IEF

After you acquire an image, you can open it in Magnet IEF with a few simple steps.

1. Start Magnet IEF.
2. Click the **MOBILE** button.
3. Choose the OS of the device image.
4. Click the **Images** button.
5. Browse to the location where you saved the device image and double-click the images.zip file.
6. Click **OK**.

GLOSSARY

Full image	A full image is a physical or file-system logical image. Magnet ACQUIRE can extract a full image from only rooted Android and jailbroken iOS devices. When an Android device is not rooted, Magnet ACQUIRE attempts to gain privileged access to the device using tested rooting methods. Magnet ACQUIRE creates a log file documenting the process, including which roots were tried and if one was successful. For Android devices, Magnet ACQUIRE saves the full physical image as a .raw file; for iOS devices, it saves the file-system logical image to a .zip file.
Jailbroken	The state in which an iOS device's security restrictions are removed, permitting privileged access to the iOS file system and manager.
Logical image	A logical image contains a file and folder structure representative of a portion of a device's memory contents or the entire memory contents.
Physical image	A physical image contains all data from all areas of the device that are capable of having data stored within them, whether defined for use or not.
Privileged access	Escalated privileges to gain access to functionality (i.e. APIs) that has been restricted by device manufacturers and carriers. Privileged access provides: • The ability to modify or delete system files • Low-level access to hardware (i.e. DD) • Full control of the CPU and kernel • Full application control, including the ability to backup, restore, or batch edit applications
Quick image	A quick image is a comprehensive logical image that contains both user data and select native application data. Magnet ACQUIRE uses multiple acquisition methods to get you as much information from the device as possible quickly so you can start examining the evidence sooner. Magnet ACQUIRE saves the quick images for both Android and iOS devices as .zip files.

Root (rooting)	See privileged access