MAGNET ACQUIRE

COMMUNITY EDITION

FAQ

CONTENTS

WHAT DEVICES DOES MAGNET ACQUIRE – COMMUNITY EDITION SUPPORT?

- Drives including HDD, SSD, USB and SD flash drives, and other external drives. Windows, Mac OS, and Linux are all supported.
- Android devices running 2.1 or later for quick images, or rooted for full images. If an Android device is not rooted, Magnet ACQUIRE attempts to gain privileged access on the Android device using tested rooting methods.
- iOS devices running 5.0 or later for quick images, or jailbroken for full images.

WHAT ARE THE SYSTEM REQUIREMENTS?

To get the best performance from Magnet ACQUIRE, ensure that your computer complies with 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.

WHY ISN'T MY MOBILE DEVICE SHOWING UP IN THE LIST OF DEVICES?

When you connect an Android or iOS 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 have USB debugging enabled (developer mode). Enabling 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 has 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

WHAT TYPE OF IMAGE SHOULD I SELECT?

For mobile, Magnet ACQUIRE can obtain two types of images: Quick and Full.

- 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. Magnet ACQUIRE can extract a full image from only rooted Android and jailbroken iOS devices. 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.

For drives, Magnet ACQUIRE supports three types of images: Entire contents of the drive, All files and folders, and Targeted acquisition.

- 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.