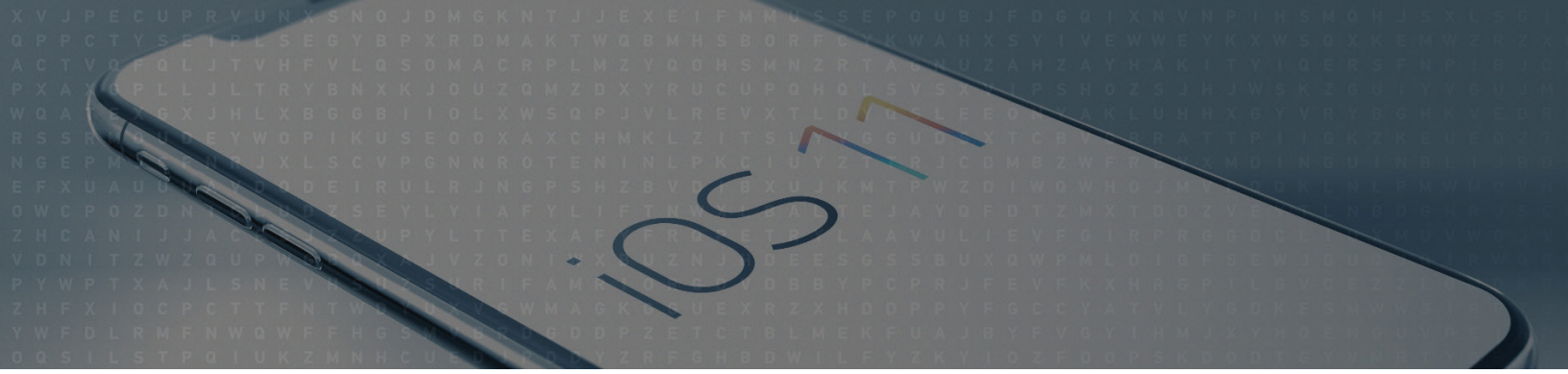

ACQUIRING AND PARSING DATA FROM IOS 11 DEVICES

A GUIDE TO THE BIG IMPACT OF APPLE'S SMALL CHANGES

MAGNET FORENSICS®

ACQUIRING AND PARSING DATA FROM IOS 11 DEVICES

Each new iOS release tends to dominate headlines with the big new features Apple hopes users will find indispensable. Those banner features often come with a lot of smaller changes that can have big effects on forensic processes, such as where you might find evidence on an iPhone, iPad or iPod.

In this white paper, we'll take you through some of the features that were introduced in the latest versions of iOS and highlight some ways you may need to change your workflow to find evidence, including:

1. How to access more evidentiary data with new acquisition methods and tools.
    - Grayshift's GrayKey device can obtain full file system and memory dumps.
    - With the ability to reset encrypted backup passwords, you can create your own encrypted backup to examine.
    - Biometric authentications let you acquire data from the cloud, even when you don't know the device PIN code.
2. Where to find new datasets, or data stored in new or different locations.
    - The database changes introduced in iOS 10 resulted in changes to .plists and SQLite database files alike, so what you're used to looking for in one location may exist elsewhere.
    - In iOS 11, .plists associated with Do Not Disturb While Driving, new tables within old databases, or even the new vision framework for object detection can affect your evidence.
3. How certain artifact changes could affect the way your forensic tool parse data.
    - The new nanosecond timestamp format in iOS 11, and its coexistence in some of the same databases alongside millisecond timestamps, affects iMessages.
    - Safari browser history stored on the device only goes back 30 days.
    - "Container" high-efficiency photo and video file formats are more prevalent.

Access More Evidentiary Data with New Acquisition Methods and Tools

Grayshift's GrayKey device has gained a lot of attention for its ability to crack iOS passcodes and allow forensic examiners to access full file system and memory dumps. Less headline-grabbing, but no less significant, are acquisition methods that rely on biometric authentications and backup password resets. Biometrics allow you to rely on cloud acquisitions to obtain data even when you don't know the handset lock code. The ability to reset encrypted backup passwords, meanwhile, lets you create your own encrypted backup to examine.

iOS Acquisitions Using Grayshift's GrayKey

Only available to law enforcement, GrayKey supports data from iPhone, iPad, and iPod Touch devices running iOS 9, 10, and 11. (GrayKey doesn't support the 32-bit iPhone 5s or 5c.)

GrayKey is best known for its ability to bypass PINs. As an acquisition tool it's capable of pulling more data than traditional iTunes backup methods, or even file systems available with jailbroken devices. For example, the full file system acquisition available from GrayKey allows you to obtain things that aren't available in iOS backups, such as iOS Mail.

> ...GrayKey can extract resident memory. This provides access to certain data which the forensic community hasn't seen[1] since Jonathan Zdziarski's boot ROM vulnerability methods[2] were available.

Once the device is plugged in, you can get some preliminary data including its UDID, UDID chip, iOS version, and device owner. When you perform a full filesystem acquisition, the GrayKey device saves it as a standard zip archive. A full keychain dump will get username/passwords including social media, every app password, and the iTunes backup password. GrayKey also provides a fully decrypted iTunes backup format, including data not available in typical iTunes backups.

Additionally, if the iOS device is in its "after first unlock" state, GrayKey can extract resident memory. This provides access to certain data which the forensic community hasn't seen since Jonathan Zdziarski's boot ROM vulnerability methods were available.

iTunes Backup Changes Include a New Reset Mechanism

Obtaining backup data is always a good idea, when possible, because it's another good source of potential evidence. However, changes in iOS 10 made it harder to process the backup file from the computer synced to the device.

Starting with iOS 10, users are prompted to create an iTunes backup password the first time the device is backed up. The challenge for many users, with this OS, was that their iTunes backup lock code was different from their device lock code. That made it easy to forget. Compounding this challenge, Apple didn't offer a way to help users retrieve their iTunes backup code. As a result, users had no way to create a new backup or push an existing one to their device.

This was a challenge for forensic examiners, too. If you didn't have the device, the backup password, or the ability to brute-force the password, the backup would remain encrypted and unusable. With access to the physical device, however, you could obtain the password even if you didn't have the device owner's consent. To achieve this, you'd need to:

1. Brute-force it using a tool such as Passware Kit Forensic[3]
2. Remove it via PIN

While Apple's backup encryption still uses iOS 10.2+ recursive iterations, in iOS 11, Apple made it possible to reset the backup password and remove previously set backup encryption.

If you have access to the physical device, and you know the handset lock code but not the encrypted iTunes backup password, you can now reset the password. In turn,the new password allows you to clear out the backup password and create new, unencrypted backups for examination.

A caveat: before trying the iTunes backup password reset on an evidence device, you should thoroughly test it on an exemplar device to see what else (besides the password) changes on the reset. However insignificant these changes may be—for example, background wallpaper—they do still need to be validated, especially if there's a chance you may testify in court.

> In iOS 11, Apple made it possible to reset the backup password and remove previously set backup encryption[4]...the new password allows you to clear out the backup password and create new, unencrypted backups for examination[5].

Changes to Backup Encryption Across iOS 10 Versions

iOS 10 had some security failures, which led to changes in backup encryption between 10.0, 10.1, and 10.2.

Pre-10.2, backup encryption passwords went through 10,000 PBKDF2 (SHA-1) iterations. Then, however, their outputs were stored in an escrow keybag, which was stored in the same location as iOS 9. An additional key was stored in the Manifest.db file, this one a SHA-256 hash.

Realizing its mistake, Apple removed the key from Manifest.db in iOS 10.1. However, the old keybag could still be located inside Manifest.plist. As a result, in iOS 10.2, Apple took backup encryption to the next level, encrypting the entire Manifest.db and adding new properties to Manifest.plist.

Decrypting the Manifest.db is still necessary to rebuild an iOS 11 backup. It also contains the public encryption keys for decrypting the files. The key plus the salt, stored in Manifest.plist, are passed though the PKBDF2, SHA-256 variant 10 million times. The resulting output is combined with another salt, also stored in Manifest.plist, and passed through PKBDF2, SHA-1 variant 10,000 times. This stored key ends up in the escrow keybag.

Use Biometric Authentication to Obtain Cloud-Based Data

TouchID or FaceID can unlock a phone, but not connect to the device. To image a device, you have to pair it to a computer.

However, new pairing restrictions require a physical lock code for an iPhone to be paired to a computer. Until now, all the user had to do to get the computer to "Trust" an iOS device was to unlock the device. (Figure 1) To get a forensic image, likewise, you can no longer use TouchID, and must use the handset lock code.

iOS 11 introduced additional enhancements to security. In particular, forensic examiners can no longer exploit biometric unlock.

Figure 1: New pairing restrictions on an iPhone paired to a computer require a physical passcode.

What USB Restricted Mode Means for Forensics

Another pairing wrinkle came with the iOS 11.4 beta and, later, the official 11.4.1 release. If you're examining a device with an earlier iOS 11 version, pairing records still work. As of the beta, not only did the records expire after 7 days; but also, if the phone wasn't unlocked within 7 days, the USB port went into "Restricted Mode." In USB Restricted Mode, only a power charge, no data, can pass through a port, rendering it impossible to use for a forensic image[6].

As of iOS 11.4.1, the window of opportunity narrowed even further—to just one hour. Fortunately for forensic examiners, research quickly showed that USB Restricted Mode could be disabled by simply plugging in a USB device such as Apple's Lightning to USB 3 Camera Adapter[7]. (Less fortunately, USB Restricted Mode was still triggered upon the device entering SOS Mode[8].)

Two things to keep in mind about USB Restricted Mode:

- It may change yet again with iOS 12 or another sub-version of iOS 11.4.
- Because the time restriction alone may not be enough of an "exigent circumstance" to create an exception to a search warrant, consider capturing data directly from iCloud.

Emergency SOS Mode can be activated when the device owner either presses the power button rapidly five times, or presses the side button simultaneously with the volume button. (This mode will only work one way or the other depending on how the user set it up.) This disables touch ID and sends an SOS message to designated contacts.

You may, depending on your jurisdiction, be able to legally compel a fingerprint but not a password. However, Emergency SOS mode can be a problem when you detain a suspect whose SOS message can, for example, ask contacts to wipe their data remotely, as well as when SOS triggers USB Restricted Mode.

Both Face ID and Touch ID fall under similar restrictions as pairing. A handset lock code is required under the following conditions:

- The device has just been turned on or restarted.
- The device has not been unlocked in more than 48 hours.
- The unlock code hasn't been used in 156 hours, and Face ID hasn't been unlocked in 4 hours.
- When the device receives an unlock command.
- Following five unsuccessful attempts to match the appropriate biometric data.
- After the phone has initiated power-off or Emergency SOS.
- Upon SIM card removal (this is not documented in the Apple Security Document.)

If you don't have the handset lock code, your options depend on your legal authorization. Acquisition without a PIN or passcode requires:

- The device itself
- Authorization for iCloud acquisition
- Username and password for the iTunes account
- Access to the backup network to force a fresh cloud backup
- Biometric access if two-factor authentication (2FA) is utilized

iCloud backups don't require a PIN. However, 2FA, which iOS 11 encourages, may be on the physical device, which you'll need to get at the backup.

More than just a text message, iOS 2FA presents the location from where the device is being accessed, and a 6-digit authorization code is hidden behind the lock screen.

iCloud backups don't require a PIN. However, 2FA, which iOS 11 encourages, may be on the physical device, which you'll need to get at the backup.

The device must also be a "Trusted Device" through iCloud. You can use iCloud tokens acquired from iDevices, Mac or PC without the need to verify the second factor step[9]. If 2FA is enabled and you want to acquire cloud data, you will have to access the device when using a tool like AXIOM Cloud to finish the authentication. Alternatively, 2FA can be "answered" using biometrics[10]. To obtain the Apple ID Verification Code, you can use TouchID or FaceID (depending on the iPhone model) to get the required verification code. Enter the code, and you will be able to obtain the backup[11].

Bear in mind that iCloud 2FA does notify the user when their password has been used to login.

Finding Data Stored in New or Different Locations

iOS 10 and its subsequent versions, 10.1 and 10.2, introduced some significant new features that continue to impact Apple devices running iOS 11.

Database Changes

The backup structure changed for the first time since iOS 4. Versions 4-9 featured SHA-1 named files, with the hash consisting of the filepath-filename. The manifest.mbdb file recorded information about the iTunes backup real filename, file directory and structure[12]. Property list, or .plist, files contained data related to browsing history, favorites, locations, configurations, etc[13]. In particular:

- Info.plist recorded information about backups, such as iOS device name, iOS version, build version, backup date, serial number and more.
- Manifest.plist recorded information about installed applications.
- Status.plist recorded the status of an iTunes backup, if the iTunes backup completed[14].

The database changes introduced in iOS 10 resulted in changes to .plists and SQLite database files alike, so what you're used to looking for in one location may exist elsewhere.

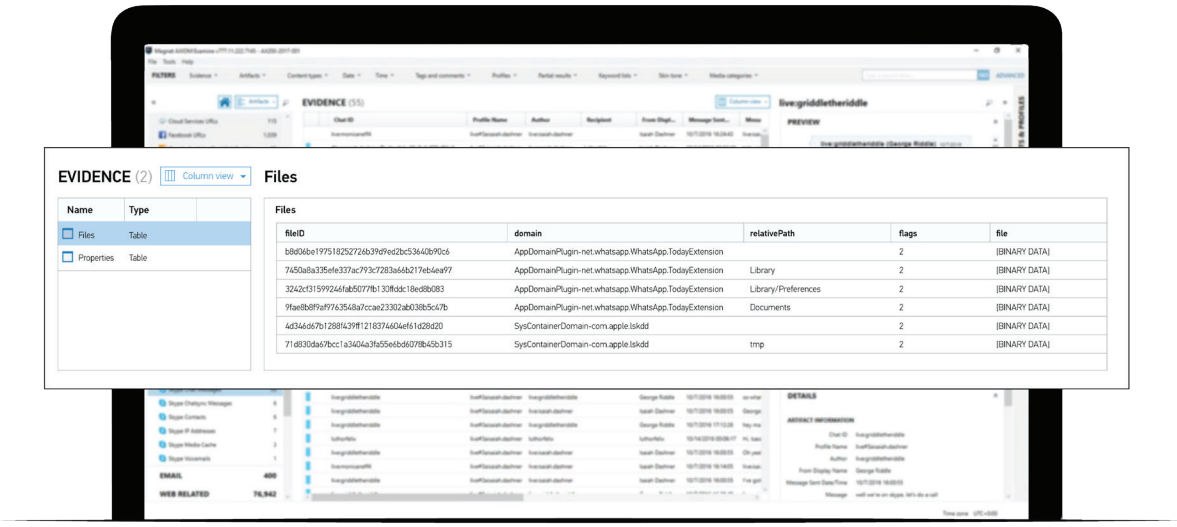

Figure 2: The Files Table found in manifest.db

The Data in Files column, meanwhile, is a binary-formatted .plist that stores metadata including the userID, file path, last modified time, protection class, and public encryption key.

In iOS 10, not only did a DB file replace the MBDB; .plist files also changed, and a new folder structure was introduced. You can map file paths using the Files Table found in manifest.db. (Figure 2) Filter on the fileID—the file's SHA-1 hash value—and the domain to get to the relativePath from which the file can be accessed, for example, Library/SMS/sms.db.

Do Not Disturb While Driving Data

One of iOS 11's most talked-about features is Do Not Disturb While Driving. This can be valuable not only in collision reconstruction investigations, but in any case where a subject claims they were or were not driving at the time of a given event.

With this feature, you may find evidence in .plists associated with Do Not Disturb While Driving, new tables within old databases, or even the new vision framework for object detection.

Users can activate the feature with one of three options: automatically, when the device senses you are in a vehicle; when connected to the vehicle's Bluetooth; or manually. Auto-reply settings include four options: send to all contacts, recent contacts, favorites, or no one.

The Do Not Disturb While Driving .plist contains a number of entries of interest, including[15]:

- CARDNDAutoReplyAudience — Which user group receives an auto-response.
- CARDNDAutoReplyMessage — The message sent by the system, which can be user-customized.
- CARDNDAutomaticTriggeringMethod — Whether the features activate automatically, manually, or when connected to Bluetooth.
- CARDNDTriggerPreferenceChangedTimestamp — The date / time and the "Triggering Method" set (CARDNDUserHasAdjustedTriggerMethod shows whether the user has ever changed the setting from default.)
- CARDNDMiniRecentRideHistory — The last five times the feature was activated. (Note: this may or may not mean the user was driving. If the user set the feature to activate automatically but was simply riding in a vehicle, Do Not Disturb may have self-activated.)

You may find evidence in .plists associated with Do Not Disturb While Driving, new tables within old databases, or even the new vision framework for object detection.

How iOS 11 Artifact Changes Can Affect Parsing

Security wasn't the only thing that changed in iOS 11. Artifacts including iMessages, Safari, and multimedia files changed too, and with them, some forensic processes.

iMessages with Both Nanosecond and Millisecond Timestamps

iMessages and SMS are one of the more challenging aspects of iOS 11. Both are still stored in the sms.db file, and multiple tables in sms.db are required to parse and join the messages correctly. However, there are two significant differences:

- Additional tables appear to be used.
- The timestamp is—sometimes—different as a result of iOS 11 iMessages' new nanosecond timestamp format[16].

While there is still a January 1, 2001 epoch date, the Mac Absolute value length varies between two formats, which can be stored simultaneously in the same column. Additionally, the tables in sms.db store the timestamp differently[17].

iCloud iMessages are separate from backups, making iCloud acquisition even more important.

Another change to iMessages came as of the iOS 11.3 beta 1, which stored iMessages in iCloud—a feature that went live in 11.4. To turn on Messages in iCloud, users have to find the feature under the iCloud settings page. From a forensic standpoint, this change resulted in new tables and columns related to cloudkit for iCloud Messages, including Attachment download state.

As of the 11.4 public beta, iMessage sync was changed from device-to-device sync to true cloud sync. As a result, when data is removed from one source, it's automatically cleared from other devices. This does allow more seamless transfer of messages between devices, so logging into an iMessage account allows the user to pull down all messages.

Again, from a forensic standpoint, not all messages will stay cached on the device if this option is enabled. Nor will all messages be cached to iCloud Backups. iCloud iMessages are separate from backups, making iCloud acquisition even more important.

Safari History

Substantial changes happened with Safari in iOS 11. Regardless of how much browser data is stored in iCloud, the history.db file on the device only displays 30 days' worth of URL and visit data, with no way to change this setting. With repeat visits to URLs, records may be kept longer than 30 days, and unique URLs are deleted. Research shows, however, that because the database doesn't autovacuum, AXIOM can carve the Safari database to recover browser history dating back to the previous year.

Acquiring Pictures and Videos with MTP Transfer

In iOS 11, Apple makes use of the High Efficiency Image File Format (HEIF) standard[18]. During a forensic examination that requires pictures and video, look for files stored with high efficiency image codec (HEIC) and high-efficiency video codec (HEVC) extensions. The user can select these formats, which act as "container" files, to keep high-resolution iPhone and iPad photos and videos from consuming available storage[19]. They're only encoded by Apple devices with the A10 chipset or later, i.e. iPhone 7 and newer.

Other potential artifacts for review: In iOS and MacOS devices, a "backwards compatibility mode" sends HEIC to JPG image format. Live Photos' HEIC have a matching MOV file with them (by filename). The .MOV file can contain audio if sound wasn't muted at the time it was recorded.

The user can change an .MOV file's display thumbnail by selecting one of the frames from the file. This frame is considered a mutation. It's stored as 'FullSizeRender.jpg'. If the user doesn't support Live Photos, the device will default down to sending the thumbnail.

Once the thumbnail is edited or the Live Photo has mutation applied, the .MOV also gets a 'FullSizeRender.mov' variant. The 5005.Jpg in the Thumbnails folder reflects the currently set display image.

Photo locations include:

> /private/var/mobile/Media/DCIM/100APPLE/
> /private/var/mobile/Media/PhotoData/Mutations/DCIM/100APPLE/[IMG NAME]/Adjustments/
> (includes the Adjustments.plist as well as FullSizeRender.jpg and/or FullSizeRender.mov)
> /private/var/mobile/Media/Thumbnails/V2/DCIM/100APPLE/[IMG NAME]
> (includes 5005.jpg, even if the image is HEIC)

iOS has evolved considerably in the space of just a year. The changes to the way users can protect, access, and store data have carried profound implications for forensics examinations—but so have new, disruptive entrants to the marketplace such as Grayshift.

In some respects, these changes have improved your job through the ability to reset backup passwords and rely on biometric authentication to obtain data. In other respects, as forensic research indicates, you may have to take some extra time to validate where and how evidence is stored and presented.

Effective iOS Forensics with Magnet AXIOM

Magnet AXIOM is comprehensive digital forensics software that can ingest and analyze data from a variety of smartphones and operating systems, including Apple iOS devices. Its capabilities include:

- A built-from-the-ground-up .plist viewer that allows you to navigate through NSKeyedArchiver Plists[20] more easily using hotlinks.
- Easily ingest images and/or memory from tools such as GrayKey and other third-party processes.
- Use Dynamic App Finder to recover additional artifacts from fragmented files and databases that are not sequential, out of order, or missing from file system and memory acquisitions of iOS devices.
- Aggregate data from multiple devices and iCloud into one case file to create a fully interactive, exportable timeline with all known data.
- Trace app and file artifact evidence back to its source location with one click to quickly verify the evidence's existence in the source data.
- Retrieve multiple artifacts from apps that go beyond just chat. Layer in filters for geotag information, dates and times, browsing history, and more.
- Access and analyze digital evidence data from the artifacts database, the file system or the registry.
- Leverage more than eight evidence views including World Map, Histogram, Timeline, Chat Thread, and more to tell the evidentiary story.
- Identify possible child luring intent in chat messages, child abuse images, and other potentially illicit content with Magnet.AI.
- Import and export pictures between AXIOM and Project VIC and CAID to process them against known hash sets; and between AXIOM and Griffeye or Semantics21 solutions to integrate uncategorized-to-categorized data back into AXIOM.
- Use Connections in AXIOM to quickly connect artifacts and files to show relationships: Where was the artifact found? How did it get on the system? How was it shared? Was there intent?
- Share all found or a targeted subset of evidence in a Portable Case to stakeholders at all technical skill levels – whether they have a license or not. Merge their comments and tags back in quickly and easily for the best collaboration.

Notes

[1] McQuaid, Jamie, "Loading GrayKey Images into Magnet AXIOM," Magnet Forensics blog, https://www.magnetforensics.com/blog/loading-graykey-images-into-magnet-axiom/, June 18, 2018, accessed June 29, 2018

[2] Mahalik, Heather, "Open Source Mobile Device Forensics" presentation, https://www.nist.gov/sites/default/files/documents/forensics/6-Mahalik_OSMF.pdf, 2014, accessed June 28, 2018

[3] Passware, "New in Passware Kit 2017 v5," https://blog.passware.com/2017/12/14/new-in-passware-kit-2017-v5/ December 14, 2017, accessed June 19, 2018

[4] Apple, "About encrypted backups in iTunes" support page, https://support.apple.com/en-us/HT205220 accessed June 27, 2018

[5] Murphy, Cindy, "Forensic Case Files – A New Solution for Previously Encrypted iOS Backups," Gillware blog, https://www.gillware.com/forensics/blog/digital-forensics-case-study/new-solution-encrypted-backups/ November 6, 2017, accessed May 24, 2018

[6] Afonin, Oleg, "iOS 11.4 to Disable USB Port After 7 Days: What It Means for Mobile Forensics," ElcomSoft blog, https://blog.elcomsoft.com/2018/05/ios-11-4-to-disable-usb-port-after-7-days-what-it-means-for-mobile-forensics/ May 8, 2018 accessed June 27, 2018

[7] Afonin, Oleg, "This $39 Device Can Defeat iOS USB Restricted Mode," ElcomSoft blog, https://blog.elcomsoft.com/2018/07/this-9-device-can-defeat-ios-usb-restricted-mode/, July 9, 2018 accessed July 10, 2018

[8] Vance, Chris (@cScottVance), "Overnight test results are in. Lightning OTG dongle kept USB Restricted Mode from enabling. More tests of more adapters coming this week. Note: this did NOT keep SOS Mode enabling of USB Restricted from working. If SOS is triggered, it will still enable USB Restricted." Twitter, July 10 2018, 8:00a.m. https://twitter.com/cScottVance/status/1016653330406432768

[9] Afonin, Oleg, "New Security Measures in iOS 11 and Their Forensic Implications," ElcomSoft blog, https://blog.elcomsoft.com/2017/09/new-security-measures-in-ios-11-and-their-forensic-implications/, September 7, 2017, accessed May 24, 2018

[10] Hyde, Jessica, "How to Acquire an iOS 11 Device without the PIN/Passcode," Magnet Forensics blog, https://www.magnetforensics.com/blog/how-to-acquire-an-ios-11-device-without-the-pinpasscode/ October 6, 2017, accessed May 24, 2018

[11] This does require the iTunes account email and password, but oftentimes this can be recovered from other devices as users often reuse accounts IDs and passwords. The Gmail account and password recovered from the computer may therefore be the same credentials necessary to recover data from the cloud.

[12] Data Recovery for iPhone, "All about iTunes backup details information," http://www.datarecoveryforiphone.com/resource/all-about-itunes-backup-details-information.html November 16, 2015, accessed May 24, 2018

[13] Proffitt, Tim, "Forensic Analysis on iOS Devices," SANS Institute Infosec Reading Room, https://www.sans.org/reading-room/whitepapers/forensics/forensic-analysis-ios-devices-34092 November 5, 2012, accessed May 24, 2018

[14] Murphy, ibid.

[15] BlackBag Training Team, "iOS 11-Do Not Disturb While Driving Analysis," BlackBag blog, https://www.blackbagtech.com/blog/2017/10/17/ios11-do-not-disturb-while-driving-analysis/ October 16, 2017, accessed May 24, 2018

[16] Mahalik, Heather, "Time Is Not on Our Side When it Comes to Messages in iOS 11," Smarter Forensics blog, https://smarterforensics.com/2017/09/time-is-not-on-our-side-when-it-comes-to-messages-in-ios-11/ September 30, 2017, accessed May 24, 2018

[17] At first, this broke forensic tools, which couldn't parse the difference between the two. AXIOM 1.2.1 solved the problem in October 2017 by adding support for iOS 11. See our blog: "Magnet AXIOM 1.2.1 Supports iOS 11 and Brings Other Enhancements," https://www.magnetforensics.com/blog/magnet-axiom-1-2-1-supports-ios11-brings-enhancements/ accessed June 25, 2018

[18] Evans, Jonny, "Apple's HEIF image format choice reinvents photography," ComputerWorld.com, https://www.computerworld.com/article/3207768/apple-mac/apple-s-heif-image-format-choice-reinvents-photography.html, July 13 2017, accessed June 27, 2018

[19] Zibreg, Christian, "How and when to choose between HEIF/HEVC & JPEG/H.264 media formats in iOS 11," iDownloadBlog.com, http://www.idownloadblog.com/2017/09/23/how-to-ios-11-heir-havc/ September 23, 2017, accessed May 24, 2018

[20] Edwards, Sarah, "Manual Analysis of 'NSKeyedArchiver' Formatted Plist Files - A Review of the NEW OS X 10.11 'Recent Items'," Mac4n6 blog, https://www.mac4n6.com/blog/2016/1/1/manual-analysis-of-nskeyedarchiver-formatted-plist-files-a-review-of-the-new-os-x-1011-recent-items, January 21, 2016, accessed June 27, 2018

If you'd like to learn more about Magnet AXIOM and how it can help extract and discover decrypted and obfuscated evidence you may be missing with other solutions, visit magnetforensics.com/magnet-axiom.

While you're there, you can learn more about the product, request an in-depth personal demo from an AXIOM expert, and request a free 30-day trial version. Additionally, visit magnetforensics.com/digital-forensics-training/courses/advanced-mobile-forensics/ to learn more about our four-day Magnet AXIOM Advanced Mobile Forensics (AX300) training course.

Learn more at magnetforensics.com

For more information call us at 1-844-638-7884
or email sales@magnetforensics.com