Collecting Data from Encrypted Phones

Originalartikel

Backup

<html> <img src=„https://media.labcompare.com/m/53/article/573193.jpg“ alt=„Collecting Data from Encrypted Phones“ width=„400“ height=„300“ itemprop=„image“ referrerpolicy=„no-referrer“ /><p><em>Welcome to&#160;</em>Forensic's<em>&#160;monthly column, Digital Intelligence in the 21st Century. This column is authored by Heather Mahalik, Senior Director of Digital Intelligence at Cellebrite. With over 18 years of experience in digital forensics, Mahalik has been an expert of choice for many law enforcement and intelligence agencies. She has worked high profile cases from child exploitation to Osama Bin Laden&#8217;s digital media. Check back the second friday of every month for more digital intelligence as Mahalik takes on managing and sharing data, testing and validation, highly encrypted phones and more.</em></p><p><em>*co-authored by Paul Lorentz, Senior Solutions Engineer, Cellebrite</em></p><p>The rise of file-based encryption on popular mobile devices like those from Google and Samsung is creating new challenges for forensic examiners. The old-school methods of gaining access to device data, like removing a chip from a circuit board, don&#8217;t do examiners any good when file encryption is the norm. However, all is not lost.</p><p>When lawful or consent-based access has been secured, if you&#8217;re confronted with devices using file-based encryption and you really need that data, there are workflows that allow your encrypted-device experts to take their best swing accessing the device. Advanced technology is also available to help examiners extract Digital Intelligence (DI) from devices. (Digital Intelligence is the data that is collected and preserved from digital sources and data types&#8212;smartphones, computers, and the Cloud&#8212;and the process by which agencies access, manage, and leverage data to more efficiently run their operations.)</p><p>Constant learning is also needed in order to gain access to data on encrypted devices. Encryption technology is changing rapidly, which means forensic examiners should never stop learning. They must stay current and continue to study up on the best approaches for each device, operating system, and encryption type. Fortunately, there is a good deal of knowledge-sharing going on in the law enforcement and digital forensics communities, with experts sharing tutorials on new encryption methods and their successes in obtaining data from these devices when lawful or consent-based access is secured.</p><p>In this column, we&#8217;ll offer some do&#8217;s and don&#8217;ts for working with encrypted devices, including advice on creating workflows and avoiding missteps due to inexperience.</p><h4><strong>Do&#8217;s and Don&#8217;ts for Working with Encrypted Devices</strong></h4><p><strong>Do document, document, document</strong></p><p>Always document what you see. Is there a lock screen on the device? Are there text or app messages visible? Note the time/date that is set on the device. Log these attributes, as they can help forensic examiners determine their approach to obtaining data from the device.</p><p><strong>Don&#8217;t manually examine the device if you are worried about making accidental/permanent changes</strong></p><p>In some jurisdictions, it is permissible to do a cursory examination of a phone upon arrest. However, tread very, very carefully here. One should ensure they have lawful access to the device prior to accessing any data. As mentioned previously, document everything you do and everything you see. This is an important lesson to pass along to tech savvy frontline responders. Even the most trained professionals can click a message marking it &#8220;read,&#8221; when really it was &#8220;unread.&#8221; It&#8217;s possible that actions done with the best intentions, like changing settings, could prevent a knowledgeable forensic examiner from gaining access to data on an encrypted device. If someone messes up a workflow as soon as the examiner has access to a device, the investigative team could miss out on obtaining crucial evidence. Bottom line: If responders are not specifically trained to manually examine device,

they <em>should not</em> do it.</p><p><em><strong>Do isolate devices from network access</strong></em></p><p>Again, a frontline responder should only access a device&#8217;s network and Wi-Fi settings if they&#8217;re familiar with that particular device and have lawful access or consent to do so. If the responders don&#8217;t have knowledge on handling mobile devices, they can place the devices in Faraday or anti-transmission bags until an expert can look over the device. Remember, if you are isolating a device that is live, connect it to a battery pack inside the Faraday bag.</p><p>If SIM Card removal needs to take place, you don&#8217;t need special tools or hardware, a simple paperclip can work. Make sure you secure that SIM card somewhere safe, so it doesn&#8217;t get lost. Also, make sure you understand that removing a SIM card from some devices may lock the device and make it harder to access during forensic extraction. Again, knowledge is key.</p><p><strong>Do keep devices powered up</strong></p><p>If possible, keep the device powered on because some of the strongest encryption today might block any data being extracted if a device is powered off.</p><p><strong>Don&#8217;t try to guess passwords</strong></p><p>Some devices will lock out users or even trigger a phone wipe after a certain number of password entry-attempts. What&#8217;s more, the person entering the guessed passwords doesn&#8217;t know how many failed attempts there have been, or how many are left.</p><p><strong>Do create standard operating procedures and workflows to ensure chain of custody</strong></p><p>Chain of custody is important as it ensures the devices are properly handled and only when legally authorized or during a consent-based situation. Standard operation procedures (SOPs) need to be in place to ensure your organization has a reason for your actions:</p><ul><li>How do you respond to devices at a scene?</li><li>Do you acquire on site or back in a lab?</li><li>How do you document what you find?</li><li>How do you handle locked or unlocked devices?</li><li>How do your store the data to ensure nothing is changed inadvertently?</li></ul><p>Ask trusted local agencies, such as associations of chiefs of police, for best practices and procedures for managing digital evidence.</p><p><strong>Do consider whether the encrypted device even needs to go to the lab</strong></p><p>Not every device needs to be added to the workflow of forensic examiners who are generally overloaded. If a device owner gives consent to allow specific pieces of evidence to be extracted from a device&#8212;like photos or text messages&#8212;then frontline responders can use relevant technology right at the scene. This way, unnecessary devices aren&#8217;t piling up in labs, and owners can get their devices back faster.</p><h4><strong>Learning never stops</strong></h4><p>It&#8217;s not easy for frontline responders and forensic examiners to keep up with the devices, operating systems, and encryption technologies on the market&#8212;but keep up they must. It&#8217;s not just the new devices: It&#8217;s also legacy devices that can turn up with a wide variety of OS upgrades, all of which might need to be managed in different ways.</p><p>Every change in OS or device type can change an examiner&#8217;s methodology and workflow. The state of the device when it becomes a part of a crime scene makes a difference. Is it powered on? Powered off? Will you face encryption challenges? That&#8217;s why knowing what&#8217;s in front of you is key before making a move to obtain data from an encrypted device.</p><h4><strong>Resources</strong></h4><p>Josh Hickman (@josh_hickman1) is a digital forensic practitioner whose <a href=„https://thebinaryhick.blog/“>blog</a> (<em>The Binary Hick</em>) is an excellent source of DFIR information. A recent <a href=„https://www.cellebrite.com/en/series/dfir-discord-channel-andrew-rathbun-senior-associate-at-kroll/“>podcast</a> from Cellebrite with special guest, Andrew Rathbun, Senior Associate at Kroll, also contains a wealth of information that those in the DFIR community will find useful.</p><p><a href=„https://www.forensicmag.com/3361-Home/#ctl05_ctl01_divContainer“ title=„Read More News“ class=„link-news“><strong>Read More News</strong></a></p> </html>

From:
https://schnipsl.qgelm.de/ - **Qgelm**

Permanent link:
https://schnipsl.qgelm.de/doku.php?id=wallabag:wb2collecting-data-from-encrypted-phones

Last update: **2025/06/27 11:17**