If You Need Mobile Device Forensics

The New England State Police Information Network (NESPIN) Can Help!

By: Chief Jim Hurley (Retired)

 NESPIN - Law Enforcement Coordinator

In Consultation With:

 Michael Breton – NESPIN Mobile Forensic Unit

 Internet/Intranet Specialist

Mobile device technology continues to change rapidly and so must the law enforcement response to collecting forensic evidence from these mobile devices. Today’s law enforcement officers are seizing mobile devices, such as smartphones, tablets, GPS devices, dash cameras, digital cameras, memory cards, and drones far more frequently than ever before. A cell phone or other mobile device found at a crime scene can be one of, if not, the most important piece of evidence an investigator finds. All of the aforementioned devices have the potential to hold evidence of criminal activity; however, officers know that seizing these devices is the easy part of the investigation. [[1]](#endnote-1) Accessing the potential evidence on the seized device proves to be the more difficult task. Officers are challenged to secure the appropriate authorization to search the phone (i.e. court order or consent) while scheduling a forensic examination of the device at the same time. Officers frequently must overcome additional hurdles/delays, including, but not limited to:

1. Frequently changing operating system platforms;
2. Constantly emerging new mobile devices;
3. Experiencing waiting periods/back logs in getting mobile devices examined;
4. The constantly growing volume of data stored on mobile devices that can be accessed by law enforcement;
5. Enhanced encryption that continually presents a challenge to law enforcement.

These delays can impact the time frame when a search warrant can be lawfully executed or give a suspect the opportunity to recant his/her “consent to search” the device that was earlier given to the police. So how can you avoid these potential pitfalls? …….call NESPIN’s Mobile Forensic Unit for assistance. The unit provides highly professional mobile forensic services in a timely manner.

“The NESPIN Forensic Lab is equipped with a Faraday Box to securely block wireless signals during extraction. Cellebrite Physical Analyzer [[2]](#endnote-2) and other tools are used to extract the most data in an organized and forensically sound manner. ” [[3]](#endnote-3) The Mobile Forensic Unit can work to potentially secure the following evidence from the devices listed below:

1. **GPS Devices (mobile)** – The evidence/data that can be retrieved from these devices depends on the quality of the device and its age, but generally the forensic examination seeks to locate:
* Historical list of locations.
* Stored multi-media.
* Address book.
* Past historical searches.

Investigators are reminded that GPS devices that are permanently mounted in the vehicle’s dash may also contain the same data. However at this point in time, NESPIN is not equipped to extract data from these in-dash devices.

1. **Dash Cameras** – While video is the primary function of a dash camera, the devices are more than just video. These devices may contain location data, vehicle speed, and the camera’s wide angle or multiple views can provide excellent views of the incident. Dash cameras with accident detection technology protect video automatically upon detecting that a vehicle has been involved in a collision. If you come across a dash camera at a crash scene you should secure the device and its memory card as potential evidence.
2. **Digital Cameras** – The NESPIN Mobile Forensic Unit works to recover stored images and video along with deleted images and data provided that there was room on the storage device to hold the deleted items. Deleted video is rarely recovered.
3. **Smartphones & Tablets -** Today’s investigators must be keenly aware that the list of data that can be recovered from a smartphone or tablet is expanding rapidly. NESPIN’s mobile forensic examiner continually trains to keep pace with the ever changing list of data that can be recovered, which may include the device’s calendar, chat logs, e-mails sent or received, browsing history, images, videos, and a whole lot more. For a full list of data that can be recovered, you can contact Mike Breton from the NESPIN Mobile Forensic Unit using the contact information at the end of this article. Investigators should be aware that data recovery is also impacted based on the model and operating system version of the device being submitted for examination. Devices that are password protected are difficult but not always impossible to access.
4. **Drones** – The drone industry has exploded and with it the number of crimes involving drones has also increased. Recently a drone flew over Fenway Park during a Red Sox game which is restricted air space. Officers seizing a drone should treat it as a mobile device. Drones can contain micro SD cards, which could store photos from the current drone flight or other previous flights. The drone’s memory may also contain multi-media content. When possible investigators should also recover the drone’s controller as it often works in conjunction with the user’s cellphone to display and store information. The user’s cellphone should also be seized.

Some of the benefits of using the NESPIN Mobile Computer Forensic Unit are:

* Frequently there are no back logs or delays and your case can be opened the same day that the device is received:
* Short turnaround times;
* Priority given for extenuating circumstances;
* If NESPIN’s Computer Forensic Unit’s cannot handle your request, they will refer you to an entity that can handle it.

But perhaps the best kept secret of using the NESPIN Mobile Computer Forensic Unit is that when you pick up the mobile device and the information that has been extracted from it, you are only a few steps away from the NESPIN Analytical Unit. You can literally walk across the hallway and have the Analytical Unit review the data you just received. “The staff is available to work with the investigator in developing crime specific analytical products focusing on innovative data analysis and presentation format.” [[4]](#endnote-4) I can state from personal experience that the link charts and analytical charts that this unit generated for my investigations over the years were highly professional and their use was very beneficial in the courtroom during trial.

As with any type of outside assistance, the question of cost always arises. There is no cost for utilizing NESPIN’s Mobile Forensic Unit. It is part of the services you receive as a member of the New England State Police Information Network (NESPIN).

For more information on the NESPIN Mobile Computer Forensic Unit e-mail the unit at MBreton@nespin.riss.net or call 508-528-8200 x229.

References/Endnotes

1. Mobile Forensics Must Keep Up With the Times by Joel Bollo; published 6/7/17 Digital Inside / Forensic Magazine found at [www.forensicmag.com/article/2017/06/mobile-forensics-must-keep-times](http://www.forensicmag.com/article/2017/06/mobile-forensics-must-keep-times) [↑](#endnote-ref-1)
2. Cellebrite ® for more information go to <https://www.cellebrite.com> [↑](#endnote-ref-2)
3. NESPIN Website – Mobile Forensic’s - <https://nespin.riss.net/?page_id=25143> [↑](#endnote-ref-3)
4. NESPIN Webist – Analytical Services - <https://nespin.riss.net/?page_id=1724> [↑](#endnote-ref-4)