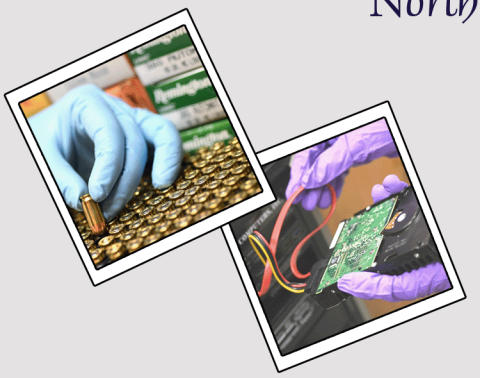
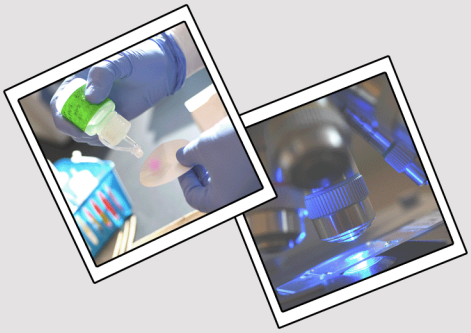
North Carolina State Crime Laboratory

Forensic Update





Volume 4, No. 2

December 22, 2020

Dear Criminal Justice Stakeholders,

In recent months, the Crime Laboratory's Digital Evidence section has received several phone calls inquiring about digital evidence submissions and the Laboratory's examination capabilities. This issue will focus on our Laboratory's current capabilities, as well as highlight frequently asked questions pertaining to audio/video and digital examinations, Laboratory policies and procedures, and proper evidence handling.

Below is a list of services currently provided by the Digital Evidence Section. The Laboratory strives to ensure its scientists are current with forensic tools, emerging trends (software and hardware), processes and techniques, training, and stakeholder updates.

As always, please contact us with any questions.

Very Respectfully,

Vanessa Martinucci

Vanessa Martinucci
Director, North Carolina State Crime Laboratory
vmartinucci@ncdoj.gov
(919) 582-8723

"Truth through science."

NCSCL DIGITAL EVIDENCE SECTION

To contact the Digital Evidence Section (**Raleigh location only**):

Digital Evidence Section - 984-204-2547
Raleigh location main line - 919-582-8700
Evidence Control Section (Raleigh, NC) - 919-582-8840

Forensic Services Provided:

1. Computer Forensics (USBs, memory cards, external hard drives)
2. Mobile Device Examination
3. Tasers
4. Vehicle Forensics
5. Audio Analysis and Video Analysis

Submission Guidelines

It is laboratory policy that only five items be submitted at a time for any single case. **Exception: 10 items may be submitted for a homicide/death case.** Any deviation to this (more than five items for non-death cases and more than 10 items for death cases) must have preapproval from the Forensic Science Manager or discipline specific Technical Leader. Additional submissions may be accepted at a later date.

Search Authority

The Digital Evidence section does require some type of search authority be submitted with the evidence. Four types of search authority that will be accepted:

1. Court order
2. Search warrant
3. Consent and/or
4. Letter stating that the device owner is deceased and does not have an expectation of privacy. (The expectation of privacy letter may be used in-lieu of a consent form.)

When reviewing a search warrant, the digital forensic scientist MUST be able to link the submitted search warrant to the submitted device. The search warrant should include *unique identifiers* to that device; however, it has been noticed that some newer mobile devices do not have any unique identifiers on the outside casing. In these circumstances, statements such as “Device belonging to Person A,” “Red iPhone in a purple case,” and “Damage noted to the touchscreen in the top right corner” are acceptable when used in conjunction with each other.

Failing to have the proper information, may result in the evidence submission being denied or the scientist calling to obtain a new search warrant. In either case, the submitted evidence will not be processed until the discrepancy has been corrected.

Mobile Device Extraction

The Laboratory has several proprietary tools to attempt security bypass and data extraction. We have success in using these techniques; however, if a passcode is not provided or the phone has been powered down, it can take an extensive amount of time to access the device, anywhere between six hours and 27 years. Due to this, any mobile device security bypass will process *for nine months*. After nine months, the device and bypass process will be re-evaluated by the scientist, and a determination will be made to continue or stop the process.

Included is a quick-reference chart for the proper handling of mobile devices (cellphones). **This chart should be disseminated to any individual that may seize a mobile device.** In general, if the device is powered on, DO NOT turn it off. If the device is unlocked, make every attempt to prevent it from locking. Do not allow the device’s battery to drain.

Due to time sensitivity, no appointment is necessary to submit a mobile device that is powered on and/or unlocked, but the device MUST be submitted at the Raleigh Laboratory location (121 E Tryon Rd., Raleigh, NC, 27603). **Call 984-204-2547 for the Digital Evidence Section or the laboratory main line, 919-582-8700.** You will be required to call ahead and give proper notice. If the device is in a powered on or in an unlocked state, the scientist will immediately take custody of the device and begin examination. Please be aware that a search authority is still required.

Disclaimer: Due to the many different model types and operating system updates, not all devices are supported. If the model and operating system is not supported, the submitting agency may resubmit the device when support becomes available or the passcode has been obtained.

Audio/Video Analysis

Many agencies are unaware of the laboratory's audio/video analysis capabilities. The Laboratory provides audio/video analysis on the following items:

1. Digital Video Recorders (security footage)
2. Vehicle dash cameras
3. Body-worn cameras
4. Recorded audio (surveillance, interview recordings, phone calls, and video that may contain audio)

Depending on several factors, audio/video enhancement (audio clarification and video/image enhancement) is available.

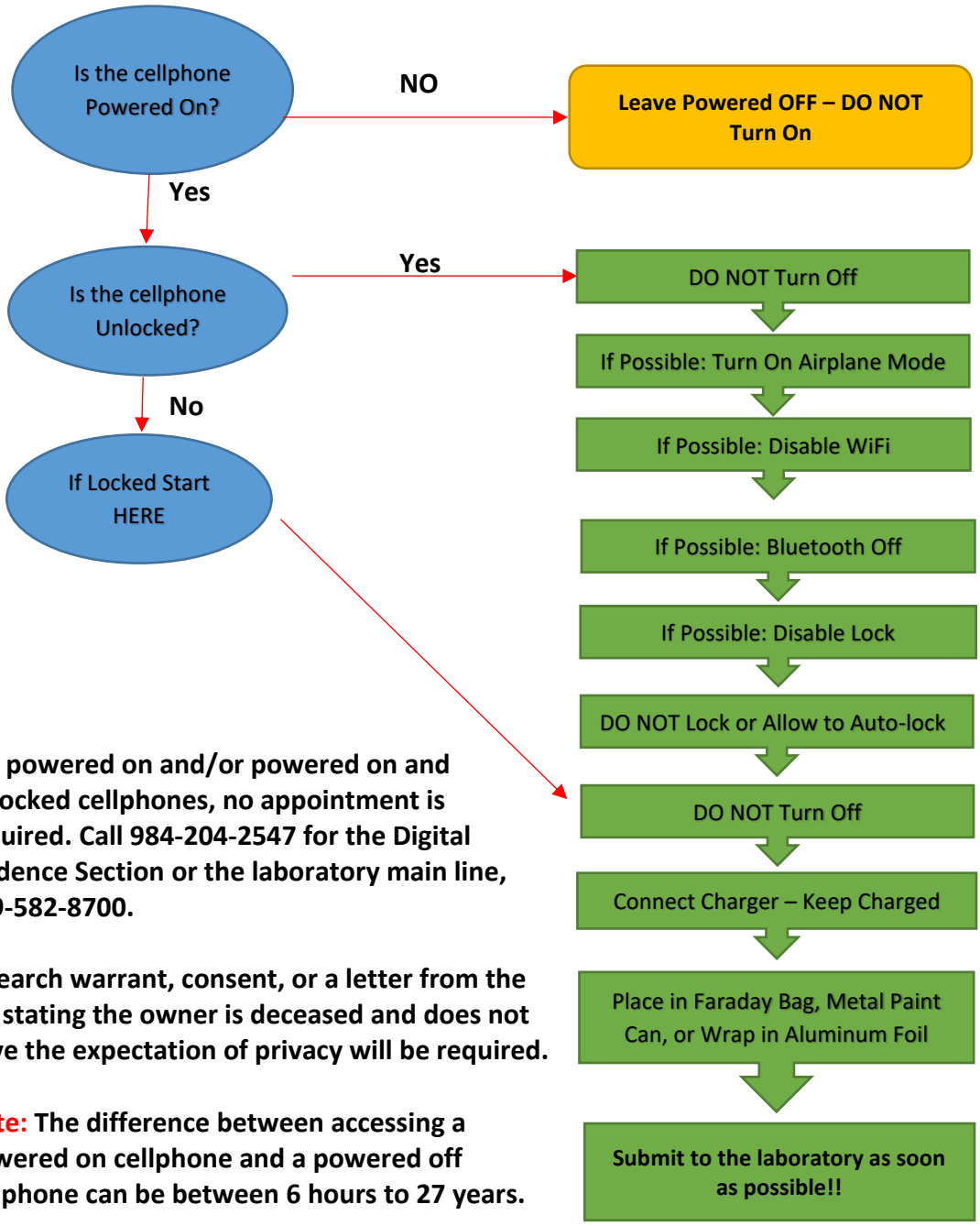
Vehicle Forensic Analysis

The Digital Evidence section now offers vehicle forensic analysis. Every vehicle is different in the type of data it stores, and many vehicles do not store data. If this is a service that you would like to explore, please call and speak to a digital forensic scientist. Please have the following information available, as it is necessary in determining if a vehicle is supported: Year, Make, Model, Trim, VIN, and a picture of the center stack (infotainment center). When speaking with the forensic scientist, he/she will discuss possible options for extracting any data.

Tasers

Tasers should be submitted as soon as it is seized, as it is a time sensitive process. Do not remove the battery. Tasers rely on its battery to retain data. **Tasers will immediately be taken and processed**.

Proper Mobile Device (All Cellphones) Handling



For powered on and/or powered on and unlocked cellphones, no appointment is required. Call 984-204-2547 for the Digital Evidence Section or the laboratory main line, 919-582-8700.

A search warrant, consent, or a letter from the DA stating the owner is deceased and does not have the expectation of privacy will be required.

Note: The difference between accessing a powered on cellphone and a powered off cellphone can be between 6 hours to 27 years.