INDIANA STATE POLICE LABORATORY DIVISION

PHYSICAL EVIDENCE BULLETIN

DIGITIAL FORENSIC EVIDENCE

INTRODUCTION: This Indiana State Police (ISP) Laboratory Division Physical Evidence Bulletin (PEB) provides steps regarding the preservation of digital evidence, packaging digital devices and submission guidelines. If you have any questions regarding this bulletin, or if an analysis can be performed, contact an ISP Digital Forensics Examiner (DFE) or Regional Laboratory.

A. DEFINITIONS

1. Digital Evidence

Digital evidence is information of probative value that is stored or transmitted in binary form (where each bit of data stored as a one or a zero) that may constitute a variety data and file types. Digital evidence can be found in a variety of digital devices, and could be relevant in any kind of criminal activity as well as probative in court.

2. Digital Device

A physical unit of equipment capable of generating, storing, processing, and/or transmitting digital data (information in binary form). The range of devices is vast and may range from mobile devices to computers – with some devices having characteristics of both.

3. Mobile Device

A portable device that includes cellular phones and tablets.

4. Computer

Any digital device designed to be more stationary, that may contain digital evidence. Computer systems utilize more complex and robust operating systems not generally designed for mobile use over wireless networks.

5. Other Devices

This may include digital cameras; portable storage devices and memory cards; optical discs such as CD, DVD, or Blu-ray discs; Digital Video Recorders (DVR's); internal and external hard drives; other types of disks; gaming consoles; Global Positioning Systems (GPS) devices; vehicle infotainment systems; drones; Internet of Things (IoT) devices; copiers; credit card skimmers; access

control devices; surveillance systems; portable digital music players such as iPods and MP3 players; smartwatches; networking equipment; servers; and any similar devices that exists or may exist as technology develops.

B. GENERAL SUBMISSION FOR EXAMINATION:

Only those items which are being used to file charges and for prosecution shall be submitted for analysis. The Request for Laboratory Examination Form shall be completed as thoroughly as possible and include the names of suspects, type of investigation, associated case numbers, and applicable cause numbers.

No items will be examined without legal authority (e.g., Search Warrant, Consent, Abandoned Property). Legal authority must include appropriate language that specifically allows for forensic examination of the digital evidence submitted and not just for the seizure of that item.

Search Warrants must be executed and open for the duration of the examination. They should contain language that states a digital examination can take months to complete because of the amount of data to be analyzed and the possibility of encryption.

The investigating officer is responsible for any search warrant returns to the court and not the responsibility of the DFE.

1. Case Prioritization

There are several factors that are considered when prioritizing case work. These factors may include the type of investigation and whether or not there are potential victims that could be identified as a result of the examination, pending court dates, the original submission date, and whether or not the devices are supported for data extraction. The DFE has the discretion to accept or reject items for suitability for examination.

2. Rush Case Requests

Requests for expedited examination should be infrequent. At least 30-days' notice must be given for such a request. Expedited examination requests are approved by the Digital Forensic Unit (DFU) Supervisor. Considerations and limitations of expedited examination requests include the nature of the investigation, number of digital devices needing examined, current DFU capabilities, and any statutory requirements. When multiple types of forensic examinations are requested for rush analysis, the customer shall also prioritize the order of the forensic examination to be performed.

3. Re-Examination

The ISP Laboratory Division DFU does not routinely examine digital devices which have been previously examined. Re-examination requests shall be made in writing to a DFU Supervisor by the submitting agency with an endorsement by the prosecuting attorney having jurisdiction in the case. Due to the complexity of re-examination cases, these requests are not available on a rush basis.

C. DIGITAL DEVICE COLLECTION AND PRESERVATION

This document contains general guidelines for collection and preservation of digital evidence; the approach should be determined based on the circumstances of each case.

1. Preparation

Crime scenes in general shall be routinely evaluated for presence of digital devices.

Ensure that there is legal authority for the anticipated seizure. Generally, law enforcement is prohibited from accessing and viewing information stored on a digital device without a warrant or consent. Consult with ISP DFU, when practical, to ensure the legal authority is appropriate for the anticipated seizure and that all necessary equipment is taken to the scene.

2. Procedure

Personal protective equipment should be properly worn when considering the possibility of latent print and/or DNA evidence. If fingerprint or DNA evidence is requested from a digital device, please collect prior to submission to the ISP DFU. See Laboratory Division PEB-10 Latent Prints or PEB-17 DNA.

3. Documentation

a. Inform the DFE of any interaction or manipulations with the device. (e.g., unlocking, placed in airplane mode) Do not scroll or browse through an evidentiary device, because doing so may alter the device.

b. Document the collection of devices in accordance with organizational guidelines and procedures. Documentation may include, but is not limited to, the following:

   1) A written description, sketches, notes, and/or photographs of the collection location and the condition of the digital evidence and other related evidence. This should be done prior to recovering and securing any evidence.

   2) Photographs of relevant digital devices and peripherals (e.g., cables, power connectors, removable media, and connected items) as a part of thorough scene documentation. Avoid touching or contaminating the devices when photographing them and the environment where found. If the device's display is in a viewable state, any changes should be photographed and documented until the screen is powered-off or in an unresponsive state.

   3) The state of the devices should be noted including whether or not a device is powered on or off, the presence of a passcode, as well as any existing physical damage.

   4) Non-electronic materials such as invoices, manuals, and packaging material may yield useful information about the capabilities of the device, its network, associated account, manufacturer, model, and unique identifiers including unlock codes.

5) The date and times of collection. The chain of custody documentation should be contemporaneous to the collection and include a description or unique identifier for the evidence, and the date and time of receipt and transfers. The record should fully identify each person (e.g., name, title, signature) taking possession of an item.

Note: Data can be received, and activities occur with digital evidence after the collection. Noting the date and time of receipt may assist in documenting what data may have changed after collection.

4. Packaging

All computer, tablets or mobile phone device evidence shall be submitted with a label attached or placed in an appropriately sized bag. USB flash drives, SD cards, and smaller digital evidence shall be placed in a sealed appropriately sized sealed bag. It is recommended that evidence is submitted in clear plastic bags unless moisture or liquids are a concern.

Evidence shall be labeled or packaged to bear the following information at a minimum:

a. Submitting agency name

b. Agency case number

c. Agency item number

D. MOBILE DEVICES

1. Storage of mobile devices submerged in liquids

a. If a mobile device is found submerged in water or other liquids, store the evidentiary device in the same liquid it was found in or isopropyl alcohol.

Note: If a battery is found in the device in question, remove the battery from the device, yet store in the same liquid it was found in or isopropyl alcohol.

b. Blood or caustic liquids may continue damaging metallic components and may need to be stored in a different liquid (i.e., water).

c. If any concerns or special circumstances arise, call a DFU examiner for further recommendations.

2. Preliminary considerations and handling

a. Observe whether the mobile device is powered “ON” or “OFF.”

b. If potential fingerprint, biological, or trace evidence may be present on the device in question, refer to the appropriate physical evidence bulletins for proper evidence handling and packaging. It may be appropriate to sub-sample a representative amount of biological/trace evidence to allow for proper preservation steps, like drying.

If the mobile device is ...	**Then ...**
“ON” or powered	• It is imperative that the device remains powered ON, even if this means connecting the device to a power source.

	• Make every attempt to preserve the data on the device by removing the device from the cellular network and disconnecting it from any known or unsecured WiFi networks. This can be accomplished by placing the device in an offline mode (commonly referred to as airplane mode) and removing the physical SIM (Subscriber Identity Module) card from the device. • If the device cannot be removed from the cellular network, store the device in some sort of shielded enclosure (e.g., faraday bag, aluminum paint can or wrap in aluminum foil) while connected to a portable power supply.
"OFF" or not powered	• If a mobile device is discovered powered off, then leave it powered off. If possible, remove the battery from a powered off device.

Note: If you place a powered "ON" cellular phone in a Faraday bag, aluminum paint can or wrap in aluminum foil WITHOUT power, the device should be examined as soon as possible because the battery will deplete during this period, and the device will turn off.

3. Collection of peripherals, SIM cards, memory cards, and passwords.

a. When seizing mobile devices, look for peripherals such as phone related software and manuals, cables, chargers, and search for SIM cards along with flash memory cards (e.g., microSD cards). Peripherals, flash memory cards, and SIM cards may be necessary to conduct a digital forensic examination.

b. Handwritten notes or papers containing potential pin codes or passwords may be near the digital devices being seized. Oftentimes, the passwords are not far from the device.

c. Ask subjects in question for passwords or PIN that may be needed for devices and Internet sites in question.

E. COMPUTER

1. Preliminary considerations and handling

a. If a computer is powered on is it is recommended that the computer not be powered down until after Random Access Memory (RAM) has been collected. This can be accomplished if a DFE is conducting an on scene triage. If a DFE is not available, then collect and submit for examination. RAM can store passwords and recent activity; RAM is volatile and will be lost as soon as it is powered off.

b. If it is determined that the computer does have password protection and/or encryption enabled, do not power down the system. Obtain the required password or passwords. If the required password or passwords are not available or inaccessible, on scene analysis should be conducted.

c. If the seizing officer is unsure if the operating system is encrypted, contact a DFE for guidance before powering off the computer.

2. **Powering off a computer**

   a. Once the decision has been made to power off a computer operating system, do so according to the guidelines listed below. If the operating system is not powered down correctly, data can be lost or the system can be damaged.

   b. To power a computer operating system off, disconnect the power cord from the back of the computer. If the computer has a removable battery, the battery should be removed as well. If the battery cannot be removed, hold the power button down until the computer turns off.

   c. If the computer is a network computer in a business operating system, do not unplug the computer; request assistance from DFU Examiner or an IT specialist who is familiar with the system.

3. **Collection of peripherals and accessories**

   a. When seizing computers, collect associated peripherals and accessories when possible. This includes power cords and/or chargers, and controls and/or controllers. Desktop computers do not need power cords collected as these are universal. iMac, All-In-One computers and laptops DO need their power cords collected.

   b. Document any attached removable devices/accessories (including their positioning in relation to the computer device under investigation); if it is decided that it is safe to detach them, they may be detached and analyzed independently.

   c. Collect accessories that may have interacted with the device under investigation and that may aid in accessing the device's content; contact an expert for guidance through the process, if necessary.

F. OTHER ELECTRONIC EVIDENCE

When seizing other electronic devices (digital cameras, SD cards, USB drives, external or bare hard drives, etc.) it shall be packaged as any other evidence.

If the device has a power cable or a cable to connect it to a computer, seize the cables with the device.

G. REPORTS

When a DFU examination is complete, a written report will be provided to the investigating officer. It will be in conjunction with the digital report that will be stored on a hard drive or disc, containing all corresponding data relevant to the examination.

It is the responsibility of the investigating officer to review the contents of these reports and corresponding data to determine if further consultation, explanation, analysis, or if further examination is warranted.

The digital report hard drive or disc is not the original evidence. However, the digital report hard drive or disc shall be securely maintained by the investigating officer until the adjudication of the case.

H. RELEASE OF EVIDENCE

Digital devices submitted for examination shall be retained by the Laboratory Division until the examination is completed. The devices, the corresponding digital report and associated hard drive or disc, if applicable, will be released to the investigating officer once the examination is completed.

I. EVIDENCE DESTRUCTION

The Laboratory Division is responsible for the security of all digital devices and destruction of only Indiana State Police cases in its possession. Evidence from outside agencies shall not be stored for destruction.

J. CONTACT INFORMATION

For further information contact the nearest ISP Regional Laboratory. The telephone numbers of the ISP Regional Laboratories are:

Evansville	812-867-3157	800-852-3970
Fort Wayne	260-436-7522	800-552-0976
Indianapolis	317-921-5300	866-855-2840
Lowell	219-696-1835	877-874-0009