Idaho State Police

Service Since 1939

Colonel Bill Gardiner
Director

Brad Little
Governor

To: Idaho Law Enforcement Agencies and Prosecutors

From: Matthew Gamette, ISP Forensic Services Laboratory System Director

Subject: ISPFS Digital Evidence

Date: February 7, 2025

Dear Colleagues:

This is notification of law enforcement implications of a recent change in leadership and management with the Idaho State Police Digital Forensics Unit.

On June 7th, 2021, Idaho State Police Forensic Services (ISPFS) started receiving and returning evidence for the ISP Cyber Crimes Unit (CCU). At that time, ISPFS started a transition plan for the CCU to be part of the forensic laboratory system. July 1, 2024, the ISP CCU became ISPFS Digital Forensics Unit (DFU), officially went under the leadership team of ISPFS, and all reports for cases received after July 1, 2024 will be issued in the ISPFS Prelog System. Effective February 7, 2025, ISPFS DFU has been through an accreditation gap assessment and will be assessed for accreditation in the next few months. We anticipate full accreditation in the discipline before July 2025.

The management and leadership of the DFU is now under ISPFS. All contact for case information, turnaround time questions, and case prioritization should be addressed to the ISPFS Meridian Laboratory Manager Rylene Nowlin. She can be reached at 208-884-7148 or rylene.nowlin@isp.idaho.gov Cases will be prioritized on a case-by-case basis for public safety, court, and other purposes.

Rush Testing: Rush status must be approved by the laboratory and can be given to cases for the following reasons in descending order of importance:

- Cell phones with security features that will destroy evidence, such as the iOS 18.0/18.0.1 reboot issue
- Exceptional public safety risk such as homicide, sexual assault, or other crimes against persons
- Safety risk to the survivor or family such as a specific death threat or physical violence threat
- Jury trial date or discovery deadline
- Exigency of the evidence to the investigation (generating investigative leads)

Urgent issues and submissions, such as the iOS 18.0/18.0.1 reboot issues, should be immediately addressed to Vinnie Montoya (208) 631-4397 or John Helton (208) 880-3064. If neither are available, contact Idaho State Police Regional Communications Center at RCC-South (208) 846-7550.

ISPFS requests that investigators provide essential information when submitting the evidence regarding the type of analysis needed on each device submitted for analysis. Specifics regarding what digital information from the device should be provided in the ISPFS Prelog System or emailed to the laboratory through the D3lab@isp.idaho.gov email address. All digital evidence must be prelogged in the ISPFS Prelog System and submitted to the Meridian ISPFS Lab. Cases will all be reported out through the same system (ISPFS reports all cases through the ISPFS Prelog System).

Any questions or concerns about the ISPFS Laboratory System, which now includes the Digital Forensics Unit, should be addressed to me at matthew.gamette@isp.idaho.gov or 208-884-7217

Packaging and Submission Instructions

Overview of Idaho State Police Forensic Services Digital Forensics Services

- ISPFS Digital Forensics Unit (DFU) Computer Forensic Examiners have been specially trained and certified in the forensic image and analysis of all digital evidence devices: Tower/Desktop/All-in-one Computers; Laptop Computers and associated tablet hybrids; digital video recorders (DVRs) for surveillance camera or home entertainment systems; game consoles with hard drive support (e.g. PS4); cellular devices (cell phones, tablets, SIM cards, etc.); memory modules of all varieties (bare hard drives (SCSI, PATA/IDE, SATA, SAS), "outdrives," external hard drives, and USB "Thumb" drives); "Flash" card media (SD, micro SD, xD, Compact Flash (CF), Smart Media (SM), Sony Memory Stick (MS); old "Legacy" pre-NTFS equipment/supporting memory media (floppy disk (3.5"), Iomega "Zip" Disk, CD/DVD, most varieties of server cassette backup tape, .MP3 player, and VHS tape).

- The DFU also provides mobile "roll-out" on-scene services (technical advisory on industry standards on search/seizure, live-RAM capture, network data dumps, and on-site imaging).

Rush Testing: Rush status must be approved by the laboratory and can be given to cases for the following reasons in descending order of importance:

- Cell phones with security features that will destroy evidence, such as the iOS 18.0/18.0.1 reboot issue
- Exceptional public safety risk such as homicide, sexual assault, or other crimes against persons
- Safety risk to the survivor or family such as a specific death threat or physical violence threat
- Jury trial date or discovery deadline
- Exigency of the evidence to the investigation (generating investigative leads)

Agency pre-log submissions to the ISPFS Laboratory Information Management System (ILIMS)

- Use the following codes and descriptors in ILIMS for DFU Evidence:
    - ***Section***: Digital Evidence
    - ***Item Types***:
        - Computer/Memory Evidence
            - Evidence that is not powered on and is not seeking a wireless network signal. This includes all tower/desktop/all-in-one computers, laptop computers, game consoles, DVRs, tablet/laptop hybrids, current and "Legacy" memory modules, "Flash," media (items not actively powered on), and cellular device memory not inserted in a cellular device (e.g. SIM cards).
        - Cellular Device Evidence
            - Cellular Devices: Devices that have the capability to access active wireless ("cellular") network signal.

- Working Copy Evidence
  - Memory modules (USB "Thumb" drive, "Flash" media, etc.) that contain a copy of audio/video evidence requiring enhancement by the DFU.

- ***Packaging Types***: Anti-static bag, brown paper wrapping, cardboard box, or standard manila evidence envelopes

PRELOG QUESTIONS:

1. Please complete a separate prelog submission for each location items seized from. In addition, please submit with the prelog form and evidence, a paper copy of search warrant affidavit and/or the investigative report.
2. Location of search site (please use address items found)
3. Authority for seizure and examination. (If other please complete question 3)
4. For verbal/other consent cases please include brief documentation from the investigator attesting to the fact that verbal consent was granted.
5. Date seized
6. Has the evidence been viewed/accessed since seizure? If yes, complete question 6.
7. Explanation of access: include date and time of view/access, please be as precise as possible.
8. Cellular device evidence status at time of seizure.
9. List any known username/passwords/pin code/swipe pattern.
10. Service requested (brief explanation).
11. Is there specific type of data being targeted/needed from the device (i.e.: text messages, email, contacts, images, etc.)? Please be specific about what is needed.
12. Is there a specific date range of interest for the target data? Please list the dates or date range.
13. Is this a CSAM case? If yes, non-pornographic images of the suspect and victim are needed.
14. Is rush processing being requested?
15. If rush processing is being requested, please detail the reasons rush processing is needed and list any court dates or discovery deadlines.

ILIMS Attachments:

DFU Computer Forensic Examiners (CFEs) will be better enabled to assist with investigations when they are given some context and background to the case as well as copies of paperwork that allows CFEs to legally image and analyze the contents of the digital evidence submitted. Please attach to ILIMS Pre-log or provide a hard copy:

- Answer Pre-log questions with clear descriptions of the nature of the case (crime type) and how a forensic review of the digital content is anticipated to contribute to the investigation
- Attach copies of legal paperwork that may apply (search warrant or written consent). DFU typically requires a search warrant or written consent to satisfy legal requirements to image/analyze the contents of any electronic device. These documents are required due to the 4th Amendment protections of digital content and the high likelihood of recorded conversations in the form of text/email/etc. that are protected by the 4th Amendment and the Electronic Communications Protection Act.
- Attach affidavits/reports or a brief case synopsis that will give context to what searches are being requested by the investigating officer.
- Attached non-pornographic images of the suspect and victim are helpful in identifying these individuals in cases of child pornography, lewd and lascivious, ritualized abuse, etc.

- Additional items may be emailed directly to the DFU examiner as the case is investigated.
- Please be specific if there is certain information or data needed for your investigation.
- Please provide court dates including discovery deadlines if available.

Acceptable Evidence Packaging

- **Tower/desktop/all-in-one computers, laptop computers, game consoles, DVRs, tablet hybrids, cellular memory cards (e.g. SIM), all memory modules (current/"Legacy") and "Flash," media:**
  - Packaged without peripheral devices (e.g. monitors, keyboards, etc.)
  - Contained in a shielded anti-static bag, cardboard box, or brown paper (bag or wrap)
  - Evidence integrity sealed via either heat seal or evidence tape (with signature and date across each seal).
  - Evidence tracking and chain-of-custody form/sticker attached.
  - All improperly packaged or unsealed digital evidence will be returned to the submitting agency for re-submission after package correction.

- **Cellular devices:**
  - Contained in a shielded anti-static bag or brown paper (bag or wrap)
  - Evidence integrity sealed via either heat seal or evidence tape (with signature and date across the seal)
  - Evidence tracking and chain-of-custody attached.
  - All improperly packaged or unsealed cellular device evidence will be returned to the submitting agency for re-submission after package correction.

  **The DFU recommends the most recent best-practice of submitting all cellular evidence: prior to evidence sealing in approved containers as noted above, the device should be packaged in at least three layers of tin/aluminum foil to prevent cellular network signal from contact with the seized device.

  DFU further recommends in cases requiring exigency or of a serious nature: if the device is on/active at the time of seizure, seal the device and a connected external battery (to extend the activity of the phone while in-transit) in at least three layers of tin/aluminum foil. Ensure the connecting cable and battery are confined within the foil with the cell phone/device. Failure to do so will allow network connectivity to the phone/device.

  Notify the ISPFS lab of this exigent/serious case and ship the evidence overnight to the ISPFS Meridian Laboratory. To ensure the phone will still have power and undergo timely processing, avoiding shipping on weekends if possible.

Acceptable evidence status

- Cellular devices:
  - If the device was powered off at the time of seizure, do not turn the device on.
  - It is recommended device status at the time of seizure is noted by the collecting agency and reflected on the evidence submission form ("The device was on/off when seized."). If the device is on at the time of seizure, it is best to leave the device on, remove from a network signal, and transport to the lab for best forensic results.
  - Regardless of device status at the time of seizure, package as outlined above and ship or transport to ISPFS as soon as possible.

- Laptop computers:
  - Laptop computers should be (if possible) shipped with all power sources removed (battery and power charger).
  - If available, ship laptops with their charging cords and batteries in the same package, but not attached to the computer.
  - In cases where a battery cannot be removed, hard shut down the device and package the evidence to ensure that the device will not inadvertently be powered on in-transit.
  - Package the evidence as outlined above.

- Tower/desktop/all-in-one computers, game consoles, DVRs, tablet hybrids, current/"Legacy" memory modules and "Flash," media:
  - All tower/desktop/all-in-one computers, DVRs, game consoles, should be shipped without power and in an "off," state. Current/"Legacy" memory modules and "Flash," media should be packaged as outlined above and transported/shipped to ISPFS.