Idaho State Police

Service Since 1939

Colonel Kedrick R. Wills
Director

Brad Little
Governor

To: Idaho Law Enforcement Agencies
From: Matthew Gamette, ISP Forensic Services Laboratory System Director
Sergeant Bret Kessinger, ISP Cyber Crime Unit Director
Subject: **Digital Evidence Submission Process Changes**
Date: May 17, 2021

Effective June 7th, 2021, all digital/cyber/electronic evidence (computers, cellular devices, copies of audio/video evidence for enhancement) for the Idaho State Police Cyber Crime Unit (CCU) will now be submitted through Idaho State Police Forensic Services (ISPFS) Meridian Laboratory.

- All evidence must be "pre-logged" in advance of submission in the ISPFS Laboratory Information Management System (ILMS). In-person customers will be asked to provide the pre-log form (see attachment for instructions) and shipping customers should place it in the shipping container.
- All evidence must be in a sealed condition and in appropriate packaging when submitted to ISPFS (see attached details).
- All submissions must be mailed by secure carrier or hand delivered to the ISPFS Meridian Laboratory. Urgent submissions must be notified in advance to Bret Kessinger (208-884-7111) and the Meridian Lab (208-884-7170) so the CCU and our evidence staff can be on standby to facilitate a quick evidence transfer to the CCU analyst working the case.
- Packaging advice and assistance may be available from the ISP evidence technicians at the ISP District Offices around the state.
- Improperly sealed evidence shipped to the lab will be returned to the submitting agency for remediation. Improperly sealed evidence submitted in person must be corrected before it will be accepted by the laboratory.
- Any additional forensic science work needed on the submitted electronic item (i.e. latent prints, DNA) must be selected in prelog and communicated to ISPFS evidence staff upon submission. ISPFS will coordinate the processing order in conjunction with the submitting agency and ISP CCU.

These changes are being implemented to document the chain of custody electronically and also to facilitate CCU examiners spending more time on casework instead of administrative duties. We anticipate these process changes will streamline the process for everyone involved.

Please do not hesitate to contact Matthew Gamette at 208-884-7217 matthew.gamette@isp.idaho.gov or Bret Kessinger at 208-884-7111 bretkessinger@isp.idaho.gov if you have any questions.

Packaging and Submission Instructions

Overview of Idaho State Police Cyber Crime Unit Services

- ISP Cyber Crime Unit (CCU) 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 CCU 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).

- Depending on case load, it is anticipated that most evidence will be processed and returned within two weeks of submission.

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

- Use the following codes and descriptors in ILIMS for CCU 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 CCU.

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

ILIMS Attachments:

CCU 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). CCU 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 CCU examiner as the case is investigated.

ILIMS Questions:

When Pre-Logging evidence into ILIMS, users will be required to answer the following questions:

1. Case Officer/Submitting Officer.
2. Suspect/Victim/Subject information.
3. Location of seizure site.
4. Authority for seizure and examination: Search Warrant, Written Consent, Probation/Parole, "Other" with a clear explanation.
5. Date Seized
6. Has the evidence been viewed/accessed since seizure?
7. Cellular device evidence status at time of seizure, "on/off."
8. Explain access: including date and time of view/access: When investigators properly document down to the minute the date/time of the view/access, CCU can confirm the access and testify that this access/viewing was not detrimental to the fidelity of the evidence.
9. Service Requested (brief explanation): This field is typically kept brief when the investigator includes the search warrant affidavit language or an investigator's report.
10. List any known username/passwords/pin code/swipe pattern.

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

  CCU further recommends in cases requiring exigency or are 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/CCU labs of this exigent/serious case and ship the evidence overnight to the ISPFS Lab. To ensure the phone will still have power and undergo timely processing, avoiding shipping on weekends if at all 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.