BEST PRACTICES FOR A QUALITY DIGITAL FORENSICS EXAMINATION

To help the Indiana State Police provide the highest level of service to its local, state, and federal law enforcement partners, the Cyber Crime Unit (CCU) recommends the following *Best Practices*:

CONTACT THE ISP FORENSIC EXAMINER IN YOUR AREA TO SCHEDULE A DATE AND TIME TO DROP OFF DIGITAL EVIDENCE – Because Examiners may be out of the office in reference to criminal investigations, trial, training, or vacation, it is important to contact them to schedule a date and time to drop off digital evidence.

MEET WITH THE ISP FORENSIC EXAMINERS AT THE BEGINNING OF AN EXAMINATION – Once digital evidence is brought to ISP CCU for review, the investigator should either meet in person or personally speak to the Examiner over the telephone about the scope of the examination. By doing so, CCU is better able to screen, prioritize, and assign the case for examination.

ENLIGHTEN THE EXAMINER – When submitting digital evidence for examination, investigators should share what they know about the case with the Examiner. While the following suggestions may seem obvious, if this information is not provided to the Examiner early on, delays may result—

- ***Inquire about the Owner's Sophistication Level –*** It is helpful for an Examiner to know if the owner enabled password protection or an encryption application. If the investigator is aware of such tactics, alert the Examiner *before* they begin the examination.

- ***Provide the Names of Suspect(s)/Victim(s) –*** Provide the Examiner with this information, including nicknames and chat handles along with the specific spellings of these names. Accuracy is absolutely key.

- ***Provide a Copy of the Search Authority –*** Provide the Examiner with a copy of the search warrant or consent to search so the Examiners knows there is legal authority to conduct the examination. Without this documentation, the Examiner cannot begin the examination.

- ***Provide a Copy of the Case Report –*** If possible, provide the Examiner with a copy of the case report. This document contains valuable information about the investigation and/or the evidence the investigator is searching for.

- ***Keep the Examiner Apprised of Active Investigative Leads and Court Dates –*** Provide the Examiner with any new information obtained during the course of the investigation, even after the evidence has been submitted for examination. This will allow the examiner to provide a better quality work product and analysis. Also, provide any discovery deadlines, requests for speedy trial, or trial dates, so these timelines may be met.

NARROW THE EXAMINATION'S SCOPE – Investigators can help an Examiner be more efficient by providing the following—

➢ ***File Names*** - If the investigator is looking for a particular file or if they know the file's location—alert the Examiner.

➢ ***Dates –*** The investigator should inform the Examiner if there is a specific date range relevant to the investigation, or if the examination is limited to certain dates by the search warrant.

➢ ***Data Sources –*** If submitting multiple computers, media, or hard drives, state which system or piece of media has the highest probability of containing what is being searched for.

➢ ***Focus the Request –*** Focus the request by identifying a particular range of dates, search terms, Web sites, user profile(s) or even a downloaded file(s). This helps the Examiner fine tune their search in these areas.

➢ ***E-Mail Addresses –*** Investigators should identify exactly which e-mail addresses the Examiner should search for.

SET TIMEFRAMES – A quality digital forensics examination may take anywhere from 30 to 90 days, sometimes longer to complete. The time spent is affected by several factors such as the amount of data that must be reviewed; whether or not encryption is involved; the user's level of technical sophistication, the complexity of the investigation, etc. Once an Examiner begins work on the case, he/she can usually determine the time frame for the examination and will inform the investigator. Conversely, if there is a change in the status of the case (e.g., discovery deadlines, trial) and the investigator needs the results sooner than expected—he/she should immediately inform the Examiner.

REMEMBER THE CCU CASE NUMBER – Every case submitted to CCU is assigned a case number. Remember that number—the Examiner uses it to provide information about the case should the investigator request it.

THE FINAL PRODUCT – The Examiner will provide his/her findings in the form of a CD, DVD, or hard drive. At that point, the Examiner's work is complete—and the investigator can now conduct a full review of the findings. It is important to remember that although the Examiners are investigators by training—they must remain impartial when conducting a digital forensics examination. Lastly, no examination is ever all-inclusive. Additional examinations and supplemental reports could follow if the investigator obtains new information or the prosecuting attorney requests further analysis in preparation for potential criminal charges or trial. Therefore, it is suggested and highly recommended the investigators, the prosecutors, and/or their designees review all of the reports and determine their evidentiary value. If further analysis is requested, please contact your Examiner immediately.

FOR MORE INFORMATION

To learn more about the Indiana State Police Cyber Crime Unit:

Cyber Crime Unit
John Richards, Lieutenant
Email: JRichards@isp.IN.gov

Mailing Address—
Indiana State Police
Office of Intelligence & Investigative Technologies
Cybercrime Investigative Technologies Section
8468 East 21st Street
Indianapolis, IN 46219