



BEST PRACTICES FOR A QUALITY DIGITAL FORENSICS EXAMINATION

FACT SHEET

To help an RCFL provide the highest level of service to its law enforcement customers, the RCFL National Program Office recommends the following “best practices” –

Meet With the RCFL Staff at the Beginning of an Examination – Once digital evidence is brought to the RCFL 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, the RCFL 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*** – If possible, 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. These documents may also contain valuable information about the investigation and/or the evidence the investigator is searching for.

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, 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, 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 and the investigator needs the results sooner than expected—he/she should immediately inform the Examiner.

Remember the RCFL Case Number – Every case submitted to the RCFL is assigned a case number. Remember that number—the Examiner uses it to provide information about the case should the customer request it.

The final product - The Examiner will provide his/her findings in the form of a DVD, CD, floppy disk, hard copy, or via a review network. 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 most Examiners are investigators by training—they must remain impartial when conducting a digital forensics examination.

FOR MORE INFORMATION

To learn more about the RCFL Program, contact the National Program Office:

RCFL National Program Office

SSA Bryan Tepper, Unit Chief
Central Number:
703-985-3677
Email: npo@rcfl.gov

Mailing Address—

Engineering Research Facility
Building 27958-A
Quantico, VA 22135
Attn: ERF Annex
RCFL National Program Office

Web Site Address—

www.rcfl.gov