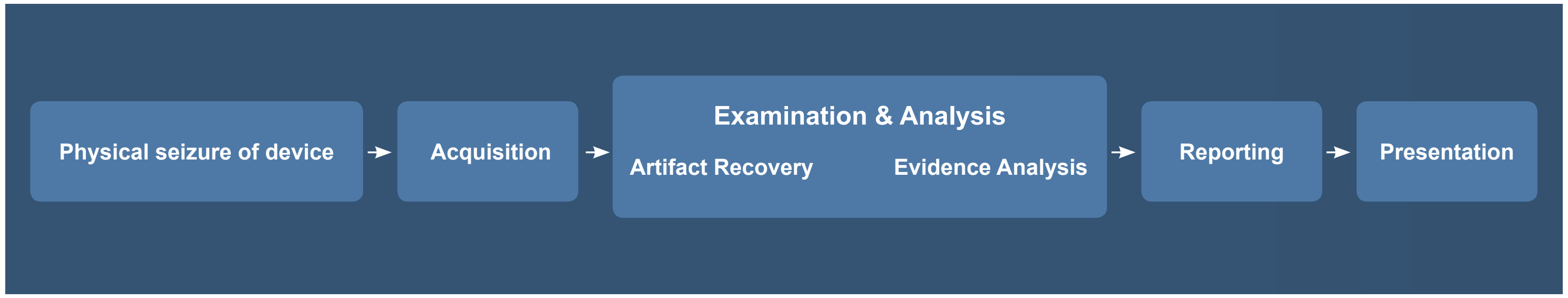
8 Tips for Presenting Digital Evidence in Court

Digital evidence is playing a progressively more important role in criminal investigations, from fraud to intellectual property theft to child exploitation. As our world becomes more "connected", digital evidence is becoming relevant to more and more cases.

But digital data is easily manipulated. If an investigator leaves undocumented gaps in their acquisition or analysis process, their evidence can easily lose credibility. Without adequate chain of custody documentation or proof of data integrity, digital evidence can become inadmissible in court. And, even if this evidence has been properly handled, investigators often encounter challenges when trying to present technical data to an audience unfamiliar with digital forensics.

Preparing to effectively present digital evidence starts long before the court date. Although you're sure to encounter tough questions when presenting or testifying, we've provided some tips to consider when presenting digital evidence and forensic reporting in court. In this resource, we'll walk through each step of the process, from seizing the device to delivering an accurate testimony. Keep in mind that although these are prudent recommendations, you should still consult your agency's legal counsel for clarification or more in-depth advice.

From Physical Device Seizure to Evidence Presentation: 8 Tips



Appropriate physical seizure of device

Tip 1: Ensure that you have legal authorization to examine data on the device seized

Although this may seem obvious, it’s crucial to ensure that you have a search warrant or other legal authorization to look at the data from the seized device. If you happen to come across additional, unrelated data for which you do not have a warrant, you should consult the prosecutor before proceeding with your search of the evidence.

Tip 2: Record the chain of custody for any device in your possession

When handling evidence following the seizure of the device, make sure to record proof of continuity. It's important to understand who had access to the device at any point in time to establish credibility for the evidence it contains. Many investigators will keep a log to demonstrate that there are no gaps in the chain of custody for the physical evidence. Depending on your jurisdiction, this can be a useful resource when pulling together a report for court.

Acquisition

Tip 3: Maintain data integrity

When acquiring raw data from a hard drive or mobile phone, always access the device through a write-blocker or a tool that protects the device from being altered. Write-blockers enable read-only access for the viewer and prevents data from being added to or changed on a hard drive. This helps back-up the integrity of your data, adding credibility to your acquisition process.

Calculating a hash value for the hard drive is another important way to demonstrate that the data has not been modified since seizure. Hashing algorithms provide a unique value for a particular sample of data, similar to a fingerprint or DNA sample. If anything is changed on the hard drive, this value will change.

Examination and Analysis

Tip 4: Validate your results

Before reporting on or presenting the results of your digital evidence analysis, you need to validate all results. Typically, investigators won't have full confidence in the digital evidence until they've double-checked the original data source, because there is always a possibility that the data at that location is slightly corrupt or there's been a software bug. Although it's best to verify the evidence for every case, this becomes especially crucial when one piece of evidence carries significant weight for an investigation. For example, if an investigator found a confession in a message from a mobile chat app that shed light on the perpetrator of a homicide, it would be important to double-check these results since they may have a substantial impact on the verdict.

In case you are asked how the software gathers data, use the glossary from the software provider (when appropriate) to prepare to describe what the artifacts present and where they are located. For reference, you should also record the software version numbers used for searches.

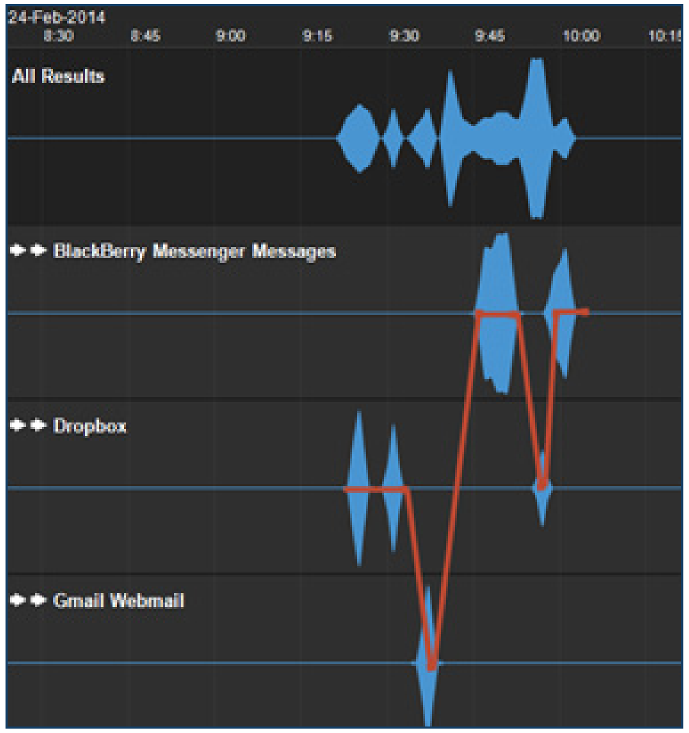
Although some may claim that the tool they use is court-approved and doesn't require validation, the reality is that no such certification exists. The best way to verify your results is by either running a second tool, or by verifying the data manually by checking the original location to confirm that it matches your original results. This ensures the court-admissibility of your evidence, so you can stand behind your results with confidence.

Reporting

Tip 5: Develop a thorough reporting format that emphasizes key findings

Having finished recovering and analyzing artifacts, you'll need to pull together a report detailing the evidence analyzed and explaining your process and findings. Although formats may vary slightly case-by-case, creating a template for presenting reports will establish consistency and allow courts to grasp the contents of reports more easily over time.

Here are a few helpful general considerations on report-writing from forensic consultant Melia Kelly.



- **Include an executive summary** detailing your results. This section should also give context to the evidence analyzed.
- **List every piece of evidence analyzed,** including serial numbers, hash values, photographs, etc.
- **Write thorough descriptions for photographs,** including information on the camera type, date, timestamps and locations.
- **Clearly show the steps taken to collect and analyze artifacts,** including listing any software or hardware used to extract and analyze data.
- **Create a timeline.** It's helpful to create a visual that demonstrates the chronological sequence of events in a way that's easy for readers to grasp.
- **Remember to put yourself in the shoes of the reader.** What questions might you have about the evidence if you were in their position? If you can adequately answer these questions in your report, you may be released from testifying.

Evidence Presentation

Tip 6: Be confident in the reliability of your evidence and your credibility as an examiner

If you are required to present your report and testify in court, make sure you're able to both validate the credibility of your data and the reliability of your tool. It's also important to ensure that you have a comprehensive list of credentials and certificates to support your training in digital forensics. Be able to tell the court how long you've been doing forensic analysis and perhaps even how many computers and mobile devices you have examined.

If you've been diligent in acquiring, analyzing and validating the evidence, you can deliver the results with full confidence. Keep in mind that lawyers may try to ask compound questions, trying to get one answer for two questions. Make it clear that you are answering one question at a time.

You should also be prepared to answer the following questions, **according to digital forensic practitioner Shayne Sherman.**

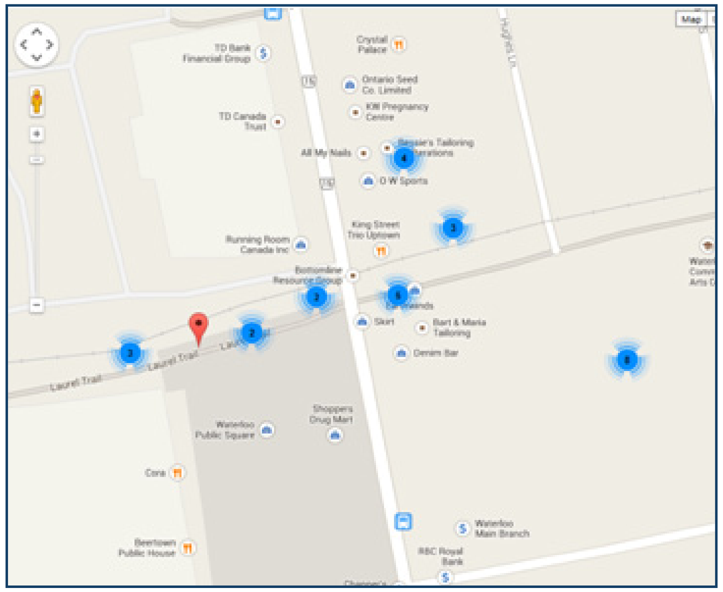
- How was the tool/technique/equipment used?
- Who was it used by?
- Where was the data found?
- How was the data validated--either manually or with a secondary tool?
- What are the strengths and weaknesses of the evidence?
- Are there alternative explanations?
- Has this acquisition or analysis technique been reliably tested?
- What is the known or potential rate of error of the technique?
- Has this technique been subjected to peer review?
- Is this technique generally accepted?

Tip 7: Interpret data to tell a story

When you’re presenting abstract concepts and technical evidence to an audience with little (if any) background in digital forensics, you can’t simply display raw evidence and expect that they will read between the lines and understand the story.

Without oversimplifying your findings, your role is to present the data in a manner that is clear and concise. When possible, try to interpret this data to tell a story. One of the best ways to lead a judge and jury through your evidence is with visual aids. Often, separate illustrative presentations may be required to give context to complicated evidence.

Tip 8: Use visuals whenever possible

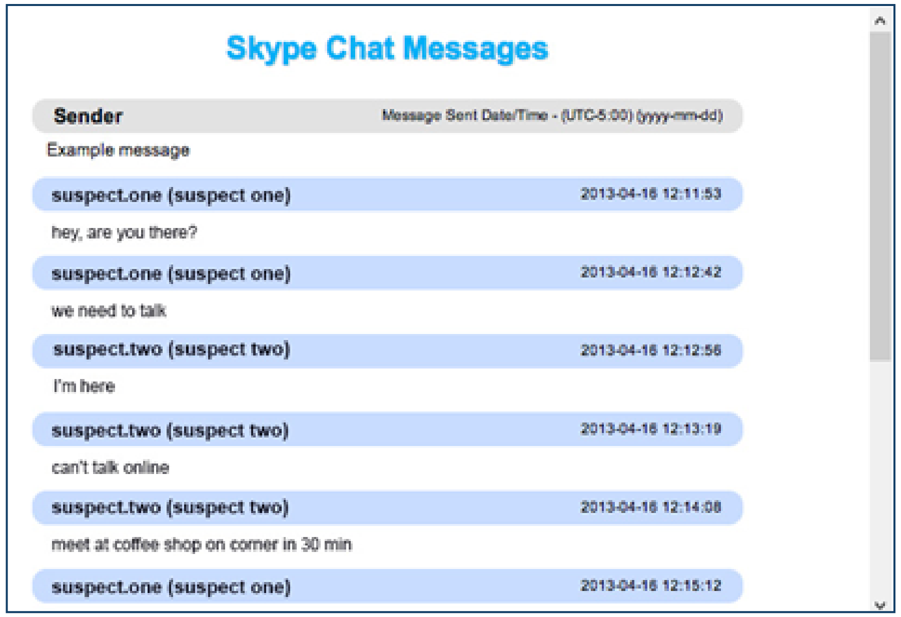


Use visuals as often as possible to help the judge and jury grasp the context and relevance of your digital evidence. There are a variety of analysis and reporting tools that can help reconstruct search history and create timeline and geolocation visualizations. Complex, technical data can be hard for the audience to understand, so leveraging these data visualization features can be indispensable for examiners preparing to present in court.

Although this is more of a logistics consideration, ensure the court room is equipped with the right gear to present digital evidence in a meaningful way. Some meaning may be lost in attempting to print digital evidence on paper vs. presenting an HTML report on a display.

When evaluating digital forensics tools, look for one that helps:

- Recover history records, dates and times of webpage visits.
- Rebuild web pages as the viewer saw them when they conducted their search.
- Plot recovered timestamp data on a visual timeline, so the judge and jury can quickly grasp a chronological series of events.
- Rebuild chat messages in threaded view, similar to the format of the original chat messaging application. For an audience who doesn't examine raw data regularly, this gives both context and visual clarity to the evidence.
- Plot recovered geolocation data from mobile messaging apps and photographs on a map.



Skype Chat Messages

Sender — Message Sent Date/Time - (UTC-5:00) (yyyy-mm-dd)
Example message

suspect.one (suspect one) — 2013-04-16 12:11:53
hey, are you there?

suspect.one (suspect one) — 2013-04-16 12:12:42
we need to talk

suspect.two (suspect two) — 2013-04-16 12:12:56
I'm here

suspect.two (suspect two) — 2013-04-16 12:13:19
can't talk online

suspect.two (suspect two) — 2013-04-16 12:14:08
meet at coffee shop on corner in 30 min

suspect.one (suspect one) — 2013-04-16 12:15:12

Our Internet Evidence Finder (IEF) has become one of the most widely used digital forensics tools for the recovery of Internet evidence. IEF can improve the efficiency and effectiveness of your investigation by:

- Automatically searching for artifacts in unstructured data sources such as unallocated space, pagefile.sys, and volume shadow copies.
- Aggregating data from time of events, location, sources and artifacts to create a fully interactive timeline that can be exported as a HTML, PDF or TLN file.
- Enabling the investigator to conduct a thorough and efficient analysis of the collected data through searching and filtering, or using visualization techniques such as mapping, rebuilding webpages and chat threads.

Conclusion

With the right tools and techniques, digital forensics analysis can yield valuable evidence that can significantly impact a criminal investigation or legal dispute. Proper artifact recovery and reporting methods are the key to ensuring that digital evidence is court admissible. It is also absolutely relevant that an examiner's findings are properly conveyed to the court in understandable terms, as even the most experienced expert can easily be misunderstood if too much jargon is used. Finally, using visuals to present digital evidence is a great way to help the audience interpret the story from the facts.

Ready to learn more?

- Watch this case study to **learn how geolocation data and timeline analysis can provide valuable insight** into a digital forensics investigation.
- Find out how to **create and export reports** in Internet Evidence Finder.
- Learn how to **use hash analysis to identify and categorize photographs** using Internet Evidence Finder.

For more information call us at 519-342-0195
or email sales@magnetforensics.com

MAGNET FORENSICS®