ArcherHall

The Essential Guide to Digital Forensics

A brief overview of computer forensics, mobile forensics, and other types of digital investigation.

Overview

Digital forensics is the application of scientific tests or techniques to collect digital evidence in connection with litigation or other types of investigation. It is an integral part of the legal discovery process, but can also be a valuable tool for avoiding or shortening litigation.

Digital forensics is typically divided into sub-specialties by data source. For example, computer forensics involves collection of data from desktops and laptops. Similarly, mobile forensics involves collection of data from cellphones and tablets. There are many other potential sources of data including email, social media, and cloud storage. A thorough investigation often involves examination of multiple sources of data and careful comparison of the information collected from each.

Digital Forensics Can Enhance an Investigation

An experienced digital forensics team can:

collect email, text, and other communications;

find critical documents;

recover deleted communications and files;

determine the activities of a specific user at a specific time.

Most importantly, forensic investigators can make connections between disparate documents, communications, logs, and data artifacts to help you draw conclusions about what may have occurred in your case.

Digital Forensics Requires Expertise

ArcherHall uses specialized equipment and software to collect and examine devices without changing the data or the metadata (such as the last modified time or the document author). This prevents you from relying on data that was inadvertently modified in the investigation. The advanced tools and years of experience also help forensic examiners collect data that has been deleted or corrupted, as well as system data that is not normally accessible to a user.

This specialized scientific approach protects the integrity of the data and ensures it is admissible in court.

Digital Evidence Checklist

This sample checklist is designed to provide guidance on the effective collection of digital evidence. It combines detailed considerations with specific checklist items for both cell phones and laptop/desktop computers.

Cell Phones and Tablets

Device Identification: Identifying the make and model is important as it dictates the forensic tools and methods required for data extraction.

What is the device make and model?

□ iPhone (model) ____________________
□ Android (model) ____________________
□ Tablet (model) ____________________
□ Other ______________________ (model)
____

Current Usage: Knowing whether the device is in use helps assess potential data modification risks.

Is the device currently in use?

□ Yes
□ No
□ Other ______________________

Desired Data: Specifying the types of data required is necessary as each type may require different collection techniques and has distinct privacy considerations.

- □ Text Messages
- □ Call Records
- □ Voicemails
- □ Media (Photos/Videos)
- □ Email*
- □ Social Media and Direct Messages (DM's)*, including:
  - □ Facebook/Facebook Messenger*
  - □ WhatsApp Messages*
  - □ WeChat Messages*
  - □ Direct Messages (DM's)* (e.g., Instagram, TikTok, Snapchat)
  - □ Other Applications

Device Storage: The device's storage capacity informs the scope of data collection and resource allocation.

Specify the storage capacity in gigabytes (e.g., "64 GB" or "256 GB"):

____

Laptop and Desktop Computers

Device Identification: The make and model are essential for selecting the appropriate forensic tools. The device's usage status can influence data preservation strategies.

What is the laptop/computer make and model?

□ Dell (model) ____________________
□ HP (model) ____________________
□ Lenovo (model) ____________________
□ Apple (model) ____________________
□ Other ______________________ (model)
____

Current Usage: Understanding current usage is critical to planning data preservation and collection.

Is the laptop/computer currently in use?

□ Yes
□ No
□ Other ______________________

Device Storage: Storage details inform the volume of data and complexity of the data recovery process, especially for deleted data.

Specify the storage capacity in gigabytes or terabytes and provide disk details:

□ Gigabytes (disk details)
____

□ Terabytes (disk details)
____

□ Other ______________________ (disk details)
____

Desired Data: Identifying specific data types to be collected directs forensic efforts towards relevant information.

- □ Copied/Deleted Data
- □ User Activity
- □ Web Browsing History
- □ Emails*
- □ Social Media*

*Original source data collection may be necessary as comprehensive data isn't stored locally

Additional Considerations

- Search Terms and Date Ranges: Focused search parameters streamline the collection process and increase the likelihood of uncovering pertinent information.
  - □ Provide relevant search terms.
  - □ List involved parties (names, email addresses, phone numbers).
  - □ Specify specific date ranges for focused data collection.

- Deleted Content: The need to recover deleted content requires specialized forensic techniques to ensure data integrity.
  - □ Determine if obtaining deleted content is a priority.
  - □ Understand how this requirement may impact preservation and data collection methods.

This checklist ensures that you are thoroughly prepared for the digital evidence collection process, facilitating targeted and efficient data gathering. Enlisting forensic experts ensures your collection is done in a forensically sound manner and gives your case every advantage.

ArcherHall
AIM HIGH

ArcherHall.com | 855.839.9084