4Discovery's

Remote Collection Protocol

A remote collection process is relatively simple to complete in a short time frame. The process requires the physical device and/or cloud account to be in working order and any pin/passcodes required to access the device and/or account provided. Devices and accounts have slightly different workflows required for collection and examples of the process for both can be found below.

Computers & Mobile Devices

Outlined below is the remote collection process for computers and/or mobile devices. If the device is not in working condition, appropriate measures to repair the device for forensic preservation will be taken, with authorization from the appropriate party. If the device is not repairable, with authorization from the appropriate party, further measures may be needed to ensure all options are exhausted to recover data from the device's internal memory, including methods that may be destructive to the original device.

1. Once information is provided to 4Discovery detailing the Custodian's shipping address, scheduling availability, and device information, 4Discovery will prepare a remote collection kit to send to the Custodian via overnight shipping.
2. The remote collection kit is prepared based on the needs of each Custodian and typically contains:
    a. One (1) laptop w/ power cable
    b. An external hard drive
    c. Appropriate cables for collecting data from applicable devices
    d. Instructions for setting up the remote collection kit
    e. Contact information of the digital forensic expert who will perform the live data collection
    f. A prepaid shipping return label
3. The laptop and external hard drive are both encrypted to protect evidence in transit.

4. Once the Custodian receives the remote collection kit, they will plug in the power cord and turn on the laptop before the commencement of their scheduled data collection session.
5. The 4Discovery digital forensics expert will call the Custodian at their scheduled session time to help them walk through the steps detailed in the remote collection kit setup instructions:
    a. Login to the laptop
    b. Connect to the internet
    c. Connect the external hard drive
    d. Connect the device to the laptop
6. During the collection process, the digital forensics expert will walk the Custodian through entering in any necessary passcodes and/or passwords, while navigating any system settings changes that are necessary for the data collection process.
7. 4Discovery will forensically acquire the device(s) in a non-destructive manner using industry standard forensic tools to collect the data available for extraction from that device. The extractions will be stored in standard imaging formats and preserved on a dedicated encrypted storage drive.
8. Once the collection is complete, 4Discovery will verify that the image is a true, accurate, and complete copy of the data available on the original device(s).
9. Once the acquisition is verified, 4Discovery will walk the Custodian through the process of disconnecting devices from the computer and preparing the equipment for return shipping. Any settings changed during the data collection process will be reverted to their original state with the digital forensics expert's assistance.
10. The Custodian will use the prepaid return shipping label to return all of the equipment and extracted data to 4Discovery. If necessary, a pick-up can be scheduled with our shipping provider at the Custodian's location.

Cloud-Based Accounts

Outlined below is the remote collection process for email, social media, and other cloud-based accounts. If the account cannot be accessed using the provided credentials, 4Discovery digital forensic experts will work with the Custodian to regain access to the account. If the account cannot be accessed, 4Discovery will follow up with counsel to discuss other potential options for obtaining the data.

1. Once information is provided to 4Discovery detailing the Custodian's scheduling availability and list of cloud-based accounts, 4Discovery will schedule a session with the Custodian to walk through accessing and collecting their cloud-based accounts.
2. The collection process for each account will vary slightly based upon the type of account and the collection methods available for that type of account.

3. In general, while on the phone with the 4Discovery, the Custodian will provide:
    a. The username and/or email address associated with the account
    b. The password for the account
    c. Any two-factor or multifactor authentication necessary to access the device
    d. Access to any connected email accounts to retrieve download links
4. During the collection process, the digital forensics expert will walk the Custodian through entering in any necessary passcodes and/or passwords, while navigating any system settings changes that are necessary for the data collection process.
5. 4Discovery will collect the account(s) in a non-destructive manner using industry standard forensic tools, native profile download options, or other collection methods if necessary to collect the data available for extraction for the account(s). The extractions will be preserved on a dedicated storage drive.
6. Once the collection is complete, 4Discovery will verify that the image is a true, accurate, and complete copy of the data available on the account(s).
7. Upon confirming a true, accurate, and complete copy of data was collected, 4Discovery will notify the Custodian the collection is complete. Any settings changed during the data collection process will be reverted to their original state with the digital forensics expert's assistance.

Sample Protective Order

Outlined below is a sample protective order to assist with pushback and objections to the collection of personal data. Protective order provisions can be modified to meet the specific concerns of each party.

Confidential Information

Any party or non-party producing the information may designate as "Confidential" any document, discovery response, or transcript that counsel determines, in good faith, contains confidential and non-public business or financial information.

Use of Designated Documents & Information

Documents designated as Confidential, as well as the information contained therein, shall not be disclosed, in whole or in part, except as set forth herein, and shall be used only for the purpose of prosecuting or defending this litigation and not for any other matter or purpose.

Designation of Confidential Information

The designation of information as Confidential shall be made either: (i) by stamping the word "CONFIDENTIAL" on the document at the time of production; or (ii) by stating on the record at the deposition that the testimony is to be accorded Confidential treatment; or (iii) by identifying transcript pages to be treated as Confidential within fifteen (15) days after the deposition.

Access to Confidential Material

Access to information designated as Confidential shall be limited to:

1. The Circuit Court, the Appellate Court, and the Supreme Court, their staffs, and members of the jury in this case;
2. Court reporters, stenographers, and videographers;
3. Counsel of record for the parties and supporting personnel employed by such counsel, including paralegals, translators, secretaries, and clerks;
4. The Defendants, their managers, and those representatives of the Defendants who are assisting counsel in the defense of this case;
5. The Plaintiff, and those representatives of the Plaintiff who are assisting counsel in the prosecution of this case; and
6. Independent experts and consultants, who are employed or retained by counsel for the parties to this action solely for the purpose of this litigation, provided that the expert or consultant agrees to be subject to the terms of this Order by signing Exhibit A.

Use of Confidential Material at Depositions

Information designated Confidential and marked as an exhibit may be shown to non-party witnesses during the course of testifying at a deposition, hearing, or trial of this case.

Additional Resources

The remote collection process has been designed to be easy and painless for all participants. If there are any questions or concerns, please don't hesitate to contact us.

4Discovery is an elite B2B digital forensics firm that provides organizations and attorneys with digital forensic, information security, and electronic discovery services.

Contact us

215 N Green St • Chicago, IL 60607
Tel: 312-924-5761
Email: info@4Discovery.com
Website: www.4Discovery.com

www.4Discovery.com