Digital**Forensics**

VESTIGE
Digital Investigations

Mobile Device Services

Vestige Mobile Device Forensic Services Are In Demand

Vestige Experts are able to extract key evidence from Smartphones, GPS units, tablets and other mobile devices using an array of specialized software and equipment designed specifically for advanced digital device forensics. We can extract active and deleted data from many types of mobile devices on the market today. Forensics level acquisition can either be performed On-site, Remotely, or In-Lab.

Data We Can Recover* | Common Requests

- App Usage (are or were privacy applications installed?)
- Calendar and Task List Entries
- Call History Logs (Dialed, Missed, Received)
- Cloud Storage (ex. is Google Drive or DropBox installed?)
- Contacts and Phonebook
- Deleted Data (texts, contacts, call history, photos, videos - sometimes)
- Emails Stored**
- Internet Browsing History (what sites visited? when?)
- Location History
- Party/Parties and Keywords
- Person's names (first, last or both)
- Photo/Multimedia Messages
- Pictures and Images
- Recovery of User Handset Lock Code
- Searches Conducted
- Social Media / Networking Artifacts
- Specific Phone number(s)
- Text Messages (SMS)
- Video and Audio Recordings
- Wiping or Factory Reset Indicators

* NOTE: This list contains typical items that Vestige is able to recover. There can be access limitations based upon restrictions of the user, the make/model of the device, software that has been installed and limitations of the carrier and/or device manufacturer, such as 2-Factor Authentication, encryption, additional passwords and general privacy considerations.

** NOTE: Email Searches – As email is generally available on the server, many of the phone models do not store the actual email on the local handset. Instead the device only pulls the "header" information (from, subject, first couple lines of message, etc.) to display in the inbox. When imaging and analyzing a mobile device, Vestige will pull down any email, if any, that is present. For comprehensive email preservation and analysis, Vestige has the capability to pull such email directly from the mailbox. Make sure to ask about this additional service if email is essential.

Other Services Available

- Detailed forensic analysis of mobile device operating system and application artifacts
- Device physical memory extraction including: TsOP and BGA Chip-Off Forensic Extractions, file system acquisitions and hex dumps

The Digital Forensics Process

WHAT VESTIGE NEEDS:

Acquisition — Access to the Device

The first step is the acquisition of the mobile device where it is believed digital evidence resides.

- The owner can voluntarily turn over the device to either the requesting party or make pick-up/shipping arrangements with Vestige; or
- The device can be subpoenaed where the owner is required by court to turn over the device; or
- If the device is owned by a company performing an internal investigation, they can either require the employee in question to turn over the device(s), or covert imaging can be performed.

- TYPE OF DEVICE - To provide a cost estimate, Vestige must know the make and model of the mobile device(s). Ex: Apple iPhone 6, Android Samsung Galaxy, Blackberry, etc. before preserving a device as different mobile devices require different methods and digital forensic tools.

Preservation of Data

You can choose how you want to preserve your mobile device data:

- **On-Site** - Vestige comes to your designated location**; or**
- **Remote** - Vestige ships a Remote Kit and works with a custodian to preserve, or an Online Remote Collection that is internet connected with a reliable, secure Wi-Fi; or
- **In-Lab -** send the device to Vestige's Digital Forensics Lab

ON-SITE DATA PRESERVATION:

Apple devices are more consistently structured and are typically easier to work with; Androids require more tools in order to acquire a reliable pool of preserved data.

APPLE - ITEMS NEEDED:

- **Unlock Passcode** - if one is set on the mobile device.
- **iTunes Backup Passcode** - if one is set on the device.
  (When Vestige images the device we use the owner's password to open, then we set our own password temporarily to make the copy; then we return it back to the owner's password. This method allows us to get an encrypted backup that provides more data ex: health, password keychains, bluetooth, wifi, etc.)
- FOR ONLINE PRESERVATION ONLY - IF there is an existing **iCloud backup account & iTunes** - the **Email & Password** is needed along with the **2-Factor Authentication Token**, if it is enabled.
  If 2FA is enabled, it requires a code via phone to open; the device custodian requests the 2FA code (a unique code to the instance), once opened, then the iCloud backup can be downloaded. It is variable what data we can get from iCloud, dependent on what was set to get backed up.
  We can get messages, photos, etc.

ANDROID - ITEM NEEDED:

- **Unlock Passcode** - if one is set on the mobile device.

REMOTE DATA PRESERVATION:

For this method, Vestige ships a Remote Kit which includes:

- Various USB connectors
- Encrypted hard drives that are pre-loaded with the software needed to preserve the digital device(s).

Once the Remote Kit is received, the client must have access to a computer with 100 GB of free space (preferred).

Vestige then connects with the client via telephone or an online conference app.
Here we direct the client through the entire Data Collection Process which includes:

- Loading preservation software
- Connecting to devices
- Performing the preservation or data acquisition itself.
  NOTE: The time this takes will greatly vary from device to device, and is dependent upon how much data is on the mobile device and the speed of the computer hardware.
- Upon completion, the files are transferred onto the Vestige provided encrypted harddrives.
- The client then packs up the Remote Kit complete with the collected data on the harddrives and ships it back to Vestige.
- Upon arrival, Vestige uses the secure pin to unlock the encrypted harddrive(s), assuring the data is secure through each step.
- We verify that it is the correct backup. Then Digital Forensic Data Analysis begins.

CAVEAT:
iPhones work well for remote preservations, and we can acquire all the same data that we get from local preservations (outside of jailbreaking). Android Devices, however, can be troublesome when performing a remote preservation, and the amount of data that can be preserved from the phone can be limited (i.e. deleted messages are not available via remote preservation). Call Vestige today to ask questions and learn more.

JAILBREAKING & ROOTING

Jailbreaking is performed on an iPhone; Rooting is performed on an Android. Both are a means for bypassing the manufacturer's restrictions placed on the operating system and allowing for full control of the device.

The benefit of Jailbreaking or Rooting a mobile device is that it allows complete access to the data on the device. In many instances, a full physical image can be made, which acquires every bit of data on the device — exposing additional evidential data.

Additional data that can be gained through Jailbreaking & Rooting includes:

- Additional Application Data
- Additional GPS Data
- Application and Operating System Log Files/Artifacts
- Email Data
- Deleted Messages on an Android, depending on the make and model
- Some File System Data - made by the operating system but is not in 'unallocated' space
- Deleted and unallocated data can also be made available but encryption can complicate recovery

Analysis

Vestige takes the data that is preserved and processes it through analysis software.

Our Forensic Experts perform analysis to:

- Gain Access to all “visible” user content
- Access hidden, protected and deleted data
- Perform artifact analysis to learn “how the device was used”
- Perform keyword and other filter searches against user content
- Extract and provide relevant data to investigating team

Our Analysts can dig deeper than just the artifacts captured by the forensic analysis tools. We frequently go beyond the capabilities of these tools employing software, applications and custom scripts resulting in extraction of artifacts that are missed by those with less expertise.

Reporting — What You Receive

Once we have relevant evidence uncovered, it can be exported in a variety of formats. We provide the evidence in your requested format(s) and provide a Verbal Report.

- Examples include MS Excel Workbooks, different load file formats for Relativity®, Concordance®, etc. or we can customize the export based on whatever the Review Tool Software requires (ie. lines, field delimiters, etc.)
- **Default:** Excel Workbook with extracted information in related worksheets, including links to attachments or native files.

  Optional: Written Report of Findings with Opinion

Vestige Digital Investigations

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com

Specialized Services for Mobile Devices

The Details

Vestige offers several specialized services in regard to cell phones and other mobile devices. These include:

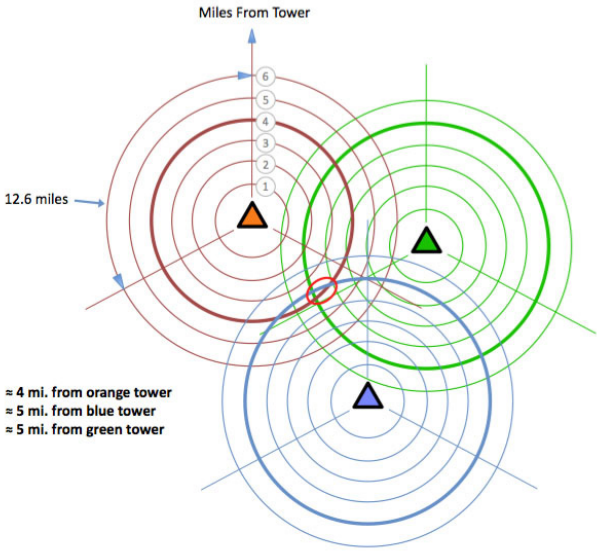
- **Location Triangulation and E-911 Services**
- **GPS - Global Positioning System Information from the Device**
- **CDR - Call Detail Records**
- **Spyware Checks**
- **Application Artifact Recovery**

Time is of the Essence!

Regardless of the type of Mobile Device Service you may need, time is of the essence! Whether the data is located with the Carrier or on a mobile device, if you wait too long, the data may no longer be available. Carriers only keep data for a limited period of time before purging it from their systems, so if the data is not requested soon enough, it may not be available at all. The same goes for cell phones, as these devices were not meant to keep an unlimited amount of information on them due to hardware limitations. Bringing Vestige in early on, even if it's just for a quick consultation, is very beneficial as we'll alert you to the important pieces of digital evidence in your matter, so you can make sure to preserve them before they're gone forever. Sometimes simply preserving the data up front, even if you don't know you'll need the analysis done in the end, keeps the costs low and saves you the headache of losing precious data that could help your case.

Triangulation Services

Mobile Device Triangulation, or localization, utilizes carrier records to pinpoint an area in which a cell phone was located during a given period of time. This is utilized by Law Enforcement in a variety of criminal matters, and at times, can be used improperly causing false information to be presented about an individual's whereabouts.



Vestige can not only review information produced by Law Enforcement to ensure the accuracy of their work, but also perform the work itself with mapping out where a particular mobile device was during a given period of time (if provided Carrier Records). Time is of the essence though, as these carrier records are only available for a limited amount of time.

GPS - Global Positioning System Services

Most mobile devices available today have GPS capabilities, which means location data could very well reside on the device. The data available is dependent on the device, application, and how they're used, although there may also be location information available via accounts the individual is utilizing as well.

Vestige has worked countless cases to determine a mobile device's location during a given period of time, and has done so utilizing our vast knowledge of mobile devices, application/accounts, and how and what is stored and available for analysis.

CDR - Call Detail Records

Call Detail Records contain information pertaining to phone calls, text messages, and data usage. Depending on the situation, these records can be utilized to help a client verify if a message was sent/received by an individual. Also, depending on the method used to send a message, the information might not appear on the Call Detail Records.

Utilizing Vestige's Expert Services, we can help you understand the differences in messages, what will and will not appear in the Call Detail Records, and help you navigate the waters to better help serve your client.

Spyware Checks

Vestige is equipped to perform Spyware Checks to determine if surveillance software is installed on a mobile device. Typically when spyware is installed it does a good job of obfuscating its presence; as such, deeper artifact analysis is required. Vestige forensic analysts are adept at identifying, documenting and removing installed spyware.

Application Artifact Recovery

Apps that are installed on a mobile device can take many forms and provide a wide range of actions — many of which happen behind the scenes. Our analysts are experts at testing and reverse engineering these applications to determine how they work, what artifacts are left behind and how those artifacts can be used to move your investigation forward.

Get Started with Vestige Today

Contact us today to learn how Vestige can partner with your organization for Expert Mobile Device Forensics and Specialized Services when in search of digital evidence, reporting, and/or testimony.

VESTIGE
Digital Investigations
TURNING DIGITAL EVIDENCE INTO INTELLIGENCE™

info@VestigeLtd.com | **800.314.4357** | www.VestigeLtd.com