ANALYSIS AND VALIDATION

1. VALIDATING FORENSICS DATA

Software validation is a part of the design validation for a finished device…considers software validation to be ‘confirmation by examination and provision of objective evidence that software specifications conform to user needs and intended uses, and that the particular requirements implemented through software can be consis- tently fulfilled.’ In practice, software validation activities may occur both during, as well as at the end of the software development life cycle to ensure that all requirements have been fulfilled. …the validation of software typically includes evidence that all software requirements have been implemented correctly and completely and are traceable to system requirements. A conclusion that software is validated is highly dependent upon comprehensive software testing, inspec- tions, analyses, and other verification tasks performed at each stage of the software development life cycle. data validation is the process of ensuring that a program operates on clean, correct and useful data. It uses routines, often called "[validation rules](https://en.wikipedia.org/wiki/Validation_rule)" "validation constraints" or "check routines", that check for correctness, meaningfulness, and security of data that are input to the system. The rules may be implemented through the automated facilities of a [data dictionary](https://en.wikipedia.org/wiki/Data_dictionary), or by the inclusion of explicit [application program](https://en.wikipedia.org/wiki/Application_program) validation logic. **data validation (data vetting, data cleaning)** The process of checking that data conforms to specification. It is usually the first process undertaken on [raw data](http://www.encyclopedia.com/doc/1O11-rawdata.html). The following are among the kinds of checks that may be carried out: number and type of characters in a [data item](http://www.encyclopedia.com/doc/1O11-dataitem.html); range of values of a data item; correctness of [check character](http://www.encyclopedia.com/doc/1O11-checkcharacter.html)(s); consistency between one data item and others in the same record; correctness of check totals for individual records; correctness of [batch controls](http://www.encyclopedia.com/doc/1O11-batchcontrol.html).

1.1 Validation methods

Allowed character checks Checks that ascertain that only expected characters are present in a field. For example a numeric field may only allow the digits 0-9, the decimal point and perhaps a minus sign or commas. A text field such as a personal name might disallow characters such as < and >, as they could be evidence of a markup-based security attack. An e-mail address might require at least one @ sign and various other structural details. Regular expressions are effective ways of implementing such checks. (See also data type checks below)Batch totals Checks for missing records. Numerical fields may be added together for all records in a batch. The batch total is entered and the computer checks that the total is correct, e.g., add the 'Total Cost' field of a number of transactions together.

Cardinality check Checks that record has a valid number of related records. For example if Contact record classified as a Customer it must have at least one associated Order (Cardinality > 0). If order does not exist for a "customer" record then it must be either changed to "seed" or the order must be created. This type of rule can be complicated by additional conditions. For example if contact record in Payroll database is marked as "former employee", then this record must not have any associated salary payments after the date on which employee left organization (Cardinality = 0).

Check digits Used for numerical data. An extra digit is added to a number which is calculated from the digits. The computer checks this calculation when data are entered. For example the last digit of an ISBN for a book is a check digit calculated modulus 10.[3]

Consistency checks Checks fields to ensure data in these fields corresponds, e.g., If Title = "Mr.", then Gender = "M".

Control totals This is a total done on one or more numeric fields which appears in every record. This is a meaningful total, e.g., add the total payment for a number of Customers.

Cross-system consistency checks Compares data in different systems to ensure it is consistent, e.g., The address for the customer with the same id is the same in both systems. The data may be represented differently in different systems and may need to be transformed to a common format to be compared, e.g., one system may store customer name in a single Name field as 'Doe, John Q', while another in three different fields: First\_Name (John), Last\_Name (Doe) and Middle\_Name (Quality); to compare the two, the validation engine would have to transform data from the second system to match the data from the first, for example, using SQL: Last\_Name || ', ' || First\_Name || substr(Middle\_Name, 1, 1) would convert the data from the second system to look like the data from the first 'Doe, John Q'

Data type checks Checks the data type of the input and give an error message if the input data does not match with the chosen data type, e.g., In an input box accepting numeric data, if the letter 'O' was typed instead of the number zero, an error message would appear.

File existence check Checks that a file with a specified name exists. This check is essential for programs that use file handling.

Format or picture check Checks that the data is in a specified format (template), e.g., dates have to be in the format DD/MM/YYYY. Regular expressions should be considered for this type of validation.

Hash totals This is just a batch total done on one or more numeric fields which appears in every record. This is a meaningless total, e.g., add the Telephone Numbers together for a number of Customers.

Limit check Unlike range checks, data are checked for one limit only, upper OR lower, e.g., data should not be greater than 2 (<=2).

Logic check Checks that an input does not yield a logical error, e.g., an input value should not be 0 when it will divide some other number somewhere in a program.

Presence check Checks that important data is actually present and have not been missed out, e.g., customers may be required to have their telephone numbers listed.

Range check Checks that the data is within a specified range of values, e.g., the month of a person's date of birth should lie between 1 and 12.

Referential integrity In modern Relational database values in two tables can be linked through foreign key and primary key. If values in the primary key field are not constrained by database internal mechanism,[4] then they should be validated. Validation of the foreign key field checks that referencing table must always refer to a valid row in the referenced table.[5]

Spelling and grammar check Looks for spelling and grammatical errors.

Uniqueness check Checks that each value is unique. This can be applied to several fields (i.e. Address, First Name, Last Name).

Table look up check A table look up check takes the entered data item and compares it to a valid list of entries that are stored in a database table.

## DATA HIDING

Data hiding is the process of making data difficult to find while also keeping it accessible for future use. "Obfuscation and encryption of data give an adversary the ability to limit identification and collection of evidence by investigators while allowing access and use to themselves."

Some of the more common forms of data hiding include encryption, [steganography](https://en.wikipedia.org/wiki/Steganography) and other various forms of hardware/software based data concealment. Each of the different data hiding methods makes digital forensic examinations difficult. When the different data hiding methods are combined, they can make a successful forensic investigation nearly impossible.

### Encryption

### One of the more commonly used techniques to defeat computer forensics is data encryption. In a presentation he gave on encryption and anti-forensic methodologies the Vice President of Secure Computing, Paul Henry, referred to [encryption](https://en.wikipedia.org/wiki/Encryption) as a "forensic expert's nightmare".[[6]](https://en.wikipedia.org/wiki/Anti-computer_forensics#cite_note-henry-6)

The majority of publicly available encryption programs allow the user to create virtual encrypted disks which can only be opened with a designated key. Through the use of modern encryption algorithms and various encryption techniques these programs make the data virtually impossible to read without the designated key.

File level encryption encrypts only the file contents. This leaves important information such as file name, size and timestamps unencrypted. Parts of the content of the file can be reconstructed from other locations, such as temporary files, swap file and deleted, unencrypted copies.

Most encryption programs have the ability to perform a number of additional functions that make digital forensic efforts increasingly difficult. Some of these functions include the use of a [keyfile](https://en.wikipedia.org/wiki/Keyfile), full-volume encryption, and [plausible deniability](https://en.wikipedia.org/wiki/Plausible_deniability). The widespread availability of software containing these functions has put the field of digital forensics at a great disadvantage.

Steganography

[Steganography](https://en.wikipedia.org/wiki/Steganography) is a technique where information or files are hidden within another file in an attempt to hide data by leaving it in plain sight. "Steganography produces dark data that is typically buried within light data (e.g., a non-perceptible digital watermark buried within a digital photograph)." Some experts have argued that the use of steganography techniques are not very widespread and therefore shouldn't be given a lot of thought. Most experts will agree that steganography has the capability of disrupting the forensic process when used correctly.

According to Jeffrey Carr, a 2007 edition of Technical Mujahid (a bi-monthly terrorist publication) outlined the importance of using a steganography program called Secrets of the Mujahideen. According to Carr, the program was touted as giving the user the capability to avoid detection by current [steganalysis](https://en.wikipedia.org/wiki/Steganalysis) programs. It did this through the use of steganography in conjunction with file compression.

### Other forms of data hiding

Other forms of data hiding involve the use of tools and techniques to hide data throughout various locations in a computer system. Some of these places can include "memory, slack space, hidden directories, bad blocks, alternate data streams, (and) hidden partitions."

One of the more well known tools that is often used for data hiding is called Slacker (part of the [Metasploit](https://en.wikipedia.org/wiki/Metasploit) framework). Slacker breaks up a file and places each piece of that file into the [slack space](https://en.wikipedia.org/wiki/Slack_space) of other files, thereby hiding it from the forensic examination software. Another data hiding technique involves the use of bad sectors. To perform this technique, the user changes a particular sector from good to bad and then data is placed onto that particular cluster. The belief is that forensic examination tools will see these clusters as bad and continue on without any examination of their contents.

## PERFORMING REMOTE ACQUISITION

In addition to the steady acquisition and live acquisition, there is also another type of acquisition, which is remote acquisition. Remote acquisition is done through a network connection and involves a client server type of architecture. In many cases, you install a client on a machine from which you want to retrieve the data. Remote acquisition is a form of live acquisition, especially because it requires that the computing device in form of a host or a host computer, is still up an running.

So the acquisition is only done while the computer is on. The current trend is that live and remote acquisitions are becoming more important and popular due to the encryption problem. Static acquisitions are now becoming more difficult, especially because the data is often encrypted when a computing device is turned off. So, what this means is. That by the time you're trying to do a static acquisition, it may be too late to retrieve the data out of a storage device.

# NETWORK FORENSICS

Network forensics is a sub-branch of [digital forensics](https://en.wikipedia.org/wiki/Digital_forensics) relating to the monitoring and analysis of [computer network](https://en.wikipedia.org/wiki/Computer_network) traffic for the purposes of information gathering, legal evidence, or [intrusion detection](https://en.wikipedia.org/wiki/Intrusion_detection). Unlike other areas of digital forensics, network investigations deal with volatile and dynamic information. Network traffic is transmitted and then lost, so network forensics is often a pro-active investigation.

* Network forensics generally has two uses. The first, relating to security, involves monitoring a network for anomalous traffic and identifying intrusions. An attacker might be able to erase all log files on a compromised host; network-based evidence might therefore be the only evidence available for forensic analysis.[[3]](https://en.wikipedia.org/wiki/Network_forensics#cite_note-3) The second form relates to law enforcement. In this case analysis of captured network traffic can include tasks such as reassembling transferred files, searching for keywords and parsing human communication such as emails or chat sessions. Network forensics is the capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. (The term, attributed to firewall expert Marcus Ranum, is borrowed from the legal and criminology fields where *forensics* pertains to the investigation of crimes.) According to Simson Garfinkel, author of several books on security, network forensics systems can be one of two kinds: *Catch-it-as-you-can" systems*, in which all [packet](http://searchnetworking.techtarget.com/definition/packet)s passing through a certain traffic point are captured and written to storage with analysis being done subsequently in batch mode. This approach requires large amounts of storage, usually involving a RAID system.
* *"Stop, look and listen" systems*, in which each packet is analyzed in a rudimentary way in memory and only certain information saved for future analysis. This approach requires less storage but may require a faster processor to keep up with incoming traffic.

Both approaches require significant storage and the need for occasional erasing of old data to make room for new. The [open source](http://searchenterpriselinux.techtarget.com/definition/open-source) programs *tcpdump* and *windump* as well as a number of commercial programs can be used for data capture and analysis.

One concern with the "catch-it-as-you-can" approach is one of privacy since all packet information (including user data) is captured. Internet service providers ([ISP](http://searchwindevelopment.techtarget.com/definition/ISP)s) are expressly forbidden by the Electronic Communications Privacy Act (ECPA) from eavesdropping or disclosing intercepted contents except with user permission, for limited operations monitoring, or under a court order. The U.S. FBI's [Carnivore](http://searchsecurity.techtarget.com/definition/Carnivore) is a controversial example of a network forensics tool.

1. EMAIL INVESTIGATION

When investigating email, we usually start with the piece of email itself and analyze the headers of the email. Since each SMTP server that handles a message adds lines on top of the header, we start at the top and work our way backward in time. Inconsistencies between the data that subsequent SMTP servers supposedly created can prove that the email in question is faked. Another investigation is that of the header contents itself. SMTP allows SMTP server ideosyncracies. If a message does not have these, then it is faked. If possible, one can obtain another email following supposedly the same path as the email under investigation and see whether these ideosyncratic lines have changed. While it is possible that the administrator of an SMTP node changed the behavior or even the routing, these changes tend to be far and in between. For example, in the following email that I sent to myself (with altered addresses), we find a large number of optinal lines that the hotmail server added, in particular the X-fields. Without these fields, the message did not originate through the bay area hotmail server.The Message-ID field is also highly characteristic. Notice that hotmail also includes the originating IP address. A simple check for this IP address might also prove that the message is a fake. (Though in fact, it is not.)

Return-path: <tschwarz@hotmail.com>  
Received: from MGW2.scu.edu [129.210.251.18]  
by gwcl-22.scu.edu; Wed, 28 Dec 2005 20:12:45 -0800  
Received: from hotmail.com (unverified [64.4.43.63]) by MGW2.scu.edu  
(Vircom SMTPRS 4.2.425.10) with ESMTP id <C0066471627@MGW2.scu.edu> for <tjschwarz@scu.edu>;  
Wed, 28 Dec 2005 20:12:44 -0800  
X-Modus-BlackList: 64.4.43.63=OK;tschwarz@hotmail.com=OK  
X-Modus-Trusted: 64.4.43.63=NO  
Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;  
Wed, 28 Dec 2005 20:12:44 -0800  
Message-ID: <BAY17-F13177DD86E6CA033897367C4290@phx.gbl>  
Received: from 129.210.18.34 by by17fd.bay17.hotmail.msn.com with HTTP;  
Thu, 29 Dec 2005 04:12:43 GMT  
X-Originating-IP: [129.210.18.34]  
X-Originating-Email: [tschwarz@hotmail.com]  
X-Sender: tschwarzsj@hotmail.com  
From: "Thomas Schwarz, S.J." <tschwarz@hotmail.com>  
To: tschwarz@scu.edu  
Bcc:   
Subject: Test  
Date: Thu, 29 Dec 2005 04:12:43 +0000  
Mime-Version: 1.0  
Content-Type: text/plain; charset=iso-8859-1; format=flowed  
X-OriginalArrivalTime: 29 Dec 2005 04:12:44.0119 (UTC) FILETIME=[1E30EE70:01C60C2E]

test

In general, it is impossible to prove that an email is genuine, but one can build a good case that it is genuine. Usually, spoofers are simply not that good. In a case where someone maintains that email appearing to originate from that some-one is faked, the date and the originating IP address could create a presumption that the email is not faked. But even in this case, the only thing one can deduce for sure is that the email originated from someone who could put a packet with that return address on the network.

As administrators get more concerned about fakemail, they put in access restrictions and also place warnings in headers, as the following example shows. (For Spam protection, I changed the email addresses used.)

De: <tschwarz@scu.edu>  
Enviado el: Wednesday, December 28, 2005 11:19:47 PM  
Ir al mensaje anterior | Ir al mensaje siguiente | Eliminar | Bandeja de entrada

Received: from CPSJ-EXCHANGE-1.calprov.org ([65.116.151.145]) by bay0-mc10-f12.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.211); Wed, 28 Dec 2005 15:19:15 -0800  
Received: from endor.engr.scu.edu ([129.210.16.1]) by CPSJ-EXCHANGE-1.calprov.org with Microsoft SMTPSVC(5.0.2195.6713); Wed, 28 Dec 2005 15:19:14 -0800  
Received: from bobadilla.engr.scu.edu (bobadilla.engr.scu.edu [129.210.18.34])by endor.engr.scu.edu (8.13.5/8.13.5) with SMTP id jBSNA9h7023258for tschwarzsj@calprov.org; Wed, 28 Dec 2005 15:19:47 -0800  
X-Message-Info: JGTYoYF78jFYzNJ5n6DdPGvy0zsH8v3C7lhJalOirZc=  
X-Authentication-Warning: endor.engr.scu.edu: bobadilla.engr.scu.edu [129.210.18.34] didn't use HELO protocol  
Return-Path: tschwarz@scu.edu  
X-OriginalArrivalTime: 28 Dec 2005 23:19:14.0587 (UTC) FILETIME=[1E1796B0:01C60C05]

## Analysis of source machine

Besides analyzing the email message itself, analyzing the machine from which an email might have originated my yield some proof. We will see this when we come to discuss hard drive evidence.

## Analysis of Logs

Even more fundamental and important than these methods are the logs that SMTP servers (and some email programs) maintain. Law enforcement has here an advantage over private investigators because they can subpoena ISP records. Unfortunately, ISP servers tend to not store the log data for a long time. It therefore makes sense to warn an ISP about a coming subpoena so that they can safe-guard the log entry. A lucky investigator might be able to trace back a message through SMTP servers to the first one that handled the message. If this server belonged to an ISP, then information from RADIUS logs might give the name of the subscriber. Otherwise, the investigator might connect the IP of the originating machine to a suspect. In case of criminal enterprises such as spammers, fraudsters, phishers, etc. this investigation will be very difficult because the originating message is often from a hacked machine that is controlled by another hacked machine. The investigator needs to spend considerable resources and talents to follow such a trail through various jurisdictions. It is possible to even set up a website in a way that cannot be traced to a person, for example using untraceable or stolen credit cards.

Here is an example of a typical smtp log from endor. Chris Tracy - a truly talented and helpful systems administrator - sent me fakemail:

Dec 31 18:26:15 endor sendmail[30597]: k012OV1i030597: from=evil@evil.com, size=147, class=0, nrcpts=1, msgid=<200601010225.k012OV1i030597@endor.engr.scu.edu>, proto=SMTP, daemon=MTA, relay=c-24-12-227-211.hsd1.il.comcast.net [24.12.227.211]  
Dec 31 18:26:15 endor spamd[28512]: spamd: connection from localhost [127.0.0.1] at port 42865   
Dec 31 18:26:15 endor spamd[28512]: spamd: setuid to tschwarz succeeded   
Dec 31 18:26:15 endor spamd[28512]: spamd: processing message <200601010225.k012OV1i030597@endor.engr.scu.edu> for tschwarz:1875   
Dec 31 18:26:15 endor spamd[28512]: spamd: clean message (4.6/5.0) for tschwarz:1875 in 0.2 seconds, 525 bytes.   
Dec 31 18:26:15 endor spamd[28512]: spamd: result: . 4 - MSGID\_FROM\_MTA\_ID,RCVD\_IN\_NJABL\_DUL,RCVD\_IN\_SORBS\_DUL scantime=0.2,size=525,user=tschwarz,uid=1875,required\_score=5.0,rhost=localhost,raddr=127.0.0.1,rport=42865,mid=<200601010225.k012OV1i030597@endor.engr.scu.edu>,autolearn=no   
Dec 31 18:26:15 endor spamd[21352]: prefork: child states: II   
Dec 31 18:26:15 endor sendmail[30726]: k012OV1i030597: to=tschwarz@engr.scu.edu, delay=00:01:02, xdelay=00:00:00, mailer=local, pri=30464, dsn=2.0.0, stat=Sent

# Information Technology Email Investigation Guidelines

This document describes the Information Technology policies and procedures related to handling of emails related to transgressions of law or of questionable content.

Pursuant to the Computing Access Agreement, Information Technology does not monitor email content or email accounts. Minimal, short-lived logging is done on the system for performance and operational use showing messages queued for delivery or system load. Email account contents may be accessed for technical reasons (assisting users or system troubleshooting) without the knowledge of the owner.

Information Technology does not officially investigate or trace emails unless directed or requested to do so from College authority offices like Campus Police, Human Resources, or Student Life. In general all issues with objectionable email of a harassing or illegal nature must be routed through one of these authorities, typically Campus Police.

Members of the College community who contact Information Technology about this issue are directed to retain the message in its original form within their account and contact Campus Police. Campus Police then typically makes an incident report and determines whether the incident warrants action by Information Technology.

The majority of information used for tracing email is extracted from the message header. The header format is a documented standard and is constructed as a product of message delivery by all involved delivery agents (from the initiating client through to the final accepting server). To some degree this information can be used to verify the legitimacy of a message. To a lesser degree this information can be used to trace the message origin. However, mail clients are easily reconfigured to obscure the identity of the sender, semi-anonymous email agents (like Yahoo! and Hotmail) are widely used, and determined individuals can certainly add enough invalid header information to make determinations very difficult.

Emails originating from The College of New Jersey systems are typically easier to trace than messages originating from off-campus sites (this includes Yahoo! and Hotmail as well as emails from other personal or commercial systems).

Information Technology NTS staff will review the message headers to determine origin, destination, or ownership of the message as required. College UNIX account contents may be reviewed to determine what roles investigation-specified users and potential suspects play in the investigation.

In the event that an email must be traced through an off-campus system, Information Technology must request the assistance of other agencies. For email originating from or destined to other sites, respective system administrators at those sites may be contacted for assistance. Information Technology staff often contact system administrators at these sites and may be able to acquire the necessary information. Certain commercial email systems require legal documents before they will release account information. For these services (like AOL, Yahoo! or Hotmail) a court order or subpoena may be required to obtain the user identity and/or message contents of the suspect account. Campus Police handles acquiring legally binding documents and may acquire those documents and possibly the related account information before contacting Information Technology.

Information Technology NTS staff maintain close contact with Campus Police (or the appropriate investigating agency) throughout the division’s action in the investigation. Information retrieved by Information Technology is provided to the investigators with explanation as required.

In most cases the action taken against an individual determined guilty of a violation of the Computing Access Agreement is determined by College authorities. The typical action is to lock the user account for a specified period of time.

1. CELL PHONE AND MOBILE DEVICE FORENSICS

ln the information age, every byte of data matters. Cell phones are capable of storing a wealth of personal information, often intentionally, and sometimes unintentionally. This holds true for almost all mobile devices, such as PDAs and iPhones as well. **Cell phone forensic experts** specialize in the [forensic retrieval of data from cell phones](http://en.wikipedia.org/wiki/Digital_forensics) and other mobile devices in a manner that preserves the evidence under forensically acceptable conditions, ensuring that it is court-admissible. A **cell phone forensic** investigation includes possible full data retrieval dependent upon the cell phone or PDA model. The cell phone and PDA forensic engineers at Kessler International will conduct a thorough examination of the data found on the cell phone’s SIM/[USIM](http://en.wikipedia.org/wiki/Subscriber_identity_module#USIM), the cell phone body itself, and any optional memory cards. Some of the kinds of data that may be retrieved and examined during a cell phone forensic investigation, even after being deleted, include:

• Call times;dialed and received calls, and call durations  
• Text messages recovery of SMS message recovery  
• Contact names & phone numbers  
• Address book entries; residential addresses and email addresses  
• Photos & graphics  
• Videos

Law enforcement officials and legal firms realize the importance of evidence contained on cell phones and other mobile devices, and how it can greatly affect the outcome of a trial. Whether working to document evidence of “[white collar crime](http://en.wikipedia.org/wiki/White-collar_crime)” or tasked by law enforcement to extract data for a criminal trial, the integrity of the firm selected for **cell phone forensics** is as important as the integrity of the data recovered. More and more court cases are being won with the proper submittal of electronic evidence, so it’s imperative that the **cell phone forensic investigator** understands the legal issues and imperatives surrounding electronic evidence gathering.

**Why and when to call Kessler International**

* Parents should contact us if they suspect that their child is misusing the device or being harassed by someone contacting or photographing them without their consent. Kessler will discreetly investigate and, if necessary, assist law enforcement by providing court-admissible data to corroborate legal claims.
* Kessler International can perform **mobile phone forensics** if an individual suspects his or her spouse of cheating. Data such as placed & received calls and phone call times, text messages, photos and other incriminating evidence can be retrieved from the spouse’s cell phone or mobile device.
* Companies and corporations should contact us to perform **cell phone forensics** if they suspect espionage by a competitor or disgruntled employee.
* Business owners who distribute cell phones to their executives and sales staff may contact us to perform **cell phone forensics** to determine if these devices are being inappropriately used to view and/or download porn, or defying restricted Internet usage company policies.
* Individuals may contact Kessler International if they suspect they have been the victim of e-stalking, the subject of inappropriate and non-consensual digital photography and other forms of digital harassment.

Kessler International’s forensic cell/mobile phone, PDA, and computer investigations are discreet, controlled, thorough and fully documented. Our professional staff is both certified and highly-experienced in their respective forensic disciplines. Forensic cell phone audits by Kessler International’s professionals yield superior results as our techniques and procedures far exceed those used in routine data recovery investigations. Our forensic examinations will document the evidence that the client needs and the respective circumstance requires. For all your **cell phone forensic** investigative needs, Kessler International is the company to call.

**A Leader in the Field of Cell Phone Forensics**

For over 25 years, Kessler International has been a leader in the field of digital forensics. The **cell phone forensic** engineers at Kessler International are fully trained in proper evidence handling and litigation support services. Our broad knowledge of these complex electronic systems combined with extensive legal training demonstrates the high standards Kessler International maintains. These standards are critical to providing the data that support an accurate presentation of the facts. Kessler has built its rock-solid reputation on it. Remember, when the bar is set high, Kessler International is the company to call.

The explosive growth in the availability and use of cell phones and other mobile devices — coupled with the expanded capabilities of these devices — has made this area of digital forensics increasingly important. For many years now, cell phones have been a recorder of information, often related to criminal or other nefarious behaviors, not to mention often being the instrument — and, occasionally, the target — of that behavior. Mobile devices contain a plethora of data, including contact lists, phone and Internet browsing history, text and multimedia messages, e-mail, photographs and videos, geolocation information, and much more. Indeed, smartphones are mobile Internet terminals and contain more probative information per byte examined than most computers.

Examination and analysis of cell phones requires a very different forensic process than that applied to computers. Every step — from seizure to preservation to transport to the exam itself — requires processes and tools to ensure minimal alteration to the original evidence. The complexity in performing a thorough exam of a mobile device and the analysis of the contents should not be underestimated; while computers today largely employ only two or three different operating systems (depending upon how you count), there are at least six major operating systems used on mobile phones that are still in circulation.

Gary has been conducting mobile phone forensic examinations since 2006. Most of this work has been on behalf of the local, state, and federal law enforcement community in Vermont and Florida, including the U.S. Attorney's Office and Internet Crimes Against Children (ICAC) Task Force. Gary has also examined mobile devices on behalf of clients in civil litigations. Gary has acted as an expert witness in several federal criminal cases, as well as numerous civil matters.

Gary is also a frequent speaker at conferences about the process of mobile device forensics. He has also conducted many training courses on mobile phone and smartphone forensics.

Gary Kessler Associates is capable of performing logical and physical analysis of most types of cell phones, tablets, GPS devices, and other mobile devices. In conjunction with partners, GKA is able to provide a broad range of services, including chip-off examinations and analysis of call detail records and cell tower information. **Mobile device forensics** is a branch of [digital forensics](https://en.wikipedia.org/wiki/Digital_forensics) relating to recovery of [digital evidence](https://en.wikipedia.org/wiki/Digital_evidence) or data from a [mobile device](https://en.wikipedia.org/wiki/Mobile_device) under [forensically](https://en.wikipedia.org/wiki/Forensic) sound conditions. The phrase *mobile device* usually refers to [mobile phones](https://en.wikipedia.org/wiki/Mobile_phone); however, it can also relate to any digital device that has both internal memory and [communication](https://en.wikipedia.org/wiki/Telecommunication) ability, including [PDA](https://en.wikipedia.org/wiki/PDA) devices, [GPS](https://en.wikipedia.org/wiki/GPS) devices and [tablet computers](https://en.wikipedia.org/wiki/Tablet_computers).

The use of phones in crime was widely recognised for some years, but the forensic study of mobile devices is a relatively new field, dating from the early 2000s. A proliferation of phones (particularly [smartphones](https://en.wikipedia.org/wiki/Smartphone)) on the consumer market caused a demand for forensic examination of the devices, which could not be met by existing [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics) techniques.[[1]](https://en.wikipedia.org/wiki/Mobile_device_forensics#cite_note-casey-1)

Mobile devices can be used to save several types of personal information such as contacts, photos, calendars and notes, [SMS](https://en.wikipedia.org/wiki/SMS) and [MMS](https://en.wikipedia.org/wiki/Multimedia_messaging_service) messages. Smartphones may additionally contain video, email, web browsing information, location information, and social networking messages and contacts.

There is growing need for mobile forensics due to several reasons and some of the prominent reasons are:

* Use of mobile phones to store and transmit personal and corporate information
* Use of mobile phones in online transactions
* Law enforcement, criminals and mobile phone devices[[2]](https://en.wikipedia.org/wiki/Mobile_device_forensics#cite_note-Rizwan-2)

Mobile device forensics can be particularly challenging on a number of levels:[[3]](https://en.wikipedia.org/wiki/Mobile_device_forensics" \l "cite_note-Murphy-3)

Evidential and technical challenges exist. for example, cell site analysis following from the use of a mobile phone usage coverage, is not an exact science. Consequently, whilst it is possible to determine roughly the cell site zone from which a call was made or received, it is not yet possible to say with any degree of certainty, that a mobile phone call emanated from a specific location e.g. a residential address.

* To remain competitive, original equipment manufacturers frequently change [mobile phone form factors](https://en.wikipedia.org/wiki/Mobile_phone_form_factors), [operating system](https://en.wikipedia.org/wiki/Operating_system) file structures, data storage, services, peripherals, and even pin connectors and cables. As a result, forensic examiners must use a different forensic process compared to [computer forensics](https://en.wikipedia.org/wiki/Computer_forensics).
*  Storage capacity continues to grow thanks to demand for more powerful "mini computer" type devices.[[4]](https://en.wikipedia.org/wiki/Mobile_device_forensics#cite_note-4)
*  Not only the types of data but also the way mobile devices are used constantly evolve.
*  Hibernation behaviour in which processes are suspended when the device is powered off or idle but at the same time, remaining active.