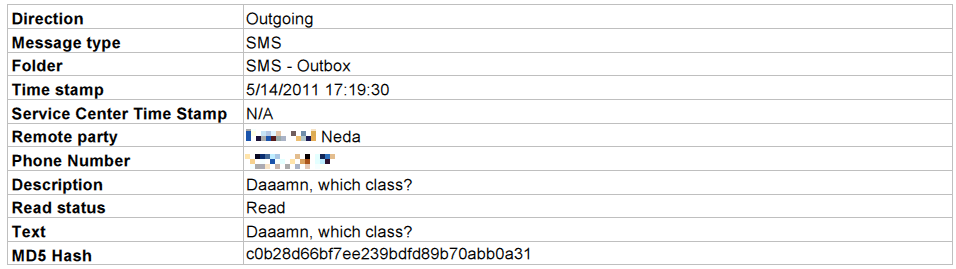
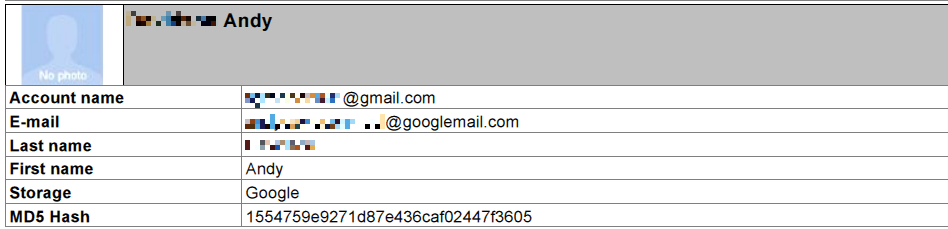
# **Cell Phone Forensics / Mobile Device Forensics**



[Cell Phone](https://evidencesolutions.com/web/ESI-Services/cell-phone-carrier-forensics-cell-phone-expert-witness.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) Forensics / [Mobile Device](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device: A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered.  A handheld computing device has an operating system (OS), and can run various types of application software, known as \“apps\”. Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) Forensics is the recovery of digital evidence, or data, from a [Cell Phone](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) using forensically sound methods. The term [Mobile Device](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device: A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered.  A handheld computing device has an operating system (OS), and can run various types of application software, known as \“apps\”. Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) usually refers to Smart Phones. However, it can also relate to other digital devices that have both internal memory and communication ability. These devices include Personal Digital Assistants (PDA) devices, [Global Positioning System (GPS)](https://evidencesolutions.com/web/ESI-Definitions/gps-definition.html" \o "GPS:  Global Positioning System. A U.S. Government-based system which utilizes satellite technology to provide reliable position, navigation and timing services on a continuous basis for any place on the planet Earth." \t "https://evidencesolutions.com/web/ESI-Services/_blank)devices and tablet computers such as iPad, smartphones and Galaxy Tablets.

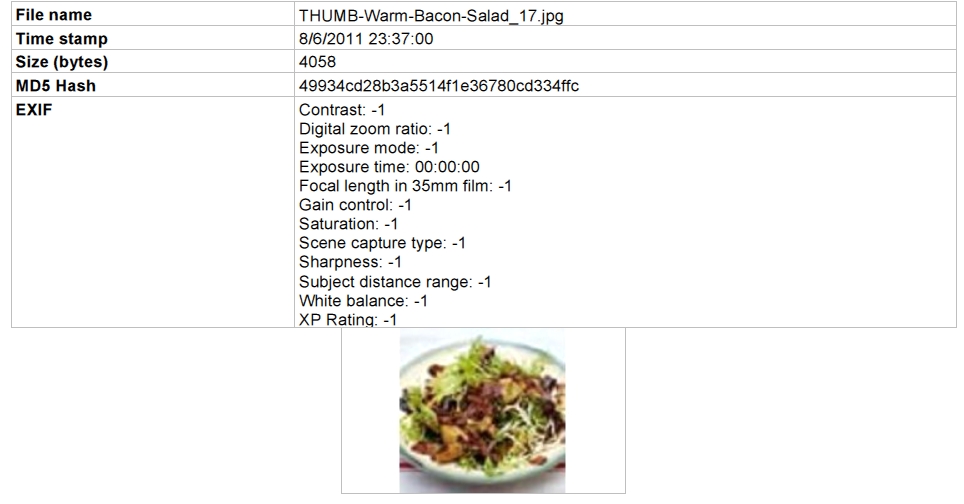
Mobile devices have the ability to store several types of personal information such as contacts, photos, calendars, notes, iMessage, [Short Message Service (SMS) Text Messages](https://evidencesolutions.com/web/ESI-Definitions/sms-or-short-message-service-definition.html" \o "SMS or Short Message Service:  Is a text messaging protocol generally used on Cell Phones. Most SMS messages are sent between two mobile devices ( aka mobile-to-mobile ). The SMS protocol also supports the exchange of messages between computers, websites, and other devices. SMS messages are limited to 160 characters per message. The protocol was originally part of the Global System for Mobile Communications (GSM) standards which were published in 1985." \t "https://evidencesolutions.com/web/ESI-Services/_blank) and [Multimedia Message Service (MMS) messages](https://evidencesolutions.com/web/ESI-Definitions/mms-or-multimedia-messaging-service-definition.html" \o "MMS or Multimedia Messaging Service:  Is a standard way to send messages which include multimedia content between Cell Phones. It extends the core SMS (Short Message Service) capability to allow the sending of photographs, videos, music, etc." \t "https://evidencesolutions.com/web/ESI-Services/_blank). In addition, more sophisticated [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank)commonly referred to as Smart Phones or Smart Cell Phones may also contain location information, videos, email, web browsing history and content, as well as Social Network, such as Facebook and LinkedIn, messages and contacts. Some [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) are also able to report the history of the cellular towers they were attached to when a call was made or a Text Message was sent.

[](https://evidencesolutions.com/web/Read-/-View-More-Pages/cell-phone-forensics-mobile-device-forensics-images1.html#cellphonesms)Sample SMS Message Extracted Using Cell Phone Forensics

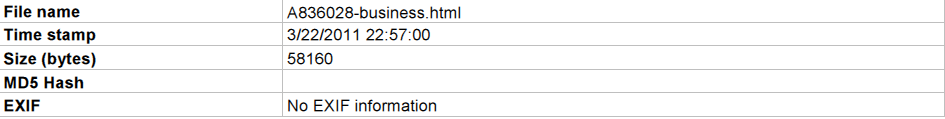
[](https://evidencesolutions.com/web/Read-/-View-More-Pages/cell-phone-forensics-mobile-device-forensics-images1.html#cellphonecontact)Sample Contact Information Extracted Using Cell Phone Forensics

The majority of [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) used in today’s society provide some ability to load additional applications, store and process personal and sensitive information independently of a desktop or notebook computer. Some applications synchronize data either to the Internet or to a local computer. As [Cell Phone](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) technology evolves, the capabilities of [Mobile Devices](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) continues to improve rapidly. When [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) or other [Mobile Devices](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) are involved in a crime or other incident, the device(s) are able to tell a significant story about what was going on with the user at the time, if the information is property captured.

[Mobile Devices](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) usually have a [Digital Camera](https://evidencesolutions.com/web/ESI-Definitions/digital-camera-definition.html" \o "Digital Camera  A camera that stores still or moving pictures in a digital format (TIFF, JPEG, MP4, etc.)." \t "https://evidencesolutions.com/web/ESI-Services/_blank) built in. Digital Photos have information embedded in them including [GPS](https://evidencesolutions.com/web/ESI-Definitions/gps-definition.html" \o "GPS:  Global Positioning System. A U.S. Government-based system which utilizes satellite technology to provide reliable position, navigation and timing services on a continuous basis for any place on the planet Earth." \t "https://evidencesolutions.com/web/ESI-Services/_blank) coordinates that can also indicate where the photo was taken.

Sample Photo Extracted Using Cell Phone Forensics

[Cell Phone](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) forensics can be particularly challenging as each device is unique and has a unique set of software installed. In addition, the storage which may be added to the device, usually in the form of an SD card, may further complicate the analysis process. This is just one reason it is critical to have an educated and trained cell phone expert involved.

[](https://evidencesolutions.com/web/Read-/-View-More-Pages/cell-phone-forensics-mobile-device-forensics-images1.html#cellphonefile)  
Sample File Information Extracted Using Cell Phone Forensics

When examining [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank), it is normal protocol to obtain the Cell Phone Carrier records. [Cell Phone Carrier Forensics](https://evidencesolutions.com/web/ESI-Services/cell-phone-carrier-forensics-cell-phone-expert-witness.html" \o "Cell Phone Carrier Forensics: It is a normal protocol to obtain Cell Phone Carrier Records when examining Cell Phones. These records can validate what was found on the Cell Phone as well as provide additional information the carrier may have which many not be on the phone. Standing alone, Cell Phone Carrier Records document calls, SMS text messages as well as data usage for webbrowsing and applications (apps)." \t "https://evidencesolutions.com/web/ESI-Services/_blank) examines records that may validate what was found on the [Cell Phones](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank) as well as information the carrier has which many not be on the phone. This information usually includes:

* Whether the call was originated by the [Cell Phone](https://evidencesolutions.com/web/ESI-Definitions/cell-phone-mobile-phone-definition.html" \o "Cell Phone, Mobile Phone  An electronic device used for full duplex two-way radio communications over a network of towers known as cell sites. Low-end or entry level cell phones are often referred to as ‘basic cell phones’. These are primarily used to make and receive telephone calls and send SMS messages. The device may have other functions, such as cameras, but in general are specifically communications devices. The more sophisticated ‘smartphones’ offer all of the features which are part of the ‘basic cell phone’, plus advanced computing, camera, music, Internet browsing, GPS navigation and many other applications." \t "https://evidencesolutions.com/web/ESI-Services/_blank).
* The quantity of data downloaded
* Text messaging history such as date and time of the text message as well as the phone numbers which were sending and receiving [Short Message Service (SMS) Text Messages](https://evidencesolutions.com/web/ESI-Definitions/sms-or-short-message-service-definition.html" \o "SMS or Short Message Service:  Is a text messaging protocol generally used on Cell Phones. Most SMS messages are sent between two mobile devices ( aka mobile-to-mobile ). The SMS protocol also supports the exchange of messages between computers, websites, and other devices. SMS messages are limited to 160 characters per message. The protocol was originally part of the Global System for Mobile Communications (GSM) standards which were published in 1985." \t "https://evidencesolutions.com/web/ESI-Services/_blank).
* Plan code (M2M - Mobile to Mobile, for instance )
* Cellular tower number and [GPS](https://evidencesolutions.com/web/ESI-Definitions/gps-definition.html" \o "GPS:  Global Positioning System. A U.S. Government-based system which utilizes satellite technology to provide reliable position, navigation and timing services on a continuous basis for any place on the planet Earth." \t "https://evidencesolutions.com/web/ESI-Services/_blank) location for the cellular tower(s) used for the phone call, text message or data exchange.

For Phone calls the carrier should give you additional information including:

* Connection date
* Connection time
* Seizure time
* Originating phone number
* Originating IMEI or MEID ( cell phone serial number )
* Originating IMSI ( SIM Serial Number )
* Terminating Phone number
* Elapsed time or call duration
* Number dialed

For Text or [SMS Messages](https://evidencesolutions.com/web/ESI-Definitions/sms-or-short-message-service-definition.html" \o "SMS or Short Message Service:  Is a text messaging protocol generally used on Cell Phones. Most SMS messages are sent between two mobile devices ( aka mobile-to-mobile ). The SMS protocol also supports the exchange of messages between computers, websites, and other devices. SMS messages are limited to 160 characters per message. The protocol was originally part of the Global System for Mobile Communications (GSM) standards which were published in 1985." \t "https://evidencesolutions.com/web/ESI-Services/_blank) the cell phone company should also provide:

* Originating phone number
* Originating IMEI or MEID ( cell phone serial number )
* Originating IMSI ( SIM Serial Number )
* Terminating Phone number

In addition to the [Mobile Device](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) and Cellular Carrier records, archives and backups of the data contained in the phone may be found either stored on the Internet or on a local computer.  Archives and backups may contain data which was deleted between the time of the backup and when the phone was examined.

It is important, when investigating an incident, to get possession of the cell phone and to capture its data early in the investigation - we call this “Rapid Seize and Freeze”.  
  
Don’t wait months, weeks or even days hoping the data is still on the [Mobile Device](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank). Generally, the sooner the data on the Smartphone or [Mobile Device](https://evidencesolutions.com/web/ESI-Definitions/mobile-device-definition.html" \o "Mobile Device:  A Mobile Device (aka a handheld device, handheld computer) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard. Mobile Devices are usually battery powered. A handheld computing device has an operating system (OS), and can run various types of application software, known as \"apps\". Most handheld devices are also equipped with Wi-Fi, Bluetooth and GPS. They typically connect to the internet via cell phone signal or Wi-Fi. Generally, these devices include: a camera, media player, calendar, task management, email clients, clocks & alarms, and an Internet Browser." \t "https://evidencesolutions.com/web/ESI-Services/_blank) is captured, the better.

Call our Cell Phone / Mobile Device Forensics Experts at: ****866-795-7166**** for a free consultantion. We can help you with preservation letters, interrogatories and requests for production.

Electronic Evidence in PLAIN English.

[Like Evidence Solutions - Electronic Evidence on Facebook](http://facebook.com/EvidenceSolutions" \o "Like Evidence Solutions Electronic Evidence Expert Witnesses on Facebook" \t "https://evidencesolutions.com/web/ESI-Services/_blank)

[Follow Evidence Solutions - Digital Evidence Division on LinkedIn](http://www.linkedin.com/company/evidence-solutions-inc." \o "Follow Evidence Solutions - Electronic Evidence Experts on LinkedIn." \t "https://evidencesolutions.com/web/ESI-Services/_blank)

[Circle Evidence Solutions - Digital Evidence Division on Google+](https://www.google.com/+EvidenceSolutions" \o "Add Evidence Solutions Electronic Evidence Division to a Google+ Circle" \t "https://evidencesolutions.com/web/ESI-Services/_blank)

[Google+ Author](http://google.com/+ScottGreene" \o "Scott Greene's Google Plus Profile" \t "https://evidencesolutions.com/web/ESI-Services/_blank)

[Google+ Publisher](https://plus.google.com/110509384799119517070?rel=publisher" \o "Evidence Solutions, Inc.'s Electronic Evidence Google Plus Page" \t "https://evidencesolutions.com/web/ESI-Services/_blank)

## ***Computer Ethics***

Computer ethics deals with the procedures, values and practices that govern the process of consuming computing technology and its related disciplines without damaging or violating the moral values and beliefs of any individual, organization or entity.  
  
Computer ethics is a concept in ethics that addresses the ethical issues and constraints that arise from the use of computers, and how they can be mitigated or prevented.

## ***Computer Ethics***

Computer ethics primarily enforces the ethical implementation and use of computing resources. It includes methods and procedures to avoid infringing copyrights, trademarks and the unauthorized distribution of digital content. Computer ethics also entails the behavior and approach of a human operator, workplace ethics and compliance with the ethical standards that surround computer use.  
  
The core issues surrounding computer ethics are based on the scenarios arising from the use of the Internet, such as Internet privacy, the publication of copyrighted content and user interaction with websites, software and related services.

**Computer ethics** is a part of [practical philosophy](https://en.wikipedia.org/wiki/Practical_philosophy" \o "Practical philosophy) concerned with how computing professionals should make decisions regarding professional and social conduct.[[1]](https://en.wikipedia.org/wiki/Computer_ethics" \l "cite_note-BynumVeryShort-1) Margaret Anne Pierce, a professor in the Department of Mathematics and Computers at Georgia Southern University has categorized the ethical decisions related to computer technology and usage into three primary influences:

1. The individual's own personal code.
2. Any informal code of ethical conduct that exists in the work place.
3. Exposure to formal codes of ethics.[[2]](https://en.wikipedia.org/wiki/Computer_ethics" \l "cite_note-2)

## **What does *Application Program* mean?**

An application program is a comprehensive, self-contained program that performs a particular function directly for the user. Among many others, application programs include:

* Email
* Web browsers
* Games
* Word processors
* Enterprise software
* Accounting software
* Graphics software
* Media players
* Database management

Because every program has a particular application for the end user, the term "application" is used. For instance, a word processor can help the user create an article, whereas a game application can be used for entertainment.

An application program is also known as an application or application software.

## ***Application Program***

Application software and system software are the two major types of software available. System software manages the internal operation of a computer, mainly via an operating system (OS). It manages peripherals like storage devices, printers and monitors as well. On the contrary, application software or an application program guides the computer to carry out instructions provided by the user.   
  
System software includes programs running in the background, which enable application programs to function. System software programs include compilers, assemblers, file management tools as well as the OS itself. Application programs function on top of the system software as the system software is built from "low-level" programs. System software is automatically installed during the OS installation. However, users have the option to select which application programs are installed on their systems.  
  
Some examples of application programs include:

* Application suite: Includes various applications packaged together
* Enterprise software: Addresses the data flow and process requirements of an organization, covering entire departments
* Information worker software: Permits users to create and administer information
* Content access software: Used mainly to gain access to content without editing
* Media development software: Creates electronic and print media
* Educational software: Includes content and/or features intended for students or educators
* Product engineering software: Develops software and hardware products

**Intellectual property** (IP) is any intangible asset that is created from an original thought, such as an idea, name, content, design, invention or digital media. Intellectual property rights (IPR) refer to the rights of IP owners and authors.

IP is divided into two categories: industrial property and copyright.

Industrial property covers:

* Patents (inventions): Require public registration and provide up to 20 years of protection against any unauthorized use, likeness and unfair competition.
* Industrial design: Protects creations that define or describe a product, including trademarks and commercial names and logos.
* Geographical source indications

Copyright protects rights related to literary and artistic creations, including:

* Art and literary works: Books, film, sound recordings, software, designs
* Performances
* Radio and TV broadcasters
* Technology-based works, such as computer programs and databases

Copyright law protects IP owners against unauthorized use or replication. Although copyright registration is not required, it is recommended to ensure formalized IP documentation.

The International Convention for the Protection of Literary and Artistic Works (Berne Convention, Berne or Bern) is an international copyright agreement that originated in Berne, Switzerland in the late 19th century. Berne governance requires that Berne Union members, or signatories, provide automatic protection for any work originally published in any Berne Union country, as well as any unpublished work of an author in other Union countries.

**Need for cyber Law**

* Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.
* Cyber law is vital because it touches almost all aspects of transactions and behavior on and concerning the Internet, the World Wide Web and Cyberspace. Primarily it may seem that Cyber laws is a very technical field and that it does not have any attitude to most activities in Cyberspace. But the actual fact is that nothing could be further than the truth. Whether we realist it or not, every work and every reaction in Cyberspace has some legal and Cyber legal perspectives.
* India introduced the law recently and every law needs some time to mature and grow. It was understood that over a period of occasion it will produce and further amendments will be bring to make it well-matched with the International standards. It is significant to realize that we need “qualitative law” and not “quantitative laws”.
* Such crimes may threaten a nation’s security and financial health. Issues surrounding this type of crime has become high-profile, mainly those surrounding cracking, copyright infringement. There are problems of privacy when private information is lost or intercepted, lawfully or otherwise.
* Cyber crimes can involve criminal activities that are traditional in nature, such as fraud, forgery, theft, mischief and defamation all of which are subject to the Indian Penal Code. The abuse of computers has also given birth to a range of new age crimes that are addressed by the Information Technology Act, 200.

# **computer forensics (cyber forensics)**

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.

Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

**Computer forensics** (also known as **computer forensic science**) is a branch of [digital forensic science](https://en.wikipedia.org/wiki/Digital_forensics" \o "Digital forensics) pertaining to evidence found in computers and digital [storage media](https://en.wikipedia.org/wiki/Storage_media" \o "Storage media). The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of [computer crime](https://en.wikipedia.org/wiki/Computer_crime" \o "Computer crime), computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to [data recovery](https://en.wikipedia.org/wiki/Data_recovery" \o "Data recovery), but with additional guidelines and practices designed to create a legal [audit trail](https://en.wikipedia.org/wiki/Audit_trail" \o "Audit trail).

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European [court systems](https://en.wikipedia.org/wiki/Court_system" \o "Court system).

### Jurisprudence of Indian Cyber Law

The primary source of cyber law in India is the **Information Technology Act, 2000** (IT Act) which came into force on 17 October 2000.  
  
The primary purpose of the Act is to provide legal recognition to electronic commerce and to facilitate filing of electronic records with the Government. The IT Act also penalizes various cyber crimes and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).  
  
An Executive Order dated 12 September 2002 contained instructions relating to provisions of the Act with regard to protected systems and application for the issue of a Digital Signature Certificate.  
  
Minor errors in the Act were rectified by the Information Technology (Removal of Difficulties) Order, 2002 which was passed on 19 September 2002.  
  
The IT Act was amended by the **Negotiable Instruments (Amendments and Miscellaneous Provisions) Act, 2002**. This introduced the concept of electronic cheques and truncated cheques.  
  
**Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004** has provided the necessary legal framework for filing of documents with the Government as well as issue of licenses by the Government. It also provides for payment and receipt of fees in relation to the Government bodies.  
  
On the same day, the **Information Technology (Certifying Authorities) Rules, 2000** also came into force. These rules prescribe the eligibility, appointment and working of Certifying Authorities (CAs). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.  
  
**Information Technology (Certifying Authority) Regulations, 2001** came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA. Two important guidelines relating to CAs were issued. The first are the Guidelines for submission of application for license to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9 July 2001.  
  
Next were the Guidelines for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in the National Repository of Digital Certificates. These were issued on 16 December 2002.  
  
The **Cyber Regulations Appellate Tribunal (Procedure) Rules, 2000** also came into force on 17 October 2000. These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.  
  
The Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.  
  
Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.  
  
On 17 March 2003, the **Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules, 2003**were passed. These rules prescribe the qualifications required for Adjudicating Officers. Their chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.  
  
The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the public interest litigation filed by students of Asian School of Cyber Laws (ASCL).  
  
The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the IT Act had come into force. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for speedy appointment of Adjudicating officers.  
  
The Bombay High Court, in its order dated 9 October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon’ble Justice A.P. Shah and Hon’ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.  
  
Following this the Central Government passed an order dated 23 March 2003 appointing the “Secretary of Department of Information Technology of each of the States or of Union Territories” of India as the adjudicating officer for that State or Union Territory.  
  
The **Information Technology (Security Procedure) Rules, 2004** came into force on 29 October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records. Also relevant are the Information Technology (Other Standards) Rules, 2003.  
  
An important order relating to blocking of websites was passed on 27 February, 2003. Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DoT) to block a website.  
  
The **Indian Penal Code** (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc. Digital evidence is to be collected and proven in court as per the provisions of the**Indian Evidence Act** (as amended by the IT Act). In case of bank records, the provisions of the Bankers’ Book Evidence Act (as amended by the IT Act) are relevant.  
Investigation and adjudication of cyber crimes is done in accordance with the provisions of the**Code of Criminal Procedure** and the IT Act. The Reserve Bank of India Act was also amended by the IT Act.  
  
The **Information Technology (Amendment) Act, 2008**, which came into force on 27th October, 2009 has made sweeping changes to the Information Technology Act, 2000.  
  
The following rules have also come into force on the same day:

(1) Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009

(2) Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

(3) Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009

(4) The Cyber Appellate Tribunal (Salary, Allowances and Other Terms and Conditions of Service of Chairperson and Members) Rules, 2009

(5) Cyber Appellate Tribunal (Procedure for Investigation of Misbehaviour or Incapacity of Chairperson and Members) Rules, 2009.

# What is Footprinting

Refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering information about the host, network and people related to the organization.

Information such as ip address, Whois records, DNS information, an operating system used, employee email id, Phone numbers etc is collected.

Footprinting helps to

****Know Security Posture**** – The data gathered will help us to get an overview of the security posture of the company such as details about the presence of a firewall, security configurations of applications etc.

****Reduce Attack Area**** – Can identify a specific range of systems and concentrate on particular targets only. This will greatly reduce the number of systems we are focussing on.

****Identify vulnerabilities**** – we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.

****Draw Network map**** – helps to draw a network map of the networks in the target organization covering topology, trusted routers, presence of server and other information.

**Footprinting** (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.

When used in the computer security lexicon, "Footprinting" generally refers to one of the pre-attack phases; tasks performed prior to doing the actual attack. Some of the tools used for Footprinting are [Sam Spade](https://en.wikipedia.org/wiki/Sam_Spade_(software)" \o "Sam Spade (software)), [nslookup](https://en.wikipedia.org/wiki/Nslookup" \o "Nslookup), [traceroute](https://en.wikipedia.org/wiki/Traceroute" \o "Traceroute), [Nmap](https://en.wikipedia.org/wiki/Nmap" \o "Nmap) and neotrace.

## Techniques used for Footprinting

* [DNS](https://en.wikipedia.org/wiki/Domain_name_services" \o "Domain name services) queries
* [Network enumeration](https://en.wikipedia.org/wiki/Network_enumerating" \o "Network enumerating)
* Network queries
* [Operating system](https://en.wikipedia.org/wiki/Operating_system" \o "Operating system) identification
* Organizational queries
* [Ping](https://en.wikipedia.org/wiki/Ping_(networking_utility)" \o "Ping (networking utility)) sweeps
* Point of contact queries
* [Port Scanning](https://en.wikipedia.org/wiki/Port_scan" \o "Port scan)
* Registrar queries ([WHOIS](https://en.wikipedia.org/wiki/WHOIS" \o "WHOIS) queries)
* [SNMP](https://en.wikipedia.org/wiki/SNMP" \o "SNMP) queries
* [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web" \o "World Wide Web) spidering

## Uses of Footprinting

It allows a hacker to gain information about the target system. This information can be used to carry out further attacks on the system. That is the reason by which it may be named a Pre-Attack, since all the information is reviewed in order to get a complete and successful resolution of the attack.

# DNS Enumeration

DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization. DNS enumeration will yield usernames, computer names, and IP addresses of potential target systems. The list of DNS record provides an overview of types of resource records (database records) stored in the zone files of the Domain Name System (DNS). The DNS implements a distributed, hierarchical, and redundant database for information associated with Internet domain names and addresses.

DNS Zone Transfer used to replicate DNS data across a number of DNS servers or to back up DNS files. A user or server will perform a specific zone transfer request from a ―name server. If the name server allows zone transfers by an anonymous user to occur, all the DNS names and IP addresses hosted by the name server will be returned in human-readable ASCII text.

## Tools:

nslookup, maltego, dnenum,dnsrecon.

# **Network reconnaissance**

Network reconnaissance is a term for testing for potential vulnerabilities in a computer network. This may be a legitimate activity by the network owner/operator, seeking to protect it or to enforce its acceptable use policy. It also may be a precursor to external attacks on the network.

Certain apparent reconnaissance activities, which would be highly suspicious if coming from outside the network, may be perfectly normal network performance and reliability monitoring when performed inside the boundaries of the network. Some [network intrusion detection systems](http://en.citizendium.org/wiki?title=Network_intrusion_detection_system&action=edit&redlink=1" \o "Network intrusion detection system (page does not exist)) have difficulty in determining if a reconnaissance activity is internal or external, and generate many false alarms causing [fear, uncertainty and doubt](http://en.citizendium.org/wiki/Fear,_uncertainty_and_doubt" \o "Fear, uncertainty and doubt).

## ***Email Spoofing* mean?**

Email spoofing is a fraudulent email activity hiding email origins. The act of e-mail spoofing occurs when imposters are able to deliver emails by altering emails' sender information. Although this is usually done by spammers and through phishing emails for advertising purposes, email spoofing can have malicious motives such as virus spreading or attempts to gain personal banking information. Simple Mail Transfer Protocol (SMTP) does not provide any type of authentication process for persons sending emails. Yet, it is the primary email system for most people, facilitating email spoofing. Now a days, most email servers can provide further security. Also many digital software vendors have created products remedying this problem.

**DEFINITION**

# **Email spoofing**

Email spoofing is the forgery of an email [header](https://whatis.techtarget.com/definition/header) so that the message appears to have originated from someone or somewhere other than the actual source. Email spoofing is a tactic used in [phishing](https://searchsecurity.techtarget.com/definition/phishing) and [spam](https://searchsecurity.techtarget.com/definition/spam) campaigns because people are more likely to open an email when they think it has been sent by a legitimate source.  The goal of email spoofing is to get recipients to open, and possibly even respond to, a solicitation.

Although most spoofed email falls into the *nuisance* category and requires little action other than deletion, the more malicious varieties can cause serious problems and pose security risks. For example, a spoofed email may purport to be from a well-known shopping website, asking the recipient to provide sensitive data such as a password or credit card number. Or the spoofed email may ask the recipient to click on a link that installs malware on the recipient's computing device. One type of [spear phishing](https://searchsecurity.techtarget.com/definition/spear-phishing) used in business email compromises, involves spoofing emails from the CEO or CFO of a company who works with suppliers in foreign countries, requesting that wire transfers to the supplier be sent to a different payment location.

Email spoofing is possible because the [Simple Mail Transfer Protocol (SMTP)](https://whatis.techtarget.com/definition/SMTP-Simple-Mail-Transfer-Protocol) does not provide a mechanism for [address](https://searchnetworking.techtarget.com/definition/address) [authentication](https://searchsecurity.techtarget.com/definition/authentication). Although email address authentication [protocols](https://searchnetworking.techtarget.com/definition/protocol) and mechanisms have been specified to battle email spoofing, adoption of those mechanisms has been slow. The SMTP AUTH extension specified in RFC 4954, "SMTP Service Extension for Authentication", defines a way for an SMTP client to negotiate an authentication mechanism with an SMTP server to authenticate the client and, if desired, to set up additional security on the [client](https://searchenterprisedesktop.techtarget.com/definition/client)-[server](https://whatis.techtarget.com/definition/server) [session](https://searchmicroservices.techtarget.com/definition/session).  
**email spoofing**

Some other proposed solutions to authenticating email senders include [Sender Policy Framework (SPF)](https://searchsecurity.techtarget.com/definition/Sender-Policy-Framework), a protocol defined in RFC 7208 to allow domain managers to authorize individual hosts to use a domain in email; Domain-based Message Authentication, Reporting and Conformance, defined as an email authentication protocol in RFC 7489; and DomainKeys Identified Mail, which provides a way to validate a domain name identity associated with a message. [Sender ID](https://whatis.techtarget.com/definition/Sender-ID), described in RFC 4407, is an experimental protocol based largely on SPF and promoted by Microsoft, but failed to gain any significant deployment.

To prevent becoming a victim of email spoofing, the FBI and the [Federal Trade Commission](https://searchcompliance.techtarget.com/definition/FTC-Federal-Trade-Commission)urge recipients to keep [antimalware software](https://searchsecurity.techtarget.com/definition/antimalware) up to date, be wary of tactics used in [social engineering](https://searchsecurity.techtarget.com/definition/social-engineering) and contact the sender directly when sharing private or financial information instead of responding through an email.

## **Definition - What does *Email Bomb* mean?**

An email bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of email to a specific email address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.

An email bomb is also known as a letter bomb.

There are three ways to create an email bomb:

* Mass mailing - involves sending numerous duplicates of the same email to one email address. Because of the simplicity of this attack, it can be easily detected by spam filters. To be done on a massive scale, an attacker can use a bot net or zombie net, computers across the globe which are under the attacker’s control due to some form of malware such as Trojans, and then instructing the bot net to send millions of emails to a single or a few addresses at once in order to perform a denial of service attack. This is harder for spam filters to detect since each email would be coming from a unique source.
* List linking - meant more to annoy rather than cause real trouble. The technique involves subscribing the address for attack to different email list subscriptions so it would always receive spam mail from these lists. The user then has to manually unsubscribe from each list. However, more legitimate lists require email verification which the user has to manually click and accept to be part of the email listing. To circumvent this, the attacker may register a new email account and subscribe that to all the lists and have it automatically forward all mail to the victim. The attacker can reply to the confirmation emails. But since the emails will be coming from a single forwarding source, it can simply be blocked by the user.
* ZIP bombing - the latest twist on email bombing using ZIP archived attachments. Mail servers always check email attachments for viruses, especially zip archives and .exe files. The idea here is to place a text file with millions or billions of arbitrary characters or even a single letter repeated millions of times so that the scanner would require a greater amount of processing power to read each one. Combining this with mass mailing techniques ups the potential for a denial of service attack to succeed.

**Data Diddling**

Data diddling occurs when someone with access to information of some sort changes this information before it is entered into a computer. This is done to provide some sort of benefit to the data diddler, generally financial, and is a common method of computer-related crime.

Data diddling can occur at various points along the chain of information entry, and it is often very subtle and virtually undetectable. It can be something as small as a time clerk substituting his own name or employee number for another employee's name or number. It can be combated by ensuring that all information is identical, whether it is a hard copy or the data within a digital system.