

Digital Forensics 101

INFORMATION IN THIS CHAPTER:

- What is Digital Forensics
- Tools for Recovering Evidence
- Do You Really Want to Do This?
- Organizing Your Case
- Understanding What You are Looking At

WHAT IS DIGITAL FORENSICS?

Digital Forensics is a branch of forensic science that focuses on the recovery, examination, and investigation of evidence stored on computers and other digital devices, as well as various media that may have been used to store data. Although it is commonly associated with criminal investigations, digital forensics has been used in civil cases, internal investigations, tribunals, and other inquiries or forums that require an exploration of data.

The Process of Digital Forensics

The process of performing a digital forensic investigation can be broken down into four stages:

- *Seizure*, in which computers, mobile devices and other devices and/or media are obtained and preserved.
- *Acquisition*, in which the data is retrieved from a device
- *Analysis*, in which an image or copy of the data acquired in the previous step is examined
- *Reporting*, in which the procedures and processed that were followed in the previous steps are documented, along with the evidentiary findings

Seizure

When a computer or other device is seized, it is taken into custody and secured with goal of preserving any potential evidence. As with every stage of a digital forensic investigation, you will document the scene, actions that were taken, and procedures that were followed. It is also important at this stage to establish a chain of custody that will carry on through all the other stages, documenting who and when and when a person had position of evidence.

In addition to photographing the scene where the computer or device was seized, photograph the computer or mobile device and what is displayed on the screen. Photographing the screen will preserve what applications were open, possible information, and will show what the user was last using doing on the computer or device. Under no circumstances should you use the computer/device, search for evidence, or alter its running condition. A rule of thumb is that if it is turned off, leave it off; if it is turned on, leave it on.

During the seizure, some steps may be taken to acquire digital evidence. If a computer is turned on, you would start by collecting any live data, inclusive to taking an image of the physical memory. A utility that can be used to image the RAM is F-Response (www.f-response.com). This tool could also be used to collect a logical image of the disk if you discovered the hard disk was encrypted. You would also gather any other data that is required for the investigation about the computer's live state, such as logged on users, its network connection state, running processes, and so on.

You should also take effort in documenting how the computer or device was found. Photographs and diagrams should be made of how it was setup when found, inclusive to any cords plugged into the machine. You should also label all of the cords, and document the model numbers and serial numbers of the computer/device and any other devices attached to it. Nothing should be disconnected from a computer or device until the previous steps have been completed.

When you are ready to transport the computer/device, you should package all of the components in anti-static bags, and seize any other storage media. This would include external hard disks, USB sticks, as well as CDs and DVDs that may contain data. To keep the media safe, you should avoid putting it near anything that may damage the data, such as magnets, radio transmitters, and so on. In gathering these additional items, you should also collect any manuals or documentation that may be related to the device. You never know if these will be helpful later in your investigation, or if they contain useful information (such as passwords, etc.).

There are additional considerations when a mobile device is seized. When a mobile device is connected to a cellular network, it may access new data that will overwrite evidence. Similarly, a mobile GPS unit that is turned on may

continue to record track points (i.e., locations that the GPS has been) as its being transported. Because a mobile phone or tablet can be sent a command to wipe the device, you also run the risk of everything on it being erased. To preserve potential evidence on a mobile phone, GPS or other device, it is important they are stored in a Faraday bag or cage. A Faraday cage is an area protected by material that blocks signals, essentially creating the same conditions of being in a “dead zone” where you cannot get a cell phone signal from your carrier. A Faraday bag is used to store mobile devices for transport, preserving any evidence stored on them.

Acquisition

The acquisition stage is where data is retrieved from a device or media, and generally occurs after the evidence has been collected, safeguarded and transported. In acquiring evidence from a device, a decision is made whether you need to perform a live or dead analysis. A live analysis is performed when a computer or device is powered on, and cannot be powered off until this information is collected. A dead analysis occurs when the machine is powered off, and transported to a lab where data can be retrieved in a controlled environment.

Acquiring data from a computer, device, or various media that may be used to store potential evidence generally requires specialized tools. This is not to say there are not times when a mobile device may require the manual acquisition of data, whereby an investigator uses the user interface of a phone or other device to view and photograph information displayed on the screen. However, in doing so, the only data that will be displayed is that which is accessible to the device’s operating system and/or apps. In addition, using the interface may result in data being written to the device. To safely acquire all of the data, inclusive to that which may have been deleted, software and hardware tools are commonly used to create a bit-for-bit copy of what is stored on the device. Once a copy of the data is acquired, the investigator can then examine the copy of the data so that the original remains untouched during analysis.

There are several ways in which you may acquire a copy of what is stored on a file system, but not all of them will provide the same results. These methods include:

- Copying files, which will only copy the files that are on the system and not ones that may have been deleted. Also, metadata related to file ownership, times a file was accessed, permissions and other data may be lost in copying the file.
- Backups, which will restore a copy of the files. Depending on the backup software used, not all of the metadata related to files will be included with the backup, and it will not capture information about deleted files.

- Copying disk partitions, which will create a bit-for-bit copy of the file system including metadata related to the files and information residing in unallocated space.
- Copying the entire disk, which creates a bit-for-bit copy of the file system, including storage space before and after disk partitions.

In looking at these methods, you can see that a bit-by-bit copy of the data will yield the most possible results. While you might think this would only apply to the hard disk of a computer, many mobile devices use file systems and may be used as storage devices. In addition, devices that use SD cards can have the card removed and processed like other removable media. By using various tools discussed later in this chapter, you will be able to collect the data on these devices, making a copy that you can then analyze to identify evidence related to your case.

Analysis

The analysis stage generally occurs after evidence has been collected. If live data is not being examined, then an investigation is conducted against static data that has been copied from a system. Once an image of data on the computer, device, or other media has been made, an examination of the data takes place. This may involve performing keyword searches relating to a crime, running scripts to identify certain types of data, manually reviewing information and content of files, and various other techniques.

By analyzing various types of data found on a machine, investigators will search for evidence that implicates or exonerates a suspect. The evidence may include digital photographs or downloaded images (as in the case of child pornography cases), electronic spreadsheets (in the case of financial crimes), email and other types of data. Using the content, metadata, or other information discovered, the investigator may reconstruct a series of events related to the case.

Reporting

Documentation is crucial to any digital forensics case. It is important to make a record of any actions taken, devices or media examined, procedures that were followed, and other details relating to the evidence. Remember that, especially after a case goes to court, there is the possibility that anything related to the case may be questioned, and your documentation may be used to provide answers.

Throughout the process of conducting an investigation, it is vital that the integrity of the data and the device storing it is preserved, and part of this involves a documented chain of custody. Once a computer, device or media is seized, it should start the chain of custody, showing who initially took possession and who had custody of it after that point. It is also important to remember that the original devices, storage media, or other items that evidence was collected

from may be requested by defense council or other parties involved in the case. In some cases, evidence files or images taken of a system may be requested. By preserving these items and ensuring there is a record of who had access to them, you can help to ensure the evidence has not been corrupted or tampered with in anyway.

It should also come as no surprise that you will need to create a report about what was found during the course of your investigation, and how it applies to the case. This could include listings and details about any files found on storage mediums (e.g., hard disks, tape, USB devices, etc.), information recovered from emails or other sources, and any other data that is being used as evidence. As we will discuss later in this chapter, many commercial tools provide features that will automatically generate reports about the files that were found. You would also write a report yourself that outlined the steps taken to acquire and analyze the data, and how the files or information found apply to the case. The reports themselves may then be submitted as evidence of an accused persons guilt or innocence.

Where Google Earth Fits In

Google Earth (GE) can be used in multiple stages of the digital forensic process. Most often, you will find that it is used in the later parts of a case, when you need to analyze coordinates from various sources, or as a reporting tool to create presentations relating to geographic locations. In some cases, it may also be used to acquire GPS data from a device, although other tools may be more suited to collecting such data for a forensic investigation.

GPS Forensics

When a person uses a GPS device, he or she will enter in locations called *waypoints* that are stored in the GPS. The waypoint may be a person's current location, or a location that he or she wants to navigate to. The GPS device will use a series of waypoints to create a *route*, showing the person how to navigate from one location to others in a specific order. Because this information can be stored on the device, it can also be retrieved and examined during an investigation.

GPS devices will also store *tracks*, which are geographic points that the unit has been. When you turn on the GPS unit, it will connect to satellites and determine its current location. As you travel, additional track points will be stored as a record of where the GPS unit has been, and stored in a *track log*. By looking at the track log, you are able to view a listing of coordinates that the portable GPS has visited and, by extension, where its owner has been.

As we saw in Chapter 3, and revisit in the next chapter, Google Earth can be used to acquire data from a Garmin or Magellan GPS unit. In performing the import, you will see the number of waypoints, tracks and routes that are imported from a GPS device, which can then be reviewed in the 3D viewer.

However, importing GPS data in this way copies the data directly off of the device into Google Earth. It does not retrieve any data that may have been deleted, or is hidden on the device.

This can be a major issue if a particular location of interested a suspect visited existed in the deleted data, and no longer appeared in the tracks you copied using Google Earth's import feature. For this reason, it is often best to use forensic tools to collect all of the data, not just what is visible to the device's interface, inclusive to any deleted or hidden data that may reside on the device.

Also, in acquiring the data from a GPS device for use with Google Earth, you want to ensure nothing is written to the GPS device. As the device will store files, your operating system or applications might write data without your knowledge or intention. If data from the original source of evidence has been modified, it could be challenged in court, and become inadmissible as evidence. To prevent this from happening, you should ensure that your forensic machine uses write protection and/or uses tools that are designed to gather evidence in a forensically sound manner, as we discuss in the next section.

TOOLS FOR RECOVERING EVIDENCE

As we have mentioned, it is important to recognize that GE is not a tool designed for digital forensic data collection. It will do a logical download of geo-location data, so anything that is been deleted from the device (i.e., waypoints, coordinates, etc.) will not be included when you use GE to import data from the device. To acquire data in a forensically sound manner, and get all the evidence that is available (regardless of whether it is deleted or hidden), more advanced tools should be considered.

In this section, we will discuss various tools that can be used to collect data from devices. There are software and hardware solutions that prevent your operating system or software like Google Earth from writing to the device or storage media, and ones that will create an exact duplicate so that you can work from an image of the data.

TIPS AND TRICKS

Working with Images and Other Copies of Data

By creating an image of what is stored on a computer or other devices, you are examining a copy of the data and not the original source. Forensic software that allows you to create an image in this way means that you can examine a computer or device without having to go through its operating system or user interface. In doing so, you are bypassing any passwords required to logon to a machine. Similarly, for mobile forensics, such tools can extract data while bypassing pattern locks, PINs or passwords.

Write Protection

Prior to acquiring data from a GPS unit with Google Earth, you should ensure that your forensic machine has USB write protection enabled. Because a GPS unit also can function as a mass storage device, it is essential to make sure that no data on the device is changed. Rather than simply plugging the GPS device into a USB port, you want to ensure that software write protection or a hardware write blocker is used to prevent any accidental modification of data.

Write blockers allow read commands to pass from a computer to a storage device, but block any write commands. In doing so, you can safely access the drive to view its contents and/or collect data. With a hardware blocker, the disk or device you are collecting evidence from plugs into a device that becomes a midway point between the forensic workstation and the storage you are acquiring data from. The ability to block writes may also be included in other forensic hardware tools that are used to image or duplicate the data on the suspect device.

There are also a number of software solutions that can be used to prevent your computer from writing to a storage device that you are collecting data from, such as a GPS device that is connected via a USB port. On a machine running Windows, you can use write protection software like:

- DSI USB Write Blocker (<http://document-solutions.biz/downloads/?did=9>)
- M2CFG USB Write Block (www.m2cfg.com/usb_writeblock.htm)
- NetWrix USB Blocker (www.netwrix.com/usb_blocker_freeware.html)
- Thumbscrew (www.irongeek.com/i.php?page=security/thumbscrew-software-usb-write-blocker)

There are also a number of tools for Mac computers that provide write protection, allowing you to safely acquire data, such as:

- Softblock (www.blackbagtech.com/software-products/softblock-1/softblock.html)
- Disk Arbitrator (<https://github.com/aburgh/Disk-Arbitrator/downloads>)

Tools Used to Acquire Evidence

In addition to the tools we have already mentioned, there are a number of products available for digital forensics investigations, which are commonly used by law enforcement and companies specializing in data collection. Using such suites of products, you will find that they have features and functions that will meet most of your needs throughout the process of acquiring, analyzing and reporting on digital evidence.

Guidance Software (www.guidancesoftware.com) is a company that creates a number of products used for digital forensics. The versions of *EnCase* are used to acquire evidence from hard drives, removable media (e.g., CDs, USB sticks, etc.), smartphones, tablets, GPS units and more. Using a GUI interface, the software can be used to acquire, analyze, and create reports to show what was found, where the data originated, details of files, and other pertinent facts that relate to your investigation. Once completed, you can have *EnCase* generate a report that can be provided to other investigators and the courts.

Cellebrite (www.cellebrite.com) is another company that is well known for its commercial digital forensic products. Using their software and hardware, you can acquire and examine data from mobile phones, GPS units, tablets, and other devices, as well as memory cards. The tools available can be used for manual acquisition, where there is a need to take screenshots or images of data, and for acquiring existing and deleted data from a device being examined.

Cellebrite also has tools specifically designed for investigations requiring the acquisition of data from GPS devices. Using these tools, you can extract data from portable GPS units like Tom Tom, Garmin and Mia, inclusive to any GPS fixes that may have been previously deleted. Once you have acquired the files using tools like Cellebrite and *EnCase*, you can then import them into Google Earth for further analysis.

File Converters

While you can import GPS data into Google Earth, you are limited to files for Garmin and Magellan units. If files have been retrieved from other types of GPS devices, then you will need to convert them prior to importing them into GE. Once converted to a Garmin or Magellan format or a KML file, you can then import the data into GE. Some of the file converters available include:

- GPSBabel (www.gpsbabel.org) is freeware application that runs on your computer, which converts waypoints, tracks and routes to different formats.
- GPS Visualizer (www.gpsvisualizer.com/gpsbabel/), which is a site that provides an online version of GPSBabel, allowing you to upload and convert the file on their site.
- TraceGPS (www.tracegps.com/en/convert.htm) is another site that allows you to upload and convert files from one format to another
- GPS Data Team (<http://tomtom.gps-data-team.com/poi/ov2-to-kml.php>), which is a site that can convert OV2 files used by Tom Tom GPS devices to a format used by Garmin devices.

DO YOU REALLY WANT TO DO THIS?

Just because you need the evidence does not mean that you should be the one to acquire it. Law enforcement may have a fulltime digital or computer forensic examiner, while a corporation or other organization may have someone on staff (such as in the I.T. department) who is trained in the collection of data using forensic methods and resources. Rather than doing the work yourself, you could have such a person collect the data for you, so you can work from a copy or image.

If you are not part of a formal investigation, you should ask *why* you are doing the work and where it might lead. Anyone using Google Earth has the ability to import and examine GPS data from a portable device, and retrieving and reviewing this information might be used for personal or non-investigative reasons. However, depending on what you find, that data may eventually become evidence in a court case, and how it was collected might be held to a higher standard. For example:

- A manager could import GPS data into Google Earth to review where an employee traveled during work hours. Is he or she traveling to meetings locations, customer offices and other work-related places, or visiting a bar or the beach? Looking at the GPS data would reveal where that employee goes, and if it was found the person was not doing their job, it could result in termination of employment. However, if the former employee challenged being fired and sued, then the data and methods of acquiring the GPS data could be questioned in civil litigation.
- If a friend was concerned that his/her spouse or significant other was cheating, you could examine where a portable GPS unit was taken in Google Earth. In doing so, you might confirm your friend's suspicions, but what if your findings became the basis for a divorce? What was a simple perusal of a person's goings on has now become evidence in a divorce case.

As you can see from these scenarios, a simple looksee can quickly change. When you acquire and examine any data, you should always assume that it could eventually become part of a criminal or civil case. Because of this, you should always try to follow best practices of data collection, documentation, and follow any procedures or policies created by your organization. By treating the acquisition of any data as a formal investigation, you will maintain good habits in the collection and analysis of evidence, and be prepared if you have to testify about it later.

ORGANIZING YOUR CASE

It is a good idea to make sure that when working on a geo-forensic case in Google Earth, you make sure you keep your work organized so that it is easy to retrieve and share, that you can recover from mistakes and most importantly

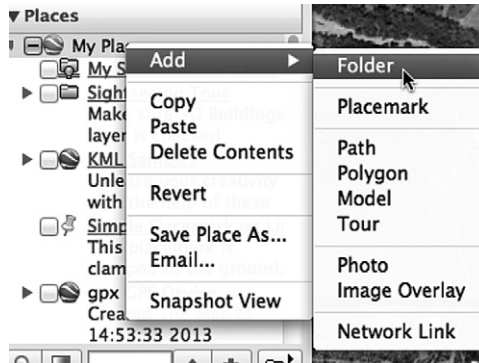


FIGURE 5.1 Adding a folder.

you can maintain consistent work flow. A recommended way to do this is to create case folders in Google Earth. It is suggested that an investigator create two types of folders when working a case in Google Earth:

- A case folder in the “My Places” top level directory for eventual case dissemination
- A “temporary” folder in the “Temporary Places” top level directory for experimenting and developing your work.

Creating a folder in Google Earth is done by right-clicking on one of the top level directories, and when the context menu shown in [Figure 5.1](#) appears, select *Add* and then click *Folder*.

Once you have created a folder, you are greeted with a dialog window to edit the settings of the folder. These settings are as follows.

- *Name*. Here is where you set the name of the folder. It is recommended that you use a consistent nomenclature for your particular organization. For instance <case name> - <case number>
- *Description*. You can give the folder a description of what it contains and a preview of this will appear below the folder. The description can also include links, photos and other HTML tags. This is covered in the previous chapters, and as well as Chapter 6.
- *Style, color*. This option becomes available once there are icons within the folder you are creating or any subfolders of the created folder. The option is used to create a universal color and label style in this folder and all its children.
- *View*. This option is used for creating one viewing angle for each of the placemarks contained in the folder. Once a view is set for a folder, double clicking on it will reset the view to match what was set. Setting the view will be covered in a section in Chapter 6.








- ▼  Google Earth For Forensics
This folder contains the final case work for the course ready for delivery to an OIC or Prosecuting Attorney.
-  Victim's Home and Route
This folder contains placemarks and information pertaining to the victim's home and route to Saguaro National Park, including relevant reports.
-  Saguaro National Park
This folder contains all the geolocation data pertaining to the scene at Saguaro National Park, including reports, measurements and location of recovered data.
- ▼  Temporary Places
 - ▼  Google Earth For Forensics
This folder contains the final case work for the course ready for delivery to an OIC or Prosecuting Attorney.
 -  Victim's Home and Route
This folder contains placemarks and information pertaining to the victim's home and route to Saguaro National Park, including relevant reports.
 -  Saguaro National Park
This folder contains all the geolocation data pertaining to the scene at Saguaro National Park, including reports, measurements and location of recovered data.

FIGURE 5.2 Folder structure template.

In Chapter 6, we will work with a scenario to use the knowledge you have acquired throughout this book. For the purposes of our scenario for this course and to get you familiar with organizing your work, create the following structure by adding folders in *My Places* and *Temporary Places*. In using this template structure, it is encouraged that you change the template and narrative contained in the description to suit the needs of your agency (Figure 5.2).

Custom Icons

As we mentioned in Chapter 2, when creating placemarks, the *Style, Color* tab of the *Properties* dialog can be used to select a unique icon for each placemark. Using different icons makes your placemarks stand out from one another in the 3D viewer, and can provide an effective graphic representation of why a location is important and/or what was found there (e.g., a crime scene, remains, evidence, etc.).

As we will discuss in Chapter 6, you can select an icon from a library of icons that is included with Google Earth, or add a custom icon. Because you may find the ones included with GE limited, it may be useful to look at online resources, and take the time to choose ones that suit your purpose. A good site for custom icons is the Map Icons Collection (<http://mapicons.nicolasmollet.com>), which has hundreds of free icons that can be downloaded and used in your project. Other useful sites include:

- The Google Developers site (<http://code.google.com/p/google-maps-icons/downloads/list>)
- Mapito (<http://www.mapito.net/map-marker-icons.html>)
- Benjamin Keen (<http://www.benjaminkeen.com/?p=105>)

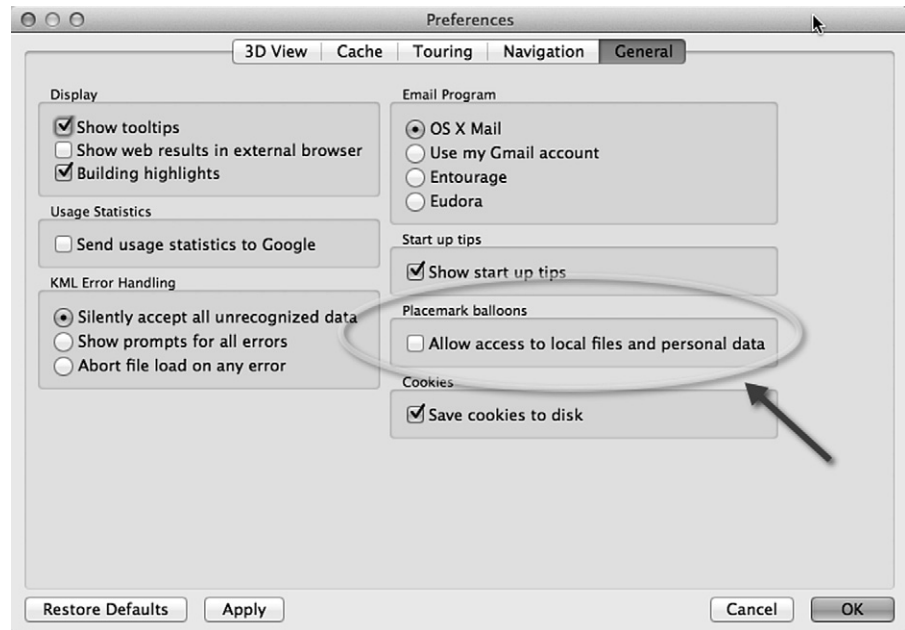


FIGURE 5.3 Enable placemark balloon local access.

Enabling Access to Local Files

Google Earth is set up natively to access the Internet to pull down content like map data or external files and pictures. But in digital forensics allowing Internet access by a program containing case data is generally considered to be a poor idea. It is of use, however, to use the capability of Google Earth to link to other files such as report PDFs or scene photographs. Below is the procedure for allowing Google Earth to link to files local to the examiner's machine (Figure 5.3).

1. From the *Tools* menu, and click the *Options* menu item (on a Mac click *Preferences*)
2. Click the *General* tab, and (as shown in the following figure) locate the *Placemark Balloons* section.
3. Click the *Allow access to local files and personal data* checkbox so it appears checked.
4. Accept the warning saying that access to local files might be risky, and click *OK*

UNDERSTANDING WHAT YOU ARE LOOKING AT

When navigating through areas in Google Earth, it is important to realize that much of what is shown is not current. Some images may be recent, but others

may be weeks, months or even years old. According to Google, most of the imagery you see is approximately 1–3 years old. As such, buildings that have been torn down may appear in GE, while those recently built are not visible. Similarly, the Street View does not contain real-time footage, so a familiar area may appear outdated as you take a virtual walk down the street. In using this tool, it is important to remember that what is displayed may not be an accurate representation of what is there now.

Why is He Blurry?

In Chapter 1, we mentioned that if you notice blurred imagery in GE, it may be due to slow or poor connections to the Internet. That being said, you can expect to see some blurred areas when viewing an area in Street View. To protect a person's privacy, Google uses an algorithm that will automatically blur a person's face and the license plates of vehicles so they cannot be identified.

Blocked Content

Generally, when you use Street View, you will not be able to access areas beyond the street. In other words, you will not be able to explore a mall's parking lot, private roads, empty fields, and so on. The reason for this is that Google uses a car with a panoramic camera on top of it to take photos as it drives down the street. It does not go off road to take photos, so you are limited to what is visible from the roadway. An exception to this is when a point of interest like Universal or Disney theme parks permit Google to enter and take digital photos of what is inside. Doing so allows you to take a virtual journey through that location.

Another time when you will notice missing content is when Google removes something that is considered inappropriate. An example of this is when you try and visit 105 Temperance Street in Manchester England, where you will find that you are prevented from navigating down a section of that roadway. The reason is that when the Google car drove by, the 15 lens panoramic camera captured multiple angles of a man and woman engaged in a sex act. The area was known for prostitution, and once it was discovered a salacious transaction had been photographed, Google blurred and later deleted the images.

Misinterpreted Content

While Google has captured unsavory and illegal acts on camera, and even used aerial imagery showing a crime scene, there are also times where people have mistakenly interpreted what is shown. An example of this occurred on Middle Road in St John's, Worcester, England when the Google car photographed a young girl lying face down in the road, with one shoe cast off in the gutter. When the images became available the next year, users of Google Maps and Google Earth were shocked to see what appeared to be a dead girl. Fortunately, things were not what they seemed. The 9-year-old was simply playing a prank on her friend, and had

been unaware that Google had snapped her picture. Before you try looking for the imagery on Google Earth, you should be aware that they have already blurred and deleted images, preventing you from navigating down that road.

Removing Content

Problems related to what appears in Google Earth and Google Maps can be reported to the company, which may result in images being blurred, replaced or removed. To report an issue, you can use Google Maps (<https://maps.google.com>) to navigate to a particular location. Enter an address, and zoom into a location. When you are viewing a map or satellite image and spot a problem, you can click on the *Report a problem* link to display a dialog box that allows you to notify Google about incorrect road information, addresses, places, directions, or other issues. By clicking on the *Other Problems* link, you can report issues with satellite imagery, Street View, or other problems.

For Street View, anyone can report inappropriate content, or request that a location or person is blurred. Accessing Street View in Google Maps is the same as in Google Earth. You would navigate to a location and either zoom in as far as you can until it switches to Street View, or drop the pegman icon onto a location. Once you are in Street View, you will notice you will see a *Report a problem* link in the lower right-hand corner. Upon clicking this, a separate browser window will open, where you can report inappropriate content. Once this window opens, you will see a picture of what you were looking at in Street View, which you can adjust to focus on a particular part of the image. You can then request that a face, your home, car or license plate, or a different object is blurred. While you have reported the issues using Google Maps, the changes will also appear in Google Earth.