Digital Forensic

By: Ivneet Singh

INTRODUCTION TO FORENSIC

In today’s world our life can’t remain untouched by electronic storage devices and computers. Bits and bytes have overaken all other advancement of human life. Forensic experts are required to work in an environment where more than 90% of records and data are stored in electronic media.

In such a situation it is essential for them to utilize their expertise of digital forensic so that in the field it may not be the person who have accidently either destroyed the electronic evidence or contaminated to make them worthless. It is essential for forensic experts to understand some basic fundamental rules of handling and preserving digital files / evidences. This is essential for a forensic expert to properly communicate with court to get its desired search conducted on files which has been retrieved from the strategic device of the suspect. Legal aspects associated with digital evidence is equally important to know.

FORENSIC CHALLENGE

The modern digital area is being tremendously increasing now days which has become a challenge for computer forensic expert to analyze the data.

It is not only about the massive amount of data but also the different types of files they come across during investigation. It has become challenging tasks for experts to analyze and investigate the image files. The image file can be in several different formats like JPG, BMP, PNG, GIF etc…

All these files have their own forensic properties which are included in forensic reports during investigation. The properties can be: Size of the file, MD5 hash value of the file, date of creation, date of deletion, date of modification and sometimes source destination of the file.

9/11 – Towers of Deception
Sample Case study: 9/11 Towers of Deception

Page: 2

Inspecting Digital Image
In-depth analysis of the image files developing various hypotheses.

Page 6

Forensic Analysis of Image
Forensic Analysis of digital image : extracting forensic properties for investigation.

Page: 4

Image Files
Explanation about image files, size and formats including compression techniques.

Page: 3

Investigating Digital Image
Converting image files and investigating further leads.

Page: 7
Sample Case Study: 9/11 – Towers of Deception

By: Ivneet Singh

Note: This sample case study is only for discussion purposes as nothing relates to actual crime scene

Cyber criminals are wreaking havoc on computer systems and are capturing front-page headlines in the bargain. It has made little difference that the administration has pledged billions in additional federal funding to combat security breaches after the 9-11 terrorists attacks.

The problem just keeps getting worse. Fortunately, the computer security field is also progressing at a brisk rate. In particular, the field of computer forensics brings new ways of preserving and analyzing evidence related to cybercrime.

You have been transferred to the forensic department of the law enforcement agency to conduct further forensic analysis of the evidence.

While conducting forensic analysis on the suspect’s hard drive you found number of similar images related to “World Trade Center” in which the current incident has taken place, the images might not surprise you since it is a very famous place on the earth. Multiple similar copies of the same images were found on the hard drive during forensic analysis.

Just looking at those images might not help you to come up with a conclusive report. In case of terrorism forensic expert should develop various hypotheses to test the evidence. You might start analyzing those images with “steganography technique” to verify the integrity of the image and start searching in depth for the forensic properties of the image file.

The foremost challenges that forensic experts sometimes come across during investigation is to conduct analysis on image files. If image does not contain steganography then most of the investigators bookmark those images as “Pictures or Similar image files”. Now we are going to discuss further how we can analyze these images which have devastating and conclusive results.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity

PICTURE THE SCENCE:

You are engaged by the law enforcement agency to assist them during the investigation at 9/11 attacks which is now considered as your crime scene. While searching around the premises you have discovered various digital evidences like laptops, desktops, USB and hard drives. All these evidence were tagged and bagged properly with full consent of the chief investigating officer. Proper investigation procedures were conducted to avoid contamination of the evidence.
**Image Files**

**By:** Ivneet Singh

---

**IMAGE FILES**

All image files have their own standard means of storing into digital image. These files contain digital data which are changed accordingly on the computer displays, printers and scanners. The image file can also be stored into compressed and uncompressed formats. Once it reaches to its final stage the image converts itself into a grid of pixels which contains number of bits to elect the color of the image which should be equal to the color depth of the device.

---

**IMAGE FILE SIZE**

The image size basically depends upon the pixels in the image and the color we have applied to the image or we can say bits per pixel of the image. We can compress the image into several ways using different algorithms which also can affect the representation of the original image. During the compression we basically compress the bits of the pixel and uncompressing can bring turn back the image into its original state. The compression of the image also depends upon the compression formats, some of the formats have less complexity which may result into a different file size.

---

**IMAGE COMPRESSIONS**

There are primarily two types of compression algorithms used for file compression.

**Lossless compression:** This algorithm does not mark the original copy of the image but moderates the file size of the image. This type of density largely occurs in larger files as likened to lossy compression. Lossless compression is used to avoid the editing into a perfect original uncompressed image file.

**Lossy Compression:** The presentation of the image is perfectly preserved but likely the changes are made into the image which may appear like perfect copy. But during bit by bit analysis of the pixels you can see the compression of the pixels.

---

**IMAGE FORMATS**

<table>
<thead>
<tr>
<th>Photographic Images</th>
<th>Graphics, including Logos or Line art</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Properties</strong></td>
<td></td>
</tr>
<tr>
<td>Photos are continuous tones, 24-bit color or 8-bit Gray, no text, few lines and edges</td>
<td>Graphics are often solid colors, with few colors, up to 256 colors, with text or lines and sharp edges</td>
</tr>
<tr>
<td><strong>For Unquestionable Best Quality</strong></td>
<td></td>
</tr>
<tr>
<td>TIF or PNG (lossless compression and no JPG artifacts)</td>
<td>PNG or TIF (lossless compression, and no JPG artifacts)</td>
</tr>
<tr>
<td><strong>Smallest File Size</strong></td>
<td></td>
</tr>
<tr>
<td>JPG with a higher Quality factor can be decent.</td>
<td>TIF LZW or GIF or PNG (graphics/logos without gradients normally permit indexed color of 2 to 16 colors for smallest file size)</td>
</tr>
<tr>
<td><strong>Maximum Compatibility (PC, Mac, Unix)</strong></td>
<td></td>
</tr>
<tr>
<td>TIF or JPG</td>
<td>TIF or GIF</td>
</tr>
<tr>
<td><strong>Worst Choice</strong></td>
<td></td>
</tr>
<tr>
<td>256 color GIF is very limited color, and is a larger file than 24-bit JPG</td>
<td>JPG compression adds artifacts, smears text and lines and edges</td>
</tr>
</tbody>
</table>
Forensic Analysis of the Digital Image

By: Ivneet Singh

The image mentioned above relates to the case study mentioned earlier. This image depicts about World Trade Center in New York USA. The image was taken through Nikon Camera on January 2nd, 2001.

The Forensic property of this image is mentioned on the right side of the column. This image was extracted from the suspect’s laptop and various other similar images were found during the investigations.

MD5 Hash:
5B99E5CC1960D25891159FDE0632E07

SHA-1
Hash: C6937E5A2745ADB0D1821154C5997054FE2

A hash value is a result of a calculation (hash algorithm) that can be performed on a string of text, electronic file or entire hard drives contents. The result is also referred to as a checksum, hash code or hashes. Hash values are used to identify and filter duplicate files (i.e. email, attachments, and loose files) from an ESI collection or verify that a forensic image or clone was captured successfully.
**Note:** The image has been plotted with red marks to explain the difference between both images.

**IMAGE - 2**

The image mentioned above related to the case study discussed earlier. This image depicts about World Trade Center in New York USA. The image was taken previously through Nikon Camera and using some tools minor changes were done to the image by marking it with target.

By comparing the forensic properties of the images you can see the difference in the Hash Values, so this is the initial stage where you can identify that image contains some more information as its value has been changed with the previous copy.

**MD5 Hash:**

B0ECC1B2FB14137304AF6DAD077539F2

**SHA-1 Hash**

72F25164D6ED7D1482FAF773B8023D4CD425F091

**Fuzzy hashing** allows the investigator to focus on potentially incriminating documents that may not appear using traditional hashing methods. The use of the fuzzy hash is much like the fuzzy logic search; it is looking for similar documents but not exact equals, called homologous files. An example would be two word processor documents, with a paragraph added in the middle of one. To locate homologous files, they must be hashed traditionally, in segments, to identify the strings of identical binary data.
Inspecting Digital Image

By: Ivneet Singh

Once suspicious images have been identified we can analyze them by using fuzzy hashing or by manually checking the hash values of the images. During forensic analysis we have also noticed that no steganography technique was used in these images which were extracted from the suspect’s hard disk.

For further analysis of the image we need to develop various types of hypothesis to test the image.

By converting the image into audio file using uncompressed algorithm we can view and compare the waves of the image with one another. The comparison of wave will clearly display the results targeting the alteration in the image done.

The Image-1 mentioned above has been converted into waves with 24 bit PCM segment including 1 mono channel with 44188 Hz.

The Image-2 mentioned above has been converted into waves with 24 bit PCM segment including 1 mono channel with 44188 Hz.
Investigating Digital Evidence
By: Ivneet Singh

The comparison of two sounds wave are required to be done using a match algorithm tool. You can also notice the major difference among Image 1 and Image 2 wave sounds.

INVESTIGATIVE LEADS
Assuming the Image 2 was designed to target certain floors of the building while attack took place in “World Trade Center”. This type of information can be very useful for an investigator to further investigating the case to write a conclusive forensic report. By analyzing other different evidence which are also pointing towards the suspect’s, certain facts can be established in the court to prove his/her involvement in the attacks.
Conclusion

By: Ivneet Singh

A research was conducted to compare digital images for forensic investigation which might offer an expert to lead the case. This technique has been developed to compare and verify the digital images if certain changes has been made to the image files. Using this technique we can do depth analysis of suspicious image files.

Limitation and Restrictions

By: Ivneet Singh

Using the image wave technique we have tested various different formats of images but results were not much appreciated every time as it depends upon the image properties. This technique will help forensic expert to analyze the image file to some extent. The conclusive result may help the forensic expert to explain in court how two images are different from each other as the presentation of the image files looks perfectly similar.

Further research is being conducted to examine certain scanned documents to confirm the counterfeit nature of the documents. We have successfully examined some of the forged documents when compared them with the original agreements or bank statements. The results were very accurate in terms of comparing waves using uncompressed algorithms.

COMPUTER FORENSIC EXPERT

Mr. Ivneet Singh,

B.Sc. (H) UK, CCI, CIEH, CCL, AFE, CFE, Human Behavior Analysts (USA)

A qualified computer forensic expert and investigator from Staffordshire University, United Kingdom. Ivneet Singh has conducted a research study on Web-Biometric system for security enhancements in Malaysia.

Using professional forensic tools he has investigated and analyzed various cases which has assisted him to establish certain facts that were early denied by the suspect. He is also involved in providing guest lectures for Computer Forensic and Digital Fraud Examination to various Law Enforcement Agencies in and around South East Asia.

He has appeared as an Expert Witness in court to provide litigation support to the lawyers. He has been appointed as Head of Computer Forensic division in a leading Forensic Accounting and Investigative firm in Malaysia.