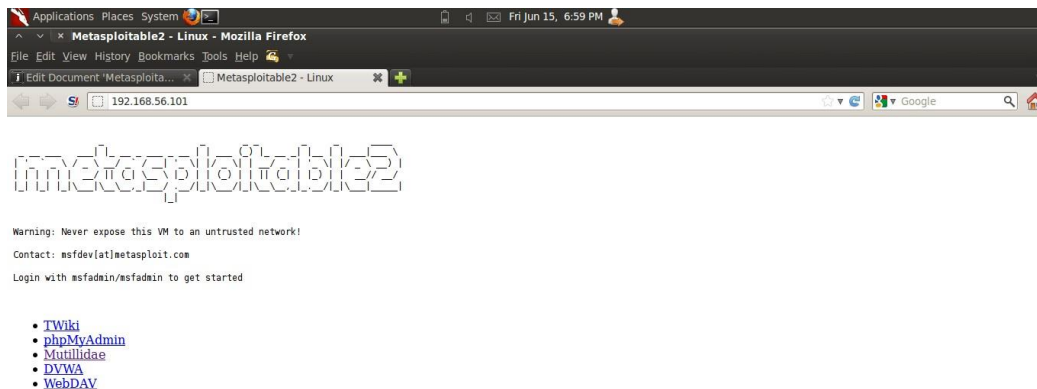


Vulnerable Web Services

Metasploitable 2 has deliberately vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. To access the web applications, open a web browser and enter the URL `http://<IP>` where `<IP>` is the IP address of Metasploitable 2. One way to accomplish this is to install Metasploitable 2 as a guest operating system in Virtual Box and change the network interface settings from "NAT" to "Host Only". (Note: A video tutorial on installing Metasploitable 2 is available [here](#).)

In this example, Metasploitable 2 is running at IP 192.168.56.101.

Browsing to `http://192.168.56.101/` shows the web application home page.



192.168.56/24 is the default "host only" network in Virtual Box. IP address are assigned starting from "101". Depending on the order in which guest operating systems are started, the IP address of Metasploitable 2 will vary.

To access a particular web application, click on one of the links provided. Individual web applications may additionally be accessed by appending the application directory name onto `http://<IP>` to create URL `http://<IP>/<Application Folder>/`. For example, the Mutillidae application may be accessed (in this example) at address `http://192.168.56.101/mutillidae/`. The applications are installed in Metasploitable 2 in the `/var/www` directory. (Note: See a list with command `ls /var/www`.) In the current version as of this writing, the applications are

- mutillidae (NOWASP Mutillidae 2.1.19)
- dvwa (Damn Vulnerable Web Application)
- phpMyAdmin
- tikiwiki (TWiki)
- tikiwiki-old

- dav (WebDav)

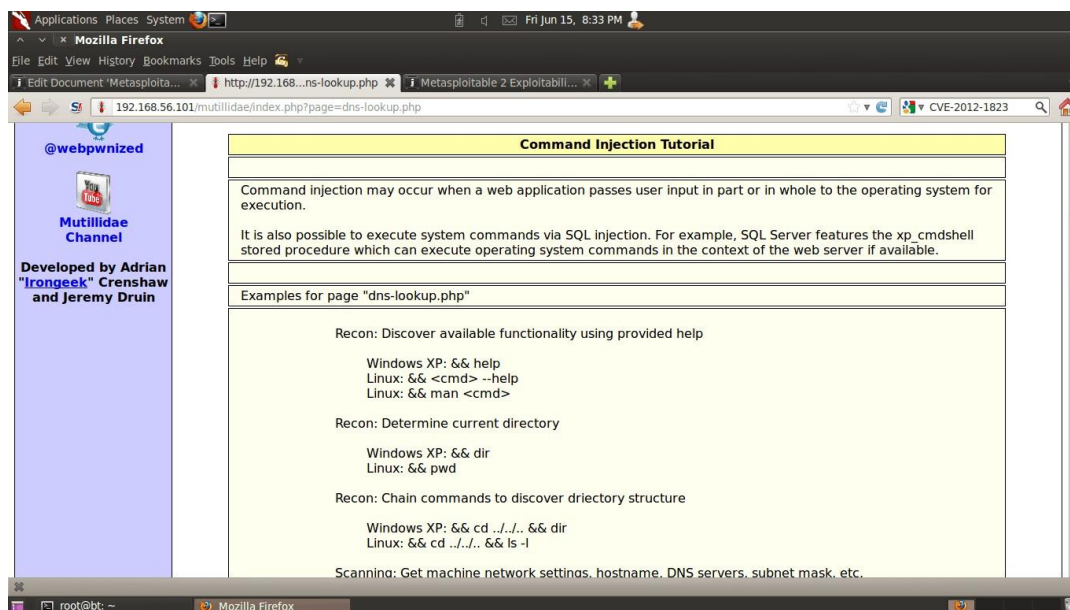
Mutillidae

The Mutillidae web application (NOWASP (Mutillidae)) contains all of the vulnerabilities from the OWASP Top Ten plus a number of other vulnerabilities such as HTML-5 web storage, forms caching, and click-jacking. Inspired by DVWA, Mutillidae allows the user to change the "Security Level" from 0 (completely insecure) to 5 (secure). Additionally three levels of hints are provided ranging from "Level 0 - I try harder" (no hints) to "Level 2 - noob" (Maximum hints). If the application is damaged by user injections and hacks, clicking the "Reset DB" button resets the application to its original state.

Tutorials on using Mutillidae are available at the webpwnized YouTube Channel.



Enable hints in the application by click the "Toggle Hints" button on the menu bar:



The Mutillidae application contains at least the following vulnerabilities on these respective pages:

Page	Vulnerabilities
add-to-your-blog.php	SQL Injection on blog entry SQL Injection on logged in user name Cross site scripting on blog entry Cross site scripting on logged in user name Log injection on logged in user name CSRF JavaScript validation bypass XSS in the form title via logged in username The show-hints cookie can be changed by user to enable hints even though they are not supposed to show in secure mode
arbitrary-file-inclusion.php	System file compromise Load any page from any site
browser-info.php	XSS via referer HTTP header JS Injection via referer HTTP header XSS via user-agent string HTTP header
capture-data.php	XSS via any GET, POST, or Cookie
captured-data.php	XSS via any GET, POST, or Cookie
config.inc*	Contains unencrypted database credentials
credits.php	Unvalidated Redirects and Forwards
dns-lookup.php	Cross site scripting on the host/ip field O/S Command injection on the host/ip field This page writes to the log. SQLi and XSS on the log are possible GET for POST is possible because only reading POSTed variables is not enforced.
footer.php*	Cross site scripting via the HTTP_USER_AGENT HTTP header.
framing.php	Click-jacking
header.php*	XSS via logged in user name and signature The Setup/reset the DB menu item can be enabled by setting the uid value of the cookie to 1
html5-storage.php	DOM injection on the add-key error message because the key entered is output into the error message without being encoded
index.php*	You can XSS the hints-enabled output in the menu because it takes input from the hints-enabled cookie value. You can SQL injection the UID cookie value because it is used to do a lookup You can change your rank to admin by altering the UID value HTTP Response Splitting via the logged in user name because it

Page	Vulnerabilities
	<p>is used to create an HTTP Header</p> <p>This page is responsible for cache-control but fails to do so</p> <p>This page allows the X-Powered-By HTTP header</p> <p>HTML comments</p> <p>There are secret pages that if browsed to will redirect user to the phpinfo.php page. This can be done via brute forcing</p>
log-visit.php	<p>SQL injection and XSS via referer HTTP header</p> <p>SQL injection and XSS via user-agent string</p>
login.php	<p>Authentication bypass SQL injection via the username field and password field</p> <p>SQL injection via the username field and password field</p> <p>XSS via username field</p> <p>JavaScript validation bypass</p>
password-generator.php	JavaScript injection
pen-test-tool-lookup.php	JSON injection
phpinfo.php	<p>This page gives away the PHP server configuration</p> <p>Application path disclosure</p> <p>Platform path disclosure</p>
process-commands.php	Creates cookies but does not make them HTML only
process-login-attempt.php	Same as login.php. This is the action page.
redirectandlog.php	Same as credits.php. This is the action page
register.php	SQL injection and XSS via the username, signature and password field
rene-magritte.php	Click-jacking
robots.txt	Contains directories that are supposed to be private
secret-administrative-pages.php	This page gives hints about how to discover the server configuration
set-background-color.php	Cascading style sheet injection and XSS via the color field
show-log.php	<p>Denial of Service if you fill up the log</p> <p>XSS via the hostname, client IP, browser HTTP header, Referer HTTP header, and date fields</p>
site-footer-xss-discussion.php	XSS via the user agent string HTTP header
source-viewer.php	Loading of any arbitrary file including operating system files.

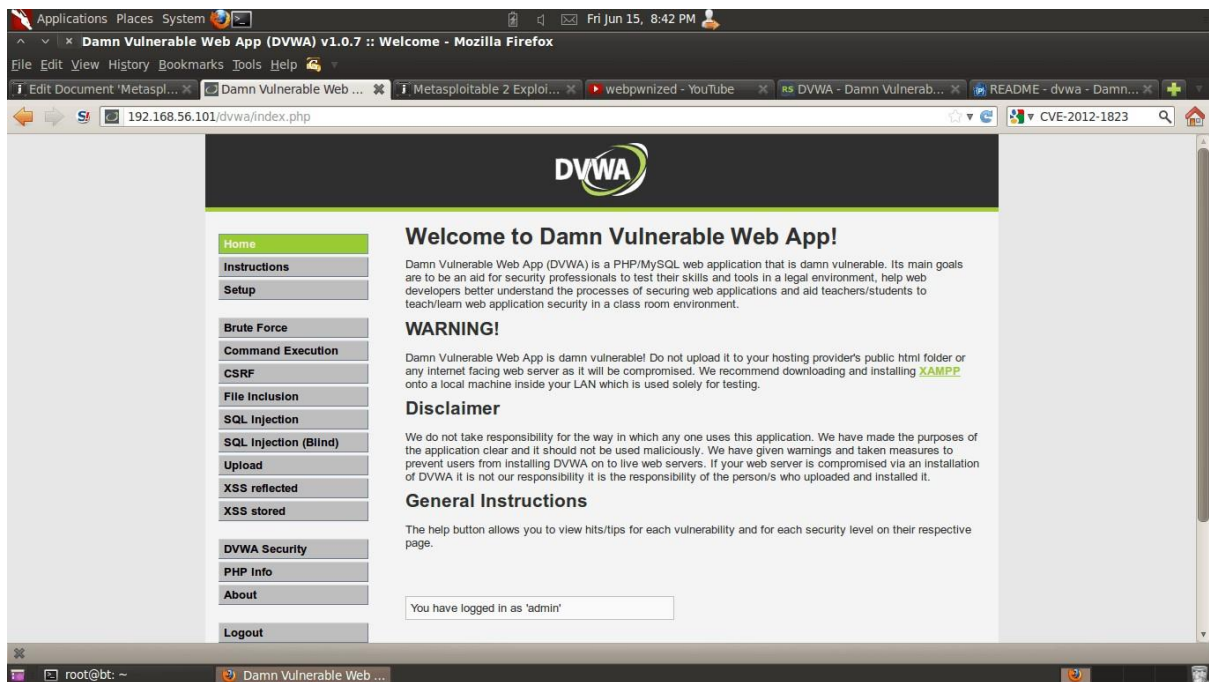
text-file-viewer.php	Loading of any arbitrary web page on the Internet or locally including the site's password files. Phishing
Page	Vulnerabilities
user-info.php	SQL injection to dump all usernames and passwords via the username field or the password field XSS via any of the displayed fields. Inject the XSS on the register.php page. XSS via the username field
user-poll.php	Parameter pollution GET for POST XSS via the choice parameter Cross site request forgery to force user choice
view-someones-blog.php	XSS via any of the displayed fields. They are input on the add to your blog page.

DVWA

From the DVWA home page: "Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment."

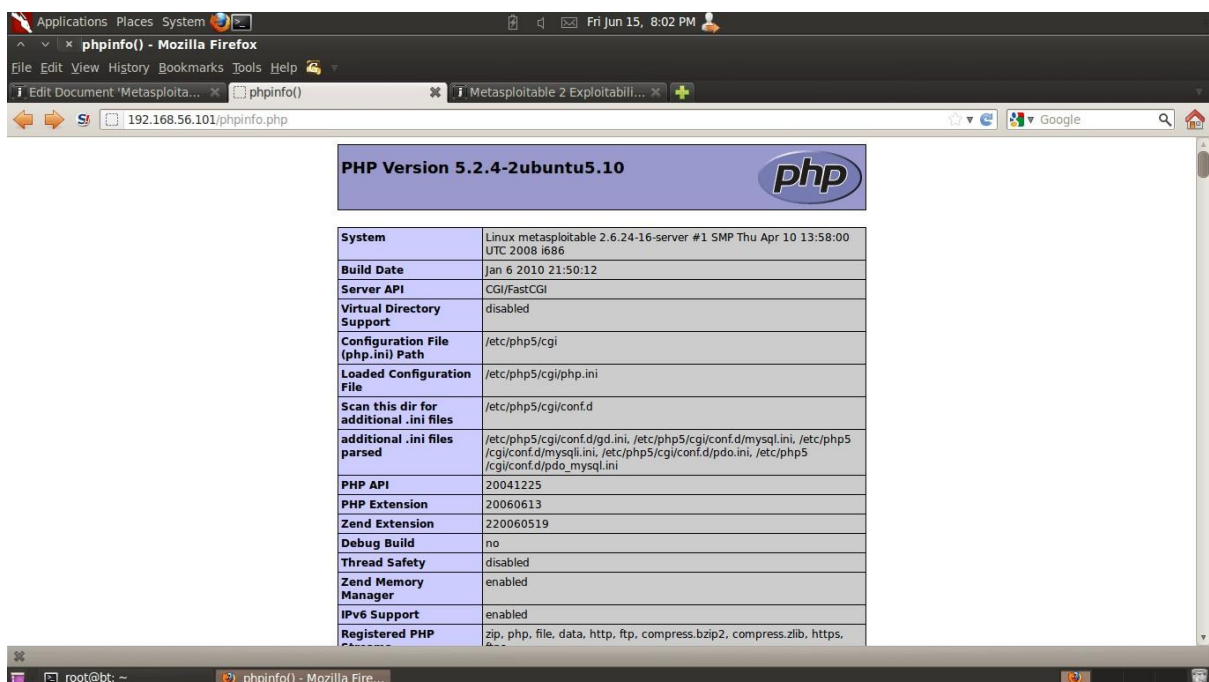
DVWA contains instructions on the home page and additional information is available at [Wiki Pages - Damn Vulnerable Web App](#).

- **Default username** - admin
- **Default password** - password



Information Disclosure

Additionally, an ill-advised PHP information disclosure page can be found at <http://<IP>/phpinfo.php>. In this example, the URL would be <http://192.168.56.101/phpinfo.php>. The PHP info information disclosure vulnerability provides internal system information and service version information that can be used to look up vulnerabilities. For example, noting that the version of PHP disclosed in the screenshot is version 5.2.4, it may be possible that the system is vulnerable to [CVE-2012-1823](#) and [CVE2012-2311](#) which affected PHP before 5.3.12 and 5.4.x before 5.4.2.



EXPLOITING A WEB SERVER:-

What we will need

- A target www.techpanda.org
- Bing search engine
- SQL Injection Tools
- PHP Shell, we will use dk shell <http://sourceforge.net/projects/icfdkshell/>

Information gathering

We will need to get the IP address of our target and find other websites that share the same IP address.

We will use an online tool to find the target's IP address and other websites sharing the IP address

- Enter the URL <https://www.yougetsignal.com/tools/web-sites-on-web-server/> in your web browser
- Enter www.techpanda.org as the target



Reverse IP Domain Check

Remote Address:

Find other sites hosted on a web server by entering a domain or IP address above.

[about](#)

Note: For those of you interested, as of August 2012, my database has grown to over 60 million domain names. I offering this [domain list for purchase](#).

A reverse IP domain check takes a domain name or IP address pointing to a web server and searches for other

- Click on Check button
- You will get the following results

Reverse IP Domain Check

IP ADDRESS: 69.195.124.112

Remote Address

Found 403 domains hosted on the same web server as www.techpanda.org (69.195.124.112)

It appears that the web server located at 69.195.124.112 may be hosting one or more web sites with explicit content. The web sites in question are highlighted in red below. There is a possibility that all of the web sites on this web server are blocked by web filtering software. Search engine rankings for these web sites may be affected as well.

809restaurant.com	ableselfstorageofga.com
abravnewme.org	achievemetam.com
ada95.com	addocumentum.com
adoptembryos.org	advantagessolarpower.com
afrostarusa.com	aiplenercon.com
alchemywoodshop.com	aldaracream.org
alexwellerstein.com	alusso.com
amanrehman.com	andrewbrooksvfx.com
apple-of-my-eye.com	asgardalliancecorp.com
assaultonpatcongcreek.com	avengerspart2.com
bartendingtraininghq.com	batesline.com
benandthehicks.com	benblumstein.com
bestmindframe.com	bing.com
blog.saltoquantico.org	bloombrandgroup.com
boardsandpowder.com	boarsbucksandbruins.com
bowersremodeling.com	bpwebmedia.com
braincentrifuge.com	brainygroveland.com
briankimskey.com	bulletin.iit2013.org
cagdeepak.com	cannes4u.com
cdilearning.com	choeun.org
christalivechurch.org	cityfarmhouse.com
clan4.net	claraofarrell.net
cleveronlinetutorials.com	cmawaterlab.com
compurig.com	coreywoodsinc.com
cosmic-reflections.com	crossfithv.com
cvesystems.com	cyberfeeder.com
danthagen.com	davidhgalley.com

Based on the above results, the IP address of the target is 69.195.124.112

We also found out that there are 403 domains on the same web server.

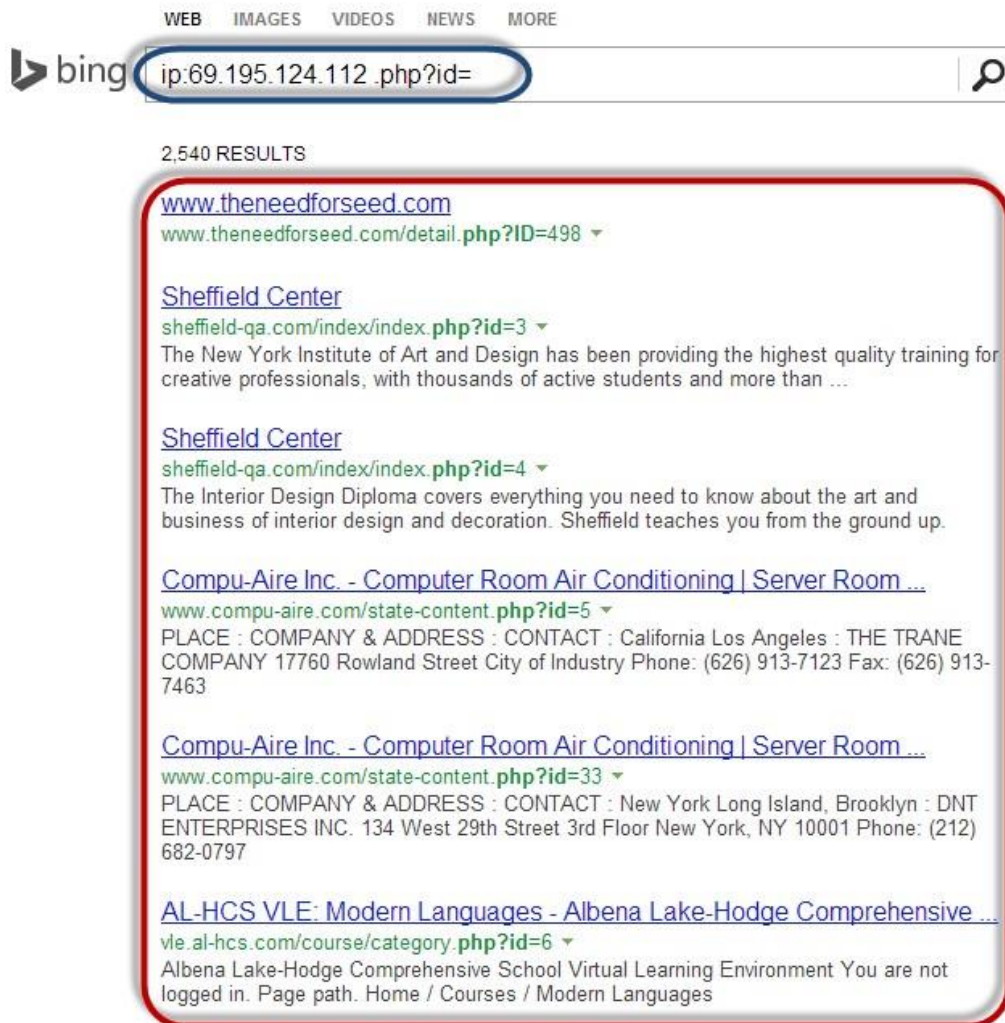
Our next step is to scan the other websites for SQL injection vulnerabilities. Note: if we can find a SQL vulnerable on the target, then we would directly exploit it without considering other websites.

- Enter the URL www.bing.com into your web browser. This will only work with Bing so don't use other search engines such as google or yahoo
- Enter the following search query `ip:69.195.124.112 .php?id=`

HERE,

- "ip:69.195.124.112" limits the search to all the websites hosted on the web server with IP address 69.195.124.112
- ".php?id=" search for URL GET variables used as parameters for SQL statements.

You will get the following results



As you can see from the above results, all the websites using GET variables as parameters for SQL injection have been listed.

The next logic step would be to scan the listed websites for SQL Injection vulnerabilities. You can do this using manual SQL injection or use tools listed in this article on SQL Injection.

Uploading the PHP Shell

We will not scan any of the websites listed as this is illegal. Let's assume that we have managed to login into one of them. You will have to upload the PHP shell that you downloaded from <http://sourceforge.net/projects/icfdkshell/>

- Open the URL where you uploaded the dk.php file.
- You will get the following window

[Files] [Console] [SafeMode] [Sql] [Php] [String tools] [Bruteforce] [Network] [Symlink] [Logout]					
Count:	Domain	User	Symlink	Link to the files	crawl
1	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
2	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
3	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
4	[REDACTED].com	[REDACTED]	[REDACTED]		Crawl
5	[REDACTED].org	[REDACTED]	[REDACTED]		Crawl
6	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
7	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
8	[REDACTED]	[REDACTED]	[REDACTED]		Crawl
9	[REDACTED]	[REDACTED]	[REDACTED]		Crawl

- Clicking the Symlink URL will give you access to the files in the target domain.

Once you have access to the files, you can get login credentials to the database and do whatever you want such as defacement, downloading data such as emails, etc.

Summary:-

- Web server stored valuable information and are accessible to the public domain. This makes them targets for attackers.
- The commonly used web servers include Apache and Internet Information Service IIS
- Attacks against web servers take advantage of the bugs and Misconfiguration in the operating system, web servers, and networks
- Popular web server hacking tools include Neosploit, MPack, and Zeus.
- A good security policy can reduce the chances of been attacked

STEGANOGRAPHY:-

Steganography is the practice of concealing a message within another message or a physical object. In computing/electronic contexts, a computer file, message, image, or video is concealed within another file, message, image, or video.

WORKING OF STEGANOGRAPHY:-

Steganography replaces unneeded or unused bits in regular computer files (Graphics, sound, text) with bits of different and invisible information. Hidden information can be any other regular computer file or encrypted data.

Steganography differs from cryptography in a way that it masks the existence of the message where cryptography works to mask the content of the message.

Steganography sometimes used in conjunction with encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden information is not seen.

TYPES OF STEGANOGRAPHY:-

There are different ways to hide the message in another, well known are Least Significant bytes and Injection.

When a file or an image is created there are few bytes in the file or image which are not necessary or least important. These type of bytes can be replaced with a message without damaging or replacing the original message, by which the secret message is hidden in the file or image.

Another way is a message can be directly injected into a file or image. But in this way the size of the file would be increasing accordingly depending on the secret message

STEGANOGRAPHY IN IMAGE:-

Digital images are the most widely used cover objects for steganography. Due to the availability of various file formats for various applications the algorithm used for these formats differs accordingly.

An image is collection of bytes (known as pixels for images) containing different light intensities in different areas of the image. When dealing with digital images for use with Steganography, 8-bit and 24-bit per pixel image files are typical. Both have advantages and disadvantages 8-bit images are a great format to use because of their relatively small size. The drawback is that only 256 possible colors can be used which can be a potential problem during encoding. Usually a gray scale color palette is used when dealing with 8-bit images such as (.GIF) because its gradual change in color would be harder to detect after the image has been encoded with the secret message. 24-bit images offer much more flexibility when used for Steganography. The large numbers of colors (over 16 million) that can be used go well beyond the human visual system (HVS), which makes it very hard to detect once a secret message, has been encoded.

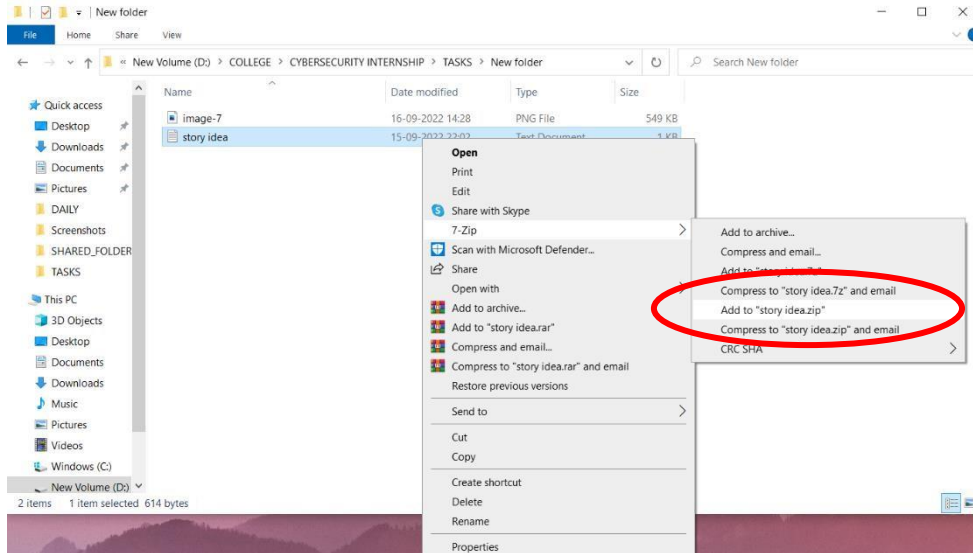
Large amount of data can be encoded in to 24-bit images as it is compared to 8-bit images. The drawback of 24-bit digital images is their size which is very high and this makes them suspicious our internet due to their heavy size when compared to 8-bit images. Depending on the type of message and type of the image different algorithms are used.

Few types in Steganography in Images:

1. Least significant bit insertion:- Least Significant Bit (LSB) insertion is most widely known algorithm for image steganography ,it involves the modification of LSB layer of image. In this technique,the message is stored in the LSB of the pixels which could be considered as random noise.Thus, altering them does not have any obvious effect to the image.
2. Masking and filtering:- Masking and filtering techniques work better with 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking the images changes the images. To ensure that changes cannot be detected make the changes in multiple small proportions. Compared to LSB masking is more robust and masked images passes cropping, compression and some image processing. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the “noise” level. This makes it more suitable than LSB with, for instance, lossy JPEG images.
3. Redundant Pattern Encoding:- Redundant pattern encoding is to some extent similar to spread spectrum technique. In this technique, the message is scattered through out the image based on algorithm. This technique makes the image ineffective for cropping and rotation. Multiple smaller images with redundancy increase the chance of recovering even when the stegano-image is manipulated.
4. Encrypt and Scatter:- Encrypt and Scatter techniques hides the message as white noise and White Noise Storm is an example which uses employs spread spectrum and frequency hopping. Previous window size and data channel are used to generate a random number.And with in this random number ,on all the eight channels message is scattered through out the message.Each channel rotates,swaps and interlaces with every other channel. Single channel represents one bit and as a result there are many unaffected bits in each channel. In this technique it is very complex to draw out the actual message from stegano-image. This technique is more secure compared to LSB as it needs both algorithm and key to decode the bit message from stegano-image. Some users prefer this methos for its security as it needs both algorithm and key despite the stegano image. This method like LSB lets image degradation in terms of image processing, and compression.
5. Least significant bit insertion:- LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF. JPEG images use the discrete cosine transform to achieve compression. DCT is a

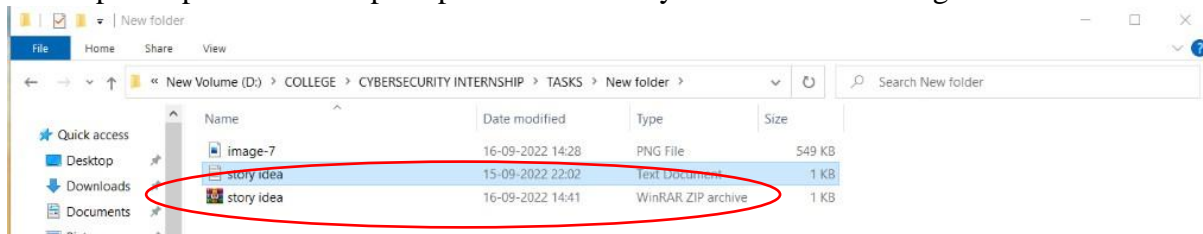
lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT.

Step -1 - convert the text into a zip file.



And the zip file is created.

Step-2:- open command prompt in that directory and do the following command



“copy /b <image.jpg>+<text_zip_file> <new_image_name.jpg>”

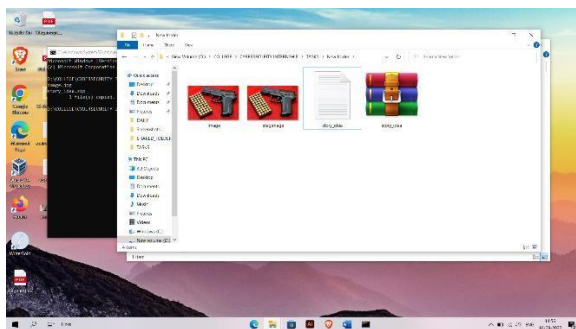
Ex:- copy /b image.jpg+story_idea.zip stegimage.jpg

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19044.1889]
(c) Microsoft Corporation. All rights reserved.

D:\COLLEGE\CYBERSECURITY INTERNSHIP\TASKS\New folder>copy /b image.jpg+story_idea.zip stegimage.jpg
image.jpg
story_idea.zip
1 file(s) copied.

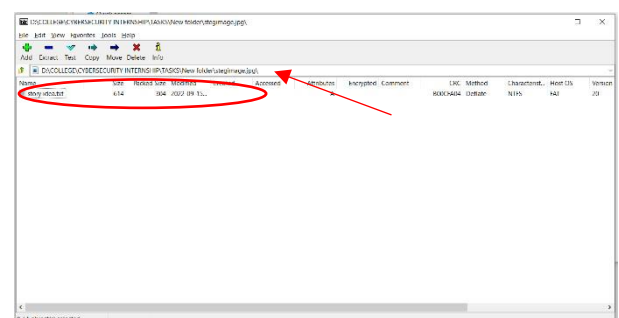
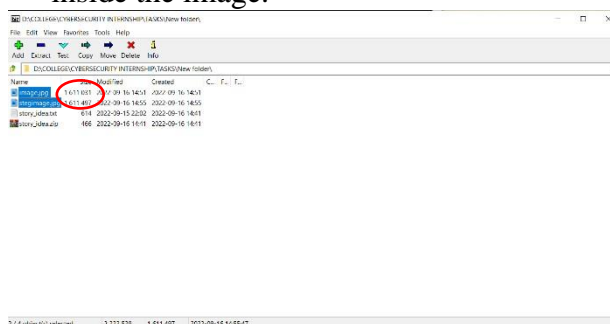
D:\COLLEGE\CYBERSECURITY INTERNSHIP\TASKS\New folder>
```

And we can see that a new image is created.



But there is a size change in the files, which means there is some extra information in that picture.

When we open the image in 7 zip file manager we can see that there is a text file inside the image.



We also can use steghide and embed a message into a image.

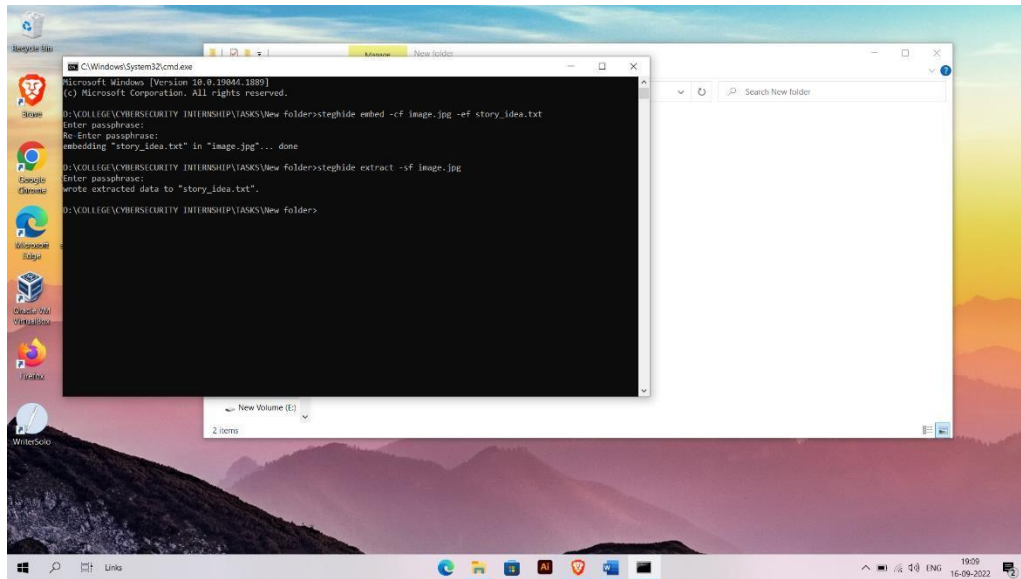
Steghide has many arguments that can be used for desired outputs.

Step-2:- now to extract we use the command. (steghide extract -sf <image.jpg>)

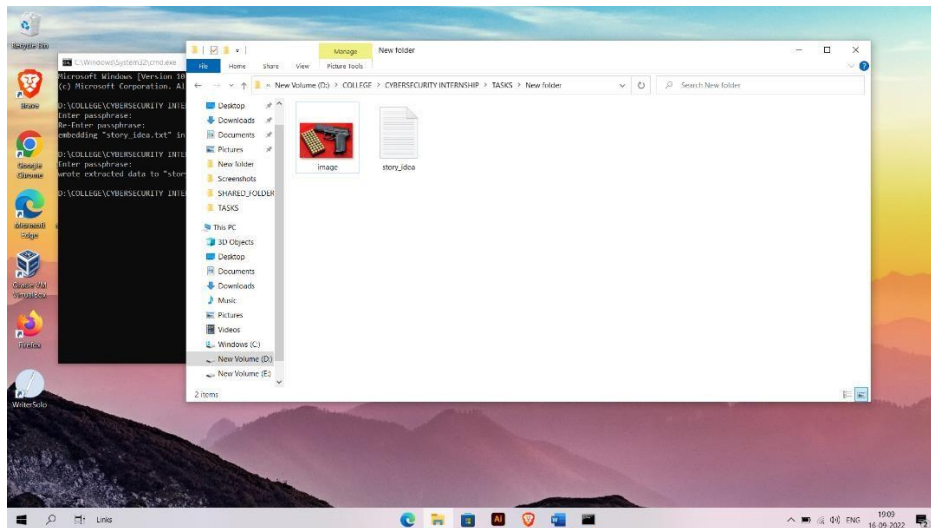
Ex:- steghide extract -sf image.jpg

Then it will ask for the pass phrase that is also a password.

After entering the password we see that the file is extracted out.



We can see that the file is extracted.



Other image steganography methods are:-

Steganographic Tools

Tool	Description
Stegosuite	Hide text inside any image
Stegohide	Hide secret file in image or audio file.
Xiao Steganography	Free software that can be used to hide secret files in BMP images or in WAV files.
SSuite Pícel	Portable application to hide text inside image file
OpenPuff	Tool to conceal files in image, audio & flash files
Camouflage	Tool that lets you hide any type of file inside of file.

STEGANOGRAPHY IN AUDIO:-

Implanting secret message into an audio is the most challenging technique in Steganography. This is because the human auditory system (HAS) has such a vibrant range that it can listen over. To put this in perspective, the (HAS) recognize over a range of power greater than one million to one and a range of frequencies greater than one thousand to one making it extremely hard to add or remove data from the original data structure. The only weakness in the (HAS) comes at trying to differentiate sounds (loud sounds drown out quiet sounds) and this is what must be exploited to encode secret messages in audio without being detected.

Below are the lists of methods which are commonly used for audio Steganography.

1. **LSB coding:-** Using the least-significant bit is possible for audio, as modifications usually would not create recognizable changes to the sounds. Another method takes advantage of human limitations. It is possible to encode messages using frequencies that are indistinct to the human ear. Using frequencies above 20.000Hz, messages can be hidden inside sound files and can not be detected by human checks.
2. **Parity coding:-** Instead of breaking a signal down into individual samples, the parity coding method breaks a signal down into separate regions of samples and encodes each bit from the secret message in a sample region's parity bit. If the parity bit of a selected region does not match the secret bit to be encoded, the process flips the LSB of one of the samples in the region. Thus, the sender has more of a choice in encoding the secret bit, and the signal can be changed in a more unobtrusive fashion.
3. **Phase coding:-** Phase coding attends to the disadvantages of the noise inducing methods of audio Steganography. Phase coding uses the fact that the phase components of sound are not as audible to the human ear as noise is. Rather than introducing perturbations, this technique encodes the message bits as phase shifts in the phase spectrum of a digital signal, attaining an indistinct encoding in terms of signal-to-perceived noise ratio.

4. Spread spectrum:- In the context of audio Steganography, the basic spread spectrum (SS) method attempts to spread secret information across the audio signal's frequency spectrum as much as possible. This is comparable to a system using an implementation of the LSB coding that randomly spreads the message bits over the entire audio file. However, unlike LSB coding, the SS method spreads the secret message over the sound file's frequency spectrum, using a code that is independent of the actual signal. As a result, the final signal occupies a bandwidth in excess of what is actually required for broadcast.
5. Echo hiding:- In echo hiding, information is implanted in a sound file by introducing an echo into the separate signal. Like the spread spectrum method, it too provides advantages in that it allows for a high data transmission rate and provides superior strength when compared to the noise inducing methods. If only one echo was produced from the original signal, only one bit of information could be encoded.

Therefore, the original signal is broken down into blocks before the encoding process begins. Once the encoding process is completed, the blocks are concatenated back together to create the final signal.

Tools used for audio steganography:-

Wavsteg[Permalink](#)

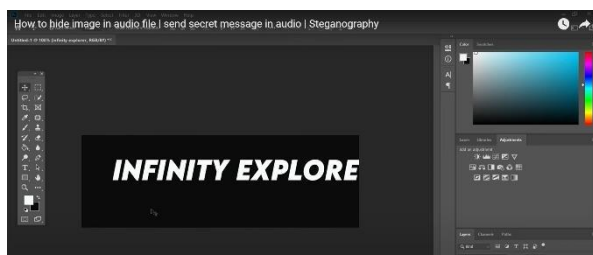
WavSteg is a python3 tool that can hide data and files in wav files and can also extract data from wav files.

You can get it from [github](#)

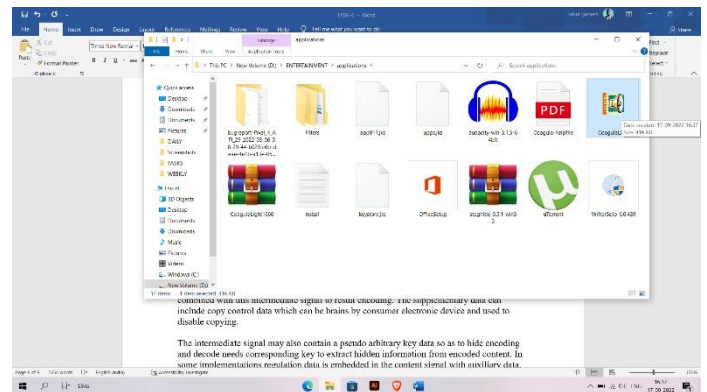
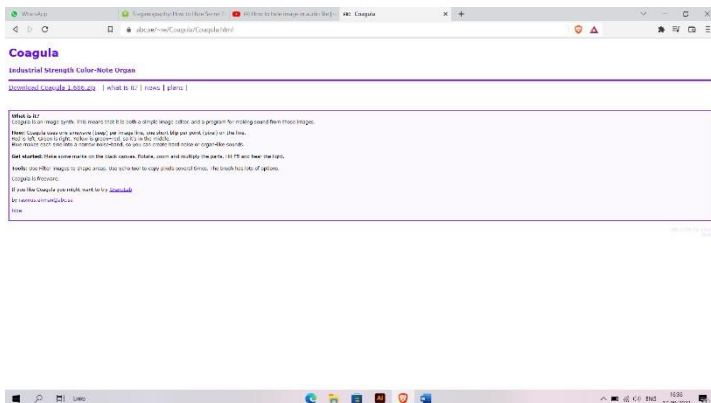
Sonic visualizer[Permalink](#)

Sonic visualizer is a tool for viewing and analyzing the contents of audio files, however it can be helpful when dealing with audio steganography. You can reveal hidden shapes in audio files.

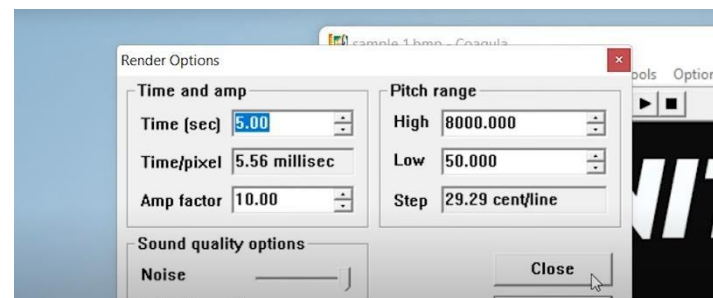
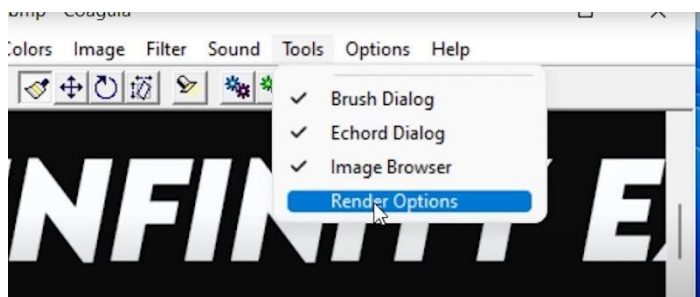
Step 1:- create a image with a bit map extension, where the text is white and the background is black.



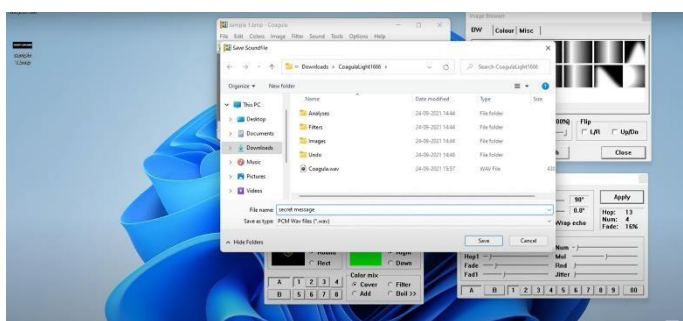
Step-2:- now download a software called coagula to convert the image that has text into an audio file.



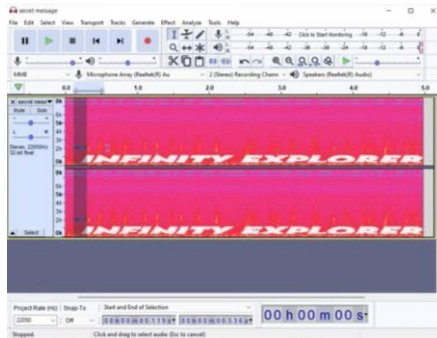
step-3:- we open the image in coagula tools>render options (to convert the image into audio)



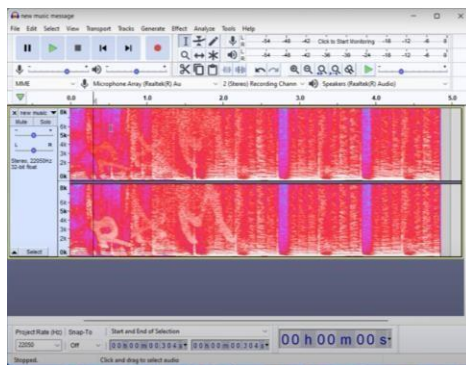
and save the audio in the desired folder.



Step-4:- now import the image into audacity.
And watch it in spectrogram.



Now if we export a new audio under this file and save both the audios as a single file we get a final output something like this.



STEGANOGRAPHY IN VIDEO:-

In video steganography, a video file would be embedded with supplementary data to hide secret messages. In the process, an intermediate signal which is a function of hidden message data and data of content signal would be generated. Content data (video file) is then combined with this intermediate signal to result encoding. The supplementary data can include copy control data which can be brains by consumer electronic device and used to disable copying.

The intermediate signal may also contain a pseudo arbitrary key data so as to hide encoding and decode needs corresponding key to extract hidden information from encoded content. In some implementations regulation data is embedded in the content signal with auxiliary data. This regulation data consists of known properties enabling its identification in the embedded content signal. This encoding is robust against scaling, resampling and other forms of content degradation, so that the supplementary data can be detected from the content which might have been degraded.

There are different approaches for video steganography apart from the above mentioned. Most widely known are listed and discussed below.

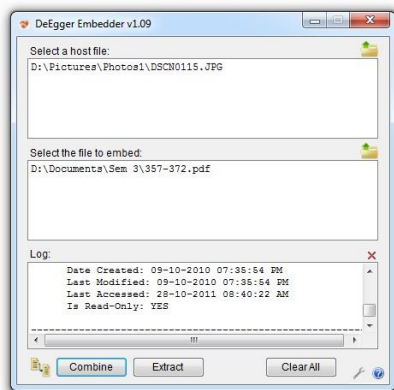
1. **Least Significant Bit Insertion:-** This is the most simple and popular approach for all types of steganography. In this method the digital video file is considered as separate frames and changes the displayed image of each video frame. LSB of 1 byte in the image is used to store the secret information. Effecting changes are too small to be recognized by human eye. This method enhances the capacity of the hidden message but compromises the security requirements such as data integrity.

2. Real time video steganography:- This kind of steganography involves hiding information on the output image on the device. This method considers each frame shown at any moment irrespective of whether it is image; text .The image is then divided into blocks. If pixel colors of the blocks are similar then changes color characteristics of number of these pixels to some extent. By labeling each frame with a sequence number it would even be easy to identify missing parts of information. To extract the information, the displayed image should be recorded first and relevant program is used then.

Tools:-

DeEgger is one of the tools for video steganography to embed text files into a video and to extract embedde text from a video.

1. Select Your Host file via drag and drop or using browser button
2. Select the file which you want to embed via drag and drop or by using browser button
3. Click on *Combine*
4. Now a dialog will come which will allow you to store the embedded file on your disk.



DeEgger Embedder:- That's all. Now your file is completely hidden in the hist file and secure from third person. Now you need to transfer that file to your friend.

Once your friend received that file, he or she will again use **DeEgger embeddR** to separate the files from each other. To extract the file you can follow this steps

1. Select the received file as host file
2. Click on *Extract*
3. That's all. Now a pop up will appear on your screen asking you location for saving embedded file

STEGANOGRAPHY IN DOCUMENTS:-

Steganography in documents just focuses on altering some of its characteristics. They can either be characteristics of text or even text formatting. Below are few ways listed and discussed to implement the same.

Since everyone can read, encoding text in neutral sentences is doubtfully effective. But taking the first letter of each word of the previous sentence, one can see that it is possible and not very difficult. Hiding information in plain text can be done in many different ways. One way is by simple adding white space and tabs to the ends of the lines of the document. The last technique was successfully used in practice and even after a text has been printed and copied on paper for ten times, the secret message could still be retrieved.

Another possible way of storing a secret inside a text is using a publicly available cover source, a book or a newspaper, and using a code which consists for example of a combination of a page number, a line number and a character number. This way, no information stored inside the cover source leads to the hidden message. Discovering it depends exclusively on gaining knowledge of the secret key.

Setting background color and font color is one of the mainly used steganographic approach. This method is focused for Microsoft word documents. Choose predefined colors and set font and background colors of invisible characters such as space, tab or the carriage return characters. R,G,B values are 8 bits means we have allowed range of 0 to 255. Most of the viewers would not feel interested about color values of these invisible characters hence 3 bytes of information is easily hidden in each occurrence of space, tab or carriage return. This approach needs no extra information to hide required bits.