The Ease of Steganography and Camouflage

John Bartlett

The Ease of Steganography and Camouflage

GSEC V1.3

John Bartlett

17 March, 2002

ABSTRACT

Steganography has a history that is of equal to any Information Technology operating in society today. Dating back to ancient Greek history "The Greek historian Herodotus describes how one of his cunning countrymen sent a secret message warning of an invasion by scrawling it on the wood underneath a wax tablet."[1] The history of steganography developed throughout the years and is becoming a threat to everyone alive. But how easy is steganography? Does the knowledge exist to counter steganography?

The ease of use in steganography has proliferated so that any person with a computer and an Internet connection can perform steganography on virtually any file. The programs that are available range from Unix and Windows based to command line or graphical user interface (GUI). Camouflage Software is easy to use, install, and a very versatile steganography tool that is free of charge and available for download to anyone with an Internet connection. In this paper we will look at the ease of use of one particular program, and the ability to detect steganographic material created by the program. "Camouflage allows you to hide files by scrambling them and then attaching them to the file of your choice."[2] Though this ease of use makes steganography highly available and threatening, it also presents obvious indications that a file has been used for steganographic purposes.

CAMOUFLAGE

Steganography techniques of the past have required extensive planning and cooperation to ensure success. Something as simple as lemon juice on paper or hidden text written on a bald mans head where older forms of steganography. As easy as they were to implement, both parties had to know what was occurring to ensure the success of the delivered message. These simple forms of steganography also limited the usefulness to the media in which they were implemented. An image would be very hard to draw with lemon juice, as would a plan on a shaved head.

Technology and the proliferation of steganography have eliminated many of the limitations of the past. Software programs can be found in numerous places on the Internet, propagating the steganographic material. **http://members.tripod.com/steganography/stego/software.html** and **http://www.topology.org/soft/crypto.html** are two of the many sites available to download steganography programs. Software has also become easier to use and more functional as technology has progressed. Though this progression has been rapid in many aspects, steganography is just starting to emerge with more powerful and full featured programs. Many steganography programs are very simple to use but have limited capability in the files used for steganography purposes. Camouflage software is a program that has eliminated the need for graphics, text files or any other specific source.

"Steganography derives from the Greek steganos, hidden or covered, plus graphein, to write."[3] The software program used to hide the information can use many techniques including insertion, injection, and substitution. Camouflage will take virtually any file format and append or "camouflage" it to any other type of file format. The result is a camouflaged file that behaves as the file used for the process.

REQUIREMENTS

The ability to run a steganography program no longer requires special equipment, extensive amounts of time or known shared keys. In the past, all parties involved with a file that had hidden data had to be aware of the file and how it was hidden. Today, as long as two people have the correct software installed, there is no need to know of the act. A simple check of the file will answer the question of whether or not there is hidden information. Camouflage software downloadable at **http://www.camouflagesoftware.com** requires Windows 95, Windows 98, Windows ME, Windows NT, or Windows 2000. With these minimal requirements, the hardware needed to use steganography is also abundantly available. The downloaded program is available as a self-extracting executable or as a zip file. If the zip file is chosen, a decompression software program will also be need to extract the file. Camouflage is oriented to the Windows operating system making the final requirement a simple browser program such as file manager or windows explorer. To accomplish the entire Steganography process, the program must be installed on both the senders and the receivers systems with the password shared if used.

INSTALLATION

After downloading and extracting if needed, the Camouflage program is a self-executing file that will step through the installation process. It is important to note during the installation that the licensing agreement specifically states the software is not to be used for illegal purposes. The installation program will complete and will be operational with very little effort. During installation the option is given as to where the executable will be located (program files) by default. After installation is complete, the program will appear in both the start menu and as right click options in Windows explorer. Figures 1 and 2 show the modified options Camouflage installed. Camouflage will appear in the add/remove programs menu making it easy to remove. This also is an example of the poor security associated with camouflage making it detectable to anyone that has access to the add/remove programs menu. Installation adds the following keys to a Windows 2000 registry after installation:

HKEY_CLASSES_ROOT*\shellex\ContextMenuHandle\Camouflage\Default
HKEY_CLASSES_ROOT\CamouflageShell.ShellExt\Default
HKEY_CLASSES_ROOT\CLSID\CamoufalgeShellExt
HKEY_CLASSES_ROOT\TypeLib\SID\3.0\Default
HKEY_CLASSES_ROOT\TypeLib\SID\3.0\0\Win32\Default
HKEY_CLASSES_ROOT\TypeLib\SID\3.0\HELPDIR\Default
HKEY_CURRENT_USER\Software\Camouflage\Default
HKEY_CURRENT_USER\Software\Camouflage\CamouflageFile
HKEY_CURRENT_USER\Software\Camouflage\frmMain\CamouflageFileList
HKEY_CURRENT_USER\Software\Camouflage\frmMain\UncamouflageFileList
HKEY_CURRENT_USER\Software\Camouflage\Settings

In addition to the above registry settings, there are also numerous settings applied to HKEY_LOCAL_MACHINE and standard windows settings for menus and options. These entries seem minor though there are some very important aspects of two of the entries in particular. These key entries will be re-addressed when the flaws of Camouflage are brought together. Installation takes no longer then a couple of minutes and the capability to perform steganography have been added to the toolbox. The

installation of Camouflage is the first step into the world of steganography and the ease at which it can be accomplished.

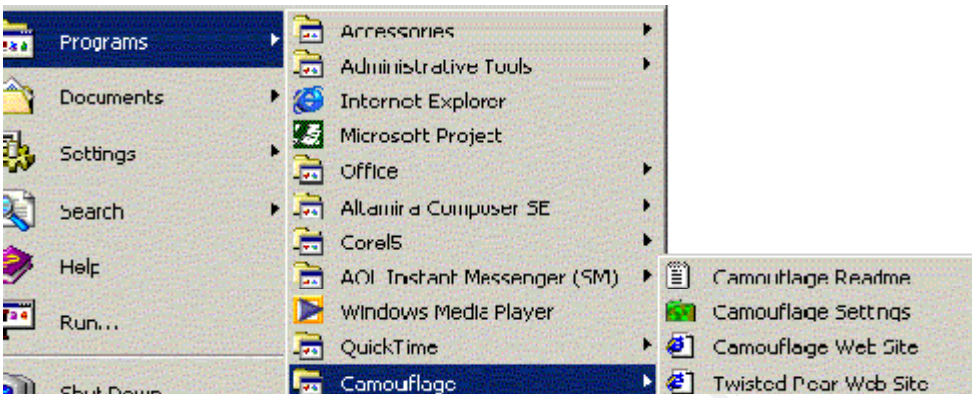

Figure 1. – Start Menu

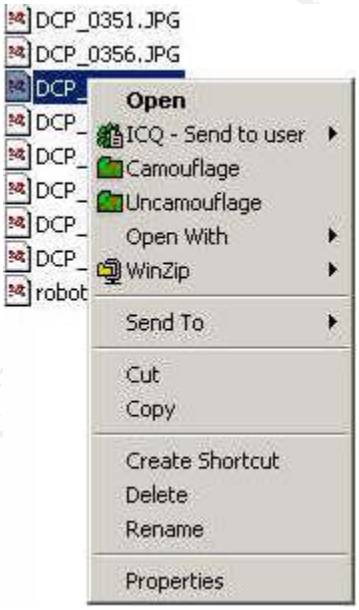

Figure 2.- Explorer Right Click

OPTIONS

The options presented with Camouflage are few, yet can be very useful. The settings of the program allow file details to be shown by a simple checkbox. The file details include size, created, modified, accessed and attributes. The program also has a checkbox to make the camouflaged file read only. This is checked by default to ensure the camouflaged file does not get corrupted. To remove the right click menu for camouflage, a simple checkbox will suffice. This combined with the ability to rename the instance of camouflage on the start menu is a perfect way to conceal the program from the average person. The software also has a link to get updates making it very easy to stay up to date with the latest changes.

CAMOUFLAGING FILES

Using Camouflage is as easy as right clicking a file and selecting the camouflage option. Figure 3 is the Camouflage window as it appears after selecting a file to camouflage.

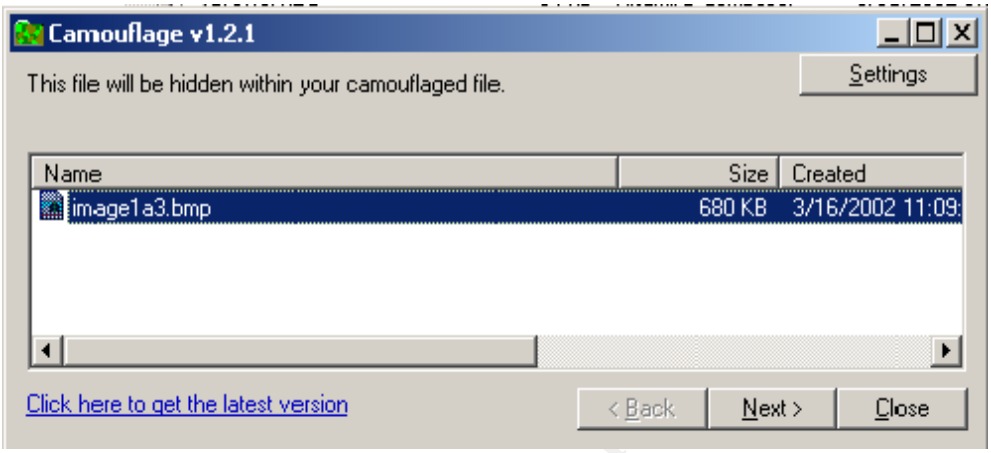

Figure 3.

The image selected "image1a3.bmp" is the image that will be camouflaged in a file selected at a later step. Note the size of the image at this point is 680KB. Selecting next will bring up Figure 4, the file selection in which to embed the image.

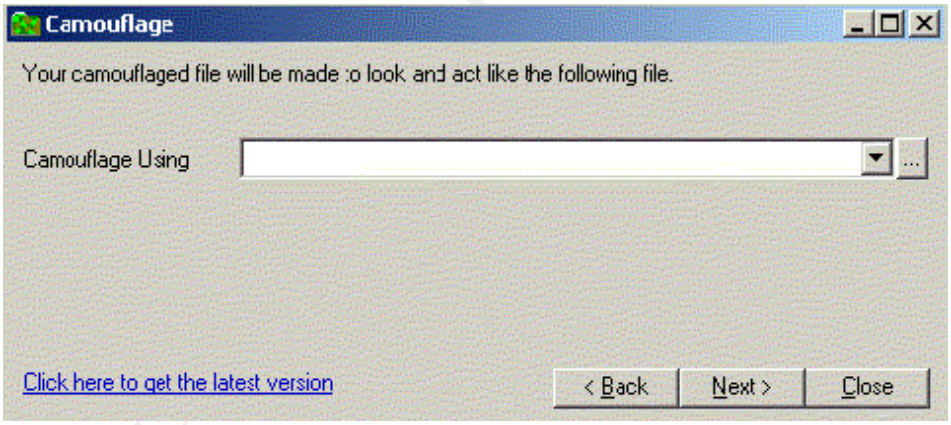

Figure 4.

At this point in the camouflage process using the browse button next to the arrow can choose a file. The file chosen can be of virtually any format and does not require consistency in the file formats. After selecting a file, the option to rename the new camouflaged file will appear as in Figure 5. Note in the figure there are two key items that are important. First, the name of the new file is in no way associated with the original file. A bitmap was chosen to camouflage and a text file is used to store the camouflage (this becomes important later when the ability to detect camouflage is discussed). Secondly, the ability to verify the file is read only is once again presented to ensure corruption of the file will not occur. The combination of various file names and read only present a very easy way to perform steganography.

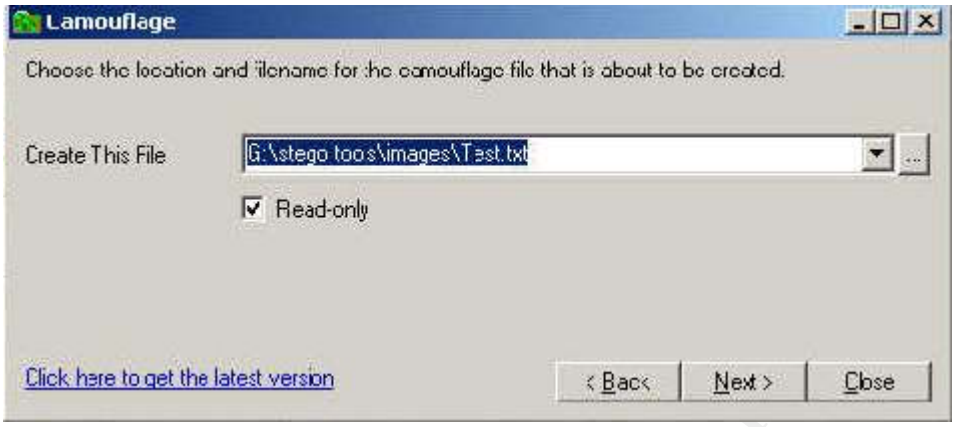

Figure 5.

The final screen presented in operations is yet another way to make the file more secure. A stored password on the file is optional but must be used to open the file if it was created when making the file. The ability to add a password to a camouflaged file will at a minimum create a lot of work for someone that does have the camouflage program has forgotten or does not have the password. Figure 6 is the password dialog box presented when finalizing a camouflaged file. The option will always be presented but a password does not have to exist for the file.

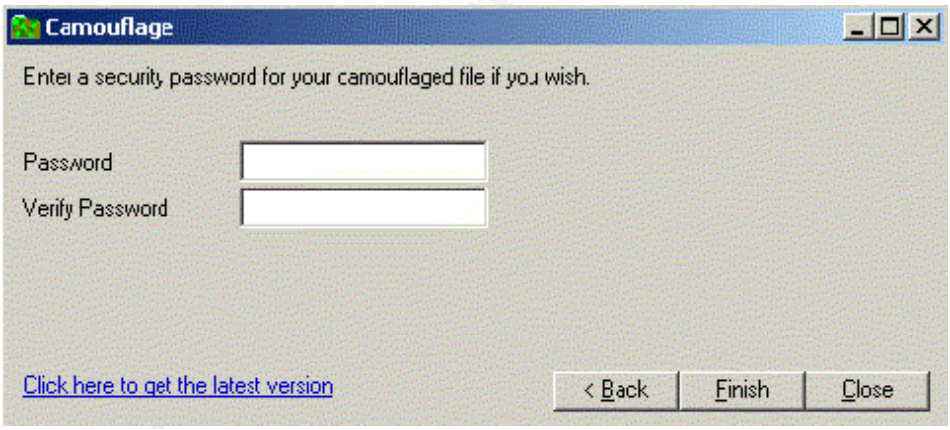

Figure 6.

To complete the camouflage process, simply select finish and a new file is created. The file will act like the file chosen during the camouflage process (in this case a text file) and will bear no resemblance to the camouflaged file (the bitmap).

The entire camouflage process takes no longer than one minute. The resultant image or text file has no visible difference than the original. If an image was camouflaged into an MS word document, when the file is opened, it acts and looks like an MS word file. If an MS word file were camouflaged in an Excel Spreadsheet, it would look and act like the spreadsheet. This capability extends to nearly every file type. To combat these problems, other aspects of the file must be addressed to determine whether or not is has went through a camouflage process.

UNCAMOUFLAGING FILES

As simple as camouflaging a file is, uncamouflaging the file is a one step process. To uncamouflage a file simply right click the file and select uncamouflage. Figure 7 will appear presenting the original file and any camouflaged files. When selecting uncamouflage, if the file was given a password, it is at this point that the password would need to be re-entered. In this file, a 1K-text file was camouflaged in a 679K bitmap (image1a3.bmp) and then the bitmap was again camouflaged in a 679K bitmap (image1a.bmp). The result of the camouflage was increased file sizes, which will be a key point in determining whether a file has been camouflaged.

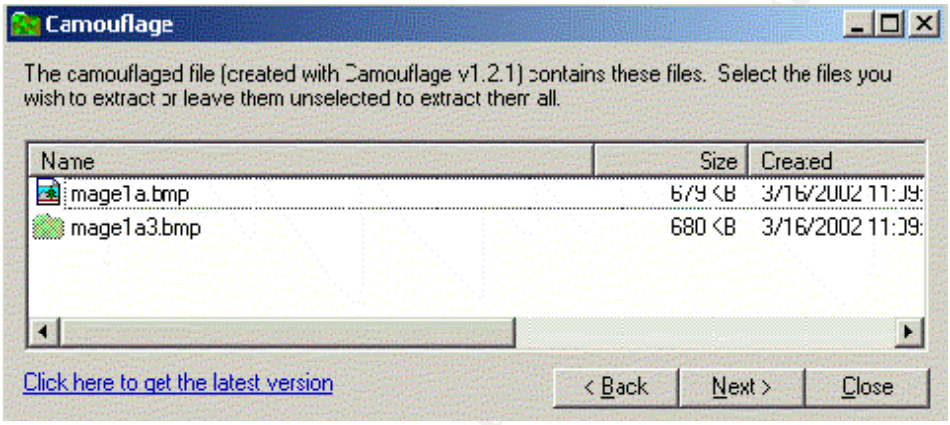

Figure 7.

Steganography has become as simple as select and click. This ability can be beneficial but it can also cause a lot of damage. The ability to simply look at a file and see that it has a hidden message is beyond the capability of the human eye. Because of this limitation, there must be other methods to determine steganography has occurred.

UNINSTALL

To uninstall the program, a person simply chooses add/remove programs and selects change/remove. Camouflage opens a wizard and uninstalls the program with no user interaction. Though the program does uninstall, it does not do a clean uninstall leaving an empty menu item on the start menu and numerous registry entries. To completely remove all traces of the program, a person must manually delete the registry settings and the start menu entry. Though the registry entries would be unknown to most people, the ability to access them after the program has been removed could be critical.

THE SIMPLICITY

In ancient Greece, heads were shaved and wood was carved among other things to create steganographic messages. As time proceeded, it was obvious steganography became easier to use. Hidden codes within words, invisible ink and other things made the process much more compatible to people. Computers soon made there way into society and have taken steganography to a whole new level in simplicity. From drag and drop programs to command line, the use of steganography has become so simple a seven-year-old child could create a message with steganography. Camouflage software allows a person to create a message with steganography in as little as eight clicks of the mouse button. To read that same file will take as little as six clicks of the mouse button. It is now easier to create a message with steganography then it is to convert many files from one form to another.

To send a file that has been camouflaged within another file, a person simply creates one or both files and steps through the camouflage process. If an e-mail is available, an attachment and a simple send will result in coded information traversing the Internet to the end user with little or no effort. This technology is available worldwide, free of charge and can be implemented in an organization within an hour. Overnight steganography for anyone in the world is feasible and very implementable. To have the ability to hide information is a concept that has been around for ages, yet has not been easily accessible. Hidden information is now a part of mainstream society in all cultures and areas of the world.

The simplicity in the use of steganography should be of concern to everyone. A search on the Internet returned over 11,000 links to steganography. These links included everything from free software downloads to mathematical formulas used in steganography. Criminals of all type try to hide data on a daily basis. This data must be intercepted and controlled to ensure at least one of the criminals techniques are thwarted.

CAMOUFLAGE FLAWS

To determine whether or not a file has been used for steganography is a key issue that will continue to grow as steganography grows. Camouflage uses a technique to append the file, which results in increased files sizes from the original. Though this is evident when both files are available, this is very rarely the case. Two basic types of files must be addressed in this case. Image files being one of the more popular are the first types to address. The nature of the Camouflage makes it susceptible to detection by file size alone. Given a generic baseline size of various file images, it is easy to detect increases in size. If the original is not available, a copy can be made of the suspected file. Recreating the file and performing color manipulation will show file size differences if it has been camouflaged. A 680K bitmap (bitmap a) was camouflaged with a second 680K bitmap (bitmap b) resulting in a 1,360K bitmap (bitmap c). All images were true color and looked exactly alike to the humane eye. Given no source file available, a copy was made of bitmap c and read only was unchecked. Opening up bitmap c, changing in to 256K and then changing it back to true color resulted in a 680K bitmap (the same size as the source). It was obvious the file has steganography applied.

Text files also are appended and result in increased size, but the ability to copy and manipulate a text file is not as evident as with images. There are other techniques that can be used to view whether or not a text file has been camouflaged. Opening a text document with a non-standard program will often result in hidden characters among other things that can not be viewed in the native program. A word file was camouflaged in another word file and when opened with MS word, there was no indication the file had a camouflaged file within the data. Opening up the two files in notepad showed a significant difference between the two files. Most notably was the encrypted data at the end of the camouflaged file. The data at the end of the camouflaged file showed no resemblance to the rest of the file and was very compressed. The text below is a small portion of the MS word file viewed in notepad. Lines one through four are all a part of the original document with lines five and six being the beginning of the camouflaged document. Notice lines five and six virtually eliminate whitespace between characters and special characters become more common. The original document ended at line four and had none of the attributes throughout the document seen in lines five and six.

1. ä - ' ³
2. - Text was here - TExt ˜ 6 >
3. PID_GUID ä A N H'- @ f1ª¢Á @ ØuÜOÂÁ @ f`-QÂÁ
4. Ó JÍÁ [&rJÍÁ [&rQÂÁ ÐÄÛÉ € ÒZkÂ-
5. áÏ¿e ož³™eJSûöuT“#Î~bÖîüäùMÒBN Àøš b9t$ `ßAË ¢·ó šÝ¬
6. *ƒ*`)òx$>„ , C”|ÇEmÚ‹ ôg6*ƒ* 7EÍ”ÿ,:=kËPO j,Õ{[

The capability to open files in non-native format is a powerful tool, and can assist in determining whether or not a file has camouflaged. The ability to determine a file that has gone through the steganographic process will continue to mature as more methods are developed.

Yet another key factor in the use of Camouflage is the registry settings mentioned earlier. The ability to search the registry can lead to a lot of information that has been produced using Camouflage.

The HKEY_CURRENT_USER\Software\Camouflage\frmMain\CamouflageFileList, keeps a list of all files that have had data camouflaged within the file. This list is update near real time as the file is camouflaged. This ability to see what files, including the file name that have been camouflaged can lead to easy detection of steganography.

Camouflage does a poor job during the uninstall process and leaves a significant fingerprint. After the uninstall is completed a search on the registry revealed numerous entries present that were not removed. More importantly, the entries still contained data indicating what files had been used with the Camouflage program. Though the files could not be uncamouflaged without the program, a simple reinstall would solve the problem.

What Camouflage lacks in security and the ability to cover the fact of a hidden file, it makes up in flexibility. The registry settings, the appended data resulting in larger file sizes, and the encrypted data at the end of a normal file all make Camouflage easily detectable. This is combated by the various files that can be used with Camouflage. If the only know threat in steganography was images, the scope of the problem could be narrowed down and addressed at a finite level. Camouflage has taken the scope and extended it so that virtually any file extension can be camouflaged or used to camouflage. The ability to add hidden data to a file of any type makes the program very versatile yet easily detectable.

THE THREAT

Steganography itself is not a threat to society and the people, but the use of steganography is and will continue to be for the unforeseen future. Terrorists, corporate espionage personnel, spies, and hackers are all likely users of steganography in the future. The technology is increasing at a pace that could make the average user a threat. Every person I know has a computer that is capable of running the Camouflage program, yet I know of very few that would expect a file had gone through the steganographic process and fewer yet that could detect that file. The average person will know what steganography is in the near future and will use the technology spreading it at an even more rapid rate.

Terrorists have used or are suspected to use steganography in many cases, and use it in many ways.

> **“**According to nameless "U.S. officials and experts" and "U.S. and foreign officials," terrorist groups are "hiding maps and photographs of terrorist targets

and posting instructions for terrorist activities on sports chat rooms, pornographic bulletin boards and other Web sites."[4]

This statement alone is enough to take notice of steganography and the effect it has on society.

As recently as five years ago FBI director Louis French spent time addressing Congress on issues involving encryption and called for restriction on domestic use of encryption. This is significant in the fact that after five years, encryption has become a daily function. All new operating systems come with encryption capabilities and those capabilities continue to grow stronger. What was not addressed by Louis French in public was the use of steganography.[5] If it took only five years to get encryption where it is today, where will steganography be in five years. The lack of addressing steganography has shown to be a possible mistake and the result is a threat today that is spreading and will continue to spread. Five years from now steganography could also be a household word with everyone "jumping on the bandwagon".

With the threat so widespread and the programs available, is there anything that can be done to prevent the damage that could occur? Knowing about the technology and the ease of use is the first step in prevention. If it is known that virtually anyone can perform steganography, the tools will be developed to fight the battle.

THE FUTURE

Steganography is growing like a worm on the Internet. All the latest "bad guys" have found a form of transmission that is secure and hard to detect. With the capability to hide plans and actions, steganography can only grow more popular with the terrorists of the world. The technology security sector needs to take actions to fight the battle of steganography used for illegal purposes. The fifth international workshop on information hiding will be held in Noordwijkerhout, Netherlands in October 2002.[6] More information on the conference can be found at http://research.microsoft.com/ih2002 including a call for papers. Research centers are taking note of steganography and are making strides in the area. A list of some of the more centers involved in the security industry can be found at http://www.jjtc.com/Security/research.htm#centers. Organizations like SANS Security Institute and those mentioned in the above web site must continue to actively pursue steganography and ensure that the industry is prepared for the onslaught to come.

New algorithms are researched and created on a daily basis. Steganography programs are reaching to other technologies such as encryption to enhance programs. The science of steganography is continually looking to improve by limiting signatures to files using steganography. In addition, techniques are being scrutinized and improved on with new techniques sure to come in the near future. Streaming video with hidden messages, wireless communiqué having hidden code, and optimization of signatures is sure to be right around the corner. As mathematics continues evolve, so will steganography. The ability to hide data with a small signature will become increasingly available as will the ability to encrypt and secure that information.

Steganography is also pressing the envelope in the amount of data that can be hidden. The ability to hide a single message within a message has is very common and continues to be easily accomplished. But what if a person could hide an entire volume of information within a file? DRIVECRYPT is able to hide entire volumes in music files using advanced stenographic techniques.[7] This ability no longer limits steganography to a

single file. Entire disks will soon be commonplace in the area of steganography with the potential to hide an entire organizational database with the simplest of ease.

Steganography is growing in both capability and ease of use. The ability to hide a file or files is built in to many software programs. Images and text are no longer the required medium to perform steganography. Music files, video, and non-standard files with rare extensions can all be used for steganography. In less than one minute a file can be hidden and sent with little or no training. The future will only improve on this capability. Operating systems have encryption as a built in function and steganography could well be the next function included for all to use.

CONCLUSION

From Ancient Greece to modern America, people have had the need to hide information. Wars have been fought with the use of information using steganography and kids have long passed coded messages to each other. Most recently, terrorists have been suspected of the use of steganography to hide plans of attacks. As information technology progresses, steganography will continue to grow. Ten years ago very few people knew of the term steganography and fewer yet knew what it would mean to society. Today anyone from a seven-year-old kid to a terrorist in need of hidden communication can create a hidden file for only known people to view.

Is steganography easy? Yes, it does not require a super-computer or a mathematical scientist to perform steganography. If a person can run a computer with a word processor, that same person can perform steganography. This ease of use will cater to everyone that is in need of sending hidden information. Unfortunately, it is also an attack on the security of Information Technology. In society today, there are few things that do not rely on technology. The global reach of technology allows for global communications both good and bad.

The Camouflage software program is an introduction into steganography and the ease of which it can accomplish the task. Is it not a perfect program and thankfully leaves a signature trail that can easily be detected by a person performing steganography detection on a file. It is also a lead into what will occur in the future. It was not long ago that computers ran on large mainframes and the word Windows as applied to software was not known. Today Windows is one of the most popular operating systems in the world and computers can be run by devices that will fit in a single hand. If steganography is to follow the path of technology, the near future will have Camouflage software that is highly encrypted, easy to use, and leaves the smallest of signatures.

Does the knowledge exist to combat steganography used for illegal purposes? The answer to this question varies and depends on background, training, and many other items. To begin to combat illegal use of steganography, multiple items must be addressed. A person must know about the science and what it accomplishes. Know how easily implementable steganography is and who has access (everyone that wishes to use steganography). The changes that occur when using steganography can be significant and identifying those changes is a key to detection. Files that have increased in size, images with multiple colors when not expected, encryption appended to a file, and changes or values applied to system settings are all indications of a file that has incorporated steganography.

Steganography is real, and it is easy. This paper has shown how a simple program can be installed and operated with very little knowledge of the subject. The ability to hide

different types of files was addressed and the ease at which is completed. If a seven-year-old can perform steganography, virtually anyone in the world can.
Also addressed was the use of various techniques to combat the illegal use of steganography. These techniques are easily implemented with the correct knowledge and background. Steganography is around to stay, and we must all be prepared to eliminate future threats.

REFERENCES

[1] McCullagh, Declan. "Bin Laden:Steganography Master." 7 Feb 2001. URL: **http://www.wired.com/news/politics/0,1283,41658,00.html** (11 Mar 2002).

[2] Twisted Pair Productions. "Overview." 2001. URL: **http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.camouflagesoftware.co.uk%2F** (7 Mar 2002).

[3] Quinion, Michael. "World Wide Words." 23 Oct 1999. URL: **http://www.worldwidewords.org/weirdwords/ww-ste1.htm** (9 Mar 2002).

[4] Lewis, Derrick. "Terrorists and Steganography." 24 Sept 2001. URL: **http://www.linuxsecurity.com/articles/cryptography_article-3725.html** (11 Mar 2002).

[5] McCullagh, Declan. "Bin Laden:Steganography Master." 7 Feb 2001. URL: **http://www.wired.com/news/politics/0,1283,41658-2,00.html** (11 Mar 2002).

[6] Petitecolas, Fabien. "the information hiding homepage digital watermarking & steganography." 28 Jan 2002. URL: **http://www.cl.cam.ac.uk/~fapp2/steganography** (10 Mar 2002).

[7] Gmbh, SecurStar. "DRIVECRYPT Secure Hard Disk Encryption." 2001. URL: **http://www.drivecrypt.com/steganography.html?reseller=swprf** (13 Mar 2002).

"5th International workshop in information hiding." 5 Feb 2002. URL: **http://research.microsoft.com/ih2002** (10 Mar 2002).

Sellars, Duncan. "An Introduction to Steganography." URL: **http://www.cs.uct.ac.za/courses/CS400W/NIS/papers99/dsellars/stego.html#SECTION00020000000000000000** (8 Mar 2002).

"Cryptography and Steganography software." URL: **http://www.topology.org/soft/crypto.html** (5 Mar 2002).

StegoArchive. "Steganography Software." 2001. URL: **http://members.tripod.com/steganography/stego/software.html** (5 Mar 2002).

Last Updated: September 25th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS October Singapore 2020	**Singapore, SG**	**Oct 12, 2020 - Oct 24, 2020**	**Live Event**
SANS Community CTF	**,**	**Oct 15, 2020 - Oct 16, 2020**	**Self Paced**
SANS SEC504 Rennes 2020 (In French)	**Rennes, FR**	**Oct 19, 2020 - Oct 24, 2020**	**Live Event**
SANS SEC560 Lille 2020 (In French)	**Lille, FR**	**Oct 26, 2020 - Oct 31, 2020**	**Live Event**
SANS Tel Aviv November 2020	**Tel Aviv, IL**	**Nov 01, 2020 - Nov 06, 2020**	**Live Event**
SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 21, 2020**	**Live Event**
SANS FOR508 Rome 2020 (in Italian)	**Rome, IT**	**Nov 16, 2020 - Nov 21, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS Wellington 2020	**Wellington, NZ**	**Nov 30, 2020 - Dec 12, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**