



Annual ADFSL Conference on Digital Forensics, Security and Law

2012
Proceedings

May 30th, 10:30 AM


The XBOX 360 and Steganography: How Criminals and Terrorists Could Be "Going Dark"

Ashley Podhradsky
Drexel University

Rob D'Ovidio
Drexel University

Cindy Casey
Drexel University

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Podhradsky, Ashley; D'Ovidio, Rob; and Casey, Cindy, "The XBOX 360 and Steganography: How Criminals and Terrorists Could Be "Going Dark"" (2012). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 3.

<https://commons.erau.edu/adfsl/2012/wednesday/3>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



THE XBOX 360 AND STEGANOGRAPHY: HOW CRIMINALS AND TERRORISTS COULD BE “GOING DARK”

Ashley Podhradsky
Drexel University

Rob D’Ovidio
Drexel University

Cindy Casey
Drexel University

ABSTRACT

Video game consoles have evolved from single-player embedded systems with rudimentary processing and graphics capabilities to multipurpose devices that provide users with parallel functionality to contemporary desktop and laptop computers. Besides offering video games with rich graphics and multiuser network play, today's gaming consoles give users the ability to communicate via email, video and text chat; transfer pictures, videos, and file;, and surf the World-Wide-Web. These communication capabilities have, unfortunately, been exploited by people to plan and commit a variety of criminal activities. In an attempt to cover the digital tracks of these unlawful undertakings, anti-forensic techniques, such as steganography, may be utilized to hide or alter evidence. This paper will explore how criminals and terrorists might be using the Xbox 360 to convey messages and files using steganographic techniques. Specific attention will be paid to the "going dark" problem and the disjoint between forensic capabilities for analyzing traditional computers and forensic capabilities for analyzing video game consoles. Forensic approaches for examining Microsoft's Xbox 360 will be detailed and the resulting evidentiary capabilities will be discussed.

Keywords: Digital Forensics, Xbox Gaming Console, Steganography, Terrorism, Cyber Crime

1. INTRODUCTION

The use of nontraditional computing devices as a means to access the internet and communicate with one another has become increasingly popular [1]. People are not just going online through traditional means with a PC anymore, they are now frequently using cell phones, smart phones, and gaming consoles as well. Criminals and terrorists also rely on these technologies to communicate while maintaining confidentiality and anonymity. When information-masking techniques are combined with non-traditional communication devices, the chances of interception or discovery are significantly reduced. Hiding information in plain site by altering image, text, or sound data has been going on for centuries. Steganography, the discipline of concealing the fact that a message or some form of communication exists, poses a major threat to our national security particularly when it is being transmitted over exploitable communication channels [2].

2. STEGANOGRAPHY

Steganography is often confused with cryptography, the latter being the art of obscuring a message so that it is meaningless to anyone except the person it is intended for [3]. Essentially, a cryptographic message hides the meaning of a message, whereas steganography conceals the fact that a message even exists [3]. The origin of the word steganography is Greek for steganos (στεγανός) which means “covered” and graphia (γραφία), which means “writing” [4]. Unlike encryption, which scrambles or encodes text, with steganography the text is inserted or hidden in another medium such as a photograph, webpage, or audio file, called the carrier file. The goal of concealing the message is to

keep the communication a secret even though it is in plain view. IT security professionals refer to this concept as security through obscurity. Unlike cryptography, where an encrypted channel sends a red flag to digital investigators, steganography offers covert communication channels which typically go unnoticed. .

Although today's technologies provide a multiplicity of avenues in which to conceal messages, steganography is not new [5]. In fact, the origins of steganography can be traced back to the ancient Greek historian Herodotus (c. 484-c 425 B.C.) [6]. In his *Histories*, Herodotus describes how a secret message was tattooed onto a slave's head. Once the slave's hair grew back, the message was concealed, thus enabling him to travel through enemy territory without the communication being discovered. Once the slave arrived at his destination, his head was shaved and the message read [6]. Another method of steganography described by Herodotus is a technique employed by the King of Sparta when he needed to send covert messages to the Greeks. The message was written onto a wooden tablet that was then covered with wax so that it appeared empty [7]. Perhaps the most well-known form of steganography is invisible ink, which became popular during the Second World War. Invisible ink can be synthetic, like the invisible ink pens many of us used to write secret messages with as children, or organic, such as body fluids or lemon juice.

There are two primary methods of steganography. The first is referred to as insertion and involves taking data from one file (the secret) and embedding it into another file (the host or carrier). With insertion, the size of the image changes once the hidden message has been added [8].

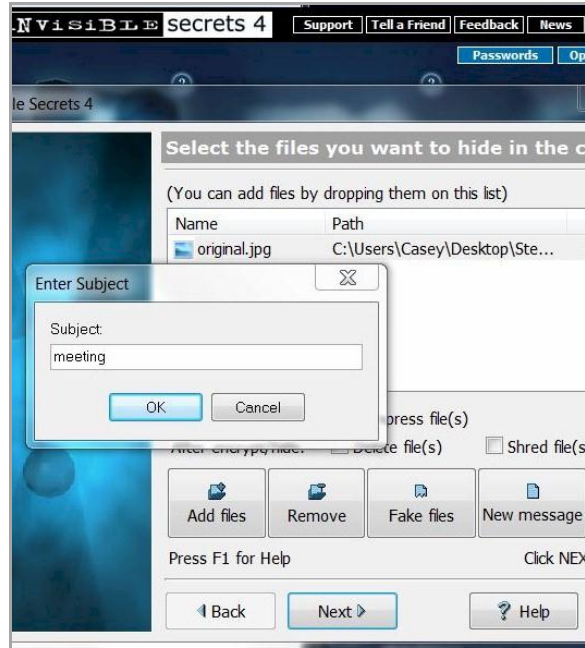
The second form of steganography is called substitution. Here bits of the host file are replaced with other bits of information. For example, in an 8-bit graphic file, the digits furthest to the left are referred to as the Most Significant Digit (MSD), while the digits furthest to the right are the Least Significant Digit (LSD). By replacing the LSD digits, the pixel will change the least. So a bit, which might read 11110000, can be changed to 11110001, and the effect on the image will be minuscule - or undetectable to the human eye [8].

Although this may initially sound complex, there is a plethora of tools available on the internet, many of which are open-source or can be downloaded for a minimal investment or free trial, which makes substitution steganography a relatively simple task.

3. INVISIBLE SECRETS

Invisible Secrets is an encryption and steganography tool which also provides an array of privacy options such as erasing internet and computer traces, shredding data to avoid recovery, and locking computer applications [9]. One of the key attributes of this software is that it affords individuals with little or no experience the opportunity to utilize the ancient practice of steganography with minimal, if any, difficulty. Invisible Secrets utilizes both encryption and steganography to create carrier files which can only be read by the individual they are intended for. By employing cryptography to transfer the key necessary to unlock the secret message as it traverses over an unsecure connection, potential Man in the Middle attacks are thwarted.

The following images illustrate how a secret message can be hidden in a JPG photograph. The two images look identical, however, a closer look shows that they differ in both size and hash value. Using Invisible Secrets, a short text message was inserted into the photograph. Hidden messages are not just limited to text - maps can also be embedded. For demonstration purposes, the message was not encrypted or compressed. Had the message been compressed, the size differences between the two images would be considerably less, making discovery more challenging.



Creating a hidden message using Invisible Secrets

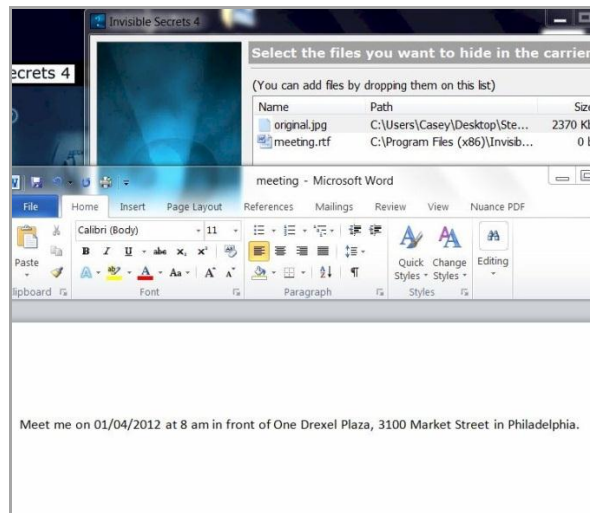


Image 1 - Inserting the secret message into the photograph

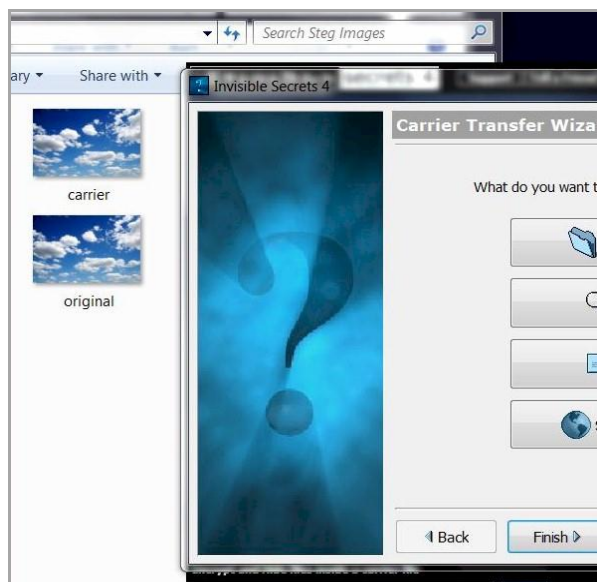


Image 2 - Carrier image created

4. STEGANALYSIS

To the human eye, the two images (titled original and carrier) are identical. However, an initial examination reveals that they differ in both size and hash value. Another way to determine if an image has been altered is to compare the histograms of the photos in question. A histogram is a visual impression or graph of the data distribution of an object obtained by mathematically calculating an object's density [10]. It is relevant to note that a histogram is dependent upon the bin size calculated [11]. If calculated poorly, when the data is tabulated it could result in misleading or incomplete information about the data [11]. Although this task is typically performed by a computer, variances should be expected, and a histogram independent of other supporting evidence may not be sufficient enough to determine if an image has been altered.



Image 3 - Original unaltered image

MD5 checksum 3e8d80d0e03324331215d83cba00caf8
Size 2.31 MB



Image 4 - Carrier image
MD5 checksum a463f9edbeeea630fb320671c5a65895
Size 4.62 MB

By comparing the histograms of the two image files using Adobe Photoshop Elements [12], an apparent difference between the two is noted. Each histogram consists of precisely 256 invisible bars which represent a different level of brightness in the image [13]. The higher the bar is on the graph, the more pixels at that specific point [13]. When placed side by side, we can see that the smoothness, where pixel values sit in relation to each instance of true color and shading transition occurs, is only present in the original image file [14].

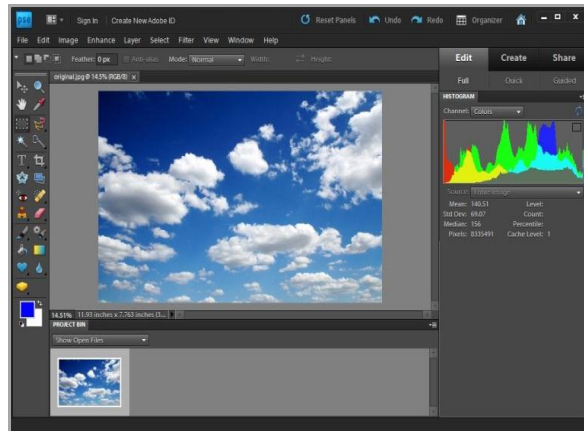


Image 5 - Examining the histogram of the image with Adobe Photoshop

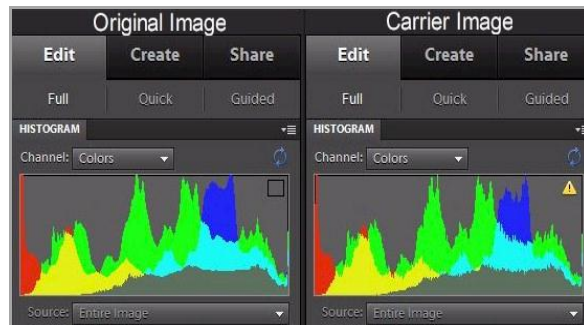


Image 6 - Comparing the two histograms

A common tool used by digital examiners when analyzing suspected steganographic images is a hex editor. Hex editors enable investigators to examine the raw data of a file at a very granular level. Using

WinHex Hexadecimal Editor [15], the two images were compared. The hexadecimal characters which denote the beginning and end of a JPG file are “FF D8” and “FF D9” respectively [16]. Within a matter of seconds we can see that data has been appended to the end of the carrier image file. Further analysis showed that there was a considerable variance in byte values between the two files. Typically, forensic examiners are not privy to both images for analysis. While there are some steganalysis tools available, investigators usually have to rely on more complex methodologies such as looking for embedded ASCII text, utilizing some type of classification or statistical algorithm such as quadratic mirror filters or raw quick pairs, or developing a model of what the suspect image *should* look like [17,18]. Not only do these techniques require advanced skill, but they are also time consuming and costly.

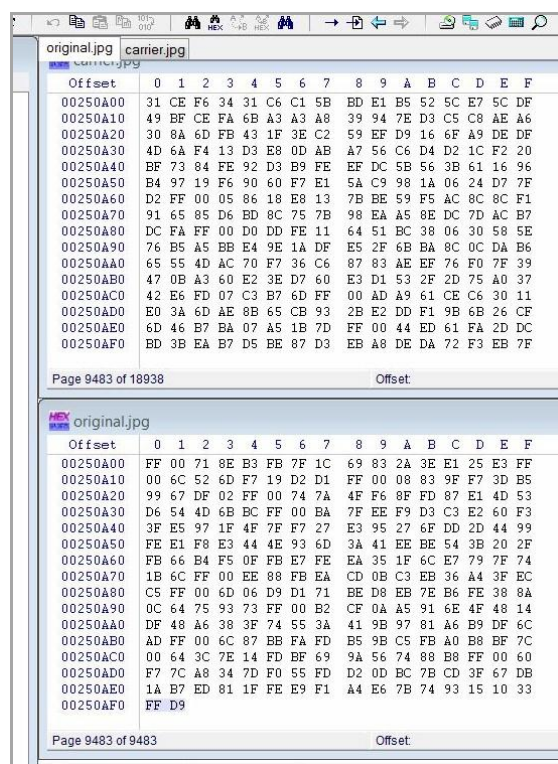


Image 7 - Comparing the two images in WinHex

StegSpy is an open-source utility that searches for steganography signatures in files and the program used to create the file [17]. StegSpy was initially developed to aid in the detection of hidden messages following the terrorist attacks of September 11, 2001 [18]. According to the developer’s website, StegSpy is capable of detecting the following steganography programs: Hiderman, JPHideand Seek, Masker, JPegX, and Invisible Secrets [17]. Although the tool did detect the presence of a hidden message in the carrier file, it identified the program used to create the file incorrectly.

In his thesis paper, “Using an Artificial Neural Network to Detect the Presence of Image Steganography”, Aron Chandrababu tested several steganalysis tools, including StegSpy, to determine their usefulness in detecting covert messages embedded in images. Chandrababu’s research concluded that StegSpy was unreliable when used to examine a sample of 100 color images - 50 containing embedded messages, and 50 containing no message at all [18]. Chandrababu’s experiment found that StegSpy was only able to detect 8 of the 50 carrier images tested with the program [18]. Thus, the probability that StegSpy is capable of revealing an image containing an embedded message is only 0.16, or 16%.

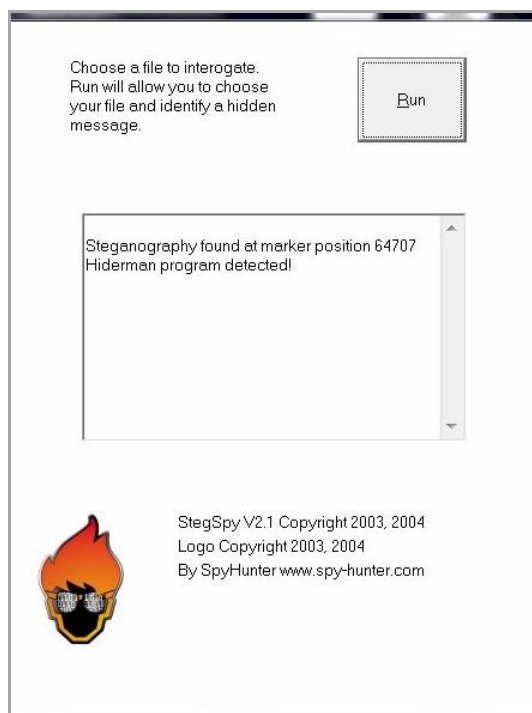


Image 8 -Examining carrier file with StepSpy V2.1

Steganalysis, regardless of the technique employed (human calculated or computer generated algorithm), is an empirical process dependent upon two primary dynamics. First, the algorithm used, and secondly, the model the dataset is being measured against [19]. A shift in any of these variables can alter the results. An additional factor investigators must consider is the fact that technology is in constant flux.

5. TERRORISM AND STEGANOGRAPHY

Shortly after the terrorist attacks in the United States on September 11, 2001, the Washington Post reported that federal agents had gathered at least three years of intelligence confirming that Osama bin Laden and members of al-Qa'ida had been communicating through embedded messages via email and on web sites [20]. Although there was no definitive evidence proving that the terrorists used steganography to plot the attacks of September 11th, it is highly probable [20].

With over 21 percent of the world's population communicating by means of the internet, it should not come as a surprise that terrorists also use the internet to communicate with each other, spread propaganda, fund their activities, and recruit [21]. In the second issue of *Technical Mujahid*, a bi-monthly digital training manual for Jihadis, section one, titled *Covert Communications and Hiding Secrets inside Images*, discusses steganography techniques, specifically hiding messages in images and audio files [22,23].

Unlike emails, which can be easily traced, steganography enables terrorists to communicate with each other while maintaining anonymity. Security expert Bruce Schneier uses the analogy of a dead drop to demonstrate exactly how steganography benefits terrorists [22]. A dead drop is a communication technique used by accused Russian spy Robert Hanssen. Hanssen never directly communicated with his Russian cohorts, but rather left messages, documents, or money in plastic bags under a bridge [22]. Chalk lines left in public places, in *plain sight*, would direct Hanssen where to collect or leave packages [22]. Consequently, the parties communicating never had to meet or even know each other's identity. According to Schneier, dead drops "...can be used to facilitate completely anonymous, asynchronous communications" [22]. So if we think of steganography as an electronic dead drop [22],

terrorist groups such as al-Qa'ida, Hezbollah, and Hamas are capable of communicating anonymously and with no shortage of places to leave their virtual chalk lines.

6. CRIME AND THE XBOX 360

The use of nontraditional computing devices as a means to access the internet and communicate with one another has become increasingly popular [1]. However, average users are not the only ones reaping the benefits of these evolving technologies, so are the criminals. Gaming consoles, specifically the Xbox 360, have become a favorite nontraditional computing medium, not only as an instrument to perform illegal activities but as a target as well.

According to a recent FBI report, Bronx Blood gang members were communicating through Sony's PlayStation 3 gaming console while under house arrest [23]. Similar to the Xbox 360, the PS3 provides users with a multiplicity of services which facilitate communication such as chat, social networking sites, instant messaging, multiplayer gaming, video downloading and sharing, and cross-game chat rooms [23].

New Jersey Regional Operations Intelligence's Threat Analysis Program reported in September 2010 that as of June 2010 Mara Salvatrucha (MS-13) gang members were conducting criminal activities, including ordering the murder of a witness, using Microsoft's Xbox 360 and Sony's PS3 [24]

Robert Lynch, a 20-year-old Michigan man, was arrested and charged in March 2011 of attempting to accost school-aged girls for immoral purposes. Lynch used his Xbox 360 gaming console to meet, befriend, and lure his young victims who were between 11 and 14 years of age [25].

In January 2011, 36-year old Rachel Ann Hicks, lied about her age to befriend under aged boys on Xbox Live. Once she gained their trust, she sent them illicit photos of herself and X-rated movies. The California resident drove from her home state to Maryland to molest one 13-year-old boy [26].

Gaming consoles enable gangs and terrorist organizations to communicate internationally while avoiding detection by the Central Intelligence Agency (CIA) and National Security Agency/Central Security Service (NSA/CSA) [27]. Defendants sentenced to house arrest, particularly sex offenders, are often prohibited from using a computer to access the internet [30,31,32]. However, if gaming consoles are not prohibited, the offender still has the capability of accessing the internet.

While many gaming consoles exist, Microsoft's Xbox 360 is the most popular among American consumers, selling over thirty-nine million consoles, six million more than their top competitor the PS3 [28]. In October 2011, Microsoft announced plans for integrating their Xbox 360 gaming dashboard with a pay television feature called Live TV. Live TV will enable Xbox Live users to access Comcast and Verizon services directly from their gaming consoles [29]. With this rise in popularity, the Xbox 360 has also become a popular medium for criminals. When Bill Gates first announced his plans for the Xbox 360 gaming system in January 2000, at the International Electronic Consumers Show in Las Vegas, some critics proclaimed that this new console was nothing more than a "...PC in a black box [30]." These critics were not too far off the mark.

The Xbox 360 is not only similar to a personal computer - it is actually *more* powerful than most average personal computers. The hardware and technical specifications found in today's Xbox 360 console includes a detachable 250GB hard drive, an IBM customized power -PC based CPU containing three symmetrical cores each capable of running 3.2 GHz, a 512 MB GDDR3 RAM (which reduces the heat dispersal burden and is capable of transferring 4 bits of data per pin in 2 clock cycles for increased throughput), and 700 MHz DDR (theoretically supplying a swift 1400 MB per second maximum bandwidth) memory [31]

7. XBOX 360 IMAGE STEGANOGRAPHY

Using open-source game modification tools, the carrier image created earlier with Invisible Secrets, and a USB 2.0 to SATA adaptor with a 50/60 Hz power supply cable, researchers tested the feasibility

of inserting a stenographic image into an Xbox 360 hard drive. The process was straightforward and the results significant.

Modio, an open-source Xbox 360 modification tool popular with gamers because it enables users to customize their console, was used to open the hard drive [32]. Once the drive was opened, theme creator was selected. Theme creator allows users to create custom Xbox 360 dashboards themes. The user interface supports four images, main, media library, game library, and system settings. The carrier image was uploaded as the main image and the original, unaltered picture of the clouds, uploaded to the media and game libraries, as well as the system settings. The theme was named Stego and saved to the device.



Image 9 - Creating a dashboard theme in Modio using the carrier image created with Invisible Secrets

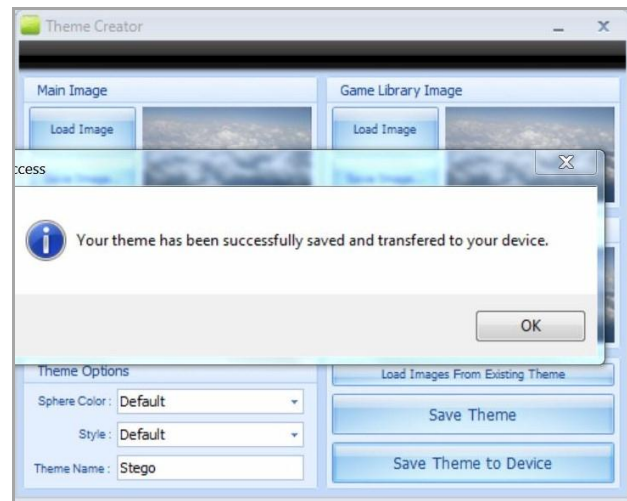


Image 10 -Saving the new theme to the hard drive

When the drive was reopened, our newly created theme, containing the carrier image complete with secret message, was found in Partition 3 under Profile Storage/Skins. The file was then extracted to the desktop and opened with wxPirs [33]. WxPirs is another open-source utility commonly used by gamers seeking to modify their gaming consoles. It enables users to open PIRS, CON, and LIVE files - commonly found on the Xbox 360 drive. When opened in wxPirs, the entire contents of the Stego theme file can be viewed. Although the contents of the newly created theme file (wallpaper1) can also

be viewed in Modio by right-clicking Open in Resigner and selecting the General File Info tab, opening the file in wxPirs reveals that the file was created in Modio, Knowing that a game modification tool created the file could warrant further investigation. The carrier file, Wallpaper1, was then extracted to the desktop and opened with Windows Photo Viewer. Although a MD5 checksum showed that the hash value and file size had changed (MD5 0ea9f8bfa3f54fb214028f1e2f578b02, size 190 KB), when the image was opened with Invisible Secrets, our secret message remained intact and unaltered. (Image 15)

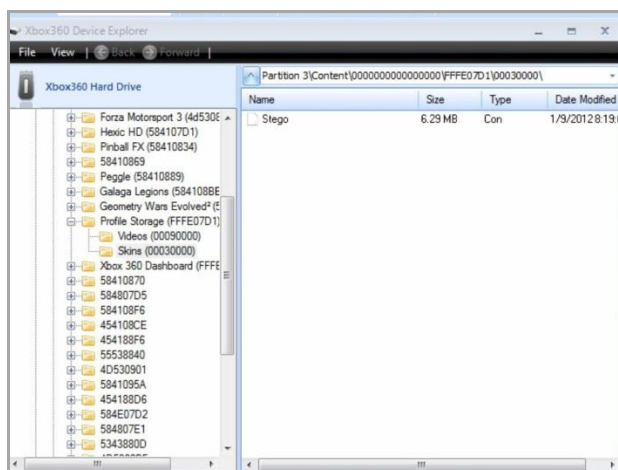


Image 11 -Newly created Stego Theme saved to hard drive

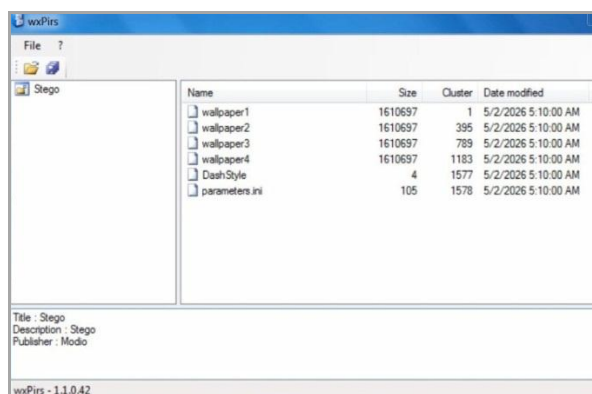


Image 12 - Stego theme opened in wxPirs

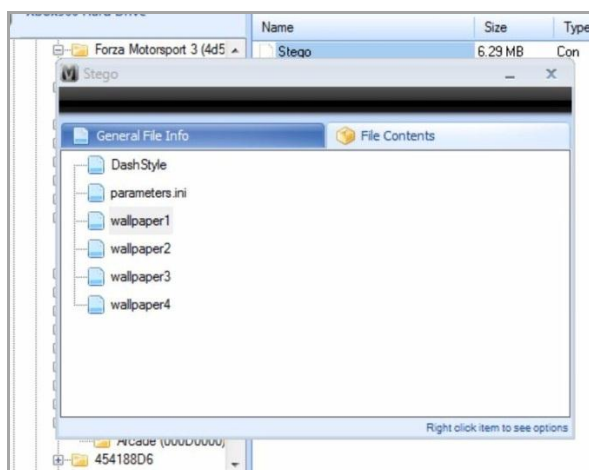


Image 13 -Stego theme examined with Modio's Resigner

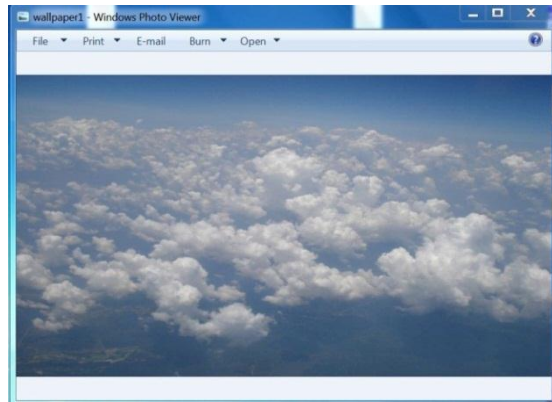


Image 14 - Extracted image opened with Windows Photo Viewer - although checksum and size have changed, no viewable differences are noticed

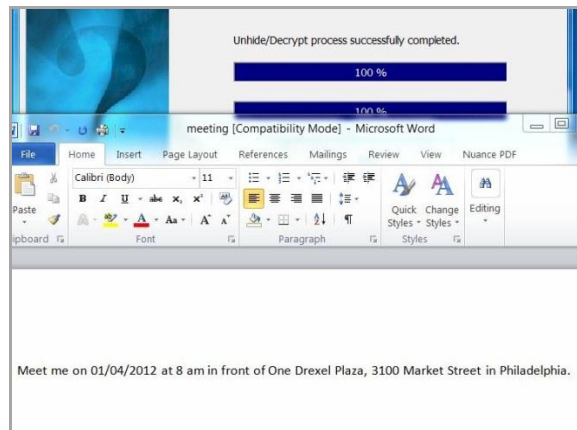


Image 15 -Wallpaper1 is then opened with Invisible Secrets to reveal the hidden message

8. VIDEO STEGANOGRAPHY

Although digital images are the most popular carriers due to their rapid proliferation and the excessive numbers of bytes available for manipulation, messages can also be embedded in audio and video files, programming and web codes, and even in network control protocols [34]. Because video files are essentially a collection of audio sounds and images, many of the techniques used for image or audio steganography can likewise be used to hide data in videos [35]. Furthermore, because a video is a moving stream of images and sound, not only is there a vast area to work with, but the continual motion makes detection extremely challenging [35]. By treating a digital video file as single frames, rather than one continuous bit stream, data can be evenly dispersed into any number of frames or images. By slightly altering the output images displayed on each video frame, when the video is played back it should not be distorted or changed enough to be recognized by the human eye [36]. This approach provides a vast field of workspace and eliminates the need for compression. Although this may involve utilizing techniques such as the Least Significant Bit (LSB), which can be tricky when working with grey-scaled images [36], inserting a message into a video file does not require expertise in video editing. There is a plethora of tools, many of which are right on the average desktop, to assist in the process. Furthermore, if the host video is one that is assumed highly unlikely of being altered, such as a proprietary video game trailer, it may possibly evade inspection altogether.

To demonstrate how this is possible, researchers extracted, altered, and then reinstated a proprietary

game trailer from an Xbox 360 hard drive using Modio and Windows Live Movie Maker. In partition 3, under contents/downloads, the file for Forza Motorsport 3 was located and opened in Modio's resigner (Image 16). Under the general info tab, the Forza Motorsport 3's movie trailer was extracted to the desktop (Image 17).

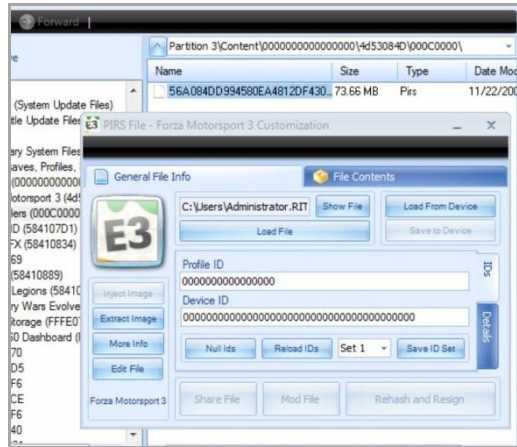


Image 16 – Forza Mothersport 3 opened in resigner



Image 17 – Forza Motorsport 3 game trailer exported to desktop

The trailer was opened from the desktop using Windows Video Maker. Several “secret messages” were inserted throughout the video (Image 18), including names and locations. At the end of the video, credits were added using the names of some of the game designers who spoke throughout the video, and one secret message. The third “name” on the list, Semaine Suivante, isn't a name at all but rather French for “next week” (Image 19). The modified video was saved as Stego.wmv.

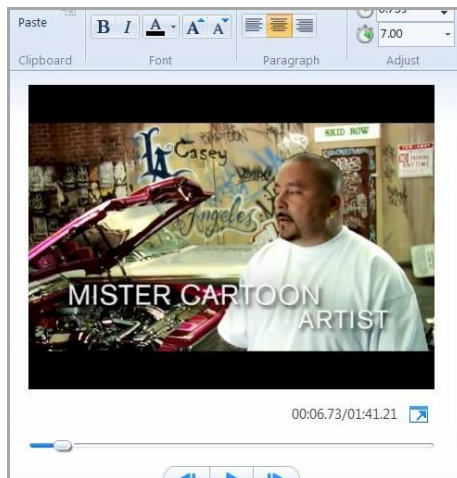


Image 18 – Name inserted in frame

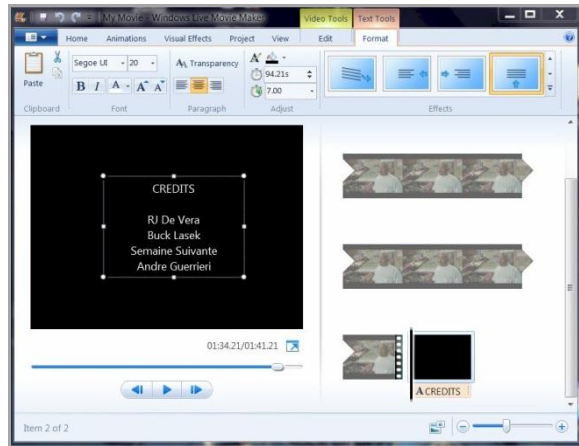


Image 19 – Credits added with hidden message

Using resigner's replace file option, the stenographic video, Stego.wmv, not only replaced the original default.wmv, but retained the original file name and date (default.wmv, 11/22/2005) as well. This is rather significant because it means that digital examiners investigating Xbox 360 hard drives may not see any evidence that a file was altered (Image 20). Thus, a stenographic file could go undiscovered unless the probable hundreds of proprietary files on the drive were extracted and examined one by one. Because the forensic analysis of gaming consoles is in its infancy, the available tools and methodologies investigators use to examine computers are not suitable for analyzing gaming consoles, this is indeed problematic at best. When the new default.wmv is extracted and played on the desktop or on a television screen, the secret messages are revealed (Image 21).

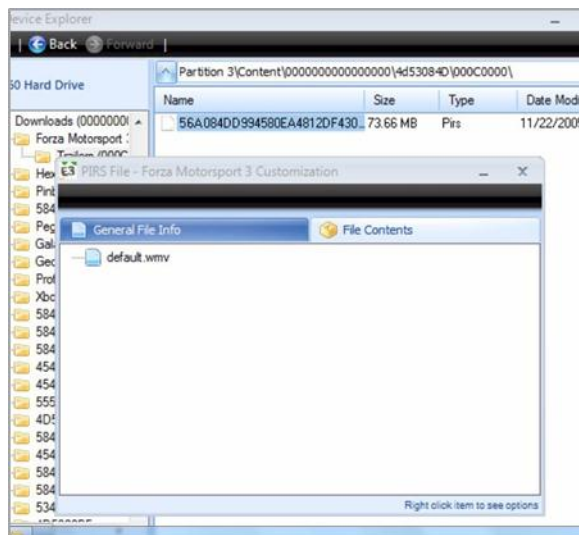


Image 20 – Stenographic file replaced original game trailer retaining the original file's name and creation date

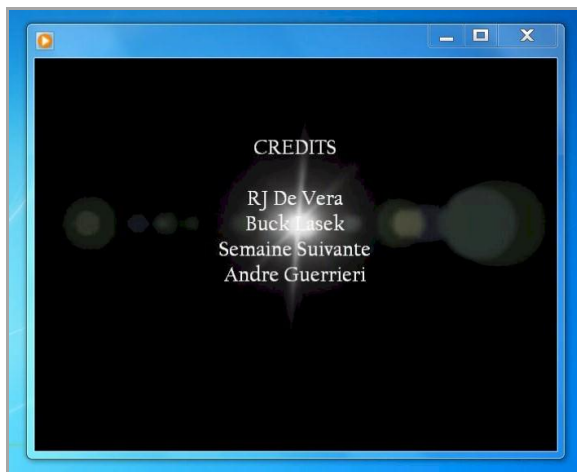


Image 21 - Altered game trailer with hidden message, Semaine Suivante, revealed

9. LINGUISTIC STEGANOGRAPHY

The decision to use a French phrase in the previous example was deliberate. Although it may initially present as somewhat simplistic, given the availability of so many user-friendly software programs and complex steganographic techniques, the use of foreign languages is still a very valuable method of hiding messages. The syntactical nature of any language can make the interpretation of a message written in a foreign language challenging enough, but when that language is deliberately skewed to conceal its true meaning, *challenging* may very well be an understatement [37].

Following the terrorist attacks of September 11, 2001, it became apparent that the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA) did not have language specialists capable of interpreting vital documents that could have forewarned security experts about the planned terrorist attacks [38]. Recognizing the significance of foreign languages as they pertain to security, the Defense Language Institute Foreign Language Center (DLIFLC) was created on November 1, 1941, upon America's entry into world War II [39].

Today the DLIFLC educational and research institute provides linguistic training through intense studies and cultural immersion to the Department of Defense (DoD) and other Federal Agencies [39]. Approximately forty languages are taught at DLIFLC including Arabic, Chinese, French, German, Russian, Spanish, and Japanese [39]. Some examples of linguistic steganography include, but are not limited to:

- Use of Arabic letter points and extensions – A technique where the extensions of pointed letters hold one bit and the un-pointed letters zero bits [40].
- Format-based Methodologies – The physical formatting of text to provide space for hiding information. May include insertion of spaces, non-displayed characters, variations in font size, and deliberate misspellings [41].
- Synonym Substitution – A common form of steganography where selected words from the cover text are replaced with one of their synonyms as predetermined by the encoding rules established [42].
- Feature Specific Encoding – Encoding secret messages into formatted text through the alteration of text attributes (i.e.: length, size) [43]

Because the Xbox 360 is an international gaming platform, it is not uncharacteristic to find multiple languages on the hard drive. On the specific drive used for this project, two instances of foreign languages, French and Dutch, were found upon examination. Both appear to be game character dialogs

and gaming instructions (Images 22, 23). From an investigative perspective, what is perplexing is that these dialogs were the only part of the proprietary game files not encrypted or compressed. This suggests that Microsoft may employ foreign languages as a security measure (security through obscurity). Previous research found Spanish, French, and German in both the marketplace files and networking files (i.e.: NAT) [44]. To date, researchers have recorded French, Spanish, Dutch, German Russian, possibly Chinese Unicode in the Xbox 360 [44].

From a steganalysis perspective, this suggests that there is an abundance of proprietary files on the hard drive where a message could be inserted using a foreign language in order to evade discovery. Where digital investigators have traditionally looked for *user data*, this is no longer the case. Proprietary files must also be diligently examined.

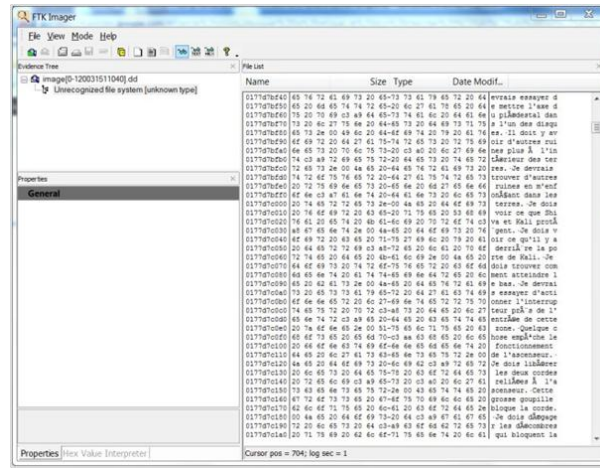


Image 22 – French dialog as viewed in FTK Imager

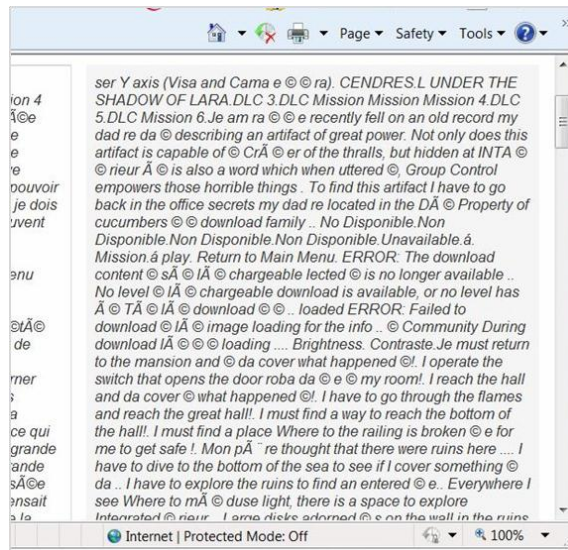


Image 23 – French translated to English using Google Translator

10. CONCLUSION

Steganography is concerned with secret communication, not indecipherable communication. Videos, proprietary and redundant programming files, and audio and digital images are all potential carriers. In

the Art of War, Sun Tzu said that “The natural formation of the country is the soldier's best ally...” [45]. However, when dealing with the Xbox 360, the topography is unknown.

The file data format used on the Xbox is FATX, which is an offshoot of the more familiar FAT32 found on older computers and storage devices [46]. Although the two possess similar format and file data layouts, they are not the same. FATX does not contain the backup boot or file system information sectors found in FAT32. The reasoning behind these variations in the file format is that the Xbox was designed primarily for entertainment as opposed to productivity. Thus, redundancy and legacy are apparently forfeited in order to increase the system's speed. It is also relevant to note that the specific Xbox 360 model, applied Microsoft updates, and condition of the drive all have an impact on what the examiner may or may not find upon examination. This, combined with the veiled nature of steganography, can make analysis very difficult.

11. RECOMMENDATIONS

The first thing the investigator should do upon receiving an Xbox 360 console is to record the 12-digit serial number which is located on the back side of the console where the USB slots are located [47]. The examiner will need to push the oval-shaped USB door open in order to view this number [47]. Each console contains a unique serial number which corresponds to a serial number stored throughout the drive. It is pertinent to record this number, as it not only identifies the system on Xbox Live but could indicate if the drive has been changed [47]. However, because gamers frequently switch hard drives in and out, these numbers may differ.

The SATA hard drive is housed securely within the detachable hard drive case inside a second enclosure. To access the actual drive two torx wrenches, sizes 6 and 10, are required. The T6 wrench is needed to remove the screws from the exterior housing. Three of the screws are easily visible, but the fourth screw is located beneath the Microsoft sticker (Image 24). Once this sticker has been removed, the Xbox warranty is voided. A missing sticker could be indicative of a drive that has been modified or tampered with.



Image 24: Removing Microsoft sticker reveals the fourth screw and indicates the drive has been accessed

As technology evolves, so must the methodologies used by examiners. Although steganography dates back to antiquity, digital steganalysis is a relatively new discipline which is in flux. Consequently, the steganalysis of an Xbox drive is a long, slow, systematic process. It is difficult to identify structural abnormalities or signs of manipulation in a digital environment which is still fundamentally undefined [48]. Compounding this is the fact that there are no current reference guides or approved tools available for forensically examining Xbox 360 drives.

12. REFERENCES

1. **The Diffusion Group.** TDG Releases New Report Examining Web Browsing from Top Consumer Electronics Devices: No Keyboard, No Mouse, No Problem? *The Diffusion Group Press Releases*. [Online] 9 8, 2001. [Cited: 1 1, 2012.] <http://tdgresearch.com/blogs/press-releases/archive/2011/09/19/tdg-releases-new-report-examining-web-browsing-from-top-consumer-electronics-devices-no-keyboard-no-mouse-no-problem.aspx>.
2. *Covert computer and network communications.* **Newman, Robert C.** New York : ACM. Proceedings of the 4th annual conference on Information security curriculum development . p. InfoSec CD 2007.
3. *On The Limits of Steganography.* **Ross J. Anderson, Fabien A.P. Petitcolas.** 1998, IEEE Journal of Selected Areas in Communications,, pp. 474-481.
4. **Fridrich, Jessica.** *Steganography in Digital Media: Principles, Algorithms, and Applications.* Cambridge : Cambridge University Press, 2009.
5. *Hide and Seek: An Introduction to Steganography.* **Honeyman, Niels Provo and Peter.** 2003, IEEE Security and Privacy , pp. 32-44.
6. **Hempstalk, Kathryn.** A Java Steganography Tool. *Source Forge*. [Online] 3 24, 2005. [Cited: 11 1, 2011.] <http://diit.sourceforge.net/files/Proposal.pdf>.
7. **Strassler, Robert B.** *The Landmark Herodotus: The Histories.* New York : Randmom House, 2009.
8. **Frank Enfinger, Amelia Phillips, Bill Nelson, Christopher Steuart.** *Guide to Computer Forensics and Investigations* . Boston : Thomson Course Technology, 2005.
9. **NeoByte Solutions.** Invisible Secrets 4. *Invisible Secrets* . [Online] 2011. [Cited: 11 2, 2011.] <http://www.invisiblesecrets.com/>.
10. **Pearson, K.** Contributions to the Mathematical Theory of Evolution. II. Skew Variation in Homogeneous Material. *Philosophical Trans-actions of the Royal Society of London*. 1885-1887, pp. 186, 343-414.
11. **Jenkinson, Mark.** Histogram Bin Size . *FMRIB Centre Research Facility* . [Online] 5 10, 2000. [Cited: 1 2, 2012.] <http://www.fmrib.ox.ac.uk/analysis/techrep/tr00mj2/tr00mj2/node24.html>.
12. **Adobe** . Elements Product Family. *Adobe* . [Online] 2012. [Cited: 1 1, 2012.] <http://www.adobe.com/products/photoshop-elements.html>.
13. **Patterson, Steve.** How To Read An Image Histogram In Photoshop. *Adobe Photoshop Tutorials and Training*. [Online] 2012. [Cited: 1 2, 2012.] <http://www.photoshopessentials.com/photo-editing/histogram/>.
14. **Liu, Matthew Stamm and K. J. Ray.** Blind Forensics of Contrast Enhancement in Digital Images . *Dept. of Electrical and Computer Engineering, University of Maryland,*. [Online] 6 13, 2008. [Cited: 1 2, 2012.] http://www.ece.umd.edu/~mcstamm/Stamm_Liu%20-%20ICIP08.pdf.
15. **X-Ways Software Technology.** WinHex 16.3. *WinHex: Computer Forensics & Data Recovery Software Hex Editor & Disk Editor*. [Online] 2012. [Cited: 1 2, 2012.] <http://x-ways.net/winhex/>.
16. **Bill Nelson, Amelia Phillips, Christopher Steuart.** *Guide to Computer Forensics and Investigations* . Florence : Cengage, 2009.
17. **spy-hunter.com.** StegSpy. *spy-hunter.com*. [Online] 2009. [Cited: 1 3, 2012.] <http://www.spy-hunter.com/stegspy>.

18. **Chandrababu, Aron.** Using an Artificial Neural Network to Detect The Presence of Image Steganography. *Thesis, The University of Akron.* Akron, OH : s.n., 5 2009.
19. **Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, Ton Kalker.** *Digital Watermarking and Steganography.* Waltham : Morgan Kaufmann, 2007.
20. **Ariana Eunjung Cha, Jonathan Krim.** Terrorists' Online Methods Elusive . *Washington Post.* [Online] 12 19, 2001. [Cited: 1 3, 2012.] <http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52687-2001Sep18>.
21. **Denning, Dorothy E.** Terror's Web: How the Internet Is Transforming Terrorism. [book auth.] Yvonne Jewkes and Majid Yar. *Handbook on Internet Crime.* Devon : Willan, 2009, pp. 194-214.
22. **Schneier, Bruce.** Terrorists and steganography. *ZDNet.* [Online] 9 24, 2001. [Cited: 1 4, 2012.] <http://www.zdnet.com/news/terrorists-and-steganography/116733>.
23. **Federal Bureau of Investigation.** *Situational Information Report, Criminal Tradecraft Alert.* New York : F.B.I., 2011.
24. **NJ Regional Operations Intelligence Center .** *NJ ROIC Analysis Element, Threat Analysis Program, AE201009-839 .* West Trenton : NJ ROIC , 2010.
25. **FOX News.** Police: Man Used Xbox to Lure Middle School Girls for Sex. *FOX News.* [Online] 3 29, 2011. [Cited: 1 2, 2012.] <http://www.myfoxdetroit.com/dpp/news/local/police%3A-man-used-xbox-to-lure-middle-school-girls-for-sex-20110329-mr>.
26. **Mick, Jason.** Woman Arrested For Molesting 13-Year-Old Xbox Friend. *Daily TECH .* [Online] 1 10, 2011. [Cited: 1 2, 2012.] <http://www.dailytech.com/Woman+Arrested+For+Molesting+13YearOld+Xbox+Friend/article20615.htm>.
27. **Storm, Darlene.** Law Enforcement: Gangs, terrorists plot evil over Xbox and PS3. *Computerworld .* [Online] 8 2, 2011. [Cited: 1 3, 2012.] http://blogs.computerworld.com/18725/law_enforcement_gangs_terrorists_plot_evil_over_xbox_and_ps3.
28. **Bloomberg Businessweek.** Microsoft's Xbox Sales Beat Wii, PS3 in February on "BioShock". *Bloomberg.com.* [Online] 3 11, 2010. [Cited: 1 2, 2011.] <http://www.businessweek.com/news/2010-03-11/microsoft-s-xbox-sales-beat-wii-ps3-in-february-on-bioshock-.html>.
29. **June, Laura.** Microsoft announces Xbox Live TV partners including Verizon, HBO, and Comcast. *The Verge.* [Online] 10 5, 2011. [Cited: 1 2, 2012.] <http://www.xbox.com/en-US/Xbox360/Consoles>.
30. **Official Xbox Magazine staff.** The Complete Hisotry of Xbox. *CVG Gaming.* [Online] 12 13, 2005. [Cited: 1 1, 2012.] <http://www.computerandvideogames.com/article.php?id=131066>.
31. **Berardini, C.** The Xbox 360 System Specifications. *Team Xbox.* [Online] 12 5, 2005. [Cited: 1 2, 2012.] <http://hardware.teamxbox.com/articles/xbox/1144/The-Xbox-360-System-Specifications/p1>.
32. **Game-Tuts.** Modio. *Game-Tuts.* [Online] [Cited: 1 2, 2012.] <http://www.game-tuts.com/community/index.php?pageid=modio>.
33. **Xbox-Scene.** <http://www.xbox-scene.com/xbox360-tools/wxPirs.php>. *Xbox-Scene.* [Online] 2010. [Cited: 1 2, 2012.] <http://www.xbox-scene.com/xbox360-tools/wxPirs.php>.
34. **T. Morkel, J.H.P. Eloff, M.S. Olivier.** An Overview of Steganography . *University of Pretoria, South Africa.* [Online] 8 27, 2005. [Cited: 5 2012, 1.] <http://martinolivier.com/open/stegoverview.pdf>.
35. *Steganography and steganalysis.* **Krenn, Robert.** California : University of California , 2004. Proceedings of IEEE Conference,. p. 143.

36. *Hiding Data in Video File: An Overview*. **A.K. Al-Frajat, H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan**. 2010, Journal of Applied Sciences, pp. 1644-1649.
37. *A Natural Language Steganography Technique for Text Hiding Using LSB's*. **Salman, Dr. Hana'a M.** 2004, English and Technology, Vol.26, No3, University of Technology, Baghdad, Iraq, p. 351.
38. **Alfred Cumming, Todd Masse**. *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*. Washington : Congressional Research Service, The Library of Congress, 2005.
39. **Defense Language Institute** . Foreign Language Center . *Defense Language Institute* . [Online] 2012. [Cited: 1 1, 2012.] <http://www.dliflc.edu/index.html>.
40. *A Novel Arabic Text Steganography Method Using Letter Points and Extensions* . **Adnan Abdul-Aziz Gutub, and Manal Mohammad Fattani**. 2007, World Academy of Science, Engineering and Technology, pp. 28-31.
41. **Bennett, Krista**. *Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text*. West Lafayette : Purdue University, 2004.
42. **Cuneyt M. Taskirana, Umut Topkarab, Mercan Topkarab, and Edward J. Delpc**. *Attacks on Lexical Natural Language Steganography Systems*. Indiana : School of Electrical and Computer Engineering, Purdue University, 2006.
43. **Dunbar, Bret**. A Detailed Look at Steganographic Techniques and their use in an Open-Systems Environment . *SANS Institute InfoSec Reading Room* . [Online] 1 18, 2002. [Cited: 1 7, 2012.] http://www.sans.org/reading_room/whitepapers/covert/detailed-steganographic-techniques-open-systems-environment_677.
44. *A Practitioners Guide to the Forensic Investigation of Xbox 360 Gaming Consoles*. **Dr. Ashley Podhradsky, Dr. Rob D'Ovidio, Cindy Casey**. Richmond : Digital Forensics, Security and Law , 2011. ADFSL Conference.
45. **Tzu, Sun**. *The Art Of War*. New York : Tribeca, 2010.
46. **Burkea, Paul K**. Xbox Forensics. *Journal of Digital Forensic Practice*. [Online] 2006. [Cited: 12 22, 2011.] <http://dx.doi.org/10.1080/15567280701417991>.
47. **Microsoft**. How to find the Xbox 360 console serial number and console ID. *Microsoft Support*. [Online] 7 27, 2010. [Cited: 1 7, 2012.] <http://support.microsoft.com/kb/907615>.
48. **Gary Kessler**. An Overview of Steganography for the Computer Forensics Examiner. *Gary Kessler Associates*. [Online] 2011. [Cited: 1 3, 2012.] http://www.garykessler.net/library/fsc_stego.html.
49. *Benchmarking steganographic and steganalysis techniques*. **Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon**. San Jose : CA, 2005. EI SPIE .
50. **Marcus, Ilana**. Steganography Detection. *University of Rhode Island* . [Online] 2011. [Cited: 1 2, 2012.] <http://www.uri.edu/personal2/imarcus/stegdetect.htm>.
51. **Bakier, Abdul Hameed**. The New Issue of Technical Mujahid, a Training Manual for Jihadis. *The Jamestown Foundation* . [Online] 3 30, 2007. [Cited: 1 2, 2012.] [http://www.jamestown.org/programs/gta/single/?tx_ttnews\[tt_news\]=1057&tx_ttnews\[backPid\]=182&no_cache=1](http://www.jamestown.org/programs/gta/single/?tx_ttnews[tt_news]=1057&tx_ttnews[backPid]=182&no_cache=1).
52. **United States Court of Appeals, Ninth Circuit**. *UNITED STATES v. REARDEN*. Los Angeles, CA : s.n., 10 9, 2003.
53. **STATE of North Dakota**. *State v Ehli* . Bismarck, N.D. : s.n., 6 30, 2004.
54. **State of Colorado**. *People vs. Harrison*. 2 8, 2005.

