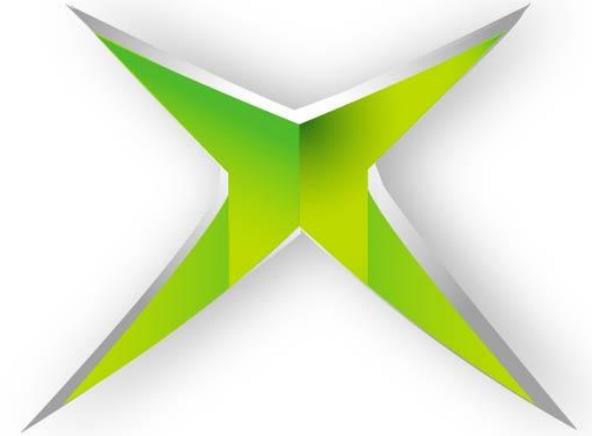




Gwynedd Mercy
University



Steganography and the Xbox:

How Terrorists may be Hiding in Plain Sight

Introduction

- ▶ Technology has introduced new mediums for criminal and terrorist activities.
- ▶ Video game consoles are sophisticated communication devices with networking capabilities equal to those found in computers.
- ▶ Can be exploited by individuals to plan and commit a variety of criminal and terrorist activities.
- ▶ To cover digital tracks of these activities, techniques, such as steganography, may be utilized to hide or alter evidence.



Crime and the Xbox

Media and law enforcement reports document the involvement of gaming consoles in a variety of crimes:

- ✓ Child Exploitation
- ✓ Drug Trafficking
- ✓ Piracy
- ✓ Hacking
- ✓ Identity Theft
- ✓ Swatting
- ✓ Credit Card Fraud
- ✓ Gang Hits
- ✓ Phishing



Encryption verses Steganography

Encryption

- ▶ Hides the meaning of a message
- ▶ Scrambles or encodes text
- ▶ Keeps the meaning of the communication a secret
- ▶ Message itself is not hidden

Steganography

- ▶ Conceals the fact that a message exists
- ▶ Text inserted or hidden in another medium
- ▶ Keeps communication a secret
- ▶ In plain view

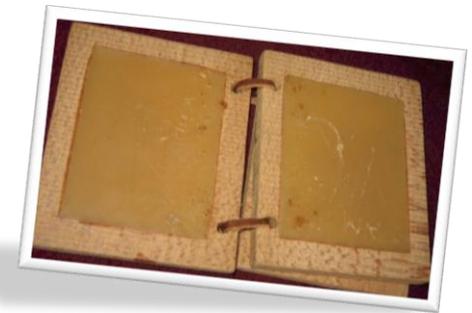
History of Steganography

Steganography can be traced back to the ancient Greek historian Herodotus (c. 484-c 425 B.C.)



Secret messages were tattooed onto a slave's head. Once the slave's hair grew back, he could travel through enemy territory without the communication being discovered. Once the slave arrived at his destination, his head was shaved and the message read.

The King of Sparta sent covert messages to the Greeks by writing the message onto a wooden tablet that was then covered with wax so it appeared empty.



Invisible Ink

- ▶ Perhaps the most well-known form of steganography is invisible ink.
- ▶ Invisible ink can be synthetic or organic.
- ▶ Used during Revolutionary War and both World Wars.
- ▶ WWII captured Long Island submarine had handkerchief with contacts on it.
- ▶ Espionage tool during Cold War.

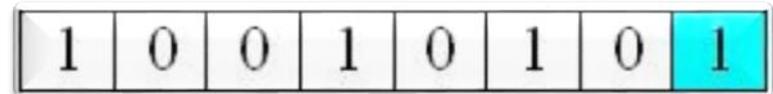


Forms of Steganography

- ▶ Hidden Watermark
- ▶ Audio frequencies
- ▶ Gray images (block technique)
- ▶ Linguistic
- ▶ Network headers
- ▶ Web Pages
- ▶ Snow method (inserting message in trailing space of each line)

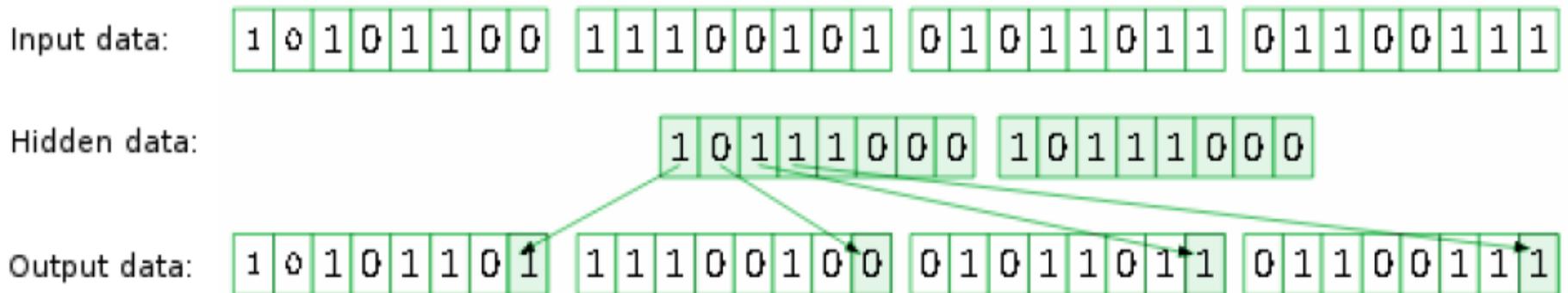
Substitution:

- ✓ Bits of the host file are replaced with other bits of information
- ✓ The digit furthest to the right, known as the Least Significant Digit (LSD), is replaced
- ✓ The change is minuscule – or undetectable to the human eye

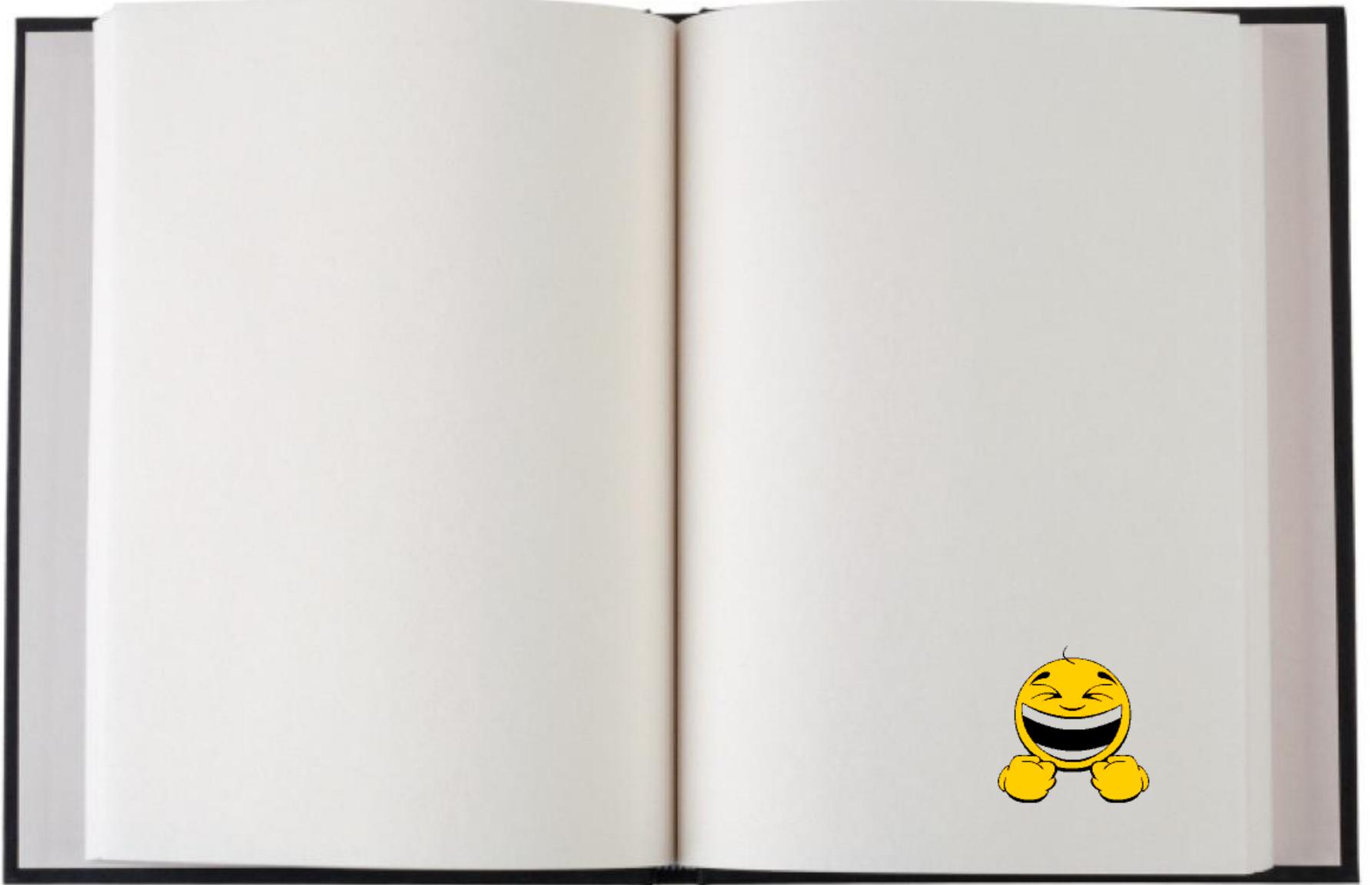


Least Significant Bit (LSB)

- ▶ Lowest significant bit in the byte value of an image pixel.
- ▶ The LSB based image steganography embeds the secret in the least significant bits of pixel values of the cover image.



```
div class="skip-link">
<a href="https://www.gmercyu.edu/academics/programs/bachelor-science-computer-information-science-cis#main-content"
to main content</a>
--بيات ومات أصدقاء جيدين|-->
div>
div class="page">
<header class="jquery-once-1-processed dynamic-header" aria-hidden="true">
<div class="super-header">
<div class="padded-row">
<div class="block block-menu-block left-nav block-menu-block-2">
<div class="menu-block-wrapper menu-block-2 menu-name-menu-utility-menu parent-mlid-0 menu-level-1">
<ul class="menu">
<li class="first leaf has-children menu-mlid-753"><a href="https://www.gmercyu.edu/news-and-events">News
&amp; Events</a></li>
<li class="leaf menu-mlid-754"><a href="https://www.gmercyu.edu/directory">Directory</a></li>
<li class="leaf menu-mlid-755"><a href="https://my.gmercyu.edu" target="_blank">MyGMercyU</a></li>
<li class="leaf menu-mlid-69591"><a href="https://selfservice.gmercyu.edu/SelfService/Search/CatalogSearch">Search</a></li>
<li class="leaf menu-mlid-756"><a href="https://www.gmercyu.edu/giving-gmercyu">Give</a></li>
<li class="leaf menu-mlid-757"><a href="https://www.gmercyu.edu/student-life/our-campuses/visit-campus">Visit Campus</a></li>
<li class="leaf menu-mlid-758"><a href="https://www.gmercyu.edu/request-information" target="_blank">Request Information</a></li>
<li class="last leaf menu-mlid-759"><a href="https://www.gmercyu.edu/admissions-aid/apply" target="_blank">Apply</a></li>
</ul>
</div>
</div>
<div class="block block-search block-search-form">
<div class="search-toggle">
</div>
<form class="search-form" role="search" action="https://www.gmercyu.edu/academics/programs/bachelor-science-computer-information-science-cis#search-form">
<div>
<div class="container-inline">
<h2 class="element-invisible">&nbsp;</h2>
<div class="row collapse">
<div class="small-8 columns">
<div class="form-item form-type-textfield form-item-search-block-form">
<input title="Enter the terms you wish to search for." class="custom-search-box form-text" placeholder="Search" type="text" value="" />
</div>
</div>
<div class="small-4 columns">
```



Using Invisible Secrets, a short text message was inserted into a photograph

Original (unaltered) image



MD5 checksum
3e8d80d0e03324331215d83
cba00caf8
Size 2.31 MB

Carrier image



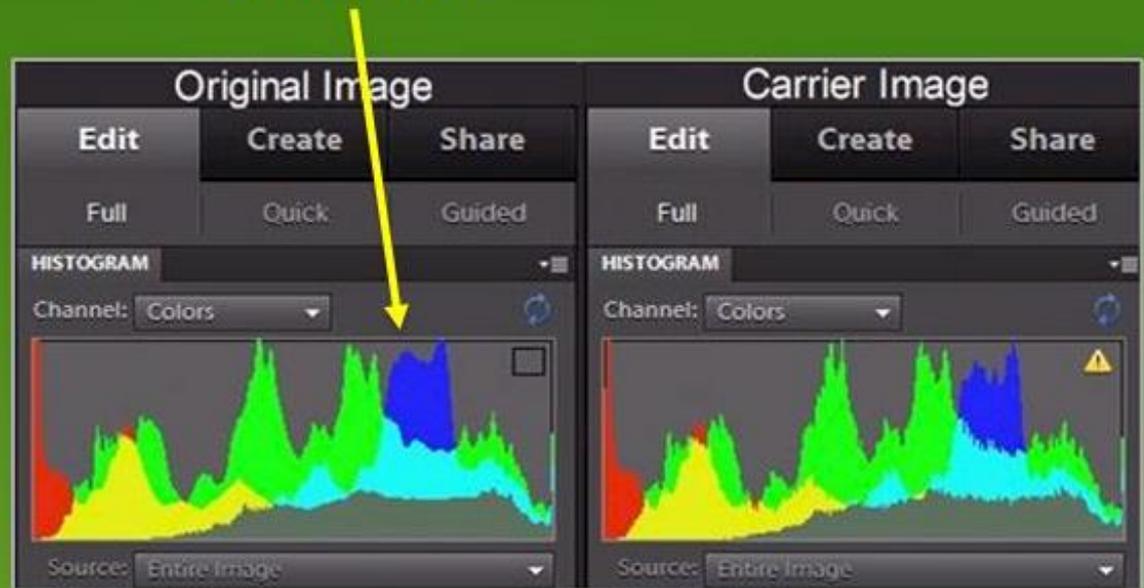
MD5 checksum
a463f9edbeeea630fb320671
c5a65895
Size 4.62 MB



To the human eye, the two images are identical. However, they differ in both size and hash value.

- A histogram consists of precisely 256 invisible bars
- Each bar represents a different level of brightness in the image
- The higher the bar is on the graph, the more pixels at that specific point

Smoothness



- 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



Hex Editor

- Using a Hex editor, the raw data of the carrier (top) and original (bottom) images are compared
- Hex editors enable investigators to examine data at a very granular level
- When the two files are compared, we can see that data has been appended to the end of the carrier image file
- There was also a considerable variance in byte values between the two files

```
original.jpg carrier.jpg
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00250A00 31 CE F6 34 31 C6 C1 5B BD E1 B5 52 5C E7 5C DF
00250A10 49 BF CE FA 6B A3 A3 A8 39 94 7E D3 C5 C8 AE A6
00250A20 30 8A 6D FB 43 1F 3E C2 59 EF D9 16 6F A9 DE DF
00250A30 4D 6A F4 13 D3 E8 0D AB A7 56 C6 D4 D2 1C F2 20
00250A40 BF 73 84 FE 92 D3 B9 FE EF DC 5B 56 3B 61 16 96
00250A50 B4 97 19 F6 90 60 F7 E1 5A C9 98 1A 06 24 D7 7F
00250A60 D2 FF 00 05 86 18 E8 13 7B BE 59 F5 AC 8C 8C F1
00250A70 91 65 85 D6 BD 8C 75 7B 98 EA A5 8E DC 7D AC B7
00250A80 DC FA FF 00 D0 DD FE 11 64 51 BC 38 06 30 58 5E
00250A90 76 B5 A5 BB E4 9E 1A DF ES 2F 6B BA 8C 0C DA B6
00250AA0 65 55 4D AC 70 F7 36 C6 87 83 AE EF 76 F0 7F 39
00250AB0 47 0B A3 60 E2 3E D7 60 E3 D1 53 2F 2D 75 A0 37
00250AC0 42 E6 FD 07 C3 B7 6D FF 00 AD A9 61 CE C6 30 11
00250AD0 E0 3A 6D AE 8B 65 CB 93 2B E2 DD F1 9B 6B 26 CF
00250AE0 6D 46 B7 BA 07 A5 1B 7D FF 00 44 ED 61 FA 2D DC
00250AF0 BD 3B EA B7 D5 BE 87 D3 EB A8 DE DA 72 F3 EB 7F

Page 9483 of 18938 Offset:

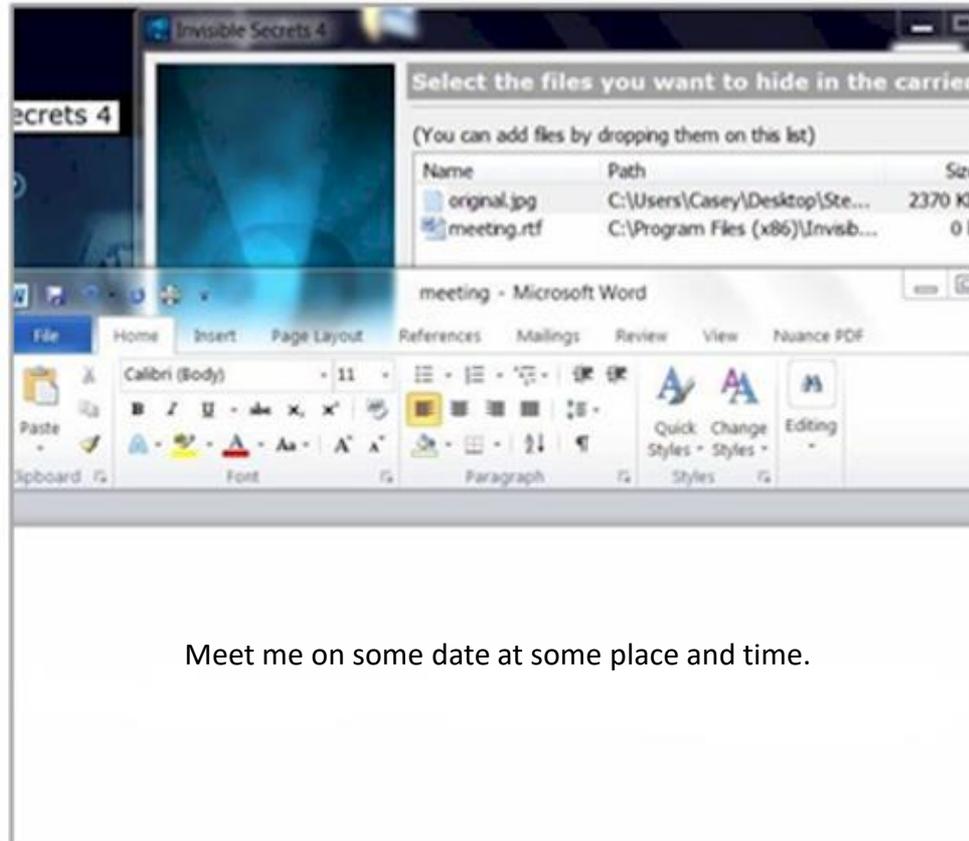
original.jpg
Offset 0 1 2 3 4 5 6 7 8 9 A B C D E F
00250A00 FF 00 71 8E B3 FB 7F 1C 69 83 2A 3E E1 25 E3 FF
00250A10 00 6C 52 6D F7 19 D2 D1 FF 00 08 83 9F F7 3D B5
00250A20 99 67 DF 02 FF 00 74 7A 4F F6 8F FD 87 E1 4D 53
00250A30 D6 54 4D 6B BC FF 00 BA 7F EE F9 D3 C3 E2 60 F3
00250A40 3F E5 97 1F 4F 7F F7 27 E3 95 27 6F DD 2D 44 99
00250A50 FE E1 F8 E3 44 4E 93 6D 3A 41 EE BE 54 3B 20 2F
00250A60 FB 66 B4 F5 0F FB E7 FE EA 35 1F 6C E7 79 7F 74
00250A70 1B 6C FF 00 EE 88 FB EA CD 0B C3 EB 36 A4 3F EC
00250A80 C5 FF 00 6D 06 D9 D1 71 BE D8 EB 7E B6 FE 38 8A
00250A90 0C 64 75 93 73 FF 00 B2 CF 0A A5 91 6E 4F 48 14
00250AA0 DF 48 A6 38 3F 74 55 3A 41 9B 97 81 A6 B9 DF 6C
00250AB0 AD FF 00 6C 87 BB FA FD B5 9B C5 FB A0 B8 BF 7C
00250AC0 00 64 3C 7E 14 FD BF 69 9A 56 74 88 B8 FF 00 60
00250AD0 F7 7C A8 34 7D F0 55 FD D2 0D BC 7B CD 3F 67 DB
00250AE0 1A B7 ED 81 1F FE E9 F1 A4 E6 7B 74 93 15 10 33
00250AF0 FF D9

Page 9483 of 9483 Offset:
```

FF D9 indicates the end of a JPG File



What did the hidden message say?

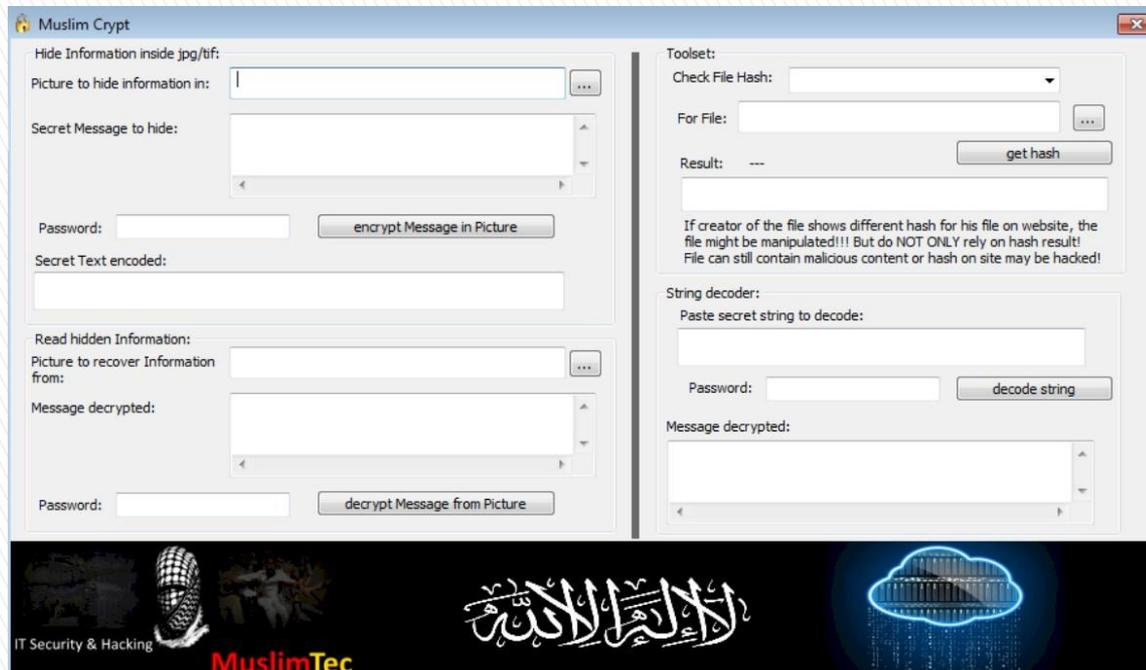


The screenshot shows a Windows desktop environment. In the foreground, a Microsoft Word document titled "meeting - Microsoft Word" is open. The ribbon is set to "Home" with the "Font" group selected. The text in the document reads: "Meet me on some date at some place and time." Above the Word window, a file selection dialog titled "Invisible Secrets 4" is open. The dialog has a header "Select the files you want to hide in the carrier" and a sub-header "(You can add files by dropping them on this list)". Below this is a table with three columns: "Name", "Path", and "Size".

Name	Path	Size
original.jpg	C:\Users\Casey\Desktop\Ste...	2370 Kb
meeting.rtf	C:\Program Files (x86)\Invisb...	0 b

MuslimCrypt

- ▶ Islamic State of Iraq and Syria (ISIS) homegrown tool.
- ▶ Uses steganography to pass discreet messages through images online and spread secret messages.
- ▶ Through propaganda and recruitment, ISIS targets outcasts in their community, minorities in their country, or people who have been discriminated against in the West.



Profile of ISIS Foreign Recruits

- ▶ Average jihadist is:
 - ✓ Male
 - ✓ 26 years-old
 - ✓ Single
 - ✓ Well-educated
 - ✓ Not an expert on the Quran
- ▶ Some studies suggest average Xbox gamer is 30 (younger for Xbox Live)

الإدارة العامة للحدود
بسم الله الرحمن الرحيم
الدولة الإسلامية في العراق والشام
الإدارة العامة للحدود
بيانات المجاهدين

الإدارة العامة للحدود

1	الاسم واللقب	
2	اللقب	
3	اسم الأم	
4	لقب الأم	
5	تاريخ الميلاد و الجنسية	1997 مولاي - هولندا من قبل مغربي
6	الحالة الاجتماعية	أزواج () متزوج () العزباء ()
7	العنوان و مكان الإقامة	هولندا - أمستردام
8	التعليم الدراسي	المتوسط
9	المستوى الدراسي	طالب علم () متوسط () بسيطة ()
10	مدى دينية قبل التحول	يبيع في سورينام
11	المدن التي سافرت إليها وكم ليلة بها	المغرب (زيارات)
12	المسافة التي تقطعت بها (المتوسطة)	أفغان - مصر باب السلام
13	هل سمعت تراتيبه ودين من	أقربا هولندا، بلجيكا، النمسا، سويسرا الهولندي

الإدارة العامة للحدود

بسم الله الرحمن الرحيم
الدولة الإسلامية في العراق والشام
الإدارة العامة للحدود
بيانات مجاهد

1	NAME	
2	FIGHTER NAME	
3	MOTHER'S MAIDEN NAME	
4	BLOOD TYPE	
5	DOB AND NATIONALITY	
6	MARRIAGE STATUS	
7	ADDRESS & PLACE OF RESIDENCE	
8	LEVEL OF EDUCATION	
9	LEVEL OF SHARIA UNDERSTANDING	

Khan Teens

- ▶ U.S.-born children of Indian immigrants living in Chicago, Illinois.
- ▶ Ages 19, 17, and 16.
- ▶ Detained at O'Hare International Airport where they were flying to Istanbul to join ISIS.
- ▶ “This nation is openly against Islam and Muslims”.
- ▶ "I cannot live under a law in which I am afraid to speak my beliefs."

Poster Girls for ISIS

- ▶ Teen girls from Vienna, 17 year-old Samra and 15 year-old Sabina fled to join ISIS.
- ▶ They appeared on ISIS websites carrying AK-47s and surrounded by groups of armed men.
- ▶ Used as sexual presents for new recruits.
- ▶ Samra was beaten to death by ISIS when she tried to flee.
- ▶ Sabina died fighting in Syria.



Paris Attacks

- ▶ Friday, November 13, 2015
 - ▶ Multiple attacks occurring concurrently in six separate locations.
 - ▶ At least 3 teams of Islamic State of Iraq and Syria (ISIS) terrorists.
 - ▶ 130 people killed and 363 seriously injured.
 - ▶ Multiple reports that the ISIS militants communicated via Sony's PlayStation 4 gaming console.
- 

Manchester Bombing

- ▶ Monday, May 22, 2017
- ▶ Suicide bomber outside Ariana Grande concert.
- ▶ 22 killed and 116 injured
- ▶ Suicide bomber did not act alone



ISIS Support System

- ▶ ISIS gains support and recruit followers around the globe using aggressive social media tactics.
 - ▶ Lone wolf operations – launch attacks in regions which would otherwise be too difficult or risky for Syrian militants to travel to.
 - ▶ However, these individuals are not acting alone, they are being vetted, trained, instructed, and stay in constant touch with Islamic State cyber-coaches
- 

Training and Communication via Games?

- ▶ Could Games like Call of Duty, Battlefield, and Grand Theft Auto be used to exchange information?
 - ▶ Because these games are mapped by satellites, gamers can even see the exact layout of certain regions to even further their accuracy in the real world.
 - ▶ 9/11 attackers used virtualization at the Flight Safety Academy in Vero Beach, Florida to train.
- 

Grand Theft Auto 5

- ▶ According to Egyptian media:
 - GTA video is meant to “...raise the morale of the Mujahideen, and the training of children and young teenagers to fight the West, and throw terror into the hearts of opponents of the state.”
- ▶ It has been reported that the state of the art ISIS media center is very well-funded.
- ▶ ISIS publishes as many as 90,000 posts per day on social media.

Grand Theft Auto 5

- ▶ ISIS Uses GTA 5 in Teen Recruitment Video
- ▶ Mocked-up GTA-style trailer features virtual fighters shouting "Allahu Akbar!" as they attack U.S. troops and law enforcement.





Hi Cindy Casey,

As you may know, our [Community Guidelines](#) describe which content we allow – and don't allow – on YouTube. Your video [RecruitmentVideoforPresentation](#) was flagged to us for review. Upon review, we've determined that it violates our guidelines and we've removed it from YouTube.

Video content restrictions

It's not okay to post large amounts of untargeted, unwanted, or repetitive content to YouTube. If the main purpose of your content is to drive people off of YouTube and onto another site, it will likely violate our spam policies. In addition, misleading descriptions, tags, titles, or thumbnails designed to increase views are not allowed. Tags should only be placed in the appropriate tag section and not in the description. [Learn more.](#)

Impact on your account

Please note that this removal has not resulted in a [Community Guidelines strike](#) or penalty on your account.

We encourage you to review all videos in your account to make sure they are in line with our community guidelines as additional violations could result in strikes on your account, or even lead to account termination.

Sincerely,
- The YouTube Team

[Help center](#) • [Email options](#) • [Report spam](#)

©2017 YouTube, LLC [901 Cherry Ave, San Bruno, CA 94066, USA](#)

Live Leak

لا إله إلا الله
الله
أمره



ISIS

قنص مجموعة من الجيش الأمريكي



0:00:45

0:02:54



SHOTS BY
Live Leak
لا إله إلا الله
الله أكبر



ISIS

عبوات صليل الصورام ،، أفجع



0:02:15

0:01:24



راية التوحيد



**THIS IS OUR CALL OF DUTY
AND WE RESPAWN IN JANNAH**

Microsoft Cracks Down on Terrorist Content

- ▶ In 2016, Microsoft announced on they will ban content 'used to promote terrorist violence or recruit for terrorist groups' on most – but not all – of its platforms.
- ▶ Terms of service updated to ban content posted by, or in support of, people or organizations on a United Nations list of terrorist entities.

Microsoft to crack down on 'terrorist content' across Xbox, Outlook

BY: Julianna Waeda
18:00, May 21, 2016



With the world growing more concerned about attacks by militant groups on civilians, Microsoft Corp has outlined new policies to crack down what it called "terrorist content" on some of its consumer services.

World of Warcraft

- ▶ NSA spied on Xbox Live and World of Warcraft to infiltrate terrorist groups.
- ▶ Agency contractor Edward Snowden leaked documents revealing that both the NSA and CIA were spying on online games since 2006.
- ▶ Leaks did not divulge what data was being collected or the methodologies used.





From a Digital Forensic Perspective...

- ▶ When information-masking techniques are combined with non-traditional communication devices, the chances of interception or discovery are significantly reduced.
- ▶ Although steganography dates back to antiquity, digital steganalysis is a relatively new discipline.
- ▶ It is difficult to identify structural abnormalities or signs of manipulation in digital environments which are still fundamentally undefined.
- ▶ Where digital investigators have traditionally looked for user data, proprietary files must also be diligently examined.





Cindy Casey, Gwynedd Mercy University
casey.cindy@gmercyu.edu



Gwynedd Mercy
University