Gwynedd Mercy University

Steganography and the Xbox:

How Terrorists may be Hiding in Plain Sight

Cindy Casey, Gwynedd Mercy University

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

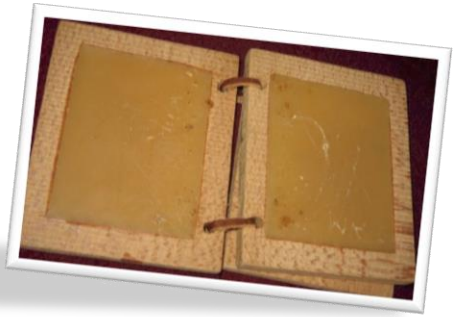
- Conceals the fact that a message exists
- Text inserted or hidden in another medium
- Keeps communication a secret
- In plain view

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

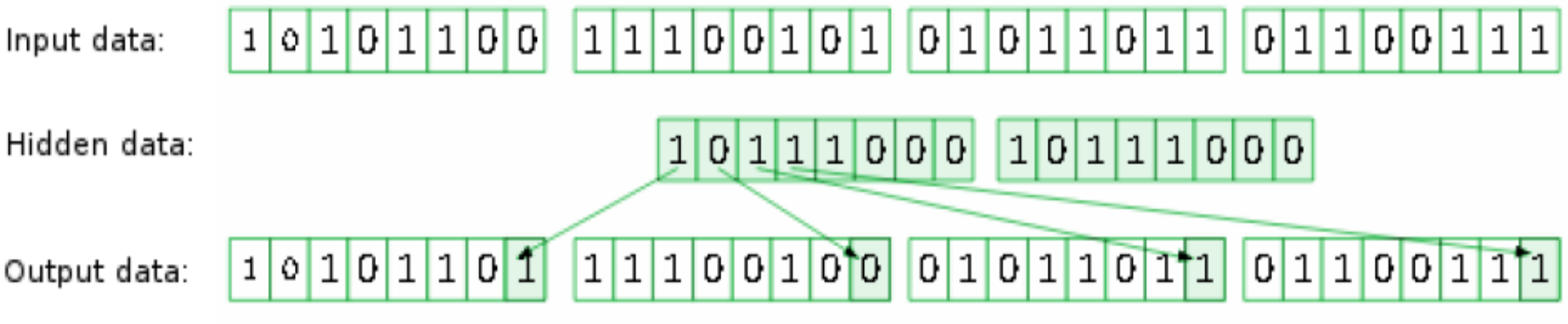
- Hidden Watermark
- Audio frequencies
- Gray images (block technique)
- Linguistic
- Network headers
- Web Pages
- Snow method (inserting message in trailing space of each line)

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.



```
iv class="skip-link">
<a href="https://www.gmercyu.edu/academics/programs/bachelor-science-computer-information-science-cis#main-conte
to main content</a>
<!--بيانات ومات أصدقاء جيدين-->
div>
iv 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">Ne
            &amp;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/CatalogSe
          <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
          <li class="leaf menu-mlid-758"><a href="https://www.gmercyu.edu/request-information" target="_blank">R
            Info</a></li>
          <li class="last leaf menu-mlid-759"><a href="https://www.gmercyu.edu/admissions-aid/apply" target="_bl
        </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-scienc
        <div>
          <div class="container-inline">
            <h2 class="element-invisible"> </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" pla
                </div>
              </div>
              <div class="small-4 columns">
```

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

Original (unaltered) image

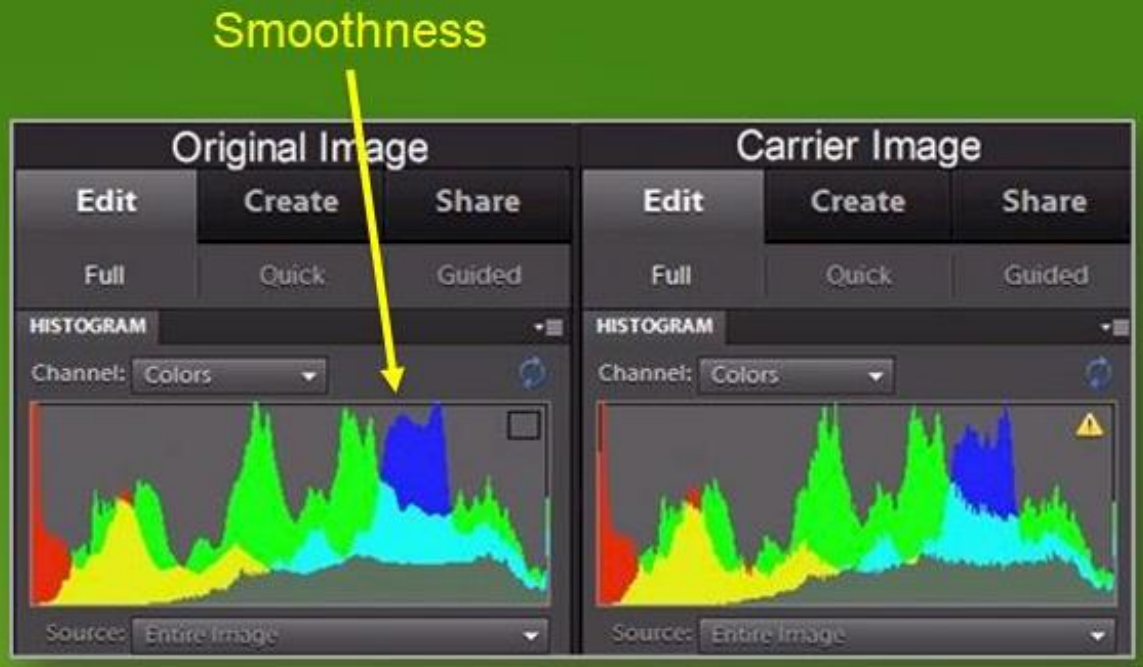
MD5 checksum
3e8d80d0e03324331215d83
cba00caf8
Size 2.31 MB

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.

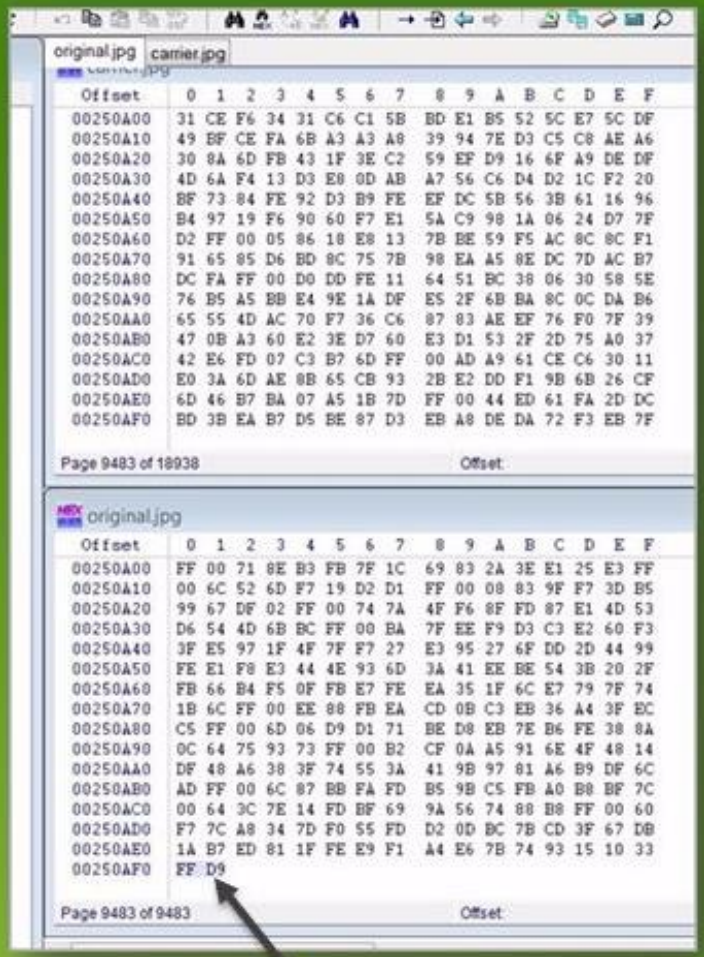
- A histogram consists of precisely 256 invisible bars
- Each bar represents a different level of brightness in the image
- The higher the bar is on the graph, the more pixels at that specific point



- 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

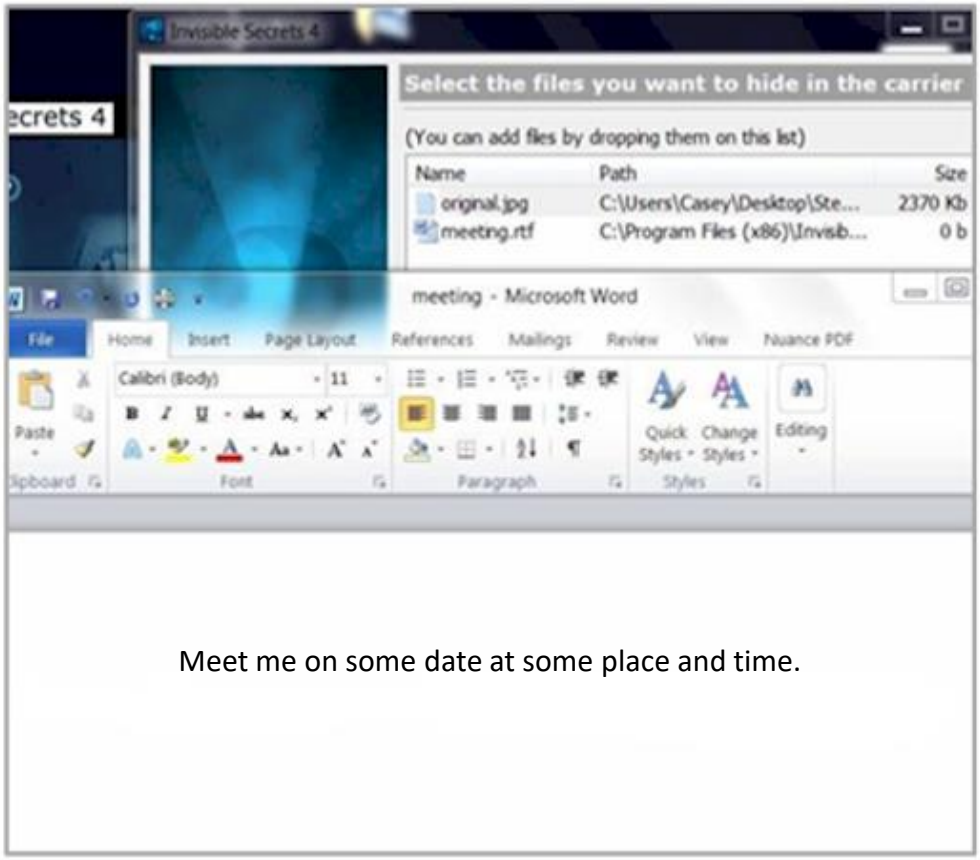
Hex Editor

- 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



FF D9 indicates the end of a JPG File

What did the hidden message say?



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)

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


LiveLeak
لا إله إلا الله
ISIS
قنص مجموعة من الجيش الإمريكي
صليل الصوارم
0:00:45
0:02:54

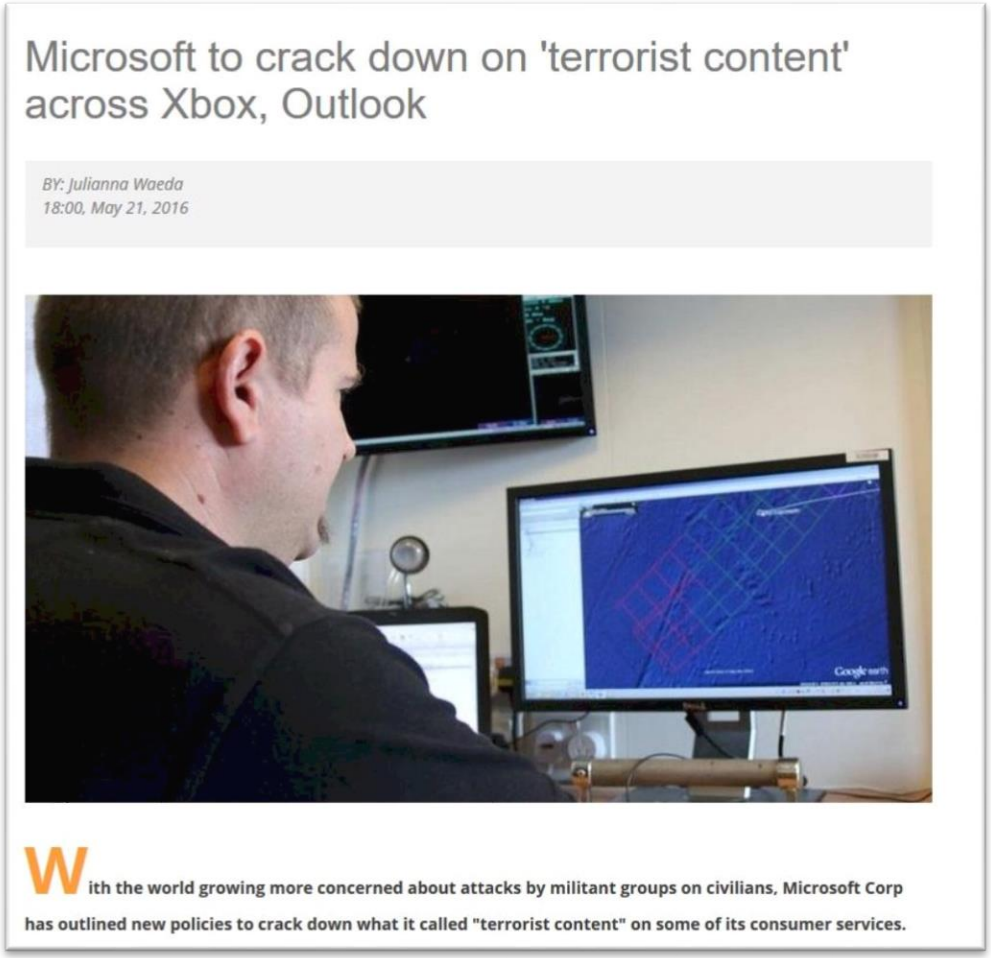
0:02:15

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.



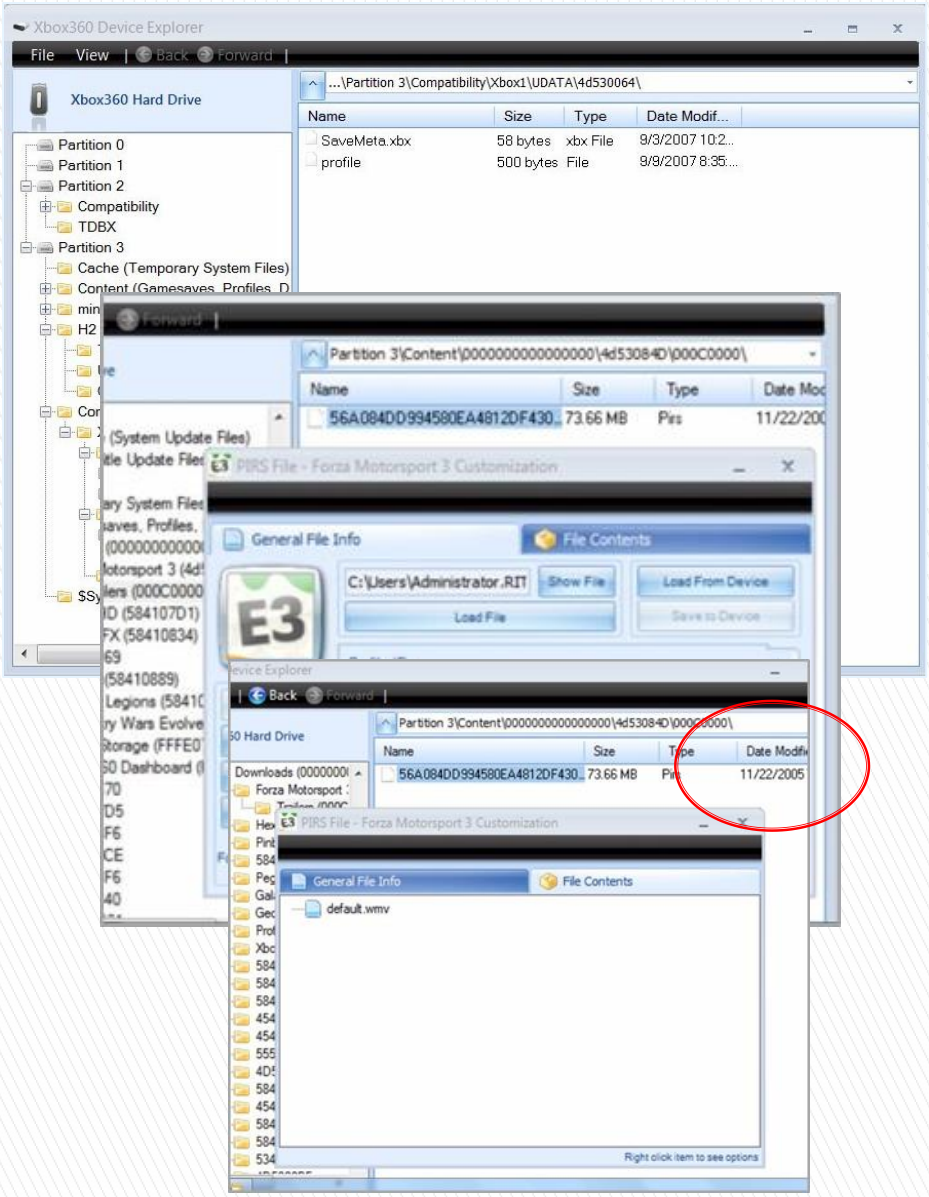
Microsoft to crack down on 'terrorist content' across Xbox, Outlook

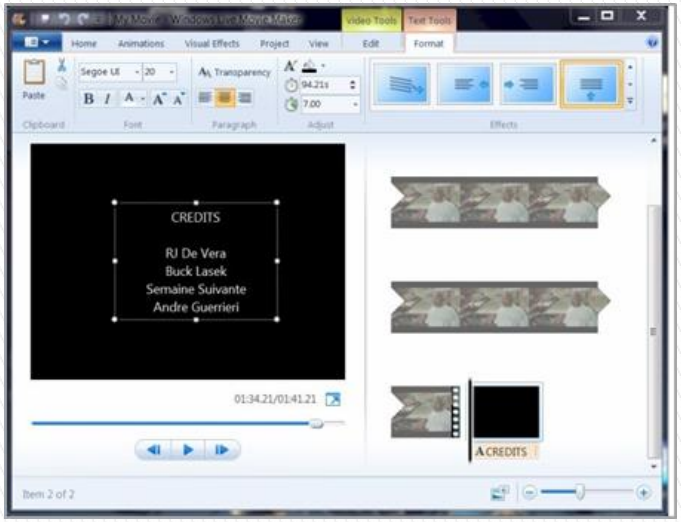
BY: Julianna Waeda
18:00, May 21, 2016

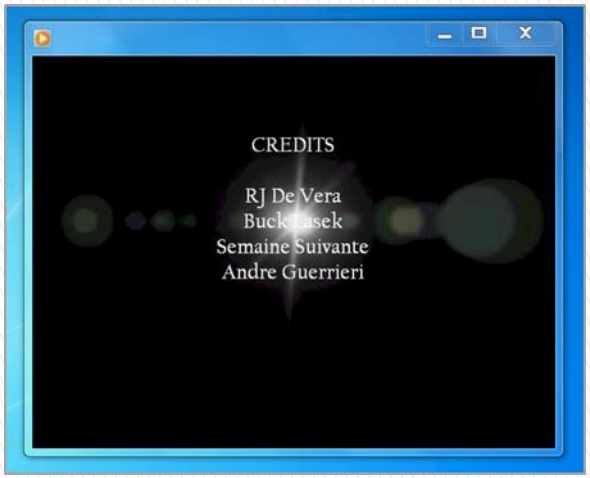
With the world growing more concerned about attacks by militant groups on civilians, Microsoft Corp has outlined new policies to crack down what it called "terrorist content" on some of its consumer services.

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.



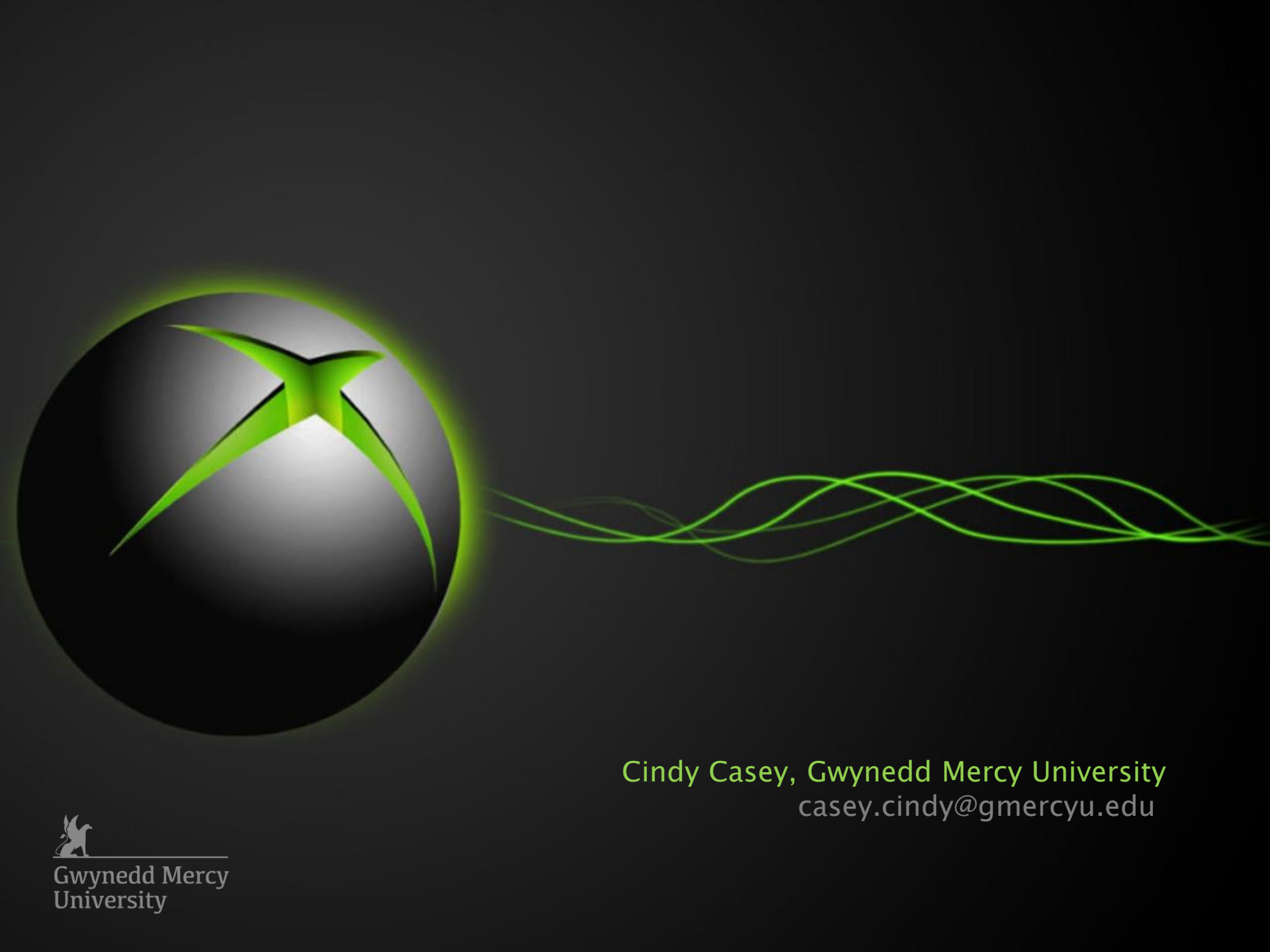




Semaine Suivante –
French for Next Week

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