

# **Steganography over the Covert Channels of TCP/IP**



## STEGANOGRAPHY HAS NOTHING TO DO WITH DINOSAURS

- Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message.
- This can be achieved by concealing the existence of information within seemingly harmless carriers or cover
- Carrier: text, image, video, audio, etc.

# Terminology

## ■ Steganography

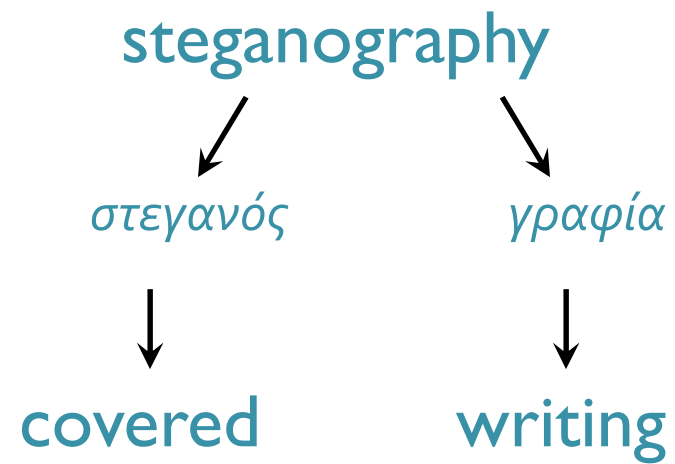
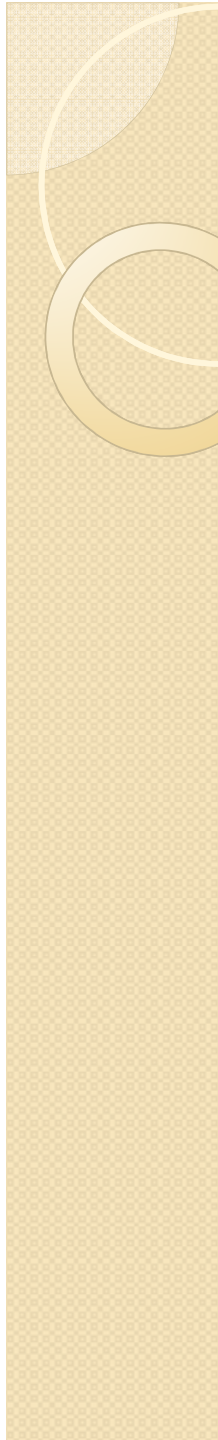
- » It is the practice of disguising the *existence* of a message

## ■ Cover

- » Generally, innocent looking carriers, e.g., pictures, audio, video, text, etc. that hold the hidden information
- » The combination of hidden data-plus-cover is known as the *stego-object*

## ■ Stegokey

- » An additional piece of information, such as a password or mathematical variable, required to embed the secret information



The art of secret (hidden) writing

# Steganography vs. Cryptography

Steganography is different from cryptography

- » *Cryptography* disguises the *content* of a message without concealing the message
- » *Steganography* disguises the *existence* of the message

Same Purpose

To hide and protect important information

# Steganography vs. Cryptography

- Steganography hides without altering
- Cryptography alters without hiding



# Steganography + Cryptography

Additional  
security can  
be obtained  
by combining  
steganography  
with cryptography



cryptology

κρυπός

λογία

hidden

speaking



# Steganography is the art and science of:

- writing hidden messages so that no one but sender and recipient realize there is a hidden message
- communicating in a way that hides the existence of a message

It is not encryption - original image/file is intact



# Coverttext

A coverttext can be anything if you're clever enough about it.

- text (.doc, .txt, .html, newspapers)
- images, video (pictures, periods)
- audio, sounds (.mp3, radio transmissions )



# Steganography works this way

- Start with a secret message
- Using a previously agreed upon algorithm insert the secret message into a cover object creating the stego object
- Send the stego object to the receiver.
- The receiver accepts the stego object
- The receiver extracts the hidden message using the agreed upon algorithm



# Steganography preceded cryptography

Before mankind was able to encode messages with cryptography, messages would be hidden with steganographic means.



# Steganography throughout History

- Dates back to 440 BC.
- Herodotus: wax tablets to Sparta
- Histiaeus: Shaving of head, Persian War
- Invisible ink
- Overwrite select characters in printed type with pencil
- Pin punctures in type

# Hide message under hair

- Shave the head of a messenger
- Tattoo a message on his head
- Wait for the hair to grow back
- Send the messenger on his way
- When he reaches his destination, shave his head and view the message
- Took too long, maybe months



# Steganographic applications

Over 1000 digital steganography and stegananalysis applications have been identified by the Steganography Analysis and Research Center.

[www.sarc-wv.com](http://www.sarc-wv.com)

# Digital Steganography Techniques

- » Three common techniques used
  - » Substitution: LSB Method – replaces the last bit in a byte
    - » Advantage: Simplest approach to hide data in an image file
    - » Disadvantage: does not take well with file changing
  - » Injection: embedding the message directly into the carrier object
    - » Disadvantage: Makes the file size much larger
  - » Generation of a new file: Start from scratch
    - » Advantage: There is never an original file to compare to





## How Is LSB Hiding Typically Done?

The simpler techniques replace the least significant bit (LSB) of each byte in the cover with a single bit for the hidden message

- LSB encoding: least significant bit(s).
- 3 bits available for 24-bit images,
- 1 bit available for 8 bit images

# Who's Using It?

- Good question... nobody knows for sure.
- The whole point to steganography is to disguise its use.
- Anybody can use it to hide data or to protect anonymity
- The strength of Steganography is “Stealth”

# Digital Watermarking

- Protection of intellectual property rights/thwart software piracy
- Watermarking has been proposed as the “last line of defense”
  - » Implements copy protection, e.g., “never copy,” “copy once”
  - » Copyright ownership and original, authorized recipient can be determined
  - » Allows trace-back of illegally produced copies for prosecution



## SDMI - Secure Digital Music Initiative

forum of more than 180  
companies (IT, consumer  
electronics, recording  
industry)



# Watermarks

- Watermark - an invisible signature embedded inside an image to show authenticity or proof of ownership
- Discourage unauthorized copying and distribution of images over the internet
- Ensure a digital picture has not been altered
- Software can be used to search for a specific watermark

# Digital Piracy

- Annual global piracy losses are in the billions
- Piracy will continue to increase due to Internet distribution methods
- Significant hacking activity by bootleggers to render watermarking techniques useless



# Many sophisticated ways

- » a hidden partition on a hard drive
- » the coefficients of the discrete cosine, fractal, or wavelet transform of the image
- » software and circuitry
- » network packets
- » strands of Human DNA (Genome coding )
- » text
- » HTML
- » the side channel of electrical systems

# Some Known Uses of Steganography

- Economic espionage - used to exfiltrate information from corporations
- Political extremists, survivalists - increasingly being used for secure communications, e.g., Germany, Tea Party
- Fraud - used as a “digital dead drop” to hide stolen card numbers on a hacked web page
- Pedophilia - used to store and transmit pornographic images
- Terrorism - used to hide terrorist communications over the Internet, e.g., Osama bin Laden’s alleged use of steganography
- Paranoid - Anyone who wants to communicate covertly and anonymously
- Individuals concerned about perceived government “snooping”



# Why Use Steganography

- Maintain anonymity
- Creating covert channels for private communications
- Data infiltration/exfiltration
- Creating covert channels for private communications
- Digital signatures for file authentication (digital watermarking or copyrighting)
- Web surfer tracking/direct marketing

# Terrorism

- Alleged use of stego by Osama bin Laden, Muslim extremists (Feb '01)
- Stego'd messages hidden on web sites to plan attacks against the US
- Maps, target photos hidden in sports chat rooms, pornographic bulletin boards, popular web sites



# Static steganography

This hiding of data within the static medium of the new digital technologies: pictures, video and audio files, Word documents, Powerpoint documents, Excel spreadsheets, movie files, et. al. Almost any digital file on a hard drive can have information embedded into it without any apparent presence.

It occurs on the bit/byte level.



# Dynamic steganography

Taking this a further step and one not apparent to the layman, data can also be hidden in the medium of the Internet, the layer that the data flows over, in the packets that travel from computer to computer, over twisted pair, Ethernet and optical connections, through firewalls and routers, from network to network, untouched by the fingers of any telegrapher or data technician, in the electrical current that flows over the power transmission lines. This is dynamic steganography.

This is the covert channel of the Internet.

# The initial concept of covert channel

- The notion of covert channel was first introduced by Lampson\*. “A covert channel is a parasitic communication channel that draws bandwidth from another channel in order to transmit information without the authorization or knowledge of the latter channel’s designer, owner or operator”.
- \* Butler W. Lampson. A note on the confinement problem. *Communications of the ACM*, 16(10):613–615, 1973.



# Covert channels

It is a means of communication that is not part of the original design of the system. It could even be said that a covert channel is a security flaw. It is a part of a program or system that can cause the system to violate its security requirements. It can be an electronic means of sending and hiding messages. Covert channels can be a means of taking any normal electronic communications and adding some secret element that does not cause noticeable interference to the original item such as a picture, sound file or other digital communication medium.

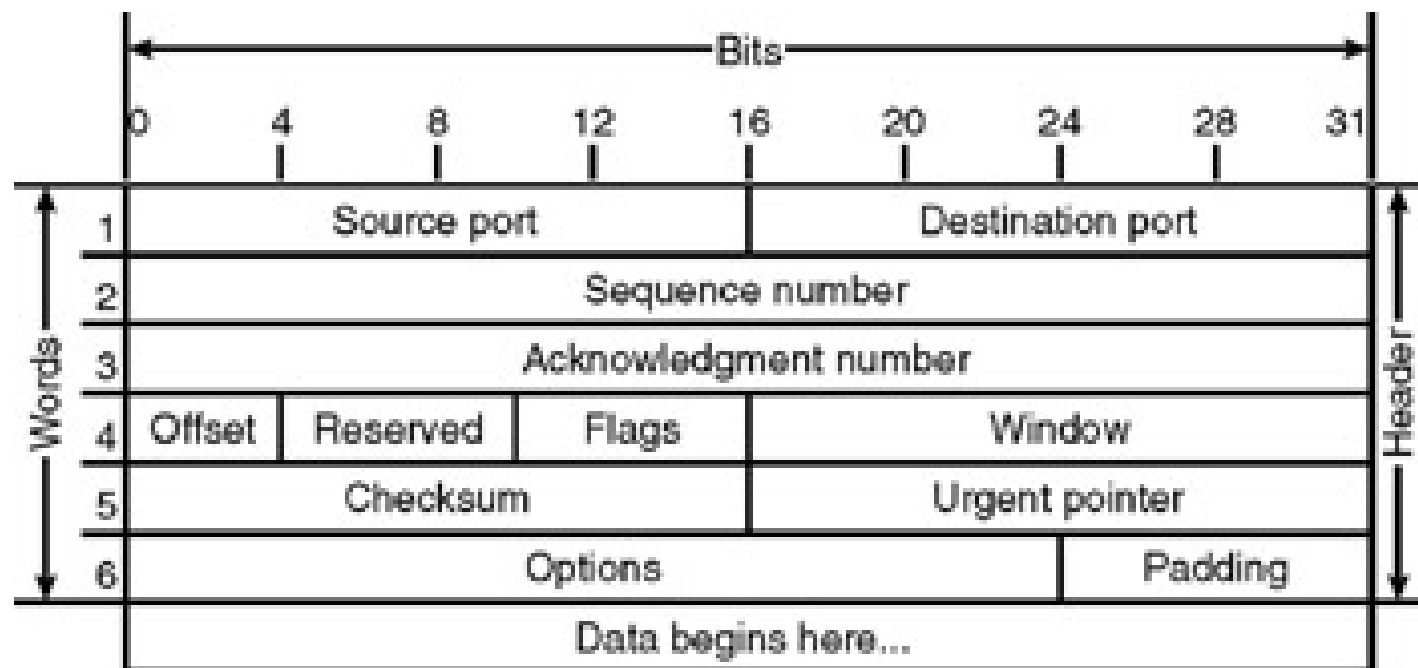


# TCP/IP Header Fields

The TCP/IP header fields that currently can be used to hide data include the following:

- TCP Sequence Number
- Type of Service
- IP Identification
- IP Flags
- IP Fragment Offset
- IP Options
- TCP Timestamp
- Packet Order

# TCP HEADER







# Leading packet crafting tools

- Hping2 : A network probing utility like ping - assembles and sends custom ICMP, UDP, or TCP packets
- Scapy : Interactive packet manipulation tool - packet generator, network scanner
- Nemesis : Packet injection simplified – command line; scripting of injected packet streams from simple shell script
- Yersinia : A multi-protocol low-level attack tool - useful for penetration testing

# Patentable?

In 2008, use of the TTL (Time to live) field in the IP header to mark certain packets was patented



US007415018B2

(12) **United States Patent**  
Jones et al.

(10) **Patent No.:** US 7,415,018 B2  
(45) **Date of Patent:** Aug. 19, 2008

(54) **IP TIME TO LIVE (TTL) FIELD USED AS A COVERT CHANNEL.** 2003/0172289 A1 9/2003 Soppera

(75) Inventors: **Emanuele Jones**, Ottawa (CA); **Olivier Le Moigne**, Ottawa (CA); **Jean-Marc Robert**, Ottawa (CA)

**OTHER PUBLICATIONS**

Abraham Yaar et al: "Pi: A path identification mechanism to defend against DDoS attacks." Proceedings of the 2003 Symposium on Security and Privacy. (S&P 2003). Berkeley, CA, May 11-14, 2003, Proceedings of the IEEE Symposium on Security and Privacy, Los Alamitos, CA: IEEE Comp. Soc., US May 11, 2003 (pp. 93-107).

(73) Assignee: **Alcatel Lucent**, Paris (FR)

(\* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 918 days.

\* cited by examiner

(21) Appl. No.: **10/663,791**

*Primary Examiner*—Chau Nguyen  
*Assistant Examiner*—Hicham B Foud

(22) Filed: **Sep. 17, 2003**

(65) **Prior Publication Data**  
US 2005/0058129 A1 Mar. 17, 2005

(57) **ABSTRACT**

(51) **Int. Cl.**  
*H04L 12/56* (2006.01)  
*H04L 12/28* (2006.01)  
(52) **U.S. Cl.** ..... 370/392; 370/401  
(58) **Field of Classification Search** ..... 370/252, 370/254, 255, 389, 392, 401  
See application file for complete search history.

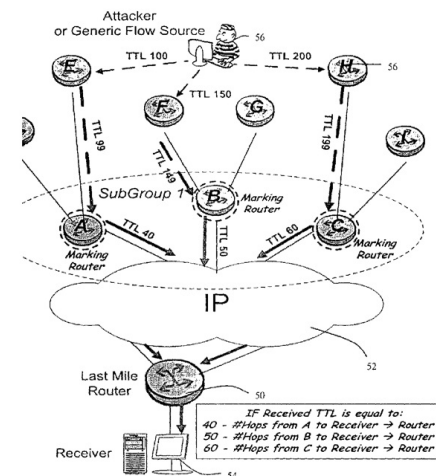
The Time to Live (TTL) field in an IP header is used as a covert channel in a communication system. More particularly the TTL field can be used to selectively mark packets with unique identifiers as they pass through an upstream station on their way to a downstream station. In this way the source of a traffic flow at least within a particular domain can be absolutely identified. This method of performing a traceback operation doesn't utilize additional resources as it relies on functionality which already exists in the system.

(56) **References Cited**

U.S. PATENT DOCUMENTS

7,200,673 B1 \* 4/2007 Augart ..... 709/238

**11 Claims, 3 Drawing Sheets**



# In 2004, Microsoft patented stealthy audio watermarking



US007266697B2

(12) **United States Patent**  
**Kirovski et al.**

(10) **Patent No.:** **US 7,266,697 B2**  
(45) **Date of Patent:** **Sep. 4, 2007**

(54) **STEALTHY AUDIO WATERMARKING**

EP 0 770 498 5/1997  
EP 0 840 513 5/1998

(75) Inventors: **Darko Kirovski**, Redmond, WA (US);  
**Henrique Malvar**, Redmond, WA (US)

(Continued)

(73) Assignee: **Microsoft Corporation**, Redmond, WA (US)

OTHER PUBLICATIONS

Cox et al., "Secure Spread Spectrum Watermarking for Multimedia", 1997, IEEE Transactions on Image Processing, vol. 6, No. 12, p. 1673-1687.\*

(Continued)

(\* ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 446 days.

Primary Examiner—Christopher Revak  
(74) Attorney, Agent, or Firm—Lee & Hayes, PLLC

(21) Appl. No.: **10/838,497**

(22) Filed: **May 3, 2004**

(57) **ABSTRACT**

(65) **Prior Publication Data**

US 2004/0204943 A1 Oct. 14, 2004

**Related U.S. Application Data**

(62) Division of application No. 09/614,660, filed on Jul. 12, 2000, now Pat. No. 7,020,285.

(60) Provisional application No. 60/143,432, filed on Jul. 13, 1999.

(51) **Int. Cl.**

**H04L 9/00** (2006.01)

**H04K 1/00** (2006.01)

(52) **U.S. Cl.** ..... **713/176; 380/201; 382/191**

(58) **Field of Classification Search** ..... None

See application file for complete search history.

(56) **References Cited**

**U.S. PATENT DOCUMENTS**

5,646,997 A 7/1997 Barton

5,687,236 A 11/1997 Moskowitz et al.

5,745,604 A 4/1998 Rhoads et al.

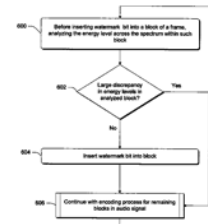
(Continued)

**FOREIGN PATENT DOCUMENTS**

EP 0 581 317 2/1994

Described herein is audio watermarking technology for inserting and detecting watermarks in audio signals, such as a music clip. The watermark identifies the content producer, providing a signature that is embedded in the audio signal and cannot be removed. The watermark is designed to survive all typical kinds of processing and malicious attacks. In one described implementation, a watermarking system employs chess spread-spectrum sequences (i.e., "chess watermarks") to improve the balance of positive and negative chips in the watermarking sequences. The balance is not imposed in an orderly fashion, which might make the watermark sequence more easily detectable to an attacker, but in a pseudo-random fashion. In that way, better sequence balance is achieved while preserving its randomness for an attacker without knowledge of the keys. In another described implementation, a watermarking system employs an energy-level trigger to determine whether to skip encoding of a portion of a watermark within a given time span of an audio clip. If a large discrepancy in energy levels exists over a given time frame, then the frame is not watermarked, to avoid audible time-dispersion of artifacts due to spectral modifications (which are similar to "pre-echo" effects in audio coding). In another described implementation, a watermarking system begins encoding of a watermark at a variable position after the beginning of an audio clip.

**7 Claims, 13 Drawing Sheets**





# Steganalysis

- » “It is the technique used to discover the existence of hidden information”.
- » A counter-measure to Steganography

# Scale of the Problem

- There is little public information on the use of data hiding techniques by cybercriminals
- Only recently has the security community started to concern itself with this subject
  - » Lack of awareness
  - » Lack of developed analysis tools and techniques
- It is believed that hiding techniques are predominantly used by more advanced criminals (organized crime) and some emerging threats, e.g., terrorists, nation-states
- Availability, new easy-to-use interfaces may increase attractiveness of stego techniques for the average user

# Steganography Software tools

- » Freeware
- » Shareware
- » Commercial

<http://www.jjtc.com/Steganography/tools.html>

# Some Steganography Software tools

## » S – Tools

- » Excellent tool for hiding files in GIF, BMP and WAV files

## » MP3Stego

- » Mp3. Offers quality sound at 128 kbps
- » Compresses, encrypts, then hides data in an MP3 bit stream

## » Hide4PGP

- » BMP, WAV, VOC

## » JP Hide and Seek

- » jpg

## » Text Hide ( commercial)

- » text

## » Stego Video

- » Hides files in a video sequence

## » Spam mimic

- » encrypts short messages into email that looks like spam
- » <http://spammimic.com>



# Steganalysis - Detection and Analysis

- » “It is the technique used to discover the existence of hidden information”.
- » A counter-measure to Steganography





# Need for Improved Detection

- Growing awareness of data hiding techniques and uses
- Availability and sophistication of shareware and freeware data hiding software
- Concerns over use to hide serious crimes, e.g., drug trafficking, pedophilia, terrorism



# Deep Packet Inspection

One way would be to develop Internet appliances that have the capability to detect anomalies in any packet header field. Such devices are, in fact available, but are not marketed to the general public. These devices go beyond the capability and functionality of normal routers, firewalls and intrusion detection systems. These appliances are only available to law enforcement agencies and operate under the radar. These are called active wardens and add to the cybersecurity defenses already available.



## There are three types of wardens

- a passive warden can only spy on the channel but cannot alter any messages;
- an active warden is able to slightly modify the messages, but without altering the semantic context;
- a malicious warden may alter the messages without impunity



## Network appliances and steganalysis detection

Network appliances such as routers and firewalls play a large role in handling and parsing network traffic. Directing data between portions of a network is the primary purpose of a router. Therefore, the security of routers and their configuration settings is vital to network operation. In addition to directing and forwarding packets, a router may be responsible for filtering traffic, allowing some data packets to pass and rejecting malformed or suspect packets. This filtering function is a very important responsibility for routers; it allows them to protect computers and other network components from illegitimate or hostile traffic.



# Intelligent Support Systems

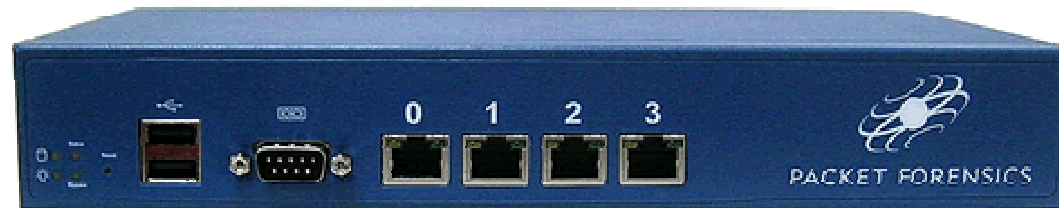
Intelligent Support Systems for Lawful Interception, Criminal Investigation, and Intelligence Gathering (ISS), holds wiretapping conferences and seminars for the law enforcement community, military, governmental agencies and homeland security agencies.



# Packet Forensics, Inc.

Packet Forensics, was marketing Internet spying boxes to the feds at a recent ISS conference. The web site of Packet Forensics lists the products available from the company, though some pages are restricted to authorized law enforcement and intelligence organizations only. These protected pages contain information too sensitive for the public. These Internet appliances automate the processes that allow observation and collection of data on Internet traffic and/or phone calls when given the legal authority by either court order or mandate provided by legal statute to do so. These Internet appliances perform lawful interception, investigative analysis and intelligence gathering while protecting the privacy rights and civil liberties of the law-abiding users of the Internet. These appliances can handle a large number of surveillance requests while collecting the evidence needed to convict the guilty and head off possible terrorist exploits before they occur. Their products are recommended to government investigators so IP communication traffic can be examined at will.

# Packet Forensics, Inc.



Packet Forensics LI-5B





# Nokia-Siemens Networks

The administration of Iran uses equipment provided by Nokia-Siemens that performs deep packet inspection. It allows the regime to search for keywords in email and voice transmissions in what is called a “lawful intercept”.





# Detection

- Can steganography be detected?
  - *Sometimes...* many of the simpler steganographic techniques produce some discernable change in the file size, statistics, or both. For image files, these include:
    - Color variations
    - Loss of resolution or exaggerated noise
    - Images larger in size than that to be expected
    - Characteristic signatures, e.g., distortions or patterns
  - However, detection often requires *a priori* knowledge of what the image or file should look like



# Detection Challenges

- Stego software has its weaknesses
- Difficult to use
- Lack of tools and techniques to recover the hidden data
- No commercial products exist for detection
- Custom tools are analyst-intensive



# Steganalysis

- Must improve stegananalysis methods
- Analyze how various Internet appliances such as routers, IDSs, et. al. handle bad and illegal data and malformed packets
- Is the data deleted?
- Is the data modified?
- Are the packets rejected?
- Are the exceptions tracked?



## Conclusions:

- Steganography works when nobody expects it
- New techniques being researched
- Sometimes the best place to hide something may be in plain sight

# Summary

- Steganography is primarily used to maintain anonymity and is easily available to most anyone
- Sophisticated tools are readily available on the Internet, and are easy-to-use
- Steganography can use almost anything as a medium to convey a hidden message
- Lack of both awareness and developed tools and analysis techniques
- Only recently has the security community started to concern itself with this subject
- Little public information on the use of data hiding
- Development/use of information hiding products far outpaces the ability to detect/recover them
- This situation is not likely to change soon

Any Questions?



**The end.**

