FORFUN

Week 6 Anti-Forensics

Soraya Harding & Rahim Taheri

Session Content

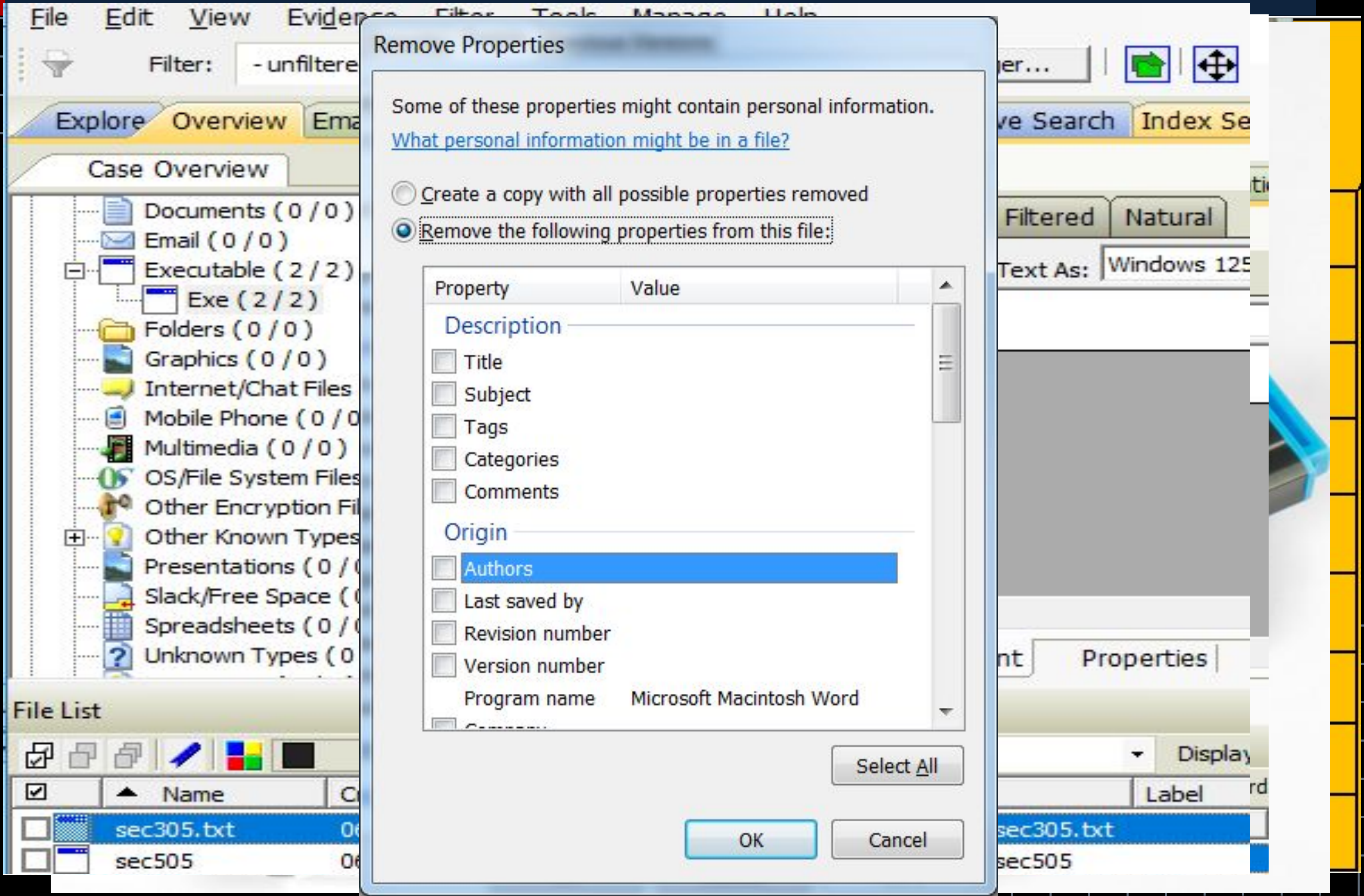
- Introduction to Anti-Forensics
- Data Hiding Techniques
- Data Encryption
- Data Forgery
- Data Deletion
- Conclusions

Introduction to Anti-Forensics

Anti-Forensics

- The use of techniques and tools to hide, modify or remove potential evidence
- Making investigations on digital media more difficult or impossible to conduct and therefore, more expensive.
- Anti-Forensic techniques
  - Data Hiding
  - Data Encryption
  - Data Forgery
  - Data Deletion

Attacks on Investigation Processes



Remove Properties

Some of these properties might contain personal information.

What personal information might be in a file?

○ Create a copy with all possible properties removed

● Remove the following properties from this file:

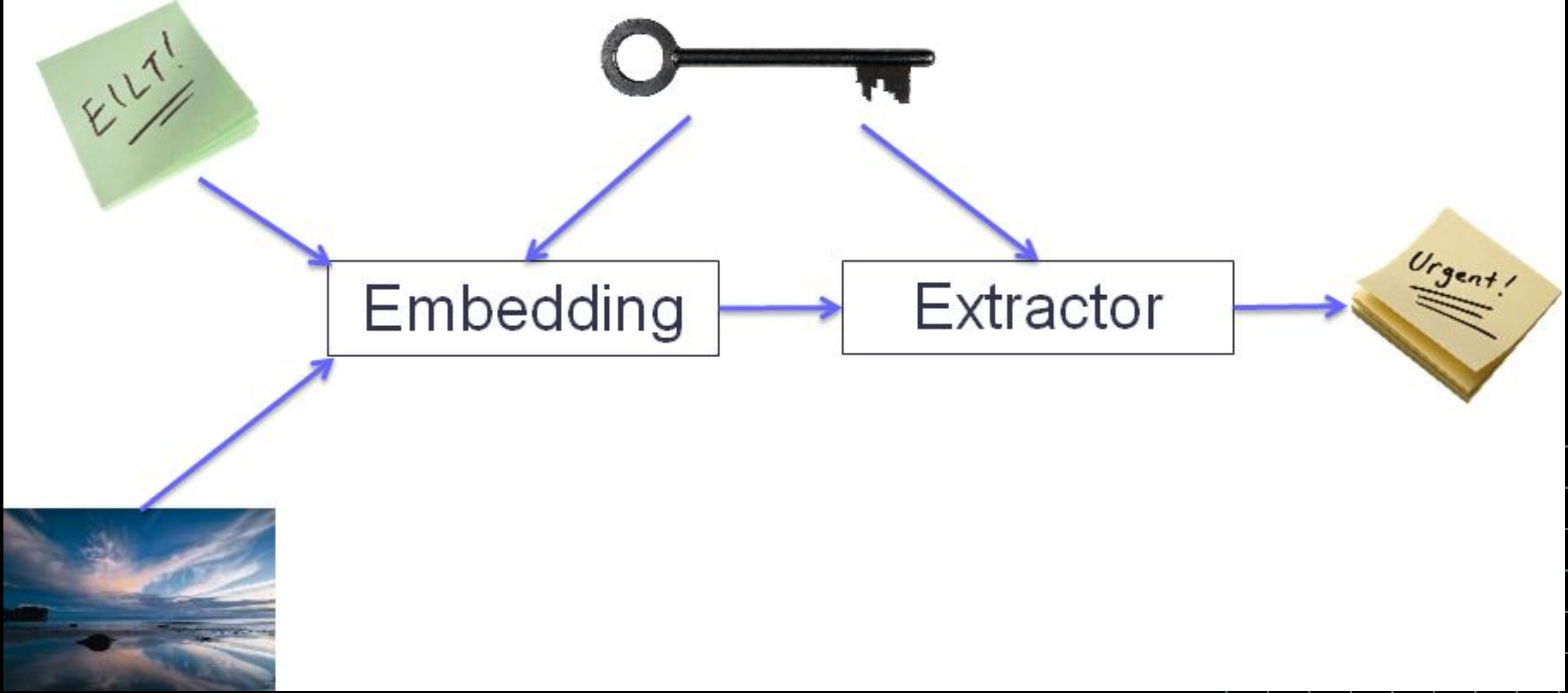
Property	Value
Description	
□ Title	
□ Subject	
□ Tags	
□ Categories	
□ Comments	
Origin	
□ Authors	
□ Last saved by	
□ Revision number	
□ Version number	
Program name	Microsoft Macintosh Word

Data Hiding

Steganography

- Steganography is the art of covered writing
- The purpose of steganography is to hide the real content of a message from a third party.
- This differs from cryptography, the art of secret writing, which is intended to make a message unreadable by a third party but does not hide the existence of the secret communication.
- Although steganography is separate and distinct from cryptography, there are many analogies between the two, and some authors categorize steganography as a form of cryptography.

Steganography



History

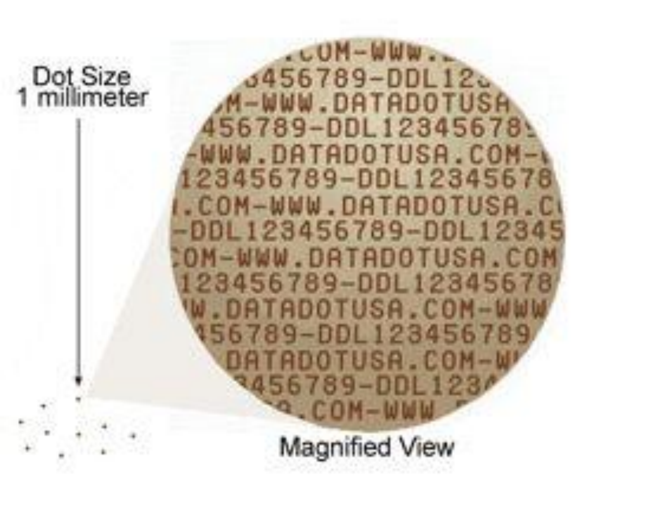
- In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves.

- Invisible ink has been in use for centuries-for fun by children and students and for serious espionage by spies and terrorists.

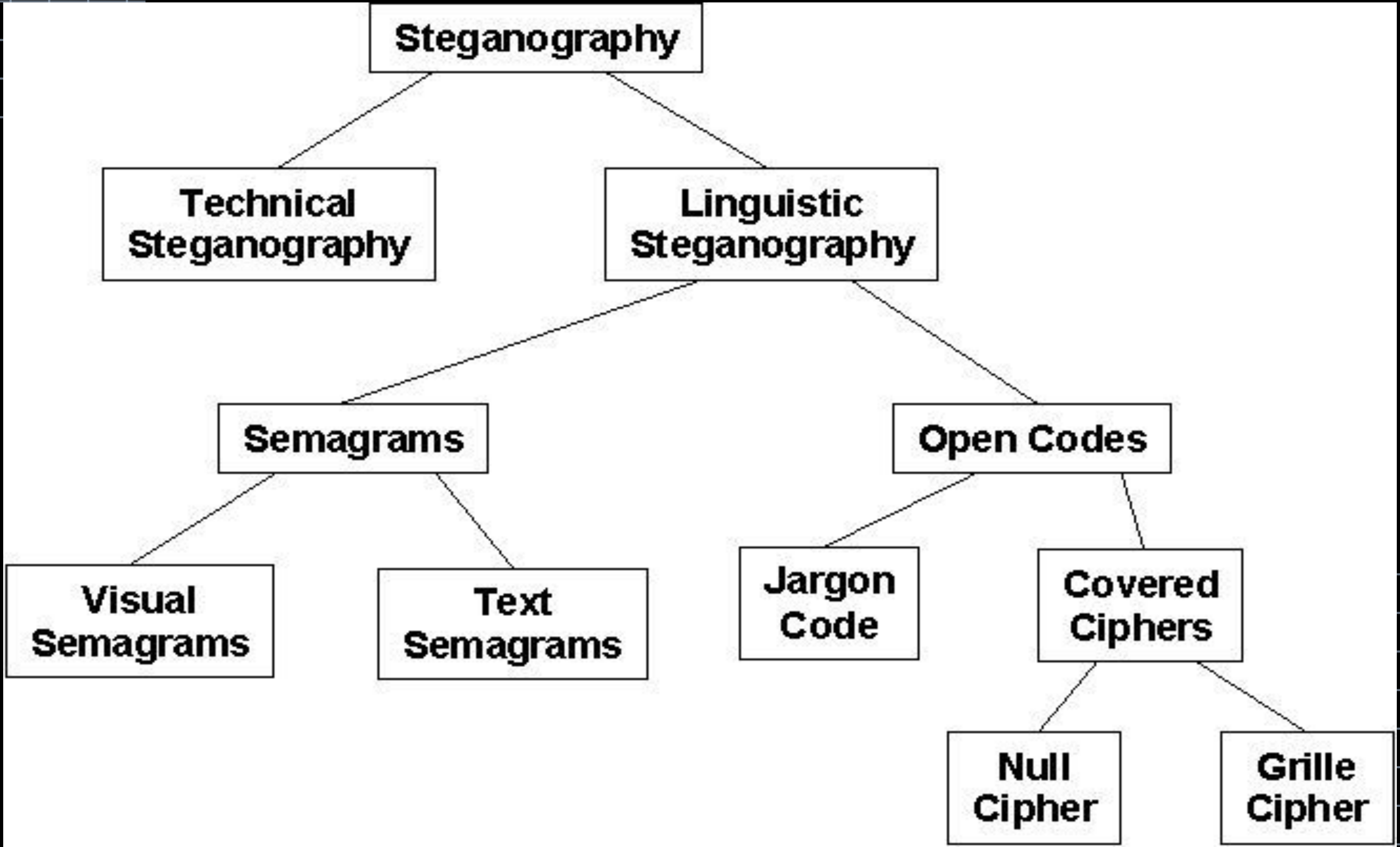
- Microdots and microfilm, a staple of war and spy movies, came about after the invention of photography.

History

INVISIBLE INK PEN
U.V Ink Pen with Black Light
INVISIBLE INK PEN
BLACK LIGHT TORCH
Write
Normal Light
Black LIGHT
OFA PRODUCTS.COM
0800 2300239


Dot Size
1 millimeter
Magnified View
.COM-WWW.DATADOTUSA.COM
123456789-DDL123456789

Classification of Steganography Techniques

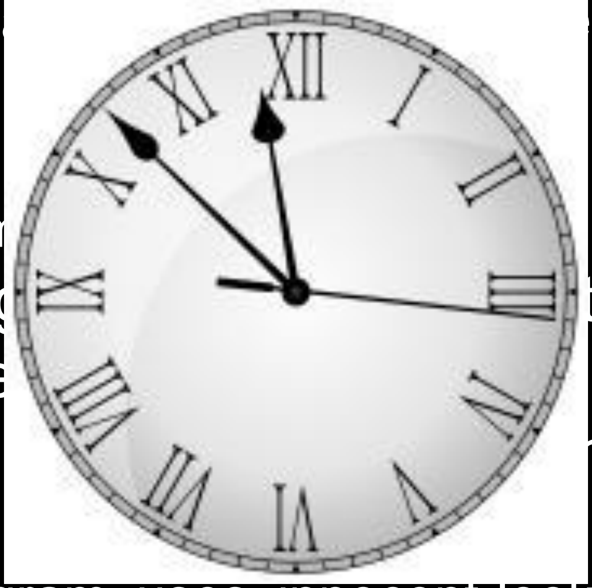


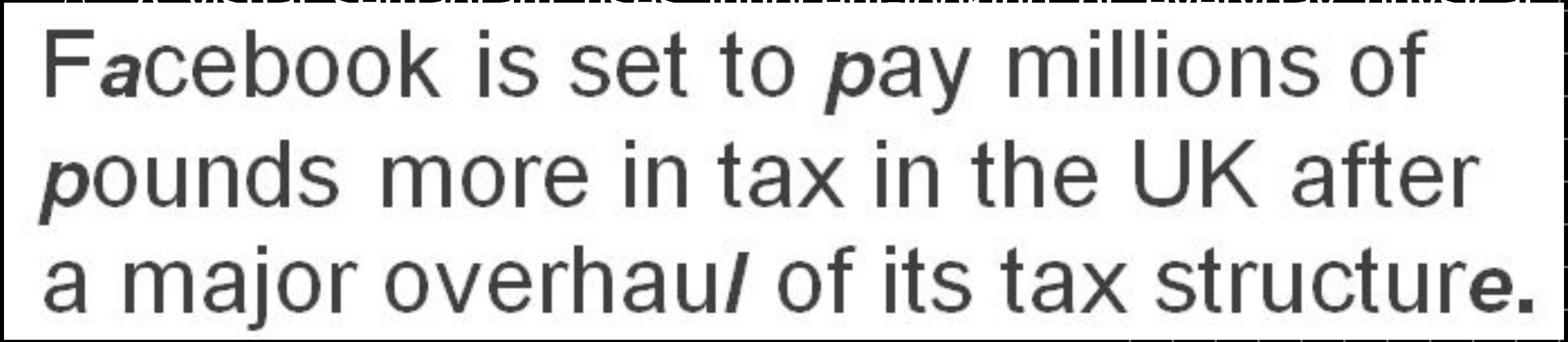
Techniques (1)

- Technical steganography uses scientific methods to hide a message
  - Examples: the use of invisible ink or microdots and other size-reduction methods.
- Linguistic steganography hides the message in the carrier in some nonobvious ways
- Semagrams hide information by the use of symbols or signs.
  - A visual semagram uses innocent-looking or everyday physical objects to convey a message, such as doodles or the positioning of items on a desk or Website.
  - A text semagram hides a message by modifying the appearance of the carrier text, such as subtle changes in font size or type, adding extra spaces, or different flourishes in letters.

Techniques (1)

- Technical steg ntific methods to hide a message
  - Examples: the or microdots and other size-reduction m
- Linguistic steg the message in the carrier in some
- Semagrams h he use of symbols or signs.
  - A visual semagram uses innocent-looking or everyday physical





Facebook is set to pay millions of pounds more in tax in the UK after a major overhaul of its tax structure.

Techniques (2)

- Open codes hide a message in a legitimate carrier message in ways that are not obvious to an unsuspecting observer. The carrier message is sometimes called the overt communication whereas the hidden message is the covert communication.
- Jargon code, as the name suggests, uses language that is understood by a group of people but is meaningless to others..
- Covered or concealment ciphers hide a message openly in the carrier medium so that it can be recovered by anyone who knows the secret for how it was concealed.

Null Ciphers

- Null ciphers are a way to hide a message in another without the use of a complicated algorithm. One of the simplest null ciphers is shown in a classic example below:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

Null Ciphers

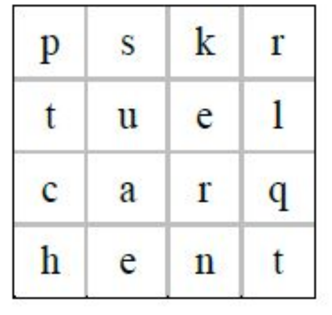
- Null ciphers are a way to hide a message in another without the use of a complicated algorithm. One of the simplest null ciphers is shown in a classic example below:

PRESIDENT'S EMBARGO RULING SHOULD HAVE IMMEDIATE NOTICE. GRAVE SITUATION AFFECTING INTERNATIONAL LAW. STATEMENT FORESHADOWS RUIN OF MANY NEUTRALS. YELLOW JOURNALS UNIFYING NATIONAL EXCITEMENT IMMENSELY.

PERSHING SAILS FROM N.Y. JUNE 1

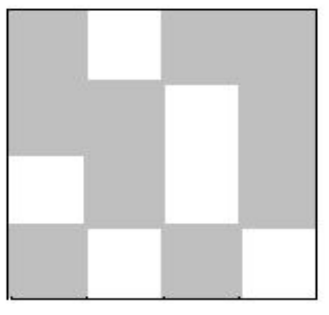
Grille Ciphers

- A grille cipher employs a template that is used to cover the carrier message. The words that appear in the openings of the template are the hidden message.

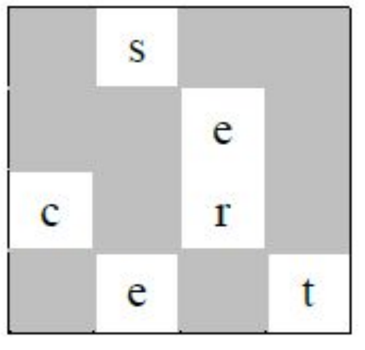


p	s	k	r
t	u	e	l
c	a	r	q
h	e	n	t

Plain text



Cardboard



	s		
		e	
c		r	
	e		t

Mapped letters

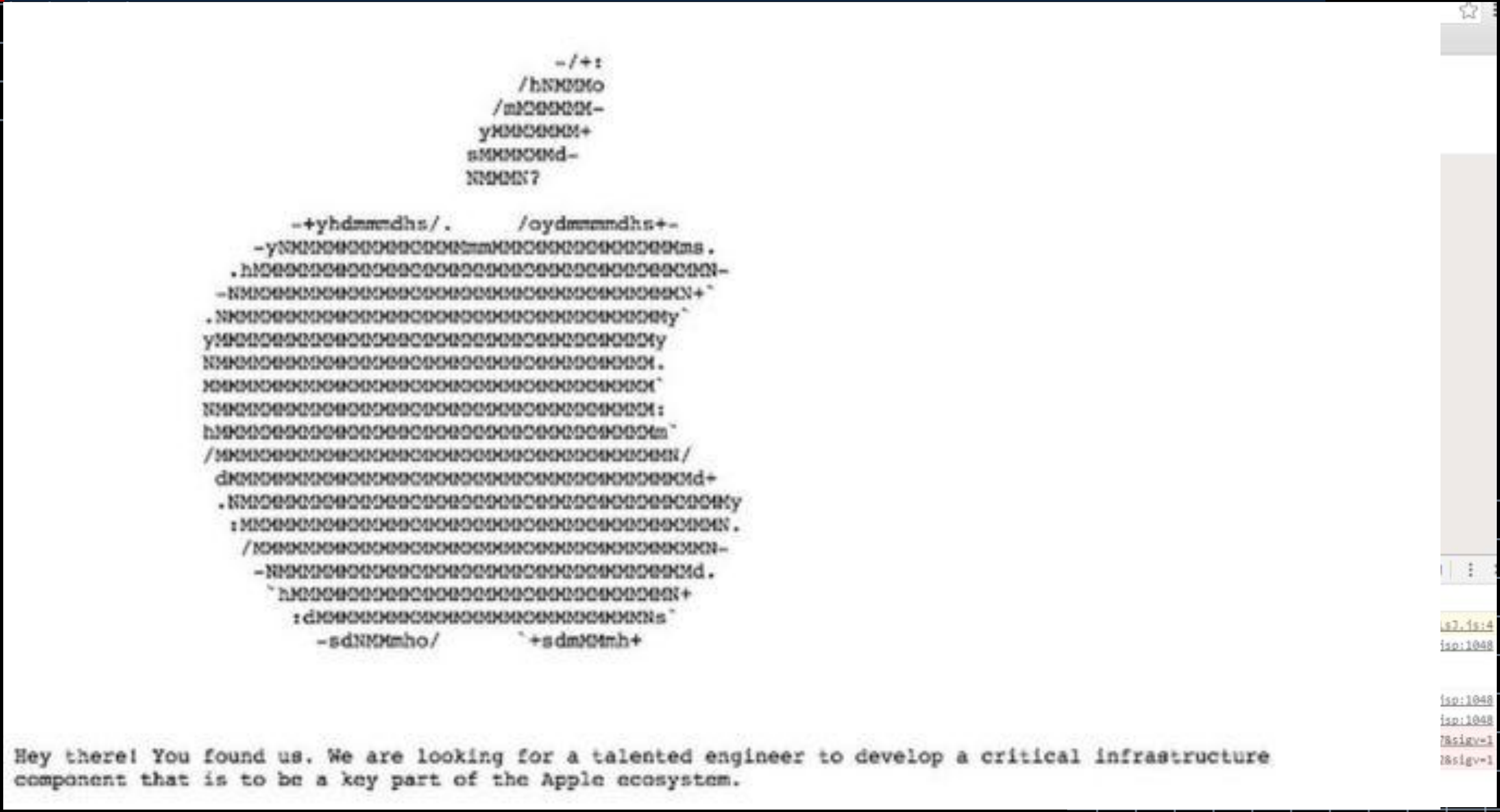
secret

Modern Days Steganography

Simple Hiding Techniques

- An image or text block can be hidden under another image in a PowerPoint file.
- Messages can be hidden in the properties of a Word file.
- Messages can be hidden in comments in Web pages or in other formatting vagaries that are ignored by browsers.
- Text can be hidden as line art in a document by putting the text in the same colour as the background and placing another drawing in the foreground. The recipient could retrieve the hidden text by changing its colour.

Simple Hiding Techniques



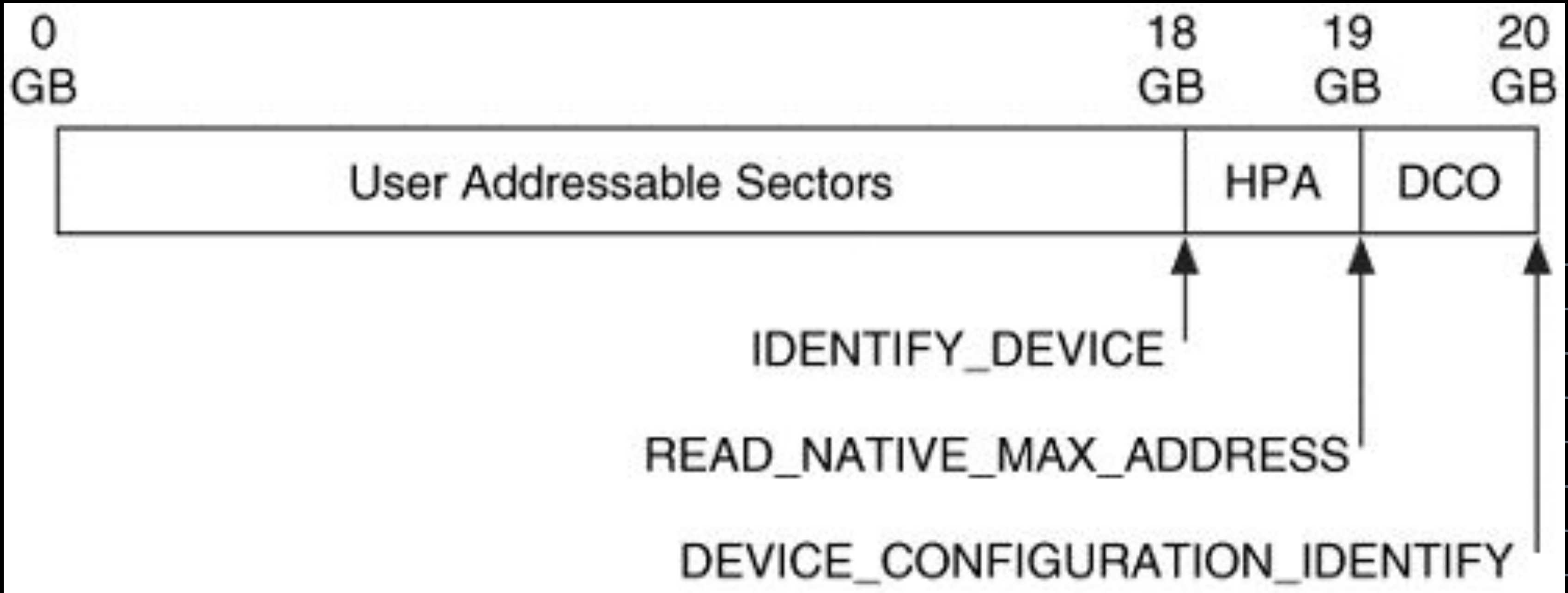
Hey there! You found us. We are looking for a talented engineer to develop a critical infrastructure component that is to be a key part of the Apple ecosystem.

Data Hiding Locations

- Host Protected Area (HPA) and Disk Configuration Overlay (DCO)
  - HPA allows users to make a manufacturer reset
  - DCO allows a hard disk size to be limited
- Unused space in MBR
  - DOS partition - 62 sectors
  - NTFS – 2,047 sectors
- Slack space: File slack
  - Slacker – part of the Metasploit Framework
- Bad sectors: *$BadClus* in NTFS

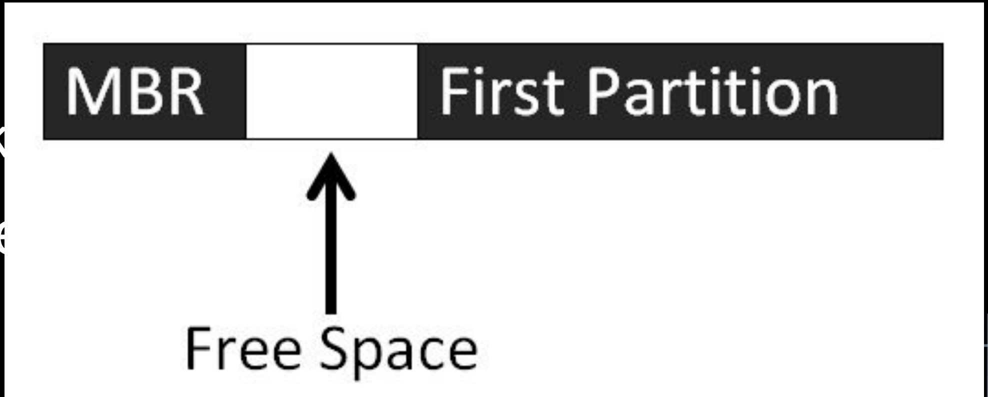
Data Hiding Locations

- Host Protected Area (HPA) and Disk Configuration Overlay (DCO)
  - HPA allows users to make a manufacturer reset
  - DCO allows a hard disk size to be limited

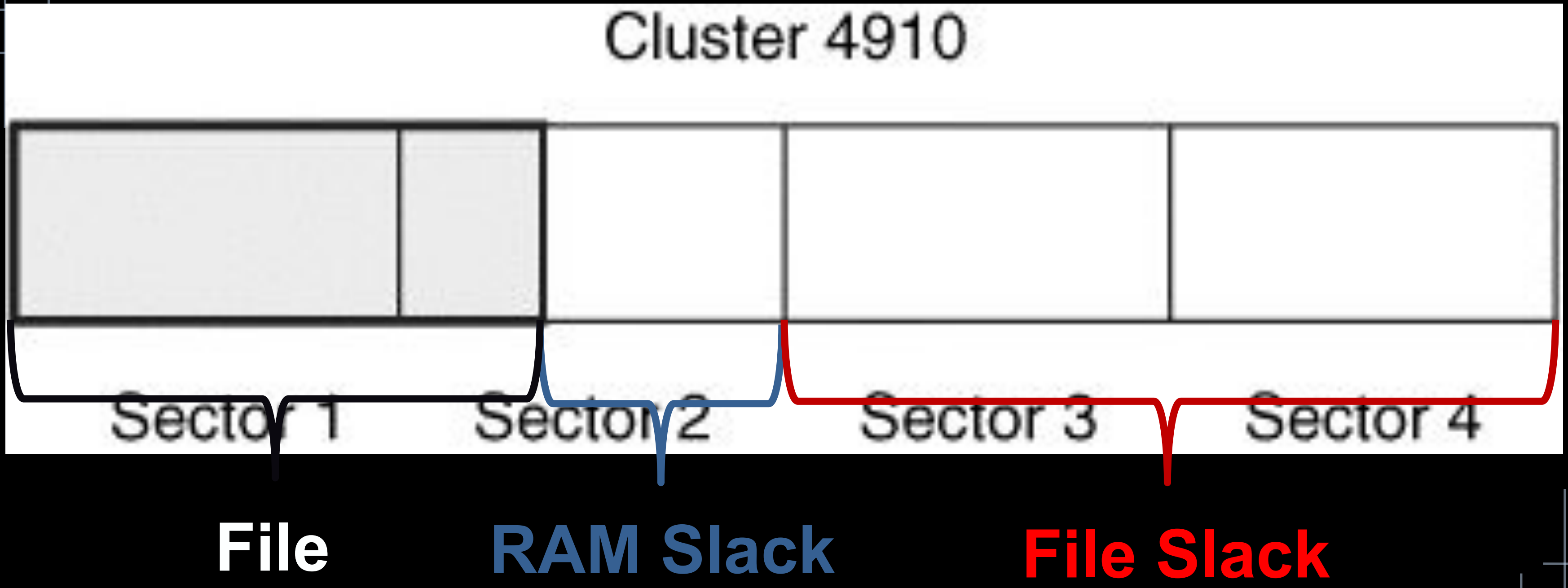


Data Hiding Locations

- Host Protected Area (HPA) and Disk Configuration Overlay (DCO)
  - HPA allows users to make a manufacturer reset
  - DCO allows a hard disk size to be limited
- Unused space in MBR
  - DOS partition - 62 sectors
  - NTFS – 2,047 sectors
- Slack
  - Slack
- Bad se



Data Hiding Locations



- Slack space: File slack
  - Slacker – part of the Metasploit Framework
- Bad sectors: *$BadClus* in NTFS

Data Hiding Locations

- Host Protected Area (HPA) and Disk Configuration Overlay (DCO)
  - HPA allows users to make a manufacturer reset
  - DCO allows a hard disk size to be limited
- Unused space in MBR
  - DOS partition - 62 sectors
  - NTFS – 2,047 sectors
- Slack space: File slack
  - Slacker – part of the Metasploit Framework
- Bad sectors: *$BadClus* in NTFS

Digital Carriers

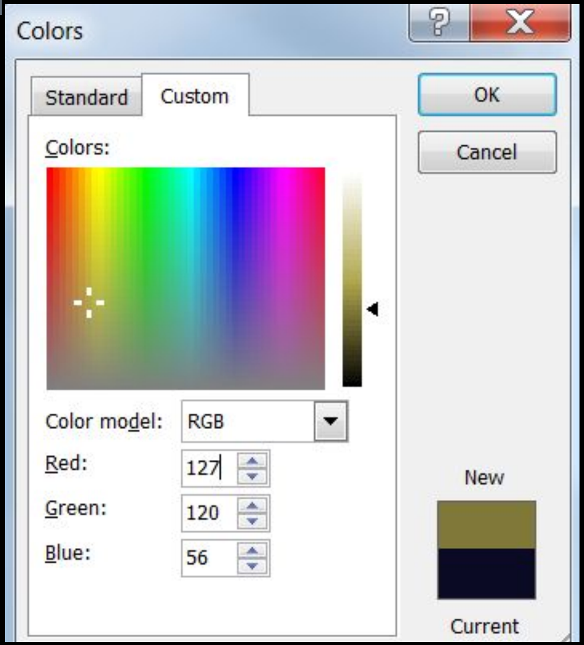
- Many common digital steganography techniques employ graphical images or audio files as the carrier medium.
- The most common steganography method in audio and image files employs some type of least significant bit substitution or overwriting.
- The high-order or most significant bit is the one with the highest arithmetic value (i.e., 2^7=128)
- The low-order or least significant bit is the one with the lowest arithmetic value (i.e., 2^0=1).

Digital Carriers

MSB

Original

LSB

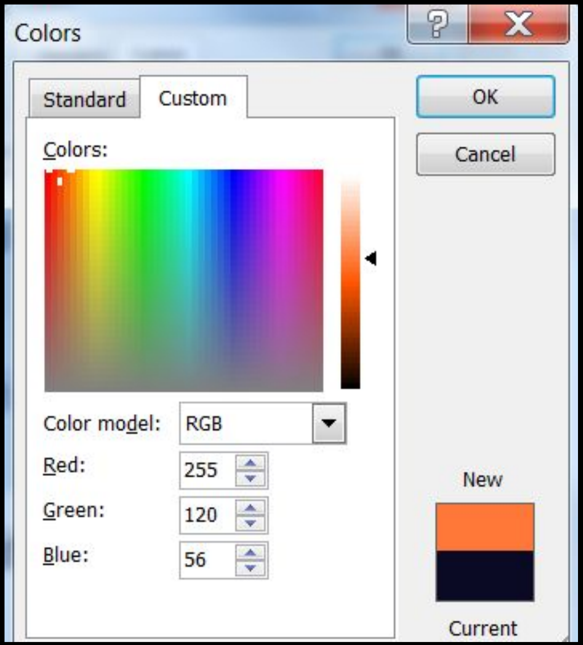


Color model: RGB

Red: 127

Green: 120

Blue: 56

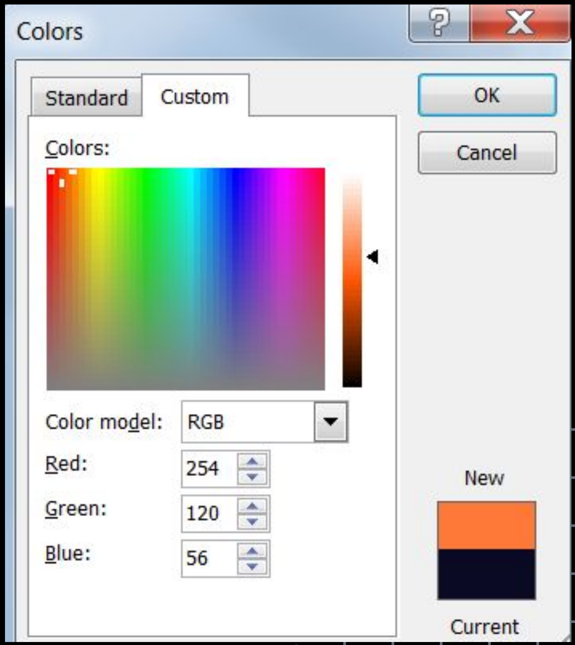


Color model: RGB

Red: 255

Green: 120

Blue: 56



Color model: RGB

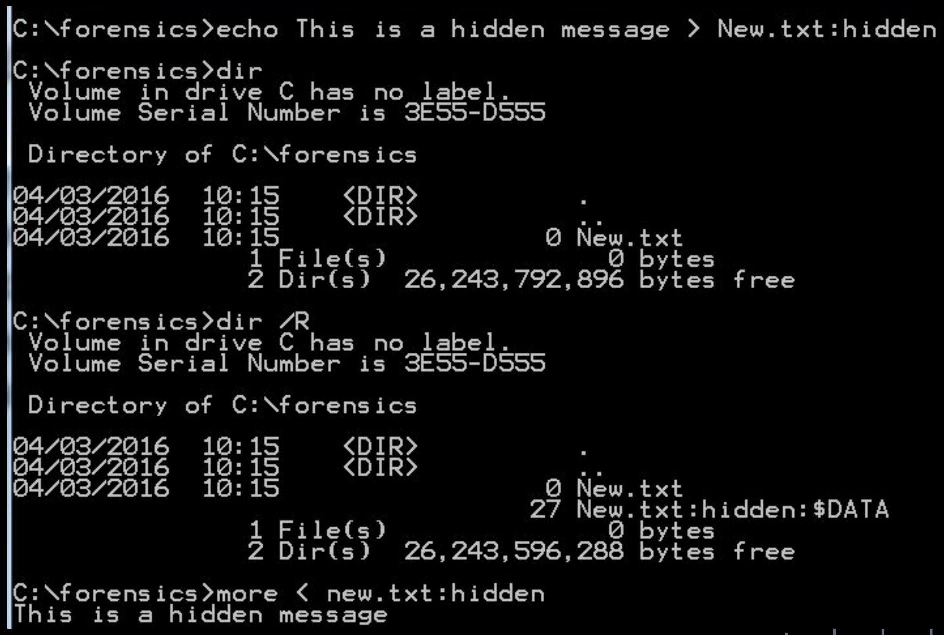
Red: 254

Green: 120

Blue: 56

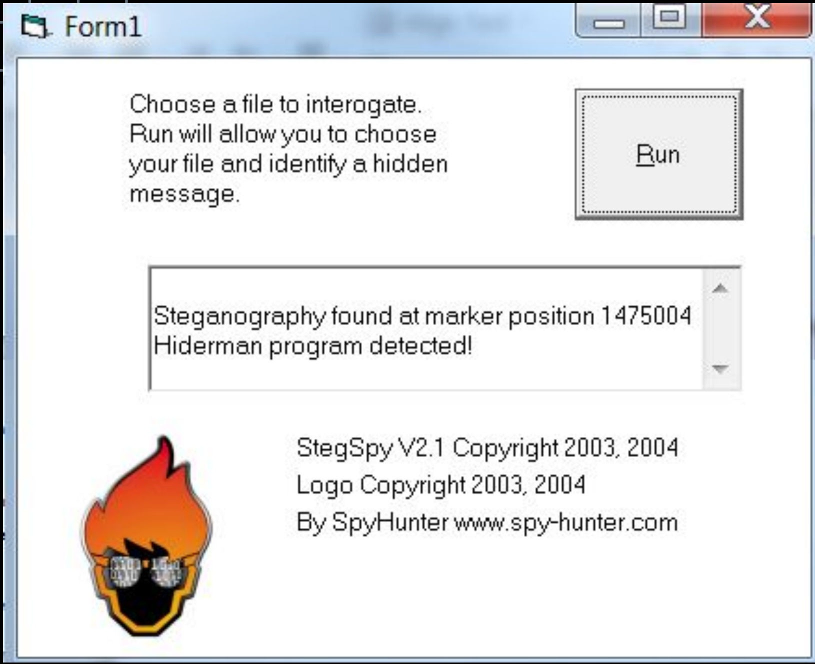
Alternate Data Streams

- Alternate Data Streams allow arbitrary metadata to be associated with files and directories on Windows NTFS
  - The size of the file will not be changed
  - If a file is moved, any ADS will move along with it.



```
C:\forensics>echo This is a hidden message > New.txt:hidden

C:\forensics>dir
 Volume in drive C has no label.
 Volume Serial Number is 3E55-D555

 Directory of C:\forensics

04/03/2016  10:15    <DIR>          .
04/03/2016  10:15    <DIR>          ..
04/03/2016  10:15                 0 New.txt
               1 File(s)              0 bytes
               2 Dir(s)  26,243,792,896 bytes free

C:\forensics>dir /R
 Volume in drive C has no label.
 Volume Serial Number is 3E55-D555

 Directory of C:\forensics

04/03/2016  10:15    <DIR>          .
04/03/2016  10:15    <DIR>          ..
04/03/2016  10:15                 0 New.txt
                                 27 New.txt:hidden:$DATA
               1 File(s)              0 bytes
               2 Dir(s)  26,243,596,288 bytes free

C:\forensics>more < new.txt:hidden
This is a hidden message
```

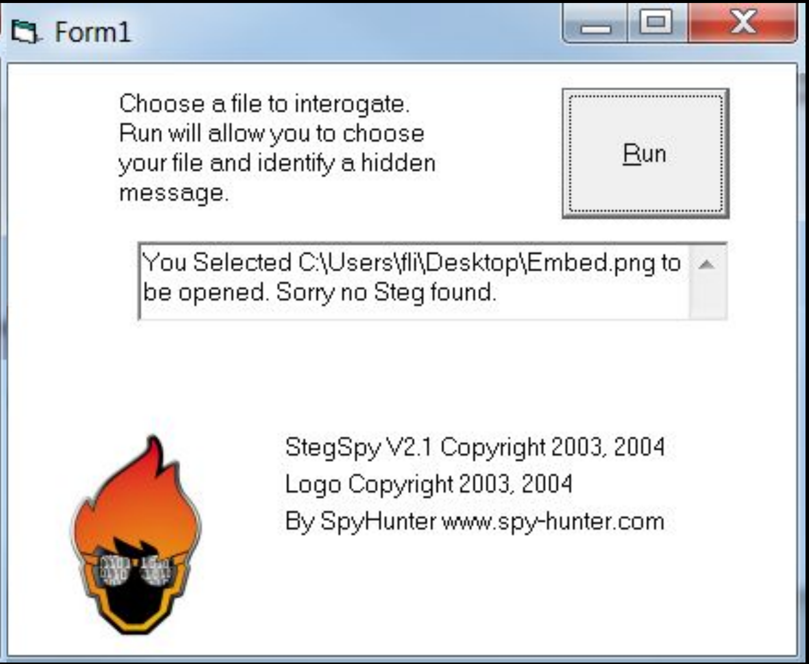
Steganography Detection



Choose a file to interogate. Run will allow you to choose your file and identify a hidden message.

Steganography found at marker position 1475004
Hiderman program detected!

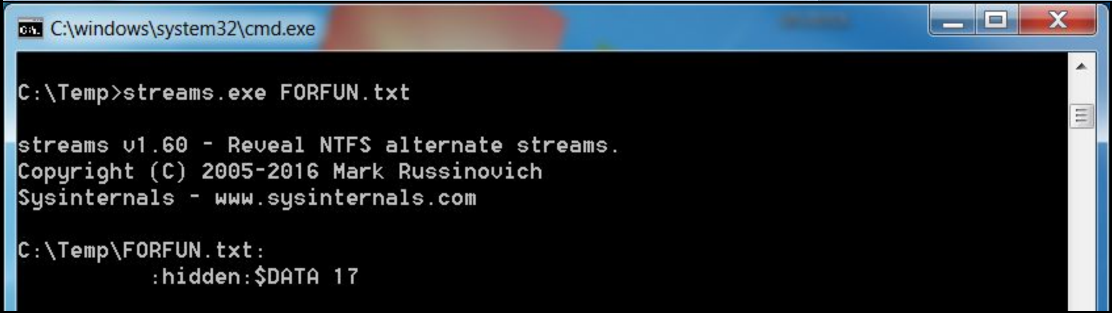
StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com



Choose a file to interogate. Run will allow you to choose your file and identify a hidden message.

You Selected C:\Users\fli\Desktop\Embed.png to be opened. Sorry no Steg found.

StegSpy V2.1 Copyright 2003, 2004
Logo Copyright 2003, 2004
By SpyHunter www.spy-hunter.com



```
C:\Temp>streams.exe FORFUN.txt

streams v1.60 - Reveal NTFS alternate streams.
Copyright (C) 2005-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

C:\Temp\FORFUN.txt:
          :hidden:$DATA 17
```

Data Encryption

Encryption

- Files are password protected and encrypted (e.g. Microsoft Office documents/Adobe PDF AES 256-bit)
- System is encrypted: Windows Encrypting File System (EFS)
- Storage is encrypted (e.g. encrypted USB sticks): Bitlocker (Windows) & FileVault(OSX)
- Regulation of Investigatory Powers Act (RIPA) forces individuals and organizations to release cryptographic keys – up to 5 years in prison

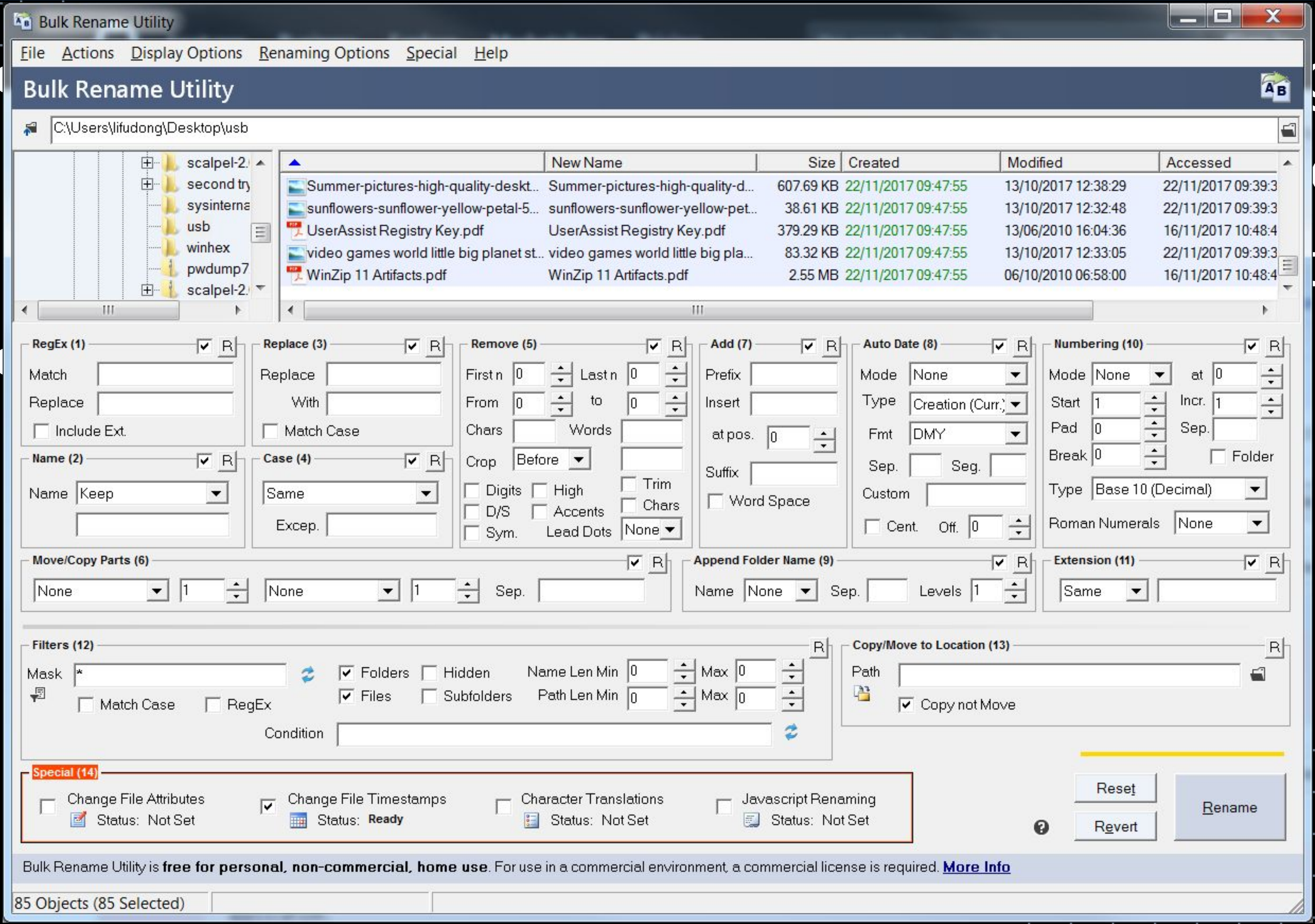
Encryption

- Example - October 2010 – Refusal to provide computer password
  - 50 character password
  - Jailed for 16 weeks
  - https://www.bbc.co.uk/news/uk-england-11479831

Data Forgery

Data Forgery

- g the
  ence
  tion
- files,



C:\Users\lifudong\Desktop\usb

	New Name	Size	Created	Modified	Accessed
Summer-pictures-high-quality-deskt...	Summer-pictures-high-quality-d...	607.69 KB	22/11/2017 09:47:55	13/10/2017 12:38:29	22/11/2017 09:39:3
sunflowers-sunflower-yellow-petal-5...	sunflowers-sunflower-yellow-pet...	38.61 KB	22/11/2017 09:47:55	13/10/2017 12:32:48	22/11/2017 09:39:3
UserAssist Registry Key.pdf	UserAssist Registry Key.pdf	379.29 KB	22/11/2017 09:47:55	13/06/2010 16:04:36	16/11/2017 10:48:4
video games world little big planet st...	video games world little big pla...	83.32 KB	22/11/2017 09:47:55	13/10/2017 12:33:05	22/11/2017 09:39:3
WinZip 11 Artifacts.pdf	WinZip 11 Artifacts.pdf	2.55 MB	22/11/2017 09:47:55	06/10/2010 06:58:00	16/11/2017 10:48:4

RegEx (1) ☑ R — Match, Replace, □ Include Ext.

Replace (3) ☑ R — Replace, With, □ Match Case

Remove (5) ☑ R — First n 0, Last n 0, From 0, to 0, Chars, Words, Crop Before, □ Digits, □ High, □ Trim, □ D/S, □ Accents, □ Chars, □ Sym., Lead Dots None

Add (7) ☑ R — Prefix, Insert, at pos. 0, Suffix, □ Word Space

Auto Date (8) ☑ R — Mode None, Type Creation (Curr.), Fmt DMY, Sep., Seg., Custom, □ Cent., Off. 0

Numbering (10) ☑ R — Mode None, at 0, Start 1, Incr. 1, Pad 0, Sep., Break 0, □ Folder, Type Base 10 (Decimal), Roman Numerals None

Name (2) ☑ R — Name Keep

Case (4) ☑ R — Same, Excep.

Move/Copy Parts (6) ☑ R — None, 1, None, 1, Sep.

Append Folder Name (9) ☑ R — Name None, Sep., Levels 1

Extension (11) ☑ R — Same

Filters (12) R — Mask *, □ Match Case, □ RegEx, ☑ Folders, □ Hidden, ☑ Files, □ Subfolders, Name Len Min 0, Max 0, Path Len Min 0, Max 0, Condition

Copy/Move to Location (13) R — Path, ☑ Copy not Move

Special (14)

□ Change File Attributes — Status: Not Set

☑ Change File Timestamps — Status: **Ready**

□ Character Translations — Status: Not Set

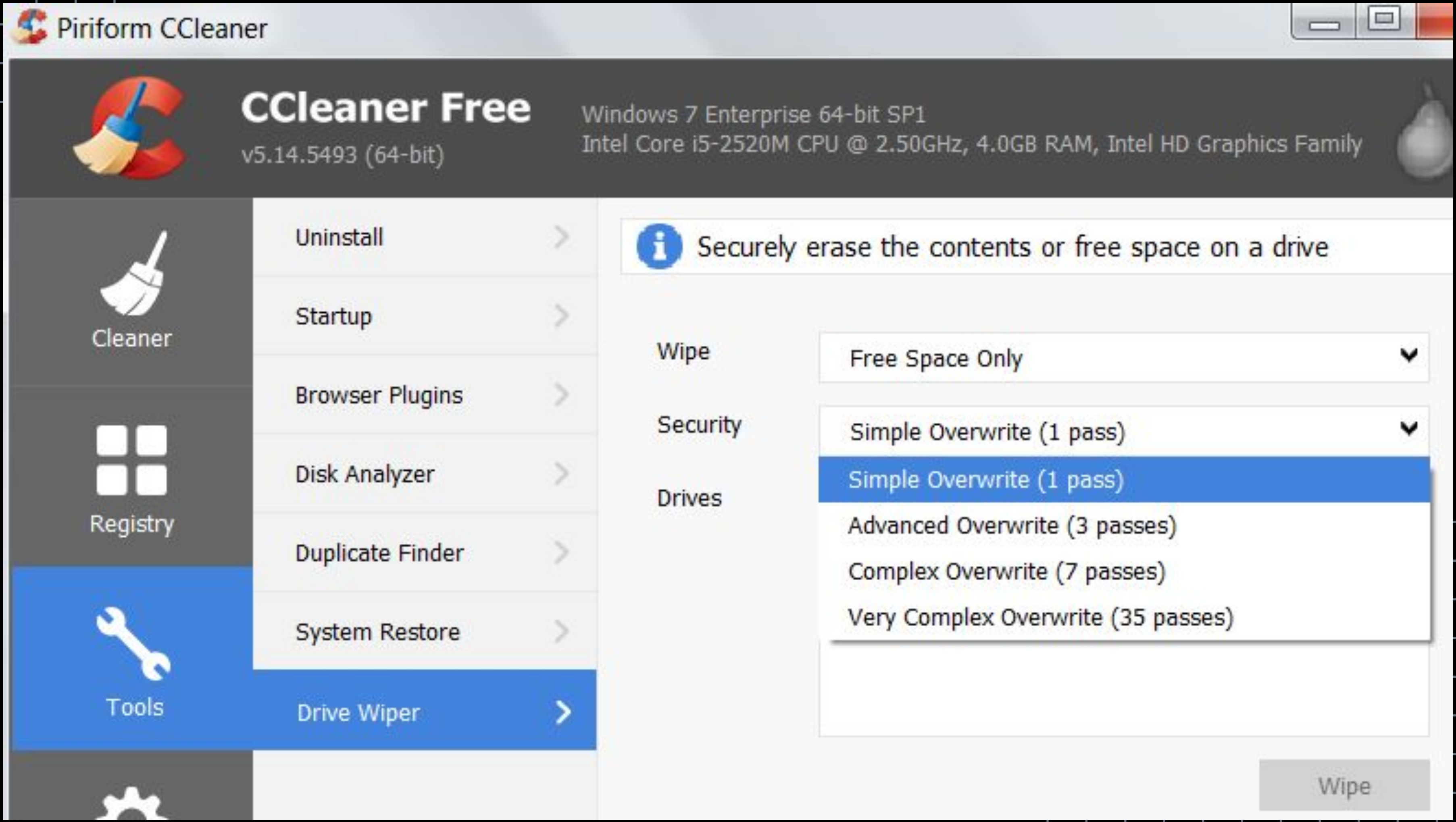
□ Javascript Renaming — Status: Not Set

Bulk Rename Utility is **free for personal, non-commercial, home use**. For use in a commercial environment, a commercial license is required. **More Info**

85 Objects (85 Selected)

Data Deletion

Artifact Wiping



Piriform CCleaner

CCleaner Free
v5.14.5493 (64-bit)

Windows 7 Enterprise 64-bit SP1
Intel Core i5-2520M CPU @ 2.50GHz, 4.0GB RAM, Intel HD Graphics Family

Securely erase the contents or free space on a drive

Wipe: Free Space Only

Security: Simple Overwrite (1 pass)

Drives

Cleaner
Registry
Tools
Uninstall
Startup
Browser Plugins
Disk Analyzer
Duplicate Finder
System Restore
Drive Wiper
Simple Overwrite (1 pass)
Advanced Overwrite (3 passes)
Complex Overwrite (7 passes)
Very Complex Overwrite (35 passes)
Wipe

Physical Destruction

- Degaussing
  - Generates a magnetic field
  - Good for large storage media and quick sanitization
  - Only for magnetic media
  - Too expensive for average users
- Destruction
  - Disintegration, pulverization, melting, incineration
  - Shredding, sanding, acid bath

Conclusions

- Digital forensics is still very much in its infancy and the approaches and techniques currently used are being compromised
- Anti forensics is an extremely concerning area of development that questions the integrity of evidence found – leading to anti-anti-forensics – an understanding of what these anti-forensic tools do