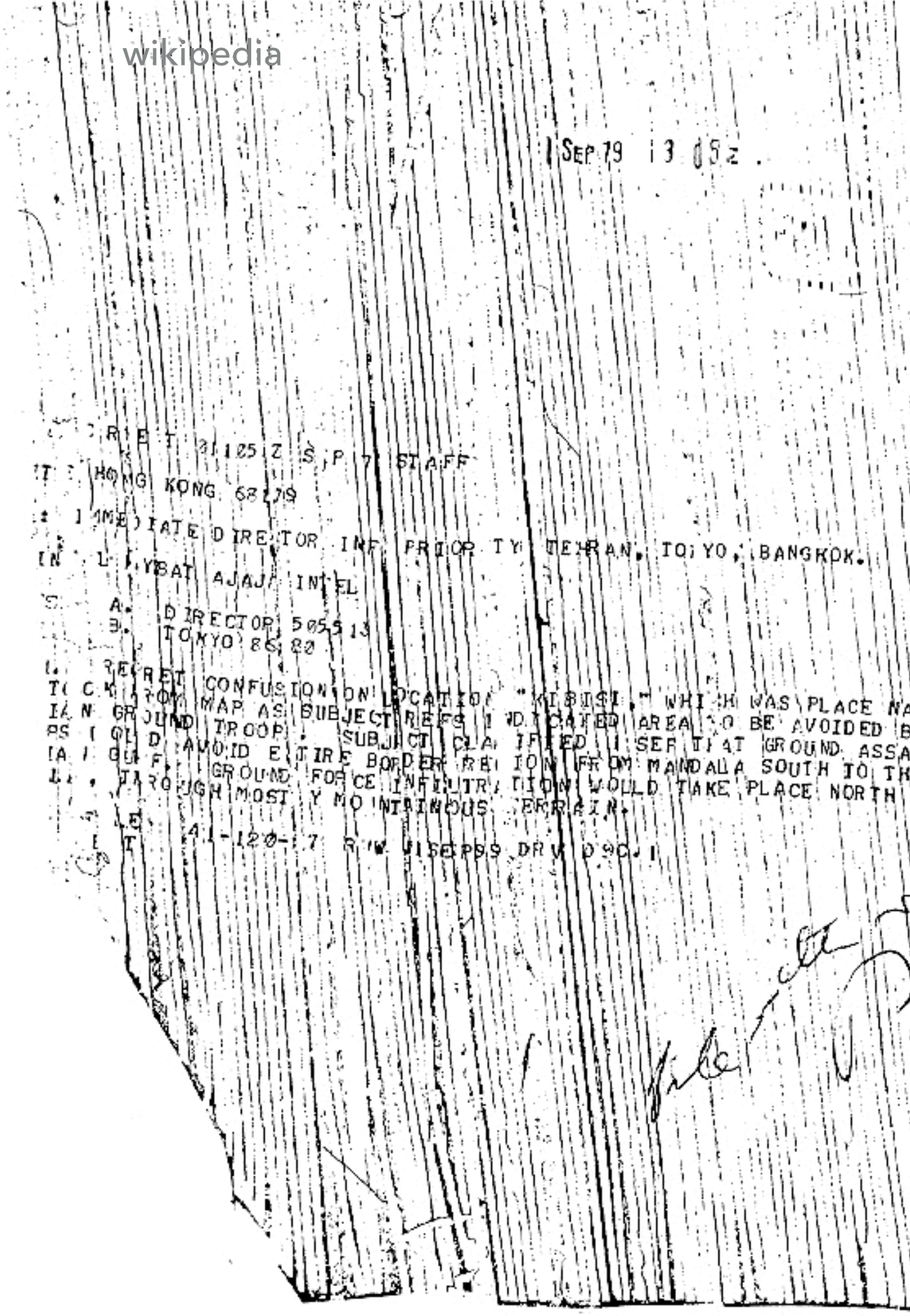
DIGITAL FORENSICS

Kunwadee Sripanidkulchai, Ph.D.

kunwadee (AT) cp.eng.chula.ac.th

HOW EVIDENCE GETS DESTROYED

kunwadee (AT) cp



WHAT IS DIGITAL FORENSICS

- We define computer forensics as the discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law. [US-Cert]

- Consists of
  - Networks (Network Forensics)
  - Small Scale Digital Devices
  - Storage Media (Computer forensics)
  - Code Analysis

CAN DIGITAL EVIDENCE BE DESTROYED?

Digital Detectives (2011) - Documentary on Computer Forensics in the DoD

https://www.youtube.com/watch?v=QKebBYsaMgU

FORENSICS PROCESS

- Acquisition or imaging of exhibits
  - Using dd, dc3dd, FTK Imager, etc.
  - Created, hashed, and write-blocked to prevent changes
- Analysis
  - Visible content such as folders on the desktop and images in user files
  - Hidden, encrypted, or deleted files
- Reporting

CASE STUDY

IMAGE TAMPERING

NIST Colloquium Series: Digital Forensics

by Dr. Hany Farid

https://www.youtube.com/watch?v=9DKJ6gP5lJY

kunwadee (AT) cp.eng.chula.ac.th


SPECULARITY
NIST


NIST

HMMM?

This is a ***retouched picture***, which means that it has been digitally altered from its original version. Modifications made by Mmxx.

kunwadee (AT) cp.eng.chula.ac.th

thispersondoesnotexist.com

DEEP FAKES AND GANS

https://www.youtube.com/watch?v=s_mWRJJHdKI


fake
real


baseline
N = 315
d' = -0.09
β = 0.99
count
0
20
40
60
80
0
20
40
60
80
100
percent correct

HMMM...

MELISSA VIRUS (1999)

Path: newsflash!news-peer1.tiac.net!news-feed1.tiac.net!newshub.
northeast.verio.net!
cpk-news-hub1.bbnplanet.com!news.gtei.net!newsfeed.cwix.com!152.163.199.19!
portc03.blue.aol.com!audrey01.news.aol.com!not-for-mail
From: skyr...@aol.com (Sky Roket)
Newsgroups: alt.sex
Subject: Passcode List 3-26-99
Lines: 283
NNTP-Posting-Host: ladder05.news.aol.com
X-Admin: ne...@aol.com
Date: 26 Mar 1999 12:15:53 GMT
Organization: AOL http://www.aol.com
Message-ID: <19990326071553.24526.00000525@ng-cg1.aol.com>
Xref: newsflash alt.sex:1680745

_=_
_=_ Part 001 of 001 of file list.zip
_=_

This message contains a zip file with the now famous list.doc
file in it. The file is infected with the Melissa virus.

- Source: https://groups.google.com/forum/#!topic/alt.comp.virus/9dnXxxxvtUA

MELISSA VIRUS (1999)

I did some "dumpster diving" in the list.doc file and found the following revision log in the file:

```
3360:07 00 FF FF 06 00 00 00  0B 00 4A 00 6F 00 68 00   ........|..J.o.h.
3370:6E 00 20 00 48 00 6F 00  6C 00 6D 00 65 00 73 00   n. .H.o.|l.m.e.s.
3380:19 00 43 00 3A 00 5C 00  57 00 49 00 4E 00 44 00   ..C.:.\.|W.I.N.D.
3390:4F 00 57 00 53 00 5C 00  44 00 65 00 73 00 6B 00   O.W.S.\.|D.e.s.k.
33A0:74 00 6F 00 70 00 5C 00  50 00 30 00 2E 00 64 00   t.o.p.\.|P.0...d.
33B0:6F 00 63 00 0B 00 4A 00  6F 00 68 00 6E 00 20 00   o.c...J.|o.h.n. .
33C0:48 00 6F 00 6C 00 6D 00  65 00 73 00 1F 00 43 00   H.o.l.m.|e.s...C.
33D0:3A 00 5C 00 57 00 49 00  4E 00 44 00 4F 00 57 00   :.\.W.I.|N.D.O.W.
33E0:53 00 5C 00 44 00 65 00  73 00 6B 00 74 00 6F 00   S.\.D.e.|s.k.t.o.
33F0:70 00 5C 00 4C 00 69 00  73 00 74 00 30 00 38 00   p.\.L.i.|s.t.0.8.
3400:31 00 39 00 2E 00 64 00  6F 00 63 00 03 00 48 00   1.9...d.|o.c...H.
3410:69 00 6D 00 1B 00 43 00  3A 00 5C 00 57 00 49 00   i.m...C.|:.\.W.I.
3420:4E 00 44 00 4F 00 57 00  53 00 5C 00 44 00 65 00   N.D.O.W.|S.\.D.e.
3430:73 00 6B 00 74 00 6F 00  70 00 5C 00 6C 00 69 00   s.k.t.o.|p.\.l.i.
3440:73 00 74 00 2E 00 64 00  6F 00 63 00 FF 40 01 80   s.t...d.|o.c..@..
```

- https://groups.google.com/forum/#!topic/alt.comp.virus/9dnXxxxvtUA

MELISSA VIRUS (1999)

Also I found this GUID in the file:

```
4BC0:5F 50 49 44 5F 47 55 49  44 00 02 00 00 00 E4 04   _PID_GUI|D.......
4BD0:00 00 41 00 00 00 4E 00  00 00 7B 00 35 00 37 00   ..A...N.|..{.5.7.
4BE0:32 00 38 00 35 00 38 00  45 00 41 00 2D 00 33 00   2.8.5.8.|E.A.-.3.
4BF0:36 00 44 00 44 00 2D 00  31 00 31 00 44 00 32 00   6.D.D.-.|1.1.D.2.
4C00:2D 00 38 00 38 00 35 00  46 00 2D 00 30 00 30 00   -.8.8.5.|F.-.0.0.
4C10:34 00 30 00 33 00 33 00  45 00 30 00 30 00 37 00   4.0.3.3.|E.0.0.7.
4C20:38 00 45 00 7D 00 00 00  00 00 00 00 00 00 00 00   8.E.}...|........
```

[redacted]

```
8230:47 00 7B 00 33 00 44 00  34 00 35 00 39 00 39 00   G.{.3.D.|4.5.9.9.
8240:36 00 32 00 2D 00 45 00  31 00 42 00 34 00 2D 00   6.2.-.E.|1.B.4.-.
8250:31 00 31 00 44 00 32 00  2D 00 39 00 45 00 42 00   1.1.D.2.|-.9.E.B.
8260:41 00 2D 00 30 00 30 00  34 00 30 00 33 00 33 00   A.-.0.0.|4.0.3.3.
8270:45 00 30 00 30 00 37 00  38 00 45 00 7D 00 23 00   E.0.0.7.|8.E.}.#.
```

[redacted]

- https://groups.google.com/forum/#!topic/alt.comp.virus/9dnXxxxvtUA

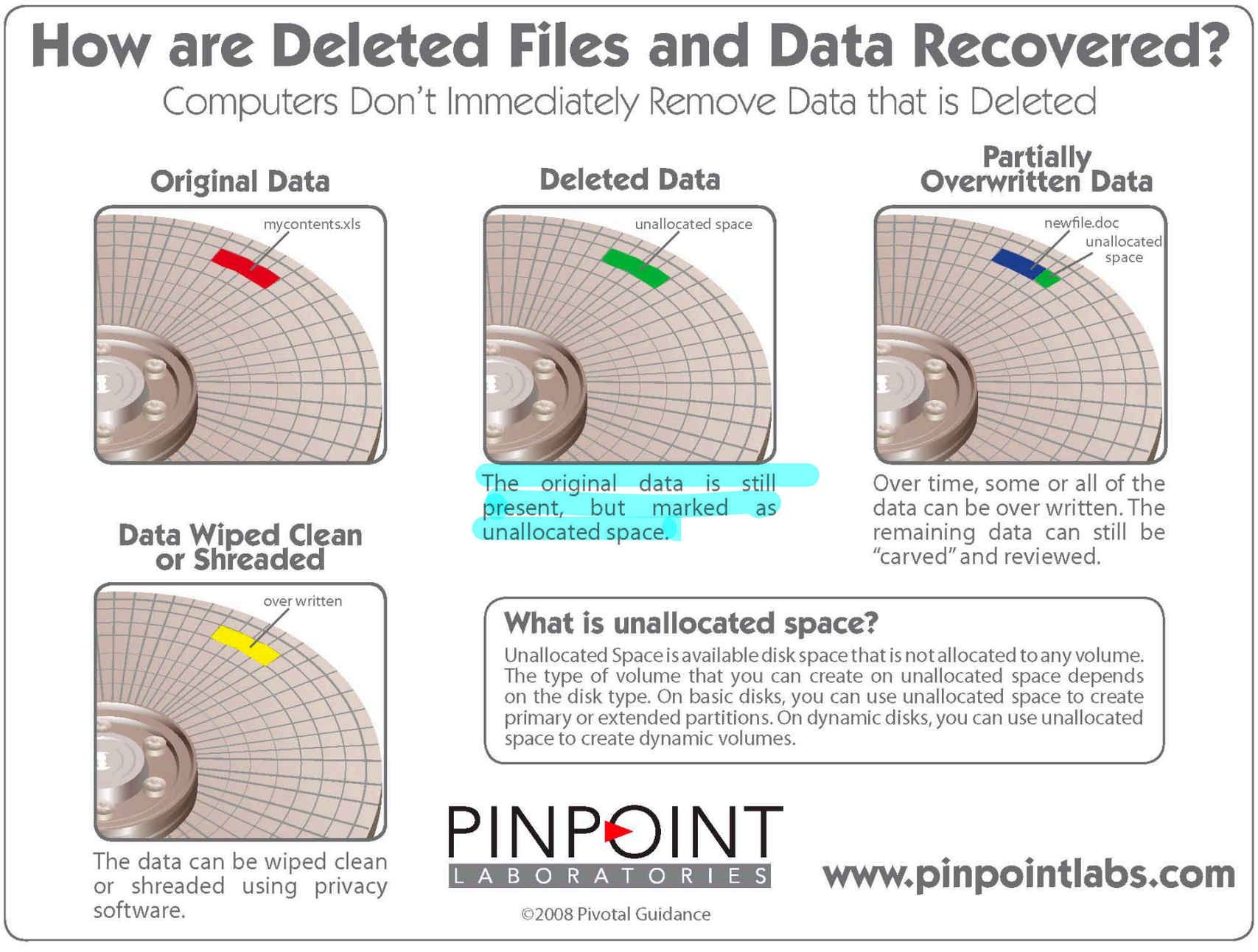
DATA HIDING: CHANGING OR MANIPULATING A FILE TO CONCEAL INFORMATION

kunwadee (AT) cp.eng.chula.ac.th

DEALING WITH DELETED FILES

File Carving แกะสลัก

- Reassemble fragments of files scattered across the file system



DATA HIDING: CHANGING OR MANIPULATING A FILE TO CONCEAL INFORMATION

- Changing file names and file extensions
- Setting file attributes to hidden
- Hiding entire partitions
- Bit-shifting
- Using encryption/password protection

kunwadee (AT) cp.eng.chula.ac.th

Modified from: Guide to Computer Forensics and Investigations, Fifth Edition, Engage Learning, 2015.

HIDING FILES BY USING THE OS

- One of the first techniques to hide data:
  - Changing file extensions
- Advanced digital forensics tools check file headers
  - Compare the file extension to verify that it's correct
  - If there's a discrepancy, the tool flags the file as a possible altered file
- Another hiding technique
  - Selecting the Hidden attribute in a file's Properties dialog box

HIDING PARTITIONS

- By using the Windows `diskpart remove letter` command
  - You can unassign the partition's letter, which hides it from view in File Explorer
- To unhide, use the `diskpart assign letter` command
- Other disk management tools:
  - Partition Magic, Partition Master, and Linux Grand Unified Bootloader (GRUB)

TO DETECT WHETHER A PARTITION HAS BEEN HIDDEN

- Account for all disk space when examining an evidence drive
- Analyze any disk areas containing space you can't account for

kunwadee (AT) cp.eng.chula.ac.th

afry - Autopsy 4.12.0

Case View Tools Window Help

Add Data Source | Images/Videos | Communications | Timeline | Close Case | Generate Report

Data Sources
- PhysicalDrive0
  - vol1 (Unallocated: 0-2047)
  - vol4 (Basic data partition: 2048-2099199)
  - vol5 (Basic data partition: 2099200-2631679)
  - vol6 (Basic data partition: 2631680-2893823)
  - vol7 (Basic data partition: 2893824-1233700863)
  - vol8 (Unknown: 1233700864-1426098175)
    - $OrphanFiles (100171)
    - $Unalloc (30)
    - bin (199)
    - boot (57)
    - cdrom (2)
    - dev (91)
    - etc (321)
    - home (3)
    - lib (31)
    - lib64 (5)
    - lost+found (2)
    - media (3)
    - mnt (2)
    - opt (5)
    - proc (2)
    - root (8)
    - run (16)
    - sbin (358)
    - snap (4)

Listing

/img_PhysicalDrive0/vol_vol8

Table | Thumbnail

Page: Pages: Go to Page:

Name	S	C	Location	Modified Time
$OrphanFiles			/img_PhysicalDrive0/vol_vol8//$OrphanFiles	0000-00-00 00:00:0
initrd.img				2018-01-18 08:43:5
initrd.img.old				2017-12-08 11:58:2
vmlinuz				2018-01-18 08:43:5
vmlinuz.20750				2017-12-08 11:58:2
vmlinuz.old				2017-12-08 11:58:2
$Unalloc			/img_PhysicalDrive0/vol_vol8//$Unalloc	0000-00-00 00:00:0
[current folder]				2019-07-29 15:20:5
[parent folder]				2019-07-29 15:20:5
bin				2019-07-31 06:52:5
boot				2019-07-31 06:57:3
cdrom				2017-04-12 12:23:5
dev				2017-02-15 15:36:3

Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

kunwadee (AT) cp.eng.chula.ac.th

Source: https://sleuthkit.discourse.group/

MARKING BAD CLUSTERS

- A data-hiding technique used in FAT file systems is placing sensitive or incriminating data in free or slack space on disk partition clusters
  - Involves using old utilities such as Norton DiskEdit
- Can mark good clusters as bad clusters in the FAT table so the OS considers them unusable
  - Only way they can be accessed from the OS is by changing them to good clusters with a disk editor
- DiskEdit runs only in MS-DOS and can access only FAT-formatted disk media

BIT-SHIFTING

- Some users use a low-level encryption program that changes the order of binary data
  - Makes altered data unreadable To secure a file, users run an assembler program (also called a “macro”) to scramble bits
  - Run another program to restore the scrambled bits to their original order
- Bit shifting changes data from readable code to data that looks like binary executable code

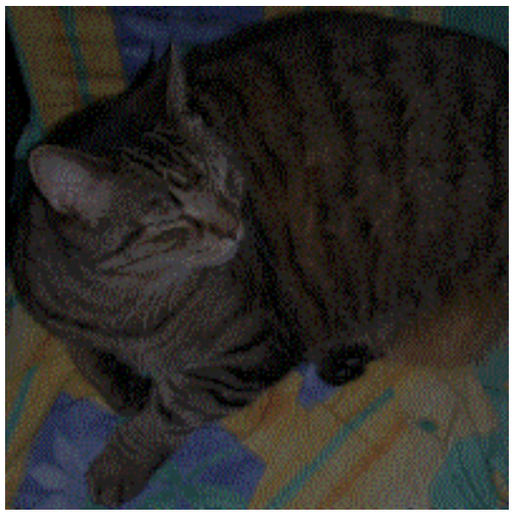
UNDERSTANDING STEGANALYSIS METHODS

- Steganography - comes from the Greek word for “hidden writing”
  - Hiding messages in such a way that only the intended recipient knows the message is there
- Steganalysis - term for detecting and analyzing steganography files
- Digital watermarking - developed as a way to protect file ownership
  - Usually not visible when used for steganography

UNDERSTANDING STEGANALYSIS METHODS

- A way to hide data is to use steganography tools
  - Many are freeware or shareware
  - Insert information into a variety of files
- If you encrypt a plaintext file with PGP and insert the encrypted text into a steganography file
  - Cracking the encrypted message is extremely difficult

Removing all but the two least significant bits of each color component and a subsequent normalization. https://en.wikipedia.org/wiki/Steganography



kunwadee (AT) cp.eng.chula.ac.th

EXAMINING ENCRYPTED FILES

- To decode an encrypted file
  - Users supply a password or passphrase
- Many encryption programs use a technology called “key escrow”
  - Designed to recover encrypted data if users forget their passphrases or if the user key is corrupted after a system failure
- Key sizes of 128 bits to 4096 bits make breaking them nearly impossible with current technology

RECOVERING PASSWORDS

- Password-cracking tools are available for handling password-protected data or systems
  - Some are integrated into digital forensics tools
- Stand-alone tools:
  - Last Bit
  - AccessData PRTK
  - ophcrack
  - John the Ripper
  - Passware

RECOVERING PASSWORDS

- Brute-force attacks
  - Use every possible letter, number, and character found on a keyboard
  - This method can require a lot of time and processing power
- Dictionary attack
  - Uses common words found in the dictionary and tries them as passwords
  - Most use a variety of languages

RECOVERING PASSWORDS

- With many programs, you can build profiles of a suspect to help determine his or her password
- Many password-protected OSs and application store passwords in the form of hash values
- A brute-force attack requires converting a dictionary password from plaintext to a hash value
  - Requires additional CPU cycle time

RECOVERING PASSWORDS

- Rainbow table
  - A file containing the hash values for every possible password that can be generated from a computer's keyboard
  - No conversion necessary, so it is faster than a brute-force or dictionary attack
- Salting passwords
  - Alters hash values and makes cracking passwords more difficult

ACTIVITY

Graphical Timeline of the Data Leakage Scenario