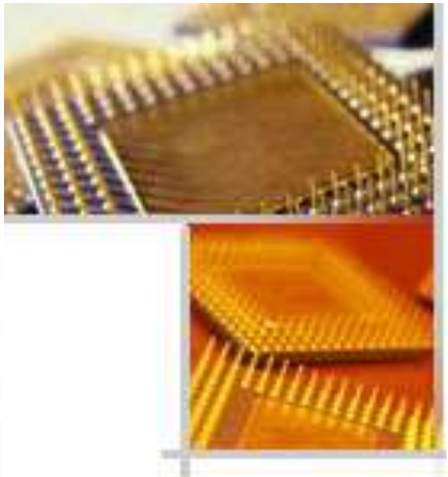
COMP 7903 Digital Investigation and Forensics

Case Study 1: Time stamps

Ao SHEN
The University of Hong Kong



Case 1

Virus Attack

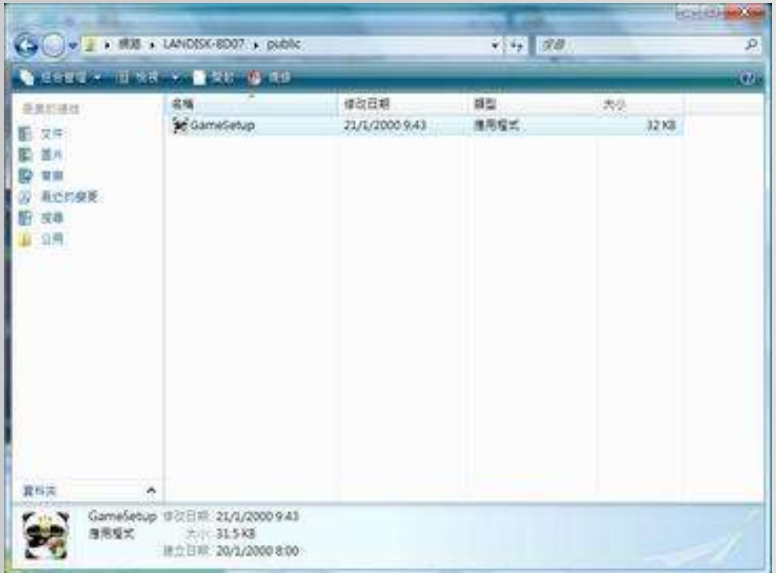
Case: Panda Burning Incense Virus (熊猫烧香) in 2007

In March 2012, Mainland China has amended its Criminal Procedure Law, which includes the introduction of a new type of evidence, i.e., digital evidence, to the court of law.

The famous “Panda Burning Incense (Worm.WhBoy.cw)” virus case that happened in 2007.

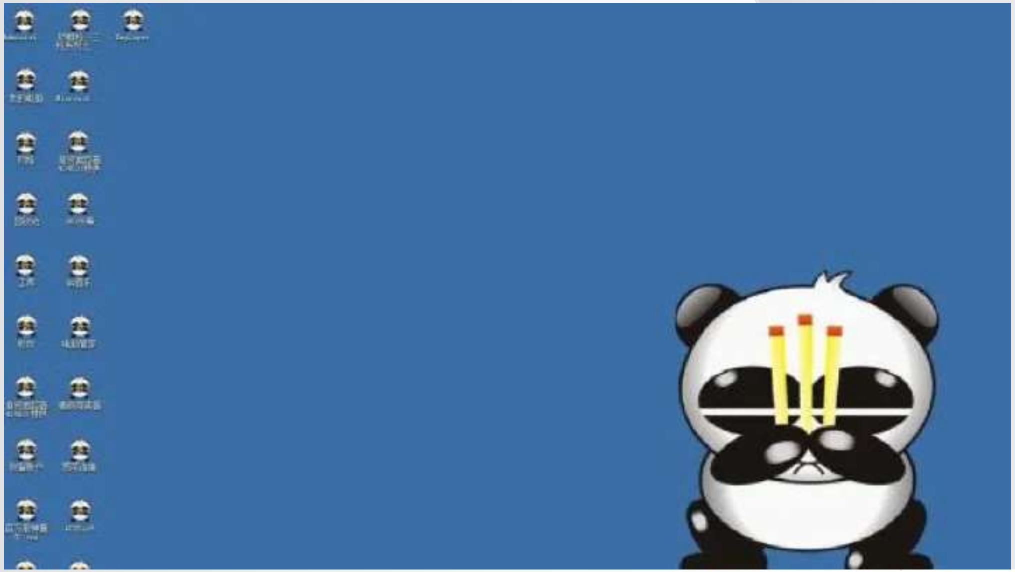
Case: Panda Burning Incense Virus (熊猫烧香) in 2007

It infected executable files on a PC. When infected, the icon of the executable file changes to an image of a panda holding three sticks of incense. The arrests were the first for virus writing in China.



名稱	修改日期	類型	大小
GameSetup	21/1/2000 9:43	應用程式	32 KB

GameSetup 修改日期: 21/1/2000 9:43
應用程式 大小: 31.5 KB
建立日期: 20/1/2000 8:00



Case: Panda Burning Incense Virus (熊猫烧香) in 2007

Establish a timer, generates setup.exe (the virus itself) autorun.inf in the root directory of the disk with a period of 6 seconds

Can infect exe, com, pif, src, html, asp and other files in the system

Stop a large number of anti-virus software processes

Delete .gho files

Forensic investigation

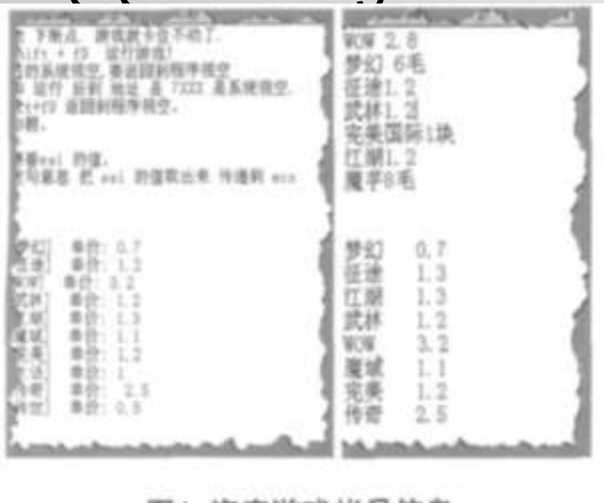
Extent of Breach: The scale of the attack affected a vast number of websites and servers across China, leading to a widespread investigation.

Digital Forensic Response: Digital forensic experts were engaged to analyze the attack vectors, identify the malware used, and trace the origins of the attack.

Forensic investigation

Evidence:

- Tools: Delphi7, Vmware, …
- Browser Favorites: Hacker discussion forums, websites of Virus techniques
- Hard disk: nc.exe, Sniffer, DDOS.EXE, Web3389.exe, ..., different versions of the virus source code
- QQ message: Screenshots of hacking activities, other customers
- and recorded bills



注：下断点，游戏就卡住不动了。
Alt + F5 运行游戏!
的系统领空，看返回到程序领空
按 运行 后到 地址 是 7XXX 是系统领空。
Ctrl+F9 返回到程序领空。
ret。

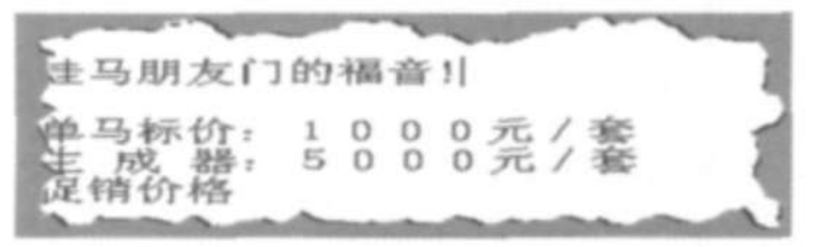
查看eax 的值。
写句菜单 把 eax 的值取出来 传递到 ecx

梦幻 单价：0.7
征途 单价：1.3
WOW 单价：3.2
武林 单价：1.2
江湖 单价：1.3
魔域 单价：1.1
完美 单价：1.2
大话 单价：1
传奇 单价：2.5
神泣 单价：0.5

WOW 2.8
梦幻 6毛
征途1.2
武林1.2
完美国际1块
江湖1.2
魔域8毛

梦幻 0.7
征途 1.3
江湖 1.3
武林 1.2
WOW 3.2
魔域 1.1
完美 1.2
传奇 2.5

图1 盗卖游戏帐号信息



挂马朋友门的福音!!

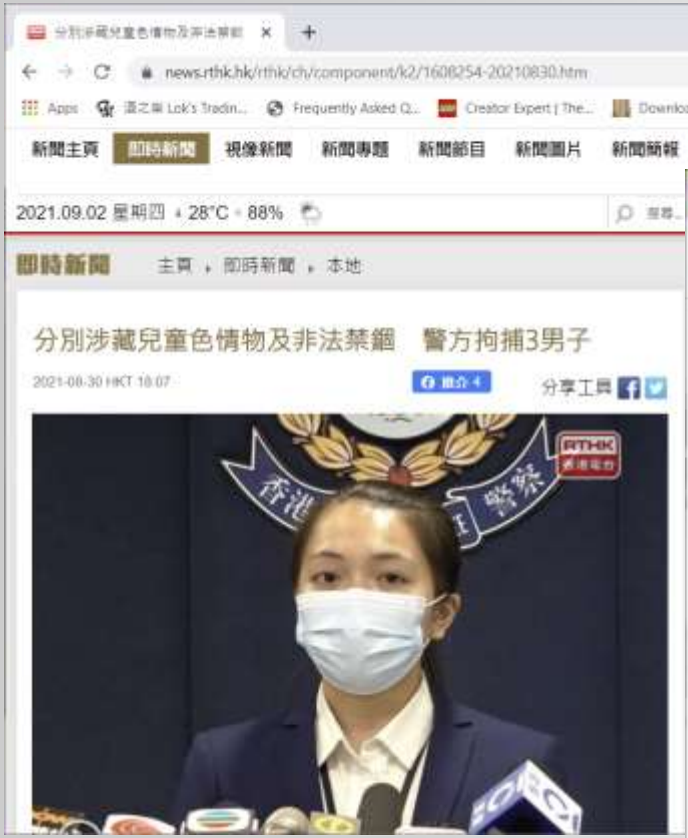
单马标价：１０００元／套
生成器：５０００元／套
促销价格

图2 “熊猫烧香”广告

Case 2

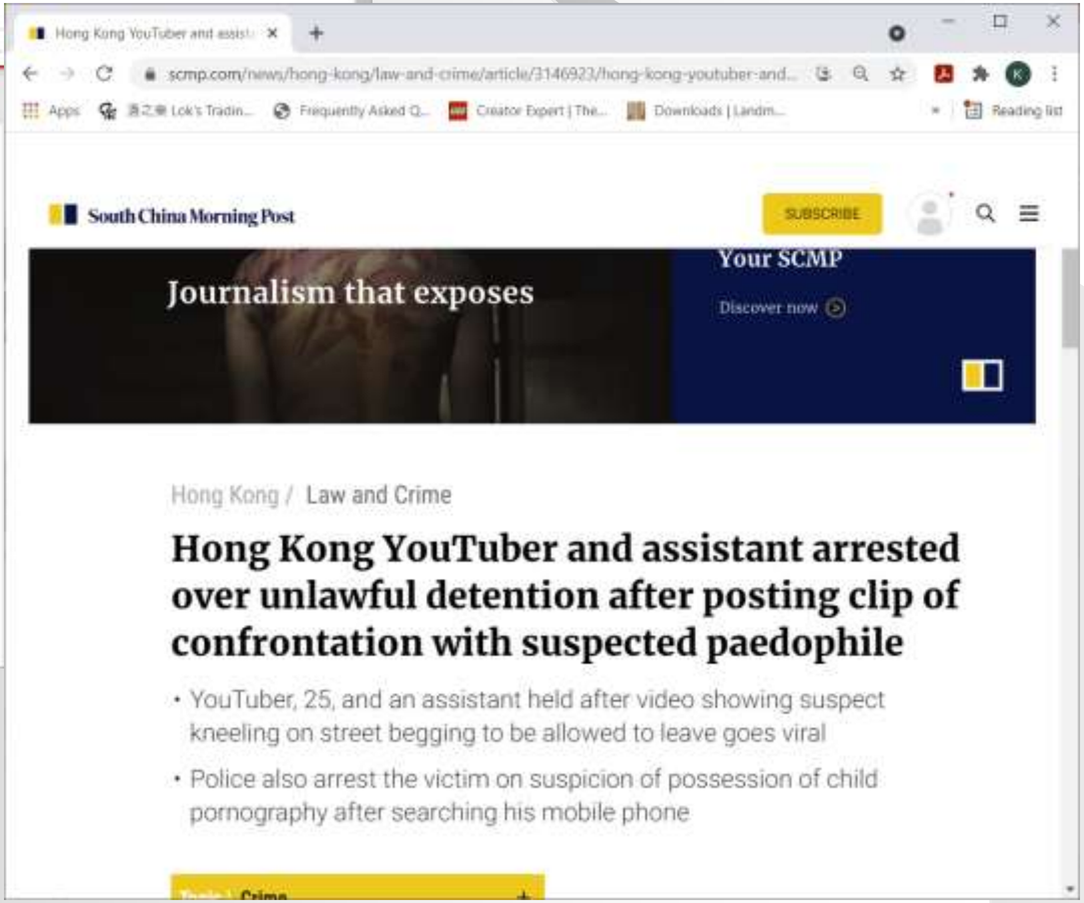
Child Pornography Case

A case in Aug 2021



分別涉藏兒童色情物及非法禁錮　警方拘捕3男子

2021-08-30 HKT 18:07



Hong Kong / Law and Crime

Hong Kong YouTuber and assistant arrested over unlawful detention after posting clip of confrontation with suspected paedophile

- YouTuber, 25, and an assistant held after video showing suspect kneeling on street begging to be allowed to leave goes viral
- Police also arrest the victim on suspicion of possession of child pornography after searching his mobile phone

Hong Kong YouTuber and assist
scmp.com/news/hong-kong/law-and-crime/article/3146923/hong-kong-youtuber-and...
South China Morning Post
SUBSCRIBE
Journalism that exposes
Your SCMP
Discover now
Topic | Crime

Prevention of Child Pornography in HK

Prevention of Child Pornography Ordinance – Sect 3

1) Any person who prints, makes, produces, reproduces, copies, imports or exports any child pornography commits an offense and is liable –

   a) On conviction on indictment to a fine of $2000000 and to imprisonment for 8 years; or

   b) On summary conviction to a fine of $1000000 and to imprisonment for 3 years.

   …

2) Any person who publishes any child pornography commits an offense and is liable –

   …

3) Any person who has in possession any child pornography commits an offense and is liable –

   …

Prevention of Child Pornography in HK

Prevention of Child Pornography Ordinance – Sect 3

4) Any person publishes or causes to be published any advertisement that conveys or is likely to be understood as conveying the message that any person has published, publishes or intends to publish any child pornography commits an offense and is liable –

a) On conviction on indictment to a fine of $2000000 and to imprisonment for 8 years; or

b) On summary conviction to a fine of $1000000 and to imprisonment for 3 years.

…

Prevention of Child Pornography in HK

1) prints, makes, produces, reproduces, copies, imports or exports any child pornography
2) publishes any child pornography
3) in possession any child pornography
4) publishes or causes to be published any advertisement that conveys or is likely to be understood as conveying the message that any person has published, publishes or intends to publish any child pornography

What is child pornography?

Definition of Child Pornography in HK

"child pornography" (兒童色情物品) means—

- a photograph, film, computer-generated image or other visual depiction that is a pornographic depiction of a person who is or is depicted as being a child, whether it is made or generated by electronic or any other means, whether or not it is a depiction of a real person and whether or not it has been modified; or
- anything that incorporates a photograph, film, image or depiction referred to in paragraph (a), and includes data stored in a form that is capable of conversion into a photograph, film, image or depiction referred to in paragraph (a) and anything containing such data;

"child" means a person under the age of 16;

Hong Kong Cases

Some accused in the past only fined or received suspended sentences

In 2008, appeal judges have issued new guidelines for dealing with people who possess child pornography

- Images of child pornography are classified into 4 levels
- Those found with <20 pictures under “Level 1” could be given a community service order
- Those found with “Level 4” images could be in jail for 1-3 years

What is Level 4?

Suggested Canadian System for Classifying Child Pornography

Level	Description
1	Non erotic, non sexualized material including nudity
2	Material where the dominant characteristic demonstrates a sexual purpose
3	Explicit sexual activity and assaults between adult-child, child-child
4	Gross assaults, penetrative assaults involving adults
5	Sadistic images

Level 4

Is it too harsh?

Appeal judges Geoffrey Ma Tao-li, Michael Stuart-Moore and Frank Stock:

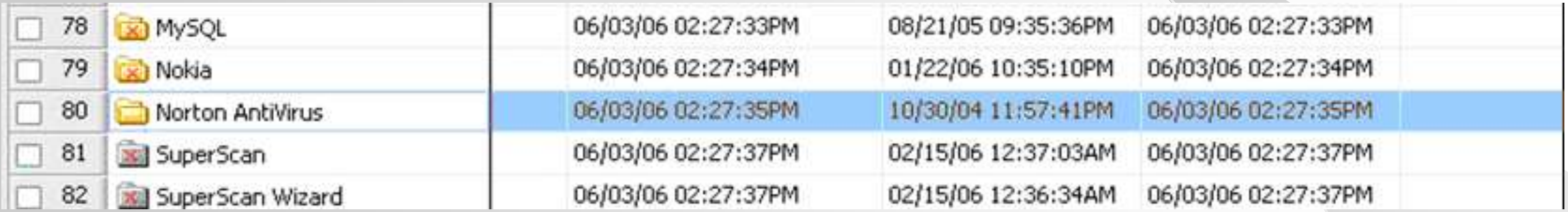
“Some may argue that in the end, the only people harmed are those who possess this sort of material in the privacy of their home, this is much too narrow a view. The courts are obliged to take into account boarder considerations, the main one here being the **protection of vulnerable children**.”

“A lots of people are still ignorant about the law and are not aware they are breaching it by sending such photos to friends or posting them online.” Priscilla Lui, Against Child Abuse director

What is the role of digital forensics?

Data Recovery

Recover deleted child pornography photos

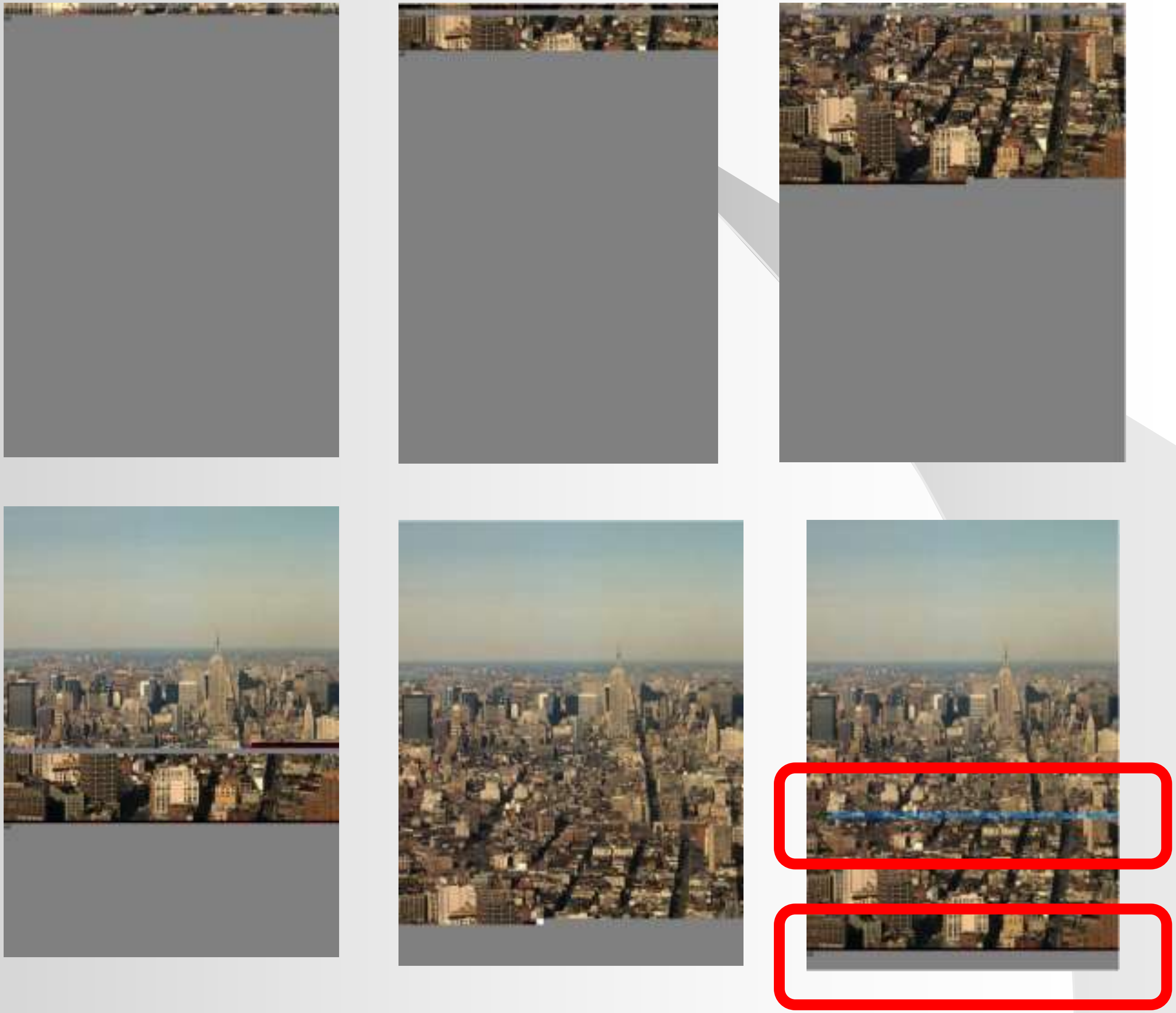


□	78	MySQL		06/03/06 02:27:33PM	08/21/05 09:35:36PM	06/03/06 02:27:33PM
□	79	Nokia		06/03/06 02:27:34PM	01/22/06 10:35:10PM	06/03/06 02:27:34PM
□	80	Norton AntiVirus		06/03/06 02:27:35PM	10/30/04 11:57:41PM	06/03/06 02:27:35PM
□	81	SuperScan		06/03/06 02:27:37PM	02/15/06 12:37:03AM	06/03/06 02:27:37PM
□	82	SuperScan Wizard		06/03/06 02:27:37PM	02/15/06 12:36:34AM	06/03/06 02:27:37PM

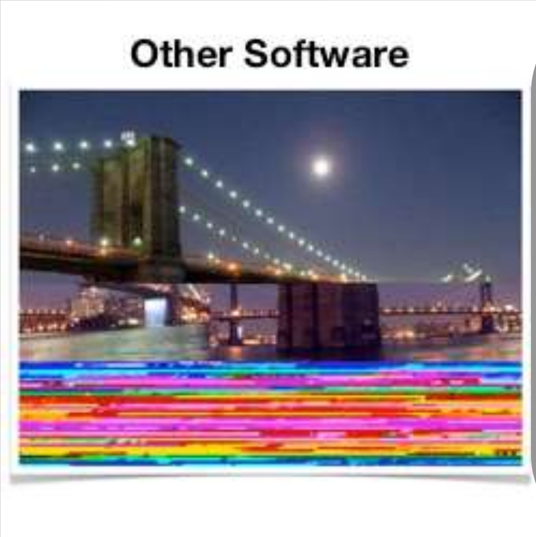
How about files that were broken up into several fragments?

Image Carving

original image (deleted already)



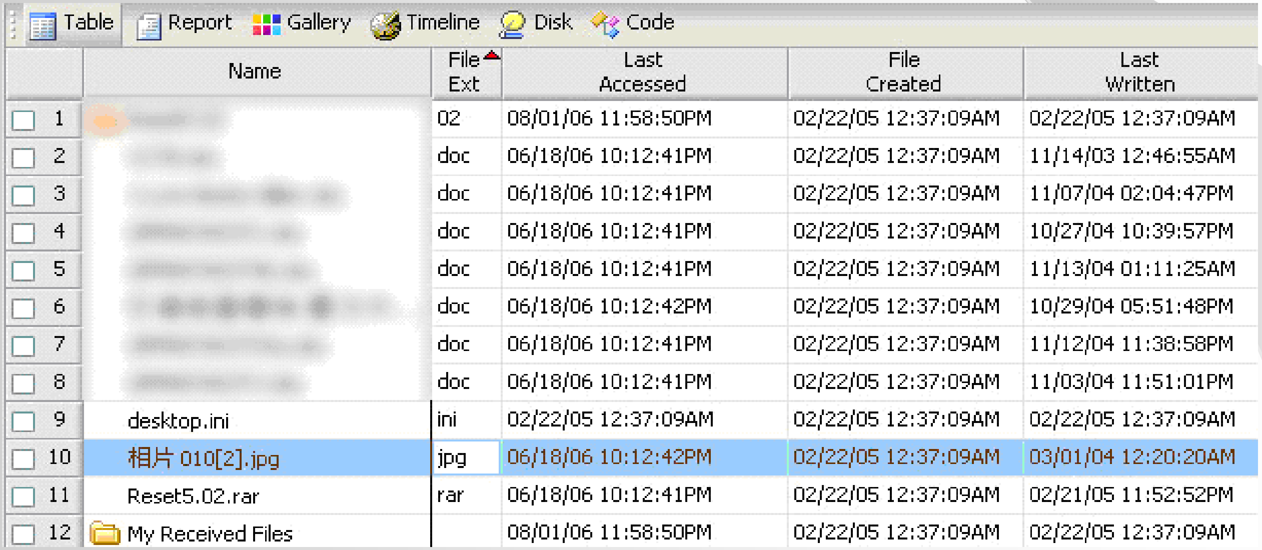
Smart Carving (Memon's Adroit)



Data in another fragment

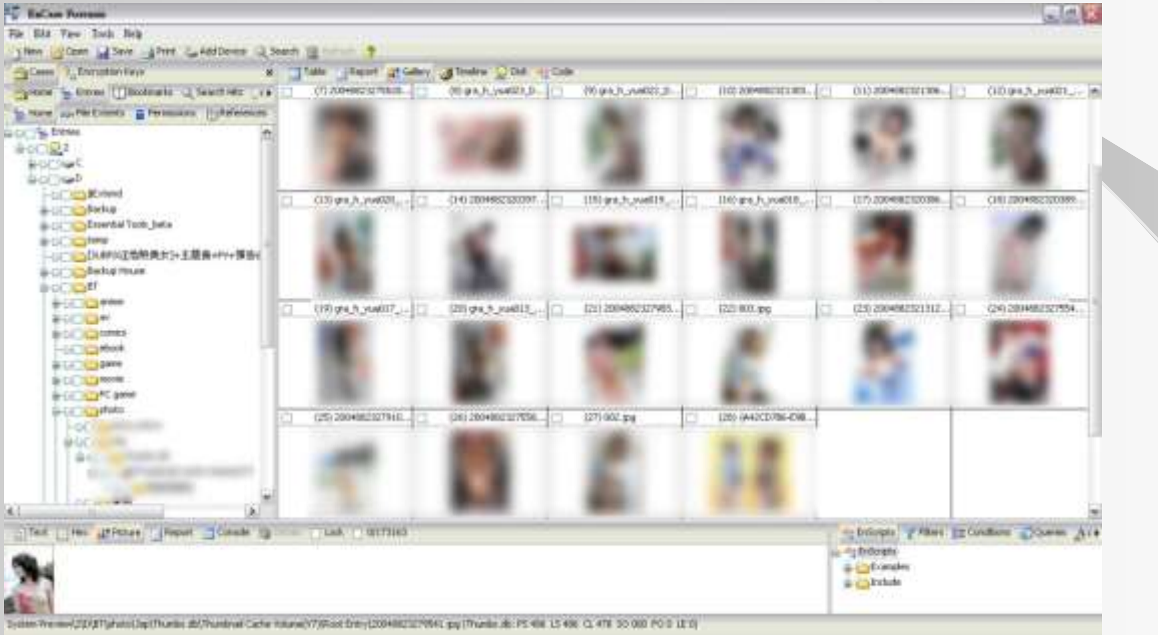
Event Reconstruction

It was found a child porn photo was copied to the current location on 22 Feb 2005



	Name	File Ext	Last Accessed	File Created	Last Written
□ 1	[redacted]	02	08/01/06 11:58:50PM	02/22/05 12:37:09AM	02/22/05 12:37:09AM
□ 2	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/14/03 12:46:55AM
□ 3	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/07/04 02:04:47PM
□ 4	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	10/27/04 10:39:57PM
□ 5	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/13/04 01:11:25AM
□ 6	[redacted]	doc	06/18/06 10:12:42PM	02/22/05 12:37:09AM	10/29/04 05:51:48PM
□ 7	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/12/04 11:38:58PM
□ 8	[redacted]	doc	06/18/06 10:12:41PM	02/22/05 12:37:09AM	11/03/04 11:51:01PM
□ 9	desktop.ini	ini	02/22/05 12:37:09AM	02/22/05 12:37:09AM	02/22/05 12:37:09AM
□ 10	相片 010[2].jpg	jpg	06/18/06 10:12:42PM	02/22/05 12:37:09AM	03/01/04 12:20:20AM
□ 11	Reset5.02.rar	rar	06/18/06 10:12:41PM	02/22/05 12:37:09AM	02/21/05 11:52:52PM
□ 12	My Received Files		08/01/06 11:58:50PM	02/22/05 12:37:09AM	02/22/05 12:37:09AM

Crime Scene Reconstruction


EnCase Forensic
File Edit View Tools Help
New Open Save Print Add Device Search
Cases Encryption Keys
Home Entries Bookmarks Search Hits
Home File Extents Permissions References
Table Report Gallery Timeline Disk Code
Entries
Backup
Essential Tools_beta
temp
Backup House
comics
ebook
game
movie
PC game
photo
Text Hex Picture Report Console Lock
EnScripts Filters Conditions Queries
Examples
Include

The suspect downloaded a collection of child porn photos and videos from the Internet on 2 Jan 2004, and paid using credit card number 0000-1111-2222-3333, and the photos were then backup to an external media on 4 Aug 2009

Let's start with a case!

The Case

Based on the intelligence from the Interpol, the police identified the home address of the suspect

The police arrived at the suspect's premises, several PCs and hard disks were found in the premises

The police performed an initial examination and found 2 hard disks which contained child pornography

- In one of the hard disk, 1 child pornography video was found
- In another hard disk, 2 child pornography videos were found

The police brought the PCs and hard disks back to the computer forensics lab for further examination

Digital Evidence

After examinations, it was confirmed that child pornography (CP) videos were found in the 2 hard disks:

- Hard disk Disk-1: 2 CP videos were found
- Hard disk Disk-2: 1 CP video was found

Disk-1

Disk-1	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-16 21:22:22	2011-06-13 00:58:40	2011-06-13 00:58:40
Lolita-1.avi	156 MB	2011-06-26 21:01:35	2011-06-26 22:10:34	2012-07-14

What are C time, M time and A time?

C time: file creation time
M time: last modified time
A time: last access time
Together they are referred to as MAC time

Example with MAC times

File	File Size	Accessed Time	Modified Time	Created Time
video1.avi	20MB	20/4/2004 13:40	23/9/2003 09:31	23/9/2003 09:31
video2.avi	35MB	20/4/2004 13:40	23/9/2003 09:15	23/9/2003 09:15
video3.avi	13MB	20/4/2004 13:39	23/9/2003 08:55	23/9/2003 08:55

- Any observation?

Example with MAC Times

File	File Size	Accessed Time	Modified Time	Created Time
video4.avi	20MB	20/5/2004 13:40	23/7/2003 09:31	23/9/2003 09:31
video5.avi	35MB	20/5/2004 13:20	20/7/2003 09:15	23/9/2003 09:15
video6.avi	13MB	20/5/2004 13:15	20/7/2003 08:55	23/9/2003 08:55

- Why the “created time” is after the “modified time”?

Any other conclusion that we can draw about from the MAC times?

Disk-1 and Disk-2

Disk-1	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-16 21:22:22	2011-06-13 00:58:40	2011-06-13 00:58:40
Lolita-1.avi	156 MB	2011-06-26 21:01:35	2011-06-26 22:10:34	2012-07-14

Disk-2	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-12 23:15:41	2011-06-13 00:58:40	2011-06-12 23:15:41

The files Lolita-1.mpg in Disk-1 and Disk-2 are identical. The files Lolita-1.mpg and Lolita-1.avi in Disk-1 have the same content.

Questions

How to check if 2 files are identical?

How to check if 2 files have the same content?

What can you say about the 3 files?

Disk-2

Disk-2	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-12 23:15:41	2011-06-13 00:58:40	2011-06-12 23:15:41

File size: 101MB
Identical C time and A time
M time after C time and A time
What’s that mean?

The suspect claimed he was online on 12 Jun 2011 evening

Disk-1

Disk-1	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-16 21:22:22	2011-06-13 00:58:40	2011-06-13 00:58:40
Lolita-1.avi	156 MB	2011-06-26 21:01:35	2011-06-26 22:10:34	2012-07-14

Disk-2	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-12 23:15:41	2011-06-13 00:58:40	2011-06-12 23:15:41

The file Lolita-1.mpg in Disk-1 and Disk-2 are identical and their M time are the same.
In Disk-1, the C time is after the M time.
What can you say about the files?

Disk-1

Disk-1	Size	C time	M time	A time
Lolita-1.mpg	101 MB	2011-06-16 21:22:22	2011-06-13 00:58:40	2011-06-13 00:58:40
Lolita-1.avi	156 MB	2011-06-26 21:01:35	2011-06-26 22:10:34	2012-07-14

Lolita-1.mpg and Lolita-1.avi have the same content,
The M time of Lolita-1.avi is after the C time.
What’s that mean?

So, what can we say about the user?

The user of Disk-1 and Disk-2

1. At 2011-06-12 11:15PM, the user downloaded the child pornography video Lolita-1.mpg and the download was competed at 2011-06-13 00:58AM
2. At 2011-06-16 9:22PM, the user copied the file Lolita-1.mpg from Disk-2 to Disk-1
3. At 2011-06-26 9:01PM, the user converted the file Lolita-1.mpg to Lolita-1.avi and the conversion was completed at 2011-06-26 10:10PM

A question for you

Do you use WinZip, WinRar or 7zip?

When you copy an archive file (a.rar) from a disk (Disk-1) to another disk (Disk-2), what will be the MAC time of the copy (a.rar) in Disk-2?

When you extracted files from the archive (a.rar), what will be the MAC time of the extracted files?

M time of the copied file on Disk-2 will be updated to the time when the copying process occurred.
A time will remain unchanged (it depends).
C time will be the time when the file was created on Disk-2 as part of the copying operation.

Any legal defence for the CP case ?

Education, scientific or medical purposes, **artistic merit**, or when it serves the public

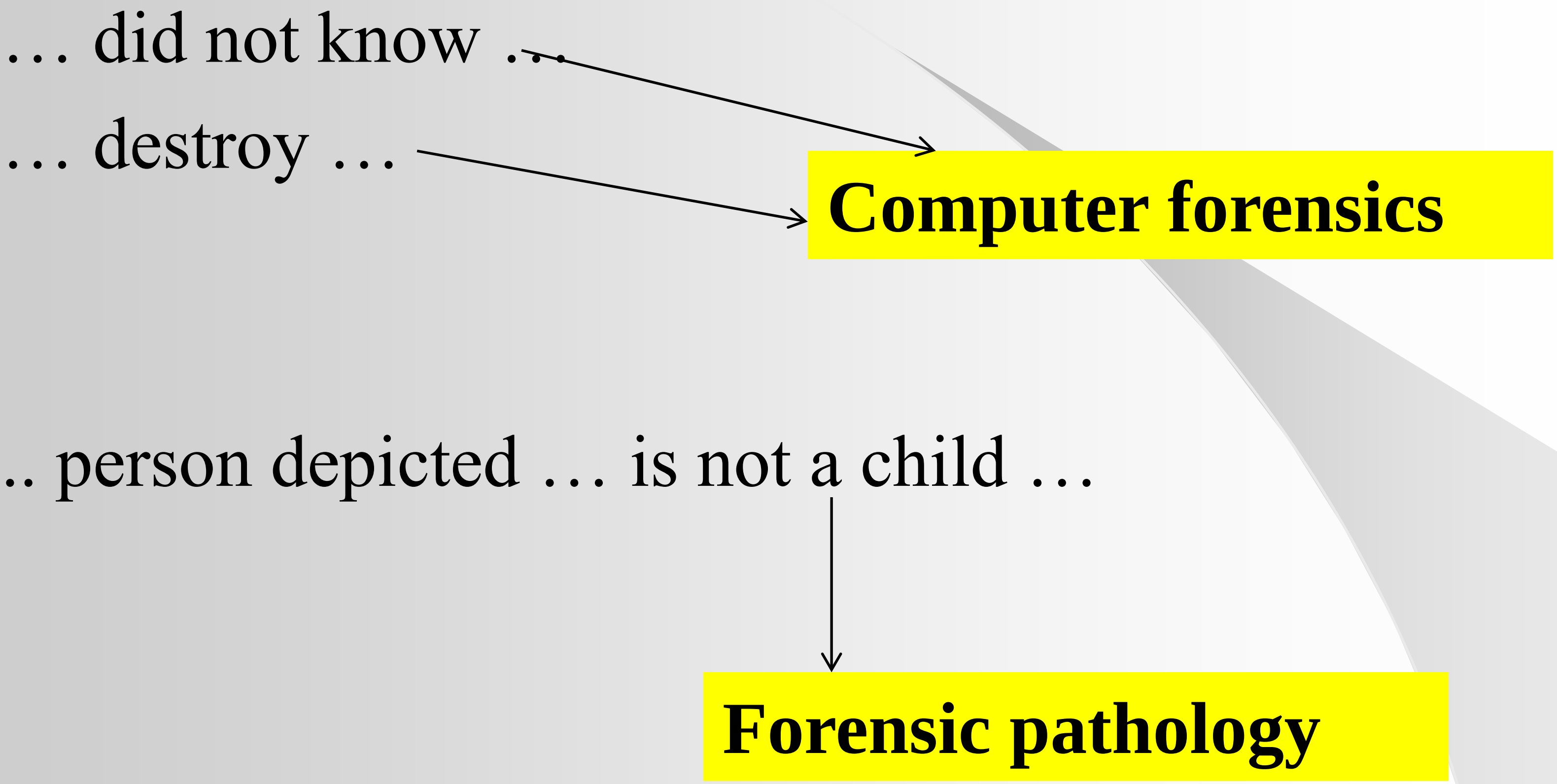
Expert opinion

When the defendant has not seen the child pornography and **did not know** … it to be child pornography

When the defendant did not ask for child pornography and tried to **destroy** it within a reasonable period …

When the suspect believes on a reasonable ground that the person depicted in the child pornography is **not a child** at the time of the depiction …

Forensic Science



… did not know …

… destroy …

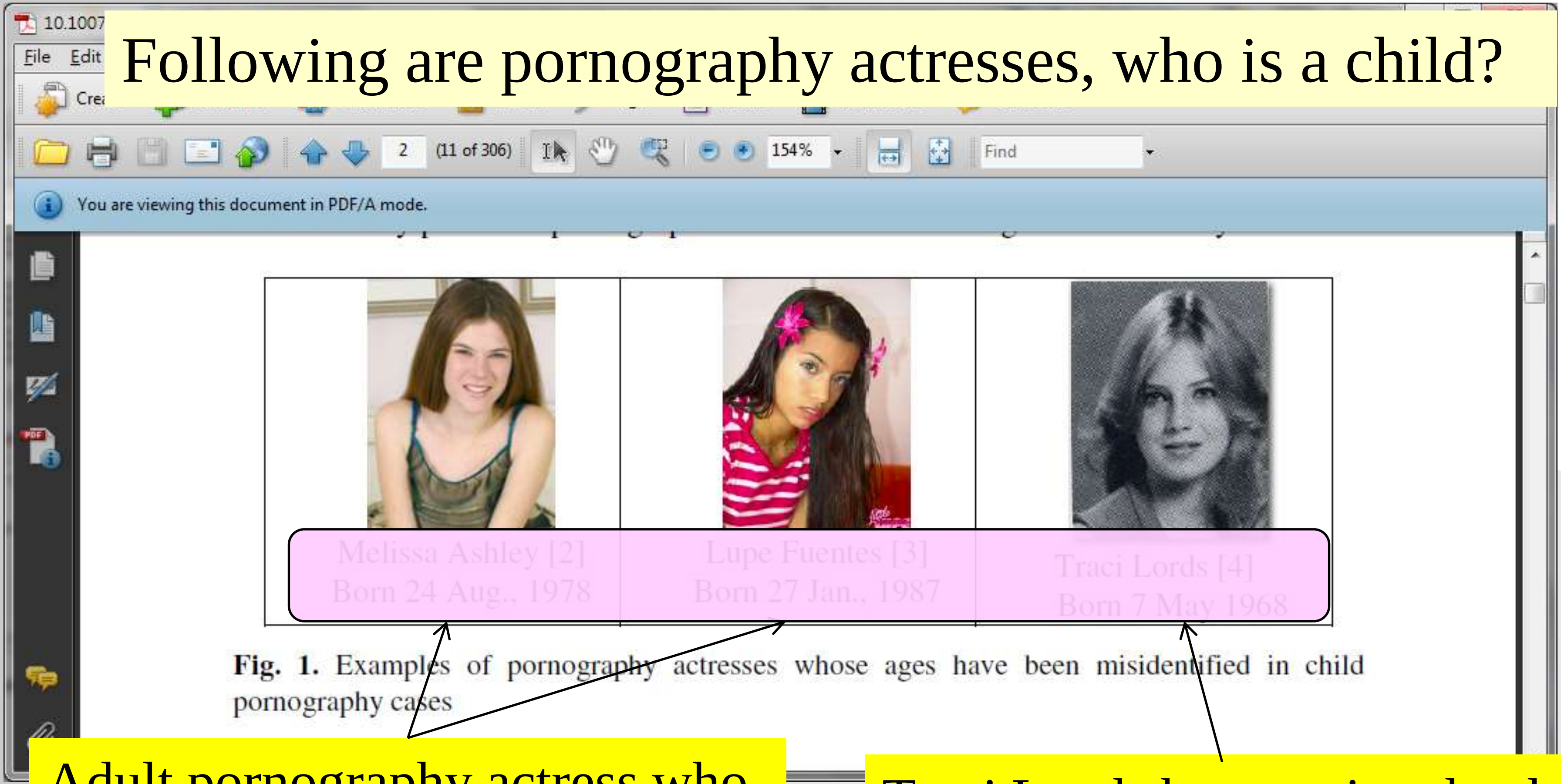
Computer forensics

.. person depicted … is not a child …

Forensic pathology

“not a child” – Age Determination

Following are pornography actresses, who is a child?



You are viewing this document in PDF/A mode.

Melissa Ashley [2]
Born 24 Aug., 1978

Lupe Fuentes [3]
Born 27 Jan., 1987

Traci Lords [4]
Born 7 May 1968

Fig. 1. Examples of pornography actresses whose ages have been misidentified in child pornography cases

Adult pornography actress who have mistakenly identified as chi

Traci Loads became involved in adult pornography at the

C.A. Murphy, The Role of Perception in Age Estimation, in Digital Forensics and Cyber Crime, ICDF2C, 2011.

Did Not Know Defences

2 Kinds of "Did not know" Defences

Trojan Horse Defence (THD)

Inadvertent Download Defence (IDD)

How likely are these defences?

Trojan Horse Defence (THD)

If 50,000 photos are found, can the defendant claim he don’t know

- No one will believe him

The lawyer came up with the Trojan Horse Defence?

How likely it is?

Trojan Horse Defence (THD) (popular in 2000-2005)

1. A Trojan installed itself on the defendant's computer;
2. The Trojan downloaded the CP image files from a remote website (most probably not a public one);
3. The Trojan placed the downloaded image files in the location on the computer where the defendant usually works;
4. The Trojan then uninstalled itself, leaving no trace of itself on the defendant’s computer.

- Lawyer still using it if unable to find other argument
- Our research: complexity based model

Complexity Based Model

In general there is more than one route by which a set of recovered digital evidence traces may have been produced.

An inverse relationship exists between the difficulty of performing a process and its probability of occurrence

- The more difficult / intricate / complex a process is, the less likely it is to occur
- We measure the difficulty of performing a process using a ***complexity metric***.

Given a recovered set of digital evidence, e.g. CP images and videos, enumerate each of the ***feasible routes*** *k* by which those traces could have been produced, e.g. prosecution argument and defense argument

Operational Complexity Model (OCM)

The complexity of each feasible route consists of two parts:

- Computer part: use computational complexity (CC) theory to count byte-wise operations
- Human part: use the Keyboard Level Model (KLM) to count keyboard / mouse operations

For each feasible route *k* we apply the OCM:

$$C_k = KLM_k + CC_k$$

$$p_k \propto C_k^{-1}$$

The ***posterior odds*** for two alternative routes *k* and *k'* leading to the formation of the ***same*** set of digital evidence *{E}* is given by:

$$O(k{:}k') = Pr(H_k|\{E\}) / Pr(H_{k'}|\{E\})$$

Some calculations

Prosecution case: *k*
Defence case: *k'*

$KLM_k = 510$

Keyboard Level Model

$KLM_{k'} = 0$

$CC_k = N + 20N/2^{19} + 1{,}844{,}346$

$CC_{k'} = (23/5)N + 20N/2^{19} + 9{,}938{,}941$

Computational Complexity

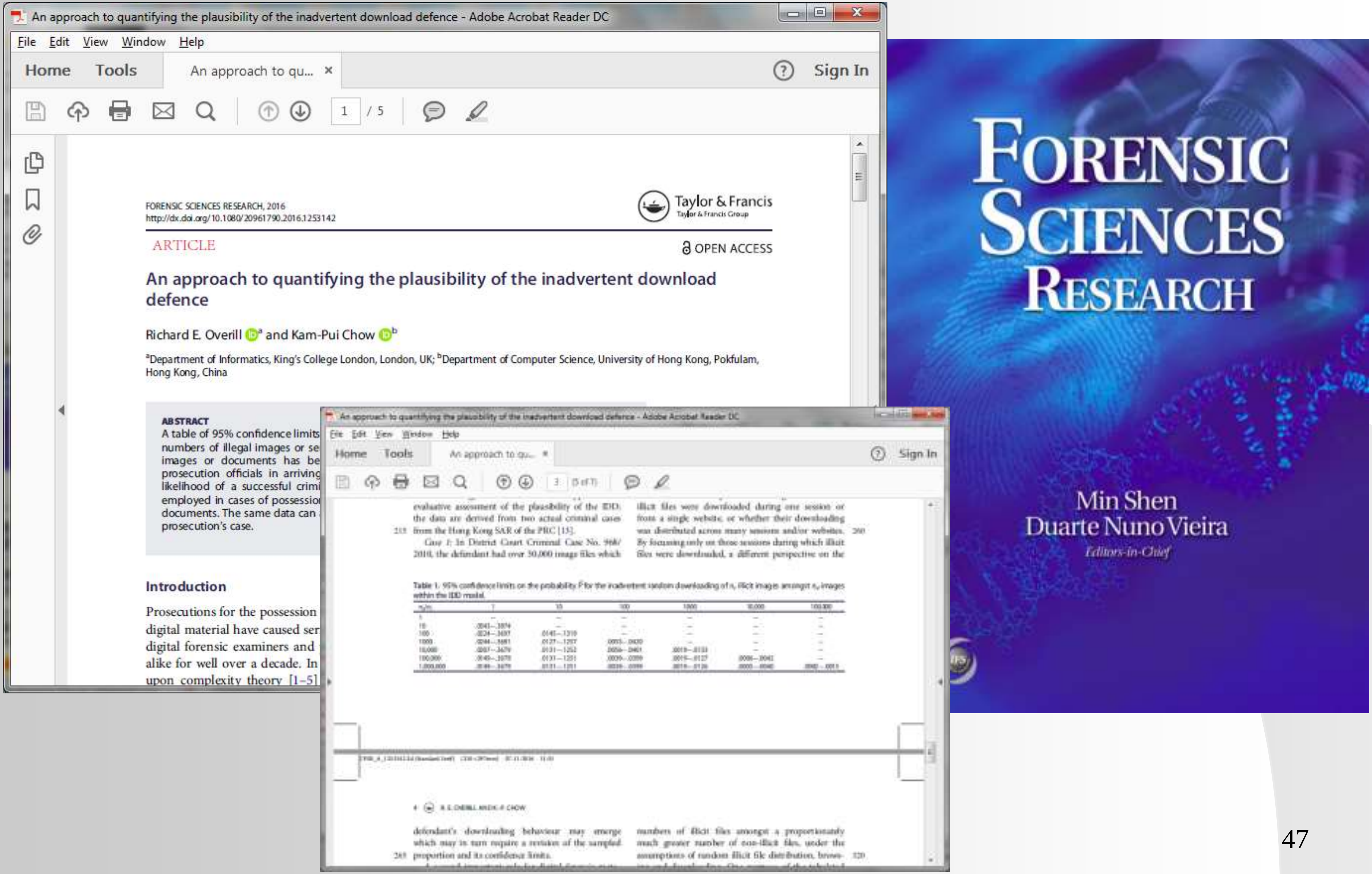
Why? Please read the paper:
Richard E Overill, Jantje A M Silomon KP Chow, A Complexity Based Model for Quantifying Forensic Evidential Probabilities

Case 1: In District Court Criminal Case No. 968/2010

The defendant has over 30,000 downloaded images, of which 248 files were CP images, the others are pornography images

Here， $N_c = 248$ and $N_d = 30000$； we calculated that 95% confidence interval lies between 0.0254 and 0.0029.

We can say with 95% confidence that, the probability that the downloading of the child porn images were due to random browsing activities is no more than 2½% (<2.5%)


An approach to quantifying the plausibility of the inadvertent download defence - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools An approach to qu... ×
Sign In
1 / 5

FORENSIC SCIENCES RESEARCH, 2016
http://dx.doi.org/10.1080/20961790.2016.1253142

Taylor & Francis
Taylor & Francis Group

ARTICLE

OPEN ACCESS

An approach to quantifying the plausibility of the inadvertent download defence

Richard E. Overill [a] and Kam-Pui Chow [b]

[a]Department of Informatics, King's College London, London, UK; [b]Department of Computer Science, University of Hong Kong, Pokfulam, Hong Kong, China

ABSTRACT
A table of 95% confidence limits
numbers of illegal images or se
images or documents has be
prosecution officials in arriving
likelihood of a successful crimi
employed in cases of possessio
documents. The same data can
prosecution's case.

Introduction

Prosecutions for the possession
digital material have caused ser
digital forensic examiners and
alike for well over a decade. In
upon complexity theory [1–5]

An approach to quantifying the plausibility of the inadvertent download defence - Adobe Acrobat Reader DC
File Edit View Window Help
Home Tools An approach to qu... ×
Sign In
3 (5 of 7)

evaluative assessment of the plausibility of the IDD, the data are derived from two actual criminal cases from the Hong Kong SAR of the PRC [13].

Case 1: In District Court Criminal Case No. 968/2010, the defendant had over 30,000 image files which

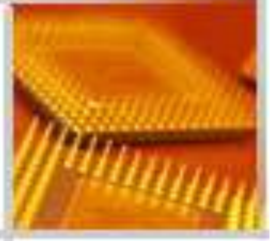
illicit files were downloaded during one session or from a single website, or whether their downloading was distributed across many sessions and/or websites. By focusing only on those sessions during which illicit files were downloaded, a different perspective on the

Table 1. 95% confidence limits on the probability P for the inadvertent random downloading of n_i illicit images amongst n_d images within the IDD model.

n_d/n_i	1	10	100	1000	10,000	100,000
1	–	–	–	–	–	–
10	.0041–.3874	–	–	–	–	–
100	.0024–.3697	.0145–.1310	–	–	–	–
1000	.0044–.3681	.0127–.1207	.0053–.0420	–	–	–
10,000	.0047–.3679	.0131–.1252	.0056–.0401	.0019–.0133	–	–
100,000	.0049–.3678	.0131–.1251	.0039–.0399	.0019–.0127	.0006–.0042	–
1,000,000	.0049–.3679	.0131–.1251	.0039–.0399	.0019–.0126	.0005–.0040	.0002–.0013

defendant's downloading behaviour may emerge which may in turn require a revision of the sampled proportion and its confidence limits.

numbers of illicit files amongst a proportionately much greater number of non-illicit files, under the assumptions of random illicit file distribution, brows-



Conclusion

Conclusion

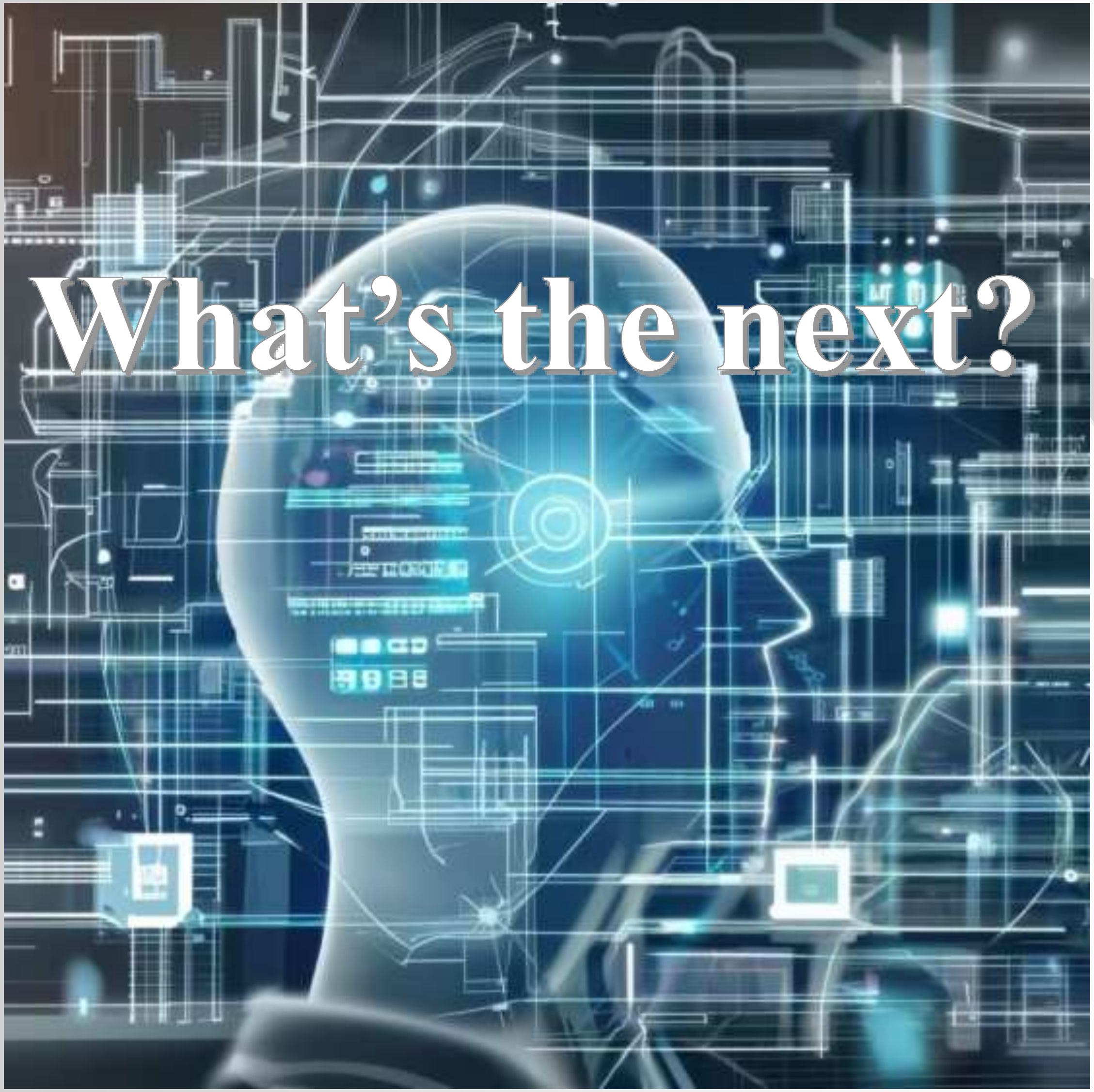
Digital forensics

Concepts and History

Digital forensics vs. traditional forensics

Forensics cases

Future of Digital Forensics



What’s the next?

Future of Digital Forensics

Technological Advancements and Impact

- AI and Machine Learning
- IoT and Cloud Forensics
- Blockchain and Cryptocurrency Forensics

Cybersecurity and Digital Forensics

- Incident Response and Threat Intelligence
- Digital Forensics in Cyber Insurance

References

Richard E Overill, Jantje A M Silomon KP Chow, A Complexity Based Model for Quantifying Forensic Evidential Probabilities

Richard E Overill, Jantje A M Silomon, KP Chow and YW Law, Quantitative Plausibility of the Trojan Horse Defence against Possession of Child Pornography

K.P. Chow, Frank Y.W. Law, Michael Y.K. Kwan, Pierre K.Y. Lai, The Rules of Time on NTFS File System, Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE) 2007

R. Overill and KP Chow, An Approach to Quantifying the Plausibility of the Inadvertent Download Defence, 2016