

The Hong Kong Police

We Serve with Pride and Care



Technology Crime Investigation in Hong Kong

LEUNG Tak-kwong, Collins

Acting Chief Inspector of Police

Computer Forensics & Training

Technology Crime Division

Commercial Crime Bureau



The Hong Kong Police Force

Outline

- What is 'Technology/Computer' Crimes ?
- Crime Statistics
- Legislation on Technology Crimes
- Where is the 'EVIDENCE' ?
- The Role of Computer Forensics
- Challenges in Computer Crime Investigations in Hong Kong
- Private Sector – Police Co-operation

What is Technology Crime?

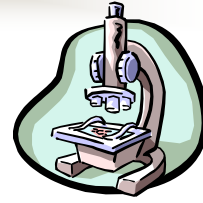
- “Any **illegal act** committed by application of **computer technologies** or such technologies being used as a **means to an end...**”
- No legal definition in Hong Kong



What is Technology Crime?

- Cyber crimes:-
 - Criminal activities in **virtual world** such as Internet
- Computer as a **target**:-
 - Criminal damage, unauthorized access to computers (hacking), DoS/DDoS, virus/worm attacks.
- Computer as a **tool**:-
 - child-pornography, drug trafficking, e-banking, e-auction, publishing obscene articles, cyber stalking.
- Others:-
 - PDA, Portable Phones (2.5G/3G), networks (local/Internet), Smart Cards, databases, skimming devices (credit card).

Scene of Crime



- Traditional:-
 - Fingerprints, photos, records(pager/portable phones), documents, DNA, samples taken from crime scenes ...
- Current:-
 - Digital evidence: e-mails, ICQs, Firewall Logs, Router Logs, MP3, hard disks and various storage media, off site evidence, ...

Technology Crime Division

Operations

- Investigation
- Incident Response

Intelligence

- Prevention/Research
- Assessment/Analysis
- Liaison, Overseas/ISP

Forensics

- Forensics Laboratory/Digital Evidence
- Training/Accreditation/Research
- Liaison with Research Institutions/Vendors



Overall Technology Crime 1995 - 2002

Title of Offence	1995	1996	1997	1998	1999	2000	2001	2002 (Jan-Jul)
Unauthorised Access to Computer by Telecommunication								
Access to Computer with Criminal or Dishonest Intent								
Criminal Damage								
Obtaining Property by Deception								
Obtaining Services by Deception								
Theft (e-Banking)								
Others								
Total								

Information to be concealed

Strategic Policing in Technology Crimes



Strategic Directions:

- Maintaining a **professional investigation capability** to deal with technology crimes
- Broadening the investigation capability **within the Force**
- Developing **accredited computer forensics**
- Proposing changes in **Laws and Policies**

Strategic Directions:

- **Prevention** through public education and awareness programs
- **Intelligence** management
- **Liaison** with the industries, professionals and overseas law enforcement agencies
- **Continuous improvement** to keep up with the advance in technology

Local Legislation on Computer Crimes

- the Telecommunication Ordinance (Cap.106)
- the Crimes Ordinance (Cap.200)
- the Theft Ordinance (Cap. 210)



Telecommunications Ordinance

- Unauthorized Access to Computer by Telecommunication

(S.27A of Cap.106)

Unauthorised Access to Computer by Telecommunications (S.27A Cap.106)

- "Any person who, by telecommunication, obtains unauthorized access to a computer commits an offence....."

- **Fine \$20,000**



Crimes Ordinance

- Access to Computer with Criminal or Dishonest Intent (S.161 of Cap.200)
- Criminal Damage (S.60 of Cap.200)
- Making a False Entry in a Bank Book etc... (S.85 Cap. 200)

Access to Computer with Criminal or Dishonest Intent (S.161 of Cap.200)

Any person who obtains access to a computer

- ↖ with intent to commit an offence
- ↖ with a dishonest intent to deceive
- ↖ with a view to dishonest gain for himself
- ↖ with a dishonest intent to cause loss to another“

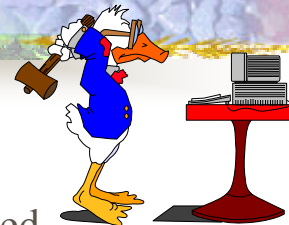
Imprisonment for 5 years

Criminal Damage (S.60 of Cap.200)

Definition of "property" extended to include:-

- computer programs and data stored in a computer
- programs or data held in a computer storage medium

Imprisonment for 10 years



Criminal Damage

Definition of "destroy or damage" extended to include:

- to alter or erase programs or data
- to add any program or data to a computer or computer storage medium
- "to cause a computer to function other than as it has been established to function by or on behalf of its owner"

Making a False Entry in a Bank Book etc... (S.85 Cap. 200)

- Extended to cover entries made into records contained in:-
 - ↖ discs, card, tape, microchips, sound track,
 - ↖ or other device in which data is recorded or stored

Life Imprisonment

Burglary



- Definition of burglary extended:-
 - any person who enters any building as a trespasser with intent to do "unlawful damage" to a computer

(S.11 Cap. 210)

14 years imprisonment

False Accounting

- The definition of a "record" extended to include:-
 - a record kept by means of a computer
- (S.19 Cap 210)

10 years imprisonment

Publishing Obscene Articles (Cap. 390 Sec. 21)

- Any person who:-
 - publishes;
 - possesses for the purpose of publication,
 - imports for the purpose of publication,
- any obscene article, whether or not he knows that it is an obscene article, commits an offence and is liable to a **fine of \$1,000,000** and to **imprisonment for 3 years**.

Definition - Publishing

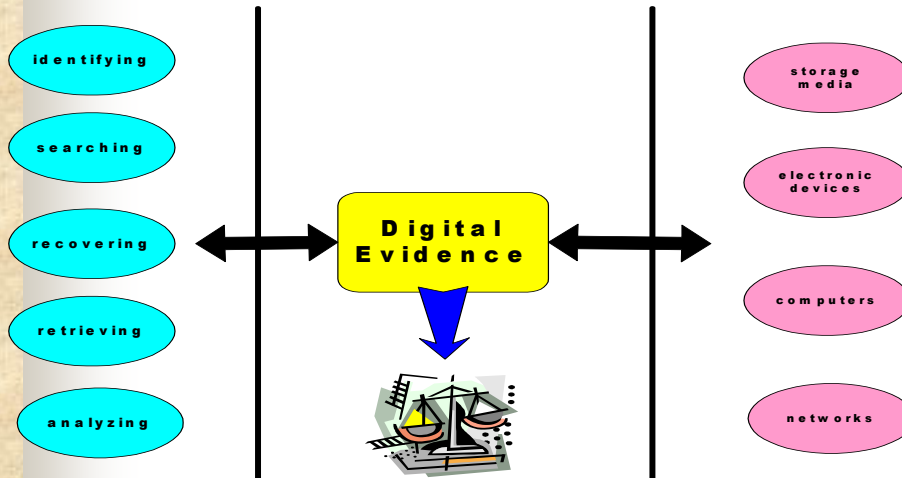
- **A person publishes an article if he, whether or not for gain :-**
 - distributes, circulation, sell, hires, gives, lends, shows, plays or projects the article to the public or a section of the public;
 - in the case of an article :-
 - consisting of or containing material to be looked at; or
 - that is a sound recording or a film, video-tape, disc or other record of an article

Evidence can be found:

- Computers / Notebooks
- Servers / Networks
- Logs – Web/Proxy/Firewall ...
- Portable phones
- PDA / DC / DV
- Storage Media
 - CF/SD/MMC/Memory Stick

What is Computer Forensic Examination?

Scientific and *Systematic* approach in:-

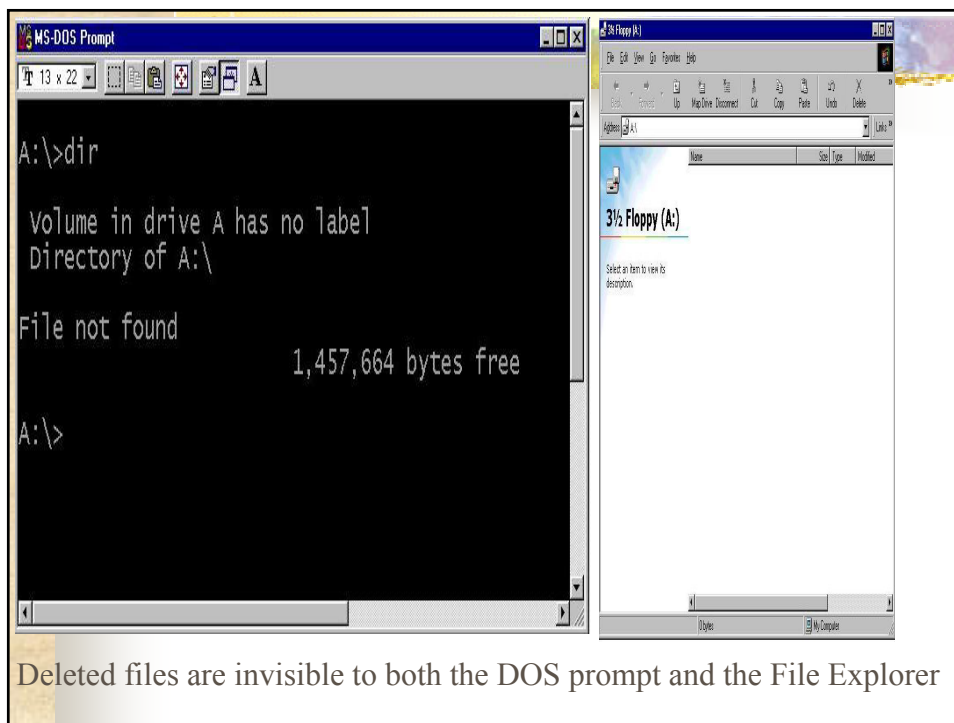
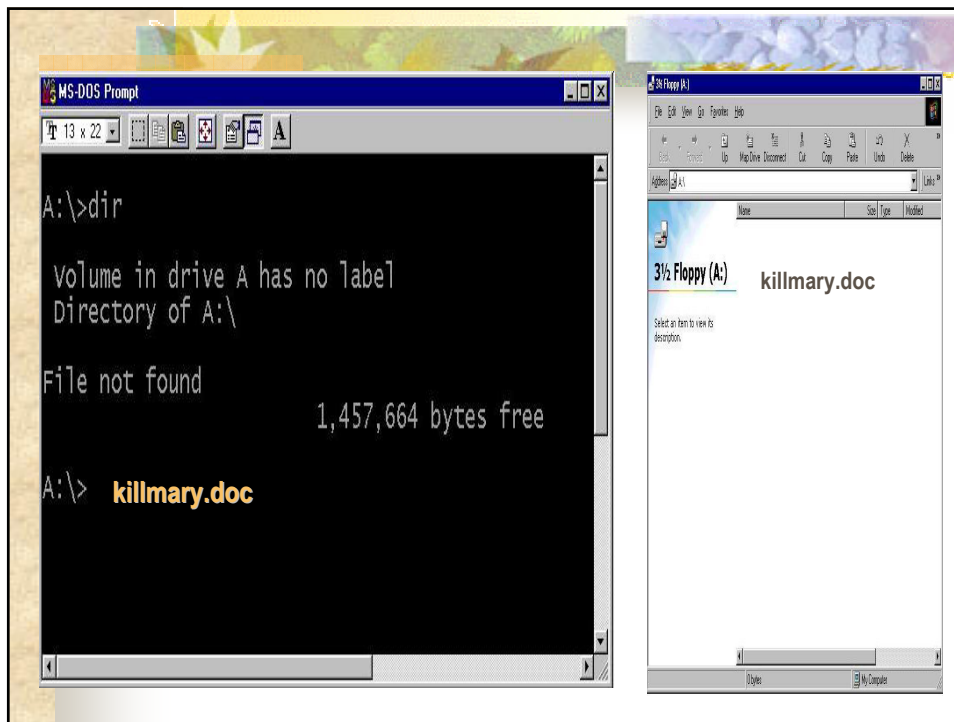


Computer Forensic Examination

Forensic Examination	1995	1996	1997	1998	1999	2000	2001	2002 (Jan-Jul)
No.of Cases								
No.of Computer Received								
No.of GB Examined								
Crime Scene Attendance								

Information to be concealed

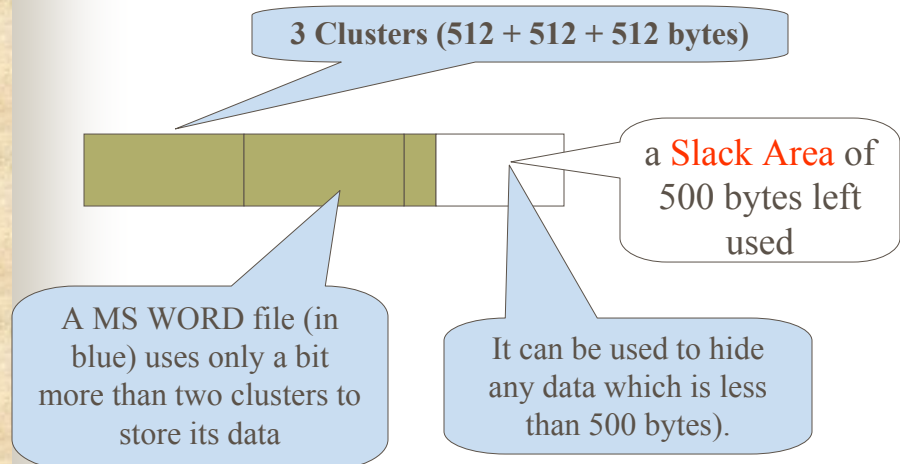
Deleted files



Slack Area

Many computer file systems (e.g. Windows 98, NT) use fixed cluster size (512 bytes). Even though a tiny computer file requires less storage than one cluster, an entire cluster is reserved for the file. The unused space is called “**Slack Area**”.

The Slack Area of a file



Steganography

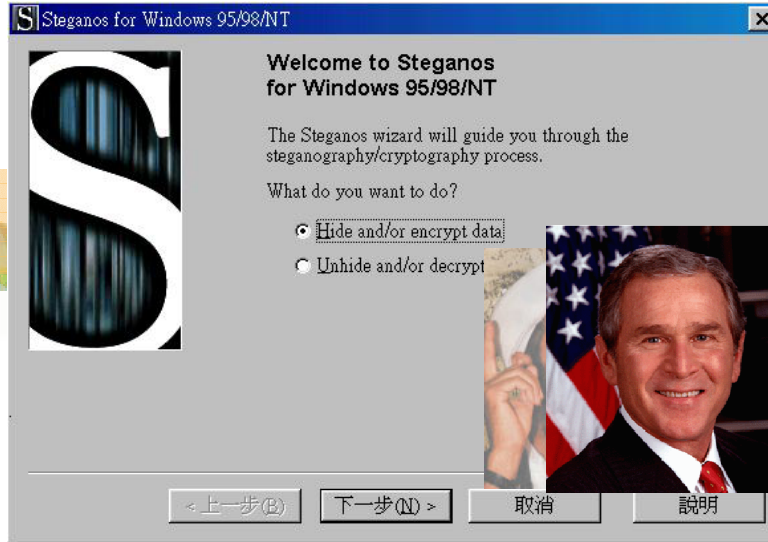


A freeware for steganography

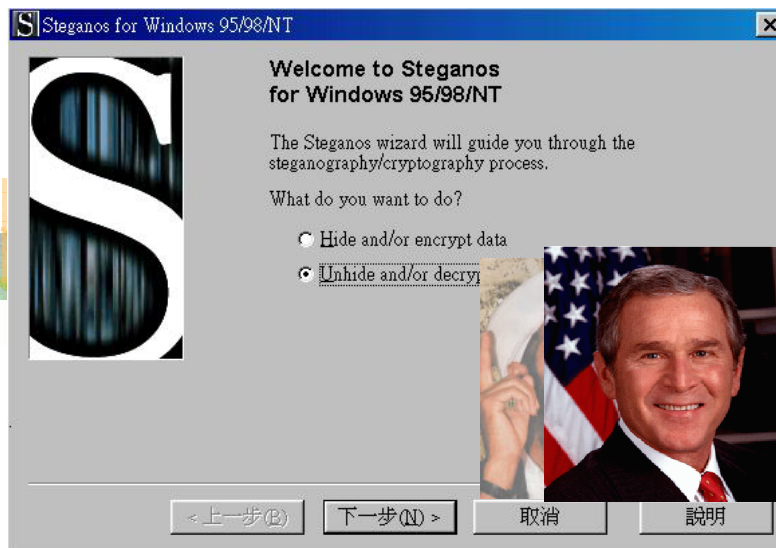
This hacker's tool can be used to hide Bin Laden's photo behind George Bush's



Hide and Encrypt a picture



Unhide and decrypt a picture



Challenges Encountered/Foreseen (1)

- Advancement of technologies
 - Encryption
 - Data Hiding
 - Remote attacks
 - Bandwidth
- Concealment / anonymity of culprits
- Data volume increasing
- Network forensics

Challenges Encountered/Foreseen (2)

- Forensic tools availability
- Forensic training
- Completeness of Records / Trails / Logs / Backups
- Jurisdiction problems
- Reluctance to report
- Diversity in operating/file systems
- Role of service providers



Private Sector vs Police

- Exchange of information
- Knowledge transfer
- Development of forensic tools
- Assistance to POLICE:
 - Keeping of logs/records/trails
 - Providing information
 - Technical assistance

Contacts:



Office: 2860 – 2625

Fax: 2802 – 2865

e-mail: collins_leung@police.gov.hk