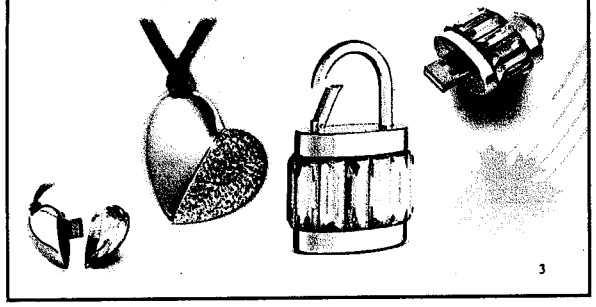
Canada

How it works?
- Flash – Camera, video games etc... (transistors)
- RAM – Computer Memory
- ROM
- How it looks
- Types (formats) of Memory out there
  - SD, MMC, PRO, DUO

2



3

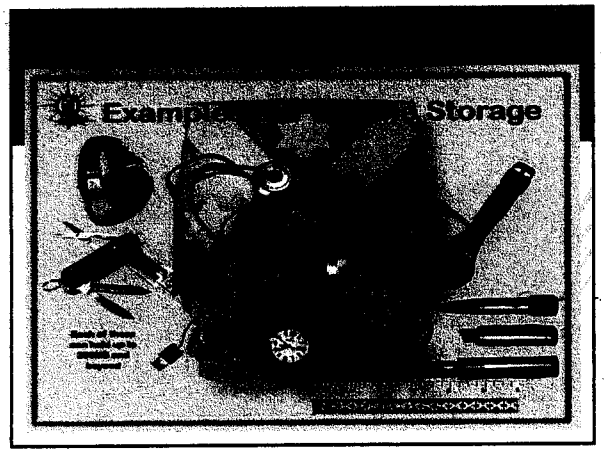
Please leave length x6

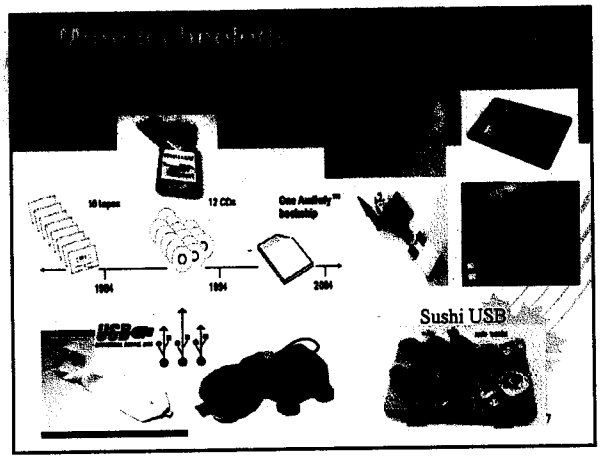
- Can contain a stack of paper (8.5x11), 35 feet higher than the CN tower
- Would take two years to print @ 24/7
- Would take two years to read at 10 seconds per page @ 24/7

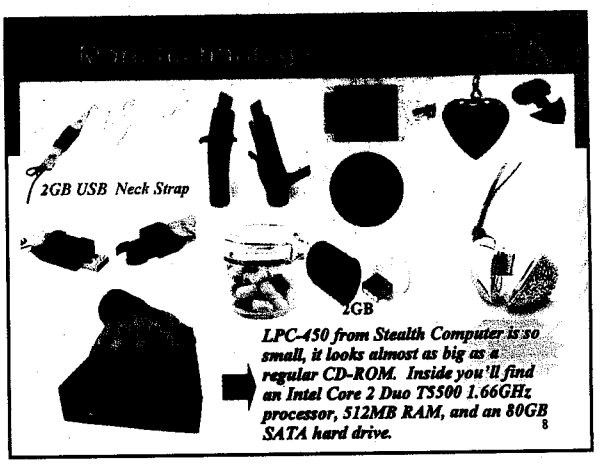
553M (1,815Ft)

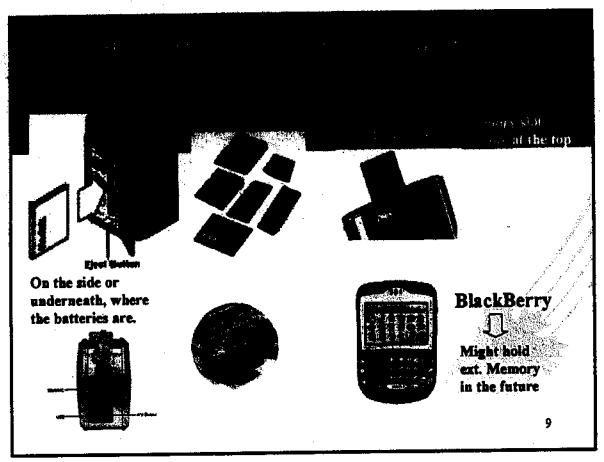
Honda Civic Coupe length x128

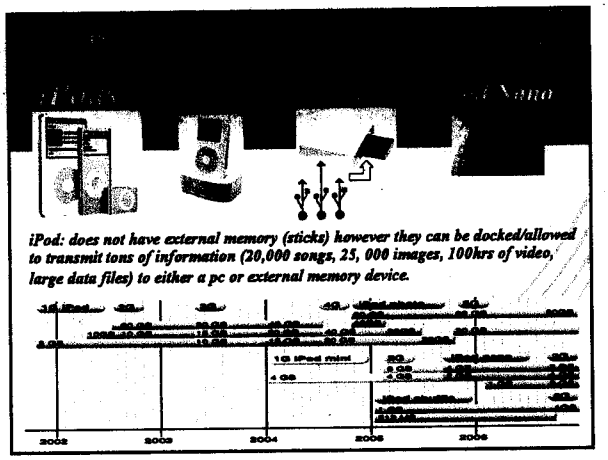
4

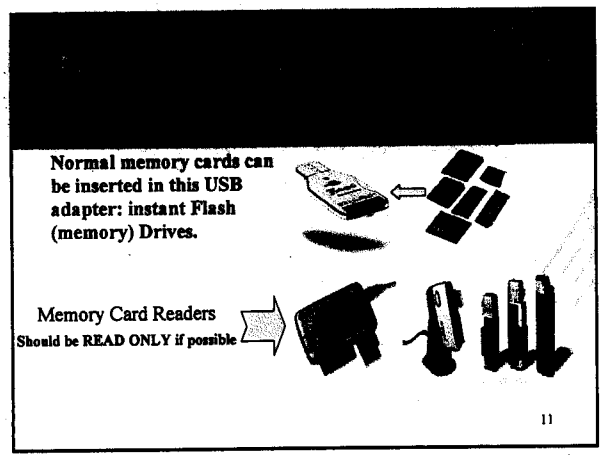


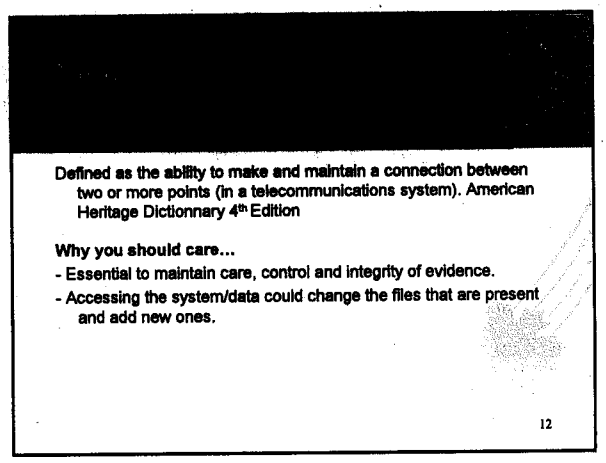


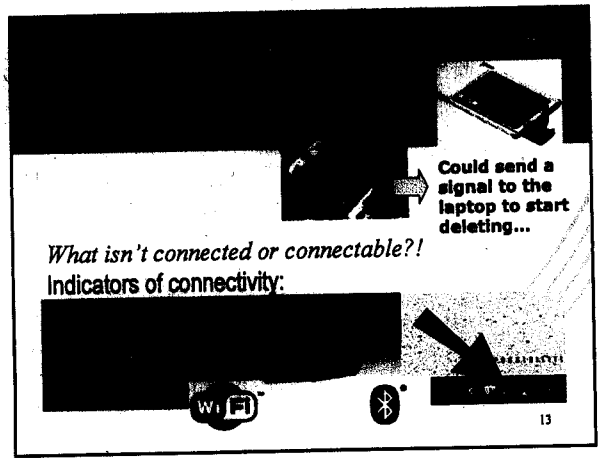


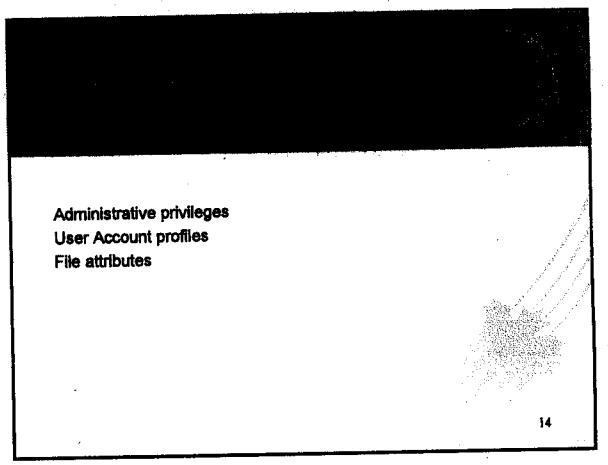


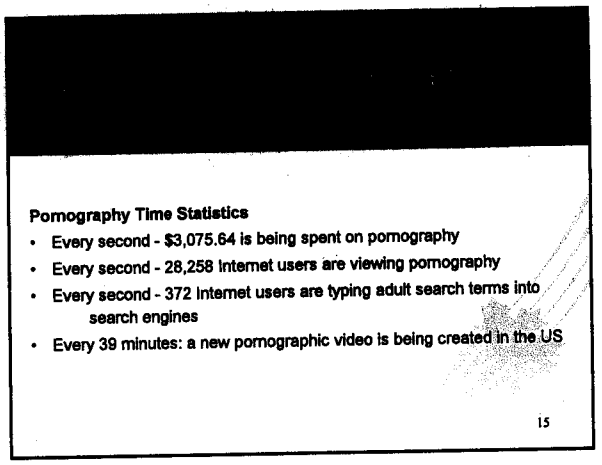


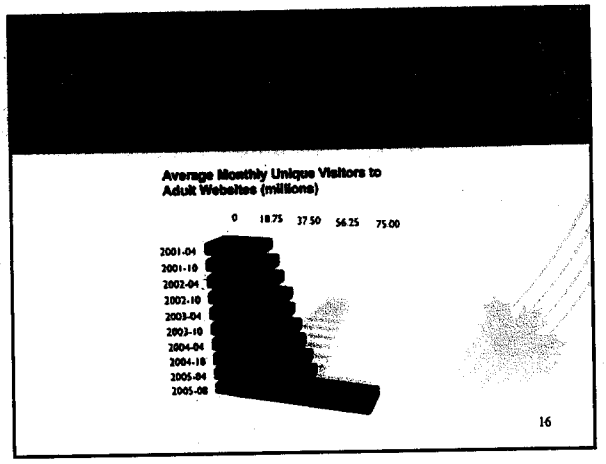


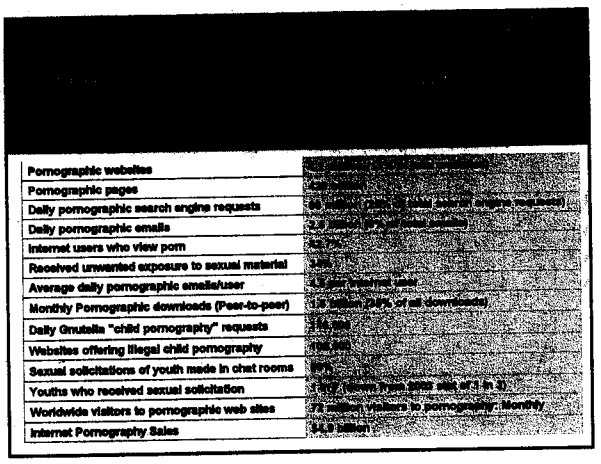


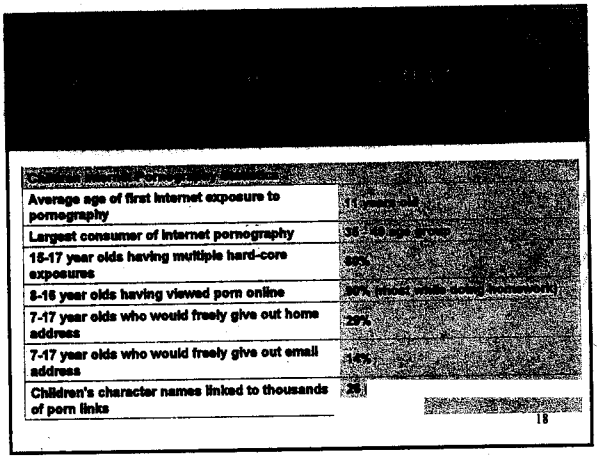




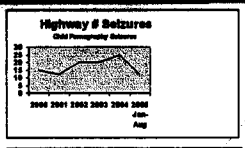


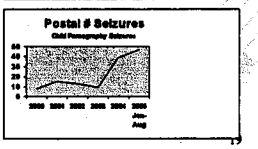






- **Seizures of child pornography / child exploitation materials are increasing**
- **Majority of seizures: via postal stream**
- **Increase of incidents along land-border POEs**
- **From Jan. 01, 2005 to June 6, 2007**
  328 seizures of child porn material





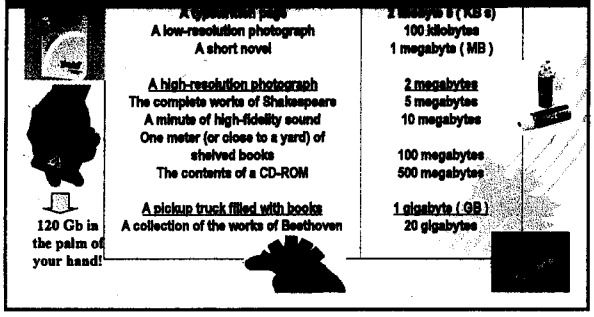
19

S

71 Port Prosecutions
328 Leads for potential prosecutions
22 Commercial Cases
68 Assistance files relating to Child Pornography

Stats obtained from: CIIMS
Customs Investigations Information Management System
Dating back to January of 2004

20



Canada Border Services Agency | Agence des services frontaliers du Canada

November 9, 2009

Regional Management
Criminal Investigations Program

Subject: Wording For Information To Obtain (ITO) A Search Warrant Regarding Computer Search and Evidence Recovery

The purpose of this bulletin is to provide for your information and distribution to all investigators updated wording to be used with all search warrants effective immediately. While some modifications are sometimes required by a judge or Justice of the Peace, this wording should generally be adhered to. This update resulted from extensive consultations with CBSA Legal Services, other law enforcement agencies, and our Computer Search and Evidence Recovery Specialists (CSERS).

The goal of this update is to strike a balance in the amount of information provided in an ITO. It is important to provide a basic explanation of the CSER process so there can be no suggestion that CBSA investigators are not authorized to search for digital evidence wherever it may be, while not limiting our legal search parameters or divulging too many details regarding specialized investigative techniques.

9 novembre 2009

Gestion régionale
Programme d'enquêtes criminelles

Objet : Formulation d'une dénonciation en vue d'obtenir un mandat de perquisition relativement à la perquisition d'ordinateurs et récupération de la preuve

Veuillez trouver ci-joint, à titre d'information et de distribution à tous les enquêteurs, la formulation mise à jour à utiliser pour tous les mandats de perquisition à compter d'aujourd'hui. Bien que quelques modifications sont parfois exigées par un juge ou un juge de paix, il faudrait généralement respecter cette formulation. Cette mise à jour a découlé de vastes consultations avec le personnel des Services juridiques de l'ASFC, d'autres organismes d'exécution de la loi et nos spécialistes des perquisitions d'ordinateurs et récupération de la preuve (PORP).

Cette mise à jour vise à équilibrer la quantité de renseignements fournis dans une dénonciation. Il est important de fournir une explication de base du processus de PORP afin qu'il ne puisse avoir aucune suggestion que les enquêteurs ne soient pas autorisés à procéder à la perquisition pour trouver des éléments de preuve numériques quel que soit l'endroit, tout en ne limitant pas nos paramètres liés aux perquisitions légales ou en ne divulguant pas trop de détails concernant les techniques d'enquête spécialisées.

Canada

While discussions are ongoing with Legal Services regarding some related issues and could result in further modifications in future, the new wording should be treated as the standard wording for the time being.

Tandis que les discussions sont en cours avec le personnel des Services juridiques concernant certaines questions connexes et qu'elles pourraient amener d'autres modifications à l'avenir, le document ci-joint devrait être considéré comme étant la formulation normalisée pour le moment.

The updated ITO wording can be found on the Computer Search and Evidence Recovery webpage on the CID intranet site at the following link (

Should you have any questions, please contact Stephen Zimmerman, Computer Search and Evidence Recovery Program, or Jag Johnston, Manager, Programs Section.

Si vous avez des questions, veuillez contacter Stephen Zimmerman, Perquisition d'ordinateur et récupération de la preuve, ou Jag Johnston, gestionnaire, Section des programmes.

Steve Sloan
Director / Directeur
Criminal Investigations Division / Division des enquêtes criminelles
Enforcement Programs Directorate / Direction des programmes d'exécution de la loi
Enforcement Branch / Direction générale de l'exécution de la loi

For the things to be searched for:

a) paragraph for documents to be searched for
b) paragraph for goods, if applicable

[Include limiting parameters such as persons, dates, products, vendors or countries involved]

For the Information to Obtain the Search Warrant:

1. Any person authorized by this warrant to search a computer system or other electronic devices/media in a building or place for data may

   (a) use or cause to be used any computer system at the building or place to search any data contained in or available to the computer system;
   (b) reproduce or cause to be reproduced any data in the form of a print-out or other intelligible output;
   (c) seize the print-out or other output for examination or copying; and
   (d) use or cause to be used any copying equipment at the place to make copies of the data.

2. On [insert date], I spoke with [insert name of CSER] of [insert division information]. He/she is a member of the Computer Search and Evidence Recovery Program and specializes in the search, seizure and analysis of computer systems and other electronic devices/media (also known as digital forensics) and as such he/she is aware of the following:
3. [Insert name of CSER] told me that members of the CSER Program can forensically examine a computer system and retrieve a wide variety of information from it. Typically, the data sought is found on the hard drive(s) contained within a computer system, the primary storage device of a computer. The examination will include searching the entire hard drive for the elements important to the investigation. It is necessary to examine the entire physical hard drive to complete a comprehensive search for electronic evidence. This information includes, but is not limited to:
   a. Copies of web pages created on the computer or downloaded from the internet;
   b. Copies of electronically created documents such as letters, journals and spreadsheets

c. Copies of e-mail messages received and sent from the computer system, as well as those that are in draft form before being sent;
d. Records of past instant messaging and online chat conversations (e.g. ICQ, IRC, MSN Messenger).

4. Deleted files or file fragments may exist for an extended period of time on the computer system due to the design of most common computer operating systems. Files that have been deleted by the user are not physically erased. Rather, the operating system merely marks the area of the storage disk where the file was stored as available to be used in the future. If the space is not re-used prior to seizure, forensic tools can retrieve these deleted files or file fragments. All evidence must be retrieved, whether it supports the investigation of the alleged offence or it proves to be exculpatory.
5. CSER Specialists (CSERS) will make an exact copy, called an "image", of the entire hard drive and conduct all subsequent forensic analysis on that copy. During the acquisition process and the subsequent forensic analysis, CSERS will use specialized hardware, software tools and techniques such as 'digital fingerprinting' (hashing) before and after the process to ensure and prove that there is ~~there is little or~~ no change to the original data. Imaging may be done at the search location or devices/media may be seized and imaged elsewhere.
6. There is a wide variety of techniques available to even the novice computer user to resist the casual examination of data saved on a hard drive. These techniques include but are not limited to:
    a. Password protection of individual files
    b. Encryption of entire hard drives
    c. Renaming files
    d. Steganography (hiding files inside other files)

    It requires time, experience, and technical resources to defeat these and other techniques. As such, it is necessary to examine the entire physical hard drive to complete a comprehensive search for electronic evidence. In that context, a CSER will ask for, but will not compel a computer owner or custodian to divulge a password or encryption key required to open a file, in order to facilitate a forensic examination.
7. CSERS will be present at the search and will assess, based on the aforementioned reasoning, whether it is necessary to seize peripherals or software in order to be able to access all relevant data.
8. While the above paragraphs deal with hard drives found in computers, the same principles and processes are applicable to any electronic devices and digital media that store data and may be found at the search location.

[Some additional case-specific details could be included in order to strengthen the link between digital evidence and the offence. For example, "copies of e-mail messages provided by the informer show that the subject counselled his clients using this method of communication so additional electronic correspondence will be searched for."]

ADDITIONAL/ ALTERNATE WORDING TO BE CONSIDERED:

Here are additional words, (and, in my opinion, more modern) that are recommended by a former Edmonton Police detective and Court Certified Computer Forensics Expert (and further tweaked by me):

"Computer equipment including magnetic or other machine readable storage equipment, programs or software associated with the said equipment, or any other device and associated software and manuals used or capable of being used to create, store, manipulate or reproduce electronic documents, records or graphic files related to the person(s) and time frame in question"