# CSCN4021
# Cyber Crime Investigations

## Introduction to cyber crime Investigation

**Course Co-Ordinator**

Dr. Jayakumar

Assistant Professor

Department of Computer Science
and Engineering
Galgotias University

Program Name: MCA

# Introduction

Introduction

- Types of crimes that involve computers
- Where to find computer evidence
- Preparing for computer search and seizure

# Types of Crimes that Involve Computers

Get Technical Support Early in the Investigation Provide:

- Search Warrant Preparation
- Pre-search Planning
- Search Execution
- Traditional computer forensics
- Interpretation of Results
- Trial Support & Testimony

# Types of Crimes that Involve Computers

Computer can be used to commit a crime, or to store evidence of a crime –

Traditional Crimes

- Computer hacking
- Child pornography – Almost any other crime
- Gangs: use computers to communicate
- Drugs: use computers to track sales, business
  - Bank Robbery
- Frauds, Identity Theft, Intellectual Property…

# Where to Find Computer Evidence

- Seize items specified in the search warrant:

  Computers, laptops, Network Equipment (hubs and switches), Cell phones

  Peripherals: CD-R's, DVD-R's, Digital cameras, PDA's

  External Media: CD's, floppy disks, USB thumb drives

  Paper notes, documentation and manuals, post-it notes.

- Document computer equipment and peripherals prior to removal.

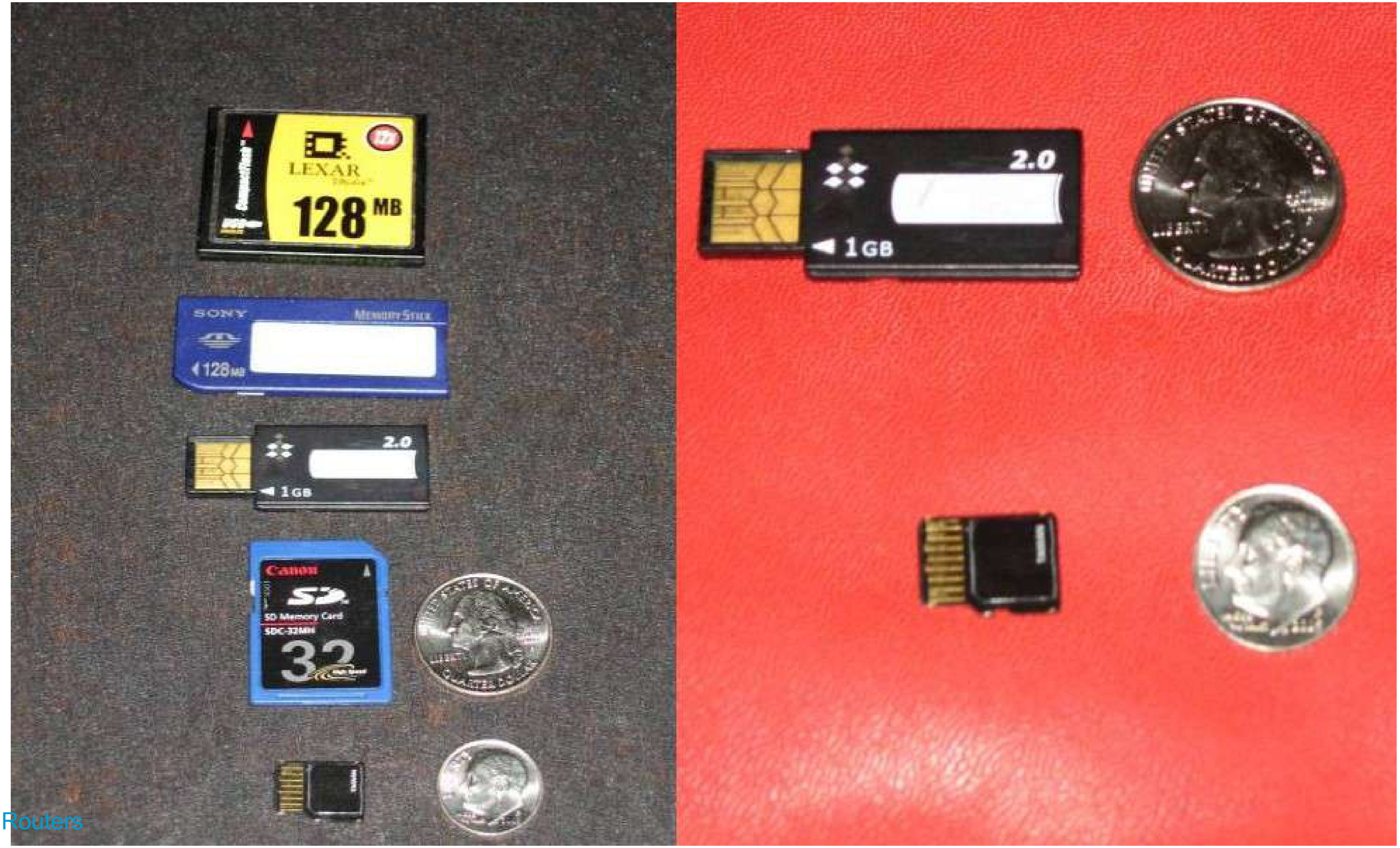
  Digital pictures, diagrams

  - Digital photos of entire house, including bedrooms, bathrooms, outdoors (to be compared with images that may be recovered from computer).

# Types of Electronic Media

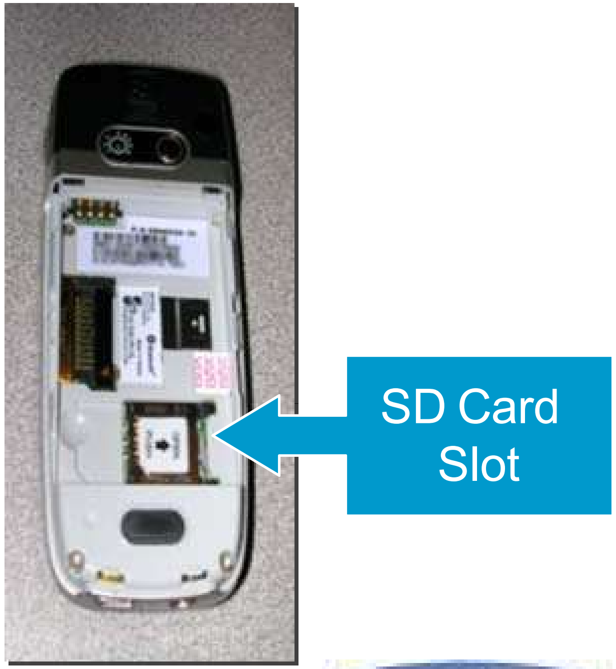
# Variety of Media

# Variety of Media

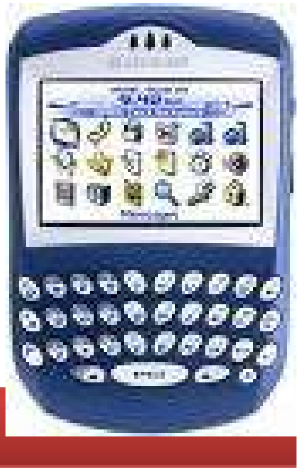


Routers

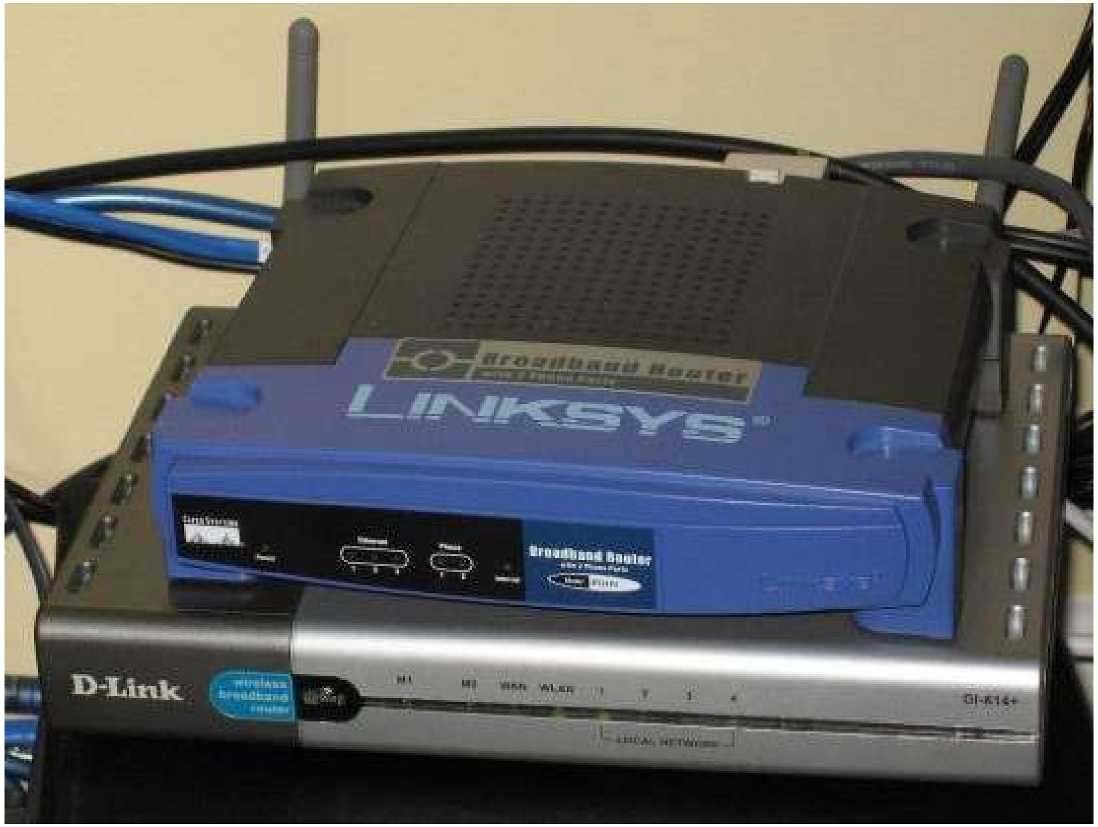
# Cell Phones



SD Card Slot



# But Wait, There's More



# iPods

iPods are becoming very popular. They’re showing up everywhere.

They’re more than music players, they are storage devices.

# What’s on an iPod?

- Music
- Videos
- Contact List
- pr0n
- Calendars
- pr0n
- Notes
- Pr0n
- Anything

# Printers

Sometimes can be easily overlooked by investigators!!

Printers can contain all sorts of data that’s often overlooked.

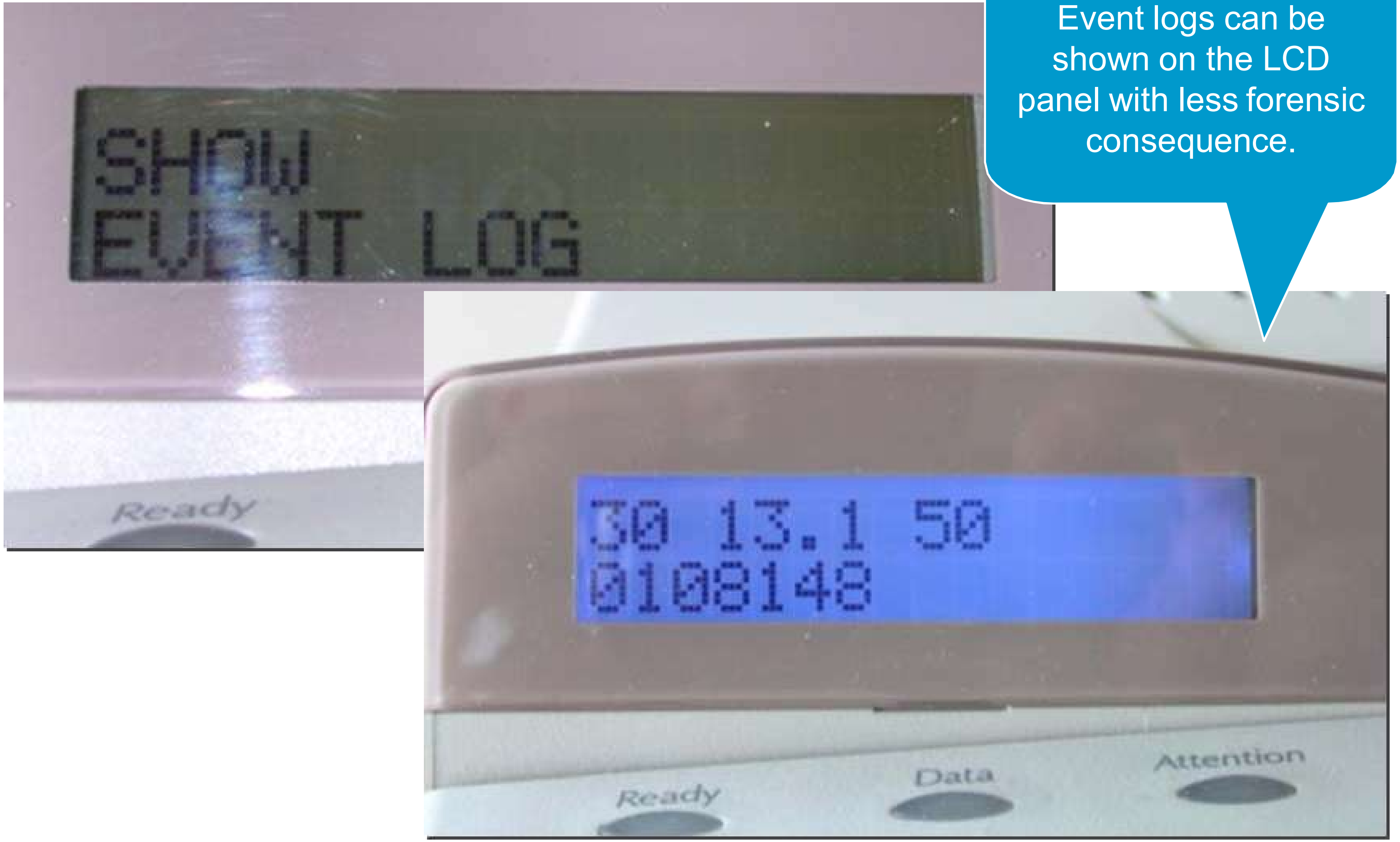
- Does the printer have a ramdisk?
- A hard disk?
- Web interface?
- Event logs?
- Job logs?
- Job schedules?
- Is there volatile or non-volatile data?

# Printer LCD Menus

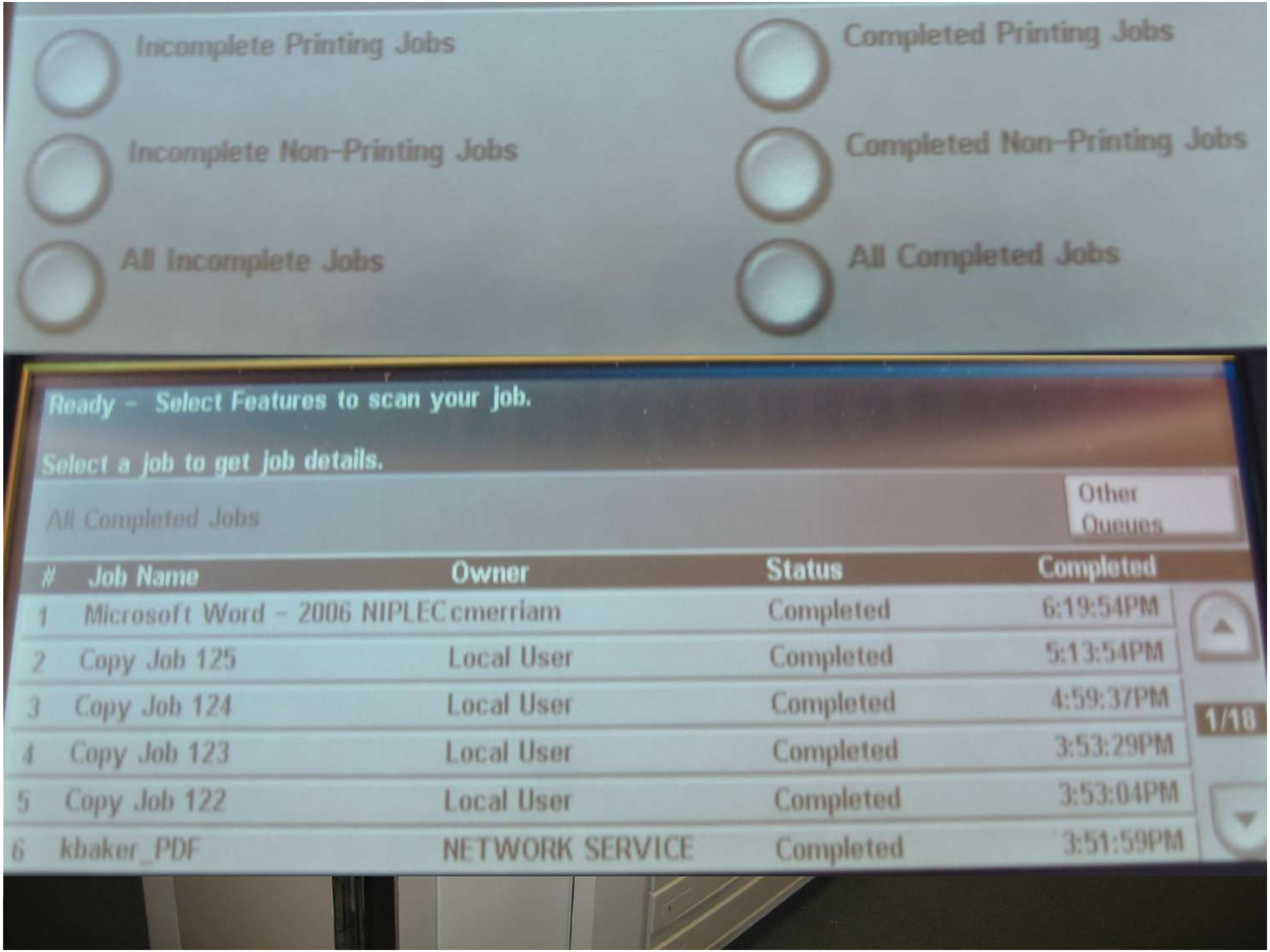
HP's Information menu is the gateway to all sorts of hidden evidence…

…like the event log…

# Printers



Event logs can be shown on the LCD panel with less forensic consequence.



○ Incomplete Printing Jobs

○ Completed Printing Jobs

○ Incomplete Non-Printing Jobs

○ Completed Non-Printing Jobs

○ All Incomplete Jobs

○ All Completed Jobs

Ready - Select Features to scan your job.

Select a job to get job details.

All Completed Jobs

Other Queues

| # | Job Name | Owner | Status | Completed |
|---|---|---|---|---|
| 1 | Microsoft Word - 2006 NIPLEC | cmerriam | Completed | 6:19:54PM |
| 2 | Copy Job 125 | Local User | Completed | 5:13:54PM |
| 3 | Copy Job 124 | Local User | Completed | 4:59:37PM |
| 4 | Copy Job 123 | Local User | Completed | 3:53:29PM |
| 5 | Copy Job 122 | Local User | Completed | 3:53:04PM |
| 6 | kbaker_PDF | NETWORK SERVICE | Completed | 3:51:59PM |

1/18

# Fax Machines

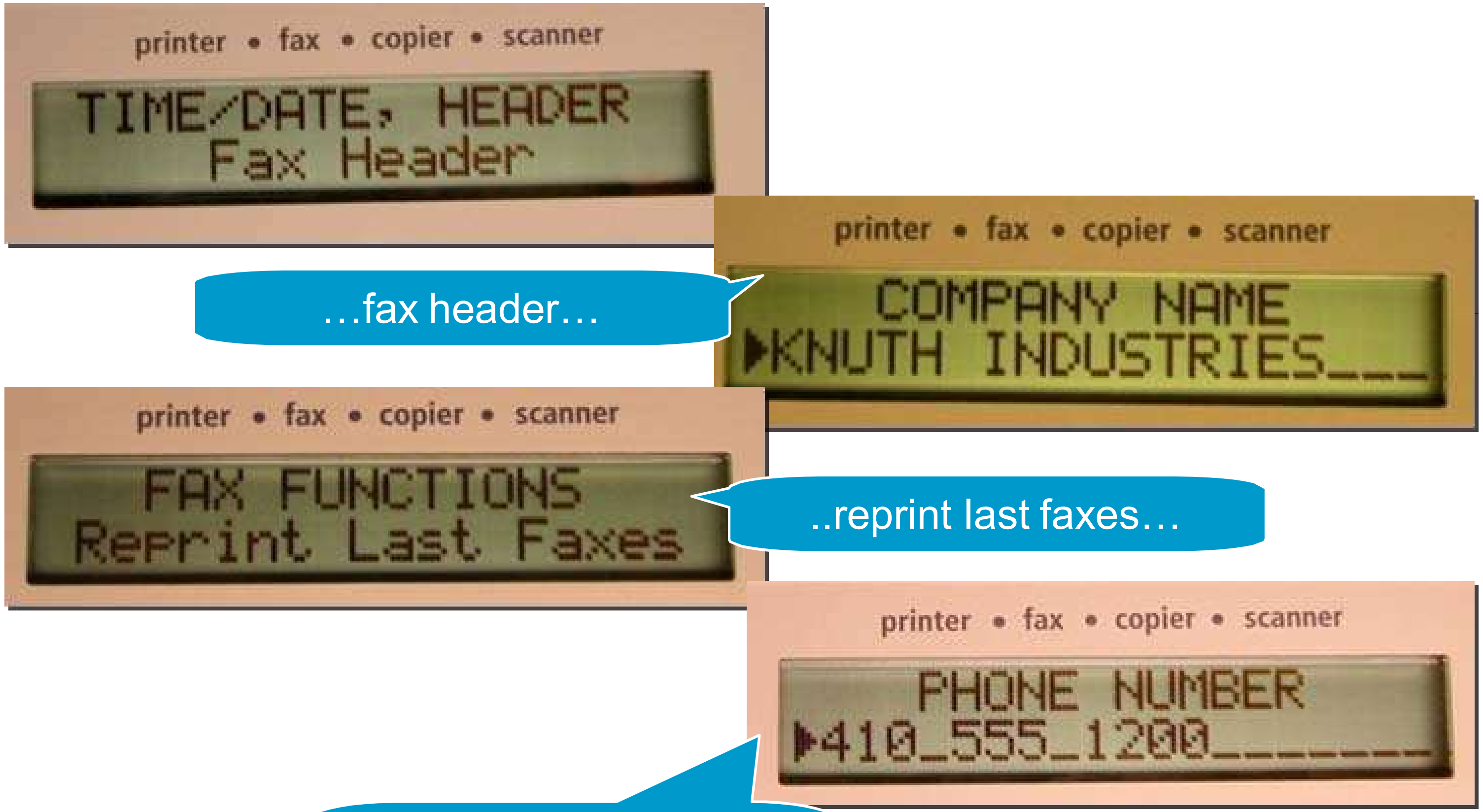
Faxes may contain:

- Event logs
- Fax Logs
- Phonebooks
- Fax Header Info
- Redial Info

Multifunction devices (fax, print, copy, etc) have all this info and more.

- Cached jobs
- Event logs

# Faxes / Multifunction


printer • fax • copier • scanner

```
TIME/DATE, HEADER
  Fax Header
```

…fax header…

printer • fax • copier • scanner

```
  COMPANY NAME
▶KNUTH INDUSTRIES___
```

printer • fax • copier • scanner

```
 FAX FUNCTIONS
Reprint Last Faxes
```

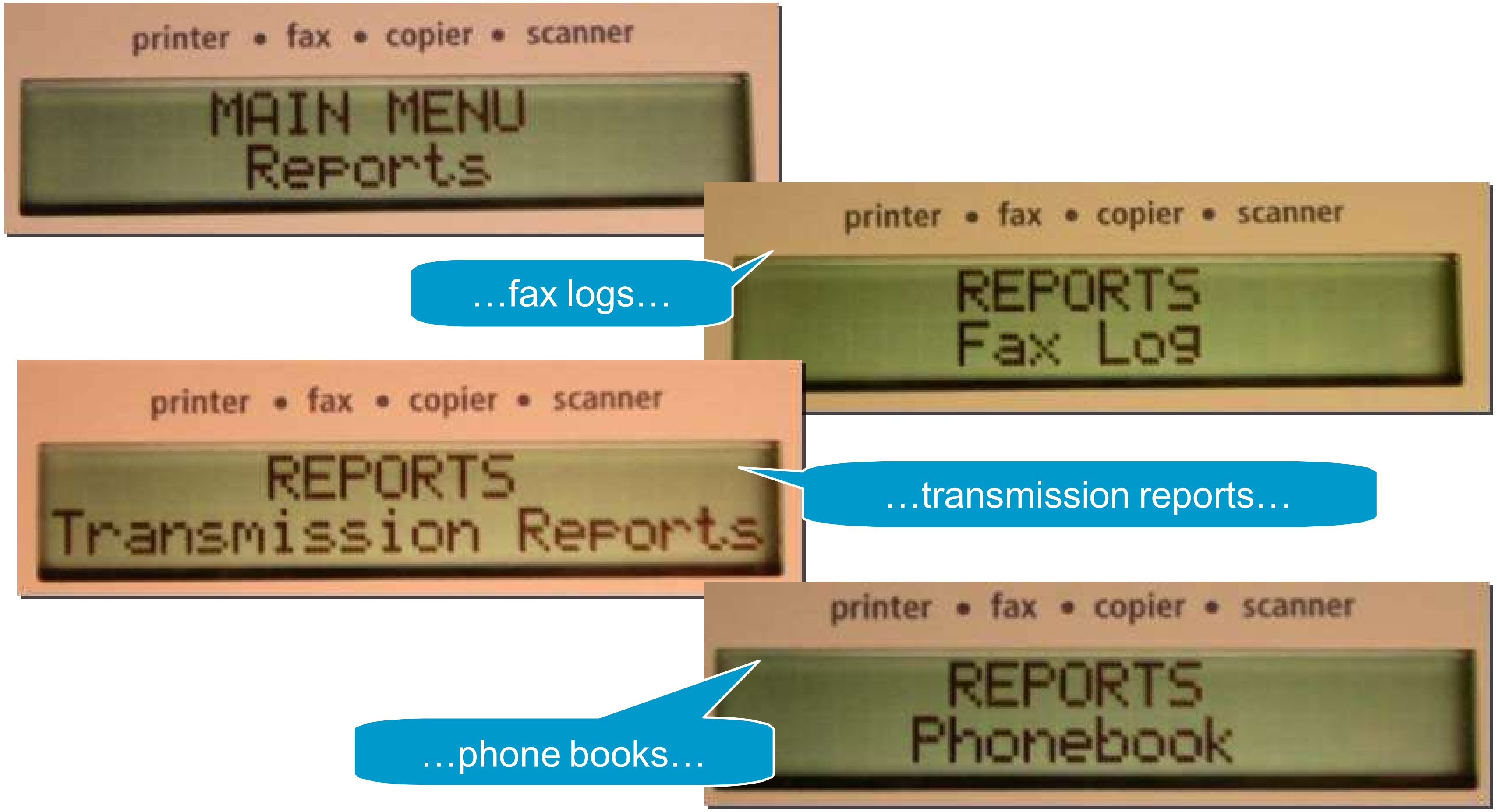
..reprint last faxes…

printer • fax • copier • scanner

```
  PHONE NUMBER
▶410_555_1200_______
```

…local FAX number
(can be fake!)

# Faxes / Multifunction



MAIN MENU
Reports

…fax logs…

REPORTS
Fax Log

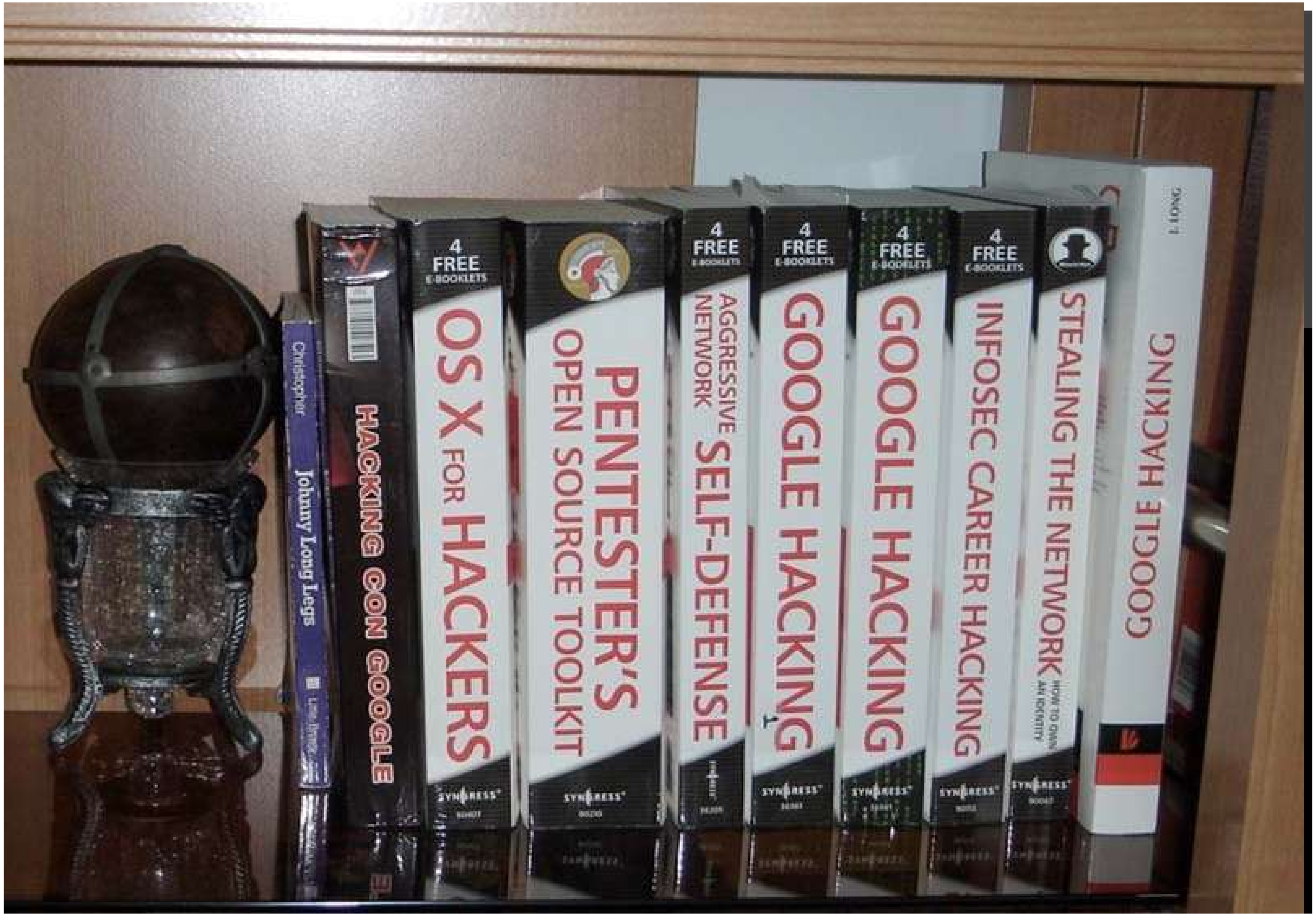
REPORTS
Transmission Reports

…transmission reports…

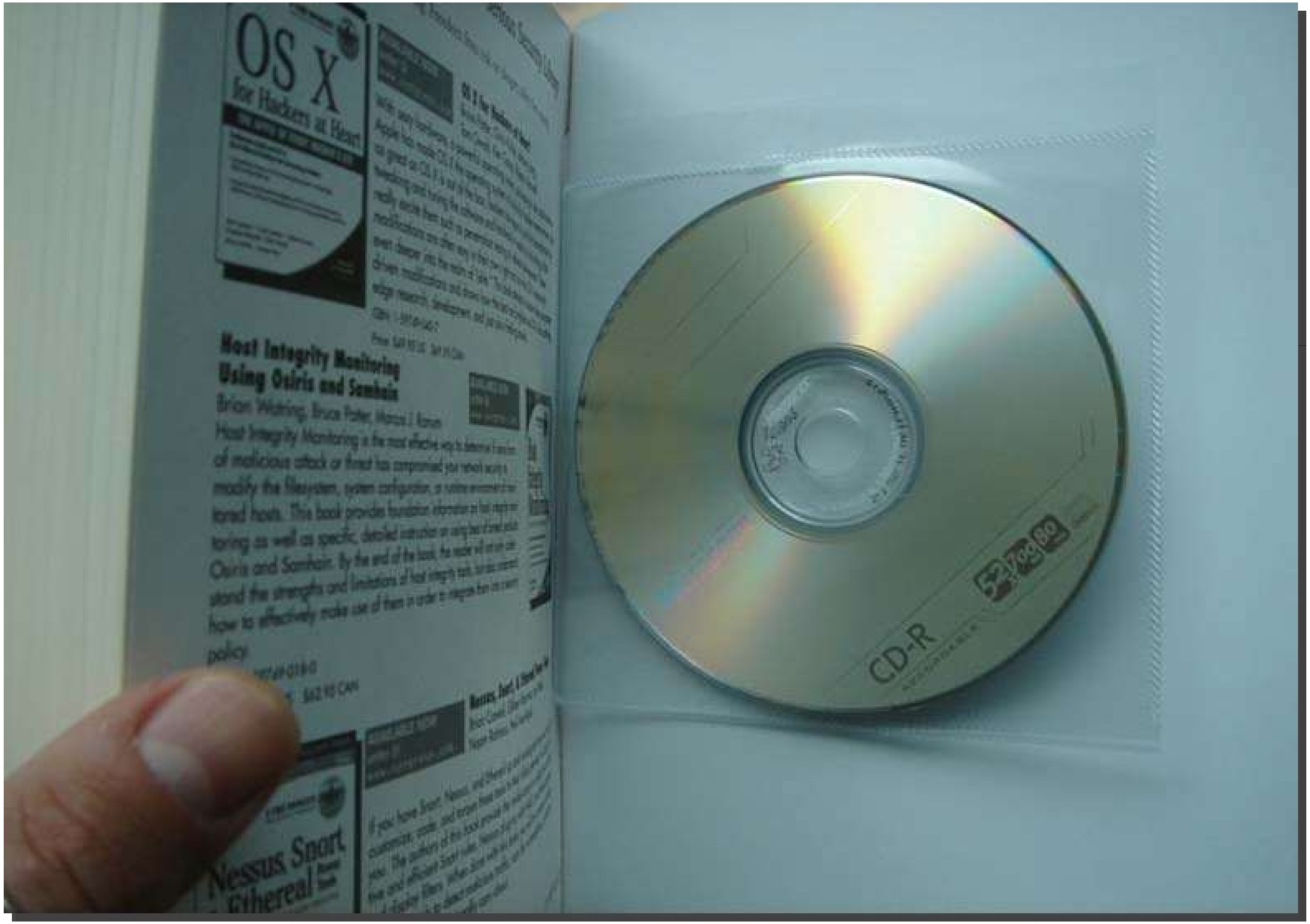
REPORTS
Phonebook

…phone books…

# Take Pictures



# Look for Evidence


OS X for Hackers at Heart
Host Integrity Monitoring Using Osiris and Samhain
Brian Wotring, Bruce Potter, Marcus J. Ranum
Nessus, Snort, & Ethereal
CD-R

# Preparing for Computer Search and Seizure

Find out what to expect

- How many computers?
- What kinds of computers?
- What kind of networking situation?
- What other equipment?

Be ready for the unexpected

- May need to search at location
- May need to take and search later

# Preparing for Computer Search and Seizure

Network danger: computers can be accessed and controlled remotely

Publicity: news of a major operation travels at the speed of the internet