Computer Forensic 101

Dewan Chowdhury

Senior Security Analyst

dnc corp

What put me into this Field?

I was working for some of the biggest Internet backbones on the planet. I was working on the CERT/Incident Handling Team. This stuff gets really boring!!! Seems to repetitive!!!!!

Hacker -> Monitor -> Stop -> Report -> Find the next hacker

Incidents in Private Sector

Majority of the time incidents would be given to “Corporate Security”.

- Not very knowledge
- Not much Power to take legal action
- Disciplinary Action Taken

Government Side

Badge and Gun!!!!! Get to kick down doors and flex your muscle.

- Any crime committed that involves computers, I saw immediate response. Engaged with law enforcement to help with their investigation.

What is Computer Forensic?

Specialized practice of investigating computer media for the purpose of discovering and analyzing available, deleted, or "hidden" information that may serve as useful evidence in a legal matter.

The major types of device can forensic be done on?

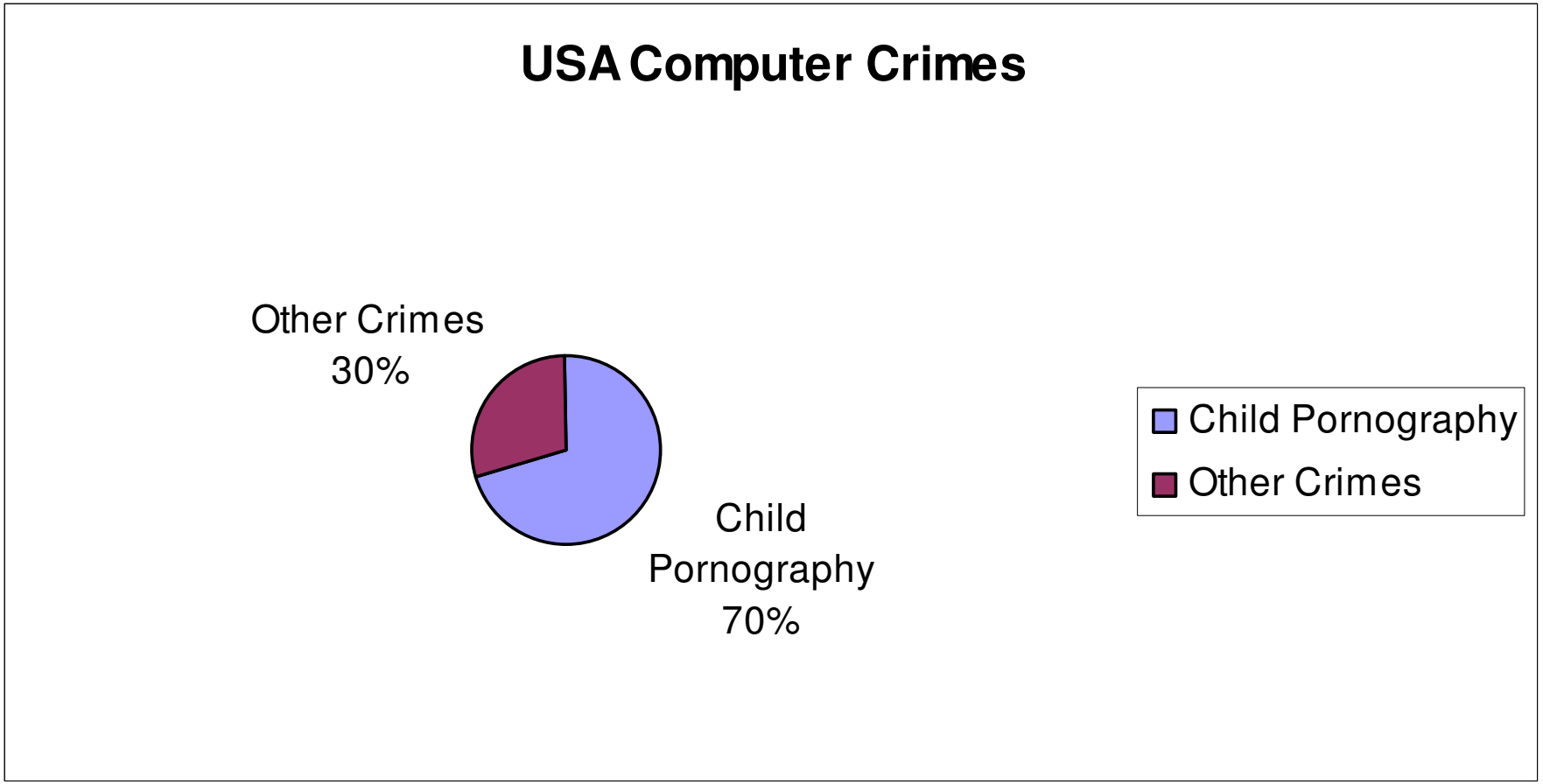
- **Computers**
- **Cell Phone**
- **PDA**

Typical Cases where computer forensic gets involved:

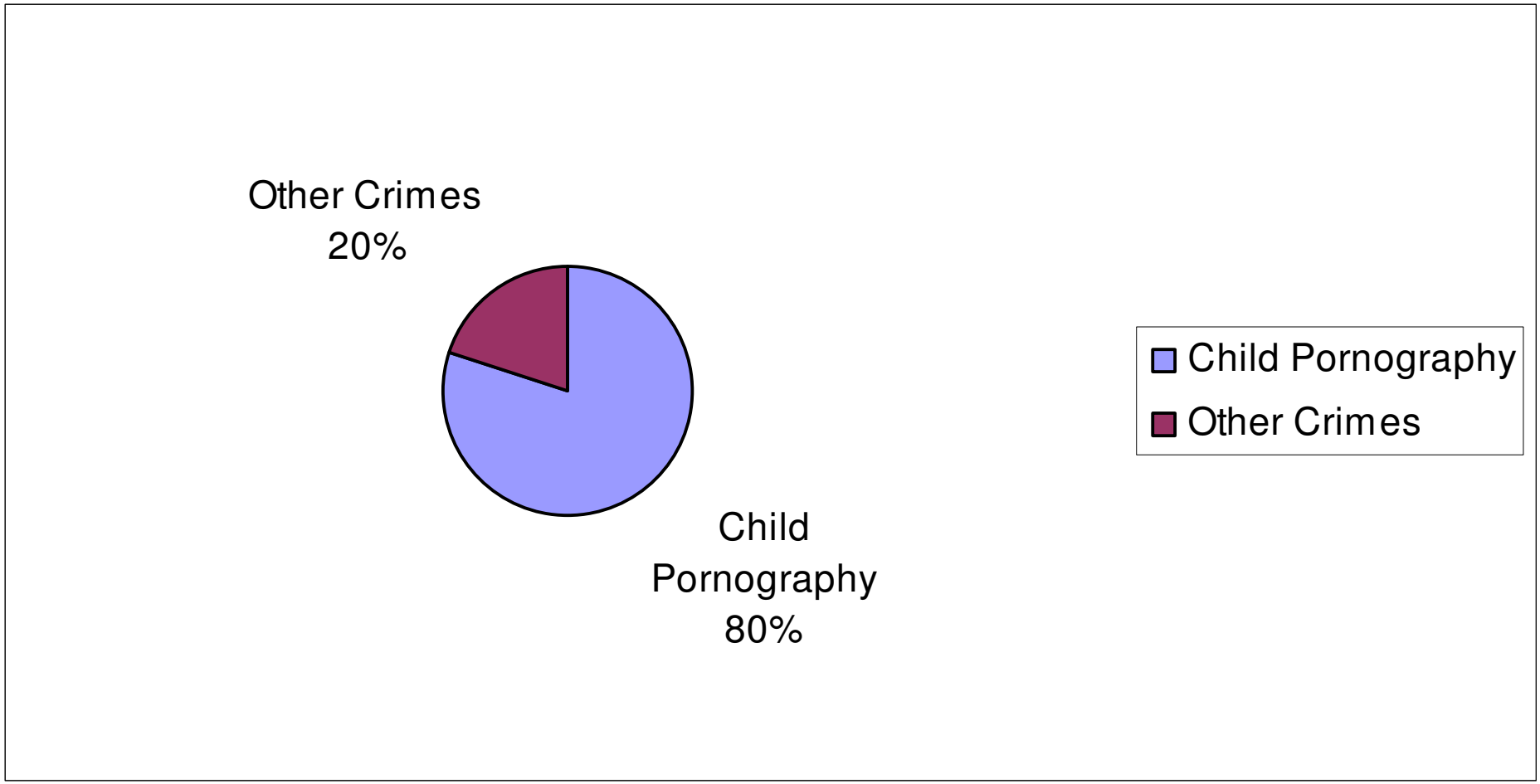
- Industrial espionage
- Money laundering
- Piracy
- Sexual harassment
- Blackmail
- Fraud
- Unauthorized use of a computer
- Child pornography (Normal Pornography as well)

Sad Truth of Computer Crimes

More then ¾ of computer crime that are dealt with by law enforcement agencies involve Child Pornography.


USA Computer Crimes
Other Crimes
30%
Child
Pornography
70%
Child Pornography
Other Crimes

New Zealand Computer Crime



When is the button pushed?

- After incident handling team determines who the suspect is.
- Corporate Security ask for forensic help
- When other investigators need help looking into media.

What You need Before you go!

PRIVATE SECTOR

NOTHING

What You need Before you go!
PUBLIC SECTOR

- WARRANTS!!!!!!!!!!!!!!!!
- WARRANTS!!!!!!!!!!!!!!!!
- Possibly the gun ;)

Time to Break the doors and take the computer! (GOVT.)

- Take pictures of environment
- Record all cables and where they are connected
- Write down info (Serial #/Support #)
- Look for all media around suspect's parameter (CDs, Floppy, Memory Sticket)
- Seize computer or Image on the computer on the spot

Time to Break the doors and take the computer! (Private)

- Take pictures of environment
- Record all cables and where they are connected
- Write down info (Serial #/Support #)
- Look for all media around suspect's parameter (CDs, Floppy, Memory Stick)
- NO RULES APPLIED ON SIEZING SINCE IT BELONGS TO THE COMPANY

Investigator and the Computer

Image the Hard Drive (Encase)

On the Spot or Takeaway

Imaging Techniques

- Computer to Computer
- Imaging Devices

After the Image Capture

- MAKE A BACK UP OF THE IMAGE!!!
- Get a MD5 Hash Value (INTEGRITY)
  - Two Fingerprint
  - What is MD5?
  - The Purpose of MD5 Hash Value

What happens to the Data?

- Everything is just 101000100101 (Binaries)
- 20 4C 69 6D 65 57 69 72 65 2F 34 2E 30 2E 38 20

Deletion of Files

- E5 HEX
- **E5** 4C 69 6D 65 57 69 72 65 2F 34 2E 30 2E 38 20 = **E5**IMEWIRE4.0/.8

Why Doesn’t it get deleted?

- Software programmers are LAZY!!!
- Time Consuming to delete everything from hard drive
- Can I format my computer and be safe?

Examine what type of Case

- Pornography
- Espionage
- Money Fraud
- Hacking

Pornography Approach:

- Look for keywords
- Look for pictures and differentiate them from thumbnail vs. actual clicked pictures
- HASH search for known child pornography
- See what files were deleted!

Espionage

- Look for keywords
- Correlate other logs (IDS/Firewall/etc.) with system file/date
- See what files were deleted!

Good Old Hackers

- 99% are STUPID
- Let me stress more VERY STUPID (Script Kiddies)
- Look for common files

Files & HEX to Look For

- L0phtCrack
- Jack the Ripper
- Netcat
- Bo2k
- Nmap dumps
- Nessus Dumps
- 90909090
- Scanresult
- Scanz
- 411
- Info
- Victim Name

Why is it so easy to get hackers?

- They don’t know the LAW
- They Confess
- Too many other factors point to them
- Associated with Groups

Interesting things to look for

- E-mail addresses
- Instant Messaging Info
- URL history
- Search Query

IDS/Firewall FORENSIC

- Useless without Payload (enable –y in snort!!!)
- Two sources is better then one.

Event Log Forensic

- Domain server logs vs. machine log
- System Events
- Correlate all other logs with time!
- HIDS

Things to Think About

- Insufficient File Info
- Broken up potential evidence
- Thumb Pics

LINKS

- www.fbi.gov - Federal Bureau of Investigations
- www.htcia.org - High Technology Crime Investigation Association
- www.cybercrime.org - National White Collar Crime Center
- Interpol: Forgot the link!

CONTACTS

dewanc@gmail.com