Obtaining and Using Evidence from Social Networking Sites

Facebook, MySpace, LinkedIn, and More

Exemption 6

Lead Computer Forensic Specialist
High Technology Investigative Unit

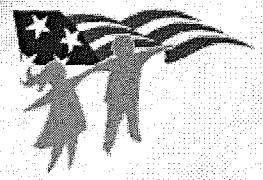
AGENDA

Introduction to Social Networking Sites

Overview of Key Social Networking Sites

How to Collect Forensic Evidence

AGENDA



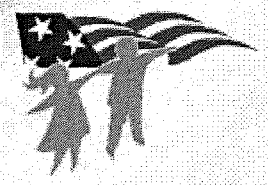
Introduction to Social Networking

Overview of Key Social Networking Sites

Practical Issues

Introduction to Social Networking

THE RISE OF ONLINE SOCIAL NETWORKS



1997	SixDegrees.com
2003	Friendster, LinkedIn
2004	MySpace
2005	Facebook
2008	Twitter

POPULAR SOCIAL NETWORKS

Worldwide: **Facebook**

U.S. and Canada: **MySpace, LinkedIn, Twitter**

Europe: **MySpace, Twitter, Hi5, V Kontakte**

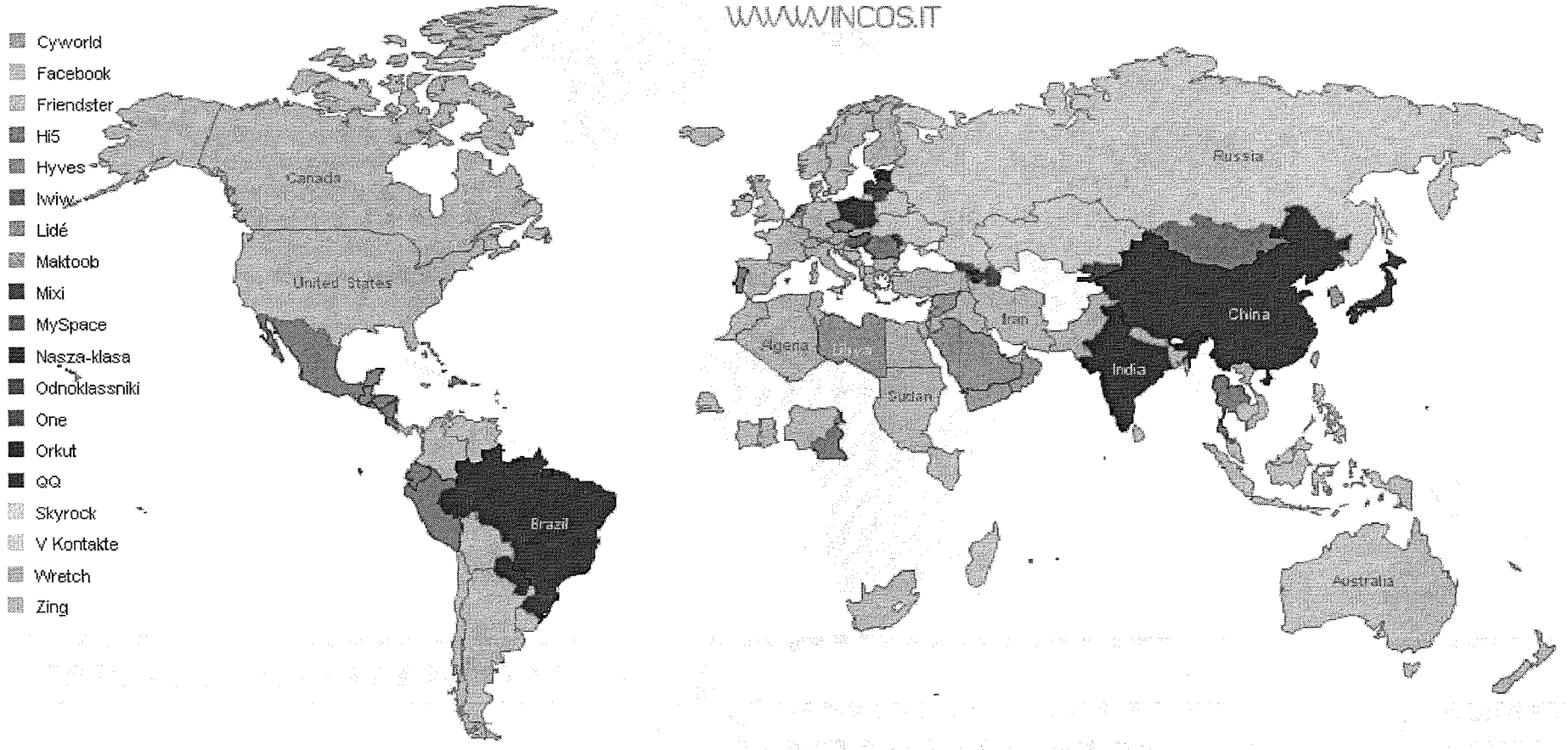
Latin America: **Hi5, Orkut, Tagged**

Asia: **QQ, Friendster, Xiaonei, Orkut, Mixi, Hi5**

Middle East and Africa: **Maktoob, Hi5**

WORLD MAP OF SOCIAL NETWORKS

WWW.VINCOS.IT



Created on Many Eyes (http://many-eyes.com) © IBM

Image courtesy Vincenzo Cosenza (VINCOS.IT), data based on Alexa and Google Trends

POPULARITY IN THE USA

Most-visited websites in the U.S. (August 2009)

1. Google
2. Yahoo
3. Facebook
4. YouTube
5. MySpace

. . .

13. Twitter

. . .

27. LinkedIn

Source: Alexa.com – August 12, 2009 list of Top 100 websites in United States.

THE BASICS

Most social-networking sites allow users to:

- Create personal profiles
- Write status updates or blog entries
- Post photographs, videos, and audio clips
- Send and receive private messages
- Link to the pages of others (i.e., "friends")

How can LE obtain data from these sites?

- Some info may be public
- Use ECPA to get info from providers
- Undercover operations?

UTILITY IN CRIMINAL CASES

Evidence from social-networking sites can

- Reveal personal communications
- Establish motives and personal relationships
- Provide location information
- Prove and disprove alibis
- Establish crime or criminal enterprise

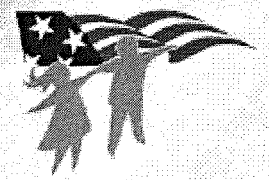
Also: instrumentalities or fruits of crime.

AGENDA

Introduction to Social Networking

Overview of Key Social Networking Sites

How to Collect Forensic Evidence



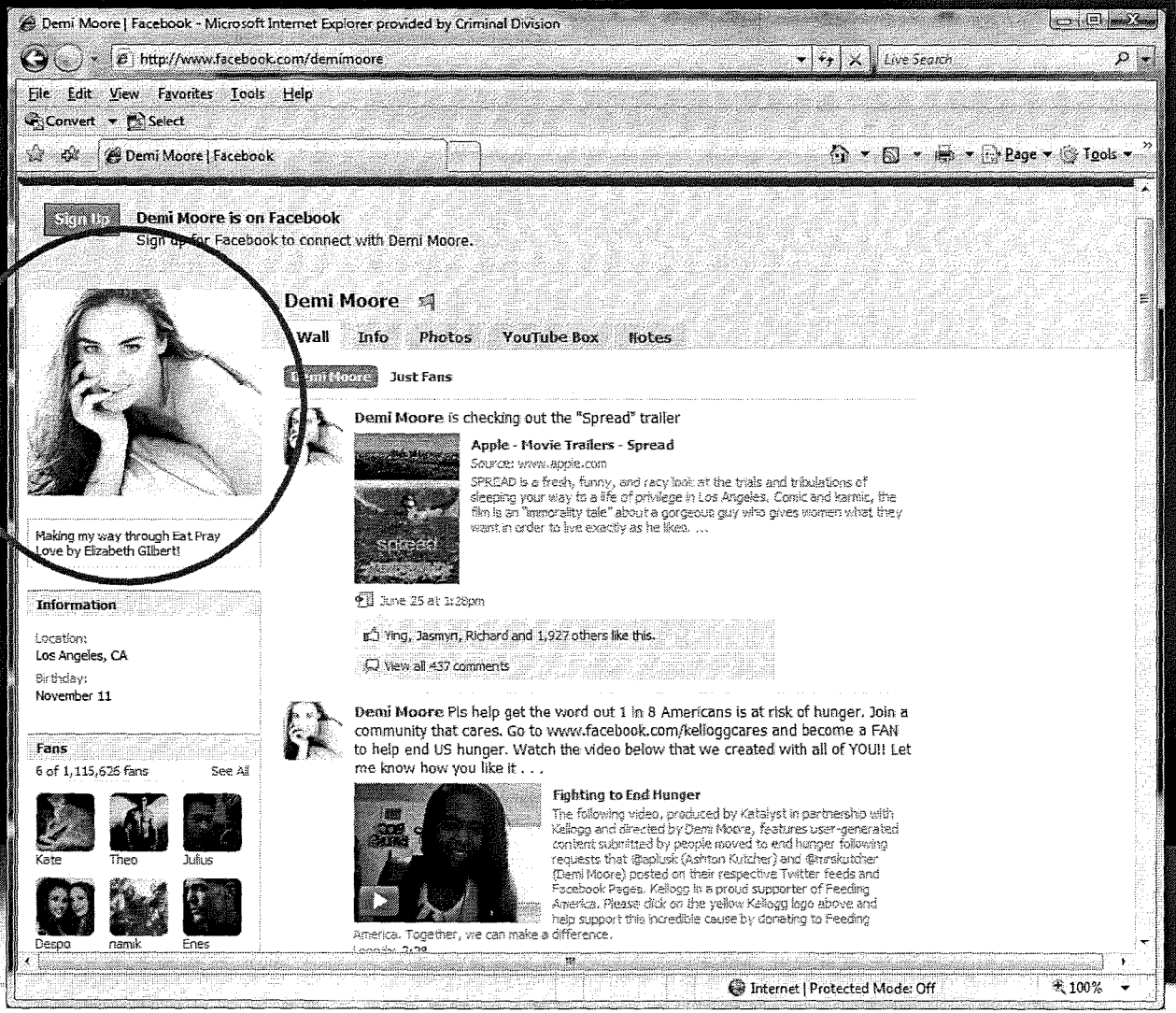
Overview of Key Social Networking Sites

FACEBOOK

- Founded in 2004, primarily catering to students
- Now over 250m active members worldwide
- Over 10b photos in Oct 2008; adds over 1b monthly
- Applications run on Facebook platform
- True names encouraged but not guaranteed
- Privacy model is highly granular; present different information to different groups or individual users
- Messaging includes mail, real-time chat, "wall"
- Now used in private background checks
- Koobface – virus/worm v

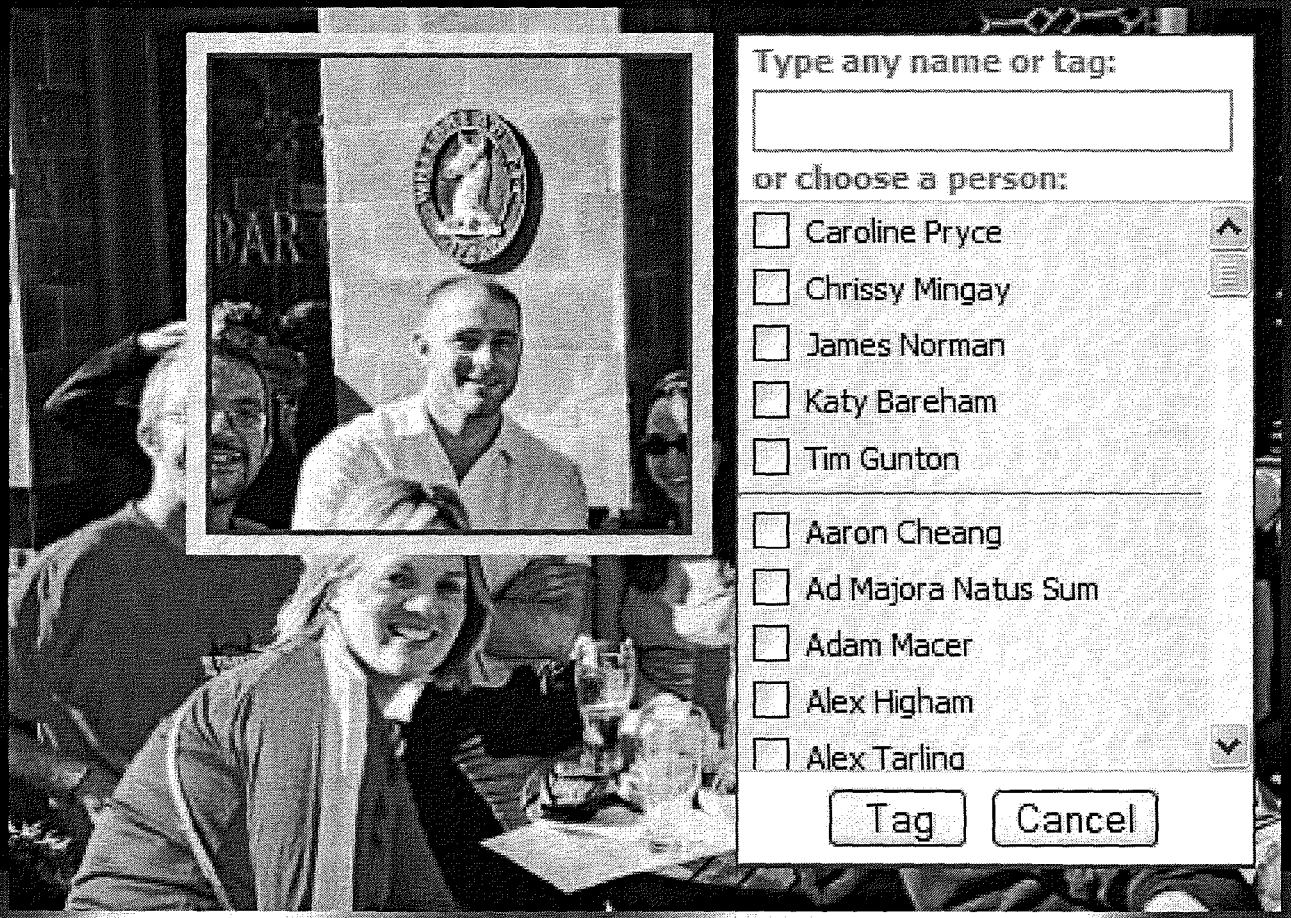
Overview of Key Social Networking Sites

FACEBOOK



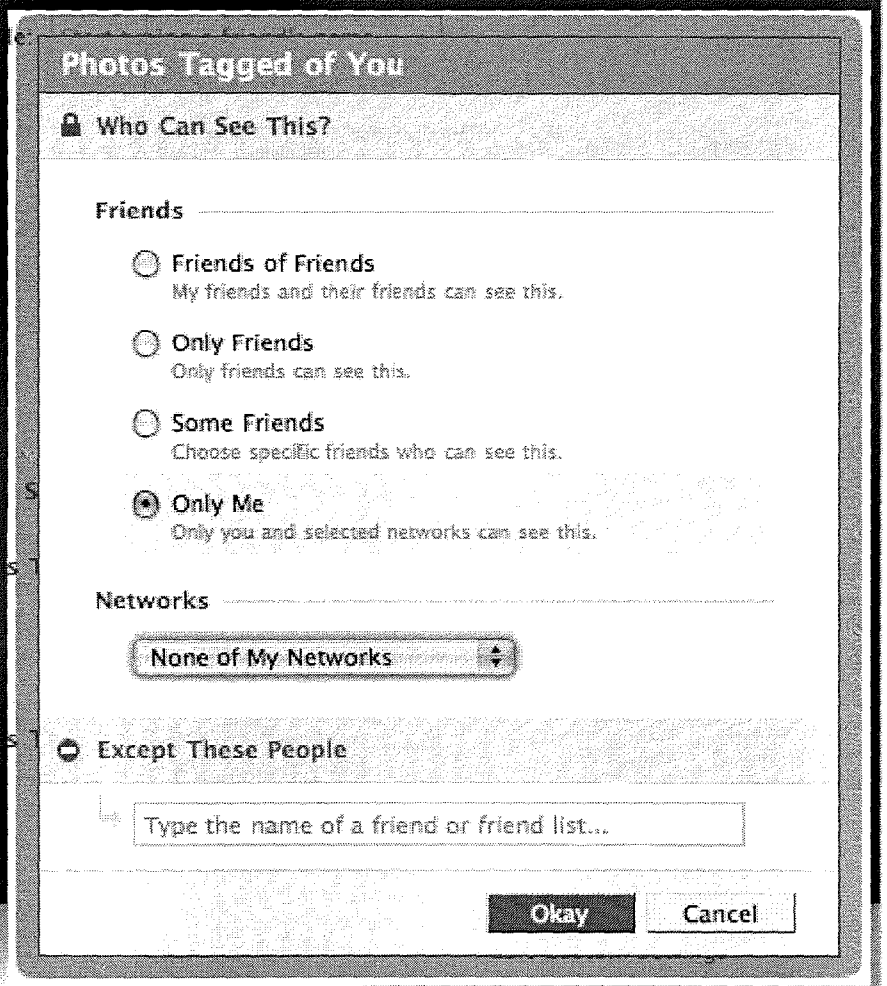
Overview of Key Social Networking Sites

FACEBOOK



Overview of Key Social Networking Sites

FACEBOOK



Overview of Key Social Networking Sites

GETTING INFO FROM FACEBOOK

Data is organized by user ID or group ID

Standard data productions (per LE guide):

Neoprint, Photoprint, User Contact Info, Group Contact Info, IP Logs

HOWEVER, Facebook has other data available.

Often cooperative with emergency requests.

Overview of Key Social Networking Sites

MYSPACE

Founded 2003, now owned by Fox Interactive Media

2006: Most popular SN; passed by Facebook in 2008

Currently tens of millions of active users monthly

True names less encouraged than Facebook

Messaging through messages, chat, friend updates

Application platform rolled out early 2008

Young user base, history of child safety concerns

Privacy is currently less granular than Facebook

Overview of Key Social Networking Sites

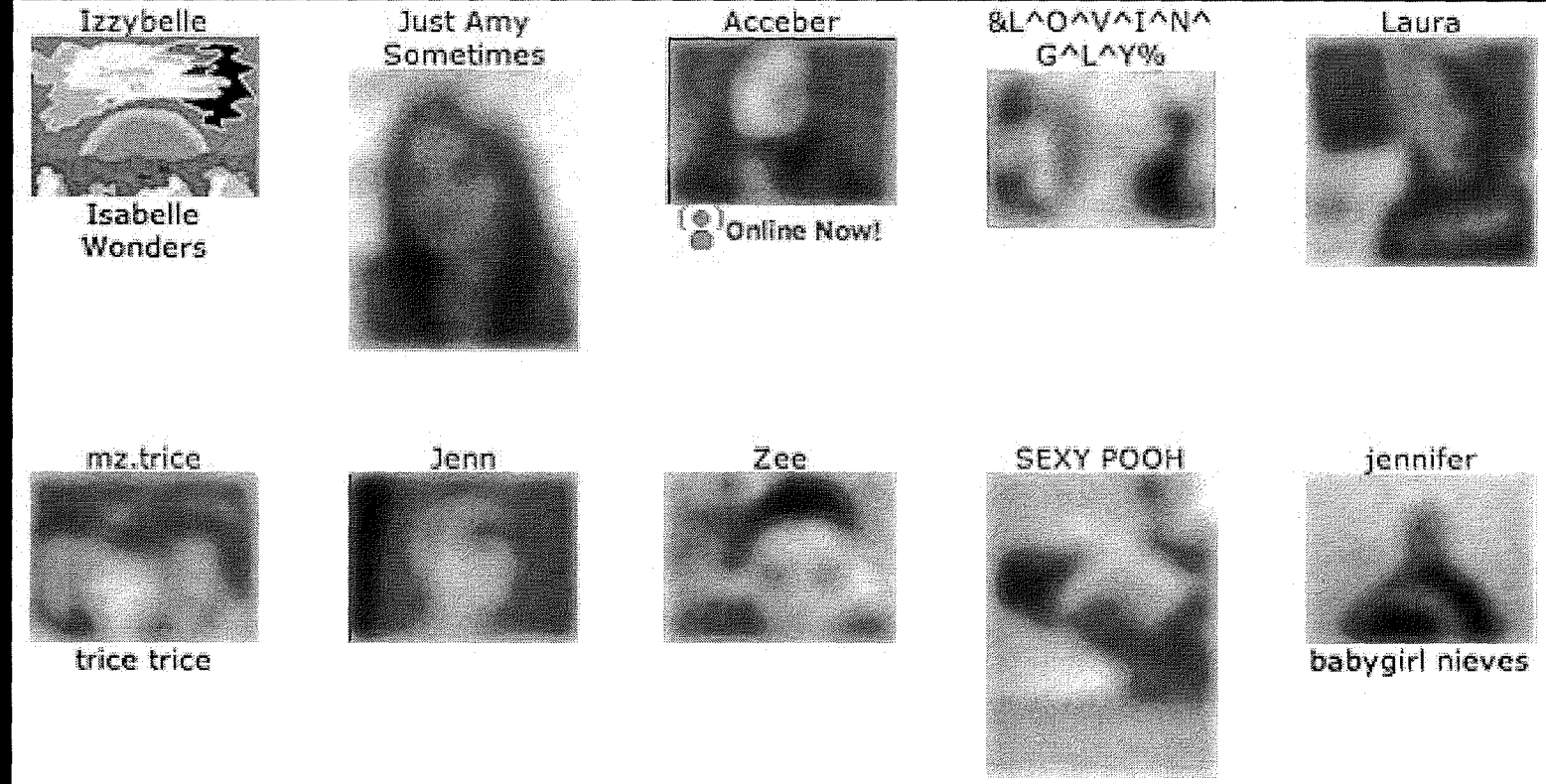
MYSPACE

Overview of Key Social Networking Sites

MYSPACE

Overview of Key Social Networking Sites

MYSPACE



Overview of Key Social Networking Sites

SECOND LIFE

Overview of Key Social Networking Sites

GETTING INFO FROM MYSPACE

Many profiles have public content.

Data is organized by FriendID – see LE guide.

MySpace requires a search warrant for private messages/bulletins less than 181 days old

- Also considers friend lists to be stored content

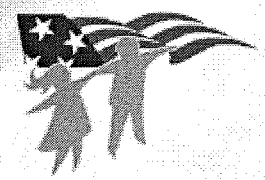
Data retention times

User info and stored files – indefinitely

IP logs, info for deleted accounts – 1 year

Overview of Key Social Networking Sites

TWITTER



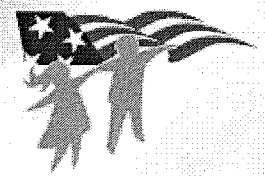
- Market leader in "micro-blogging"
- Began in mid-2006 as "status message" service
- Ubiquity and ease of updating, but limited space
- Breaking news, real-time updates: USAir, Iran
- Most multimedia handled by 3d party links
- Simplified privacy model: updates public or private
- Direct messages are private; sender can delete
- Short URLs used to serve malicious links and code

Overview of Key Social Networking Sites

TWITTER

Overview of Key Social Networking Sites

GETTING INFO FROM TWITTER



The good news

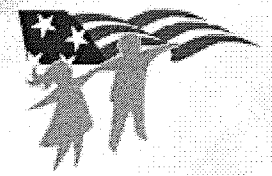
- Most Twitter content is public
- Private messages kept until user deletes them

The bad news

- No contact phone number
- Only retain last login IP
- Will not preserve data without legal process
- Stated policy of producing data only in response to legal process (i.e., no 2702)
- No Law Enforcement Guide

Overview of Key Social Networking Sites

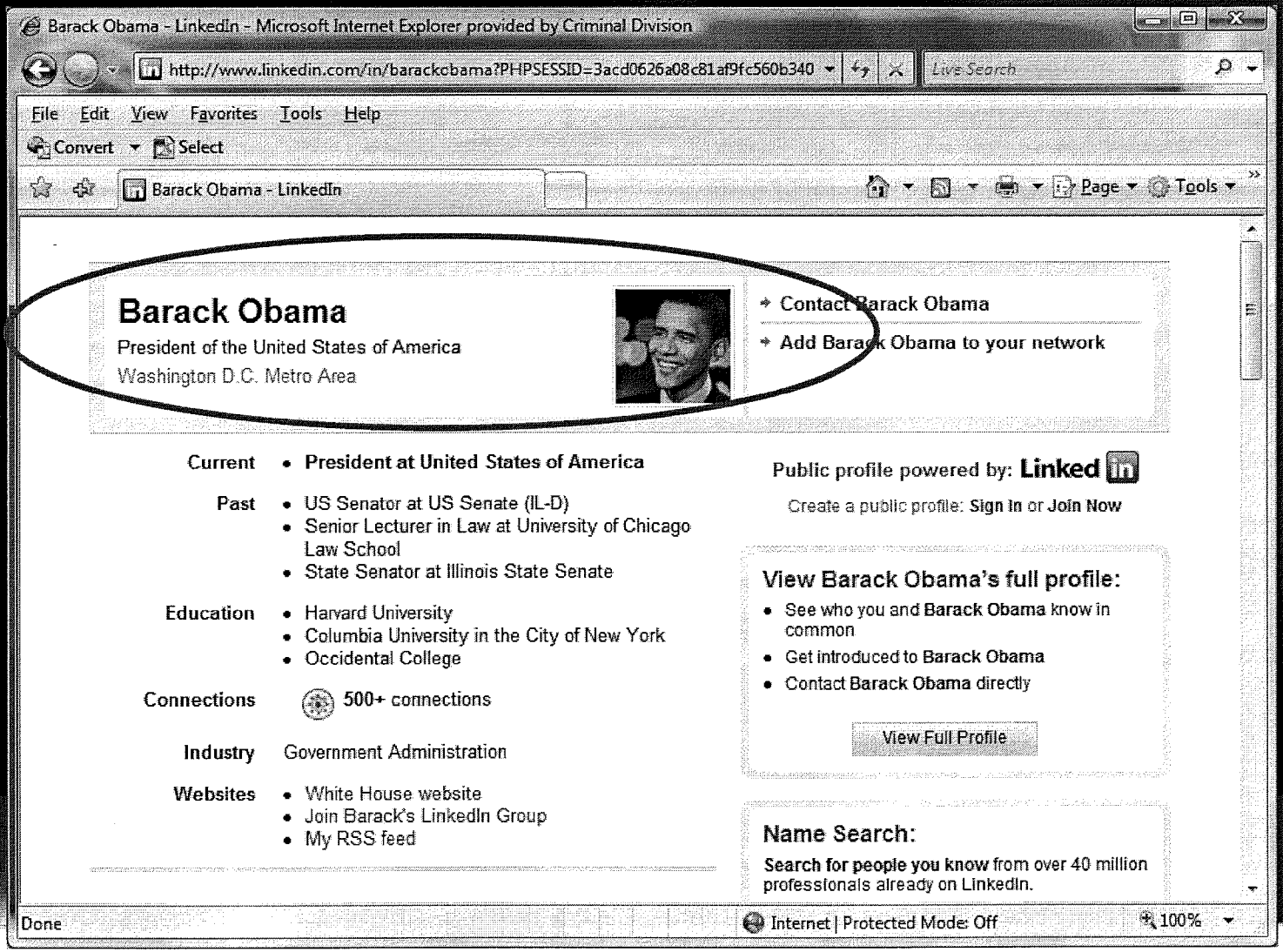
LINKEDIN



- Business-focused with enforced limits to interaction
- Profiles focused on education and work experience
- Use for criminal communications appears limited
- But can be used to identify experts
- Can check background of defense experts
- Privacy model similar to Facebook
- Profile information is not checked for reliability

Overview of Key Social Networking Sites

LINKEDIN



AGENDA

Introduction to Social Networking

Overview of Key Social Networking Sites

How to Collect Forensic Evidence

Legal Process

- Following law enforcement guide aka legal compliance guide
- TIME is critical → move on preservation orders
  - E.g. Woogie account on MySpace

Item #9

"Obtaining and Using Evidence From Social Networking Sites" PowerPoint Slides

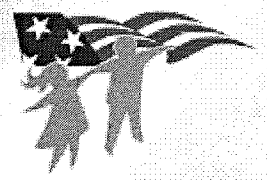
~~~~~

4 Pages Withheld In Full

Pursuant to FOIA Exemption 7(E)
~~~~~

Practical Issues

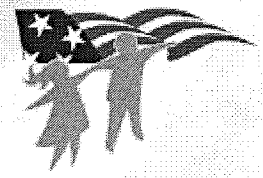
SW ON COMPUTER SYSTEM



- Computer Forensics will identify past communications
- Corroborate UC communications
- Identify additional leads (National Ops)

Practical Issues

WITNESSES & SOCIAL NETWORKS



Many witnesses have social-networking pages

- **Valuable source of info on defense witnesses**
- **Potential pitfalls for government witnesses**

Knowledge is power

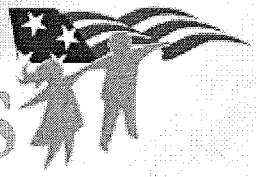
- **Research <u>all</u> witnesses on social-networking sites**
- **Discovery obligations?**

Advise your witnesses:

- **Not to discuss cases on social-networking sites**
- **To think carefully about what they post**

Practical Issues

OTHER COURTROOM ISSUES



Social networking and the courtroom can be a dangerous combination

- Use caution in "friending" judges, defense counsel
- Warn jurors about social-networking sites

Social networking + mobile devices = real-time updates on courtroom events

Item #9

"Obtaining and Using Evidence From Social Networking Sites" PowerPoint Slides

~~~~~

1 Page Withheld In Full

Pursuant to FOIA Exemption 6
~~~~~