Forensic Investigation of Peer-to-Peer File Sharing Networks

Marc Liberatore[1] Robert Erdely[2] Thomas Kerle[3]
Brian Neil Levine[1] Clay Shields[4]

[1]University of Massachusetts Amherst

[2]Pennsylvania State Police

[3]Massachusetts State Police

[4]Georgetown University

Digital Forensics Research Conference (DFRWS 2010)

UMASS AMHERST

Take-Home Messages

- The most active venue for trafficking of child pornography is p2p networks, and it is a serious concern of law enforcement.
- If done correctly, P2P protocols provide enough information to successfully investigate criminal acts.
- We built an investigator-friendly p2p client, RoundUp, wrote training materials, and have trained nearly 1,000 investigators.
- RoundUp reports to a central DB, which allows investigators to pool results. At least 3,000 investigations are ongoing, with hundreds of arrests.

Outline

Motivation

2001: 1,713 arrests for child pornography possession in US
2006: 3,672 arrests

June 2010: 61,169 p2p users observed sharing child pornography

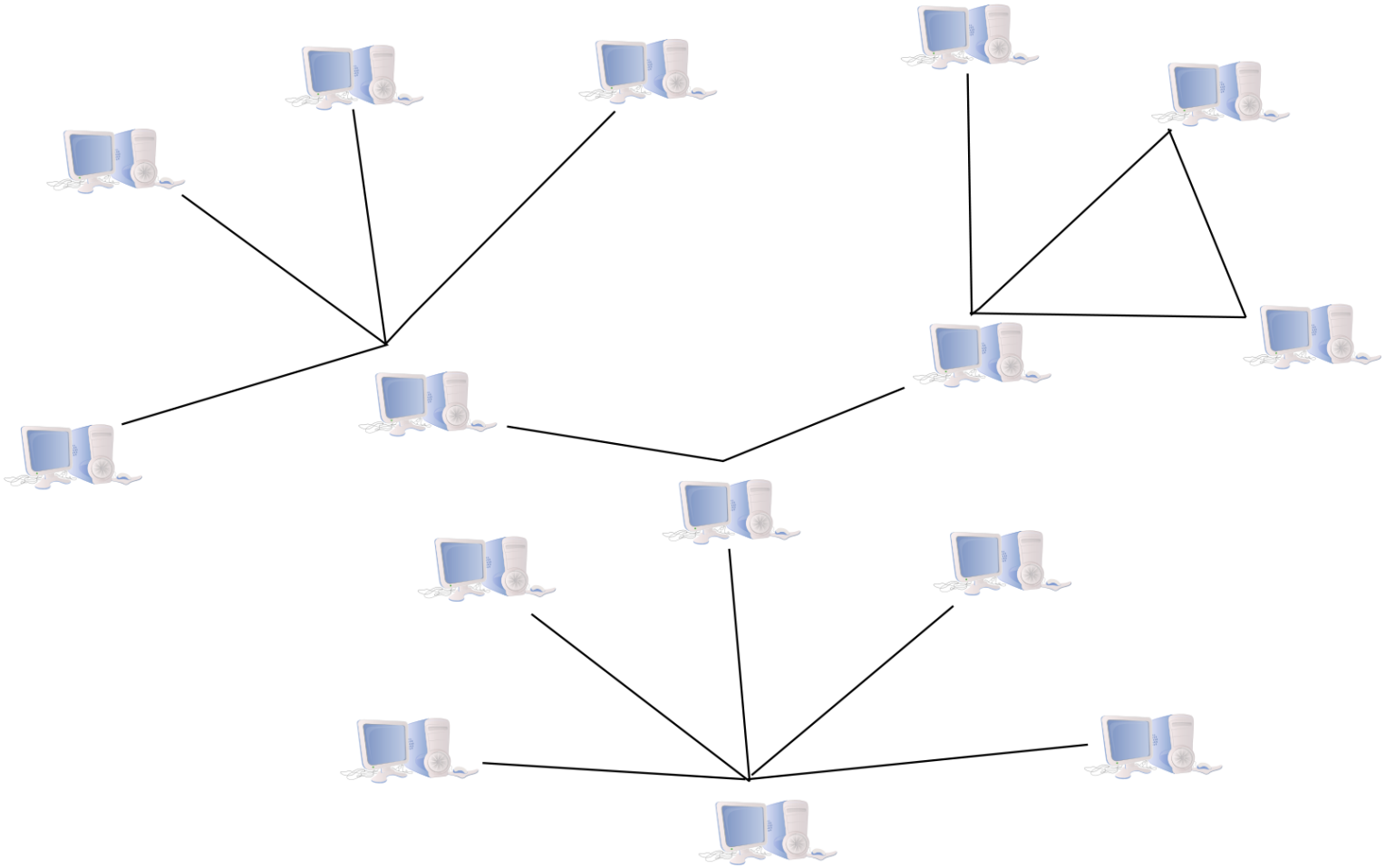
Past studies [Wolak, et al.] have found:

- 21% of possessors had images of extreme violence
- 28% had images of children under three

16% of investigations ended with discovery of a contact offender

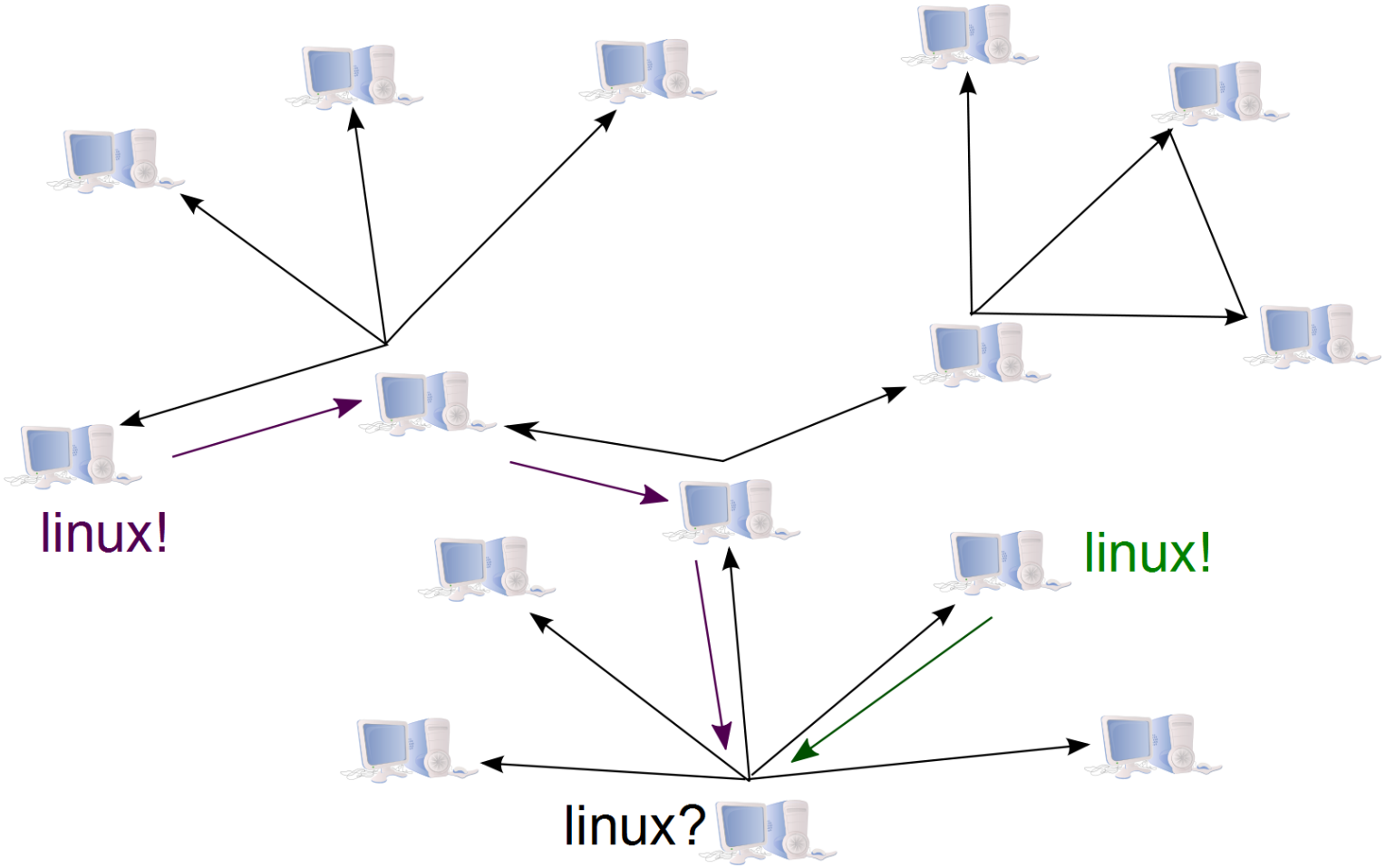
Gnutella
Overview

Gnutella is a decentralized protocol for file search and sharing.



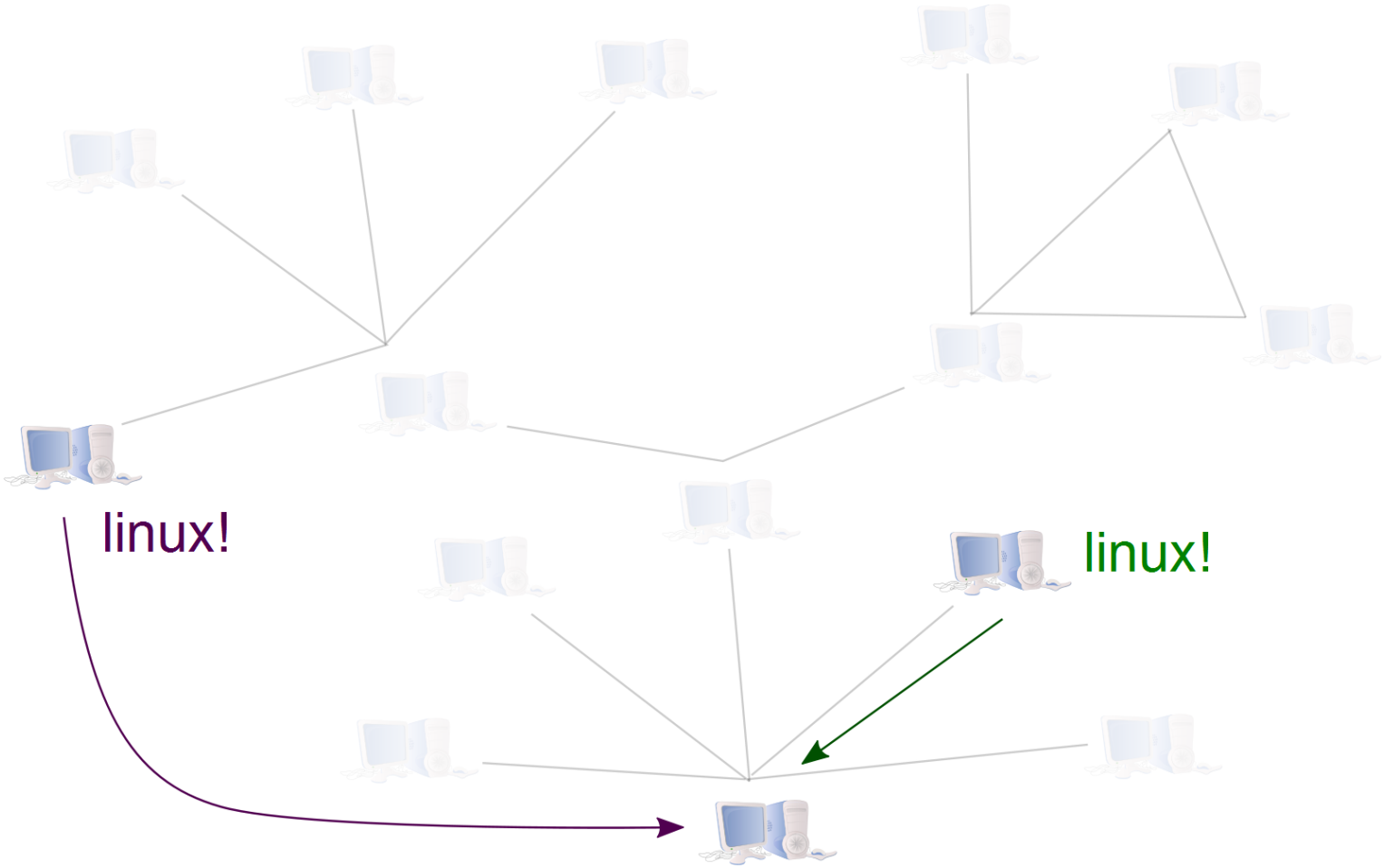
Gnutella
Searching

Queries are broadcast; searches are routed.



Gnutella
Downloading

Downloads are direct TCP connections between peers.



Finding Candidates

Goal

Find evidence of a crime through observations on the Internet.

Evidence:

- may be direct or hearsay
- includes files of interest, hash values, filenames
- is ultimately associated with a user (IP address? GUID?)

Use the p2p system to find candidates for further investigation.

Evidence

A candidate is chosen for further investigation, by jurisdiction, type/quantity of files, observed history.

The investigator directly connects to:

- determine all files shared by a peer
- find other corroborating evidence (IP, GUID, vendor id)
- perform a single-source download

Subpoena and Search Warrant

Network investigation done; shoe-leather work remains:

- Subpoena ISP for DHCP records / billing information
- Search warrant for premises — written broadly

Once on site, examine media and seize if appropriate.

Legal / Technical Issues

Main Concern

Law enforcement investigators must not break the law!

Aside from liability, US has a "Fruit of the Poisonous Tree" doctrine. Other issues:

- 4th Amendment
- Kyllo v US
- Encryption
- "No uploads" interacts poorly with tit-for-tat

Results
Observed Candidates

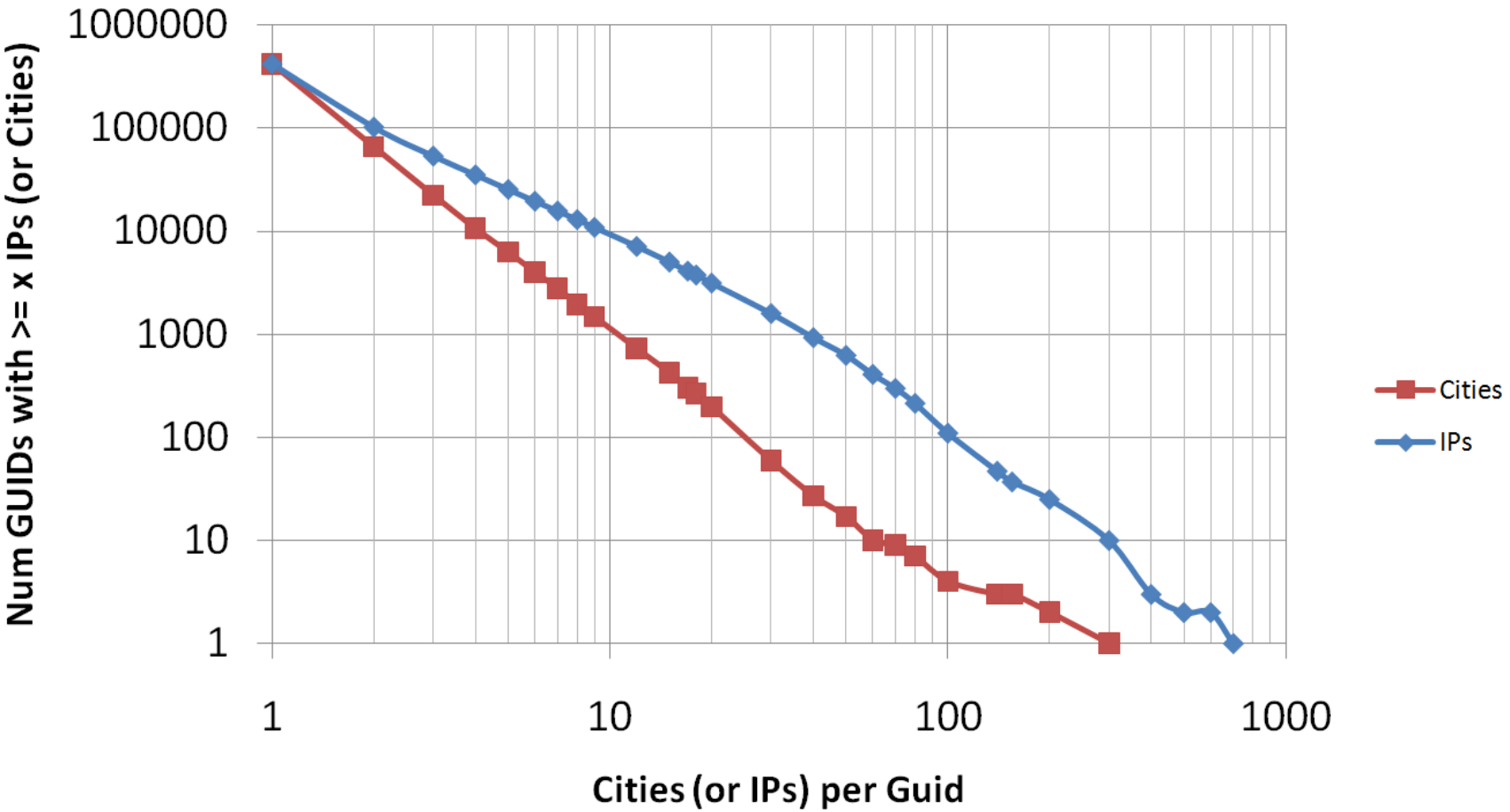
Month	Global Records	US Records	US IPs	US GUIDs
2010 Jan	24,391,816	7,584,534	127,440	65,890
Feb	20,132,466	6,254,073	127,161	68,572
Mar	29,716,269	9,353,050	127,035	55,481
Apr	27,231,255	8,444,572	107,880	45,620
May	29,626,273	8,957,398	117,194	47,822
Jun	21,630,795	9,834,193	136,481	61,169

Results

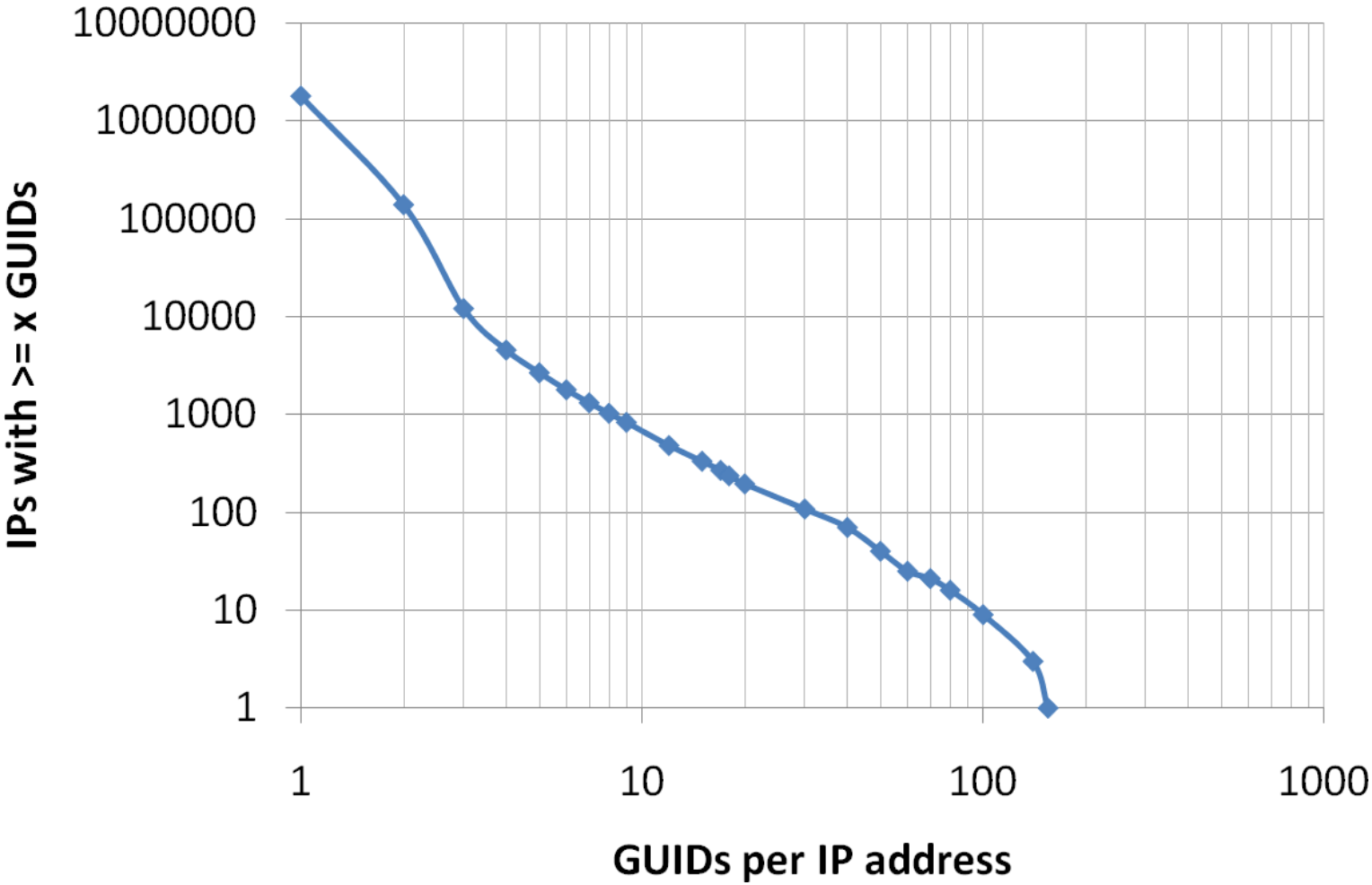
Investigators and Results in the US

Date	Investigators	Task Forces	Cases	Searches	Arrests
2009 Oct	102	<20	748	242	15
Nov	429	28	875	316	57
Dec	472	48	1,096	367	93
2010 Jan	502	51	1,291	471	144
Feb	587	52	1,606	558	193
Mar	665	52	1,862	682	233
Apr	712	52	2,065	791	282
May	915	56	2,395	905	349
Jun	974	58	2,762	995	406

IPs per GUID


1000000
100000
10000
1000
100
10
1
Num GUIDs with >= x IPs (or Cities)
1
10
100
1000
Cities (or IPs) per Guid
Cities
IPs

GUIDs per IP


10000000
1000000
100000
10000
1000
100
10
1
IPs with >= x GUIDs
1
10
100
1000
GUIDs per IP address

Lessons Learned

- Things that are straighforward to computer scientists are surprising to police (push proxies), and vice versa (use of search warrants).
- Finding knowledgable partners was key to our success. Luck favors the prepared.
- Usability is key for rapid technology transfer.

Breaking News

Yesterday, DOJ released the first " National Strategy to Combat Child Exploitation, Prevention and Interdiction" at `http://www.projectsafechildhood.gov/docs/natstrategyreport.pdf`.

RoundUp is mentioned prominently as a tool used to identify and investigate CP traffickers.

Summary

- Successful p2p investigation requires knowledge of the law and of p2p protocols.
- RoundUp's success is due to academics: wringing maximum evidentiary value from the protocol.
- RoundUp's success is due to LE personnel: willing to guide tool development and to function as ambassadors.

Acknowledgments

This work was supported in part by National Institute of Justice Award 2008-CE-CX-K005 and in part by the National Science Foundation awards CNS-0905349 and DUE-0830876. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect those of their employers, the U.S. Department of Justice, or the National Science Foundation.

UMASS AMHERST