

Forensic Investigation of Peer-to-Peer File Sharing Networks

Marc Liberatore¹ Robert Erdely² Thomas Kerle³
Brian Neil Levine¹ Clay Shields⁴

¹University of Massachusetts Amherst

²Pennsylvania State Police

³Massachusetts State Police

⁴Georgetown University

Digital Forensics Research Conference (DFRWS 2010)



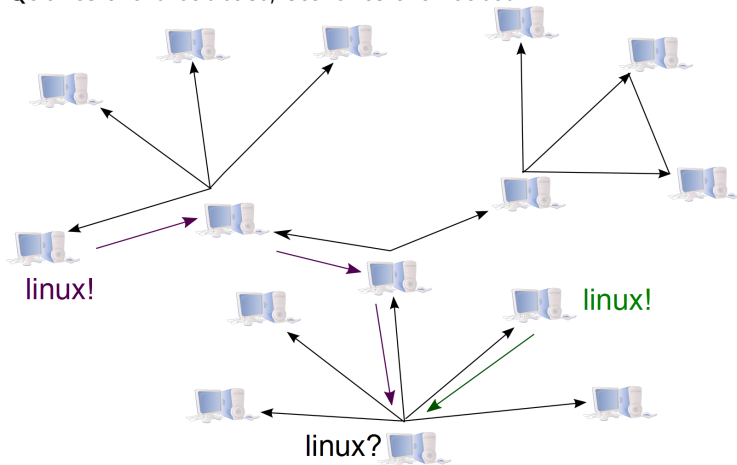
Outline

- 1 Motivation
- 2 P2P Overview
- 3 Investigations and Legal Issues
- 4 Results and Tool

Gnutella

Searching

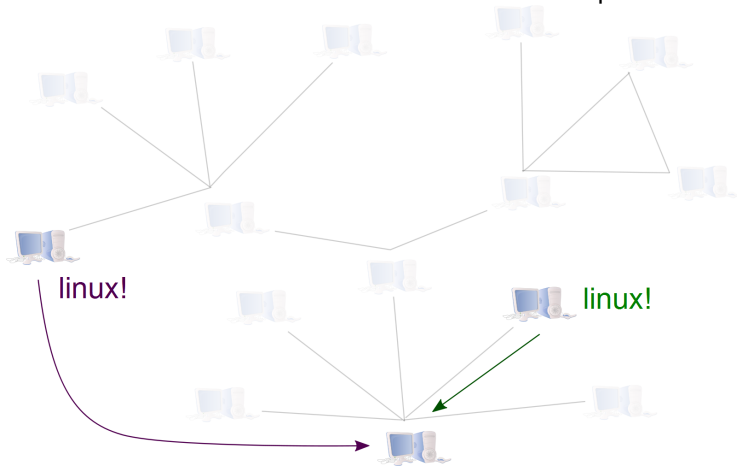
Queries are broadcast; searches are routed.



Gnutella

Downloading

Downloads are direct TCP connections between peers.



Results

Observed Candidates

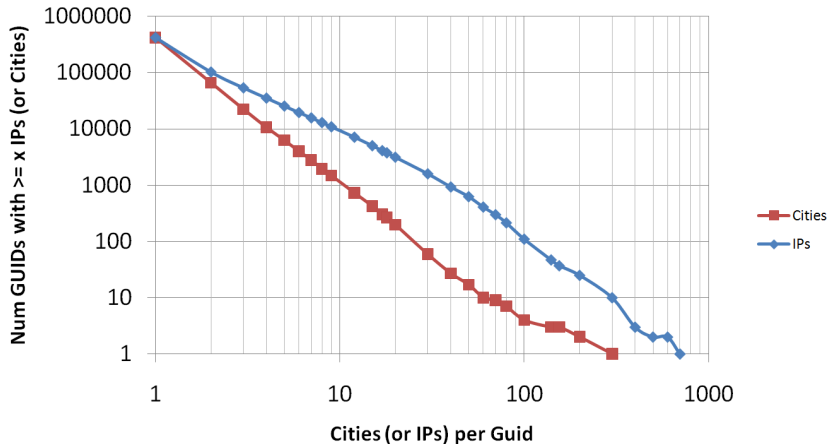
Month	Global Records	US Records	US IPs	US GUIDs
2010 Jan	24,391,816	7,584,534	127,440	65,890
Feb	20,132,466	6,254,073	127,161	68,572
Mar	29,716,269	9,353,050	127,035	55,481
Apr	27,231,255	8,444,572	107,880	45,620
May	29,626,273	8,957,398	117,194	47,822
Jun	21,630,795	9,834,193	136,481	61,169

Results

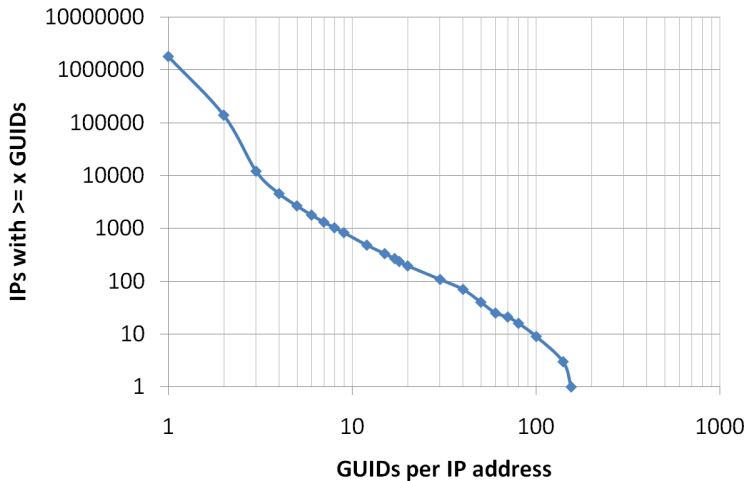
Investigators and Results in the US

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



GUIDs per IP



Lessons Learned

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

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.