

# BitPredator: Discovery Algorithm for BitTorrent Initial Seeders and Peers

Raymond C. Borges Hink

Polytechnic University of Puerto Rico

Research Alliance in Math and Science

Computational Sciences and Engineering Division, Oak Ridge National Laboratory

Mentors: Dr. Robert Patton and Dr. Houssain Kettani

<https://sites.google.com/site/rams2011borgesraymond>

## Introduction

- BitTorrent Peer-to-Peer (P2P) protocol used for file sharing
- Content massively distributed in BitTorrent networks determined mostly illegal goes untraced
- Methodology to accurately profile initial content producers and peers needed

## Background

- Oak Ridge National Laboratory partnered with law enforcement agencies and PROTECT
- Child predator monitoring framework to be developed via RAMS and Polytechnic University of Puerto Rico collaboration

## Objectives

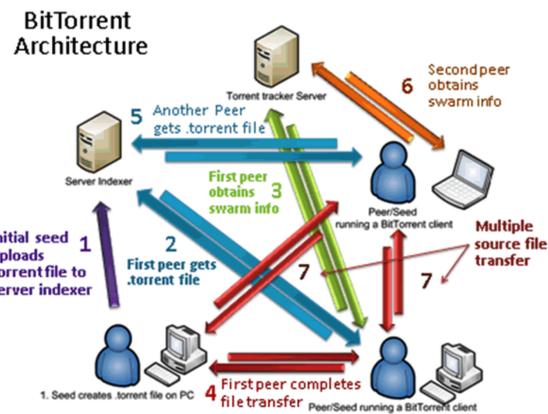
Main objective:

Establish methodology that automatically identifies initial seeders and peers

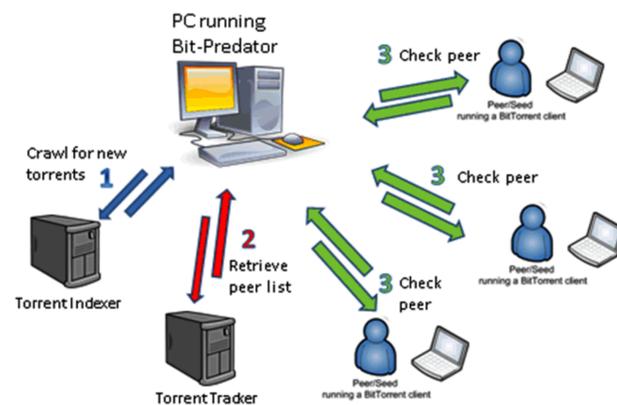
Goals:

- Track torrent indexing sites
- Identify specific content
- Query torrent tracker servers
- Filter out fake IP's addresses
- Verify IP addresses in peer lists
- Print reports with initial seeder IP addresses with dates and times
- Map IP's to Google Maps

## BitTorrent Protocol



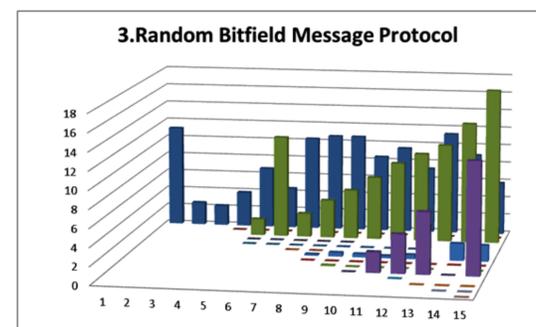
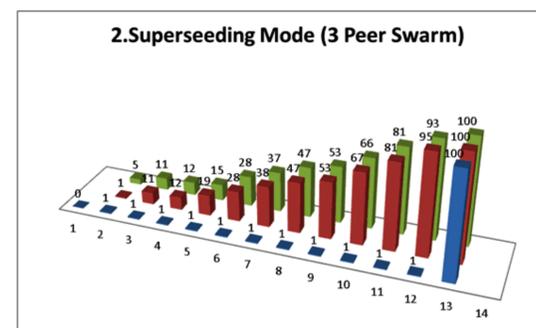
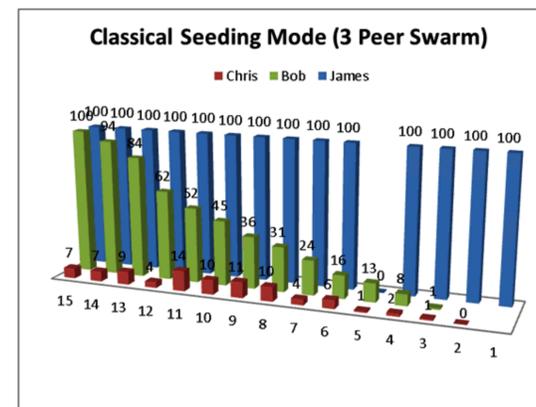
## Methodology



## Experimental Results

Three experiments were carried out to track initial seeders and peers using:

- Classical BitTorrent seeding protocol
- Superseeding BitTorrent protocol
- Random bitfield message protocol



## Main Results

- Torrents captured before file is shared completely once will yield initial seeder 100% of the time
- The fastest transfer is given by: 
$$\frac{\text{filesize}(\text{bytes})}{\text{floor}(\text{peer speeds})\left(\frac{\text{bytes}}{\text{s}}\right)} = \text{download time}(s)$$
- Patterns used when superseeding variation or misleading bitfield messages present to make initial seeder and peer discovery possible

## Conclusion

- By pattern matching initial seeders can be identified for any torrent with public trackers within a given time window
- Software was tested by law enforcement agencies July 2011

## Future Work

- Create graphical user interface (GUI)
- Sort and display useful data
- Design to display data in real-time
- Develop additional profiling techniques

## Selected References

Le Blond et al. "Spying the World from your Laptop – Identifying and Profiling Content Providers and Big Downloaders in BitTorrent" 3rd USENIX Workshop on Large-Scale Exploits and Emergent Threats LEET, 2010.

Bauer, McCoy, Grunwald, and Sicker, "BitStalker: Accurately and Efficiently Monitoring BitTorrent Traffic" IEEE, 2009.