TRACT: Threat Rating and Assessment Collaboration Tool

Robert Hollinger and Doran Smestad

Advised by: George Heineman (WPI), Philip Marquardt (MIT/LL)

Worcester Polytechnic Institute Major Qualifying Project Presentation

October 16th, 2013

Group 51: Cyber Systems and Operations

This work is sponsored by the Assistant Secretary of Defense for Research & Engineering under Air Force Contract #FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

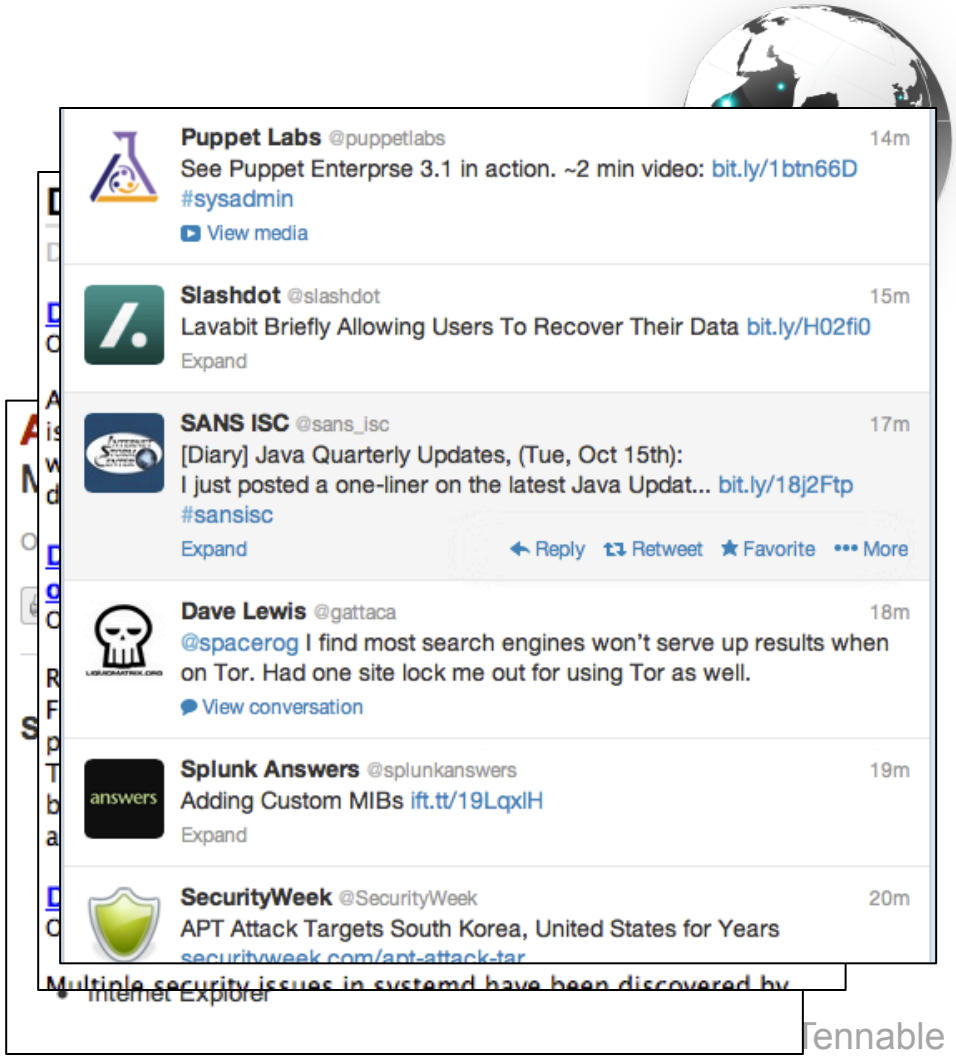
Network Analyst

- Identify cyber vulnerabilities and threats
  - The possibility of a malicious attempt to damage or disrupt a computer network or system.
- Take necessary steps to protect their network against such threats
- Sources of Information
  - Intrusion Detection System (IDS)
  - Intrusion Prevention System (IPS)
  - Server Logs
  - *Online Sources*
- Analyst Tools
  - Tools exist to process many of these sources (e.g. Splunk)
  - However, no tool exists to process the noisy online source data

Problem Area - Sources

Sources of Information:

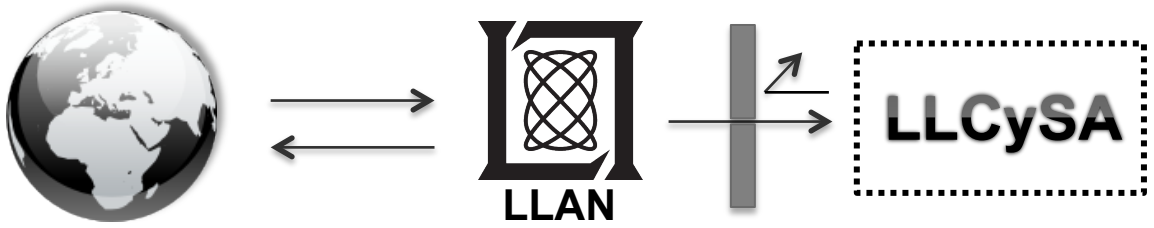
- Twitter
- Blogs
- Security Updates
- Reported Vulnerabilities



Background

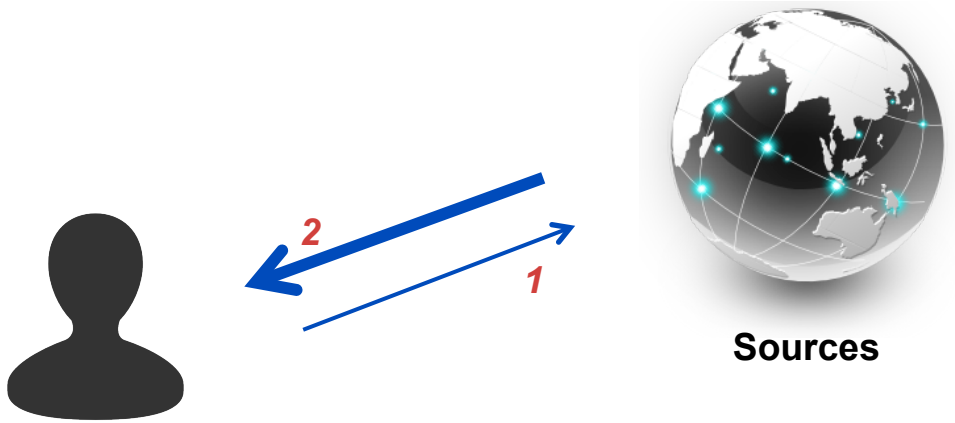
Determine which threats apply to us

- **L**incoln **R**esearch **N**etwork **O**peration **C**enter (LRNOC)
  - Holds Lincoln Laboratory Network Data
  - Research Environment to Build Better Cyber Tools
  - Isolated Network
- **L**incoln **L**aboratory **Cy**ber **S**ituational **A**wareness (LLCySA) Platform
  - Framework to query data from the LRNOC



Problem Statement

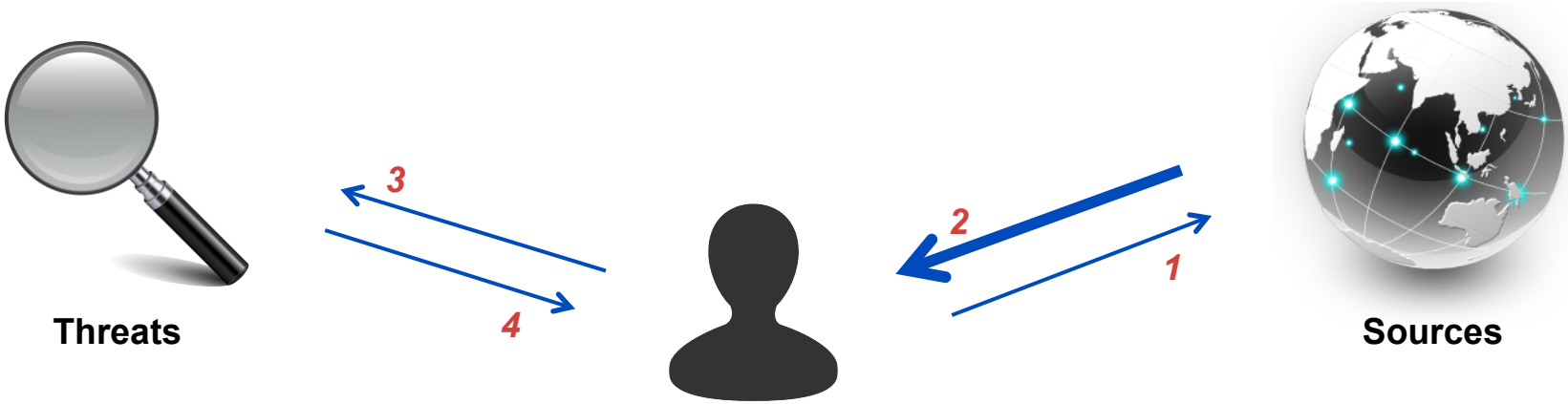
1,2 – Analysts receive large amounts of data from online sources.



Analyst: “Is there a threat?”

Problem Statement

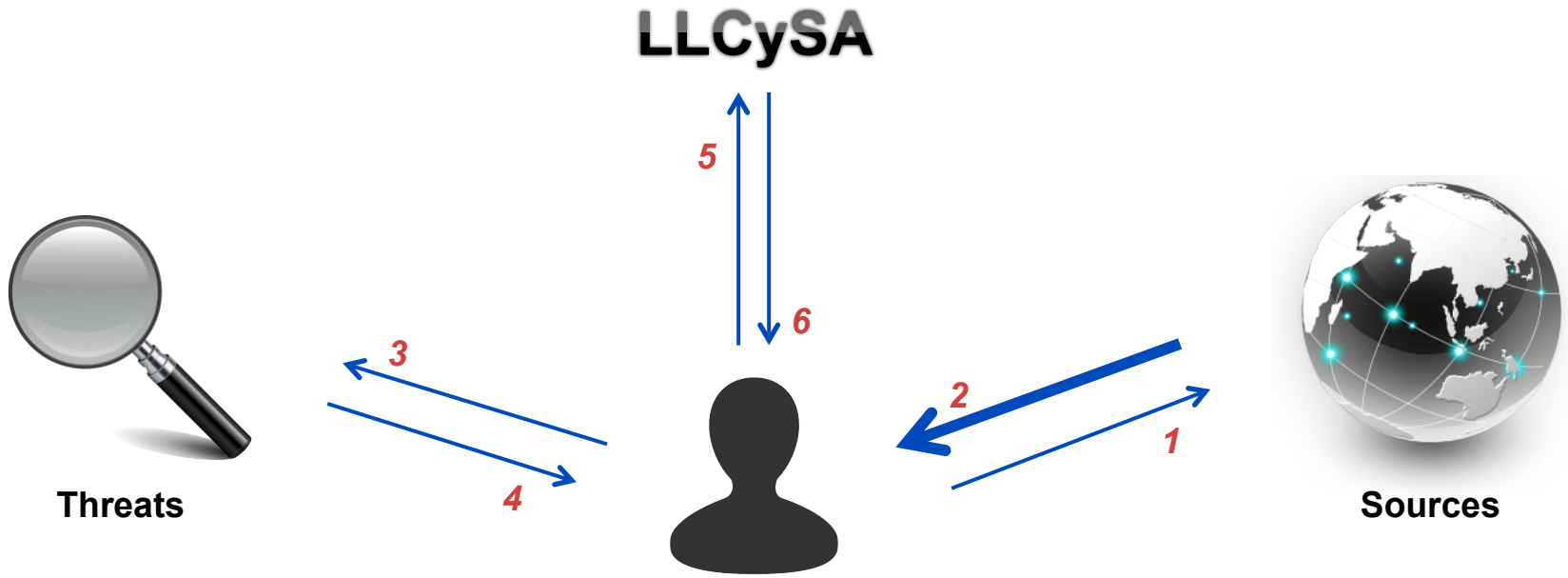
3,4 – Analysts review source data for possible threats.



Analyst: "Is there a threat?"

Problem Statement

5,6 – Analysts can query LLCySA to determine relevance.

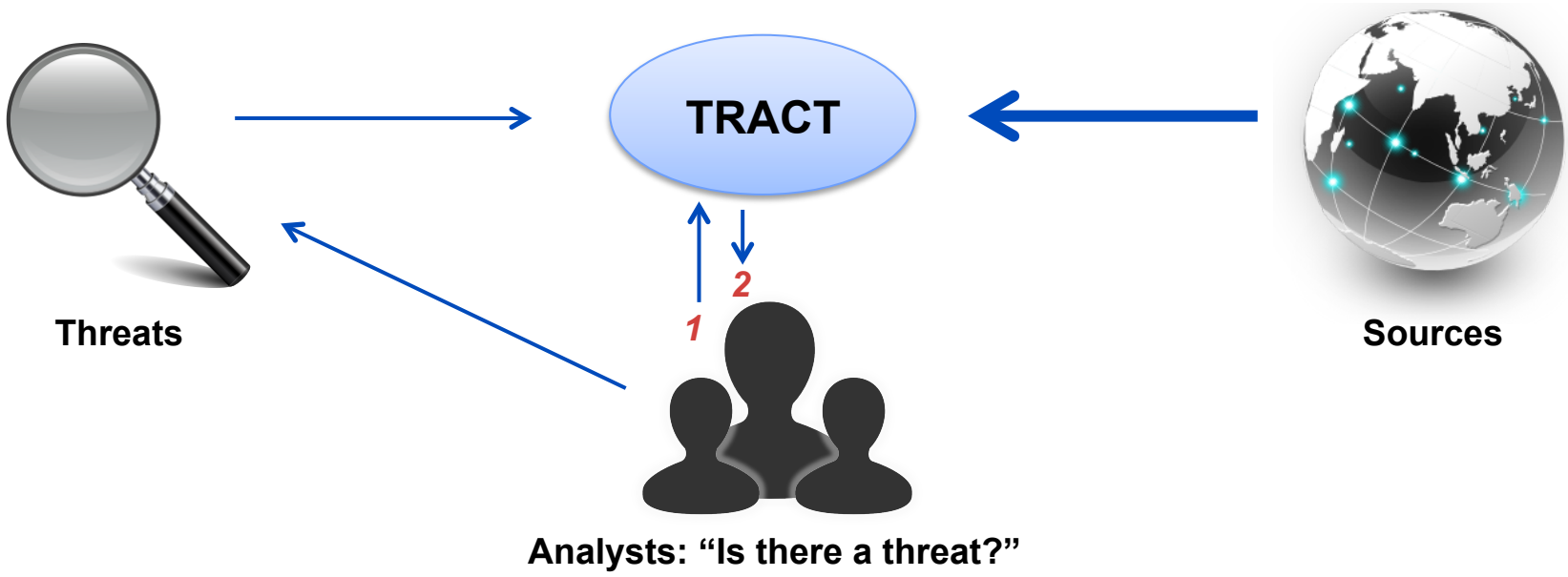


Analyst: "Is there a threat?"

Analysts are required to manually review search, sort, and organize data.

Threat Rating and Assessment Collaboration Tool

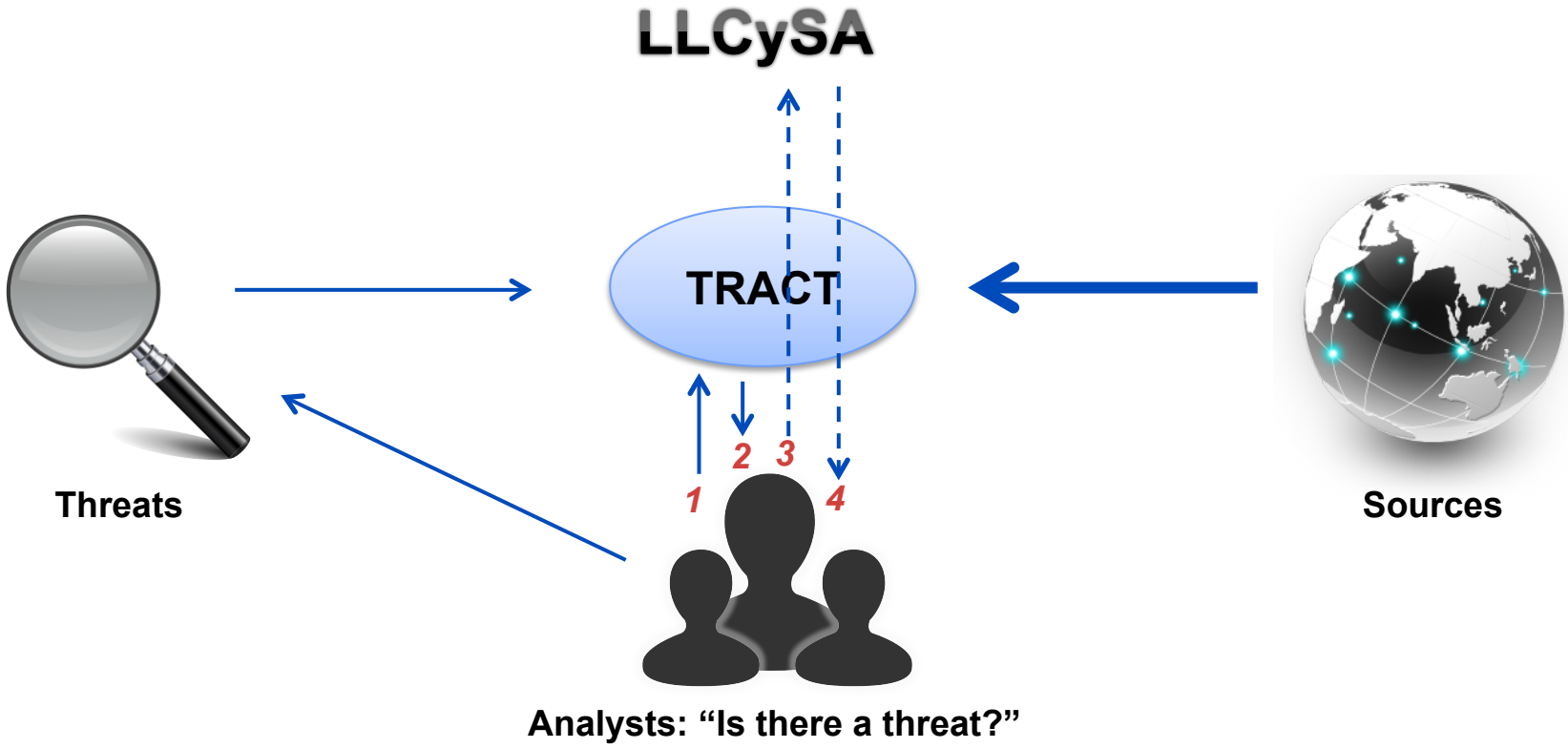
1,2 – Analysts search data held by TRACT



UNCLASSIFED

Threat Rating and Assessment Collaboration Tool

3,4 – Analysts query LLCySA to determine relevance



TRACT allows Analysts to collectively process more data with less noise.

Information Retrieval

Information Retrieval:

Location of relevant documents from a corpus of information

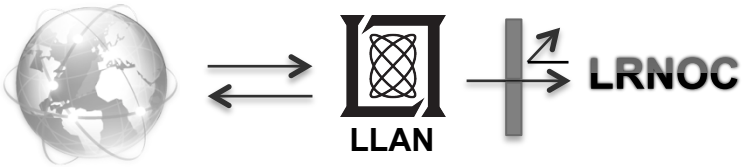
Regular Expression:

Sequence of characters describing a text pattern

Examples:

- (Firefox)
- (Firefox)|(Chrome)
- (Firefox).{0-5}(4)
- ([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})

Design Considerations

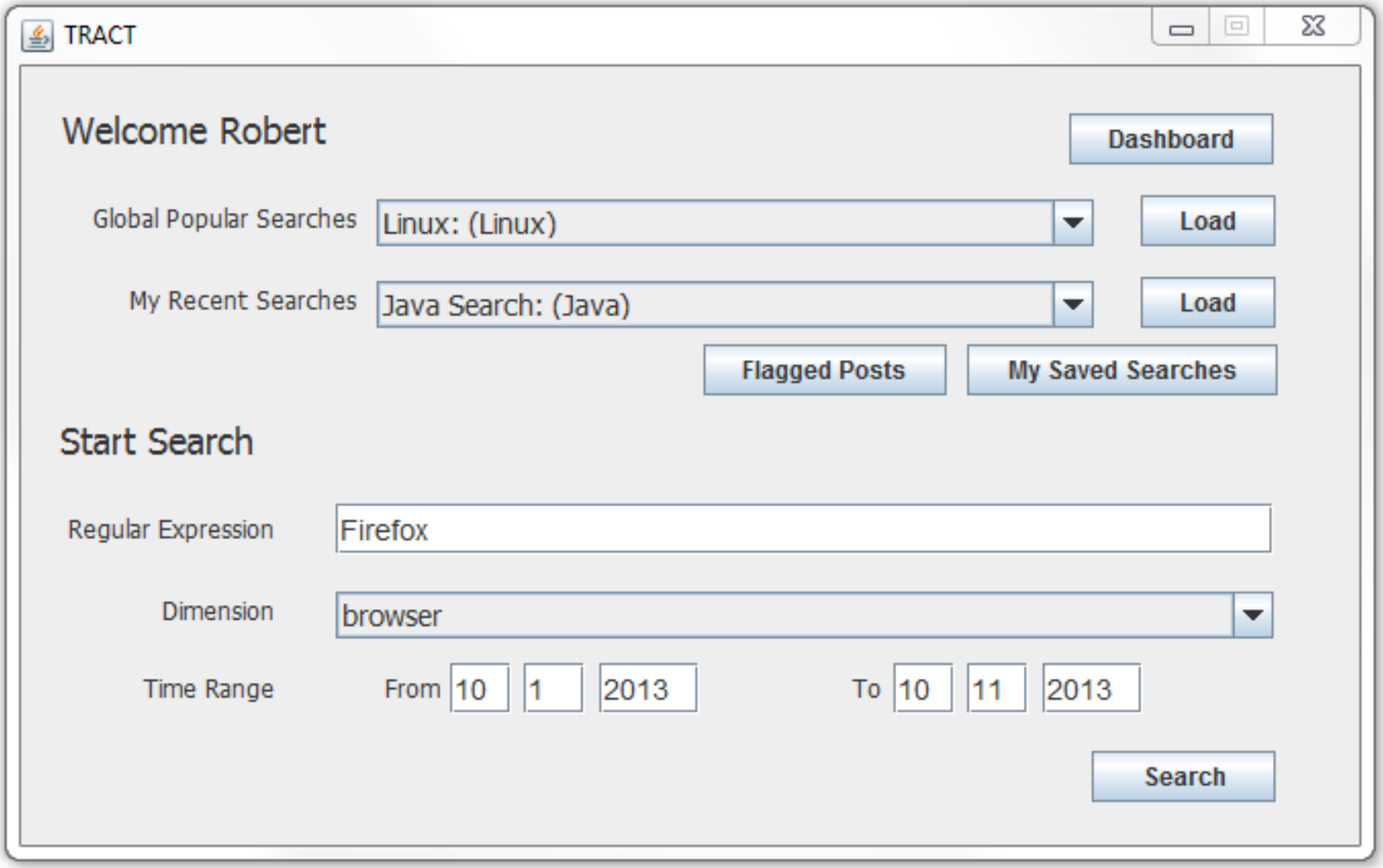


- Transfer of Information
- Permanent Storage of Information
- User Interface communication with the database
- Collaboration between Analysts

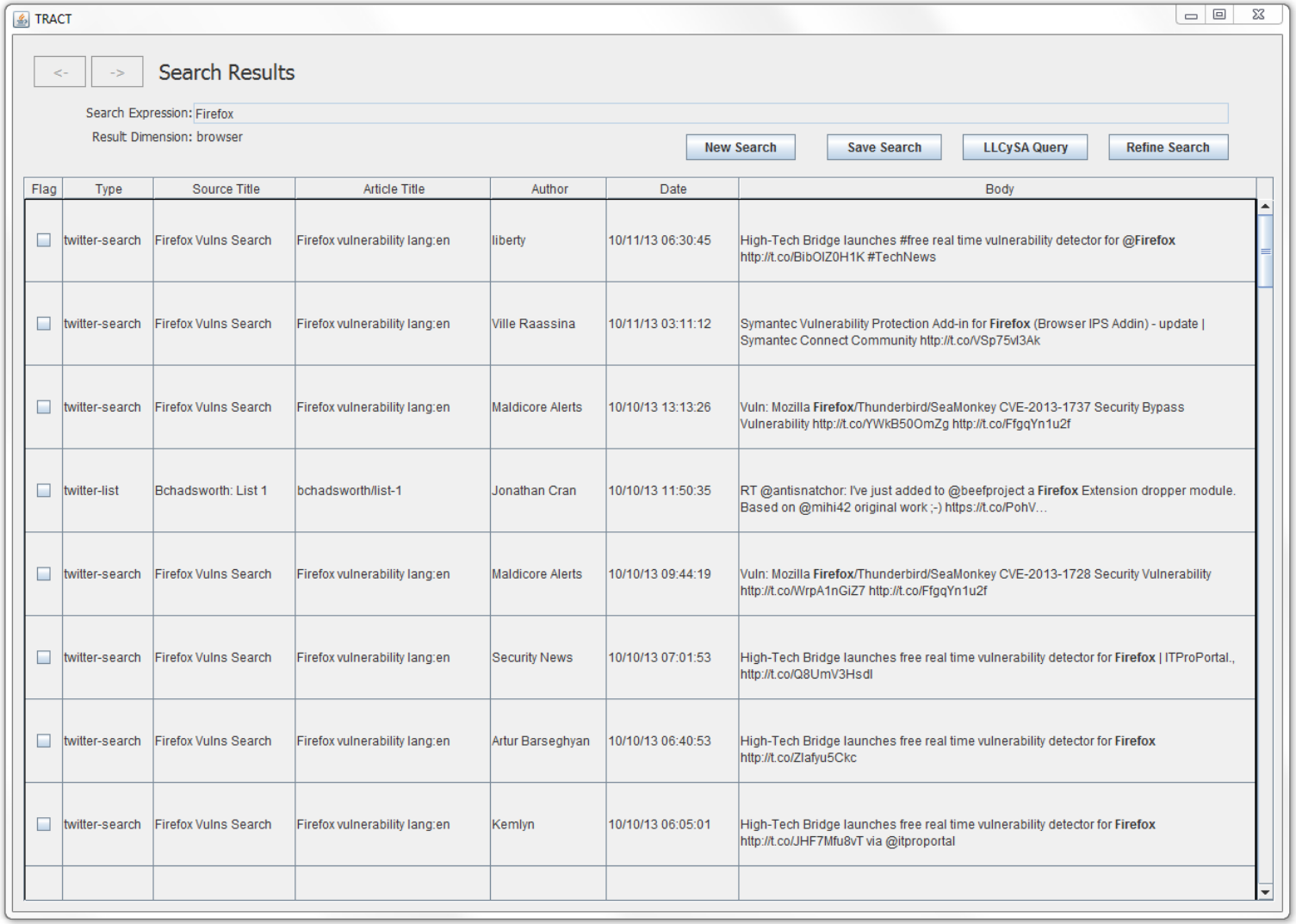
SQLite

MySQL®

User Interface - Welcome

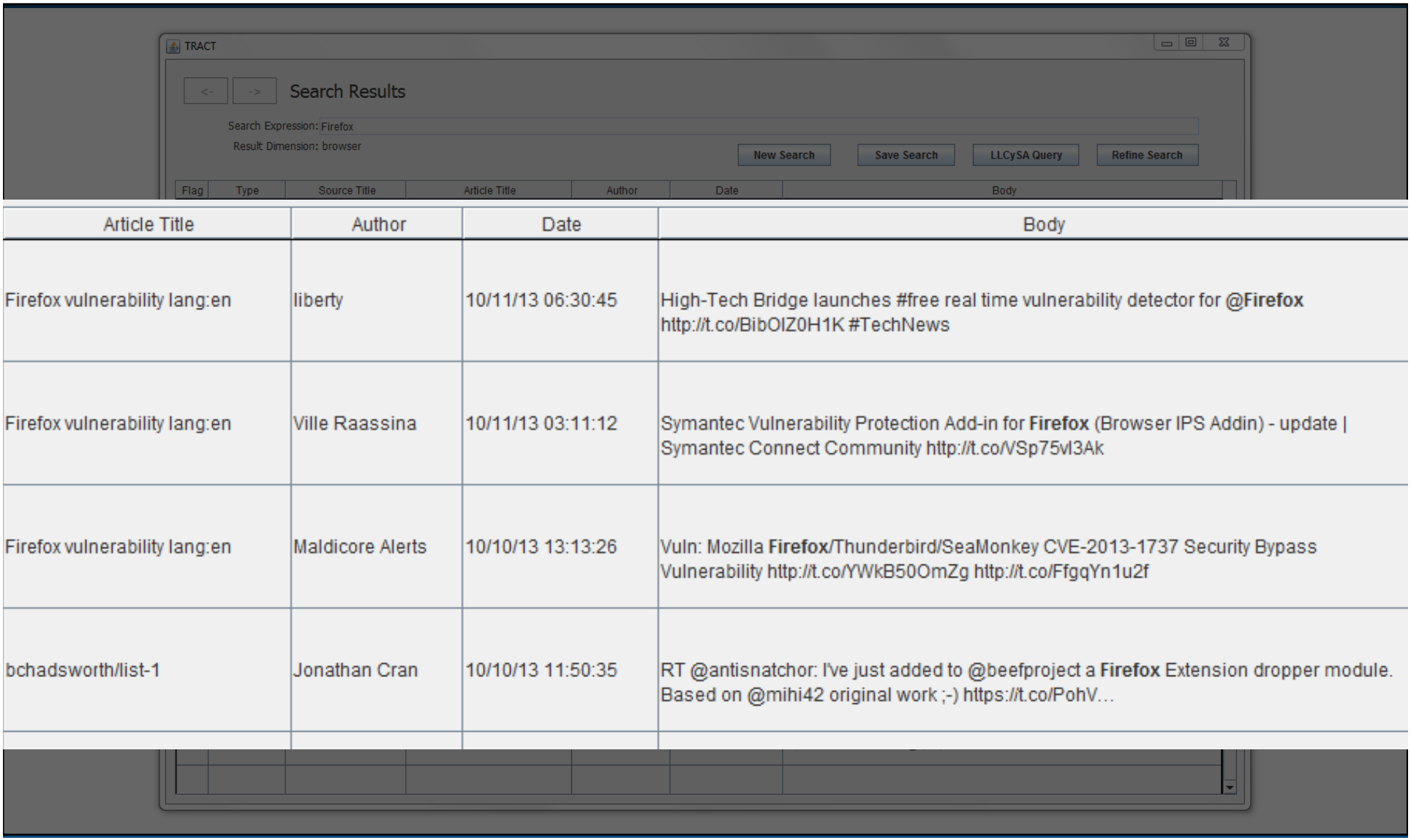


User Interface - Search



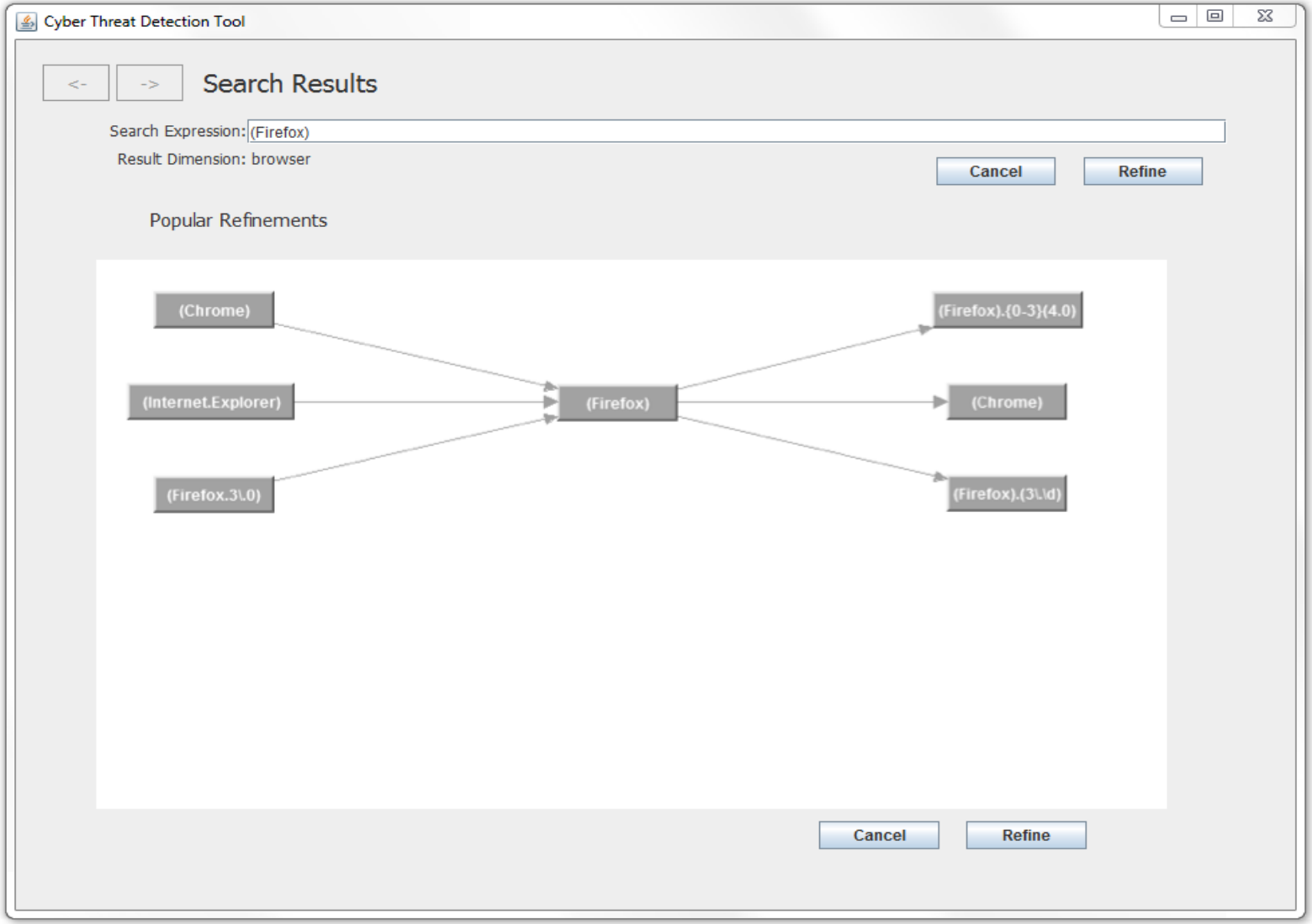
Flag	Type	Source Title	Article Title	Author	Date	Body
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	liberty	10/11/13 06:30:45	High-Tech Bridge launches #free real time vulnerability detector for @**Firefox** http://t.co/BibOlZ0H1K #TechNews
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Ville Raassina	10/11/13 03:11:12	Symantec Vulnerability Protection Add-in for **Firefox** (Browser IPS Addin) - update | Symantec Connect Community http://t.co/VSp75vl3Ak
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 13:13:26	Vuln: Mozilla **Firefox**/Thunderbird/SeaMonkey CVE-2013-1737 Security Bypass Vulnerability http://t.co/YWkB50OmZg http://t.co/FfgqYn1u2f
☐	twitter-list	Bchadsworth: List 1	bchadsworth/list-1	Jonathan Cran	10/10/13 11:50:35	RT @antisnatchor: I've just added to @beefproject a **Firefox** Extension dropper module. Based on @mihi42 original work ;-) https://t.co/PohV…
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 09:44:19	Vuln: Mozilla **Firefox**/Thunderbird/SeaMonkey CVE-2013-1728 Security Vulnerability http://t.co/WrpA1nGiZ7 http://t.co/FfgqYn1u2f
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Security News	10/10/13 07:01:53	High-Tech Bridge launches free real time vulnerability detector for **Firefox** | ITProPortal., http://t.co/Q8UmV3Hsdl
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Artur Barseghyan	10/10/13 06:40:53	High-Tech Bridge launches free real time vulnerability detector for **Firefox** http://t.co/Zlafyu5Ckc
☐	twitter-search	Firefox Vulns Search	Firefox vulnerability lang:en	Kemlyn	10/10/13 06:05:01	High-Tech Bridge launches free real time vulnerability detector for **Firefox** http://t.co/JHF7Mfu8vT via @itproportal

User Interface - Search

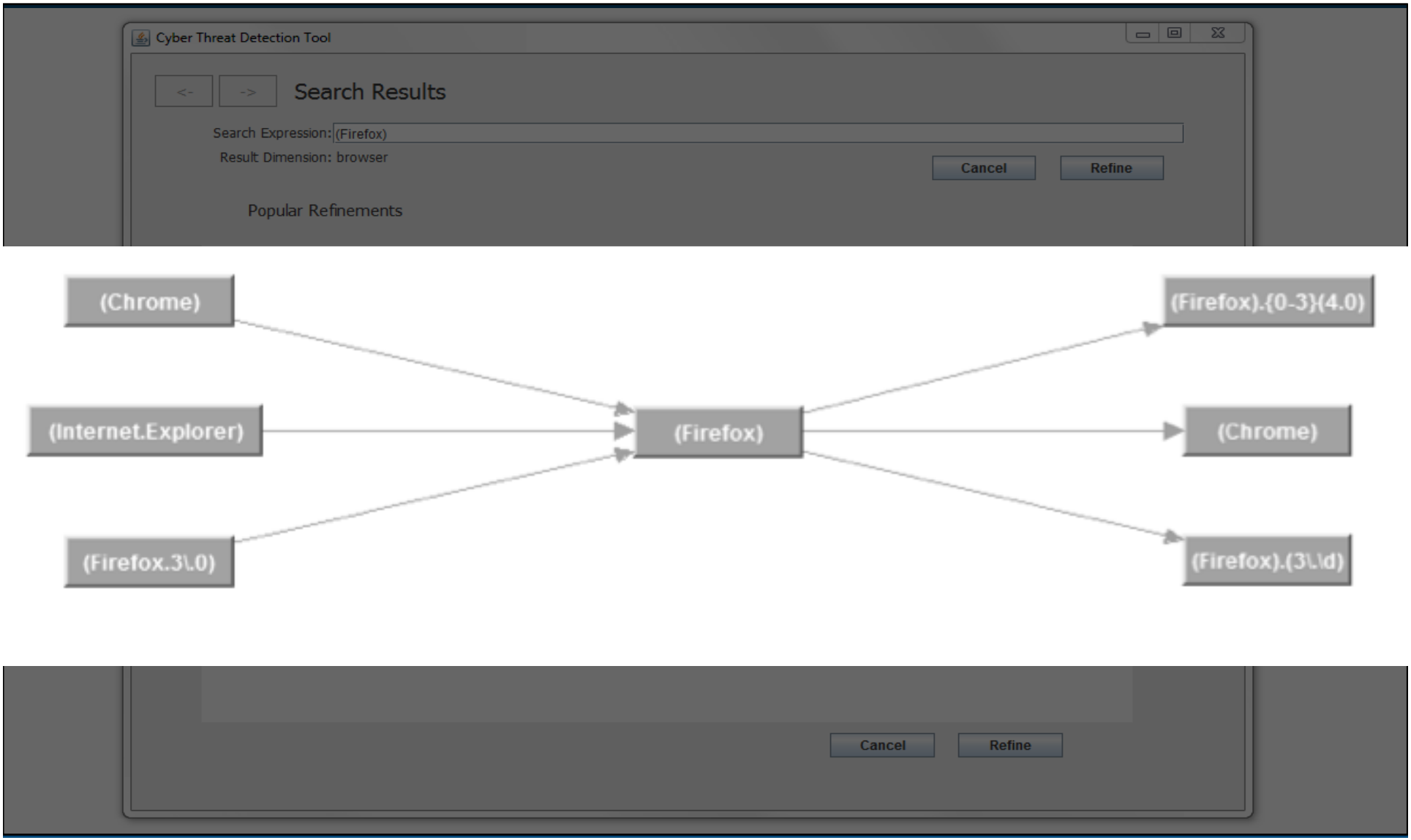


Article Title	Author	Date	Body
Firefox vulnerability lang:en	liberty	10/11/13 06:30:45	High-Tech Bridge launches #free real time vulnerability detector for @**Firefox** http://t.co/BibOIZ0H1K #TechNews
Firefox vulnerability lang:en	Ville Raassina	10/11/13 03:11:12	Symantec Vulnerability Protection Add-in for **Firefox** (Browser IPS Addin) - update | Symantec Connect Community http://t.co/VSp75vl3Ak
Firefox vulnerability lang:en	Maldicore Alerts	10/10/13 13:13:26	Vuln: Mozilla **Firefox**/Thunderbird/SeaMonkey CVE-2013-1737 Security Bypass Vulnerability http://t.co/YWkB50OmZg http://t.co/FfgqYn1u2f
bchadsworth/list-1	Jonathan Cran	10/10/13 11:50:35	RT @antisnatchor: I've just added to @beefproject a **Firefox** Extension dropper module. Based on @mihi42 original work ;-) https://t.co/PohV…

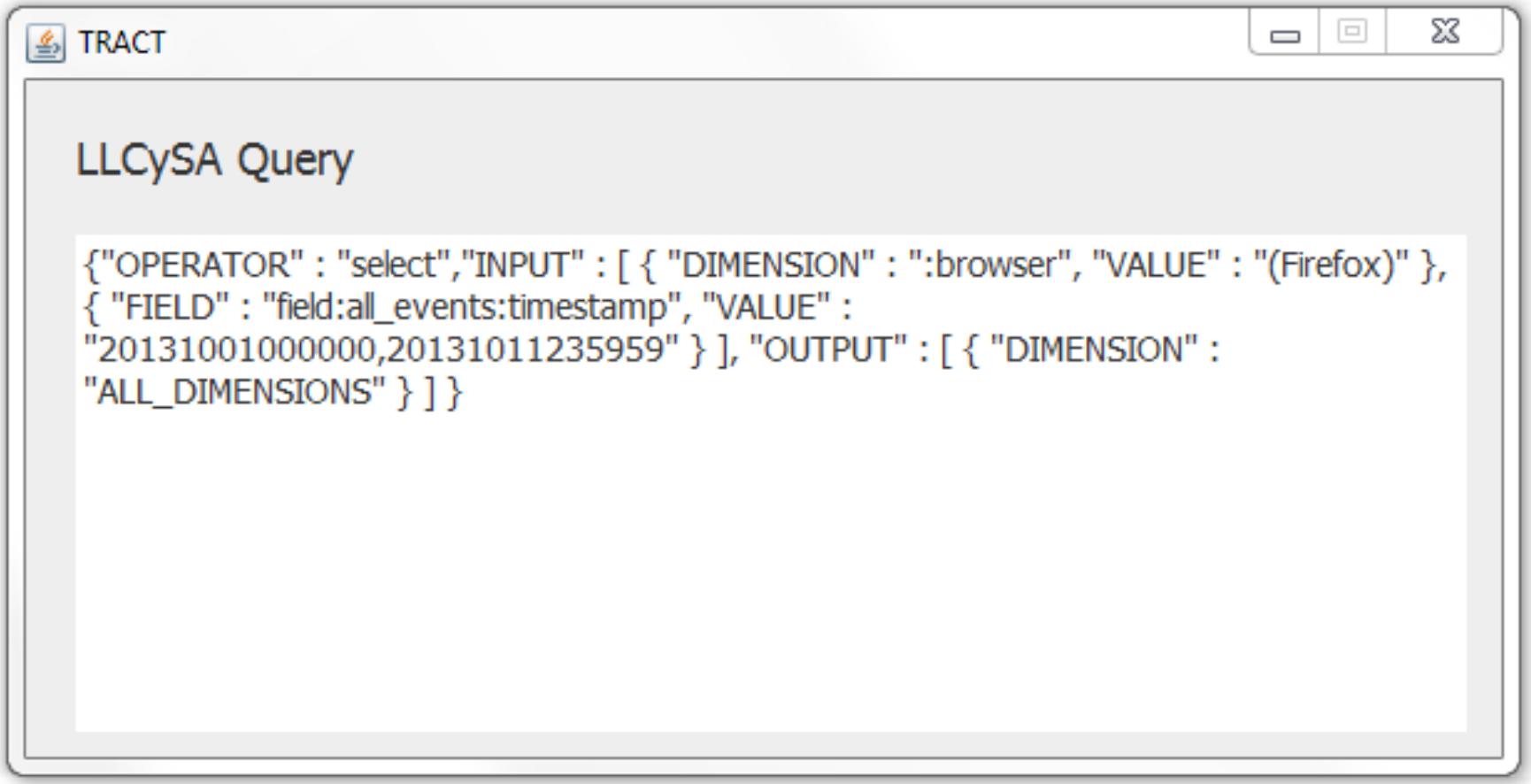
User Interface - Refine



User Interface - Refine

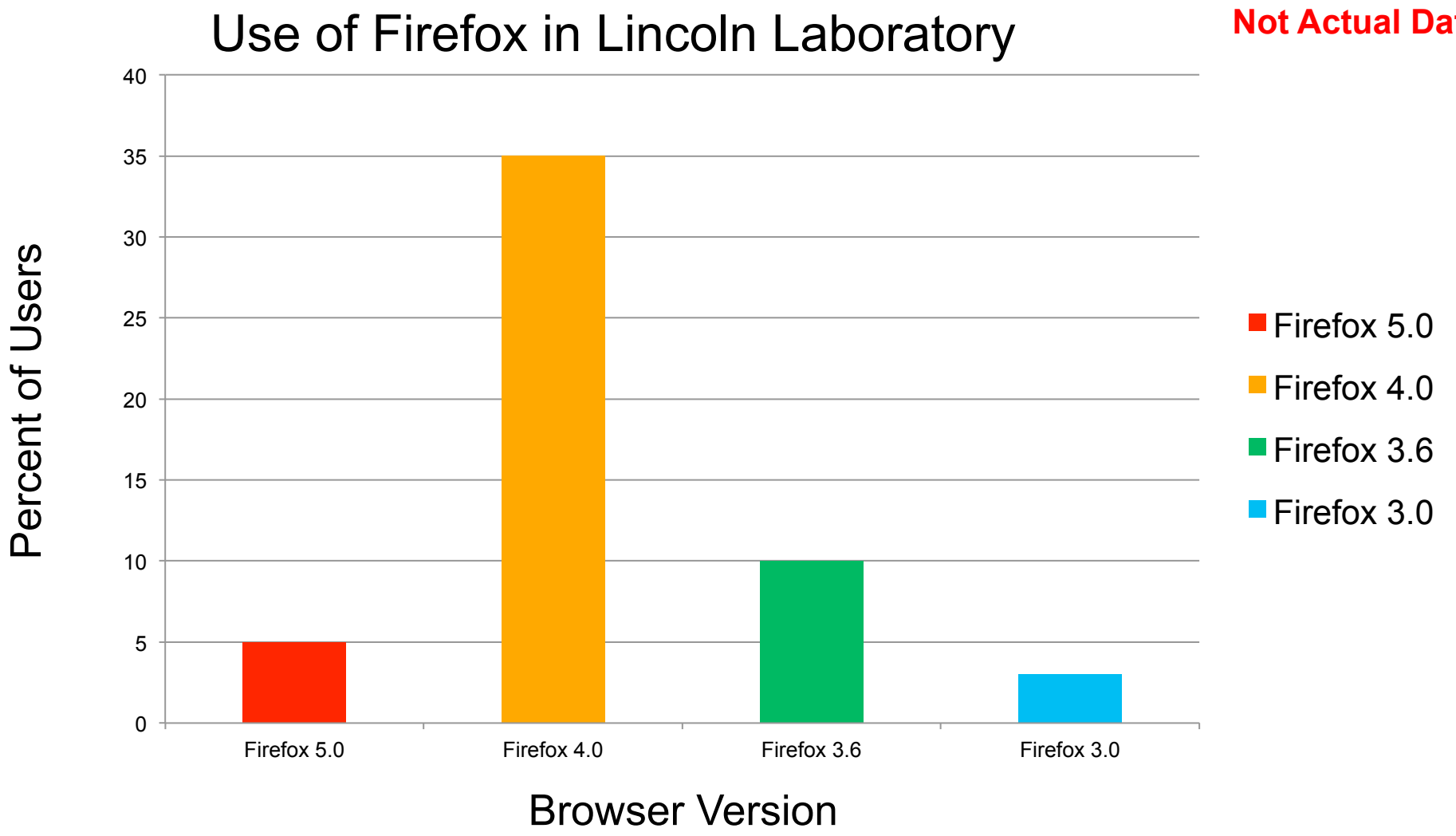


User Interface - LLCySA

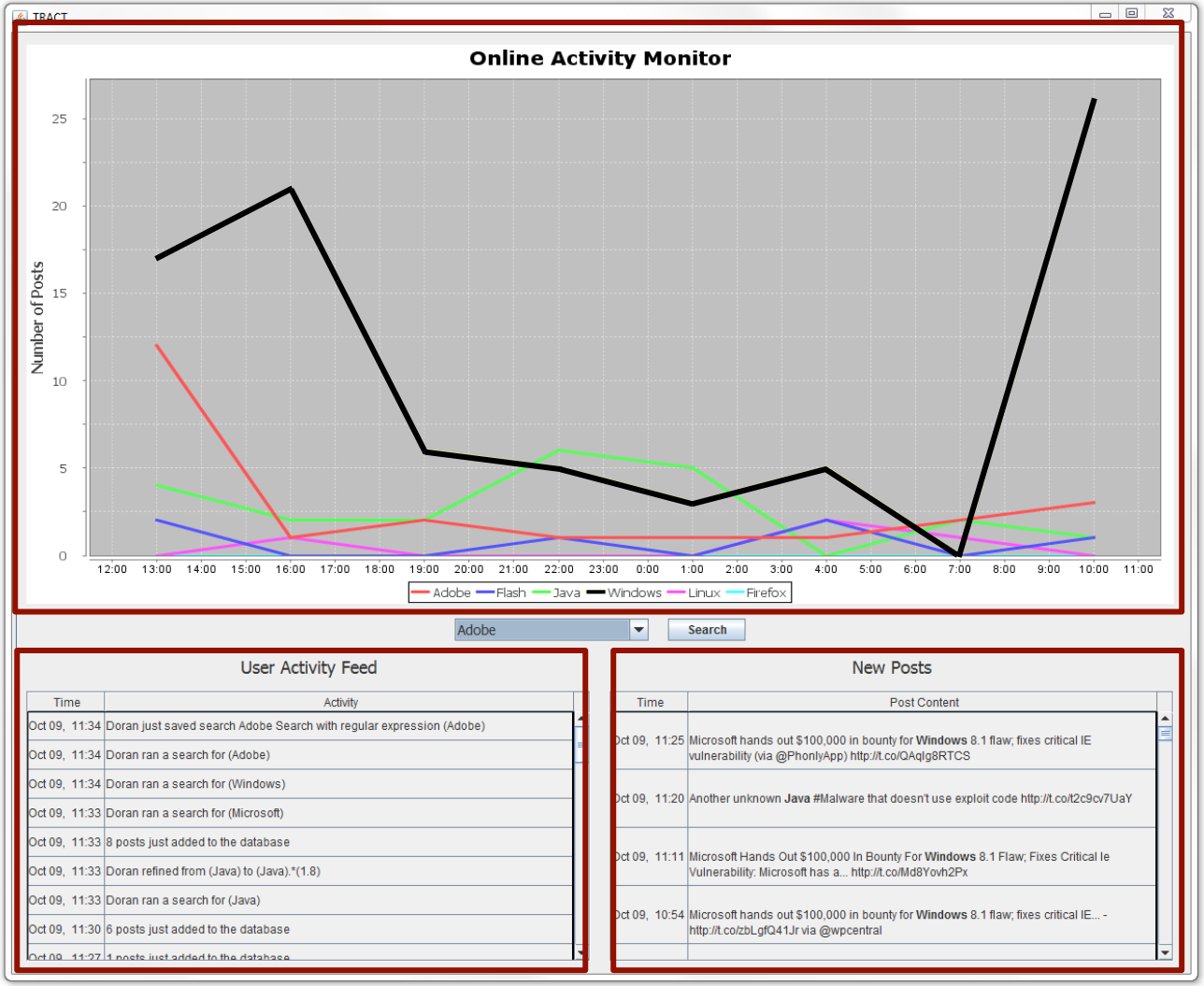


User Interface - LLCySA

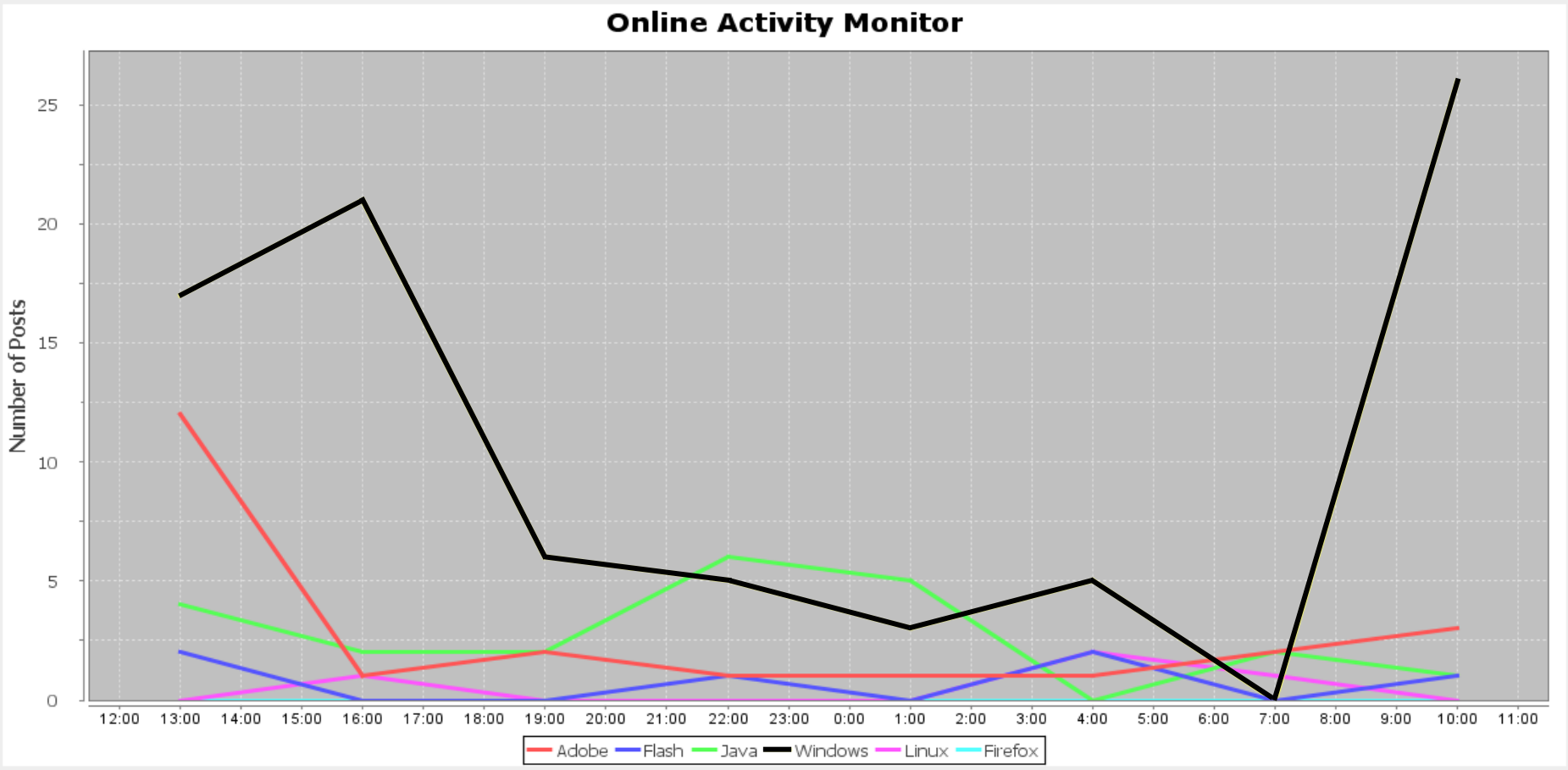
Example Purposes Only
Not Actual Data



User Interface - Dashboard



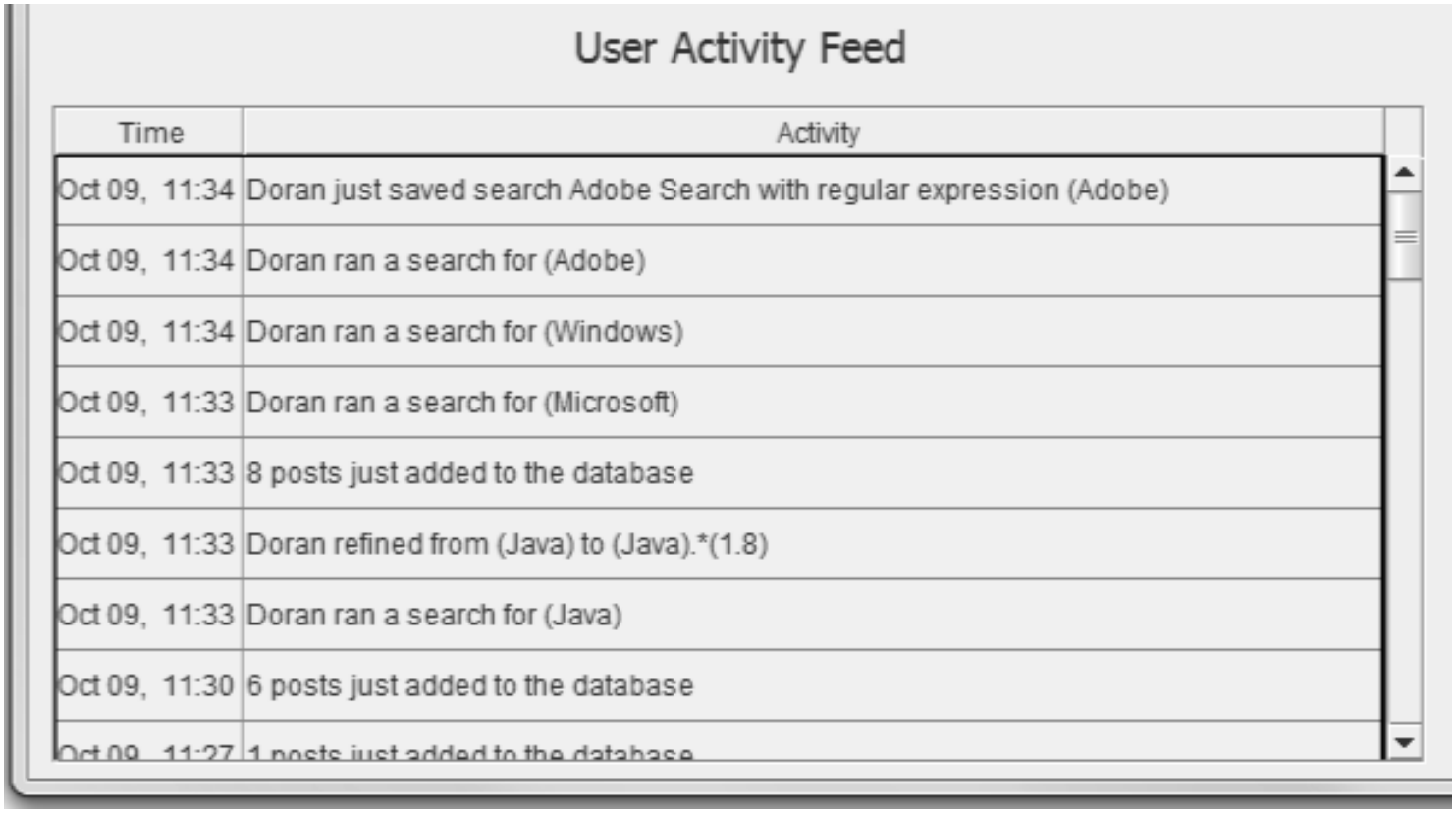
User Interface - Dashboard



UNCLASSIFED

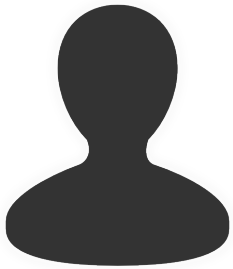
User Interface - Dashboard

User Interface - Dashboard



Evaluation

LRNOC



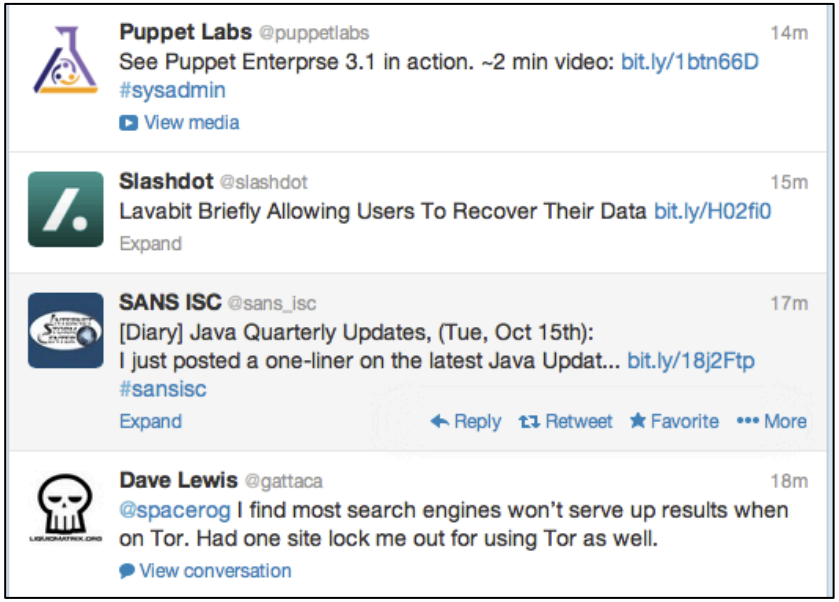
Analysts

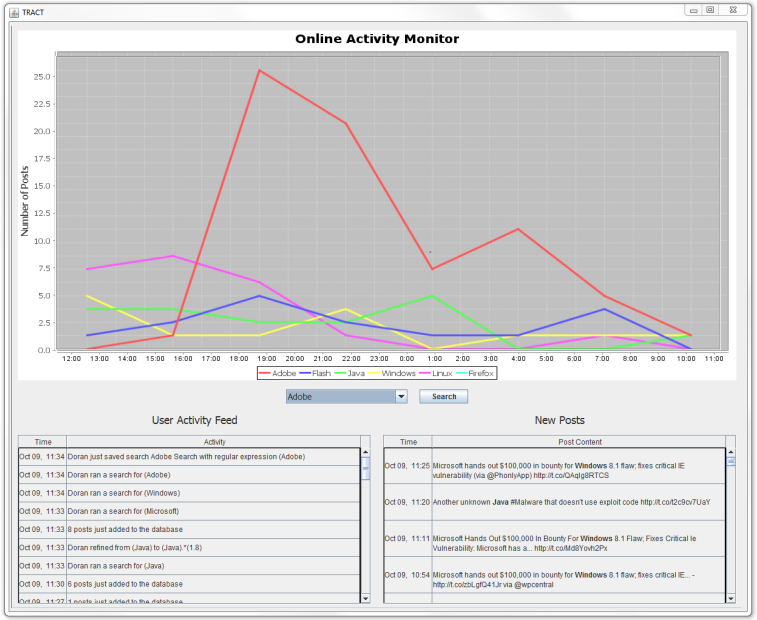
LLCySA

- Dedicated display to show our Dashboard in the LRNOC
- Ingestion of user refinement data into the LLCySA platform
- Received positive reaction from Analysts and they plan to use it in their work

Conclusion

- Identified a gap in the analyst toolset
- Developed system to assist analysts in the process of gaining relevant threat information from online sources
- Reviewed system with analysts





UNCLASSIFED

Future Work

Advanced Information Retrieval

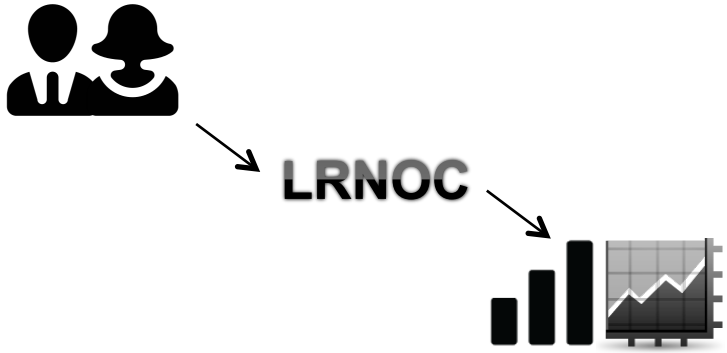
Google

Lucene

A 語 52

Full Graphing of Refinements

Full integration with LRNOC



Acknowledgements

Philip Marquardt, MIT/LL Advisor, LRNOC Lead

George Heineman, WPI Advisor

David O'Gwynn, LLCySA Technical Staff

Kathleen Haas, MQP Coordinator

Ted Clancy, WPI Project Site Lead

BACKUP SLIDES

System Flow of Information