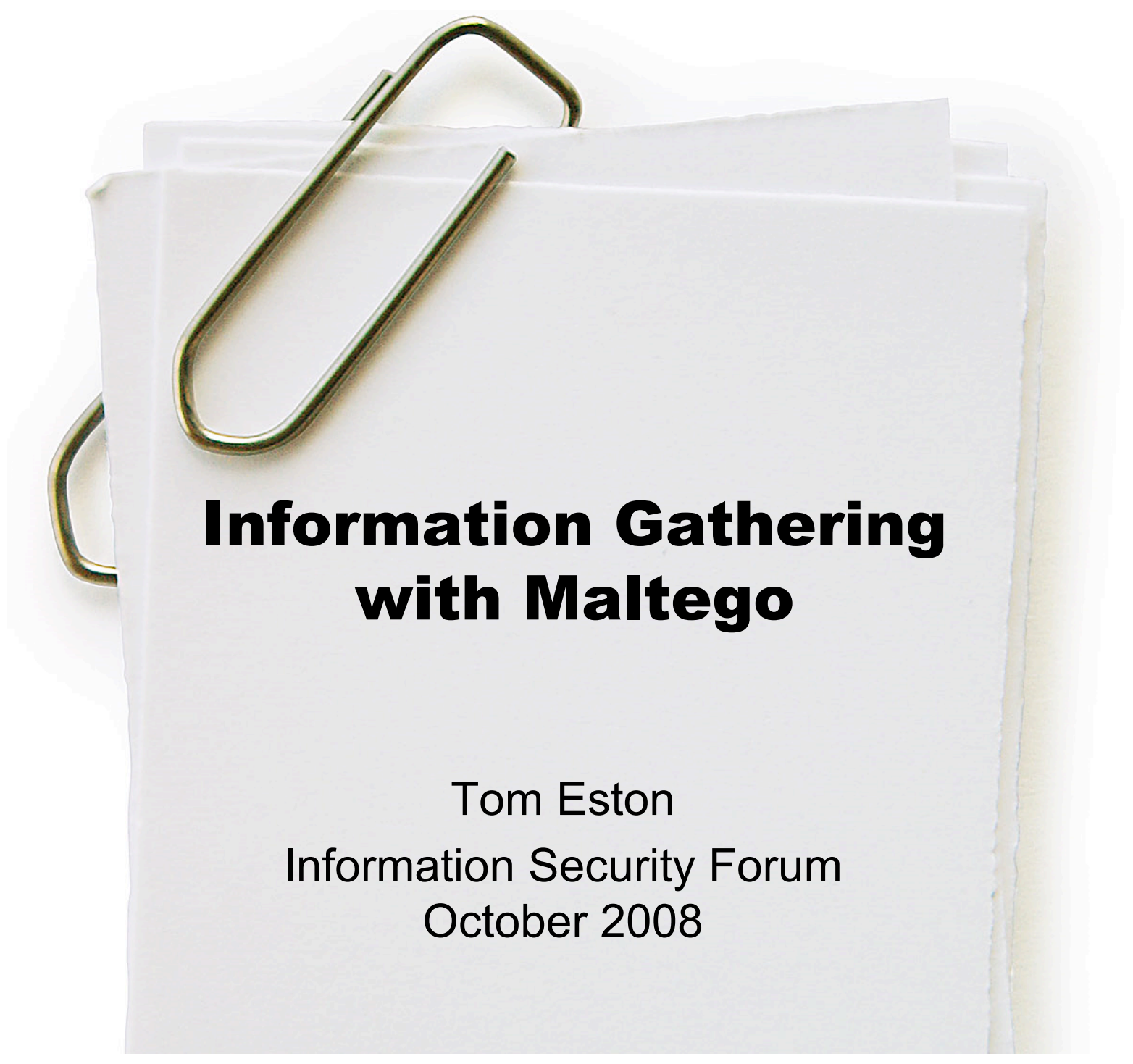


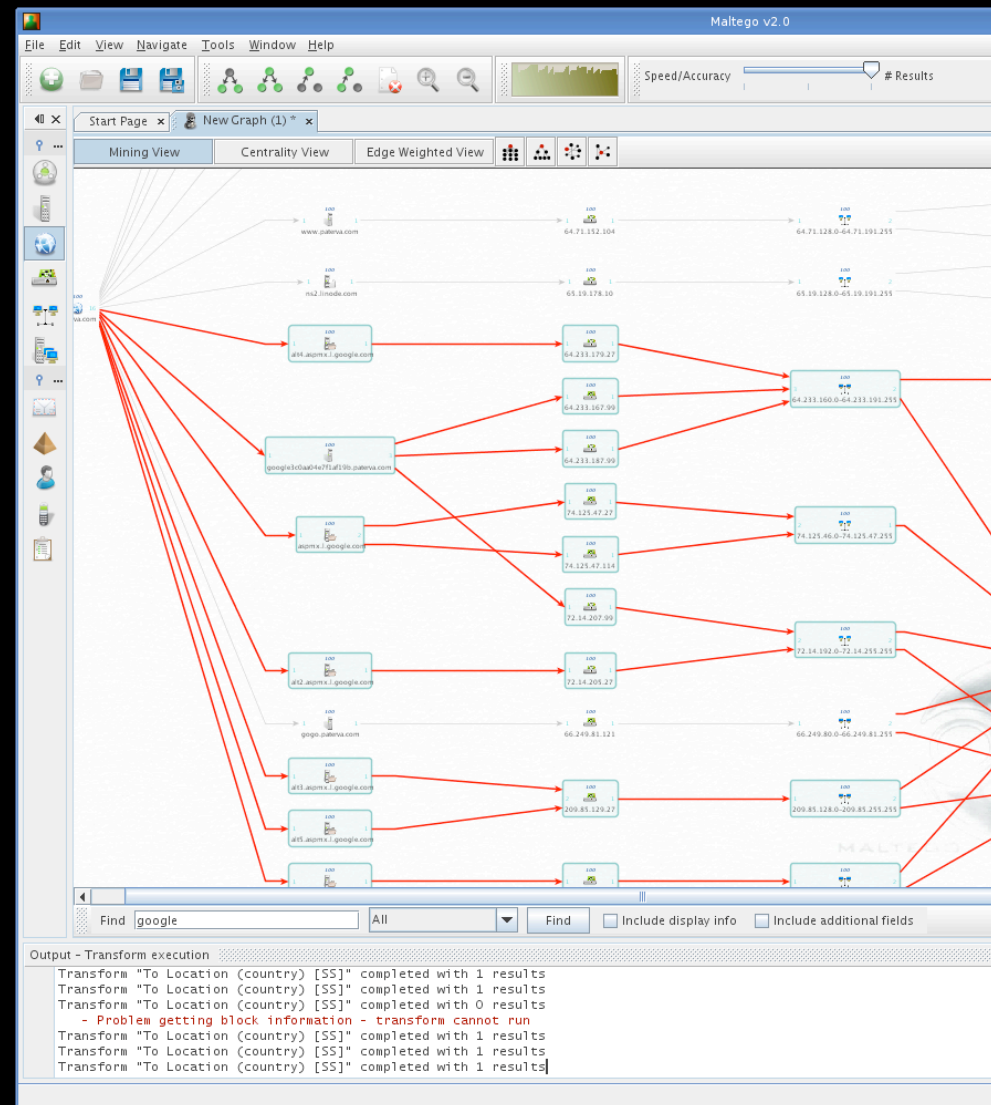


Information Gathering with Maltego

Tom Eston
Information Security Forum
October 2008

What is Maltego?

- Data mining and information gathering tool
- Identify key relationships between information and find unknown relationships
- Uses “transforms”

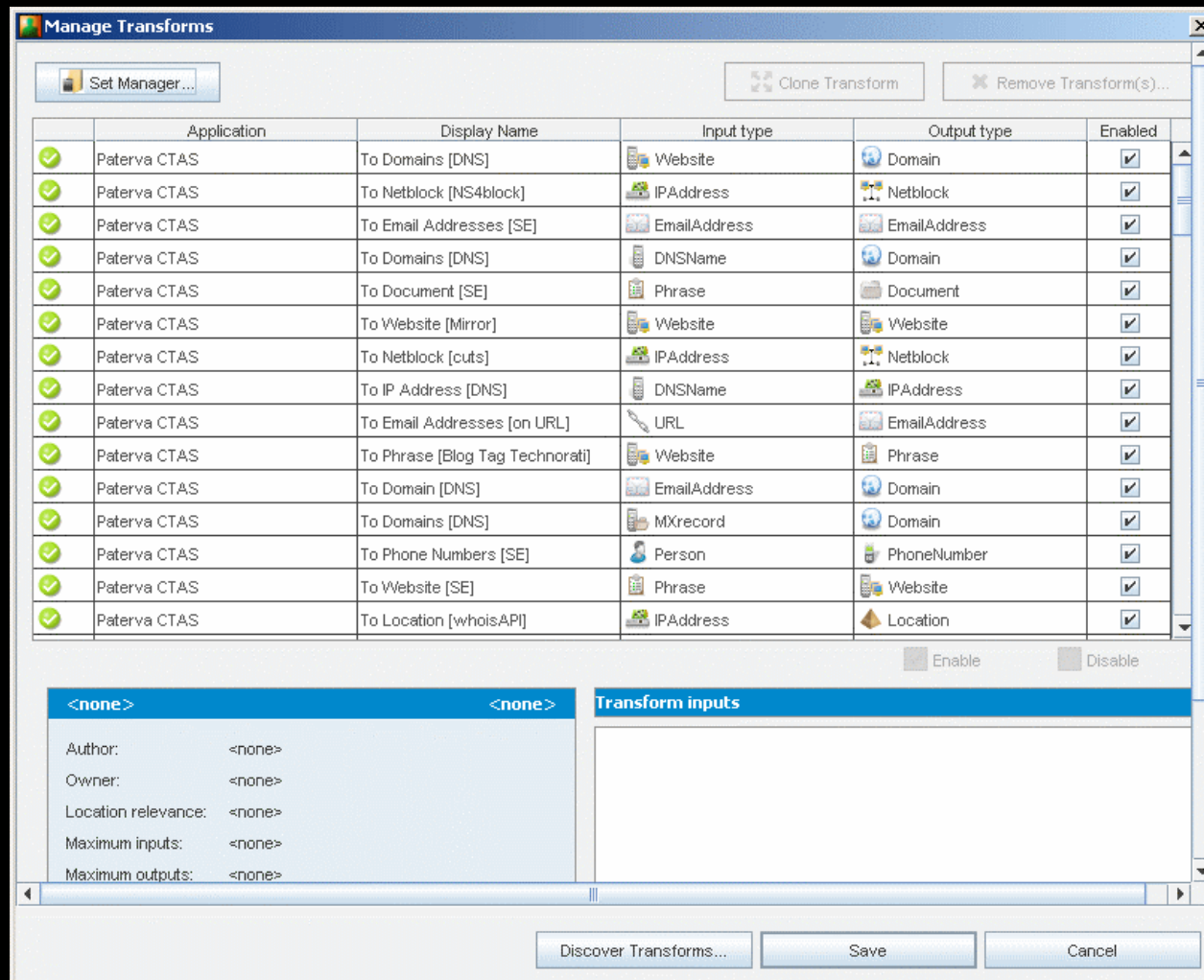


What does Maltego do?

- Helps determine real world links between...
 - People
 - Social Networks
 - Companies/Organizations
 - Web sites
 - Internet Infrastructure (DNS, Domains, Netblocks)
 - Phrases
 - Documents and files

How does it work?

Maltego Transforms



What is logged?

- API key
- IP Address (yours)
- The transform executed
- The time it executed
- Your user ID (which gives first name, last name and email address)
- The questions asked or the results are NOT logged
 - Except for a few transforms that use web services...

What can it do for you?

- Information gathering phase of all security related work
 - Assessments
 - Investigations
 - Public information about a company or person
- Saves time
- Easier to use then Google “hacking”
- Hits more then just Google!

Where to get it?

- Community edition
 - Download via paterva.com also found on Backtrack 3
 - No saving, limited to 75 transforms, etc...
- Full version has no limitations
 - \$430 per year
- Runs on Linux, OS X, Windows

<http://www.paterva.com/maltego/>

More Information

- **Room362.com**
 - Maltego 2 and beyond
<http://www.room362.com/archives/225-Maltego-2-and-beyond-Part-1.html>
- **EthicalHacker.net**
 - Chris Gates Maltego Series
<http://www.ethicalhacker.net/content/view/202/1/>

Demo...