

# CIS 700/002 : Special Topics : Maltego

Sangdon Park

CIS 700/002: Security of EMBS/CPS/IoT  
Department of Computer and Information Science  
School of Engineering and Applied Science  
University of Pennsylvania

*March 17, 2017*

# Brief Introduction

- Software used for reconnaissance
  - Visualize publically available information

The screenshot displays the Maltego Kali Linux Edition 4.0.11 interface. The main window shows a graph visualization of entities and their relationships. The graph consists of several nodes connected by lines, representing a network of information. The nodes are color-coded: purple for Domain, orange for IP v4 Address, teal for Netblock, yellow for Phrase, dark blue for Email Address, and red for DNS Name. The graph shows a central node (purple) connected to several other nodes (orange, teal, yellow, dark blue, red). The interface includes a menu bar with options like Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import | Export, and Windows. Below the menu bar are buttons for Run Machine, Stop all Machines, New Machine, and Manage Machines. The left sidebar contains an Entity Palette with categories like Netblock, URL, Tracking Code, Website, Locations, Malware, and Penetration Testing. The right sidebar shows a detail view for a machine named 'Footprint L1' with a progress bar and a list of relationships (Incoming and Outgoing). The bottom status bar indicates '1 of 15 entities'.

# Terminology

- Entity
  - It is represented as a node on a graph and can be anything such as a domain, person, phone number, etc.
  - 20 entities + custom entities
- Transform
  - It is a piece of code that takes one entity to another
- Machine
  - It chains multiple transforms together to automate common/tedious tasks.

# Caution!

- Data crawling may be illegal depending on the terms of use of websites

### 3. Safety

We do our best to keep Facebook safe, but we cannot guarantee it. We need your help to keep Facebook safe, which includes the following commitments by you:

1. You will not post unauthorized commercial communications (such as spam) on Facebook.
2. You will not collect users' content or information, or otherwise access Facebook, using automated means (such as harvesting bots, robots, spiders, or scrapers) without our prior permission.
3. You will not engage in unlawful multi-level marketing, such as a pyramid scheme, on Facebook.
4. You will not upload viruses or other malicious code.
5. You will not solicit login information or access an account belonging to someone else.
6. You will not bully, intimidate, or harass any user.
7. You will not post content that: is hate speech, threatening, or pornographic; incites violence; or contains nudity or graphic or gratuitous violence.
8. You will not develop or operate a third-party application containing alcohol-related, dating or other mature content (including advertisements) without appropriate age-based restrictions.
9. You will not use Facebook to send spam.
10. You will not do any activity that interferes with the proper functioning of the service, such as page rendering or other activities that interfere with the service.
11. You will not facilitate or encourage any activity that interferes with the proper functioning of the service, such as page rendering or other activities that interfere with the service.

## PETE WARDEN'S BLOG

*Ever tried. Ever failed. No matter. Try Again. Fail again. Fail better.*

[HOME](#) [ABOUT](#)

### *How I got sued by Facebook*

APRIL 5, 2010  
By Pete Warden  
in [UNCATEGORIZED](#)  
40 COMMENTS



FOLLOW @PETEWARDEN ON TWITTER

Tweets by [@petewarden](#)

 Pete Warden Retweeted 

 **Douglas Eck**  
[@douglas\\_eck](#)

# Run a machine

The screenshot displays the Maltego Kali Linux Edition 4.0.11 interface. The main window shows a graph with a central entity 'cis.upenn.edu' and several outgoing relationships to other entities. The entities are categorized as DNS (orange icons) and WWW (green icons). The DNS entities include 'aaa104-1.cis.upenn.edu', 'alewife.cis.upenn.edu', 'alur.cis.upenn.edu', 'alpha.cis.upenn.edu', and 'ambert.cis.upenn.edu'. The WWW entities include 'ftp.cis.upenn.edu', 'itre.cis.upenn.edu', 'cis.upenn.edu', 'cg.cis.upenn.edu', and 'rtg.cis.upenn.edu'. The interface also shows a sidebar with various tool palettes and a right-hand panel with a 'Footprint L1' machine completion status.

**Entity Palette**

- URL
- Tracking Code
- Website
- Locations
- Malware
- Hash
- Penetration Testing
- Run View
- Transforms
- Machines
- Prune Leaf Entities
- Twitter Monitor

**Output - Transform Output**

```
Transform To AS number returned with 2 entities (from entity "156.130.6.0-156.130.6.255")
Transform To AS number done (from 2 entities)
Running transform To Company [Owner] on 1 entities (from entity "55")
Transform To Company [Owner] returned with 3 entities (from entity "55")
Transform To Company [Owner] done (from entity "55")
```

**Footprint L1**  
[cis.upenn.edu]

**Machine completed**

```
run(NetblockToAS_SS)
run(ASNumberToCompany)
Machine completed with 3 entities
```

**Detail View**

Phrase  
maltego.Phrase  
Comcast Cable  
Communications, Inc.

**Relationships**

- Incoming
- Generator detail

**Source** 55 (AS)

**Property...** Hub Transform...

**Properties**

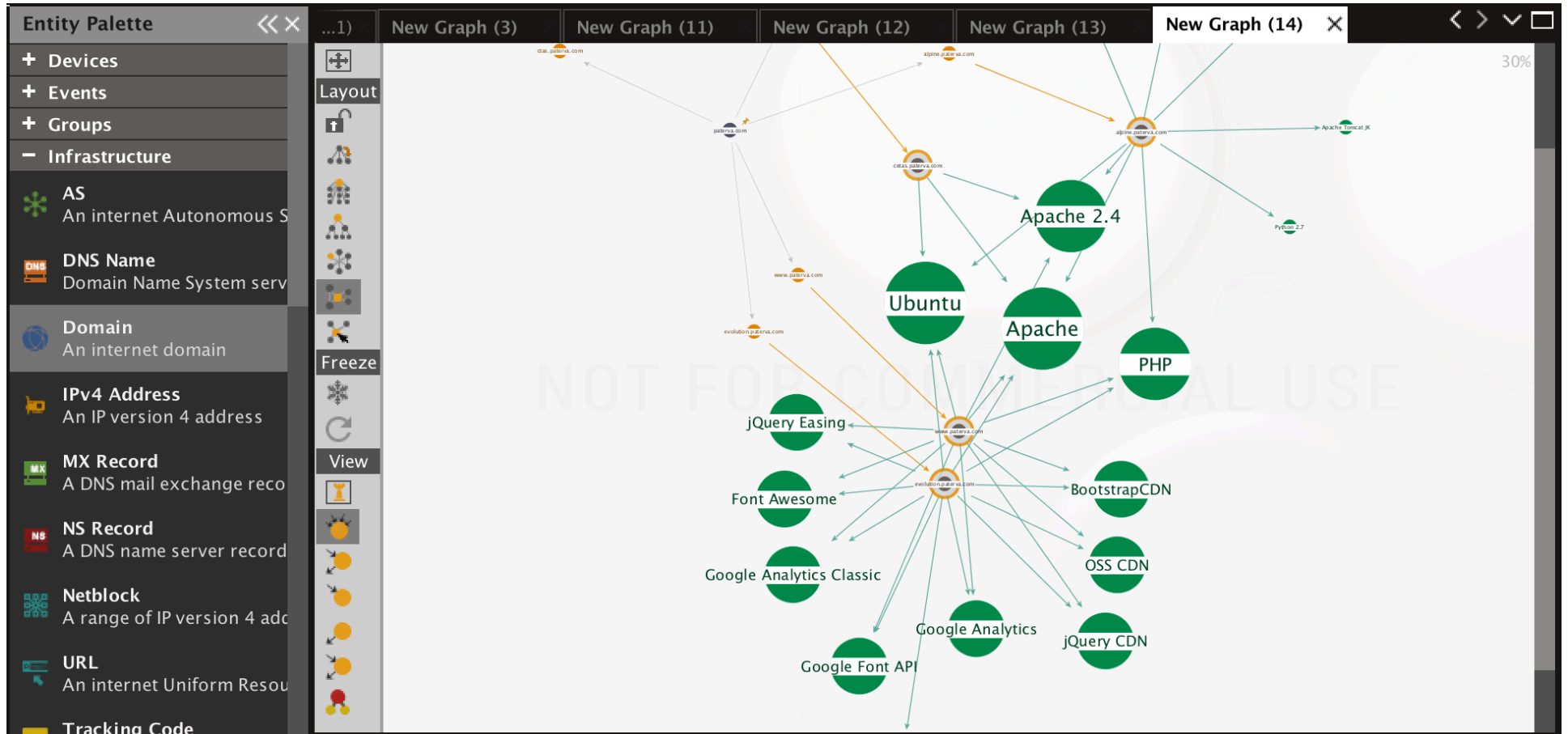
Type	Phrase
Text	Comcast Cable ...

**Graph info**

Weight	100
Incoming	1
Outgoing	0
Bookmark	

1 of 39 entities

# Build My Entity Graph from Scratch



# Maltego OpenSSL Heartbleed Transform

The screenshot shows the Maltego interface with a window titled "heartbleed2". The interface includes a sidebar with "Layout", "Freeze", and "View" sections. A "Website (1.9K)" pop-up window is open, displaying a list of domains:

Website (1.9K)
02ef.net
0daydownloads.com
1001retsept.ru
101cargames.com
10tl.net
168.am
16personalities.com
1clickday.com
1doost.com
1jux.net
1linkdescarga.com
20dollars2surf.com
21cineplex.com
220-volt.ru
258.com

Below the pop-up, a diagram illustrates the transform: a green monitor icon with "WWW" is labeled "koreabridge.net", with an arrow pointing to a yellow speech bubble icon labeled "OpenSSL Heartbleed". A large watermark "NOT FOR COMMERCIAL USE" is visible in the background.

# Maltego OpenSSL Heartbleed Transform

Secure https://filippo.io/Heartbleed/

## Heartbleed test

[FAQ/status](#)



If there are problems, head to the [FAQ](#)

Results are now cached globally for up to 6 hours.

Enter a URL or a hostname to test the server for CVE-2014-0160.

Go!

**koreabridge.net IS VULNERABLE.**



# Reference

- [cis.upenn.edu/~sangdonp/demo-maltego.html](http://cis.upenn.edu/~sangdonp/demo-maltego.html)

# Practice Problems

- Check the heartbleed vulnerability of all web servers under \*.cis.upenn.edu domain
- What is the most used server technologies of \*.paterva.com sites?