CIS 700/002 : Special Topics : Maltego

Sangdon Park

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science

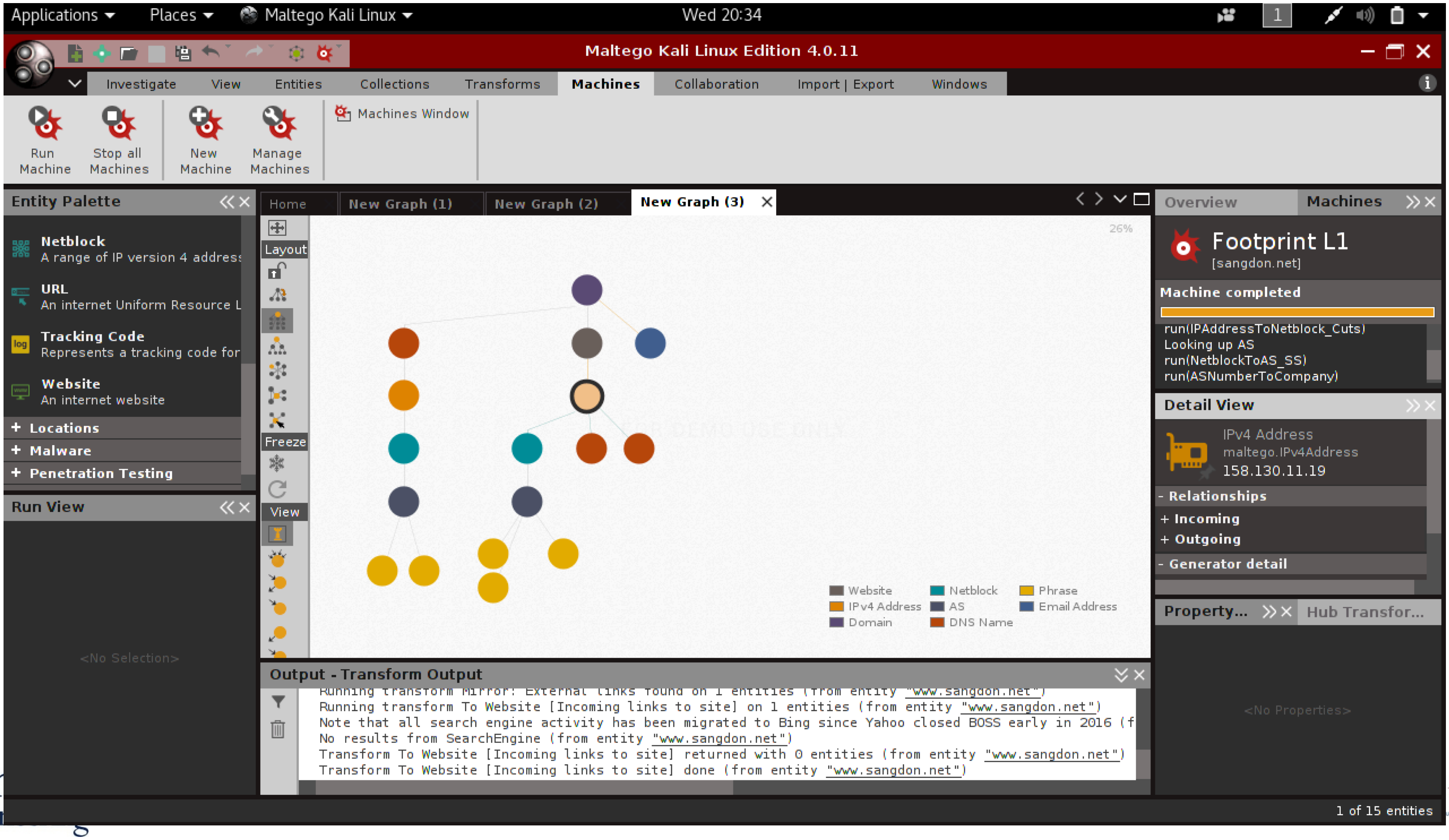
School of Engineering and Applied Science

University of Pennsylvania

March 17, 2017

Brief Introduction

- Software used for reconnaissance
  - Visualize publically available information



Footprint L1
[sangdon.net]

Machine completed

```
run(IPAddressToNetblock_Cuts)
Looking up AS
run(NetblockToAS_SS)
run(ASNumberToCompany)
```

IPv4 Address
maltego.IPv4Address
158.130.11.19

```
Running transform Mirror: External links found on 1 entities (from entity "www.sangdon.net")
Running transform To Website [Incoming links to site] on 1 entities (from entity "www.sangdon.net")
Note that all search engine activity has been migrated to Bing since Yahoo closed BOSS early in 2016 (f
No results from SearchEngine (from entity "www.sangdon.net")
Transform To Website [Incoming links to site] returned with 0 entities (from entity "www.sangdon.net")
Transform To Website [Incoming links to site] done (from entity "www.sangdon.net")
```

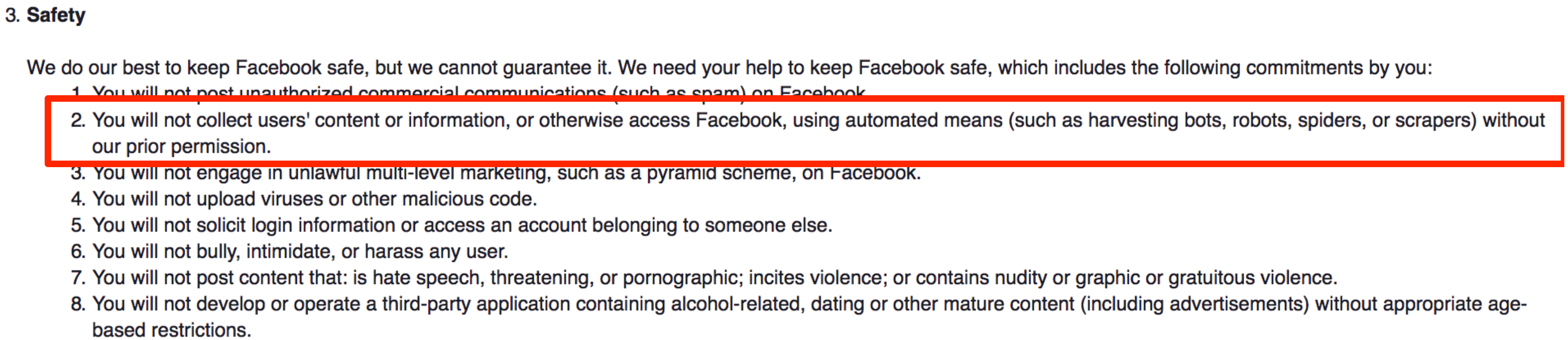
Terminology

- 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.

https://docs.paterva.com/en/user-guide/getting-started/

Caution!

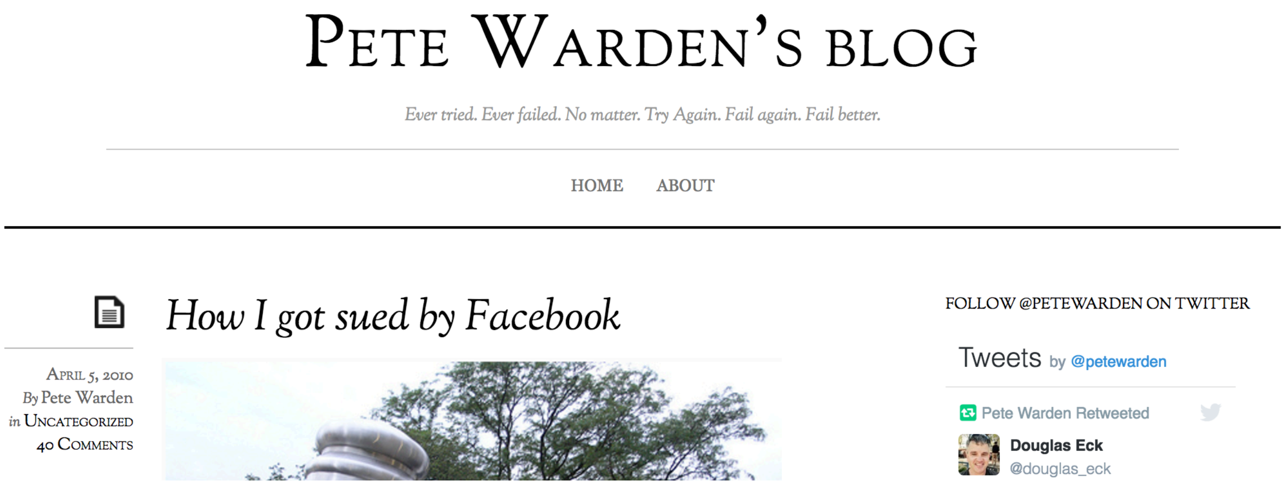
- Data crawling may be illegal depending on the terms of use of websites



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 Fa
10. You will not do any ttack or interference with page rendering or (
11. You will not facilitat



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

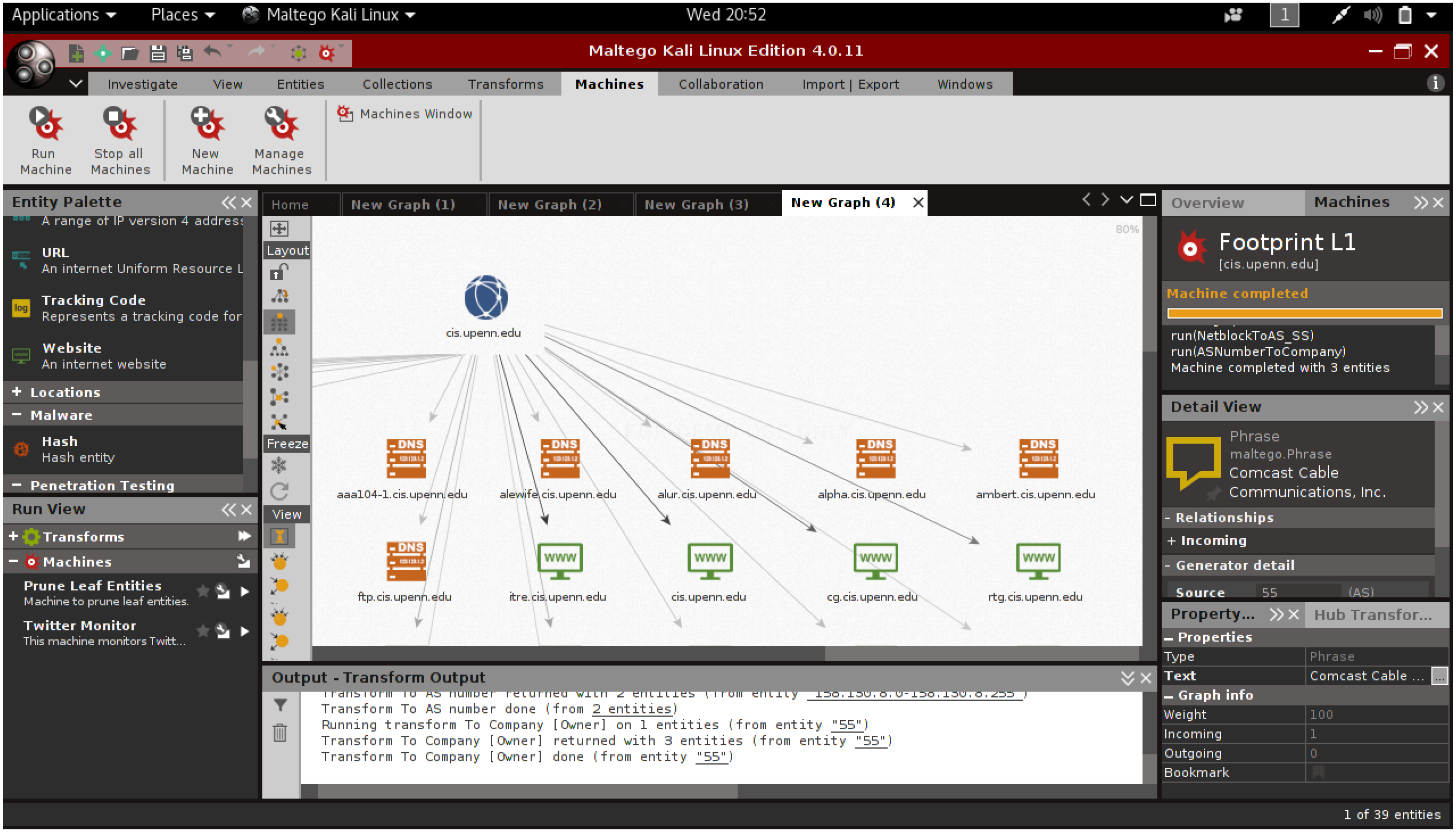
Pete Warden Retweeted

Douglas Eck
@douglas_eck

Penn Engineering

PRECISE

Run a machine



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

Phrase
maltego.Phrase
Comcast Cable Communications, Inc.

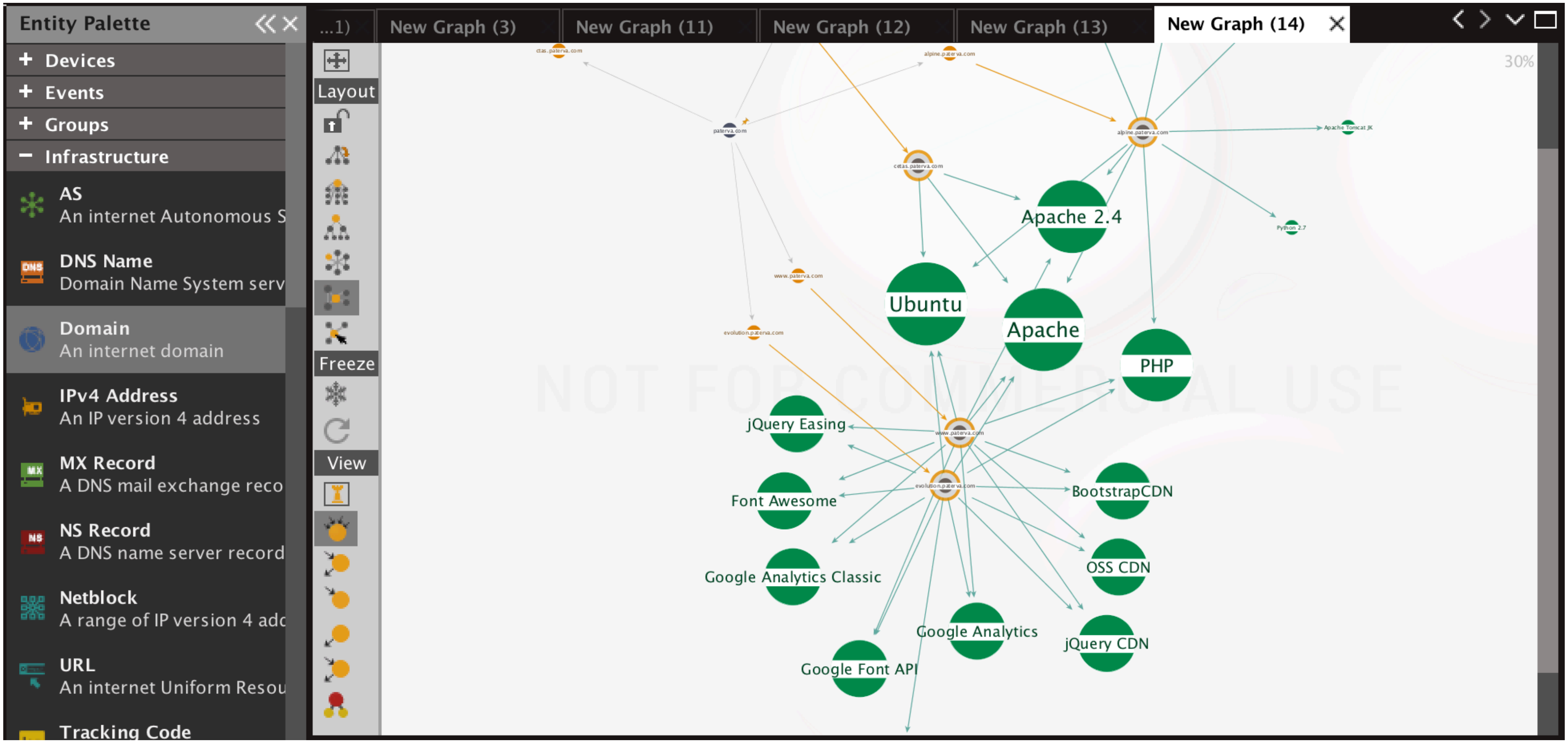
- Relationships
+ Incoming
- Generator detail

Source 55 (AS)

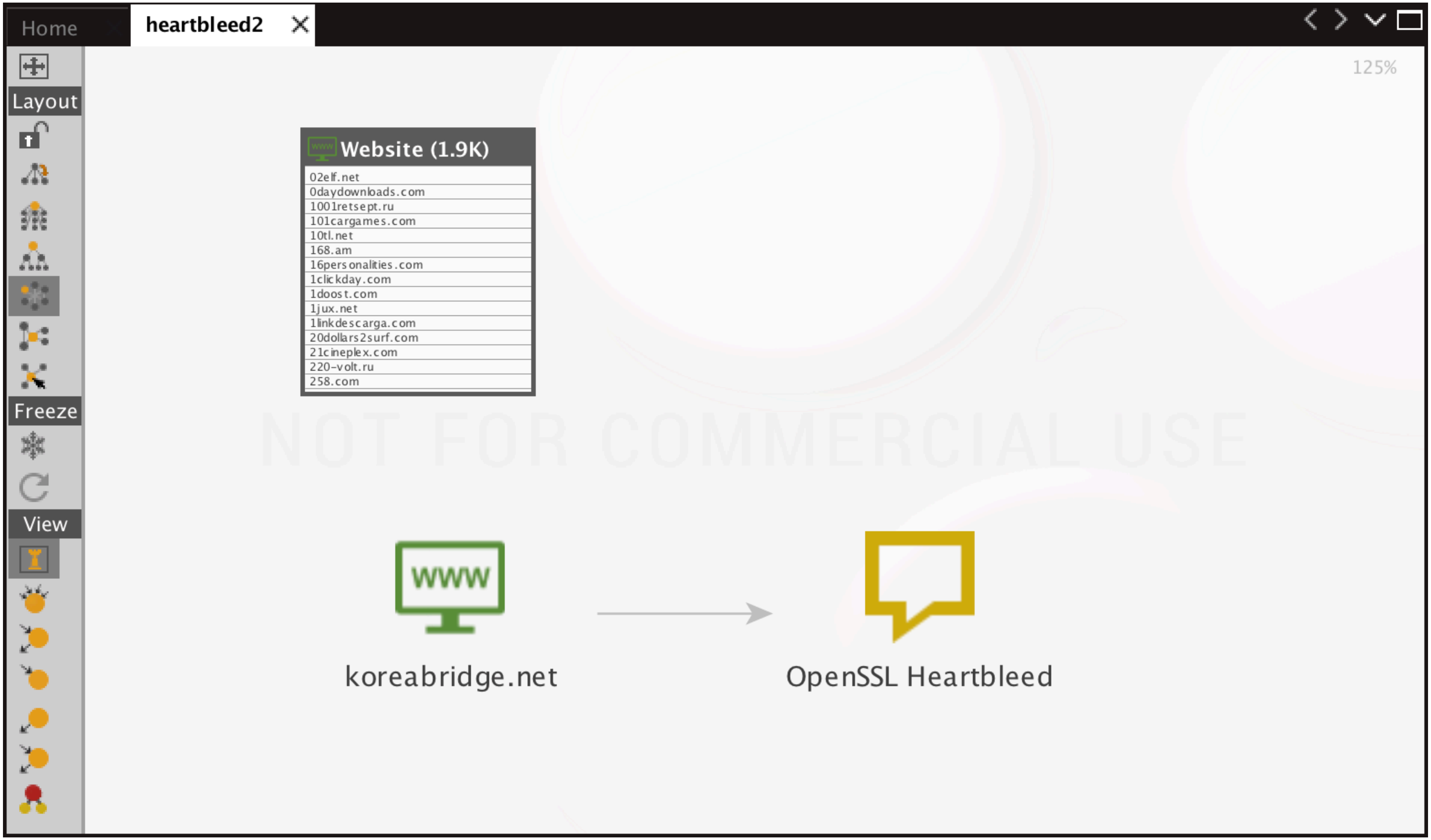
```
Transform To AS number returned with 2 entities (from entity "158.130.0.0-158.130.0.255")
Transform To AS number done (from 2 entities)
Running transform To Company [Owner] on 1 entities (from entity "55")
Transform To Company [Owner] returned with 3 entities (from entity "55")
Transform To Company [Owner] done (from entity "55")
```

– Properties	
Type	Phrase
Text	Comcast Cable ...
– Graph info	
Weight	100
Incoming	1
Outgoing	0
Bookmark	

Build My Entity Graph from Scratch



Maltego OpenSSL Heartbleed Transform

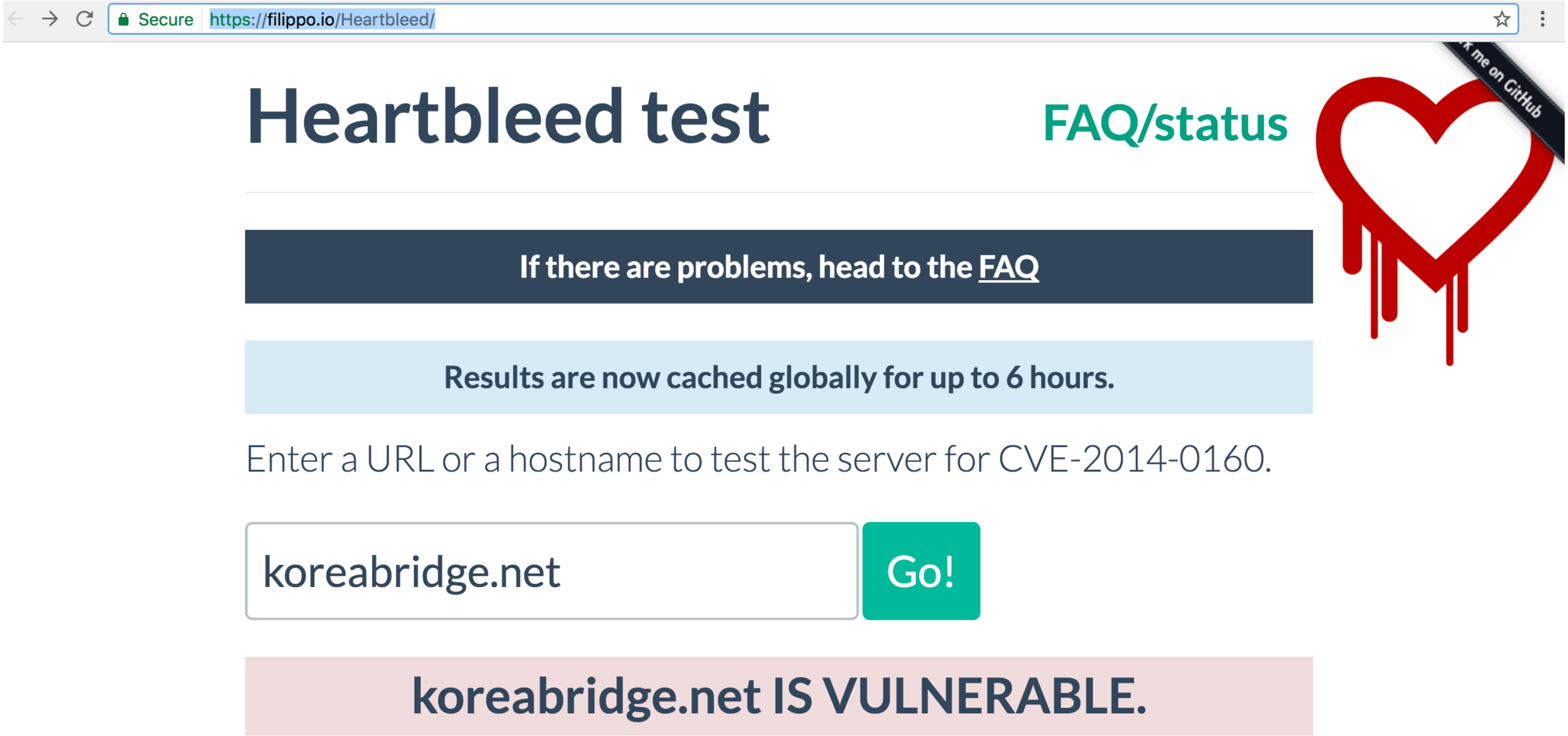


Website (1.9K)

02elf.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

https://disk0nn3ct.svbtle.com/maltego-openssl-heartbleed-transform

Maltego OpenSSL Heartbleed Transform



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.

koreabridge.net

Go!

koreabridge.net IS VULNERABLE.

Reference

- cis.upenn.edu/~sangdonp/demo-maltego.html

Practice Problems

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