TCP Input Text

Christian Heinrich aka “cmlh”

Updated: February 2012

TCP Input Text

Used in the “Recon” Phase of Penetration Test

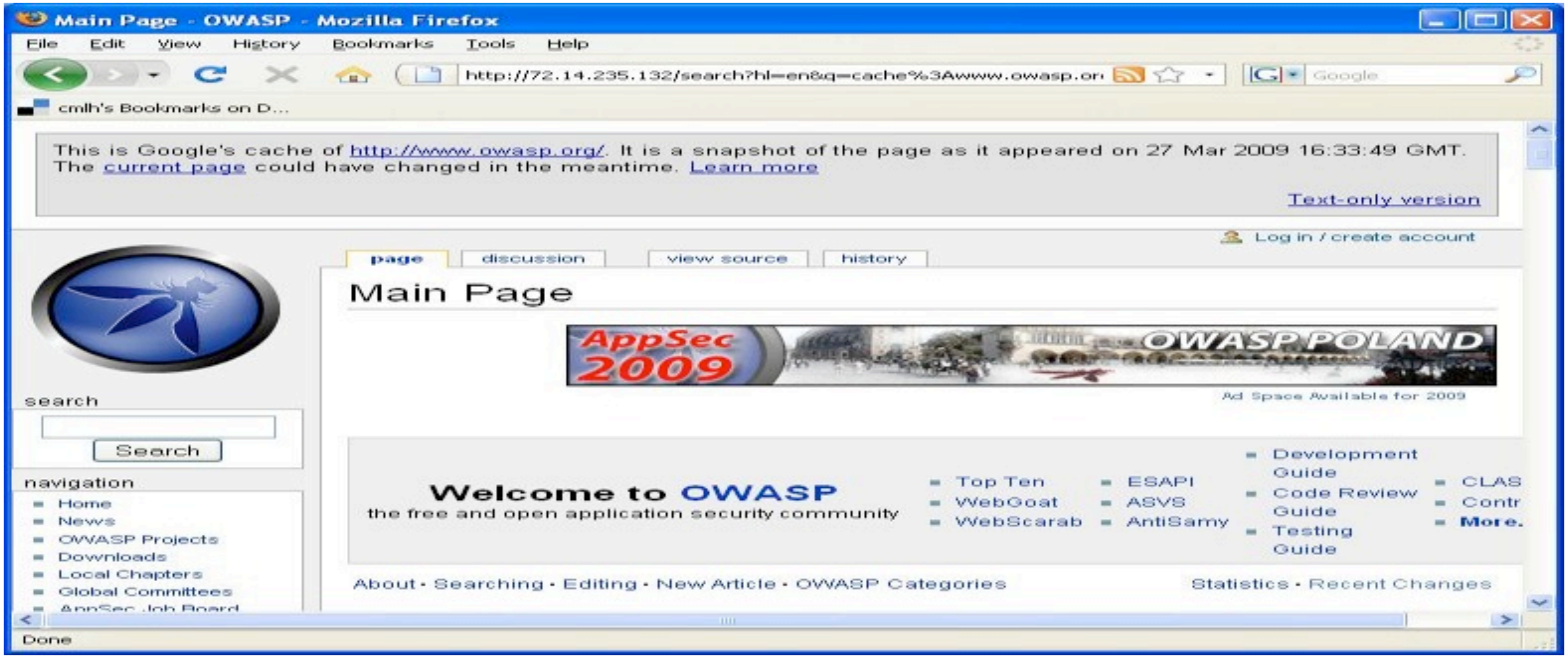
Enumerates FQDN and TCP Ports

Implements the

- Google SOAP Search API
- Bing API v2 (new)

cache:

May be out of date since last crawl by “Googlebot”



This is Google's cache of http://www.owasp.org/. It is a snapshot of the page as it appeared on 27 Mar 2009 16:33:49 GMT. The current page could have changed in the meantime. Learn more

Hence, positive assurance by **`nmap`**, **`nc`**, etc

Output Plug-In Architecture

TCP Port and FQDN

- **`nmap`**
- netcat aka **`nc`**
- **`maltego (new)`**
- `.csv` File

Output Files written to

`./[`*`query`*`]/tit/Bing|Google`

Regular Expression

```
=~m|(\w+)://([^/:]+)(:\d+)?/(.*)|;

my $Protocol = $1;
my $Domain_Name = $2;
my $URI = ("/" . $4);  // discarded
if ($3 =~ /:(\d+)/) {$TCP_Port = $1}
  else {$TCP_Port = 80}
```

`tit_FQDN.csv`

Forward Lookup with **`dig`** and/or **`nslookup`**

Scan for TCP Ports *not* within Search Results.

- Neither TCP/80 or TCP/443

Output Files written to

`./[`*`query`*`]/tit/Bing|Google`

`tit_FQDN.csv` Example

```
glcfapp.umiacs.umd.edu
www.speedguide.net
inside.c-spanarchives.org
www.wsu.edu
torrents.freebsd.org
sammelpunkt.philo.at
arc.cs.odu.edu
www.ripn.net
phy043.tours.inra.fr
202.188.95.52
```

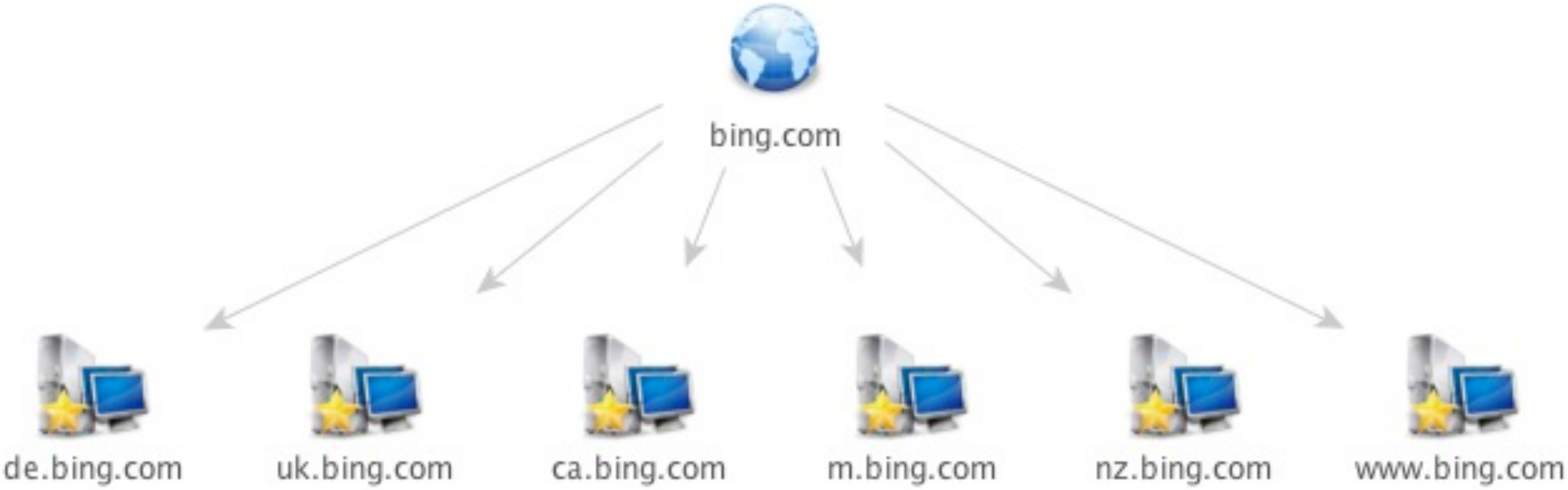
tit_FQDN_TCP.csv Example

```
glcfapp.umiacs.umd.edu,8080
www.speedguide.net,8080
inside.c-spanarchives.org,8080
www.wsu.edu,8080
torrents.freebsd.org,8080
sammelpunkt.philo.at,8080
arc.cs.odu.edu,8080
www.ripn.net,8080
phy043.tours.inra.fr,8080
202.188.95.52,8080
```

`tit_maltego.csv` Example

```
ca.bing.com,http,80
de.bing.com,http,80
m.bing.com,http,80
nz.bing.com,http,80
uk.bing.com,http,80
www.bing.com,http,80
```

`tit_maltego.csv` Example



`tit_nc.sh` Example

```
nc -vz glcfapp.umiacs.umd.edu 8080
nc -vz www.speedguide.net 8080
nc -vz inside.c-spanarchives.org 8080
nc -vz www.wsu.edu 8080
nc -vz torrents.freebsd.org 8080
nc -vz sammelpunkt.philo.at 8080
nc -vz arc.cs.odu.edu 8080
nc -vz www.ripn.net 8080
nc -vz phy043.tours.inra.fr 8080
nc -vz 202.188.95.52 8080
```

`tit_nmap.sh` Example

```
nmap -PN -sT -p T:8080 glcfapp.[snip]
nmap -PN -sT -p T:8080 www.spee[snip]
nmap -PN -sT -p T:8080 inside.c[snip]
nmap -PN -sT -p T:8080 www.wsu.edu
nmap -PN -sT -p T:8080 torrents[snip]
nmap -PN -sT -p T:8080 sammelpu[snip]
nmap -PN -sT -p T:8080 arc.cs.odu.edu
nmap -PN -sT -p T:8080 www.ripn.net
nmap -PN -sT -p T:8080 phy043.t[snip]
nmap -PN -sT -p T:8080 202.188.95.52
```

Output Plug-In Architecture

To remove duplicate entries

```
cmlh$ sort file | uniq > nodups_file
```

Output Files written to

`./[query]/tit/Bing|Google`

DataDumper.txt Example

```
$VAR1 = bless( {
  'searchTime' => '0.116592',
  'endIndex' => '10',
  'searchComments' => '',
  'documentFiltering' => 0,
  'searchTips'
  'estimatedTota
  '51700000',
  'searchQuery' => 'inurl:8080',
  'startIndex' => '1',
  'resultElements' => [
     bless( {
                [SNIP]
```

Deprecated for json_debug_log.txt

`json_debug_log.txt`

Divided into three major sections marked with “#”:

1. `$bing_json_url`
2. `$bing_http_request->get($bing_json_url)->content`
3. `decode_json($bing_http_response)->{SearchResponse}->{Web}->{Results}`

`Smart::Comments` are also supported for v0.3.

`tit` Roadmap

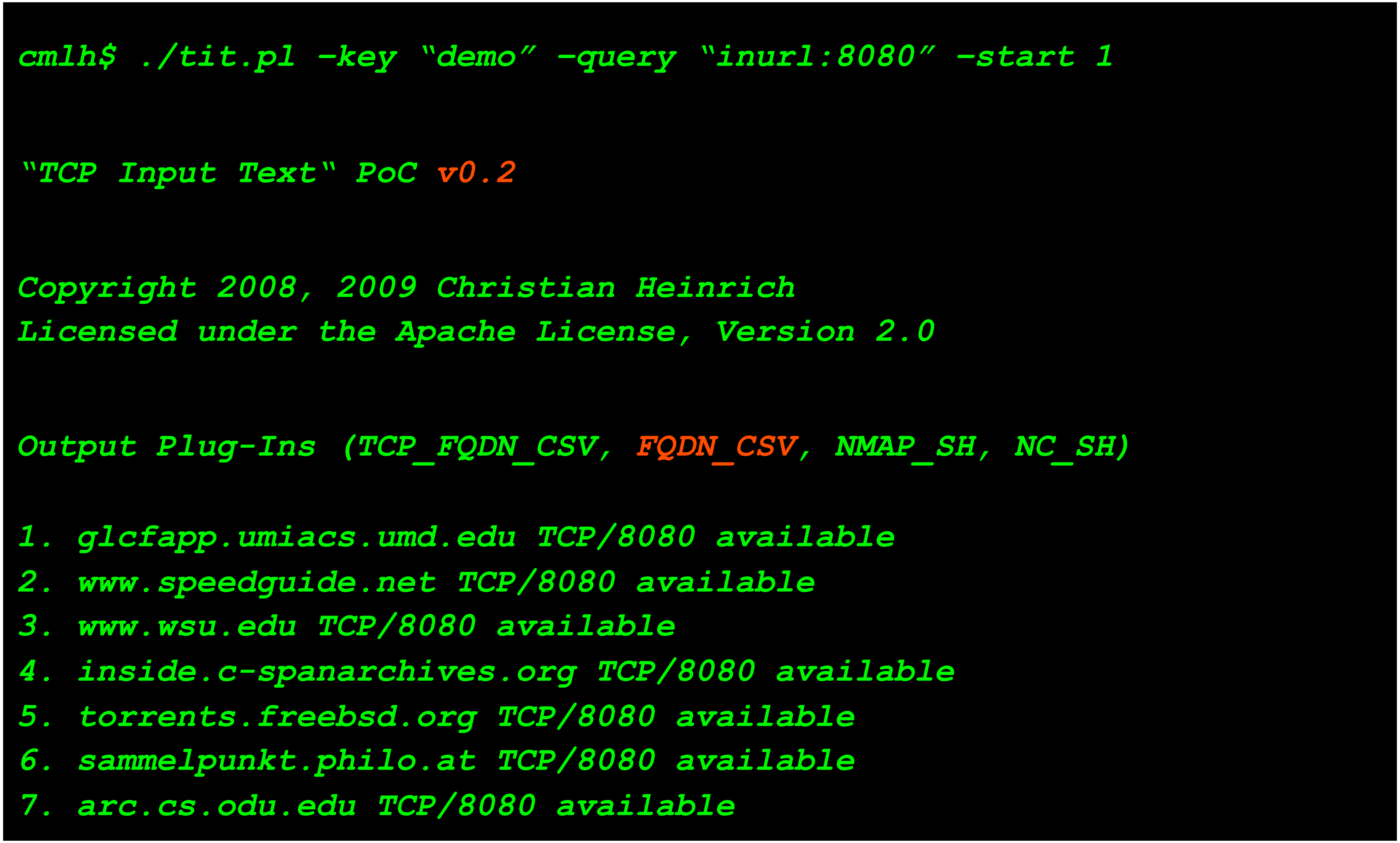
PoC v0.1 (RUXCON 2K8 in Sydney, AU, Nov 2008)

- Previewed at ToorCon(US) and SecTor (CA)

Alpha v0.2 (SyScan’09 Singapore)

- Moving repository to `code.google.com/p/tit`
- Added FQDN Output Plug-In
- Previewed at OWASP AU 2009 (February) and 5th CONFidence 2009 (Poland)

Changes from v0.1 to v0.2



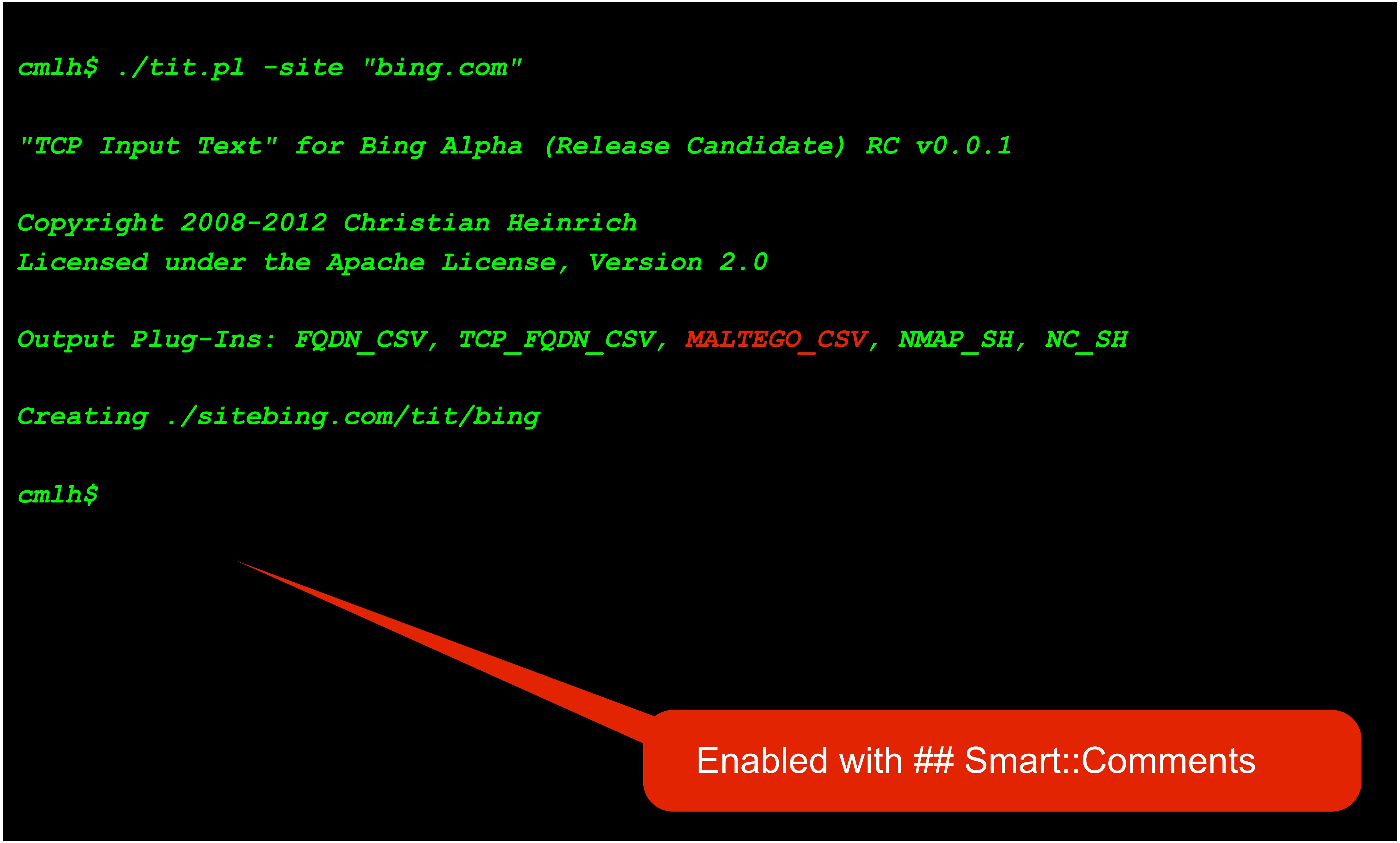
```
cmlh$ ./tit.pl -key “demo” -query “inurl:8080” -start 1


“TCP Input Text“ PoC v0.2


Copyright 2008, 2009 Christian Heinrich
Licensed under the Apache License, Version 2.0


Output Plug-Ins (TCP_FQDN_CSV, FQDN_CSV, NMAP_SH, NC_SH)

1. glcfapp.umiacs.umd.edu TCP/8080 available
2. www.speedguide.net TCP/8080 available
3. www.wsu.edu TCP/8080 available
4. inside.c-spanarchives.org TCP/8080 available
5. torrents.freebsd.org TCP/8080 available
6. sammelpunkt.philo.at TCP/8080 available
7. arc.cs.odu.edu TCP/8080 available
```

`tit` Roadmap

Alpha v0.3

- Support for Bing API v2
  - Repository at `tit.codeplex.com`
- Maltego Local Transform (CSV)
  - Repository at `github.com/cmlh/maltego`

Changes from v0.2 to v0.3



```
cmlh$ ./tit.pl -site "bing.com"

"TCP Input Text" for Bing Alpha (Release Candidate) RC v0.0.1

Copyright 2008-2012 Christian Heinrich
Licensed under the Apache License, Version 2.0

Output Plug-Ins: FQDN_CSV, TCP_FQDN_CSV, MALTEGO_CSV, NMAP_SH, NC_SH

Creating ./sitebing.com/tit/bing

cmlh$
```

Enabled with ## Smart::Comments

`tit` Roadmap

Beta v0.4 and onwards

- Merge **`tit-google-soap.pl`** and **`tit-bing.pl`**
  - Repository at **`github.com/cmlh/dic`**
- **`sub output_plugin`**
  - curl and/or wget (i.e. replay web intercepting proxy)
  - Google Translate (Speak English or Die)

Questions

Latest Slides Available From:

- **http://slideshare.net/cmlh/tit**
- **https://github.com/cmlh/tit**

Contact:

- **christian.heinrich@cmlh.id.au**
- **http://cmlh.id.au/contact**