Untangle: Multi-Layer Web Server Fingerprinting

Cem Topcuoglu, Kaan Onarlioglu*, Barhuz Jabiyev, Engin Kirda

Northeastern University, *Akamai Technologies, Darthmouth College

Web server fingerprinting

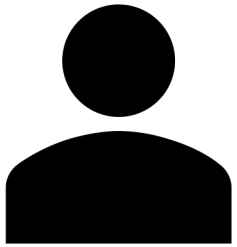
- Reconnaissance
- Security management
  - Asset discovery
  - Vulnerability tracking
- Attack surface discovery

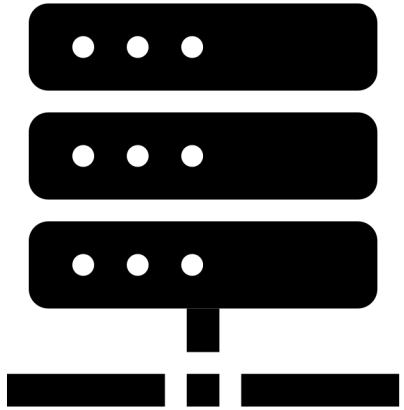
Web server fingerprinting

- Reconnaissance
- Security management
  - Asset discovery
  - Vulnerability tracking
- Attack surface discovery

- Tools: Nmap, Nessus

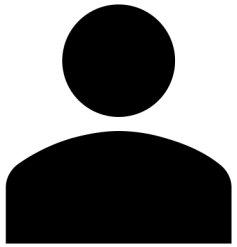
Monolithic web

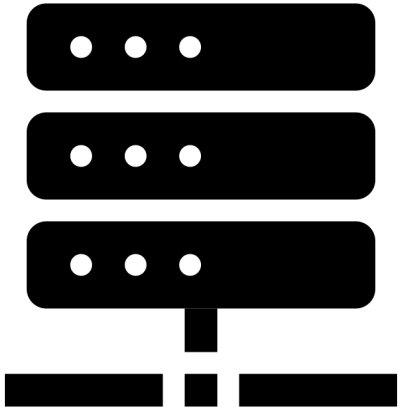




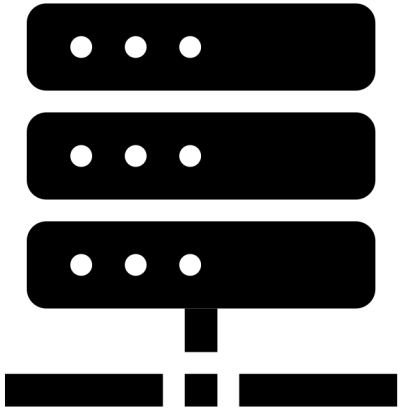
NGINX

Tangled web

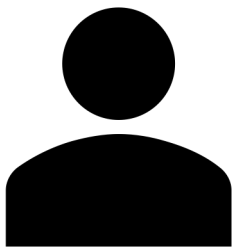




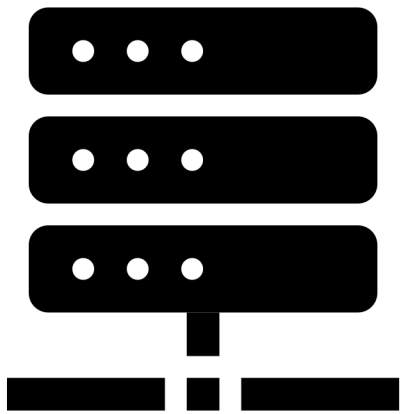
Cloudflare



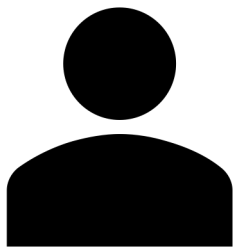
NGINX



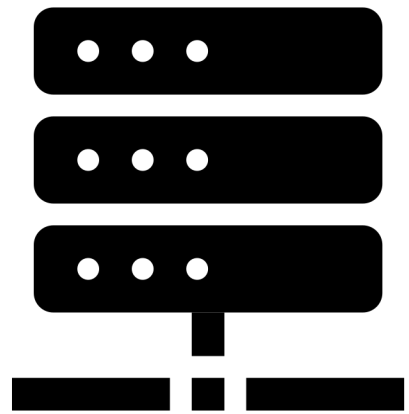
,GET / HTTP/1.1
Host: dummy.com
…



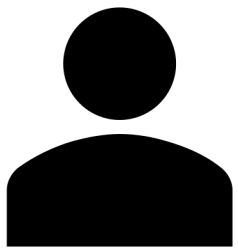
NGINX



,GET / HTTP/1.1
Host: dummy.com
…



NGINX



HAProxy

```
HTTP/1.1 400 Bad request
Host: dummy.com
…
```

ATS

```
HTTP/1.1 400 Invalid HTTP Request
Host: dummy.com
…
```

NGINX

```
HTTP/1.1 400 Bad Request
Host: dummy.com
Server: NGINX
…
```

HAProxy

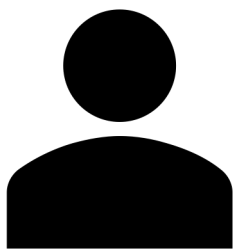
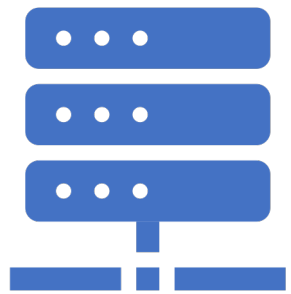
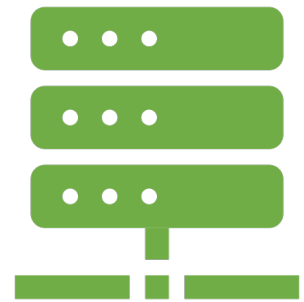
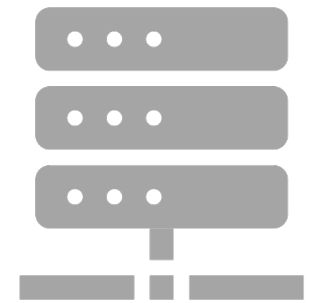
```
HTTP/1.1 400 Bad request
Host: dummy.com
…
```

ATS

```
HTTP/1.1 400 Invalid HTTP Request
Host: dummy.com
…
```

NGINX

```
HTTP/1.1 400 Bad Request
Host: dummy.com
Server: NGINX
…
```


Is it NGINX? Are there additional layers? Which one is NGINX?

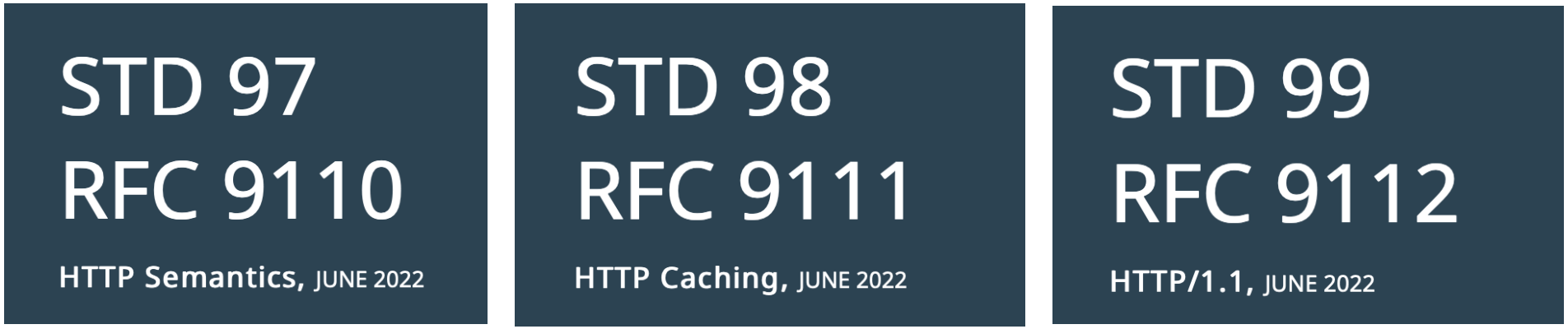
Our approach: Untangle

Use HTTP processing discrepancies to fingerprint **everything**!

Both server type and order.

Processing discrepancies

- RFCs are open to interpretation
- Implementation and design choices



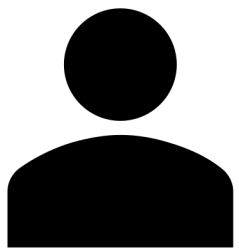
Case study

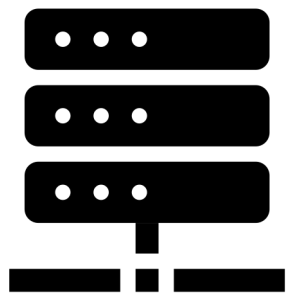
Let’s assume we have a

Behavior Repository

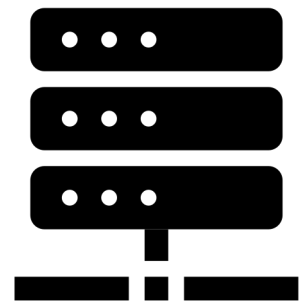
that includes requests and corresponding behaviors of each server to these requests

Behavior Repository			
	Request 1	Apache:	Returns an Error
		ATS:	Returns an Error
		NGINX:	Returns an Error
		...:	Returns an Error
		Cloudflare:	Returns an Error
	Request 2	Apache:	Returns an Error
		ATS:	Returns an Error
		NGINX:	Forwards
		...:	Returns an Error
		Cloudflare:	Returns an Error

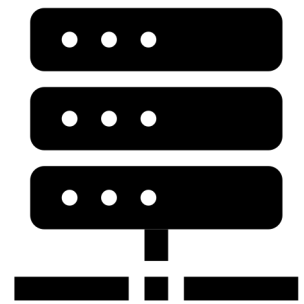




Cloudflare

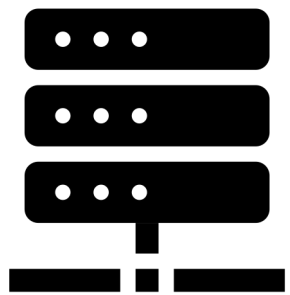


Squid

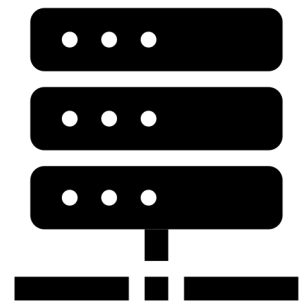


Tomcat

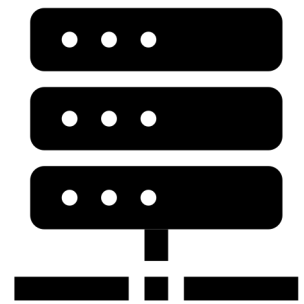
Untangle



Cloudflare



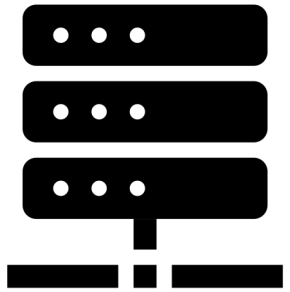
Squid



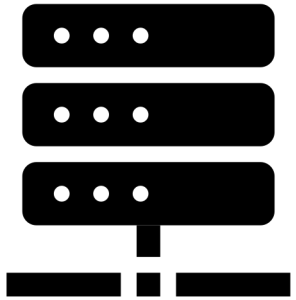
Tomcat

Untangle finds a request such that all servers return an error

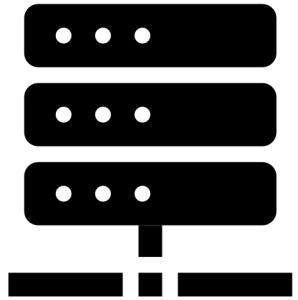
Untangle



Cloudflare



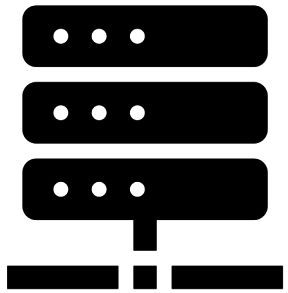
Squid



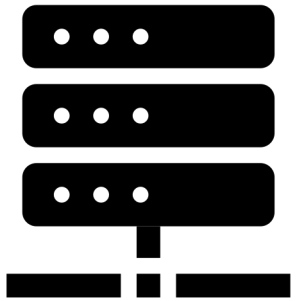
Tomcat

Behavior Repository		
	Request 1	Cloudflare: Returns an error
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 2	Cloudflare: Forwards
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 3	Cloudflare: Forwards
		Squid: Forwards
		Tomcat: Returns an error
		...: Returns an error
		Haproxy: Returns an error

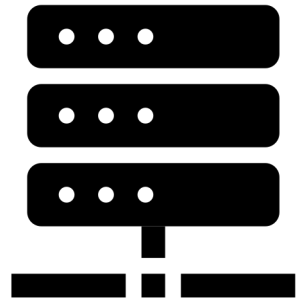
Untangle



Cloudflare



Squid

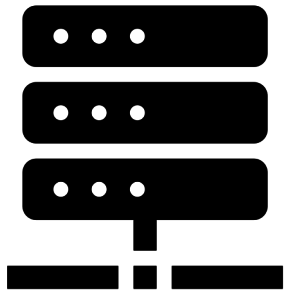


Tomcat

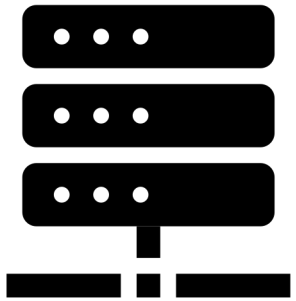
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

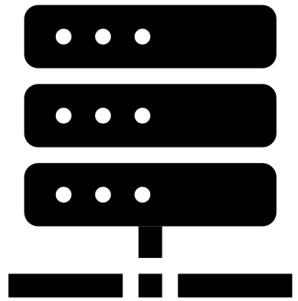
Request 1



Cloudflare



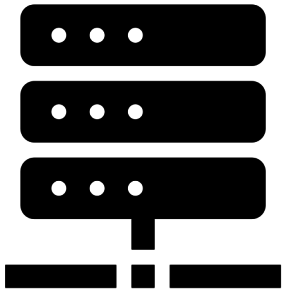
Squid



Tomcat

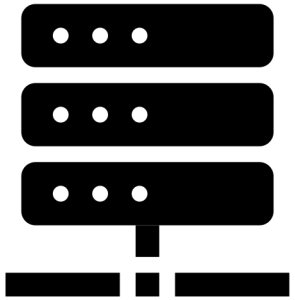
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

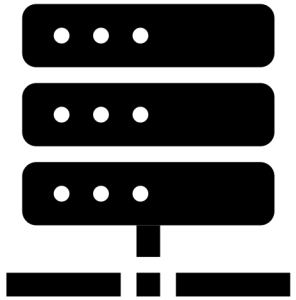


Cloudflare

Request 1



Squid

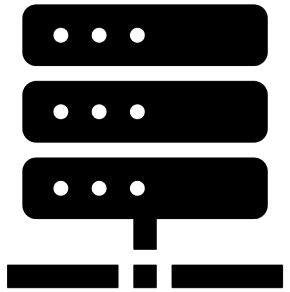


Tomcat

Behavior Repository

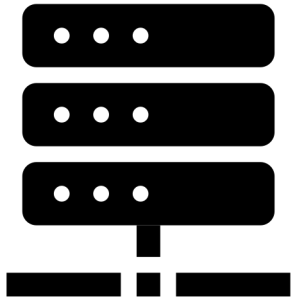
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

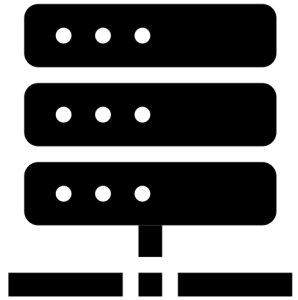


Cloudflare

Error response



Squid



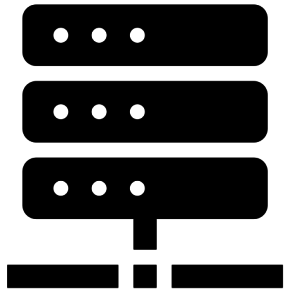
Tomcat

Behavior Repository

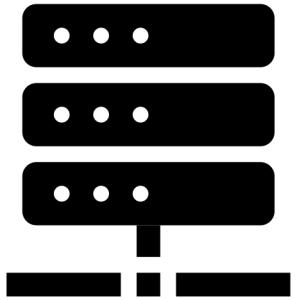
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

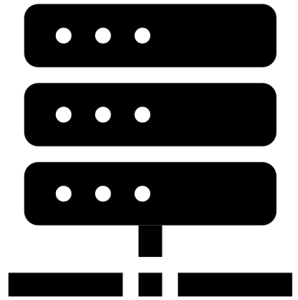
Error response



Cloudflare



Squid

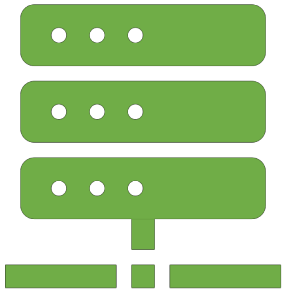


Tomcat

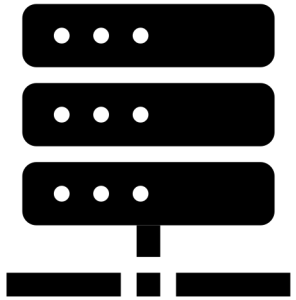
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

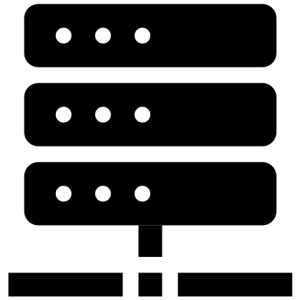
Error response



Cloudflare



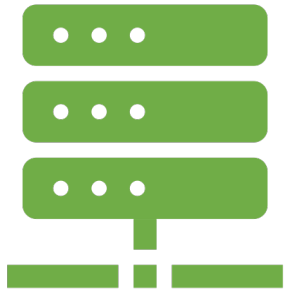
Squid



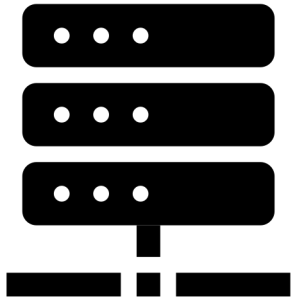
Tomcat

Untangle finds a request such that all servers return an error, except Cloudflare forwards the request

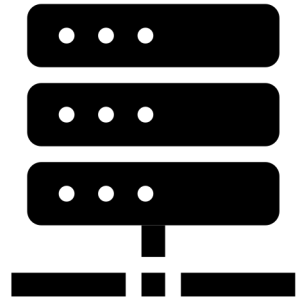
Untangle



Cloudflare



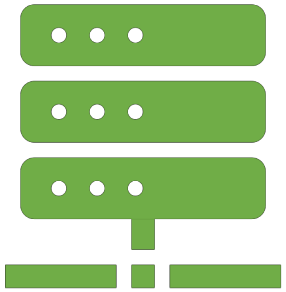
Squid



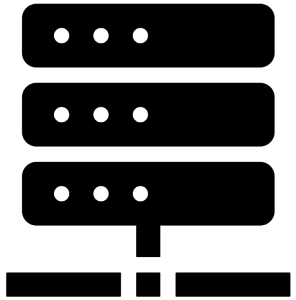
Tomcat

Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

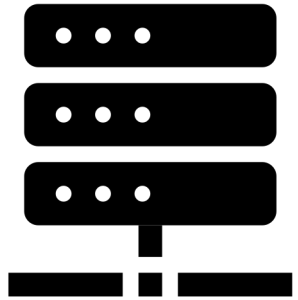
Untangle



Cloudflare



Squid

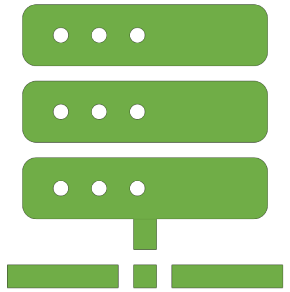


Tomcat

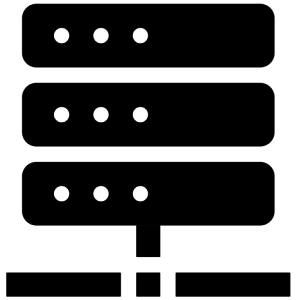
Behavior Repository		
	Request 1	Cloudflare: Returns an error
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 2	Cloudflare: Forwards
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 3	Cloudflare: Forwards
		Squid: Forwards
		Tomcat: Returns an error
		...: Returns an error
		Haproxy: Returns an error

Untangle

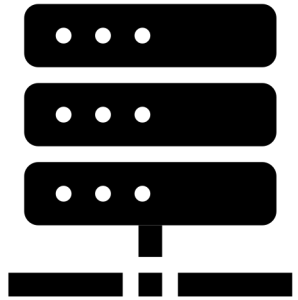
Request 2



Cloudflare



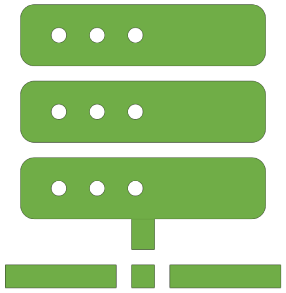
Squid



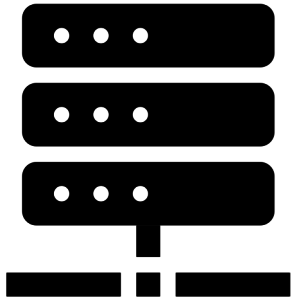
Tomcat

Behavior Repository		
	Request 1	Cloudflare: Returns an error
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 2	Cloudflare: Forwards
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 3	Cloudflare: Forwards
		Squid: Forwards
		Tomcat: Returns an error
		...: Returns an error
		Haproxy: Returns an error

Untangle

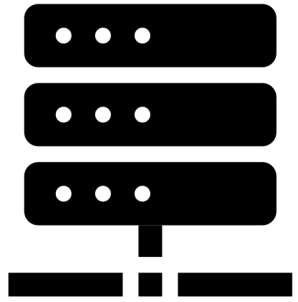


Cloudflare



Squid

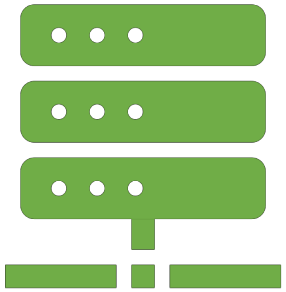
Request 2



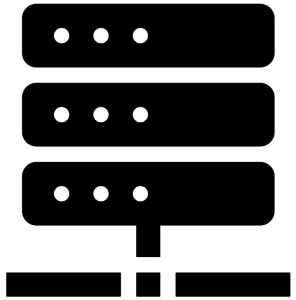
Tomcat

Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

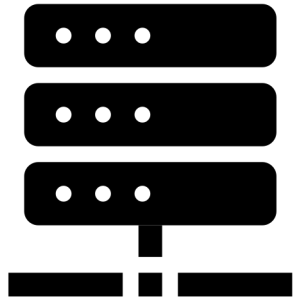


Cloudflare



Squid

Error response

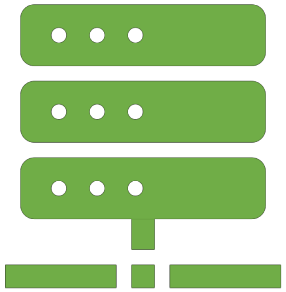


Tomcat

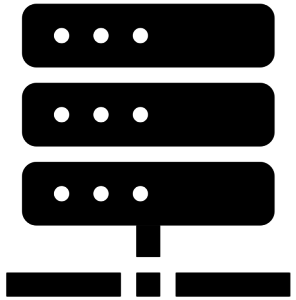
Behavior Repository		
	Request 1	Cloudflare: Returns an error
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 2	Cloudflare: Forwards
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 3	Cloudflare: Forwards
		Squid: Forwards
		Tomcat: Returns an error
		...: Returns an error
		Haproxy: Returns an error

Untangle

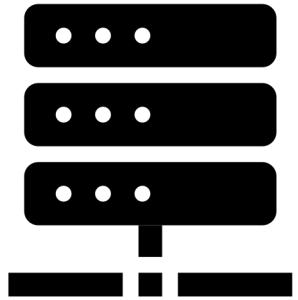
Error response



Cloudflare



Squid

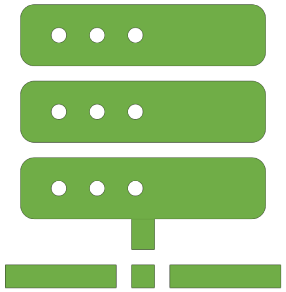


Tomcat

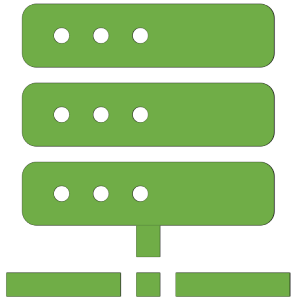
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

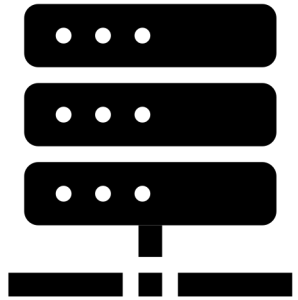
Error response



Cloudflare



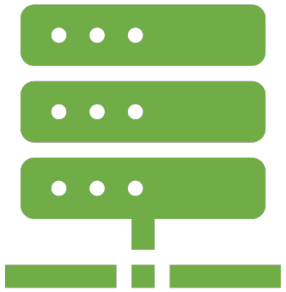
Squid



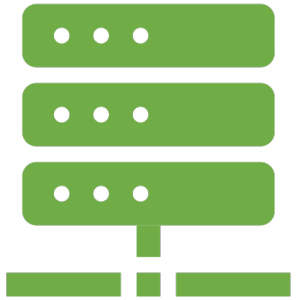
Tomcat

Untangle finds a request such that all servers return an error, except Cloudflare and Squid forward the request

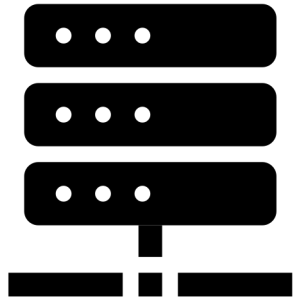
Untangle



Cloudflare



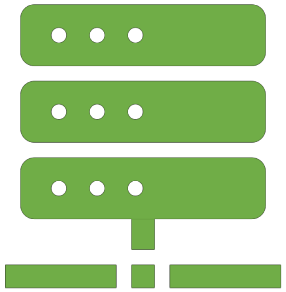
Squid



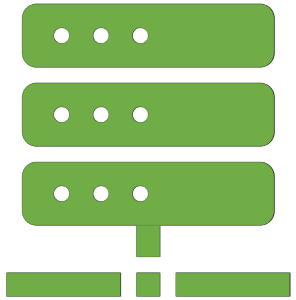
Tomcat

Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

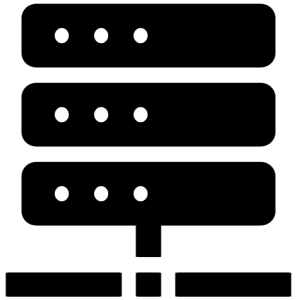
Untangle



Cloudflare



Squid

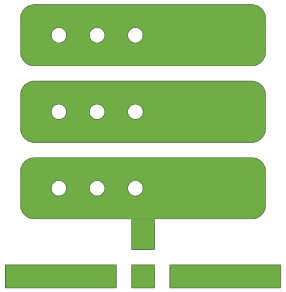


Tomcat

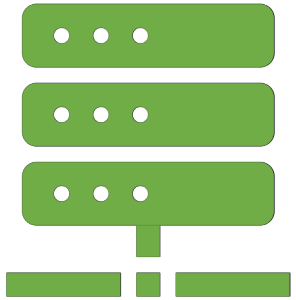
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

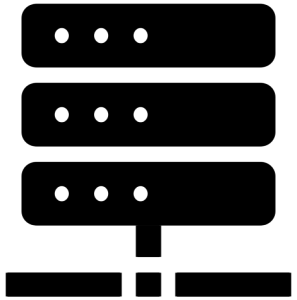
Request 3



Cloudflare



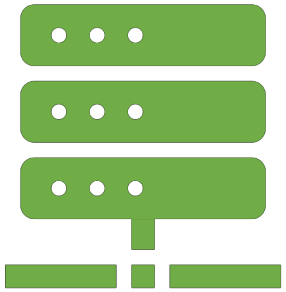
Squid



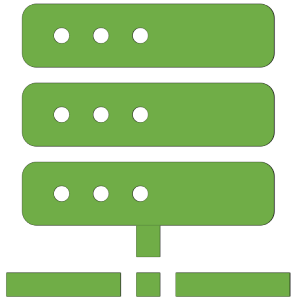
Tomcat

Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

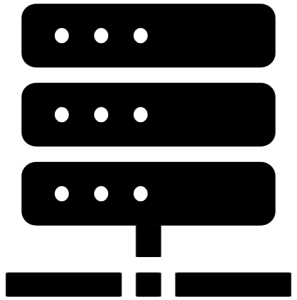
Untangle



Cloudflare



Squid

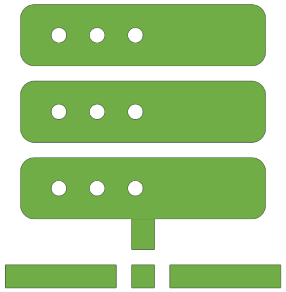


Tomcat

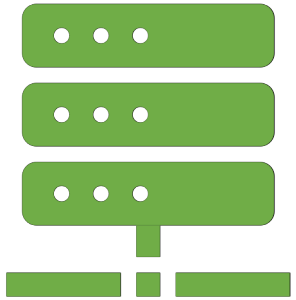
Request 3

Behavior Repository		
	Request 1	Cloudflare: Returns an error
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 2	Cloudflare: Forwards
		Squid: Returns an error
		Tomcat: Returns an error
		...: Returns an error
		HAProxy: Returns an error
	Request 3	Cloudflare: Forwards
		Squid: Forwards
		Tomcat: Returns an error
		...: Returns an error
		Haproxy: Returns an error

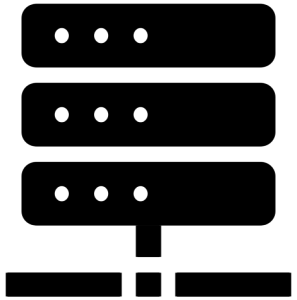
Untangle



Cloudflare



Squid



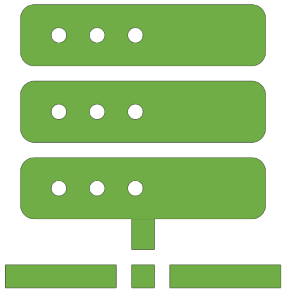
Tomcat

Error response

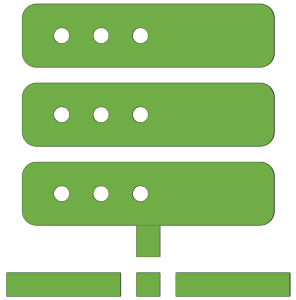
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

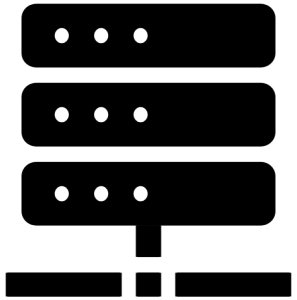
Error response



Cloudflare



Squid

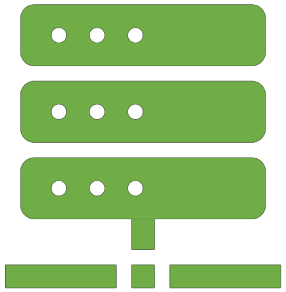


Tomcat

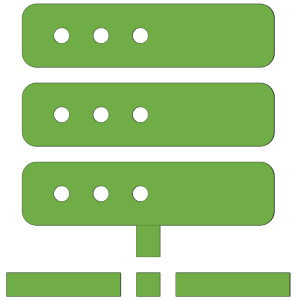
Behavior Repository		
Request 1	Cloudflare:	Returns an error
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 2	Cloudflare:	Forwards
	Squid:	Returns an error
	Tomcat:	Returns an error
	...:	Returns an error
	HAProxy:	Returns an error
Request 3	Cloudflare:	Forwards
	Squid:	Forwards
	Tomcat:	Returns an error
	...:	Returns an error
	Haproxy:	Returns an error

Untangle

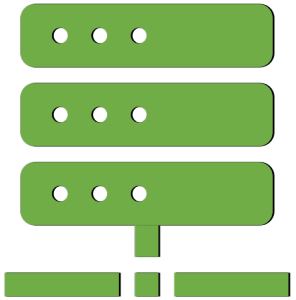
Error response



Cloudflare



Squid



Tomcat

Untangle in real life

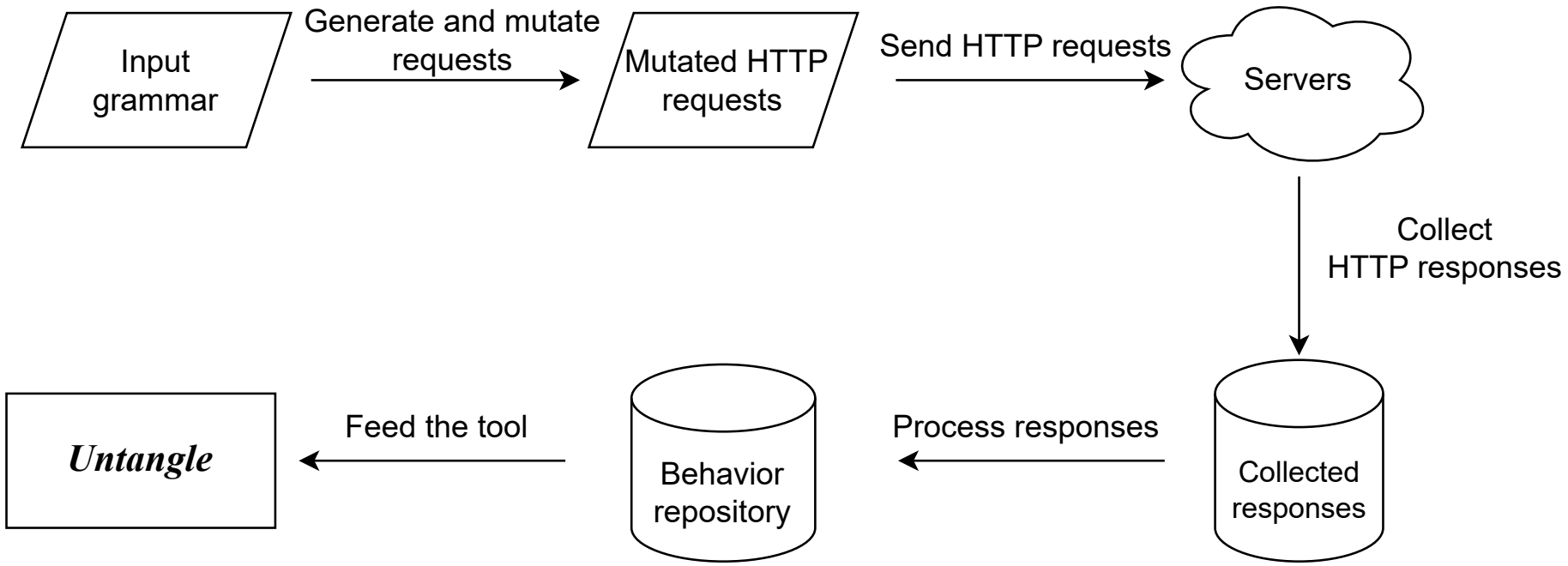
- We do not know if our behavior repository is complete
  - There might not be discrepancies between every server
  - Even if there are, we might not be able to find them

Untangle in real life

- We do not know if our behavior repository is complete
  - There might not be discrepancies between every server
  - Even if there are, we might not be able to find them
- Untangle can work with an incomplete behavior repository
  - Presents complete or partially ordered results
  - For details, please refer to the paper

Creating the behavior repository

- Pick common web servers, load balancers, CDNs (13 in total)
- Differential fuzzing



Evaluation

- Deployed 3-layered topologies
- All viable permutations of the 13 servers and tested them using Untangle

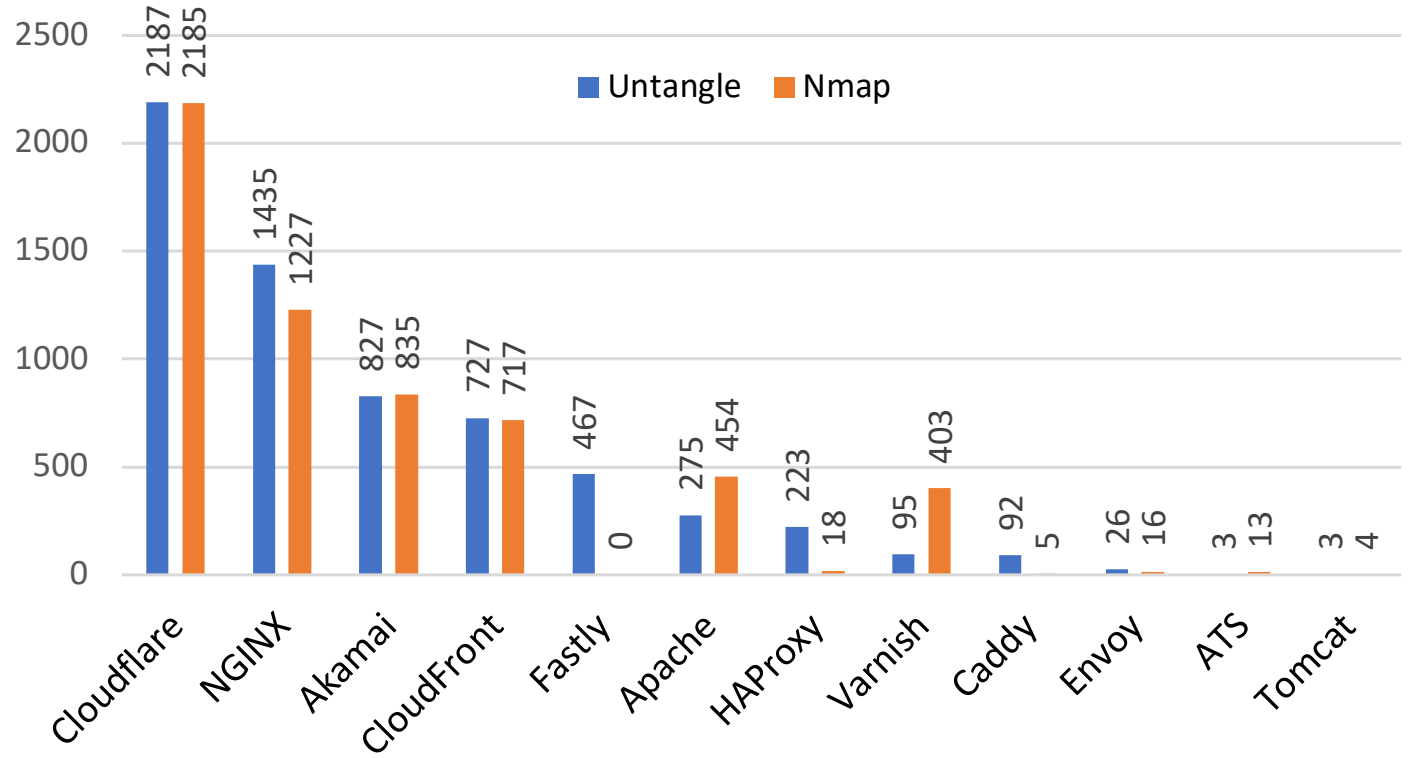
Evaluation

Experiment	Layer 1	Layer 2	Layer 3
Untangle	756 (100.0%)	683 (90.3%)	383 (50.7%)

Evaluation

Experiment	Layer 1	Layer 2	Layer 3
Untangle	756 (100.0%)	683 (90.3%)	383 (50.7%)
Nmap	450 (59.5%)	0 (0.00%)	0 (0.00%)

Testing in the wild



Conclusion

Novel

and the first way to fingerprint multi-layered web servers

Source code

- https://github.com/cemtopcuoglu/untangle
- Please report your experiences by using on your server

Thank you!

Any Questions?

Cem Topcuoglu

topcuoglu.c@northeastern.edu

cemtopcuoglu.com