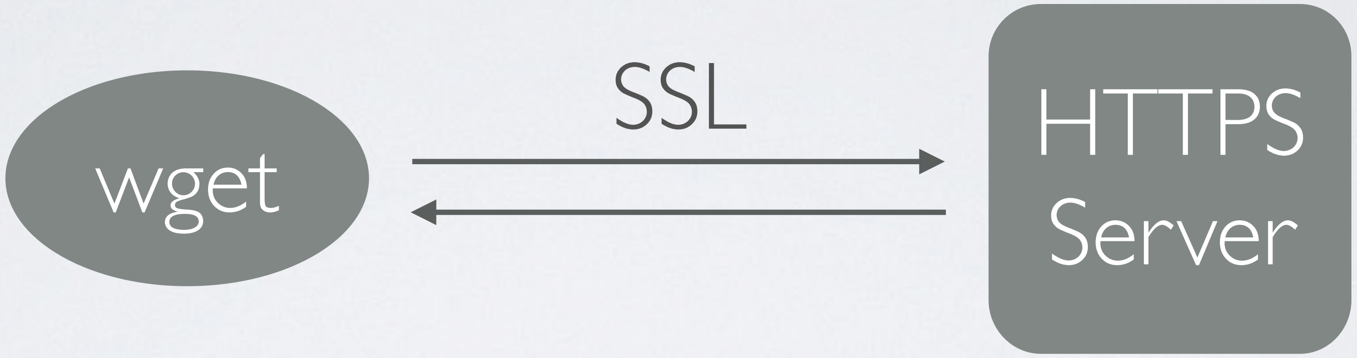
Implementation-Based Characterization Of Network Flows

Stephen Magill, Joseph Ranweiler, David Burke

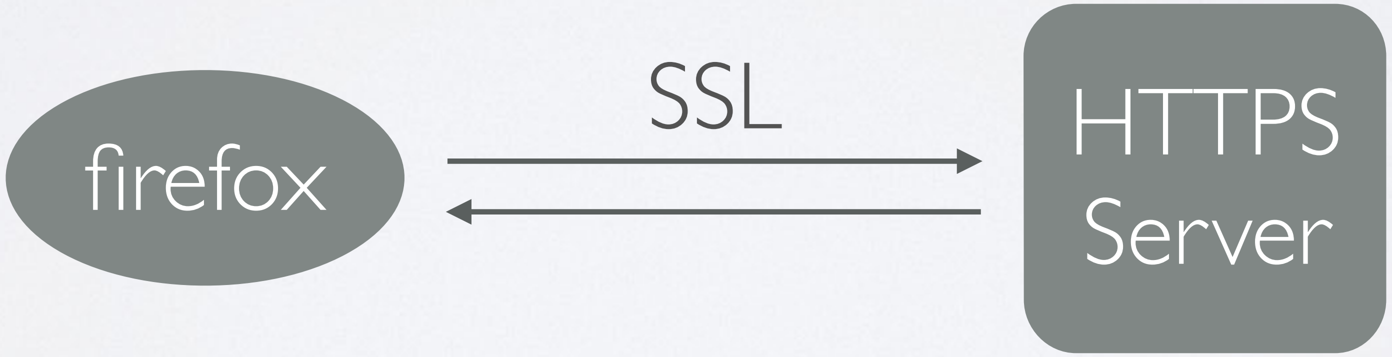
galois

QUESTION

Does this:



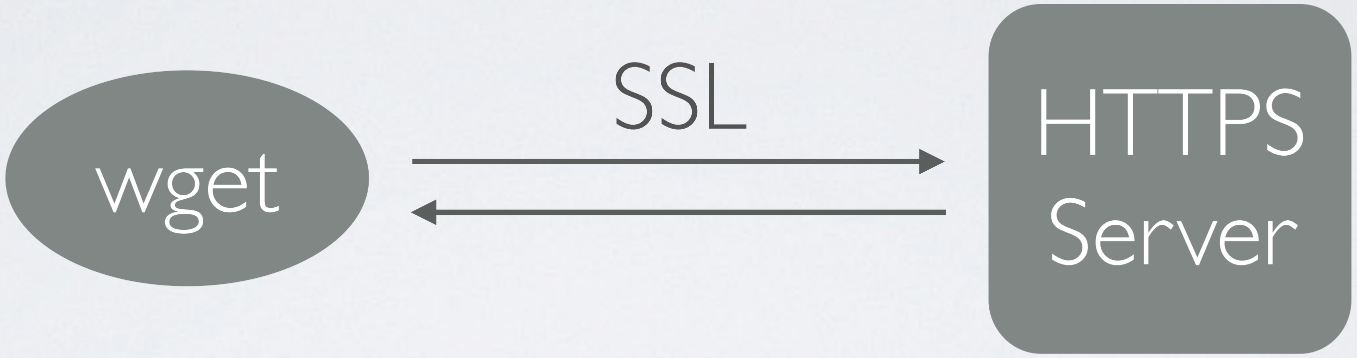
Look different from this:



?

QUESTION

Does this:

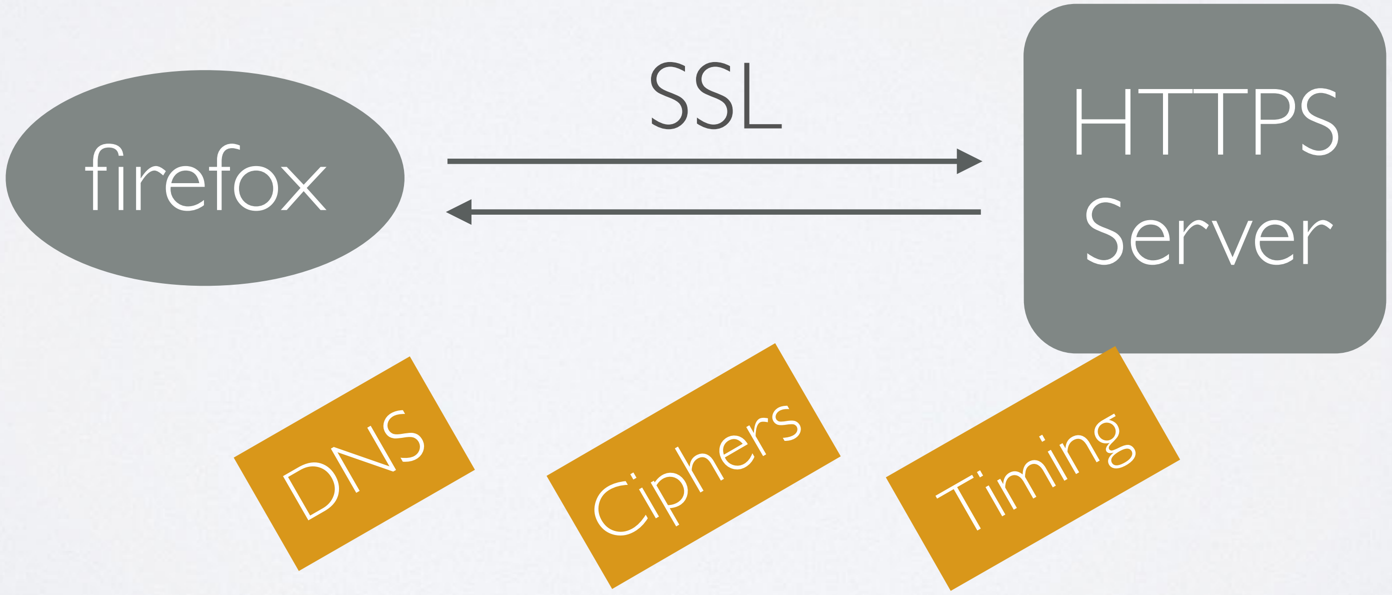


wget

SSL

HTTPS Server

Look different from this:



firefox

SSL

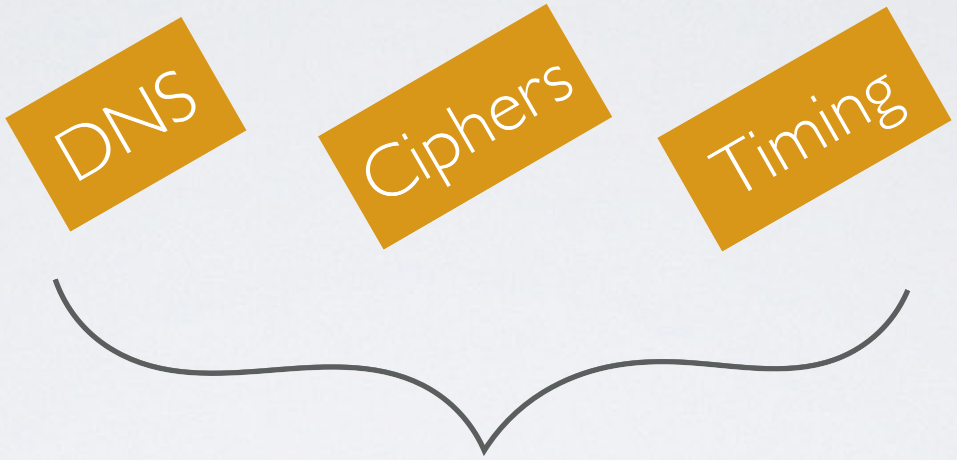
HTTPS Server

DNS

Ciphers

Timing

OBSERVATION



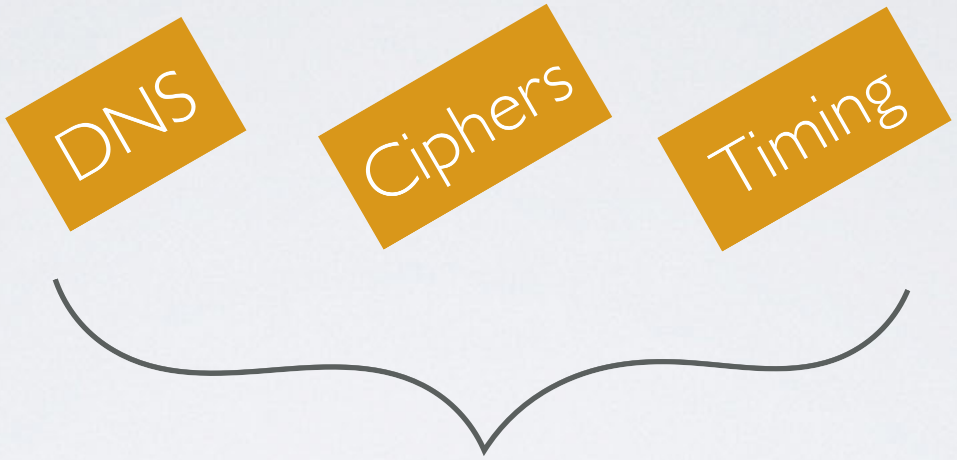
DNS

Ciphers

Timing

These differences arise due to differences in the **code**

OBSERVATION



DNS

Ciphers

Timing

These differences arise due to differences in the **code**

Ciphers

```
SSL_CTX_set_cipher_list
  (ssl_ctx,
   “HIGH:MEDIUM:!RC4:\
    !SRP:!PSK:!RSA:\
    !aNULL@STRENGTH”);
```

wget

```
static ssl3CipherSuiteCfg cipherSuites[...] = {
#ifndef NSS_DISABLE_ECC
 { TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
 { TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
 …
#endif /* NSS_DISABLE_ECC */
 { TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
 { TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
 { TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
```

firefox

OBSERVATION

Ciphers

```
SSL_CTX_set_cipher_list
  (ssl_ctx,
   “HIGH:MEDIUM:!RC4:\
    !SRP:!PSK:!RSA:\
    !aNULL@STRENGTH”);
```

wget

```
static ssl3CipherSuiteCfg cipherSuites[...] = {
#ifndef NSS_DISABLE_ECC
 { TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
 { TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
 …
#endif /* NSS_DISABLE_ECC */
 { TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
 { TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
 { TLS_DHE_DSS_WITH_AES_128_CBC_SHA,
```

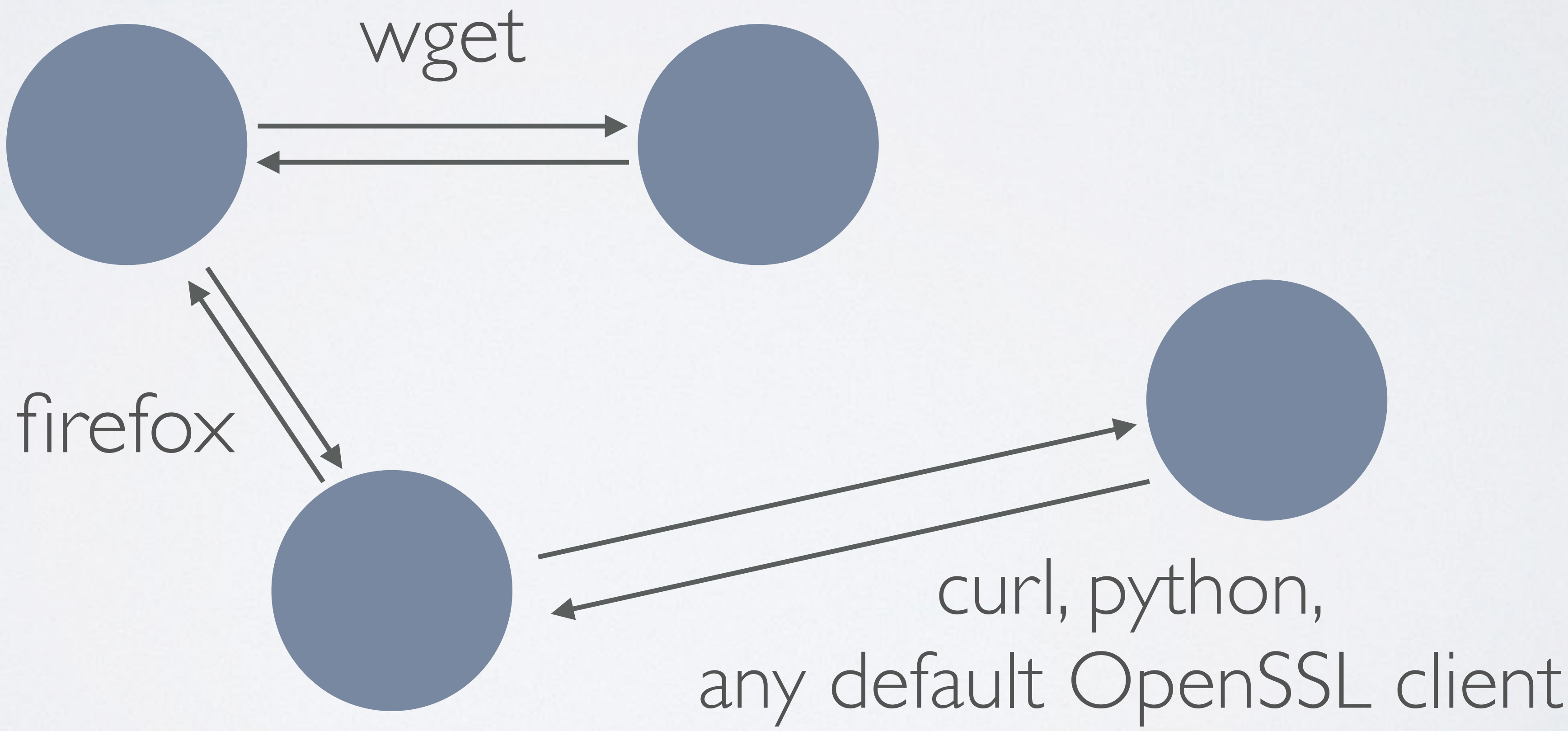
firefox

```
C030C02CC028C024C014C00A00A3009F006B006A0039003800880
087C032C02EC02AC026C00FC005009D003D00350084C012C00800
160013C00DC003000AC02FC02BC027C023C013C00900A2009E006
70040003300320009A009900450044C031C02DC029C025C00EC004
009C003C002F00960041C011C007C00CC00200050004001500120
009001400110008000600030 0FF
```

```
C02BC02FC00AC009C013C014C012C007C011003300320045
0039003800880016002F004100350084000A00050004
```

HYPOTHESIS

Static code analysis can be used to generate network signatures for known applications.



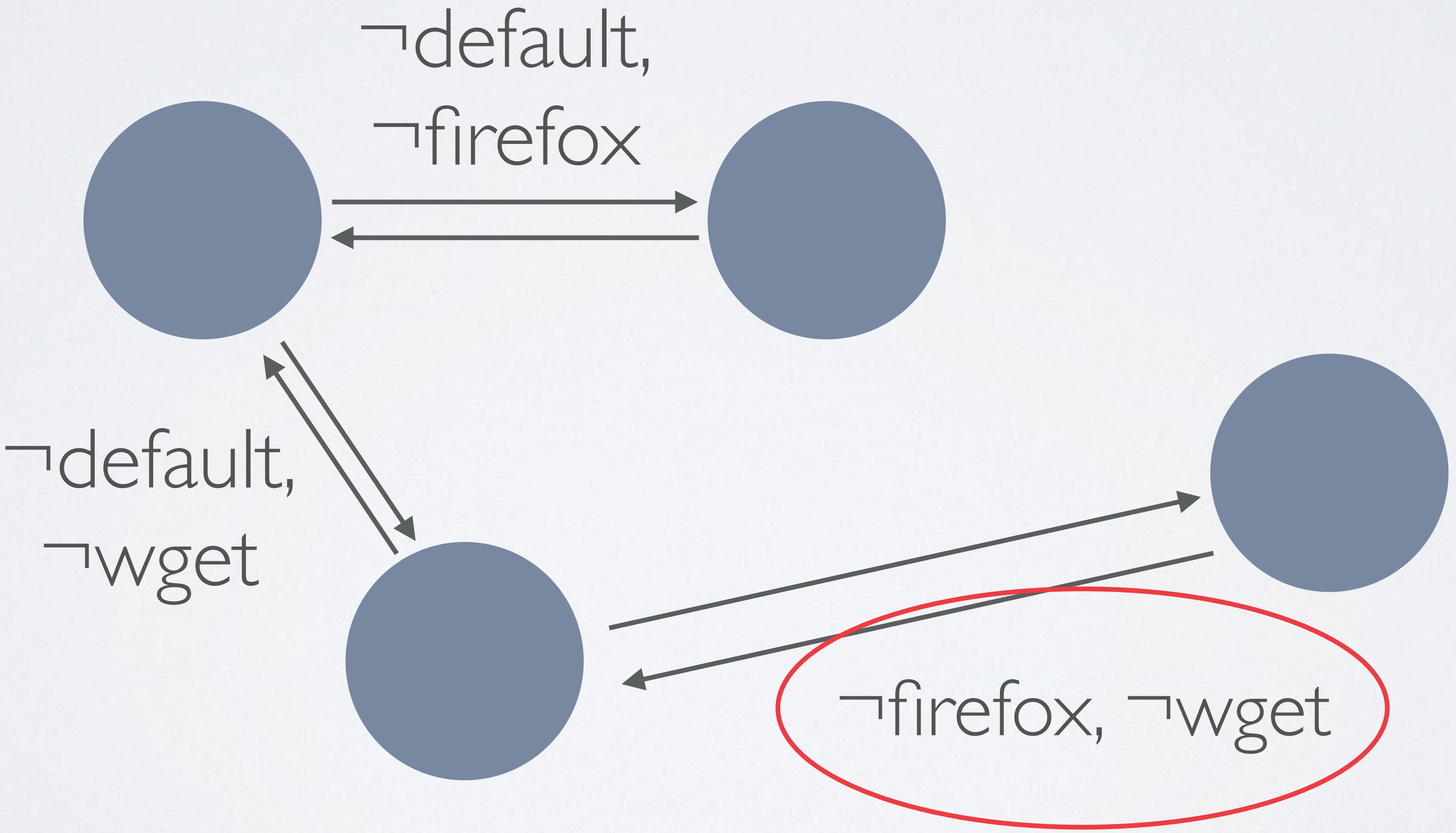
wget

firefox

curl, python,
any default OpenSSL client

OBSERVATION

Our strongest conclusions are about what applications are **not** involved.

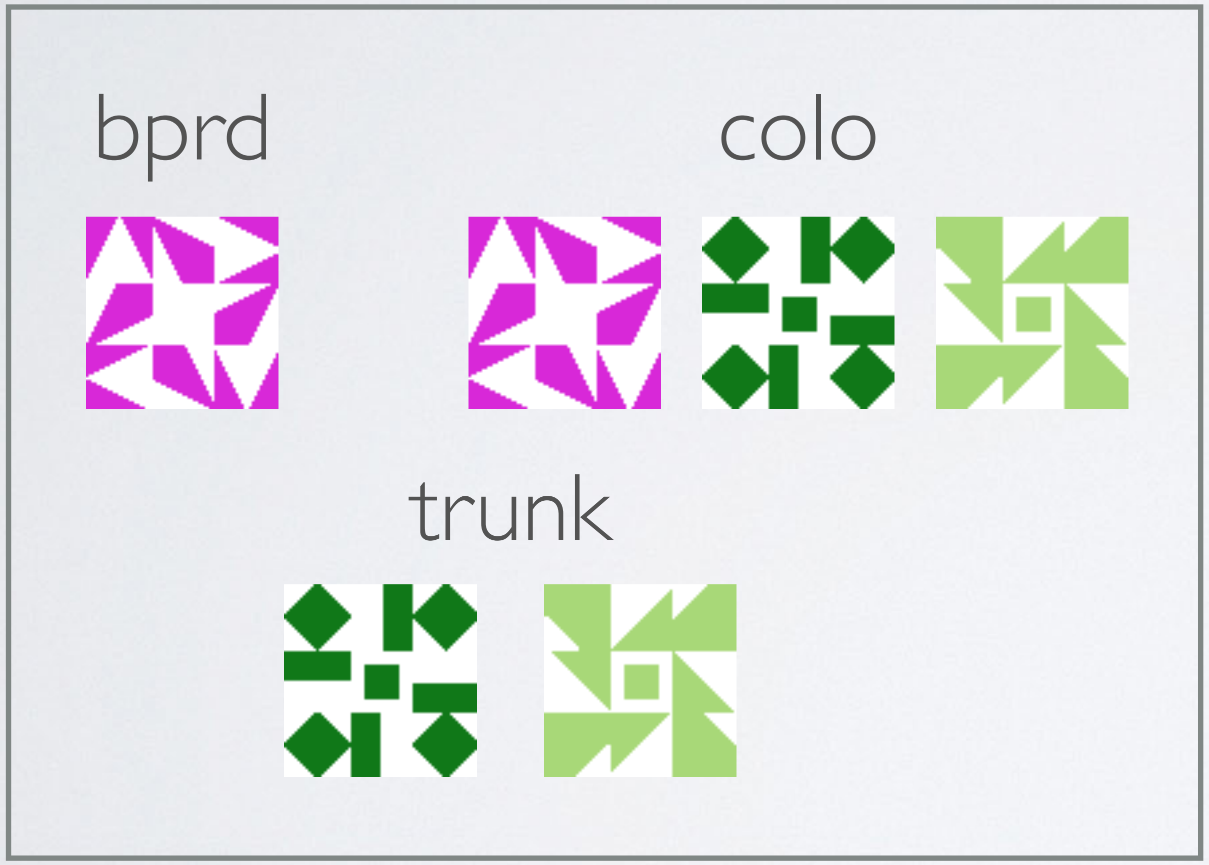


RESULTS

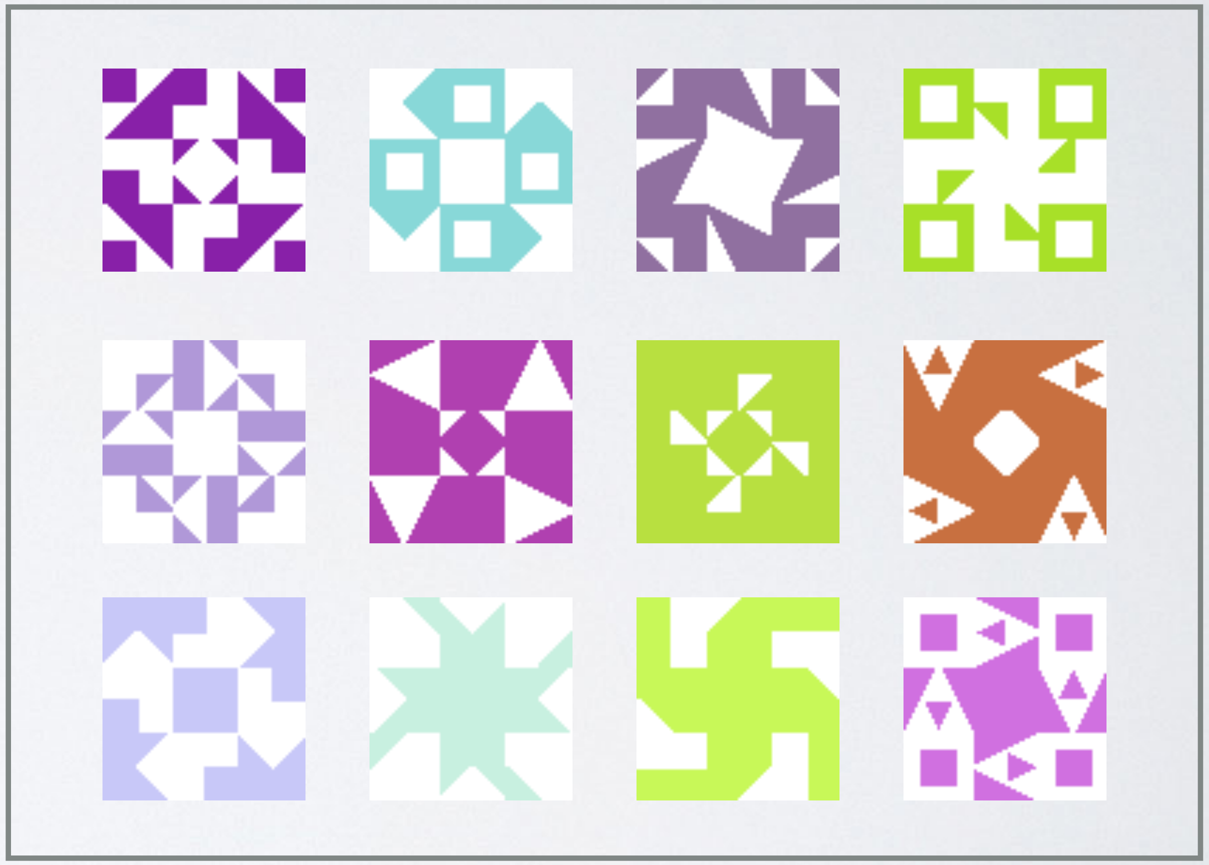
On-wire Signatures

(SSL Cipher List, PREDICT Datasets)

Skaion



NCCDC 2014



(x5)

RESULTS

Application Labeling

Firefox

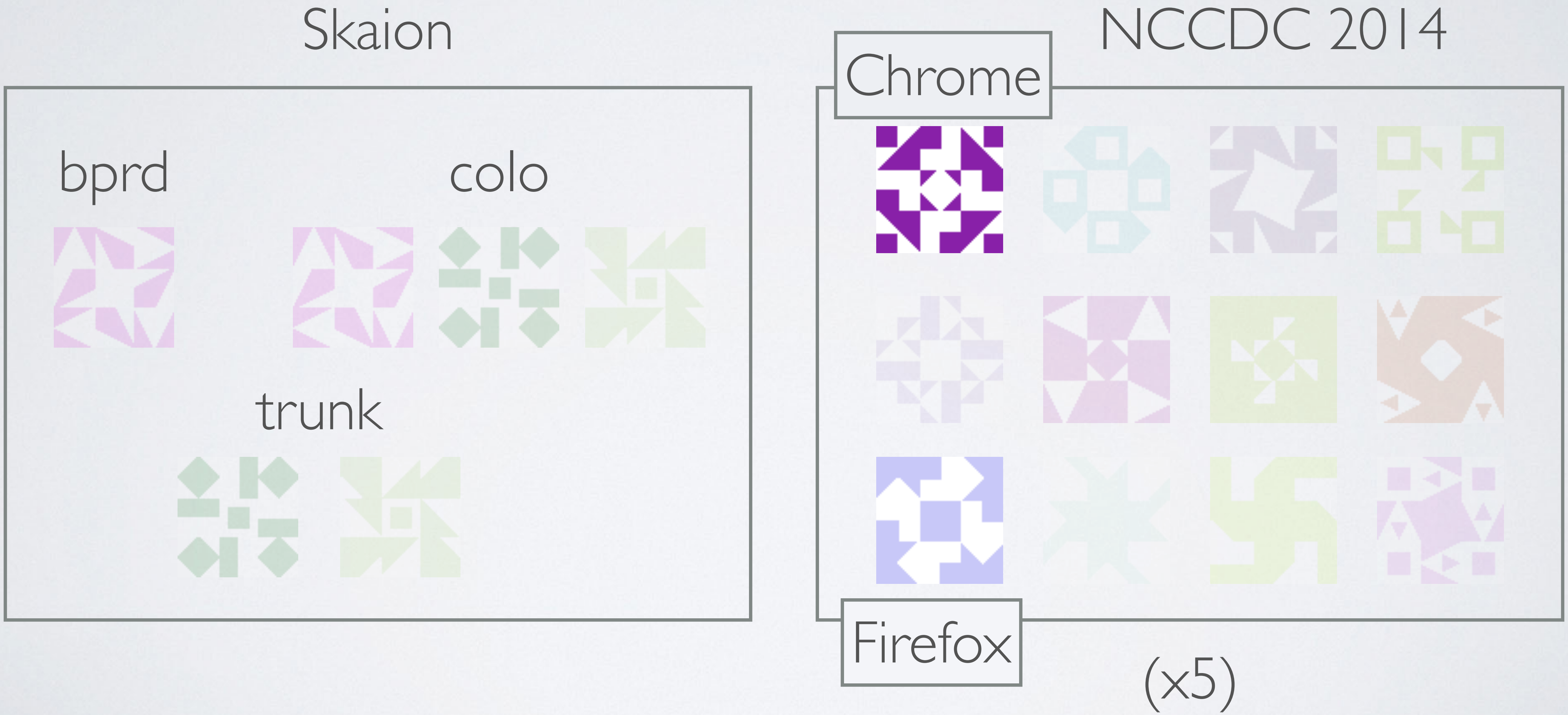
wget

Chrome

curl

RESULTS

On-wire Signatures



Skaion

bprd

colo

trunk

NCCDC 2014

Chrome

Firefox

(x5)

FUTURE WORK

- Automate signature production from source code
  - "Automated code review"
- Multi-packet signatures
- Apply to entire Linux source base
  - 51 packages mention cipher_list