OONI

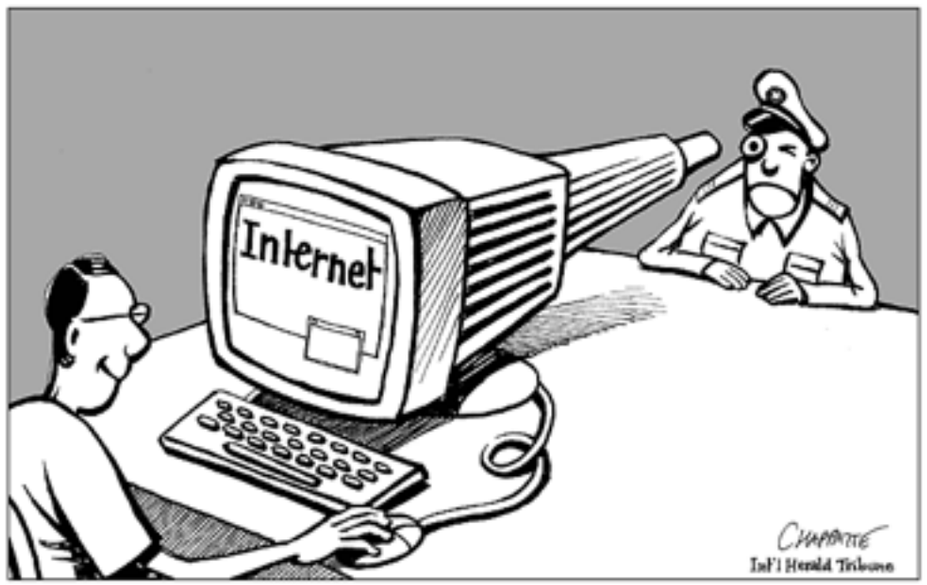
un framework per la misurazione della censura su Internet

Sorveglianza

- Il fenomeno è facilitato dalle nuove tecnologie.

- Spesso chi ne è vittima non ne capisce l'impatto o l'esistenza.

- Può portare all'auto-censura.



Censura Internet.

- E’ un sottoinsieme della sorveglianza.
- Permette a chi detiene il potere di alterare la realtà.

Filternet

- Si crea una visione alternativa della realtà.
- Non garantisce uguale accesso alla rete a tutti.

La censura internet non ha senso.

- Sistema fallato perché sempre aggirabile.
- Rafforza soltanto i divari sociali.
- Cittadini di serie A e serie B

Perché misurare la censura?

- E’ un barometro che permette di capire la libertà di espressione in un dato paese.

- Cercare di capire quando si ha un caso di sovra-blocco o sotto-blocco.

- Rivela anche connessioni economiche tra venditori di apparecchiature censorie e regimi.

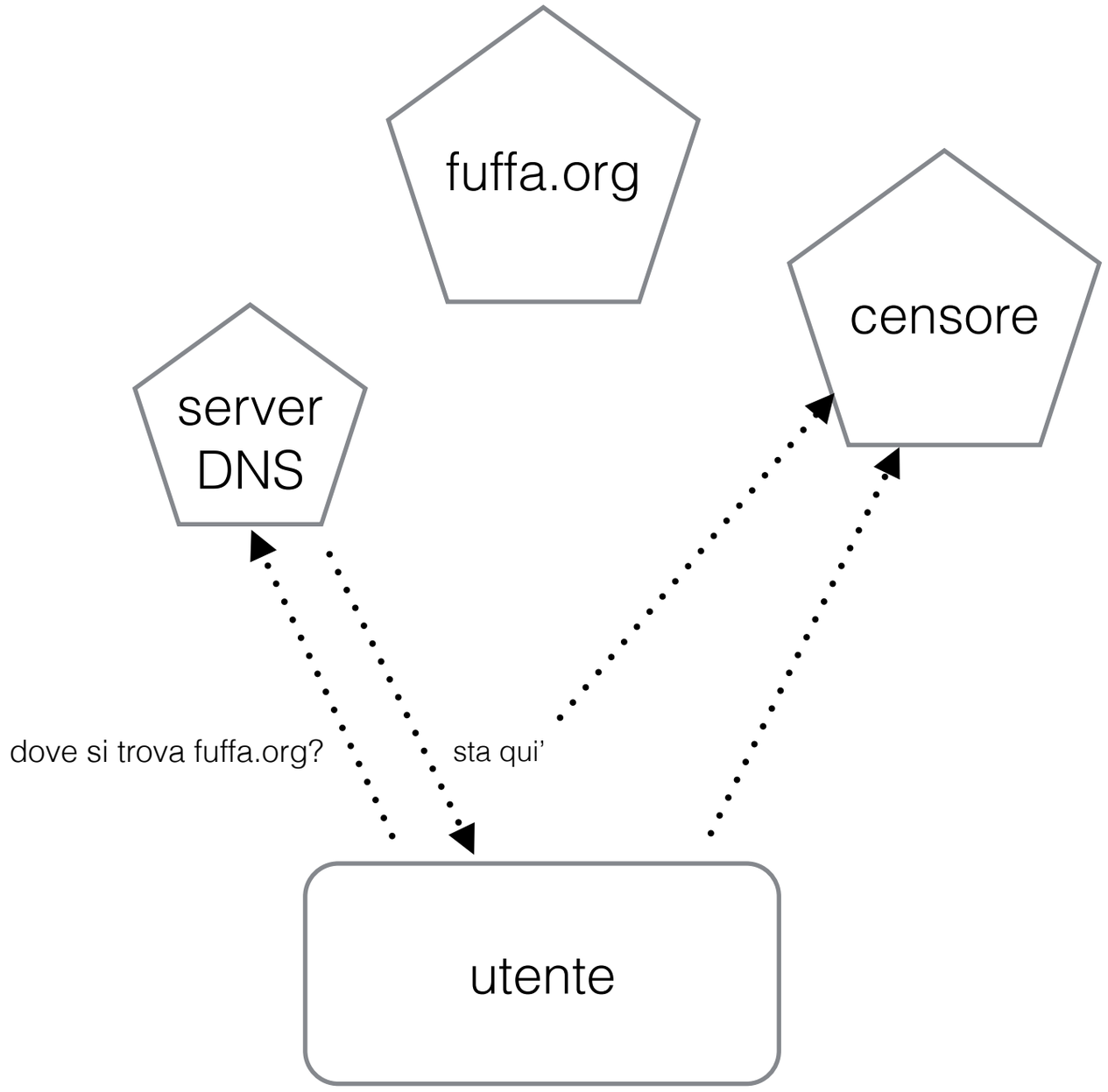
Come viene censurata la rete?

Blocco su base IP

- Uno dei metodi più semplici di blocco.
- Non è affatto preciso come metodo.
- Relativamente semplice da implementare, abbastanza costoso da manutenere.

Blocco su base DNS

- Più preciso.
- Spesso molto facilmente aggirabile.
- Differenza tra spoofing DNS e manipolazione dei server DNS.



Blocco su base HTTP

- Ancora più preciso del blocco su base DNS.
- Permette di bloccare specifiche pagine.
- Non funziona se viene utilizzato HTTPS.
- Spesso molto costoso da implementare.

Blocco o rallentamento di certi protocolli

- Tecnica molto avanzata.
- Serve ad evitare che certe applicazioni vengano utilizzate.
- Molto costoso da implementare e spesso richiede soluzioni ad-hoc.
- Generalmente usato solo da regimi.

Filtro di protocolli cifrati

- Se il tipo di crittografia è sicura, richiede modifiche del client.
- Vedi caso di TomSkype o filtri su SSL applicati in aziende.

Il nostro approccio

- Portare trasparenza al mondo della raccolta di dati sulla censura.

- Raccogliere dati grezzi usando metodologie documentate.

- Lo strumento che viene usato per la raccolta è rilasciato con licenza libera.

- I dati raccolti vengono pubblicati in open data.

A chi ci rivolgiamo?

- I **ricercatori** che possono fare ricerche basandosi su dati.
- A chi produce **visualizzazioni** che hanno bisogno di dati grezzi su cui lavorare.
- Ai **legislatori** che possono basare le loro decisioni di fatti e dati verificabili.
- A chi fa **data journalism** che vuole poter citare una fonte attendibile da cui ha ottenuto i dati
- Al **pubblico** che vuole meglio comprendere il fenomeno della censura internet.

Che cosa misuriamo?

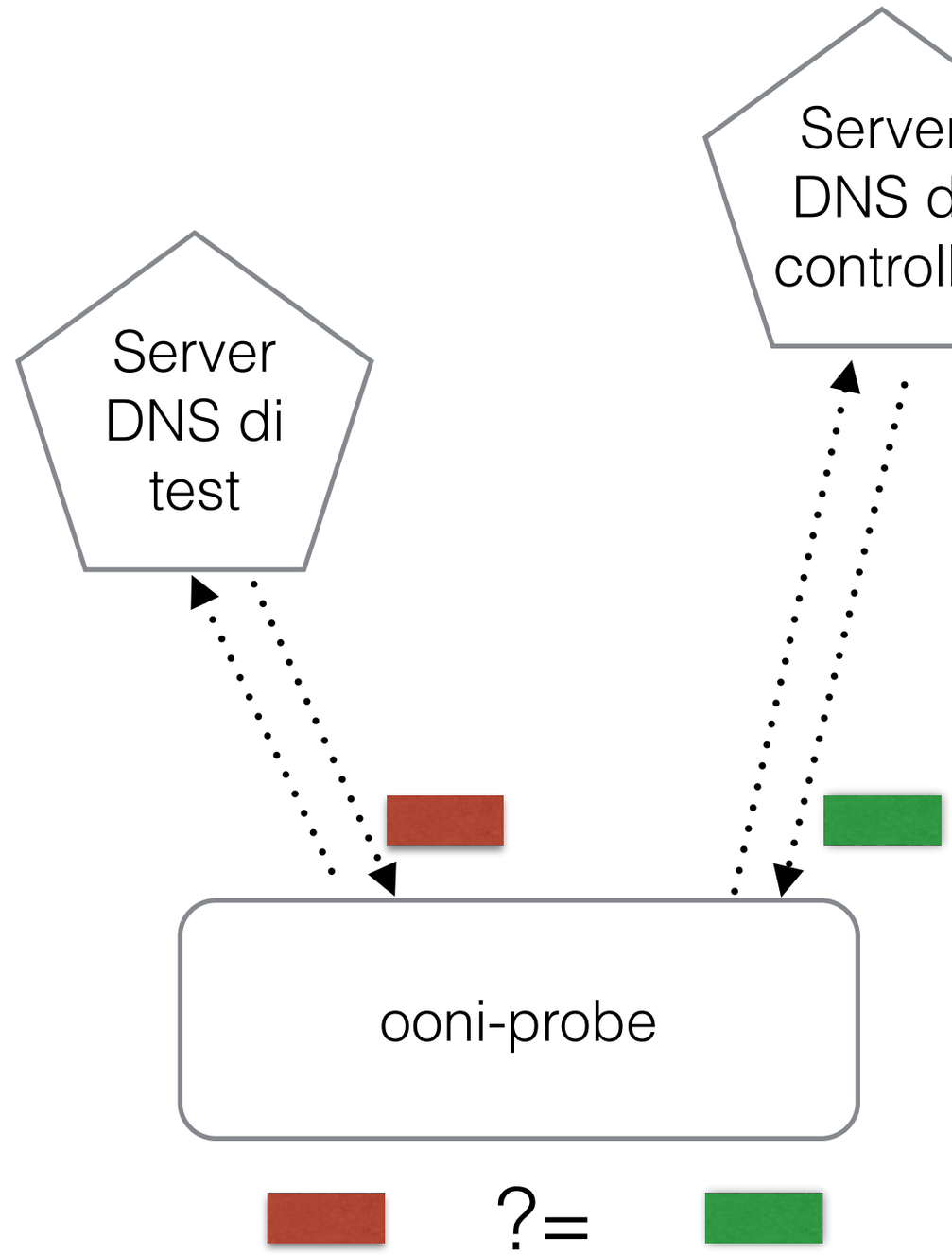
- Le tipologie di censura che andiamo a misurare rientrano in 2 categorie:

- **Manipolazione del traffico**

- **Blocco del contenuto**

DNS Consistency

- Misura la consistenza tra un resolver DNS buono ed uno di prova.



Esempio: Turchia 2014-04-02

Risposta server DNS Turk Telekom

```
- addrs: [195.175.254.2]
  answers:
  - [<RR name=youtube.com type=A
class=IN ttl=86400s auth=True>, <A
address=195.175.254.2
      ttl=86400>]
  query: '[Query(''youtube.com'',
1, 1)]'
  query_type: A
  resolver: &id010 [195.175.39.40,
53]
```

Risposta server DNS di controllo

```
- addrs: [74.125.239.35, …]
  answers:
  - [<RR name=youtube.com type=A class=IN
ttl=299s auth=False>, <A
address=74.125.239.35
      ttl=299>]
…
   - [<RR name=youtube.com type=A
class=IN ttl=299s auth=False>, <A
address=74.125.239.39
      ttl=299>]
  query: '[Query(''youtube.com'', 1, 1)]'
  query_type: A
  resolver: &id002 [64.9.225.221, 57004]
```

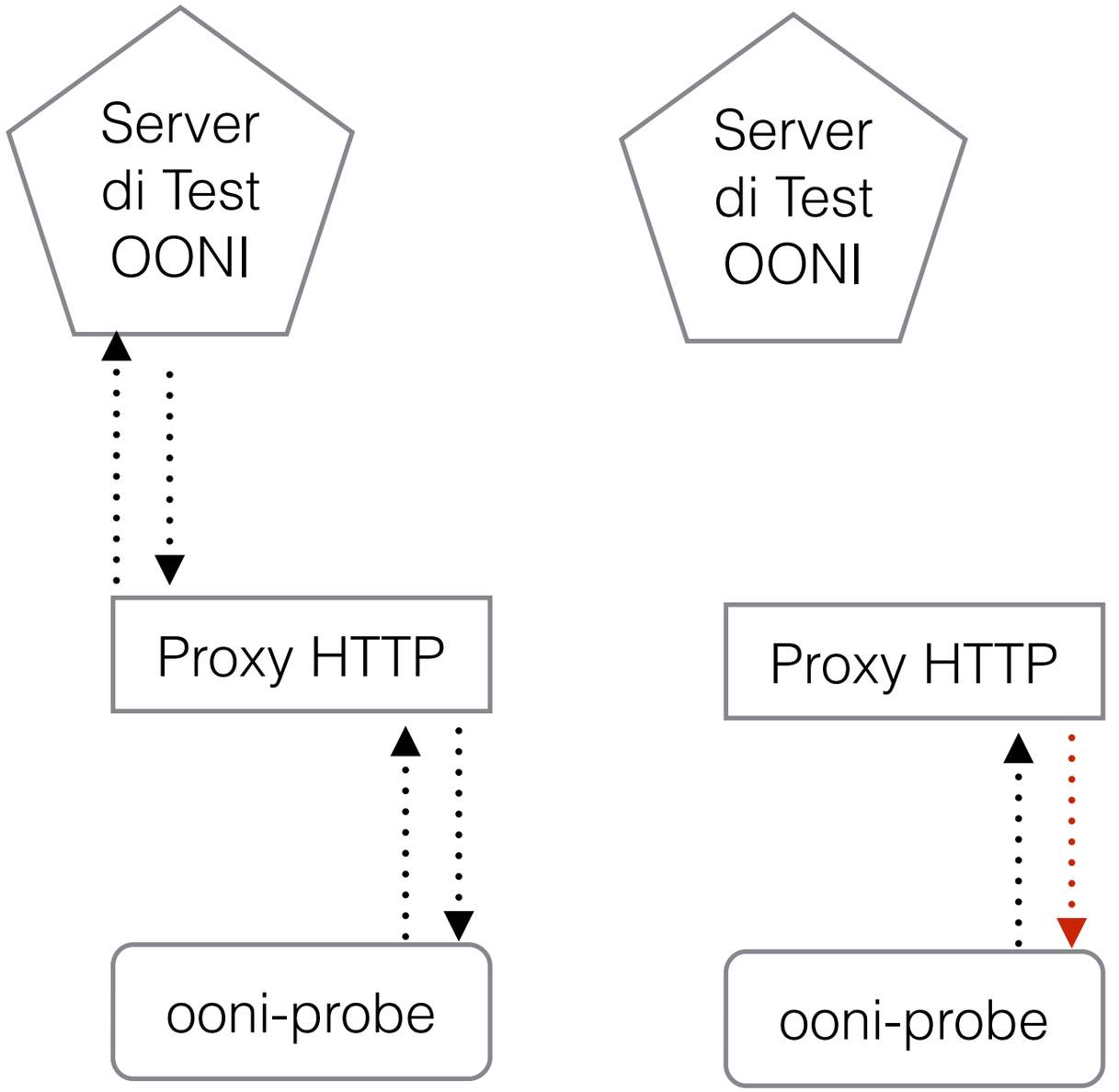
Esempio: Turchia 2014-04-02


```
tampering: {193.255.146.53: true, 195.175.39.39: true, 195.175.39.40:
true, 195.49.216.15: true, 212.252.114.8: true, 212.58.3.2: true,
  212.58.3.7: true, 212.58.3.8: true, 85.29.26.8: true, 88.255.242.6:
true}
```

HTTP Invalid Request Line

- Genera delle richieste HTTP invalide cercando di far ritornare un errore ad un dispositivo che sta intercettando il traffico.

- Spesso ci permette anche di capire la versione esatta del software utilizzato



Esempio: Moldavia 2013-09-12

```
input: null
received: ["HTTP/1.0 400 Bad
Request\r\nServer: squid/
3.1.10\r\n …"]
sent: ["P6jxr FYuhk YP5pg
ai5bp\n\r"]
tampering: true
```

Stato attuale

- Abbiamo **1629** misurazioni da **27** diversi paesi.
- Abbiamo sviluppato **16** diversi test che misurano varie tecniche di censura.
- Al momento i dati non sono fruibili da un pubblico più ampio.

Il fine ultimo

- Raggiungere la verità su quello che è lo stato della censura nel mondo.

- Andare quindi oltre dati aneddotici e avere prove certe.

- Sulla base di questo riuscire quindi a prendere le migliori decisioni.

Altre risorse

- http://ooni.nu/
- I dati grezzi raccolti fino ad adesso: https://ooni.torproject.org/reports/0.1/
- Le specifiche delle metodologie di misurazione e il formato dei dati si possono trovare su http://github.com/TheTorProject/ooni-spec/.

Domande?

Grazie per l’attenzione!