Network Measurement & Monitoring for Detecting and Mitigating Emerging Threats

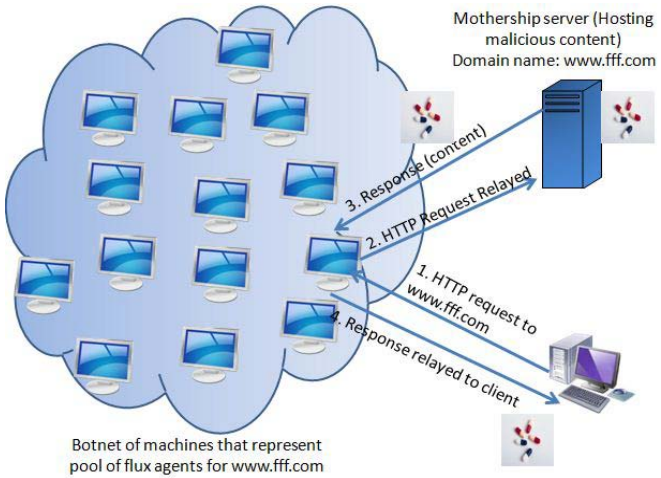
Basheer Al-Duwairi

Jordan University of Science & Technology

Outline

- Examples of using network measurements /monitoring
  - Example 1: fast flux detection
  - Example 2: DDoS mitigation as a service
- Future trends
  - Hot topics
  - Challenges

Detection and Characterization of Fast Flux Networks

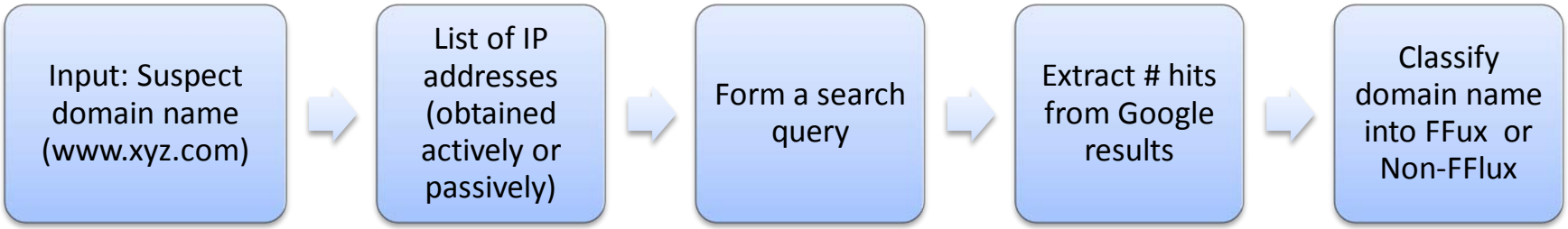



```
;; ANSWER SECTION:
09-service.ru.          9       IN      A       136.169.214.129
09-service.ru.          9       IN      A       158.181.153.20
09-service.ru.          9       IN      A       176.215.247.0
09-service.ru.          9       IN      A       178.129.215.113
09-service.ru.          9       IN      A       194.28.140.134
09-service.ru.          9       IN      A       91.226.57.151
09-service.ru.          9       IN      A       95.81.53.162
09-service.ru.          9       IN      A       176.109.54.103
09-service.ru.          9       IN      A       176.97.101.11
09-service.ru.          9       IN      A       128.73.112.222
```

```
;; ANSWER SECTION:
09-service.ru.          9       IN      A       176.109.54.103
09-service.ru.          9       IN      A       176.97.101.11
09-service.ru.          9       IN      A       176.8.245.247
09-service.ru.          9       IN      A       128.71.255.82
09-service.ru.          9       IN      A       46.0.62.42
09-service.ru.          9       IN      A       136.169.168.197
09-service.ru.          9       IN      A       37.99.17.53
09-service.ru.          9       IN      A       180.211.154.217
09-service.ru.          9       IN      A       109.254.85.172
09-service.ru.          9       IN      A       188.191.237.220
```

[B. Al-Duwairi et. al , "GFlux: A Google-Based Approach for FFlux Detection ", Technical Report. Jordan Univ. of Science & Technology]

GFlux- System Overview



GFlux- Input: domain hosted by CDN

```
;; ANSWER SECTION:
images.amazon.com.      60      IN      CNAME   ecx.images-
amazon.com.c.footprint.net.
ecx.images-amazon.com.c.footprint.net. 230 IN A 204.160.107.126
ecx.images-amazon.com.c.footprint.net. 230 IN A 198.78.205.126
ecx.images-amazon.com.c.footprint.net. 230 IN A 198.78.213.126
```

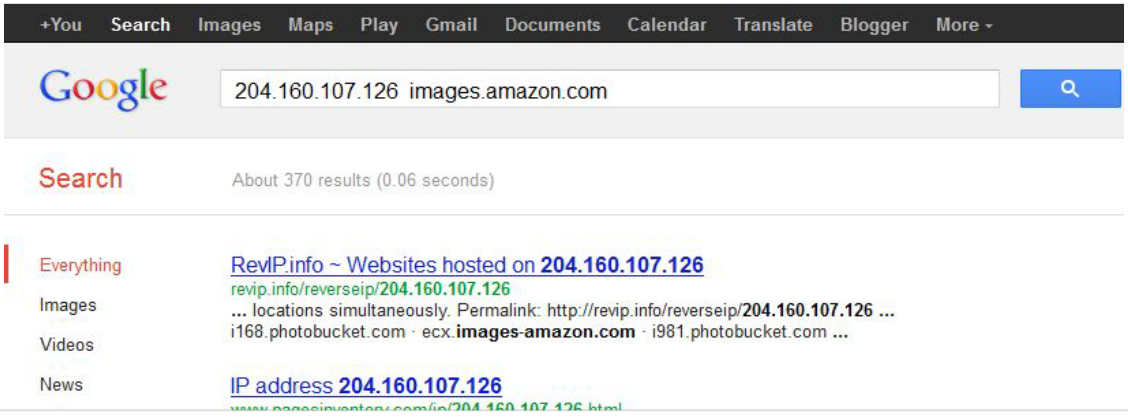
Input:
images.amazon.com

List of IP addresses (obtained actively or passively)

Form a search query

Extract # hits from Google results

Classify domain name into FFux or Non-FFlux



GFlux- Input: FFlux domain

```
;; ANSWER SECTION:
09-service.ru.          9       IN      A       136.169.214.129
09-service.ru.          9       IN      A       158.181.153.20
09-service.ru.          9       IN      A       176.215.247.0
09-service.ru.          9       IN      A       178.129.215.113
09-service.ru.          9       IN      A       194.28.140.134
09-service.ru.          9       IN      A       91.226.57.151
09-service.ru.          9       IN      A       95.81.53.162
09-service.ru.          9       IN      A       176.109.54.103
09-service.ru.          9       IN      A       176.97.101.11
09-service.ru.          9       IN      A       128.73.112.222
```

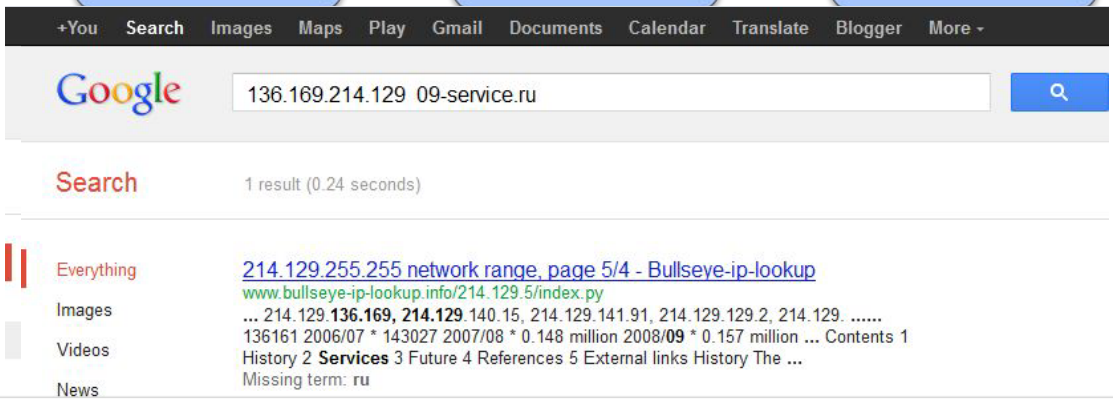
Input: 09-service.ru

List of IP addresses (obtained actively or passively)

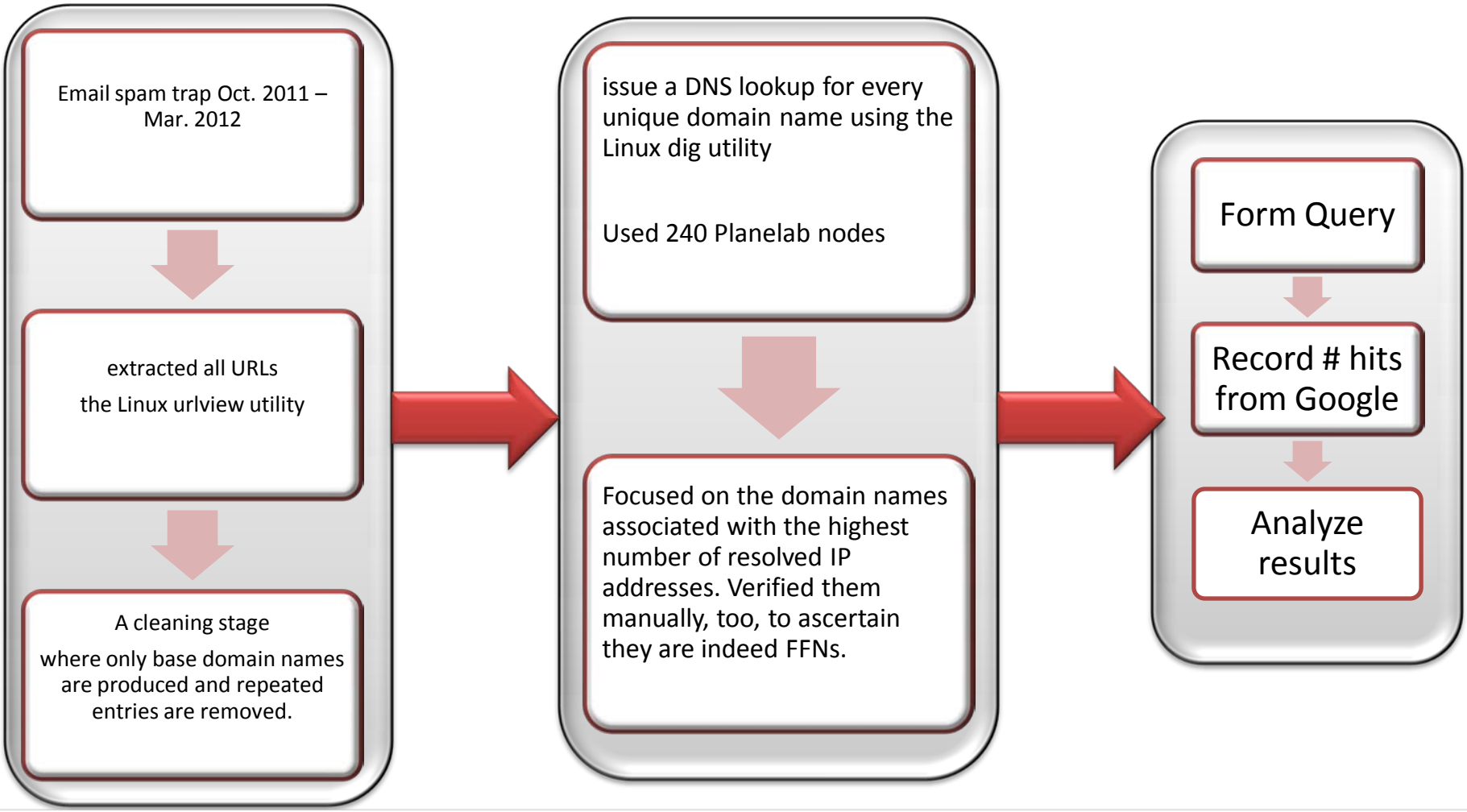
Form a search query

Extract # hits from Google results

Classify domain name into FFux or Non-FFlux

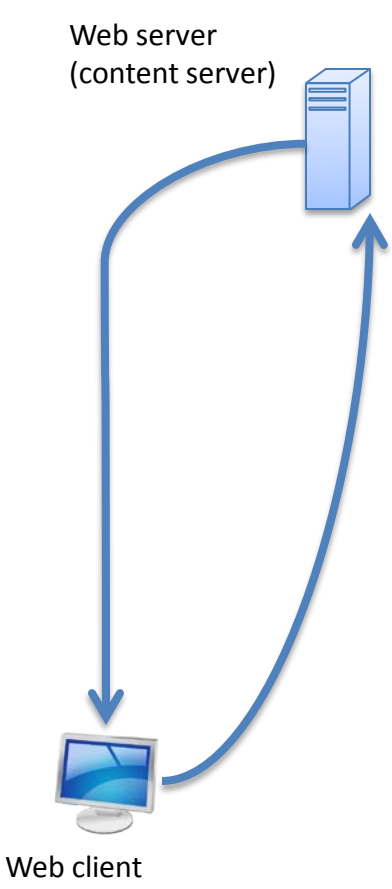


Data Collection

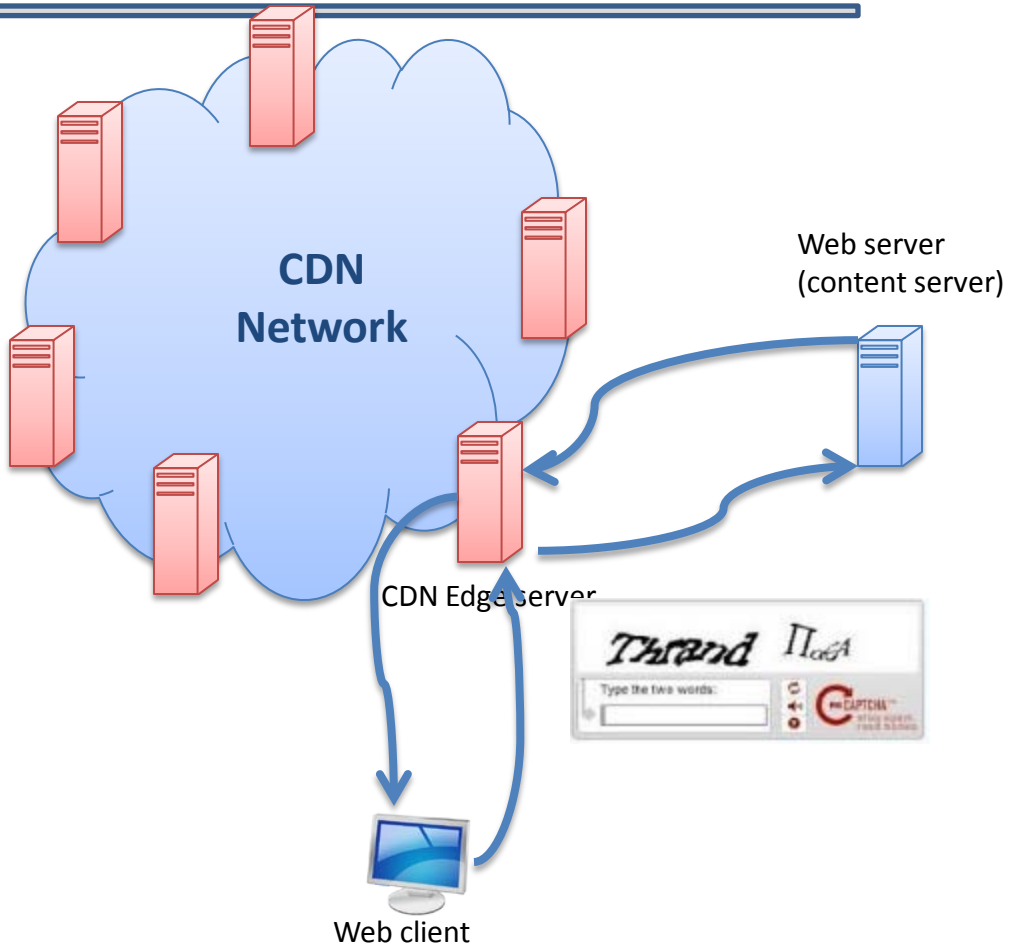


[Zakaria Al-Qudah, Basheer Al-Duwairi, and Osama Al-Khaleel, "DDoS Protection as a Service: Hiding Behind the Giants", To appear in International Journal of Computational Science and Engineering]

DDoS Protection as a Service



(a) In the absence of an attack



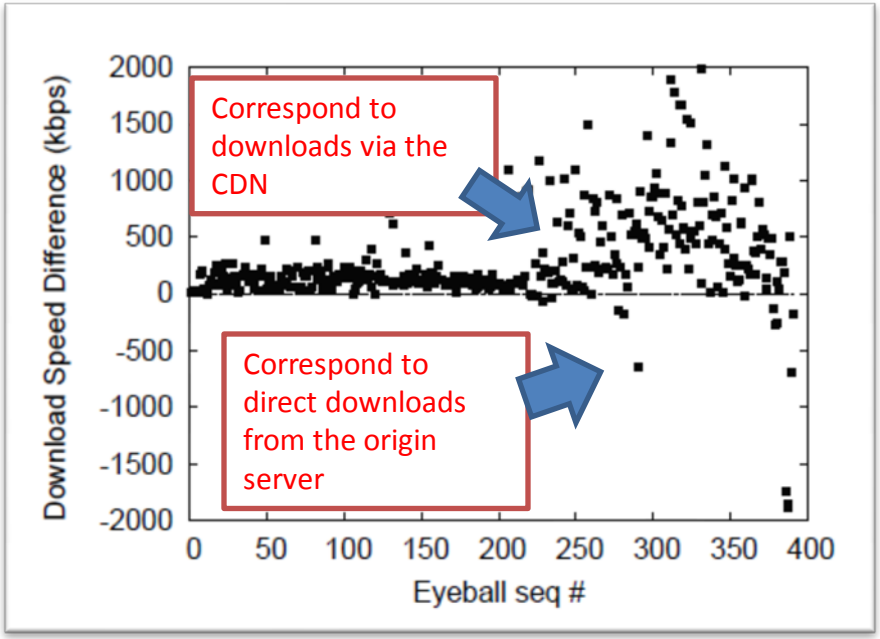
(a) During an attack

Performance evaluation/ experiments

- Downloading static object from origin server vs. via an CDN edge server acting like a proxy
  - Object type: PDF file
  - Object size: 3.1 MB
  - Origin Server: fedex.com
  - CDN network: Akamai
- Downloads are performed from 391 Planetlab nodes
  - For each node two downloads for the identified object: one from origin.fedex.com and the other from images.fedex.com
  - Frequency: once every hour for a period of 24 hours
  - Important issue: ensuring that the CDN edge server fetches a fresh copy of the object
  - Solution: We append the download from images.fedex.com with a random query string

Performance Results

- The figure plots the difference between effective download bandwidth in the two cases (CDN download minus direct download).
- Most of the Planetlab nodes, downloading via the CDN have better performance.
- This is due to the fact that CDNs optimize the path through which they fetch objects from the origin server.



Future trends: Hot topics + main challenges

- Most of web traffic is referred by search engines + social networks websites
  - Google, yahoo, Facebook, twitter, etc.
  - What traffic needs to be collected/monitored to infer malicious activities?
- Collecting data from social networks
  - investigating and exploring the tradeoffs between services and privacy guarantees

Challenges / Future Trends

- Collecting SMS traffic traces across multiple mobile network operators
- Operators need greater visibility and understanding of the applications running in their networks
  - Explosive growth in the number of web and mobile applications
  - Application hiding techniques like encryption, port abuse, and tunneling
- Little research has been done to characterize/detect spam/scam campaigns
  - What percentage of email spam received users is effective?