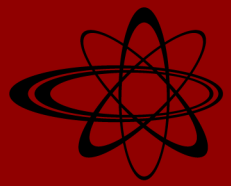


SNRG
Security and Networks Research Group

DNS tricks and other nifty things

By: Etienne Stalmans
Supervisor: Mr Barry Irwin

Telkom
amatole telecommunication services
Bright Ideas Projects 39
STORTECH For Your Information
THRIP Technology and Human Resources for Industry Programme
COMVERSE
MARS TECHNOLOGIES
tellabs

RHODES UNIVERSITY
Where leaders learn

Why DNS?

- It is everywhere
- Used by most (read: all) programs requiring internet connection
- This includes Malware
- Modern botnet structures rely on DNS

Botnets and DNS

- Fast-Flux
  - Avoid detection
  - Prevent shut down of Command and Control servers
  - Increase robustness
- If bots use DNS, can we use DNS to detect the bots?

Botnet structure

- Many hosts
- Receive instructions from C&C servers
- C&C servers in different locations
- Botnet controllers have limited control over availability and performance of C&C servers
- C&C servers constantly shifting to prevent botnet shutdown

Fast-flux DNS Query

```
;; QUESTION SECTION:
;championogogo.ru.                IN      A

;; ANSWER SECTION:
championogogo.ru.        300     IN      A       60.13.74.23
championogogo.ru.        300     IN      A       62.42.100.212
championogogo.ru.        300     IN      A       148.217.94.55
championogogo.ru.        300     IN      A       212.69.189.125
championogogo.ru.        300     IN      A       217.217.199.129
```

IP Address	Net block	ASN	Country
60.13.74.23	60.13.64.0/18	4837	CN
62.42.100.212	62.42.0.0/16	6739	ES
148.217.94.55	148.217.0.0/16	6503	MX
212.69.189.125	212.69.160.0/19	8218	DE
217.217.199.129	217.216.0.0/15	6739	ES

Features

- Short TTL
- Multiple A records, different IP ranges
- Multiple Autonomous System Numbers (ASNs)
- Name-servers in different network ranges

Malicious or not?

- Manual inspection
  - Why when it can be automated?
- Heuristics
  - Need kept up to date
- C5.0 decision tree
  - Same as heuristics
- Naïve Bayesian classifier
  - Evolve along with botnets

Results

Domain	Safe Score	Malicious Score	Classification
gingerbucksea.com	0.005304578	0.3550235	Fast-flux
pearlrumor.ru	3.059976e-14	7.490562e-13	Fast-flux
wordpress.com	1.536894e-08	4.250896e-10	Legitimate
champiogogo.ru	3.395984e-09	1.723838e-06	Fast-flux
yahoo.com	1.940412e-15	1.509179e-69	Legitimate (CDN)

- Detects fast-flux domains missed by C5.0 classifier and rule based classifier
- Better distinguishing between Content Distribution Networks and fast-flux
- Fast

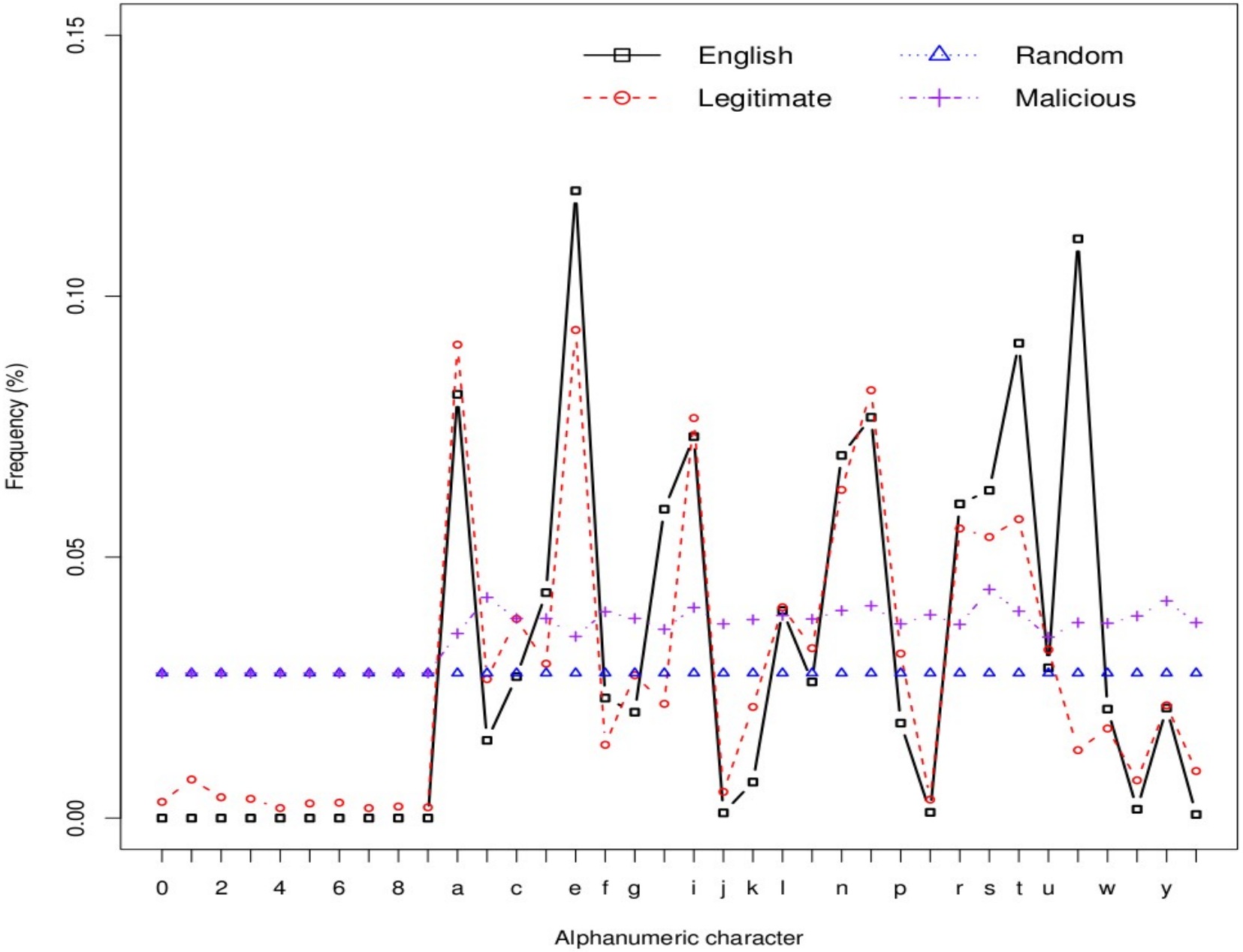
Extra goodies

- Detection of “Domain fluxing” using stats
- Conficker, Kraken, Torpig all use algorithmically generated domain names for C&C servers
- Conficker-C generates 50 thousand names a day
- Not possible to block, shut down and pre-register so many domains

But how?

- Site name: www.facebook.com
- Malicious domain: bbhkxkjh.com.fj
- Easy to tell them apart, well as a human, yes.
- Computer needs to “learn”
- You have got to love stats...

Frequency distributions



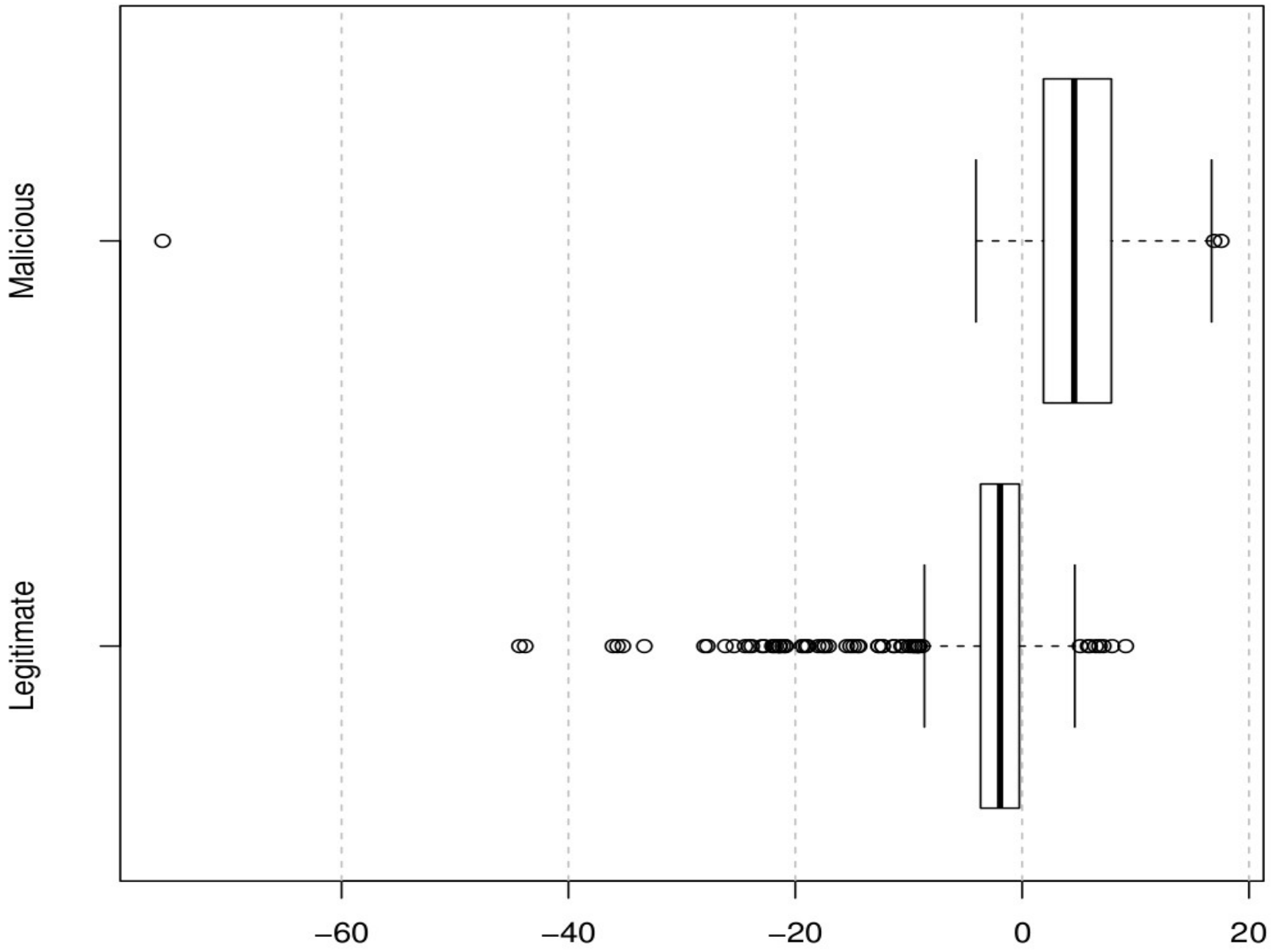
Classifiers

- Naïve Bayesian Classifier
- Bayesian Classifier
- Probability distribution
- Variation distance

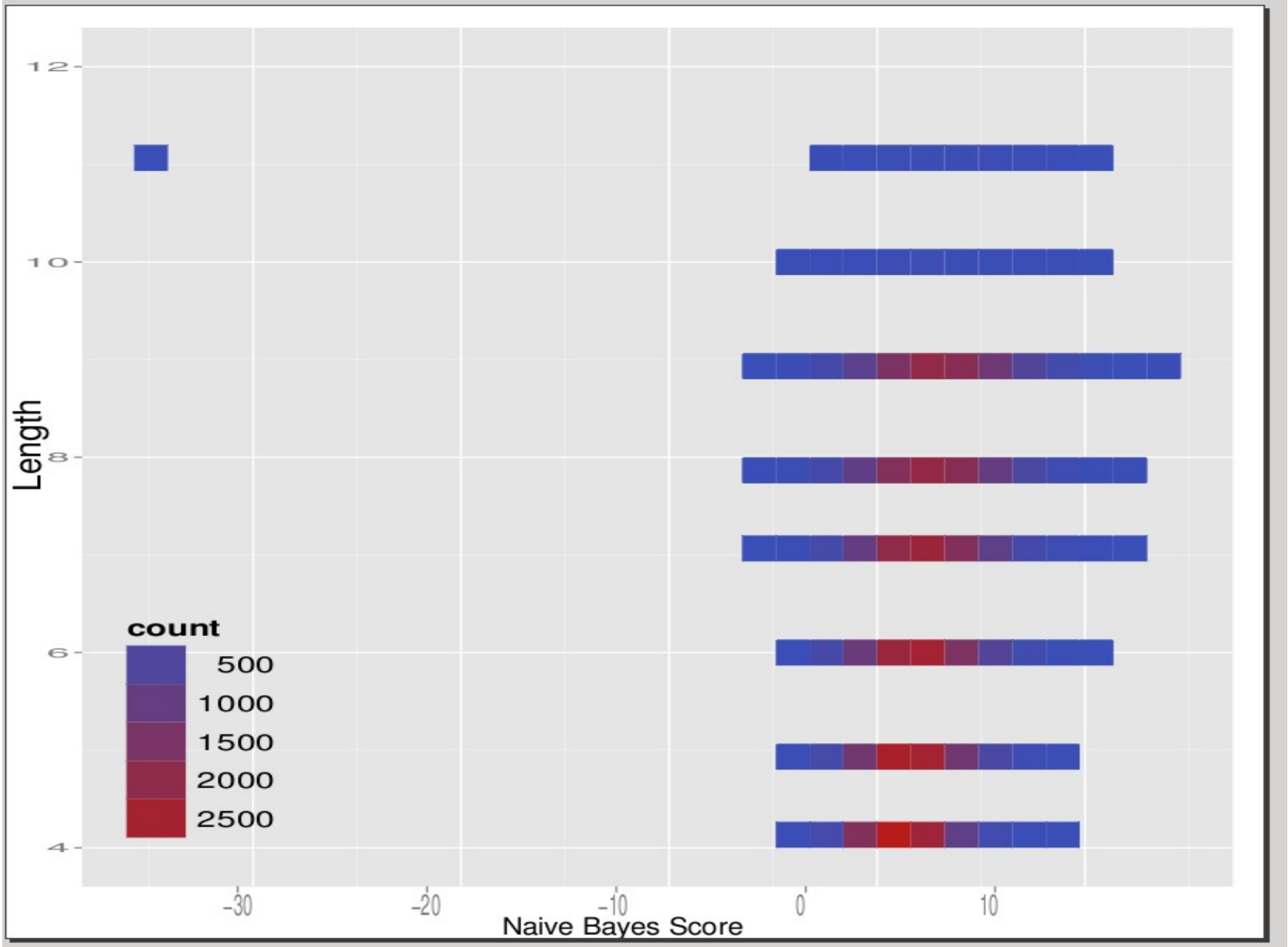
Classifier	Accuracy	TPR	FPR
Naive Bayesian	86.5%	82%	8.3%
Variation	82.4%	80%	17%
Probability	84.3%	86%	17%
Bayesian	85%	81.3%	11%

TPR:True Positive Rate
FPR:False Positive Rate

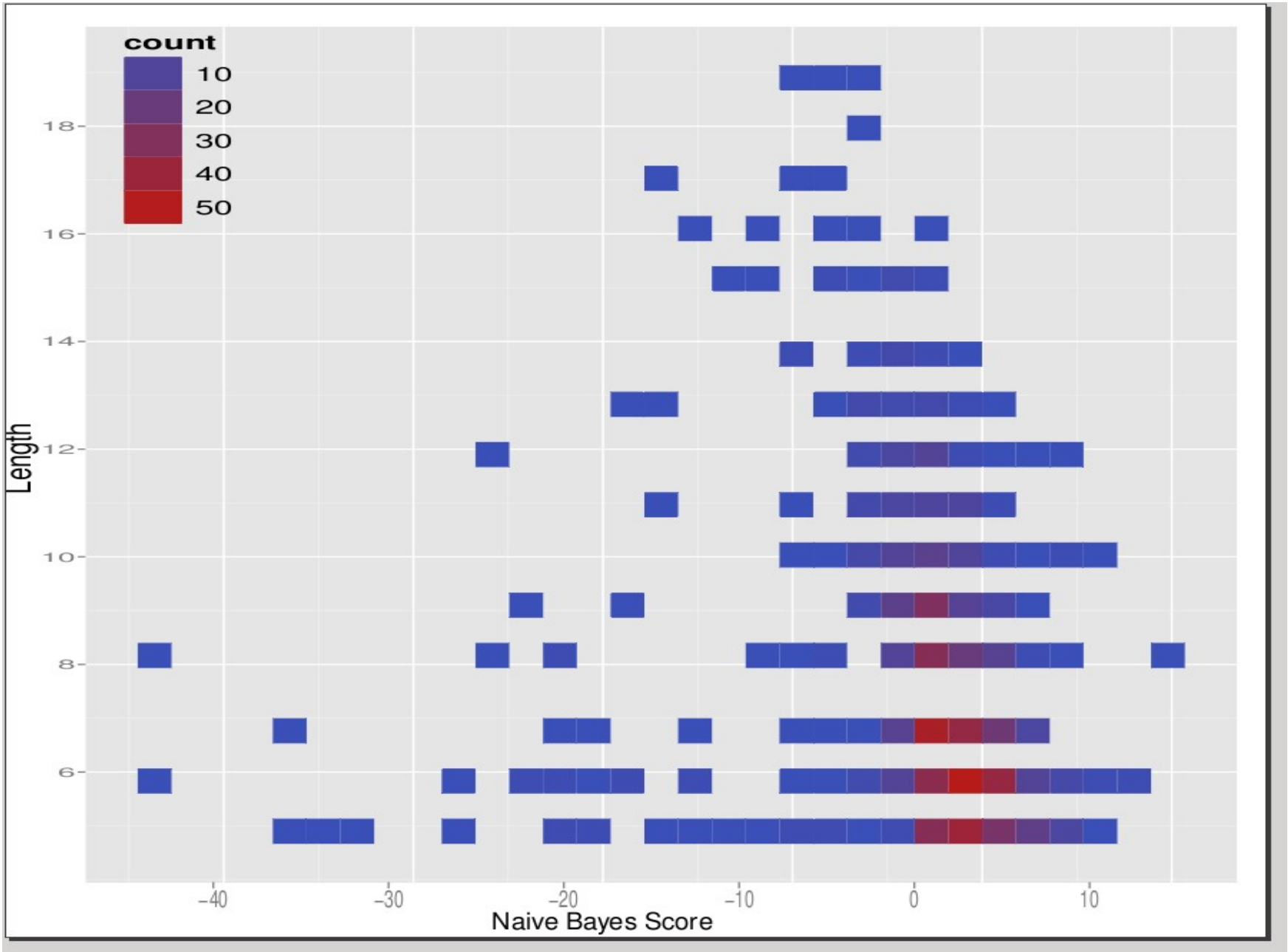
Box-plot, because it's sexy



Malicious Domains heatmap



Legitimate Domains heatmap



Questions