



# GOING ABOUT CRACKING HASHES

LOOKING BACK AT THE DOTS

- VIREN | CHHABRIV@TCD.IE
- ARUN | THUNDYIA@TCD.IE

# GETTING STARTED

- Wordlist
  - *Rockyou*
  - English Words
- Combinator
  - Linux Words – 4+4
  - From extracted combined password list
- Masks
  - |
  - a

# ANALYZE

```
*** Character Frequency ***
e -- 6908 / 83896 (8.23%)
a -- 6588 / 83896 (7.85%)
o -- 5284 / 83896 (6.3%)
i -- 4994 / 83896 (5.95%)
h -- 3215 / 83896 (3.83%)
s -- 2786 / 83896 (3.32%)
n -- 2554 / 83896 (3.04%)
l -- 2544 / 83896 (2.92%)
r -- 2453 / 83896 (2.83%)
u -- 2373 / 83896 (2.59%)
t -- 2172 / 83896 (2.14%)
c -- 1796 / 83896 (2.11%)
m -- 1774 / 83896 (1.92%)
j -- 1610 / 83896 (1.88%)
d -- 1580 / 83896 (1.84%)
p -- 1543 / 83896 (1.71%)
o -- 1436 / 83896 (1.69%)
b -- 1416 / 83896 (1.58%)
g -- 1414 / 83896 (1.48%)
y -- 1258 / 83896 (1.48%)
z -- 1244 / 83896 (1.48%)
k -- 1241 / 83896 (1.48%)
f -- 961 / 83896 (1.48%)
g -- 896 / 83896 (1.15%)
w -- 847 / 83896 (1.07%)
v -- 837 / 83896 (1.01%)
x -- 822 / 83896 (1.0%)
q -- 822 / 83896 (0.98%)
```

```
*** Char Count Stats ***
Total -- 12651
5 chars -- 5464 (43.19)
7 chars -- 2904 (22.95)
8 chars -- 2030 (16.05)
6 chars -- 709 (5.6)
9 chars -- 513 (4.06)
10 chars -- 476 (3.76)
11 chars -- 198 (1.57)
12 chars -- 132 (1.04)
13 chars -- 83 (0.66)
14 chars -- 49 (0.39)
15 chars -- 31 (0.25)
4 chars -- 31 (0.25)
3 chars -- 9 (0.07)
2 chars -- 8 (0.06)
16 chars -- 6 (0.05)
18 chars -- 2 (0.02)
```

```
-- upper
count: 88
percent: 0.695597185993
minimum_length: 5
maximum_length: 14
-- lower
count: 8337
percent: 65.8999288594
minimum_length: 1
maximum_length: 28
-- num
count: 794
percent: 6.27618370089
minimum_length: 2
maximum_length: 15
-- alnum
count: 3057
percent: 24.1640976998
minimum_length: 4
maximum_length: 19
-- other
count: 365
percent: 2.88514741918
minimum_length: 5
maximum_length: 20
```

# LEARNINGS

- Pitfalls
  - Rosetta is good and will work!
  - Pot files are updated regularly
  - Use all devices – CPU, GPU
  - Bigger is better
- Moving Forward
  - Start Simple
  - Engineer the attack
  - Collaborate – collaborate – collaborate !!!

