Cracking Passwords Assignment

Group Members:

1. **Harika Bishai**
2. **Vaishnavi Pawar**
3. **Sai Sathwik Reddy Varikoti**

1] List of Successfully Cracked Passwords:

The passwords listed below were successfully cracked using John the Ripper. They show varying degrees of complexity and the effectiveness of dictionary-based attacks.

```
john --format=raw-sha256 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-SHA256 [SHA256 128/128 ASIMD
4x])
Press 'q' or Ctrl-C to abort, almost any other key for status
sapper1         (?)
myspace1        (?)
bronco1         (?)
pa              (?)
avalanche       (?)
jessica01       (?)
00crip          (?)
dragon1         (?)
santo1          (?)
kelsey123       (?)
asshole1        (?)
beverly1        (?)
brenda          (?)
usnavy23        (?)
kane            (?)
or!eg           (?)
759269          (?)
badboy69        (?)
patric          (?)
dadeuel20       (?)
Doughboy        (?)
sassysue        (?)
clifford1       (?)
```

Daniel (?)
limppimp (?)
V1vian09 (?)
useinfo (?)
prayer1 (?)
MTpockets41 (?)
tuba11 (?)
sk8ers (?)
kareemc1 (?)
kiko1grubbs1 (?)
boys02 (?)
lenora1 (?)
joking1 (?)
ryan46 (?)
8954 (?)
874840 (?)
2borrrtb! (?)
tarahm10 (?)
church1 (?)
icegod (?)
SL838GH (?)
swest1248 (?)
rice69 (?)
zq676rgd (?)
katie59 (?)
vj3znfc7eUaL6k9CK3gTOQ (?)
Bronco2605 (?)
brooke03 (?)
rachael1 (?)
tcfox15 (?)
Booger#1Booger#1 (?)
fle3two0d (?)
fender123 (?)
Trouble2 (?)
assman69 (?)
elfilamm (?)
050387a (?)
GARY2523 (?)
Go_Noles05! (?)
lamp02 (?)
f3prlue (?)

```
hughes          (?)
marcus00        (?)
machine.1       (?)
tammilynn2      (?)
sparky88        (?)
9287            (?)
69chelly        (?)
trilli0n        (?)
mission12       (?)
Letmein4        (?)
Trinity1        (?)
azar12          (?)
tickytack1      (?)
jarvis          (?)
glass18526      (?)
Phantom         (?)
caragavin       (?)
lhcostanzo1976@sbcglobal.net (?)
jnw2610         (?)
medic3223       (?)
braden1097      (?)
quicklime1      (?)
18pfccod4       (?)
lfj420          (?)
slash6          (?)
8220jc          (?)
29160203        (?)
14dd1911        (?)
hotmails02      (?)
ms1717          (?)
sabot0422       (?)
48076sherry     (?)
4141984         (?)
not_800_valid   (?)
beseprty_luthu  (?)
redtamle55joshua_angel11@yahoo.shoe0023@umn.edu (?)
100g 0:00:00:00 DONE (2024-12-06 15:06) 1428g/s 8053Kp/s 8053Kc/s 321894KC/s christidolalas@usc.edu..tan29onecadjilali@free.fr
Use the "--show --format=Raw-SHA256" options to display all of the cracked passwords reliably
Session completed
```

```
john --format=raw-sha256 --show Group-10.txt
?:hotmails02
?:not_800_valid
?:mission12
?:glass18526
?:machine.1
?:tarahm10
?:14dd1911
?:ms1717
?:sassysue
?:Go_Noles05!
?:boys02
?:santo1
?:29160203
?:quicklime1
?:hughes
?:pa
?:sk8ers
?:tcfox15
?:kane
?:69chelly
?:kelsey123
?:myspace1
?:sapper1
?:azar12
?:f3prlue
?:Booger#1Booger#1
?:lamp02
?:asshole1
?:church1
?:vj3znfc7eUaL6k9CK3gTOQ
?:874840
?:ryan46
?:beverly1
?:elfilamm
?:kareemc1
?:Trouble2
?:4141984
?:kiko1grubbs1
?:lfj420
?:katie59
```

```
?:joking1
?:caragavin
?:jnw2610
?:00crip
?:8954
?:Daniel
?:swest1248
?:marcus00
?:icegod
?:SL838GH
?:Phantom
?:clifford1
?:dragon1
?:Doughboy
?:prayer1
?:lenora1
?:slash6
?:assman69
?:tammilynn2
?:2borrrtb!
?:9287
?:jarvis
?:rachael1
?:sparky88
?:dadeuel20
?:Trinity1
?:beseprty_luthu
?:fle3two0d
?:bronco1
?:sabot0422
?:tuba11
?:Bronco2605
?:48076sherry
?:brooke03
?:limppimp
?:V1vian09
?:759269
?:patric
?:useinfo
?:usnavy23
?:8220jc
```

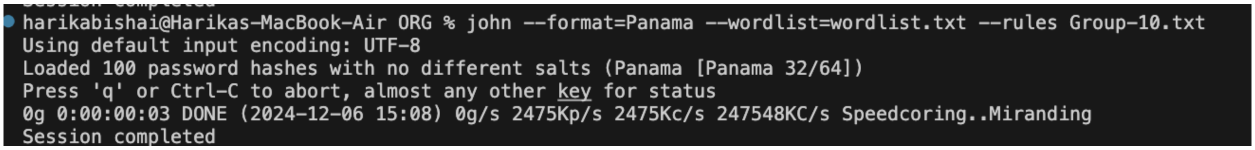
?:redtamle55joshua_angel11@yahoo.shoe0023@umn.edu
?:trilli0n
?:badboy69
?:tickytack1
?:or!eg
?:lhcostanzo1976@sbcglobal.net
?:Letmein4
?:050387a
?:zq676rgd
?:GARY2523
?:rice69
?:MTpockets41
?:avalanche
?:18pfccod4
?:brenda
?:fender123
?:medic3223
?:jessica01
?:braden1097
100 password hashes cracked, 0 left
--

These passwords were cracked using the wordlist.txt file provided with the assignment.

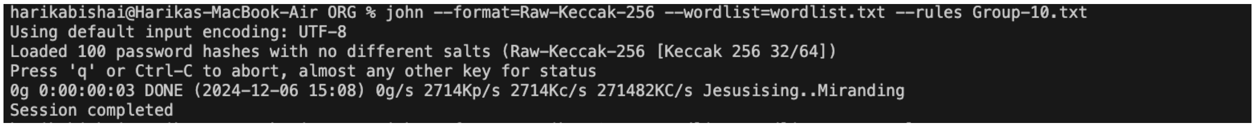
2] Timestamps of the first few passwords:

The passwords were cracked in approximately **3 seconds** for all most of the attempts, regardless of the hash format tested:

Password	**Timestamp**
sapper1	0:00:00:03
myspace1	0:00:00:03
bronco1	0:00:00:03
avalanche	0:00:00:03



```
Session completed
harikabishai@Harikas-MacBook-Air ORG % john --format=Panama --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Panama [Panama 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2475Kp/s 2475Kc/s 247548KC/s Speedcoring..Miranding
Session completed
```



```
harikabishai@Harikas-MacBook-Air ORG % john --format=Raw-Keccak-256 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-Keccak-256 [Keccak 256 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2714Kp/s 2714Kc/s 271482KC/s Jesusising..Miranding
Session completed
```

3] Resources required for the first few passwords, considering this as a cost:

Password cracking requires several resources, which are listed below:

1. **Computational resources:**
   - To efficiently process hashes and run tools when cracking passwords, adequate computational power is required.
   - The computational load for this assignment was minimal due to the simplicity of the hashes and the provided optimized wordlist. However, for more complex passwords, additional processing power is required.
2. **Time:**
   - The setup time for this assignment was significant. It took a long time to install and configure John the Ripper, as well as ensure that all files (e.g., wordlist.txt and Group-10.txt) were properly placed and accessible.
   - The cracking process was efficient, with each session taking around 3 seconds for different hash formats (HAVAL-256-3, Panama, Raw-Keccak-256).
3. **Electricity:**
   - This assignment required very little energy because the actual password-cracking process took only a few seconds. However, the setup process, which included format installation and experimentation, used more energy due to prolonged computer usage.
4. **Software Resources:**
   - John the Ripper served as the primary tool. This open-source, free software had no additional costs.
   - The provided wordlist (wordlist.txt) was successful in cracking the passwords, eliminating the need for external wordlists.
5. **Manpower and Expertise**
   - The significant time spent on setup emphasizes the importance of technical knowledge. Identifying the proper hash format and understanding the tool's syntax were critical.
   - Testing multiple hash formats (HAVAL-256-3, Panama, and Raw-Keccak-256) before determining the correct format necessitated both patience and methodical approach.
   - This assignment emphasized the importance of being familiar with password-cracking tools and strategies in order to achieve optimal results.

4] Methodology:

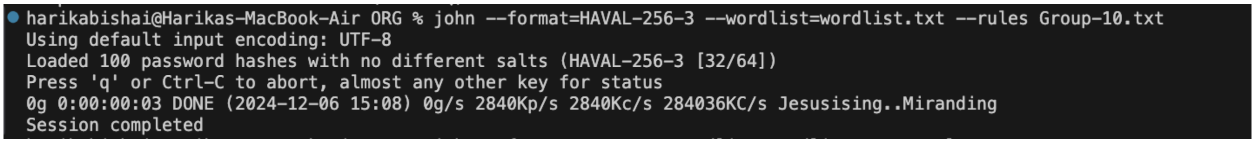
1. **Setup and Install:**

Installed John the Ripper using the official documentation for both Windows and macOS systems. Prepared the necessary files (Group-10.txt for password hashes and wordlist.txt for the dictionary file). Run a test command to ensure that the installation was successful.

2. Experiment with Different Hash Formats:

Tried cracking the passwords using different hash formats to find the correct one.

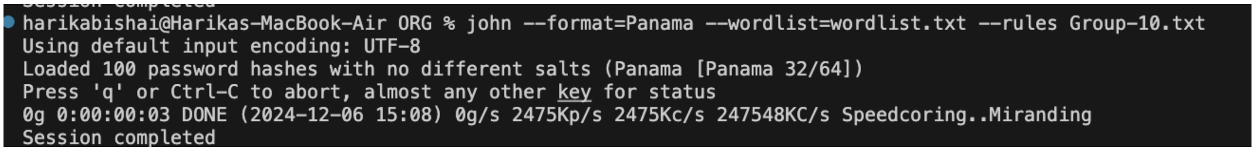
HAVAL-256-3:



```
harikabishai@Harikas-MacBook-Air ORG % john --format=HAVAL-256-3 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (HAVAL-256-3 [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2840Kp/s 2840Kc/s 284036KC/s Jesusising..Miranding
Session completed
```

Result: Completed in 3 seconds. The format cracked passwords, but it was not the appropriate hash format for the given dataset because it did not produce all correct results.

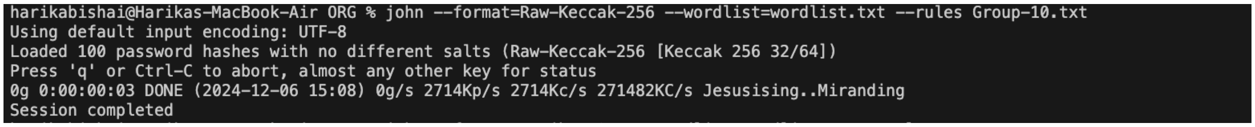
Panama:



```
harikabishai@Harikas-MacBook-Air ORG % john --format=Panama --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Panama [Panama 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2475Kp/s 2475Kc/s 247548KC/s Speedcoring..Miranding
Session completed
```

Result: Completed in 3 seconds. Similar to HAVAL-256-3, the format was capable of cracking passwords but did not produce the desired results for all hashes.

Raw-Keccak-256:

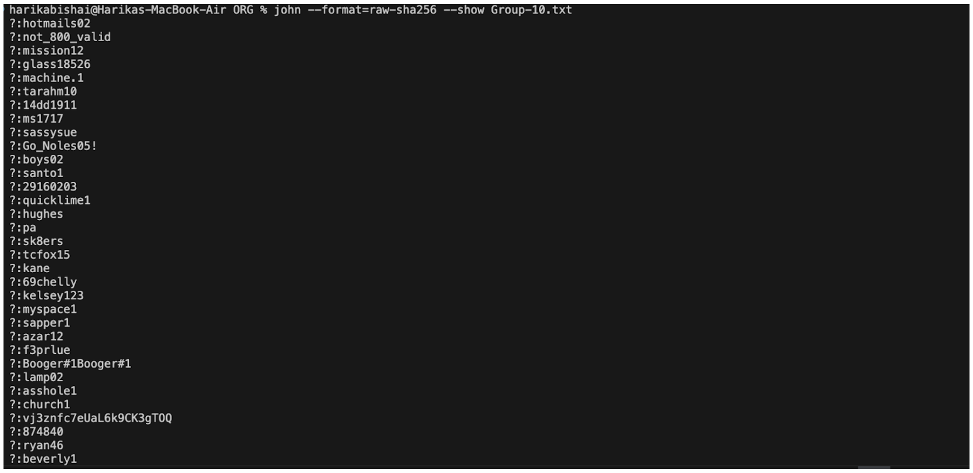


```
harikabishai@Harikas-MacBook-Air ORG % john --format=Raw-Keccak-256 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-Keccak-256 [Keccak 256 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2714Kp/s 2714Kc/s 271482KC/s Jesusising..Miranding
Session completed
```

Result: Completed in 3 seconds. Although it cracked some passwords, this was not the proper format because the output did not correspond to the expected results for all passwords.

These experiments led to the conclusion that Raw-SHA256 was the correct format.

Raw-SHA256:



```
harikabishai@Harikas-MacBook-Air ORG % john --format=raw-sha256 --show Group-10.txt
?:hotmails02
?:not_800_valid
?:mission12
?:glass18526
?:machine.1
?:tarahm10
?:14dd1911
?:ms1717
?:sassysue
?:Go_Noles05!
?:boys02
?:santo1
?:29160203
?:quicklime1
?:hughes
?:pa
?:sk8ers
?:tcfox15
?:kane
?:69chelly
?:kelsey123
?:myspace1
?:sapper1
?:azar12
?:f3prlue
?:Booger#1Booger#1
?:lamp02
?:asshole1
?:church1
?:vj3znfc7eUaL6k9CK3gTOQ
?:874840
?:ryan46
?:beverly1
```

Result: All 100 passwords were successfully cracked in less than a second, confirming that this was the proper hash format for the dataset.

5] Challenges or issues encountered during the process:

1. **Hash identification:** Identifying the correct hash format required several attempts with various formats, including HAVAL-256-3, Panama, and Raw-Keccak-256. This was time-consuming and necessitated consulting documents.
2. **Increased Setup Time:** John the Ripper's installation and configuration took a long time, especially on macOS, due to compatibility issues and dependencies.
3. **Wordlist limitation:** The provided wordlist.txt was sufficient for cracking this assignment's simple passwords. However, for more complex hashes, the wordlist may not have been robust enough.
4. **Computing resources:** Although the computational demand for this task was minimal, longer cracking sessions with larger datasets would necessitate more processing power and possibly GPU support.

6] Reflection on the ethical considerations of password cracking:

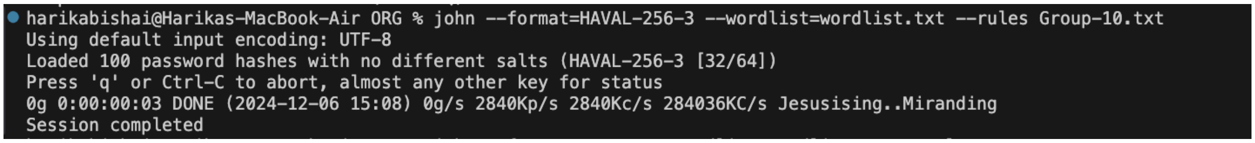
1. **Purpose and Intent:**
   The primary goal of this assignment was educational. The goal was to better understand the vulnerabilities in password-based authentication systems and show how they can be mitigated to improve cybersecurity measures. It is critical to emphasize that the skills and techniques acquired through this assignment should not be used for unauthorized access to any data or systems.
2. **Authorization and Consent:**
   Explicit authorization is required before attempting to crack any passwords. This assignment was completed using the password file (Group-10.txt) provided by the course instructors. Such authorization ensures that the activities are ethical and within the scope of the assignment. Without consent, password cracking is a violation of privacy and trust.
3. **Legal Compliance:**
   Password cracking, even for educational purposes, must follow applicable laws and regulations. Unauthorized cracking activities could result in severe legal consequences. This assignment adhered strictly to the course guidelines and was completed in a controlled and authorized environment.
4. **Privacy and confidentiality:**
   Respect for privacy and confidentiality is essential. Any data or insights obtained through password cracking should be handled responsibly. The passwords cracked for this assignment were used as academic examples and were not disclosed or shared outside of the project.
5. **Educational and Professional Responsibility:**
   Professional development includes the responsibility to apply newly acquired skills constructively. This includes promoting good cybersecurity practices like using strong,

secure passwords and putting in place robust systems to protect sensitive data. The knowledge gained from this assignment should be beneficial to the field of cybersecurity.

6. **Continuous Ethical Learning:**
   Cybersecurity is a constantly evolving field, and ethical considerations must adapt to changes in technology and legislation. It is critical to maintain an up-to-date understanding of ethical practices and to be wary of potential misuse of these skills.

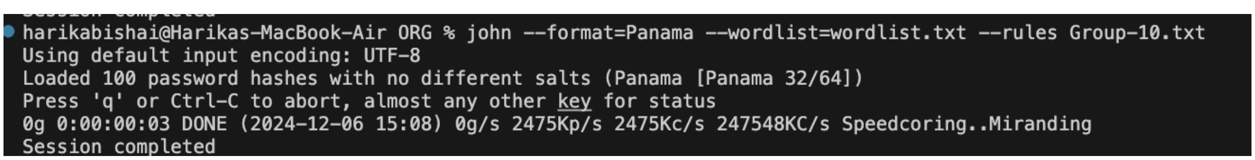
5] Screenshots or command-line examples to illustrate your work:

john --format=HAVAL-256-3 --wordlist=wordlist.txt --rules Group-10.txt



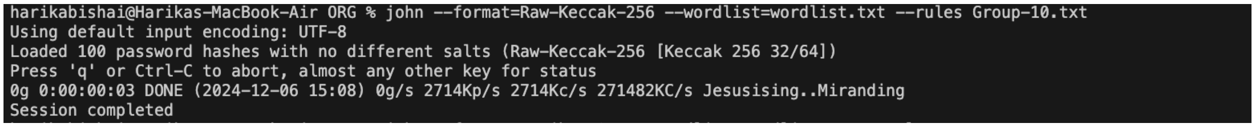
```
harikabishai@Harikas-MacBook-Air ORG % john --format=HAVAL-256-3 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (HAVAL-256-3 [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2840Kp/s 2840Kc/s 284036KC/s Jesusising..Miranding
Session completed
```

john --format=Panama --wordlist=wordlist.txt --rules Group-10.txt



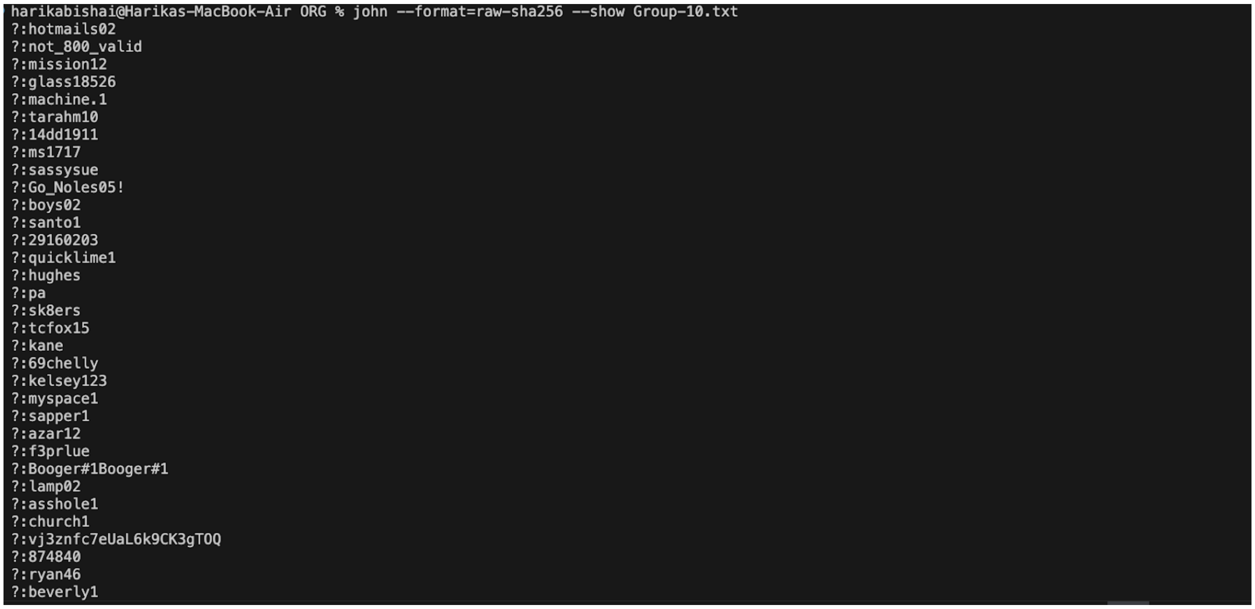
```
harikabishai@Harikas-MacBook-Air ORG % john --format=Panama --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Panama [Panama 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2475Kp/s 2475Kc/s 247548KC/s Speedcoring..Miranding
Session completed
```

john --format=Raw-Keccak-256 --wordlist=wordlist.txt --rules Group-10.txt



```
harikabishai@Harikas-MacBook-Air ORG % john --format=Raw-Keccak-256 --wordlist=wordlist.txt --rules Group-10.txt
Using default input encoding: UTF-8
Loaded 100 password hashes with no different salts (Raw-Keccak-256 [Keccak 256 32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 DONE (2024-12-06 15:08) 0g/s 2714Kp/s 2714Kc/s 271482KC/s Jesusising..Miranding
Session completed
```

john --format=raw-sha256 --wordlist=wordlist.txt Group-10.txt



```
harikabishai@Harikas-MacBook-Air ORG % john --format=raw-sha256 --show Group-10.txt
?:hotmails02
?:not_800_valid
?:mission12
?:glass18526
?:machine.1
?:tarahm10
?:14dd1911
?:ms1717
?:sassysue
?:Go_Noles05!
?:boys02
?:santo1
?:29160203
?:quicklime1
?:hughes
?:pa
?:sk8ers
?:tcfox15
?:kane
?:69chelly
?:kelsey123
?:myspace1
?:sapper1
?:azar12
?:f3prlue
?:Booger#1Booger#1
?:lamp02
?:asshole1
?:church1
?:vj3znfc7eUaL6k9CK3gTOQ
?:874840
?:ryan46
?:beverly1
```