Reverse Linux password hash: 1.2C

➢ **A graphical diagram on the analysis of the /etc/shadow entry**

The /etc/shadow file actually consists of passwords that are encrypted in and are in hash form. `/etc/shadow` file is the text file that holds the information about User password, the hash algorithm used to create hash, the salt value used to create hash and some details related to password expiry. This is the most secured way to store the passwords. We use colon symbol (:) to separate different fields in hash file.

```
Gurjant:$6$5H0QpwprRiJQR19Y$bXGOh7dIfOWpUb :  16431  :  0  :  99999  :  7  :   :    :
|---1---|----------2-----------------------|----3----|--4--|----5----|--6-|-7-|--8-|
```

1. **Username field**: The username field contains the username of the user with which the user enters in his account
2. **Password field**: The password field stores the password in encrypted format.
3. **Last Password Change**: This field denotes the number of days, the last password change happened.
4. **Minimum days between password changes**: This field shows the minimum number of days after which a user has the authority to change his password.
5. **Password validity**: The password validity shows the validity of the password after the validity the user has to change his password.
6. **Warning threshold**: This field denotes the number of days before which the user will receive a warning notification about the password expiry.
7. **Account inactive**: This field denotes the number of days after which the account will be disabled, when the password is expired.
8. **Time since account is disabled**: This field denotes the number of days, from UNIX time, since which the account is disabled.