Structure de l'empreinte

- Exemple d'une empreinte (obtenue par une fonction de hachage)
  - 1abcdefgh$cHJi5PXp/ki/ktXzqlk6l1
- Signification des différents termes : $(**1**)$(**abcdefgh**)$(**cHJi5PXp/ki/ktXzqlk6l1**)
  - $1 : Algorithme MD5
    - $2 : Algorithme Blowfish
    - $5 : Algorithme sha256
    - $6 : Algorithme sha512
- $2 : Piment (salt)
  - Protection contre les attaques par dictionnaire précalculé
  - Piment en clair
- $3 : Empreinte résultante

Format du hash du password

- Les mots de passe sont hachés avec une variante de MD5 s'ils commencent par 1 (une variante du DES était utilisée avant, avec deux caractères de sel).
- la simple récupération des fichiers `/etc/shadow` et `/etc/passwd` suffit
- Fusion des deux fichiers par `unshadow` pour une utilisation par « `John The Ripper` »
  - `john -s ~/unshadow.txt`