Entendendo os Hashes

+ Hashes são códigos que estão atrelados de maneira única a outros arquivos.
+ São gerados por protocolos como SHA256, MD5 e outros

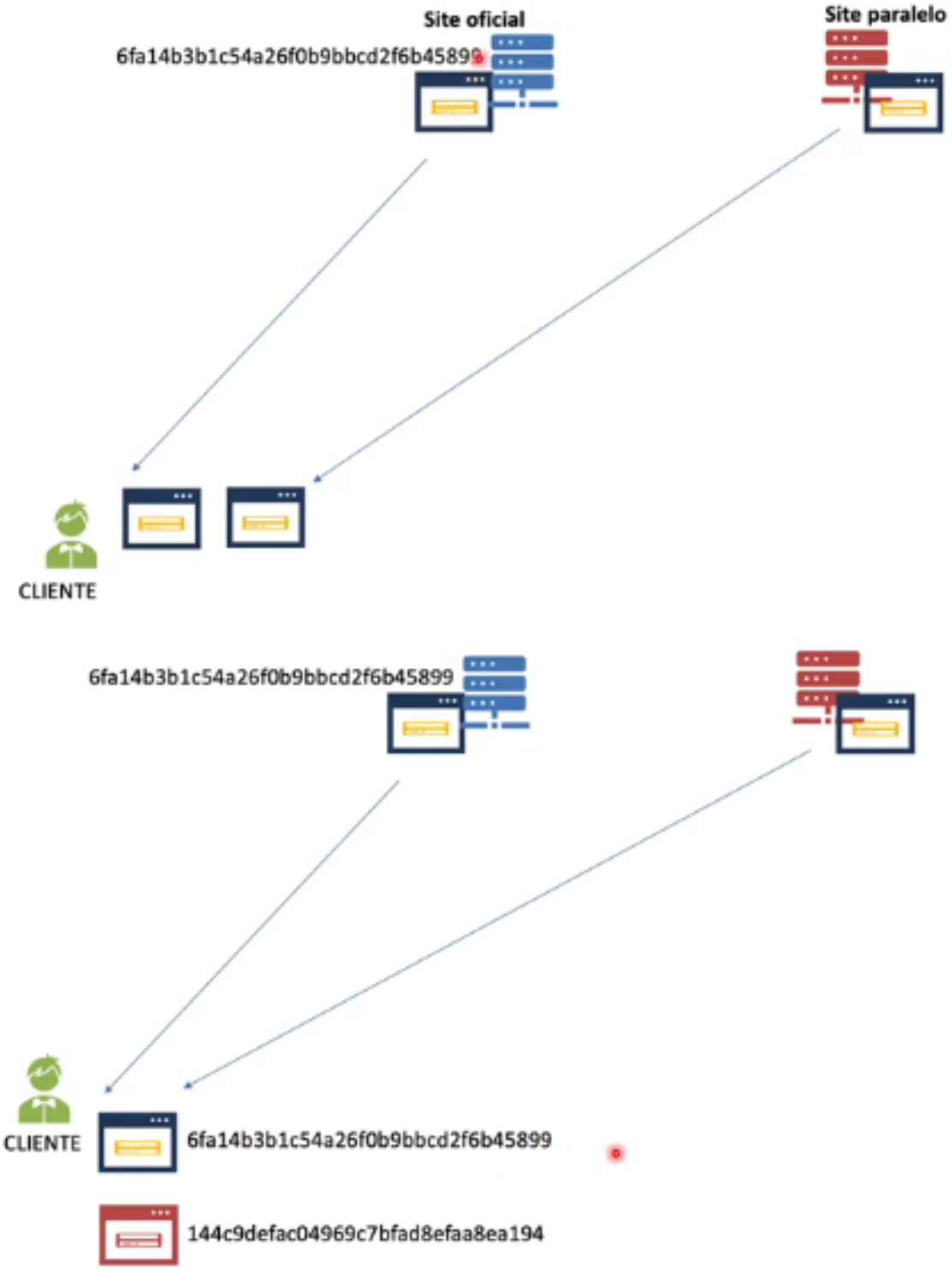
```
desec@pentesting:~$ ./hashes.sh
Exemplo de hash MD5
5a7bb2d0444500e6248c223c4cb24090  -
----------------------------
Exemplo de hash SHA 256
eab06f14966652c95370dffed451d33d34dc7bf483cdbc24544ab4f8cf6e1213  -
desec@pentesting:~$
```

→ um fato importante sobre os hashes é que eles sempre têm um tamanho fixo, independente de estar associados à um arquivo (de senha, por exemplo) grande ou pequeno

+ Exemplos de uso: Autenticação

→ Uma boa prática de segurança é a de tratar as senhas de um determinado sistema com os protocolos de hash como o SHA.
→ Se o desenvolvedor faz as senhas dos clientes serem armazenadas diretamente na base de dados local, um vazamento dessa base de dados implica uma forma direta de acesso para terceiros. Com isso, quando tratamos a senha com um protocolo de hash, que gera um hash único, na hora do acesso o host irá verificar se o hash está ou não cadastrado no banco de dados.

+ Exemplo de uso: Integridade



→ Quando formos baixar um programa, aplicação, etc, devemos olhar se os hashs demonstrados no checksum coincidem ou não com o do arquivo baixado