# Solution : ConnectArcade

Le challenge a pour objectif de déchiffrer une capture Wireshark. Une fois déchiffrée, il sera possible de récupérer le contenu d'un fichier users.json, notamment un hash SHA1, cassable par John the Ripper.

## Déchiffrement des flux dans la capture

Dans la deuxième capture *Capture_Tous_Les_Soirs.pcapng*, il s'agit d'utiliser les informations récoltées dans la première partie pour déchiffrer une partie de la capture. L'objectif est de récolter le contenu d'un fichier *users.json* qui contient un Hash en SHA1 cassable via la wordlist *RockYou*.

- Ajout des clés TLS dans Wireshark pour déchiffrer les trames : *Editer -> Préférences -> Protocols -> TLS -> Pre-Master-Secret log filename*
- Filtrage des trames web avec le filtre *http*
- Demande douteuse de fichier users.json à la trame 1606
- Récupération du hash SHA1 dans la trame 1608 dans *JS Object Notation -> Array -> Object -> Member : passwordHash -> stringvalue*
- Hash à casser : *9637e2d6097ad0e11625f319813218628cd7054a*
- Utiliser John the Ripper :
    - *john --format=raw-sha1 --wordlist=/usr/share/wordlists/rockyou.txt hash.txt*

Le flag final est FMCTF{Saintmalo07}.