We used the “Jumbo” community version of john the ripper to find the following password(https://github.com/magnumripper/john)

Oilers password: igor%Vyazmikin

Process:

We got the players names on the early 90s roster for the oiler(89-95) using a site called “www.hockeydb.com”. Then we wrote a python script(part4.py) to handle the different mangling options and pass the output into a new file. Then we simply supplied the mangled word list to john the ripper. It took about 5 hours to compile the names and write the python script. It took john the ripper 0 seconds to find the password when supplied the mangled wordList.

Commands Ran on the command line

1. We gathered the player names on the early 90s roster (89-85) into a file named “OilersWordList”
2. Supplied that wordlist to the python program to handle the mangling and produce another file with the mangled names:
    - python3 OilersWordList mangledOilersList
3. The python program then we ran that file with JTR against the hashed passwords:
    - nice -19 ./john --wordlist=OilersWordList part4Hashes

English word with leet password: rel47ionship

Process:

We got a list of 275,000 english words from a git repository (https://github.com/words/an-array-of-english-words). Then we wrote a python script(leetpwd.py) to handle the conversions of 2 different characters for words and passed the output into a file. Then supplied the converted words to john the ripper. It took about 5 hours to do research on leet and create a good algorithm to convert the words based on the assignment description. It took john the ripper 1minute and 30s to find the password when supplied the converted wordlist.

Commands Ran on the command line

1. To generate list of english words(based on the website above):
    - words > englishWords
2. Supply the file to the python program to create a wordlist with the appropriate leet conversions:
    - python3 leetpwd.py englishWords
3. The python program will create a file called “leetOption1”, then we ran that file with JTR against the hashed passwords:
    - nice -19 ./john --wordlist=leetOption1 part4Hashes

Hexadecimal number password: bbf0f777

Process:

We created a character set of 0-9 and a-f, then used incremental mode with that character set on the hashes given to us. It took john the ripper about 22hrs to find the correct password.(21:44:09)

Commands Ran on the command line

1. Created pot file character set :
    - echo “:0123456789abcdef” > hex.pot
2. Created character set from pot file:
    - ./john --make-charset=hex.chr -pot=hex.pot
3. Running incremental mode with the character set file (specified in john-local.conf) with john the ripper.
    - nice -19 ./john --incremental=hex part4Hashes

Spanish Word password: desengoznara

Process:

We got a list of 636,000 spanish words from a website (https://www.npmjs.com/package/an-array-of-spanish-words), then we supplied the list to john the ripper against the hashes given to us. It took about 15 seconds to get the correct password.

Commands Ran on the command line

1. To generate list of spanish words(based on the website above);
    - palabras > spanishWords

2. Running the generated wordList with JTR:
    - nice -19 ./john --wordlist=spanishWords part4Hashes