

Proxmark3 DESFire Cheat Sheet

Analyzing traces

Open proxmark3 in offline mode

```
./pm3 -o
```

Load and analyze a trace file

```
trace load -f ../path/to/file.trace  
hf mfdes list
```

General tips

--no-auth is your friend (force proxmark to skip auth altogether)

-h is your friend (options & examples for all commands)

hf mfdes help is your friend (grouped list of all DESFire commands)

-n/-t/-k specify the key parameters used in authentication (only use when required)

Analyzing cards

```
hf mfdes info  
hf mfdes lsapp  
hf mfdes lsfiles --aid <app-id>  
hf mfdes read --aid <app-id> --fid <file-id>
```

Programming cards

App operations

```
hf mfdes createapp --aid <app-id> --dstalgo <DES|2TDEA|3TDEA|AES>  
hf mfdes deleteapp --aid <app-id>
```

File operations

```
hf mfdes createfile --aid <app-id> --fid <file-id> --size <size>  
hf mfdes deletefile --aid <app-id> --fid <file-id>  
hf mfdes chfilesettings --aid <app-id> --fid <file-id>  
hf mfdes write --aid <app-id> --fid <file-id> -d <hex>
```

Key operations

```
hf mfdes changekey --aid <app-id> --newkeyno <keyno> --newkey <hex>
```