📖

NTDS.DIT

> 💡 This article is a quick guide on how to setup and install the tools needed to read out an NTDS.DIT file on Linux. It is useful to parse the NTDS.dit file IoT find the creation date of accounts in the domain for example.
> **REQUIREMENTS**: the **NTDS.dit file** AND the **SYSTEM hive**

> ⚠️ This has been tested on a clean Ubuntu and Kali machine.

> ℹ️ *Source: https://blog.ropnop.com/extracting-hashes-and-domain-info-from-ntds-dit/*

> ➡️ Example NTDS.dit file from Didier Stevens: https://didierstevens.com/files/data/ntds.zip

First, you need to extract the tables from the NTDS.dit file using `esedbexport`, which is a part of `libesedb`. Make sure that you install python2 and python2-dev since the tools we'll be using are quite old.

```
sudo apt-get update && apt-get upgrade
sudo apt-get install autoconf automake autopoint libtool pkg-config make python2 curl python2-dev
wget https://github.com/libyal/libesedb/releases/download/20210424/libesedb-experimental-20210424.tar.gz
tar xf libesedb-experimental-20210424.tar.gz
cd libesedb-20210424
```

Then configure, compile and install the tool.

```
./configure # run with the option --disable-dependency-tracking if you are configuring on a clean Ubuntu (on Kali it's not nescessary)
make
make install
ldconfig
```

Now that the tool is ready, use it to export the tables from your NTDS.dit file. This will create a new directory called `ntds.dit.export`. The two most important tables are datatable and link_table, as we are going to use them next to parse the user information.

> ⚠️ If the NTDS.dit file is big, it can take a while to export all the info.

```
/usr/local/bin/esedbexport -m tables <path/to/ntds.dit>
```

Now that we've exported the tables to ASCII, we need to use the tool `ntdsxtract` to parse the data. Clone the repo and install the script.

```
cd .. # if you are still in libesedb-20210424/
git clone https://github.com/csababarta/ntdsxtract.git
```

```
cd ntdsxtract
python2 setup.py build && python2 setup.py install
```

If you would run the tools from `ntdsxtract` right now, you'll probably get errors indicating that some modules are missing (Crypto.Hash). To solve this, we'll need to download the package installer pip for python2 and add those python2 modules. Once pip2 is installed, just note that it will initially not be added to PATH.

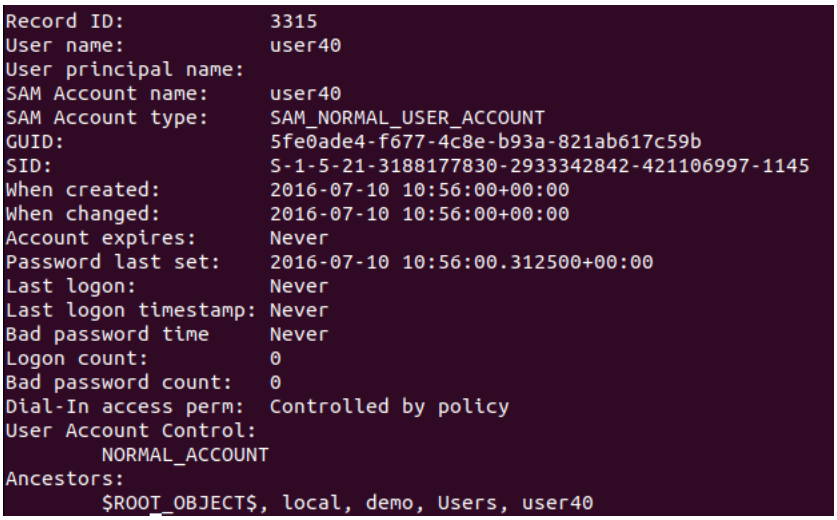
```
curl https://bootstrap.pypa.io/pip/2.7/get-pip.py -o ../get-pip.py
python2 get-pip.py
pip2 install --upgrade setuptools
pip2 install pycrypto
```

Now you can use `ntdsxtract`!

```
# Parse user info from the datatable and the linktable
python2 dsusers.py <datatable> <linktable> ./output --syshive <systemhive> --csvoutfile output.csv
# It could be that the script asks for the correct schema id, just try all the different shema id's untill one works. I don't know how to '

# Make a timeline of events from the datatable
python2 dstimeline.py ntds.dit.export/datatable.3 ./output-timeline --csv --outfile timeline.csv

# Parse computer info from the datatable and the SYSTEM hive
python2 dscomputers.py ntds.dit.export/datatable.3 ./ --syshive <PATH/TO/SYSTEMHIVE> --csvoutfile output.csv
```



Example output from dsusers.py. You can also export this info into a .csv.

```
2016-07-10 10:55:45.375000+00:00|Password changed|3307|user32 (7bb96027-6c60-4a25-b257-2a415849c200) (Person)
2016-07-10 10:55:45.390625+00:00|Password changed|3308|user33 (7eaf10b7-f90d-4692-945d-ae7e8cfcf3b9) (Person)
2016-07-10 10:55:45.421875+00:00|Password changed|3309|user34 (bccd90da-4c25-499c-a2e5-3341392bcf8f) (Person)
2016-07-10 10:55:48+00:00|Created|3310|user35 (c353c6ed-3f64-41ac-9baa-600cbe7f4c69) (Person)
2016-07-10 10:55:48+00:00|Modified|3310|user35 (c353c6ed-3f64-41ac-9baa-600cbe7f4c69) (Person)
2016-07-10 10:55:48.125000+00:00|Password changed|3310|user35 (c353c6ed-3f64-41ac-9baa-600cbe7f4c69) (Person)
2016-07-10 10:55:51+00:00|Created|3311|user36 (e1409149-9b9a-4bc3-9cf1-e184259029b1) (Person)
2016-07-10 10:55:51+00:00|Modified|3311|user36 (e1409149-9b9a-4bc3-9cf1-e184259029b1) (Person)
2016-07-10 10:55:51.843750+00:00|Password changed|3311|user36 (e1409149-9b9a-4bc3-9cf1-e184259029b1) (Person)
2016-07-10 10:55:53+00:00|Created|3312|user37 (9ae58f38-d8a1-4076-a2b5-15e44cc2eb77) (Person)
2016-07-10 10:55:53+00:00|Modified|3312|user37 (9ae58f38-d8a1-4076-a2b5-15e44cc2eb77) (Person)
2016-07-10 10:55:53.343750+00:00|Password changed|3312|user37 (9ae58f38-d8a1-4076-a2b5-15e44cc2eb77) (Person)
2016-07-10 10:55:54+00:00|Created|3313|user38 (c0661e29-7525-46c2-964c-c6764d67ead8) (Person)
2016-07-10 10:55:54+00:00|Modified|3313|user38 (c0661e29-7525-46c2-964c-c6764d67ead8) (Person)
2016-07-10 10:55:54.015625+00:00|Password changed|3313|user38 (c0661e29-7525-46c2-964c-c6764d67ead8) (Person)
2016-07-10 10:55:59+00:00|Created|3314|user39 (505873dc-26c9-4a42-9b9c-6e3a5331f8de) (Person)
2016-07-10 10:55:59+00:00|Modified|3314|user39 (505873dc-26c9-4a42-9b9c-6e3a5331f8de) (Person)
2016-07-10 10:55:59.453125+00:00|Password changed|3314|user39 (505873dc-26c9-4a42-9b9c-6e3a5331f8de) (Person)
2016-07-10 10:56:00+00:00|Created|3315|user40 (5fe0ade4-f677-4c8e-b93a-821ab617c59b) (Person)
2016-07-10 10:56:00+00:00|Modified|3315|user40 (5fe0ade4-f677-4c8e-b93a-821ab617c59b) (Person)
2016-07-10 10:56:00.312500+00:00|Password changed|3315|user40 (5fe0ade4-f677-4c8e-b93a-821ab617c59b) (Person)
```

Example output from dstimeline.py. You can export this info into a .csv.

```
List of computers:
==================
Record ID:            1836
Computer name:        ADDEMO
DNS name:             addemo.demo.local
GUID:                 f999af36-a3bb-42cc-96d1-8f86cc1ffe6d
SID:                  S-1-5-21-3188177830-2933342842-421106997-1003
OS name:              Windows Server 2003
OS version:           5.2 (3790)
When created:         2016-07-10 08:15:31+00:00
When changed:         2016-07-10 08:16:17+00:00
Dial-In access perm:  Controlled by policy
Ancestors:
        $ROOT_OBJECT$ local demo Domain Controllers ADDEMO
```

Example output from dscomputers.py. You can export this info into a .csv.