We're continuing to fight for universal access to quality information—and you can help as we continue to make improvements. Will you chip in?

https://github.com/yosqueoy/ditsnap Go JUN NOV MAY
7 captures 24
11 Jun 2018 - 18 Se 2018 2020 2022 About this capture

yosqueoy / **ditsnap**

Watch 7 Star 54 Fork 12

Join GitHub today

GitHub is home to over 50 million developers working together to host and review code, manage projects, and build software together.

Sign up

Dismiss

master 1 branch 2 tags Go to file Code

yosqueoy Migrate to CommonMark aecc314 on 1 Apr 2017 **79** commits

EseDataAccess	refactoring	4 years ago
VssCopy	refactoring	4 years ago
ditsnap_exe	clean	4 years ago
images	update image	4 years ago
.gitignore	refactoring	4 years ago
LISENCE.md	Update LISENCE.md	4 years ago
README.md	Migrate to CommonMark	4 years ago
ditsnap.sln	refactoring	6 years ago

README.md

DIT Snapshot Viewer

DIT Snapshot Viewer is an inspection tool for Active Directory database, ntds.dit. This tool connects to ESE (Extensible Storage Engine) and reads tables/records including hidden objects by low level C API.

The tool can extract ntds.dit file without stopping lsass.exe. When Active Directory Service is running, lsass.exe locks the file and does not allow to access to it. The snapshot wizard copies ntds.dit using VSS (Volume Shadow Copy Service) even if the file is exclusively locked. As copying ntds.dit may cause data inconsistency in ESE DB, the wizard automatically runs **esentutil /repair** command to fix the inconsistency.

The executable is available here. Download ditsnap.exe

Screenshots

About

An inspection tool for Active Directory database

Readme

Releases 2

ditsnap.exe 1.4.3.0 Latest
on 26 Sep 2016

+ 1 release

Packages

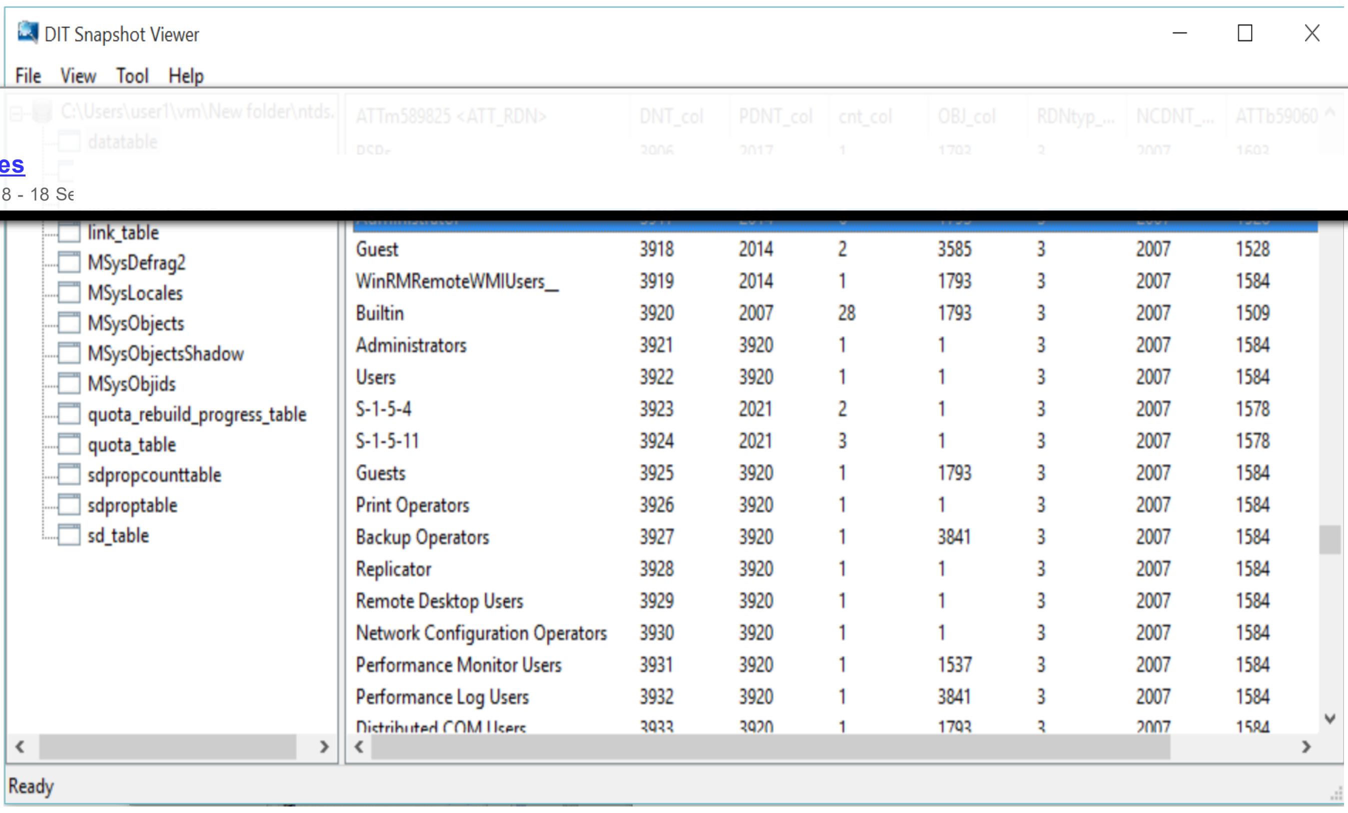
No packages published

Languages

● C 47.4% ● C++ 38.9%
● Objective-C 13.7%

We use **optional** third-party analytics cookies to understand how you use GitHub.com so we can build better products. Learn more.

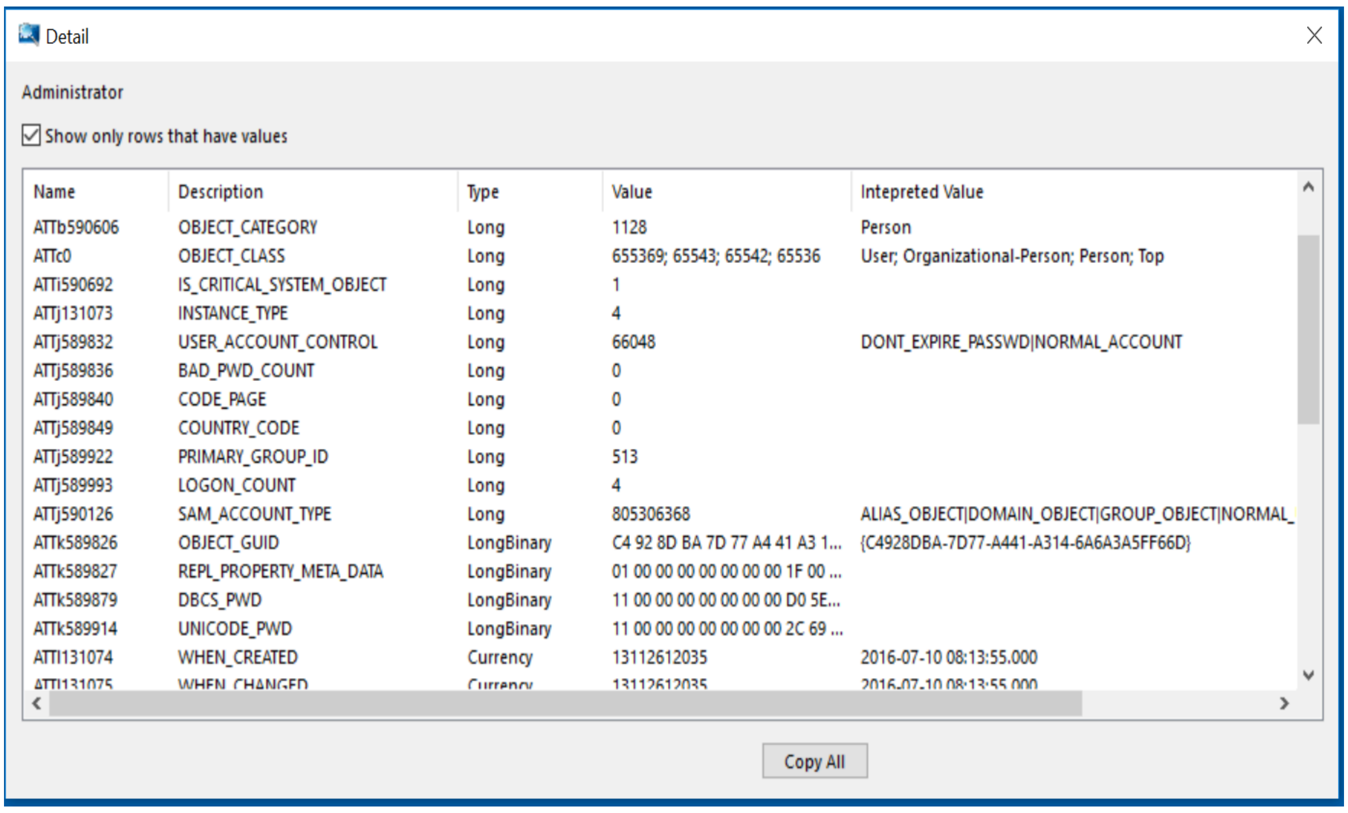
Accept Reject



ATTm589825 <ATT_RDN>	DNT_col	PDNT_col	cnt_col	OBJ_col	RDNtyp_...	NCDNT_...	ATTb59060
Guest	3918	2014	2	3585	3	2007	1528
WinRMRemoteWMIUsers__	3919	2014	1	1793	3	2007	1584
Builtin	3920	2007	28	1793	3	2007	1509
Administrators	3921	3920	1	1	3	2007	1584
Users	3922	3920	1	1	3	2007	1584
S-1-5-4	3923	2021	2	1	3	2007	1578
S-1-5-11	3924	2021	3	1	3	2007	1578
Guests	3925	3920	1	1793	3	2007	1584
Print Operators	3926	3920	1	1	3	2007	1584
Backup Operators	3927	3920	1	3841	3	2007	1584
Replicator	3928	3920	1	1	3	2007	1584
Remote Desktop Users	3929	3920	1	1	3	2007	1584
Network Configuration Operators	3930	3920	1	1	3	2007	1584
Performance Monitor Users	3931	3920	1	1537	3	2007	1584
Performance Log Users	3932	3920	1	3841	3	2007	1584
Distributed COM Users	3933	3920	1	1793	3	2007	1584

7 captures
11 Jun 2018 - 18 Se
JUN NOV MAY
2018 24 2020 2022
About this capture

Detail Dialog



Administrator

☑ Show only rows that have values

Name	Description	Type	Value	Intepreted Value
ATTb590606	OBJECT_CATEGORY	Long	1128	Person
ATTc0	OBJECT_CLASS	Long	655369; 65543; 65542; 65536	User; Organizational-Person; Person; Top
ATTi590692	IS_CRITICAL_SYSTEM_OBJECT	Long	1	
ATTj131073	INSTANCE_TYPE	Long	4	
ATTj589832	USER_ACCOUNT_CONTROL	Long	66048	DONT_EXPIRE_PASSWD|NORMAL_ACCOUNT
ATTj589836	BAD_PWD_COUNT	Long	0	
ATTj589840	CODE_PAGE	Long	0	
ATTj589849	COUNTRY_CODE	Long	0	
ATTj589922	PRIMARY_GROUP_ID	Long	513	
ATTj589993	LOGON_COUNT	Long	4	
ATTj590126	SAM_ACCOUNT_TYPE	Long	805306368	ALIAS_OBJECT|DOMAIN_OBJECT|GROUP_OBJECT|NORMAL_
ATTk589826	OBJECT_GUID	LongBinary	C4 92 8D BA 7D 77 A4 41 A3 1...	{C4928DBA-7D77-A441-A314-6A6A3A5FF66D}
ATTk589827	REPL_PROPERTY_META_DATA	LongBinary	01 00 00 00 00 00 00 00 1F 00 ...	
ATTk589879	DBCS_PWD	LongBinary	11 00 00 00 00 00 00 00 D0 5E...	
ATTk589914	UNICODE_PWD	LongBinary	11 00 00 00 00 00 00 00 2C 69 ...	
ATTl131074	WHEN_CREATED	Currency	13112612035	2016-07-10 08:13:55.000
ATTl131075	WHEN_CHANGED	Currency	13112612035	2016-07-10 08:13:55.000

Interpreted Value

Interpreted Value column in Detail Dialog shows human-readable representaions of raw ESE column values. Here are the exmamples.

OBJECT_CATEGORY

The attribute is stored as a 32-bit integer in ESE, which points to DNT (Distinguished Name Tag) of another Active Directory object. Interpreted Value for the attribute shows RDN (Relative Distinguished Name) of the object.

OBJECT_CLASS

The attribute is stored as a multi-valued 32-bit integer column in ESE, which points to GOVERNS_ID of other objects. Interpreted Value for the attribute shows RDNs of the objects.

PWD_LAST_SET, LAST_LOGON, LAST_LOGOFF, ACCOUNT_EXPIRES

Those attributes are stored as 64-bit integers in ESE, which are treated as FILETIME in Active Directory. Interpreted Value column for the attributes shows it as a date format.

WHEN_CREATED, WHEN_CHANGED

We use **optional** third-party analytics cookies to understand how you use GitHub.com so we can build better products.
Learn more.

shows it as a date format.

USER_ACCOUNT_CONTROL

The attribute is stored as a 32-bit integer in ESE, which are treated as flags that control the behavior of the user account. Interpreted Value for the attribute shows the list of flags. See

7 captures
11 Jun 2018 - 18 Se
JUN NOV MAY
2018 24 2020 2022
About this capture

EseDataAccess static library

EseDataAccess static library can be used for other ESE inspection applications. EseDataAccess.h contains C++ object-oriented representation of ESE C API. For example, ESE table is represented by EseTable class defined as below.

```
class EseTable
{
        public:
                EseTable(const EseDatabase* const eseDatabase, string tableName);
                ~EseTable();
                void MoveFirstRecord() const;
                bool MoveNextRecord() const;
                void Move(uint rowIndex) const;
                int CountColumnValue(uint columnIndex) const;
                wstring RetrieveColumnDataAsString(uint columnIndex, uint itagSequ
                uint GetColumnCount() const;
                wstring GetColumnName(uint columnIndex) const;
}
```

© 2020 GitHub, Inc. Terms Privacy Security Status Help Contact GitHub Pricing API Training Blog About

We use **optional** third-party analytics cookies to understand how you use GitHub.com so we can build better products.
Learn more.