


 [dsnezhkov](#) / [TruffleSnout](#) Public

 Notifications

 Fork 19

 Star 85

[Code](#) [Issues 1](#) [Pull requests](#) [Actions](#) [Security](#) [Insights](#)






[TruffleSnout](#) / [TruffleSnout](#) / [Docs](#) / [USAGE.md](#) 





457 lines (370 loc) • 17.6 KB

[Preview](#) [Code](#) [Blame](#)

[Raw](#)     

# Intro

TruffleSnout is designed to help operators in a targeted discovery of immediate and adjacent AD infrastructure, query AD objects. It is designed to work in iterative fashion and provides granular control of the types of queries the operator can issue. This helps preserving a degree of operational security where the operator can limit and vary queries to match the perceived defenses and avoid triggering alerts or generate excessive logging.

The tool follows the natural discovery workflow many operators execute on the internal networks and helps answer precise questions like:

- Which forest am I in
- What domains exist in this forest
- What properties and components does a domain have
- What types of trusts do forest and domains have
- What is the first and primary domain in the forest
- Where are the Global catalogs
- What are sites and links
- Can I connect and ask the same of the remote domain

- Can I be flexible with method connection.
- Can I query objects via AD LDAP.
- Can I query a specific attribute or a list of the object
- Can I search for patterns in the returned result.

A few initial utilities to analyze the returned information are provided. By being flexible on the LDAP queries operators are not restricted in their exploration of AD objects to commonly used sets like groups, users, computers. Operators can query DNS, Certificates and other types of resources stored in the hierarchy.

## Examples

### Forest level

```
.\TruffleSnout.exe forest -n top.int
[*] Discovering forest top.int
Forest Name: top.int
      Forest Mode: unknown
      Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
```

```
.\TruffleSnout.exe forest -n top.int -d
[*] Discovering forest top.int
Forest Name: top.int
      Forest Mode: unknown
      Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
      Forest Root Domain: top.int
      Domains in Forest:
          * top.int
          - twin.local
```

```
.\TruffleSnout.exe forest -n top.int -s
[*] Discovering forest top.int
Forest Name: top.int
      Forest Mode: unknown
      Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
      Forest Sites:
          AD Site: Default-First-Site-Name
          Site Link: DEFAULTIPSITELINK
```

```
.\TruffleSnout.exe forest -n top.int -g
[*] Discovering forest top.int
```

```
Forest Name: top.int
  Forest Mode: unknown
  Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
  Forest GCs (Discoverable):
    GlobalCatalog: win-3gk559644av.twin.local 10.0.2.100, win-3gk559644av.twin.local 10.0.2.100, win-inemggj3oef.top.int 10.0.2.200, win-inemggj3oef.top.int 10.0.2.200
  Forest GCs (All):
    GlobalCatalog: WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-3GK559644AV.twin.local 10.0.2.100, WIN-3GK559644AV.twin.local 10.0.2.100
```

```
.\TruffleSnout.exe forest -n top.int -t
[*] Discovering forest top.int
Forest Name: top.int
  Forest Mode: unknown
  Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
  Forest Trust:
    Source: top.int, Target: other.int, Direction: Bidirectional, TrustLevel: Full
```

```
.\TruffleSnout.exe forest -n top.int -a
[*] Discovering forest top.int
Forest Name: top.int
  Forest Mode: unknown
  Forest FSMO Master DC: WIN-INEMGGJ30EF.top.int
  Forest GCs (Discoverable):
    GlobalCatalog: win-3gk559644av.twin.local 10.0.2.100, win-3gk559644av.twin.local 10.0.2.100, win-inemggj3oef.top.int 10.0.2.200, win-inemggj3oef.top.int 10.0.2.200
  Forest GCs (All):
    GlobalCatalog: WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-INEMGGJ30EF.top.int 10.0.2.200, WIN-3GK559644AV.twin.local 10.0.2.100, WIN-3GK559644AV.twin.local 10.0.2.100
  Forest Sites:
    AD Site: Default-First-Site-Name
    Site Link: DEFAULTIPSITELINK
  Forest Trust:
    Source: top.int, Target: other.int, Direction: Bidirectional, TrustLevel: Full
  Forest Root Domain: top.int
  Domains in Forest:
    * top.int
    - twin.local
```

```
.\TruffleSnout.exe forest -n other.int -a -U user1 -P interactive
Enter <masked> credentials for `user1` : *****
```

```
[*] Discovering forest other.int
Forest Name: other.int
```

```
Forest Mode: unknown
Forest FSMO Master DC: WIN-VC752UMUPSS.other.int
Forest GCs (Discoverable):
    GlobalCatalog: win-vc752umupss.other.int 10.0.2.250, win-vc752umup:
Forest GCs (All):
    GlobalCatalog: WIN-VC752UMUPSS.other.int 10.0.2.250, WIN-VC752UMUP:
Forest Sites:
    AD Site: Default-First-Site-Name
    Site Link: DEFAULTIPSITELINK
Forest Trust:
    Source: other.int, Target: top.int, Direction: Bidirectional, Trus:
Forest Root Domain: other.int
Domains in Forest:
    * other.int
```

```
.\TruffleSnout.exe forest -n other.int -a -U user1 -P *****
```

## Domain level

```
.\TruffleSnout.exe domain -n twin.local
[*] Discovering domain twin.local
Domain Name: twin.local
Domain Forest: top.int
Domain Mode: Unknown
Domain Parent: None
Domain PDC: WIN-3GK559644AV.twin.local
Domain RID Master: WIN-3GK559644AV.twin.local
All DCs:
    DomainController : WIN-3GK559644AV.twin.local, Windows Server 2016 Standard
All Discoverable DCs:
    DomainController :
        Name: win-3gk559644av.twin.local
        Domain: twin.local
        Forest: top.int
        Time: 3/16/2020 7:20:27 PM
        IP Address: 10.0.2.100
        OS Version: Windows Server 2016 Standard
        Site Name: Default-First-Site-Name
        Is GC?: True
Inbound Replication: CN=1ee4f7a7-e917-43a7-937a-35b9cf010e35 WIN-INEMGGJ30EF.top.i
Outbound Replication: CN=88f32859-af2e-4cc0-b114-e3e293d7eda9 WIN-3GK559644AV.twin
Domain Children: None
Domain Trusts:
    Source: twin.local, Target: top.int, Direction: Bidirectional, Tru:
```



```
.\TruffleSnout.exe domain -n twin.local -U user1 -P ***
```

## Directory level

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&(objectClass=
[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))

LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
  admincount:Int: 1
  samaccountname:String: Administrator
  cn:String: Administrator
  pwdlastset:Int: 132280093628558583
  whencreated:DateTime: 3/6/2020 11:14:29 PM
  badpwdcount:Int: 0
  lastlogon:Int: 132286144697837082
  samaccounttype:Int: 805306368
  countrycode:Int: 0
  objectguid:Bytes : 225 20 177 89 145 45 176 72 185 152 192 115 11 134 172 1
  lastlogontimestamp:Int: 132280106153805870
  usnchanged:Int: 12769
  whenchanged:DateTime: 3/6/2020 11:33:13 PM
  name:String: Administrator
  objectsid:Bytes : 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 51 26 1 202
  logoncount:Int: 13
  badpasswordtime:Int: 0
  accountexpires:Int: 0
  primarygroupid:Int: 513
  objectcategory:String: CN=Person,CN=Schema,CN=Configuration,DC=other,DC=in
  useraccountcontrol:Int: 512
  description:String: Built-in account for administering the computer/domain
  dscorepropagationdata:DateTime: 3/6/2020 11:33:13 PM
  dscorepropagationdata:DateTime: 3/6/2020 11:33:13 PM
  dscorepropagationdata:DateTime: 3/6/2020 11:18:03 PM
  dscorepropagationdata:DateTime: 1/1/1601 6:12:16 PM
  distinguishedname:String: CN=Administrator,CN=Users,DC=other,DC=int
  iscriticalsystemobject:System.Boolean: True
  objectclass:String: top
  objectclass:String: person
  objectclass:String: organizationalPerson
  objectclass:String: user
```


```
usncreated:Int: 8196
memberof:String: CN=Group Policy Creator Owners,CN=Users,DC=other,DC=int
memberof:String: CN=Domain Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Enterprise Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Schema Admins,CN=Users,DC=other,DC=int
memberof:String: CN=Administrators,CN=Builtin,DC=other,DC=int
adspath:String: LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
lastlogoff:Int: 0
logonhours:Bytes : 255 255 255 255 255 255 255 255 255 255 255 255 255 255
instancetype:Int: 4
codepage:Int: 0
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
iscriticalsystemobject:System.Boolean: True
samaccountname:String: Guest
cn:String: Guest
pwdlastset:Int: 0
whencreated:DateTime: 3/6/2020 11:14:29 PM
badpwdcount:Int: 0
lastlogon:Int: 0
samaccounttype:Int: 805306368
countrycode:Int: 0
objectguid:Bytes : 63 61 74 97 39 244 73 66 164 18 41 101 168 209 91 162
usnchanged:Int: 8197
whenchanged:DateTime: 3/6/2020 11:14:29 PM
name:String: Guest
objectsid:Bytes : 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 51 26 1 202
logoncount:Int: 0
badpasswordtime:Int: 0
accountexpires:Int: 9223372036854775807
primarygroupid:Int: 514
objectcategory:String: CN=Person,CN=Schema,CN=Configuration,DC=other,DC=in
useraccountcontrol:Int: 66082
description:String: Built-in account for guest access to the computer/doma
dscorepropagationdata:DateTime: 3/6/2020 11:18:03 PM
dscorepropagationdata:DateTime: 1/1/1601 12:00:01 AM
distinguishedname:String: CN=Guest,CN=Users,DC=other,DC=int
objectclass:String: top
objectclass:String: person
objectclass:String: organizationalPerson
objectclass:String: user
usncreated:Int: 8197
memberof:String: CN=Guests,CN=Builtin,DC=other,DC=int
adspath:String: LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
lastlogoff:Int: 0
instancetype:Int: 4
codepage:Int: 0
```

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&(objectClass=

[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))

LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
    badpwdcount:Int: 0
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
    badpwdcount:Int: 0

.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&(objectClass=
```

```
.\TruffleSnout.exe directory -l LDAP://other.int/DC=other,DC=int -f '(&(objectClass= 

[*] Directory LDAP://other.int/DC=other,DC=int
Auth type: Secure
[*] Query: (&(objectClass=user))

LDAP://other.int/CN=Administrator,CN=Users,DC=other,DC=int
    cn:String: Administrator
    badpwdcount:Int: 0
    memberof:String: CN=Group Policy Creator Owners,CN=Users,DC=other,DC=int
    memberof:String: CN=Domain Admins,CN=Users,DC=other,DC=int
    memberof:String: CN=Enterprise Admins,CN=Users,DC=other,DC=int
    memberof:String: CN=Schema Admins,CN=Users,DC=other,DC=int
    memberof:String: CN=Administrators,CN=Builtin,DC=other,DC=int
LDAP://other.int/CN=Guest,CN=Users,DC=other,DC=int
    cn:String: Guest
    badpwdcount:Int: 0
    memberof:String: CN=Guests,CN=Builtin,DC=other,DC=int
LDAP://other.int/CN=DefaultAccount,CN=Users,DC=other,DC=int
    cn:String: DefaultAccount
    badpwdcount:Int: 0
    memberof:String: CN=System Managed Accounts Group,CN=Builtin,DC=other,DC=i
LDAP://other.int/CN=WIN-VC752UMUPSS,OU=Domain Controllers,DC=other,DC=int
    cn:String: WIN-VC752UMUPSS
    badpwdcount:Int: 0
LDAP://other.int/CN=krbtgt,CN=Users,DC=other,DC=int
    cn:String: krbtgt
    badpwdcount:Int: 0
    memberof:String: CN=Denied RODC Password Replication Group,CN=Users,DC=oth
LDAP://other.int/CN=TOP$,CN=Users,DC=other,DC=int
```

```
cn:String: TOP$  
badpwdcount:Int: 0
```

```
.\TruffleSnout.exe util --expires 9223372036854775807  
Expires? True
```

```
.\TruffleSnout.exe util --ticks2date 132280170552471892  
3/7/2020 1:10:55 AM
```

```
.\TruffleSnout.exe util -s 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 51 26 :  
SID: S-1-5-21-3779288577-439595492-2162805249-1104
```

```
.\TruffleSnout.exe util -g 24 184 226 216 110 108 41 79 149 222 213 140 6 116 20  
GUID: d8e2b818-6c6e-4f29-95de-d58c0674c8ac
```

## Usage

### Actions

```
> .\TruffleSnout.exe help
```

forest	Forest discovery workflow
domain	Domain discovery workflow
directory	Directory discovery workflow
util	Utilities
help	Display more information on a specific command.
version	Display version information.

### Forest



> .\TruffleSnout.exe help forest



-n, --name	Required. The name of a forest or `current` Example: -n top.int
-d, --domains	Get forest domains Example: -d
-t, --trusts	Get forest trusts Example: -t
-s, --sites	Get forest sites Example: -s
-g, --gcs	Get Global Catalogs Example -g
-a, --all	Get all forest info. This is a shortcut to -g -s -d -t Example: -a
-U, --username	(Auth) User Name for connection to the service Example: -U username
-P, --password	(Auth) Password fot the user. Provide: `interactive` to ask for a password. OpSec: Clear text passwords on the command line if used without Example: -P <password>    -P interactive
--help	Display this help screen.
--version	Display version information.

## Domain

> .\TruffleSnout.exe help domain



-n, --name	Required. The name of a domain or `current`
-c, --controller	Get domain controllers
-t, --trusts	Get domain trusts
-a, --all	Get all domain info. This is a shortcut to -c -t

Example: `-a`

- `-U, --username` (Auth) User Name **for** connection to the service  
Example: `-U username`
- `-P, --password` (Auth) Password fot the user.  
Provide: ``interactive`` to ask **for** a password.  
OpSec: Clear text passwords on the command line **if** used with  
Example: `-P <password> || -P interactive`
- `--help` Display this help screen.
- `--version` Display version information.

## Directory

`.\TruffleSnout.exe help directory`



- `-l, --ldap` Required. LDAP Connection Path. Can include starting DN  
Example: `LDAP://other.int/DC=other,DC=int`
- `-f, --filter` Required. Query Filter, **in** relation to the starting DN  
Syntax: <https://docs.microsoft.com/en-us/windows/win32/adsis/>  
Example: `'(&(objectClass=user))'`
- `-a, --attr` Limit query to specific attribute(s). Attributes separated by  
``meta`` - shows the attribute keys.  
Example: `-a meta || -a badpwdcount,cn,memberof`
- `-c, --count` Required. Limit of entries returned **in** a query  
Example: `-c 10`
- `-n, --nonsecure` **Do** basic authentication. **Do** not use Kerberos/NTLM. This is a  
Opsec: clear text connectivity.  
Example: `-n`
- `-s, --ssl` Connect as LDAP/S (SSL). This assumes certificates are proper.  
Note: to specify port use the format provided **in** ``-l`` option:  
Example: `-s`
- `-U, --username` (Auth) User Name **for** connection to the service  
Example: `-U username`
- `-P, --password` (Auth) Password fot the user.

Provide: `interactive` to ask **for** a password.  
OpSec: Clear text passwords on the command line **if** used without  
Example: `-P <password> || -P interactive`

`--help` Display this help screen.

`--version` Display version information.

## Utilities

> `.\TruffleSnout.exe help util`



`-t, --ticks2date` Convert time ticks to DateTime.  
Example: `-t 132280170552471892`. Output: `3/7/2020 1:10:55 AM`

`-e, --expires` Check **if** a value of record expires  
Example: `-e 9223372036854775807`. Output: Expires? Yes

`-s, --bytes2SID` Convert Bytes to SID. Used **in** `objectsid` attribute  
Example: `-s 1 5 0 0 0 0 0 5 21 0 0 0 1 94 67 225 228 177 51 0`  
Output: SID: S-1-5-21-3779288577-439595492-2162805249-1104

`-g, --bytes2GUID` Convert Bytes to GUID. Used **in** `objectguid` attribute  
Example: `-g 24 184 226 216 110 108 41 79 149 222 213 140 6 1 0 0`  
Output: GUID: d8e2b818-6c6e-4f29-95de-d58c0674c8ac

`--help` Display this help screen.

`--version` Display version information.