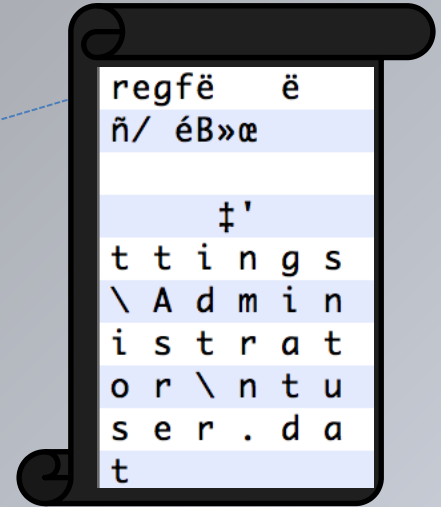
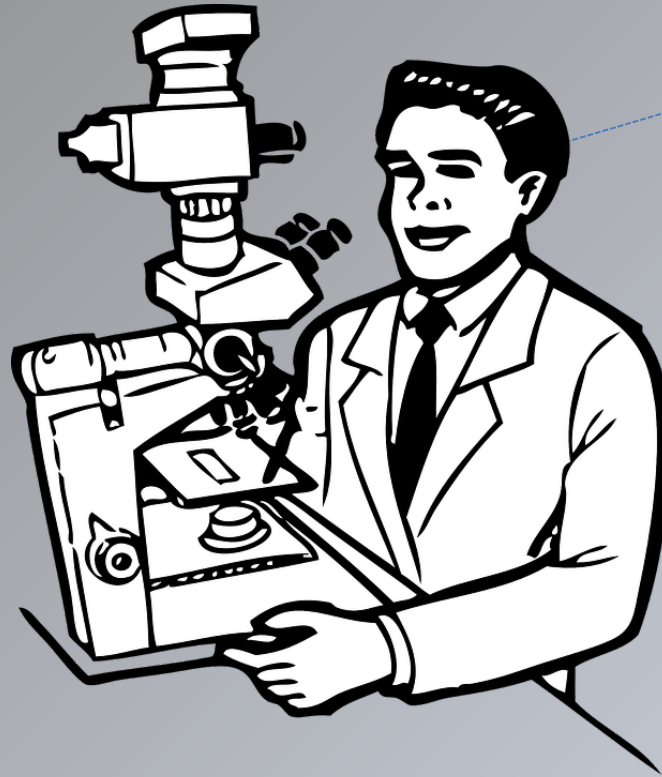


regmagnet

Windows Registry Parser

- Registry File Types
- Registry File Format
- Regmagnet plugins
- Regmagnet output
- Registry Handlers



References

- ▮ Registry File Types and Format: **Maxim Suhanov** @**errno_fail**
 - ▮ <https://github.com/msuhanov/regf>
 - ▮ ...
 - ▮ ...

Regmagnet Plugins

Regmagnet consist of several built-in plugins briefly described below.

Note: To get more details about plugin's purpose and capabilities, pass **-h** to plugin's arguments:

-p "plugin_name -h"

Default plugins:

- **parser** □ Allows to query registry keys and values (**Wildcard / Regex / String / Binary / Owner / Security / Size / Datetime patterns**)
- search
- autoruns
- anomaly
- macro
- cit
- Office
- rdp

Regmagnet output

Regmagnet can send the output to `stdout` or to a `file`.

The output can be represented in one of following formats:

- Comma separated: `-f csv`
- Tab separated: `-f tab`
- Windows Registry Editor: `-f winreg`
- SQLite: `-f sqlite`

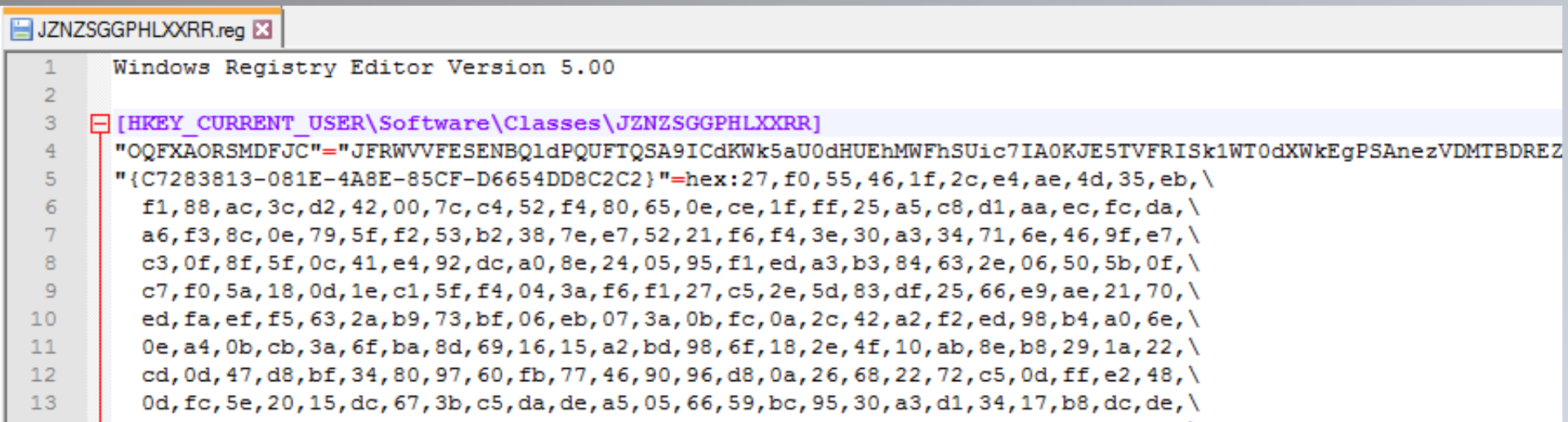
To option: `-o file_path` sends to output to given file path

Few output format examples:

```
-s "UsrClass-admin-live.dat" -f tab -p "parser -qk JZNZSGGPHLXXRR"
```

parser	HKEY_CURRENT_USER\Software\Classes	2015-10-20	04:49:51.206532	0	3	JZNZSGGPHLXXRR	OQFXAORSMDFJC	JFRWVFESENBQldPQUFTQSA9ICdKwK5aU0dHUEhMWFhSUiC7IA0KJESTVFRISk1WT0dXWkEgPSAnezVDMTBDREZ
parser	HKEY_CURRENT_USER\Software\Classes	2015-10-20	04:49:51.206532	0	3	JZNZSGGPHLXXRR	{C7283813-081E-4A8E-85CF-D6654DD8C2C2}	b'\'\xf0UF\x1f,\xe4\xaeM5\xeb\xcf1
parser	HKEY_CURRENT_USER\Software\Classes	2015-10-20	04:49:51.206532	0	3	JZNZSGGPHLXXRR	{5C10CDFD-6C47-4A83-B146-67012C633039}	b'\'\xf0UF\x1f,\xe4\xaeM5\xeb\xcf1

```
-s "UsrClass-admin-live.dat" -f winreg -p "parser -qk JZNZSGGPHLXXRR" -o JZNZSGGPHLXXRR.reg
```



```
JZNZSGGPHLXXRR.reg

1  Windows Registry Editor Version 5.00
2
3  [HKEY_CURRENT_USER\Software\Classes\JZNZSGGPHLXXRR]
4  "OQFXAORSMDFJC"="JFRWVFESENBQldPQUFTQSA9ICdKwK5aU0dHUEhMWFhSUiC7IA0KJESTVFRISk1WT0dXWkEgPSAnezVDMTBDREZ
5  "{C7283813-081E-4A8E-85CF-D6654DD8C2C2}"=hex:27,f0,55,46,1f,2c,e4,ae,4d,35,eb,\
6  f1,88,ac,3c,d2,42,00,7c,c4,52,f4,80,65,0e,ce,1f,ff,25,a5,c8,d1,aa,ec,fc,da,\
7  a6,f3,8c,0e,79,5f,f2,53,b2,38,7e,e7,52,21,f6,f4,3e,30,a3,34,71,6e,46,9f,e7,\
8  c3,0f,8f,5f,0c,41,e4,92,dc,a0,8e,24,05,95,f1,ed,a3,b3,84,63,2e,06,50,5b,0f,\
9  c7,f0,5a,18,0d,1e,c1,5f,f4,04,3a,f6,f1,27,c5,2e,5d,83,df,25,66,e9,ae,21,70,\
10 ed,fa,ef,f5,63,2a,b9,73,bf,06,eb,07,3a,0b,fc,0a,2c,42,a2,f2,ed,98,b4,a0,6e,\
11 0e,a4,0b,cb,3a,6f,ba,8d,69,16,15,a2,bd,98,6f,18,2e,4f,10,ab,8e,b8,29,1a,22,\
12 cd,0d,47,d8,bf,34,80,97,60,fb,77,46,90,96,d8,0a,26,68,22,72,c5,0d,ff,e2,48,\
13 0d,fc,5e,20,15,dc,67,3b,c5,da,de,a5,05,66,59,bc,95,30,a3,d1,34,17,b8,dc,de,\
```

Output fields (aka. Format Fields)

You have full control over the fields being displayed or exported. This setting can be configured through `-ff` parameter or in plugin's configuration file via `default_format_fields` entry.

```
-s "UsrClass-admin-live.dat" -f csv -ff "value_path,value_type_str" -p "parser -qk JZNZSGGPHLXXRR".
```

```
JZNZSGGPHLXXRR\0QFXA0RSMDJFC,RegSZ  
JZNZSGGPHLXXRR\{C7283813-081E-4A8E-85CF-D6654DD8C2C2},RegBin  
JZNZSGGPHLXXRR\{5C10CDFD-6C47-4A83-B146-67012C633039},RegBin
```

parser.py.conf

×

```
{  
  "plugin_name": "parser",  
  "author": "wit0k",  
  "version": "0.1",  
  "url": "https://github.com/wit0k",  
  "default_format_fields": ["plugin_name", "hive_mapping", "key_timestamp", "key_subkey_count", "key_value_count",  
                           "hive_user", "key_path", "value_name", "value_content"]  
}
```

Registry Handlers

A registry handler is like CyberChef's recipe which interacts with the data exposed via registry fields and perform predefined encoding/decoding/converting or decrypting operations.

To display all available registry handlers, run following command: -

`cyberchef --help --arg=registry`

Registry Handlers:

```
[+] dump_to_file - dump_to_file() -> Saves the input data buffer to a file specified by a parameter
[+] decompress_gzip - decompress_gzip() -> Attempts to un-gzip the input data
[+] decrypt_rc4 - decrypt_rc4(Key) -> Decrypts the input data with a string key specified
[+] sxor - sxor(Key) -> XOR the input data with a string key specified
[+] str - str() -> Converts the input data to String
[+] unescape_url - unescape_url -> Unescapes the input data string/url
[+] cit_dump - cit_dump() -> Dumps the unicode string and converts it to human readable format (Used for strings originating from cit plugin)
[+] utf8_dump - utf8_dump() -> Dumps the unicode string and converts it to human readable format
[+] rslice - slice(start) -> Slice the input data [Range: start:]
[+] slice - slice(0, stop) -> Slice the input data [Range: 0:stop]
[+] b64_dump - Dump and decode base64 strings from the input data
[+] b64_decode - Decode the input data as base64 string
[+] b64_encode - Encode the input data to base64 string
[+] decode_vbe - Attempts to VBE decrypt the input data
[+] nothing - Do nothing, reserved for plugin developers...(Mainly used when only custom handler is required)
[+] entropy - entropy() -> Calculates the entropy of the input data
```


Registry Handler Format

To specify a registry handler you may use any of following commands.

- ▮ Each handler shall be comma separated (without any space)
- ▮ Multiple parameters or fields have to be semicolon separated (without any space)

-rh handler_name

-rh handler_name,another_or_same_handler_name

-rh handler_name<param>parameter1

-rh handler_name<param>parameter1;parameter2

-rh handler_name<field>field_name

-rh handler_name<field>field_name;field_name

-rh handler_name<field>field_name<param>parameter

-rh handler_name<field>field_name<rfield>field_name

-rh handler_name<field>field_name<param>parameter<rfield>field_name

Following query uses few registry handlers in the following way:

- ▮ Get the value content of `HKEY_CURRENT_USER\Software\Classes\JZNZSGGPHLXXRR\OQFXAORSMDFJC`
- ▮ Decode the value content from base64 and store it in the value content
- ▮ Dump/Save decoded value content to a file named OQFXAORSMDFJC.ps1

```
"HKEY_CURRENT_USER\Software\Classes\JZNZSGGPHLXXRR\OQFXAORSMDFJC"
parser,HKEY_CURRENT_USER\Software\Classes,2015-10-20 04:49:51.206532,0,3,,JZNZSGGPHLXXRR,OQFXAORSMDFJC,JFRwVVFESENBQldPQUFTQSA9ICdKwk5aU0dHUEhMWf
```

```
-s "UsrClass-admin-live.dat" -rh "b64_decode,dump to file<param>OQFXAORSMDFJC.ps1" -p "parser -
parser,HKEY_CURRENT_USER\Software\Classes,2015-10-20 04:49:51.206532,0,3,,JZNZSGGPHLXXRR,OQFXAORSMDFJC,$TVUQDHCABW0AASA = 'JZNZSGGPHLXXRR'; ;$NSTTHJMV0GWZA = '{5C10CDFD
```

```
0-OQFXAORSMDFJC.ps1 x
1 $TVUQDHCABW0AASA = 'JZNZSGGPHLXXRR';
2 $NSTTHJMV0GWZA = '{5C10CDFD-6C47-4A83-B146-67012C633039}';
3 $YFMBMEFIULQEHONISFTG = '{C7283813-081E-4A8E-85CF-D6654DD8C2C2}';
4 Function at0jmDsbDtKiL{
5     Param([Parameter( Position = 0, Mandatory = $true )][Byte[]]$QEHFIVPHHMEN,[Parameter(Position = 1, Mandatory = $true)][Byte[]]$ZXYTXUDDZLQXAS)
6     [Byte[]]$k = New-Object Byte[] 256;
7     [Byte[]]$s = New-Object Byte[] 256;
8     for ($i = 0; $i -lt 256; $i++){
9         $s[$i] = [Byte]$i;
10        $k[$i] = $ZXYTXUDDZLQXAS[$i % $ZXYTXUDDZLQXAS.Length];
11    }
12 }
```