nmantani-Plugin訓練座学

訓練概要

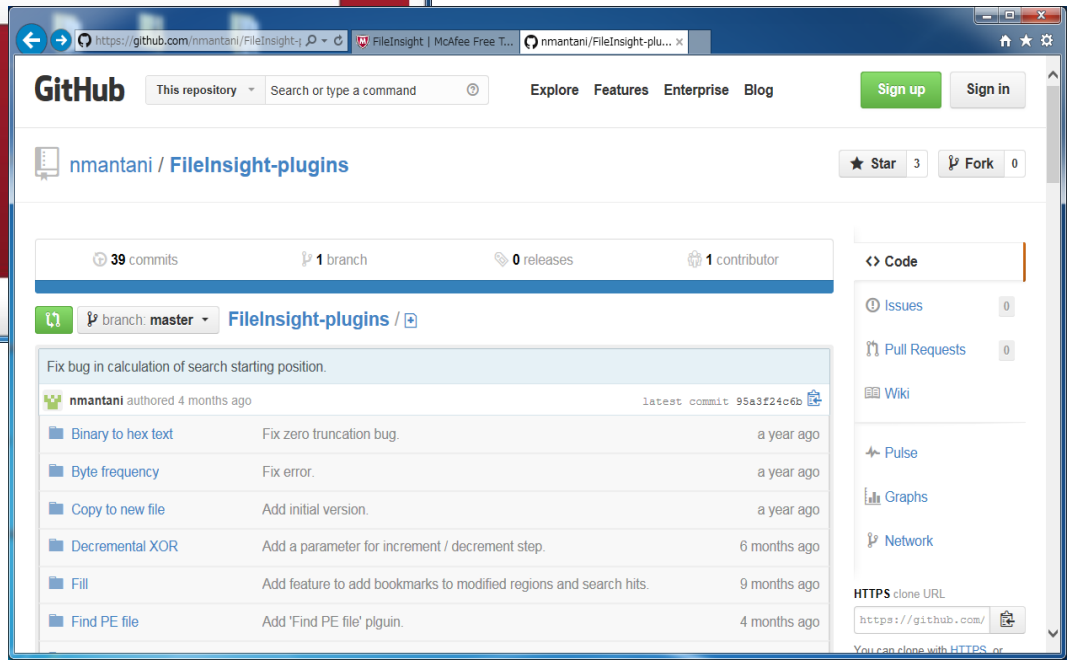
- **訓練目的**
  - 表層解析の技術を用いて、難読化された検体ファイルから目的のオブジェクト（実行可能ファイル，偽装ドキュメント等）を抽出できる様にする。
- **受講対象**
  - マルウェアの解析作業（主に動的解析）を行う者
  - マルウェア解析のサポート・支援作業を行う者
- **受講可能レベル**
  - マジックナンバー（フォーマット識別子）の意味を理解しており、その知識を活用して一般的なファイル種別（MS-Office，PDF，実行ファイル等）を判別できるレベルの者
  - または、相当する知識を有する者（「表層解析訓練」受講者含む）
- **事前知識**
  - １６進数の読み方
  - （ビット）論理演算（AND／OR／NOT／XOR／シフト／ローテート)

FileInsight/nmantaniの紹介

http://www.mcafee.com/au/downloads/free-tools/fileinsight.aspx

[McAfee FileInsight]

McAfee社が提供する無償のファイル操作ツール。マルウェア解析に有用な機能を備えている。



[nmantani/FileInsight-Plugins]

Nobutaka Mantani氏が作成したFileInsightの機能を更に強化するプラグイン集

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

FileInsight/nmantaniによる オブジェクト抽出の可能性

- **ドキュメント型マルウェアの一般的構造**
  - 実行ファイルをドロップするマルウェアの場合、何処かにその素がある
  - 通常マルウェア作成者はシェルコードを極力小さく作りたがる
  - 小さくするため、複雑な復号ロジック等の余計なコードは書きたくない

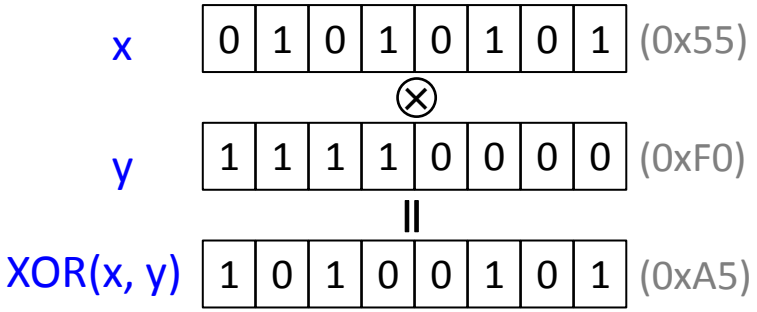
MS-Officeの場合

この様なタイプのマルウェアの場合、難読化と言っても高度な暗号やパックされることは少ないためビット演算、ビット操作、シフト演算等を駆使して解くことが出来る可能性がある

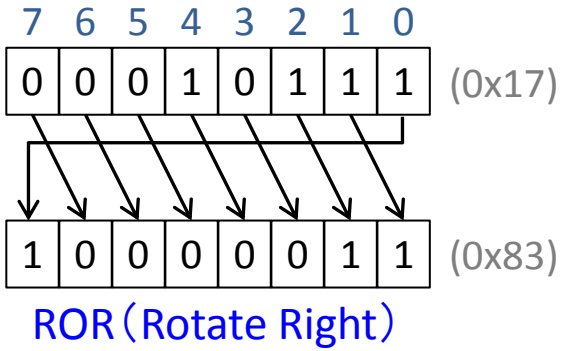
難読化解除の基礎知識

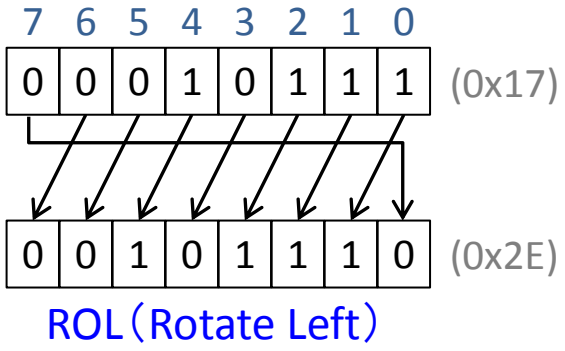
- **ビット演算**
  - XOR（Exclusive OR：排他的論理和）が多用される（これだけは覚える）

x	y	AND(x, y)	OR(x, y)	XOR(x, y)
0	0	0	0	0
0	1	0	1	1
1	0	0	1	1
1	1	1	1	0



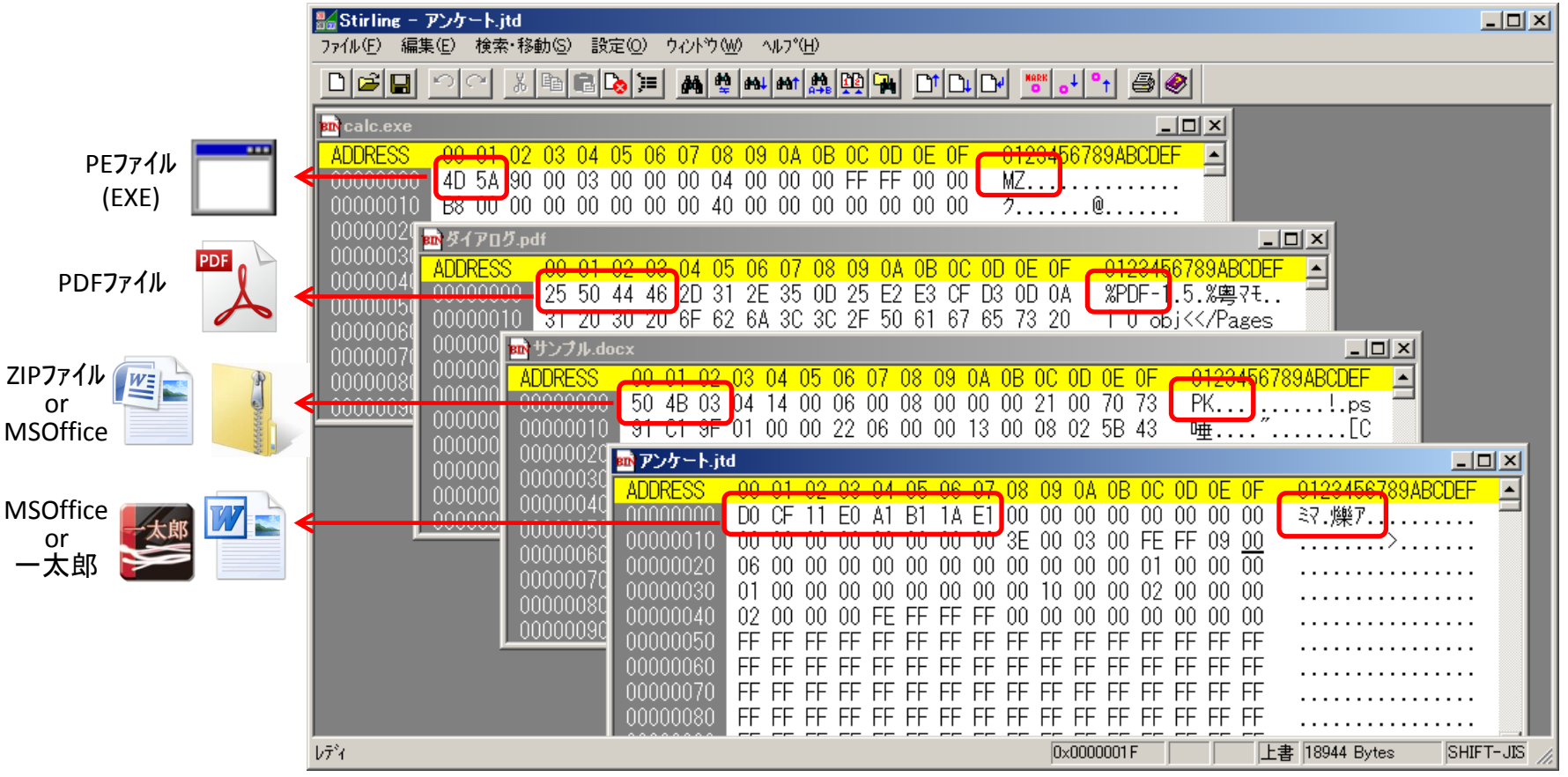
- **シフト演算**
  - ROR（Rotate Right）とROL（Rotate Left）が多用される（これだけは覚える）



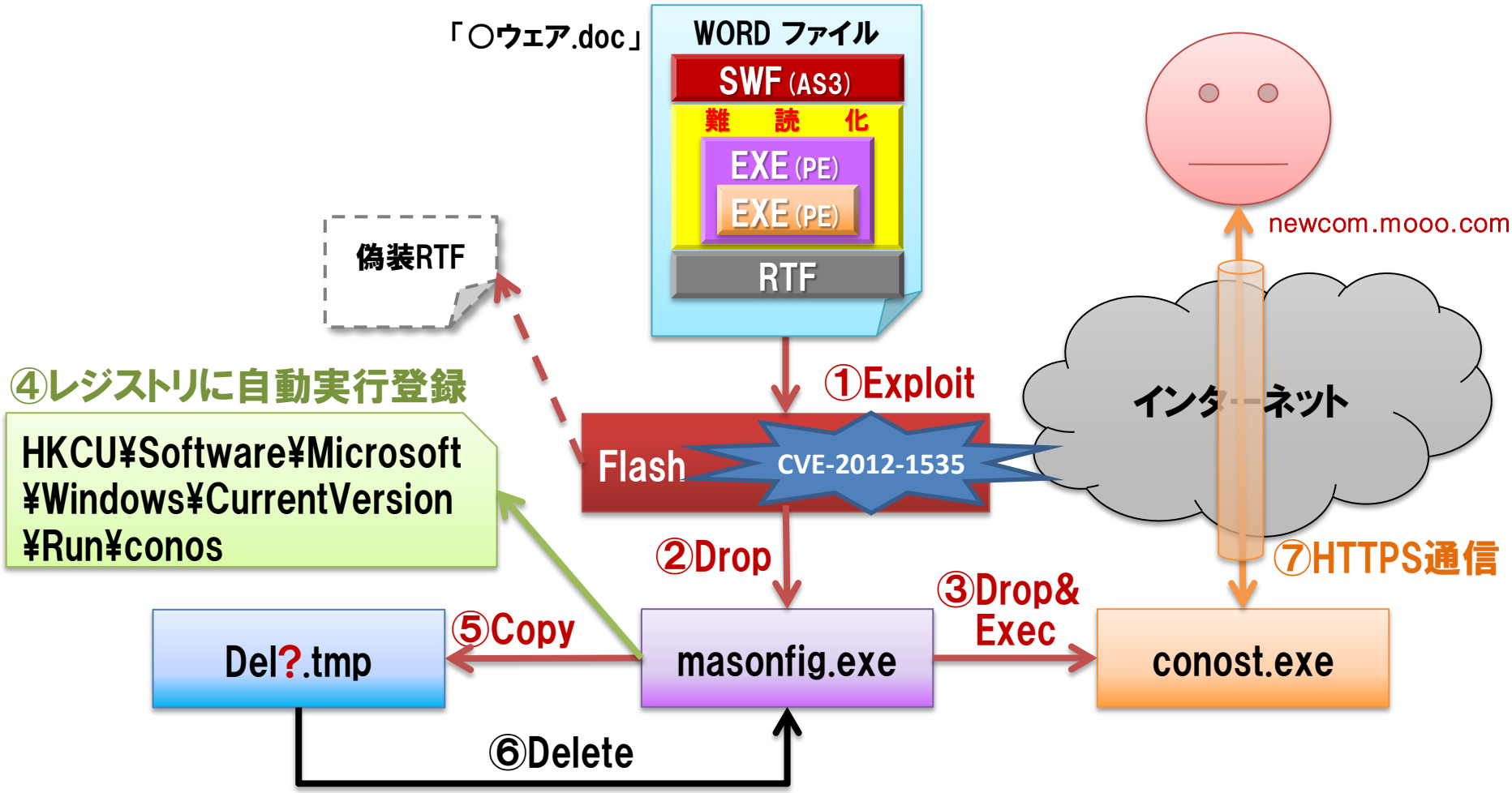


オブジェクト抽出の基礎知識

- **マジックナンバー（ファイル識別子）**
  - 大抵ファイルの先頭数バイトを確認することでファイル種別が分かる



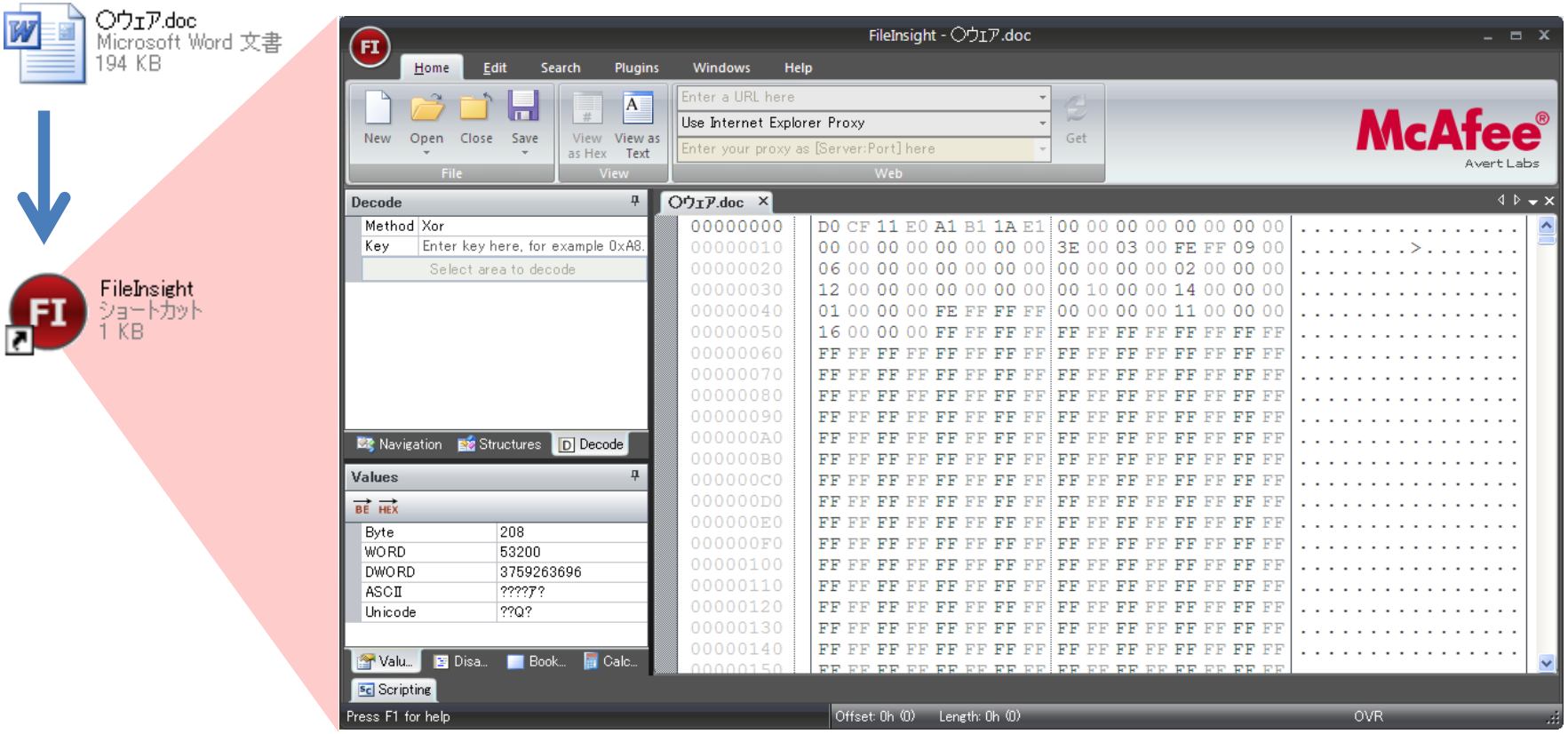
オブジェクト抽出を試みる検体



MD5	[conost.exe] 3efa2b76c4929ae62fbcb454c50f8f95 [masonfig.exe] a75412693f6ebf505f9127df6308f1d8 [Del?.tmp] a75412693f6ebf505f9127df6308f1d8

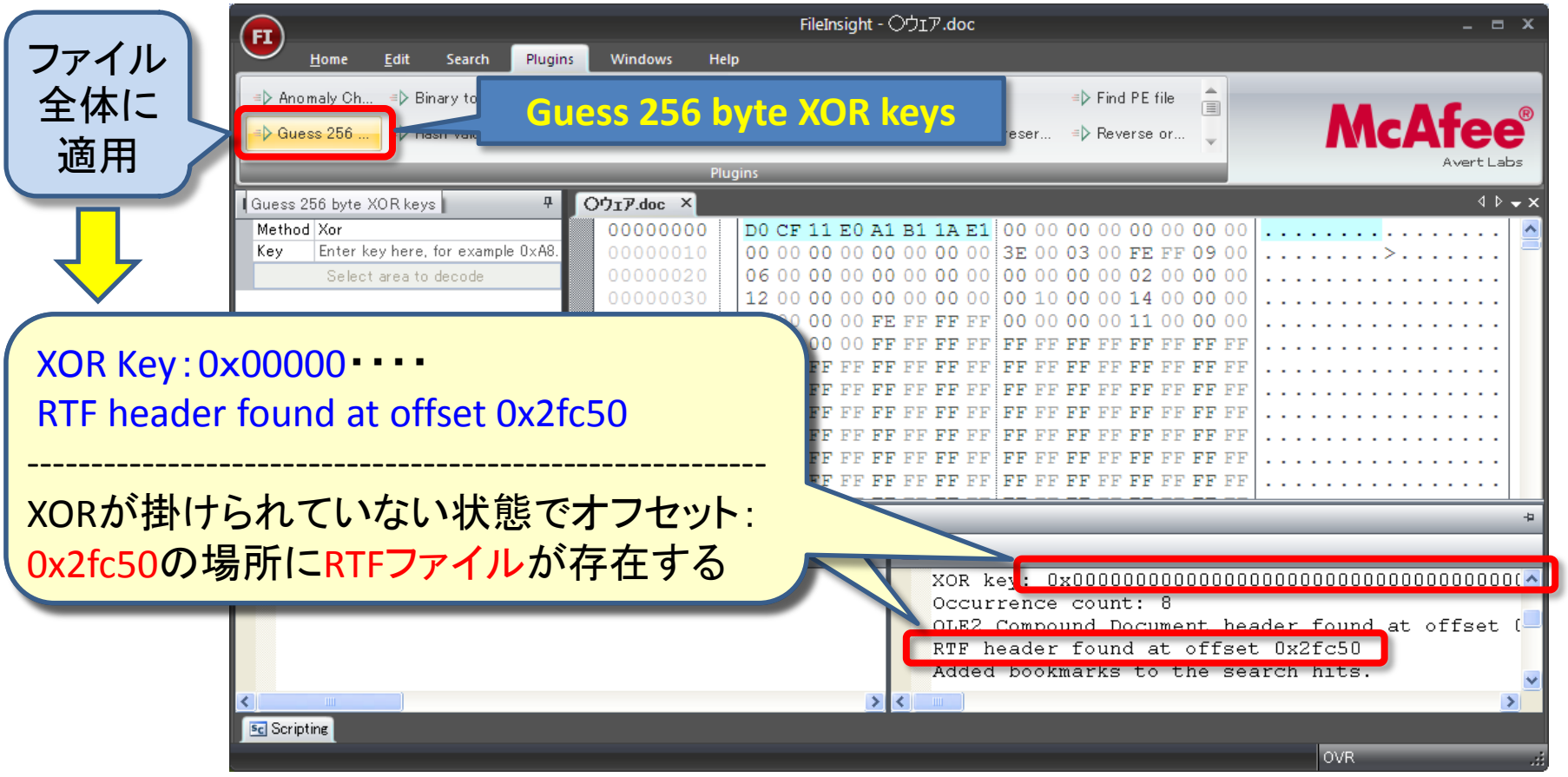
オブジェクト抽出

- **抽出作業の開始**
  - FileInsightアイコンへマルウェア検体をドラッグ＆ドロップ」



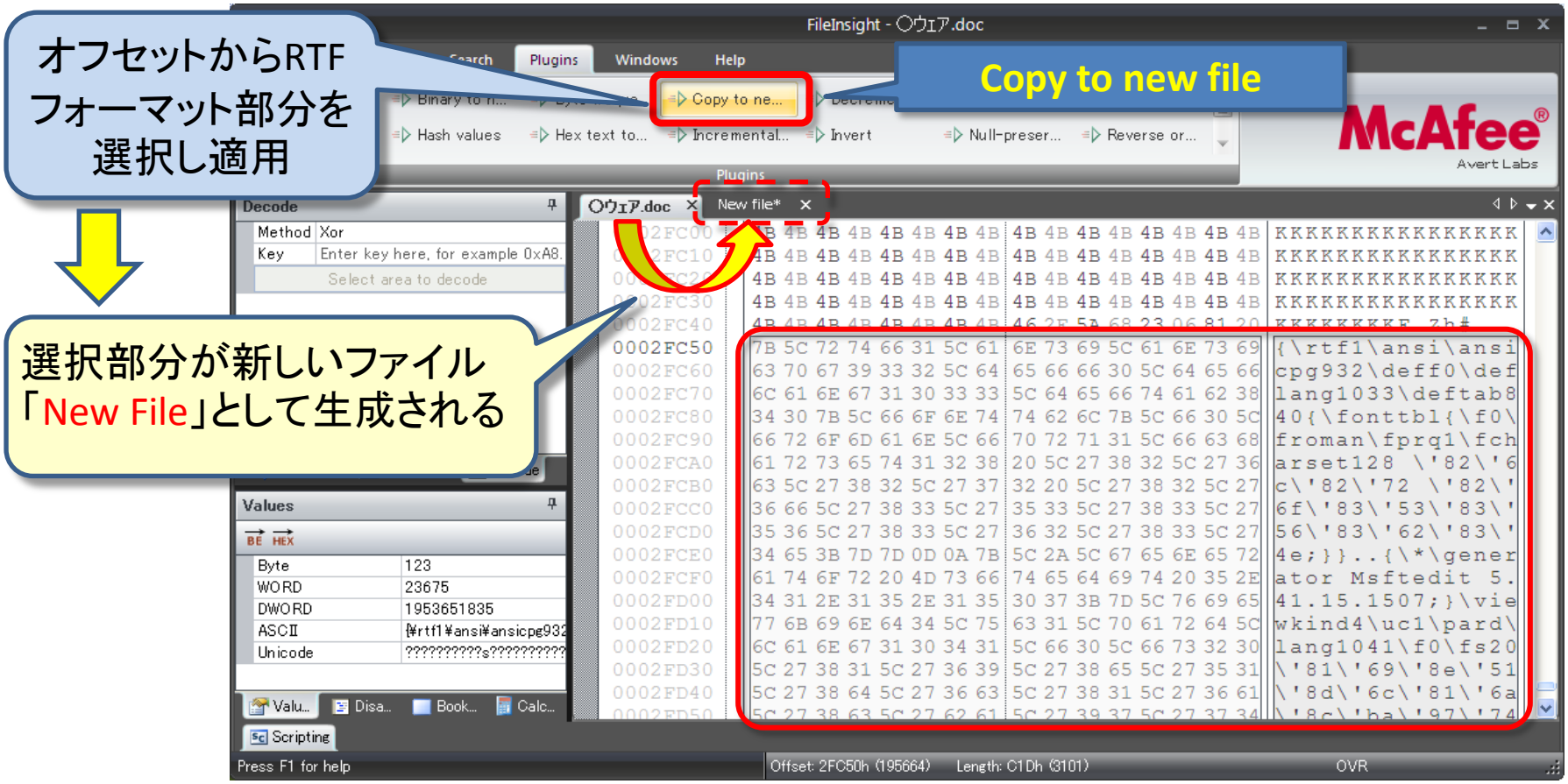
オブジェクト抽出

- **隠れたオブジェクトの検索（解除Key検索）**
  - 「Guess 256 byte XOR keys」を用いて隠れたオブジェクトが無いか検索



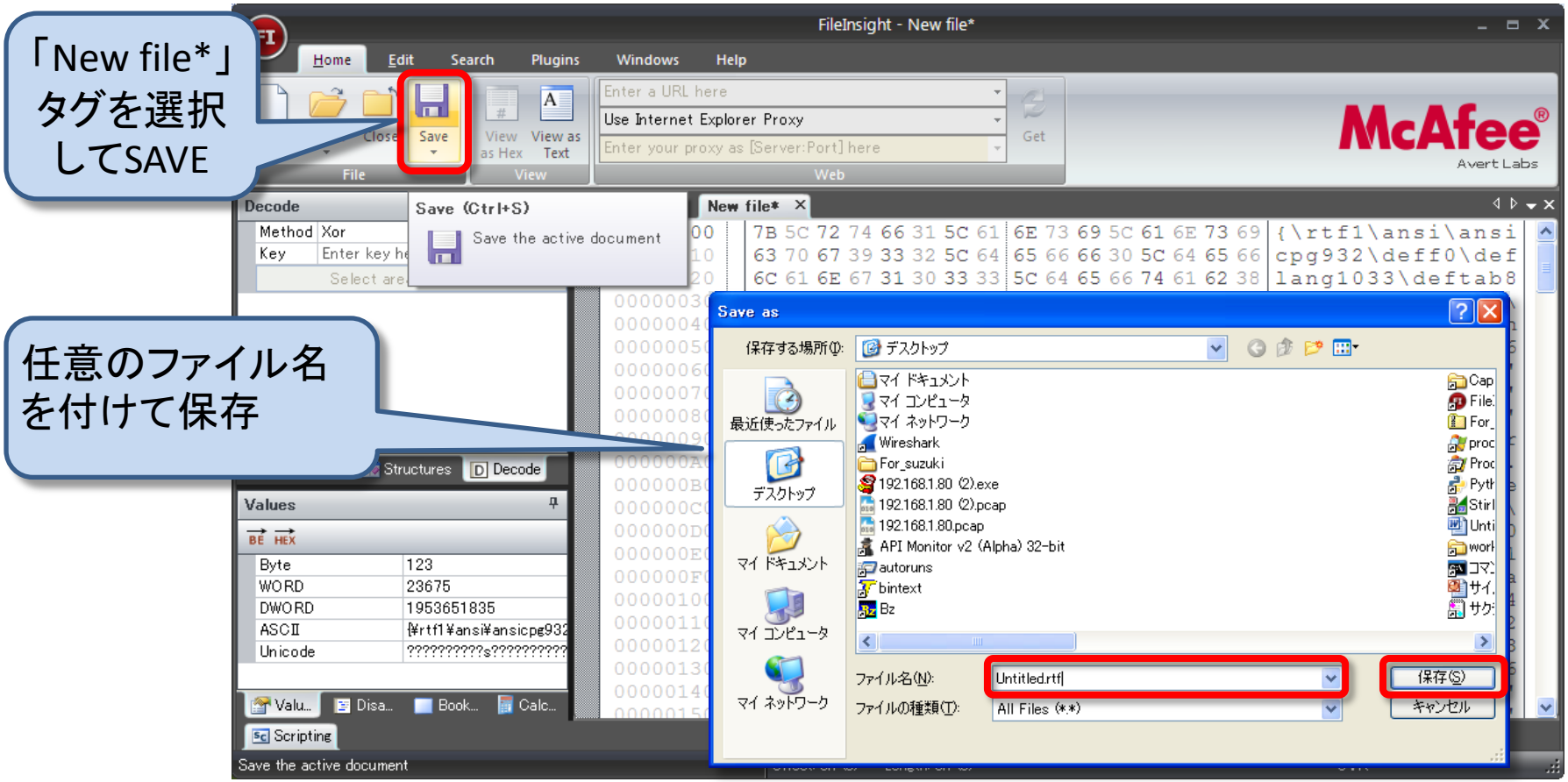
オブジェクト抽出

- **偽装RTFファイルを抽出してコピー＆保存**
  - 「Copy to new file」を用いて偽装RTF部分をコピー



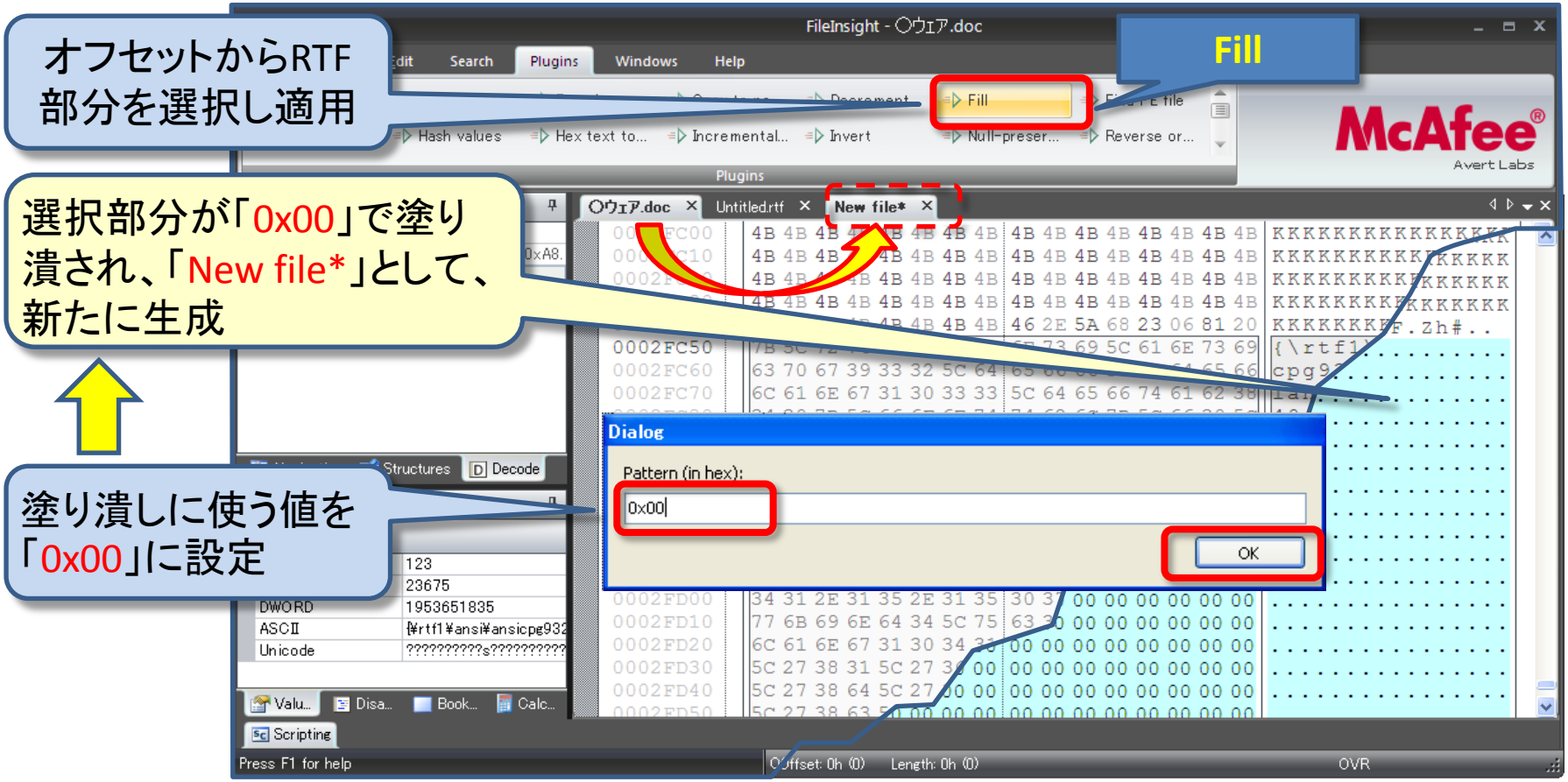
オブジェクト抽出

- **偽装RTFファイルを抽出してコピー＆保存**
  - 「Home」メニュー「Save」を選択し、偽装ファイルを保存



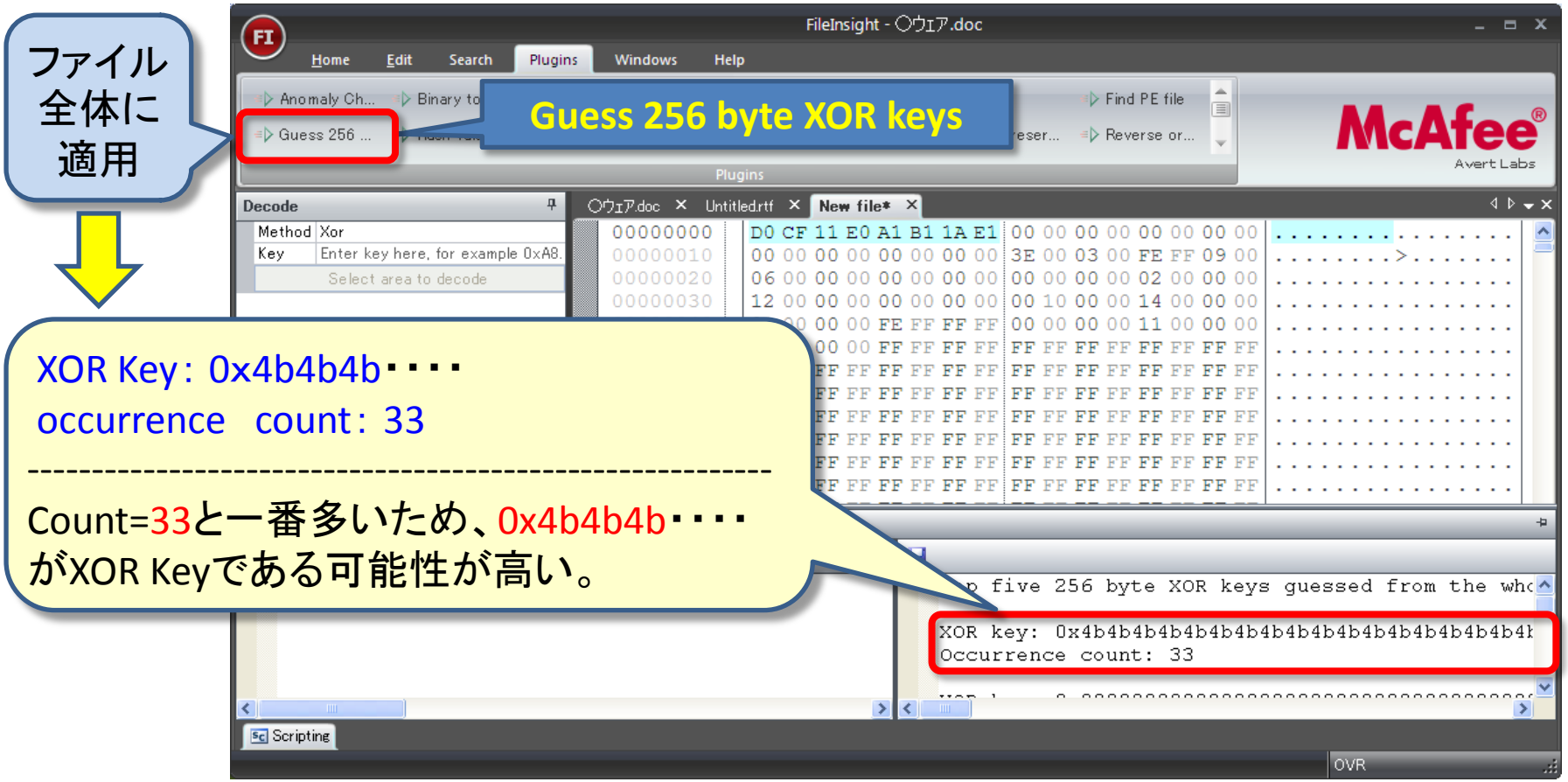
オブジェクト抽出

- **偽装RTF抽出後の後処理**
  - 解析進める上で邪魔となるため、抽出したRTF部分をNULLで塗り潰す。



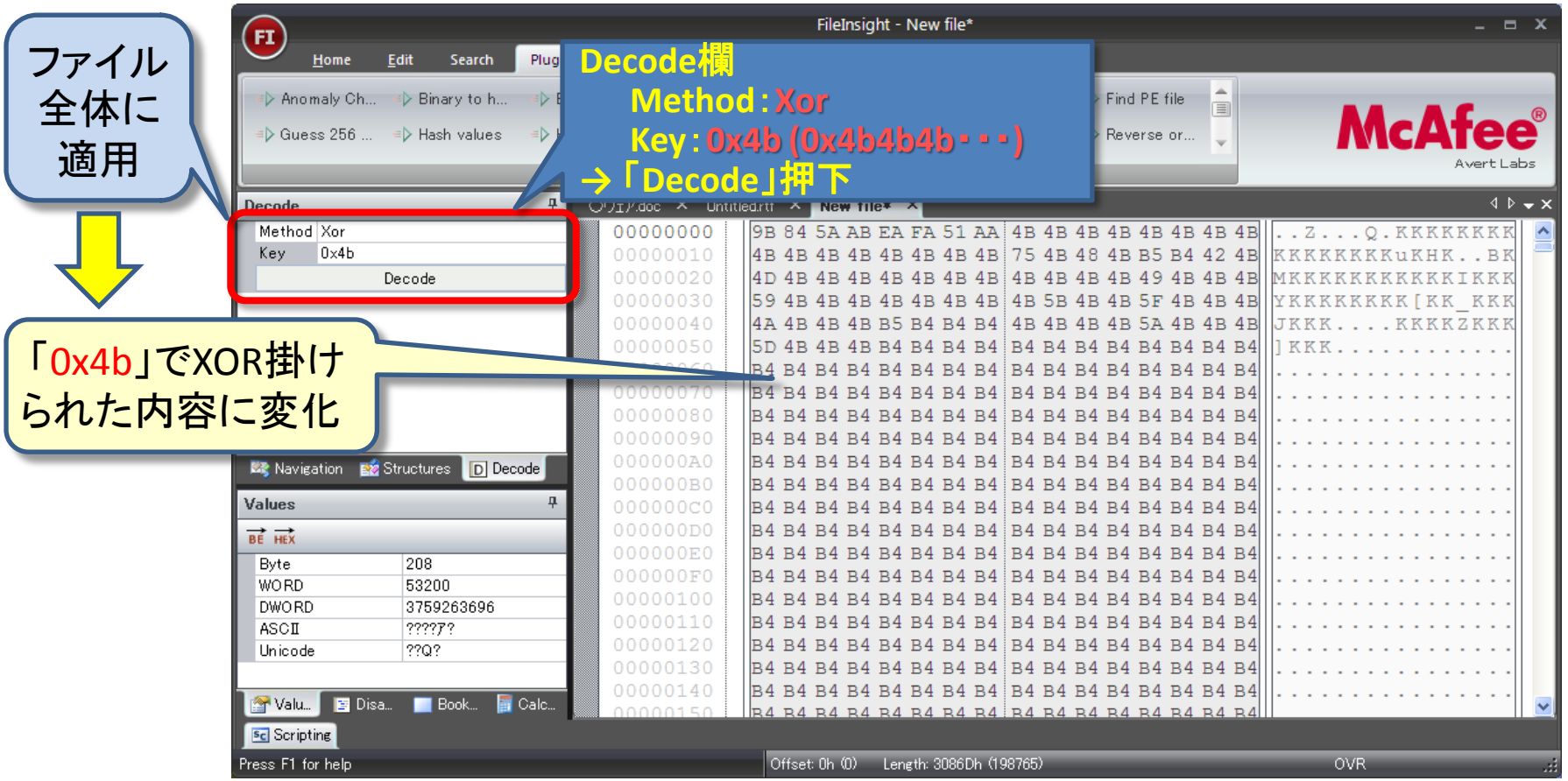
オブジェクト抽出

- **再度隠れたオブジェクトを検索（解除Key検索）**
  - 「Guess 256 byte XOR keys」を用い、改めて隠れオブジェクトを検索



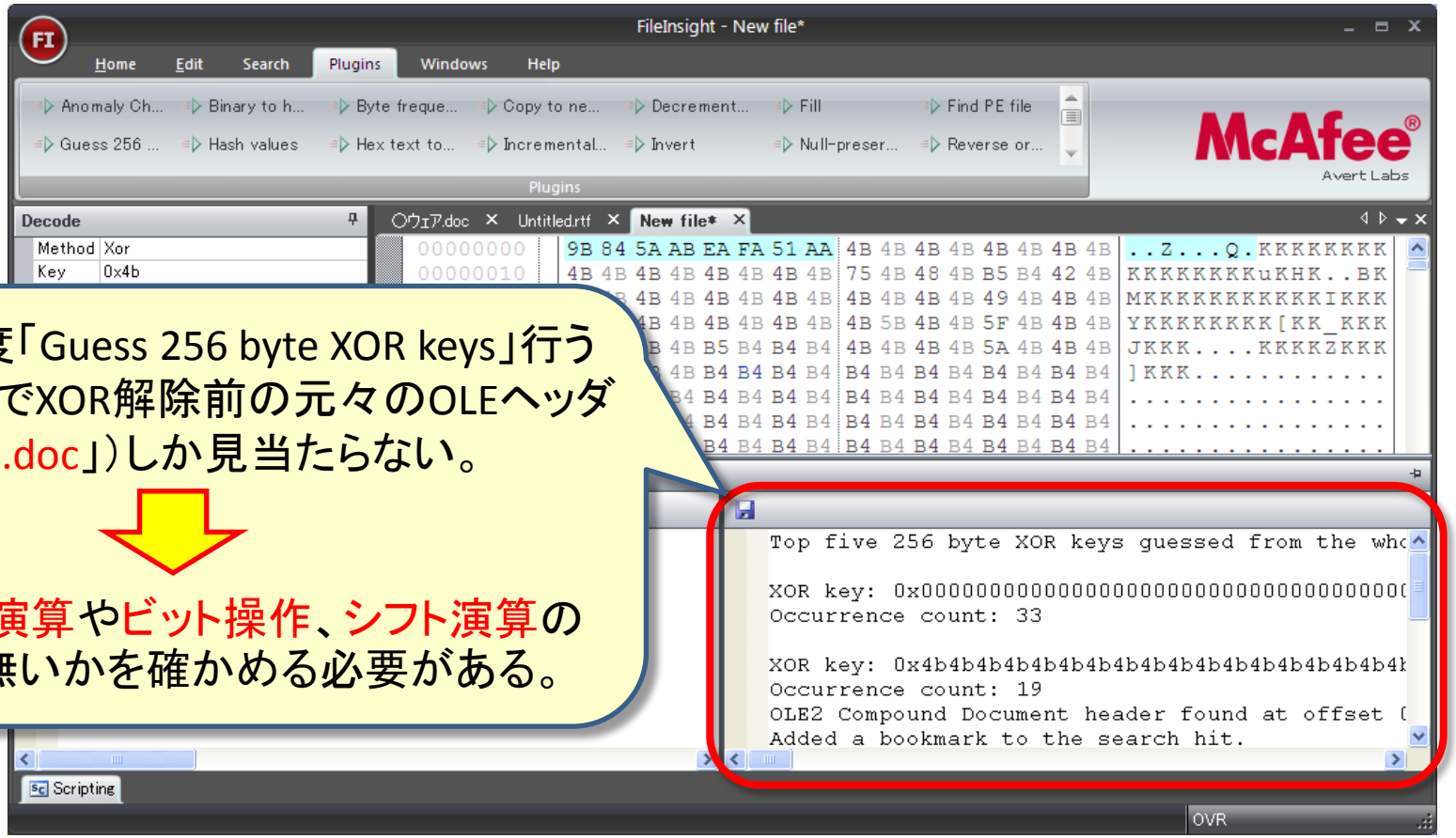
オブジェクト抽出

- **難読化解除の開始**
  - 推測したXOR Keyを手掛かりに難読化を紐解いていく



オブジェクト抽出

- **難読化解除方針の再考**
  - XOR Keyのみでは解除できないため、次の手段を検討する

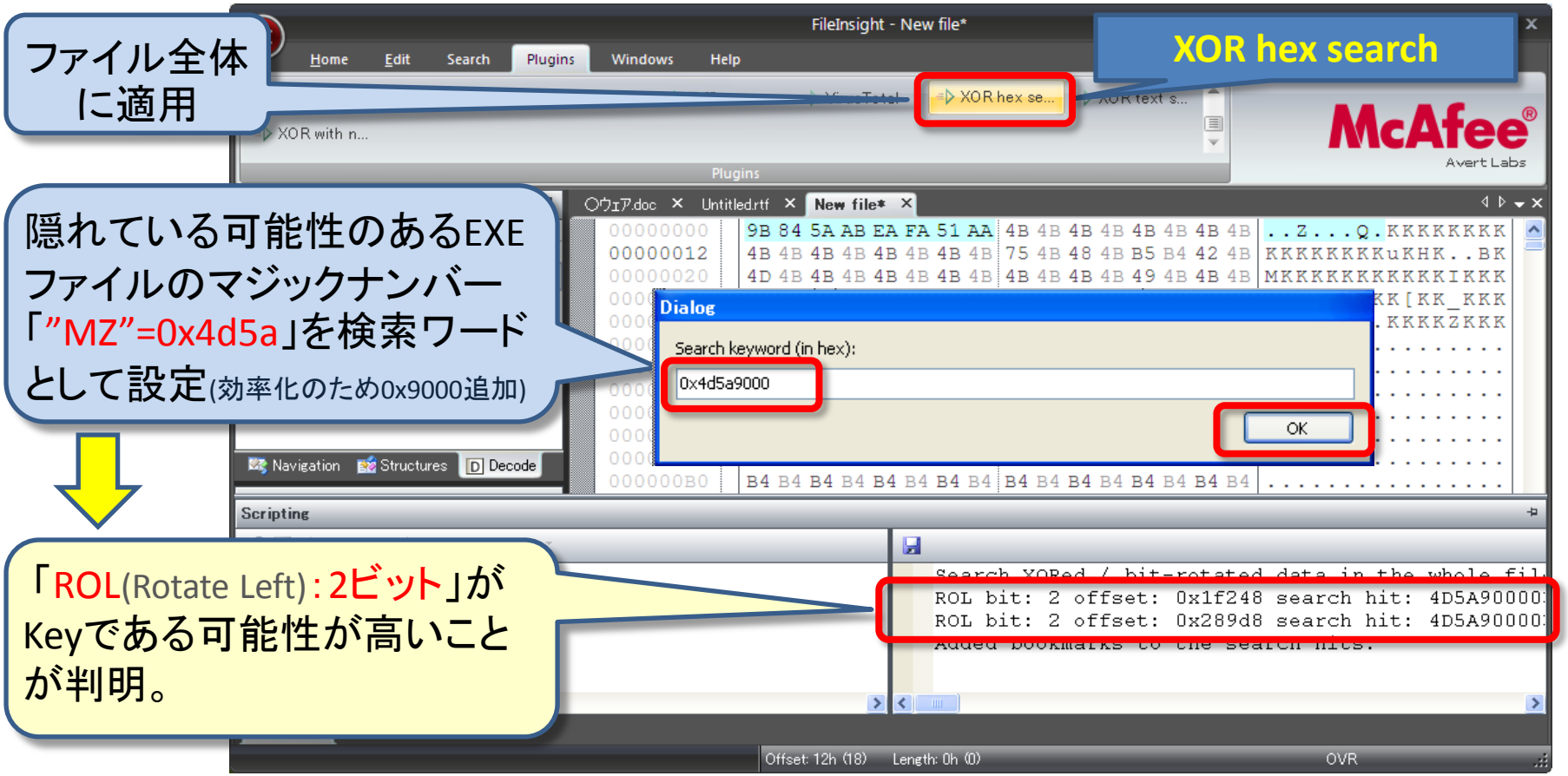


試しに再度「Guess 256 byte XOR keys」行うも、「0x4b」でXOR解除前の元々のOLEヘッダ（「〇ウェア.doc」）しか見当たらない。

他のビット演算やビット操作、シフト演算の可能性が無いかを確かめる必要がある。

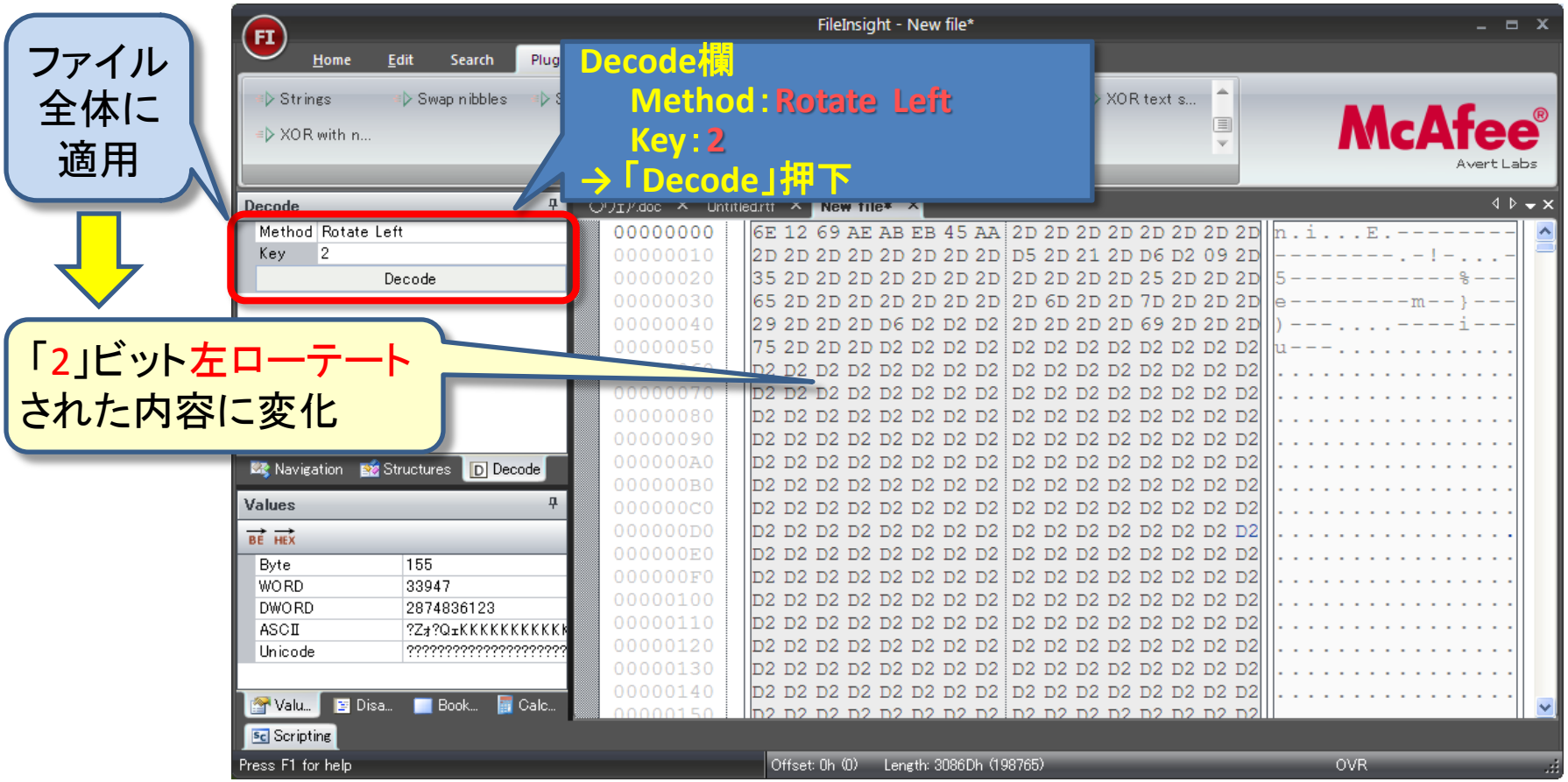
オブジェクト抽出

- **再度解除Keyを検索**
  - 他のビット操作やシフト演算がKeyとなる可能性の有無を調べる



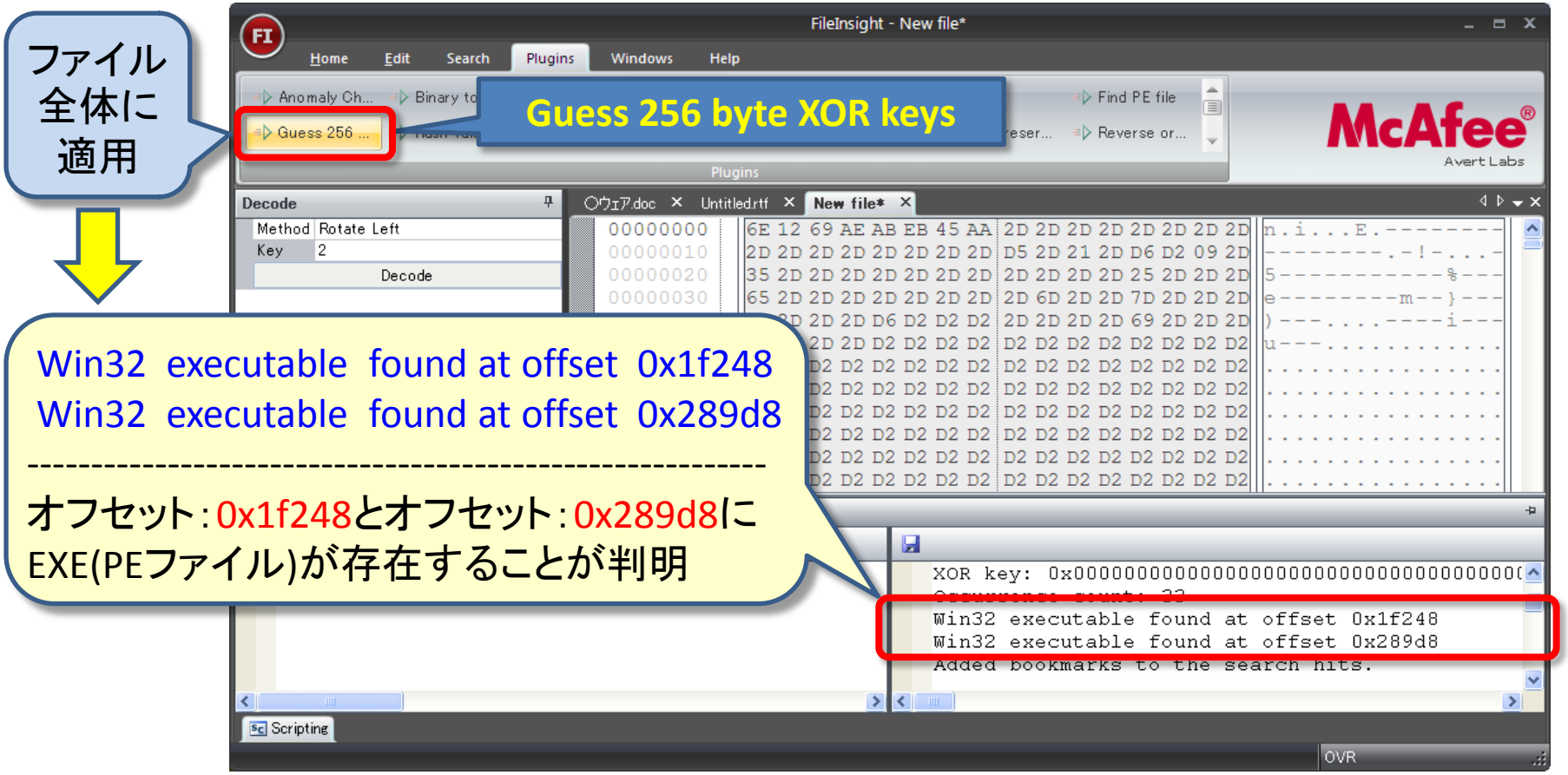
オブジェクト抽出

- **難読化解除の再開**
  - 推測したROL Keyを用いて難読化を解除



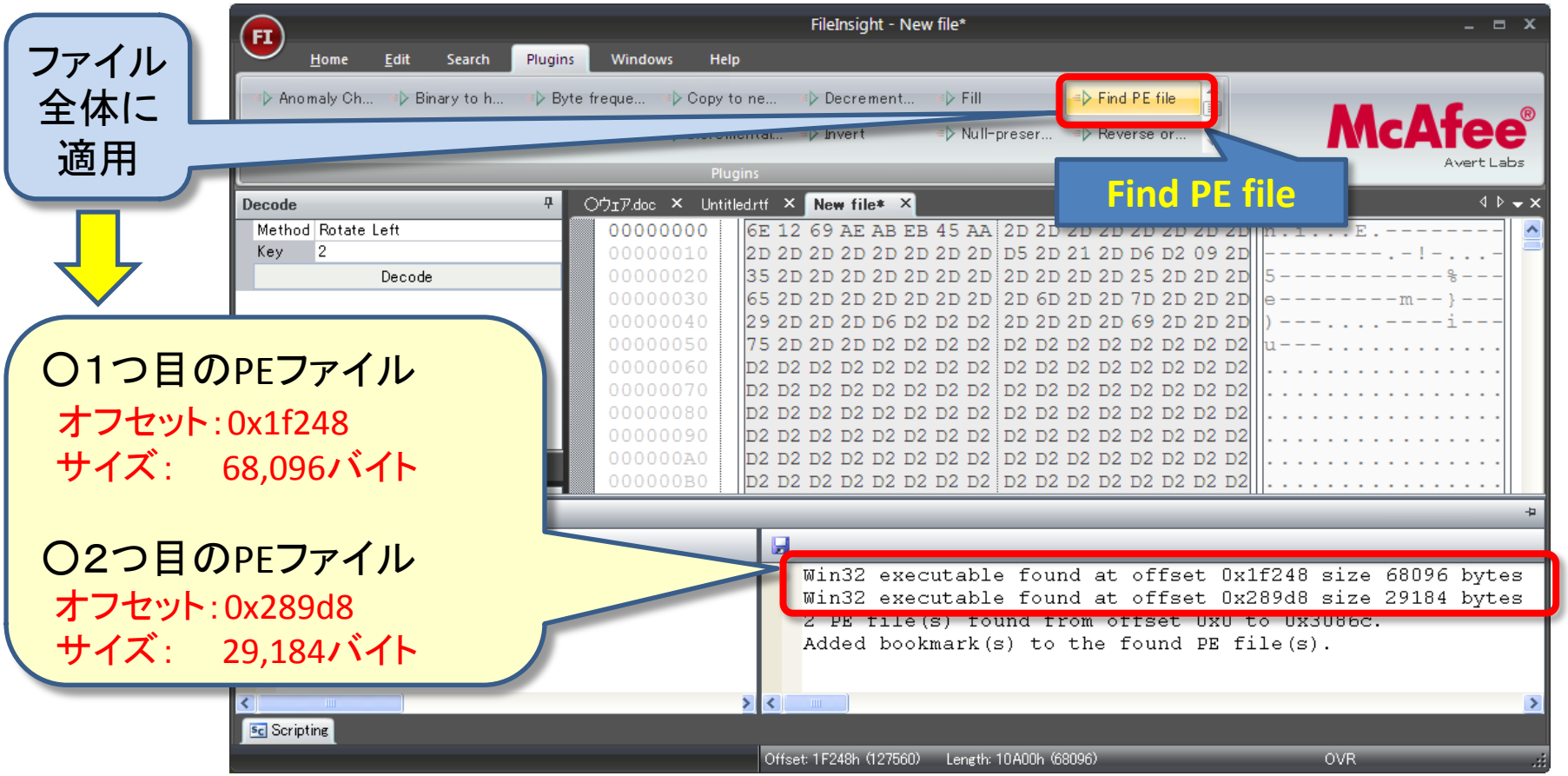
オブジェクト抽出

- **再度オブジェクトを検索**
  - 「Guess 256 byte XOR keys」を用い、改めて隠れオブジェクトを検索



オブジェクト抽出

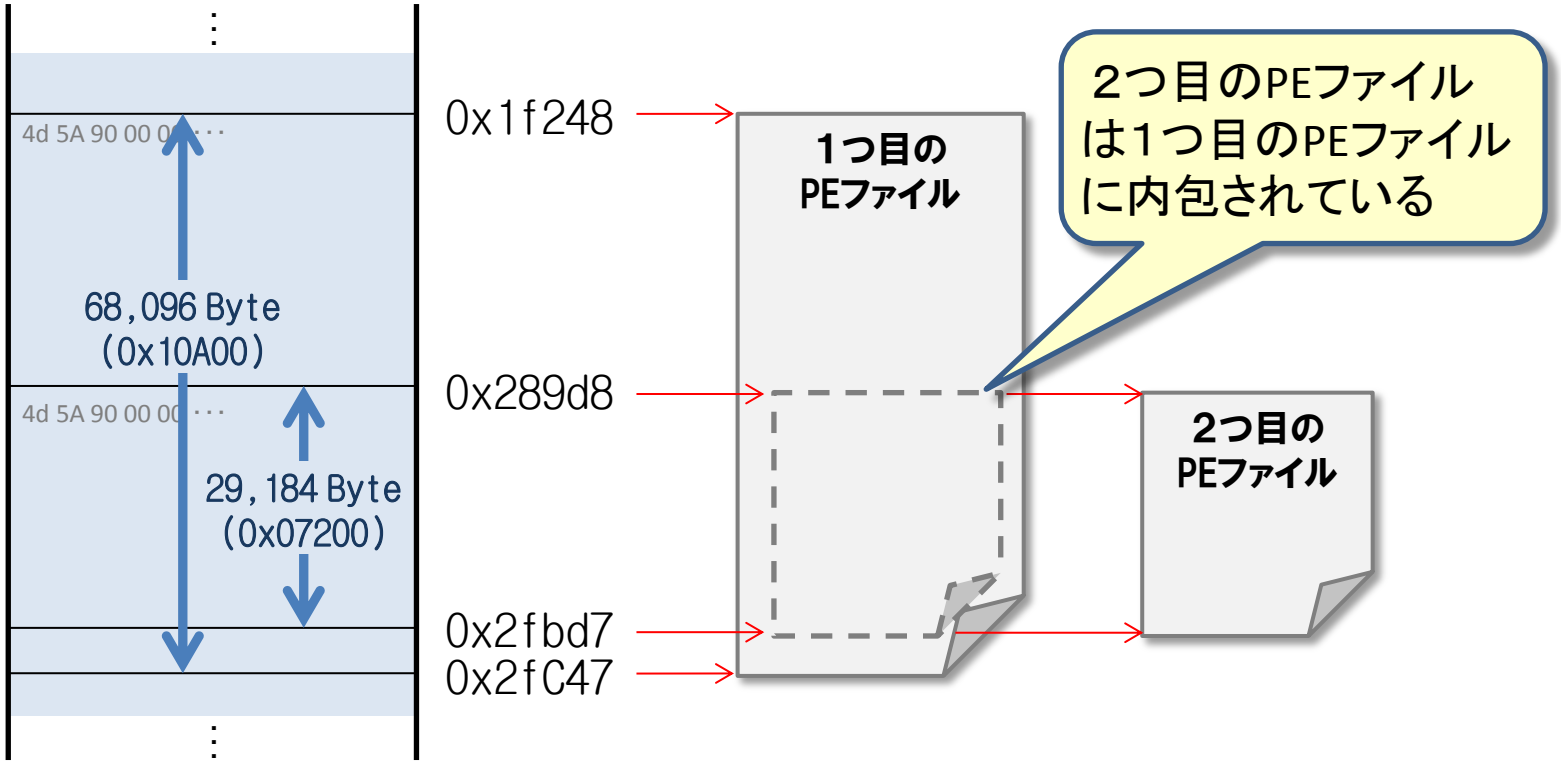
- **再度オブジェクトを検索**
  - 「Find PE file」を用いてサイズを含めて再度確認



オブジェクト抽出

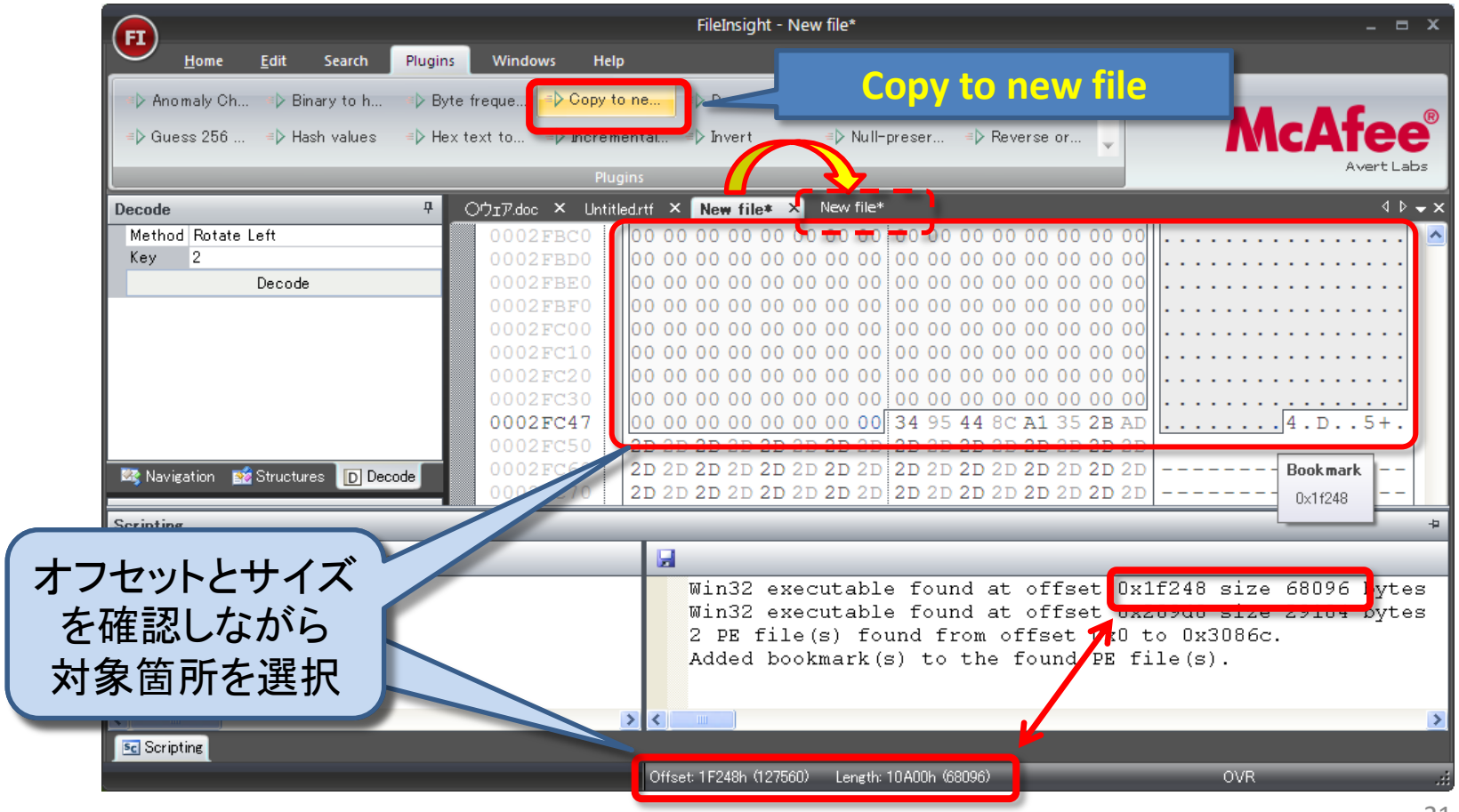
- **発見したPEファイル間の相関**
  - 各オフセット値とサイズからPEファイル間の関係を確認

```
Win32 executable found at offset 0x1f248 size 68096 bytes
Win32 executable found at offset 0x289d8 size 29184 bytes
```



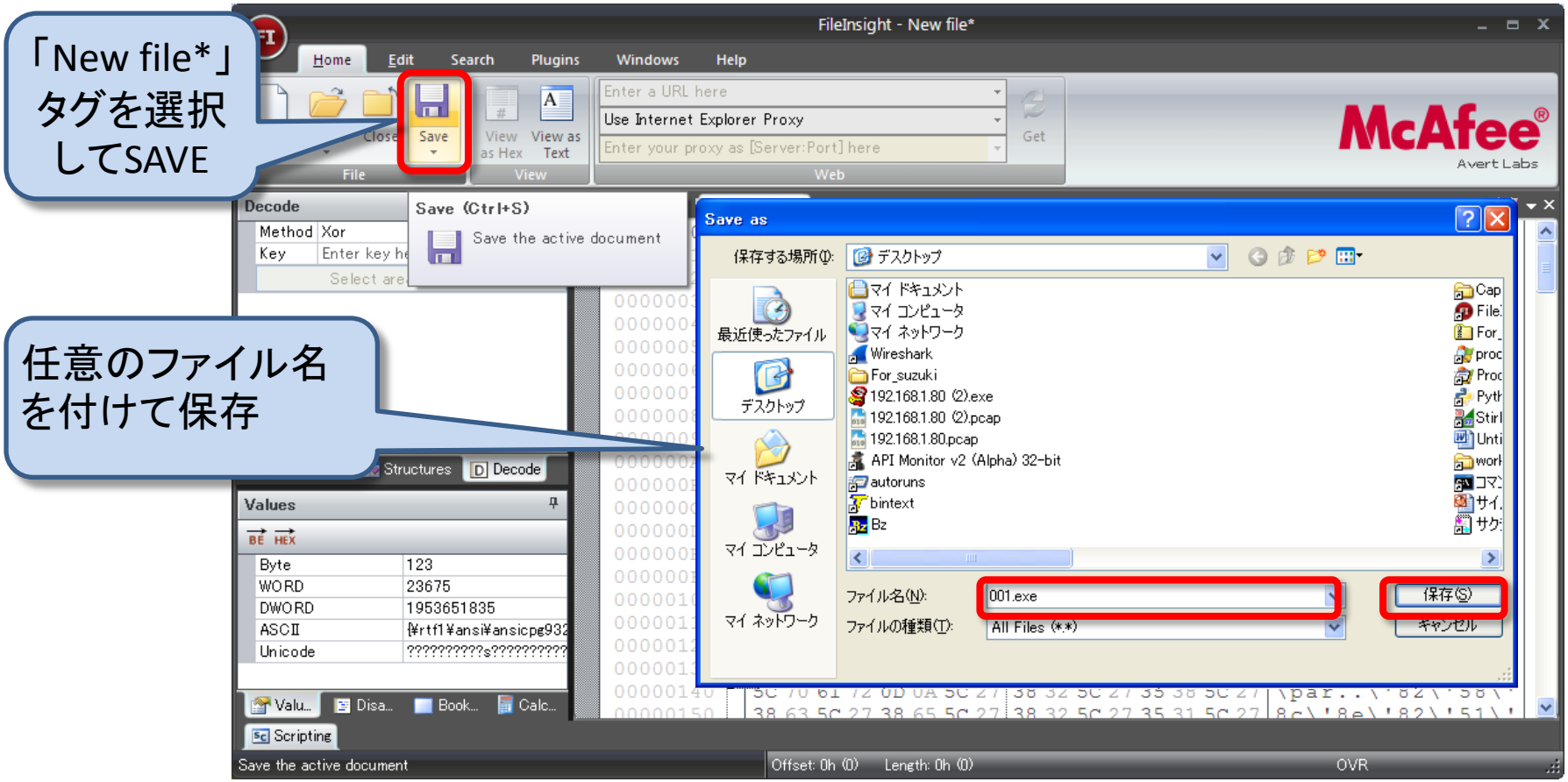
オブジェクト抽出

- **PEファイル抽出**
  - 1つ目のPEファイル部分を選択しコピー



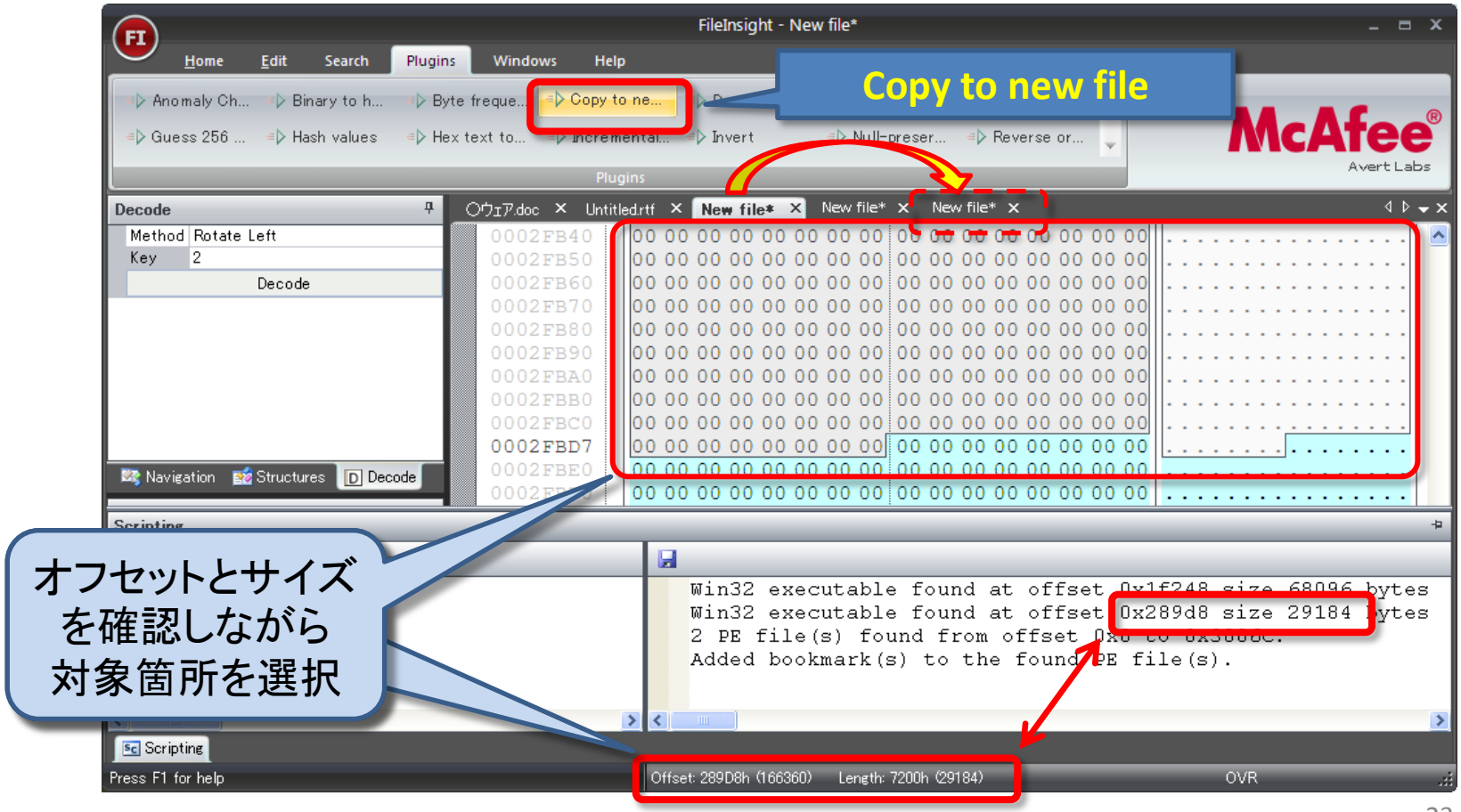
オブジェクト抽出

- **PEファイル抽出**
  - 1つ目のPEファイル部分を任意ファイルとして保存



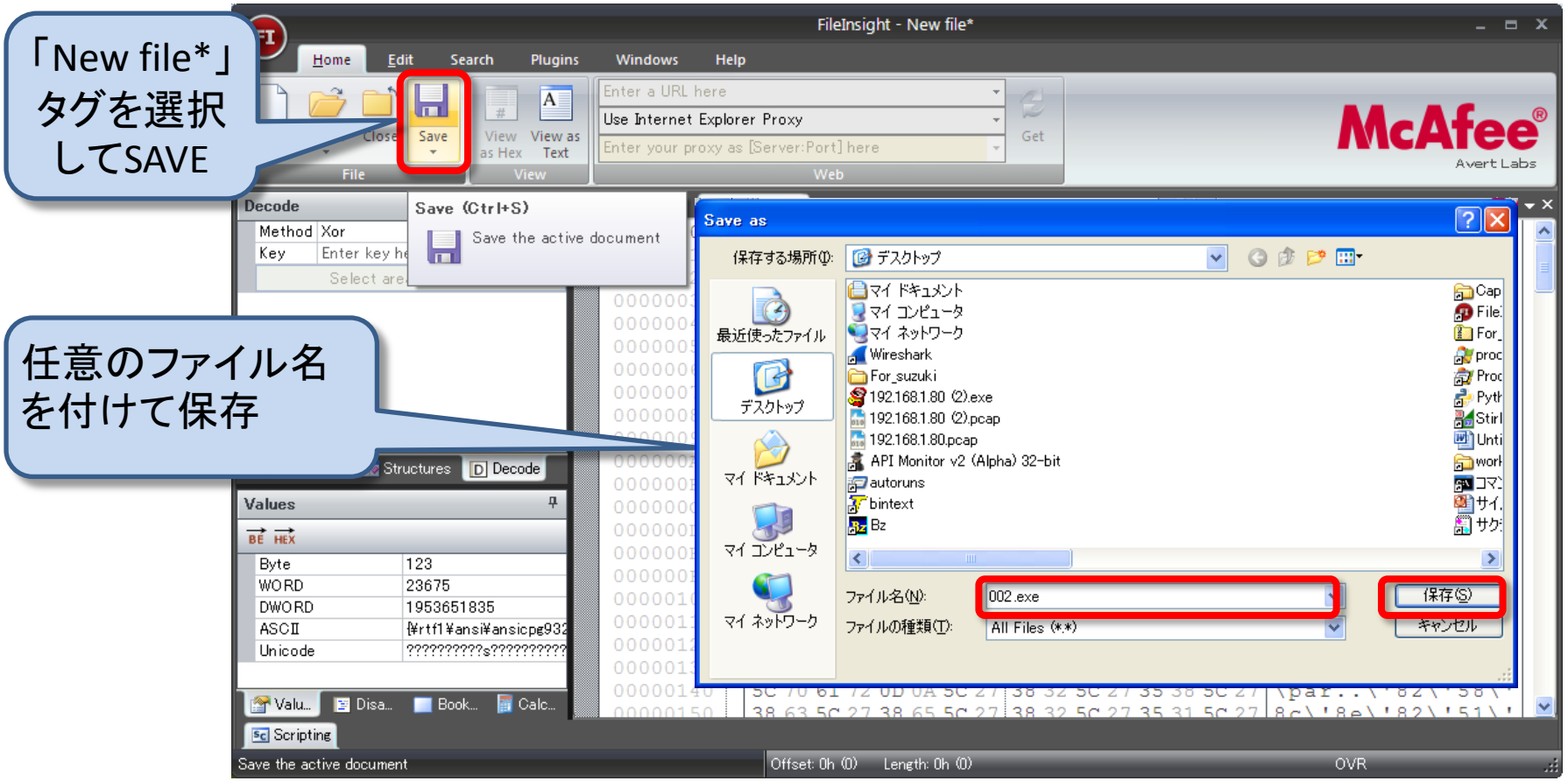
オブジェクト抽出

- **PEファイル抽出**
  - 2つ目のPEファイル部分を選択しコピー



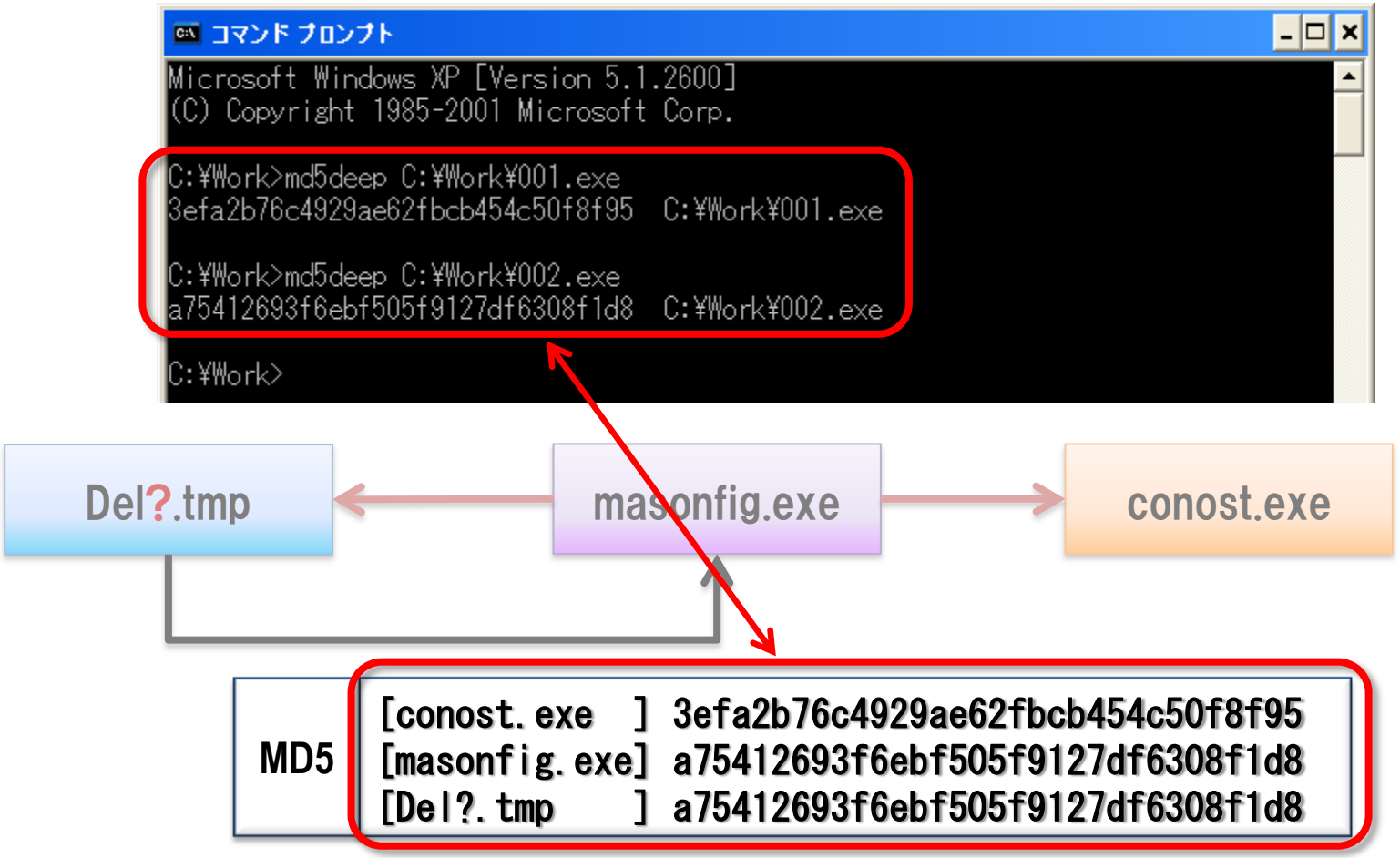
オブジェクト抽出

- **PEファイル抽出**
  - 2つ目のPEファイル部分を任意ファイルとして保存



オブジェクト抽出の結果

- **抽出したPEファイルの確認**
  - 動的解析にて抽出したPEファイルと比較してみる



オブジェクト抽出の結果

- **その他の成果**
  - 動的解析の様に環境を汚染させることなく抽出ができた
  - 静的解析の様にシェルコードの構造を調べることなく抽出ができた
  - 動的解析では失敗していた「偽装ファイル」の抽出にも成功した
  - 攻撃対象アプリケーションのバージョン等を気にせず抽出ができた

- **今後の課題**
  - シェルコードの挙動を調べていないため、複雑なマルウェアの場合、構成要素間の相関や因果関係が逆に分かり辛くなる可能性がある
  - 高度な暗号や圧縮、パックされたマルウェアには通用しない
  - ファイルをドロップするマルウェアでない場合は通用しない可能性有