Malcat

Renaud Tabary (www.malcat.fr)

OSSIR - 8 Octobre 2024

Plan

MALCAT - POURQUOI ?

Figure: Pourquoi Malcat ?

MALCAT - POUR QUI ?

- Analyste SOC
  - **Triage**
  - Création de règles de détection
- Antivirus
  - RE léger
  - **Triage**
- Réponse à incident
  - **Triage**
  - Carving
- Ingénierie inverse
  - Analyse de **données**
  - Identification de patterns

MALCAT - EN CHIFFRES

- Début du developement: depuis 2020
- Commercialisation: depuis 2022
- Environ 200 utilisateurs journaliers:
  - Antivirus
  - SOCs
  - CERTs (nationaux / externes / internes)
  - Labs
  - Formation
  - etc.

Plan

SUMMARY & ANOMALIES

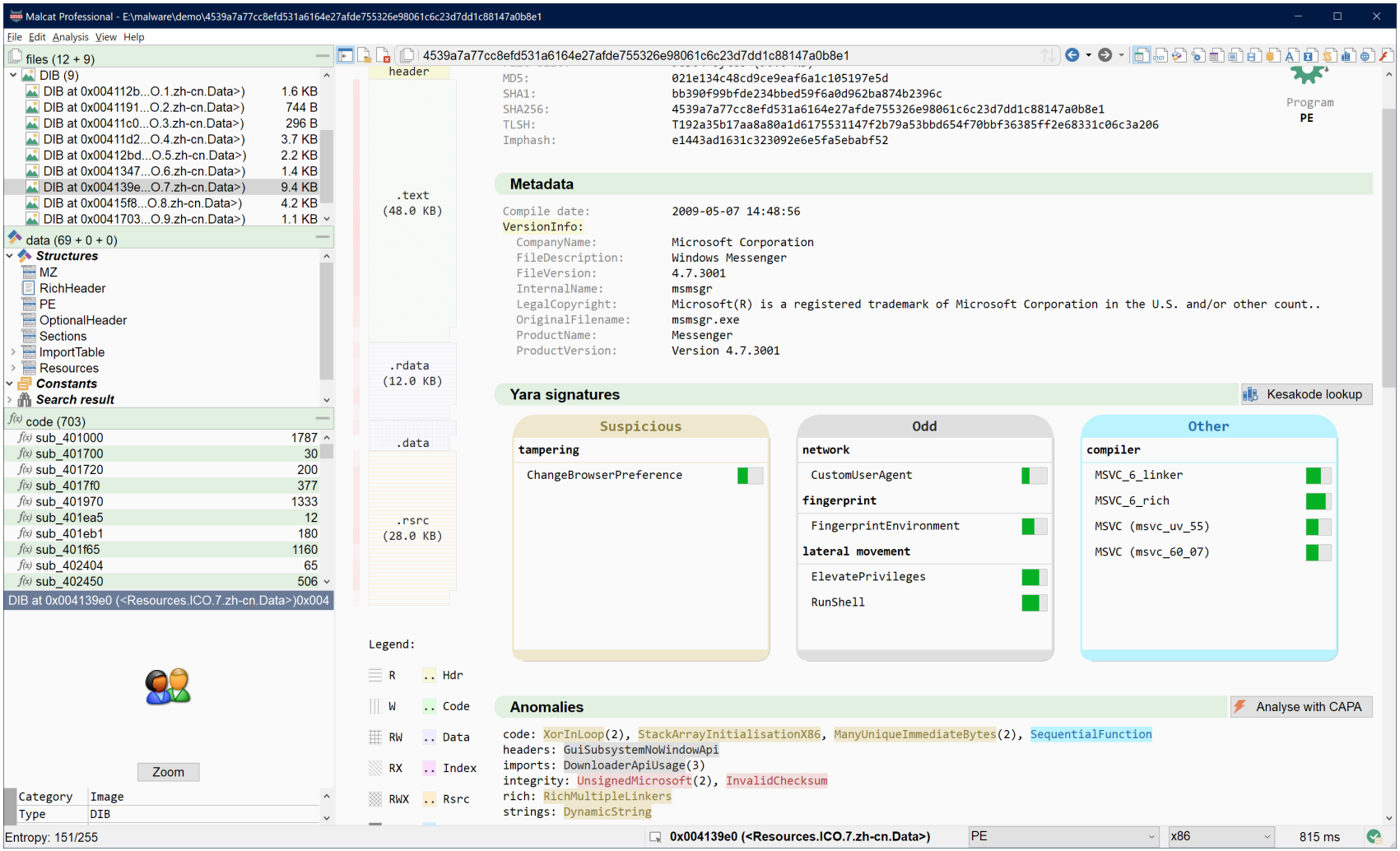

Figure: Summary view with anomalies

HEXA & STRUCTURES

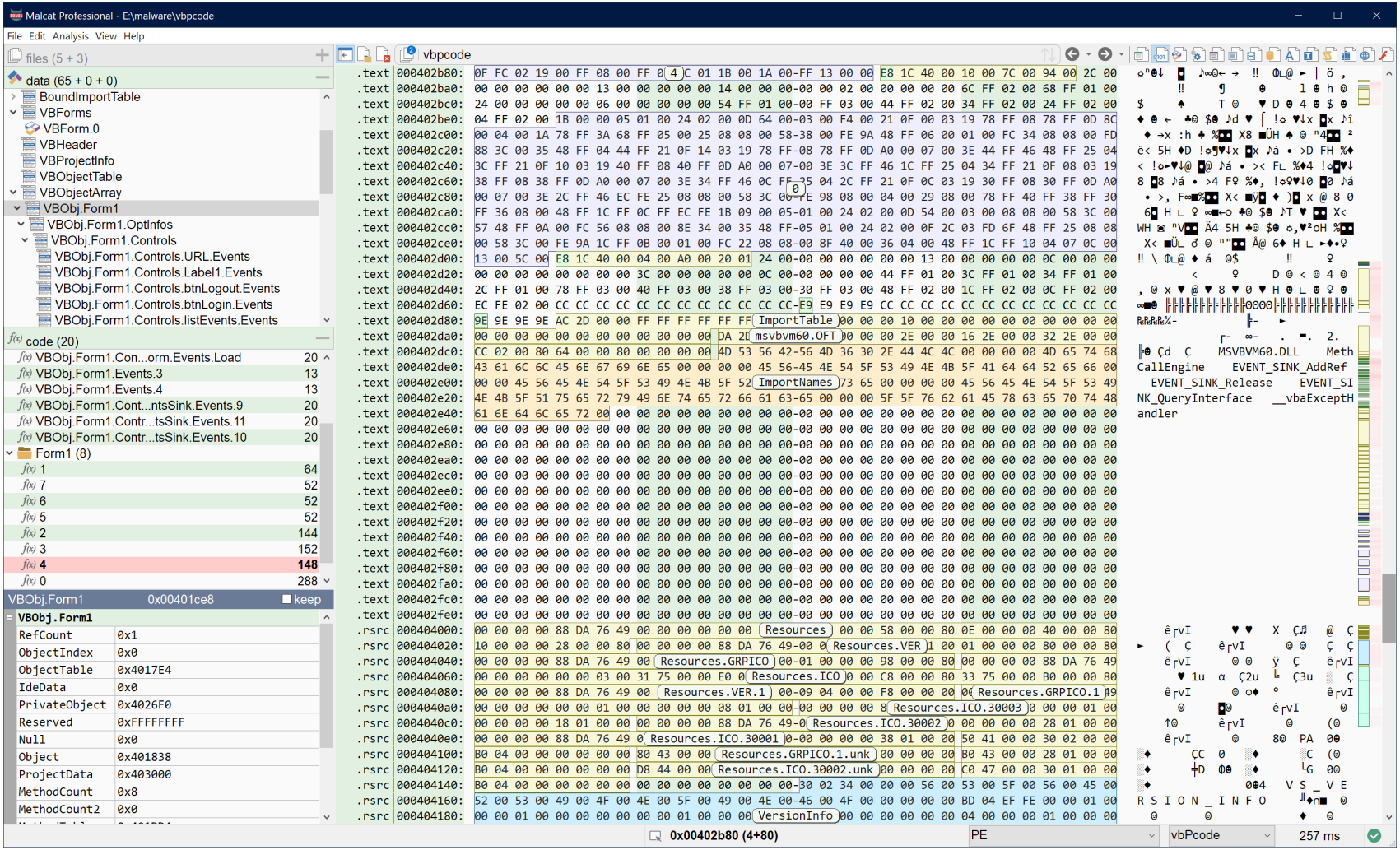

Figure: Hexadecimal view

DÉSASSEMBLEUR

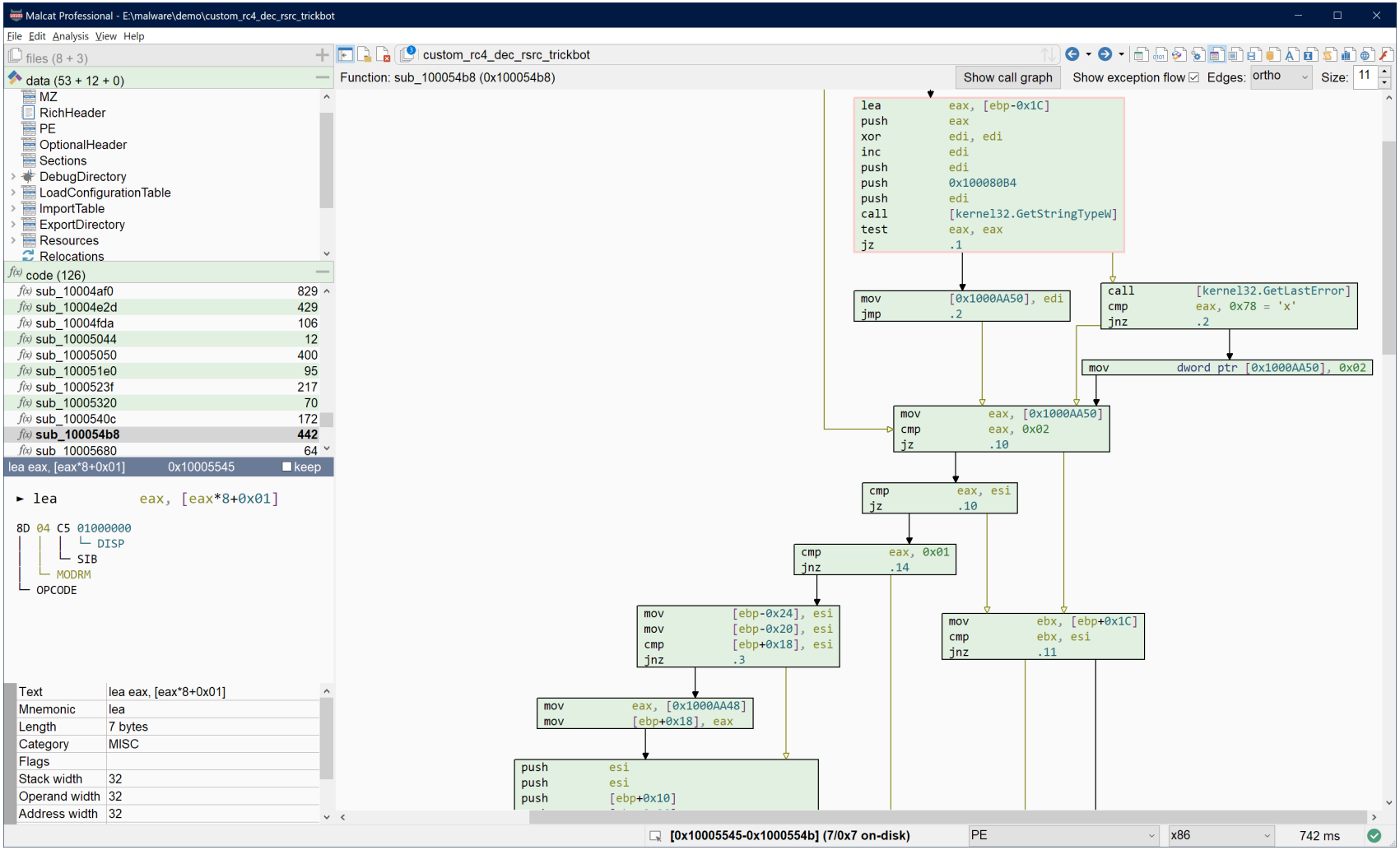

Figure: Desassembleur

Editeur Yara

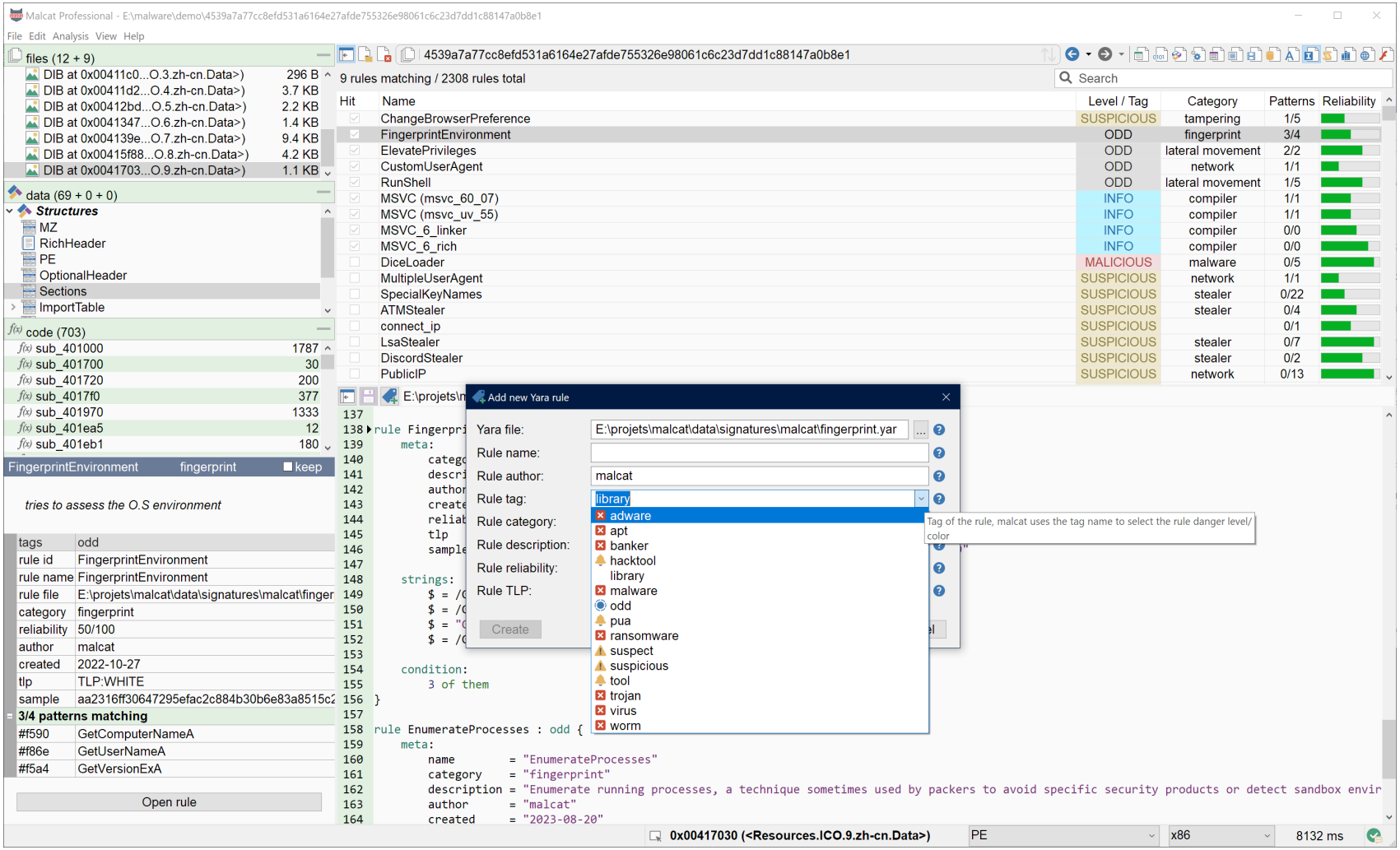

Figure: Yara editor

DIFF MODE

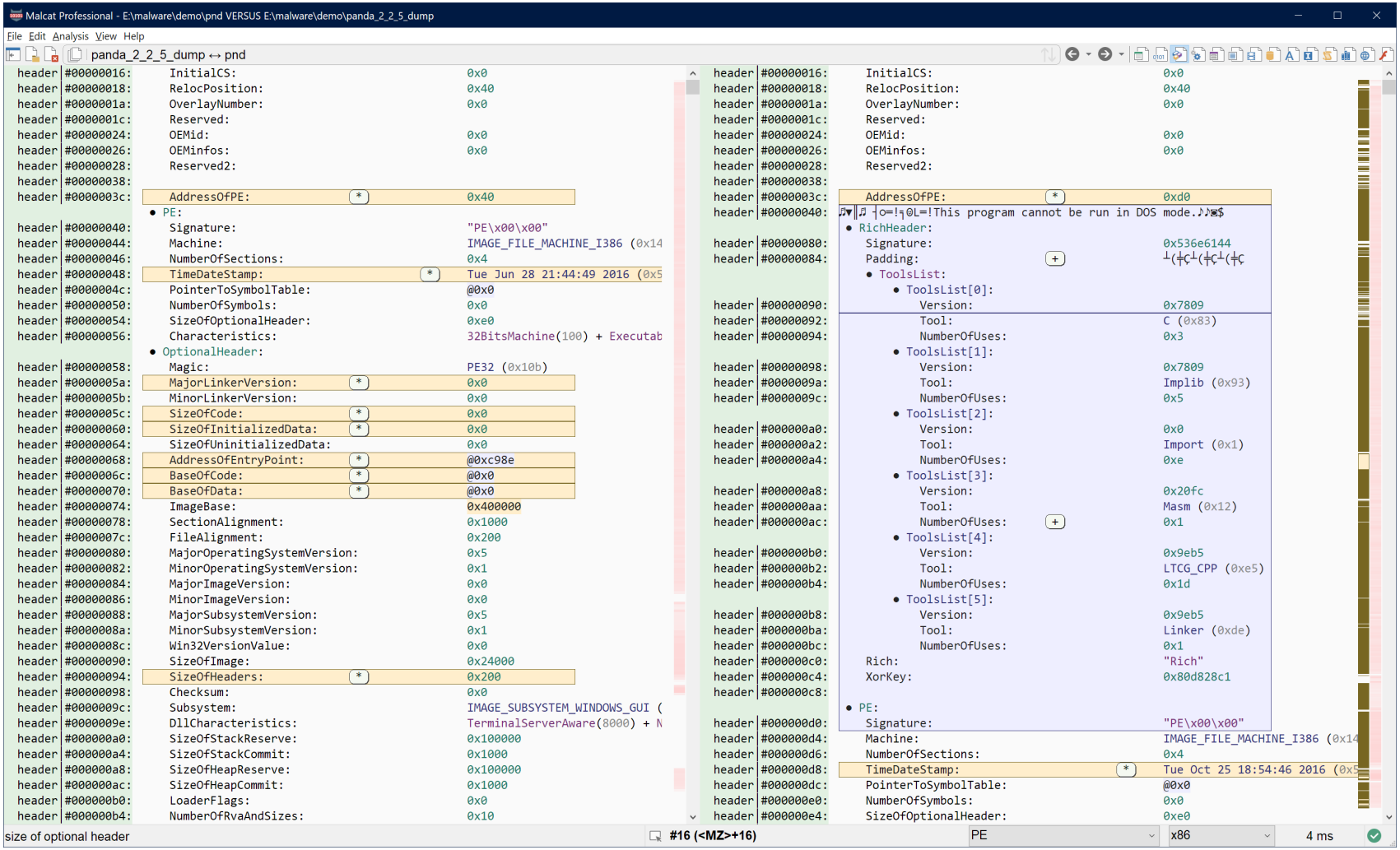

Figure: Binary diffing

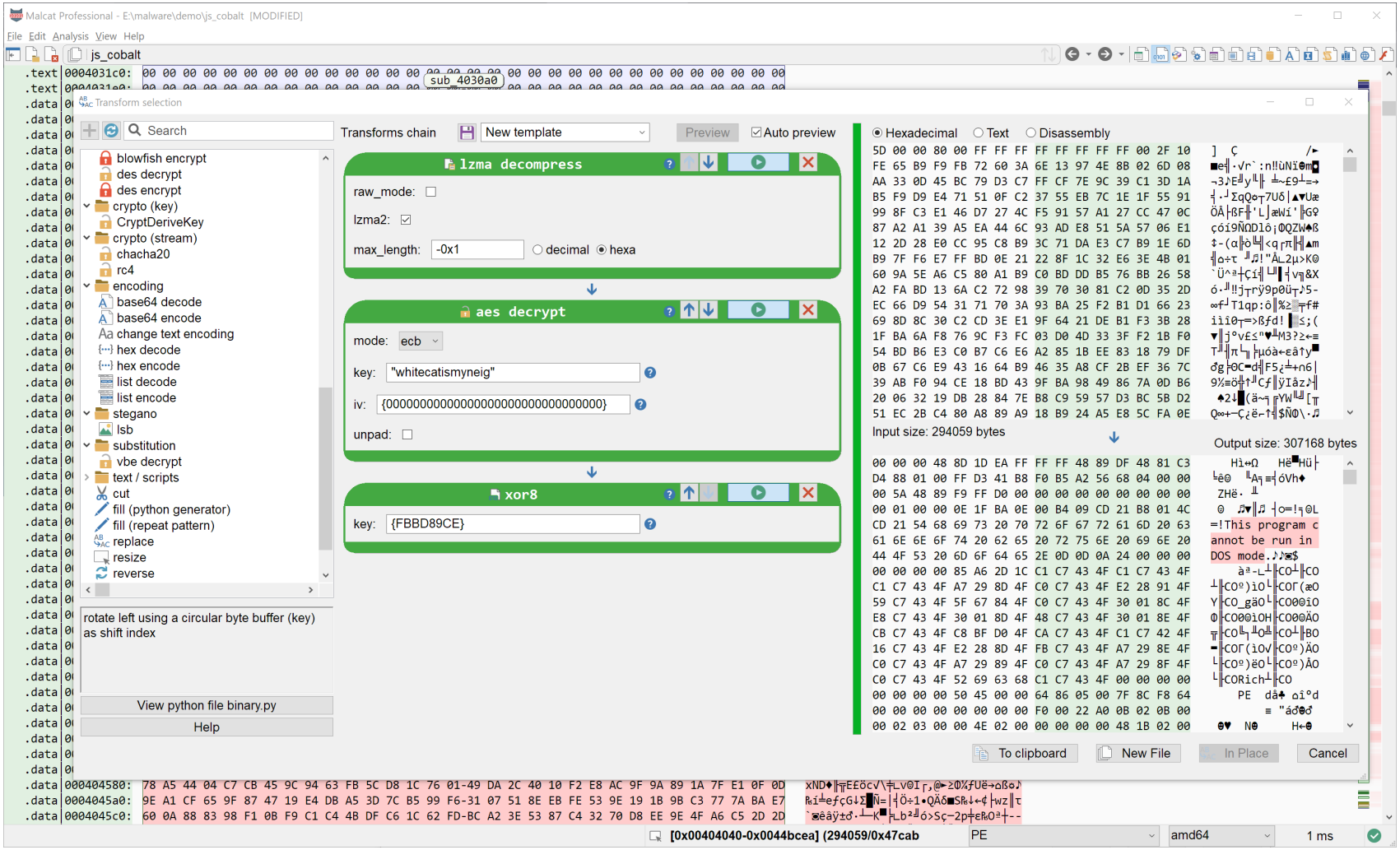

Figure: Transforms

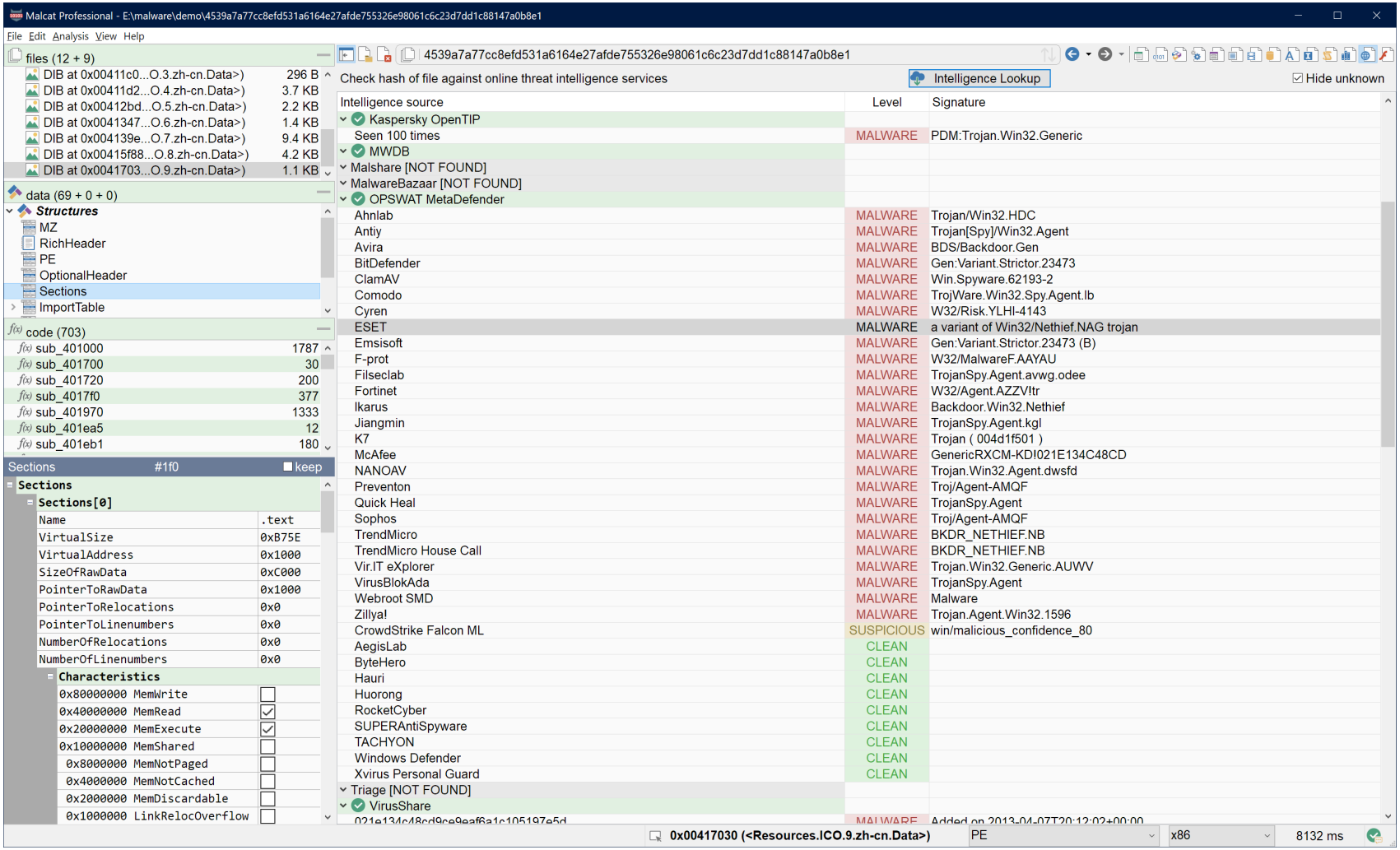

Figure: Threat intelligence

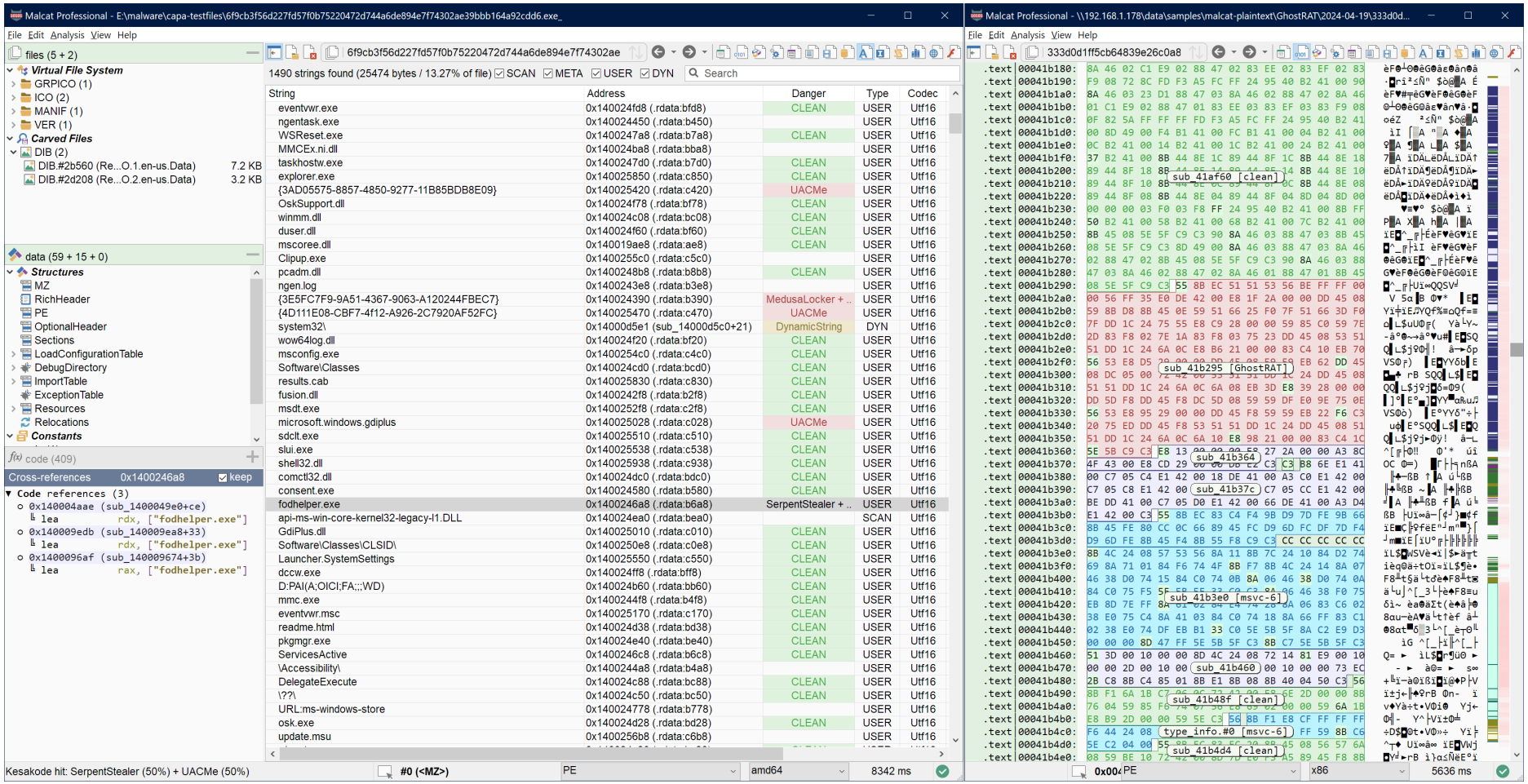

Figure: Kesakode: coloring

En chiffres

- Rapide!
- Plus de 50 formats de fichiers supportés:
  - Programmes, images, archives, FS, documents, Office, etc.
  - Parsers en python
  - Extraction de fichiers / carving
- Multi-architecture:
  - x86/x64, .NET, .PYC, VB p-code
  - Mais aussi: VBA, NSIS VM, InnoScript, macros Excel, tables MSI
    ...
- Reconnaissances de patterns:
  - Plus de 300 anomalies
  - Support signatures FLIRT
  - Plus de 400k constantes (hash API, crypto, GUIDs, etc.)
  - Kesakode (function/string/constants online lookup)

Moteur d'analyse en C++, décorélé de la GUI:

- Bindings en python
- Documentation complète
- Possibilité de lancer des analyse depuis la CLI ou depuis python
- Traitements en batch / multi-threading
- Rapport / templates

SYNERGIES

Interaction entre les outils:

- Désassembleur / editeur hexa -> Yara
- Transforms -> file carving
- Désassembleur -> script / émulation, Yara
- Késakode -> Strings, Yara, désassembleur
- etc.

AVANTAGES

- Adapté à tout niveau de compétence
  - Débutant: rapport d'analyse, anomalies, threat intel
  - Intermédiaire: editeur Yara, désassembleur
  - Avancé: scripting, intégration OEM
- Gain de temps pour l'analyste
  - Analyse rapide
  - Beaucoup d'outils en un
  - Support de 99% des types de fichiers "malveillants"
- Gain d'argent pour l'entreprise