

# Static Analysis: Identifying Malware

---



**Tyler Hudak**

INCIDENT RESPONDER

@secshoggoth



# Overview

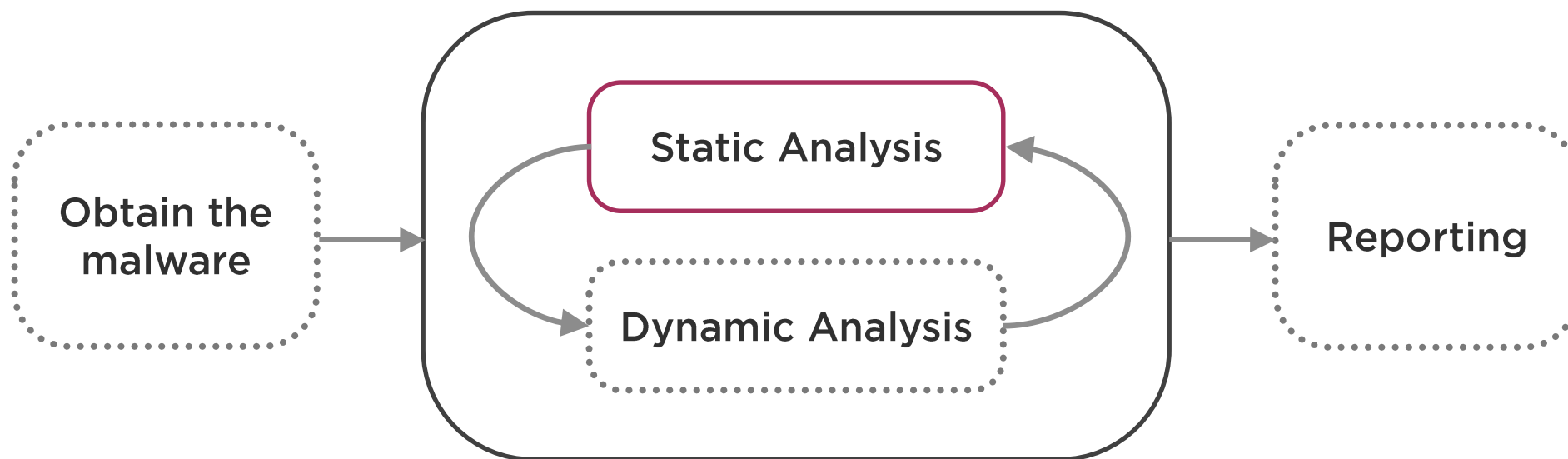


Identifying Files

Hashing and Finding Other Information



# Malware Analysis Process



# Focus Your Analysis

**What kind of  
file is this?**

**Is any information  
already known  
about it?**

**What do the  
embedded strings  
tell about it?**

**Is there anything  
unusual in the  
PE header?**

**Is it packed?  
If so, what packer?**

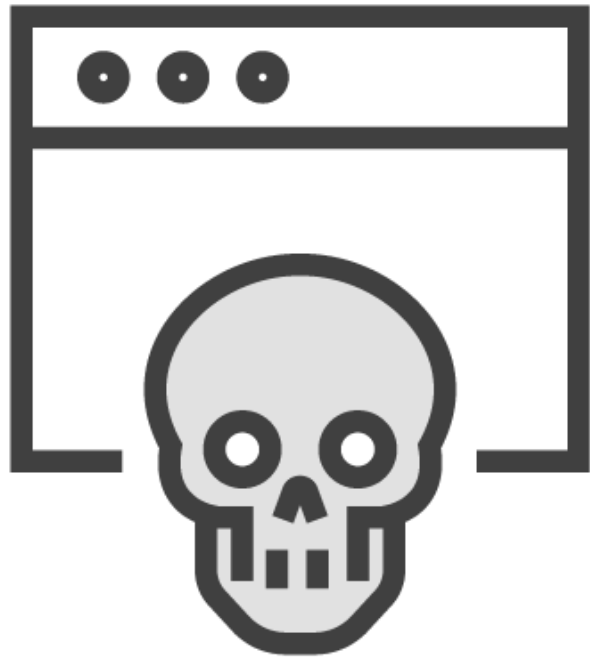




**Static analysis can still lead to malware execution!**

**Analyze your new tools like malware!**

- Know how your tools work
- Ensure there are no backdoors





<http://bit.ly/malfund-1>

- Password is “infected”

**This is real malware!**

# File Identification

**Determine the type of file you are examining**

**Attackers try to disguise files**

- Double extensions
- Archives

**Packer detection**





# File Signatures

```
[C:\Windows\System32\notepad.exe] - Frhed
File  Disk  Edit  View  Options  Registry  Bookmarks  Misc  Help

000000 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....ÿÿ..
000100 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ,.....@.....
000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000300 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 .....à...
000400 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ..°..´.Í! ,.LÍ!Th
000500 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
000600 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
000700 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$.
000800 b2 be c2 62 f6 df ac 31 f6 df ac 31 f6 df ac 31 ¼Âböß-1öß-1öß-1
000900 ff a7 39 31 f5 df ac 31 ff a7 3f 31 eb df ac 31 ÿ§91öß-1ÿ§?1ëß-1
000a00 f6 df ad 31 00 df ac 31 ff a7 2f 31 e9 df ac 31 öß-1.ß-1ÿ§/1éß-1
000b00 ff a7 28 31 f4 df ac 31 ff a7 38 31 f7 df ac 31 ÿ§(1ôß-1ÿ§81÷ß-1
000c00 ff a7 3d 31 f7 df ac 31 52 69 63 68 f6 df ac 31 ÿ§=1÷ß-1Ríchöß-1
000d00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
000e00 50 45 00 00 4c 01 04 00 0f c6 5b 4a 00 00 00 00 PE..L....Æ[ ]...
000f00 00 00 00 00 e0 00 02 01 0b 01 09 00 00 a8 00 00 ....à.....
001000 00 24 02 00 00 00 00 00 89 36 00 00 00 10 00 00 .$.
001100 00 c0 00 00 00 00 00 01 00 10 00 00 00 02 00 00 .À.....
001200 06 00 01 00 06 00 01 00 06 00 01 00 00 00 00 00 .....
001300 00 00 03 00 00 04 00 00 41 97 03 00 02 00 40 81 .....
                                         Δ      @

Offset 182=0xb6 Bits=10101100 Unsigned: B:172,W:12716,L:2818519468 ANSI / OVR / L Size: 179712
```



# File Signatures You Should Know

Windows Executable

“MZ” in bytes 0-1

---

PDF

“%PDF-” followed by  
number within first  
1024 bytes

---

Old Office Doc

0xD0CF11E0  
("DOCFILE")

---

Zip Archive

“PK” in bytes 0-1



# File

Compares file header with known signatures

<http://gnuwin32.sourceforge.net/packages/file.htm>



# File – openme.doc.exe



```
C:\Windows\system32\cmd.exe

C:\temp>file openme.doc.exe
openme.doc.exe; PE32+ executable for MS Windows (GUI)
```

The image shows a Windows command prompt window with a blue title bar. The title bar text is 'C:\Windows\system32\cmd.exe'. The window contains a black command prompt area with white text. The text shows the command 'file openme.doc.exe' being executed, followed by the output 'openme.doc.exe; PE32+ executable for MS Windows (GUI)'. The window has standard Windows window controls (minimize, maximize, close) in the top right corner.



## Exeinfo PE

Analyzes Windows PE header information

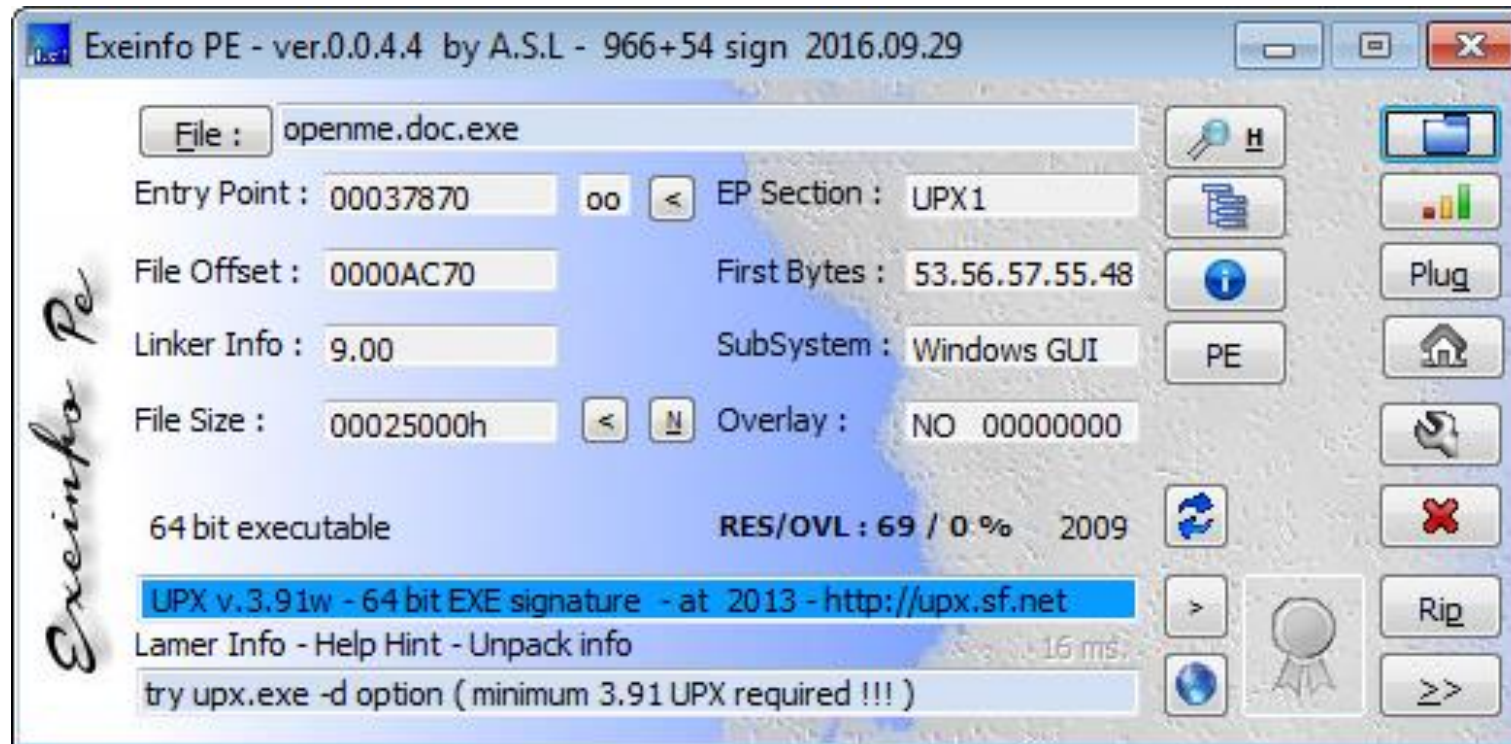
Packer detection

Gives hints on how to unpack

<http://exeinfo.atwebpages.com/>



# Exeinfo PE - openme.doc.exe



## TrID

Uses pattern database to determine type

Gives likelihood of detected type

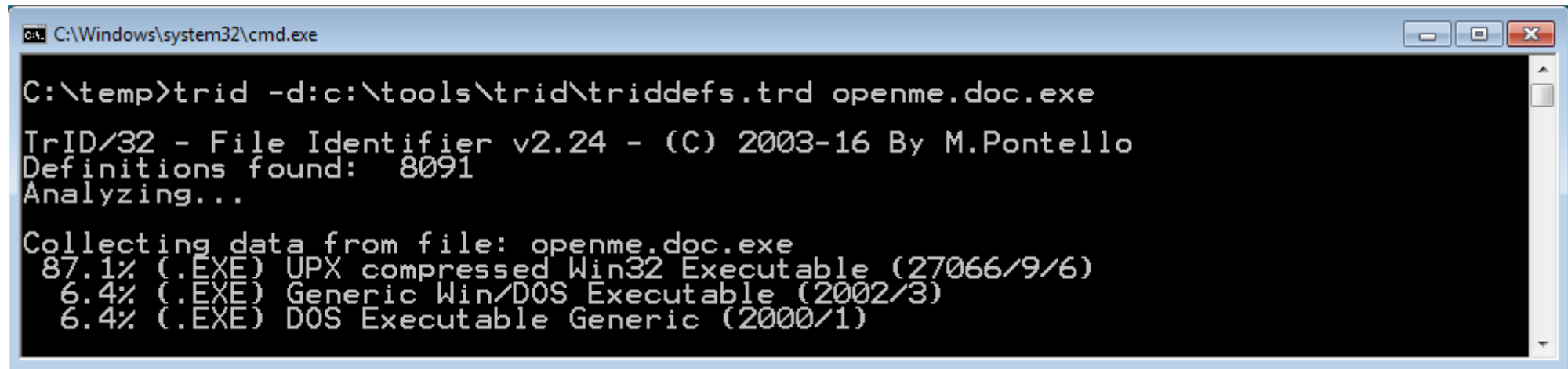
<http://mark0.net/soft-trid-e.html>

### Options

-d:PATH : Path to pattern database



# TrID - openme.doc.exe



```
C:\Windows\system32\cmd.exe

C:\temp>trid -d:c:\tools\trid\triddefs.trd openme.doc.exe

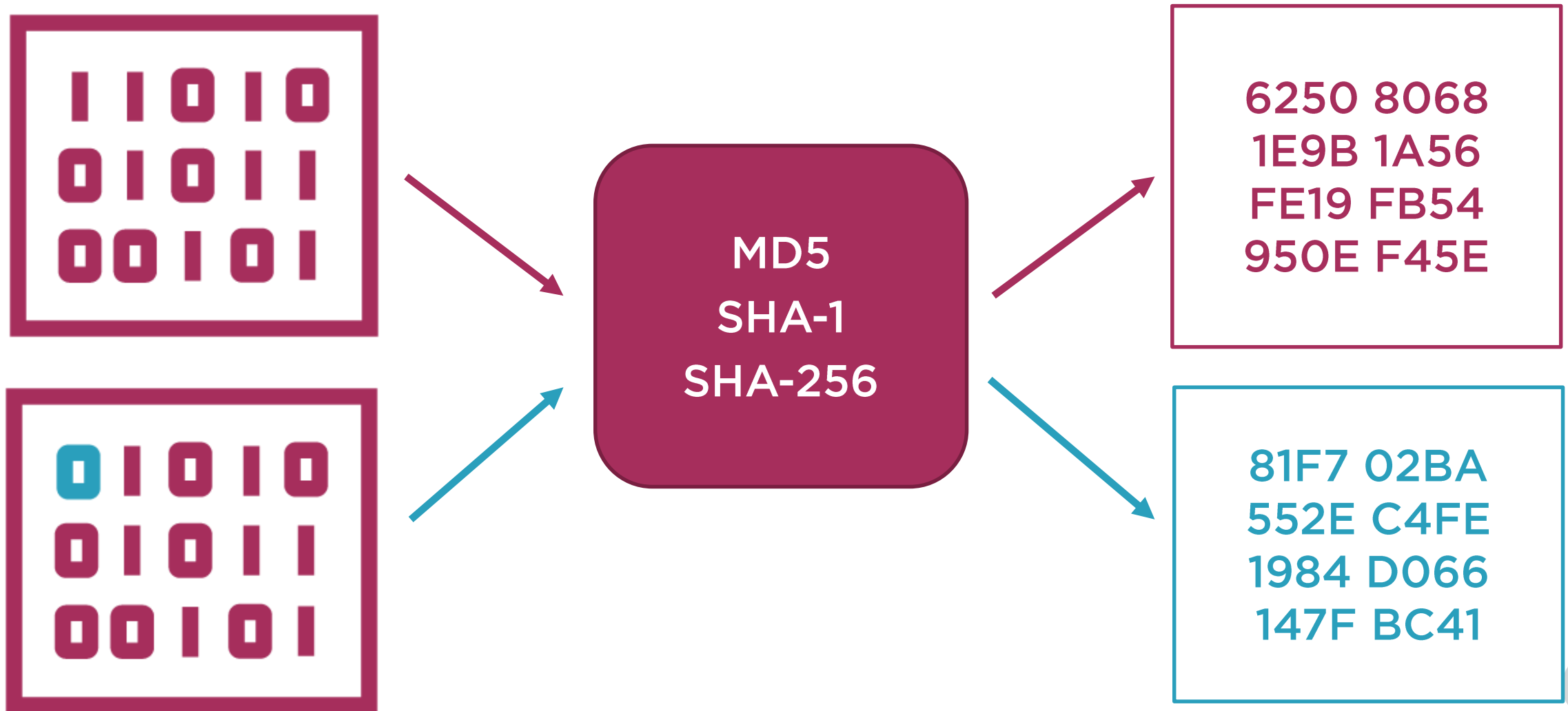
TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found: 8091
Analyzing...

Collecting data from file: openme.doc.exe
87.1% (.EXE) UPX compressed Win32 Executable (27066/9/6)
6.4% (.EXE) Generic Win/DOS Executable (2002/3)
6.4% (.EXE) DOS Executable Generic (2000/1)
```

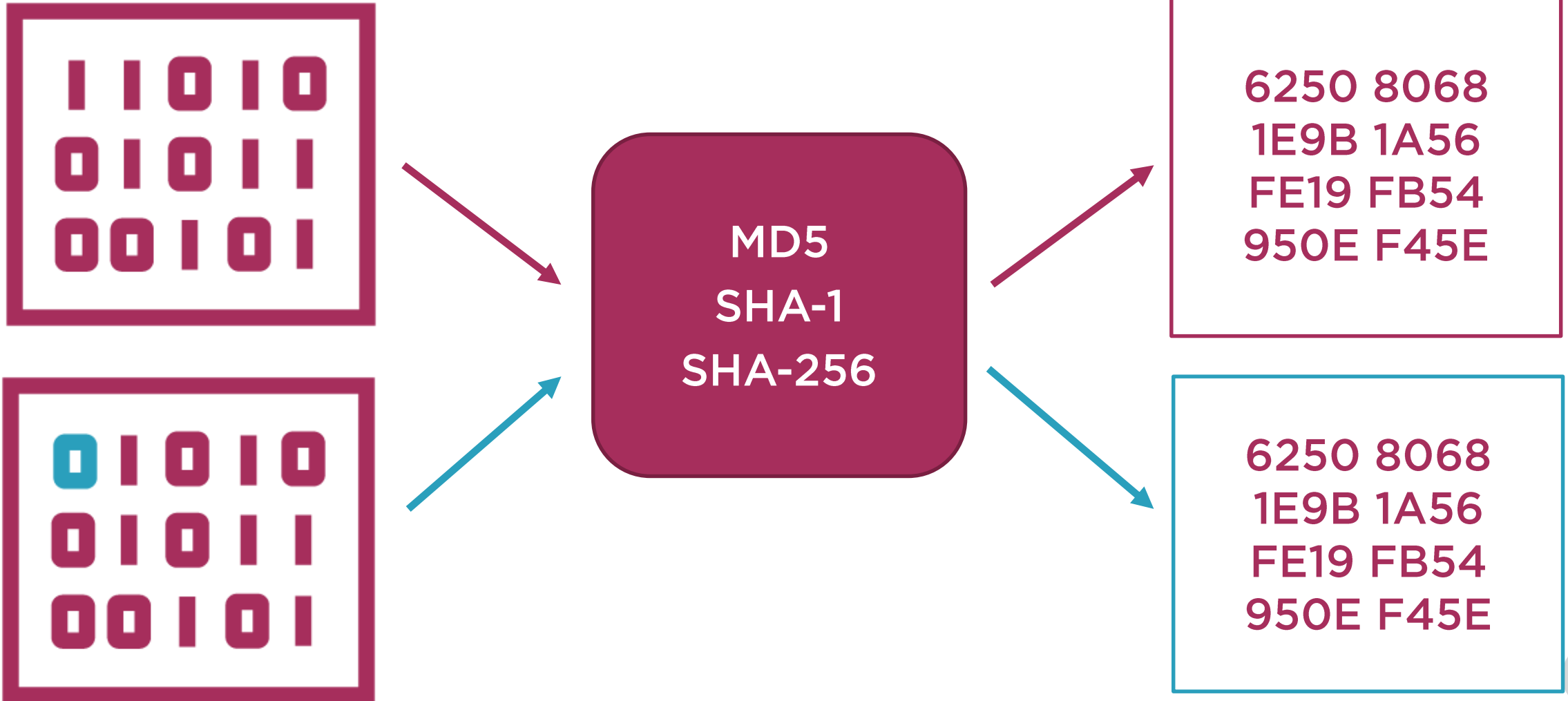




# Cryptographic Hashes



# Collisions



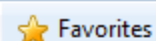
# Using Cryptographic Hashes

**Organize and identify specific samples**

**Hash with multiple algorithms**

**Find additional online information**





VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

[File](#)[URL](#)[Search](#)[Enter Term](#)[Search it!](#)[Find out more about searching](#)



# Google

[Advanced search](#)  
[Language tools](#)[Advertising Programs](#)[Business Solutions](#)[+Google](#)[About Google](#)© 2017 - [Privacy](#) - [Terms](#)

# Compute Hash

**Generates MD5, SHA1, SHA256 hashes of files**

**<http://www.subisoft.net/ComputeHash.aspx>**



# Demo



## File identification and hashing

<http://bit.ly/malfund-1>



budget-report.exe

**Windows 32-bit executable**

**Not packed**

**Was already on VirusTotal**

**VirusTotal detects it as malware**





# Summary



**Identify files to determine what you are analyzing**

- Helpful to identify packers

**Generate cryptographic hashes to identify other analysis**