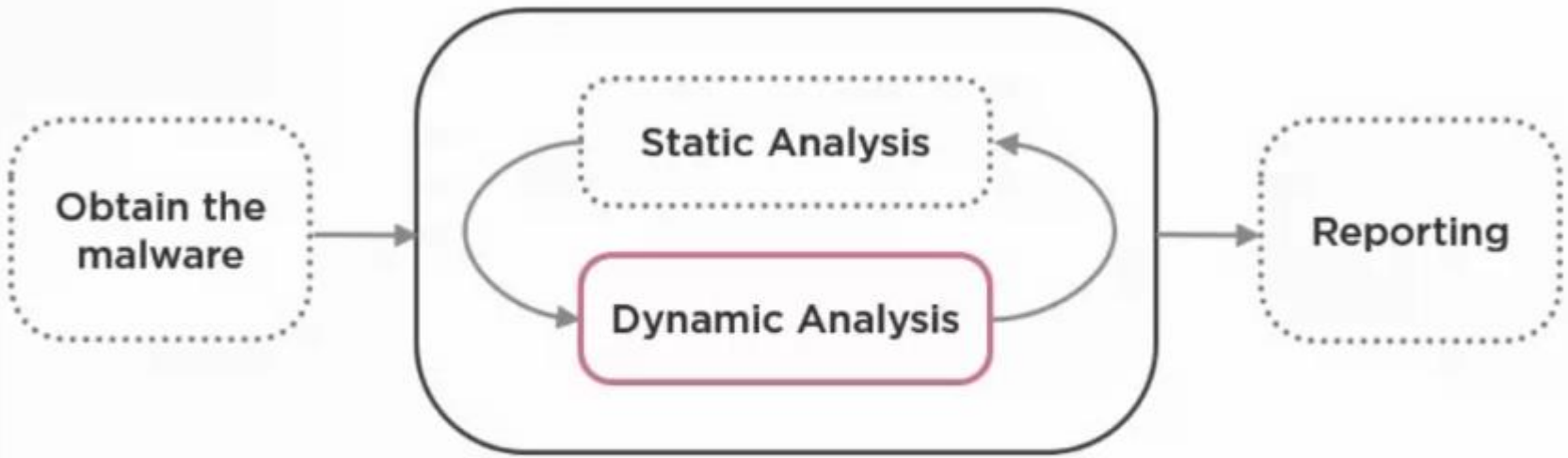
Malware Analysis Process

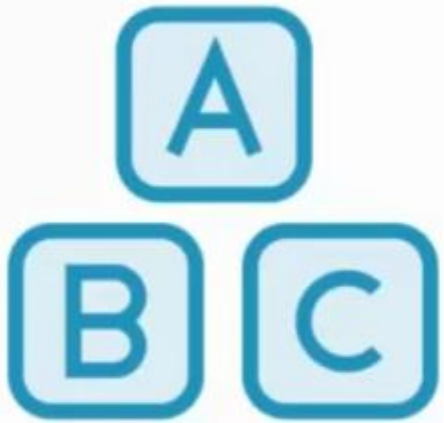
Malware Analysis Process



Static Analysis – Analyzing malware without execution

Dynamic Analysis – Analyzing the behavior of malware through execution

Static Analysis Techniques



Embedded Strings Analysis

Extract and examine groups of readable characters from the document

Encrypted Data

Search the document for encrypted or encoded strings or data

Pattern and Signature Analysis

Common and repeatable attacks

Identify patterns in the attacks

Write signatures to detect attacks

Yara

Write signatures to detect patterns and identify malware or attacks

Robust language

Repositories

- https://github.com/Yara-Rules/rules

https://virustotal.github.io/yara/

```
yara RULES_FILE FILE_TO_SCAN
```

Options

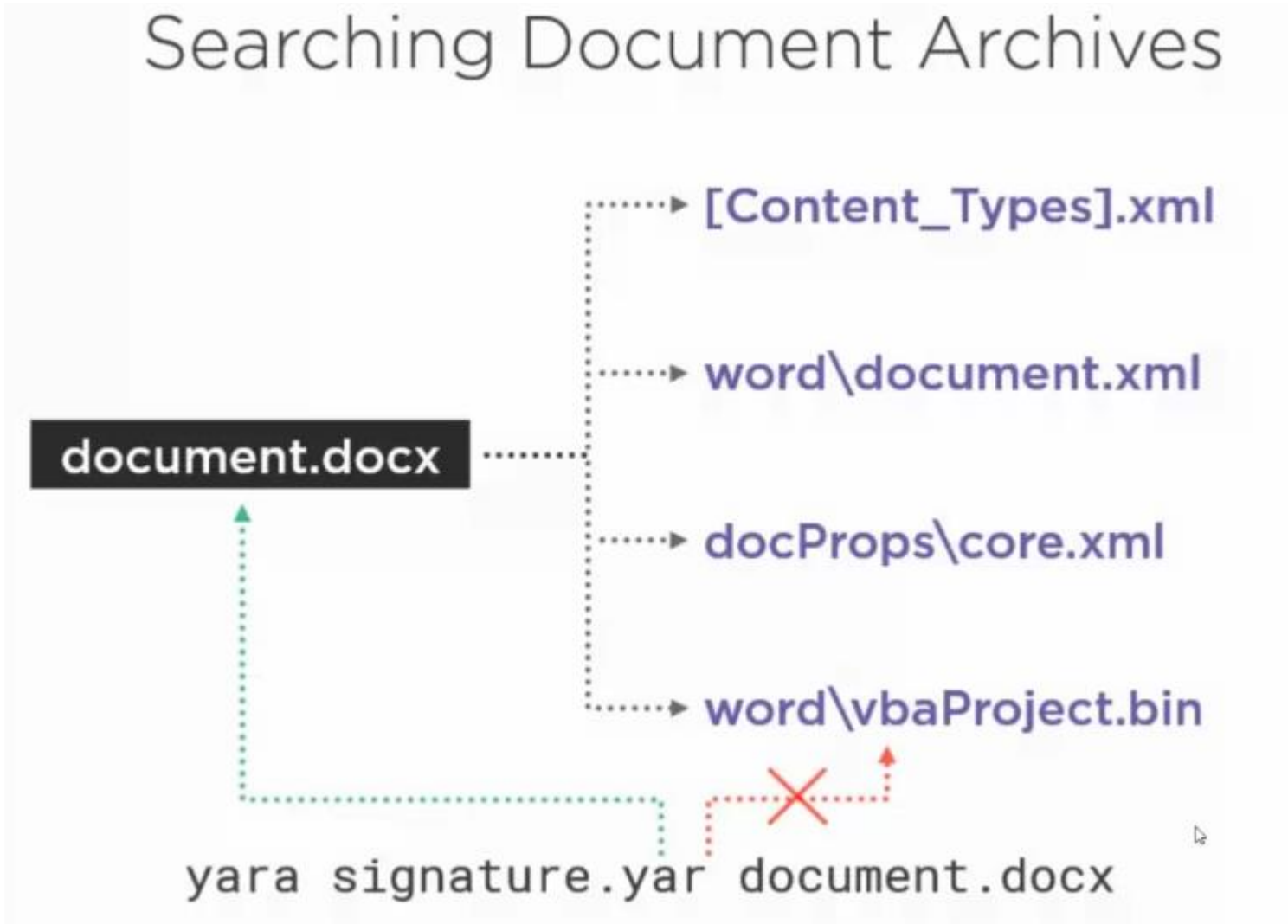
-w: Turn off warnings

-g: Print tags

-m: Print metadata

-s: Print matching strings

Searching Document Archives



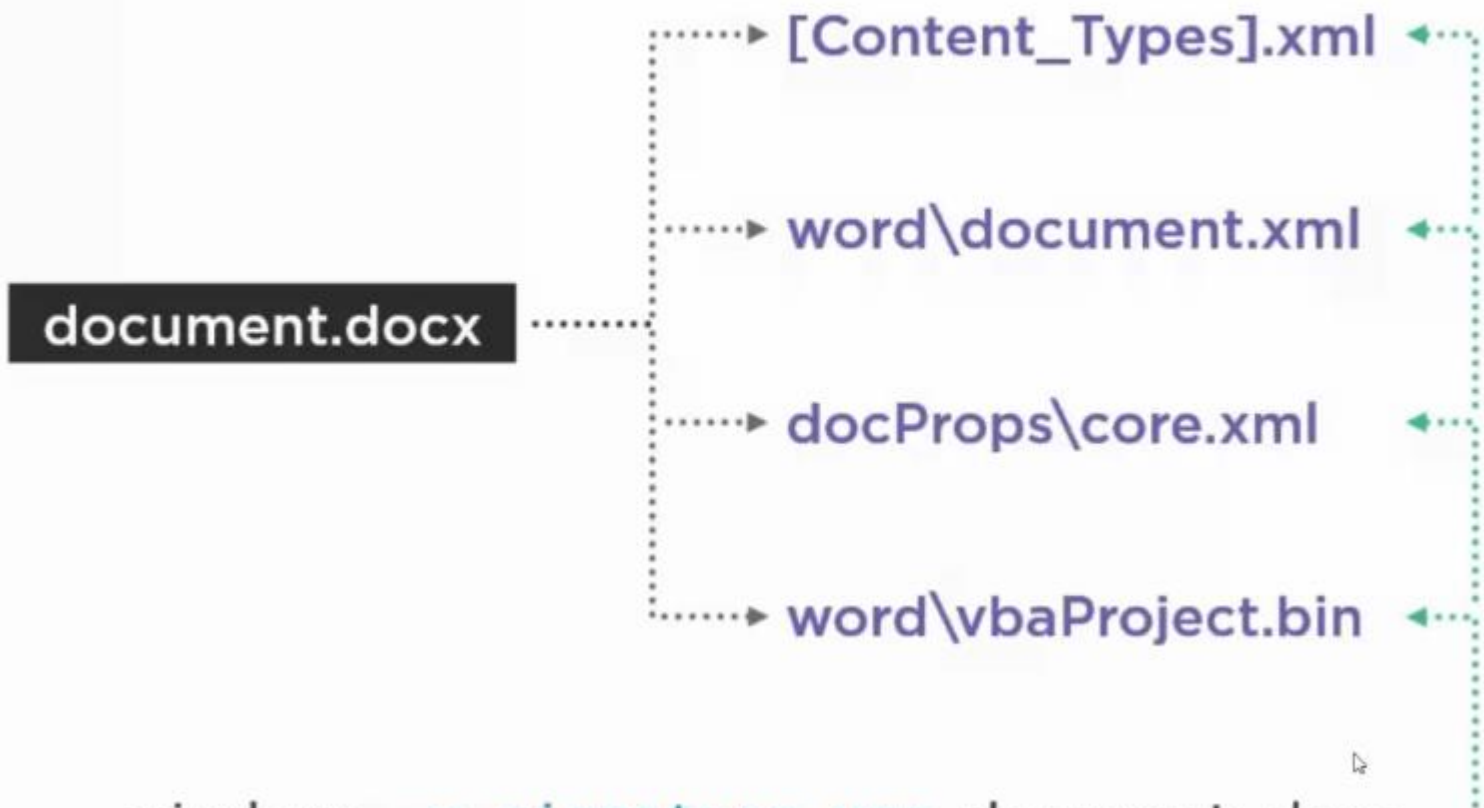
zipdump

Iterate over files within a zip archive

Run Yara signatures against each file

https://github.com/DidierStevens

Searching Document Archives




```
zipdump -y signature.yar document.docx
```

Metadata

Information about the document contained within the document.

- Date and timestamps
- Author info
- Language
- Document specific info

exiftool

Extracts metadata from dozens of file types

https://www.sno.phy.queensu.ca/~phil/exiftool/

```
MIME Type                       application/msword
Code Page                       Windows Simplified Chinese (PRC, Singapore)
Title
Total Edit Time                 1.0 minutes
Author
Title Of Parts
File Type                       DOC
File Modification Date/Time     2012:08:14 20:28:04-04:00
Create Date                     2007:09:18 04:34:00
Template                        Normal.dot
Keywords
Security                        0
Software                        Microsoft Word 11.0
Company                         VRHEIKER
Modify Date                     2007:09:18 04:35:00
Subject
```

Thank you