Hunting Malware with Yara rules

* Yara is a multiplatform used in pattern matching such as matching text and hex strings.

* Hello

* Yara rule extenstion .yar

>> yar test.yar /home/

Test.yar →

rule string_checker {

meta: author - Description

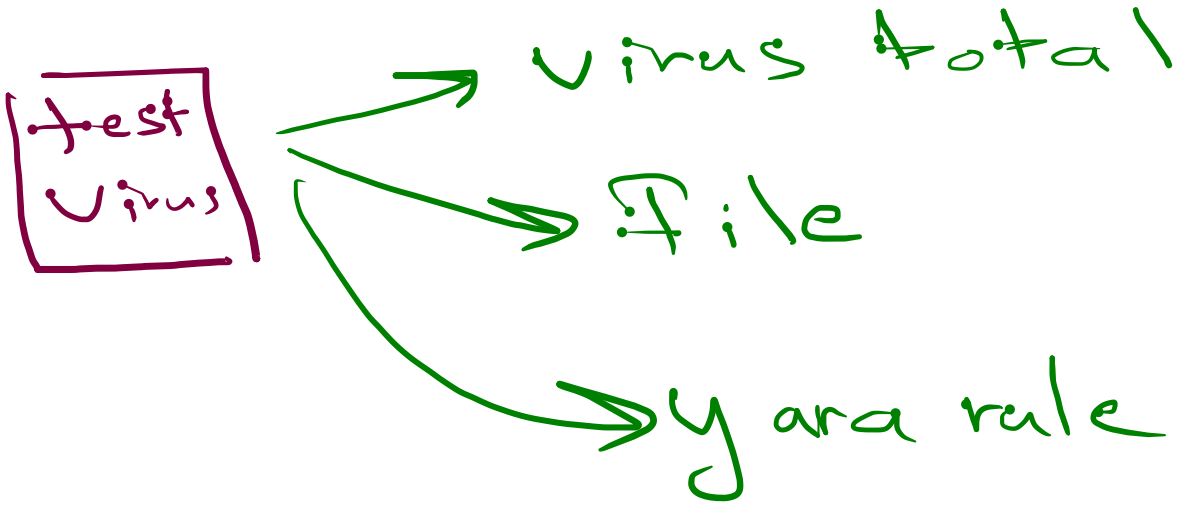
Strings: $variables = "Hello"

Condition:

$varname

and
or
not

}


test
virus
virus total
file
yara rule