Digital Forensics

By: Andrew Fallin, Clem Izurieta

This information was graciously provided by Will Peteroy and Blackthorn Consulting

Andrew Fallin

- Masters/PhD Student- Distributed Energy Resource Cyber Security (Montana State University)
- Former Software Engineer for Sonalysts
- Washington State University

Digital Forensics - Outline

- Introduction to Digital Forensics
- Conducting an Investigation
- Digital Evidence/ Capturing Digital Evidence
- Memory Forensics
    - Volatility2 & 3 (Common Plugins)

Digital Forensics - Outline

- Hands On Tutorial!
  - Set Up
  - Walkthrough
  - Individual

Disclaimer!

What is Digital Forensics?

Introduction to Digital Forensics

Digital Forensics- the collection, analysis, and interpretation of **digital** evidence.

What is Digital Evidence?

“Any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or an alibi”

What is Digital Evidence?

“Digital evidence is information and data of investigative value that are stored on or transmitted by a computer.”

What is Digital Evidence?

“Digital data that support(s) or refutes a hypothesis about digital events or the state of digital data”

What are some types of Digital Data?

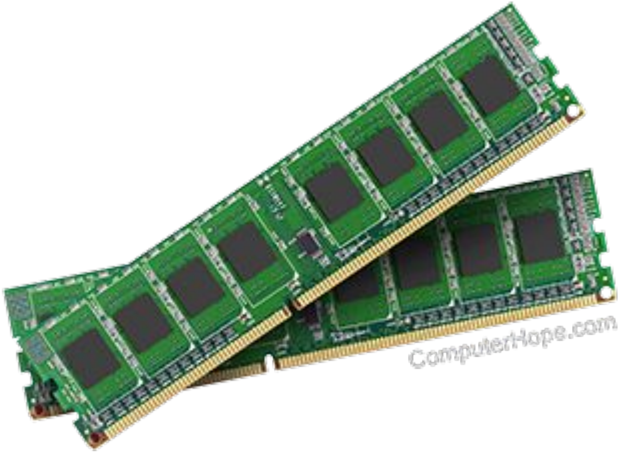
(think very broad)

What is Digital Data?

- Open Computer Systems
  - Computers
  - Laptops
  - Servers

What is Digital Data?

- Open Computer Systems
  - Standard System
    - HDD
    - HID
    - RAM



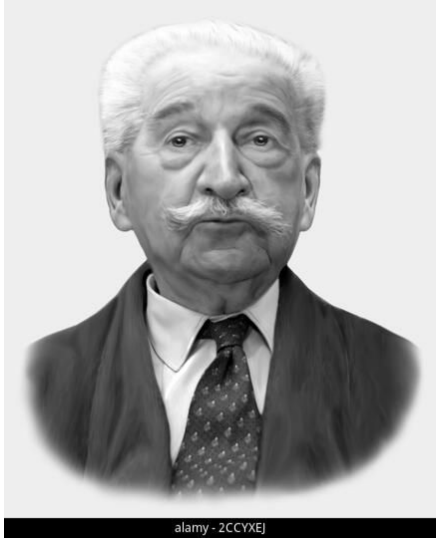
What is Digital Data?

- Communications
  - Networks
  - Embedded Computer Systems
    - Mobile Devices
    - Smart Devices

Principles of Digital Forensics

- Certainty
  - Almost never “certain”, use with extreme care
  - Only have a limited amount of information
  - Present *possibilities* or *hypotheses* with evidence and information to support or refute them

Principles of Digital Forensics


alamy - 2CCYXEJ

- Evidence Exchange
  - Locard’s Exchange Principle
    - contact between two items will result in an exchange

Principles of Digital Forensics

- Evidence Characteristics
  - Class characteristics
    - Similar traits between a group of items
    - Common traits
    - Example: File format characteristics

Principles of Digital Forensics

- Evidence Characteristics
    - Individual characteristics
        - Unique traits that can be tied to an individual
        - Example: MAC Address

Principles of Digital Forensics

- Forensic Soundness
  - How was the evidence handled?
  - Non-Modification
  - Documentation
    - (Time, Tools, Methods, etc.)

Principles of Digital Forensics

- Authentication
  - Integrity of Analyzed Data/ Records
  - Must be able to show:
    - Contents of record are unchanged
    - Information originates from purported source
    - Extraneous info (i.e date of collection) is accurate

Principles of Digital Forensics

- Chain of Custody
  - Documentation that proves continuity of possession of evidence

Principles of Digital Forensics

- Evidence Integrity
  - Show evidence has not been modified since the time of collection
  - Use message digests (hash) to prove it hasn't been modified
  - Most practitioners use SHA256 but some tools only support MD5 and SHA1

Principles of Digital Forensics

- Repeatability
  - Crucial that the process by which evidence is analyzed is well documented for repeatability
  - Enables independent verification

Conducting an Investigation

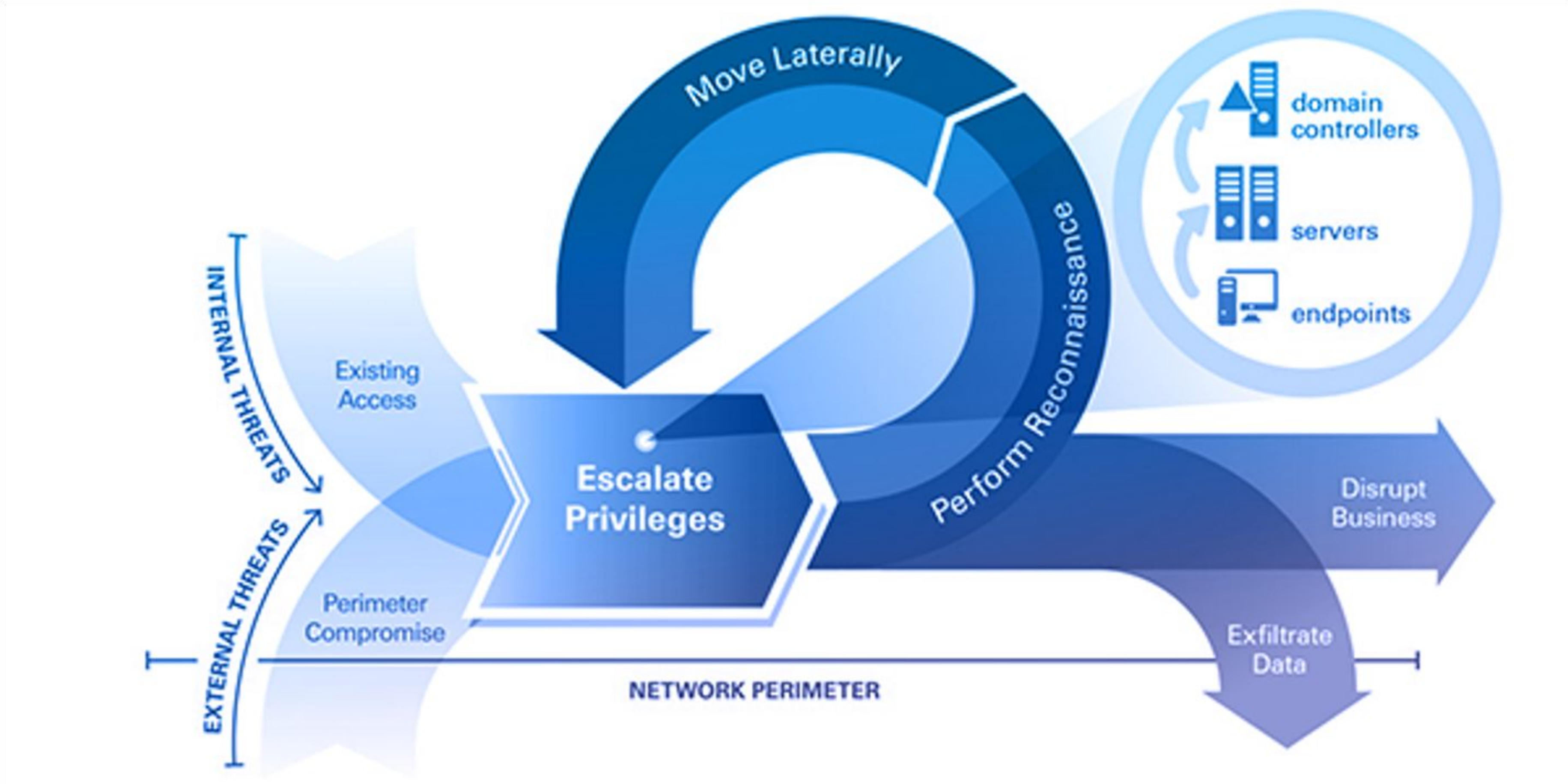
The Investigative Process

- Communications
  - Contact Information
  - On-Call Information
  - Incident Reporting Mechanisms
  - Issues Tracking Software

The Investigative Process

- Communications
  - Encryption Software
  - War Room
  - Secure Storage Facility

Attack Lifecycle


Move Laterally
domain controllers
servers
endpoints
INTERNAL THREATS
Existing Access
Escalate Privileges
Perform Reconnaissance
Disrupt Business
EXTERNAL THREATS
Perimeter Compromise
Exfiltrate Data
NETWORK PERIMETER

The Investigative Process

- Attack Vectors

The Investigative Process

- Attack Vectors
  - External Removable Media
  - Web Based Attacks
  - Email Attacks
  - Impersonation

The Investigative Process

- Attack Vectors
  - Improper Usage
  - Loss of theft of equipment
  - etc.

The Investigative Process- Signs of An Incident

- Precursors
    - Web Server logs indicate the presence of unauthorized vulnerability scanning
    - Announcement of a new Relevant Vulnerability
    - Threat group stating private or publicly they are targeting an organization

The Investigative Process- Signs of An Incident

- Indicators of Compromise

The Investigative Process- Signs of An Incident

- Indicators of Compromise
  - Alerts from a NIDS of HIDS
  - Suspicious Log / Audit Log entries for key services
  - Configuration Changes
  - Multiple Failed login attempts

The Investigative Process

- Analysis
  - Profile Networks and Systems
  - Baseline Normal Behavior
  - Perform Event Correlation
  - Maintain and use a knowledge base of information

The Investigative Process

- Analysis
  - Use the internet for research
  - Collect Additional data
  - Filter the data
  - Get help from others

The Investigative Process

- Documentation
  - Current Status of the Incident
  - Summary of the Incident
  - Indicators of the Incident
  - Related Incidents

The Investigative Process

- Documentation
  - Actions taken by incident handlers
  - Chain of Custody (if applicable)
  - Related Impact Assessments
  - List of Gathered Evidence
  - Next Steps Taken

The Investigative Process

- Prioritization (THIS IS CRITICAL)
  - Functional Impact
    - Impact the incident will have on IT systems
  - Information Impact
    - Impact on CIA

The Investigative Process

- Prioritization (THIS IS CRITICAL)
    - Recoverability
        - Size of incident, degree of compromise, what it affects will all determine amount of resources necessary for recovery

The Investigative Process

- Notification
  - Key Stakeholders must be notified of the incident severity and impacts
  - Compliance Bodies may need to be notified
  - Authorities may also need to be notified

The Investigative Process

- Containment
  - Strategies vary
    - must balance the need to prevent additional damage or theft with need to maintain and collect evidence

The Investigative Process

- Containment
  - Premature Containment can lead to an adversary not being fully “evicted”
  - Must include root cause analysis

The Investigative Process

- Evidence Collection
  - Time to figure out what happened!
  - Identify
    - Attacking hosts
    - Root Causes
  - Build a timeline from the root cause of the incident

The Investigative Process

- Eradication and Recovery
    - Eradication
        - Removing Adversary Access
    - Recovery
        - Ensuring systems are functioning within expected parameters

The Investigative Process

- Eradication and Recovery
  - Any strategy needs to balance business capabilities against attacker access based on evidence gathered
  - Phased approaches generally work better
  - DON’T FORGET TO ADDRESS THE ROOT CAUSE

The Investigative Process

- Lessons learned
  - What happened, when?
  - Did the staff and organizations perform as expected?
  - What would the staff do differently next time?

The Investigative Process

- Lessons learned
    - What corrective actions can prevent similar incidents in the future?

The Investigative Process

- Post incident analysis
  - Functional Impact, Information Impact, Recoverability
  - Did we make the right call?

Digital Evidence/ Capturing Digital Evidence

Digital Evidence/ Capturing Digital Evidence

- Volatile VS Non-Volatile Evidence
  - Volatile

Digital Evidence/ Capturing Digital Evidence

- Volatile VS Non-Volatile Evidence
  - Volatile
    - Does not persist across power cycles
    - Example: RAM

Digital Evidence/ Capturing Digital Evidence

- Volatile VS Non-Volatile Evidence
  - Non- Volatile

Digital Evidence/ Capturing Digital Evidence

- Volatile VS Non-Volatile Evidence
  - Non- Volatile
    - DOES persist across power cycles
    - Example: Hard drive contents

Digital Evidence/ Capturing Digital Evidence

- Capturing Non-Volatile Evidence
    - Need to determine how to:
        - Access the data
        - Power on the device
    - Implement Write Blockers

Digital Evidence/ Capturing Digital Evidence

- Physical Disk Capture
  - Pros:
    - Might get deleted files
    - Can parse the entire “raw” disk and data structures

Digital Evidence/ Capturing Digital Evidence

- Physical Disk Capture
  - Cons:
    - Capture used AND “unused” disk space
    - Time Consuming
    - LARGE output file

Digital Evidence/ Capturing Digital Evidence

- Logical Disk Capture (capture logical contents of drive)
  - Pros:
    - Get all files from OS’s point of view
    - Quick
    - Smaller output files

Digital Evidence/ Capturing Digital Evidence

- Logical Disk Capture (capture logical contents of drive)
  - Cons:
    - Won’t get “unused” disk space
    - No chance of recovering deleted files

Digital Evidence/ Capturing Digital Evidence

- Capturing Volatile Evidence
  - Really we’re looking at RAM
  - RAM does not persist across power cycles
  - Need to interact with a running system
  - Typically done remotely over SSH using RAM capture tools (Volexity Surge)

Digital Evidence/ Capturing Digital Evidence

- Capturing Volatile Evidence
  - Considerations
    - Need admin access
    - You could be creating new files on disk
    - You can fill a disk and crash the machine

Memory Forensics

- What is it??
  - Volatile Evidence
  - Information we can get

Memory Forensics

- What is it??
  - Volatile Evidence
  - Information we can get
    - Running (and sometimes dead) processes
    - Network Connections
    - Memory Mapped Files

Memory Forensics

- What is it??
  - Volatile Evidence
  - Information we can get
    - User logins and credentials
    - Cached Files
    - AND MORE!

Memory Forensics

- WHY?
  - Can be the fastest way to find extract malware running on a system
  - Ability to access elements that aren’t logged
  - Data transfer Volumes
  - Interhost communication and lateral movement

Memory Forensics

- WHY?
  - Command and Control activity (C2)
  - Remote Access
  - Difficult to tamper with

Volatility

- Modular framework
- Written in Python
- Runs on Windows, Mac, and Linux
- Extensible and Scriptable API
- Community modules

Volatility

- IT DOES NOT:
  - Collect memory samples
  - Have a GUI
  - Claim to be bug free
  - Support every operating system out of the box

Volatility

- Plugins
  - Pretty dope
  - Don’t work with every version of Volatility
  - Don’t work with every target operating system
  - Over 200 analysis plugins

Virus Total

- Website that lets you upload suspicious files, domains, IPs and URLs to detect malware and other breaches
- Can be really useful in Digital forensics
- Might come in handy in one of the labs

Cyber Chef

- Called the “Cyber Swiss Army Knife”
- Its “a web app for encryption, encoding, compression and data analysis”
- Will be helpful today!

Goldfynch PST Viewer

- Online tool that lets you read the contents of a pst file
- PST file is a “Personal Storage Table”
- Microsoft programs use them to store
    - Emails
    - Contacts
    - Calendar Events

Helpful Volatility Plugins

- Imageinfo/windows.info
  - gives us information on the disk image (i.e os profile)
- pslist
  - lists the running processes

Helpful Volatility Plugins

- netscan
  - what is process are connected to the internet
- malfind
  - potentially malicious running processes
- pstree
  - shows a process tree

Helpful Volatility Plugins

- memmap/procdump
  - dumps data for a target process into a dmp file
- dumpfiles
  - dumps all the files associated with a process

Things to look out for

Things to look out for/ remember

- Generally speaking code operates inside of a process
- Process can create another process do something
    - This is called a child process
    - Child processes can only have one parent
    - Parents can have more than one child

Things to look out for/ remember

- Code on Windows is executed through .exe or .dll files
- Executed directly through the command line or other binaries
- It is common for attackers to run malware as .dll or library
    - harder to detect

Things to look out for/ remember

- Malware can hide in executable scripting languages
    - Powershell, Jscript, VBScript

Set Up

Set Up

- cd <directory name> -> change directory (cd with no directory goes back to home)
- ls -> list files
- cd .. -> move up a directory
- mkdir <directory name> -> makes a new directory

Set Up

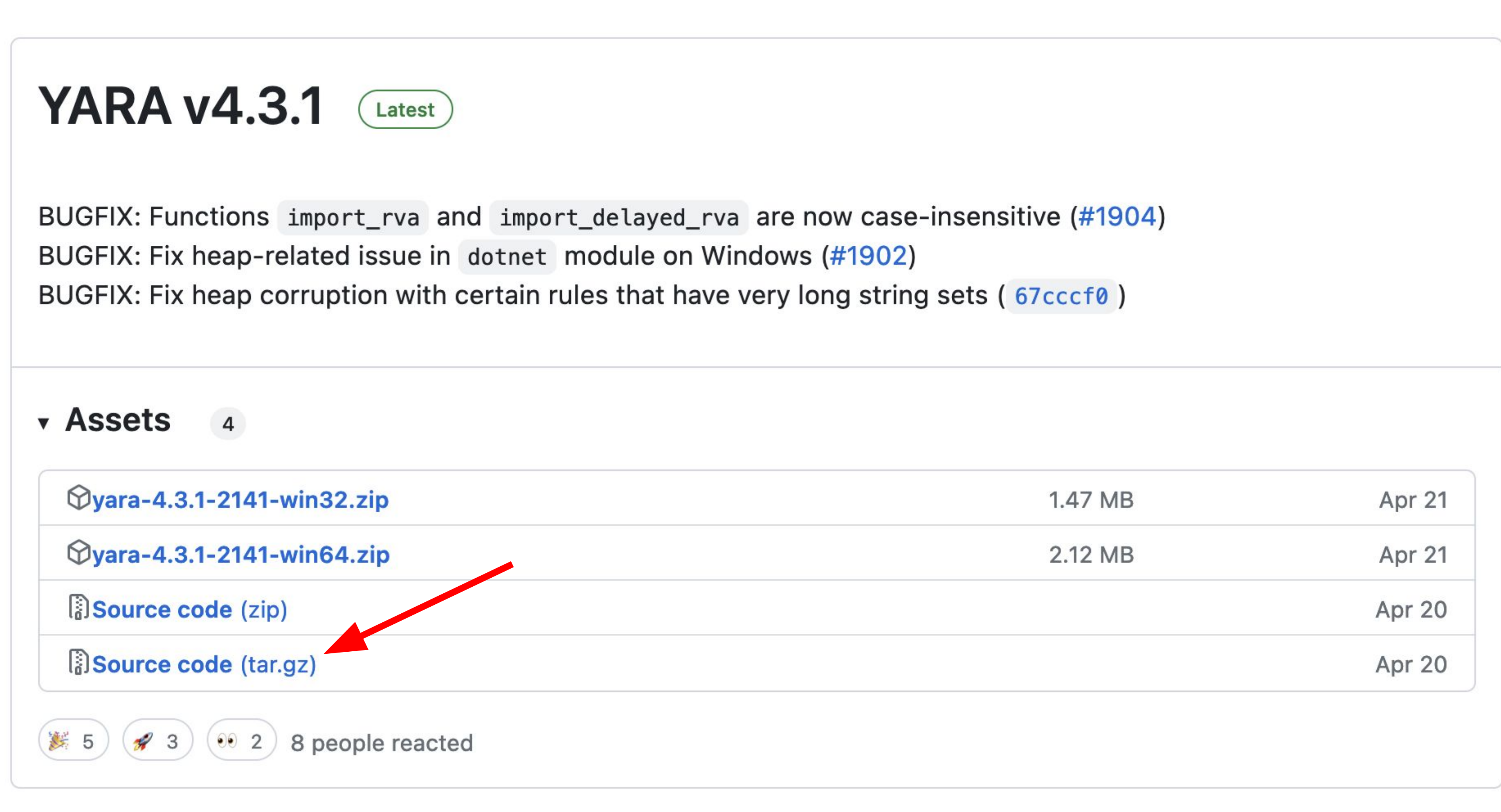
- Log in to your AWS Workspace provided by WSU
- Open Terminal
- sudo yum update
- sudo yum upgrade
- sudo yum install autoconf automake libtool make gcc pkg-config libhdf5-dev

Set Up

-
  ```
  sudo yum install libtiff5-dev libjpeg8-dev libopenjp2-7-dev zlib1g-dev libfreetype6-dev liblcms2-dev libwebp-dev tcl8.6-dev tk8.6-dev python3-tk libharfbuzz-dev libfribidi-dev libxcb1-dev
  ```

Set Up

- Download Yara from tarball: https://github.com/VirusTotal/yara/releases



YARA v4.3.1

BUGFIX: Functions `import_rva` and `import_delayed_rva` are now case-insensitive (#1904)
BUGFIX: Fix heap-related issue in `dotnet` module on Windows (#1902)
BUGFIX: Fix heap corruption with certain rules that have very long string sets (`67cccf0`)

▾ Assets 4

yara-4.3.1-2141-win32.zip	1.47 MB	Apr 21
yara-4.3.1-2141-win64.zip	2.12 MB	Apr 21
Source code (zip)		Apr 20
Source code (tar.gz)		Apr 20

Set Up

```
tar -zxf yara-4.3.1.tar.gz
cd yara-4.3.1
./bootstrap.sh
./configure
make
sudo make install
```

Set Up

- make check
- **Test a yara rule**
- echo "rule dummy { condition: true }" > my_first_rule
  yara my_first_rule my_first_rule
- **IF “DUMMY MY_FIRST_RULE” IS NOT OUTPUT CALL ME OR AUSTIN OVER**

Set Up

- **Install Python 2.7**
- sudo yum install -y build-essential git libdistorm3-dev yara libraw1394-11 libcapstone-dev capstone-tool tzdata
- sudo yum install -y python2 python27-devel libpython2-dev

Set Up

- curl https://bootstrap.pypa.io/pip/2.7/get-pip.py --output get-pip.py
- sudo python2.7 get-pip.py
- sudo python2.7 -m pip install -U setuptools wheel
- sudo yum install openssl-devel

Set Up

- python2.7 -m pip install -U distorm3 yara-python pycrypto pillow openpyxl ujson pytz ipython capstone
- sudo python2.7 -m pip install yara-python

Set Up

- **Need to create a symbolic link between libyara.so to usr/local/lib (look in usr/lib)**
- sudo ln -s /usr/local/lib/libyara.so /usr/lib/libyara.so
- **Install Python3**
- sudo amazon-linux-extras install python3.8
- sudo yum install python38-devel python38-wheel

Set Up

- sudo python3.8 -m pip install --upgrade setuptools
- python3.8 -m pip install -U distorm3 yara-python pycrypto pillow openpyxl ujson pytz ipython capstone
-

Set Up

- **Go back to home directory (cd)**
- git clone https://github.com/volatilityfoundation/volatility3.git
- cd volatility3
- python3 setup.py build
- sudo python3 setup.py install
- python3 vol.py -h