



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
Posts and Telecommunications Institute of Technology

# PHÂN TÍCH MÃ ĐỘC

**KHOA AN TOÀN THÔNG TIN**  
**TS. ĐÌNH TRƯỜNG DUY**



HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
Posts and Telecommunications Institute of Technology

# PHÂN TÍCH MÃ ĐỘC

## Phân tích động

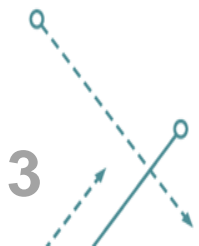
KHOA AN TOÀN THÔNG TIN

TS. ĐINH TRƯỜNG DUY

# Giới thiệu

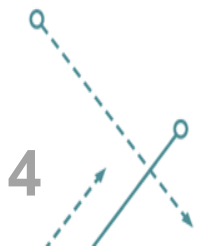
## Phân tích mã độc dựa trên kỹ thuật phân tích động

1. Tổng quan về phân tích động
2. Một số công cụ phân tích động phổ biến
3. Quy trình phân tích động
4. Đánh giá về phân tích động
5. Thực hành phân tích động sử dụng công cụ
  - 5.1 chuẩn bị môi trường thực nghiệm
  - 5.2 chuẩn bị mã độc, chạy



# Tổng quan về phân tích động

- Phân tích động (phân tích hành vi) liên quan đến việc phân tích một mẫu bằng cách thực thi nó trong một môi trường cô lập và theo dõi các hành vi của nó (hoạt động, tương tác và tác động của nó lên hệ thống).
- → Theo dõi những chức năng, hoạt động thật sự của mã độc



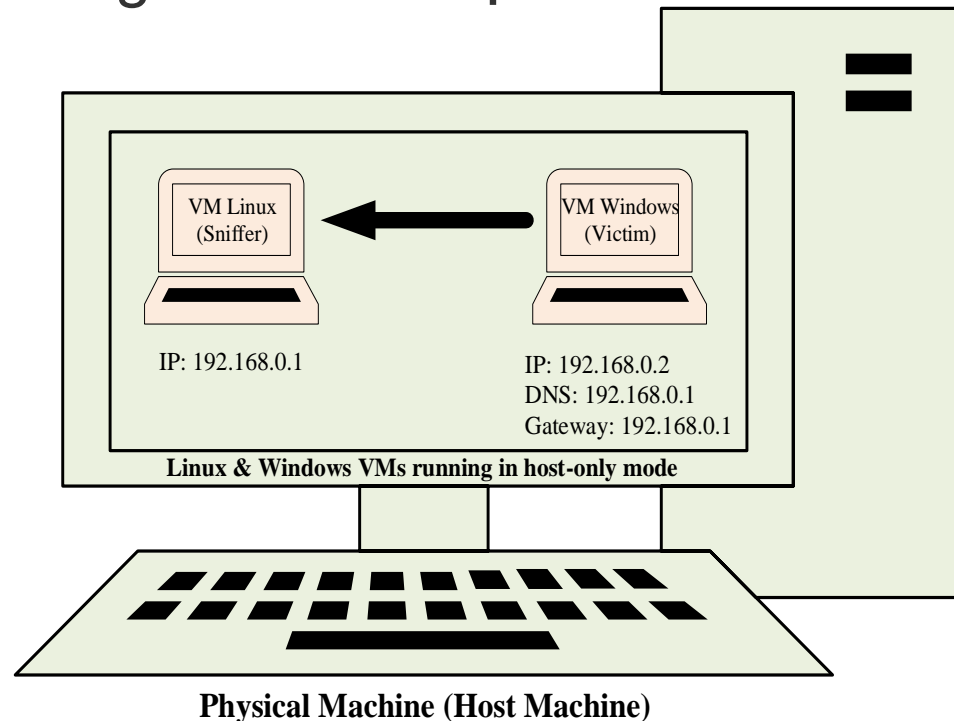
# Tổng quan về phân tích động

- Thường được thực hiện sau phân tích tĩnh cơ bản.
- Một cách hiệu quả để xác định chức năng của phần mềm độc hại.
- Cung cấp thông tin quý giá.
- Hữu ích nhưng không tiết lộ tất cả các chức năng.



# Tổng quan về phân tích động

- Cài đặt mỗi trường lab cách biệt



<https://www.malwaretech.com/2017/11/creating-a-simple-free-malware-analysis-environment.html>

<https://blog.christophetd.fr/malware-analysis-lab-with-virtualbox-inetsim-and-burp/>

# Sandboxes & Online Malware Analysis Tools

- Để chạy các chương trình không đáng tin cậy trong một môi trường an toàn
  - Thông tin đã thu thập có thể phục vụ như một chỉ báo xâm nhập (IOC)
  - dễ dàng hiểu được output
- Các dạng của sandbox
  - Tự xây dựng với các công cụ tự cài đặt
  - Sử dụng sandbox có trả phí
  - Sử dụng sandbox mã nguồn mở
- <https://github.com/sroberts/awesome-iocs>
- <https://zeltser.com/automated-malware-analysis/>
- <https://medium.com/@su13ym4n/15-online-sandboxes-for-malware-analysis-f8885ecb8a35>

# Sandboxes & Online Malware Analysis Tools

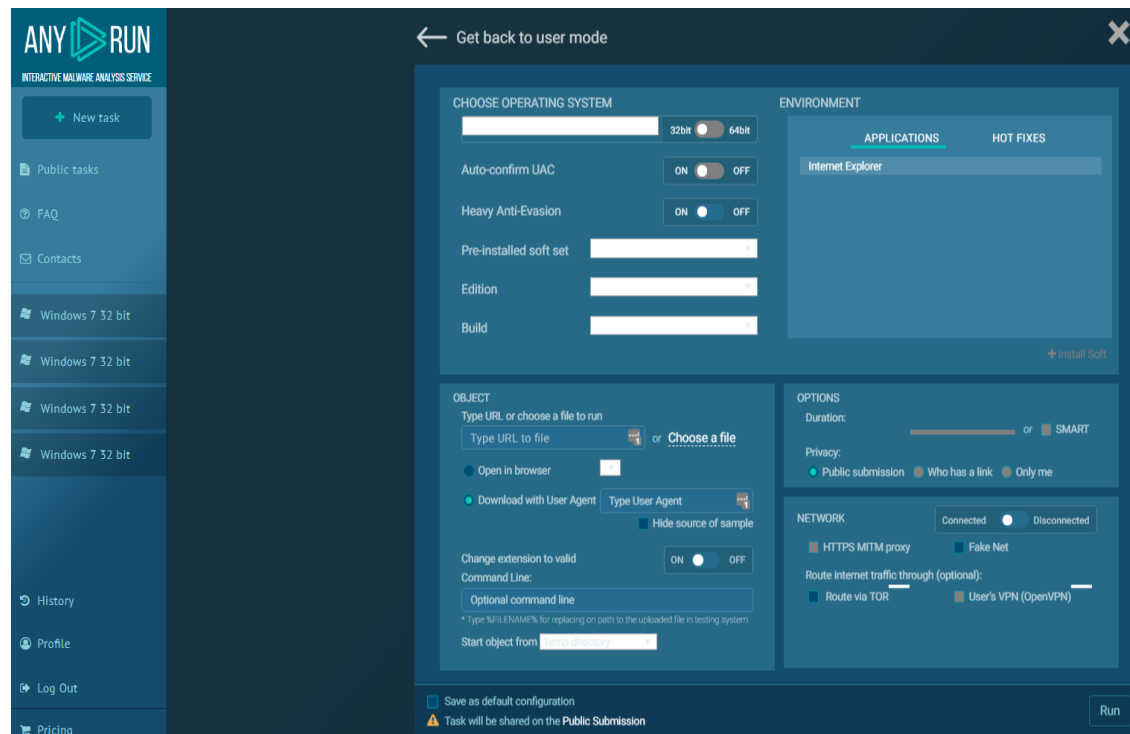
- Nhược điểm
  - Có thể không cung cấp hết các lựa chọn
  - Có thể không ghi lại tất cả các sự kiện do thời gian chờ lâu
  - Mã độc có thể phát hiện ra là đang chạy trên máy ảo và dừng hoạt động hoặc hoạt động khác đi.
  - Một số phần mã độc yêu cầu một số registry hoặc tệp tin cụ thể trên hệ thống mà có thể không tìm thấy trong môi trường sandbox.
  - Nếu phần mã độc là một tệp DLL → cần cung cấp các tùy chọn/đối số bổ sung.
  - OS của sandbox có thể không phù hợp cho dòng mã độc nghiên cứu
  - Thông tin nhạy cảm có thể bị tiết lộ



# Sandboxes & Online Malware Analysis Tools

## 1. Any.run (<https://app.any.run>): Free & Premium

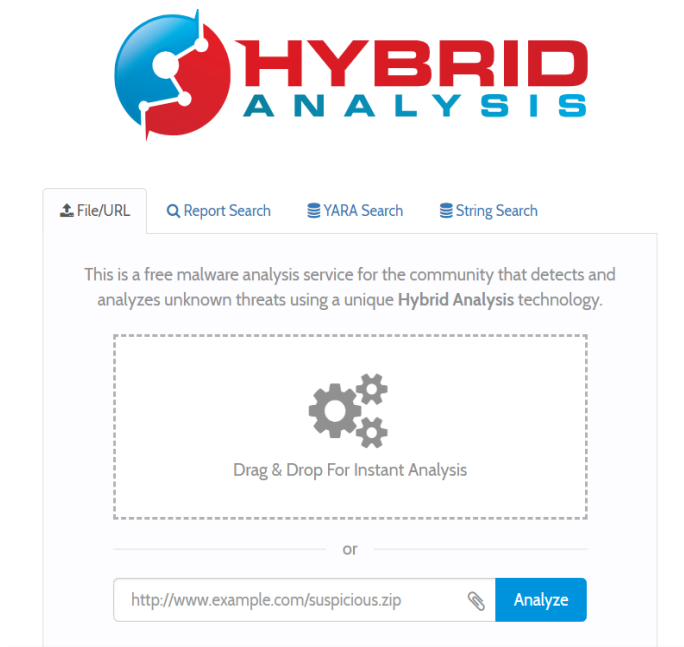
- Any.Run cho phép người dùng tải lên một tệp và tương tác trực tiếp với môi trường sandbox trong khi nó phân tích tệp.
- Không cần cài đặt.
- Xem quá trình điều tra và điều chỉnh khi cần thiết.



# Sandboxes & Online Malware Analysis Tools

## 2. Hybrid-analysis (<https://www.hybrid-analysis.com/>): Free

- Hybrid Analysis kết hợp phân tích tĩnh và động để phát hiện hành vi độc hại trong quá trình thực thi.
- Kích thước tối đa cho phép tải lên là 100 MB.



### Incident Response

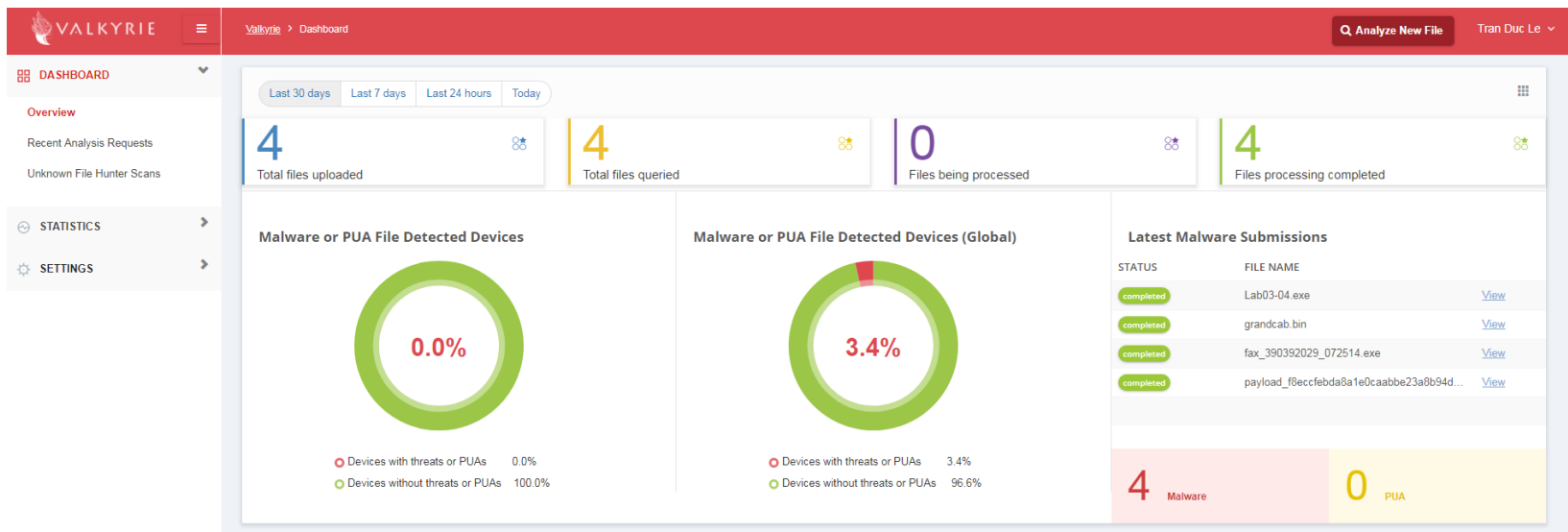
#### Risk Assessment

Remote Access	Reads terminal service related keys (often RDP related)
Fingerprint	Reads the active computer name

# Sandboxes & Online Malware Analysis Tools

## 3. Valkyrie (<https://valkyrie.comodo.com/dashboard/>): Free

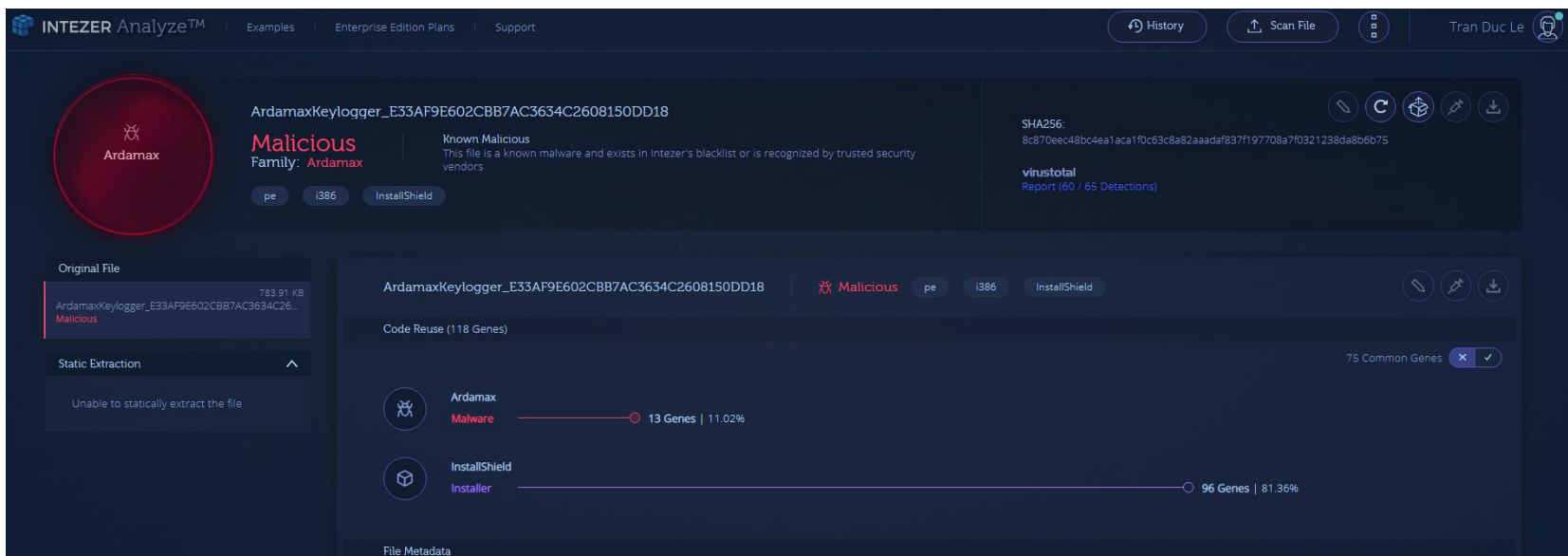
- Phân tích toàn bộ hành vi của một tệp trong quá trình thực thi do đó nó hiệu quả hơn trong việc phát hiện các mối đe dọa zero-day mà hệ thống phát hiện dựa trên chữ ký của các phần mềm antivirus không phát hiện được.
- Không cần cài đặt, chỉ cần tải lên tệp để phân tích.
- Phân tích Tĩnh & Động
- Kích thước tối đa cho phép tải lên là 150 MB



# Sandboxes & Online Malware Analysis Tools

## 4. Intezer Analyze (<https://analyze.intezer.com/#/analyze>): Free & Premium


- Phân tích và phân loại phần mã độc thông qua code DNA mapping → Intezer có khả năng phát hiện việc tái sử dụng mã nguồn từ các phần mã độc đã biết, cũng như mã nguồn đã xuất hiện trong các ứng dụng đáng tin cậy.
- Định dạng được hỗ trợ: các tệp tin thực thi Windows như .exe, .dll, .sys...; các tệp tin thực thi Linux - x86, x64 ELF; không hỗ trợ các tài liệu như .doc, .ppt, .xls, .odt...
- Kích thước tối đa cho phép tải lên là 20 MB.




The screenshot shows the Intezer Analyze web interface. The top navigation bar includes links for Examples, Enterprise Edition Plans, and Support, along with buttons for History, Scan File, and a user profile for Tran Duc Le. The main content area displays the analysis results for a file named 'ArdamaxKeylogger\_E33AF9E602CBB7AC3634C2608150DD18'. The file is identified as 'Malicious' and belongs to the 'Ardamax' family. The interface shows various analysis results, including SHA256, VirusTotal report, and a detailed breakdown of code reuse (118 Genes) showing 13 Genes (11.02%) for 'Ardamax Malware' and 96 Genes (81.36%) for 'InstallShield Installer'.


# Sandboxes & Online Malware Analysis Tools

## 5. Vichcek (<https://vichcek.ca/submitfile.php>): Free

 **VICHECK**

[Submit File](#) [Hash Search](#) [Contact Us](#) [Tools](#)

 E-Mail Address

 Comments or Email Header

[+ Add files...](#)

[Start upload](#)

[Cancel upload](#)

Drag your files for analysis onto the page. Upload them to get a malware/virus detection report determined using a variety of tools.

[Display Combined Report](#)

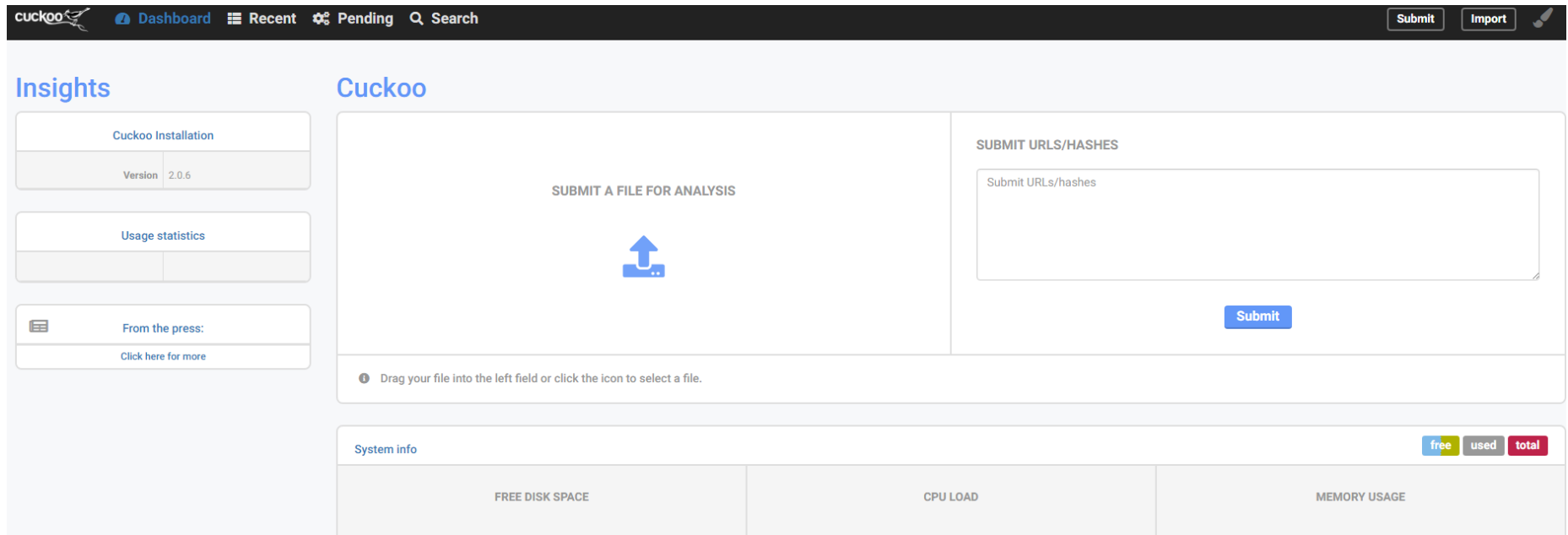
### Malware Sample Submission Notes

- The maximum file size for uploads using this form is **29M**.
- Only image files (**JPG, GIF, PNG**) are displayed with a preview.
- Some analysis results may take a few minutes to generate depending on CPU load.
- Record the file hash code to use in other search/reporting utilities if desired.
- For email analysis, please try to include the full email headers wherever possible:
  - You may need to view headers then copy and paste them into the forwarded message.

# Sandboxes & Online Malware Analysis Tools

## 6. Online Cuckoo Sandbox

- <https://cuckoo.cert.ee/>
- <http://sandbox.pikker.ee/>



The screenshot displays the Cuckoo Sandbox web interface. The top navigation bar includes links for Dashboard, Recent, Pending, and Search, along with Submit and Import buttons. The main content area is divided into two sections: Insights and Cuckoo. The Insights section on the left contains a Cuckoo Installation box showing Version 2.0.6, a Usage statistics box, and a From the press: section with a link to Click here for more. The Cuckoo section on the right features a large box for submitting a file for analysis, a text input field for submitting URLs/hashes, and a Submit button. A footer section titled System info provides details on Free Disk Space, CPU Load, and Memory Usage.

FREE DISK SPACE	CPU LOAD	MEMORY USAGE

# Sandboxes & Online Malware Analysis Tools

## 7. SNDBOX

- <https://app.sndbox.com>

SNDBOX

Install\_LiveManagerPlayer. vir

OVERVIEW STATIC ANALYSIS DYNAMIC ANALYSIS NETWORK

Search...

83% Malicious

VERDICT: MALICIOUS

GENERAL INFORMATION

METADATA

File Name	Install_LiveManagerPlayer.exe.vir
Tags	+
Upload Date	19/02/2019 19:10 (a minute ago)
File size	4.71 MB
MD5	845b54844e8be6c912947bdb8798c927
SHA1	2f243455274d41e259d19ce7f81035d0f4faedaf
SHA256	91d8e75e88d401e64b609e637fae7a9594df6ed0e600f3c63bbb69d0cdec21f4
File type	PE32 executable (GUI) Intel 80386, for MS Windows, RAR self-extracting archive

NAVIGATION

- General Information
- Signatures
- Threat Detection Alliance
- Dynamic

PRIVACY DISCLAIMER

This analysis is public. Therefore, it may be accessed by anyone.

ENVIRONMENT SETUP SETTINGS

- Execution time set to 120 seconds
- Timebombs enabled with mode calm
- Command line is disabled

Windows v7.1.2  
Windows 7 ultimate with SP1

Installed software  
Click to view

# Sandboxes & Online Malware Analysis Tools

## 7. Các phần mềm khác

- <http://www.malwaretracker.com/pdf.php> (PDF)
- <https://andrototal.org/> (Android)
- <https://apkscan.nviso.be/> (Android)
- <https://amaaas.com/> (Android)
- <https://drakvuf.com/> (Need to install)
- <https://cuckoosandbox.org/> (Need to install)
- <https://github.com/monnappa22/Limon> (Linux malware)
- <https://www.misp-project.org/> (MISP – Need to install)
- <http://bsa.isoftware.nl/> (Need to install + Sandboxes)
- <https://github.com/sankio/H2Sandbox> (H2Sandbox)
- <https://certsocietegenerale.github.io/fame/> (FAME Automates Malware Evaluation)



## Running malware

- Tập trung vào các dạng file mà mã độc thường nhắm đến: EXEs & DLLs
- **Tại sao kẻ tấn công lại sử dụng DLLs:**
  - Một tệp tin DLL không thể được chạy bằng cách nhấp đúp chuột → DLL cần một tiến trình chủ để chạy. Mã độc có thể tải DLL của mình vào bất kỳ quy trình nào, bao gồm cả quy trình hợp pháp → Ẩn các hoạt động của mã độc.
  - Khi một tệp tin DLL được tải vào bộ nhớ của một tiến trình, DLL sẽ có quyền truy cập vào toàn bộ không gian bộ nhớ của tiến trình → Có khả năng thay đổi chức năng của tiến trình.
  - Phân tích một tệp tin DLL khó hơn so với phân tích một tệp tin EXE.
  - Lưu ý: Sau khi tải DLL, phần mềm độc hại có thể xóa chính nó → Khi thực hiện phân tích có thể chỉ tìm thấy tệp tin DLL.

# Phân tích DLL sử dụng *rundll32.exe*

```
C:\>rundll32.exe <full_path_to_DLL>, <export_function> <optional arguments>
```

```
C:\>rundll32.exe <full_path_to_DLL>, #<ordinal number> <optional arguments>
```

- **full\_path\_to\_DLL**: Yêu cầu chỉ định đường dẫn đầy đủ đến tệp tin DLL và đường dẫn này không được chứa khoảng trắng hoặc ký tự đặc biệt.
- **export\_function**: Đây là một hàm trong DLL sẽ được gọi sau khi DLL được tải vào.
- **optional arguments**: Các đối số tùy chọn. Nếu có thì những đối số này sẽ được truyền vào hàm xuất (export function) khi nó được gọi.

• Ví dụ

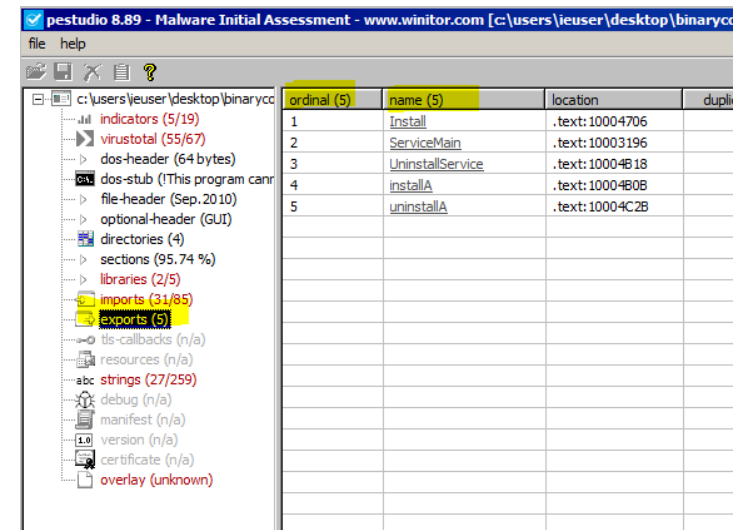
```
C:\>rundll32.exe lab03-02.dll, Install
```

```
C:\>rundll32.exe lab03-02.dll, #1
```

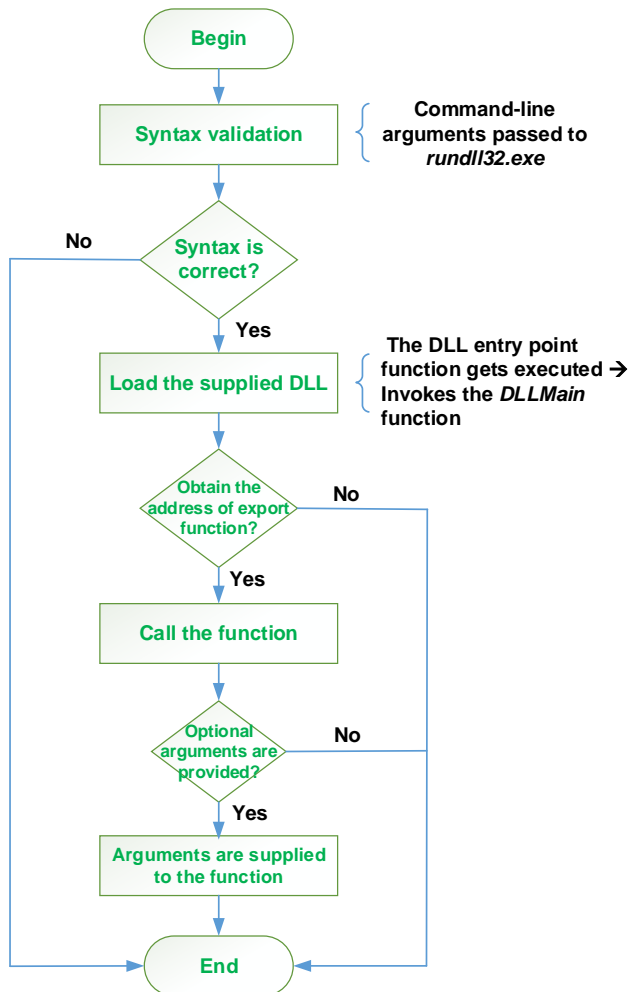
```
C:\>rundll32.exe abcd.dll, _flushfile@16 file_to_delete.txt
```

- Để chạy tự động tất cả **export functions**  
DLLRunner tool

<https://github.com/Neo23x0/DLLRunner>



# Quy trình hoạt động của *rundll32.exe*



Nếu một DLL không có hàm xuất (export function)?

- Kẻ tấn công có thể triển khai các chức năng độc hại (như keylogging, đánh cắp thông tin...) trong hàm *DLLMain* mà không xuất bất kỳ hàm nào.
- Tất cả các chức năng độc hại có thể được triển khai trong hàm *DLLMain*

Chạy câu lệnh

C:>\rundll32.exe abcd.dll, **test**

→ Error “Missing entry: test” tuy nhiên DLL vẫn được thực hiện.

# Công cụ phân tích động cơ bản

- Các loại giám sát khác nhau được thực hiện trong quá trình phân tích động:
  - **Process monitoring** – giám sát tiến trình
  - **File system monitoring** – giám sát hệ thống tệp
  - **Registry monitoring** – giám sát registry
  - **Network monitoring** – giám sát mạng

Lưu ý: các công cụ sử dụng cần chạy dưới quyền admin



# Công cụ phân tích động cơ bản

- **Process monitoring – giám sát tiến trình**
  - Giám sát hoạt động của tiến trình
  - Kiểm tra các thuộc tính có được từ kết quả tiến trình trong khi thực thi mã độc
  - Các công cụ: Process Hacker, Process Monitor, Process Explorer
- **File system monitoring – giám sát hệ thống tệp**
  - Giám sát theo thời gian thực hoạt động của hệ thống tệp trong khi thực thi mã độc
  - Các công cụ: Process Monitor, Noriben



# Công cụ phân tích động cơ bản

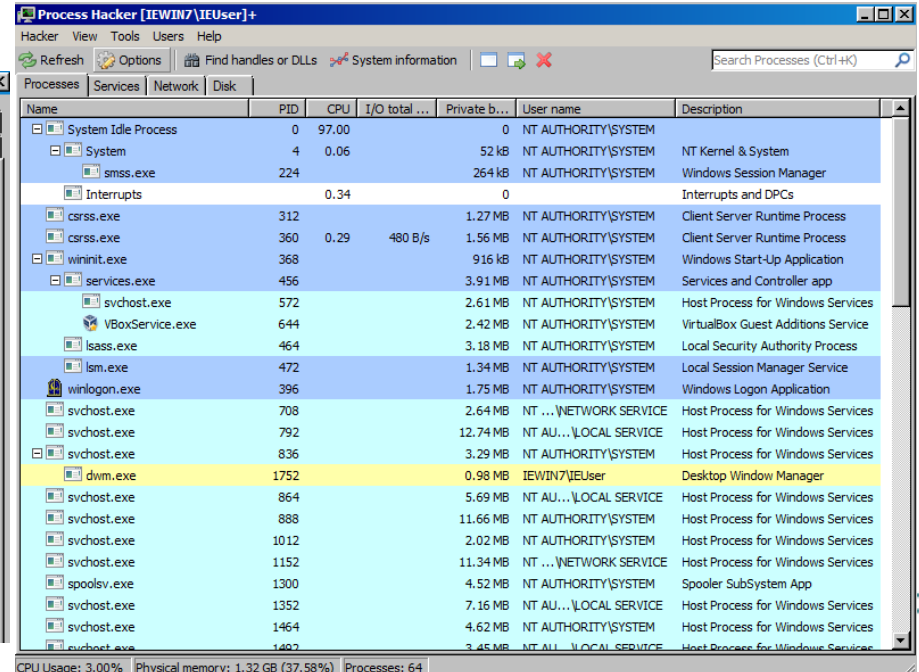
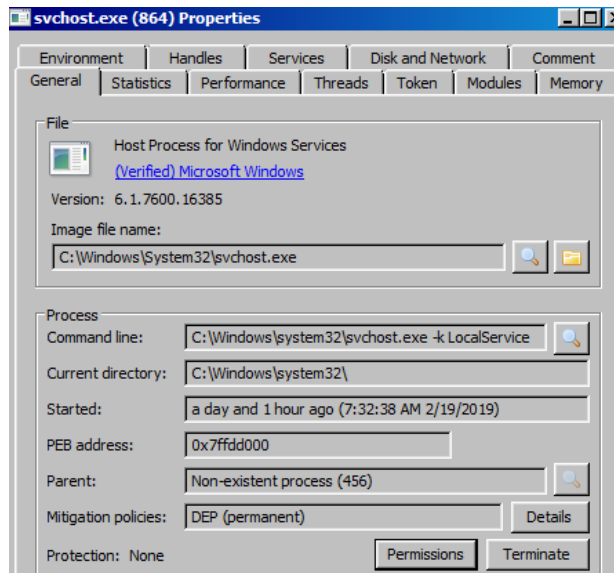
- **Registry monitoring – giám sát registry**
  - Giám sát các khóa registry được truy cập, chỉnh sửa và dữ liệu registry đang được đọc/ghi bởi tập nhị phân độc hại
  - Các công cụ: Regshot, Process Monitor
- **Network monitoring – giám sát mạng**
  - Giám sát lưu lượng truy cập thời gian thực đến và đi từ hệ thống trong quá trình thực thi mã độc.
  - Các công cụ: Wireshark, INETsim, Netcat, ApateDNS, Fakenet-NG



# Các công cụ để giám sát tiến trình

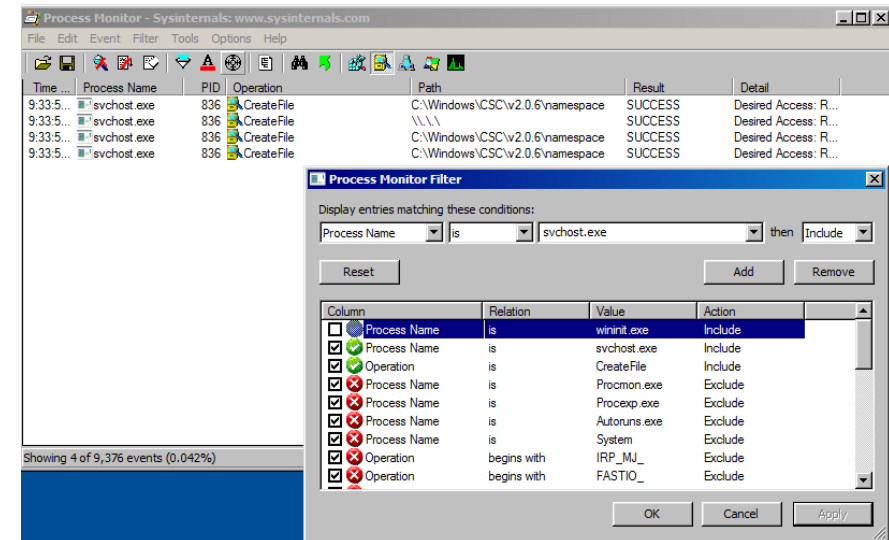
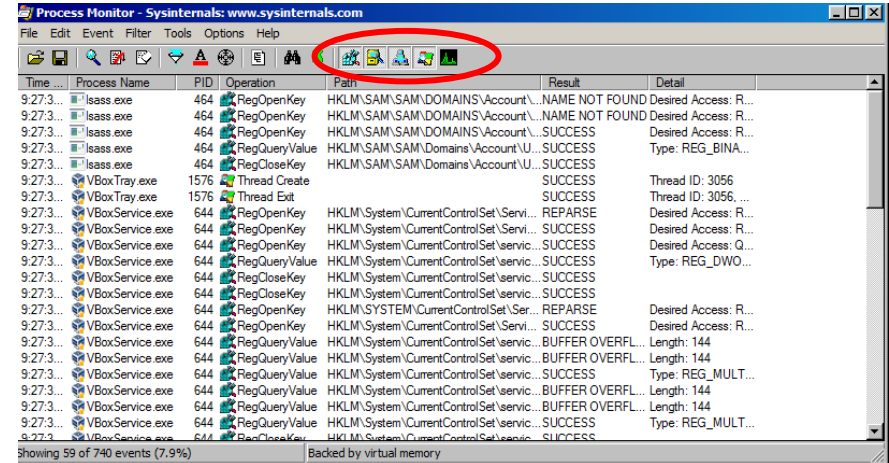
- **Process Hacker** là một công cụ tuyệt vời để kiểm tra các quy trình đang chạy trên hệ thống và kiểm tra các thuộc tính của quy trình. Ngoài ra, nó cũng cung cấp khả năng khám phá các dịch vụ, kết nối mạng và hoạt động của ổ đĩa → giúp cho việc xác định các tiến trình độc hại mới được tạo ra thông qua process name, process ID.

Right-click  
vào một tiến  
trình →  
Properties  
→ Examine  
various  
process  
attributes



# Các công cụ để giám sát tiến trình

- **Process Monitor (ProcMon)** là một công cụ giám sát các hoạt động liên quan đến registry, hệ thống tệp, mạng, tiến trình và luồng trên hệ thống.
  - Nó thu thập thông tin bằng cách giám sát các lời gọi hệ thống và ghi lại các sự kiện trong thời gian thực.
  - Sử dụng bộ nhớ RAM để lưu trữ các sự kiện được ghi lại cho đến khi nó được dừng → có thể làm cho máy ảo (VM) bị treo hoặc ảnh hưởng đến hiệu suất hệ thống.
  - Để giảm thông tin nhiễu → sử dụng bộ lọc (Filters)
    - Bộ lọc cho một mẫu malware cụ thể
    - Bộ lọc cho từng lời gọi hệ thống cụ thể (Ví dụ: RegSetValue, CreateFile...)
- những bộ lọc quan trọng khi phân tích mã độc là: Process Name, Operaton & Detail.





# Các công cụ để giám sát tiến trình

Ghi nhật ký hoạt động của hệ thống bằng *Noriben*

(<https://github.com/Rurik/Noriben>)

- Là một tập lệnh Python hoạt động cùng với Procmon giúp thu thập, phân tích và báo cáo các chỉ số thời gian chạy của phần mềm độc hại.
- Ưu điểm của việc sử dụng Noriben là nó có các bộ lọc mặc định giúp giảm thông tin nhiễu và cho phép tập trung vào các sự kiện liên quan đến phần mềm độc hại.
- Lưu kết quả dưới dạng text file (.txt) và csv file (.csv) trong cùng một thư mục. Text file chứa sự kiện được phân loại, còn csv file thì ghi các sự kiện theo thời gian

```

[==] Sandbox Analysis Report generated by Noriben v1.8.3
[==] Developed by Brian Baskin: brian @@ thebaskins.com @bbaskin
[==] The latest release can be found at https://github.com/Rurik/Noriben

[==] Execution time: 26.04 seconds
[==] Processing time: 1.45 seconds
[==] Analysis time: 47.03 seconds

Processes Created:
=====
[CreateProcess] svchost.exe:540 > "%WinDir%\system32\DllHost.exe /Processid:{E10F6C3A-Fl

File Activity:
=====
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools

```

```

[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools\Noriben-master
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools
[CreateFolder] Explorer.EXE:516 > %UserProfile%\Desktop\Tools

Registry Activity:
=====
[RegSetValue] svchost.exe:844 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\F
[RegSetValue] svchost.exe:844 > HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\F

Network Traffic:
=====
[UDP] System:4 > 192.168.0.255:137
[UDP] 192.168.0.2:137 > System:4
[UDP] svchost.exe:1144 > 192.168.0.1:53
[UDP] fe80:0:0:0:e877:aa98:4cff:9410:53988 > svchost.exe:1144
[UDP] svchost.exe:1144 > 224.0.0.252:5355
[UDP] fe80:0:0:0:e877:aa98:4cff:9410:57469 > svchost.exe:1144
[UDP] System:4 > 192.168.0.1:137

Unique Hosts:
=====
192.168.0.1
192.168.0.2
192.168.0.255
224.0.0.252
fe80

```



# Các công cụ để giám sát tiến trình

**Process Explorer (Procexp)** quản lý tiến trình. Các thông tin cung cấp:

- Danh sách các tiến trình đang chạy, DLLs được sử dụng bởi các tiến trình, các thuộc tính, quyền của tiến trình và thông tin chung của hệ thống
- Quản lý tiến trình: Có thể tắt hoặc khởi động lại các tiến trình, tìm kiếm thông tin trên mạng về tiến trình cụ thể, xem các thuộc tính và quyền của tiến trình, và xem các tệp và registry liên quan.
- Cho phép xem các liên kết giữa các tiến trình, bao gồm các tiến trình cha, tiến trình con, và các tiến trình chia sẻ tài nguyên.
- Có thể tìm kiếm các tiến trình cụ thể hoặc áp dụng bộ lọc để hiển thị chỉ các tiến trình đáp ứng các tiêu chí cụ thể.
- Cập nhật theo giây

Process Explorer - Sysinternals: www.sysinternals.com [IEWIN7\IEUser] (Administrator)

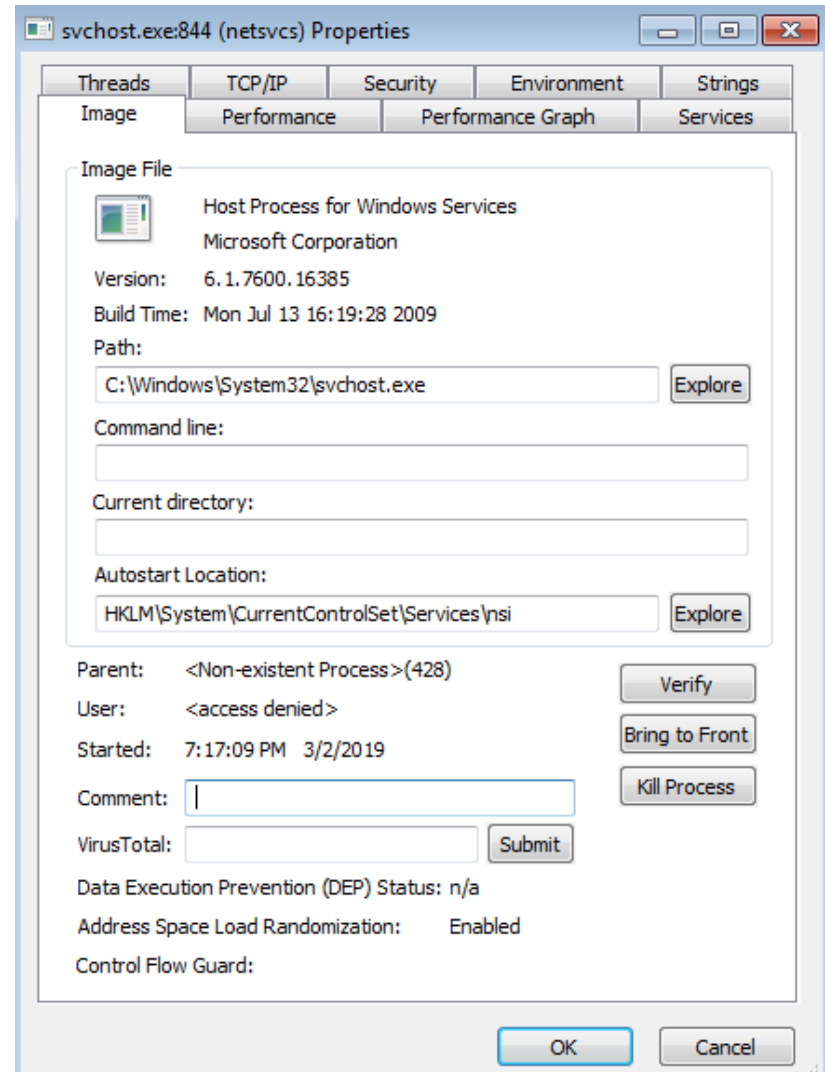
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		2,764 K	22,072 K	708	Host Process for Windows S...	Microsoft Corporation
svchost.exe		13,048 K	48,960 K	792	Host Process for Windows S...	Microsoft Corporation
audiodg.exe		13,676 K	8,992 K	2992	Windows Audio Device Grap...	Microsoft Corporation
svchost.exe		3,344 K	50,808 K	836	Host Process for Windows S...	Microsoft Corporation
dwm.exe		1,072 K	23,960 K	1752	Desktop Window Manager	Microsoft Corporation
svchost.exe		6,008 K	71,380 K	864	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.01	14,256 K	48,516 K	888	Host Process for Windows S...	Microsoft Corporation
taskeng.exe		984 K	3,800 K	2652	Task Scheduler Engine	Microsoft Corporation
svchost.exe		2,008 K	20,924 K	1012	Host Process for Windows S...	Microsoft Corporation
svchost.exe	0.03	11,524 K	41,728 K	1152	Host Process for Windows S...	Microsoft Corporation
spoolsv.exe		4,624 K	34,184 K	1300	Spooler Sub System App	Microsoft Corporation
svchost.exe		7,336 K	30,160 K	1352	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,736 K	73,696 K	1464	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,532 K	26,752 K	1492	Host Process for Windows S...	Microsoft Corporation
taskhost.exe	0.01	10,948 K	49,868 K	1652	Host Process for Windows T...	Microsoft Corporation
explorer.exe	0.15	53,108 K	90,668 K	1764	Windows Explorer	Microsoft Corporation
VBxTray.exe	0.01	1,560 K	30,356 K	1576	VirtualBox Guest Additions Tr...	Oracle Corporation
chrome.exe	1.87	74,432 K	165,060 K	3428	Google Chrome	Google Inc.
chrome.exe		1,040 K	26,164 K	3452	Google Chrome	Google Inc.
chrome.exe		956 K	29,904 K	3496	Google Chrome	Google Inc.
chrome.exe	3.82	19,568 K	153,480 K	1260	Google Chrome	Google Inc.
chrome.exe		29,928 K	127,408 K	1688	Google Chrome	Google Inc.
chrome.exe		26,332 K	111,668 K	1560	Google Chrome	Google Inc.
chrome.exe		40,588 K	129,204 K	3144	Google Chrome	Google Inc.
chrome.exe		18,100 K	101,368 K	3104	Google Chrome	Google Inc.
chrome.exe		26,220 K	110,420 K	3244	Google Chrome	Google Inc.
chrome.exe		29,904 K	118,548 K	1460	Google Chrome	Google Inc.
chrome.exe		28,408 K	114,892 K	3848	Google Chrome	Google Inc.
chrome.exe		18,416 K	101,400 K	3380	Google Chrome	Google Inc.
chrome.exe		17,608 K	101,192 K	2396	Google Chrome	Google Inc.
chrome.exe		18,068 K	100,864 K	2440	Google Chrome	Google Inc.
chrome.exe		18,128 K	100,700 K	2732	Google Chrome	Google Inc.
chrome.exe		17,984 K	101,172 K	3964	Google Chrome	Google Inc.
chrome.exe		17,276 K	100,164 K	1264	Google Chrome	Google Inc.
chrome.exe		17,020 K	100,028 K	2972	Google Chrome	Google Inc.
chrome.exe		17,528 K	100,908 K	2544	Google Chrome	Google Inc.
chrome.exe		16,864 K	100,048 K	3320	Google Chrome	Google Inc.
chrome.exe		16,372 K	100,056 K	3936	Google Chrome	Google Inc.
chrome.exe		30,388 K	120,292 K	1408	Google Chrome	Google Inc.
chrome.exe	< 0.01	30,172 K	71,068 K	632	Google Chrome	Google Inc.

CPU Usage: 8.48% Commit Charge: 18.83% Processes: 65 Physical Usage: 36.71%

# Các công cụ để giám sát tiến trình

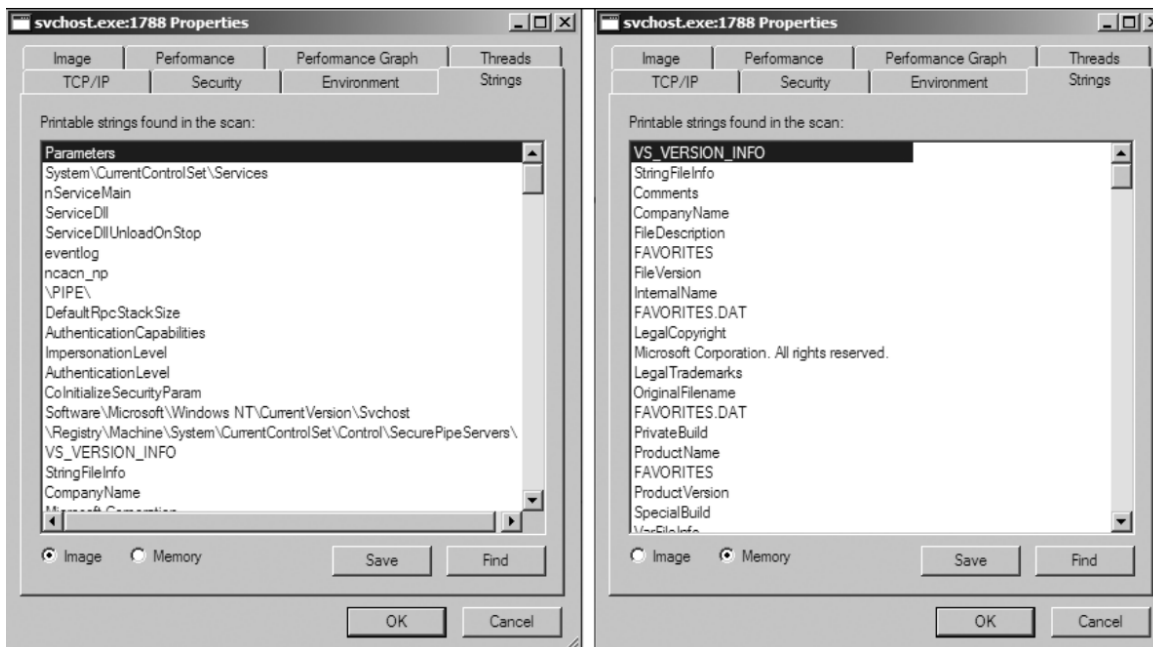
- **Threads tab:** tắt cả hoạt động của luồng
- **TCP/IP tab:** hiển thị các kết nối đang hoạt động hoặc các cổng đang lắng nghe.
- **Image tab:** cung cấp đường dẫn trên đĩa đến tệp thực thi của tiến trình

→ **Verify button:** xác minh tính toàn vẹn của tệp Windows (.EXE) trên đĩa. Tuy nhiên nó sẽ vô dụng nếu kẻ tấn công sử dụng kỹ thuật thay thế tiến trình → để lại fingerprint  
→ so sánh strings để kiểm tra



# Các công cụ để giám sát tiến trình

- **So sánh strings:** kiểm tra xem strings trên đĩa (image) với trên bộ nhớ
- **Sử dụng Dependency Walker (depends.exe):**
  - sử dụng khi tìm thấy một DLL độc hại và muốn kiểm tra xem có tiến trình nào đang dùng không.
  - Để xác định xem một DLL có được tải vào một tiến trình sau khi tiến trình đã được khởi động hay không bằng cách so sánh danh sách DLL trong Process Explorer với các DLL được hiển thị trong Dependency Walker.

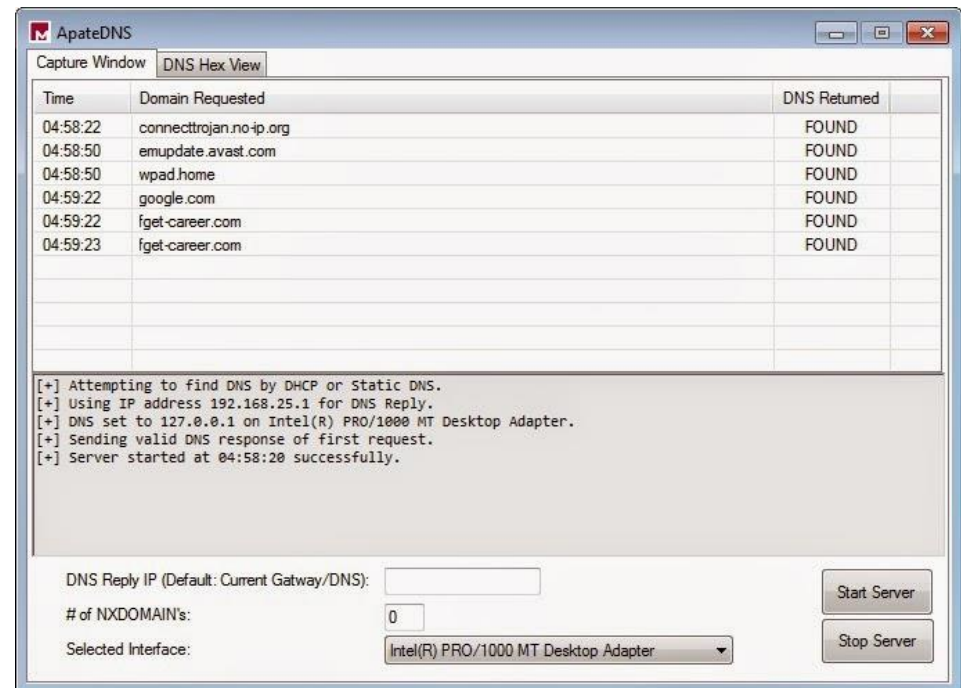


# Các công cụ để giám sát tiến trình

- **Faking a network:** tạo một mạng giả để phân tích mã độc, bao gồm đầy đủ các thông số về DNS, IP, Packet signatures nhưng không có kết nối mạng
- **Sử dụng ApateDNS:**
  - Giả mạo các phản hồi DNS đến một địa chỉ IP được người dùng chỉ định bằng cách lắng nghe trên cổng UDP 53 trên máy cục bộ.
  - Phản hồi các yêu cầu DNS bằng cách thiết lập phản hồi DNS về một địa chỉ IP được chỉ định.

- **Các bước thực hiện**

1. Set IP
2. Select interface
3. Start server
4. Run Malware
5. Watch as DNS requests appear



# Các công cụ để giám sát tiến trình

- **Giám sát mạng với Netcat:** Port scanning, Tunneling, Proxying, Port forwarding...

Cấu hình: sever – listen mode; client – connect mode

```
C:\> nc -l -p 80
```

- nc: required to listen on a port
- -l: listen
- -p: port number

Phần mềm độc hại kết nối đến trình nghe Netcat vì đang sử dụng ApateDNS để chuyển hướng

```
C:\> nc -l -p 80 ❶  
POST /cq/frame.htm HTTP/1.1  
Host: www.google.com ❷  
User-Agent: Mozilla/5.0 (Windows; Windows NT 5.1; TWFsd2FyZUhhbnRlcg==;  
rv:1.38)  
Accept: text/html, application  
Accept-Language: en-US, en;q=  
Accept-Encoding: gzip, deflate  
Keep-Alive: 300  
Content-Type: application/x-form-urlencoded  
Content-Length
```

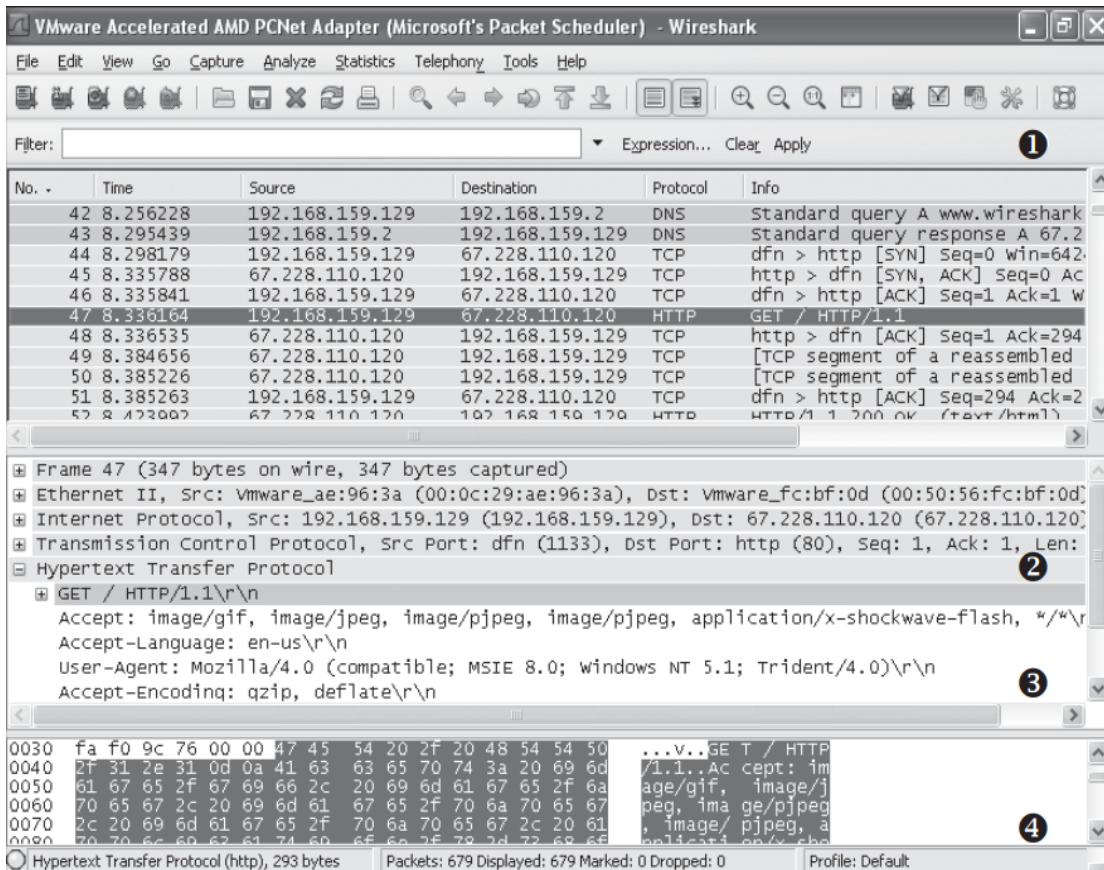
```
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.
```





# Các công cụ để giám sát tiến trình

- **Giám sát dữ liệu mạng với Wireshark:** Để hiểu kênh giao tiếp được sử dụng bởi phần mềm độc hại. Để giúp xác định các chỉ số dựa trên mạng



1 Filter box: to filter the packets displayed

2 Packet listing

3 Packet detail window

4 Hex window

-Right-click any TCP packet & select **Follow TCP Stream** → To view the contents of TCP session.

## Các công cụ để giám sát tiến trình

- **Giả lập các dịch vụ với INETSim:** hầu hết các mã độc được thực thi sẽ kết nối đến máy chủ C&C. Khi phân tích mã độc yêu cầu cần xác định hành vi mã độc mà không cho phép nó kết nối đến máy chủ C&C nhưng vẫn phải phát hiện được các dịch vụ mà mã độc thực hiện.
- INETSim là phần mềm miễn phí trên nền tảng Linux cho phép giả lập các dịch vụ internet cơ bản: DNS, HTTP/HTTPs, FTP, IRC, SMTP ... Có thể cấu hình tin phản hồi cho các yêu cầu HTTP/HTTPs và trả về bất kỳ tệp nào dựa trên phần mở rộng (extensions)





# Các công cụ để giám sát tiến trình

```
sniffer@sniffer-VirtualBox:~$ ps -ef | grep inetsim
root      1584      1  0 09:06 ?        00:00:01 inetsim_main
inetsim   1742    1584  0 09:07 ?        00:00:00 inetsim_dns_53_tcp_udp
inetsim   1743    1584  0 09:07 ?        00:00:00 inetsim_http_80_tcp
inetsim   1745    1584  0 09:07 ?        00:00:00 inetsim_http5_443_tcp
inetsim   1746    1584  0 09:07 ?        00:00:00 inetsim_smtp_25_tcp
inetsim   1747    1584  0 09:07 ?        00:00:00 inetsim_smtps_465_tcp
inetsim   1748    1584  0 09:07 ?        00:00:00 inetsim_pop3_110_tcp
inetsim   1749    1584  0 09:07 ?        00:00:00 inetsim_pop3s_995_tcp
inetsim   1750    1584  0 09:07 ?        00:00:00 inetsim_ftp_21_tcp
inetsim   1751    1584  0 09:07 ?        00:00:00 inetsim_ftps_990_tcp
inetsim   1752    1584  0 09:07 ?        00:00:01 inetsim_tftp_69_udp
inetsim   1753    1584  0 09:07 ?        00:00:07 inetsim_irc_6667_tcp
inetsim   1754    1584  0 09:07 ?        00:00:00 inetsim_ntp_123_udp
inetsim   1755    1584  0 09:07 ?        00:00:00 inetsim_finger_79_tcp
inetsim   1756    1584  0 09:07 ?        00:00:00 inetsim_ident_113_tcp
inetsim   1757    1584  0 09:07 ?        00:00:00 inetsim_syslog_514_udp
inetsim   1761    1584  0 09:07 ?        00:00:00 inetsim_time_37_tcp
inetsim   1762    1584  0 09:07 ?        00:00:00 inetsim_time_37_udp
inetsim   1765    1584  0 09:07 ?        00:00:00 inetsim_daytime_13_tcp
inetsim   1766    1584  0 09:07 ?        00:00:00 inetsim_daytime_13_udp
inetsim   1767    1584  0 09:07 ?        00:00:00 inetsim_echo_7_tcp
inetsim   1768    1584  0 09:07 ?        00:00:00 inetsim_echo_7_udp
inetsim   1769    1584  0 09:07 ?        00:00:00 inetsim_discard_9_tcp
inetsim   1781    1584  0 09:07 ?        00:00:00 inetsim_discard_9_udp
inetsim   1782    1584  0 09:07 ?        00:00:00 inetsim_quotd_17_tcp
inetsim   1783    1584  0 09:07 ?        00:00:00 inetsim_quotd_17_udp
inetsim   1789    1584  0 09:07 ?        00:00:00 inetsim_chargen_19_tcp
inetsim   1790    1584  0 09:07 ?        00:00:00 inetsim_chargen_19_udp
inetsim   1791    1584  0 09:07 ?        00:00:00 inetsim_dummy_1_tcp
inetsim   1792    1584  0 09:07 ?        00:00:00 inetsim_dummy_1_udp
sniffer   2099    2082  0 09:29 pts/4    00:00:00 grep --color=auto inetsim
```

1. Infected system (192.168.1.50)
  - trying to communicate → C&C server: (rnd009.....com)
  - Linux VM does not have a DNS server running → **Domain could not be resolved**
2. Infected system (192.168.1.50)
  - INetSim running on Linux VM
  - C&C domain is resolved → Makes an HTTP communication → **Download file settings.ini**

No.	Time	Source	Destination	Protocol	Length	Info
5	3.174453370	192.168.1.50	192.168.1.100	DNS	82	Standard query 0xdb99 A rnd009.googlepages.com
6	3.174473089	192.168.1.100	192.168.1.50	ICMP	110	Destination unreachable (Port unreachable)
7	3.175928441	192.168.1.50	192.168.1.100	DNS	82	Standard query 0x90ec A rnd009.googlepages.com
8	3.175942095	192.168.1.100	192.168.1.50	ICMP	110	Destination unreachable (Port unreachable)
9	3.176474369	192.168.1.50	192.168.1.100	DNS	82	Standard query 0x0ec8 A rnd009.googlepages.com
10	3.176482649	192.168.1.100	192.168.1.50	ICMP	110	Destination unreachable (Port unreachable)
11	3.178283604	192.168.1.50	192.168.1.100	DNS	82	Standard query 0x7190 A rnd009.googlepages.com
12	3.178291685	192.168.1.100	192.168.1.50	ICMP	110	Destination unreachable (Port unreachable)

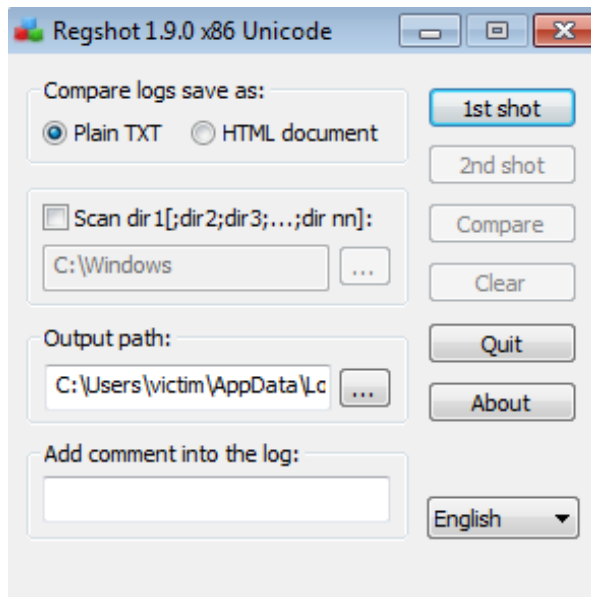
  

No.	Time	Source	Destination	Protocol	Length	Info
5	14.687164101	192.168.1.50	192.168.1.100	DNS	82	Standard query 0xdb99 A rnd009.googlepages.com
6	14.741586271	192.168.1.100	192.168.1.50	DNS	98	Standard query response 0xdb99 A rnd009.googlepages.com A 192.168.1.100
7	14.744866993	192.168.1.50	192.168.1.100	TCP	66	49166 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
8	14.744944799	192.168.1.100	192.168.1.50	TCP	66	80 → 49166 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1 WS=1..
9	14.747176177	192.168.1.50	192.168.1.100	TCP	60	49166 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
10	14.747225954	192.168.1.50	192.168.1.100	HTTP	158	GET /setting.ini HTTP/1.1
11	14.747243298	192.168.1.100	192.168.1.50	TCP	54	80 → 49166 [ACK] Seq=1 Ack=105 Win=29312 Len=0

# Các công cụ để giám sát tiến trình

- So sánh Registry Snapshots với *Regshot*:

- Cách so sánh: lưu trạng thái ban đầu, cho mã độc thực thi, lưu trạng thái lúc này → so sánh



```

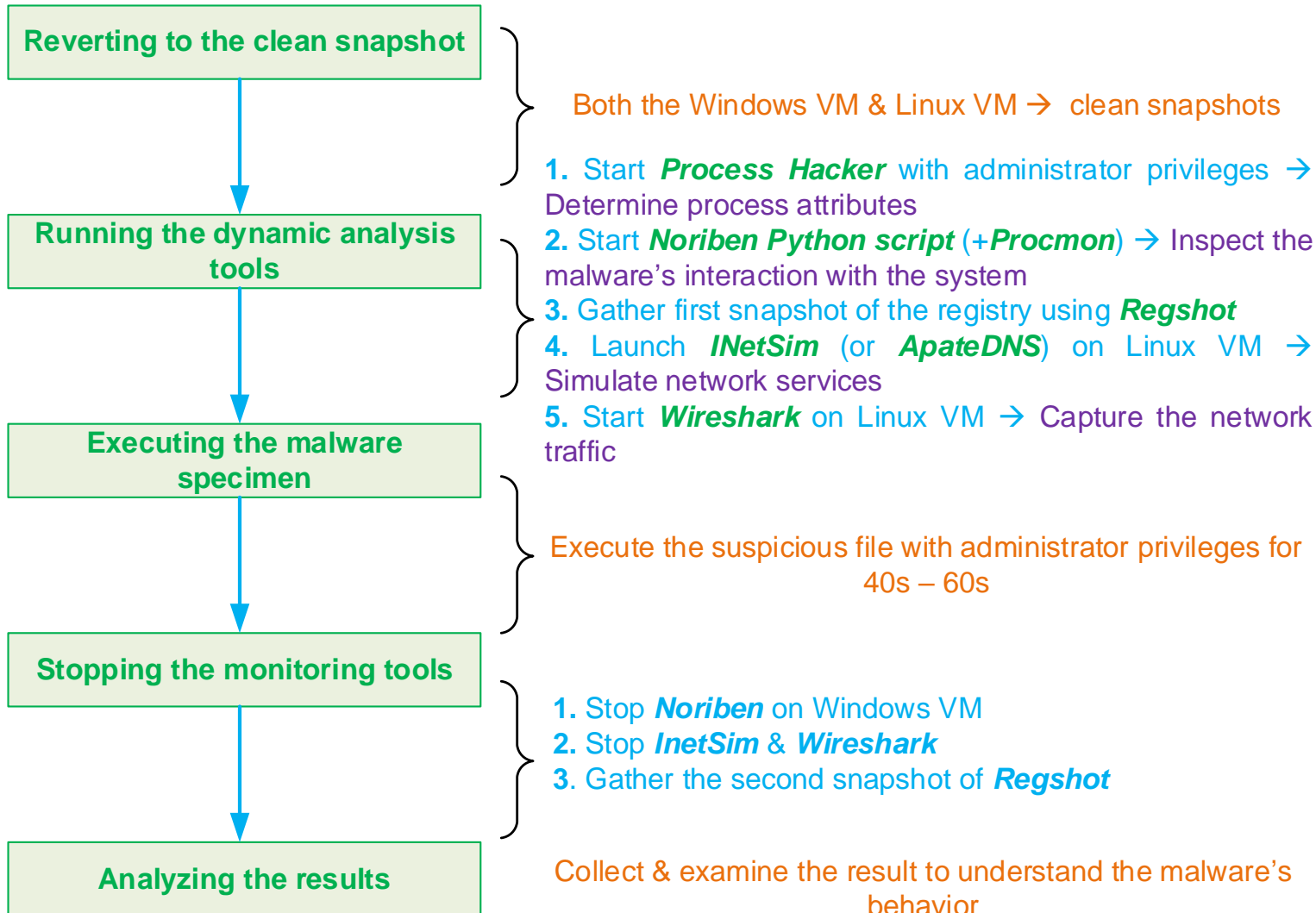
Regshot
Comments:
Datetime: <date>
Computer: MALWAREANALYSIS
Username: username

-----
Keys added: 0
-----
-----
Values added:3
-----
① HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ckr:C:\WINDOWS\system32\
ckr.exe
...
...

-----
Values modified:2
-----
② HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 00 43 7C 25 9C 68 DE 59 C6 C8
9D C3 1D E6 DC 87 1C 3A C4 E4 D9 0A B1 BA C1 FB 80 EB 83 25 74 C4 C5 E2 2F CE
4E E8 AC C8 49 E8 E8 10 3F 13 F6 A1 72 92 28 8A 01 3A 16 52 86 36 12 3C C7 EB
5F 99 19 1D 80 8C 8E BD 58 3A DB 18 06 3D 14 8F 22 A4
...

-----
Total changes:5
-----
    
```

# Quy trình phân tích động



PEview - C:\Users\IEUser\Desktop\BinaryCollection\Chapter\_31\Lab03-02.dll

File View Go Help

Lab03-02.dll

- IMAGE\_DOS\_HEADER
- MS-DOS Stub Program
- IMAGE\_NT\_HEADERS
  - Signature
  - IMAGE\_FILE\_HEADER
  - IMAGE\_OPTIONAL\_HEADER
  - IMAGE\_SECTION\_HEADER .text
  - IMAGE\_SECTION\_HEADER .rdata
  - IMAGE\_SECTION\_HEADER .data
  - IMAGE\_SECTION\_HEADER .reloc
  - SECTION .text
  - SECTION .rdata
  - SECTION .data
  - SECTION .reloc

pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	4CA13E29	Time Date Stamp	2010/09/28 Tue 01:00:25 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	210E	Characteristics	
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPED
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPPED
		0100	IMAGE_FILE_32BIT_MACHINE
		2000	IMAGE_FILE_DLL

PE Explorer - C:\Users\IEUser\Desktop\file malware demo\Lab03-02.dll

File View Tools Help

HEADERS INFO

Address of Entry Point: 10004E4D ✓ Real Image Checksum: 00000184h

Field Name	Data Value	Description
Machine	014Ch	i386
Number of Sections	0004h	
Time Date Stamp	4CA13E29h	28/09/2010 01:00:25
Pointer to Symbol Table	00000000h	
Number of Symbols	00000000h	
Size of Optional Header	00E0h	
Characteristics	210Eh	
Magic	0108h	PE32
Linker Version	0006h	6.0
Size of Code	00004000h	
Size of Initialized Data	0000CA00h	
Size of Uninitialized Data	00000000h	
Address of Entry Point	10004E4Dh	
Base of Code	00001000h	
Base of Data	00005000h	

Field Name	Data Value	Description
Section Alignment	00001000h	
File Alignment	00000200h	
Operating System Version	00000004h	4.0
Image Version	00000000h	0.0
Subsystem Version	00000004h	4.0
Win32 Version Value	00000000h	Reserved
Size of Image	00013000h	77824 bytes
Size of Headers	00000400h	
Checksum	00000000h	
Subsystem	0002h	Win32 GUI
Dll Characteristics	0000h	
Size of Stack Reserve	00100000h	
Size of Stack Commit	00001000h	
Size of Heap Reserve	00100000h	
Size of Heap Commit	00001000h	

20.02.2019 00:59:11 : Calculating Checksum: SUCCESS (Header's Checksum: 00000000h / Real Checksum: 00000184h)

20.02.2019 00:59:11 : EOF Extra Data From: 00005E00h (24064)

20.02.2019 00:59:11 : Length of EOF Extra Data: 00000001h (1) bytes.

20.02.2019 00:59:11 : EOF Position: 00005E01h (24065)

20.02.2019 00:59:11 : Done.

For Help, press F1

Characteristics Editor

- ☐ 0x0001 Relocation information is stripped from the file
- ☒ 0x0002 The file is executable (no unresolved external references)
- ☒ 0x0004 Line numbers are stripped from the file
- ☒ 0x0008 Local symbols are stripped from the file
- ☐ 0x0010 Aggressively trim the working set
- ☐ 0x0020 The application can handle addresses larger than 2 GB
- ☐ 0x0040 Use of this flag is reserved for future use
- ☐ 0x0080 Bytes of word are reversed (REVERSED\_LO)
- ☒ 0x0100 Computer supports 32-bit words
- ☐ 0x0200 Debugging information is stored separately in a .dbg file
- ☐ 0x0400 If the image is on removable media, copy and run from the swap file
- ☐ 0x0800 If the image is on the network, copy and run from the swap file
- ☐ 0x1000 The file is a system file such as a driver
- ☒ 0x2000 The file is a dynamic link library (DLL)
- ☐ 0x4000 File should be run only on a uniprocessor computer
- ☐ 0x8000 Bytes of the word are reversed (REVERSED\_HI)

Ok Cancel