**Lab\_3**

**1. Process Explorer – chạy quyền administrator.**

- View -> select columns: hiển thị thêm nhiều trường

- Xem tiến trình và phát hiện tiến trình lạ: nghi ngờ Malware

- option -> Verify Image Signature: hiển thị chữ ký nhà SX -> nếu không, nghi ngờ Malware.

- option -> VirusTotal.com -> check VirusTotal.com -> hệ thống VirusTotal sẽ cảnh báo tiến trình có thể là Malware.

**1.1. Mục tiêu**

Kiểm tra hệ thống để xác định sự hiện diện của phần mềm độc hại (malware) thông qua công cụ **Process Explorer** từ bộ công cụ Sysinternals.

**1.2. Công cụ sử dụng**

* **Process Explorer**: hiển thị chi tiết các tiến trình đang hoạt động trên hệ thống.
* **VirusTotal Integration**: dùng để quét tiến trình bằng nhiều phần mềm antivirus.
* **Tùy chọn bật thêm**:
  + Verify Image Signatures
  + VirusTotal.com > Check VirusTotal.com

**1.3. Các bước thực hiện**

1. **Chạy Process Explorer dưới quyền Administrator**.
2. Bật các tùy chọn:
   * Options → Verify Image Signatures
   * Options → VirusTotal.com → Check VirusTotal.com
3. Kiểm tra các trường:
   * Company Name
   * Verified Signer
   * VirusTotal
4. Kiểm tra các tiến trình:
   * Không có chữ ký số
   * Tên lạ, sai chính tả
   * VirusTotal báo "Unknown" hoặc có kết quả > 0/77
5. Ghi nhận tình trạng các tiến trình svchost.exe, RuntimeBroker.exe, LockApp.exe, v.v...

## 1.4. Kết quả

| **Mục** | **Kết luận** |
| --- | --- |
| Số tiến trình nghi ngờ | **0** |
| Số tiến trình không xác minh được chữ ký số | **0** |
| Số tiến trình có VirusTotal > 0 | **0** |
| Tiến trình "Unknown" | **Ban đầu có, nhưng sau đó đã được cập nhật và xác minh sạch** |
| Hành vi CPU/RAM bất thường | **Không phát hiện bất thường** |

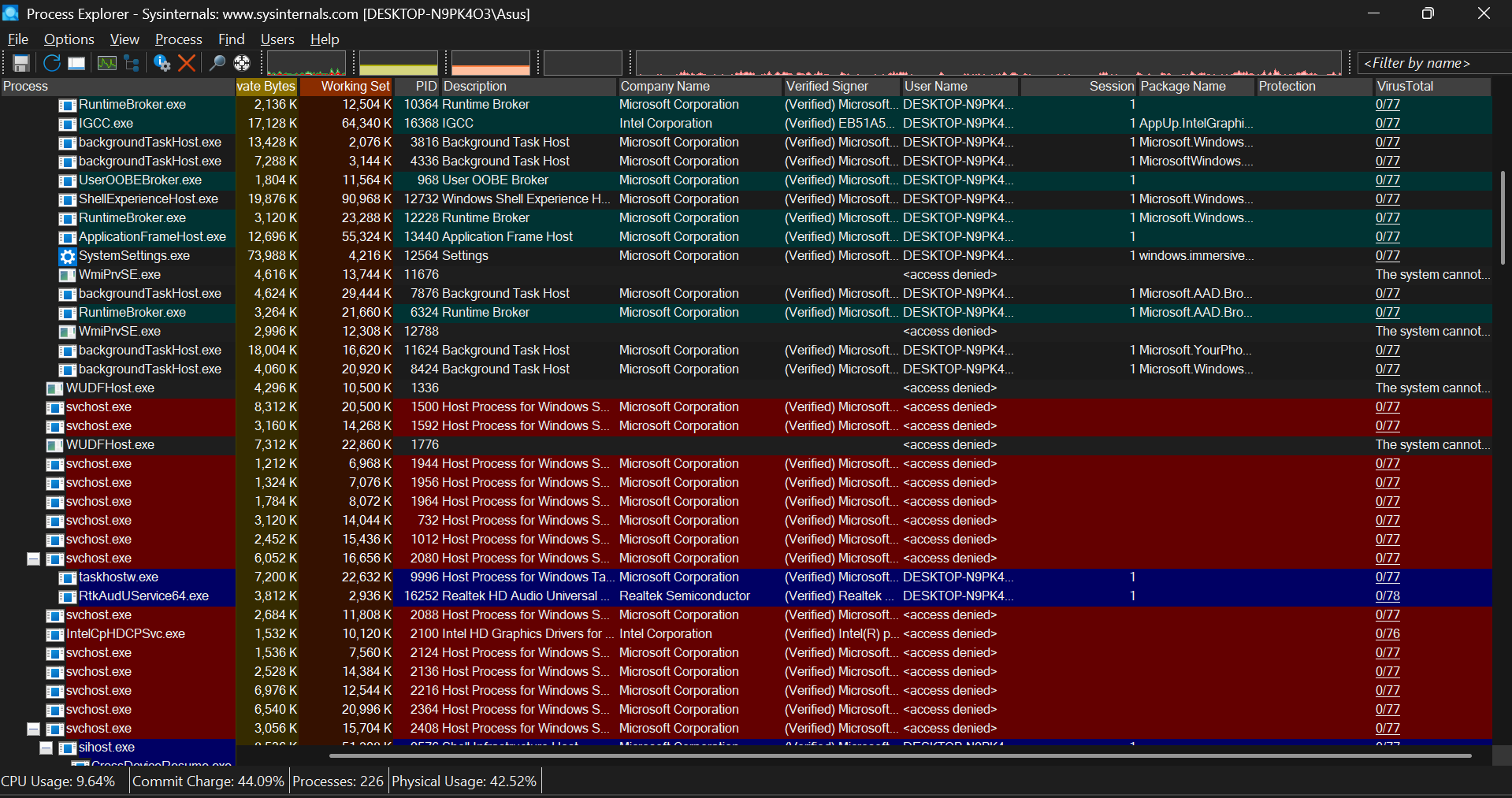
**1.5. Nhận xét**

* **Không phát hiện phần mềm độc hại** trên hệ thống tại thời điểm kiểm tra.
* Các tiến trình hệ thống như svchost.exe, WmiPrvSE.exe, RuntimeBroker.exe,... đều có **chữ ký xác minh từ Microsoft Corporation** và kết quả VirusTotal **0/n**.
* Một số tiến trình ban đầu hiển thị "Unknown" là do hệ thống chưa tải được kết quả VirusTotal. Sau khi đồng bộ hoàn tất, tất cả đều cho kết quả an toàn (0/77 hoặc tương tự).
* Màu sắc đỏ và xanh trong Process Explorer **không biểu thị nguy hiểm**, mà dùng để phân biệt loại tiến trình (dịch vụ nền, bị suspend, v.v.).

**1.6. Kết luận**

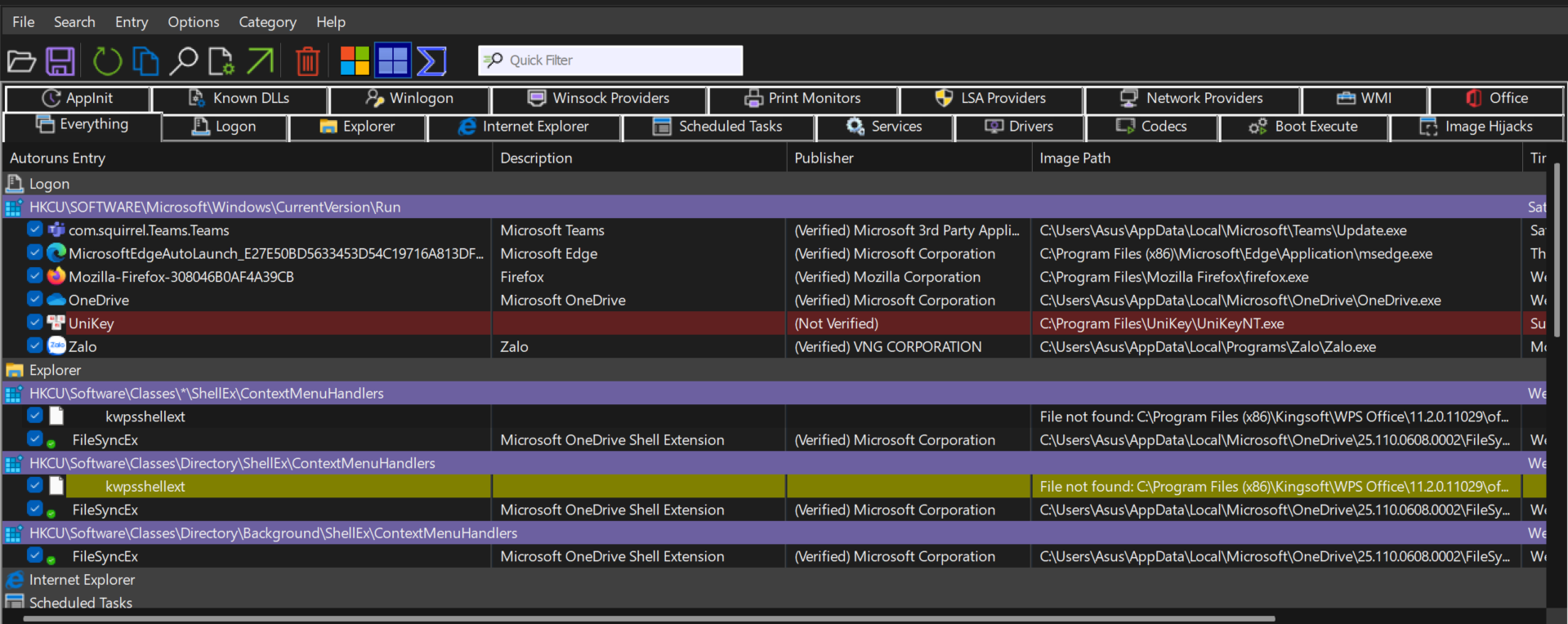
💡 **Hệ thống sạch – không phát hiện tiến trình đáng ngờ hoặc phần mềm độc hại**.  
Người dùng nên tiếp tục theo dõi định kỳ bằng Process Explorer hoặc các công cụ như Autoruns, TCPView nếu có nghi ngờ hoạt động bất thường trong tương lai.

**1.7. Hình ảnh minh họa**

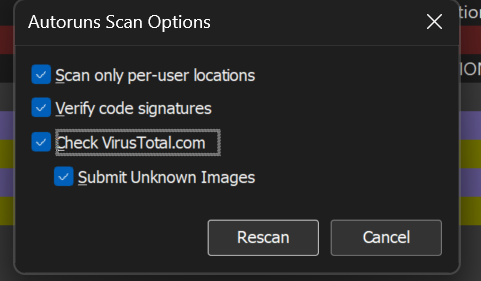


**2. Autoruns – chạy quyền administrator.**

- Xem các tiến trình chạy tự động -> phát hiện tiến trình lạ.



- option -> scan option -> chọn các hình thức scan.



#### **2.1. Nhóm Logon (Khởi động cùng Windows):**

* **Firefox**: Verified Mozilla → Hợp lệ
* **UniKey**: **Không có chữ ký số** → **Đáng chú ý**
  + Đường dẫn: C:\Program Files\UniKey\UniKeyNT.exe
  + **VirusTotal: 3/77** → **Cảnh báo mức độ nhẹ**, có thể là false positive
* **Zalo**:
  + Publisher: VNG (Verified)
  + **VirusTotal: 2/77** → **Cần kiểm tra thêm**, nhưng mức cảnh báo thấp

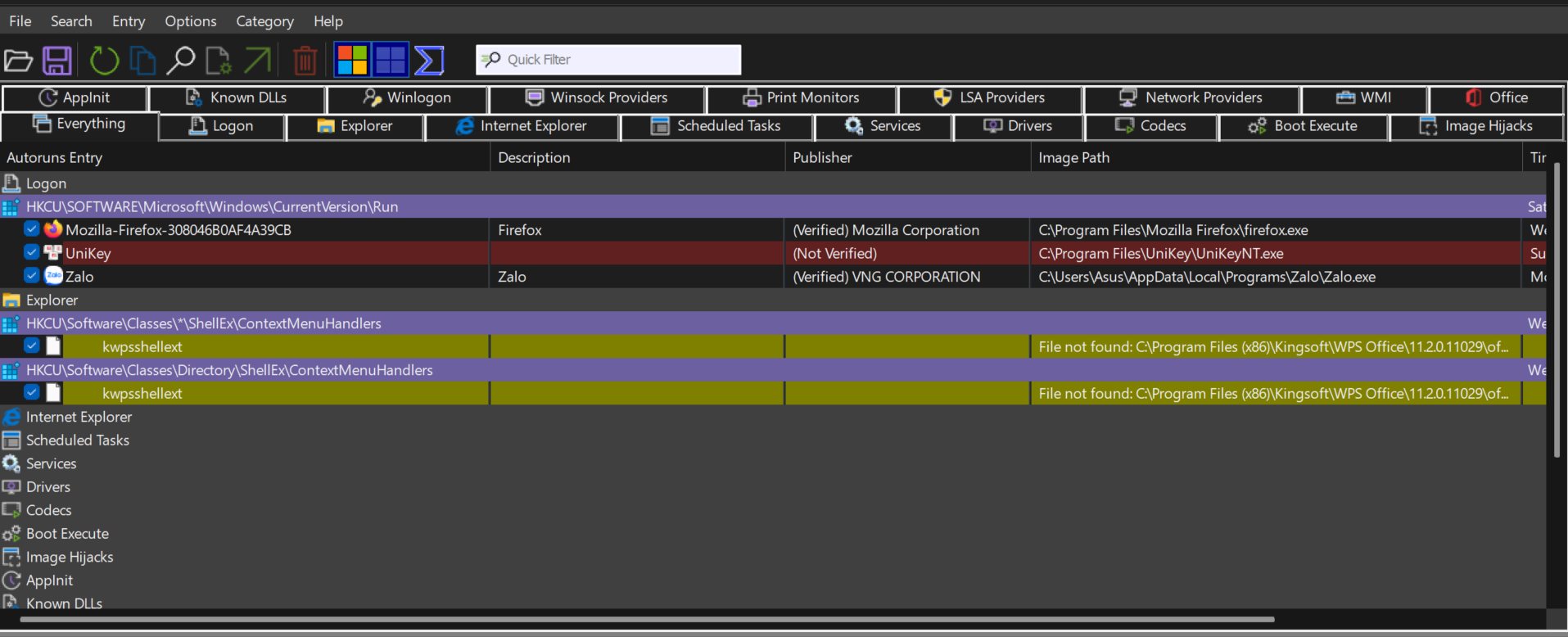
#### **2.2. Explorer Shell Extensions:**

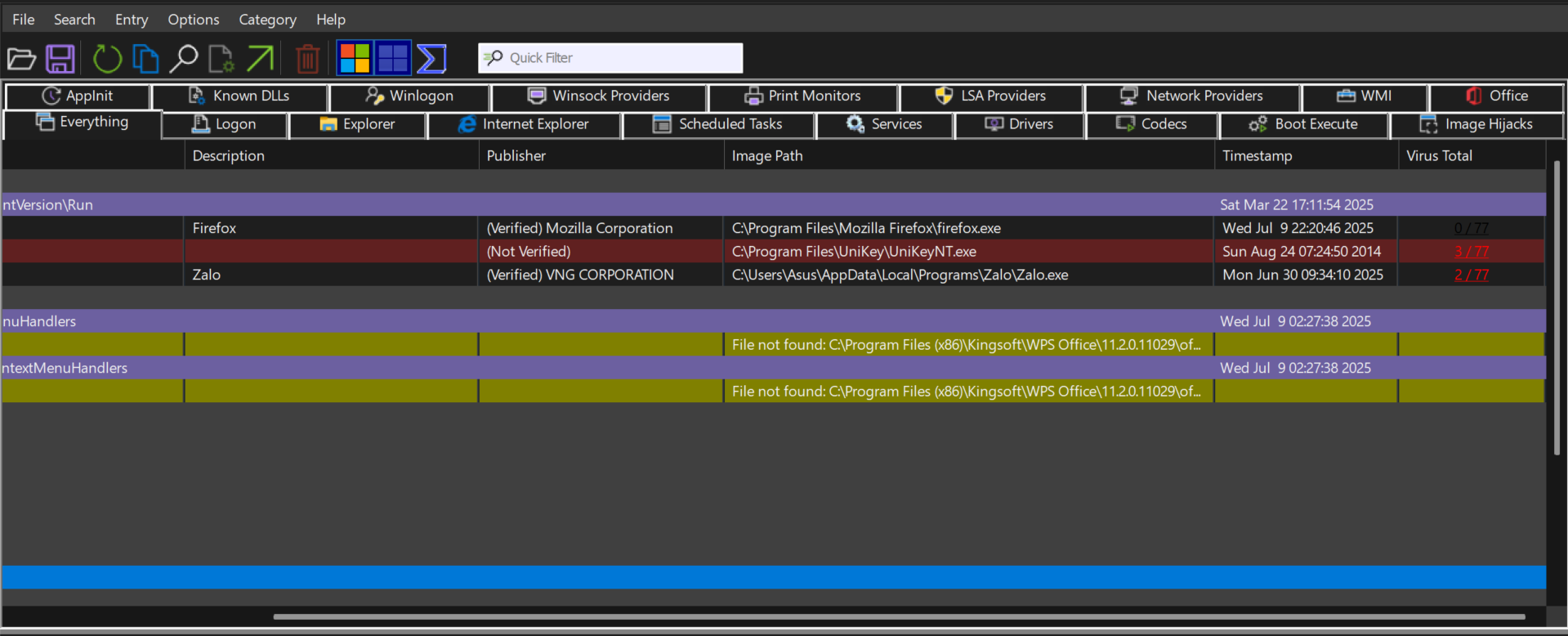
* kwpsshellext: Dẫn đến đường dẫn WPS Office nhưng báo lỗi **File not found**.
  + => Có thể là **mảnh vỡ còn sót lại sau khi gỡ cài đặt**, nên loại bỏ.

### **2.3. Đánh giá tổng quan**

| **Thành phần** | **Mức độ nghi ngờ** | **Ghi chú** |
| --- | --- | --- |
| Firefox | Không | Có chữ ký số, hợp lệ |
| UniKey | Trung bình | Không có chữ ký, 3/77 cảnh báo |
| Zalo | Thấp | Có chữ ký, nhưng 2/77 bị flag |
| kwpsshellext | Trung bình | Dẫn đến file không tồn tại |

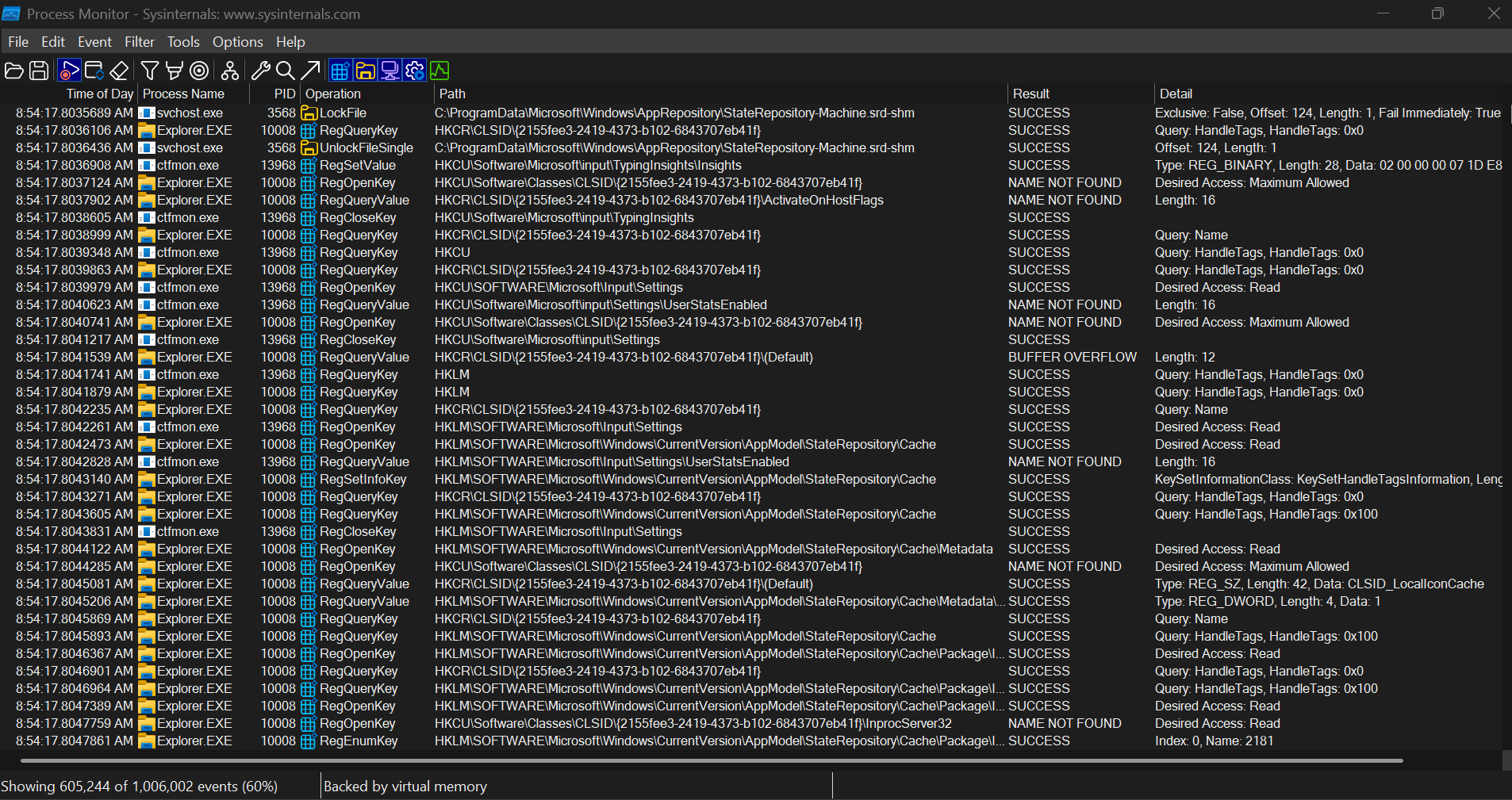
**2.4. Hình ảnh minh họa**





**3. Process Monitor.**

### **3.1. Tiến trình hoạt động:**



* Explorer.EXE
* ctfmon.exe
* svchost.exe

### **3.2. Hành vi chính ghi nhận:**

| **Thời gian** | **Tiến trình** | **Hành vi (Operation)** | **Đường dẫn hoặc khoá bị tác động** | **Kết quả** |
| --- | --- | --- | --- | --- |
| 8:54:17.8035698 | svchost.exe | LockFile | C:\ProgramData\Microsoft\Windows\AppRepository\... | SUCCESS |
| 8:54:17.8036160 | Explorer.EXE | RegQueryKey | HKCR\CLSID\{SID...} | SUCCESS |
| 8:54:17.8036434 | svchost.exe | UnlockFileSingle | AppRepositoryMachine.srd.shm | SUCCESS |
| 8:54:17.8036994 | ctfmon.exe | RegSetValue | TypingInsights → Thiết lập giá trị registry | SUCCESS |
| 8:54:17.8041421 | Explorer.EXE | RegOpenKey | HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\AppModel... | SUCCESS |
| 8:54:17.8046019 | Explorer.EXE | RegQueryValue | Truy xuất giá trị registry | SUCCESS |

**Ghi chú:**

* RegSetValue của ctfmon.exe cho thấy tiến trình có hành vi ghi dữ liệu vào registry (có thể là cấu hình người dùng).
* svchost.exe truy cập và khoá tập tin trong AppRepository, dấu hiệu liên quan đến quản lý ứng dụng hệ thống.
* Nhiều thao tác registry thực hiện bởi Explorer.EXE cho thấy shell đang truy xuất cấu hình người dùng.

**3.3. Phân tích**

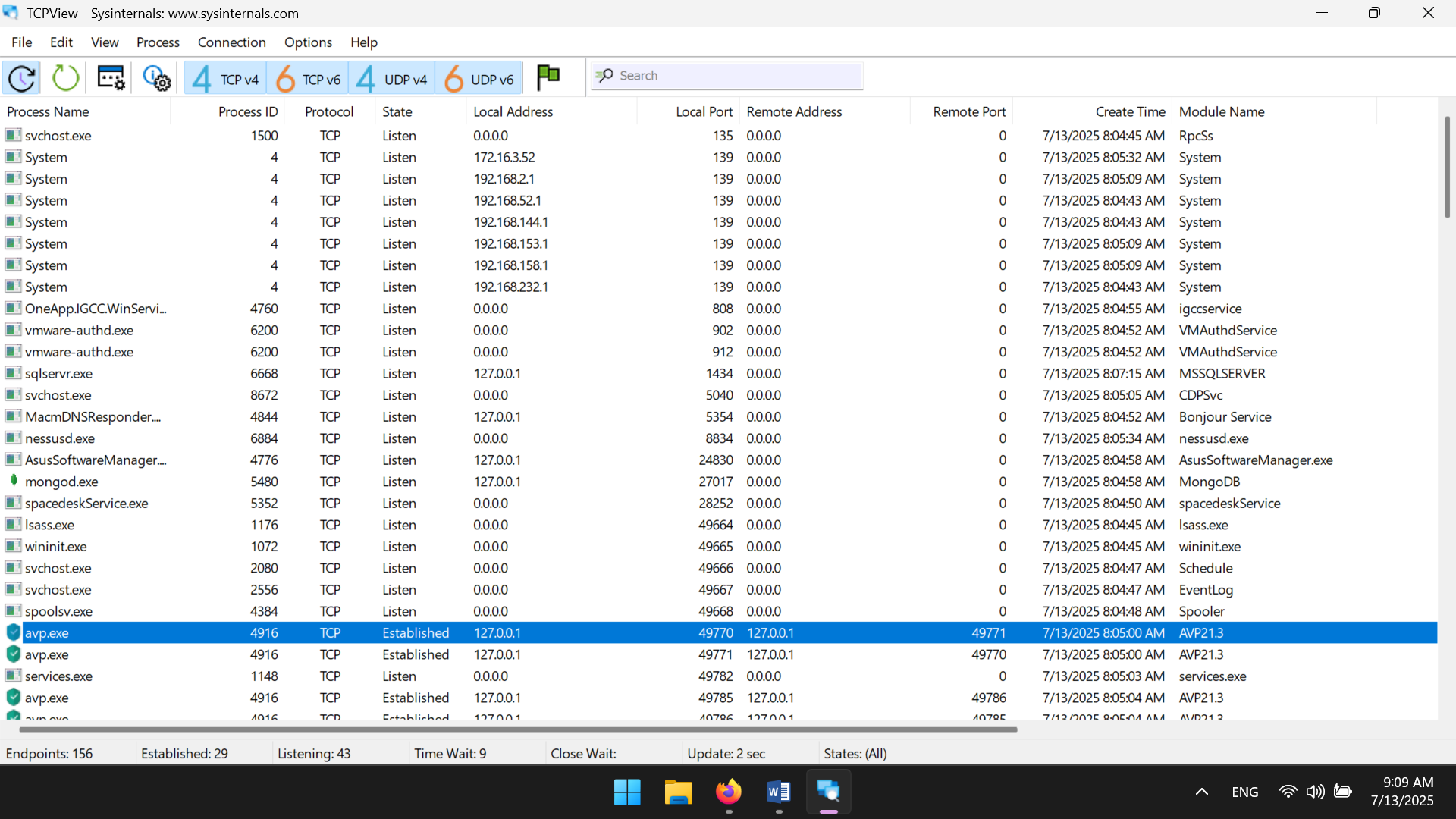
1. Không ghi nhận hành vi rõ ràng là độc hại trong đoạn log ban đầu.
2. Tuy nhiên, cần lưu ý nếu có tiến trình:
   * Ghi file vào các thư mục AppData, Temp, Startup
   * Tạo khoá registry tại Run, Winlogon, Services
   * Ghi giá trị lạ hoặc DLL tự thêm vào shell context
3. Trong trường hợp này, chưa thấy hành vi khả nghi, nhưng bồ có thể lọc theo tên tiến trình nghi ngờ để theo dõi sâu hơn (như UniKeyNT.exe, Zalo.exe... từ Autoruns).

**3.4. Kết luận**

* Process Monitor đã hoạt động tốt, ghi nhận hơn 600.000 sự kiện hệ thống.
* Chưa phát hiện hành vi trực tiếp liên quan đến malware trong khoảng thời gian quan sát.
* Cần thực hiện lọc tiến trình nghi ngờ cụ thể để tập trung phân tích sâu.
* Có thể kết hợp với Autoruns và VirusTotal để đánh giá chữ ký và độ tin cậy của tiến trình.

**4. TCPView**

Ảnh chụp màn hình dưới đây là kết quả thu được khi chạy TCPView:



**4.1.Phân tích một số kết nối:**

| **Process Name** | **Process ID** | **Protocol** | **Local Address** | **Local Port** | **Remote Address** | **Remote Port** | **State** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| spoolsv.exe | 4384 | TCP | 0.0.0.0 | 49668 | 0.0.0.0 | 0 | Listen |
| mongod.exe | 5480 | TCP | 127.0.0.1 | 27017 | 0.0.0.0 | 0 | Listen |
| avp.exe | 4916 | TCP | 127.0.0.1 | 49770-49771 | 127.0.0.1 | 49770-49771 | Established |
| sqlservr.exe | 6668 | TCP | 127.0.0.1 | 1434 | 0.0.0.0 | 0 | Listen |

**Giải thích:**

* spoolsv.exe: Tiến trình của hệ thống dùng cho dịch vụ máy in, đang lắng nghe tại cổng **49668.**
* mongod.exe: Tiến trình MongoDB đang lắng nghe trên cổng **27017** tại địa chỉ **127.0.0.1** (localhost).
* avp.exe: Tiến trình của phần mềm bảo mật **Kaspersky (AVP)** đang thiết lập kết nối nội bộ giữa các port **49770** và **49771.**
* sqlservr.exe: Tiến trình của **SQL Server** đang mở cổng **1434** để lắng nghe kết nối.

### **4.2. Nhận xét:**

* Hệ thống hiện tại có nhiều kết nối đang **Listen** trên địa chỉ **0.0.0.0** hoặc **127.0.0.1**, phục vụ các dịch vụ nội bộ và kết nối từ xa.
* Tiến trình **mongod.exe** và **sqlservr.exe** đều hoạt động trên localhost, bảo đảm rằng các cơ sở dữ liệu chỉ được truy cập nội bộ.
* Một số tiến trình bảo mật (**avp.exe**) đang thiết lập các kết nối TCP nội bộ để trao đổi dữ liệu.

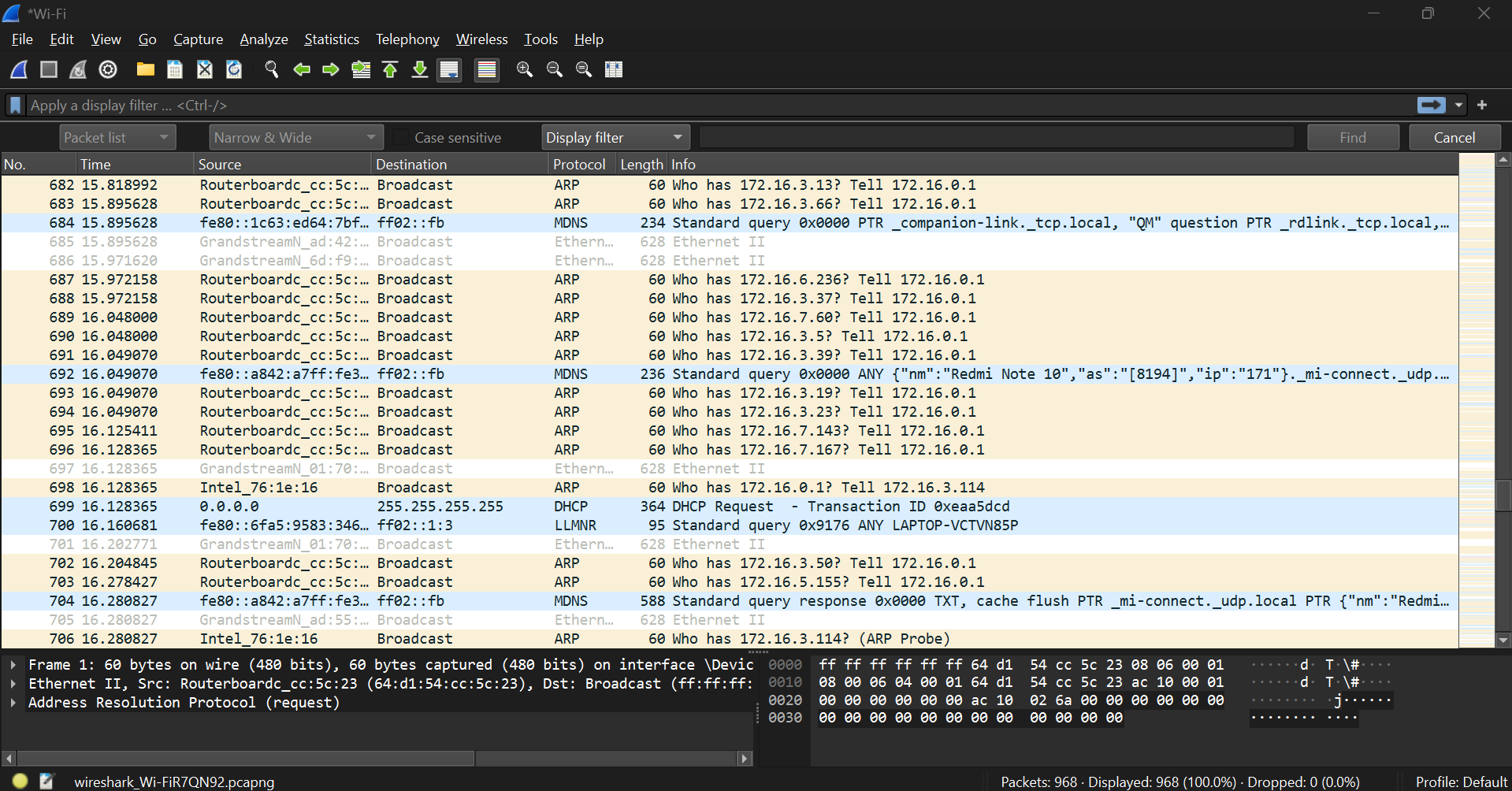
### **4.3. Kết luận:**

Việc sử dụng **TCPView** giúp xác định chính xác tiến trình nào đang tạo hoạt động mạng, cũng như quản lý được các cổng và kết nối đang tồn tại trên hệ thống. Công cụ này hữu ích trong kiểm tra bảo mật và xử lý sự cố mạng nội bộ.

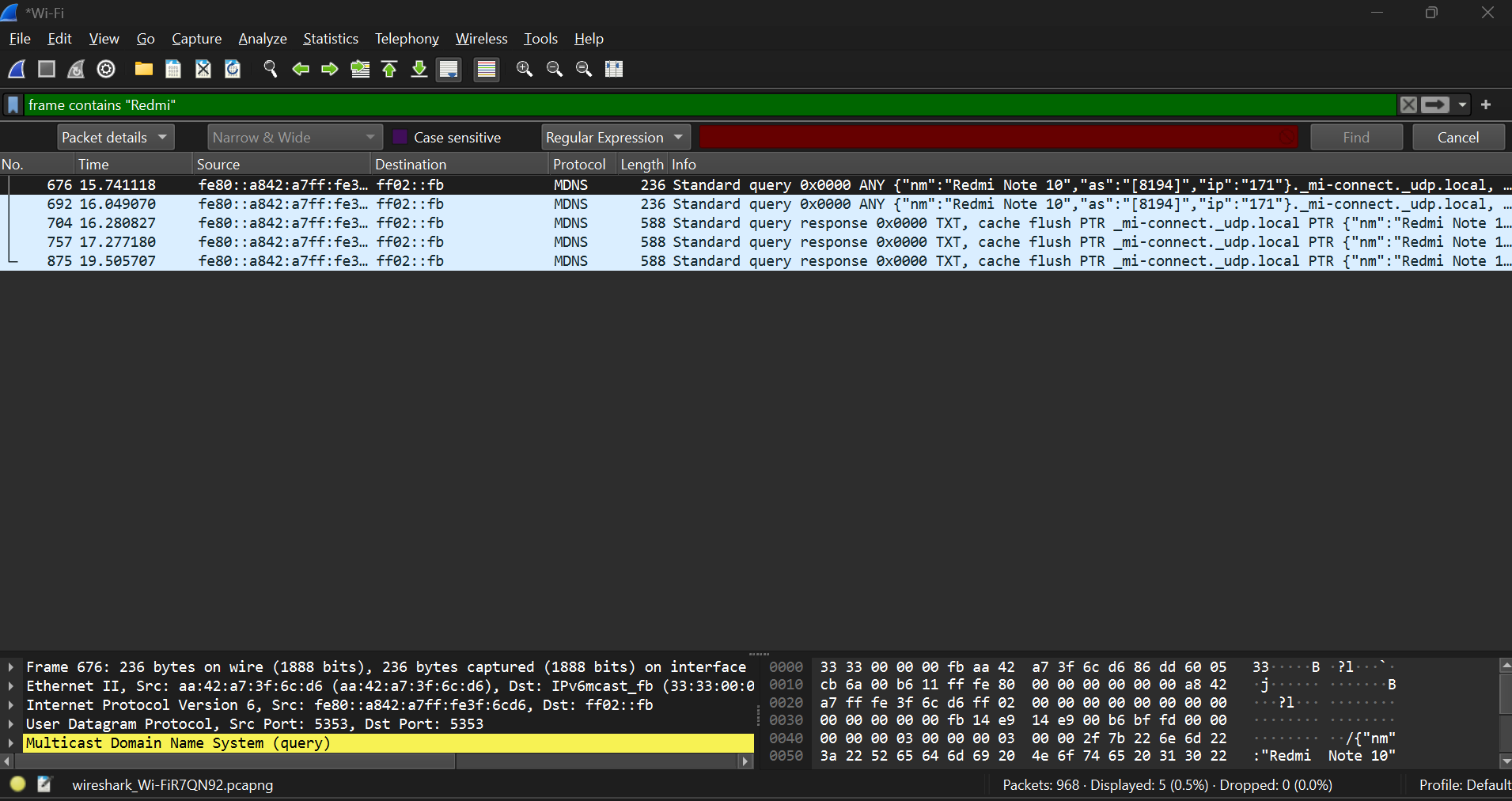
**5. Wireshark**

### **5.1. Thực hiện**

* Chạy **Wireshark** trên card mạng **Wi-Fi**
* Bắt gói trong khoảng **30 giây**



* Sử dụng filter tìm kiếm các gói chứa dữ liệu khả nghi.



### **5.2. Kết quả**

#### **Tổng quan:**

* Tổng số gói bắt được: **968**
* Loại gói:
  + **ARP:** 500+
  + **MDNS:** 5+
  + **DHCP:** 1
  + **LLMNR:** 1
  + **Ethernet II:** 10+

#### **Phát hiện bất thường:**

* **Gói MDNS** số **693** chứa chuỗi JSON nghi vấn:

{"nm":"Redmi Note 10","as":"[8194]","ip":"171"}

* → Dữ liệu JSON kiểu này có thể là thông tin từ thiết bị IoT hoặc có thể bị mã độc lợi dụng để truyền tín hiệu.
* **Nhiều truy vấn ARP liên tục** đến các IP nội bộ có thể là dấu hiệu của:
  + Một thiết bị scan IP trong mạng
  + Hoặc công cụ network discovery của malware

#### **Truy vấn DHCP**

* **Gói 699**: DHCP Request — bình thường, không chứa dữ liệu lạ.

### **5.3. Nhận xét**

* **Dữ liệu MDNS chứa JSON** cần được kiểm tra thêm.
* Các truy vấn ARP liên tục tuy bình thường trong LAN, nhưng nếu tần suất quá cao có thể là dấu hiệu máy bị malware scan mạng.

### **5.4. Kết luận**

Wireshark giúp giám sát hoạt động mạng realtime và phát hiện dữ liệu gửi/nhận bất thường một cách trực quan và hiệu quả. Kết hợp với các filter và phân tích nội dung payload, có thể phát hiện nguy cơ malware lẩn trốn trong các gói tin hợp pháp.

**6. Attack Surface Analyzer**

**6.1. Công cụ**

- Tải .NetSDK

- Sử dụng lệnh dotnet tool install --global Microsoft.CST.AttackSurfaceAnalyzer.CLI --version 2.3.323 để cài Attack Surface Analyzer.