



(12) **BẢN MÔ TẢ SÁNG CHẾ THUỘC BẢNG ĐỘC QUYỀN SÁNG CHẾ**

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)

CỤC SỞ HỮU TRÍ TUỆ

(11) 

1-0021095

(51)⁷ G06F 17/30

(13) B

(21) 1-2014-00935

(22) 14.06.2012

(86) PCT/CN2012/076874 14.06.2012

(87) WO2013/034006 14.03.2013

(30) 201110260036.X 05.09.2011 CN

(45) 25.06.2019 375

(43) 25.06.2014 315

(73) TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED (CN)

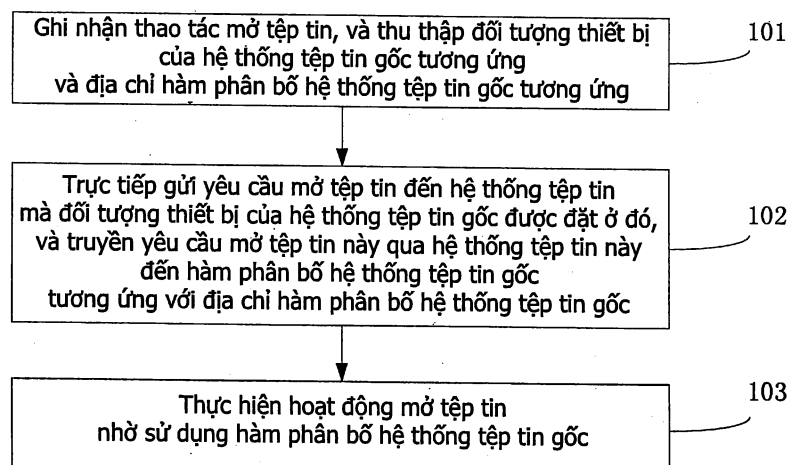
Room 403, East Block 2, SEG Park, Zhenxing Road, Futian District, Shenzhen, Guangdong 518044, China

(72) XIE, Fei (CN), GAO, Xiaoming (CN), MA, Jinsong (CN), LIU, Guize (CN)

(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) **PHƯƠNG PHÁP MỞ TẬP TIN, THIẾT BỊ MỞ TẬP TIN VÀ THIẾT BỊ ĐẦU CUỐI**

(57) Sáng chế đề cập đến các công nghệ xử lý dữ liệu, cụ thể là đến phương pháp, thiết bị mở tệp tin, và thiết bị đầu cuối. Phương pháp này bao gồm các bước: ghi nhận thao tác mở tệp tin, và thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng; và trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, truyền yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc, và thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc này. Theo sáng chế, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.



Lĩnh vực kĩ thuật được đề cập

Sáng chế đề cập đến các công nghệ xử lý dữ liệu, cụ thể là đến phương pháp, thiết bị mở tệp tin, và thiết bị đầu cuối.

Tình trạng kĩ thuật của sáng chế

Cùng với sự phát triển nhanh chóng của các công nghệ mạng và sự tăng lên không ngừng của lượng dữ liệu, thì lượng thông tin lưu trữ các tệp tin điện tử khác nhau cũng đang tăng lên. Cho dù là lúc rảnh rỗi và tiêu khiển hàng ngày hay trong công việc bận rộn thì cũng đều có liên quan đến hoặc phải sử dụng đến các tệp tin khác nhau. Do đó, việc người ta mở các tệp tin mỗi ngày gần như đã trở thành công việc thường nhật.

Phương pháp mở tệp tin thông thường được thực hiện bằng cơ chế API (Application Programming Interface - giao diện lập trình ứng dụng) đã phổ biến của Windows, và hoạt động mở tệp tin có thể được ghi nhận và được điều khiển bởi trình điều khiển bộ lọc tệp tin. Trình điều khiển bộ lọc tệp tin là một loại chương trình điều khiển của Windows, nó được cài đặt trên hệ thống tệp tin để ghi nhận hoạt động truy cập của hệ thống vào tệp tin và cung cấp các chức năng như chức năng điều khiển bộ lọc. Trên máy có cài phần mềm chống virus, mỗi khi thao tác mở tệp tin được trình điều khiển bộ lọc tệp tin ghi nhận, thì hoạt động quét virus sẽ được kích hoạt.

Trong quá trình thực hiện sáng chế, các tác giả sáng chế đã nhận thấy rằng giải pháp kĩ thuật đã biết gặp phải ít nhất là các vấn đề sau đây:

Với phương pháp mở tệp tin thông thường thì việc hoạt động quét virus được kích hoạt mỗi lần mở tệp tin là gần như không cần thiết vì điều này làm tăng gánh nặng cho hệ thống; ngoài ra, khi có nhiều loại phần mềm

chống virus được cài đặt, mỗi khi tệp tin thuộc loại phần mềm chống virus này được mở, thì loại phần mềm chống virus khác cũng được kích hoạt để thực hiện hoạt động quét virus, và khi tệp tin đã được quét này được mở thì loại phần mềm chống virus khác nữa lại được kích hoạt để thực hiện hoạt động quét virus lần nữa, từ đó gây ra việc tệp tin bị mở đi mở lại, và còn gây ra vấn đề về tính tương thích.

Bản chất kĩ thuật của sáng chế

Nhằm cải thiện tính tương thích hệ thống khi mở tệp tin và giảm gánh nặng cho hệ thống, thì sáng chế đề xuất phương pháp, thiết bị mở tệp tin, và thiết bị đầu cuối. Các giải pháp kĩ thuật theo sáng chế là như sau.

Một khía cạnh của sáng chế đề xuất phương pháp mở tệp tin, phương pháp này bao gồm các bước:

ghi nhận thao tác mở tệp tin, và thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng; và

trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, truyền yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc, và thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc này.

Ngoài ra, trước bước ghi nhận thao tác mở tệp tin thì phương pháp này còn bao gồm bước:

tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

trong đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước vốn thay thế địa chỉ hàm gốc.

Ngoài ra, sau bước ghi nhận thao tác mở tệp tin thì phương pháp này còn bao gồm bước:

ghi lại thông số tương ứng với thao tác mở tệp tin;

trong đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số được ghi.

Bước thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng trong cấu trúc VPB (Volume Parameter Block - khối thông số ổ đĩa) vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều khiển ghi sẵn.

Bước thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

khởi động chương trình điều khiển ghi sẵn theo cách BOOT (khởi động), và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

Bước trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó bao gồm bước cụ thể là:

trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm IoCreateFileSpecifyDeviceObjectHint, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

Khía cạnh khác của sáng chế đề xuất thiết bị mở tệp tin, thiết bị này bao gồm:

môđun ghi nhận, được cấu hình để ghi nhận thao tác mở tệp tin;

môđun thu thập thứ nhất, được cấu hình để thu thập đối tượng thiết bị

của hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận ghi nhận được thao tác mở tệp tin;

môđun thu thập thứ hai, được cấu hình để thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận ghi nhận được thao tác mở tệp tin;

môđun gửi, được cấu hình để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc, thu thập được nhờ môđun thu thập thứ nhất, được đặt ở đó, và chuyển yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc mà môđun thu thập thứ hai thu thập được; và

môđun mở, được cấu hình để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc.

Ngoài ra, thiết bị này còn bao gồm:

môđun thay thế, được cấu hình để tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

tương ứng theo đó, môđun mở được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước, vốn được môđun thay thế thay thế cho địa chỉ hàm gốc.

Ngoài ra, thiết bị này còn bao gồm:

môđun ghi lại, được cấu hình để ghi lại thông số tương ứng với thao tác mở tệp tin mà môđun ghi nhận ghi nhận được; và

tương ứng theo đó, môđun mở được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số mà môđun ghi lại ghi được.

Môđun thu thập thứ nhất được cấu hình cụ thể để tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng trong cấu trúc VPB vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều

khiển ghi sẵn.

Môđun thu thập thứ hai được cấu hình cụ thể để khởi động chương trình điều khiển ghi sẵn theo cách BOOT, và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

Môđun gửi được cấu hình cụ thể để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm IoCreateFileSpecifyDeviceObjectHint, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

Khía cạnh khác nữa của sáng chế đề xuất thiết bị đầu cuối, thiết bị đầu cuối này bao gồm thiết bị mở tệp tin đã mô tả trên đây.

Giải pháp kỹ thuật theo sáng chế có thể đem lại các tác dụng có lợi như sau:

Thao tác mở tệp tin được ghi nhận, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.

Mô tả vắn tắt các hình vẽ

Các hình vẽ kèm theo, vốn minh hoạ các phương án thực hiện sáng chế, sẽ được mô tả vắn tắt dưới đây để làm cho giải pháp kỹ thuật của sáng chế rõ ràng hơn. Tất nhiên là các hình vẽ kèm theo này chỉ minh hoạ một số phương án theo sáng chế, và các chuyên gia trung bình trong lĩnh vực này cũng có thể tạo ra các hình vẽ khác dựa vào các hình vẽ này mà không cần

đến bất kì hoạt động có tính sáng tạo nào.

Fig.1 là lưu đồ của phương pháp mở tệp tin theo một phương án thực hiện của sáng chế;

Fig.2 là lưu đồ của phương pháp mở tệp tin theo một phương án thực hiện của sáng chế;

Fig.3 là lưu đồ của tiến trình qua mặt trong lúc mở tệp tin, theo một phương án thực hiện của sáng chế;

Fig.4 là sơ đồ cấu trúc của thiết bị mở tệp tin theo một phương án thực hiện của sáng chế;

Fig.5 là sơ đồ cấu trúc của thiết bị mở tệp tin theo phương án thực hiện khác của sáng chế; và

Fig.6 là sơ đồ cấu trúc của thiết bị mở tệp tin theo phương án thực hiện khác nữa của sáng chế.

Mô tả chi tiết các phương án thực hiện sáng chế

Các phương án thực hiện sáng chế sẽ được mô tả chi tiết dưới đây dựa vào các hình vẽ kèm theo để làm cho các mục đích, giải pháp và các ưu điểm của sáng chế rõ ràng hơn.

Theo phương pháp mở tệp tin thông thường, thao tác mở tệp tin sẽ được ghi nhận và được điều khiển bởi trình điều khiển bộ lọc tệp tin, từ đó kích hoạt hoạt động quét virus. Hoạt động này không chỉ làm tăng gánh nặng cho hệ thống mà còn gây ra vấn đề về tính tương thích giữa các loại phần mềm chống virus. Do đó, phương án này đề xuất phương pháp mở tệp tin. Theo phương pháp này, trình điều khiển bộ lọc tệp tin của cách mở tệp tin gốc sẽ được qua mặt, và yêu cầu mở tệp tin sẽ được gửi trực tiếp đến hệ thống tệp tin để thực hiện hoạt động mở tệp tin. Điều này giảm bớt gánh nặng cho hệ thống vốn bị gây ra bởi hoạt động điều khiển của trình điều khiển bộ lọc tệp tin, và còn cải thiện tính tương thích hệ thống. Như được thể hiện trên Fig.1, phương pháp theo phương án này bao gồm các bước như

sau:

101: ghi lại thao tác mở tệp tin, và thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng; và

102: trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, và truyền yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc;

103: thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc.

Ngoài ra, trước bước ghi nhận thao tác mở tệp tin thì phương pháp này còn bao gồm bước:

tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

trong đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước vốn thay thế địa chỉ hàm gốc.

Bảng nhập các tệp tin thư viện liên kết động 32-bit ghi lại địa chỉ hàm API của hệ thống cần thiết cho tệp tin thực thi được. Địa chỉ hàm API là địa chỉ hàm được chứa trong bảng nhập này, ví dụ, địa chỉ của các hàm NtCreateFile và NtOpenFile. Địa chỉ hàm trong bảng nhập sẽ được thay thế bằng địa chỉ hàm định trước, sao cho trước khi trình điều khiển bộ lọc tệp tin có thể ghi nhận và điều khiển được hoạt động mở tệp tin, thì trình điều khiển bộ lọc tệp tin sẽ bị qua mặt để trực tiếp chuyển yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, và thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc. Điều này sẽ hạn chế các hoạt động không cần thiết của việc quét virus mỗi lần mở tệp tin, và còn tránh được vấn đề làm tăng gánh nặng hệ thống

và vấn đề tương thích vốn bị gây ra bởi hoạt động quét virus do việc mở đi mở lại các tệp tin khi có nhiều loại phần mềm chống virus được cài đặt. Theo phương án thực hiện cụ thể, địa chỉ của hàm định trước MyNtCreateFile hoặc hàm định trước khác có thể được sử dụng để thay thế địa chỉ hàm được chứa trong bảng nhập. Phương án này không giới hạn địa chỉ hàm định trước cụ thể, và bất kì địa chỉ hàm nào mà có thể được sử dụng để qua mặt trình điều khiển bộ lọc tệp tin thì cũng đều có thể được áp dụng.

Ngoài ra, trước bước ghi nhận thao tác mở tệp tin thì phương pháp này còn bao gồm bước:

ghi lại thông số tương ứng với thao tác mở tệp tin;

trong đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số được ghi.

Bước thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng trong cấu trúc VPB vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều khiển ghi sẵn.

Bước thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

khởi động chương trình điều khiển ghi sẵn theo cách BOOT (khởi động), và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

Bước trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó bao gồm bước cụ thể là:

trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm

IoCreateFileSpecifyDeviceObjectHint, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

Theo phương pháp theo phương án này, thao tác mở tệp tin sẽ được ghi nhận, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.

Phương án nêu trên đã mô tả chi tiết về phương pháp theo phương án này. Chi tiết có thể được tìm thấy ở phương án nêu trên.

Phương án này đề xuất phương pháp mở tệp tin. Theo phương pháp này, trình điều khiển bộ lọc tệp tin của cách mở tệp tin gốc sẽ được qua mặt, và yêu cầu mở tệp tin sẽ được gửi trực tiếp đến hệ thống tệp tin để thực hiện hoạt động mở tệp tin. Điều này giảm bớt gánh nặng cho hệ thống vốn bị gây ra bởi hoạt động điều khiển của trình điều khiển bộ lọc tệp tin, và còn cải thiện tính tương thích hệ thống. Như được thể hiện trên Fig.2, phương pháp theo phương án này bao gồm các bước như sau:

201: Tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước.

Bảng nhập các tệp tin thư viện liên kết động 32-bit là bảng nhập tệp tin kernel32.dll cần thiết cho tệp tin thực thi được, trong đó có ghi địa chỉ của các hàm API hệ thống cần thiết cho các tệp tin. Tiến trình tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước là tiến trình móc.

Bằng cách móc vào lớp ứng dụng vòng, thì các hoạt động như mở tệp tin có thể được điều khiển đầu tiên, để sau khi thay thế địa chỉ, khi hàm gốc được gọi, thì tiến trình sẽ tiếp tục với việc hàm định trước thay thế hàm gốc. Phương án này không giới hạn về địa chỉ hàm gốc được chứa trong bảng nhập và địa chỉ hàm thay thế địa chỉ hàm gốc. Hàm được móc có thể là hàm `NtCreateFile` và `NtOpenFile`. Địa chỉ hàm định trước để thay thế địa chỉ hàm gốc có thể được thiết đặt nếu cần. Theo phương án thực hiện cụ thể, địa chỉ của hàm định trước `MyNtCreateFile` hoặc hàm định trước khác có thể được sử dụng để thay thế địa chỉ hàm được chứa trong bảng nhập. Phương án này không giới hạn địa chỉ hàm định trước cụ thể, và bất kì địa chỉ hàm nào mà có thể được sử dụng để qua mặt trình điều khiển bộ lọc tệp tin thì cũng đều có thể được áp dụng.

Như được minh hoạ trên Fig.3, sau khi thay thế địa chỉ hàm được chứa trong bảng nhập, thì tiến trình mở tệp tin sẽ được thay đổi từ tiến trình như được thể hiện bằng các hình mũi tên đứt nét sang tiến trình như được thể hiện bằng các hình mũi tên liền nét, nhờ đó qua mặt trình điều khiển bộ lọc tệp tin vốn có thể tồn tại ở tiến trình gốc.

Cần lưu ý rằng khi một tệp tin được mở nhiều lần hoặc nhiều tệp tin được mở đồng thời, thì bước 201 không cần phải được thực hiện lặp đi lặp lại, và địa chỉ hàm API của hệ thống được ghi trong bảng nhập `kernel32.dll` chỉ cần phải được thay thế một lần. Sau khi thay thế, mỗi lần hàm API gốc của hệ thống được gọi, thì hàm tương ứng với địa chỉ đã thay thế hàm gốc sẽ được gọi thực tế, nhờ đó qua mặt trình điều khiển bộ lọc tệp tin gốc. Tất nhiên là nếu cần đặt lại địa chỉ hàm định trước thì bước liên quan có thể được thực hiện lại để thay thế địa chỉ hàm được chứa trong bảng nhập bằng địa chỉ hàm định trước mới. Phương án này không đặt giới hạn nào về việc có thực hiện bước này hay không mỗi lần thực hiện phương pháp mở tệp tin này.

202: Ghi nhận thao tác mở tệp tin, và ghi lại thông số tương ứng với

thao tác mở tệp tin này.

Đối với bước này, phương án này không đặt giới hạn nào về cách thức ghi nhận thao tác mở tệp tin. Việc ghi nhận thao tác mở tệp tin có thể được thực hiện theo phương pháp thông thường, do phương pháp mở tệp tin thông thường cũng có thể bao gồm hoạt động ghi nhận thao tác mở tệp tin.

Phương án này không đặt giới hạn nào đối với thông số tương ứng với thao tác mở tệp tin. Thông số này bao gồm, nhưng không bị giới hạn ở, tên tệp tin, quyền được cấp, hoặc các yếu tố tương tự. Việc ghi lại thông số tương ứng với thao tác mở tệp tin là thao tác lưu thông số tương ứng với thao tác mở tệp tin vào bộ nhớ, để sau đó hoạt động mở tệp tin được thực hiện theo thông số được ghi.

203: Thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng.

Cụ thể, hệ thống tệp tin là ổ đĩa hoặc phân vùng để chứa các tệp tin, còn đối tượng thiết bị của hệ thống tệp tin có thể là ổ đĩa hoặc phân vùng cụ thể. Các tệp tin khác nhau thì tương ứng với các đối tượng thiết bị của hệ thống tệp tin khác nhau. Ví dụ, nếu tệp tin cần mở nằm ở ổ đĩa C, thì ổ đĩa C có thể được sử dụng như đối tượng thiết bị của hệ thống tệp tin tương ứng với tệp tin này. Hàm phân bố hệ thống tệp tin được sử dụng để thực hiện hoạt động mở tệp tin. Đối với các đối tượng thiết bị của hệ thống tệp tin khác nhau, thì nhiều hàm phân bố hệ thống tệp tin có thể được gọi. Khi đối tượng thiết bị của hệ thống tệp tin nhận được yêu cầu mở tệp tin, thì hàm phân bố hệ thống tệp tin tương ứng có thể được gọi. Theo phương án này, đối với đối tượng thiết bị của hệ thống tệp tin và hàm phân bố hệ thống tệp tin vốn được ghi nhận và được cải biến bởi trình điều khiển bộ lọc tệp tin, thì phương án này coi đối tượng thiết bị của hệ thống tệp tin tương ứng với tệp tin gốc mà trình điều khiển bộ lọc tệp tin chưa cải biến là đối tượng thiết bị của hệ thống tệp tin gốc. Hàm phân bố hệ thống tệp tin được gọi bởi đối tượng thiết bị của hệ thống tệp tin gốc thì được gọi là hàm phân bố hệ thống

tệp tin gốc.

Phương án này không đặt giới hạn nào về cách thức thu thập đối tượng thiết bị của hệ thống tệp tin gốc và địa chỉ hàm phân bố hệ thống tệp tin gốc. Trên thực tế, chương trình điều khiển để thu thập đối tượng thiết bị của hệ thống tệp tin gốc và địa chỉ hàm phân bố hệ thống tệp tin gốc có thể được ghi sẵn, và đối tượng thiết bị của hệ thống tệp tin gốc và địa chỉ hàm phân bố hệ thống tệp tin gốc có thể được thu thập nhờ sử dụng chương trình điều khiển được ghi sẵn này.

Do cấu trúc VPB ghi lại các đối tượng thiết bị của hệ thống tệp tin, nên đối tượng thiết bị của hệ thống tệp tin gốc tương ứng có thể được tìm kiếm trong cấu trúc VPB vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin này, nhờ sử dụng chương trình điều khiển ghi sẵn. Ngoài ra, do khi chương trình điều khiển ghi sẵn được khởi động theo cách BOOT, thì thông tin được ghi lại trong hệ thống là thông tin chưa bị cải biến và được tin cậy, hàm phân bố hệ thống tệp tin địa chỉ thu thập được trong lúc khởi động chương trình điều khiển theo cách BOOT là địa chỉ hàm phân bố hệ thống tệp tin gốc. Do đó, chương trình điều khiển ghi sẵn có thể được khởi động theo cách BOOT, và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng có thể được thu thập nhờ sử dụng chương trình điều khiển ghi sẵn này.

204: Trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, và truyền yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc.

Cụ thể là, khi yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, thì phương án này không đặt giới hạn nào về cách thức gửi yêu cầu mở tệp tin này. Trong quá trình thực hiện cụ thể, hàm `IoCreateFileSpecifyDeviceObjectHint` có thể được sử dụng, và yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, nhờ sử

dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

Hàm `IoCreateFileSpecifyDeviceObjectHint` là hàm API hiện có trên hệ thống Windows. Nhờ sử dụng hàm này mà yêu cầu mở tệp tin có thể được gửi trực tiếp đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó. Sau khi yêu cầu mở tệp tin được gửi đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, thì đối tượng thiết bị của hệ thống tệp tin gốc sẽ được kích hoạt để gọi hàm phân bố hệ thống tệp tin gốc tương ứng. Theo cách này, hệ thống tệp tin sẽ chuyển yêu cầu mở tệp tin đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc, và hàm phân bố hệ thống tệp tin gốc sẽ thực hiện hoạt động mở tệp tin, nhờ đó tránh được trình điều khiển bộ lọc tệp tin trung gian.

205: Thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước vốn thay thế địa chỉ hàm gốc và thông số được ghi.

Ở bước này, khi hàm phân bố hệ thống tệp tin gốc thực hiện hoạt động mở tệp tin theo địa chỉ hàm định trước vốn thay thế địa chỉ hàm gốc, thì tiến trình mở tệp tin gốc sẽ được cải biến. Như được minh họa trên Fig.3, các hình mũi tên đứt nét biểu thị tiến trình mở tệp tin gốc, trong đó, hàm `NtCreateFile` đã được thay thế bằng hàm `MyNtCreateFile`, và tiến trình mở tệp tin đã được cải biến từ tiến trình như được thể hiện bằng các hình mũi tên đứt nét sang tiến trình như được thể hiện bằng các hình mũi tên liền nét, nhờ đó tránh được trình điều khiển bộ lọc tệp tin vốn có thể tồn tại trong đó, và ngăn chặn các hoạt động không cần thiết như hoạt động quét virus đối với tệp tin do việc ghi nhận hoạt động truy cập của trình điều khiển bộ lọc vào tệp tin. Theo cách này, ngay cả khi có nhiều loại phần mềm chống virus được cài đặt, khi một tệp tin được mở bằng phương pháp theo phương án này, thì loại phần mềm chống virus khác sẽ không thể phát hiện được thao tác mở tệp tin, và không được kích hoạt để tiến hành hoạt động quét virus

trên tệp tin này, nhờ đó ngăn chặn vấn đề tương thích hệ thống và vấn đề tăng gánh nặng hệ thống.

Ngoài ra, cách mở tệp tin gốc sẽ được sử dụng khi hoạt động mở tệp tin được thực hiện nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số được ghi. Ví dụ, thông số tương ứng với thao tác mở tệp tin gốc thì biểu thị rằng tệp tin là có quyền đọc. Trong trường hợp này, trong lúc ghi lại thông số này và mở tệp tin theo thông số này, thì quyền đọc của tệp tin sẽ được duy trì để thống nhất với yêu cầu quyền đã được chỉ định theo phương pháp mở tệp tin gốc, nhờ đó sử dụng yêu cầu ban đầu của người dùng khi mở tệp tin.

Theo phương pháp theo phương án này, thao tác mở tệp tin sẽ được ghi nhận, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.

Phương án này đề xuất thiết bị mở tệp tin, trong đó, thiết bị này được cấu hình để thực hiện phương pháp mở tệp tin theo các phương án đã được mô tả trên đây. Như được thể hiện trên Fig.4, thiết bị này bao gồm

môđun ghi nhận 401, được cấu hình để ghi nhận thao tác mở tệp tin;

môđun thu thập thứ nhất 402, được cấu hình để thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận 401 ghi nhận được thao tác mở tệp tin;

môđun thu thập thứ hai 403, được cấu hình để thu thập địa chỉ hàm

phân bố hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận 401 ghi nhận được thao tác mở tệp tin;

môđun gửi 404, được cấu hình để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc, thu thập được nhờ môđun thu thập thứ nhất 402, được đặt ở đó, và chuyển yêu cầu mở tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc mà môđun thu thập thứ hai 403 thu thập được; và

môđun mở 405, được cấu hình để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc.

Chi tiết về cách thức mà môđun ghi nhận 401 ghi nhận thao tác mở tệp tin có thể được tìm thấy ở phần mô tả liên quan của bước 202 theo phương án đã được mô tả trên đây. Chi tiết về cách thức mà môđun thu thập thứ nhất 402 thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và cách thức mà môđun thu thập thứ hai 403 thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng có thể được tìm thấy ở phần mô tả liên quan của bước 203 ở phương án đã được mô tả trên đây. Chi tiết về cách thức mà môđun gửi 404 trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc, thu thập được bởi môđun thu thập thứ nhất 402, được đặt ở đó, và việc truyền yêu cầu mở tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc, thu thập được bởi môđun thu thập thứ hai 403, có thể được tìm thấy ở phần mô tả liên quan của bước 204 ở phương án đã được mô tả trên đây. Chi tiết về cách thức mà môđun mở 405 thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc có thể được tìm thấy ở phần mô tả liên quan của bước 205 ở phương án đã được mô tả trên đây. Do đó, các phần này sẽ không được mô tả thêm nữa.

Ngoài ra, với phần mô tả ở bước 201 theo phương án nêu trên, như được thể hiện trên Fig.5, thiết bị này còn bao gồm:

môđun thay thế 406, được cấu hình để tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

tương ứng theo đó, môđun mở 405 được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước, vốn được môđun thay thế 406 thay thế cho địa chỉ hàm gốc.

Ngoài ra, với phần mô tả ở bước 202 theo phương án nêu trên, như được thể hiện trên Fig.6, thiết bị này còn bao gồm:

môđun ghi lại 407, được cấu hình để ghi lại thông số tương ứng với thao tác mở tệp tin mà môđun ghi nhận 401 ghi nhận được; và

tương ứng theo đó, môđun mở 405 được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số mà môđun ghi lại 407 ghi được.

Môđun thu thập thứ nhất 402 được cấu hình cụ thể để tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng trong cấu trúc VPB vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều khiển ghi sẵn.

Môđun thu thập thứ hai 403 được cấu hình cụ thể để khởi động chương trình điều khiển ghi sẵn theo cách BOOT, và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

Môđun gửi 404 được cấu hình cụ thể để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm IoCreateFileSpecifyDeviceObjectHint, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

Với thiết bị theo phương án này, thao tác mở tệp tin sẽ được ghi nhận, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực

hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.

Phương án này còn đề xuất thiết bị đầu cuối, trong đó, thiết bị đầu cuối này bao gồm thiết bị mở tệp tin theo phương án đã được mô tả trên đây.

Thiết bị đầu cuối này có thể là thiết bị đầu cuối di động, hoặc có thể là máy tính cá nhân, hay các thiết bị đầu cuối khác. Phương án này không áp đặt giới hạn nào về dạng cụ thể của thiết bị đầu cuối.

Với thiết bị theo phương án này, thao tác mở tệp tin sẽ được ghi nhận nhờ sử dụng thiết bị mở tệp tin, yêu cầu mở tệp tin được gửi trực tiếp đến hệ thống tệp tin mà ở đó đối tượng thiết bị của hệ thống tệp tin gốc được đặt, và hoạt động mở tệp tin được thực hiện bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc. Hoạt động này sẽ qua mặt trình điều khiển bộ lọc tệp tin, nhờ đó giảm bớt các hoạt động không cần thiết của việc quét virus mỗi lần tệp tin được mở. Ngoài ra, khi có nhiều loại phần mềm chống virus được cài đặt, thì gánh nặng của hệ thống, vốn bị gây ra bởi hoạt động quét do việc mở đi mở lại các tệp tin, cũng được giảm bớt, nhờ đó mà tính tương thích hệ thống sẽ được cải thiện hơn nữa.

Cần lưu ý rằng, trong lúc mở tệp tin bằng thiết bị mở tệp tin theo phương án nêu trên, thì thiết bị này chỉ được mô tả bằng cách lấy một nhóm trong số các môđun chức năng nêu trên làm ví dụ. Trên thực tế, các hàm nêu trên có thể được ấn định cho các môđun chức năng khác nhau để thực hiện khi cần. Cụ thể là, xét về cấu trúc bên trong, thì thiết bị này được chia ra thành các môđun chức năng khác nhau để thực hiện toàn bộ hoặc một phần trong số các hàm đã được mô tả trên đây. Ngoài ra, thiết bị mở tệp tin và

thiết bị đầu cuối theo các phương án nêu trên là dựa trên cùng nguyên lý với phương pháp mở tệp tin theo sáng chế. Phương án thực hiện cụ thể của các thiết bị này có thể được suy ra từ các phương án về phương pháp nêu trên nên không được mô tả thêm nữa.

Chuyên gia trong lĩnh vực kỹ thuật này cần hiểu rằng các phương án về thiết bị nêu trên là chỉ được nêu làm ví dụ. Cụ thể là, các nhóm môđun nêu trên chỉ là nhóm chức năng logic, và chúng có thể là các nhóm khác khi thực hiện thực tế. Ví dụ, các khối/môđun chức năng khác nhau theo sáng chế có thể được hợp nhất lại thành một khối/môđun xử lý, hoặc là các khối/môđun độc lập về mặt vật lý; hoặc hai hay nhiều khối/môđun chức năng có thể được hợp lại thành một khối/môđun. Khối/môđun hợp nhất được có thể được thực hiện dưới dạng phần cứng, hoặc có thể được thực hiện dưới dạng khối/môđun chức năng phần mềm.

Chuyên gia trong lĩnh vực kỹ thuật này cần hiểu rằng toàn bộ hoặc một phần các bước của các phương pháp trên đây có thể được thực hiện bằng phần cứng hoặc phần cứng theo lệnh của các chương trình. Các chương trình này có thể được chứa trên phương tiện lưu trữ bất biến đọc được bằng máy tính, và có thể được thực thi bởi ít nhất một bộ xử lý. Phương tiện lưu trữ này có thể là bộ nhớ chỉ đọc, đĩa từ hoặc đĩa CD.

Phần mô tả trên đây chỉ là các phương án thực hiện ưu tiên của sáng chế chứ không nhằm giới hạn sáng chế. Các phương án cải biến, thay thế hoặc cải tiến tương đương mà không vượt quá ý tưởng và nguyên lý của sáng chế thì cũng nằm trong phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ:

1. Phương pháp mở tệp tin, phương pháp này bao gồm các bước:

ghi nhận thao tác mở tệp tin, và thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng và địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng; và

trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, truyền yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc, và thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc này.

2. Phương pháp theo điểm 1, trong đó, trước bước ghi nhận thao tác mở tệp tin, phương pháp này còn bao gồm bước:

tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

tương ứng theo đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước vốn thay thế địa chỉ hàm gốc.

3. Phương pháp theo điểm 1, trong đó, sau bước ghi nhận thao tác mở tệp tin, phương pháp này còn bao gồm bước:

ghi lại thông số tương ứng với thao tác mở tệp tin;

tương ứng theo đó, bước thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc bao gồm bước cụ thể tương ứng là:

thực hiện hoạt động mở tệp tin bằng cách sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số được ghi.

4. Phương pháp theo điểm 1, trong đó, bước thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng trong cấu trúc VPB (Volume Parameter Block - khối thông số ổ đĩa) vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều khiển ghi sẵn.

5. Phương pháp theo điểm 1, trong đó, bước thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng bao gồm bước cụ thể là:

khởi động chương trình điều khiển ghi sẵn theo cách BOOT, và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

6. Phương pháp theo điểm 1, trong đó, bước trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó bao gồm bước cụ thể là:

trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm IoCreateFileSpecifyDeviceObjectHint, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

2.7. Thiết bị mở tệp tin, thiết bị này bao gồm:

môđun ghi nhận, được cấu hình để ghi nhận thao tác mở tệp tin;

môđun thu thập thứ nhất, được cấu hình để thu thập đối tượng thiết bị của hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận ghi nhận được thao tác mở tệp tin;

môđun thu thập thứ hai, được cấu hình để thu thập địa chỉ hàm phân bố

hệ thống tệp tin gốc tương ứng sau khi môđun ghi nhận ghi nhận được thao tác mở tệp tin;

môđun gửi, được cấu hình để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc, thu thập được nhờ môđun thu thập thứ nhất, được đặt ở đó, và chuyển yêu cầu mở tệp tin này qua hệ thống tệp tin này đến hàm phân bố hệ thống tệp tin gốc tương ứng với địa chỉ hàm phân bố hệ thống tệp tin gốc mà môđun thu thập thứ hai thu thập được; và

môđun mở, được cấu hình để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc.

8. Thiết bị theo điểm 7, thiết bị này còn bao gồm:

môđun thay thế, được cấu hình để tìm kiếm bảng nhập các tệp tin thư viện liên kết động 32-bit và thay thế địa chỉ hàm được chứa trong bảng nhập này bằng địa chỉ hàm định trước;

tương ứng theo đó, môđun mở được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo địa chỉ hàm định trước, vốn được môđun thay thế thay thế cho địa chỉ hàm gốc.

9. Thiết bị theo điểm 7, thiết bị này còn bao gồm:

môđun ghi lại, được cấu hình để ghi lại thông số tương ứng với thao tác mở tệp tin mà môđun ghi nhận ghi nhận được; và

tương ứng theo đó, môđun mở được cấu hình cụ thể để thực hiện hoạt động mở tệp tin nhờ sử dụng hàm phân bố hệ thống tệp tin gốc theo thông số mà môđun ghi lại ghi được.

10. Thiết bị theo điểm 7, trong đó, môđun thu thập thứ nhất được cấu hình cụ thể để tìm kiếm đối tượng thiết bị của hệ thống tệp tin gốc tương ứng

trong cấu trúc VPB vốn ghi lại các đối tượng thiết bị của hệ thống tệp tin, nhờ sử dụng chương trình điều khiển ghi sẵn.

11. Thiết bị theo điểm 7, trong đó, môđun thu thập thứ hai được cấu hình cụ thể để khởi động chương trình điều khiển ghi sẵn theo cách BOOT, và thu thập địa chỉ hàm phân bố hệ thống tệp tin gốc tương ứng nhờ sử dụng chương trình điều khiển ghi sẵn này.

12. Thiết bị theo điểm 7, trong đó, môđun gửi được cấu hình cụ thể để trực tiếp gửi yêu cầu mở tệp tin đến hệ thống tệp tin mà đối tượng thiết bị của hệ thống tệp tin gốc được đặt ở đó, nhờ sử dụng hàm `IoCreateFileSpecifyDeviceObjectHint`, và nhờ sử dụng đối tượng thiết bị của hệ thống tệp tin gốc làm tham số.

13. Thiết bị đầu cuối bao gồm thiết bị mở tệp tin theo điểm bất kì trong số các điểm từ 7 đến 12.

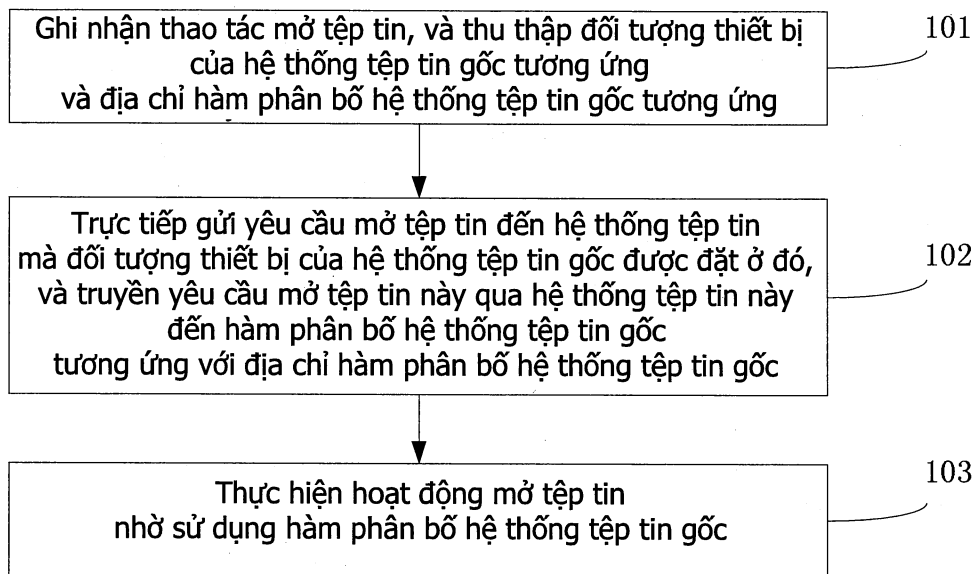


Fig.1

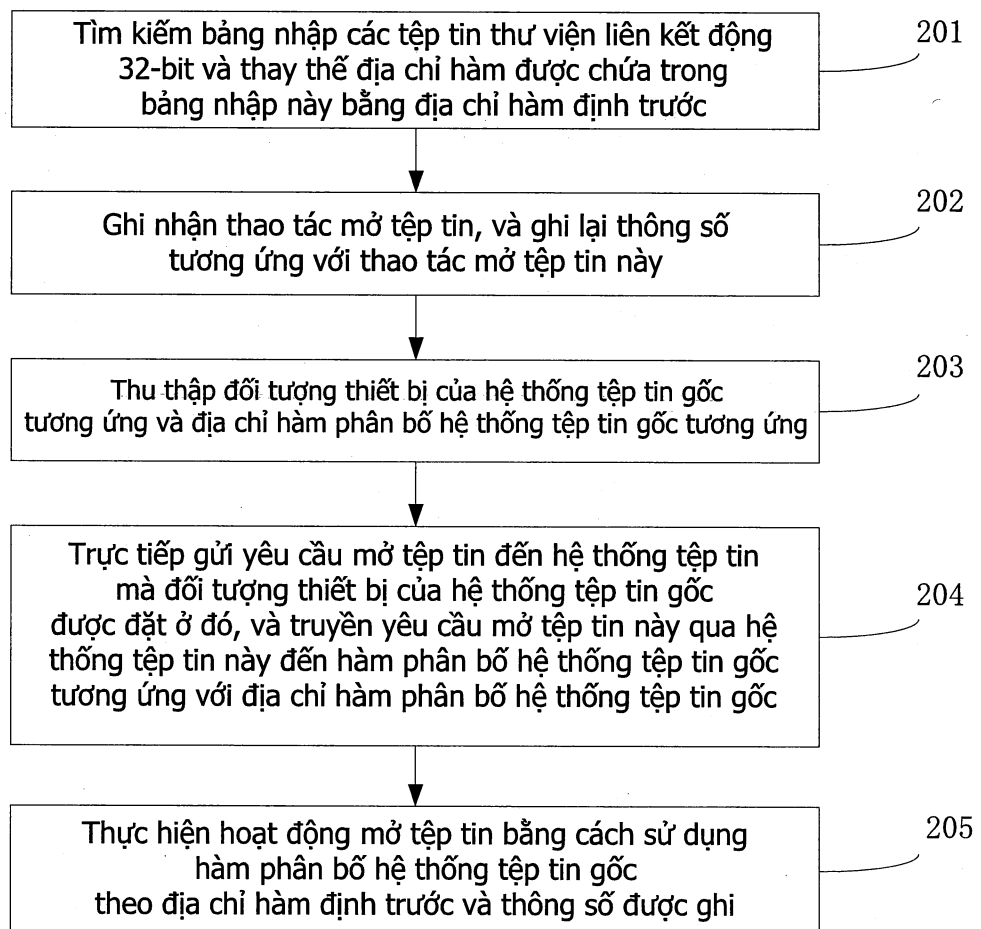


Fig.2

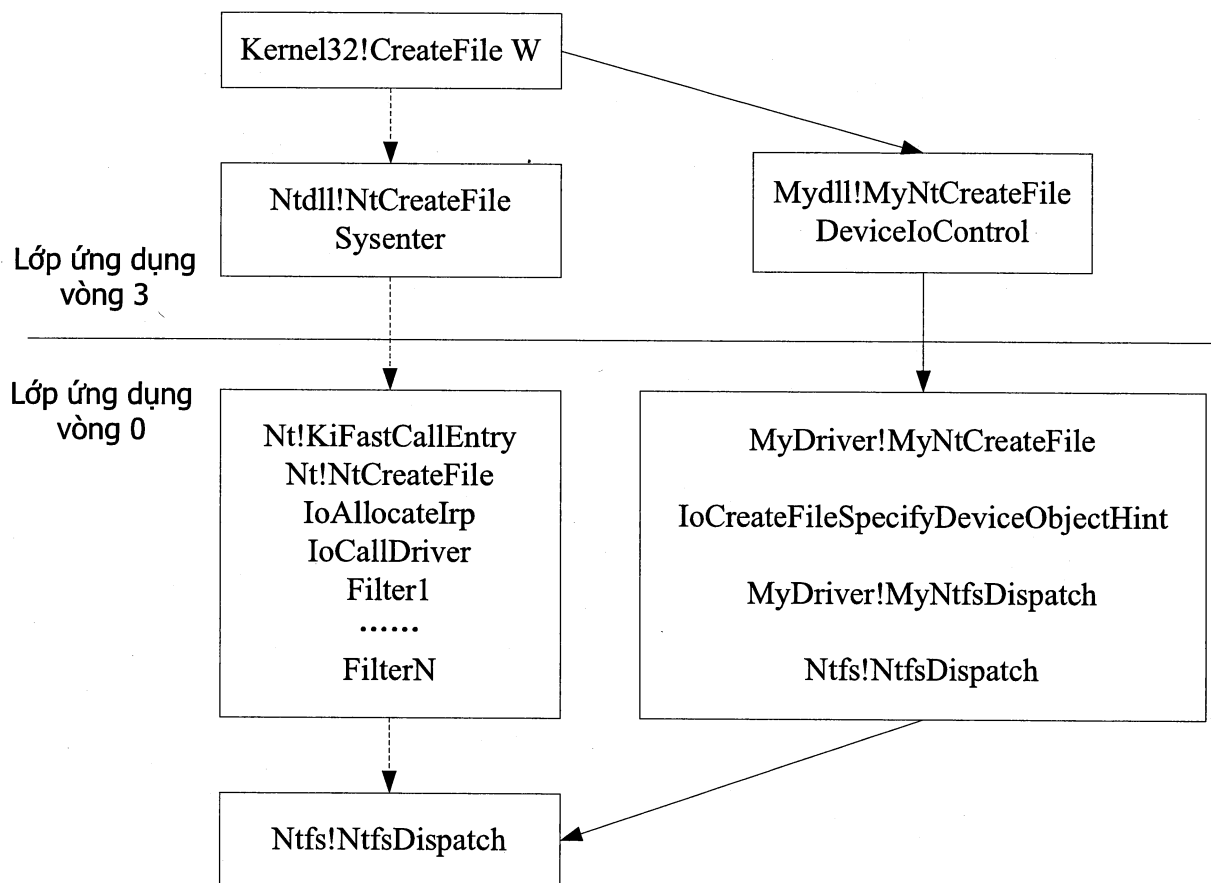


Fig.3

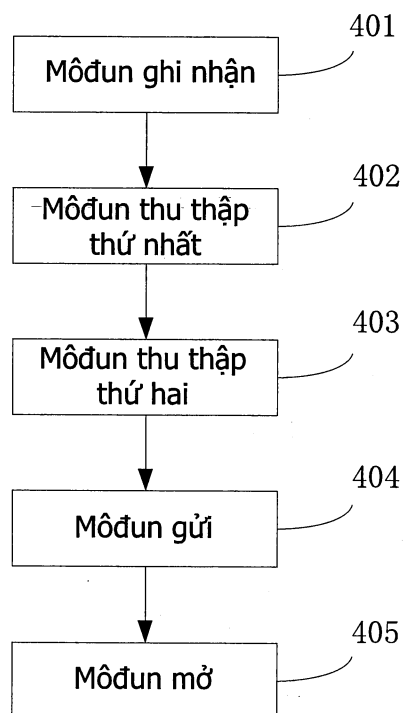


Fig.4

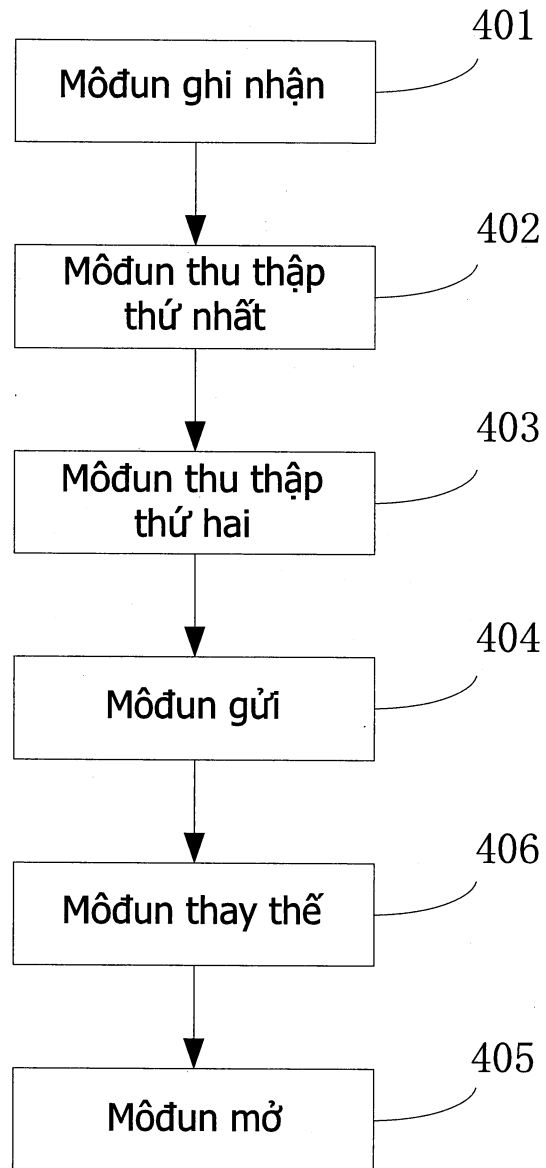


Fig.5

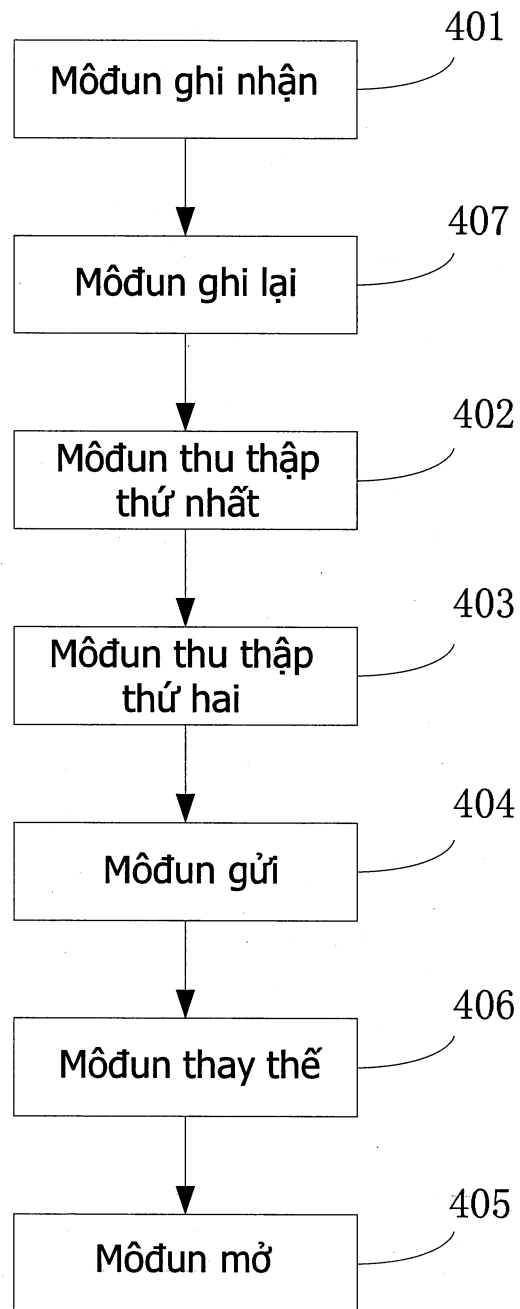


Fig.6