



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/528,127	09/27/2006	David H. Hanes	82224176	5903
22879	7590	12/02/2016	EXAMINER	
HP Inc. 3390 E. Harmony Road Mail Stop 35 FORT COLLINS, CO 80528-9544			JACKSON, JENISE E	
			ART UNIT	PAPER NUMBER
			2439	
			NOTIFICATION DATE	DELIVERY MODE
			12/02/2016	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipa.mail@hp.com  
barbl@hp.com  
yvonne.bailey@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* DAVID H. HANES

---

Appeal 2015-004014  
Application 11/528,127  
Technology Center 2400

---

Before CAROLYN D. THOMAS, JOHN F. HORVATH, and  
JOHN R. KENNY, *Administrative Patent Judges*.

THOMAS, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant seeks our review under 35 U.S.C. § 134(a) of the Examiner's Final Rejection of claims 4, 8, 12, 16, 18, and 20–22. Claims 1, 5, 9, and 17 are canceled and claims 2, 3, 6, 7, 10, 11, 13–15, 19, and 23 are indicated as either allowed or allowable. *See* Claim Appendix. We have jurisdiction over the appeal under 35 U.S.C. § 6(b).

We REVERSE.

The present invention relates generally to a virus scan process on a network attached storage device. *See* Abstract.

Claim 4 is illustrative:

4. A method, comprising:
  - initiating, by a network attached storage device, a virus scan process on the network attached storage device;
  - receiving, by the network attached storage device, a first file access request that identifies a file;
  - suspending the virus scan process to respond to the first file access request, wherein the virus scan process scans at least a subset of files in the network attached storage device; and
  - after suspending the virus scan process, initiating a virus scan process on the file identified in the first file access request.

Appellant appeals the following rejections:

Claims 4, 8, 12, 16, 18, and 20–22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Caccavale (US 7,363,657 B2, Apr. 22, 2008), McCorkendale (US 7,818,807 B1, Oct. 19, 2010), and Raz (US 7,861,302 B1, Dec. 28, 2010).

## ANALYSIS

**Issue:** Did the Examiner err in finding that McCorkendale teaches or suggests suspending the virus scan process to respond to the first access request, as set forth in each of independent claims 4, 12, 18, and 20?

Appellant contends that “it is clear that the malware scanning process **continues** to proceed when a request for a file is received (intercepted) in McCorkendale; there is clearly nothing in McCorkendale to indicate that any malware scanning is **suspended**” (App. Br. 7; *see also* Reply Br. 3).

In response, the Examiner finds that “McCorkendale discloses in a malware scanning scenario, security software is configure to intercept requests to execute particular files . . . Thus, the suspending, is the intercepting to respond to the file access request” (Ans. 2) because “[i]n the

Appeal 2015-00004014

Application 11/528,127

case that there are no associated prefetch files, security software **then initiates scanning** of the requested file” (*id.* at 3). We disagree with the Examiner.

In part, the Examiner directs our attention *supra* to when McCorkendale initiates scanning on the requested file, i.e., McCorkendale discloses “[i]n the case that there are no associated prefetch files, security software **30** then initiates scanning of the requested file” (5:10–12). However, we note that Appellant’s contention is directed to whether the virus scan is suspended, not when the requested file is scanned.

The Examiner also finds that “McCorkendale discloses suspending the virus scan process to respond to the first file access request . . . Thus, the suspending, is the intercepting to respond to the file access request” (Ans. 2). Regarding the intercepting of requests, McCorkendale specifically discloses that “[d]uring a scanning scenario, a control interception module **33** intercepts requests to execute one or more particular files” (*see* McCorkendale 4:55–57). In other words, McCorkendale’s intercepting of requests, i.e., responding to a file access request, is being performed during a scanning scenario. The Examiner has not explained how this equates to *suspending* the virus scan process to respond to the file access request. Given the lack of any supporting evidence in McCorkendale, we are constrained to conclude that the Examiner’s determination that the virus scan is suspended rests on speculation, unfounded assumptions and/or hindsight reconstruction of the claimed invention.

The Examiner also has not found that any of the other references of record teach or suggest this feature. Since we agree with at least one of the arguments advanced by Appellant, we need not reach the merits of

Appeal 2015-00004014

Application 11/528,127

Appellant's other arguments. Accordingly, we will *not* sustain the Examiner's obviousness rejection of the claims.

#### DECISION

The decision of the Examiner to reject claims 4, 8, 12, 16, 18, and 20–22 is reversed.

REVERSED