DECLARATION UNDER PENALTY OF PERJURY

RE: IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data;

BY: Daniel David Rigmaiden

I, Daniel David Rigmaiden, declare[1] the following:

1. On August 3, 2008, the government searched my home while executing the N.D.Cal. 08-70460-HRL/PVT search warrant.[2] During the search, the government physically seized my home computer, physical data storage devices, encrypted virtual drives, and various physical evidence. During the physical search of my home and in the months[3] following the search, IRS-CI Agent Tracy L. Daun imaged my data storage devices and encrypted virtual drives by mirroring/copying them to government hard drives.[4] Likewise, the data storage device and encrypted virtual drive seized from my storage unit during the August 4, 2008 execution of the N.D.Cal. 08-70502-PVT search warrant[5] were imaged by IRS-CI Agent Daun in the same fashion.[6]

---

1. This declaration is being submitted under the protections of *Simmons*. *See* Simmons v. United States, 390 U.S. 377, 394 (1968) (Holding that "when a defendant testifies in support of a motion to suppress evidence on Fourth Amendment grounds, his testimony may not thereafter be admitted against him at trial on the issue of guilt unless he makes no objection."). I object to the government attempting to introduce this declaration as evidence at trial.

2. *See Submission Of Materials Related To Search Warrant No. 08-70460, Authorized By Magistrate Judge Patricia V. Trumbull, Northern District Of California, On July 30, 2008* (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #464-1, p. 20) (return).

3. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 8) (table with "1/9/2009" entry marking the last DriveCrypt encrypted virtual drive that was imaged).

4. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Tracy L. Daun stating that she conducted a partial live acquisition of my "T" drive using WinRAR and imaged the remainder of the drives using IXimager).

5. *See Submission Of Documents Related To Northern District Of California 08-70502-HRL Search Warrant Used To Physically Search Storage Unit No. A-47* (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #846-2).

6. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #863-1, p. 29-36) (IRS-CI Agent Daun discussing physical data storage device and encrypted virtual drive seized from storage unit No. A-47).

DECLARATION UNDER PENALTY OF PERJURY

RE: IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data;

BY: Daniel David Rigmaiden

---

2. Once the seized data storage devices and encrypted virtual drives were imaged, IRS-CI Agent Daun began what would end up being a 401-day exploratory rummaging through the files contained on my home computer, data storage devices, and encrypted virtual drives. According to the October 22, 2012 prosecution report, IRS-CI Agent Daun would not complete her search and seizure of data from the forensic images and virtual machine clones until September 8, 2009[7]—371 days past the 30-day deadline for search/seizure of data as permitted by the N.D.Cal. 08-70460-HRL/PVT warrant[8] and 370 days past the 30-day deadline for search/seizure of data as permitted by the N.D.Cal. 08-70502-PVT warrant.[9]

3. In addition to taking 401 days to *complete* her forensic analysis, IRS-CI Agent Daun took nearly **six months** to even *begin* her forensic analysis of the DriveCrypt encrypted virtual drives corresponding to "filesalot.dcv," "filesalot_bak_3-1-2008.dcv," and "filesalot_bak_3-31-2008.dcv"[10]—the drives containing the bulk of the digital *in-scope* evidence seized from my home and storage unit. Likewise, IRS-CI Agent Daun took more than

7. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 9) (table with "8/14/2009 through 9/8/2009" entry stating "Prepared reports and extracted files from the analysis on the computer media.").

8. *See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #566-2, p. 16) ("The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and **no later than thirty (30) calendar days** after the initial execution of the warrant." (emphasis added)).

9. *See Submission Of Documents Related To Northern District Of California 08-70502-HRL Search Warrant Used To Physically Search Storage Unit No. A-47*, "Computer Search Protocol For The Northern District Of California," ¶ 5 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #846-2, p. 8) ("The government must complete an off-site search of a device that agents removed in order to search for evidence of crime as promptly as practicable and **no later than thirty (30) calendar days** after the initial execution of the warrant." (emphasis added)).

10. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 8) (table with "2/2/2009," "2/13/2009," and "3/1/2009" entries indicating the dates IRS-CI Agent Daun began her forensic analysis of my DriveCrypt encrypted virtual drives).

---

nine months to even *begin* her forensic analysis of the WinRAR live acquisition image of the "T" drive, *i.e.*, "T_drive.rar."[11] Although IRS-CI Agent Daun and the other case agents began arbitrarily rummaging through virtual machine clones of my entire computer system immediately after the physical drives were seized, the forensic analyses intended to determine whether any irrelevant, personal information was improperly seized was not started for **any** imaged drive until February 2, 2009.[12]

4. In order to facilitate the seizure of data at the conclusion of her initial 401-day exploratory rummaging, IRS-CI agent Daun searched through the forensic images, extracted all files that fell within the scope of the warrants, and then copied some of those files to DVDs and a CD so that they would be isolated (*i.e.*, seized) from the images. This forensic search process, occurring off and on between February 2, 2009 and September 8, 2009, took **219 days** even while IRS-CI Agent Daun admitted that she could have been finished in roughly **60 days**, *i.e.*, "by late March or early April."[13] IRS-CI Agent Daun had plenty of free time to complete her forensic analysis from the start, however, she instead opted to spend the first 33 days, *i.e.*, August 3, 2008 through September 4, 2008,[14] creating virtual machine clones of my entire

11. *See id.*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 9) (table with "5/20/2009" entry stating "Started analysis on WinRAR live acquisition ran onsite at search warrant.").

12. *See id.*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 8).

13. *See Sixth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #933-1); A review of the entries in the October 22, 2012 table also support IRS-CI Agent Daun's claim of being *capable* of completing the analysis within **60 days**. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 8-9) (For example, filesalot.dcv forensic analysis took 16 days, filesalot_bak_3-1-2008.dcv forensic analysis took 11 days, and IBM ThinkPad forensic analysis took 3 days.).

14. *See id.*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 9) (table with 8/3/2008 through 9/4/2008 entries detailing the time IRS-CI Agent Daun devoted to creating the virtual machine clones instead of

computer system to facilitate the untrained exploratory rummaging of three other case agents. Apart from the three other case agents, the actual process of searching and seizing my digital data **through a forensic analysis** is explained in IRS-CI Agent Daun's "Computer Forensic Report," originally provided to the defense via discovery on February 25, 2010[15]—more than **six months** after the report's completion on September 8, 2009. The "Computer Forensic Report" states under numerous "Analysis" headings that, "[t]he following is a summary of the evidence located on the computer that fell within the parameters of the Search Warrant and the Items to be Seized."[16]

5. After conducting her initial 401-day search, IRS-CI Agent Daun continued her personal exploratory rummaging into the forensic images at least until January 1, 2012,[17] *i.e.*, an additional 28 months following the September 8, 2009 creation of the noted CD and DVDs.

6. In order to justify IRS-CI Agent Daun's extended 401-day search and additional 28-month search, the prosecution claimed that "the length of time that the United States has spent analyzing the lawfully seized material is reasonable in light of... the defendant's efforts at concealing his crimes through encryption..."[18] In reply, I pointed out to the Court and to the

conducting the forensic analysis).

15. *See Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #863-1) ("Computer Forensic Report" by IRS-CI Agent Daun RE: search of data storage devices and encrypted virtual drives seized from apartment No. 1122 and storage unit No. A-47).

16. *See id.*, p. 31.

17. *See Fifth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #929-1, p. 9) (table indicating that IRS-CI Agent Daun reaccessed the forensic images on "1/12/2012" to extract data for the prosecution).

18. *Government's Response To Defendant's Motion To Suppress* (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #873, p. 68).

DECLARATION UNDER PENALTY OF PERJURY

RE: IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data;

BY: Daniel David Rigmaiden

---

prosecution that IRS-CI Agent Daun was able get around my DriveCrypt encryption as soon as she sat down at my home computer.[19][20] This declaration details my efforts to locate additional evidence showing the government's lack of need and/or interest in decrypting my encrypted data. As a result of the efforts detailed in this declaration, I determined that the government chose to not seize one of my DriveCrypt encrypted virtual drives, *i.e.*, "installed.dcv," of which IRS-CI Agent Daun could not decrypt and access when she sat down at my computer. The noted encrypted virtual drive was not mounted as a logical hard drive at the time of the search and IRS-CI Agent Daun was not able to decrypt the data considering she did not know the password. Even while the warrant permitted the seizure of encrypted data for the sole purpose of cracking encryption over an extended period of time,[21] IRS-CI agent Daun had no interest in "installed.dcv." This lack of interest further bellies the government's claim that the extended search was reasonable due to the government's interest in my encrypted data —an interest that was clearly nonexistent.

7. The efforts explained in this declaration were conducted using my defense laptop

---

19. *Id.* (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #873, p. 26) ("Fortunately for the investigation team,... [w]hen entry was made pursuant to the search warrant, [the] defendant's computer was found to be unsecured and logged on, no password was needed in this instance in order to access the files.").

20. *See Fourth Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 14 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #898-1) (**August 25, 2008** email from IRS-CI Agent Daun to AUSA Battista: "I was able to image each of the items and feel pretty confident that I have gotten around the encryption issue.").

21. *See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California," ¶ 3 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #566-2, p. 15-16) ("The government may also remove and retain the device, equipment, or document if the government determines that the information on the device is encrypted, until such reasonable time as it is determined that it does not contain any information that falls within the scope of the warrant.").

computer (*i.e.*, IBM ThinkPad T43), which has an NTFS formatted system drive running the Microsoft Windows XP SP3 operating system,[22] while logged in with Administrator permissions. In order to conduct my tests, I used software called AccessData FTK Imager, Nuance PDF Reader, and Microsoft Windows file explorer. Because there was a lack of necessity, no expert level computer knowledge or expert level computer forensic knowledge was referenced.

8. Via the October 26, 2011 discovery set provided to the defense by the government, I received three hard drives containing data copied from various physical hard drives seized by the government. The government also provided instructions on how to access the seized data. One of the hard drives (Hard Drive #3) contained forensic images of hard drives connected to my personal home computer located at 431 El Camino Real, Apartment No. 1122, Santa Clara, CA 95050 at the time of the execution of the N.D.Cal. 08-70460-HRL/PVT search warrant.

9. Following the government's instructions, I used my defense laptop computer and software called AccessData FTK Imager to mount (in read only mode)[23] one of the

22. Attached to this declaration as ATTACHMENT 01 is a screenshot of relevant system information and disk partition information as displayed by my defense laptop computer using the command line commands "Systeminfo" and "Diskpart." The precise command entered at the command-prompt was as follows:

```
echo. & date /t & time /t & echo. & systeminfo | findstr /b /c:"OS Name" /c:"OS
Version" /c:"System Up Time" & echo. & echo list volume | diskpart | findstr
/c:"Volume #" /c:"Volume 1" & echo.
```

23. In order to access drive "K," I employed both hardware based and software based write-protection. Hardware based write-protection was implemented using a Digital Intelligence Write Blocker hard drive enclosure. *See* Digital Intelligence [website], *USB3 Write Blocker Hard Drive Enclosure*, http://www.digitalintelligence.com/cart/ComputerForensicsProducts/3.5-Inch-USB3-Hard-Drive-Enclosure---WRITE-BLOCKER.html (last accessed: Feb. 3, 2011). Software based write-protection was implemented using AccessDate FTK

government's images contained on Hard Drive #3: 1000220515_S1_RmA_C2_hdd0 – forensic image files of the Acer MS2180 laptop hard drive.[24] Once mounted, a new drive letter (*i.e.*, drive "K") appeared within my operating system and I could read the data within the image.[25]

10. Located in the root directory of drive "K" was the DriveCrypt encrypted virtual drive, "installed.dcv."[26] IRS-CI Agent Daun noted in her "Computer Forensic Report" that "[t]he only item located on the [Acer] computer that fell within the parameters of the Search Warrant and the Items to be Seized was recovered text from a deleted file that referred to IRS publications."[27] In other words, IRS-CI Agent Daun made no mention of seizing "installed.dcv." In order to confirm that "installed.dcv" was not seized, I used Nuance PDF Reader to search through IRS-CI Agent Daun's list of seized *in-scope* files.[28] The list was provided to me in a series of PDF files via the government's June 2, 2011 discovery set. As a result of my search, Nuance reported that "installed.dcv" was not one of the files listed, *i.e.*, "Search Total Num: 0."[29] Even while the warrant permitted the seizure of encrypted data for

Imager. *See* AccessData Group [website], *Computer Forensics Software for Digital Investigations*, http://www.accessdata.com/products/digital-forensics/ftk (last accessed: Nov. 19, 2012).

24. *See* ATTACHMENT 02; *see also Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #863-1, p. 28) ("Computer Forensic Report" by IRS-CI Agent Daun discussing the Acer MS2180 laptop).

25. *See* ATTACHMENT 03.

26. *See* ATTACHMENT 04.

27. *Third Submission Of Consolidated Exhibits Relating To Discovery And Suppression Issues*, EXHIBIT 01 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #863-1, p. 28) ("Computer Forensic Report" by IRS-CI Agent Daun discussing the Acer MS2180 laptop).

28. Attached to this declaration as ATTACHMENT 05 and ATTACHMENT 06 are screenshots of the Nuance PDF search.

29. Attached to this declaration as ATTACHMENT 07 is a screenshot of the Nuance PDF search showing zero results

---

the sole purpose of cracking encryption over an extended period of time,[30] IRS-CI agent Daun had no interest in "installed.dcv." This lack of interest further bellies the government's claim that the extended search was reasonable due to the government's interest in my encrypted data —an interest that was clearly nonexistent.

* * * * *

11. I declare, certify, verify, and state under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge, except as to those matters which are therein stated on information and belief, and, as to those matters, I believe it to be true. *See* 28 U.S.C. § 1746 ("Wherever... any matter is required or permitted to be supported, evidenced, established, or proved by the sworn... affidavit, in writing of the person making the same [], such matter may, with like force and effect, be supported, evidenced, established, or proved by the unsworn declaration..., in writing of such person which is subscribed by him, as true under penalty of perjury, and dated..."); 18 U.S.C. § 1621 ("Whoever... in any declaration... under penalty of perjury as permitted under section 1746 of title 28, United States Code, willfully subscribes as true any material matter which he does not believe to be true... is guilty of perjury and shall, except as otherwise expressly provided by law, be fined under this title or imprisoned not more than five years, or both....").

---

for "installed.dcv.".

30. *See Submission Of Documents Related To Original Northern District Of California 08-70460-HRL Search Warrant Used To Physically Search Apartment No.* 1122, *Warrant*, "Computer Search Protocol For The Northern District Of California," ¶ 3 (U.S. v. Rigmaiden, CR08-814-PHX-DGC, D.Ariz., Dkt. #566-2, p. 15-16) ("The government may also remove and retain the device, equipment, or document if the government determines that the information on the device is encrypted, until such reasonable time as it is determined that it does not contain any information that falls within the scope of the warrant.").

DECLARATION UNDER PENALTY OF PERJURY

RE: IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data;

BY: Daniel David Rigmaiden

Executed on January 30, 2013, in Florence, Arizona, United States of America.

Daniel David Rigmaiden

Daniel Rigmaiden

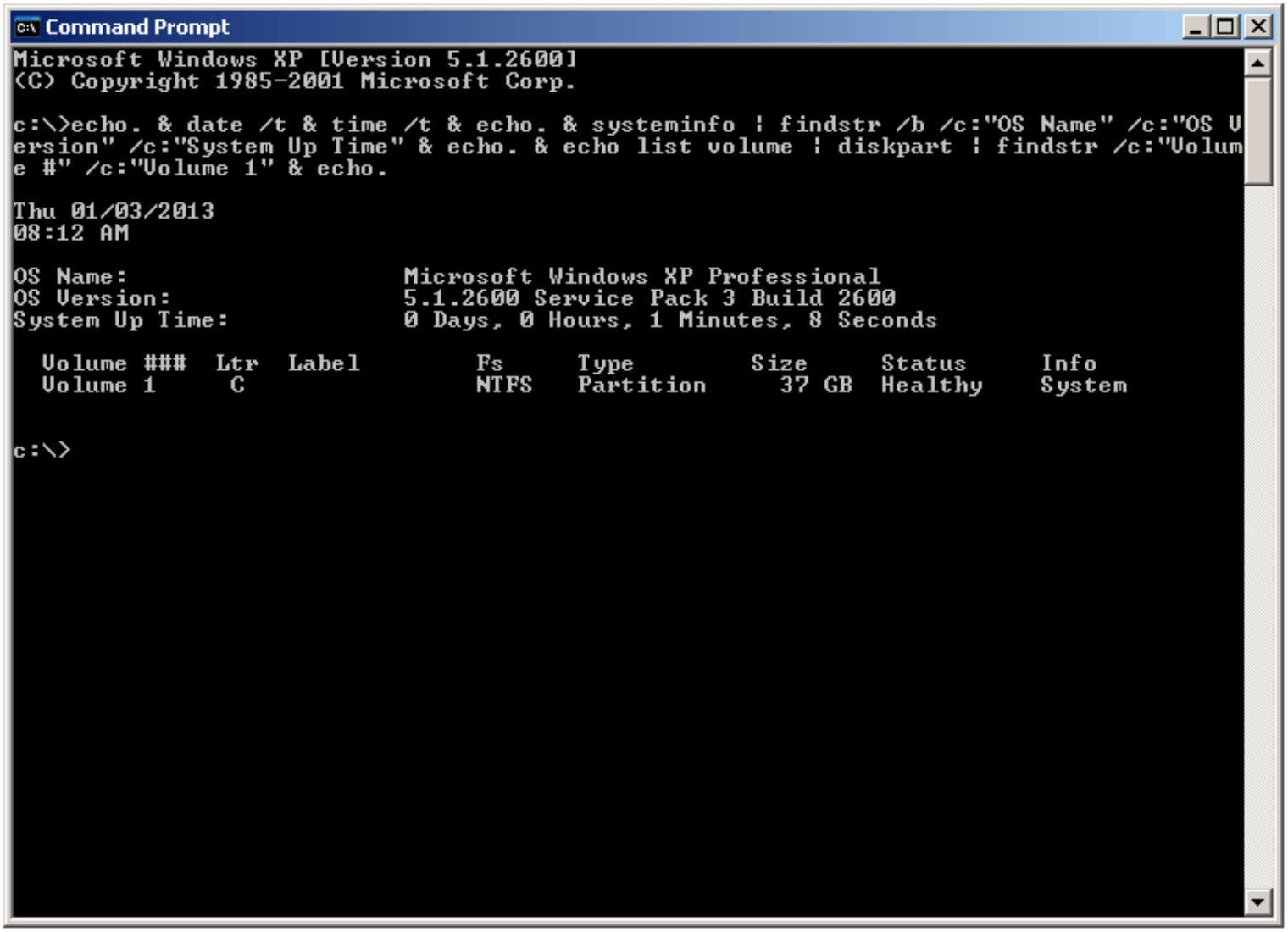
Daniel Rigmaiden
Agency # 10966111
CCA-CADC
PO Box 6300
Florence, AZ 85132

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 01

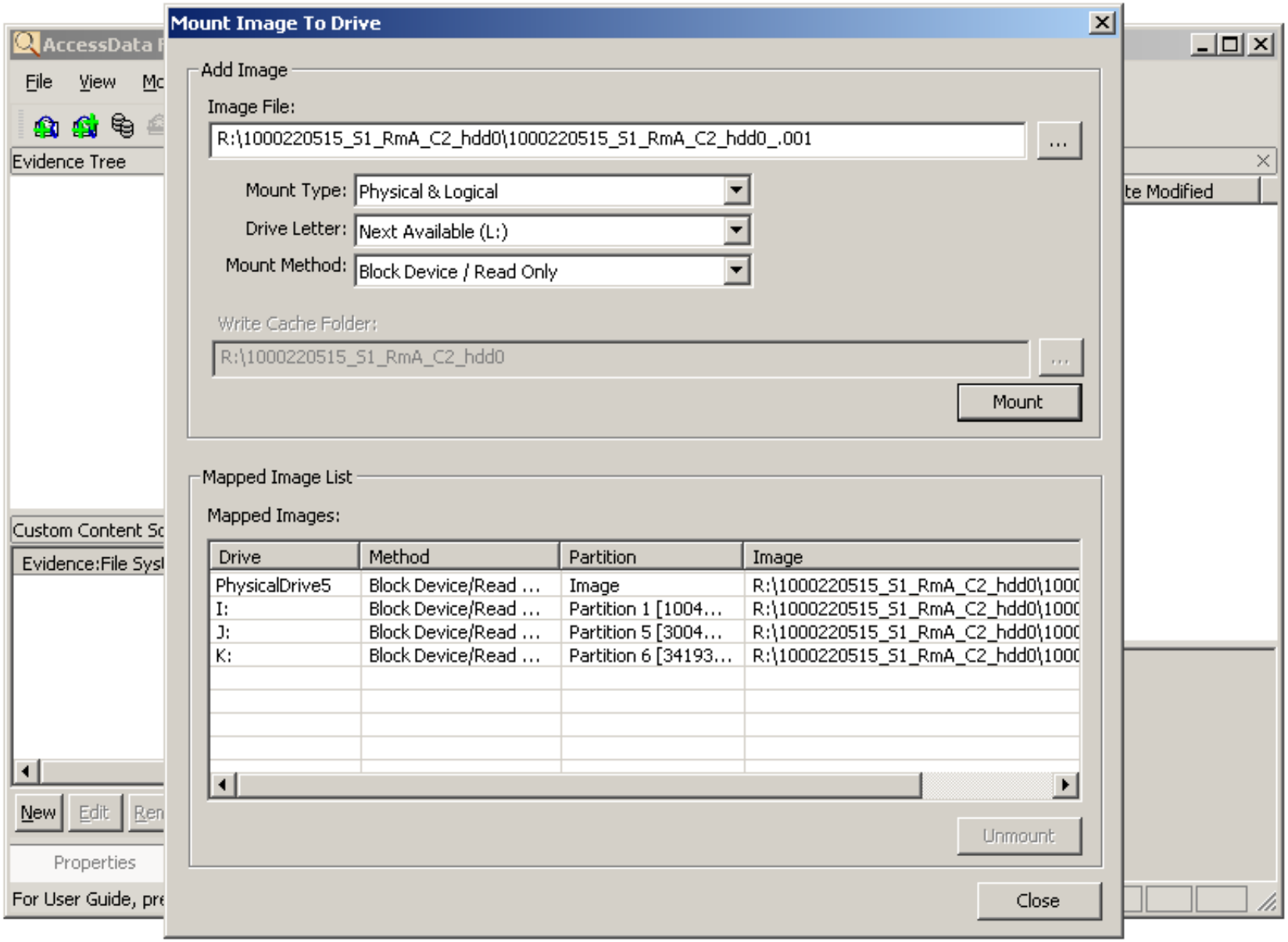

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
c:\>echo. & date /t & time /t & echo. & systeminfo | findstr /b /c:"OS Name" /c:"OS V
ersion" /c:"System Up Time" & echo. & echo list volume | diskpart | findstr /c:"Volum
e #" /c:"Volume 1" & echo.
Thu 01/03/2013
08:12 AM
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Service Pack 3 Build 2600
System Up Time: 0 Days, 0 Hours, 1 Minutes, 8 Seconds
Volume ### Ltr Label Fs Type Size Status Info
Volume 1 C NTFS Partition 37 GB Healthy System
c:\>

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 02

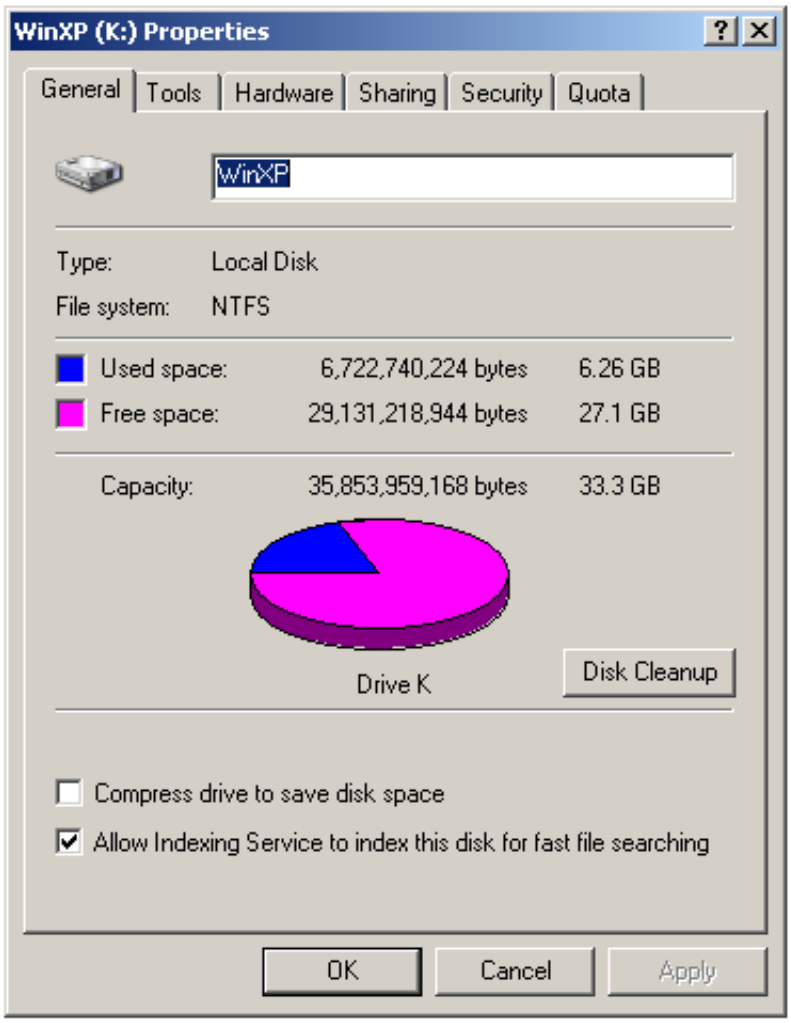

Mount Image To Drive
Add Image
Image File:
R:\1000220515_S1_RmA_C2_hdd0\1000220515_S1_RmA_C2_hdd0_.001
Mount Type:
Physical & Logical
Drive Letter:
Next Available (L:)
Mount Method:
Block Device / Read Only
Write Cache Folder:
R:\1000220515_S1_RmA_C2_hdd0
Mount
Mapped Image List
Mapped Images:
Drive
Method
Partition
Image
PhysicalDrive5
Block Device/Read ...
Image
R:\1000220515_S1_RmA_C2_hdd0\1000
I:
Block Device/Read ...
Partition 1 [1004...
R:\1000220515_S1_RmA_C2_hdd0\1000
J:
Block Device/Read ...
Partition 5 [3004...
R:\1000220515_S1_RmA_C2_hdd0\1000
K:
Block Device/Read ...
Partition 6 [34193...
R:\1000220515_S1_RmA_C2_hdd0\1000
Unmount
Close
AccessData
File
View
Evidence Tree
Custom Content Sc
Evidence:File Syst
New
Edit
Properties
For User Guide, pre
te Modified

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 03

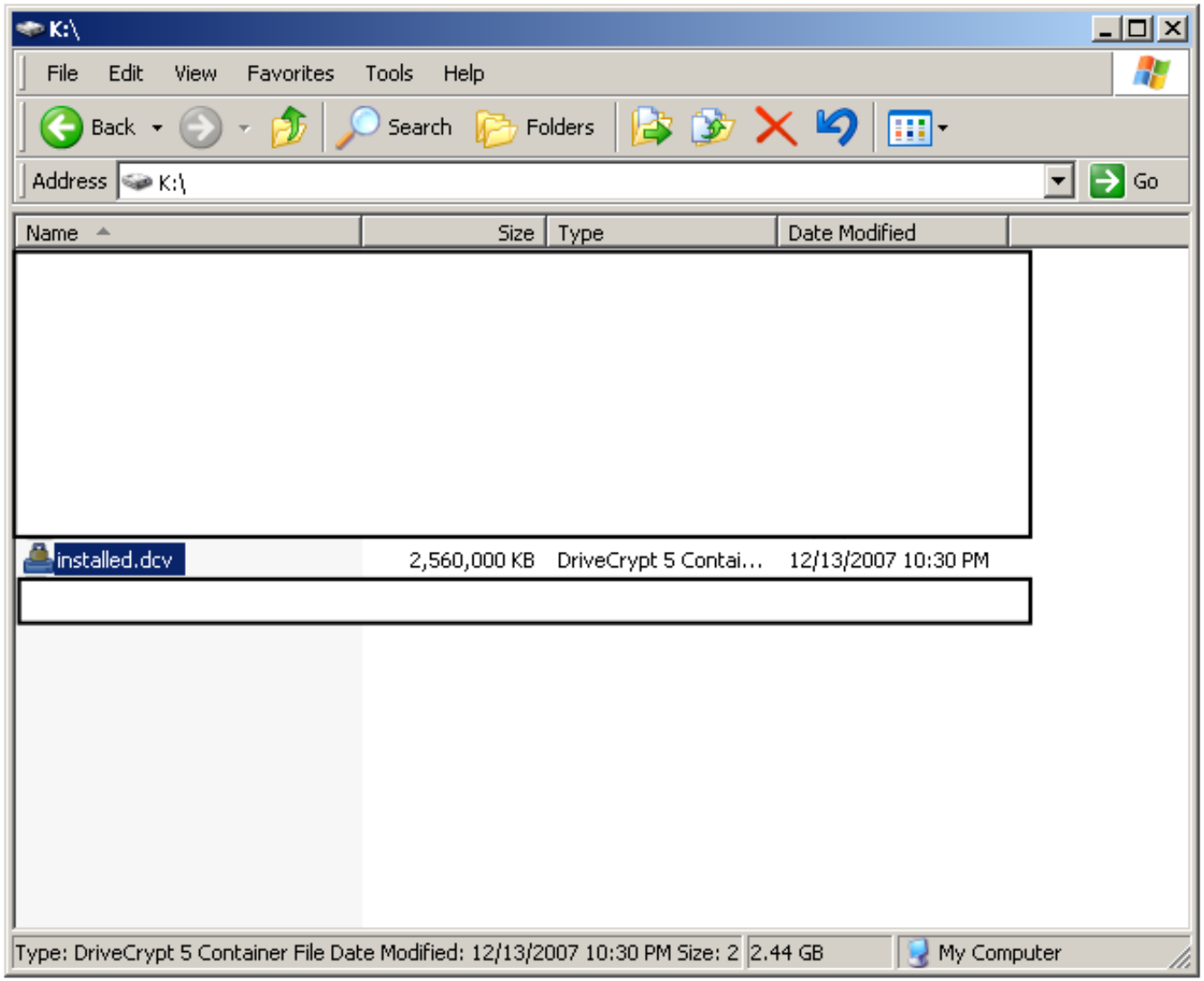

WinXP (K:) Properties
General
Tools
Hardware
Sharing
Security
Quota
WinXP
Type: Local Disk
File system: NTFS
Used space: 6,722,740,224 bytes 6.26 GB
Free space: 29,131,218,944 bytes 27.1 GB
Capacity: 35,853,959,168 bytes 33.3 GB
Drive K
Disk Cleanup
Compress drive to save disk space
Allow Indexing Service to index this disk for fast file searching
OK
Cancel
Apply

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 04

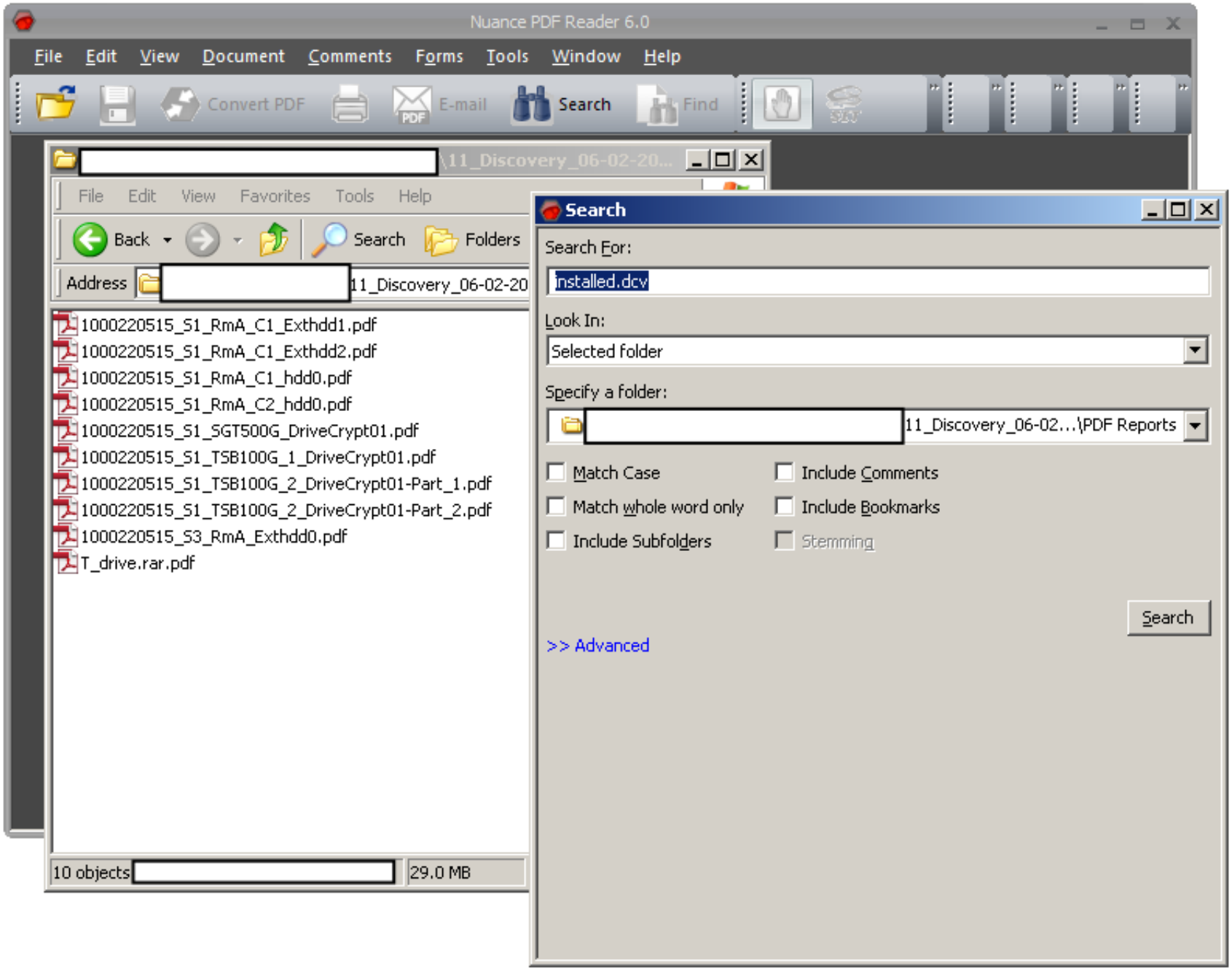

K:\
File Edit View Favorites Tools Help
Back Search Folders
Address K:\
Go
Name Size Type Date Modified
installed.dcv 2,560,000 KB DriveCrypt 5 Contai... 12/13/2007 10:30 PM
Type: DriveCrypt 5 Container File Date Modified: 12/13/2007 10:30 PM Size: 2
2.44 GB
My Computer

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 05

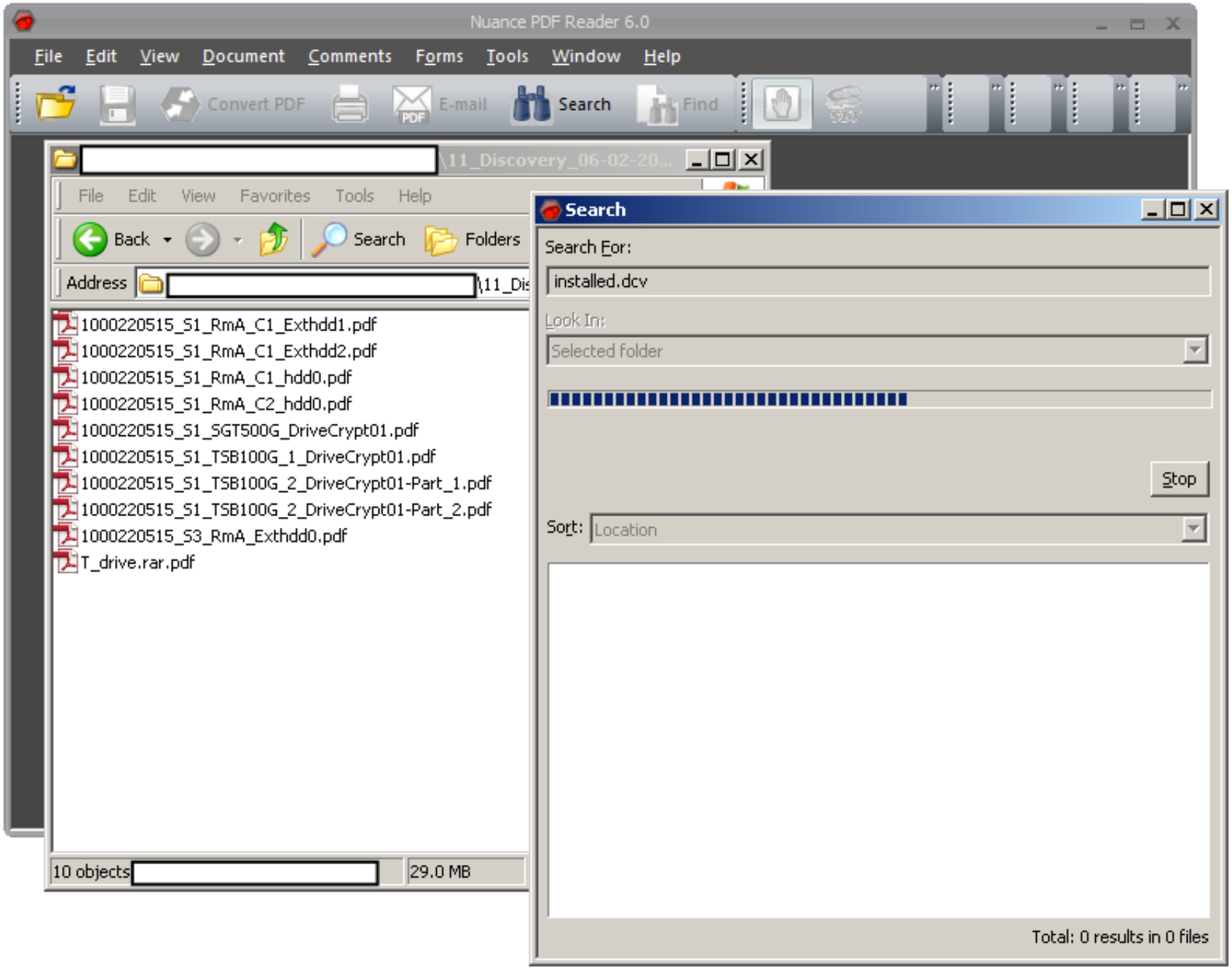

Nuance PDF Reader 6.0
File Edit View Document Comments Forms Tools Window Help
Convert PDF
E-mail
Search
Find
11_Discovery_06-02-20...
File Edit View Favorites Tools Help
Back
Search
Folders
Address
11_Discovery_06-02-20
1000220515_S1_RmA_C1_Exthdd1.pdf
1000220515_S1_RmA_C1_Exthdd2.pdf
1000220515_S1_RmA_C1_hdd0.pdf
1000220515_S1_RmA_C2_hdd0.pdf
1000220515_S1_SGT500G_DriveCrypt01.pdf
1000220515_S1_TSB100G_1_DriveCrypt01.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_1.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_2.pdf
1000220515_S3_RmA_Exthdd0.pdf
T_drive.rar.pdf
10 objects
29.0 MB
Search
Search For:
installed.dcv
Look In:
Selected folder
Specify a folder:
11_Discovery_06-02...\PDF Reports
Match Case
Match whole word only
Include Subfolders
Include Comments
Include Bookmarks
Stemming
Search
>> Advanced

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 06

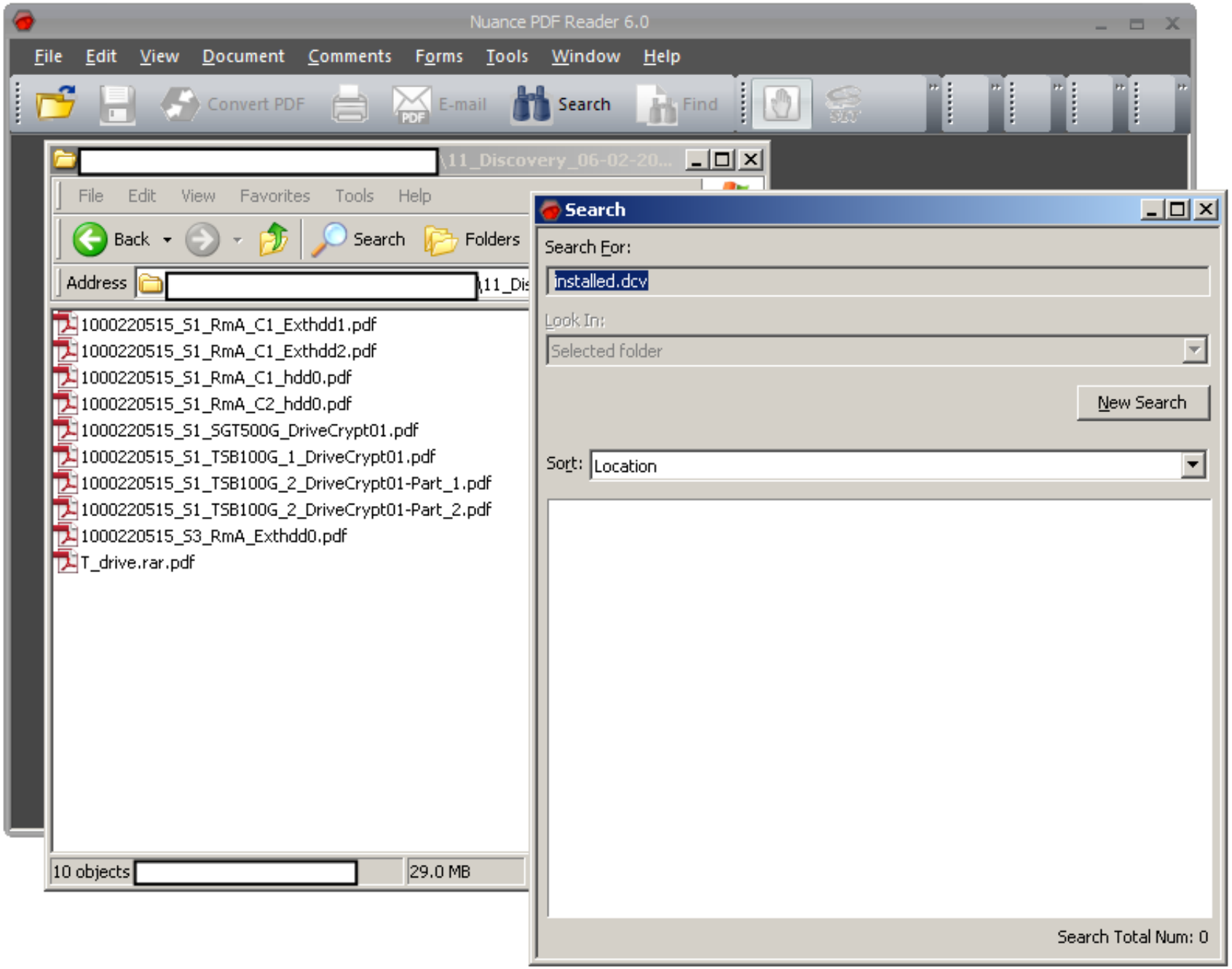

Nuance PDF Reader 6.0
File Edit View Document Comments Forms Tools Window Help
Convert PDF
E-mail
Search
Find
File Edit View Favorites Tools Help
Back
Search
Folders
Address
1000220515_S1_RmA_C1_Exthdd1.pdf
1000220515_S1_RmA_C1_Exthdd2.pdf
1000220515_S1_RmA_C1_hdd0.pdf
1000220515_S1_RmA_C2_hdd0.pdf
1000220515_S1_SGT500G_DriveCrypt01.pdf
1000220515_S1_TSB100G_1_DriveCrypt01.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_1.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_2.pdf
1000220515_S3_RmA_Exthdd0.pdf
T_drive.rar.pdf
10 objects
29.0 MB
Search
Search For:
installed.dcv
Look In:
Selected folder
Stop
Sort:
Location
Total: 0 results in 0 files

DECLARATION UNDER PENALTY OF PERJURY

IRS-CI Agent Daun's 401-day search and additional 28-month search of Rigmaiden's computer system was not for the purpose of circumventing or paying additional attention to encrypted data

By Daniel Rigmaiden

ATTACHMENT 07


Nuance PDF Reader 6.0
File Edit View Document Comments Forms Tools Window Help
Convert PDF
E-mail
Search
Find
File Edit View Favorites Tools Help
Back
Search
Folders
Address
1000220515_S1_RmA_C1_Exthdd1.pdf
1000220515_S1_RmA_C1_Exthdd2.pdf
1000220515_S1_RmA_C1_hdd0.pdf
1000220515_S1_RmA_C2_hdd0.pdf
1000220515_S1_SGT500G_DriveCrypt01.pdf
1000220515_S1_TSB100G_1_DriveCrypt01.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_1.pdf
1000220515_S1_TSB100G_2_DriveCrypt01-Part_2.pdf
1000220515_S3_RmA_Exthdd0.pdf
T_drive.rar.pdf
10 objects
29.0 MB
Search
Search For:
installed.dcv
Look In:
Selected folder
New Search
Sort:
Location
Search Total Num: 0