

KNOPPIX
Bootable CD
Validation Study
for
Live Forensic
Preview of Suspects
Computer

By:

Ernest Baca

www.linux-forensics.com
ebaca@linux-forensics.com

Introduction

I have recently become very interested in the Linux approach to previewing a suspect's computer. In many instances a forensics examiners job requires that they preview a suspect's computer and locate evidence before further search or seizure can take place. I have utilized a very reliable and suitable Windows tool to accomplish this task in the past. Although I believed that this tool is very suitable for forensic preview of a suspect's computer, I also believe that computer forensics agents should have alternative solutions for accomplishing computer forensic tasks. The more tools a computer forensics agent has gives him / her the flexibility to solve computer forensics issues more efficiently and effectively. The tool should be chosen given the circumstances of each situation.

I have become very involved in the use of Linux as a data forensic tool. Linux brings power and flexibility to data forensics. One of the beauties of Linux is the ability to mount partitions in read only mode. This dispenses with the need for hardware or software write blockers. I also like the idea that a full Linux system will fit on a bootable disk. I recently became aware of a bootable CD distribution of Linux called KNOPPIX. What makes KNOPPIX different than most bootable CD distributions of LINUX? What makes it different is the fact that KNOPPIX is a full GUI distribution of Linux on a bootable CD which is easy to use and very flexible.

I began to examine this distribution of Linux and felt that it would make a very useful tool for data forensic previews. I also noticed that it had excellent hardware detection capabilities. As a matter of fact it places icons on your desktop for each partition on the system. When you click on the icon KNOPPIX will mount the partition in read only mode. Experimenting with it revealed that conducting a data forensic preview with KNOPPIX was almost seamless. I have also read several post on the national HTCIA listserv that indicate that law enforcement is already using KNOPPIX as a data forensic preview solution.

I quickly began to research to see if KNOPPIX had been validated for data forensics. I was unable to find any validation studies so I decided to do a validation study of my own. This paper gives the results of my study. I think you will find some of the results to be very startling.

Hardware Equipment

Custom Built Computer
AMD 2000+ XP processor
512MB DDR PC2700 RAM
USB2.0
2 Removable Hard Drive Bays
PQI Intellistick Thumb Drive

Software Equipment

Gentoo Linux System – Found at www.gentoo.org

SMART Data Forensics Software for Linux – Found at www.asrdata.com.

KNOPPIX Bootable CD – Found at www.knopper.net.

Media Being Previewed

1 20GB Western Digital Hard Drive with SUSE Linux 8.1 installed

/dev/hda1 → EXT3 partition

/dev/hda2 → Linux Swap

/dev/hda3 → reiserfs Partition

/dev/hda4 → EXT2 partition

Note: I only chose these Linux file systems because they are the most common

1 20GB Western Digital Hard Drive with Windows XP installed

/dev/hda1 → NTFS partition

1 20GB Western Digital Hard Drive with Windows 200 installed

/dev/hda1 → FAT32 partition

Testing Methodology

A. Validation of Tools

1. Boot computer in to Gentoo Linux system with test drive installed in removable bay.
2. Load SMART data forensic software and obtain initial hash of test drive (Save hash results to thumb drive using SMART reporting function).
3. Shutdown system and then boot system again into Gentoo Linux system.
4. Load SMART data forensic software and obtain another hash (Save hash results to thumb drive using SMART reporting function) and compare with previous values from step 2. If values match, neither Gentoo nor SMART changed state of drive therefore validating them as tools for this test.
5. Shutdown Gentoo and remove Gentoo hard drive from system.

B. Testing Phase

1. With test drive still in boot KNOPPIX CD with *noswap* option, mount partition read-only, search for JPG and WAV files using file manager, unmount partition, shutdown KNOPPIX, and turn off computer.
2. Re-insert Gentoo hard drive and boot into Gentoo system.

3. Load SMART data forensic software and obtain another hash (Save hash results to thumb drive using SMART reporting function) and compare with previous values from previous hash of drive. Examine hash values for any changes. If changes occur use current hash value as new benchmark hash.
4. If more than one partition on drive repeat steps 5 through 8 and compare hash value with previous hash value to observe any changes.
5. Do testing phase for each drive.

Initial Hash for ETX2, Linux Swap, EXT3, reiser Drive for Validation

SMART Report

Created by: SSA Ernest Baca
Mon May 26 10:38:56 2003

Session Login (*Time:* Mon May 26 08:58:44 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Mon May 26 08:59:29 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Mon May 26 10:28:52 2003 - *User:* SSA Ernest Baca)
Elapsed time: 1 hours, 29 minutes, and 23 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: 943eec24dc99295967062db0ca700a8c
→ **Hash of Entire Drive**
2. 0:32256: ab52361bf7ec4d4688bd9618786916f5
→ **Unallocated Space (MBR)**

3. 32256:526385664: b808c06c08f3892ba9414f6e490853d4
→ **EXT3 Partition (Boot Partition) /dev/hda1**
4. 526417920:1077511680: c7e7fb801960b68f16f2014ddb46a3f7
→ **Linux Swap (Swap Partition) /dev/hda2**
5. 1603929600:12889013760: 8c0b839eabbd128272d443998553bec4
→ **reiserfs Partition (root partition) /dev/hda3**
6. 14492943360:5527388160: 796049a029d30117ba06c2f602fa1bef
→ **EXT2 Partition (Home Directory partition) /dev/hda4**
7. 20020331520:64512: 18b2002279d695f8b7963aa1e1212b89
→ **Unallocated space (wasted space)**

User Note (*Time:* Mon May 26 10:38:51 2003 - *User:* SSA Ernest Baca)
Initial hash of Linux system with ETX2, ETX3, reiserfs on 20 Gig Western Digital ATA 100 drive.

Test Note: Initial hash of system

Validation Step

SMART Report

Created by: SSA Ernest Baca
Tue May 27 11:00:24 2003

Session Login (*Time:* Tue May 27 09:22:07 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Tue May 27 09:22:16 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Tue May 27 10:54:46 2003 - *User:* SSA Ernest Baca)

Elapsed time: 1 hours, 32 minutes, and 30 seconds.

Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: 943eec24dc99295967062db0ca700a8c
→ **Hash of Entire Drive**
2. 0:32256: ab52361bf7ec4d4688bd9618786916f5
→ **Unallocated Space (MBR)**
3. 32256:526385664: b808c06c08f3892ba9414f6e490853d4
→ **EXT3 Partition (Boot Partition) /dev/hda1**
4. 526417920:1077511680: c7e7fb801960b68f16f2014ddb46a3f7
→ **Linux Swap (Swap Partition) /dev/hda2**
5. 1603929600:12889013760: 8c0b839eabbd128272d443998553bec4
→ **reiserfs Partition (root partition) /dev/hda3**
6. 14492943360:5527388160: 796049a029d30117ba06c2f602fa1bef
→ **EXT2 Partition (Home Directory partition) /dev/hda4**
7. 20020331520:64512: 18b2002279d695f8b7963aa1e1212b89
→ **Unallocated space (wasted space)**

User Note (*Time:* Tue May 27 11:00:18 2003 - *User:* SSA Ernest Baca)

Hash to Verify that Gentoo system and SMART did not change drive state. After initial hash and shutdown of computer without mounting drive.

Test Note: No changes to drive noticed. Gentoo nor SMART changed state of drive

Hash after booting with KNOPPIX CD with *noswap*, mounting EXT2 partition (/dev/hda4) read-only, search for JPG and WAV files using KDE file manager and shutdown of computer.

SMART Report

Created by: SSA Ernest Baca

Tue May 27 12:42:23 2003

Session Login (*Time:* Tue May 27 11:10:31 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Tue May 27 11:10:37 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Tue May 27 12:39:44 2003 - *User:* SSA Ernest Baca)
Elapsed time: 1 hours, 29 minutes, and 7 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: 943eec24dc99295967062db0ca700a8c
→ **Hash of Entire Drive**
2. 0:32256: ab52361bf7ec4d4688bd9618786916f5
→ **Unallocated Space (MBR)**
3. 32256:526385664: b808c06c08f3892ba9414f6e490853d4
→ **EXT3 Partition (Boot Partition) /dev/hda1**
4. 526417920:1077511680: c7e7fb801960b68f16f2014ddb46a3f7
→ **Linux Swap (Swap Partition) /dev/hda2**
5. 1603929600:12889013760: 8c0b839eabbd128272d443998553bec4
→ **reiserfs Partition (root partition) /dev/hda3**
6. 14492943360:5527388160: 796049a029d30117ba06c2f602fa1bef
→ **EXT2 Partition (Home Directory partition) /dev/hda4**
7. 20020331520:64512: 18b2002279d695f8b7963aa1e1212b89
→ **Unallocated space (wasted space)**

User Note (*Time:* Tue May 27 12:42:18 2003 - *User:* SSA Ernest Baca)
Hash after Boot of KNOPPIX Bootable CD and read-only mount of EXT2 partition (/dev/hda4). Then shutdown of KNOPPIX.

Test Note: No changes in any hash values noticed when comparing current hash values to previous hash values. Mounting EXT2 read-only did not change the state of the drive.

Hash after booting with KNOPPIX CD with *noswap* option, mounting reiserfs partition read-only(/dev/hda3), search for JPG and WAV files using KDE file manager and shutdown of computer.

SMART Report

Created by: SSA Ernest Baca
Tue May 27 14:48:48 2003

Session Login (*Time: Tue May 27 13:15:37 2003*)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time: Tue May 27 13:16:03 2003 - User: SSA Ernest Baca*)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time: Tue May 27 14:46:44 2003 - User: SSA Ernest Baca*)
Elapsed time: 1 hours, 30 minutes, and 41 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: 66da2d11dfb5f47da2f58441027d1679
→ **Hash of Entire Drive**
2. 0:32256: ab52361bf7ec4d4688bd9618786916f5
→ **Unallocated Space (MBR)**
3. 32256:526385664: b808c06c08f3892ba9414f6e490853d4
→ **EXT3 Partition (Boot Partition) /dev/hda1**
4. 526417920:1077511680: c7e7fb801960b68f16f2014ddb46a3f7

- **Linux Swap (Swap Partition) /dev/hda2**
5. 1603929600:12889013760: c34c2ccd4494a5a25f38b5a8485af67d
→ **reiserfs Partition (root partition) /dev/hda3**
6. 14492943360:5527388160: 796049a029d30117ba06c2f602fa1bef
→ **EXT2 Partition (Home Directory partition) /dev/hda4**
7. 20020331520:64512: 18b2002279d695f8b7963aa1e1212b89
→ **Unallocated space (wasted space)**
-

User Note (*Time:* Tue May 27 14:48:42 2003 - *User:* SSA Ernest Baca)
Hash after KNOPPIX Booable CD, mount read-only of reiserfs partition (/dev/hda3), search for JPG and WAV files, unmount and shutdown of computer.

Test Note: When comparing current hash values with hash values from the previous test a change was noticed in Line 1 which is the entire drive hash. Change also noticed on Line 5 which is the reiserfs partition. Mounting reiserfs partition seems to have changed that partition thus changing the state of the drive. Please note the current hash value will be used to compare next set of hash values.

Hash after booting with KNOPPIX CD with *noswap* option, mounting EXT3 partition read-only(/dev/hda1), search for JPG and WAV files using KDE file manager and shutdown of computer.

SMART Report

Created by: SSA Ernest Baca
Tue May 27 19:51:09 2003

Session Login (*Time:* Tue May 27 18:09:55 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Tue May 27 18:10:02 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (Time: Tue May 27 19:38:25 2003 - User: SSA Ernest Baca)

Elapsed time: 1 hours, 28 minutes, and 23 seconds.

Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: b76b9805f4f7f2d3e15d1935519b8f97
→ **Hash of Entire Drive**
2. 0:32256: ab52361bf7ec4d4688bd9618786916f5
→ **Unallocated Space (MBR)**
3. 32256:526385664: 43915c9dd0803d5a3a2a3f71d5ebd511
→ **EXT3 Partition (Boot Partition) /dev/hda1**
4. 526417920:1077511680: c7e7fb801960b68f16f2014ddb46a3f7
→ **Linux Swap (Swap Partition) /dev/hda2**
5. 1603929600:12889013760: c34c2ccd4494a5a25f38b5a8485af67d
→ **reiserfs Partition (root partition) /dev/hda3**
6. 14492943360:5527388160: 796049a029d30117ba06c2f602fa1bef
→ **EXT2 Partition (Home Directory partition) /dev/hda4**
7. 20020331520:64512: 18b2002279d695f8b7963aa1e1212b89
→ **Unallocated space (wasted space)**

User Note (Time: Tue May 27 19:51:03 2003 - User: SSA Ernest Baca)

Hash after Boot of KNOPPIX Bootable CD, Mount of EXT3 Partition (/dev/hda1), search for JPG and WAV files, then shutdown of KNOPPIX.

Test Note: When comparing current hash values with hash values from previous test a change was noticed in Line 1 which is the entire drive hash. Change also noticed on Line 3 which is the EXT3 partition (Partition that was mounted read-only). Mounting EXT3 partition seems to have changed that partition thus changing the state of the drive.

Initial hash of Windows XP NTFS Drive

SMART Report

Created by: SSA Ernest Baca
Wed May 28 06:48:16 2003

Session Login (*Time: Tue May 27 23:59:03 2003*)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time: Tue May 27 23:59:13 2003 - User: SSA Ernest Baca*)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time: Wed May 28 01:27:40 2003 - User: SSA Ernest Baca*)
Elapsed time: 1 hours, 28 minutes, and 27 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: c71fd32eb91caa5e2b15d52bd8ab02da
→ **Hash of Entire Drive**
 2. 0:32256: 54ebd8e1ac69875e0e7bc26e8d1dc56c
→ **Unallocated Space (MBR)**
 3. 32256:20012073984: aab29139cb9d12b4b36af2298e87bb79
→ **Windows XP NTFS Partition /dev/hda1**
 4. 20012106240:8289792: 0e5ff6fbd67ceef3f1f33ec4c73d5020
→ **Unallocated space (wasted space)**
-

User Note (*Time: Wed May 28 06:48:03 2003 - User: SSA Ernest Baca*)
Initial hash of NTFS Windows XP system.

Test Note: Initial hash of Windows XP NTFS System

Hash after booting with KNOPPIX CD with *noswap* option, mounting NTFS partition read-only(/dev/hda1), search for JPG and WAV files using KDE file manager and shutdown of computer.

SMART Report

Created by: SSA Ernest Baca
Wed May 28 22:03:39 2003

Session Login (*Time:* Wed May 28 20:32:56 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Wed May 28 20:33:06 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Wed May 28 22:02:26 2003 - *User:* SSA Ernest Baca)
Elapsed time: 1 hours, 29 minutes, and 20 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: c71fd32eb91caa5e2b15d52bd8ab02da
→ **Hash of Entire Drive**
 2. 0:32256: 54ebd8e1ac69875e0e7bc26e8d1dc56c
→ **Unallocated Space (MBR)**
 3. 32256:20012073984: aab29139cb9d12b4b36af2298e87bb79
→ **Windows XP NTFS Partition /dev/hda1**
 4. 20012106240:8289792: 0e5ff6fbd67ceef3f1f33ec4c73d5020
→ **Unallocated space (wasted space)**
-

User Note (*Time:* Wed May 28 22:03:32 2003 - *User:* SSA Ernest Baca)
Hash after KNOPPIX Bootable CD boot, mount read-only of Windows XP NTFS partition, search for JPG and WAV files, and shutdown of computer.

Test Note: A comparison of hash values shows no change. Appears that mounting NTFS read-only did not change the state of the drive.

Initial hash of Windows 2000 FAT32 Drive

SMART Report

Created by: SSA Ernest Baca
Thu May 29 23:24:36 2003

Session Login (*Time:* Wed May 28 23:51:23 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Wed May 28 23:51:34 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Thu May 29 01:17:51 2003 - *User:* SSA Ernest Baca)
Elapsed time: 1 hours, 26 minutes, and 17 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: a078850e38c02bce7392377a08dc2b2b
→ **Hash of Entire Drive**
 2. 0:32256: b94a9cc7990ec6b02dc354b096b779d4
→ **Unallocated Space (MBR)**
 3. 32256:20012073984: 10d6cead8ce2adadfb6c0a9b42f1d504
→ **Windows 2000 FAT32 Partition /dev/hda1**
 4. 20012106240:8289792: 0e5ff6fbd67ceef3f1f33ec4c73d5020
→ **Unallocated space (wasted space)**
-

User Note (*Time:* Thu May 29 23:24:30 2003 - *User:* SSA Ernest Baca)
Initial Hash of Windows 2000 system on FAT32 partition.

Test Note: Initial hash to Windows 2000 FAT32 Drive

Hash after booting with KNOPPIX CD with *noswap* option, mounting FAT32 partition read-only(/dev/hda1), search for JPG and WAV files using KDE file manager and shutdown of computer.

SMART Report

Created by: SSA Ernest Baca
Fri May 30 07:38:08 2003

Session Login (*Time:* Thu May 29 23:58:00 2003)
User 'SSA Ernest Baca' logged in.

'Produce Hash' task started. (*Time:* Thu May 29 23:58:48 2003 - *User:* SSA Ernest Baca)
Hashing: /dev/ide/host0/bus0/target1/lun0/disc

'Produce Hash' task complete. (*Time:* Fri May 30 01:24:18 2003 - *User:* SSA Ernest Baca)
Elapsed time: 1 hours, 25 minutes, and 30 seconds.
Hash: /dev/ide/host0/bus0/target1/lun0/disc

Hash Summary

MD5 Span Hashes

1. total span hash: a078850e38c02bce7392377a08dc2b2b
→ **Hash of Entire Drive**
2. 0:32256: b94a9cc7990ec6b02dc354b096b779d4
→ **Unallocated Space (MBR)**
3. 32256:20012073984: 10d6cead8ce2adadfb6c0a9b42f1d504
→ **Windows 2000 FAT32 Partition /dev/hda1**

4. 20012106240:8289792: 0e5ff6fbd67ceef3f1f33ec4c73d5020
→ **Unallocated space (wasted space)**
-

User Note (*Time: Fri May 30 07:38:03 2003 - User: SSA Ernest Baca*)

Hash after Boot of KNOPPIX CD, mount of FAT32 partition read-only, search for JPG and WAV files, and then shutdown of KNOPPIX.

Test Note: A comparison of hash values shows no change. Appears that mounting FAT32 read-only did not change the state of the drive.

Conclusion

It was quite startling to find that mounting EXT3 and reiserfs partitions read-only changed the state of the drive. I was very perplexed as to why the hash values changed. I quickly tried to do some further testing by trying to write to a reiserfs and EXT3 partition mounted read-only while booted with the KNOPPIX CD. I found that it would not let me write to the drive, which is telling me it is mounted read-only. At first I thought it was KNOPPIX so I conducted several similar tests on other Linux systems and came up with the same results. This is possibly a problem with Linux in general. I can only figure that since EXT3 and reiserfs are journaling file systems the journal is somehow changed. I am no expert on file systems so I can't be sure.

The one thing that comes out of this test is that Law Enforcement must be careful in using this tool when encountering Linux systems. This may become a possible evidence issue. Now take in to consideration that this paper is not offering a solution to this potential problem. It is only pointing out a potential problem that may be overcome by other means such as a hardware write blocker or enough knowledge to explain in a court of law that the data was not changed. In order to accomplish the latter more research needs to be done to explain exactly what happened.

The KNOPPIX CD comes with a partition info program that can tell the investigator what type of partitions he / she has on the drive. Now I know that many people will want to know why I didn't try to mount the partitions different ways to see the results. One has to remember I took on this project as a validation study that the Probation Officer or Task Force Member to use to validate his / her work in the field. I conducted these test as if I was that Probation Officer or Task Force Officer using KNOPPIX. KNOPPIX is built on ease of use. You click on the hard drive icon and there you go a hard drive mounted read-only. Many times the initial preview is done by a trained Task Force Member before an actual forensic examiner can look at it due to the shortage of examiners in

every agency. I wanted those officers to feel comfortable that what they were doing is safe.

As you can see it may not be so safe when it comes to EXT3 and reiserfs partitions. It is not the end of the world. It is not something that can't be overcome by research and education. For now I would suggest only using KNOPPIX for live previewing of EXT2, FAT32, and NTFS partitions. If you want to preview EXT3 and reiserfs partitions use a hardware write-blocker.

In a nutshell I can reliably say that KNOPPIX is validated for live preview of EXT2, FAT32, and NTFS partitions. I can not validate the use of KNOPPIX for the live preview of EXT3 or reiserfs partitions until more research is done to either explain why or a solution is found to mount the drives read-only without changing the state of the drive. Remember that this is a validation study for KNOPPIX and KNOPPIX derivatives and not other Linux systems.

Disclaimer:

The procedures in this paper have worked for the writer of this article on many occasions. The writer does not guarantee that it will work in every case. The world of computer forensics presents many different scenarios that cannot be guaranteed by this process. This is also a method that should only be utilized by experienced computer forensic examiners. The writer also takes no responsibility as to any damage that this procedure may cause. It is recommended that you have good backups of your computer before attempting this. The opinions of this author are his sole opinions. The author is in no way associated with Microsoft, KNOPPIX, Gentoo, ASRData or SUSE. This paper is not an endorsement for those products.

Legalities:

All trademarks are the property of their respective owners.

© 2002 Ernest Baca (ebaca@linux-forensics.com): This document may be distributed, in its entirety, including the whole of this copyright notice, without additional consent if the redistributer receives no remuneration and if the redistributer uses these materials to assist and/or train members of law enforcement. Otherwise, these materials may not be redistributed without the express written consent of Ernest Baca.

About the Author:

The Author of this paper graduated from the University of Texas Pan American with a Bachelors of Science in Computer Science in 1989. My emphasis during my college studies was systems programming and data communications (Back in the days of the 2400 baud modem, the Internet was called Bitnet and consisted of only educational institutions and large corporations. Boy am I ancient). Upon graduation I began my career in Federal Law Enforcement as a Criminal Investigator for the

United States Marshals Service. In 1997, I transferred to another Federal Law Enforcement Agency as a Special Agent. I have been involved as a computer forensic examiner since the year 2000. I have also served as an instructor on the subject of Linux as a data forensics tool. I have just recently begun to relearn and apply my prior Unix knowledge to computer forensics. I hope this article helps out. If it did or you have any suggestions on revising this paper or new paper ideas, please send me an email or you can find me on the Linux Forensics listserv.

