

1-1-2014

## Testing the forensic soundness of forensic examination environments on bootable media

Ahmed Fathy Abdul Latif Mohamed  
*Zayed University*

Andrew Marrington  
*Zayed University*

Farkhund Iqbal  
*Zayed University*

Ibrahim Baggili  
*University of New Haven*

Follow this and additional works at: <https://zuscholars.zu.ac.ae/works>



Part of the [Computer Sciences Commons](#)

---

### Recommended Citation

Mohamed, Ahmed Fathy Abdul Latif; Marrington, Andrew; Iqbal, Farkhund; and Baggili, Ibrahim, "Testing the forensic soundness of forensic examination environments on bootable media" (2014). *All Works*. 3327.

<https://zuscholars.zu.ac.ae/works/3327>

This Conference Proceeding is brought to you for free and open access by ZU Scholars. It has been accepted for inclusion in All Works by an authorized administrator of ZU Scholars. For more information, please contact [Yrjo.Lappalainen@zu.ac.ae](mailto:Yrjo.Lappalainen@zu.ac.ae), [nikesh.narayanan@zu.ac.ae](mailto:nikesh.narayanan@zu.ac.ae).

Contents lists available at [ScienceDirect](#)

# Digital Investigation

journal homepage: [www.elsevier.com/locate/diin](http://www.elsevier.com/locate/diin)

## Testing the forensic soundness of forensic examination environments on bootable media



Ahmed Fathy Abdul Latif Mohamed <sup>a, \*</sup>, Andrew Marrington <sup>a, \*</sup>, Farkhund Iqbal <sup>a</sup>, Ibrahim Baggili <sup>b</sup>

<sup>a</sup> Advanced Cyber Forensics Research Laboratory, College of Technological Innovation, Zayed University, PO Box 19282, Dubai, United Arab Emirates

<sup>b</sup> Tagliatela College of Engineering, University of New Haven, West Haven, CT, USA

### A B S T R A C T

#### Keywords:

Bootable examination environment  
Bootable CD  
Bootable DVD  
Hash functions  
Differential analysis

In this work we experimentally examine the forensic soundness of the use of forensic bootable CD/DVDs as forensic examination environments. Several Linux distributions with bootable CD/DVDs which are marketed as forensic examination environments are used to perform a forensic analysis of a captured computer system. Before and after the bootable CD/DVD examination, the computer system's hard disk is removed and a forensic image acquired by a second system using a hardware write blocker. The images acquired before and after the bootable CD/DVD examination are hashed and the hash values compared. Where the hash values are inconsistent, a differential analysis is performed on the image files. The differential analysis allows us to quantify and explain the alterations made to the image files by the bootable CD/DVD examination. Our approach can be used to experimentally validate new bootable CD/DVD distributions as forensically sound.

© 2014 Digital Forensics Research Workshop. Published by Elsevier Ltd. All rights reserved.

### Introduction

A plethora of forensic bootable CD/DVD/USB Linux distributions are available for use in digital investigations. Both commercial and community-developed distributions are available, and most make the claim that they provide a forensically sound examination environment. The bootable CD/DVDs are used by forensic examiners to boot into a trusted operating system on the suspect's computer system. This has numerous advantages in some scenarios:

1. Conducting a quick examination of the suspect's machine at the scene in a trusted operating system.

2. Examining the system without the need to perform a time consuming hard disk acquisition where the suspect's machine needs to be powered off and disconnected, the disk removed, and then acquired.
3. Acquiring an image of the RAM of a live system from a trusted operating system, albeit with some degradation caused by the reboot.

However, despite their utility, forensic bootable CD/DVDs are known to have several problems which compromise their utility and potentially call the digital evidence they are used to collect into doubt ([Forensicswiki.org](http://Forensicswiki.org), 2012). Chief amongst these problems is that the bootable live CD/DVD examination environments may alter the suspect computer system's hard disks during the examination process. Such an alteration calls into question the forensic soundness of the examination.

\* Corresponding author. Tel.: +971 4 402 1199; fax: +971 4 402 1017.

E-mail addresses: [m80002419@zu.ac.ae](mailto:m80002419@zu.ac.ae) (A.F.A.L. Mohamed), [marrington@computer.org](mailto:marrington@computer.org) (A. Marrington), [farkhund.iqbal@zu.ac.ae](mailto:farkhund.iqbal@zu.ac.ae) (F. Iqbal), [ibaggili@unh.edu](mailto:ibaggili@unh.edu) (I. Baggili).

In this work we test various forensic bootable CD/DVDs based on Linux, through an experiment to evaluate the changes those CD/DVDs make to the suspect's hard disk. A detailed, repeatable method is detailed for the testing of bootable CD/DVDs and bootable USB devices designed for forensic examinations. We use differential analysis to find the nature and quantify the extent to which those distributions change the suspect's hard disk. From these experiments we draw findings and propose future work.

## Related work

Conducting forensic investigations is becoming more challenging due to the pervasive nature of internet and the increasing size of computer storage media, including hard drives and tape devices (Adelstein, 2006). The traditional approach to computer forensics, where an investigator first switched off the suspect's machine, took it to a laboratory, removed the hard disk and then took images of confiscated computer hard disk for further analysis is time consuming. On the principle that “justice delayed is justice denied”, it is often preferable to conduct some sort of triage or preliminary investigation *in situ* – indeed, this may even elicit a confession from a suspect when confronted with evidence of their wrong doing at the scene (Casey et al., 2009). Forensic examination environment boot media can be used in these cases in three main ways:

- To provide “known-good” binaries for live analysis of a system.
- To conduct a dead analysis of the system at the scene without the need to disassemble the computer, and image its hard disk drive.
- To use the suspect's hardware to examine the disk in cases where the forensic examiner may not have access to specialist or legacy hardware which may be necessary to image certain types of hard disks.

In all of these types of investigation, the suspect's computer is being used to investigate activities which have taken place on the suspect's computer, and thus it may be asked whether we are conducting a live or dead analysis. We differentiate on the basis of whether the suspect computer's operating system is being used by the investigator. Live analysis uses the suspect system's operating system and its resources to conduct forensics. By contrast, dead analysis takes place when that operating system is no longer running, such as when the computer has been booted into another operating system from removable media (Carrier, 2005). To differentiate between uses of forensic examination environments on CD, DVD and other removable media, we call CD/DVDs which are used for live analysis “tools CDs” (or DVDs) and those used for dead analysis “boot CDs” (or DVDs), since the suspect computer will be rebooted using the operating system on the optical media in the second case. We should note that the terms “live CDs” and “boot CDs” are often used interchangeably in the literature, among the Linux user community, and among the digital forensics community.

Live forensics gives access to information on running processes, open network connections, and open Dynamically Linked Libraries (DLL) in addition to non-volatile static information (Carvey, 2007). The main forensic purpose of live CD/DVDs is in investigations where evidence is likely to be found in memory or in other volatile storage locations, where powering down or restarting the computer for a dead analysis is likely to cause that evidence to become corrupt, overwritten or otherwise irretrievable. Live CD/DVDs can be used to provide trusted tools and utilities for forensic analysis for an investigator to use rather than depending on tools which are found on the suspect computer's hard drive, which might be infected by malware or be otherwise modified and unreliable. In this respect they address to a limited extent the concern that live forensics may be invalidated by low system integrity, but there are still significant problems in their use (Hay et al., 2009).

In this work we focus on boot CD/DVDs, not live CD/DVDs, according to the distinction we have given above. Although boot CD/DVDs are not subject to concerns about system integrity caused by a compromised host operating system, there is a growing awareness in the DF community that forensic bootable CD/DVDs can still be problematic and most particularly that their claims that the suspect's hard disk will not be altered have rarely been tested. For example, in the Forensics Wiki<sup>1</sup> an excellent discussion of the issues with forensic bootable CD/DVDs has been a featured article for some time (Forensicswiki.org, 2012). However, despite this growing awareness in the research-active part of the DF community, the identified issues are still commonplace in many bootable CD/DVD distributions, and even where they have been fixed, new versions frequently reverse those fixes.

## Experimental testing of bootable CD/DVDs

We designed a simple experiment to test whether a bootable CD/DVD examination altered the hard disk of the suspect's computer system when the system was booted using the bootable CD/DVD.

### Equipment

In our experiments, we used standard equipment found in most digital forensics laboratories. There were three key devices, which will be described in more detail below, but which, in generic terms can be described as:

1. A suspect computer.
2. A hardware write blocker.
3. A forensic workstation.

Our simple experiment should be easy to replicate in any forensic laboratory which has reasonable stand-ins for these three items, and the cabling to connect the three as appropriate. Specific requirements and details of the equipment we used are discussed for each of these three items below.

<sup>1</sup> <http://www.forensicswiki.org>.

### Suspect computer

Our suspect computer had a single hard disk drive and a bootable optical media drive – the simplest configuration which would be encountered in the field. The computer was configured to boot from the optical drive before the hard disk drive. The format and state of the hard disk drive is the most crucial feature of the suspect computer for the purposes of the experiment. Bootable CD/DVDs should be tested on all file systems which they are intended to examine – this means that the methodology described in the Methodology Section should be repeated for as many different suspect computers with as many different file systems as are necessary to provide sufficient test coverage.

In our experiments, we used several suspect computers running Windows XP. In all cases, the hardware and software specifications of the suspect computer was the same. We used IBM Thinkpad T42 laptops as the suspect computers in our experiments. Although an old model, they are common in our laboratory, and their relatively small 40 GB hard disk makes the image acquisition steps in the Methodology Section faster. The suspect computers used in our experiments all had Windows XP installed, and their hard disks were formatted using the NTFS file system.

### Hardware write blocker

A hardware write blocker is a device which sits between a hard disk and a forensic workstation which blocks instructions sent to the disk to write data, but allows instructions sent to read data. There are a variety of write blockers available. In our experiments we used a Tableau eSATA Forensic Bridge write blocker, as shown in Fig. 1. The National Institute of Standards and Technology runs a *Computer Forensic Tool Testing* program, and have laboratory tested a number of hardware write blockers (National Institute of Standards and Technology, 2012), any of which would be suitable for use in experiments following the methodology we outline in the Methodology Section.

### Forensic workstation

The forensic workstation, which was used to create bitwise images of the suspect computers before and after examination using the bootable CD/DVD forensic

examination environments, was a Lenovo desktop computer of the following specifications:

- Intel Core 2 Quad CPU Q8400 @ 2.66 GHz
- 8 GB RAM
- 2 TB external hard disk for storage of bitwise image files of suspect computers
- AccessData FTK Imager v3
- AccessData FTK 1.71
- WinDiff

### Methodology

Each bootable forensic examination environment was tested according to the following methodology:

1. An artificial “suspicious usage” scenario was performed on the suspect computer.
2. The suspect computer's hard disk was removed from the (powered down) suspect computer.
3. The suspect computer's hard disk was connected to a hardware write blocker (see Fig. 2).
4. The write blocker was connected to the forensic workstation.
5. An image of the suspect computer's hard disk was acquired using FTK Imager (call this image *img*).
6. The suspect computer's hard disk was disconnected from the write blocker.
7. The suspect computer's hard disk was reinstalled in the suspect computer.
8. The suspect computer was booted from the bootable media containing the forensic examination environment.
9. A forensic examination of the suspect computer's hard disk was performed using the tools on the bootable media.
10. The suspect computer was shut down gracefully.



Fig. 1. Hardware write blocker.



Fig. 2. The suspect hard disk connected (via IDE adapter) to the write blocker.

11. The suspect computer's hard disk was removed from the suspect computer.
12. The suspect computer's hard disk was connected to the write blocker (and forensic workstation) once again.
13. An image of the suspect computer's hard disk was acquired using FTK Imager (call this image *img'*).
14. Hash values were calculated for *img* and *img'*.

If the hash values for the two images matched, then the bootable CD/DVD examination did not alter the suspect computer system's hard disk. If the hash values for the two images did not match, then the bootable CD/DVD examination altered the suspect computer's hard disk. We generated SHA1 hash values for all images in our experiment.

In our experiment we examined the following bootable forensic examination environments:

- Knoppix v7.0
- Helix 3 Pro 2009R3
- Kali Linux v1.0

This list is by no means exhaustive. The methodology we have employed is easily repeatable and can be applied to test any bootable digital forensics examination environment.

## Differential analysis

*Differential forensic analysis* compares two disk images (or other pair of equivalent artifacts) to reveal and attempt to explain the differences between them (Garfinkel et al., 2012). By taking the image of the suspect computer's hard disk acquired before the bootable CD/DVD examination, and the image of the suspect computer's hard disk acquired after the bootable CD/DVD examination, we are able to perform a differential analysis and quantify the changes to the suspect computer's hard disk which occurred as a result of the bootable CD/DVD examination. We wanted to find out what changes were made by the bootable CD/DVD examination and whether those changes seem reasonable and *predictable*.

The question of predictability is important. Although a bootable CD/DVD examination may alter a hard disk, if it alters the hard disk in a predictable way, and that alteration is both minor and documented, then the examination process may still be considered forensically sound, even if it is not ideal. Outside of the digital forensics discipline, there are many other forensic sciences which modify samples in some way. Even within digital forensics, in many investigations of small scale digital devices such as smart phones, it is necessary to install a rootkit on the device (as in (Al Mutawa et al., 2012)) or to modify a non-user partition (such as the Android recovery partition as in (Vidas et al., 2011)) in order to acquire an image of the device's primary storage. Although altering the original evidence is undesirable, we contend that alterations are permissible so long as they are:

1. *Minimal* in terms of their impact upon the data which is of evidentiary value,
2. *Well-understood* in terms of the nature and extent of those alterations, and

3. *Documented* properly and in sufficient detail so as to accurately represent the cause, nature, and extent of the alterations.

It might be argued that since, unlike the modifications which are sometimes necessary in forensic examinations of mobile phones, we are able to acquire evidence from computer hard disks without modifying them through the use of write blockers, the question of whether a bootable CD/DVD examination causes predictable changes or not is moot. We contend that it is not, since in some investigations it may not be practical to disassemble a computer and remove its hard disk to be plugged into a hardware write blocker and either imaged or directly examined on a second computer. In some investigations, such a process may be considered unnecessarily or unfairly disruptive to the operations of a business, for example, especially in cases where that business may be simply a third-party whose disks may contain relevant evidence. In these cases, the use of bootable CD/DVD examination environments which cause only predictable changes to the hard disk may still be acceptable.

We performed our differential analysis manually using FTK's differencing features (as discussed in (Garfinkel et al., 2012)), which allowed us to identify which files had changed, which had been added, and which had been removed when comparing images taken before and after the use of the bootable forensic examination environment. We added both images to a case in FTK and excluded "duplicate" files/items. On FTK, when a file occurs twice within a case, the file encountered second is marked as the duplicate and the file added first is marked as the "primary" file. In order to exclude files/items which existed on both images, we therefore manually omitted items marked as a primary through sorting evidence items. This left us with a list of files/items recovered from unallocated space which either existed only on one image, or were different between the two images. During our experiments, we found that it was simpler to export a list of evidence items from FTK for each disk, and to use `diff` to compare the lists and draw attention to the files which had been added/removed/changed than to use FTK's "duplicate" filter. Exported lists were easier to refer to again later as well.

## Findings

In this section we present our findings after conducting simulated investigations using several popular bootable forensic examination environments, all based on the Linux operating system. In all environments, we mounted the suspect computer's hard disk (read-only) manually (auto-mounting was disabled if we had that option), and conducted keyword searches for terms relevant to our simulated suspicious usage scenario.

### Knoppix

Knoppix is one of the most popular bootable Linux environments, although it is not specifically designed for digital forensics. Despite this, it has a long tradition of being employed in digital forensics (Willis, 2003), and is the basis

for several forensics/security focused bootable media Linux distributions. We performed this experiment using Knoppix 7.0, which we downloaded as an ISO file and then burned to a blank CD to create our Knoppix boot CD. We used the following command to mount the suspect computer's primary hard disk partition as read-only:

```
sudo mount -t ntfs-3g -o ro /dev/sda1 /media/sda1
```

As can be seen in Table 1, the SHA1 hash values calculated for *img* and *img'* were different, and thus Knoppix altered the suspect computer's hard disk during the course of the examination. We therefore performed a differential analysis in order to quantify this change.

Further, after conducting our keyword searches, we attempted to create files on the suspect computer's hard disk out of interest. Knoppix allowed us to do so just using the graphical shell logged in as the default user, which obviously changed the disk again. These changes were made despite the disk supposedly being mounted as read-only. Care must be exercised to avoid creating files when using Knoppix in real investigations.

The total number of file items reported by FTK for both *img* and *img'* was 77,295. Therefore the Knoppix examination process did not add any files. We also found no difference in the size of any individual files or in the size of the image as a whole. The only differences we found were in the last access date and time for four files:

1. C:\[root]\\$I30
2. C:\[root]\\$MFT
3. C:\[root]\Documents and Settings\Administrator\Local Settings\\$I30
4. C:\[root]\Program Files\Cisco Packet Tracer 5.3.1\sounds\simulationTab.wav

While none of these changes are desirable, the final file in this list is particularly perplexing. Unlike *\$I30* or *\$MFT*, which contain file system metadata, the *simulationTab.wav* file is part of the laboratory SOE installed on the laptops which served as the suspect computers in our experiment. It is an audio file used as part of an application. Although nothing was changed but the access date, the change to this file was especially concerning, as it suggests that any file on the suspect computer's hard disk could be changed by Knoppix's mounting and keyword search processes. On this basis we conclude that Knoppix is inappropriate for use as a bootable forensic examination environment.

### Helix3 Pro

Helix3 Pro is a forensic examination environment on CD which can serve as both a live CD and a boot CD. We tested

**Table 1**  
Comparison of images for Knoppix v7.0

Image	SHA1 Hash Value
<i>img</i>	e942df9b391053ce33a2ddfc8cdd19713413e43a
<i>img'</i>	fd041692beb80245c6468ae13a087b0df61cd092

**Table 2**  
Comparison of images for Helix3 Pro 2009R3.

Image	SHA1 Hash Value
<i>img</i>	6aa81d809c1c2bdff55baa8d4a8a95682718344d
<i>img'</i>	d454ab49357118618daaad214a40b66dc0ebd7df

it as a bootable forensic examination environment. Unlike Knoppix, Helix3 Pro is a commercial product and is explicitly marketed as a forensics tool. Users therefore have a reasonable expectation of forensic soundness.

As can be seen in Table 2, *img* had a different SHA1 hash value to *img'*, and therefore we can say that we altered the hard disk when we mounted it and performed keyword searches using Helix3 Pro. We used the following command to mount the suspect computer's primary hard disk partition as read-only:

```
mount -t ntfs-3g -o ro /dev/hda5 /mnt/hda5
```

We performed a differential analysis on the two images in order to quantify the change.

Using FTK we noticed no change in the number of file items found on *img* and *img'*. However, when we generated a list of file items from each image, and performed differencing<sup>2</sup> on the list, we found that the access times had changed for the following three files:

1. C:\[root]\\$I30
2. C:\[root]\\$MFT
3. C:\[root]\WINDOWS\bootstat.dat

These files seem to be accessed during the process of mounting the suspect's hard disk using Helix3 Pro. None of the "user data" files in the *img'* hard disk image had been modified. The contents of these system files listed in Table 2 have not been changed – just the accessed timestamps. Although no changes are desirable, we conclude that the changes made to the hard disk by Helix3 Pro may be minimal and predictable enough that its use can be considered forensically sound.

### Kali

Kali Linux is a penetration testing distribution of the Linux operating system, which has evolved from the popular BackTrack distribution. Like BackTrack, it also includes many tools for digital forensics. We used the Kali Linux 1.0 DVD ISO to create a bootable Kali DVD. Using the boot DVD, we investigated our artificial suspicious usage scenario. Kali automatically mounted the partition as read/write at boot. We immediately unmounted the partition and mounted it as read-only using the following command:

```
mount -t ntfs-3g -o ro /dev/sda5 /mnt/sda5
```

As can be seen in Table 3, *img* had a different SHA1 hash value to *img'*, and therefore we can say that we altered the hard disk when we mounted it and performed keyword searches using Kali Linux. As before, we performed a differential analysis on the two images in order to quantify the change.

<sup>2</sup> Using WinDiff.

**Table 3**  
Comparison of images for Kali Linux v1.0

Image	SHA1 Hash Value
<i>img</i>	1c473f5fee75dec2e9c2703f57d2a2bac0a59b75
<i>img'</i>	693bbfe4fd20b6afb7f3d581501cd6402af3c6a

Using FTK we noticed an additional file item in *img'* when compared to the number of file items found on *img*. The additional file was a thumbnail graphics file. The new file was a duplicate of an existing file found on *img* and in another location on *img'*. Strangely, when we generated a list of file items for each image and compared them using WinDiff, we could not identify the reported additional graphics file. It is possible that FTK reported its existence in the “Overview” pane erroneously, or that the file item was otherwise not shown in the file list, possibly as a result of a software bug. In any event, based on the comparison of the two file lists, the following files had different access times on *img'*, with no other changes to file size or contents:

1. C:\[root]\\$I30
2. C:\[root]\\$LogFile
3. C:\[root]\\$MFT
4. C:\[root]\WINDOWS\bootstat.dat

These files seem to be accessed during the process of mounting the disk using Kali. We are unable to explain why FTK reported an additional thumbnail graphics file in *img'* as compared to in *img* and why we were not able to locate this file in our exported file lists. However, as the file was reported as a duplicate of an existing file only in the “Overview” pane of FTK, we assume its creation would not interfere overmuch with a forensic investigation. We can only assume that FTK's overview panel misreported the total number of thumbnails. No files in the “user data” areas of the disk appear to have been modified by the mounting and keyword search process in Kali. However, the automatic booting of the partition as read/write at boot time makes Kali inappropriate for use as a bootable forensic environment.

### Future work

We see four major items of future work coming out of this work. The first is a new set of experiments involving multiple computers with a variety of “common” configurations, in order to evaluate whether the bootable CD/DVD distributions we have tested make *predictable* alterations, or whether the alterations are different after every examination. The second is the expansion of our testing to a much broader set of bootable forensic examination environments, including non-Linux based environments and more commercial tools. The third is a deeper differential analysis of images generated during our testing process. The primary benefit of the second and third items of future work will be to raise awareness about the alterations (if any) made to hard disks during routines conducted with the tested bootable forensic examination environments,

and to assist in the answering of the question about whether those distributions are suitable for use in forensic examinations of the host computer's hard disks. The fourth major item of future work is to investigate the causes of the changes made by tested distributions and of the variables involved which may contribute to, mitigate, or prevent such changes.

### Predictability

By performing a differential analysis on pairs of images from *multiple* computer systems, we can establish whether the changes which are made by a given bootable CD during the examination process are similar on several different suspect computers. The purpose of performing the differential analysis on pairs of images from multiple computers is to attempt to determine whether the changes made by a bootable CD examination are predictable.

### Broader testing

There are more Linux live/boot CD/DVD distributions than just those we have tested in this work. We would like to undertake a program of systematic testing of forensic examination environment boot CD/DVDs and bootable USB drives, including those based on operating systems other than Linux. All boot media would be tested according to the methodology discussed in the Methodology Section. We expect, however, that the results would be similar to those reported in the Findings Section.

### Deeper differential analysis

Garfinkel, Nelson and Young have developed some automated tools for differential analysis (Garfinkel et al., 2012), dependent on the generation of DFXML (Garfinkel, 2012) using the “fiwalk” software. We would like to be able to employ automated differential analysis in the future to make sure that we understand the full extent of the alterations made by bootable forensic examination environments. This may also shine light on some of the ambiguity we encountered with *Kali* using FTK. Also, automated differential analysis could be incorporated into scripts to automate much of the methodology we describe in the Methodology Section, to more easily facilitate large scale, rapid testing of bootable forensic examination environments.

### Root cause analysis

Since all of the bootable CD/DVDs we examined in this work were Linux distributions, there are common implementation details which will lead to common pitfalls which some or all distributions may encounter. For example, the auto-mounting of partitions is common in many live CD/DVD Linux distributions, including some intended for use in forensic examinations (Forensicswiki.org, 2012). Mounting a partition, even as read-only, may still lead to changes being made to that partition, as we have seen in our Findings. Auto-mounting a partition is even more perilous as the user

may not even be presented with the option to attempt to avoid changes being made.

In addition to common implementation details, there are many details which will either be distribution-specific, or case-specific. In this work we examined NTFS file systems from Windows XP computers. In cases involving Linux computers, using Ext3 and Ext4 file systems, mounting as read-only (using `mount -o ro` for example) may still cause journal recovery actions on damaged disks, modifying the disk (Suhanov, 2009). Combined with auto-mounting of partitions, this issue may be further compounded as even a user aware of this problem when examining potentially damaged Ext3/Ext4 partitions may still inadvertently modify those partitions just by booting a supposedly-safe forensic examination environment.

While some preliminary work has been made publicly available about the causes of problems using bootable forensic examination environments, a major item for future research is the systematic surveying of available distributions for issues mounting common file system types. This survey would deeply examine the default configuration of each surveyed distribution and the forensic issues peculiar to each file system type. Such a survey can both inform the development of future bootable forensic examination environments, and can help examiners select the “safest” option from existing distributions for the file systems they anticipate that they will encounter in their case.

## Conclusions

Using bootable media-based forensic examination environments has become important in digital forensic investigations. The notion of altering the data during a forensic investigation has also become more acceptable, providing that we know what, where and how much of the data is being altered. The results from this study indicate that some data on the disk does change when using several popular bootable CD/DVDs, and we document where these changes take place using differential analysis helping both digital practitioners and scientists understand what happens to a disk when a bootable CD/DVD is used on a machine.

The results, summarized in Table 4, indicated a variation in the amount of data that is being changed on the disk when Helix 3 Pro, Kali and Knoppix are used. All the bootable CD/DVDs altered the disk, but none added any

files to the disk during the course of searching the disk by file types and keywords. Knoppix allowed the disk to be written to even when the user has mounted the disk as read only, permitting us to create files using the graphical shell, meaning that it would be easier for a file to be accidentally created and the suspect's disk altered by an examiner using Knoppix. Most of the changes made by the bootable CD/DVDs we tested were in `C:\[root]\$LogFile`, `C:\[root]\$MFT` and occasionally in the file `C:\[root]\WINDOWS\bootstat.dat`. Knoppix also altered some other files as well, which is documented in our Knoppix findings. In all cases the only modifications were the “last accessed” timestamps. These changes are minimal, easily attributed to the examination process (since the timestamp reflects the time of the bootable CD/DVD examination), and unless timestamps are somehow relevant to the investigation, unlikely to have any evidentiary impact. In Table 4 we have listed that the alterations made by Helix3 Pro and Kali were acceptable in respect of this minimal impact, however, given Knoppix permits the user to write to the suspect's disk in addition to the timestamp alterations, we have indicated that we do not regard these alterations as acceptable for forensic use, and we believe Kali's auto-mounting hard disk partitions as read-write at boot time makes Kali unacceptable for forensic use even though the alterations it made were minimal. We stress that this assessment is our own, and encourage others to make their own assessment of the forensic soundness/acceptability of a given bootable forensic examination environment for themselves on the basis of their own testing.

We conclude that even though disk alterations are made, they can be documented through experimentation, which can help during an investigation when a question arises on the integrity of using a bootable CD/DVD during an investigation. With the proper testing to support their choice of examination environment and to document and explain any minor changes that environment may make to the original disk, it may therefore be possible for an examiner to justify the use of a particular bootable CD/DVD. Whether any changes are justifiable or not, what is certain is that rigorous testing of bootable forensic examination environments is required to support their usage in digital forensics, and that such environments, even community-developed forensics-dedicated distributions, cannot be assumed to be safe without such testing.

**Table 4**  
Summary of results.

	Helix3 Pro 2009R3	Kali v1.0	Knoppix v7.0
Hard disk altered?	Yes	Yes	Yes
Files changed (hash values differ) during search	\$LogFile \$MFT C:\WINDOWS\ bootstat.dat	C:\\$I30 \$LogFile \$MFT C:\WINDOWS\ bootstat.dat	C:\\$I30 \$MFT C:\Documents And Settings\Administrator\ Local Settings\I30 C:\Program Files\Cisco Packet Tracer 5.3.1\ sounds\simulationTab.wav
Forensic usage acceptable?	Yes	No	No



## References

- Adelstein F. Live forensics: diagnosing your system without killing it first. *Commun ACM* 2006;49(2):63–6. <http://dx.doi.org/10.1145/1113034.1113070>.
- Al Mutawa N, Baggili I, Marrington A. Forensic analysis of social networking applications on mobile devices. *Digit Investig* 2012; 9(Suppl.):S24–33. <http://dx.doi.org/10.1016/j.diin.2012.05.007>.
- Carrier B. *File system forensic analysis*. Upper Saddle River: Addison-Wesley; 2005.
- Carvey H. *Windows forensic analysis DVD Toolkit* [Tech. rep.]; 2007.
- Casey E, Ferraro M, Nguyen L. Investigation delayed is justice denied: proposals for expediting forensic examinations of digital evidence. *J Forensic Sci* 2009;54(6):1353–64. <http://dx.doi.org/10.1111/j.1556-4029.2009.01150.x>.
- Forensicswiki.org, Forensic Live CD issues. [http://www.forensicswiki.org/wiki/Forensic\\_Linux\\_Live\\_CD\\_issues](http://www.forensicswiki.org/wiki/Forensic_Linux_Live_CD_issues); 2012.
- Garfinkel S, Nelson AJ, Young J. A general strategy for differential forensic analysis. *Digit Investig* 2012;9(Suppl):S50–9. <http://dx.doi.org/10.1016/j.diin.2012.05.003>.
- Garfinkel S. Digital forensics xml and the dFXML toolset. *Digit Investig* 2012;8(3):161–74.
- Hay B, Bishop M, Nance K. Live analysis: progress and challenges. *Secur Priv IEEE* 2009;7(2):30–7.
- National Institute of Standards and Technology. *Computer forensics tool testing handbook* [Tech. rep.]; 2012.
- Suhanov M., *Linux for computer investigators: <> of mounting filesystems*, [http://www.computer-forensics-lab.org/pdf/Linux\\_for\\_computer\\_forensic\\_investigators.pdf](http://www.computer-forensics-lab.org/pdf/Linux_for_computer_forensic_investigators.pdf); 2009.
- Vidas T, Zhang C, Christin N. Toward a general collection methodology for Android devices. *Digit Investig* 2011;8:S14–24. <http://dx.doi.org/10.1016/j.diin.2011.05.003>.
- Willis CF. *Forensics with linux 101 or how to do forensics for free*. In: *Black Hat USA 2003, Las Vegas*; 2003.