Rethinking “Don’t Touch” And Live Box Examination

A brief look at relevant issues.

Jim Tanner, Ph.D., GSLC
President, KBSolutions Inc.

September, 2008

Dr. Tanner can be reached at lists (at) kbsolutions (dot) com

Table of Contents

Introduction

Since 1998, I have endeavored to advance the capabilities of probation and parole line officers to manage the computer use of convicted sex offenders. As I trained nationally on what I called "Field Forensics", I became aware of the strengths and weaknesses of the variety of Linux approaches to field examinations (e.g. Knoppix, Helix, SPADA, etc.). My experience with hundreds of line officers brought me to several conclusions regarding approaches to computer monitoring:

1. Bootable Linux approaches were effective and valuable tools.

2. Linux approaches didn't always work. In the early days, they failed on about 20% of the computers. This has improved, but they still don't work on all boxes.

3. Linux approaches often required the installation of drivers in the RAM kernel to accomplish their tasks.

4. Line officers in probation and parole were moderately 'computer literate', but were uncomfortable working outside the standard Windows® environment.

4. While Linux approaches were not overly difficult, they were not being widely used by probation and parole. When asked why they weren't being used, officers generally explained they were too complicated and required too much "extra" work to produce viable reports.

5. Probation and parole officers were generally choosing to not monitor computer use rather than use Linux based tools they considered too complex.

6. The resulting failure to monitor computer use of convicted sex offenders was unacceptable to me.

I realized we needed a way for the vast majority of line officers to monitor and manage computer use while using a tool that ran in Windows® and was easy to use. I decided to create such a tool. Toward that end, I joined forces with Jim Persinger of PM Investigations Inc., and Joe Russo of the National Law Enforcement and Corrections Technology Center - Rocky Mountain Region (NLECTC). We developed Field Search; an easy to use, live-box examination tool running on the native Windows® platform. Field Search is distributed free to law enforcement and government agencies thorough NLECTC and KBSolutions.

Field Search was first released in August of 2006. Its approach was based on a model of computer management I had developed during more than 1,200 examinations of convicted sex offenders' computers using standard forensic tools (EnCase® , X-Ways Forensics® , FTK® , and various flavors of Linux tools). In brief, Field Search was designed for use by the majority of line staff officers who have limited to no technical training in forensics. It ran live in a native Windows® environment and provided a fast, powerful, yet easy method of monitoring computer use. In essence, Field Search blends preview functions with evidence gathering and reporting functions.

Since 2006 we have updated Field Search 4 times, making it more powerful in each successive version. In September of 2008, we introduced a second application which runs live in the Mac OS X® environment and allows officers to examine MacIntosh products in the field. Currently, the two Field Search products are called FSWin (Windows® version) and FSMac (MacIntosh® version).

In September of 2008, there are more than 7,500 users of FSWin. In classes funded by NLECTC, APPA, and various other agencies, we have trained more than 2,300 probation and parole officers in 32 states in its use. We have conducted labs which trained an additional 1,000+ officers in Field Search at a variety of conferences sponsored by HTCIA, Dallas Children's Advocacy Center, and numerous other entities. FSWin is in use in the U.S., Canada, U.K., and Australia.

Reports from the field indicate Field Search has been successfully used in hundreds of revocation hearings. Further, evidence collected by Field Search has been successfully used in the criminal prosecution for new charges of child exploitation (CP). To our knowledge, information collected by Field Search has always been admitted into evidence and has never been successfully challenged.

As FSWin's use grew among probation and parole agencies, local law enforcement began to examine it as a potential tool for first responders and case investigators. FSWin began to be added to the "jump kits" used by local law enforcement. In brief, it is generally considered as **ONE** of the tools available under specific circumstances (e.g. "Knock and Talk" and/or consent searches).

This trend - movement from probation and parole's use, to being used by first responders and case investigators in situations where its results might wind up as an element in new criminal charges - has brought about a discussion regarding live box examination. The discussion was at first held among forensic examiners and RCFL staff. It is beginning to expand beyond this small circle of extremely knowledgeable individuals. As the discussion expands outside forensic circles, I am seeing a reiteration of conversations held months, if not years ago.

Intent Of This Paper

I am writing this paper in an attempt to accelerate the various conversations being held in and between local departments nation-wide. I believe live-box examinations pose no problem for forensic labs, subsequent evidentiary elements, or informed prosecution. In fact, I believe appropriate use of live-box tools like Field Search expedites the justice system and saves the valuable resources of forensic labs for the higher-level and more complex cases. Moreover, appropriate use of live-box tools like Field Search empowers detectives and investigators to use their other well-honed skills to resolve cases more efficiently (by a timely removal of individuals from persons of interest lists, making them full-fledged suspects, or getting admissions at first interview).

It is my experience that discussions about live-box examination usually begin from the time-honored "Don't Touch The Box" position. The "Don't Touch" position has been a cornerstone of computer forensics for a long time and for good reasons. It is how I was trained as an examiner, and is an important and valuable caveat for all computer forensic examinations.

However, I know of no legal scholar who feels current approaches to digital evidence have kept pace with the rapid changes in the digital world. We are still applying rules of evidence adopted before digital evidence, or rules of evidence which were adopted in the early days of computing. These rules and approaches may not make sense in today's world. For example, there is no such thing as an "image" of a cell phone, PDA, or any other device which uses constantly shifting memory management. "Imaging a network" is an oxymoron. The best we can often do is take "snapshots" of some devices, as they change in the next few seconds. Media size affects our actions as well. Imaging a several terabyte device is not only time consuming but the analysis of the resulting data is mind-boggling to even the most experienced examiner. We must move away from "devices and media as evidence" to "information as evidence" or we will surely be crushed under the weight of our task.

In short, live-box examination is coming of age. It is not IF we do it, it is WHEN and HOW we do it. Our discussions around live-box examination can no longer begin with the assumption that it is always bad to touch the device. We must have a broader and more informed perspective or we will get buried in backlogs and cases will continue to stall in the coming years.

Having said the above, my intent in writing this paper is NOT to prove my position is correct. My position is clear to anyone reading this paper. However, a jurisdiction must come to agreement on when and how live-box examinations are conducted. My purpose in writing this paper is to provide a "friend of the discussion" paper. It is my intent to help discussions be expansive and thought provoking. It is my hope that a reading of the materials in this paper will enhance the discussions and lead to informed decisions that work for a jurisdiction - regardless of whether I agree with the decision or not.

Levels of Investigation

There are three general situations where an officer might want to view the contents of a computer. The methods used in each situation or phase vary. These levels of investigation are briefly discussed below.

Preliminary Investigation and/or Interview ("Knock and Talk").

During this phase of an investigation the target is a person of interest to the investigation and generally not a formal suspect. The approach tends to be more information gathering and informal interview in nature. Searches of any digital devices is generally by consent and is usually time limited. Taking possession of the device and/or imaging it is generally not an option under these circumstances. Searches must be fast and appear to be informal. Risk of the target withdrawing consent to search is generally increased as the device owner's perception of the level of intrusion increases. Live-box examination techniques are ideal for this type of investigation.

Investigation Authorized by Conditions of Supervision (Probation/Parole exams)

This type of investigation occurs in probation and parole. Under these circumstances the target of the exam is a device owned or controlled by a convicted offender. The examination is conducted for the purpose of establishing compliance with terms and conditions of supervision. Generally, evidentiary items found during this type of examination result in technical violations of supervision and are required to meet a lower standard of evidence than those resulting in new criminal charges. Live-box examination techniques are well suited for this type of investigation.

Formal Examination (Seizure & Search).

This type of investigation generally occurs subsequent to probable cause and warrant. This type of examination may also occur pursuant to a consent search where evidence of a new crime is found. Traditional approaches (i.e. seizure, imaging, examination of image) are preferred under these circumstances. If live-box tools are used, they should generally be used behind write-blocker technology and/or using approaches that mount the target drive in a read-only state (e.g. Linux). They may be used without these protections when exigency of the situation demands immediate action.

There is little disagreement on the requirements of this level of investigation. Once a device is determined to be part of a body of evidence potentially supporting a new charge, we need to preserve integrity of data, establish chain of custody, and follow 'standard' forensic protocols. It is assumed in this paper that **once seized**, the computer is reasonably protected against any changes to the drive or device.

It should be noted, however, that the geometric advances in the size of storage devices may lead to even this level of examination being considered for live-box techniques. The shift from "devices and media as evidence" to "information as evidence" is needed, even in formal examination situations.

For the purposes of this document, however, this level of examination (i.e. by a trained forensic examiner and in a computer forensic lab) is **not** the focus of our discussion and is considered excluded from the remainder of this paper. It is also assumed that a system may have been examined using live-box technology PRIOR to being seized. What is of importance is that devices and media are protected ONCE SEIZED. **Any events occurring prior to seizure simply constitute the state of the device when seized and have no effect on subsequent procedures or admissibility of evidence from a computer lab.**

Commonly Held Concerns About Live-Box Examinations Using The Native OS

The concerns voiced about using native OS as the platform for live-box examinations fall into three broad categories; allegations of planting evidence, data contamination, and data destruction.. Each will be discussed below.

Planting Evidence.

While this issue can always be raised by the defense, it is rarely entertained by the courts absent clear evidence of tampering. The simple allegation that it could occur has not proven to be a successful defense strategy in court. Planting evidence that is undetectable as falsified is a substantial undertaking in a Windows® environment. Competent forensic examiners can explain the numerous and complex steps it would take to use Windows® native environment to successfully introduce bogus digital evidence onto media while leaving no trace of its imposition.

Windows became increasingly more journaled as it progressed from FAT to NTFS, and finally TxF. Artifacts of file movement and changes are written to several places on a drive (e.g. event logs, link files, MRU keys, write behind cache managers, etc.). To successfully introduce falsified data to a drive which could not be identified as falsified requires expert knowledge, painstaking attention to detail, knowledge of the file structure on the drive, an understanding of the state of the computer (what is running and the box's policies) and changes to or removal of a variety of artifacts. The task is compounded by the fact that each change to an original artifact generates artifacts tracking that change. Simply put, it sounds easy, but isn't. That is why computer forensics works in the first place.

Interestingly enough, this complex task becomes even more difficult in situations where the alleged perpetrator (in this case the officer) has no prior knowledge of the organization of the hard drive, the state of the system, or the policies that are set on the box (s)he is examining. It is even further exacerbated by the fact that generally a consent search is a one time, time-limited event where the system owner is generally present. This is exactly the situation in live-box examinations or "Knock and Talk" scenarios. Officers are working cold, with no prior knowledge of the computer or its contents, in the presence of the person of interest, and in a time-limited environment. This does not lend itself to planting evidence.

Further, I hold that using the native OS actually increases the protection against the imposition of falsified data. It would be much easier to plant evidence on a drive when using an external OS (e.g. Linux). **The fact that the native OS documents changes in numerous places on the drive could (and probably should) be viewed as an ad-hoc audit trail of the investigating officer's actions.** It is, admittedly, stored in an odd location - the target drive. But it would be available IF the computer is seized subsequent to the examination based on information uncovered during the examination.

Nobody wants to be in the position of defending their veracity. However, I propose when we find ourselves in the situation where the possibility of planting evidence comes into question, we continue in our role of neutral fact finder. In those circumstances, I suggest we simply state the obvious: " It is possible, but not probable." In follow-up questioning, we can educate the bench or jury about the magnitude of the task. Depending on the operating system involved, it would take me 20-30 minutes of testimony to give a simple explanation of what one would have to do to successfully inject evidence onto a drive in a way it couldn't be detected as falsified. It is unlikely judge or jury would give the suggestion of planting evidence any weight after such testimony.

Data Contamination

Live-box examination utilizing the native OS results in some changes to the drive. Using native APIs, built-in procedure calls and interrupts results in the OS generating writes to the local drive. Simply put, we "touch the drive". There are two important questions to be resolved when considering changes to digital evidence in these circumstances.

Question 1: Relevance

First we must ask if the contamination is relevant. This goes back to the notion of "information as evidence" versus "device as evidence". An analogy may be helpful here. When investigating a murder case in a home, we do not seize the entire house. We extract evidence from the house in the form of fibers, trace elements, fluids for DNA analysis, fingerprints, splatter patterns and so on. The house is simply a container. We take samples from those areas which we believe to be relevant and leave the house behind.

More to the point, we actually ENTER the house to get our samples. No matter what an investigating officer does, they are contaminating a crime scene by simply investigating it. Officers drop their DNA throughout the house, they may even leave their fingerprints, stray hairs, fibers from their uniforms and a host of other artifacts which show they were present. Regardless of how many booties and rubber gloves investigators don, they drag in contaminating trace elements and distribute them throughout the crime scene.

Fortunately, we have developed approaches to exclude these contaminants in the physical world. The officer documents his/her actions and we take samples from the officer. We exclude the officer's DNA, hair, fibers, trace elements, etc. from the analysis because we understand they were innocently introduced to the scene in the act of investigating it.

I contend we should think the same way about a computer. It is a container. Our goal should be to extract relevant information as evidence. Fortunately (or perhaps unfortunately for labs), seizing the entire container is easier with a computer than with a house. We often seize the entire computer simply because we don't know where in the container evidence might be located. We run the same risk with the house - evidence could be anywhere- but seem to ignore that issue entirely because we understand we can't seize the house. In the house, we make our best judgement on where evidence is located and do an iterative examination which increases the chances of our finding all the places where evidence might lie. We can do the same with a computer.

This brings us back to the relevance of contamination. Other than destruction of evidence (covered in the next section), should we be concerned with the addition of an MRU in the registry, an entry in the Prefetch or Superfetch folder, a link established in the recent folder, or some other artifact generated as a result of executing a preview tool in the native OS? For all but a few rare cases, such entries are benign as they do not affect the evidentiary items of the case. Images on the drive, email containers, and other items of interest remain unchanged. In fact <u>most</u> of the drive is unaffected by the use of live-box examination tools running in native

OS.

Those elements which are affected generally have additions made to them (e.g. event logs, prefetch folder, recent folder, etc.). The addition of the entries generated by live-box tools rarely affects pre-existing entries in these locations; they are additions, not substitutions. As in the physical world, we simply have to document what the investigator did when using the live-box tool and produce a footprint map of what the tool does. Any competent computer forensic lab can then exclude from analysis any artifacts created by the tool ; just as we exclude the officer's DNA, fibers, etc. from the physical crime scene.

Question 2: Reasonableness

The second question we must address is whether or not the changes to the drive were reasonable. This is a bit more ethereal. Given that we are discussing live-box examination under "Knock and Talk" or conditions of supervision circumstances, I would argue moderate changes are reasonable to expedite investigations and protect the public.

Despite hyperbole, the alternative to live box examination has proven to realistically be one of three things:

A) **Do nothing**. The investigator does nothing. They don't have the tools or are afraid to use them, so they do nothing. This is unacceptable. Innocent individuals are not removed from persons of interest lists, and guilty people do not get elevated to the status of suspect. In short, the case stalls.

B) **Come back later.** The investigator does nothing and schedules with a trained person who returns later and executes a non-intrusive preview of the device. This is also unacceptable. It increases the chance evidence will be lost due to normal use of the device, it alerts the guilty party the device may be inspected at a later date and allows them time to purge data, it delays case processing, and does not remove innocent persons from interest lists or elevate guilty individuals to the status of suspect. In short, the case stalls at best and at worst the guilty individual is given the chance to destroy a case completely.

C) **Have someone else take charge.** In this circumstance the investigator takes the device and transfers it to a lab for examination. This is problematic at best. First, there may be no probable cause for seizing the device. Second, it transfers the heart of the investigation to an "outside agent" (the forensic examiner). In essence, the case investigator is removed from the loop while waiting for the forensic lab to complete its work. While one might argue this is similar to sending DNA to a lab, the comparison is weakened by the fact that there is no simple method for a line investigator to conduct DNA testing while there IS a way for them to conduct simple examination of a computer. Sending every computer to a lab is akin to sending every person to the hospital for BAC testing instead of using field sobriety tests, nystagmus or intoxilyzer testing. It simply doesn't make sense when there are easy to use alternatives which can quickly provide the information needed to make case decisions immediately. In short, the case stalls.

I would rather give investigators access to the information contained on a computer immediately, expedite the case, and protect the public (by removing innocent individuals from interest lists, elevating guilty individuals to suspect status, or potentially gaining an immediate admission). I think "contamination" is easily dismissed in evidentiary hearings as long as the officer documents what tools were used and what actions were taken.

Data Destruction

It is given that using any technology which generates writes to the target drive has the potential of destroying (overwriting) data of value to the investigation. In a "Knock and Talk", consent, or supervision compliance environment there are four questions we must answer:

1. What is the probability of destroying data?
2. What is the probability of the destroyed data being key to the investigation?
3. What can we do to mitigate the effects of the data destruction?
4. What is the relative gain of using a live tool compared to the potential loss of relevant data?

Probability of Destruction

It is impossible to determine the actual probability of data destruction in K&T, consent or supervision compliance environments. There are three primary types of destruction of concern in these circumstances; A) date/time changes and B) overwrites of data in unallocated space (free space), and C) overwriting of data in existing files managed by the system (e.g. Pagefile).

Date/time changes

In general, date/time changes occur when the native OS opens a file or folder for examination/modification or executes a file. Walking the data tree in FAT systems has no impact on the Last Access Date (LAD) of the folders. Walking the data tree in NTFS systems changes the LAD on folders, but not files. Walking the data tree in TxF systems has no impact on the LAD of files or folders unless the User has turned off the disablelastaccess policy on the system (disablelastaccess is defaulted ON in Vista®). Modifying a file or folder will result in a change to the Modified date/time stamp in all Windows® platforms as well as the LAD in FAT and NTFS environments.

The probability of destroying MAC dates varies between OS platforms. When simply walking the file tree, destruction of the existing LAD on folders is almost assured on NTFS systems, but is zero on FAT and near zero on TxF systems. MAC dates are changed on some folders and files by simply running any executable in native OS (e.g. prefetch, link folders, event logs, etc.)

Once the investigating officer begins to "drill down" in a search, the probability of making changes to date/time stamps increases. As long as the officer doesn't open a file, there are few changes to LAD by drilling down. If an officer opens a file, the LAD of that file is changed on the target drive (unless it is a TxF system in default policy mode). In FAT and NTFS systems, the previous date/time stamp is destroyed and lost to subsequent examinations. If the preview tool didn't capture the existing LAD, that information is lost to the case.

In short, depending on an officer's actions, some MAC dates do change (and are subsequently lost to future examinations) during a live-box examination of most Windows® platforms.

Overwrites of Free Space

Changing MAC dates should not cause overwriting of data in free space. The MAC dates already have allocated positions on the drive and are simply overwritten in place. There is no loss of data from free space when MAC dates are updated by Windows®.

The addition of new files and the expansion of existing files will not overwrite data that remains logical on the drive (has not been deleted) unless the file name (and full path) of a new file is identical to an existing file. Simple expansion of a registry hive, addition of an entry into the prefetch/superfetch or recent folders, or addition of a new digest file will not affect existing files which remain logical.

However, the addition of new files and the expansion of existing files does present the potential to overwrite files or file clusters which are no longer logical (have been deleted and Recycler emptied). Where Windows® decides to place new data is a function of many things. In essence, there are two factors at play; A) the proportion of the drive that is available as free space, and B) the drive load equalization function of the operating system.

NTFS and TxF attempt to prolong the life of a drive by equalizing the use of physical drive space. This is a complex process - I have just enough knowledge to be dangerous. However, NTFS and TxF do not necessarily use the first available cluster on a drive for writing new data (we are talking clusters here, because Windows® doesn't actually track individual sectors). This spreads new data across the drive in such a way as to optimize the life cycle of the media. Hence, there is no way to know where new additions to a file system will be located.
As a result, there is no way to calculate the probability of an existing cluster in free space being overwritten by new data. Obviously, the greater the number of free clusters, the lower the probability a single cluster will be used. Lets do some simple math as an experiment. In a small (80GB) hard drive running NTFS that is 20% utilized, there are approximately 16,777,216 available clusters of free space. All are not equally likely to be utilized by NTFS for the new file. Assuming only ½ have a reasonable probability to be used, this leaves 8,388,608 clusters available. If the file written is 12KB, we would have a 1 in 2,779,536 (1 in 2.8 million) chance in hitting a cluster which contained data of interest.

There is no way to calculate whether the 1 in 2.8 million writes hits a critical cluster that is the **ONLY** critical cluster on the entire drive. Thus, there is no reasonable way to calculate the odds of a single write destroying a case. It would be remote at best. In my experience, if your case hangs on one and only one evidentiary item, you probably won't prevail no matter how pristine your forensic approach.

Overwriting System Managed Files

Another concern occasionally voiced is that running in the native OS can cause overwrites to occur in the Pagefile/Swapfile. This is certainly true. How much the Memory Manager utilizes the Pagefile is a function of many things (e.g. the size of available physical memory, the working set of application, the number of threads running, the number of dirty pages existing in memory, read-ahead/write-behind functions, etc.)

There is simply no way to estimate whether writes to the Pagefile will occur. Those examiners who have actually had to carve items out of a Pagefile know it is messy work at best and hair-pulling at worst. Windows® is a bit psychotic in its use of the Pagefile. Testimony on Pagefile elements can be daunting if you are up against a skilled attorney. Not that examiners haven't prevailed on Pagefile evidence, but my experience is that if your case hangs on an element recovered from a Pagefile with no other evidentiary elements, you probably won't prevail no matter how pristine your forensic approach.

Overwriting other system managed elements are of less concern. Kernel mode elements are unavailable to standard forensic exam - they disappear when the box is crashed. System managed User mode elements that are written to disk are few, the most common used in cases are the spooler files often found in free space. Damage to or destruction of these files can effect a case. As indicated in the section above, the probability of hitting a critical file with a write is low, though not zero.

Mitigation

We have established that albeit low, there is a probability of destroying some data relevant to a case. This raises the question of how to mitigate this problem if we choose to use live-box examination. There is only one approach, but it has its drawbacks.

The approach is to minimize the footprint left on the target drive. This is accomplished in 3 ways:

1. Hold as much in RAM as possible. Purposefully design the application to hold data tables, reports, internal working elements, and digests in RAM to the greatest extent possible. Field Search is designed precisely this way. This, however, leads to a secondary problem. As you hold more in working memory, you increase the size of the working set, which concomitantly increases the probability that Windows® will swap portions of the application's pages and their data to the Pagefile. This, of course, increases the chance of overwriting some element in the Pagefile - though by how much we don't know.

2. Minimize the number of calls to procedures which can result in writes. Field Search is also designed to do this. We attempt to reduce the number of standard API calls which can generate writes to the target drive. However, as we decrease the number of standard API calls, we also reduce the power of the application, or we reduce the likelihood it can be migrated to future versions of Windows®. We tried to strike a balance in Field Search, giving the User as much power as possible, but explaining in the documentation how each of their actions could generate writes to the drive.

3. Document actions within the application to generate an 'audit trail'. This assists labs when previewed devices wind up being seized and enter into a formal forensic environment. The log assists the lab in verifying the changes which were a result of the officer's actions. Field Search logs actions which can modify the target drive.

Relative Gains

The decision to utilize live-box examinations revolves around comparing the relative gains of its use against the problems it raises for the case. An abbreviated comparison of the two approaches is found below.

	Live Box Exam	No Live Box Exam
Case Gains	No delays in case processing. Public Safety immediately enhanced. Investigators remain empowered in case. Increased probability of admissions earlier in case.	No data lost due to officer actions. Less complex lab testimony.
Case Losses	Low, but not zero, probability of data destruction. More complex lab testimony.	Delays in case processing. Public safety not immediately enhanced. Case Investigator not empowered. Lowered probability of admissions earlier in case.

Should Live-Box Be Used?

As indicated above, this must be a local decision. All stakeholders should carefully examine the issues involved in live-box examination under other than formal exam circumstances (e.g. "Knock and Talk", consent search, and condition of supervision investigations). A full evaluation of the costs and benefits of live-box exams will, in my opinion, lead to a decision they are a viable and valuable tool in many of these situations.

The enhancements to case processing and the concomitant furthering of public safety outweigh any minor problems caused by the tools' use. For those cases where the device is entered into evidence subsequent to a live-box examination, we see no problems for competent labs to maintain forensic protocols once the device is seized, and to easily explain the impact of the live-box exam had on the target device. Moreover, we believe the footprint on the target drive is, and should be, viewed as an audit log of the officer's actions. This information combined with the documentation provided by the officer during the live-box exam should easily quash any objections raised at trial.

Coordinated Policy

While we favor use of live-box exam tools in non-formal exam situations, we recommend against implementation without coordination between line officers, computer labs, and prosecuting attorneys. Guidelines or policies should be implemented such that a common approach by investigators results in a consistent picture of the effects of live-box exams to judges and juries. Implementation without stakeholder input can lead to divisiveness and confusion between and among the agencies.

Conclusion

The current philosophy of "Don't Touch" appears to be failing our justice system in the evolving digital era. Based on rules of evidence established prior to or during the early days of digital evidence, "Don't Touch" is out of step with both advances in technology and the volume of cases which include digital evidence. Cases are being stalled for unacceptable amounts of time due to backlogs in labs. Public safety is not enhanced by delays in case management, nor is justice expeditiously served to both innocent and guilty parties.

We believe a careful examination of the elements involved will lead jurisdictions to the conclusion controlled live-box exams during non-formal phases of case management are overwhelmingly positive with little to no adverse impact on a case. We further believe a careful examination of the situation will lead to the realization that not implementing live-box exams generally results in case stalls or complete collapse of a case through inactivity. Case stalls and collapse are unacceptable.

Not making an informed decision concerning live-box examinations during non-formal phases of case management is making a decision to continue practices that are clearly failing. Whether a jurisdiction chooses to adopt live-box exams or implements other approaches which remove case stalls and case collapse is a local choice. It is our hope that this paper advances the decision, regardless of the way a jurisdiction decides.