

Final Technical Report

NIJ Support of NCFS Research and Activities (2005-2009)

Virtual Digital Evidence Laboratory

Award(s): 2005-MU-MU-K044

2005-MU-MU-K044 Supplement 1

J. Philip Craiger, Ph.D.
Assistant Director for Digital Evidence
National Center for Forensic Science
University of Central Florida
&
Associate Professor
Department of Engineering Technology
Daytona State College

Questions regarding this research should be addressed to:

Dr. Philip Craiger
Assistant Director for Digital Evidence
National Center for Forensic Science
University of Central Florida
Orlando, FL, 32816
Email: philip@craiger.net or craigep@daytonastate.edu

Abstract

The traditional modes of storage, analysis, and presentation of digital evidence occurs in a single geographic location, typically within the jurisdiction where the electronic crime occurred. This is an inefficient model because local and state law enforcement agencies typically, and unnecessarily duplicate, digital forensics resources – computers, forensic tool suites, storage, etc. -- that are available elsewhere. A further problem is that law enforcement agencies must verify and validate forensic tools, a process duplicated by all law enforcement agencies for all tools used. Digital evidence labs of the future will not be limited by geographic boundaries or located in a single place. We propose the concept of ‘virtual labs’ to replace, or supplement, traditional physical labs. Virtual labs will consist of cutting-edge technology located in various places, connected via ‘ultra high-speed’ networking. As such, the technology and resources (expertise, storage, tools, etc.) required to accomplish the collection, storage, analysis, and presentation of the evidence may be located in geographically separate parts of the U.S., yet accessible by any law enforcement agency that has a connection to the Internet. Virtual labs will reduce unnecessary duplication of resources and tasks, provide all law enforcement with cutting-edge tools and resources, provide specific expertise when needed, and reduce the costs of digital evidence examinations. The Digital Evidence Section of the National Center for Forensic Science created a prototype virtual digital evidence lab (VDEL) as a proof of concept of a distributed, secure, and validated compilation of hardware and forensic tools suites, accessible via the Internet. This report describes the beta testing of our VDEL by three experienced law enforcement digital forensic examiners.

Table of Contents

Abstract	2
Table of Contents	3
Executive Summary	5
Procedural/Legal Issues	6
Technical Issues	8
Introduction	11
Method	12
Logical Architecture	12
Network	12
Authentication.....	13
Analysis	15
Storage.....	16
Security	16
Physical Architecture	18
VDEL Hardware Specifications.....	18
Network	22
Storage.....	23
Security	23
Virtualization.....	24
Virtual Machine Configuration	25
Device Installation.....	26
Purpose of the Beta Test	26
Subject Matter Experts	27
Beta Test Procedure	28
Results	29
Report for Sgt Dan Purcell	29
VDEL Performance	29
Discussion of VDEL.....	30
Observed Performance	33
Reporting.....	33
Sgt. Purcell’s Conclusion and Recommendations	35
Report for Sgt. Kevin Stenger	37
Organization of Local and State Law Enforcement.....	37
Defense Experts and Legal Issues	38
Results	40
Virtual Desktop Logon	41
Tool Testing.....	41
Server Resource Use	42
Speed of Access to Evidence	43

Virtual Digital Evidence Laboratory

Obtaining Extracted Exhibits and Evidence.....	43
Shipping	44
Sgt. Stenger’s Conclusion / Recommendations	44
Conclusions	45
Procedural/Legal Issues	45
Technical Issues	47
Recommended Modifications by Subject Matter Experts	51
Acknowledgements	53
Dissemination of Findings	54
Publications	54
Professional Presentations	54
Local Onsite Dissemination.....	55
References and Associated Readings	56
Appendix	58
Resumes of Subject Matter Experts and Investigator	59
Sgt. Dan Purcell, MSDF	60
Sgt. Kevin Stenger, MSDF	61
Officer Eric Walton	63
J. Philip Craiger, Ph.D.	64
Procedures Used for Creating Test Images	80
Image One: Windows XP/Dell.....	80
Image Two: Windows 7/Dell PC.....	82
Image Three: Linux OS/Dell PC.....	84
Image Four: Mac OS X/MacBook Pro	86

Executive Summary

The traditional modes of storage, analysis, and presentation of digital evidence occurs in a single geographic location, typically within the jurisdiction where the electronic crime occurred. This is an inefficient model because local and state law enforcement agencies typically, and unnecessarily duplicate, digital forensics resources – computers, forensic tool suites, storage, etc. -- that are available elsewhere. A further problem is that law enforcement agencies must verify and validate forensic tools, a process duplicated by all law enforcement agencies for all tools used. Digital evidence labs of the future will not be limited by geographic boundaries or located in a single place. We propose the concept of ‘virtual labs’ to replace, or supplement, traditional physical labs. Virtual labs will consist of cutting-edge technology located in various places, connected via ‘ultra high-speed’ networking. As such, the technology and resources (expertise, storage, tools, etc.) required to accomplish the collection, storage, analysis, and presentation of the evidence may be located in geographically separate parts of the U.S., yet accessible by any law enforcement agency that has a connection to the Internet. Virtual labs will reduce unnecessary duplication of resources and tasks, provide all law enforcement with cutting-edge tools and resources, provide specific expertise when needed, and reduce the costs of digital evidence examinations. The Digital Evidence Section of the National Center for Forensic Science created a prototype virtual digital evidence lab (VDEL) as a proof of concept of a distributed, secure, and validated compilation of hardware and forensic tools suites, accessible via the Internet. This report describes the beta testing of our VDEL by three experienced law enforcement digital forensic examiners.

Virtual Digital Evidence Laboratory

The beta testing provided our research team with valuable information on the strengths and shortcomings of the VDEL. Feedback is logically partitioned into two categories: those related to procedural/legal issues, and technical issues. Below we include a synopsis of the issues raised by the SMEs, and where appropriate, responses from the investigator.

Procedural/Legal Issues

- Sharing information across legal and geographical boundaries may be problematic. For instance, differences between State laws, or between State and Federal laws, must be addressed with respect to information sharing using the VDEL.
 - **Investigator's Response:** This was considered during our design of the VDEL and would have to be addressed alongside various law enforcement agencies possibly on a case-by-case basis.
- Law enforcement agencies technical administration management must be on board in order to facilitate deployment of a VDEL in a law enforcement setting.
 - **Investigator's Response:** This is true and is applicable to any organization that desires to bring in new technology that will affect the entire organization, e.g., a new operating system or new computer system.
- Reports containing child pornography or other contraband must maintain strict adherence to the chain of custody, evidence security, and transmission to authorized personnel. This may result in limiting use of the VDEL to sworn law enforcement officers only.
 - **Investigator's Response:** This was considered during our design of the VDEL, and the reason we proposed the use of three-factor authentication, which includes, something the user 'has' (hardware token), something the user 'knows' (PIN), and

Virtual Digital Evidence Laboratory

static IP address authentication (the user must have physical access to a computer with a particular IP address).

- The discovery process in criminal cases could be problematic for prosecutors unless they are given access to the VDEL and the report itself. Transmission of the report and evidentiary items (if requested) must be a consideration of the overall design.
 - **Investigator's Response:** This was considered during the design of the VDEL, but was not part of this beta testing.
- The VDEL does not reduce or eliminate the requirement for training of forensic examiners on various forensic tool suites.
 - **Investigator's Response:** In the VDEL's current implementation this is true. However, we have proposed the use of onsite subject matter experts that could assist remote end users with problems they might have. The cost effectiveness of this would have to be addressed.
- When the defense attorney's find out about the network topology and Internet-based access of the VDEL and possible security vulnerabilities, what resources will be required to negate the obvious battles of the courtroom? Will the examiner and organization that implements the VDEL be able to sustain such arguments?
 - **Investigator's Response:** The investigator agrees that this could be a very significant issue as defense attorneys would attempt to attack the credibility of the security of the VDEL, and perhaps draw parallels with recent well-known intrusions on the "big guys" (e.g., Google, Microsoft, etc.). The questions posed by the SME are valid, and we are attempting to identify solutions.

Technical Issues

- One SME had difficulties installing/running Cisco VPN software on some hardware configurations.
 - **Investigator's Response:** This may require a 'pre-tested list' of suggested hardware for use with the VPN software.
- Transportation of post examination evidentiary files may require significant resources required by the local agencies.
 - **Investigator's Response:** We have designed the VDEL such that prosecutors, defense attorneys, and other individuals with a need to know can be provided with restricted access to the VDEL in order to download reports and evidentiary files.
- Archiving of old case files would require significant added storage requirements to the VDEL.
 - **Investigator's Response:** We do not foresee any way around this problem. The one compelling issue is that storage space is getting cheaper and cheaper.
- Proposed method of shipping original evidence to the VDEL source, as opposed to Internet upload, would be costly and time consuming.
 - **Investigator's Response:** We plan on testing the performance of uploading large image files over the network to the VDEL, pending funding. This would require that the local law enforcement agencies have the capability (equipment and training) to create a forensic duplicate.
- Potential for overloading the VDEL computing resources if too many examiners simultaneously use the VDEL.

Virtual Digital Evidence Laboratory

- **Investigator's Response:** We plan on testing resource saturation at a latter date, pending funding.
- Transmitting the report from the examiner's virtual machine to the examiner's connecting machine is not possible using remote desktop alone.
 - **Investigator's Response:** In its current implementation this is true. We have planned to have a separate area of storage on the SAN that would allow end users (e.g., anyone with a 'need to know') download copies of the reports using a secure protocol (e.g., SSH over the VPN).
- The examiner cannot create custom reports without some level of local authentication to the VM within the LAN of the VDEL. Other options include local access to the shared volumes, but again, the examiner must be within the LAN to do so.
 - **Investigator's Response:** VDEL administrator can provide users with this access on a case-by-case basis.)
- Remote access to workstation does not give examiner full access to install programs stored on media outside of VDEL network.
 - **Investigator's Response:** We believe this to be a desirable feature. Providing forensic examiners with escalated privileges (e.g., root or admin) can lead to issues regarding his/her qualifications to make certain changes to the VMs.
- If hardware problems occur on the examiner's workstation (whether physical or VM application), the examiner may not be able to fix some problems.
 - **Investigator's Response:** This would be true on the physical side of the connection (i.e., the examiner's desktop). Hardware issues on the VDEL side would have to be addressed by a person knowledgeable with the hardware/software.

Virtual Digital Evidence Laboratory

- Full administrative control of the examination environment is not possible in the current implementation of the VDEL, which deviates from the norm in stand-alone forensics.
 - **Investigator's Response:** To reiterate, we believe this to be a desirable feature. Providing forensic examiners with escalated privileges (e.g., root or admin) could lead to issues regarding his/her qualifications to make certain changes to the VMs.
- The examination environment is susceptible to the Internet although port 80 is shutdown in the current implementation of the VDEL. By virtue of design, the VDEL must be connected to the Internet, and this deviates from best practices in computer/digital forensics.
 - **Investigator's Response:** To reduce the possibility of intrusion we have deployed three-factor authentication. Three-factor authentication combined with high-grade encryption makes the possibility of such an intrusion nil. Moreover, it would be nearly impossible for a man-in-the-middle attack to occur because of the high-grade encryption (AES).
 - Since the VDEL is connected to the Internet, the LAN is susceptible to penetration and intrusion. Further testing is required to ensure full security. Moreover, it seems regular testing and monitoring would be required to secure the network.
 - **Investigator's Response:** To reiterate: to reduce the possibility of intrusion we have deployed three-factor authentication. Three-factor authentication combined with high-grade encryption makes the possibility of such an intrusion nil. Moreover, it would be nearly impossible for a man-in-the-middle attack to occur because of the high-grade encryption (AES).

Introduction

Most law enforcement agencies, regardless of how many resources they may or may not have, are required to perform investigations and examinations of digital evidence. This can be a problem, however, as agencies with limited resources find that a traditional digital forensic unit often requires a number of different tools and software along with the training required to utilize them properly. It is these agencies that can benefit from virtual digital evidence lab (VDEL) technology. The VDEL could be hosted anywhere with a proper Internet connection and is designed to provide multiple remote users the tools they need to perform digital forensic examinations. This helps defer the costs of acquiring the tools and training of a traditional digital forensic lab due to the fact that several agencies can fund and share a single VDEL.

In its most basic form, the VDEL provides a remote user with a virtual machine loaded with forensic software as well as secure storage through which they can perform forensic examinations of evidence using only a basic desktop computer with a standard Internet connection. The connection to the VDEL is both secured and closely monitored. End users will be able to upload their evidence directly into the VDEL before analyzing it in their assigned virtual machine. From within this virtual machine, users can manipulate the evidence through any number of forensic programs, generate reports, and even share this information with other users that are authorized to view it.

The advantages of this new model over the traditional digital evidence lab include:

1. Reducing or eliminating unnecessary duplication of resources (examination machines, digital forensic tools, terabyte storage, secure storage, etc.)
2. Reducing or eliminating unnecessary duplication of tasks (verification and validation of all tools in a single location).

Virtual Digital Evidence Laboratory

3. Providing secure (via three-factor authentication), reliable (via VMotion and RAID-5), and validated tools (via subject matter experts) to law enforcement.
4. Provide expert assistance with certified examiner specialists (e.g., Mac OS X, Solaris, network forensics, etc.).

We begin this report by describing the logical architecture of the VDEL, followed by its physical implementation. Next we describe the beta testing procedures, followed by the subject matter experts (SMEs) feedback based on their extensive beta testing of the VDEL. We conclude with a listing of the issues encountered by the SMEs during beta testing, and recommendations for modifications to the VDEL.

Method

Logical Architecture

Network

The network is designed to be as straightforward as possible from the end user to the end virtual machine. At the front of the VDEL network we have a mid-range Cisco firewall and concentrator that we can configure to only accept connections from certain sites. As additional security all access will be on an IP-based basis (i.e., IP authentication). Figure 1 is a ‘sanitized’ logical schematic view of the VDEL.

Virtual Digital Evidence Laboratory

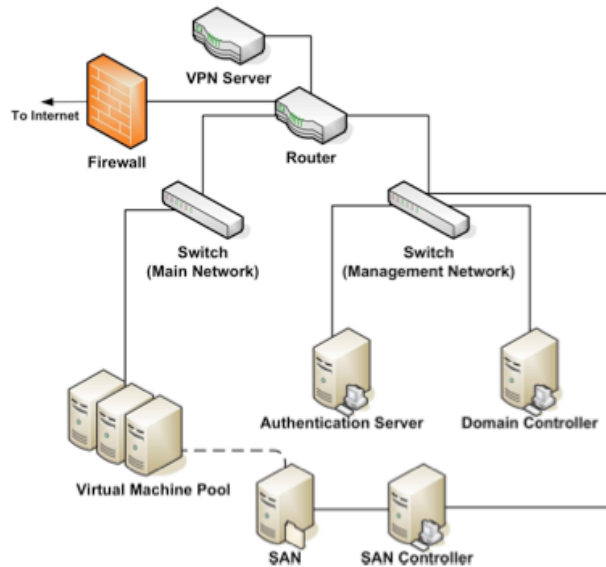


Figure 1. VDEL Logical Schematic.

Connections from remote nodes (i.e., end users) are initiated over a Cisco IPsec Virtual Private Network (VPN) link. The link itself is configured to use AES-128 or AES-256, depending on security concerns and performance requirements. (Note: AES – Advanced Encryption Standard, is the Federal Government approved [FIPS-197] encryption standard to protect sensitive (unclassified) information. AES is a symmetric algorithm with key lengths from 128 to 256 bits.) A Cisco VPN hardware device manages the encryption while an RSA Authentication Manager backend handles authentication.

Authentication

For the final implementation of the VDEL propose three-factor authentication to increase the security of the system. These factors would include: a) a hardware token that is synchronized with the authentication server, b) a PIN to be used with the hardware token, and c) static IP address access control, i.e., only certain pre-determined IP addresses would be allowed to connect through to the VDEL. Three factor authentication would thus require that users must

Virtual Digital Evidence Laboratory

have physical control of the hardware token, know the PIN number, and have physical access to a computer with a particular IP address.

For the beta test however we used two-factor authentication, i.e., static IP address authentication was not used. The hardware tokens used were RSA's SecureID token. Using RSA's SecurID tokens coupled with a PIN, users connect to the VPN. Our initial round of testing will have 10 SecurID tokens along with the backend software running on a dedicated hardware appliance (itself running Windows 2003 Server). Figure 2 is a picture of an RSA SecureID.



Figure 2. RSA SecureID Hardware Token

The authentication system is highly modular; the RSA software enables us to pick any number of VPN solutions. The tokens themselves support a wide range of authentication systems; they could be used elsewhere in the system although this is not particularly necessary after initial authentication.

We may offer an additional layer of protection for each virtual machine (e.g., passwords for logging in to the VPN could be different from the user passwords for the virtual machines). On the other hand, the possibility of a single-sign on system exists if we can get Active Directory to play well with all of the systems involved.

Other issues include the integration of our Active Directory domain with the Linux and Mac OS X clients in the future (this is a notorious problematic and may not work properly), developing a universal ACL (access control list) scheme for users of the system (to

Virtual Digital Evidence Laboratory

accommodate group collaboration on a case, etc), and determining what aspects of case management can be automated.

Analysis

Through virtual machine technology (specifically VMware™), we have a multitude of options regarding virtual machines. Our current model has virtual machine images booting dynamically for forensic examiners upon login. The images contain a standard Windows XP install with the standard forensic suites. Due to dongle compatibility issues we may limit our initial offerings to iLook (a forensic tool suite available to law enforcement only: www.perlustro.com/ustreasury_website/index.html), as we will likely get excellent cooperation from the iLook team and can use this as a leverage point with AccessData (Forensic Tool Kit FTK: www.accessdata.com) and Guidance Software (EnCase: www.guidancesoftware.com).

The virtual machine images themselves will static, that is not change and will be the same for each examiner; instead we will use roaming profiles via Active Directory to store user preferences and separate storage on the SAN will store case data.

Outside of the aforementioned dongle problems, the largest issue here relates to performance benchmarking and determining the typical load for an "average" case. Determining how to automatically spawn an analysis virtual machine when an analyst logs in is another major goal. Both tasks are tied in with an investigation into VMware's VirtualCenter, which provides the possibility of shifting loads to different ESX servers in addition to offering management features.

Storage

Due to the movement towards VMware ESX-based virtualization within the VDEL system, two storage options have arisen as potential models. The first remains similar to our initial model: everything exists on the SAN.

We create small RAID-5 arrays on each ESX server to store copies of the virtual machines that we have developed. This reduces issues with the SAN and allows for local access to the images (which would still not be unique for each case). This may cause issues should we decide to implement VMware's VirtualCenter, software which allows for the seamless transferring of virtual machines (VM) from one machine to another in order to facilitate load balancing (VMotion).

Other issues regarding storage primarily deal with access control over the evidence section of the SAN: how ACLs can be effectively implemented and if dynamically creating a virtual disk within the SAN for each case is feasible (and if it is possible to bond these disks to the virtual machines on the fly).

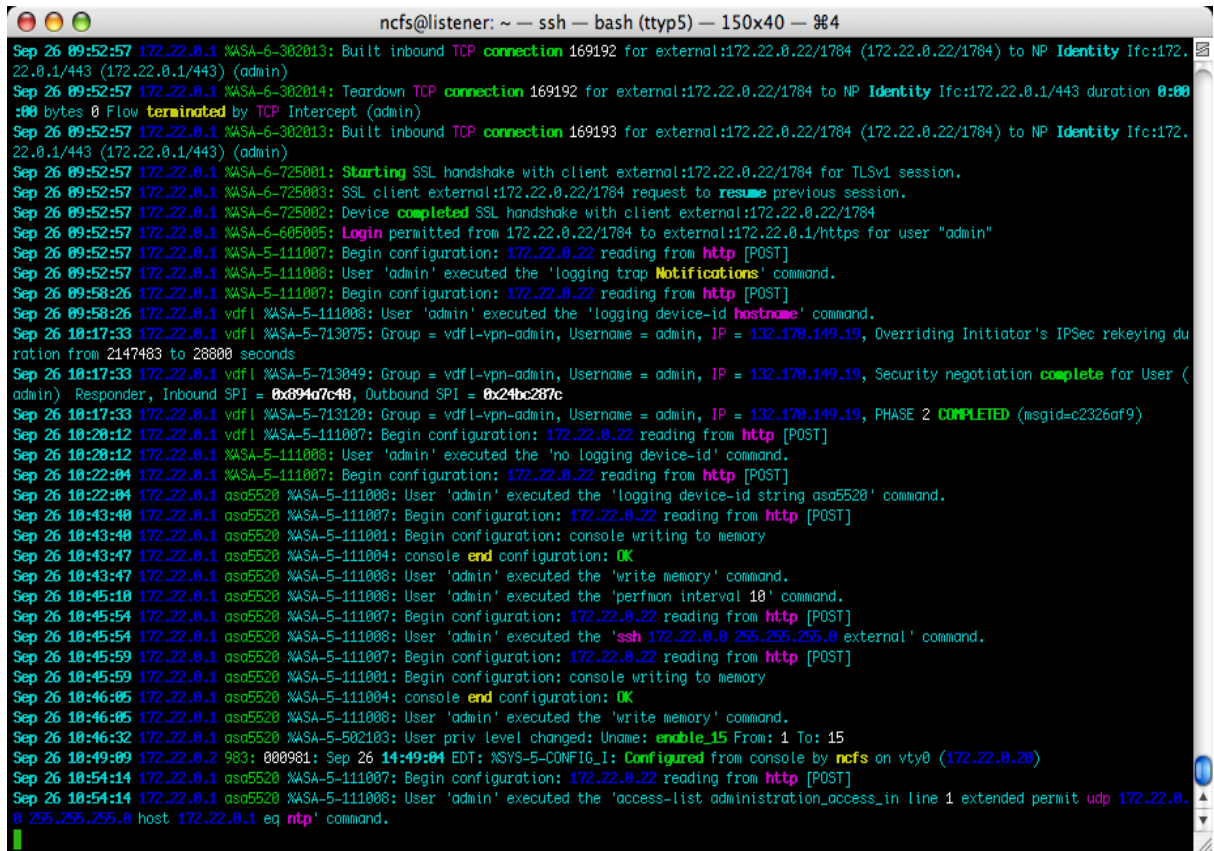
Security

This is by far the most abstract area and more of a catchall than something that has a specific physical component. In the implementation of the VDEL we plan on testing the security of the system at each major step. The primary concern is to create a system that provides not only significant barriers from both external and internal compromise but a log trail as well.

It is desirable to implement a dedicated log server, where all virtual and real machines in the system reporting to it. In order to provide additional security the logs may be encrypted over the main Ethernet backbone or be piped over serial lines. This may prove difficult with the latter for virtual machines as there may not be enough physical serial ports on a server to accommodate

Virtual Digital Evidence Laboratory

the number of virtual machines logging, in addition to the difficulty of mapping such hardware to the proper virtual machine. A hybrid model will likely be employed in the end. Automated log file analysis with reporting is a future topic that will be explored. Figure 3 is a graphic showing a VDEL log file.



```
ncfs@listener: ~ -- ssh -- bash (tty5) -- 150x40 -- 84
Sep 26 09:52:57 172.22.0.1 %ASA-6-302013: Built inbound TCP connection 169192 for external:172.22.0.22/1784 (172.22.0.22/1784) to NP Identity Ifc:172.22.0.1/443 (172.22.0.1/443) (admin)
Sep 26 09:52:57 172.22.0.1 %ASA-6-302014: Teardown TCP connection 169192 for external:172.22.0.22/1784 to NP Identity Ifc:172.22.0.1/443 duration 0:00:00 bytes 0 Flow terminated by TCP Intercept (admin)
Sep 26 09:52:57 172.22.0.1 %ASA-6-302013: Built inbound TCP connection 169193 for external:172.22.0.22/1784 (172.22.0.22/1784) to NP Identity Ifc:172.22.0.1/443 (172.22.0.1/443) (admin)
Sep 26 09:52:57 172.22.0.1 %ASA-6-725001: Starting SSL handshake with client external:172.22.0.22/1784 for TLSv1 session.
Sep 26 09:52:57 172.22.0.1 %ASA-6-725003: SSL client external:172.22.0.22/1784 request to resume previous session.
Sep 26 09:52:57 172.22.0.1 %ASA-6-725002: Device completed SSL handshake with client external:172.22.0.22/1784
Sep 26 09:52:57 172.22.0.1 %ASA-6-605005: Login permitted from 172.22.0.22/1784 to external:172.22.0.1/https for user "admin"
Sep 26 09:52:57 172.22.0.1 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 09:52:57 172.22.0.1 %ASA-5-111008: User 'admin' executed the 'logging trap Notifications' command.
Sep 26 09:58:26 172.22.0.1 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 09:58:26 172.22.0.1 vdf1 %ASA-5-111008: User 'admin' executed the 'logging device-id hostname' command.
Sep 26 18:17:33 172.22.0.1 vdf1 %ASA-5-713075: Group = vdf1-vpn-admin, Username = admin, IP = 132.178.149.19, Overriding Initiator's IPsec rekeying duration from 2147483 to 28800 seconds
Sep 26 18:17:33 172.22.0.1 vdf1 %ASA-5-713049: Group = vdf1-vpn-admin, Username = admin, IP = 132.178.149.19, Security negotiation complete for User (admin) Responder, Inbound SPI = 0x094a7c48, Outbound SPI = 0x24bc287c
Sep 26 18:17:33 172.22.0.1 vdf1 %ASA-5-713120: Group = vdf1-vpn-admin, Username = admin, IP = 132.178.149.19, PHASE 2 COMPLETED (msgid=c2326af9)
Sep 26 18:20:12 172.22.0.1 vdf1 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:20:12 172.22.0.1 %ASA-5-111008: User 'admin' executed the 'no logging device-id' command.
Sep 26 18:22:04 172.22.0.1 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:22:04 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'logging device-id string asa5520' command.
Sep 26 18:43:40 172.22.0.1 asa5520 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:43:40 172.22.0.1 asa5520 %ASA-5-111001: Begin configuration: console writing to memory
Sep 26 18:43:47 172.22.0.1 asa5520 %ASA-5-111004: console end configuration: OK
Sep 26 18:43:47 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'write memory' command.
Sep 26 18:45:10 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'perman interval 10' command.
Sep 26 18:45:54 172.22.0.1 asa5520 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:45:54 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'ssh 172.22.0.0 255.255.255.0 external' command.
Sep 26 18:45:59 172.22.0.1 asa5520 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:45:59 172.22.0.1 asa5520 %ASA-5-111001: Begin configuration: console writing to memory
Sep 26 18:46:05 172.22.0.1 asa5520 %ASA-5-111004: console end configuration: OK
Sep 26 18:46:05 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'write memory' command.
Sep 26 18:46:32 172.22.0.1 asa5520 %ASA-5-502103: User priv level changed: Uname: enable_15 From: 1 To: 15
Sep 26 18:49:09 172.22.0.2 983: 000981: Sep 26 14:49:04 EDT: NSYS-5-CONFIG_I: Configured from console by ncfs on vty0 (172.22.0.20)
Sep 26 18:54:14 172.22.0.1 asa5520 %ASA-5-111007: Begin configuration: 172.22.0.22 reading from http [POST]
Sep 26 18:54:14 172.22.0.1 asa5520 %ASA-5-111008: User 'admin' executed the 'access-list administration_access_in line 1 extended permit udp 172.22.0.0 255.255.255.0 host 172.22.0.1 eq ntp' command.
```

Figure 3. VDEL Log

In the future a simple intrusion detection system (IDS) can be employed to detect possible malicious activity from the ESX servers; in combination with an egress firewall to prevent the majority of network traffic from escaping the VDEL the network should be reasonably secure. Determining what analysts should be allowed to do (e.g., surf the Web, download files from FTP) should be a priority before this.

Physical Architecture

The VDEL consists of hardware and software to emulate a fully functional digital forensics lab accessible via the Internet for agencies with limited resources, but a need to access those tools. The basic hardware setup of the VDEL includes:

- 5 servers for the virtual machines
- 1 firewall/router
- 1 RSA security token
- 1 switch
- 1 SAN
- 1 fibre switch for the SAN (Storage Area Network)
- 1 KVM
- 1 Uninterruptable Power Source (s)

All equipment is housed in single rack, networked together with one interface on the firewall/router facing outward to the Internet. All other connectivity is maintained within the VDEL environment to facilitate virtual machine creation and maintenance, storage, VPN and security.

VDEL Hardware Specifications

The follow is the list of hardware that was used in the development of the VDEL:

- Router – Catalyst 2960G series
- Switch – ASA 5520
- Active Directory (AD) server – Dell PowerEdge 860
- RSA server – RSA SecurID Appliance with Authentication Manager 6.1
- KVM – TRIPP LITE NetDirector Rackmount Console KVM Switch (B020-016-17)
- Xserve – Apple Intel Xserve, 16TB of storage
- SAN – Promise VTrak VTM610i, by Promise Technologies Inc.
- Fibre switch – QLogic SANbox 1400
- ESX servers – Dell PowerEdge 2950
- UPS – APC Smart-UPS 3000

The current layout of the VDEL for testing purposes is as shown in Figure 4. Figure 5 is a picture (front view) of the VDEL.

Virtual Digital Evidence Laboratory

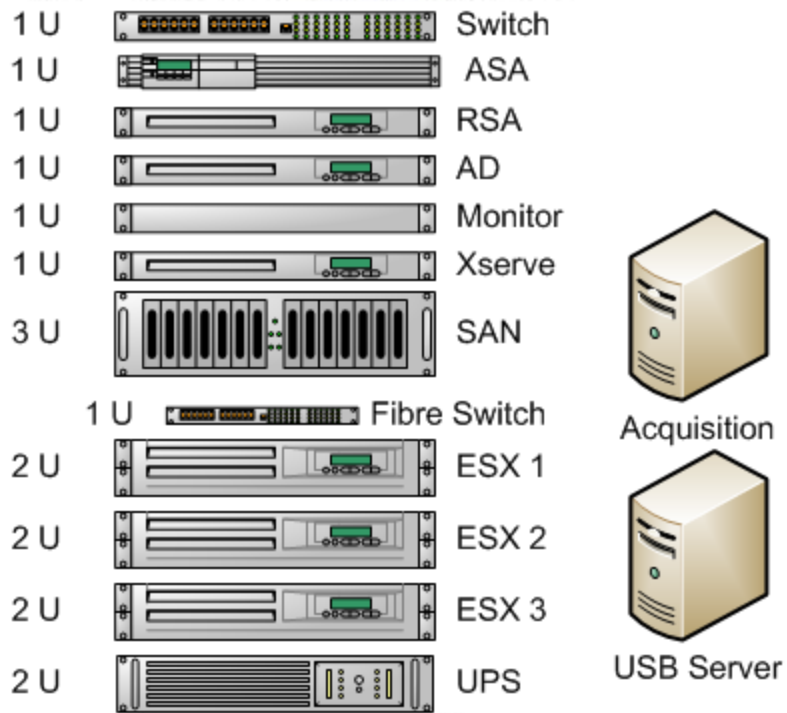


Figure 4: VDEL Schematic



Figure 5: Photograph (front view) of the VDEL

There are two components that are currently external to the VDEL rack, including two desktop computers; one running Microsoft Windows XP (Service Pack 3) and one running Ubuntu Linux 9.04 (www.ubuntu.org). These computers currently handle separate functions that are integrated into the VDEL. The XP machine is the acquisition machine for creating forensic duplicates of evidence, and bringing that evidence into the VDEL, and the Linux machine serves as a USB server for handling any hardware dongle licenses.

The first server in the VDEL is the Active Directory (AD) Server. It runs Microsoft Windows Server 2003 and controls the domain for the VDEL (the DNS services and the AD services), as well as the Virtual Infrastructure Manager (VIM) used to control the VMs used by the end users (the VMs themselves reside on the three ESX servers). Additionally, access to the

Virtual Digital Evidence Laboratory

ASA and switch are achieved via this machine through any terminal client software, i.e. putty (a Windows-based telnet/ssh application).

The second server in the VDEL is the Xserve that runs OS X server. Its sole purpose is to provide a console connection for the SAN, the switch, and the router.

The remaining 3 servers in the VDEL are used as VMware ESX servers as each machine runs ESX version 3.5. These servers host the VMs used by the end user and are controlled and monitored by the VIM running on the AD server.

The RSA SecureID token is also a server in the VDEL, though it comes customized and preconfigured. It runs Microsoft Windows Server 2003 and the RSA suite of software that control access to the VDEL through the use of authentication tokens.

The router for the VDEL is also acts as its firewall and VPN end point. This device handles routing in and out of the VDEL to the Internet and also routes traffic between the individual virtual LANs (VLANs) within the VDEL.

The switch for the VDEL handles the bulk of the network configuration and traffic within the VDEL. It is broken up into three separate VLANs. The first VLAN is for Administration purposes, and allows traffic to move between all of the physical devices in the VDEL. The second VLAN is for Vmotion only, the program used by the VIM to manipulate VMs and move them from server to server as necessary. The third VLAN is used solely for VM traffic; this is the VLAN on which all end user VM communication in and out of the VDEL will take place.

The fibre switch is for the purpose of connecting the SAN to the individual ESX servers, providing a high speed, high bandwidth connection for data transmission.

The SAN is a 16TB storage device used by the VMs to house their individual data for analysis. The SAN is partitioned into 2TB blocks (or 1.99TB blocks) for use by the VMs;

Virtual Digital Evidence Laboratory

restrictions by the ESX server will not allow these partitions to be larger than 2TB in size. Each VM is given only a portion of this space to maximize both storage and access.

The monitor for physical user interface on the VDEL is handled by a 16 port KVM switch that allows for the interaction with each server within the network. Once the entire network is brought online, a VPN connection can be utilized to manipulate the VDEL from any workstation with appropriate authorization.

The uninterruptable power source (UPS) for the VDEL provides the power for the entire rack as well as a battery back up. The size of the UPS will depend solely on the components installed in the VDEL.

The Acquisition machine is provided solely as a source by which to introduce evidence into the VDEL for use by end users through their VMs. It runs Windows XP and should have the minimal amount of software installed on it as possible.

The USB server provides a means by which the software license dongle for particular software (such as Encase or FTK) can be made available for the end user and their VM. The server runs the Linux distribution CentOS v5.2 and the software USB Server for Linux by INCENTIVES Pro. The client software installed onto each VM is called USB Redirector for Windows.

Network

The network is designed around a gigabit switch to allow for high throughput of any data transfer within the VDEL. The switch will be able to create multiple virtual LANs to logically and securely segment the different traffic roles. The switch also offers physical access controls to the network since every port will be configured to accept only known and authorized connections. A hardware based firewall solution will also be implemented to control and filter all

traffic traveling in, out and within the VDEL's network.

Storage

Storage is paramount in dealing with digital evidence due to the ever-decreasing costs of an ever-increasing amount of storage space. To help cope with the storage needs of several concurrent forensic examinations the use of a SAN will be employed. The storage space is accessed over a fibre channel connection to further ensure the necessary bandwidth when dealing with multiple users possibly dealing with large amounts of storage space. Logical partitions will be utilized to segment the storage space needs of the users and the virtual machine stores, as well as strict access controls applied through the management database will define what storage space is readable and writable to any user or group. Long-term storage is another issue with the type of data that this project will be handling, in that the data could possibly be needed at any future point. Long-term storage will be provided to cope with this need, and the design will be able to add any future storage needs accordingly.

Security

Due to the nature of this project, security has to be an integral part of the VDEL's entire framework. Every component needs to be securely implemented using best practice techniques and procedures that the technology industry creates. This includes following the NSA security guides (www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml) for any applicable hardware and/or software as closely as possible. The utilization of strict access controls for authentication and authorization to any available resource is again paramount for the actual use of this project by making sure that only the correct users are able to access the data that they need to access. Logging all user access and resource utilization to perform the necessary system accounting will also be utilized to its fullest extent.

Virtual Digital Evidence Laboratory

The system authentication is handled by a RSA authentication server that employs hardware ‘tokens’ to produce pseudo-random codes. Access to the network is controlled via a hardware based VPN appliance that authenticates against our organizations central VPN authentication management system. Once authenticated with the VPN, user access to their personalized workspace is granted with two-factor authentication, via a combination of username, password and hardware token. The internal user authentication and authorization for the VDEL is handled by a centralized management database, allowing greater flexibility by handling the access control for all components within the VDEL.

Virtualization

One of the paramount features of the VDEL is the use of virtual machines and environments that allow several users the ability to work simultaneously while requiring the use of only a few actual physical machines. This virtualization also extends to the way data can be shared among authorized users, allowing for only specific data to be shared with specific users without the use of any physical medium (CDs, hard drives, flash drives, etc.). VMware™’s software, which is widely used in commercial and governmental sectors, is the basis for this virtualization.

Since most computers are idle for a majority of time, the use of virtualization software will allow better utilization of the underlying hardware. This can cut costs with buying fewer, more powerful, machines instead of several, less powerful machines. The use of virtualization technologies also substantially decreases deployment time of any new user environments since the hardware is standardized through the virtualization software and can utilize custom templates. The virtualization software also allows for decreased downtime by allowing

Virtual Digital Evidence Laboratory

administrators the ability to move active virtual machines between servers, in real time, if there is a pressing need to do so.

Virtual Machine Configuration

We created two distinct VM configurations. The XP configuration is used by forensic examiners to perform their forensic examinations. The Server 2003 configuration is used for shared storage.

Configuration 1:

- Windows XP (with Service Pack 3)
- Memory: 768 MBs
- CPU: 1
- Virtual floppy drive, CD/DVD, network adapter
- Hard drive: 15GB
- Software:
 - 7zip
 - AccessData FTK 1.80
 - Encase 6.11
 - Registry Viewer
 - Dongle drivers (for FTK and Encase)
 - Adobe Reader
 - Avast Antivirus; Java
 - Microsoft Office 2003
 - USB Redirector Lite
 - VLC
 - RSA software
 - VMWare Tools

Virtual Digital Evidence Laboratory

Configuration 2:

- Server 2003 (SP2)
- Memory: 512 MBs
- CPU: 1
- Virtual floppy drive, CD/DVD, network adapter
- Hard drive: 15GB, 500GB (shared)

Device Installation

The physical construction of the VDEL is a relatively simple process. The necessary components are installed into the rack as directed by the instructions for each device. There are no specific limitations on placement of the devices within the rack required to create the VDEL. The rack size and the number and sizes of the devices used to create the VDEL will often dictate the overall physical design.

Purpose of the Beta Test

The purpose of our beta test is to identify problematic issues with respect to the functionality, usability, or performance of the VDEL system. We developed the VDEL to be as ‘transparent’ (user friendly) as possible, while maintaining system and network security. These goals, however, are often in conflict. Moreover, true “transparency” is a difficult goal particularly for this system: The VDEL is an interactive system composed of numerous complex components (hardware, software, networking, etc.) that requires end users to connect to the VDEL over a network Virtual Private Network (VPN) software (to ensure security through encrypted communications); use a public key-based authentication tokens and a password to login to the VDEL (forced user authentication); boot and login to a virtual machine (VM) (2nd step of authentication); and employ forensic tools to perform forensic examinations. Our beta test will allow us to assess issues with system performance, usability, and functional issues.

Virtual Digital Evidence Laboratory

Subject Matter Experts

We identified three experienced law enforcement examiners to participate in our beta test. Combined these authors have nearly 30 years as forensic examiners in law enforcement. Each examiner was chosen for their forensic examination experience, their knowledge of various forensic tool suites, and their experience in teaching forensic examinations. Their resumes are included in the Appendix. Information about these forensic examiners is listed below.

Dan Purcell, Sergeant, MSDF, CFCE/EnCE
IACIS CFCE Chairman
Seminole County Sheriff's Office
Economic & Computer Crimes Unit/Computer Forensics
100 Bush Blvd.
Sanford, FL 32773
(407) 665-6948
dpurcell@seminolesheriff.org

Sgt. Kevin Stenger, MSDF, CFCE/EnCE
Orange County Sheriffs Office
Computer Crimes Squad
2500 W Colonial Dr.
Orlando, FL 32804
(407) 254-7229
kevin.stenger@ocfl.net

Officer Eric Walton
University of Central Florida Police Department
University of Central Florida
Orlando, FL
407 823 6460
ewalton@mail.ucf.edu

Sgt. Purcell and Sgt. Stenger were asked to perform logon and beta testing of the VMs, server performance, and forensic tools, whereas Officer Walton assisted our research team in providing a 'law enforcement' view on possible legal and procedural issues with the VDEL, and with early pre-beta testing of the VDEL.

Beta Test Procedure

Prior to starting the beta testing we provided our subject matter experts (SMEs) with training on the use of the RSA SecureID for authentication, as well as description of the architecture and logon procedures for the VDEL. All testing performed by the SMEs was completed offsite, i.e., beta testers performed their beta testing from an offsite computer to best mimic the actual use of the VDEL. This is consistent of course with the ‘distributed, networked’ goal of the VDEL.

Lab scientists created four test images for the beta test: A Windows XP (Service Pack 3), Windows 7 (Release Candidate 1), Linux (Ubuntu 9.04), and Mac OS X 10.5 image. A description of the procedures used to create the images is located in the Appendix.

We provided the beta testers with training on how to use the RSA SecureID token to authenticate to the system. We then asked the beta testers to spend approximately 50 hours logging into the system, booting into a VM, and performing typical forensic examination tasks (indexing, text searching, recovering deleted files, viewing files, etc.) with the available forensic tool suites using their own computer systems. Beta testers were asked to note any issues with regard to system performance, functionality, or usability that they feel are problematic. They were also asked to address any procedural or legal issues that they feel may be problematic with respect to law enforcement examiners using a VDEL.

Results

Below we present the reports of the two subject matter experts who performed the beta testing. We performed little, if any, editing on the SME's reports, as we did not wish to possibly 'taint' the report's interpretation by rephrasing, adding additional material, or deleting any material via the editing process.

Report for Sgt Dan Purcell

The Virtual Digital Forensics Lab (VFDL) is a network-based model that allows an examiner to remotely access a virtual workstation and utilize common forensic applications to examine digital evidence. Access to the network is accomplished via a common Internet connection to a specified IP address. Secure communication is established through an RSA server and Cisco VPN connections. Examiners are able to access VMware virtual machines through Microsoft's Remote Desktop services. The virtual machines, also referred to as virtual workstations, are loaded with Microsoft Windows XP Professional and common forensic tools that run on a Windows platform. During testing, Access Data's Forensic Toolkit 1.8 and EnCase 6 were used. Internet access was prevented by a domain policy preventing access on port 80.

VDEL Performance

The hardware specifications of the physical server running the virtual machines throughout the assessment period are unknown. However, no major deficits in performance were noted. Windows XP Professional (Service Pack 3) was the primary operating system, and the virtual machines were configured to provide maximum performance.

Software performance will vary from one application to another. Some forensic applications are designed to run in a 32-bit environment as opposed to 64-bit. For example, EnCase Forensic Version 6.15 (current release) will run under Windows XP, Vista, and 7 (32 or

Virtual Digital Evidence Laboratory

64 bit version). However, FTK will run in specific environments as of this writing. FTK also requires a significant amount of disk space for the Oracle database. Hardware requirements from Access Data indicate a separate hard drive or RAID configuration is recommended for the Oracle database. EnCase uses the Outside-In engine, and the same recommendations apply to EnCase as well. It may be wise to consider hardware requirements on the server side of the VDEL and if a single server (workstation) should be used for each examiner as opposed to virtual machines. The VDEL can be configured to host a number of different physical, rack-mounted machines all tied in to a single domain for account configuration, security, and other policies. The machines can be configured with multiple operating system environments through VMware technologies as well. The key is hardware configuration for any forensic application.

Discussion of VDEL

The normal flow of a criminal case involving digital evidence is as follows:

Report of Crime → investigation leads to digital evidence → digital evidence seized → digital evidence forensically imaged by examiner → examination/analysis of evidence → reporting →
judicial process

The first parts of the process mentioned above require the physical presence of the examiner. The examination and analysis of digital evidence can be accomplished from any network (WAN or LAN) that can connect to the VDEL. If the examination is only possible through the VDEL, there are some pros and cons to this implementation. The digital evidence must be forensically imaged and placed on a volume within the VDEL for access by the examiner. A number of questions regarding the imaging process and transfer of the forensic

Virtual Digital Evidence Laboratory

image files must be determined well in advance of full migration to this concept. The following points are offered for consideration:

- A qualified technician or examiner must handle the digital evidence during the intake phase and initial processing. Will the forensic image files be uploaded by an examiner by remote access in the field or within the local LAN by a qualified individual?
- Chain of custody must be adhered to regardless of local triage or remote uploads.
- A process for verifying the forensic image files after acquisition, prior to upload and after the upload to the VDEL servers must be performed by someone in the chain of custody and likely at numerous points in the process. What is the most secure and valid protocol or means to accomplish this task?
- A triage form must be documented at the onset of handling the digital evidence. For example, local clock on a computer must be compared to real time, RAID configurations must be documented, and so on. This information must be available to a remote examiner accessing the evidence within the VDEL.

Once the forensic image files are uploaded to the VDEL server(s), the examiner can access the media anywhere in the world where Internet access is possible. There are pros and cons to the concept of remote access that one should be aware of, and I noted these issues during the testing phase of the VDEL.

Pros of VDEL Examination and Analysis:

- Remote access to the evidence anywhere in the world.

Virtual Digital Evidence Laboratory

- If the VDEL expands to allow uploading of forensic image files in a secure fashion, physical access to the computers by a technician or examiner within physical location of the VDEL.
- Minimizes travel expenses of qualified examiners within an organization
- Greatly increases the timeliness of access to evidence when examiners are located offsite
- Reduces IT costs and overhead maintenance of multiple workstations

Cons of VDEL Examination and Analysis:

- Remote access to workstation does not give examiner full access to install programs stored on media outside of VDEL network
- If hardware problems occur on the examiner's workstation (whether physical or VM application), the examiner may not be able to fix some problems.
- Full administrative control of the examination environment is not possible in the current implementation of the VDEL, which deviates from the norm in stand-alone forensics.
- The examination environment is susceptible to the Internet although port 80 is shutdown in the current implementation of the VDEL. By virtue of design, the VDEL must be connected to the Internet, and this deviates from best practices in computer/digital forensics.
- Since the VDEL is connected to the Internet, the LAN is susceptible to penetration and intrusion. Further testing is required to ensure full security. Moreover, it seems regular testing and monitoring would be required to secure the network.
- When the defense attorney's find out about the network topology and Internet-based access of the VDEL and possible security vulnerabilities, what resources will be required

Virtual Digital Evidence Laboratory

to negate the obvious battles of the courtroom? Will the examiner and organization who implements the VDEL be able to sustain such arguments?

Observed Performance

During testing I was able to connect to the VDEL with no problems whatsoever. Using the Cisco VPN utility for Windows, I was able to connect via two separate Internet connections under Windows Vista business and Windows 7 RC1. Windows Remote Desktop under both operating systems performed without any problems. It should be noted that both of the operating systems were installed to a virtual machine on a MacBook Pro notebook computer running OS X Snow Leopard (10.6). Connections were made via wired and wireless connections (Wireless G and N). No performance issues were noted on the local machine(s).

Once connected to the VDEL, I was able to utilize Windows Remote Desktop to access the virtual machine running Windows XP Professional. The VM was loaded with EnCase 6.x and FTK 1.8x. Several evidence files were loaded on a shared volume within the VDEL. The forensic image files were loaded in several cases with varying levels of pre-processing or intentional search options after the items were added to the application(s). Both FTK and EnCase performed without any notable errors. EnCase was used quite often when I conducted testing. Common functions such as evidence file verification, indexing, keyword searching, file signature analysis, hash analysis/calculation, and other recovery options were run within the case.

Reporting

Assembling a report within the VDEL could be problematic for some organizations. If the reporting method is to export EnCase or FTK application reports and simply write a written report using a common word processing utility, the results could be exported and electronically submitted to the recipient. Customized reports could be problematic such as those created on

Virtual Digital Evidence Laboratory

CD/DVD media. There are a number of reporting limitations via the VDEL, but likewise, there are solutions beyond the intended implementation of the VDEL to expand the concept for review of evidence and reports.

- Transmitting the report from the examiner's virtual machine to the examiner's connecting machine is not possible using just remote desktop.
- Reports containing child pornography or other contraband must maintain strict adherence to the chain of custody, evidence security, and transmission to authorized personnel.
- The examiner cannot create custom reports without some level of local authentication to the VM within the LAN of the VDEL. Other options include local access to the shared volumes, but again, the examiner must be within the LAN to do so.
- The discovery process in criminal cases could be problematic for prosecutors unless they are given access to the VDEL and the report itself. Transmission of the report and evidentiary items (if requested) must be a consideration of the overall design.
- In some cases, the defense will request a copy of the forensic image files and all associated data derived from the case (exported data, reports, etc). The VDEL does not provide a portal to readily access this data. An alternative is to provide the defense's export witness with a VM that contains read-only access to the evidence where he or she is monitored by law enforcement or an authorized individual.
- One solution to the reporting process is to create a portal using the same security and credentialing (Cisco VPN, RSA key, etc.) and create a web-interface for reporting that would allow the reviewer to view reports through a web browser or the same methodology of a virtual machine.

Sgt. Purcell's Conclusion and Recommendations

The current design of the VDEL is a good platform for remote examination of digital evidence. The design is excellent for military, large organizations, and other government entities that need the ability to examine data from afar. However, the inherent problem is the lack of a portal to upload large forensic image files to a secure volume within the VDEL. The likely implementation of such design is for organizations that need the ability to create forensic image of media, upload the same to the VDEL volumes, and allow access to another examiner elsewhere in the world. I offer the following suggestions as we look forward in further designing the VDEL:

- Create a secure portal to upload forensic image files with the ability to error check the file transfer with some level of hashing built in to the protocol. Perhaps a software solution can be implemented to hash segments of the forensic image files prior to upload, and during the upload process, the files can be hashed on the VDEL side while written to disk. The ability to “restart” and provide a specific segment that doesn’t verify should be considered in this design. This could be referred to as a hash map of the file wherein 64k or 128k segments of the file are hashed, stored, and presented to the sender and receiver (VDEL) for error checking and file verification. The examiner would perform full verification during the forensic examination of the evidence, but in the interest of time and resources, the initial upload of the evidence should have some level of verification and ability to upload specific segments for network errors, packet loss, and other common failures in network file transfers.
- Create a VM for users to review evidence who not “techies” or forensic examiners. Provide an easy interface and software solution to browse evidence. Once the forensic

Virtual Digital Evidence Laboratory

image of evidence is uploaded, the examiner or case agent should be able to authorize access to the evidence for simple browsing in a program less complicated than EnCase or FTK.

- Create a VM for prosecutors, intelligence analysts, defense attorneys (or designee), or other applicable persons to review forensic reports with an option to download the forensic image files from the VDEL as authorized by the courts or organization with control over the evidence. This must include read-only access, chain of custody logging, permissions to access certain files within the volumes on the VDEL, etc.
- Assemble a team of network intrusion experts to penetrate and determine vulnerabilities within the VDEL. This must be an ongoing process to determine security breaches, unexpected security risks, and so forth.
- Instead of using individual dongles for EnCase and FTK, move to the NAS option, which provides a series of licenses on the network based on the purchase of the hosting VDEL.

It has been a pleasure testing and evaluating the VDEL under the National Center for Forensic Science. I hope my commentary and suggestions will be useful in expanding the overall concept of the VDEL as we move forensic in the field of digital forensics.

Virtual Digital Evidence Laboratory

Report for Sgt. Kevin Stenger

As understood, the purpose of the VDEL is to provide assistance to small local and state law enforcement agencies with digital forensic examinations. The VDEL would provide access to forensic hardware and software allowing agencies to focus on providing trained personnel for examinations and relieving them of the cost of the hardware and software.

Organization of Local and State Law Enforcement

Some basic statistical data on local and state law enforcement agencies should be of assistance to VDEL project personnel in understanding the potential client base of the project. The Department of Justice provides statistics on the size of local and state law enforcement agencies. Data from the 2004 census of state and local law enforcement agencies is summarized in the chart below.

Number of Agencies

<u>Sworn personnel*</u>	<u>Number</u>	<u>Percent</u>
1,000 or more	79	0.4%
500-999	89	0.5%
250-499	217	1.2%
100-249	714	4.0%
50-99	1,259	7.0%
25-49	2,304	12.9%
10-24	4,213	23.6%
5-9	3,513	19.7%
2-4	3,286	18.4%
1	2,202	12.3%

Total	17,876	100%

Table 1: Source 2004 Census of State and Local Law Enforcement Agencies DOJ statistics

Assuming the primary target client for the VDEL project is local law enforcement agencies it should be noted that 97.9% of agencies in the United States have less than 250 officers. 86.9% have less than 50. Most of these agencies have no full time personnel dedicated

Virtual Digital Evidence Laboratory

to computer forensics or computer investigations. Most of these same law enforcement agencies do not have direct control over their computer, software or network assets and rely on the governmental units they serve to support their needs in this area. A suggested source of information on the actual type of computer infrastructure available to local law enforcement in Florida would be the personnel assigned to the FINDER project at the University of Central Florida.

FINDER personnel regularly interact with local and state agencies across Florida and have detailed personnel knowledge on the computer and network resources available to law enforcement agencies in Florida. Personnel at FINDER have reported to me that some law enforcement agencies in North Florida do not have access to computers at all. They state that the computers provided by the FINDER project were actually the first at the agency.

It is important to note that many of the law enforcement agencies attempting to utilize this project would be subject to the policy of Information Management departments that is frequently beyond their control. City, County and State Agencies may have to get support of administrators outside of their agency in order to take advantage of this project. In addition both project personnel and the law enforcement agency may have to coordinate both conflicting written policy on the access of outside networks as well as hardware and software conflicts.

Defense Experts and Legal Issues

In the event that the clients of the VDEL extend to different States project personnel will need to take into account differing State law on access to the evidence. Most State laws permit the defense to have access to the images utilized by law enforcement and the prosecution. Case law varies from State to State on the material that the defense is permitted to access. This may

Virtual Digital Evidence Laboratory

be as simple as the evidence files itself or may include logs, policies and records kept by the VDEL project.

There are potential conflicts between State and Federal law that may require research by the VDEL project. Some States permit defense experts to obtain copies of digital evidence that contains child pornography. Federal rules of procedure as well as some State laws forbid defense experts to have unsupervised access to child pornography.

IV. Configuration of Computers for Tests

Computer 1

- Hardware
 - Dell XPS Generation 2
 - Pentium 4 3.00GHz processor with hyper threading on.
 - 3 GB RAM
 - Linksys ED1032 v3 Instant Gigabit Network Adaptor
 - Netgear WNDR3300 router connected directly via Cat 5e
 - Scientific American cable modem connected to BrightHouse cable.
- Software
 - Windows XP SP3
 - Cisco VPN Client 5.0.00.0340 installed initially.
 - Cisco VPN Client 5.0.02.0090 attempted install.
 - Kaspersky Internet Security 2009 8.0.0.506

Computer 2

- Hardware
 - Toshiba Satellite A205 Laptop
 - Pentium T2330 1.6GHz processor
 - 2 GB RAM
 - Marvell Yukon 88E8039 PCI-E Fast Ethernet Controller
 - Netgear WNDR3300 router connected directly via Cat 5e
 - Scientific American cable modem connected to BrightHouse cable.
- Software
 - Windows Vista Home Premium

Virtual Digital Evidence Laboratory

- Cisco VPN Client 5.0.02.0090 installed
- F-Secure Client Security 8.01 build 133

Results

Computer 1

The existing Cisco VPN client was used to attempt to connect to the VDEL server first without success. Installation of the updated Cisco VPN client was attempted on Computer 1 first. The client was never successfully installed on Computer 1 due to software conflicts most likely associated with older versions of the Cisco VPN. Installation was abandoned on Computer 1 due to severe system corruption resulting from the installation of the Cisco client. The following are notes from the installation attempts on Computer 1.

Attempt to connect with initial Cisco VPN client results in error with no connection. Attempted to connect with firewall and anti virus turned off with same results. Attempted to connect directly to modem bypassing router with same results.

Installed new Cisco version over existing version without uninstalling. Initial install hung on installation of Cisco VPN Deterministic Network Enhancer. Install would not complete and on reboot it resulted in a corrupted registry that degraded rapidly and required eventual reinstall of operating system.

After restoring system old version of Cisco was uninstalled and after reboot new version was installed after antivirus was closed. Install hung on installation of Cisco VPN Adapter. The installation appeared to roll back however on reboot Windows crashed to the blue screen requiring second reinstall of operating system.

Examination of Cisco knowledge base as well as other sources on the Internet indicate that the Cisco VPN client has a number of reported issues and bugs with various routers as well as antivirus products. Problems with the router were ruled out during the installation of the VPN

Virtual Digital Evidence Laboratory

client on Computer 1. While the antivirus program was turned off during one installation attempt Internet trouble shooting sources indicate that in some instances the antivirus must be completely uninstalled prior to the installation of the Cisco VPN client. The antivirus program can then be reinstalled. Solutions vary depending on the hardware and software combination.

In addition Internet sites report problems with automatic uninstall of certain versions of Cisco VPN. Some versions will not uninstall completely requiring manual uninstall of certain features before a new version can be successfully installed. Examination of the registry and folder structure indicate that this was the most likely scenario with the installation of the VPN client on Computer 1.

Computer 2

Computer 2 utilizes a different operating system and antivirus program from Computer 1. In addition Computer 2 had no prior installation of the Cisco VPN client. Installation of Cisco VPN Client 5.0.02.0090 was successful without incident. Computer 2 was used for testing the VDEL project.

VDEL Server Logon

Initial logon attempts to the VDEL server were unsuccessful. The server reported that the password was incorrect. Personnel at NCFS reset the password and logon was accomplished.

Virtual Desktop Logon

Logon to the virtual desktop was completed. The initial setup of the virtual desktop took some time and new users may need to be informed that the delay is normal.

Tool Testing

Encase and FTK were tested on the virtual desktop. No problems were encountered with the use of these tools through the VPN. One notable incident occurred while waiting for FTK to

Virtual Digital Evidence Laboratory

finish indexing. The VPN disconnected before FTK finished indexing. This required the user to reestablish the connection. FTK had finished even though the connection had been broken.

It is possible that the VPN is configured to disconnect after a given period of time. I would recommend that if this is the case that the time out period for the VPN be increased. Many functions in both Encase and FTK require a long period of time and the examiner may wish to stay logged in to monitor them.

Server Resource Use

An important consideration in the use of the VDEL will have to be the use of available system resources on the server coupled with the number of personnel utilizing the system. Encase and FTK 1.X currently only use one processor however they can use extensive amounts of RAM. Obviously the more users on the system the more pressure they will be putting on the server's available resources. FTK 2,3 PRTK (Password Recovery Toolkit) other password breaking tools and upcoming versions of Encase are expected to utilize multiple processors. This could put extensive pressure on the available processing on the server unless restrictions are placed on the amount of system resources made available to each user.

Different functions in Encase and the different versions of FTK can tax differing system resources depending on the function they are performing at any given time. FTK 1.X during indexing put an extensive drain on both drive output as well as processor time. Current versions of Encase only utilize one processor but during certain functions will utilize all the drive output available. Several users on the server at the same time could severely tax the available drive storage output unless the server is set up specifically to accommodate that.

Another potential resource use will be image storage. Currently the Orange County Sheriffs Office has image files stored on our local server amounting to approximately six

Virtual Digital Evidence Laboratory

terabytes. All of this data is compressed. Image files are stored until the case is closed and all appeals are exhausted. Homicide cases and unsolved sex crimes cases have no statute of limitation on them and the files must be maintained indefinitely. We make an effort to delete old cases as often as we can but our storage needs continue to grow. The VDEL project will have to make a determination on where archived image files will be stored. If the VDEL center is to keep them the storage needs for the project can be expected to be significant.

Speed of Access to Evidence

Due to the fact that evidence must be shipped to the main VDEL center for imaging there will be a delay in beginning any exam. Until the personnel at the VDEL image the devices and put it online the examination cannot begin. This defeats one of the most useful attributes of Encase as well as FTK2 and 3 that is the ability to start an examination while an acquisition is being conducted. This can be of vital importance in homicides, missing children and abduction cases where access to the information as fast as possible is vital.

Obtaining Extracted Exhibits and Evidence

Another consideration in the use of a VDEL would be how examiners would get access to exported reports and files that were determined to be of evidentiary value. Common forensic software all allow for the export of a report in either some type of document format or html. Depending on the type of case these reports can be very large possibly in the gigabyte range. An agency working with anything less than a very high speed connection with the VDEL may not be able to download these reports and may have to have the VDEL ship them back to the agency. This is a significant problem in any case where large numbers of files must be exported for review by other experts or presentation in court. The most common example would be a child pornography case where over 100 gigabytes of movie files must be exported for review. It may

Virtual Digital Evidence Laboratory

not be feasible to download this much material on the typical Internet connection available to most agencies.

Shipping

Shipping will be a significant part of the cost of the VDEL project as well as a delay. Assuming a best-case scenario an agency will ship original evidence to the VDEL for imaging. The original evidence will then be shipped back. A report will be generated by the examiner and exported from the VDEL to the local user via the VPN connection.

In a worst case scenario the evidence original evidence will be shipped to and from the VDEL center then the exported exhibits and reports will have to be shipped. If the VDEL center cannot or does not wish to store the image files these too will have to be shipped back to the originating agency.

Sgt. Stenger's Conclusion / Recommendations

At the present time I cannot recommend that the VDEL project be considered for use by small local law enforcement agencies. The only cost savings that I foresee are in the purchase of hardware and software. Due to the function of government agencies often it is easier to obtain funding for hardware and software than personnel and training. A VDEL project will have the added cost of shipping which may offset any savings in hardware or software. The delay in time to access any digital evidence while it is being shipped and imaged is not ideal.

There might be a use for something similar to the VDEL for Intelligence functions by Federal agencies. Seized media overseas could be brought to intelligence locations with access to high-speed data transmission facilities in the country. The devices could be imaged from the country to a facility similar to the VDEL proposal. Once the images are stored on a central

location back in the U.S. examiners and analysts could access the images via a VPN from different Intelligence agencies.

Conclusions

The beta testing provided our research team with valuable information on the strengths and shortcomings of the VDEL. Feedback is logically partitioned into two categories: those related to procedural/legal issues, and technical issues. Below we include a synopsis of the issues raised by the SMEs, and where appropriate, responses from the investigator.

Procedural/Legal Issues

- Sharing information across legal and geographical boundaries may be problematic. For instance, differences between State laws, or between State and Federal laws, must be addressed with respect to information sharing using the VDEL.
 - **Investigator's Response:** This was considered during our design of the VDEL and would have to be addressed alongside various law enforcement agencies possibly on a case-by-case basis.
- Law enforcement agencies technical administration management must be on board in order to facilitate deployment of a VDEL in a law enforcement setting.
 - **Investigator's Response:** This is true and is applicable to any organization that desires to bring in new technology that will affect the entire organization, e.g., a new operating system or new computer system.
- Reports containing child pornography or other contraband must maintain strict adherence to the chain of custody, evidence security, and transmission to authorized personnel. This may result in limiting use of the VDEL to sworn law enforcement officers only.

Virtual Digital Evidence Laboratory

- **Investigator's Response:** This was considered during our design of the VDEL, and the reason we proposed the use of three-factor authentication, which includes, something the user 'has' (hardware token), something the user 'knows' (PIN), and static IP address authentication (the user must have physical access to a computer with a particular IP address).
- The discovery process in criminal cases could be problematic for prosecutors unless they are given access to the VDEL and the report itself. Transmission of the report and evidentiary items (if requested) must be a consideration of the overall design.
 - **Investigator's Response:** This was considered during the design of the VDEL, but was not part of this beta testing.
- The VDEL does not reduce or eliminate the requirement for training of forensic examiners on various forensic tool suites.
 - **Investigator's Response:** In the VDEL's current implementation this is true. However, we have proposed the use of onsite subject matter experts that could assist remote end users with problems they might have. The cost effectiveness of this would have to be addressed.
- When the defense attorney's find out about the network topology and Internet-based access of the VDEL and possible security vulnerabilities, what resources will be required to negate the obvious battles of the courtroom? Will the examiner and organization that implements the VDEL be able to sustain such arguments?
 - **Investigator's Response:** The investigator agrees that this could be a very significant issue as defense attorneys would attempt to attack the credibility of the security of the VDEL, and perhaps draw parallels with recent well-known intrusions on the "big

Virtual Digital Evidence Laboratory

guys” (e.g., Google, Microsoft, etc.). The questions posed by the SME are valid, and we are attempting to identify solutions.

Technical Issues

- One SME had difficulties installing/running Cisco VPN software on some hardware configurations.
 - **Investigator’s Response:** This may require a ‘pre-tested list’ of suggested hardware for use with the VPN software.
- Transportation of post examination evidentiary files may require significant resources required by the local agencies.
 - **Investigator’s Response:** We have designed the VDEL such that prosecutors, defense attorneys, and other individuals with a need to know can be provided with restricted access to the VDEL in order to download reports and evidentiary files.
- Archiving of old case files would require significant added storage requirements to the VDEL.
 - **Investigator’s Response:** We do not foresee any way around this problem. The one compelling issue is that storage space is getting cheaper and cheaper.
- Proposed method of shipping original evidence to the VDEL source, as opposed to Internet upload, would be costly and time consuming.
 - **Investigator’s Response:** We plan on testing the performance of uploading large image files over the network to the VDEL, pending funding. This would require that the local law enforcement agencies have the capability (equipment and training) to create a forensic duplicate.

Virtual Digital Evidence Laboratory

- Potential for overloading the VDEL computing resources if too many examiners simultaneously use the VDEL.
 - **Investigator's Response:** We plan on testing resource saturation at a latter date, pending funding.
- Transmitting the report from the examiner's virtual machine to the examiner's connecting machine is not possible using remote desktop alone.
 - **Investigator's Response:** In its current implementation this is true. We have planned to have a separate area of storage on the SAN that would allow end users (e.g., anyone with a 'need to know') download copies of the reports using a secure protocol (e.g., SSH over the VPN).
- The examiner cannot create custom reports without some level of local authentication to the VM within the LAN of the VDEL. Other options include local access to the shared volumes, but again, the examiner must be within the LAN to do so.
 - **Investigator's Response:** VDEL administrator can provide users with this access on a case-by-case basis.)
- Remote access to workstation does not give examiner full access to install programs stored on media outside of VDEL network.
 - **Investigator's Response:** We believe this to be a desirable feature. Providing forensic examiners with escalated privileges (e.g., root or admin) can lead to issues regarding his/her qualifications to make certain changes to the VMs.
- If hardware problems occur on the examiner's workstation (whether physical or VM application), the examiner may not be able to fix some problems.

Virtual Digital Evidence Laboratory

- **Investigator's Response:** This would be true on the physical side of the connection (i.e., the examiner's desktop). Hardware issues on the VDEL side would have to be addressed by a person knowledgeable with the hardware/software.
- Full administrative control of the examination environment is not possible in the current implementation of the VDEL, which deviates from the norm in stand-alone forensics.
 - **Investigator's Response:** To reiterate, we believe this to be a desirable feature. Providing forensic examiners with escalated privileges (e.g., root or admin) could lead to issues regarding his/her qualifications to make certain changes to the VMs.
- The examination environment is susceptible to the Internet although port 80 is shutdown in the current implementation of the VDEL. By virtue of design, the VDEL must be connected to the Internet, and this deviates from best practices in computer/digital forensics.
 - **Investigator's Response:** To reduce the possibility of intrusion we have deployed three-factor authentication. Three-factor authentication combined with high-grade encryption makes the possibility of such an intrusion nil. Moreover, it would be nearly impossible for a man-in-the-middle attack to occur because of the high-grade encryption (AES).
 - Since the VDEL is connected to the Internet, the LAN is susceptible to penetration and intrusion. Further testing is required to ensure full security. Moreover, it seems regular testing and monitoring would be required to secure the network.
 - **Investigator's Response:** To reiterate: to reduce the possibility of intrusion we have deployed three-factor authentication. Three-factor authentication combined with high-grade encryption makes the possibility of such an intrusion nil. Moreover, it

Virtual Digital Evidence Laboratory

would be nearly impossible for a man-in-the-middle attack to occur because of the high-grade encryption (AES).

Recommended Modifications by Subject Matter Experts

- Create a secure portal to upload forensic image files with the ability to error check the file transfer with some level of hashing built in to the protocol. Perhaps a software solution can be implemented to hash segments of the forensic image files prior to upload, and during the upload process, the files can be hashed on the VDEL side while written to disk. The ability to “restart” and provide a specific segment that doesn’t verify should be considered in this design. This could be referred to as a hash map of the file wherein 64k or 128k segments of the file are hashed, stored, and presented to the sender and receiver (VDEL) for error checking and file verification. The examiner would perform full verification during the forensic examination of the evidence, but in the interest of time and resources, the initial upload of the evidence should have some level of verification and ability to upload specific segments for network errors, packet loss, and other common failures in network file transfers.
 - **Investigator’s Response:** Clearly there needs to be some sort of automated verification of the evidence. We are currently identifying solutions to achieve this goal.
- Create a VM for users to review evidence who not “techies” or forensic examiners. Provide an easy interface and software solution to browse evidence. Once the forensic image of evidence is uploaded, the examiner or case agent should be able to authorize access to the evidence for simple browsing in a program less complicated than EnCase or FTK.
 - **Investigator’s Response:** This had been a planned feature from the outset. We can implement this fairly easily pending future funding.

Virtual Digital Evidence Laboratory

- Create a VM for prosecutors, intelligence analysts, defense attorneys (or designee), or other applicable persons to review forensic reports with an option to download the forensic image files from the VDEL as authorized by the courts or organization with control over the evidence. This must include read-only access, chain of custody logging, permissions to access certain files within the volumes on the VDEL, etc.
 - **Investigator's Response:** This had been a planned feature from the outset. We can implement this fairly easily pending future funding.
- Assemble a team of network intrusion experts to penetrate and determine vulnerabilities within the VDEL. This must be an ongoing process to determine security breaches, unexpected security risks, and so forth.
 - **Investigator's Response:** This is a good idea: A network and security audit. This is something that we could perform internally, and later by an external source. We suggest that audits should be performed on a periodic and frequent basis to ensure network integrity.
- Instead of using individual dongles for EnCase and FTK, move to the NAS option, which provides a series of licenses on the network based on the purchase of the hosting VDEL.
 - **Investigator's Response:** This is a very good idea and one we could implement pending future funding.
- In some cases, the defense will request a copy of the forensic image files and all associated data derived from the case (exported data, reports, etc). The VDEL does not provide a portal to readily access this data. An alternative is to provide the defense's

Virtual Digital Evidence Laboratory

export witness with a VM that contains read-only access to the evidence where he or she is monitored by law enforcement or an authorized individual.

- **Investigator's Response:** This is a feature we had planned from the beginning, and something we could implement pending future funding.
- One solution to the reporting process is to create a portal using the same security and credentialing (Cisco VPN, RSA key, etc.) and create a web-interface for reporting that would allow the reviewer to view reports through a web browser or the same methodology of a virtual machine.
 - **Investigator's Response:** This is a feature we had planned from the beginning, and something we could implement pending future funding.

Acknowledgements

We would like to thank Mark Pollitt, M.S. (FBI, retired), Officer Eric Walton (Florida Electronic Crimes Task Force), Chris Marberry (ManTech) and Paul Burke (MIT Lincoln Labs) for input, feedback, and dedicated work on this project.

Dissemination of Findings

The final authorized version of this report will be made available on the NCFS website (www.ncfs.org). Sources of dissemination are diverse, including forensic sciences community, law enforcement, and academia. These sources are listed below.

Publications

G. Dorn, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics V*, Springer, New York. pp. 69-82. 2009.

M. Pollitt, K. Nance, B. Hays, R. Dodge, P. Craiger, P. Burke, C. Marberry, and B. Brubaker. Virtualization and digital forensics: A research and education agenda. *Journal of Digital Forensics Practice*, 4, pp. 74-82, 2008.

P. Craiger, C. Marberry, P. Burke, and M. Pollitt. A virtual digital evidence lab. In I. Ray and S. Sheno (Eds). *Advances in Digital Forensics IV*. IFIP. New York. Pp. 357-365. 2008.

P. Craiger, C. Marberry, G. Dorn, and S. Conrad. 2009. A Virtual Architecture for Digital Forensic Tool Validation. *Proceedings of the American Academy of Forensic Science 61st Annual Meeting*, Denver, Colorado, 2009, pp. 209.

Professional Presentations

P. Craiger, C. Marberry, P. Burke, and M. Pollitt. A virtual digital evidence lab. Presentation for the 4th Annual Meeting of IFIP Working Group 11.9 Digital Evidence, Kyoto, Japan, January 2008.

P. Craiger, C. Marberry, G. Dorn, and S. Conrad. 2009. A Virtual Architecture for Digital Forensic Tool Validation. Presentation for the 61st Annual Meeting of the American Academy of Forensic Science, Denver, Colorado, February 2009.

Local Onsite Dissemination

We have provided dozens of onsite presentations and demonstrations of our lab to interested parties, including local, state, and federal law enforcement, Department of Defense personnel, academic researchers, and local school children.

References and Associated Readings

- C. Marberry and P. Craiger. CD-R acquisition hashes affected by write options. *Journal of Digital Forensics Practice*, New York, Taylor & Francis, 4, pp. 1-10. 2007.
- C. Maryberry and P. Craiger, Burn options affect cryptographic one-way hashes of CD-R Media. In P. Craiger and S. Shenoi (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 149-161. 2008.
- G. Dorn, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. In G. Peterson and S. Shenoi (Eds.), *Advances in Digital Forensics V*, Springer, New York. pp. 69-82. 2009.
- M. Pollitt, K. Nance, B. Hays, R. Dodge, P. Craiger, P. Burke, C. Marberry, and B. Brubaker. Virtualization and digital forensics: A research and education agenda. *Journal of Digital Forensics Practice*, 4, pp. 74-82, 2008.
- P. Burke and P. Craiger, Forensic Analysis of Xbox Consoles. In P. Craiger and S. Shenoi (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 269-280. 2008.
- P. Burke and P. Craiger, Trace evidence of secure delete programs. In M. Olivier and S. Shenoi (Eds.), *Advances in Digital Forensics II*. Springer, New York, 185-198, 2006.
- P. Burke and P. Craiger. Xbox forensics. *Journal of Digital Forensics Practice*, New York, Taylor & Francis, 4, pp. 275-282, 2007.
- P. Craiger, C. Marberry, P. Burke, and M. Pollitt. A virtual digital evidence lab. In I. Ray and S. Shenoi (Eds). *Advances in Digital Forensics IV*. IFIP. New York. Pp. 357-365. 2008.
- P. Craiger and P. Burke, Mac OS X Forensics. In M. Olivier and S. Shenoi (Eds.), *Advances in Digital Forensics II*, Springer, New York, 159-170, 2006.
- P. Craiger, C. Marberry, G. Dorn, and S. Conrad. 2009. A Virtual Architecture for Digital Forensic Tool Validation. *Proceedings of the American Academy of Forensic Science 61st Annual Meeting*, Denver, Colorado, 2009, pp. 209.
- P. Craiger, Computer forensics methods and procedures In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 736-755, 2006.
- P. Craiger, Digital Evidence. In H. Bigdoli (Ed.), *Handbook of Technology Management*. Vol 2. New York: John Wiley & Sons, pp. 921-930, 2010.
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Evidence*. Humana Press, pp. 11-22. 2008
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Evidence*. Humana Press, pp. 11-20. 2008.

Virtual Digital Evidence Laboratory

P. Craiger. (May 2004). Linux: Portable forensics Toolkit. Presentation accepted for the 26th Annual Department of Energy Computer Security Training Conference. St. Louis, MO.

S. Conrad, C. Rodriguez, C. Marberry, and P. Craiger. Forensic analysis of the Sony Playstation Portable. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics V*, Springer, New York. pp. 119-132. 2009.

S. Conrad, G. Dorn, and P. Craiger. Forensic analysis of PlayStation 3 Game Console. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics VI*, Springer, New York. To appear.

P. Craiger, M. Pollitt and J. Swauger, Digital Evidence and law enforcement In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 739-777, 2006.

P. Craiger, Recovering digital evidence from Linux systems, In S. Sheno and M. Pollitt (Eds), *Advances in Digital Forensics*, New York, Springer, pp. 233-243, 2006.

P. Craiger, J. Swauger, and C. Marberry. Digital forensic software tool validation. In P. Kanellis (Ed) *Digital Crime and Forensic Science in Cyberspace* Idea Group, 91-108, 2006.

P. Craiger, P. Burke, and C. Marberry. Forensics Analysis of Phishing Cases Using Open Source and Free Tools. *Anti-phishing and Online Fraud. Journal of Digital Forensics Practice*, New York, Taylor & Francis, 223-230, 2007.

P. Craiger. (Sept, 2002). An applied course in network forensics. Presentation for the Workshop for Dependable and Secure Systems. University of Idaho, Moscow, Idaho, Sept 23-35.

P. Craiger, & M. Pollitt (to appear). Computer forensics and law enforcement. In H. Bigdoli (Ed.), *Handbook of Information Security*. John Wiley & Sons.

Appendix

Resumes of Subject Matter Experts and Investigator

Virtual Digital Evidence Laboratory

**Sgt. Dan Purcell,
MSDF**

- Twelve years in active, fulltime law enforcement
- Computer forensic examiner for 10 years
- Approximately 400+ forensic examinations (single cases involving thousands of media)

Experience

Deputy Sheriff/Investigator/Investigator Sergeant

- Master's of Science in Digital Forensics, from the University of Central Florida, 2007.
- Uniformed patrol and trained new deputy sheriffs, 1995 to 1997.
- General assignment and economic crimes investigator, 1998 to 2002.
- Promoted to the rank of Sergeant in March of 2002, leading and managing the Economic & Computer Crimes Unit.
- Developed and manages computer forensic program at the Seminole County Sheriff's Office
- Conducted numerous digital forensic examinations resulting in multiple convictions in state and federal court.
- Instrumental in forming partnerships with other law enforcement agencies and private businesses internationally concerning high-tech crimes investigations and digital forensics.
- Active participant in the Internet Crimes Against Children Task Force.
- Sworn U.S. Deputy Marshal with the United States Secret Service Electronic Crimes Task Force in Central Florida and one of fifty specialists nationwide on the Secret Service National Response Team for major incidents and complex investigations.
- Instructs introductory, intermediate, advanced, and expert level computer forensic courses throughout the nation.
- Regular instructor at the Federal Law Enforcement Training Center for SCERS and BCERT courses.
- Familiar with a variety of hardware and software titles relating to computer forensics examinations. Conducted numerous hardware and software product validations.
- Instructor for the International Association of Computer Investigative Specialists (IACIS), 2001 to 2005.
- Eastern United States CFCE Administrator for the IACIS Certified Forensic Computer Examiner certification process. Leads and manages all states east of the Mississippi River including students in Europe.
- Testified as an expert in the field of computer forensics in the following cases in which the defendant(s) were convicted in state or federal court:
 - 18th Judicial Circuit, Seminole County, FL, State of Florida v. M. Belkerdid, 99-3368-CFA
 - U.S. District Court, Middle District of FL, U.S. v. Rebecca Zangwill, 6:05-CR-34-ORL-22JGG

Virtual Digital Evidence Laboratory

Sgt. Kevin Stenger, MSDF

Forensic Computer Examiner

2500 W Colonial Dr.

Orlando, FL 32804

(407) 254-7229

Certified: International Association of Computer Investigative Specialists
Guidance Software (EnCE)

Education and Training

- Master's of Science in Digital Forensics, from the University of Central Florida, 2007.
- Bachelor of Science in Business Administration (Accounting) from the University of Central Florida, 1984.
- International Association of Computer Investigative Specialists two week computer forensic course, 1996.
- International Association of Computer Investigative Specialists training seminars 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2007.
- Guidance Software, Encase Intermediate Computer Forensics Class 1999, Advanced Computer Forensics Class March 2006.
- Information Technology Study Group seminar 2/2000, 10/2000, 5/2001, 10/2002, 10/2004, 10/2005.
- AccessData Bootcamp January 2007. Windows Forensics September 2007
- Graduate Certificate in Computer Forensics from the University of Central Florida 2002
- Computer and Enterprise Investigations Conference CEIC 5/2007

1. Experience

- Hired by the Orange County Sheriff's Office 1986
- Supervisor of the Computer Crimes Squad since 2002.
- Member of the United States Secret Service-Florida Electronic Evidence Task force (FLEET) since 2004.
- Supervisor of the Economic Crimes Squad from 1998 to 2002.
- Computer Forensic Examiner for the Orange County Sheriffs Office since 1998.
- As of February 2008 seized approximately 469 devices and examined 455.

2. Certification

- Certified by the International Association of Computer Investigative Specialists. Holding the DOS Seizure Certificate (DSC) 1996, DOS Processing Certificate (DPC) 1996, and the Certified Forensic Computer Examiner Certificate (CFCE) 1998, IACIS Proficiency

Virtual Digital Evidence Laboratory

Exam 2002, Certified Computer Forensic Instructor 2004, IACIS Proficiency Exam 2005.

- Certified by Guidance Software as an Encase Certified Examiner (EnCE) 2001.
- CompTIA - A+, September 2003 Network+, October 2004

3. **Teaching Experience**

- Coach and instructor for the annual IACIS training seminars and the Certified Forensic Computer Examiner process.
- South East Regional Director for the IACIS CFCE process 2007.
- Taught computer crimes for the Orange County Sheriffs Office and for outside agency classes.
- Given lectures at the University of Central Florida in Computer Forensics.
- Part time lead instructor for Guidance Software on the Encase computer forensics program and methodology.

4. **Professional Associations**

- International Association of Computer Investigative Specialists

Officer Eric Walton

Federal Marshal

U.S Secret Service Electronic Crimes Task Force

University of Central Florida Police Department

EMPLOYMENT HISTORY

- UCF Police Department 1991-Present
- Investigator Technology Base Crime Unit 2002- Present

PROFESSIONAL QUALIFICATIONS

Certifications and Accreditations

- National White Collar Crime Center basic data recover class 2000
- Florida Department of Law Enforcement Internet Investigation 2000
- Federal Bureau of Investigation FBI National Academy Network Investigation 2001
- United States Secret Service Electronic Crime Special Agent Program (ECSAP) 2004 Class consisted of three parts Preliminary basic computer crime Basic Forensic Investigation Advance Electronic Crime Investigation courses were conducted at the Department of Homeland security training center In Georgia The Course was eight weeks long upon completion I was certified to conduct forensic exams for the United States Secret Service, Immigration Customs and Enforcement (ICE)and the Internal Revenue service (IRS)
- Access Data Certification Basic 2005
- Access Data Certification Advance 2005
- Guidance Software Encase Basic certification 2005
- Parbens Cell Phone Forensic 2006
- Forty Hours mandatory training with yearly re-certification exam
- Name Lab Director of the Florida Law Electronic Evidence Team (FLEET) 2004 by the taskforce steering committee
- Instructor for the Secret Service Basic Investigation Electronic Crime Program (BIECP) 2006- present
- Access Data Decryption Class 2007
- Encase version 5 update Class 2007
- Federal Law Enforcement Training Center Network Investigation 2008
- National White Collar Crime Center Forensic Triage Class 2008
- Co-lead instructor United States Postal Service Internet Investigation 2008

Cases processed: 500+ cases on the state and local level

Virtual Digital Evidence Laboratory

J. Philip Craiger, Ph.D.

Assistant Director for Digital Evidence
National Center for Forensic Science
12354 Research Parkway
University of Central Florida
Orlando FL, 32826
Email: philip@craiger.net
Voice: (407) 823-3527

Assistant Professor
Department of Engineering Technology
University of Central Florida
Orlando, FL 32816
Email: pcraiger@mail.ucf.edu

EDUCATION

- Ph.D., 1992, Industrial/Organizational Psychology. University of South Florida, Tampa, FL. Minor in Artificial Intelligence from the Department of Computer Science.
 - Dissertation title: A heuristic procedure for mapping knowledge, skills, and abilities to tasks.
 - Published as: P. Craiger and M. Coovert (1993) A fuzzy system for mapping worker attributes to task. *Behavior Research Methods, Instruments and Computers*, 26, 107-111.
- M.S., 1990. Industrial/Organizational Psychology. University of South Florida, Tampa, FL.
- B.S., 1980. Political Science (Government). Minor in Criminology. Florida State University, Tallahassee FL.

EDITED BOOKS

- P. Craiger and S. Sheno. *Advances in Digital Forensics III*, International Federation for Information Processing, New York, 2007.

JOURNAL S (PEER-REVIEWED)

- M. Pollitt, K. Nance, B. Hays, R. Dodge, P. Craiger, P. Burke, C. Marberry, and B. Brubaker. Virtualization and digital forensics: A research and education agenda. *Journal of Digital Forensics Practice*, 4, pp. 74-82, 2008.
- P. Burke and P. Craiger. Xbox forensics. *Journal of Digital Forensics Practice*, New York, Taylor & Francis, 4, pp. 275-282, 2007.
- C. Marberry and P. Craiger. CD-R acquisition hashes affected by write options. *Journal of Digital Forensics Practice*, New York, Taylor & Francis, 4, pp. 1-10. 2007.
- P. Craiger, P. Burke, and C. Marberry. Forensics Analysis of Phishing Cases Using Open Source and Free Tools. Anti-phishing and Online Fraud. *Journal of Digital Forensics Practice*, New York, Taylor & Francis, 223-230, 2007.
- P. Craiger, M. Coovert and M. Teachout, Fuzzy rule-based system for predicting job performance, *International Journal of Information Technology and Decision Making*, 2003.
- M. Coovert and P. Craiger, An expert system for integrating multiple fit-indices for structural equations modeling, *New Review of Applied Expert Systems*, 6, pp 131-140, 2001.
- J. Shroder, M. Bishop, J. Olsenholler and P. Craiger, *Geomorphology education and the World Wide Web Geomorphology and Public Policy*, 47, pp 343-363, New York, Elsevier, 2002.

Virtual Digital Evidence Laboratory

- M. Coovert, P. Craiger and M. Teachout, The effectiveness of the direct product versus confirmatory factor model for reflecting the structure of multimethod-multirater job performance data, *Journal of Applied Psychology*, 2, pp. 271-280, 1997.
- P. Craiger, R. Weiss, D. Goodman and A. Butler, Simulating organizational behavior with fuzzy cognitive maps. *International Journal of Computational Intelligence and Organizations*, 3, pp. 120-133, 1996.
- P. Craiger and M. Coovert, A fuzzy system for mapping worker attributes to tasks, *Behavior Research Methods, Instruments and Computers*, 26, pp. 107-111, 1993.
- P. Craiger and M. Coovert, Fuzzy Fit-Index Tutoring System (FFITS): An intelligent system for interpreting and integrating fit indices from covariance structure modeling solutions, *Applied Psychological Measurement*, 15, p. 292, 1991.
- L. Penner, S. Harris, J. Llobet and P. Craiger, Studying personnel decisions about female managers: Methodological considerations, *Equal Opportunities International*, 10, pp. 3-9, 1991.

BOOK CHAPTERS (REFEREED)

- S. Conrad, G. Dom, and P. Craiger. Forensic analysis of PlayStation 3 Game Console. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics VI*, Springer, New York. To appear.
- P. Craiger, Digital Evidence. In H. Bigdoli (Ed.), *Handbook of Technology Management. Vol 2*. New York: John Wiley & Sons, pp. 921-930, 2010.
- G. Dom, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics V*, Springer, New York. pp. 69-82. 2009.
- S. Conrad, C. Rodriguez, C. Marberry, and P. Craiger. Forensic analysis of the Sony Playstation Portable. In G. Peterson and S. Sheno (Eds.), *Advances in Digital Forensics V*, Springer, New York. pp. 119-132. 2009.
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Evidence*. Humana Press, pp. 11-22. 2008
- P. Burke and P. Craiger, Forensic Analysis of Xbox Consoles. In P. Craiger and S. Sheno (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 269-280. 2008.
- C. Maryberry and P. Craiger, Burn Options Affect Cryptographic One-way Hashes of CD-R Media. In P. Craiger and S. Sheno (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 149-161. 2008.
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Evidence*. Humana Press, pp. 11-20. 2008.
- P. Craiger and P. Burke, Mac OS X Forensics. In M. Olivier and S. Sheno (Eds.), *Advances in Digital Forensics II*, Springer, New York, 159-170, 2006.
- P. Burke and P. Craiger, Trace evidence of secure delete programs. In M. Olivier and S. Sheno (Eds.), *Advances in Digital Forensics II*. Springer, New York, 185-198, 2006.
- P. Craiger, Computer forensics methods and procedures In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 736-755, 2006.
- P. Craiger, M. Pollitt and J. Swauger, Digital Evidence and law enforcement In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 739-777, 2006.
- P. Craiger, Recovering digital evidence from Linux systems, In S. Sheno and M. Pollitt (Eds), *Advances in Digital Forensics*, New York, Springer, pp. 233-243, 2006.
- P. Craiger, J. Swauger, and C. Marberry. Digital forensic software tool validation. In P. Kanellis (Ed) *Digital Crime and Forensic Science in Cyberspace* Idea Group, 91-108, 2006.
- M. Coovert, L. Foster and P. Craiger, Technology and Stress, J. Barling, K. Kelloway and M. Frone (Eds), *Handbook of Work Stress*, New York, Sage Publications, pp.5-9, 2003.
- P. Craiger and V. Collins. Practical guide to evaluating computer-enabled communication in organizations. In J. Edwards, J. Scott and N. Raju, N (Eds), *The Human Resources Handbook of Program Evaluation*, New York: Sage Publishing, pp. 34-56, 2003.

Virtual Digital Evidence Laboratory

- P. Craiger, Computer-assisted instruction, In M. Zeleny (Ed), Handbook of Information Technology in Business, London: Thompson International Publishing, pp. 34-55, 2000.
- P. Craiger, Human-Computer Interaction, In M. Zeleny (Ed), Handbook of Information Technology in Business, London: Thompson International Publishing, pp. 450-66, 2000.
- M. Coovert and P. Craiger, Modeling performance and establishing training criteria in training systems. In J. K. Ford (Ed), Improving training effectiveness in work organizations pp 47-71 Hillsdale, NJ: Lawrence Erlbaum Associates. 1996.
- M. Coovert, P. Craiger and J. Cannon-Bowers, Innovations in modeling and simulating team performance: Implications for decision making. In R. Guzzo and E. Salas (Eds), Team effectiveness and decision making in organizations: Frontiers in industrial and organizational psychology pp 149-203 New York: Jossey-Bass. 1996.
- L. Penner, B. Fritzsche, P. Craiger and T. Freifeld, Measuring the prosocial personality In J. Butcher and C. D. Spielberger (Eds) Advances in personality assessment (Vol 10) Hillsdale, NJ: Lawrence Erlbaum, 1995.
- L. Penner and P. Craiger, Individual performance in a team context: The weakest link. R. Swezey and E. Salas (Eds), Teams: Their training and performance New York: ABLEX. 1991.

GRANTS AND CONTRACTS

2009-2010:

- P. Craiger (CO-PI). \$167,217. NIJ Support of NCFS Research and Activities (ID: 1043669). National Institute of Justice.
- P. Craiger & C. Whitcomb \$30,000. NIJ Support of Virtual Forensics Digital Laboratory (ID: 1049467). National Forensic Science Technology Center
- P. Craiger & C. Whitcomb \$343,800.00. Experimental Study of the Validity and Reliability of Digital Forensics (ID: 1049539). National Institute of Justice.

2006-2008:

- P. Craiger & C. Whitcomb \$210,000 Virtual Digital Evidence Lab. National Institute of Justice.
- P. Craiger & C. Whitcomb \$53,749 Digital Evidence Markup Language. National Institute of Justice.
- P. Craiger & C. Whitcomb \$52,000 Digital Evidence Certification. National Institute of Justice.

Virtual Digital Evidence Laboratory

2005:

- P. Craiger & C. Whitcomb \$84,000 Digital Evidence Markup Language-Digital Evidence Certification. National Institute of Justice.
- P. Craiger & C. Whitcomb \$64,000 Virtual Digital Evidence Lab. National Institute of Justice.

2003:

- B. Burnham, P. Craiger (Primary Author: 95%) and V. Winter, Cybercorp Scholarships at the University of Nebraska at Omaha Information Assurance Program, National Science Foundation, DUE- 0313691, \$2.2 Million (4 years).
- B. Burnham and P. Craiger (Primary author: 90%) Department of Defense Information Assurance Program Scholarships at the University of Nebraska at Omaha Information Assurance Program, U.S. Department of Defense, Awarded \$294,000.
- P. Craiger, Computer and Network Forensics NASA Nebraska Space Grant and EPSCoR Seed Research Program \$1,000.
- P. Craiger and K. Gubbels, Honey pots for Defense in Depth, NASA Nebraska Space Grant and EPSCoR Seed Research Program \$1,200

2001:

- P. Craiger, Ubiquitous Computing Lab, The Nebraska Foundation. \$60,000.
- M. Bishop, P. Craiger and A. Stoyen, Global Land-Ice Measurements from Space NASA Nebraska Space Grant Consortium, \$10,000.
- M. Bishop, P. Craiger and A. Stoyen, Global Land-Ice Measurements from Space NASA Nebraska Space Grant and EPSCoR Seed Research Program. \$1,000.
- P. Craiger, NASA Space Grant and EPSCoR Program Seed Program. \$3,000.

Pre-2000:

- PI P. Craiger A statistical model of Marine Corps Quality of Life, US Army Research Office Contract DAAH04-96-C-0086. \$20,000.
- P. Craiger and D. Peak, AT&T Peter Kiewit Foundation for Educational Technology (Co-Principal Investigator). \$1500.
- P. Craiger (SME) Statewide education for advanced practice community health nursing Subject matter expert (Federal Department of Health and Human Services), \$4,000 subcontract to UNO.
- PI, P. Craiger, Navy QoL Predictive Model Project US Army Research Office Contract No DAL03-91-C-0034, TCN 96217 Awarded \$38,000.
- PI, P. Craiger and J. Crehan, National Aeronautics and Space Administration Space Grant Consortium. \$7,500.
- P. Craiger First Data Corp (Non disclosure contract: Proprietary contract work) Principal investigator Awarded, \$17,000
- P. Craiger and R. Weiss, Conagra Contract (Non disclosure contract: Proprietary contract work) Research design and data analysis Statistical package training. 3,000.
- PI, P. Craiger Navy Quality of Life Predictive Model Project US Army Research Office Scientific Services Program, Contract DAAL03-91-C-0034, Awarded \$54,000.
- D. Peak, P. Craiger and R. Bernier, Environmental Justice Through Pollution Prevention (Environmental Protection Agency PY90060204). \$75,000.

Virtual Digital Evidence Laboratory

PROFESSIONAL CONFERENCE PROCEEDINGS (PEER-REVIEWED)

- P. Craiger, P. Burke, and M. Pollitt. Lessons learned from teaching a distance delivered incident response course. Presentation at the *62nd Annual Meeting of the Academy of Forensic Sciences*. February 22. Seattle, WA.
- P. Craiger, C. Marberry, G. Dorn, and S. Conrad. 2009. A Virtual Architecture for Digital Forensic Tool Validation. Proceedings of the *American Academy of Forensic Science 61st Annual Meeting*, Denver, Colorado, 2009, pp. 209.
- S. Conrad, G. Dorn, and P. Craiger. Forensic analysis of PlayStation 3 Game Console. Presentation at the *Sixth Annual Meeting of the International Federation for Information Processing*, Hong Kong, China.
- G. Dorn, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. Presentation at the *Fifth Annual Conference of the International Federation for Information Processing*, Orlando, FL.
- S. Conrad, C. Rodriguez, C. Marberry, and P. Craiger. Forensic analysis of the Sony Playstation Portable. Fifth Annual Conference International Federation for Information Processing, Orlando, FL.
- P. Craiger, L. Ponte, C. Whitcomb, and M. Pollitt. Master's in Digital Forensics. Proceedings of the 40th Annual Hawaii International Conference on System Sciences. To appear.
- P. Craiger, M. Pollitt, C. Marberry, and P. Burke. CD-ROM Write Options Affect Calculation of One-way Cryptographic Hashes. Proceedings of the 2007 Annual Meeting of the American Academy of Forensic Science. To appear.
- P. Craiger, J. Swauger and C. Marberry, Digital evidence obfuscation: recovery techniques. The Proceedings of the International Society for Optical Engineering, pp. 777-888, 2005.
- P. Craiger, Portable forensics with Linux. Proceedings of the Annual Meeting of the Nebraska Academy of Sciences, Lincoln, NE, 2004.
- P. Craiger, et al, An applied course in network forensics. Proceedings of the Workshop for Dependable and Secure Systems University of Idaho, Moscow, Idaho, Sept 23-35, 2002.
- R. Weiss and P. Craiger, Implications of the Elaboration Likelihood Model for automation monitoring failure. Proceedings of the Annual Meeting of the Nebraska Academy of Sciences, Lincoln, NE, 2002.
- M. Coovert, Elliot, L. Foster and P. Craiger, Measurement in synthetic task environments for teams: A methodological typology. Proceedings of the Eighth International Conference on Human-Computer Interaction, 2002.
- P. Craiger, M. Coovert and M. Teachout, Fuzzy neural models in industrial psychology research. Proceedings of the World Congress on Neural Networks, Vol II, 617-620, 1993.
- R. Weiss, J. de Groot and P. Craiger, Presenting the Programmable Task Battery for research into automation bias/automation induced complacency. Proceedings of the Annual Meeting of the Human Factors and Ergonomics Society, Chicago, IL, 1998.
- P. Craiger, D. Goodman, R. Weiss and J. DeGroot, Mental models and pilot performance: A cognitive science approach. Proceedings of the Nebraska Academy of Sciences Meeting, Lincoln, NE, 1997.
- P. Craiger and M. Coovert, Modeling dynamic social and psychological processes with fuzzy cognitive maps. Proceedings of the Third IEEE World Conference on Fuzzy Systems, 3, 1873-1877, 1994.
- P. Craiger, Discovering causal model implications with fuzzy cognitive maps: Help for the behavioral scientist. Proceedings of the Fourth IEEE World Conference on Neural Networks, 2, 836-841, 1994.
- M. Coovert, E. Salas, J. Cannon-Bowers, P. Craiger and P. Takalkar, Understanding team performance measures: Application of Petri nets Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, pp 387-393, Washington, D C: IEEE Computer Society Press, 1990.

CHAired CONFERENCES/PROGRAM PANELS

- (Chair) International Federation for Information Processing Working Group 11.9 (Digital Forensics),

Virtual Digital Evidence Laboratory

January, 2007, Orlando FL.

- (Program panel) Computer Forensics Track of the ACM SAC 2007, The 22nd Annual ACM Symposium on Applied Computing, Seoul Korea.
- (Co-chair), Anti-Phishing Working Group Fall Meeting, November, 2006, Orlando, FL.
- (General Chair) International Federation for Information Processing Working Group 11.9 (Digital Forensics), January, 2006, Orlando FL.
- (Member) Technical Working Group on Training and Education in Digital Forensics. NIST/NIJ Sponsored Education Committee.
- (General Chair) International Federation for Information Processing Working Group 11.9 (Digital Forensics), January, 2005, Orlando FL.

CONFERENCE PRESENTATIONS (REFEREED)

- P. Craiger, P. Burke, M. Pollitt. Lessons learned from teaching a distance delivered incident response course. Presentation at the 62nd Annual Meeting of the Academy of Forensic Sciences. February 22. Seattle, WA.
- P. Craiger, M. Pollitt, C. Marberry, and P. Burke. CD-ROM Write Options Affect Calculation of One-way Cryptographic Hashes. Presentation for the 2007 Annual Meeting of the American Academy of Forensic Science. February 2007, San Antonio, TX.
- M. Pollitt, C. Whitcomb, P. Craiger, N. Bebe, and A. Brill. A Primer and update on digital evidence. Presentation for the 2007 Annual Meeting of the American Academy of Forensic Science. February 2007, San Antonio, TX.
- P. Craiger, L. Ponte, C. Whitcomb, and M. Pollitt. Master's in Digital Forensics. Presentation for the 40th Annual Hawaii International Conference on System Sciences. January, 2007, Hawaii, Hawaii.
- P. Craiger, P. Burke, and C. Marberry. Forensics Analysis of Phishing Cases Using Open Source and Free Tools. 2006 Anti-Phishing Working Group Fall General Meeting. November, 2006, Orlando, FL.
- P. C. Maryberry and P. Craiger, Burn Options Affect Cryptographic One-way Hashes of CD Media. Presentation at the Third Annual International Federation for Information Processing Working Group 11.9 (Digital Forensics) Meeting, January, 2007, Orlando, FL.

- P. Burke and P. Craiger, Forensic Analysis of Xbox Consoles. In P. Craiger and S. Sheno (Eds.), Presentation at the Third Annual International Federation for Information Processing Working Group 11.9 (Digital Forensics) Meeting, January, 2007, Orlando, FL.
- P. Craiger and P. Burke. Mac OS X Forensics. Second Annual Conference of the International Federation for Information Processing Working Group 11.9 (Digital Forensics). Feb. 2, 2006, Orlando, FL.
- P. Burke and P. Craiger Trace evidence of secure delete programs. Second Annual Conference of the International Federation for Information Processing Working Group 11.9 (Digital Forensics). Feb. 2, 2006, Orlando, FL.
- R. Eaglin and P. Craiger, Data Sharing and the Digital Evidence Markup Language. 1st Annual GJXDM Users Conference, Atlanta, GA. (not peer reviewed), 2005.
- P. Craiger, Recovering digital evidence from Linux systems, First Annual Conference of the International Association of Information Professionals Working Group 11.9 (Digital Forensics), Orlando, FL, February, 2005.
- P. Craiger, Digital evidence obfuscation: Recovery techniques Meeting of the International Society for Optical Engineering Orlando, FL, April, 2005.
- P. Craiger, Portable Linux Forensics, Presentation accepted for the 26th Annual Department of Energy Conference on Computer Security Training Kansas City MO, May, 2004.
- P. Craiger and S. Webb, Forensics with Linux/ Presentation for the 8th Annual INFOTEC Conference Omaha, NE, April, 2004.
- P. Craiger, Network forensics investigative techniques, 25th Annual Department of Energy Conference on Computer Security Training Baltimore MD, April, 2003.
- S. Webb and P. Craiger, Defensive Battle Stations In Network-Centric Warfare: Rapid-response Computer and Intrusion Forensics Proceedings of the 6th Annual Systems Engineering Conference, San Diego, CA, October, 2003.
- K. Gubbels and P. Craiger, Honeypots for Defense-in-Depth. 25th Annual Department of Energy Conference on Computer Security Training Baltimore MD, April, 2003.
- P. Craiger, Computer and network forensics. Seventh Annual INFOTEC Conference Omaha, NE, April, 2003.
- K. Gubbels and P. Craiger, Defense-in-depth with honeypots. Seventh Annual INFOTEC Conference Omaha, NE, April, 2003.
- P. Craiger, An applied course in network forensics. Workshop for Dependable and Secure Systems University of Idaho, Moscow, Idaho, Sept 23-35, September, 2002.
- P. Craiger, Ubiquitous Security? Sixth Annual INFOTEC Conference, April, 2002.
- S. Whalen and P. Craiger. Attacking and Defending Wireless Networks, Sixth Annual INFOTEC Conference, April, 2002.
- P. Craiger and R. Weiss. Supporting Telework: Applications of Distance-Based Training In M. Covert (Chair), The Future Organization: Telework, Intelligent Agents and Nomadic Computing Presented at the 14th Annual Conference of the Society for Industrial and Organizational Psychology, April, 1999.

- P. Craiger, A. Stoyen, M. Bishop, J. Shroder and H. Sharif. Grand Challenge Computing Problems in Environmental Monitoring: UNO's Geomatics Program, Presentation for the American Association for the Advancement of Science, Omaha, NE, 1999.
- M. Bishop, P. Craiger, J. Shroder and A. Stoyen. Web-based software for the Global Land-Ice Measurements from Space 1st International Conference on Global Land-Ice Measurements from Space, Zurich, Switzerland, 1999.
- M. Bishop, P. Craiger, J. Shroder and A. Stoyen. UNO/CMIT Geomatics Program, 1st International Conference on Global Land-Ice Measurements from Space, Zurich, Switzerland, 1999.
- M. Hawkins and P. Craiger, Differential effects of computer-based instruction, In P. Craiger (Chair), Human-Computer Communication Systems: Research and Application accepted for the 14th Annual Conference of the Society for Industrial and Organizational Psychology, Atlanta, GA, 1999.
- M. Coover, L. Elliot, L. Foster and P. Craiger. Measurement in synthetic task environments for teams: A methodological typology Eighth International Conference on Human-Computer Interaction Munich, Germany, 1999.
- J. Shroder, M. Bishop, M. Olsenholler and P. Craiger, Geomorphology education and the World Wide Web. 30th Biennial Conference on Geomorphology, Binghamton, New York, 1999.
- P. Craiger, J. McGourty, M. Hawkins and K. Ury. Human-Computer Communication Systems: Research and Application Symposium for the 14th Annual Conference of the Society for Industrial and Organizational Psychology, 1999.
- P. Craiger, R. Weiss and A. Butler. Marital status and gender differences in a model of work-family conflict. 13th Annual Conference of the Society for Industrial and Organizational Psychology, Dallas, TX, 1998.
- R. Weiss, J. de Groot, and P. Craiger. Presenting the Programmable Task Battery for research into automation bias/automation induced complacency. Annual Meeting of the Human Factors and Ergonomics Society, Chicago, IL, 1998.
- M. Coover, P. Craiger and D. Dorsey, Integrating fit-indices for structural equations modeling. 13th Annual Conference of the Society for Industrial and Organizational Psychology, Dallas, TX, 1998.
- P. Craiger, M. Coover, J. Beaubien and D. Banks. The Internet as A Research Tool: Challenges and Opportunities Symposium. 13th annual Conference of the Society for Industrial and Organizational Psychology, Dallas, TX, 1998.
- M. Coover, P. Craiger and D. Riddle, New statistical tools for modeling, analysis and evaluation Symposium. 12th Annual Conference of the Society for Industrial and Organizational Psychology, St Louis, MO, 1997.
- P. Craiger, D. Goodman, R. Weiss and J. DeGroot, Mental models and pilot performance A cognitive science approach. 1997 Nebraska Academy of Sciences Meeting, Lincoln, NE, 1997.
- P. Craiger, J. Weiss, A. Butler, D. Goodman, and J. Dutcher, Navy quality of life: Validation of latent variable models for rank and station subgroups. Eleventh Annual Conference of the Society for Industrial and Organizational Psychology, 1996.
- G. Wilcove, P. Craiger and J. Dutcher, Quality of life in the Navy. 15th Biennial Applied Behavioral Sciences Symposium, 1995.

- V. Collins, D. Koch, R. Reiter-Palmon and P. Craiger, Flexibility as a predictor of leadership activity. Annual Conference of the Midwest Psychological Association, 1995.
- P. Craiger, R. Weiss, A. Butler, D. Goodman and J. Dutcher, Navy quality of life: Validation of latent variable models. 11th Annual Conference of the Society for Industrial and Organizational Psychology, 1995.
- M. Coovert, P. Craiger and M. Teachout, Application of a neuro-fuzzy system to model the relationship between job experience and performance. Annual Conference of the Society for Multivariate Experimental Psychology, 1995.
- P. Craiger, M. Coovert and M. Teachout, Fuzzy neural models in industrial psychology research In R. Yager and L. Zadeh (Chairs), Neural-Fuzzy Systems I Symposium conducted at the 11th Annual Meeting of the World Congress on Neural Networks, 1995.
- P. Craiger, A heuristic procedure for mapping worker attributes to tasks In P. Craiger (Chair), Innovative applications of computers in industrial/organizational psychology research. 102nd Annual Meeting of the American Psychological Association, Los Angeles, CA, 1994.
- P. Craiger, J. Houston, J. Dutcher, C. Heller and D. Glaser, Gender differences in ship- and shore-based quality of life for Navy personnel. 102nd Annual Meeting of the American Psychological Association, Los Angeles, CA, 1994.
- J. Dutcher and P. Craiger, Artificial intelligence in classification problems In P. Craiger (Chair), Innovative applications of computers in industrial/organizational psychology research, Symposium conducted at the 102nd Annual Meeting of the Psychological Association, Los Angeles, CA, 1994.
- J. Dutcher and P. Craiger, Human resources management: Organizations in transition, In P. Craiger (Chair), Managing Change in the 21st Century Organization Paper accepted for the 102nd Annual Meeting of the American Psychological Association, Los Angeles, CA, 1994.
- J. Houston and P. Craiger, Cultural diversity in the workplace: An integrated model, In P. Craiger (Chair), Managing Change in the 21st Century Organization. 102nd Annual Meeting of the American Psychological Association, Los Angeles, CA, 1994.
- E. Kerce and P. Craiger, Quality of life: An omnibus model In P. Craiger (Chair), Managing Change in the 21st Century Organization Paper session presented at the 102nd Annual Meeting of the American Psychological Association, Los Angeles, CA, 1994.
- P. Craiger and M. Coovert, Modeling dynamic social and psychological processes with fuzzy cognitive maps. IEEE International Conference on Fuzzy Systems, Orlando, FL, 1994.
- P. Craiger and M. Coovert, Discovering causal model implications with fuzzy cognitive maps: Help for the behavioral scientist, World Congress on Neural Networks, San Diego, CA, 1994.
- P. Craiger, Fuzzy cognitive maps and causal modeling. 9th Annual Conference of the Society for Industrial and Organizational Psychology, Nashville, TN, 1994.
- P. Craiger and J. Houston. A causal model of Navy quality of life. 1st Academy of Management Research Methods Division Conference on Causal Modeling, Purdue University, West Lafayette, IN, 1994.
- J. Houston and P. Craiger, A causal model of fairness in the workplace. 1st Academy of Management Research Methods Division Conference on Causal Modeling, Purdue University, West Lafayette, IN, 1994.
- P. Craiger and M. Coovert, A fuzzy system for mapping worker attributes to tasks. 26th Annual Conference of the Society for Computers in Psychology, Washington, DC, 1993.

Virtual Digital Evidence Laboratory

- P. Craiger, M. Coovert and M. Teachout, A comparison of additive versus direct product solutions for multimethod-multirater job performance data In C Smith (Chair), The psychology of method variance Symposium conducted at the 8th Annual Conference of the Society for Industrial and Organizational Psychology, San Francisco, CA, 1993.
- P. Craiger and M. Coovert, Modeling team performance: Objects and streams Paper presented at 100th Annual Meeting of the American Psychological Association, Washington, DC , 1992.
- M. Coovert, P. Craiger and M. Teachout, A comparison of additive versus multiplicative models for multitrait-multimethod data . 7th Annual Conference of the Society for Industrial and Organizational Psychology, Montreal, Quebec, 1992.
- L. Penner and P. Craiger, The "altruistic personality" . 99th Annual Meeting of the American Psychological Association, San Francisco, CA, 1991.
- P. Craiger and M. Coovert, The relationship between job experience and ratings of performance In M Teachout (Chair), Understanding the work experience construct in personnel research and practice Symposium conducted at the 6th Annual Conference of the Society for Industrial and Organizational Psychology, St Louis, MO, 1991.
- M. Coovert and P. Craiger, Determining the dimensionality of work experience and the prediction of job performance In M Teachout (Chair), Understanding the work experience construct in personnel research and practice Symposium conducted at the 6th Annual Conference of the Society for Industrial and Organizational Psychology, St Louis, MO, 1991.
- P. Craiger and L. Penner, The willingness to help AIDS victims: An experimental investigation . 37th Annual Meeting of the Southeastern Psychological Association, New Orleans, LA, 1991.

PROFESSIONAL NONREFEREED ARTICLES

- P. Craiger and B. Burnham, Computer security. *The Industrial and Organizational Psychologist*, 23, 155-168, 2001.
- P. Craiger, Traveling in cyberspace: Psychology of software design: Usability evaluation *The Industrial and Organizational Psychologist*, 21, 134-145, 2000.
- P. Craiger, Traveling in cyberspace: Psychology of software design, Part 1 *The Industrial and Organizational Psychologist*, 21, 113-122, 1999.
- P. Craiger and R. Weiss, Traveling in cyberspace: Speech recognition systems *The Industrial and Organizational Psychologist* 36, 79-86, 1999.
- P. Craiger and R. Weiss, Traveling in cyberspace: Video-mediated communications *The Industrial and Organizational Psychologist*, 35, 83-92, 1998.
- P. Craiger and R. Weiss, Traveling in cyberspace, the final frontier: An interview with Donald Norman *The Industrial and Organizational Psychologist*, 35, pp 21-29, 1998.
- P. Craiger, Weiss, RJ (January, 1998) Traveling in cyberspace: The evolution of SIOP on the web *The Industrial and Organizational Psychologist*, 35, 13-15
- P. Craiger and R. Weiss (October, 1997) Traveling in Cyberspace: Web-based instruction *The Industrial and Organizational Psychologist*, 35, 11-17
- P. Craiger (January, 1997) Technology, organizations and work in the 20th century *The Industrial and Organizational Psychologist*, 36, 89-97

Virtual Digital Evidence Laboratory

- R. Weiss and P. Craiger (April, 1997) Traveling in cyberspace: Computer-based training The Industrial and Organizational Psychologist 34, 70-75
- P. Craiger (October, 1996) Traveling in cyberspace: Computer mediated work The Industrial and Organizational Psychologist, 34, 14-18
- P. Craiger and R. Weiss (July, 1996) Traveling in cyberspace: More Internet tools and services and Intranets The Industrial and Organizational Psychologist, 34, 16-23 .
- P. Craiger and R. Weiss (April, 1996) Traveling in cyberspace: Internet tools and services The Industrial and Organizational Psychologist, 33, 13-17 .
- P. Craiger (January, 1996) Traveling in cyberspace: Getting connected to the Internet and the World Wide Web The Industrial and Organizational Psychologist pp 12-19 .
- P. Craiger and R. Weiss (October, 1995) Traveling in cyberspace: The World Wide Web The Industrial and Organizational Psychologist, 33, pp 16-20.
- P. Craiger (July, 1995) Traveling in cyberspace: TIP on the World Wide Web The Industrial and Organizational Psychologist, 33, p 11.

TECHNICAL REPORTS

- P. Craiger, Structural Equation Models of Marine Corp Quality of Life US Army Scientific Services Program, Contract DAAH04-96-C-0086, 1999.
- P. Craiger and R. Weiss, A comparison of mathematical models of the Navy Quality of Life Data US Army Scientific Services Program, DAL03-91-C-0034, TCN96217, 1997.
- P. Craiger and M. Coovert, A model of the relationship between job experience and job sample test performance: Application of a neuro-fuzzy system (Report no F4162294P3620), Armstrong Laboratory, Brooks AFB, TX, 1994.
- P. Craiger, R. Weiss, B. Butler and D. Goodman, Navy Quality of Life Predictive Model Project: Results of the second administration San Diego, CA: Navy Personnel Research and Development Center, 1995.
- Dutcher, JS and P. Craiger, Navy Quality of Life Predictive Model Project: Results of the first administration San Diego, CA: Navy Personnel Research and Development Center, 1994.
- M. Coovert and P. Craiger, Data analysis summary: Job experience assessment (Report no 10/DI-A-5023) San Antonio, TX: Air Force Human Resources Laboratory, 1990.
- M. Coovert and P. Craiger, A graphical representation of the AAWC, IDS, EWS and TIC positions with the VISTA programming tool (Contract DAAL03-86-D-0001) Orlando, FL: Naval Training Systems Center, 1992.
- M. Coovert, J. Ford, P. Craiger, D. Sego, M. Quinones and J. Speer, Final report on research and development: Job experience and assessment (Report no 15/DI-S-30591) San Antonio, TX: Air Force Human Resources Laboratory, 1990.
- M. Coovert, G. Campbell, P. Craiger, J. Cannon-Bowers and E. Salas, The conceptual application of Petri nets to the modeling of team performance Orlando, FL: Naval Training Systems Center, 1992.
- C. Nelson, A. Kurtz, E. Gulitz, G. Hacker, M. Lee, P. Craiger, S. Roberts and A. Reno, The accuracy of behavioral surveys in predicting evacuation behavior: The Hurricane Elena study Tallahassee, FL: Florida Division of Emergency Management, 1988.

Virtual Digital Evidence Laboratory

HONORS AND AWARDS

- 2009 Teaching Incentive Program Award (University of Central Florida)
- 2006 I was recognized by the Orange County Sheriff's Office with a Sheriff's Citation for my work with our UCF Digital Forensics Undergraduate and Graduate Certificate programs.
- 2006 I was recognized by the Department of Homeland Security - United States Secret Service with a certificate of Appreciation for a talk I performed for their Quarterly meeting held on June 20, 2006.

NEW COURSES DEVELOPED

- CIS 6395 Incident Response Technologies (University of Central Florida)
- CIS 6386: Operating System and File System Forensics (University of Central Florida)
- CET 4886: Information Security Processes (University of Central Florida)
- CET 4885: Digital Investigative Technologies (University of Central Florida)
- CET 3592: Linux Administration and Applications (University of Central Florida)
- CET 4932: Current Topics in Computer Security (University of Central Florida)
- CIST 4350: Technical Systems Administration (University of Nebraska @ Omaha)
- CSCI 4380: Computer and Network Forensics (University of Nebraska @ Omaha)
- CIST 4370: Security Administration (University of Nebraska @ Omaha)
- CSCI 2980: Advanced Java Programming (University of Nebraska @ Omaha)
- CSCI 2830: Java Programming (University of Nebraska @ Omaha)
- CSCI 4360/8366: Computer Security (University of Nebraska @ Omaha)
- CSCI 4260/8266: User Interface Design with Java (University of Nebraska @ Omaha)
- CSCI 4250/8256: Human-Computer Interaction (University of Nebraska @ Omaha)

NEW PROGRAMS DEVELOPED

- Master's of Science in Digital Forensics, 2005-07, University of Central Florida
- Information Systems Technology Information Security Concentration, 2004-05, University of Central Florida
- Information System Technology Concentration, College of Information Science and Technology, University of Nebraska @ Omaha, 2000-2002
- Information Security Program, University of Nebraska @ Omaha, 2001-2004.

STUDENT ADVISING

- Adviser, Professional Track of the Master's of Science in Digital Forensics
- Adviser, UCF SCUBA Club
- Adviers, UCF Linux Forensics Club

Virtual Digital Evidence Laboratory

PREVIOUS EMPLOYMENT

- 2000-2004 Associate Professor of Computer Science
College of Information Science and Technology
The Peter Kiewit Institute
University of Nebraska @ Omaha
Omaha, NE 68182
- 1996-1999 Assistant Professor of Computer Science
College of Information Science and Technology
The Peter Kiewit Institute
University of Nebraska @ Omaha
Omaha, NE 68182
- 1994-1996 Assistant Professor, Center for Management of Information Technology and Department
of Psychology
University of Nebraska @ Omaha
Omaha, NE 68182
- 1999-2001 Senior Technical Scientist, 21st Century Systems
Responsibilities include human-factors contributions to distributed agent-enabled war fighting soft- ware; writing proposals for Department of Defense RFPs; interfacing with government agencies (Department of the Navy, DARPA, others)

PROFESSIONAL CERTIFICATIONS

- Certified Information System Security Professional (CISSP)
- SANS GIAC Certified Computer Forensic Analyst (GCFA)
- American Society of Crime Labs/Laboratory Accreditation Board (ASCLD/LAB) Certified Inspector
- SANS GIAC Certified Security Essentials (GSEC)
- EC-Council Certified Ethical Hacker (CEH)

PROFESSIONAL AFFILIATIONS

- American Academy of Forensic Scientists (Member)
- Digital Forensics Working Group
- International Federation of Information Professionals 9.11 Digital Forensics Group
- Association for Computing Machinery (ACM)
- Anti-Phishing Working Group

Virtual Digital Evidence Laboratory

AWARDS AND PROFESSIONAL SERVICE

- 2007-2009 Reviewer Journal of Forensic Sciences
- 2007-2009 Coordinator for the Professional Track of the Master of Science in Digital Forensics.
- 2005-07 One of the primary authors of the Masters of Science in Digital Forensics proposal.
- 2006-2007 Planning Panel, Technical Working Group on Training and Education in Digital Evidence.
- 2007 Co-chair, International Federation of Information Processing Working Group 11.9 Conference
- 2008-09 Reviewer 52ND and 53rd American Academy of Forensic Science Annual Conference
- 2007 Reviewer National Institute of Justice Cybercrime Grant Proposals
- 2006 Reviewer IFIP WG 11.9 2007 Conference
- 2006 Reviewer Course Technology (2 textbooks)
- 2005 Reviewer, Handbook of Information Security
- 2005 Reviewer, Course Technology (Textbook)
- 2005 Reviewer IFIP WG 11.9 2006 Conference
- 2005 Reviewer, International Journal of Human-Computer Studies
- 2004 NASA Faculty Research Associate
- 2004 Reviewer, Handbook of Information Security
- 2004 Reviewer IFIP WG 11.9 2005 Conference
- 2003 Reviewer, The Internet Encyclopedia
- 2002-03 Reviewer, Journal of Information Sciences
- 2003 NASA Faculty Research Associate
- 2002 NASA Faculty Research Associate
- 2002 Course Technology Inc (Information Security publications)
- 2001 Invited Reviewer, National Science Foundation Information Technology Research (Computer-Human Interaction)
- 2001 NASA Faculty Research Associate
- 2000 NASA Faculty Research Associate
- 1999 NASA Faculty Research Associate
- 1999 Invited reviewer, National Defense Engineering and Science Fellowship Program, Cognitive and Behavioral Division
- 1999 Reviewer, Decision Support Systems
- 1997-00 UNO Faculty Senate
- 1997-98 Reviewer, Personnel Psychology

Virtual Digital Evidence Laboratory

- 1996-98 Reviewer, Journal of Applied Psychology
- 1996 Voted Graduate Faculty Member
- 1996 Reviewer for West Publishing Co
- 1995 Reviewer for the IEEE Transactions on Systems, Man, and Cybernetics
- 1995-01 Columnist for TIP, the official newsletter of the Society for Industrial and Organizational Psychology

PERSONAL CERTIFICATIONS

- Technical Dive Instructor - National Association of Underwater Instructors (2009) Certified to teach:
 - Cave 1
 - Helitrox (Trimix to 150')
 - Decompression Procedures
 - Advanced Nitrox (40-100% Nitrox)
- Instructor - National Association of Underwater Instructors (NAUI) 2008
- Sidemount diver - National Speleological Society-Cave Diving Section (NSS-CDS), 2008
- Dive Propulsion Vehicle - National Association of Cave Divers (NACD), 2008
- Dive Master - National Association of Underwater Instructors (NAUI), 2008
- Advanced Trimix - Technical Diving International (TDI), 2008 • Advanced Nitrox - Technical Diving International (TDI), 2007
- Decompression Procedures - Technical Diving International (TDI), 2007
- Cave Diver - National Speleological Society-Cave Diving Section (NSS-CDS), 2007
- Cave Diver - National Association of Cave Divers (NACD), 2007
 - Apprentice Cave (NACD)
 - Introduction to Cave (NACD)

- Cavern Diver - Professional Association of Diving Instructors (PADI), 2006
- Rescue Diver - Professional Association of Diving Instructors (PADI), 2006
- Advanced Open Water Scuba - National Association of Underwater Instructors (NAUI), 2005
- Open Water Scuba - Professional Association of Diving Instructors (PADI), 2005

Procedures Used for Creating Test Images

Image One: Windows XP/Dell

Hardware:

Dell OPTiplex GX 620
Intel Pentium D 2.80 GHz processor
OCZ 30GB solid state hard drive
3574 MB of RAM
DVD R/W drive
floppy drive

Software:

Information about the Operating System:

Windows XP
User name: Bob Dobbs
Password: subgenius

Procedure:

Process of setting up the case:

Windows was updated
A Sandisk Cruzer mini (512MB) thumb drive was plugged in
The following driver was successfully installed
Ethernet Card - R97582.exe
Chipset - R132539.exe
Audio - R97809.exe
Video - R98241.exe

The following websites were visited:

Google.com - the following was searched for

- anarchist cookbook
- galvanized pipe
- pipe fittings
- pipe
- pipe bombs
- body armor
- diesel fuel and fertilizer

Virtual Digital Evidence Laboratory

The following bookmarks were created [with their general URL]:

- how to make a pipe bomb [http://www.bombshock.com/homemade_bombs/]
- ANFO, diesel and fertilizer [<http://en.wikipedia.org/wiki/ANFO>]
- body armor [<http://www.abovetopsecret.com/forum/thread421155/pg1>]
- body armor [<http://www.xdtalk.com/forums/xdtalk-chatter-box/93472-home-made-bullet-proof-vest-body-armor.html>]
- body armor [http://www.globaldefender.net/new_page_1.htm]
- body armor [<http://www.bodyarmor.com/>]

Folder created on Desktop - Project

Encrypted

- Word Pad document - instructions to create pipe bomb
- Word Pad document - instructions to create pipe bomb
- JPEG image - body armor
- GIF image - body armor

Word Pad document created of Favorites URLs; saved to Project folder, then copied to Desktop, encryption removed, and file deleted.

Image Two: Windows 7/Dell PC

Hardware:

Dell OPTiplex GX 620
Intel Pentium D 2.80 GHz processor
OCZ 30GB solid state hard drive
3574 MB of RAM
DVD R/W drive
floppy drive

Software:

Information about the OS:

Windows 7, RC 7100 (32-bit)

User: Mike

Password: cloverfeild

The clock was set for Eastern Time and set to auto adjust for daylight savings time

Process of setting up the case:

Windows was updated

Adobe flash player was installed

No drivers were installed

Procedure:

The following websites were visited:

Google.com - the following was searched for

- where to buy credit card skimmers
- how to make credit card skimmers
- how to make credit card cloner
- how to make credit card cloner -dvd
- where to buy credit card numbers
- sell cvv
- where to buy cvv
- where to buy social security numbers
- where to buy social security numbers -protection
- where to buy identities
- buy and sell identities
- check fraud
- check printing software

Ebay.com - the following was searched for

- credit card machine
- credit card swipe reader

Virtual Digital Evidence Laboratory

download.com - the following was searched for

- check printing
- check printing software

The following bookmarks were created [with their general URL]:

- cvv prices [www.talk-hyip.com]
- more cvv [www.backwire.com]
- cvv very cheap [www.caribbeanhotdeals.com]

The following software was installed:

- Check printing software 2000
- Password: smile

-PrimeCheck

- User: Mike
- Company: NA
- password: freemoney

Image Three: Linux OS/Dell PC

Hardware

Dell OPTiplex GX 620
Intel Pentium D 2.80 GHz processor
OCZ 30GB solid state hard drive
3574 MB of RAM
DVD R/W drive
floppy drive

Software:

Information about the Operating System:

Fedora 11
Machine name: fedoravdfl
Root password: mayberry
User name: Ernest T. Bass / ernie
User password: griffith

Procedure:

Process of setting up the case:

Fedora 11 was installed and all updates were downloaded and installed.

The following types of articles and sites were searched for using the Firefox browser.
Bookmarks were created for most of the search results.

From the Google start page:

- crystal methamphetamine
- meth
- Acacia
- psuedophedrine
- clandestine chemistry
- shake-n-bake meth
- RFID credit cards
- credit card number generators

Several pictures were downloaded from the same searched sites.

The pictures depict several forms of crystal meth.

A text file was created with directions for creating meth.

The file was deleted.

Virtual Digital Evidence Laboratory

A folder was created, titled 'Funding'.

A script/program for generating credit card numbers was saved to this folder.
The permissions were changed for the folder to 'owner' only.

Image Four: Mac OS X/MacBook Pro

Hardware:

MacBook Pro A1211
Intel 2.33 GHz Core 2 Duo processor
OCZ 30 GB solid state hard drive
2GB 667MHz DDR2 SDRAM
DVD R/W drive

Procedure:

Process of setting up the case:

OS X updated
Firefox downloaded and installed

The following websites were visited:

Google.com - the following were searched for

- hiding IP address
- hijacking IP address
- hacking tools and code
- hacking with a mac
- hacking using a mac
- server racks / rooms
- hacking windows network with a mac

The following bookmarks were created [with their general URL]

hide IP address [about.com]
anonymous proxy [youhide.com]
IP hijacking [wikipedia.com]
how to hijack IP [hacking-guides.blogspot.com]
hacking codes and tools [remote-exploit.org]
hacking windows with Mac [macshadows.com]
what is my IP [whatismyip.com]

Saved html page of server rack;

- page
- page files
All information was moved to trash

Created one image with internal camera

Picture was moved to trash.