FEASIBILITY STUDY REPORT

Violent Crime Digital Evidence Recovery (VCDER)

DOJ-059

State of California
Department of Justice

August 2008 v1.1

FEASIBILITY STUDY REPORT

Violent Crime Digital Evidence Recovery
DOJ-059

APPROVED BY:

KAREN SHERWOOD Date
Project Manager
Special Agent In Charge
Bureau of Investigation and Intelligence
Division of Law Enforcement

RANDY BRYANT Date
Assistant Chief
Bureau of Investigation and Intelligence
Division of Law Enforcement

CRAIG BEUHLER Date
Chief
Bureau of Investigation and Intelligence
Division of Law Enforcement

GEORGE ANDERSON Date
Director
Division of Law Enforcement

JOYCE WALTON Date
Acting Bureau Chief
Application Development Bureau
California Justice Information Services Division

FEASIBILITY STUDY REPORT

Violent Crime Digital Evidence Recovery
DOJ-059

SHERI HOFER Date
Bureau Chief
Departmental Services Bureau
Computer Operations Bureau
California Justice Information Services Division

RICK KEEFER Date
Acting Bureau Chief
Infrastructure Support Bureau
California Justice Information Services Division

TERRY BUCKLEY DATE
Data Processing Manager IV
California Justice Information Services Division

JOE DOMINIC DATE
Network Information Security Unit Project Manager
California Justice Information Services Division

DIANA YOUNG Date
Manager
Information Technology Project Office
California Justice Information Services Division

FEASIBILITY STUDY REPORT
Violent Crime Digital Evidence Recovery
DOJ-059

Version Control

VERSION NO.	DATE	ANALYST	DESCRIPTION	SECTION & SUBSECTION
1.0	8/28/2008	Sue Simon	ITPO Manager Approval	All
1.1	9/22/08	Sue Simon	Change wording from Wireless	4.1.2 and 4.1.3
			to Wired DSL and Cellular Digital	

FEASIBILITY STUDY REPORT

Violent Crime Digital Evidence Recovery
DOJ-059

TABLE OF CONTENTS

TABLE OF CONTENTS—contd.

1.0 - INFORMATION TECHNOLOGY PROJECT SUMMARY PACKAGE

SECTION A: EXECUTIVE SUMMARY

1.	Submittal Date	

		FSR	SPR	PSP Only	Other:
2.	Type of Document	X			
	Project Number	DOJ-059			

			Estimated Project Dates	
			Start	End
3.	Project Title	Violent Crime Digital Evidence Recovery		
	Project Acronym	VCDER	9/1/2008	12/30/2008
4.	Submitting Department	Department of Justice		
5.	Reporting Agency	Not Applicable		

6. Project Objectives

The business objective is to provide DOJ BII with the capability to recover digital evidence.

7.	Major Milestones	Est Complete Date
	FSR Approval	9/1/2008
	Hardware/software procurement	10/1/2008
	Workstation Implementation	12/31/2008
	PIER	8/31/2009
	Key Deliverables	
	Installed & Tested Forensic Workstations	12/31/2008

8. Proposed Solution

Acquire and install digital and video forensic workstations for use by specially trained investigators to collect, preserve, analyze, process, and examine digital and video evidence used by those involved in crimes and ensure its admissibility as evidence in court proceedings.

Project #	DOJ-059
Doc. Type	FSR

Executive Contacts								
	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-Mail
Agency Secretary	N/A							
Dept. Director	James	Humes	916	324-5435				James.Humes@doj.ca.gov
Budget Officer	Jennifer	Byington	916	445-8215				Jennifer.Byington@doj.ca.gov
CIO	Gary	Cooper	916	227-8155				Gary.Cooper@doj.ca.gov
Proj. Sponsor	Craig	Beuhler	916	319-8296				Craig.Beuhler@doj.ca.gov

Direct Contacts								
	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-Mail
Doc. Prepared by	Sue	Simon	916	227-3084		916	227-3100	Sue.Simon@doj.ca.gov
Primary contact	Sue	Simon	916	227-3084		916	227-3100	Sue.Simon@doj.ca.gov
Program contact	Karen	Sherwood	916	227-2849		916	227-1228	Karen.Sherwood@doj.ca.gov
Project Manager	Karen	Sherwood	916	227-2849		916	227-1228	Karen.Sherwood@doj.ca.gov

1.	What is the date of your current Operational Recovery Plan (ORP)?	Date	5/8/2008
2.	What is the date of your current Agency Information Management Strategy (AIMS)?	Date	10/31/2007
3.	For the proposed project, provide the page reference in your current AIMS and/or strategic business plan.	Doc.	
		Page #	

Project #	DOJ-059
Doc. Type	FSR

		Yes	No
4.	Is the project reportable to control agencies?		X
	If YES, CHECK all that apply:		
	a) The project involves a budget action.		
	b) A new system development or acquisition that is specifically required by legislative mandate or is subject to special legislative review as specified in budget control language or other legislation.		
	c) The estimated total development and acquisition cost exceeds the departmental cost threshold and the project does not meet the criteria of a desktop and mobile computing commodity expenditure (see SAM 4989 – 4989.3).		
	d) The project meets a condition previously imposed by Finance.		

Project #	DOJ-059
Doc. Type	FSR

Budget Augmentation Required?		
	No	X
	Yes	

If YES, indicate fiscal year(s) and associated amount:

FY 2008/09	FY 2009/10	FY 2010/11	FY 2011/12	FY 2012/13	FY 2013/14
$0	$0	$0	$0	$0	$0

PROJECT COSTS

	Fiscal Year	2008/09	2009/10	2010/11	2011/12	2012/13	2013/14	TOTAL
1.								
2.	One-time Cost	526,512	0	0	0	0	0	$526,512
3.	Continuing Costs	0	0	0	0	0	0	$0
4.	TOTAL PROJECT BUDGET	526,512	0	0	0	0	0	$526,512

SOURCES OF FUNDING

5.	General Fund	0	0	0	0	0	0	$0
6.	Redirection (existing)	95,391	0	0	0	0	0	$95,391
7.	Reimbursements	0	0	0	0	0	0	$0
8.	Federal Funds	0	0	0	0	0	0	$0
9.	Special Funds	0	0	0	0	0	0	$0
10.	Grant Funds	431,121	0	0	0	0	0	$431,121
11.	Other Funds	0	0	0	0	0	0	$0
12.	PROJECT BUDGET	526,512	0	0	0	0	0	$526,512

PROJECT FINANCIAL BENEFITS

13.	Cost Savings/Avoidances	$0	$0	$0	$0	$0	$0	$0
14.	Revenue Increase	$0	$0	$0	$0	$0	$0	$0

Note: The totals in Item 4 and Item 12 must have the same cost estimate.

Project #	DOJ-059
Doc. Type	FSR

Vendor Cost for FSR Development (if applicable)	$0
Vendor Name	

VENDOR PROJECT BUDGET

		2008/09	2009/10	2010/11	2011/12	2012/13	2013/14	TOTAL
1.	Fiscal Year							
2.	Primary Vendor Budget	44,876	0	0	0	0	0	$44,876
3.	Independent Oversight Budget	0	0	0	0	0	0	$0
4.	IV&V Budget	0	0	0	0	0	0	$0
5.	Other Budget	354,267	0	0	0	0	0	$354,267
6.	Total Vendor Budget	$399,143	0	0	0	0	0	$399,143

----------(Applies to SPR only)----------

PRIMARY VENDOR HISTORY SPECIFIC TO THIS PROJECT

7.	Primary Vendor	
8.	Contract Start Date	
9.	Contract End Date (projected)	
10.	Amount	

PRIMARY VENDOR CONTACTS

	Vendor	First Name	Last Name	Area Code	Phone #	Ext.	Area Code	Fax #	E-mail
11.									
12.									
13.									

Project #	DOJ-059
Doc. Type	FSR

RISK ASSESSMENT

	YES	NO
Has a Risk Management Plan been developed for this project?		X

General Comment(s)

2.0 BUSINESS CASE

2.0 BUSINESS CASE

2.1 Business Program Background

As chief law officer of California, the Attorney General (AG) ensures the uniform and adequate enforcement of state and federal laws. The AG carries out these constitutional responsibilities through programs at the California Department of Justice (DOJ).

Division of Law Enforcement (DLE)

DLE's mission is to provide services in forensic sciences, forensic education, narcotics investigations, criminal investigations, intelligence, and training. The DLE endeavors to be on the cutting edge of the delivery of these services.

The DLE provides a wide range of support services to local, state, and federal law enforcement agencies in their fight against crime. DLE is organized into the following areas:

- Bureau of Forensic Services
- Office of the Director, Executive Unit
- Western States Information Network
- Bureau of Firearms
- Bureau of Gambling Control
- Bureau of Narcotic Enforcement
- **Bureau of Investigation and Intelligence**

Bureau of Narcotic Enforcement (BNE)

The mission of the BNE is to provide leadership, coordination, and support to law enforcement agencies in combating drugs, illegal weapons, and violent crime in California.

Bureau of Investigation and Intelligence (BII)

The BII's mission is to provide expert levels of investigative and criminal intelligence services statewide to local law enforcement agencies through their innovative programs, technological support, and dedicated, professional personnel.

Digital Evidence

With the increase in the use of technology by criminals, more and more evidence is stored electronically as digital evidence. Digital information is included in most aspects of everyday life; it is prevalent in our communication, banking and financial institutions, entertainment and transportation. We rely on the Internet, smart phones, cell phones, and personal data assistants (PDAs). We use digital cameras and video equipment. Our vehicles today are equipped with on-board computers and GPS directional devices. We also utilize laptops, both hardwire and wireless, in our homes and away. Those persons responsible for violent crime use these devices as well, and each of these devices has the capability in some form to communicate and store memory. Digital systems can contain evidence that a crime has been committed, as well as contain evidence identifying the suspect and his crimes.

Information vital to solving crime and obtaining criminal convictions is a direct result of the ability to examine and analyze computer systems and digital information from all types of digital computing devices.

Digital evidence must be collected, processed and handled in such a way as to maintain the integrity of the digital information in the same state as it was recovered. Simply turning a digital system off or on may change the evidence, and warrant it unusable for investigation or prosecution. Knowing with whom the victim/suspect has communicated, where the victim/suspect traveled or planned to travel, in addition to accessing other data stored on any digital device, may be the critical evidence needed to bring a criminal to justice.

If a crime scene or other investigative effort reveals the presence of digital devices, investigators may attempt to acquire the digital information from the digital media themselves, seriously compromising the chain of evidence. The investigators may collect the evidence, book the evidence (providing it can be stored), and await a determination of which resource (agency) may be available to review the evidence, seriously delaying identification and follow up on investigative leads. Investigators may request the assistance of a high-tech task force, but if they are not a participating agency of the task force, or if the crime element does not fit specifically into the mission of the high-tech task force, these investigators will not get the assistance they need to acquire digital information immediately.

Investigators have the option to submit evidence to the FBI for analysis. However, the backlog prevents rapid response to the evidence. The delays may permit the perpetrator to continue committing crimes, or escape apprehension. Extreme delays or inability of the FBI to process the evidence may also contribute to unsuccessful prosecutions. In many instances, the investigators do not pursue digital forensic support simply because it is too difficult to obtain.

2.2 Business Problem or Opportunity

The DOJ BII lacks the equipment to analyze or collect digital evidence.

- Forensic analysis computers must meet or exceed the technical specifications of the devices being investigated. These devices include personal computers, digital devices such as cell phones, Personal Digital Assistants (PDAs), digital cameras, global positioning systems (GPS), gaming devices, music/video devices, and recorders, etc. With BII offices statewide, the need for forensic workstations and software is crucial to support gang related violent crime investigations.

- The rapid analysis of digital evidence provides the opportunity for investigators to act quickly to identify specific criminal acts, locate and apprehend suspects, and prevent additional crimes.

BII has received federal grant funding from the Edward Byrne Foundation to cover the cost of this specialized equipment and training. Because BII is a statewide law enforcement agency respected for its ability to provide high quality investigative resources, it is the best agency to provide this type of statewide resource to local agencies.

2.3 Business Objectives

The business objective is to provide DOJ BII with the capability to recover digital evidence.

2.4 Business Functional Requirements

To obtain the business objective, the following business functional requirements must be met:

1. The solution must provide equipment for obtaining digital evidence from personal computers, digital cell phones, personal digital assistants, global positioning systems, and other digital media.
2. The solution must provide training for selected agents in the latest digital forensic techniques to collect, preserve, analyze and examine digital and video evidence taken from electronic sources of all types and to ensure its admissibility in legal proceedings.

3.0 BASELINE ANALYSIS

3.0 BASELINE ANALYSIS

3.1 Current Method

While the DOJ BII provides many services to local jurisdictions, the BII has no capability to do so in digital evidence cases.

Some local law enforcement agencies have formed high-tech task force teams to process digital evidence. There are currently five of these teams in California. These teams do not routinely provide crime scene assistance, and due to heavy workload are unable to complete data extraction analysis in a timely manner.

Local jurisdictions that need to process digital evidence must utilize their own local digital evidence units, arrange with a team of other agencies, or arrange with the Federal Bureau of Investigation for digital evidence extraction. In cases where storage media is damaged, agencies utilize private vendors to recover data from the damaged media. Data recovery and extraction from damaged media is extremely expensive and costs can amount to thousands of dollars to recover data from a single hard drive.

In the event that DOJ agents recover digital evidence pursuant to an investigation, BII is currently unable to provide any data extraction expertise to those agents. The investigating agents must arrange with a local digital evidence team, such as the Sacramento Regional Task Force, to have the data extracted.

3.2 Technical Environment

The DOJ currently has no digital evidence system.

4.0 PROPOSED SOLUTION

4.0 PROPOSED SOLUTION

4.1 Solution Description

To meet the business objective, the solution will provide digital and video forensic workstations for use by investigators to collect, preserve, analyze, process, and examine digital and video evidence used by those involved in crimes

These investigators must be specially trained in digital crime investigations and the analysis and acquisition of digital evidence in field examinations. Using specialized equipment, the investigators will provide a rapid, coordinated, comprehensive recovery to gang related crimes wherein digital evidence may be an element. In addition to the specialized equipment and tools, the investigators knowledge and expertise will be established and sustained by continual education and training specific to the field of digital evidence analysis.

4.1.1 Hardware

The following hardware is required. This equipment is not to be confused with the PCs included as standard complement. Descriptions of the products are included in Attachment A.

Desktop Workstation
Portable Workstation
Shuttle Workstation
Cell Phone Data Extractor
Secure View Kit for Forensics – Data Pilot
Write Blocker Ultra Kit – Includes USB Write Blocker and Forensic Card Reader
Hard Drive Imager – Digital Intelligence Hardcopy
Hard Drive Imager – Logicube Forensic Talon
Shadow Drive
Flash Drive (2)
Hard Disk Drives – Maxtor SATA 250 GB
Hard Disk Drives – Maxtor IDE ATA 250 GB
Laptop Hard Drives – Toshiba 100 GB IDE ATA
Laptop Hard Drives – Toshiba 100 GB SATA

CD/RW Discs
DVD/RW Discs
Terabyte Network Storage
KVM Switch

4.1.2 Software

The workstations will be preconfigured with the following suggested or comparable software products. Descriptions of the products are included in Attachment A.
Guidance Software – Encase
AccessData – Ultimate Forensic Tool Kit
Technologies Pathways – ProDiscover Incident Response
Digital Detective – Net analysis
Logicube – Celldek licensing
Wired DSL for non-mobile systems
Cellular digital wireless service for portable systems
Virus Software
Image Software
Office Suite
CD/DVD Diagnostic (recovery)
VM Ware

4.1.3 Technical Platform

The workstations must be compatible for conducting computer forensic exams, otherwise known as recovery of digital evidence. The computers will have a Windows XP Pro operating system, computer forensic software, and high speed Internet access required to download updates to the operating system and virus protection software. The solution will consist of remote workstations that will not be connected to the DOJ network.

All equipment and software purchased must conform to existing Hawkins Data Center (HDC) security policies, standards and guidelines. HDC staff will be contacted by BII staff to assist in ensuring that the systems will be in compliance with these standards.

4.1.4 Development Approach

Software will be Commercial Off-the-shelf (COTS). No system development or modification will be needed.

4.1.5 Integration Issues

No significant integration issues have been identified. The solution will be standalone.

4.1.6 Procurement Approach

Procurement activities will comply with the intent of any existing Departmental of General Services (DGS) technology acquisition policies.

4.1.7 Technical Interfaces

The solution will be standalone and isolated from other DOJ systems. However, the system will need to interface with a variety of equipment and data formats for the purpose of data and evidence extraction. Commercial off-the-shelf equipment and software will be acquired to allow the workstations to access various data devices.

4.1.8 Testing Plan

No significant testing issues have been identified.

4.1.9 Resource Requirements

The project coordinator will perform tasks related to setting up equipment and procedures and establishing techniques for data extraction and analysis.

4.1.10 Training Plan

The program Special Agents will require specialized training and certifications to properly operate the forensic equipment and conduct the investigations.

4.1.11 On-going Maintenance

The resource efforts to support and maintain the software are minimal (less than .1 PY), and will the responsibility of the program staff (Special Agents).

4.1.12 Information Security

The DOJ Information Security Office monitors departmental compliance with information security requirements. These requirements are included in the Information Practices Act (Civil Code, section 1798 et seq.); the Public Records Act (Government Code, section 6250 et seq.); criminal identification provisions in the California Penal Code (section 11100 et seq.); the State Administrative Manual (Section 4840 et seq.); and the Government Code(section 11771 et seq.)

The Hawkins Data Center (HDC) is the custodian of DOJ automated systems, and oversees system security and disaster recovery for both mainframe and Cal-DOJ network. The HDC has developed plans to prevent unauthorized system intrusion, corruption, or loss of electronic information. The HDC is in compliance with the Security and Risk Management policy outlined in section 4840, et seq., of the State Administrative Manual.

Due to the unknown content and nature of the forensic investigations, the workstations will not be connected to the DOJ network.

4.1.13 Confidentiality

The solution will not interact with any other DOJ systems.

4.1.14 Impact on End Users

The proposed solution will allow only specially trained agents to analyze digital media for evidentiary purposes.

4.1.15 Impact on Existing System

There is no existing system.

4.1.16 Consistency With Overall Strategies

The solution is consistent with the following DOJ strategies identified in the Agency Information Management Strategy (AIMS):

- Defend public civil law rights
- Promote cost-effective law enforcement
- Promote the uniformity of enforcement of state law

4.1.17 Impact on Current Infrastructure

The proposed solution will be remote standalone equipment and will not impact DOJ's infrastructure.

4.1.18 Impact on Data Center(s)

The HDC is an entity within the DOJ and is one of the State's consolidated data centers and is assigned to serve the DOJ.[1] The proposed solution will run on isolated stand-alone equipment. The HDC has given approval for the proposed solution to be housed outside of the data center facilities.

4.1.19 Data Center Consolidation

The proposed solution does not constitute a system subject to this policy. The proposed solution involves acquisition of standalone hardware and specialized commercial-off-the-shelf software to facilitate forensic investigations.

4.1.20 Backup and Operational Recovery

Because the proposed solution will be standalone from HDC systems, it will fall outside of HDC backup and operational recovery procedures. The workstations will have either digital media or electronic download capabilities to recover or rebuild if necessary. The forensic data is saved to a hard drive and/or a CD consistent with evidence handling procedures.

[1] State Administrative Manual (SAM) Section 4982.1.

4.1.21 Public Access

The proposed solution does not provide public access to State databases by private sector organizations or individuals.

4.1.22 Costs and Benefits

Costs are itemized in Section 7.0 (Economic Analysis Worksheets).

The benefits to be achieved through these efforts include:

- Local law enforcement will benefit from the capability to analyze forensic evidence statewide
- Faster apprehension of suspects and prevention of the commission of further acts of violence
- Stronger cases for prosecution and potential reduction of prosecution costs through more compelling evidence
- Faster discovery of digital data
- Faster identification and analysis of digital evidence at the crime scene
- Digital evidence will be interpreted quicker and provide information to reduce risk to victims, and improve public safety.

4.1.23 Sources of Funding

The DOJ has received federal Byrne grant funding and will use existing spending authority.

4.2 Rationale for Selection

The solution meets the objectives that will provide BII with equipment to meet the DOJ0's investigative needs.

4.3 Other Alternatives Considered

The following alternatives were considered, but not selected:

Alternative 1. Do nothing. Without sufficient equipment and dedicated/trained staff, DOJ has nowhere to turn for the timely analysis of digital evidence. FBI resources are backlogged for months. The lack of coordinated multi-jurisdictional effort against violent criminals at the state level exposes more citizens to greater dangers.

5.0 PROJECT MANAGEMENT PLAN

5.0 PROJECT MANAGEMENT PLAN

5.1 Project Manager Qualifications

Special Agent in Charge (SAC) Karen Sherwood is the Project Manager and primary Team member for this project. She currently manages the BII Intelligence Operatioins Program and has oversight/coordination responsibilities. She has been with DOJ for 20 years. She was a team member for the project to create the Sexual Predator Apprehension Teams.

5.2 Project Management Methodology

The project management methodology is the "Hawkins Data Center IT Project Management Practices", based on the "Project Management Body of Knowledge" (PMBOK®).

5.3 Project Organization

Under the management of SAC Sherwood, a Special Agent will be responsible for procurement, installation, set-up, testing and implementation of all hardware and software. These team members are experienced and trained in set-up, use, application, and testing of the forensic tools and computer equipment.

5.4 Project Priorities

Managing a project requires the balancing of three factors: schedule, scope, and resources. These three factors are interrelated; a change in one results in changes to the other two. The following project trade-off matrix shows the relative importance of each factor for this proposal:

- ***Constrained*** means the factor cannot be changed
- ***Accepted*** means the factor is somewhat flexible to the project circumstance
- ***Improved*** means that the factor can be adjusted

Schedule	Scope	Resources
Improved	***Constrained***	***Accepted***

5.5 Project Plan

5.5.1 Project Scope

The scope of the Violent Crime Digital Evidence Recovery project is limited to the procurement, installation and testing of commercial off-the-shelf hardware and software.

5.5.2 Project Assumptions

The Project Management Plan is based on the following assumptions:

- That grant funding is available.
- There will be no significant changes in hardware/software costs.

5.5.3 Project Phasing

The project is not phased.

5.5.4 Roles and Responsibilities

Project Sponsor

Project Sponsor responsibilities will include:

- Ensuring that the project has sufficient priority;
- High-level policy and financial decisions;
- Open issue resolution from a high-level perspective;
- Allocation of appropriate staff to the project.

DOJ Project Manager

The DOJ Project Manager will be responsible for:

- Coordination and monitoring of project activities, participants, and stakeholders.
- Project planning and control, including management of communications, risks, issues, change requests, and incident tracking;
- Keeping all stakeholders informed of plans, progress, and issues;
- Preparation of formal progress reports;
- Getting requisite sign-offs;
- Ensuring that all timeframes and cost estimates are met;

- Ensuring that state policies and procedures are followed;
- Contract management
- Risk planning and notification;
- Escalation and/or resolution of issues.

Other roles and responsibilities will be defined in the Project Plan prior to project initiation.

5.5.5 Project Schedule

The project will encompass the following activities:

Activity	Estimated Start	Estimated Completion	Milestone
FSR Approval	5/15/2008	9/1/2008	FSR Approved
Hardware/software Procurement	9/1/2008	10/1/2008	Hardware/software received
Installation, testing	10/1/2008	12/31/2008	Workstation implementation
Post-Implementation Evaluation	6/15/2009	8/31/2009	Post Implementation Evaluation Report (PIER)

5.6 Project Monitoring

The DOJ Project Manager will use a detailed project plan to establish baseline metrics. The manager will use additional tools to monitor changes to the baseline and will recalculate tasks and milestones, effort, budget, and scope accordingly. The Project Manager will identify and track issues, mitigation strategies, and solutions. Project status will be communicated to stakeholders through regularly scheduled meetings and reports. Please refer to section 5.10 below for Department Oversight Plan.

5.7 Project Quality

The project manager will ensure project results meet the stated objectives.

5.8 Change Management

The selected project management methodology defines change management processes, procedures, tools, and templates. The Project Manager is responsible for notifying all team members of the change process and individual responsibilities.

5.9 Authorization Required

FSR approval is required from the DOJ BII Chief, DLE Director, DOJ IT Bureau Chiefs, and DOJ Executive Management (Chief Information Officer; Director, Administrative Services Division; and Chief Deputy Attorney General).

5.10 Department Oversight Plan

5.10.1 Oversight Approach

The DOJ embraces the project oversight concept as a necessary quality assurance and cost containment effort and will follow the DOF *IT Project Oversight Framework* with regard to review of project status reports, documentation and activities, risk assessment, and oversight report preparation. An oversight report of findings will be prepared and submitted to the Project Manager, Executive Sponsor, and CIO. Oversight reports for the most critical projects will be submitted to the Attorney General.

5.10.2 DOF IT Project Oversight Framework Requirements

The DOJ has established the Project Oversight Unit within the Project Office to conduct independent IT project oversight of normal (low criticality rating) and critical (medium criticality rating) projects. The Project Office contracts with consultants for oversight of the most critical projects (high criticality rating) in support of technical solutions for any project where this service is warranted. DOJ anticipates a low criticality rating and intends to use internal staff to perform oversight analysis of the Violent Crime Digital Evidence Recovery project.

5.10.3 Independent Project Oversight - Departmental

All reportable and non-reportable IT projects are subject to independent oversight (reference Governor's Executive Order D-59-02 and DOF Budget Letter 03-04).

Oversight review and monitoring tasks are to ensure the projects successful implementation by identifying project risks (in the areas of time, costs, solution) and their successful mitigation. The Staff Information Systems Analyst from the DCJIS IT Project Office (ITPO) will perform project oversight through the independent review and analysis of project activities and documentation to determine if the project is on track with respect to costs, schedule, and scope. The analyst will identify and report to the ITPO manager on a quarterly basis any issues and risks affecting cost, schedule, and scope. The analyst will also investigate whether project management and system development best practices and standards are being followed.

6.0 RISK MANAGEMENT PLAN

6.0 RISK MANAGEMENT PLAN

6.1 Risk Management Approach

The DOJ Hawkins Data Center has adopted and implemented an IT Project Management Practices based on PMBOK. These practices include an approach to manage project risk. The Violent Crime Digital Evidence Recovery project will employ this approach to develop and execute a Risk Management Plan.

The Risk Management Plan will include identification of internal and external threats, defining each threat as probable or severe, devising and implementing a strategy to avoid or mitigate each threat, and incorporating these strategic actions into the overall project plan. The Risk Management Plan will also address monitoring of the identified risks during the project life cycle. Risk Reports will be used as a risk management tool. These reports will contain information for each key risk, describing the threat, impact on the project, current status.

The Project Manager will monitor, brainstorm mitigation strategies, and manage the Risk Management Plan through the use of ongoing team meetings and risk reports. Contingency measures will be thoroughly discussed, approved, and implemented through the Executive Team.

6.2 Risk Management Worksheet (RMW)

The following initial risks and preventative measures have been identified:

RISK	Probability	Affected Area	Prevention Plan	Contingency Plan
Organization/Management Risks				
Lack of specific technical expertise	medium	Schedule Budget	Select project team, from executive sponsor down, carefully. Ensure that all required skills are represented within the team. For projects for which no executive sponsor can be identified, reassess viability of project.	Initiate quality-control procedures with vendor and/or development staff.
External environment Risks				
Key software or hardware components become unavailable, unsupported or are unexpectedly scheduled for de-support	low	Schedule Budget Software Hardware	Unforeseeable: no preventive measures identified.	Meet with project team to investigate alternative resources, facilities or technologies. If no alternative is available, alter schedule and/or assign additional resources. If 10% slip to schedule or costs, initiate SPR.

7.0 ECONOMIC ANALYSIS WORKSHEETS

EXISTING SYSTEM/BASELINE
COST WORKSHEET

Department: Justice **Date: August 2008 v1**

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
Continuing Information Technology Costs						
Staff (salaries & benefits)	0.0	0	0.0	0	**0.0**	**0**
Hardware Lease/Maintenance		0		0		**0**
Software Maintenance/Licenses		0		0		**0**
Contract Services		0		0		**0**
Data Center Services		0		0		**0**
Agency Facilities		0		0		**0**
Other		0		0		**0**
Total IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Continuing Program Costs:						
Staff	0.0	0	0.0	0	**0.0**	**0**
Other		0		0		**0**
Total Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
TOTAL EXISTING SYSTEM COSTS	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**

* There is no existing system.

PROPOSED ALTERNATIVE: (Procure digital equipment)

Department: Justice

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs						
Staff (Salaries & Benefits)	0.7	95,391	0.0	0	0.7	95,391
Hardware Purchase		258,227		0		258,227
Software Purchase/License		140,915		0		140,915
Telecommunications		0		0		0
Contract Services						
Software Customization		0		0		0
Project Management		0		0		0
Project Oversight		0		0		0
IV&V Services		0		0		0
Other Contract Services		0		0		0
TOTAL Contract Services		**0**		**0**		**0**
Data Center Services		0		0		0
Agency Facilities		0		0		0
Other		31,979		0		31,979
Total One-time IT Costs	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
Continuing IT Project Costs						
Staff (Salaries & Benefits)	0.0	0	0.0	0	0.0	0
Hardware Lease/Maintenance		0		0		0
Software Maintenance/Licenses		0		0		0
Telecommunications		0		0		0
Contract Services		0		0		0
Data Center Services		0		0		0
Agency Facilities		0		0		0
Other		0		0		0
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Project Costs	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
Continuing Existing Costs						
Information Technology Staff	0.0	0	0.0	0	0.0	0
Other IT Costs		0		0		0
Total Continuing Existing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Program Staff	0.0	0	0.0	0	0.0	0
Other Program Costs		0		0		0
Total Continuing Existing Program Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Continuing Existing Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
TOTAL ALTERNATIVE COSTS	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
INCREASED REVENUES		0		0		**0**

Proposed Alternative (Detail): (Procure digital equipment)

Department: Justice

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
One-Time IT Project Costs						
Staff (Salaries & Benefits)	**0.7**	**95,391**	**0.0**	**0**	**0.7**	**95,391**
Existing						
Special Agent	0.3	34,002	0.0	0	0.3	34,002
Special Agent Supervisor	0.3	44,409	0.0	0	0.3	44,409
Special Agent In Charge	0.1	16,980	0.0	0	0.1	16,980
Hardware Purchase		**258,227**		**0**		**258,227**
Desktop Workstation - Alienware w/monitors (4)		44,876		0		44,876
Portable Workstation - Alienware (4)		28,351		0		28,351
Shuttle Workstation (4)		33,342		0		33,342
Cell Phone Data Extractor (2)		53,875		0		53,875
Secure View Kit (4)		12,930		0		12,930
Write Blockers		7,017		0		7,017
Hard Drive Imager (4)		24,392		0		24,392
Shadow Drive (4)		8,055		0		8,055
Flash Drive (8)		1,293		0		1,293
Hard Disk Drives (160)		30,170		0		30,170
Laptop Hard Drives (840)		3,689		0		3,689
CD/RW Discs (20)		539		0		539
DVD/RW Discs (20)		754		0		754
Terabyte Network Storage (4)		5,711		0		5,711
KVM Switch (4)		1,509		0		1,509
Laserjet Printer (2)		1,724		0		1,724
Software Purchase/License		**140,915**		**0**		**140,915**
Guidance Software - Encase (12)		38,790		0		38,790
Access Data - Ultimate Forensic Tool Kit (12)		25,201		0		25,201
ProDiscover Incident Response (4)		61,034		0		61,034
Digital Detective - Net Analysis (12)		776		0		776
Logicube - Celldek licensing (2)		4,310		0		4,310
Wireless Card ($79 per month) (4)		4,086		0		4,086
Virus Software (12)		647		0		647
Image Software (12)		647		0		647
Office Suite (12)		3,879		0		3,879
VM Ware (4)		901		0		901
CD/DVD Diagnostic (recovery) (12)		647		0		647
Telecommunications		**0**		**0**		**0**
Contract Services						
TOTAL Contract Services		**0**		**0**		**0**
Data Center Services		**0**		**0**		**0**
Agency Facilities		**0**		**0**		**0**
Other		**31,979**		**0**		**31,979**
DGS Purchasing Fees (2.27%)		9,061		0		9,061
Ongoing Standard Comp (existing positions)		22,918		0		22,918
Total One-time IT Costs	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
Continuing IT Project Costs						
Staff (Salaries & Benefits)	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Hardware Lease/Maintenance		**0**		**0**		**0**
Software Maintenance/Licenses		**0**		**0**		**0**
Telecommunications		**0**		**0**		**0**
Contract Services						
TOTAL Contract Services		**0**		**0**		**0**
Data Center Services		**0**		**0**		**0**
Agency Facilities		**0**		**0**		**0**
Other		**0**		**0**		**0**
Total Continuing IT Costs	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
Total Project Costs	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**

Proposed Alternative Staff - Detail (A)

Department: Justice
Project: Violent Crime Digital Evidence Recovery **Date: August 2008 v1.1**

Proposed Positions	Monthly Salary	Annual Salary	Salary Savings	Benefit Rate	Benefit Amount	**Salary (minus Savings) + Benefits**	One-time Standard Complenent	Ongoing Standard Complement
TOTAL	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**

Proposed positions are costed at mid-step.

Existing Positions	Monthly Salary	Annual Salary		Benefit Rate	Benefit Amount	**Salary + Benefits**		Ongoing Standard Complement
Special Agent	6,534	78,408		44.55%	34,931	**113,339**		32,740
Special Agent Supervisor	8,534	102,408		44.55%	45,623	**148,031**		32,740
Special Agent In Charge	9,789	117,468		44.55%	52,332	**169,800**		32,740
TOTAL	**24,857**	**298,284**	**0**	**1.3365**	**132,886**	**431,170**	**0**	**98,220**

Existing positions are costed at top step.

Proposed Alternative Staff - Detail (B)

Department: Justice
Project: Violent Crime Digital Evidence Recovery

	One-Time							
	FY 2008/09				FY 2009/10			
Existing Positions	PYs	Salaries + Benefits		Ongoing Std Comp.	PYs	Salaries + Benefits		Ongoing Std Comp.
Special Agent	0.3	34,002		9,822	0.0	0		0
Special Agent Supervisor	0.3	44,409		9,822	0.0	0		0
Special Agent In Charge	0.1	16,980		3,274	0.0	0		0
TOTAL	**0.7**	**95,391**		**22,918**	**0.0**	**0**		**0**

Date: August 2008 v1.1

Department: Justice
Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
EXISTING SYSTEM						
Total IT Costs	0.0	0	0.0	0	0.0	0
Total Program Costs	0.0	0	0.0	0	0.0	0
Total Existing System Costs	0.0	0	0.0	0	0.0	0
PROPOSED ALTERNATIVE	**(Procure digital equipment)**					
Total Project Costs	0.7	526,512	0.0	0	0.7	526,512
Total Cont. Exist. Costs	0.0	0	0.0	0	0.0	0
Total Alternative Costs	0.7	526,512	0.0	0	0.7	526,512
COST SAVINGS/AVOIDANCES	(0.7)	(526,512)	0.0	0	(0.7)	(526,512)
Increased Revenues		526,512		0		0
Net (Cost) or Benefit	(0.7)	0	0.0	0	(0.7)	(526,512)
Cum. Net (Cost) or Benefit	(0.7)	0	(0.7)	0		

PROJECT FUNDING PLAN

Department: Justice **Date: August 2008 v1.1**

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
TOTAL PROJECT COSTS	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
RESOURCES TO BE REDIRECTED						
Staff	0.7	95,391	0.0	0	**0.7**	**95,391**
Funds:						**0**
Existing System		0		0		**0**
Other Fund Sources		431,121		0		**431,121**
TOTAL REDIRECTED RESOURCES	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
ADDITIONAL PROJECT FUNDING NEEDED						
One-Time Project Costs	0.0	0	0.0	0	0.0	0
Continuing Project Costs	0.0	0	0.0	0	0.0	0
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	**0.0**	**0**	**0.0**	**0**	**0.0**	**0**
TOTAL PROJECT FUNDING	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
Difference: Funding - Costs	0.0	0	0.0	0	0.0	**0**

Total Estimated Cost Savings	0.0	0	0.0	0	0.0	0

ADJUSTMENTS, SAVINGS AND REVENUES WORKSHEET

Department: Justice **(DOF Use Only)** **Date: August 2008 v1.1**

Project: Violent Crime Digital Evidence Recovery

Annual Project Adjustments	FY 2008/09 PYs	FY 2008/09 Amts	FY 2009/10 PYs	FY 2009/10 Amts	
One-time Costs					
Previous Year's Baseline	0.0	0	0.0	0	
(A) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	
(B) Total One-Time Budget Actions	0.0	0	0.0	0	
Continuing Costs					
Previous Year's Baseline	0.0	0	0.0	0	
(C) Annual Augmentation /(Reduction)	**0.0**	**0**	**0.0**	**0**	
(D) Total Continuing Budget Actions	0.0	0	0.0	0	
Total Annual Project Budget Augmentation /(Reduction) [A + C]	**0.0**	**0**	**0.0**	**0**	

[A, C] Excludes Redirected Resources

Total Additional Project Funds Needed [B + D]

Annual Savings/Revenue Adjustments

Cost Savings	0.0	0	0.0	0	
Increased Program Revenues		0		0	

PROJECT FUNDING PLAN - Detail

Department: Justice **Date: August 2008 v1.1**

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
TOTAL PROJECT COSTS	**0.7**	**526,512**	**0.0**	**0**	**0.7**	**526,512**
RESOURCES TO BE REDIRECTED						
Staff	**0.7**	**95,391**	**0.0**	**0**	**0.7**	**95,391**
Existing Staff: One-time						
Special Agent	0.3	34,002	0.0	0	0.3	34,002
Special Agent Supervisor	0.3	44,409	0.0	0	0.3	44,409
Special Agent In Charge	0.1	16,980	0.0	0	0.1	16,980
Funds:						
Existing System	0.0	0	0.0	0		0
Other Fund Sources		431,121		0	0.0	431,121
Grant Funds	0.0	431,121	0.0	0	0.0	431,121
One-Time Project Costs	0.0	431,121	0.0	0	0.0	431,121
Hardware Purchase		258,227		0		258,227
Desktop Workstation - Alienware w/monitors (4)		44,876		0		44,876
Portable Workstation - Alienware (4)		28,351		0		28,351
Shuttle Workstation (4)		33,342		0		33,342
Cell Phone Data Extractor (2)		53,875		0		53,875
Secure View Kit (4)		12,930		0		12,930
Write Blockers		7,017		0		7,017
Hard Drive Imager (4)		24,392		0		24,392
Shadow Drive (4)		8,055		0		8,055
Flash Drive (8)		1,293		0		1,293
Hard Disk Drives (160)		30,170		0		30,170
Laptop Hard Drives (840)		3,689		0		3,689
CD/RW Discs (20)		539		0		539
DVD/RW Discs (20)		754		0		754
Terabyte Network Storage (4)		5,711		0		5,711
KVM Switch (4)		1,509		0		1,509
Laserjet Printer (2)		1,724		0		1,724
Software Purchase/License		140,915		0		140,915
Guidance Software - Encase (12)		38,790		0		38,790
Access Data - Ultimate Forensic Tool Kit (12)		25,201		0		25,201
ProDiscover Incident Response (4)		61,034		0		61,034
Digital Detective - Net Analysis (12)		776		0		776
Logicube - Celldek licensing (2)		4,310		0		4,310
Wireless Card ($79 per month) (4)		4,086		0		4,086
Virus Software (12)		647		0		647
Image Software (12)		647		0		647
Office Suite (12)		3,879		0		3,879
VM Ware (4)		901		0		901
CD/DVD Diagnostic (recovery) (12)		647				
Telecommunications		0		0		0
Contract Services		0		0		0
Data Center Services		0		0		0
Agency Facilities		0		0		0
Other		31,979		0		31,979
DGS ITPP Review		0		0		0
DGS Purchasing Fees (2.27%)		9,061		0		9,061
Standard Complement (Existing staff, one time ongoing)		22,918		0		22,918
Continuing Project Costs	0.0	0	0.0	0	0.0	0
Staff	0.0	0	0.0	0	0.0	0
Hardware Lease/Maintenance		0		0		0
Software Maintenance/Licenses		0		0		0

PROJECT FUNDING PLAN - Detail

Department: Justice **Date: August 2008 v1.1**

Project: Violent Crime Digital Evidence Recovery

	FY 2008/09		FY 2009/10		TOTAL	
	PYs	Amts	PYs	Amts	PYs	Amts
Telecommunications		0		0		0
Contract Services		0		0		0
Data Center Services		0		0		0
Agency Facilities		0		0		0
Other		0		0		0
TOTAL REDIRECTED RESOURCES	0.7	526,512	0.0	0	0.7	526,512
ADDITIONAL PROJECT FUNDING NEEDED						
None: project uses grant funds and existing spending authority	0.0	0	0.0	0	0.0	0
TOTAL ADDITIONAL PROJECT FUNDS NEEDED BY FISCAL YEAR	0.0	0	0.0	0	0.0	0
TOTAL PROJECT FUNDING	0.7	526,512	0.0	0	0.7	526,512
Difference: Funding - Costs	0.0	0	0.0	0	0.0	0
Total Estimated Cost Savings	0.0	0	0.0	0	0.0	0

ATTACHMENT A

Hardware and Software Descriptions

Equipment List

HARDWARE

Desktop Workstation: Used in the office workstation to conduct full forensic examinations of digital evidence. Desktop workstation will be equipped with four (4) monitors to allow preview of multiple functions at one time. Provides for added efficiency and effectiveness in examinations. Additional workstations, as described below, are necessary as it is impractical to haul a full desk top into the field to conduct examinations or field previews.

Portable Workstation: A laptop workstation is utilized in the field for quick previews or minor examinations. The laptop provides minimal setup, and connection to the target is made easier through use of the portable workstation allowing for quick process of a preview or examination.

Shuttle Workstation: Shuttles are utilized as a secondary or backup desktop, both in the field and in the office. Shuttles are considerably faster acquiring evidence in the field due to connecting directly to a computer's motherboard, as compared to a laptop USB or firewire ports. The Shuttle is basically a portable desktop and has more versatile connections to almost ANY digital storage device. The shuttle usually has more processing power and offers a separate keyboard and mouse. A shuttle is a necessity in any high volume, intense, field work.

In the examination process, examiners often will acquire evidence on one computer, conduct an exam/analysis on a second, and write a report on the third. Current examiners assigned to task forces have between 3 and 5 towers and laptops which may be used in every examination.

Cell Phone Data Extractor: Allows the examiner to immediately extract and review critical information at the crime scene from nearly ANY cellular telephone, blackberry device or PDA. Users can identity cell brand, model, and dimensions. Extracted data is unaltered and time stamped as an audit/investigative trail. Extracted data includes images, video and audio.

Secure View Kit for Forensics – Data Pilot: Provides the examiner with logical data extraction of the content stored in a mobile phone. Examiners may gain access to vital information in seconds with out the need to wait for a full examination. Able to detect all mobile content in a variety of cell formats that are different than offered in other hardware tool kits, including recent calls, contacts, calendar, pictures, and video. Includes two free years of software updates and cables.

Extracting data from cell phones, PDAs, smart phones and other portable digital devices is very new. Not all products (software/hardware) work on all the phones. It is imperative to have available to the examiner, those products that will provide the most coverage for the digital devices on the market.

Write Blocker Ultra Kit – Includes USB Write Blocker and Forensic Card Reader: Allows the examiner to extract images from mass storage devices, including multimedia and memory cards, without altering the data, thus providing the best evidence. Data will

not be modified inadvertently during the acquisition process. The write blocker card reader can be connected directly to digital cameras, MP3 players, voice recorders, PDA's, cell phones, computers and other digital storage devices. The USB Bridge allows flexible operation of a full range of forensic tools and software and can be used with thumb drives and external disk drives.

Hard Drive Imager – Digital Intelligence Hardcopy
Hard Drive Imager – Logicube Forensic Talon: Used by the examiner as a powerful data capturing system specifically designed for law enforcement. The product will simultaneously image and verify data and run advanced key word searches, ensuring that the source drive is not changed.

Shadow Drive: Allows the examiner to boot the suspect's hard drive in the native environment without making changes to the suspect's hard drive.

Flash Drive (2): Flash drives will be used by the examiner for portable storage, exporting data, tools, and software in conducting examinations and analysis.

Hard Disk Drives – Maxtor SATA 250 GB
Hard Disk Drives – Maxtor IDE ATA 250 GB: The hard disk drives are necessary for sterile target drives in creating the duplicate digital working images. 250 GB is a moderate contemporary storage capacity; however, terabyte storage capacity is becoming available to common citizens. SATA and IDE ATA are the two common connections found in all systems. Examiners must be prepared to encounter both connections at any time.

Laptop Hard Drives – Toshiba 100 GB IDE ATA
Laptop Hard Drives – Toshiba 100 GB SATA: The laptop hard disk drives are necessary for sterile target drives in creating the duplicate digital working images from a laptop computer. Laptop hard drives are necessary due to the physical difference in size of the laptop hard drive, which is 2.5 inches in comparison to the hard drive of a desk top which is 5.25 inches.

Forensics is a dynamic practice with every situation being unique and different. You may assume with every investigative call out, mirror imaging will be a requirement which will necessitate the use of a hard drive. Each hard drive may then be unavailable for use until the investigation is adjudicated.

CD/RW Discs
DVD/RW Discs: The CD and DVD discs will be used to copy data and evidence to provide to the investigation requester (local agency) or prosecutor for review and court. These items will not be returned by the agency. These items are not perishable and do not have a shelf life. However, items will need to be replenished on a regular basis to maintain a constant inventory.

Terabyte Network Storage: Provides the examiner a powerful storage solution and can accommodate expanded networked storage of multiple devices, and allows for quick swap out replacements.

KVM Switch: Allows the examiner to view four dual display computers from a single console and keyboard.

SOFTWARE

Guidance Software – Encase: Used to analyze digital evidence. Industry standard.

AccessData – Ultimate Forensic Tool Kit: Used to analyze digital evidence. Industry standard.

Technologies Pathways – Prodiscover Incident Response: Used to analyze digital evidence. Industry standard.

Digital Detective: Used to analyze Internet evidence. Industry standard.

Logicube – Celldek licensing: Software required to utilize Celldek hardware.

Wired DSL for non-mobile systems and Cellular Digital Wireless Card: Used to access wireless web and Internet in a remote location, including a crime scene.

Virus Software: Installed on each workstation to prevent intrusions and interruptions of data and examinations.

Image Software: Utilized to create working drive as mirror image to protect source drive from contamination or inadvertent changes.

Office Suite: Word processing and accessory software to provide examiner with full ability to prepare reports, charts, data spread sheets, and office tools.

CD/DVD Diagnostic: An industry standard product used by examiner to recover data. Recovers data files and video files. This product supports CD and DVD recovery and PC and MAC users.

VM Ware: The VM Ware software is a tool that gives the examiner the ability to recreate the suspect computer in a virtual PC window on the forensic computer. This system feature allows the examiner to see the system as the suspect/victim saw the system and gives the examiner the ability to inspect a live system from a user standpoint, without using the suspect's hardware. Utilizing this software adds additional security as it allows the examiner to review a suspect's hard drive without infecting the forensic computer or the evidence in the event any malicious code is present.