THE EMERGENCE, EVOLUTION AND NECESSITY OF DIGITAL FORENSIC CRIME LABS

ATTORNEY GENERAL OF WASHINGTON

WASHINGTON STATE PATROL
WSP

TABLE OF CONTENTS

COVER LETTER FROM AG MCKENNA AND CHIEF BATISTE

October 30, 2009

Hon. Brad Owen
President of the Senate
P.O. Box 40400
Olympia, WA 98504-0400

Hon. Frank Chopp
Speaker, House of Representatives
P.O. Box 40600
Olympia, WA 98504-0600

RE: **SB 5184**

Dear Lt. Governor Owen and Speaker Chopp:

As directed by SB 5184, Chapter 27, Laws of 2009, we present the findings of the digital forensic crime lab work group, as convened by the Attorney General's Office and the Washington State Patrol. As the authorizing legislation notes, there is a growing incidence of cybercrimes committed against Washington residents. However, the ability of law enforcement to investigate, prosecute and obtain convictions for online crimes is severely limited by the lack of facilities and personnel dedicated to the analysis of digital forensic evidence.

As the work group evaluated the need for a digital forensic crime lab, it was guided by the goals of the American Society of Crime Lab Directors: "To assist in the development of laboratory management principles and techniques; acquire, preserve and disseminate forensic based information; maintain and improve communications among crime laboratory directors; and to promote, encourage and maintain the highest standards of practice in the field."

Accordingly, the work group conducted informal surveys of law enforcement organizations and prosecutors across the state and submitted a set of written questions to the directors of existing digital forensic crime labs in New Hampshire, Massachusetts, Minnesota and Arizona. Our efforts culminated in a nationwide teleconference, the conclusions of which are reflected in the attached report and appendices.

We hope the Legislature finds these conclusions useful as lawmakers consider how to respond to the 21st century threat of cybercrime.

Sincerely,

Rob McKenna

ROB MCKENNA
Attorney General

John R. Batiste

JOHN R. BATISTE
Chief, Washington State Patrol

NATIONAL TELECONFERENCE SEPTEMBER 3, 2009

Larry Amos
New Hampshire State Police

Randy Arthur
Arizona Department of Public Safety

Greg Ayco
Seattle Police Department

Christopher Burgess
Cisco Systems

T.J. Campana
Microsoft

Donald Cheung
Minnesota Department of Public Safety

David Dunn
Seattle Police Department

Hunter Goodman
Washington State Attorney General's Office

Chris Gunderman
Washington State Patrol

Hon. Mike Humphreys
Walla Walla County Sheriff's Office

Jeremy Hursh
Minnesota Department of Public Safety

Chris Johnson
Washington State Attorney General's Office

Lisa Johnson
King County Prosecutor's Office

Eric Knutson
Minnesota Department of Public Safety

Mark Larson
King County Prosecutor's Office

Troy Larson
Microsoft

Hedda Litwin
National Association of Attorneys General

Jim Lord
U.S. Department of Justice, Western District of WA

Andrew MacPherson
University of New Hampshire

Hon. Dave McEachran
Whatcom County Prosecutor's Office

Neil Nelson
Saint Paul Police Department

David Papargiris
Massachusetts Attorney General's Office

Meredith Rabehl
Minnesota Department of Public Safety

Tom Ralph
Massachusetts Attorney General's Office

Jesse Regalado
Washington State Patrol

John Shehan
National Center for Missing and Exploited Children

Andrew Valentine
Verizon Business

EXPERT REVIEW PANEL MEMBERS AND CRIME LAB REPRESENTATIVES

YOUTH INTERNET SAFETY TASK FORCE

Adam Agensky
IAC Search and Media

Mike Andrew
Edmonds Community College

Theo Angelis
K&L Gates

Joanna Arlow
Washington Association of Sheriffs and Police Chiefs

Bill Ashworth
Yahoo!

Greg Ayco
Seattle Police Department/ Internet Crimes Against Children

Leslie Bar-Ness
Symantec

Wes Beaty
United States Postal Inspection Service

Jerry Bender
Association of Washington School Principals

Mark Berejka
Microsoft

Tim Braniff
Washington State Patrol

Brian Bujdoso
United States Immigration and Customs Enforcement

Christopher Burgess
Cisco Systems

Bob Calaff
T-Mobile USA

Lizanne Coker
LOOK**BOTH**WAYS

Chuck Cosson
Microsoft

Linda Criddle
LOOK**BOTH**WAYS

Milt Doumit
Verizon Northwest

Lisa Erwin
Washington State Attorney General's Office

Hunter Goodman
Washington State Attorney General's Office

Kate Greenquist
United States Attorney's Office, Western District of WA

Mira Guertin
American Electronics Association

Bill Guidera
News Corporation

Steve Hailey
Edmonds Community College

Stu Halsan
AOL

Sue Hotelling
Microsoft

Brent Howard
Educational Service District 101

Scott Huber
Columbia Bank

Joe Ingoglia
Boys and Girls Clubs of Thurston County

Chris Johnson
Washington State Attorney General's Office

Chris Johnson
King County Sexual Assault Resource Center

Lisa Johnson
King County Prosecutor's Office

Sarah Johnson
K&L Gates

Mark Kovach
T-Mobile USA

Kevin Laverty
Washington State School Directors' Association

Kirk Lawrence
AC Search and Media

Stephanie Lister
United States Attorney's Office, Eastern District of WA

Nicholas Lovrich Jr.
Washington State University

Tim Luckie
Seattle Police Department/ Internet Crimes Against Children

Simrin Mangat
Fox Interactive Media

Kelly Martin
Office of the Superintendent of Public Instruction

Tom McBride
Washington Association of Prosecuting Attorneys

Hon. Rob McKenna
Washington State Attorney General's Office

Warren McKenzie
National Research Council of Canada Institute for IT

Lew McMurran
Washington Technology Industry Association

Barbara Mertens
Washington Association of School Administrators

John Murphy
United States Postal Inspection Service

Hemanshu Nigam
Fox Interactive Media

Don Pierce
Washington Association of Sheriffs and Police Chiefs

Gavin Pinchback
T-Mobile USA

Deb Ramsay
Educational Service District 101

Melissa Reed
T-Mobile USA

Jesse Regalado
Washington State Patrol

Roger Rogoff
United States Attorney's Office, Western District of WA

John Rendell
FBI Citizens' Academy Alumni

Shauna Rumsey
King County Sexual Assault Resource Center

Leanne Shirey
Seattle Police Department

Delee Shoemaker
Microsoft

Sumeer Singla
Verizon Northwest

Dennis Small
Office of the Superintendent of Public Instruction

Brad Thomas
Seattle Police Department

Brent Thompson
IAC Search and Media

Barbara Thurman
Office of the Superintendent of Public Instruction

Jason Timm
Kuzoa

Tyson Vogeler
Office of the Superintendent of Public Instruction

Rhonda Weaver
Comcast

Lana Weinmann
Washington State Attorney General's Office

Brian Werner
United States Attorney's Office, Western District of WA

Kari Wilkinson
Washington State PTA

Fred Yancey
The Nexus Group/Boys and Girls Club

Lucinda Young
Washington Education Association

Brian Zwit
AOL

INTRODUCTION AND EXECUTIVE SUMMARY

In response to the Youth Internet Safety Task Force's (YISTF) recommendation that Washington create a state-level digital forensic crime lab, the Attorney General's Office in 2009 approached the Legislature with SB 5184 (relating to evaluating the need for a digital forensic crime lab).

The YISTF's Law Enforcement Subcommittee sought to determine what additional training and resources were needed to detect, investigate and prosecute crimes related to online sex predation against children. The subcommittee identified the need for such a lab because law enforcement personnel and prosecutors increasingly find that many types of cases, including identity theft and fraud, are touched by technology. Crime in the 21st century often involves computers, cell phones, cameras and other digital devices not encountered in years past. Law enforcement cannot successfully catch the criminals of today with the technology of yesterday.

The study group convened in response to SB 5184 sought to evaluate the need for a digital forensic crime lab and remote case review system, and to determine which template, if any, would prove the most suitable for replication in Washington.

To accomplish this, the Attorney General's Office and the Washington State Patrol formed a work group/expert review panel to research the origins and operating practices of existing digital forensic crime labs in New Hampshire, Massachusetts, Minnesota and Arizona. Prior to hosting a nationwide teleconference, staff conducted an informal survey of law enforcement and prosecutors within the state to determine if and how a digital forensic crime lab would benefit them in successfully investigating and prosecuting crime in their jurisdictions.

SURVEY RESULTS

The Washington Association of Sheriffs and Police Chiefs sent out a statewide survey to determine if law enforcement jurisdictions across the state need a digital forensic lab. Of the 41 agencies that responded, 97 percent reported investigating crimes which involved digital evidence contained in computers, cell phones or related storage media. Additionally, 78 percent of respondents reported they had some ability to forensically recover digital evidence. However, only 34 percent of the respondents indicated a sufficient number of forensic examiners were available to meet the needs of their respective departments. All agreed they would be willing to share resources with other departments.

Most respondents, 87 percent, said they would submit phones for evaluation if a statewide digital forensic lab was available. Additionally, 58 percent reported that they do not have the resources to identify, locate and collect evidence from computers. The most telling response was that 53 percent of the respondents reported that delay in receiving a computer forensic report has had an adverse impact on an investigation.

The Washington Association of Prosecuting Attorneys also sent a survey to members to determine if increased access to digital forensics would impact cases. Although there were not enough responses from elected prosecutors to be statistically significant, the responses that were received provide insights into the value that timely digital forensic reports could provide to a successful prosecution. In particular, respondents indicated they would be more likely to file charges and pursue a case if the forensic report was available sooner than the current nine months, with a 30 to 60-day time frame being most preferable. The general consensus was if it takes nine months to examine a computer that may provide key evidence in a case, the current 90-day speedy trial limit for suspects in custody will have already expired.

FINDING: Backlogs at existing digital forensic crime labs are sufficient to hamper investigations or preclude prosecutions.

In evaluating the need for additional forensic crime lab facilities and trained forensic examiners, the YISTF's Interim Report noted that the existing Washington State Patrol computer labs "are not designed from either an equipment or personnel standpoint, to handle existing or future demand for computer forensics." The current backlog at the Washington State Patrol computer lab is estimated at 30 to 60 days at current operating capacity, without any additional cases received.

Washington law enforcement agencies utilizing the federal Regional Computer Forensics Laboratory (RCFL) in Portland report delays ranging from nine to 12 months for completed forensic reports. Crime lab directors in the four states interviewed confirm similar results: An eight to ten-month backlog at the Federal Bureau of Investigation (FBI) lab in Phoenix, an eight to 14-month backlog at the RCFL in San Diego, an eight to 12-month backlog at the FBI lab in Minneapolis and similar delays at the RCFL in Chicago. Massachusetts could not confirm a uniform backlog with federal labs, but noted that the FBI, Immigrations and Customs Enforcement (ICE) and Internet Crimes Against Children (ICAC) facilities were all in close proximity to the state digital forensic crime lab in Boston.

RECOMMENDATION: Given that federal facilities exist primarily to process evidence in support of federal investigations and prosecutions, it is recommended that Washington expand its capacity to process digital evidence within the 30 to 60-day time frame needed by local prosecutors to file charges against suspects already in custody.

ACCREDITATION AND CERTIFICATION

The four states that took part in the expert review panel have all successfully implemented statewide digital forensic crime labs, albeit in very different ways.

There are many models a state might employ to design, develop and implement a forensics lab. Accreditation and certification is no different in that it avails the states with many potential solutions for establishing standards of operation that are committed to the highest ethical and professional standards.

Though accreditation is not required for the development or implementation of a forensic lab, many labs use the American Society of Crime Lab Directors (ASCLD) as a framework for lab development. ASCLD offers programs of accreditation, specifically targeted towards enhancing the laboratory service provided to the criminal justice system while also providing a construct/ criteria for assessing performance levels at the lab site.

ASCLD provides an objective, impartial overview by performing a robust and comprehensive operational review of the lab and personnel. This overview assists in identifying those facilities that meet established standards.[1]

RECOMMENDATION: After considerable inquiry, we have determined ASCLD or similar certification to be advantageous for several reasons. First, trends indicate that funding of labs in this ever-evolving forensic field will depend on adhering to established lab standards of national accreditation and certification. Secondly, forensic science is a very dynamic field and thus necessitates opportunities for peer review and regular requirements for an accrediting agency to conduct on-site reviews. Such reviews will ensure lab personnel comply with the highest standards of scientific inquiry and apply the most accepted investigation methods.

Though much of our focus was on the lab facility, we have not overlooked the necessity of ensuring we have the most competent forensic investigators and lab technicians. Again, we believe that accreditation through a nationally recognized agency, such as ASCLD, will ensure that lab personnel meet consistent and quantifiable standards. Therefore, we believe that accreditation of the lab facility and personnel will undoubtedly aid in successful prosecutions.

The development of a forensic lab and the procurement of investigators and technicians with the requisite skills to staff a complex lab in such a dynamic area of criminal justice will require time and significant funding. The aforementioned states clearly recognize this challenge and thus have, in some instances, deferred seeking accreditation until after a lab was up and running. However, even when a state elected to defer accreditation, they were always cognizant of nationally recognized standards. This deference to established standards will help expedite later accreditation while preserving the lab's value to law enforcement and prosecutorial agencies.

1. See ASCLD website, www.ascld-lab.org.

FACILITY REQUIREMENTS

During the nationwide teleconference, participants engaged in an in-depth discussion to determine the footprint for a fully functional digital forensic crime lab and independent training facility. The group also discussed how to ensure that the lab and training facility could be co-located without contaminating each other in any way. Additionally, we must ensure that the lab meets not only today's needs, but is also scalable to meet emerging modalities of Internet and digital crime of the future.

Each of the four states has different space requirements based on the model of their respective lab. For example, Arizona co-locates its facility inside the FBI's Phoenix field office. New Hampshire uses a relatively small footprint because it utilizes 183 "T1" lines to connect with all of the state's law enforcement agencies via remote access. Minnesota, which currently utilizes 550 square feet of lab space, recognized the need for a larger footprint from the lab's inception. Representatives from all four states reported that scalability is of the utmost importance and must be considered before a lab is developed. Sufficient resources must be available to fully utilize a lab's potential to investigate a wide variety of crimes, including identity theft and financial fraud.

FINDING: Not dissimilar to most issues raised in this report, there is no "one size fits all" model. However, each facility must have space to accommodate several work stations that are equipped with Internet and email connectivity, an imaging work station with no connection to the Internet and a secure server room with backup located off-site as minimum requirements.

JURISDICTIONAL AND GOVERNANCE ISSUES

Teleconference participants also discussed which agency was best suited to provide digital forensic crime lab services on a statewide level. Representatives of the existing digital forensic crime labs, as well as those representing state and local law enforcement in Washington, agreed that deciding on a host agency was of paramount importance.

FINDING: It is essential that any state agency that proposes to act as the central repository for digital forensic evidence must have the concurrence of the local law enforcement agencies it will serve. Such concurrence is needed regardless of which entity has original jurisdiction for investigating and prosecuting various criminal offenses.

Massachusetts has a complex system of overlapping criminal jurisdiction. Historically, local police departments handle most criminal investigations, while the state police provide service to rural areas and on state and federal highways. The state police can only operate in municipalities by agreement. District attorneys prosecute all crimes and have appellate jurisdiction, while the attorney general has overlapping plenary jurisdiction and represents the commonwealth in federal court. Sheriffs have primary responsibility for prisoner oversight and transfer.

While there is a network of general crime labs across Massachusetts, the attorney general's office hosts the state digital forensic lab. The lab is housed in that office because Attorney General Coakley developed a detailed plan to fight cybercrime, including identifying the need for training in digital crime scene response. The digital forensic lab, which was developed after completion of a comprehensive survey and a series of meetings with law enforcement across the state, is one piece of that strategy.

New Hampshire, which differs from Massachusetts in criminal jurisdiction, developed a separate model. The attorney general prosecutes homicides and has jurisdiction over all major felonies. The state police act as the host agency for a statewide crime lab and the digital forensic lab, which is centrally located in Concord. Local law enforcement agencies are connected to the lab via the state police network, utilizing a remote case review system. Procedures, protocols and metrics were developed in cooperation with the University of New Hampshire.

The Arizona digital forensic crime lab is sited in Phoenix, the state's fusion center. A fusion center is a law enforcement information sharing center developed by the Department of Homeland Security and the United States Department of Justice. The lab supervisor is a sergeant with the Arizona Department of Public Safety. There are also two civilian examiners and 21 sworn officers representing 11 different agencies co-located in the same facility. Because there is no formal memorandum of understanding which governs interagency participation, each agency determines its own caseload. To avoid duplication of skills, all lab personnel go through basic forensic training and then develop a specific skill, such as cell phone examination.

The Saint Paul Police Department, which was lead agency for the state's ICAC Task Force from 2000 to 2006, developed and hosted the first Minnesota digital forensic lab. Since that time, the Minnesota State Legislature has allocated resources to the state Bureau of Criminal Apprehension

to operate the lab. However, the focus remains on ICAC related crimes and not on financial crimes or identity theft. The digital lab is adjacent to the state's general crime lab in the Department of Public Safety, but the two are not affiliated.

RECOMMENDATION: Washington should adopt and implement a hybrid digital forensic crime lab model that will consist of a central repository for digital evidence. The lab should be supplemented by a system of regional hubs where evidence may be deposited.

Washington has its own unique system of public safety. Local police departments and sheriffs' offices act as first responders to most crimes, and locally elected prosecutors have original jurisdiction over all criminal matters governed by state law. In addition to other duties, the Washington State Patrol operates the state system of general crime labs. The Attorney General's Office takes criminal cases upon the referral of local prosecutors and maintains a database of homicide and sexual assault crime scene information.

As noted earlier, the Regional Federal Crime Lab system exists first to evaluate evidence in support of federal investigations. Local jurisdictions sending forensic evidence to the RFCL in Portland may face backlogs of six to nine months before receiving forensic reports. A state digital forensic crime lab must primarily provide assistance to local law enforcement and prosecutors.

Creating a true remote case review system would be expensive and would require local agencies to hire and train additional personnel. Also, a single central facility could easily become inundated with evidence. A hybrid model would enable agencies across the state to deliver evidence to a regional collection facility, where evidence technicians would create a copy or "clone" of the evidence. The evidence would subsequently be sent to the central repository for evaluation by forensic examiners. The submitting jurisdiction would retain custody of the original evidence, but remote viewing stations would exist at regional facilities.

As shown by the models implemented in other states, training for both cyber investigators and forensic examiners is essential to the success of this proposal in Washington. Presumably, the regional collection facilities would also serve as the location for regional "train the trainer" exercises. This would allow local law enforcement agencies to obtain the appropriate training for first responders without extensive travel.

STAFFING AND MANAGEMENT MODELS

Each existing state digital forensic crime lab has a separate staffing model, in part based on available resources and demand for services. The Massachusetts lab, which is operated by the attorney general, supports three to five forensic examiners and one supervisor. The New Hampshire lab, which is housed by the state police but is operated by civilians, consists of two full-time examiners, one half-time examiner and a director. Minnesota's lab, which provides support for ICAC-related investigations, has four civilian examiners, a special agent in charge (SAC) and a senior special agent.

As related earlier, the Arizona digital forensic lab consists of two civilian forensic examiners, 23 sworn officers representing 11 law enforcement agencies and one supervisor from the Arizona Department of Public Safety. Despite different pay scales and levels of training, there does not appear to be any segregation between civilians and sworn officers.

FINDING: There is no general staffing ratio for digital forensic labs. For instance, while the New Hampshire lab averages 25 cases per examiner per year, this ratio seems to be more a function of demand and funding than on a specific business model.

From the outset, it has been assumed that a digital forensic crime lab in Washington should exist to evaluate digital evidence on all crimes with a 30 to 60-day turnaround for the production of finished forensic reports. It is conceivable that a facility such as the state fusion center or other facility used by a federalized task force could provide space for a co-located, multijurisdictional facility. However, this work group cannot speculate on the willingness of federal partners to engage in such an enterprise or ensure that such an arrangement would prioritize services for local law enforcement agencies and prosecutors.

RECOMMENDATION: To develop an effective staffing and training model, the group recommends further evaluation into the development of a state digital forensic crime lab. The lab could be hosted by the Investigative Assistance Division within the Investigative Services Bureau of the Washington State Patrol.

The Investigative Assistance Division currently includes the Missing and Exploited Children Task Force, the High Tech Crime Unit and the Missing Persons Unit. Existing personnel within these units are already specialists in digital forensics, and a staffing model could be developed which takes into account current supervisor to staff ratios, as well as the capacity of existing personnel and capital facilities. Additionally, the location of regional digital collection facilities at the eight existing WSP detachments would enable the digital forensic lab to take advantage of the secure network already in place.

WORKLOAD METRICS

Determining caseload metrics is difficult because of the variables that exist in each lab environment. We must consider the scope of the lab's jurisdiction and the type of evidence investigated. Such evidence may come from computers, digital cameras, thumb drives, memory sticks and mobile devices (like IPODs, cell phones and PDAs).

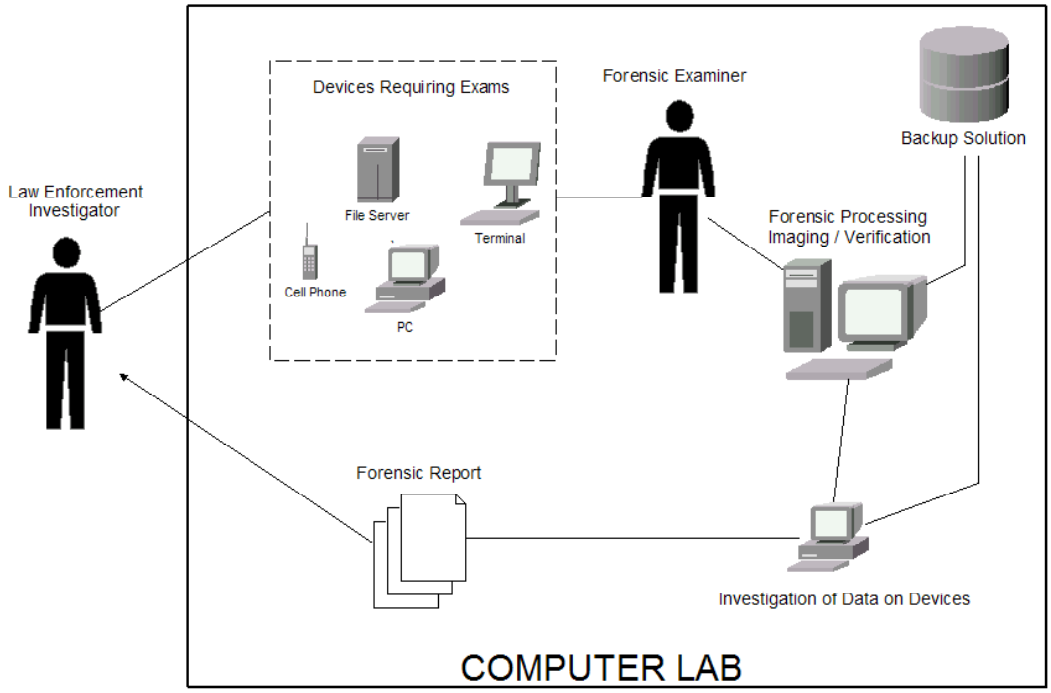
In 2008, the Washington State Patrol's High Tech Crime Unit (HTCU) received 158 cases from state agencies and local police departments. The unit operated with a total of six full-time personnel and one supervisor. Evidence was collected from various criminal and internal investigations ranging from homicides to sex crimes. The types of crime and digital evidence collected are similar to what would be submitted to a regional lab.

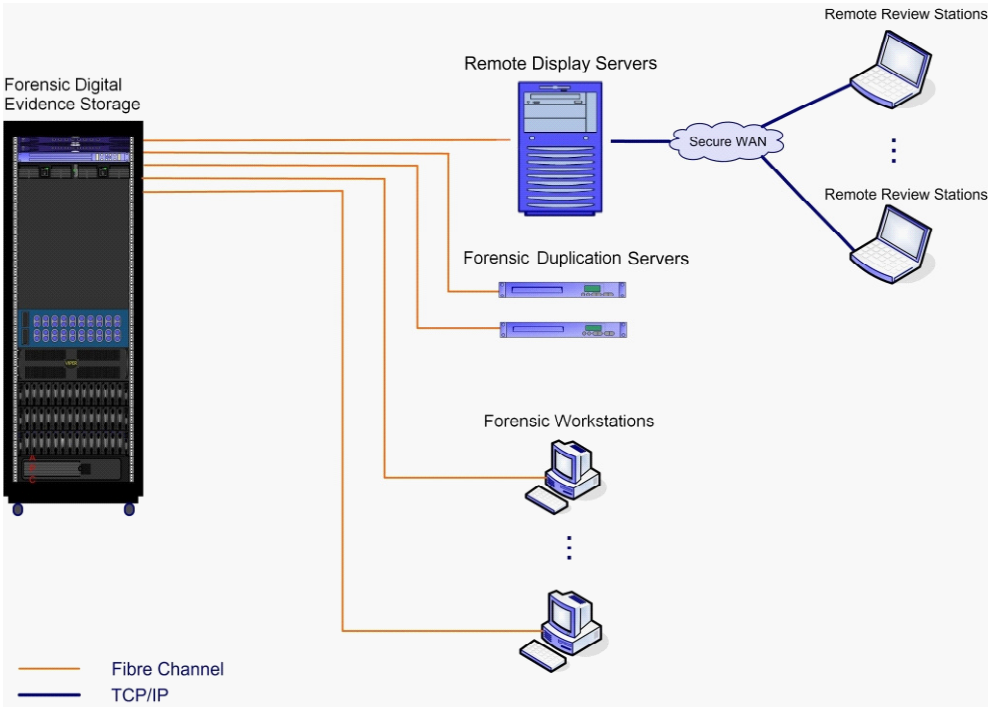
Of the 158 cases the HTCU received, 144 were completed during 2008. The remaining 14 cases were completed in 2009. The cycle time for these cases was approximately eight months for case completion. This time estimate included the other activities the unit provides including training, court appearances, search warrants, meetings, and other operational duties as needed. The average cases worked per examiner is between 25 to 29 cases per year. The supervisor completed a minimal number of examinations and was not included in the case count average work completion calculation.

These statistics are generally consistent with what Arizona, Massachusetts, Minnesota and New Hampshire have experienced.

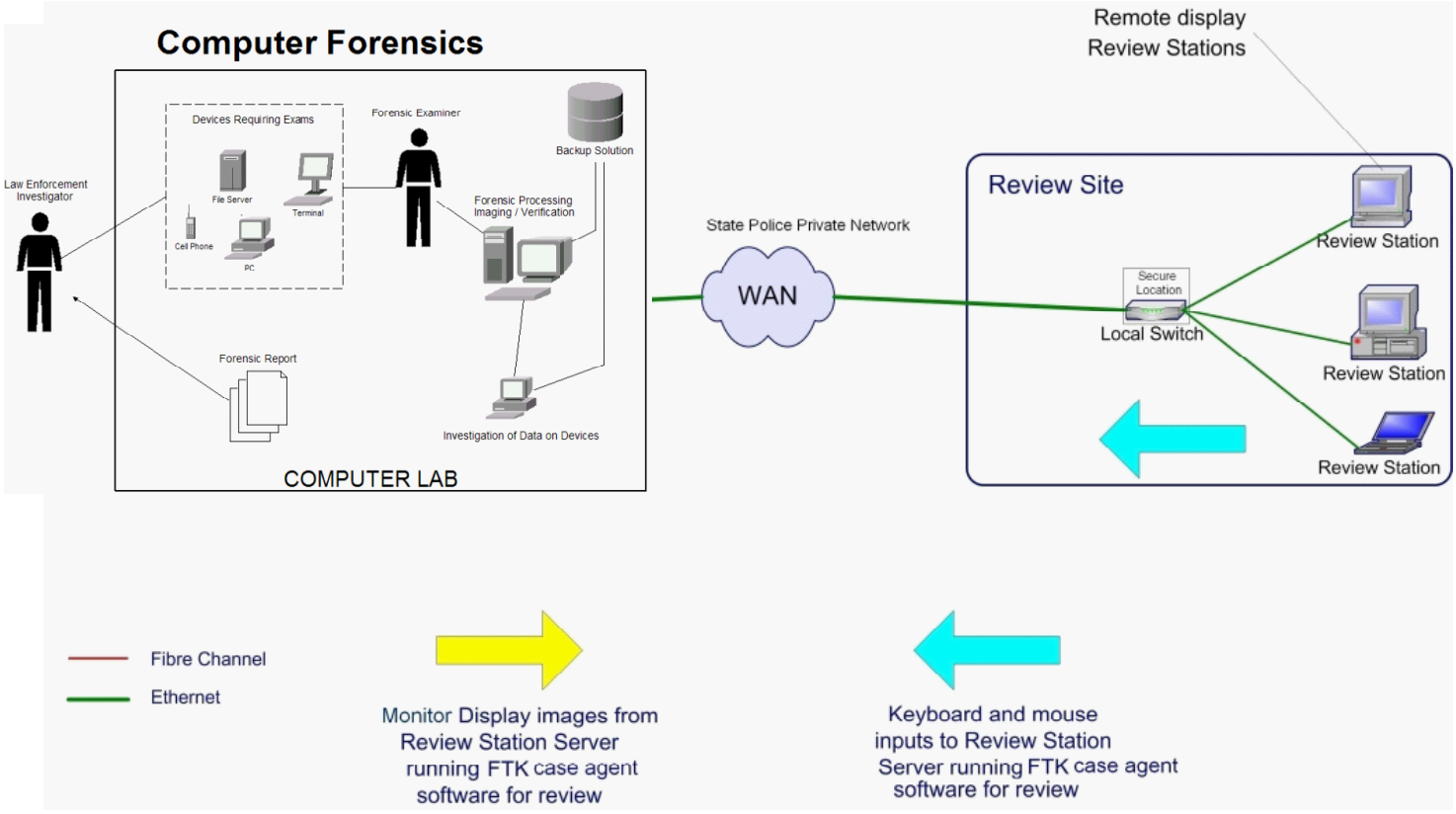
FINDING: Caseload numbers are not useful in indicating the level of support needed for a case or the complexity of a case. Staffing and other lab support must be flexible due to the dynamic environment of a lab. Caseload metrics are also driven by new modalities of digital crime. As crime evolves, training becomes increasingly important to the digital crime investigator and lab technician, thus pulling them away from their casework.

COMPUTER FORENSICS





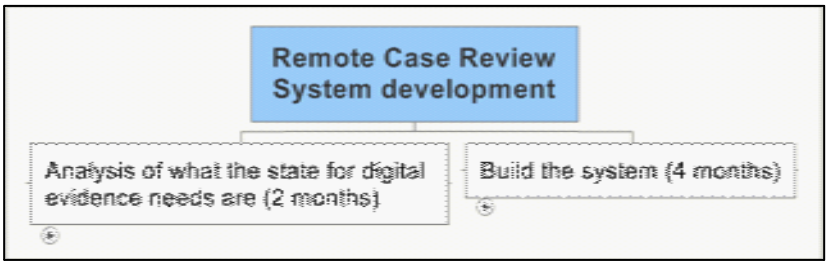
DIGITAL EVIDENCE VIEWING NETWORK

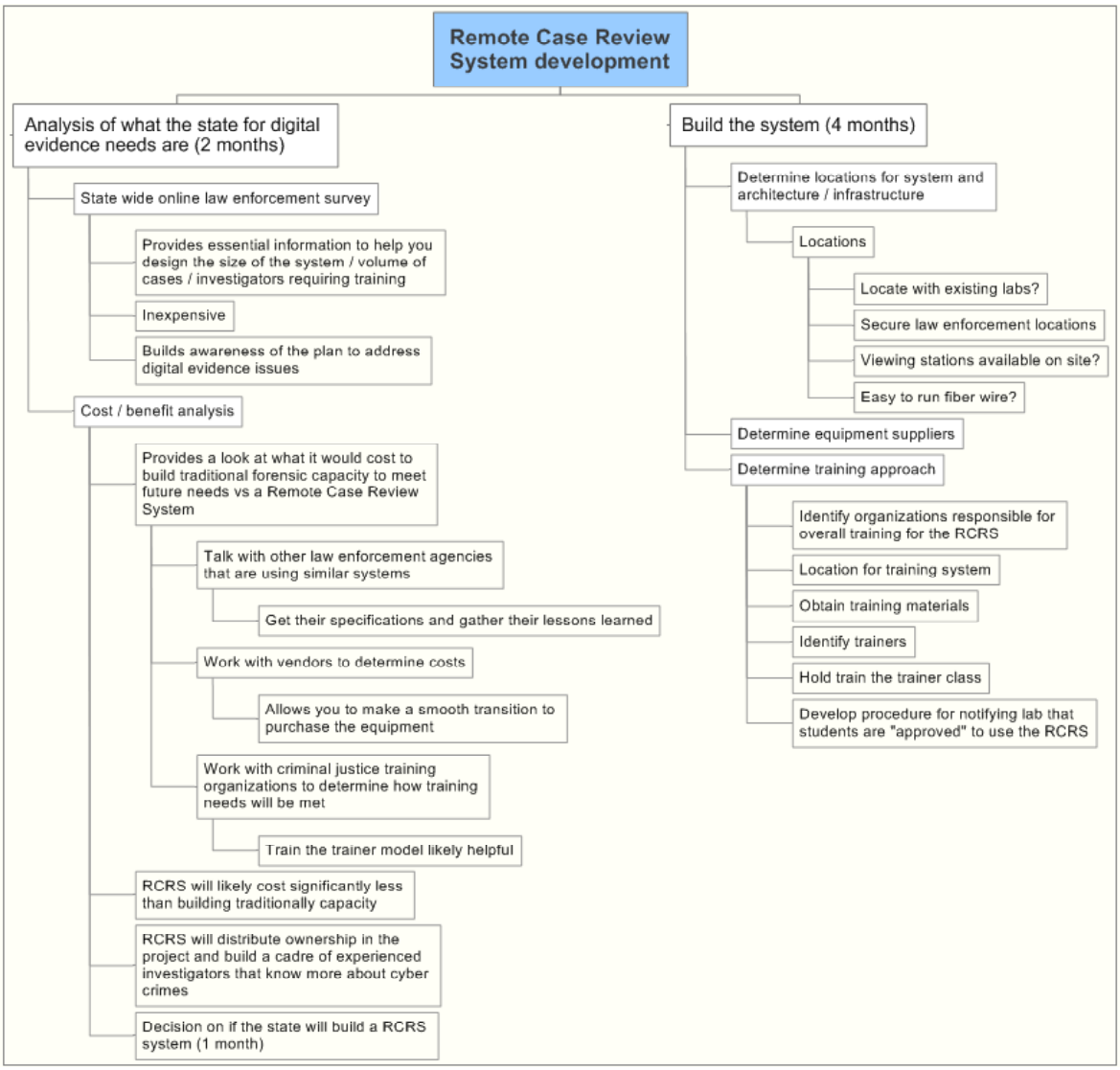


DIGITAL EVIDENCE VIEWING NETWORK TRAINING

- Case Reviewer

REMOTE CASE REVIEW SYSTEM DEVELOPMENT





DIGITAL EVIDENCE UNIT TRAINING CHECKLIST

(State of New Hampshire)

Training for: _____

Training by: _____

	Item	*Trainee Initials*	*Date Performed*	*Trainer Initials*	*Date Reviewed*
Digital Evidence Unit Orientation	Digital Evidence Unit Specific Evidence Handling & SOP's				
	Supply storage orientation				
	Manuals (Equipment QC, Quality Assurance, Unit Procedures)				
	Hardware & Software Equipment Manuals and/or User's Guides Configuration, Connectivity & Application				
	Publications (Computer Corner) Training Files/Manuals				
	Unit Specific Safety				
	Validation Quality Control				
Laboratory Training	Training In Lab Set-Up, Preparation & Handling Precautions				
	Training in Pre-Examination Procedures				
	Training in Evidence Preservation & Acquisition				
	Training in Case Review Configuration and Presentation				
	Training in Evidence Analysis & Recovery				
	Training In Digital Evidence Extraction from Mock or Supervised Evidence Exhibits				
	Training in Interpreting Digital Evidence				
	Training in Post-Examination Procedures				
	Report Writing				
Competency Tests	Successful Completion of Mock Or Supervised Casework				
	Successful Completion of Oral Or Written Exam				

Additional training reviewed/comments:

_____

SAMPLE TRAINING PROTOCOL FOR EXAMINER'S IN THE NEW HAMPSHIRE DIGITAL EVIDENCE UNIT

OBJECTIVE
To outline a procedure by which all employees will be oriented into and trained for Digital/Forensic Laboratory digital evidence unit.

SCOPE
This applies to all employees who will be performing digital evidence examinations or additionally any employee who may serve to gain from knowledge of digital evidence unit's policies and procedures.

This is a new and dynamically evolving area in evidence collection and examination and not all of the training and special areas of expertise are listed.

PROCEDURE

1. **Record training on Digital Evidence Unit Training Checklist.**

2. **Background**
   - 2.1. Review all digital evidence handling procedures carefully.
   - 2.2. The equipment section of the manual will be reviewed as well as any applicable general procedures for equipment.
   - 2.3. Safety
     - 2.3.1. Every employee is entitled to and responsible for a safe working environment. Each trainee will be educated as to general safety standards and specific safety standards for that unit. This will include:
       - Reading the unit specific standard operating procedure.
       - Reading the individual standard operating procedures precaution and disposal sections.
       - Reading safety specific literature for that unit.
       - A qualified analyst will go over each standard operating procedure with the trainee and make them aware of any special precautions within the procedure (i.e.: equipment, biohazards, chemical hazards, electrical, hoods, disposal, crime scene safety, etc.).

3. **Literature**
   - 3.1. The entire digital evidence unit procedure manuals will be reviewed, paying special attention to examinations that will be performed by the analyst being trained.
   - 3.2. Required readings
     - 3.2.1. A list of required and recommended readings is maintained by the senior criminalist.

4. Experience

4.1. Required Experience:

4.1.1. Analysts must have/gain a comprehensive understanding of how digital information is created, stored and accessed on electronic media utilizing a variety of hardware, software and operating system configurations.

4.1.2. Analysts must have/gain experience with the installation, configuration, operation and maintenance of hardware, software and communications equipment in simple to complex networking and computing environments.

4.1.3. Analysts must have an in-depth working knowledge of the Internet.

4.2. Desired Experience:

4.2.1. Certified Computer Forensic Examiner (IACIS see training below) or the completion of the requirements to obtain certification within the current year of hire.

4.2.2. Experience in the field of computer crime, laboratory procedure and evidence handling.

5. Training

5.1. Required

5.1.1. A+ Certification Course or equivalent (ASCLD or other)

5.1.2. BDRA - Basic Data Recovery and Analysis; National White Collar Crime Center) or equivalent.

5.1.3. ADRA - Advanced Data Recovery and Analysis; National White Collar Crime Center (www.nw3C.org) or equivalent.

5.1.4. Forensic software basics or introduction in the use of FTK, ENCASE, ILOOK, etc; or equivalent.

5.1.5. During all of this outside training, the analyst will also be performing mock cases in various areas which represent typical case submissions, with the guidance of a qualified examiner and shadowing a qualified examiner as they perform casework.

5.2. Recommended

5.2.1. Seized Computer & Evidence recovery + Computer Evidence Analysis; Federal Law Enforcement Training Center (www.fletc.gov)

5.2.2. Certified Computer Forensic Examiner Course; The International Association of Computer Investigative Specialists (www.cops.org)

6. Examination background training

6.1. Lab set-up, special handling considerations, proper use of controls and maintenance of proper case documentation shall also be reviewed.
6.2. There will be training in DEU analysis and interpretation.
6.3. Validation studies will be reviewed.
6.4. Report writing procedures will be reviewed and practice reports may be written using DEU data sets provided by the technical leader.

7. Analyst Competency/Proficiency

7.1. This will include an examination of a mock case(s) by the trainee.
7.2. The trainee will examine the item(s) and prepare a laboratory report.
7.3. An oral or written examination will be administered to ensure the trainee is familiar with the topics covered during the training.
7.4. A proficiency test will be administered as soon as available.
7.5. Analysts will be trained in courtroom techniques as per TRA-050.

1125 Washington St. SE
PO Box 40100
Olympia WA 98504-0100
(360) 753-6200
www.atg.wa.gov

General Administration Building
PO Box 42600
Olympia WA 98504-2600
(360) 596-4000
www.wsp.wa.gov