

**Virtual Digital Evidence Lab:
A Distributed Forensic Resource
Network**

Dr. Philip Craiger
National Center for Forensic Science &
Department of Engineering Technology
University of Central Florida

Abstract

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,’ which 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.

Digital Evidence Labs: 2006

Currently, the collection, 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 in that local and state law enforcement agencies typically, and unnecessarily duplicate, resources that are available elsewhere. A further problem is that each law enforcement agency must verify and validate examination tools, a process duplicated by all law enforcement agencies for all tools they in digital forensic examinations.

Virtual Digital Evidence Labs

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,’ which 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.

‘Virtual labs’ will consist of cutting-edge technology located in various places, connected via ‘ultra high-speed’ networking. Florida LambdaRail is As such, the technology and resources (expertise, storage, tools, etc.) required to perform 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.

Advantages

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).
3. Provide expert assistance with certified examiner specialists (e.g., Mac OS X, Solaris, network forensics, etc.).

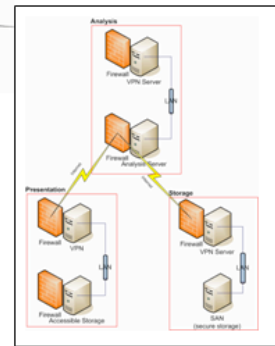
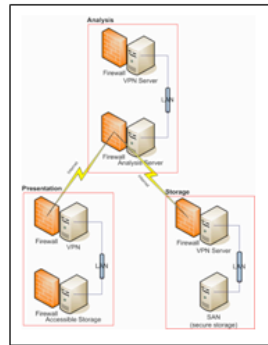
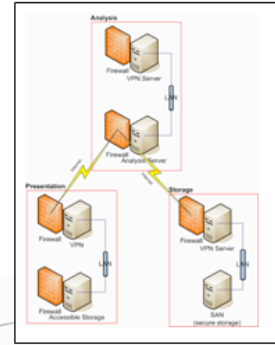
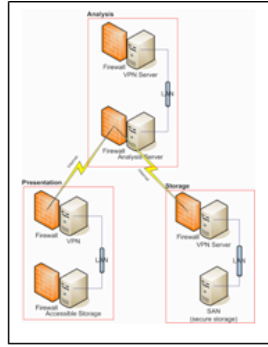
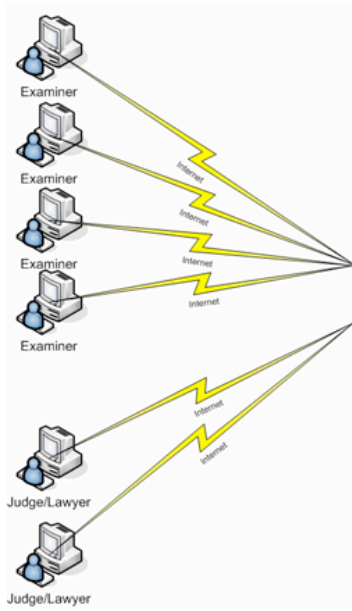
Technical Overview

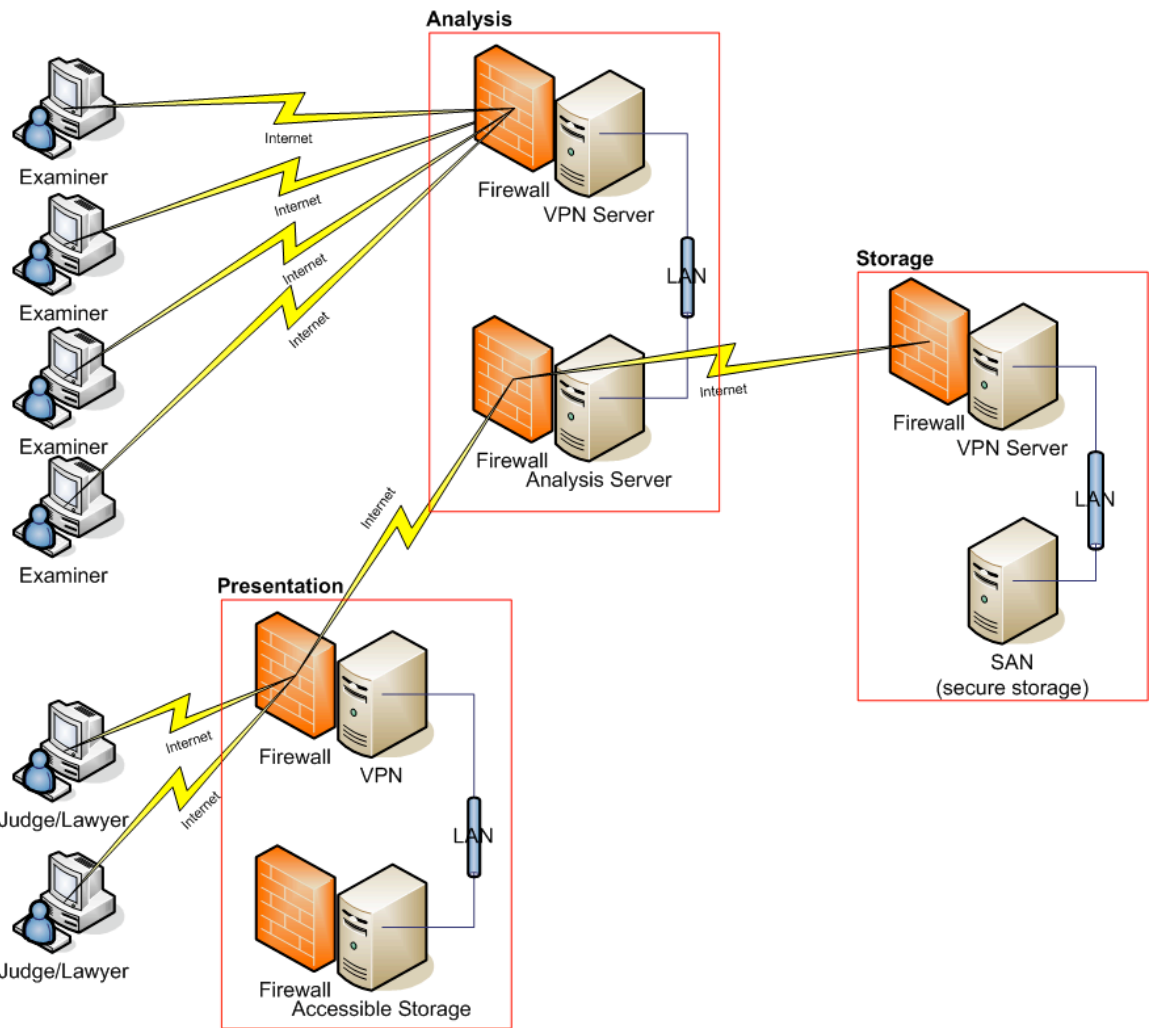
We propose to develop an experimental prototype virtual lab consisting of distributed, shared digital forensic resources accessible by law enforcement. This lab would consist of technological resources such as examination machines; digital forensic software and utilities; large-scale evidence storage; and case management software (See Figure 1). Strong authentication and encryption would be used to ensure the integrity of the evidence. Access would be provided over a high-speed networking infrastructure, Florida LambdaRail (FLR).

FLR is Florida's research and education network that is connected to Internet 2/Abilene Network. The foundation of the FLR is a dense wave division multiplexing (DWDM)-based optical footprint using Cisco Systems' 15454 optical electronic systems with a capacity of 32 wavelengths per fiber pair. Each wavelength can support transmission up to 10 billion bits per second (10 Gbps). On top of the optical infrastructure is built an Ethernet based MPLS transport facility. This provides for Internet, Internet2 and high speed IPv4 and IPv6 transit between participants. Additionally private layer 2 or layer 3 services (VPN) may also be provisioned.

Objective

Our primary objective is to develop a virtual lab that would be accessible by any law enforcement agency, providing them the tools, services, and resources for digital forensics examinations that they would not be able afford on their own. The largest benefit of virtual labs would be for smaller law enforcement agencies, even more so in rural areas, who often have to decide whether to buy ammunition or computers.





Research Partners

We will work with Seminole and Orange County Florida Sheriff's Offices, researchers from the Florida State Florida Cybersecurity Institute, and business/industry partners, researchers from FLRNET.