Third International Workshop on Systematic Approaches to Digital Forensic Engineering

A Research Configuration for a Digital Network Forensic Lab

Jeffrey S. Marean; Mike Losavio, JD; Dr. Ibrahim Imam, PhD.

J. B. Speed School of Engineering

University of Louisville

Louisville, KY 40292

[jsmare01, ibrahim.imam, michael.losavio] @ louisville.edu

Abstract

The digital forensic network lab is implemented with the goal of providing all students and faculty with a configurable research environment ideally suited for conducting network forensic testing on all TCP/IP network protocols passing through it. Of particular interest are protocols that are commonly used for file sharing, message passing, and those that actively obfuscate or encrypt message traffic. Notably, Bit Torrent protocol, P2Pprotocols , IM (instant messaging) protocols, and anonymizing protocols such as I2P, Thor, and Freenet. Items of interest in protocol analysis include packet payload, sender and receiver real IP address, and crypto analysis.

The forensic test bed consists of an A Main Node populated with a Cisco WAN router. This is the master router for the lab. It routes internal traffic between the three research nodes and selected outside networks. Populating the A Node and the two remote Nodes, B and C, are a combination of a Cisco routers, Cisco firewalls, Cisco switches, and computers.

Each node has five dual core X86 computers capable of running combinations of Linux x86-32 or -64 OS's, Microsoft x86-32 or -64 OS's, and, if necessary, both OS's can be configured to either use Microsoft, VMWare or Xen virtualization software.

The A Main Node is connected remotely to the C Node via a campus Fast Ethernet circuit. While the B Node, co-located with the A Main Node, is connected together via a Fast Ethernet and T1 circuit.

To increase the infrastructure component of the lab we have the ability to selectively place the forensic lab into an existing classroom domain for wider access to students and faculty researchers .

Figure 1 show the Digital Forensic Network Lab overview.

978-0-7695-3171-7/08 $25.00 © 2008 IEEE
DOI 10.1109/SADFE.2008.23

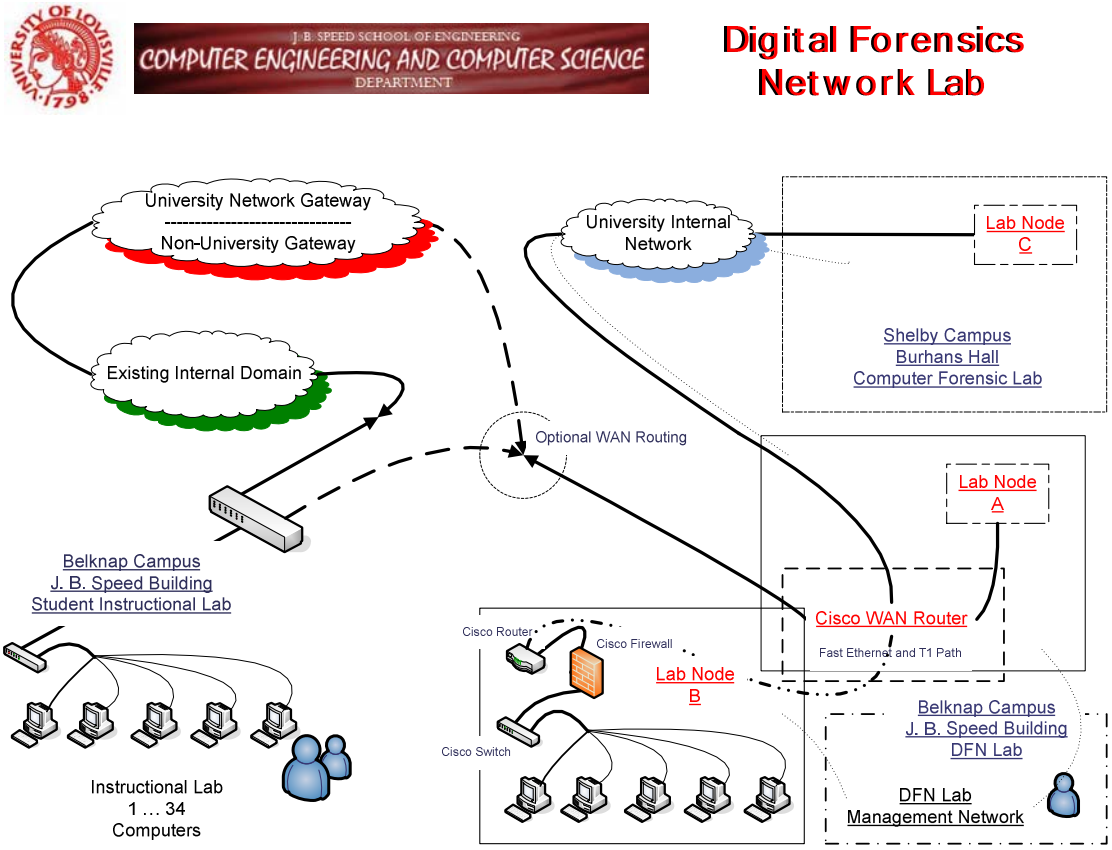

Figure 1 Digital Forensic Network Lab Overview