A Lessons Learned Repository for Computer Forensics

By

Warren Harrison, George Heuston, Mark Morrissey, David Aucsmith, Sarah Mocas, Steve Russelle

Presented At

The Digital Forensic Research Conference

DFRWS 2002 USA Syracuse, NY (Aug 6th - 9th)

A Lessons Learned Repository for Computer Forensics

2002 Digital Forensics Research Workshop

Warren Harrison
David Aucsmith
George Heuston
Sarah Mocas
Mark Morrissey
Steve Russelle

Digital Devices and Forensics

Computer forensics involves the *preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary … analysis* (W.G. Kruse, and J.G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, 2002)

Proliferation of Digital Devices

Digital devices are commonplace in society, and may contain information useful in developing a criminal case

- PDAs
- Cell Phones
- Computers
- USB Flash Cards
- FAX Machines

Digital Forensics and Law Enforcement

- Every new hardware configuration poses a unique challenge to the forensics specialist
- Forensics specialists are stretched thin – case loads seldom allow in-depth research for handling new devices

Learning from Others' Experiences

- We can optimize our effort if we can avoid reinventing the wheel and limit dead ends
- Often someone else may have already encountered the same device or configuration

A Lessons Learned Repository

- Allows past experiences to be shared among a community
- Learn about techniques that worked for someone else, as well as techniques that have not

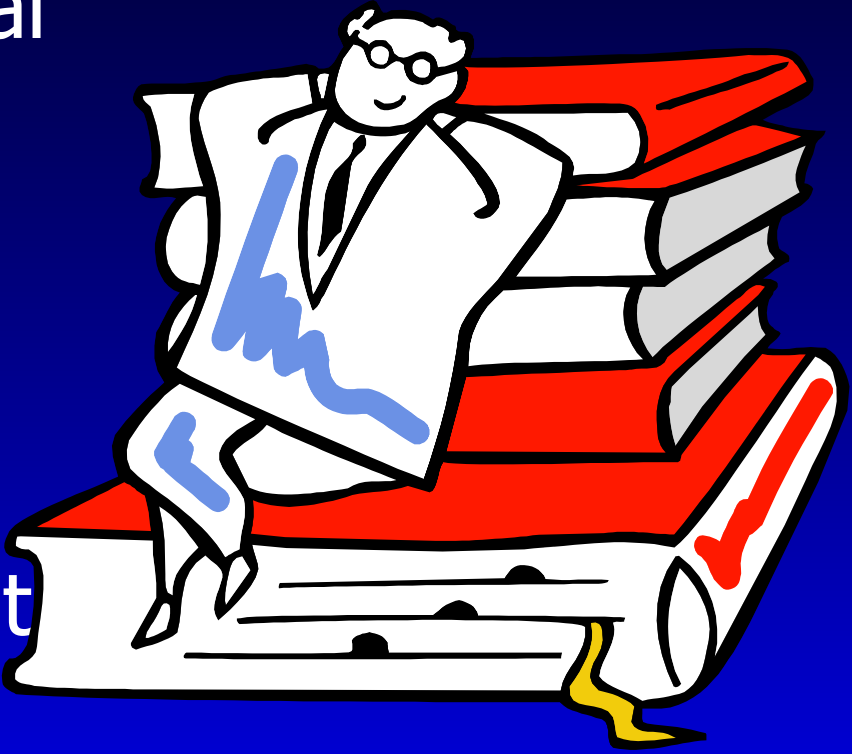
Why Maintain a Lessons Learned Repository?

- The goal of maintaining a Repository of Lessons Learned is:

  broad dissemination of information about experiences that will *discourage the use of work practices that lead to undesirable outcomes* and *encourage the use of work practices that lead to desirable outcomes*

A Lessons Learned Repository is *Not*

- A collection of general best practices
- A set of tutorials
- “How-to” documents
- “Official Guidelines”
- Academic ideas about what *should* work



Attributes of a Lesson

- **Implemented**. The work practice or approach being described must have really been exercised - not just a speculation
- **Applicable**. Lesson phrased generally enough so that it is transferable, yet specific enough to identify a particular action
- **Valid**. The contribution must have a significant impact on some outcome and be factually and technically correct.

Key Issues for the Lessons Learned Repository

- Motivation
  - Motivation of contributors
    - Why go to the trouble to contribute a Lesson?
  - Motivation of users of contributions
    - Why go to the trouble to extract a Lesson?
      - *Lessons are easy to find*
      - *Lessons are useful*
- Examples of repositories of volunteered information exist – Xerox Eureka and Epinions

Xerox Eureka

(http://www.apqc.org/free/casestudies/KM-18.pdf)

- Used by Xerox's service organization
- Over 25,000 repair tips
- Service reps contribute their solutions to undocumented problems
- Tips don't get published until colleagues review them and agree that they will work
- Reps' names associated with each tip – recognition thought to motivate contributions

Epinions

how epinions delivers trust

- Web-based Information Exchange – advice, reviews, opinions, recommendations
- Content is free to user - contributor gets paid by how often contributions are read
- Contributors identified (bio, list of reviews, comments, etc.) so users know who to trust
- "Web of Trust" - network of contributors the user, or people the user trusts, has consistently found to be valuable

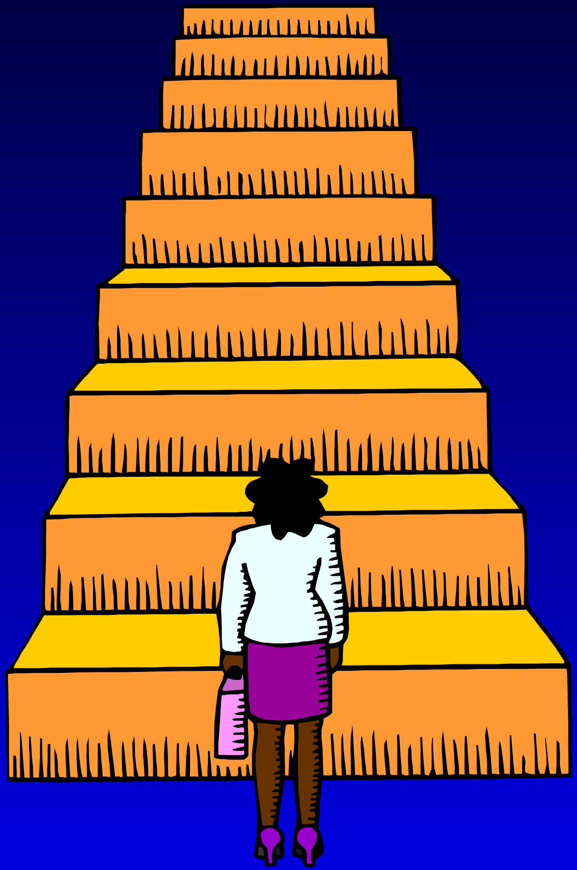
Important Aspects of a Lessons Learned Repository

- Collecting the Lessons
- Storing and Maintaining the Lessons
- Retrieving and Using the Lessons

Collecting the Lessons

- The value of a Lessons Learned Program is a function of how much experience people are willing to contribute
- Users must contribute Lessons that are useful and well-indexed for other users to access

Obstacles to Collecting Lessons

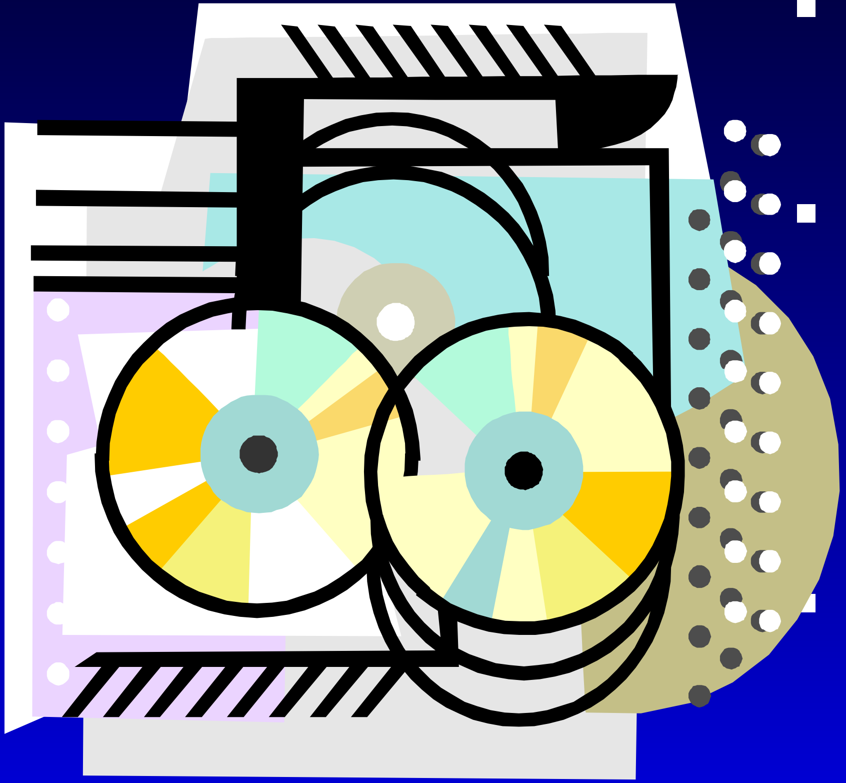


- Getting users to take the time to record a Lesson is a significant impediment
- Useful and consistent indexing will be a challenge – issue of "index sprawl" which reduces usefulness

Retrieving and Distributing the Lessons

- Allow users to quickly retrieve pertinent Lessons
- Do not overwhelm users with inapplicable Lessons
- Convey adequate details for the user to recognize and use a pertinent Lesson
- Ensure user trusts Lessons

Storing and Maintaining the Lessons



- Lessons must be organized for easy access
- Prototype maintains Lessons by Beneficiary, Phase, Classification and Technology
- Lessons are stored as mixed HTML/XML pages - for stand-alone linkage

Repository Policies

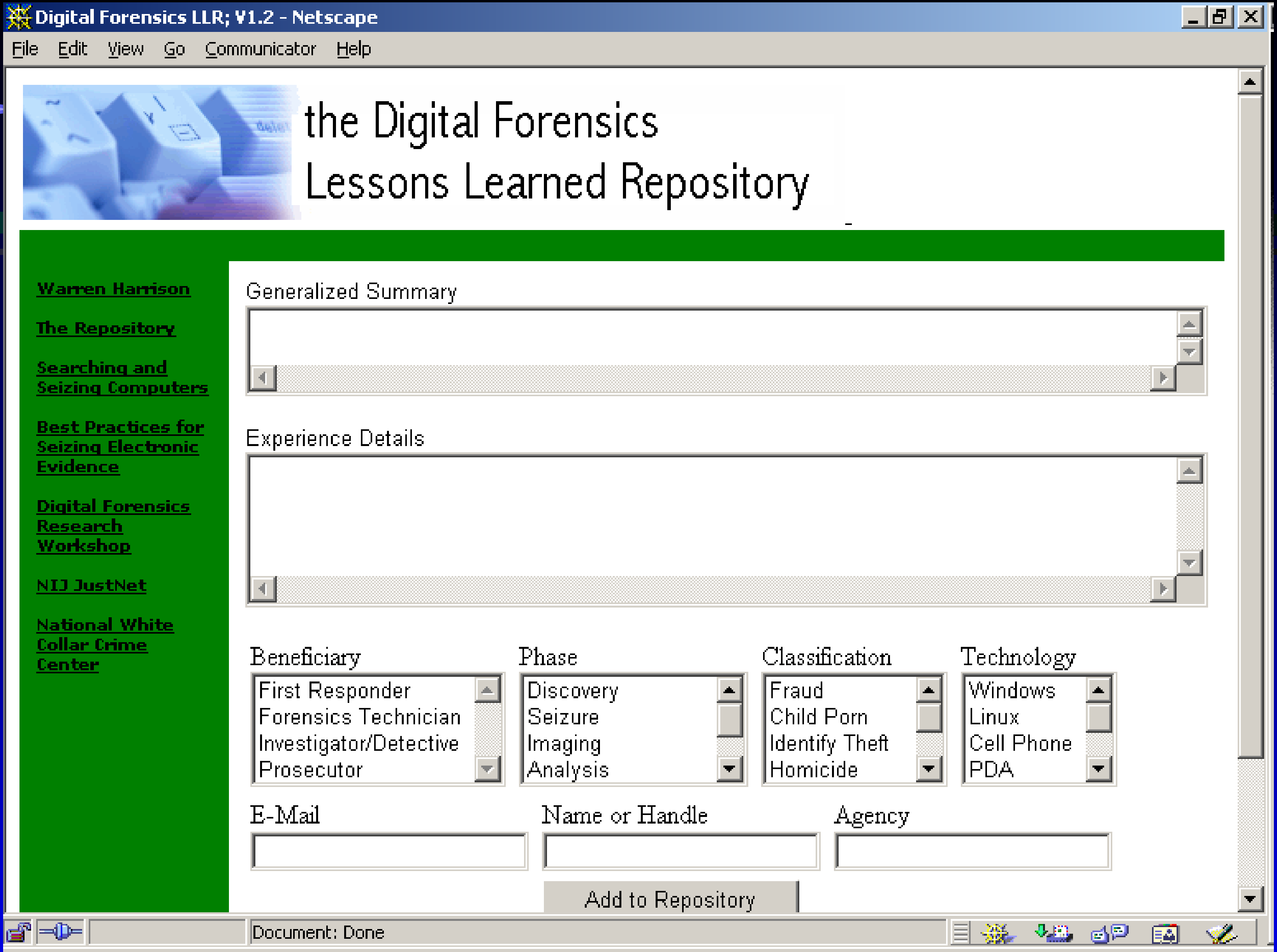
- Who can add a Lesson?
- Who can read a Lesson?
- Who (if anyone) filters Lessons?
- Are contributors anonymous?
- How much does a contributor need to tell us about themselves?

Policies will affect contributions and use

A Prototype Forensics Lessons Learned Repository

- Proof of Concept Prototype
- Illustrates Lesson Collection and Retrieval
- Not ready for “prime time”

http://forensics.LessonsLearnedRepository.org



Digital Forensics LLR; V1.2 - Netscape
File Edit View Go Communicator Help
the Digital Forensics
Lessons Learned Repository
Warren Harrison
The Repository
Searching and Seizing Computers
Best Practices for Seizing Electronic Evidence
Digital Forensics Research Workshop
NIJ JustNet
National White Collar Crime Center
Add to Repository
Document: Done

Generalized Summary

Experience Details

Beneficiary: First Responder, Forensics Technician, Investigator/Detective, Prosecutor

Phase: Discovery, Seizure, Imaging, Analysis

Classification: Fraud, Child Porn, Identify Theft, Homicide

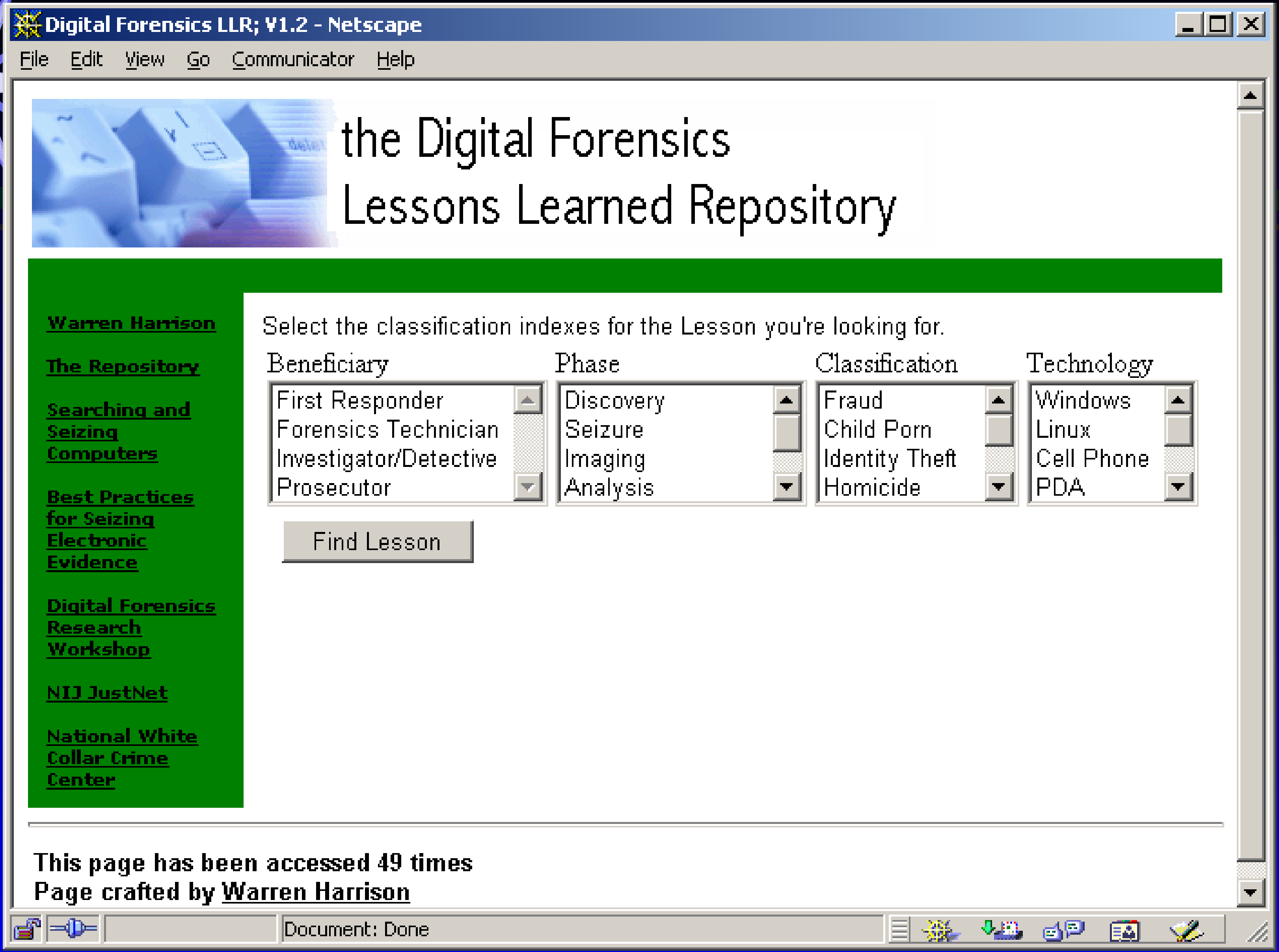
Technology: Windows, Linux, Cell Phone, PDA

E-Mail

Name or Handle

Agency

A Lessons Learned Repository for Computer Forensics



the Digital Forensics Lessons Learned Repository

Warren Harrison

The Repository

Searching and Seizing Computers

Best Practices for Seizing Electronic Evidence

Digital Forensics Research Workshop

NIJ JustNet

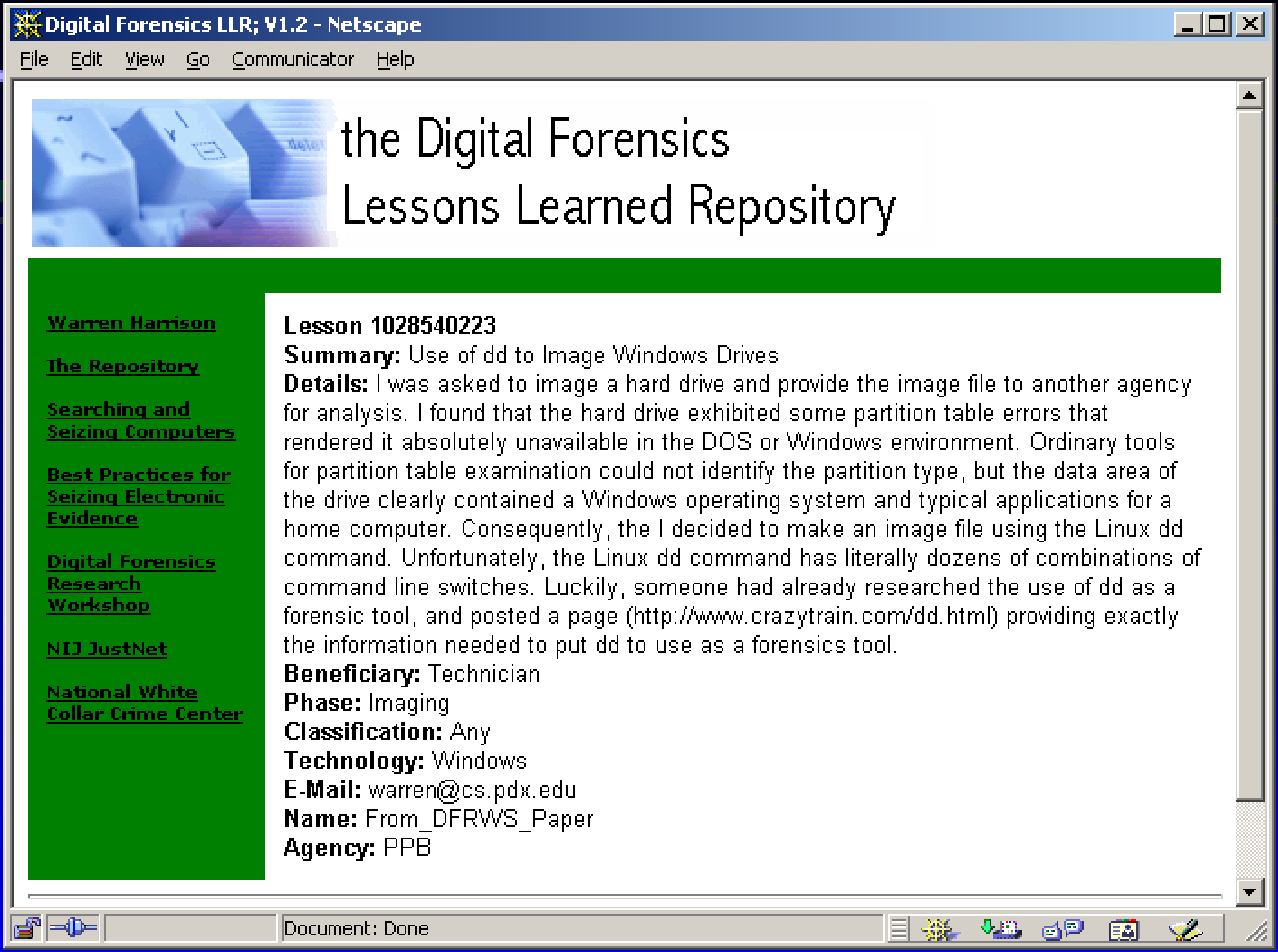
National White Collar Crime Center

Select the classification indexes for the Lesson you're looking for.

Beneficiary	Phase	Classification	Technology
First Responder	Discovery	Fraud	Windows
Forensics Technician	Seizure	Child Porn	Linux
Investigator/Detective	Imaging	Identity Theft	Cell Phone
Prosecutor	Analysis	Homicide	PDA

This page has been accessed 49 times
Page crafted by Warren Harrison

A Lessons Learned Repository for Computer Forensics



the Digital Forensics Lessons Learned Repository

- Warren Harrison
- The Repository
- Searching and Seizing Computers
- Best Practices for Seizing Electronic Evidence
- Digital Forensics Research Workshop
- NIJ JustNet
- National White Collar Crime Center

Lesson 1028540223
Summary: Use of dd to Image Windows Drives
Details: I was asked to image a hard drive and provide the image file to another agency for analysis. I found that the hard drive exhibited some partition table errors that rendered it absolutely unavailable in the DOS or Windows environment. Ordinary tools for partition table examination could not identify the partition type, but the data area of the drive clearly contained a Windows operating system and typical applications for a home computer. Consequently, the I decided to make an image file using the Linux dd command. Unfortunately, the Linux dd command has literally dozens of combinations of command line switches. Luckily, someone had already researched the use of dd as a forensic tool, and posted a page (http://www.crazytrain.com/dd.html) providing exactly the information needed to put dd to use as a forensics tool.
Beneficiary: Technician
Phase: Imaging
Classification: Any
Technology: Windows
E-Mail: warren@cs.pdx.edu
Name: From_DFRWS_Paper
Agency: PPB

Lessons Learned About Lessons Learned

- Multi-year experience with Software Engineering LLRs:
  - We cannot anticipate every possible organizational structure - requires extensibility
  - Lesson matches are rarely binary outcomes - scoring function is important
  - Users will not use an empty Repository - you have to prime the pump

Future Work on LLRs

- technology improvement
- establish public and private Lesson Repositories - priming the pump and soliciting contributions
- experiment with integrating LLR feedback with documented processes
- dealing with incompatible vocabularies