

Final Technical Report

NIJ Support of NCFS Research and Activities (2005-2009)

Digital Evidence Markup Language: An Object-Oriented, XML-based Model for Sharing Computer Crime-related Information

Award Number: 2005-MU-MU-K044
2005-MU-MU-K044 Supplement 1

Dr. J. Philip Craiger, CISSP
Assistant Director for Digital Evidence
National Center for Forensic Science
University of Central Florida
&
Associate Professor
Department of Engineering Technology
Daytona State College

Correspondence regarding this document should be sent to:

Dr. Philip Craiger, CISSP
Assistant Director for Digital Evidence
PO Box 162367
University of Central Florida
Orlando, FL 32816
Email: philip@craiger.net or craigep@daytonastate.edu

Abstract

Experts suggest that technologies that allow disparate law enforcement jurisdictions to share crime-related information will facilitate fighting crime. One of these technologies is the Global Justice XML Data Model (GJXDM: which is now converging with the National Information Exchange Model: www.niem.gov). Global JXDM served as a data reference model for the exchange of information within the justice and public safety communities (NIJ, 2004). The Global JXDM is a product of the Global Justice Information Sharing Initiative's (Global) Infrastructure and Standards Working Group (ISWG) and was developed by the Global ISWG's XML Structure Task Force (NIJ, 2004). One of its limitations at its current level of development is the lack of a “model,” or a method to model, digital evidence. As a solution we developed a prototype model for a digital evidence markup language (DEML). DEML is an extension to GJXDM.

Our prototype model is a schema based on XML that supports the standardization of digital evidence-related artifacts. We developed our model using an object-oriented representation of digital evidence and associated media and technology, relying upon existing and accepted sources (e.g., Best Practices of Seizing Electronic Evidence, U.S. Secret Service, Volume 2, several forensic tool suites, and law enforcement forensic examiners) to identify classes and class properties. We employed the Unified Modeling Language as the basis for a graphic representation of our model. UML supports the creation of class diagrams, which are hierarchical representations of classes, along with associations between classes, their objects, and associated properties. We translated the class diagrams into an XML representation to serve as an

Digital Evidence Markup Language (DEML)

extensible plug-in to GJXDM. This prototypes XML code is hosted on National Information Exchange Model (NIEM) website.

Because the one of the charters of NIJ is to assist local and state law enforcement, we developed our prototype model with practicality in mind, i.e., a model that is easily understood by local and state law enforcement (rather than a purely academic perspective), and is therefore more likely to be employed by forensics examiners, law enforcement, and the courts, as a means to identify and describe digital evidence.

Table of Contents

Abstract	2
Table of Contents.....	4
Executive Summary	5
Introduction.....	8
Problem Statement	9
Existing Literature.....	10
Method	11
Object-Oriented Modeling: An Overview	11
The Unified Modeling Language.....	13
Classes and Objects	14
Results.....	19
Statement of Results	19
Sources for Class and Properties.....	19
A Note about Class Properties.....	22
DEML NIEM Formatted XML Code.....	79
View the XML.....	91
Conclusions	98
Discussion of Findings	98
Implications for Policy and Practice.....	99
Implications for Future Research.....	100
Acknowledgements	101
References and Additional Readings	102
Dissemination of Findings	105

Executive Summary

Technologies that allow justice and public service communities to share crime-related information transparently facilitate fighting crime. One of these technologies is the Global Justice XML Data Model (GJXDM). One of its limitations at its current level of development is the lack of a “model,” or a method to model, digital evidence. As a solution, the National Center for Forensic Science, using experts in psychology, computer science, law enforcement, information technology, and modeling, developed a prototype model for digital evidence we call the digital evidence markup language (DEML), an extensible plug-in to Global JXDM. Global JXDM serves as a data reference model for the exchange of information within the justice and public safety communities (NIJ, 2004). The Global JXDM is a product of the Global Justice Information Sharing Initiative's (Global) Infrastructure and Standards Working Group (ISWG) and was developed by the Global ISWG's XML Structure Task Force (NIJ, 2004). (Note that at the current time GJXDM is converging with the National Information Exchange Model: www.niem.gov).

Our prototype DEML model is a schema based on XML that supports the standardization of the description of digital evidence-related artifacts. XML is, simply, a means of organizing and structuring text by applying tags to various properties/fields. We developed a prototype model using an object-oriented representation with the Unified Modeling Language (www.uml.org). UML is a language to visualize and construct models as represented in a class-object hierarchy. UML is most commonly used in software engineering as a means of designing and visualizing software. The

figure below is a high-level class diagram describing simple relationships and associations between common digital evidence elements.

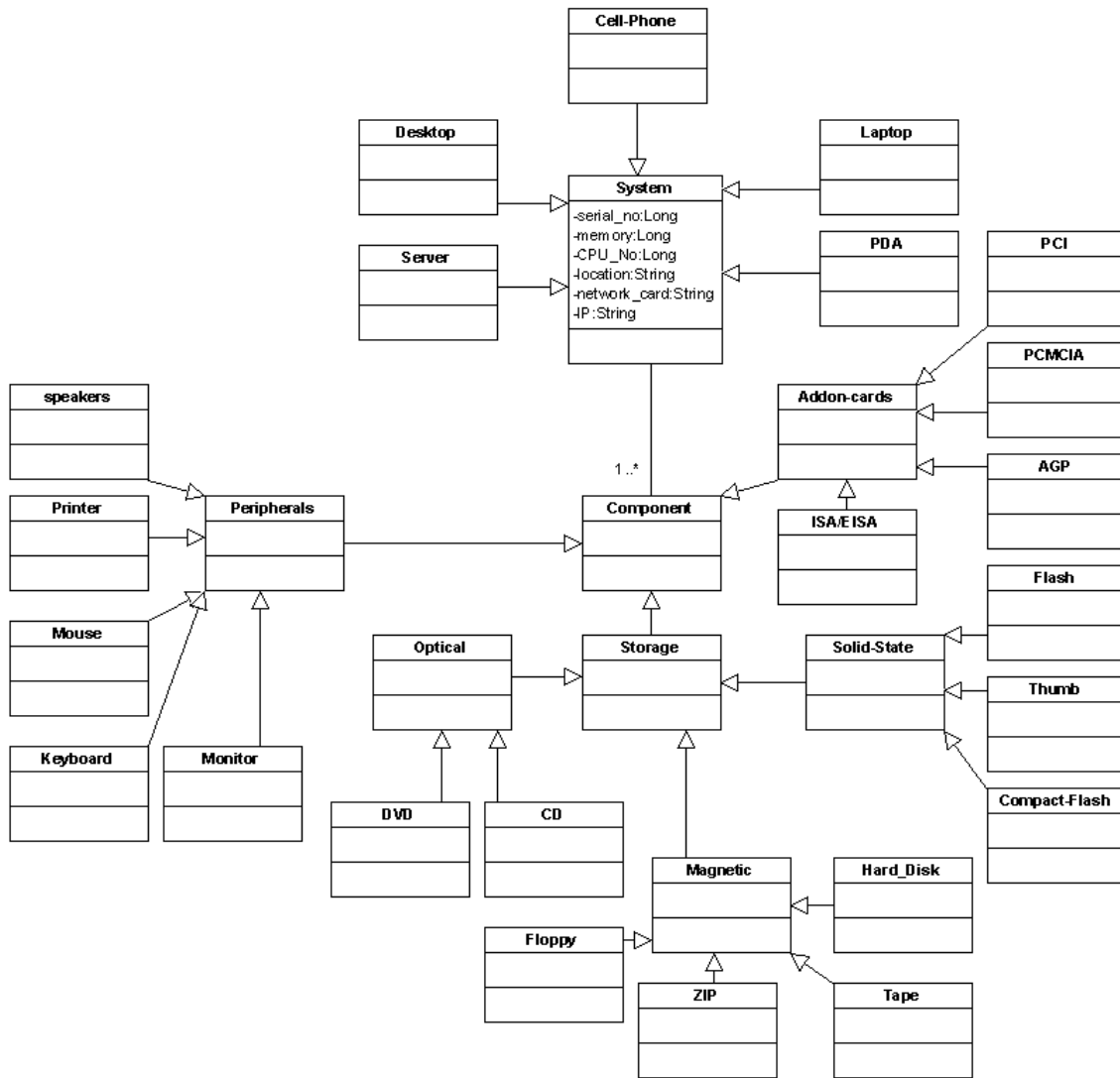


Figure 1. Class diagram of a digital evidence (high-level: draft version)

The classes used to compose our model were extracted from several sources, including *Best Practices of Seizing Electronic Evidence, U.S. Secret Service, Volume 2* for physical class objects (media, types of computers, computer components, etc.), 24 popular forensic tool suites (commercial as well as open source) for data file objects

Digital Evidence Markup Language (DEML)

and associated properties, and several select law enforcement forensic examiners to provide feedback on our model.

We subsequently translated our DEML class diagram into an XML representation using the National Information Exchange Model (and hosted on its website: www.niem.gov). Because the one of the charters of NIJ is to assist local and state law enforcement, we developed our prototype model with *practicality* in mind, i.e., a model that is easily understood by local and state law enforcement, rather than a purely academic, theoretical perspective. A practical model is more likely to be employed by forensics examiners, law enforcement, and the courts, as a means to identify, describe, and share information related to digital evidence-related crimes.

Introduction

A byproduct of the growth of information technology has been in ‘computer-related crime.’ Forensic evidence at a crime scene once limited to physical items and attributes (physical evidence: carpet fibers, tool marks, fingerprints), and biological matter (biological evidence: hair, blood, saliva) now often includes digital evidence.

In 1999, the Scientific Working Group on Digital Evidence (www.swgde.org) defined digital evidence as:

“Information of probative value stored or transmitted in binary form.”

Examples of digital evidence include common application files (word processing, spreadsheets, etc.), graphical files, audio and video recordings and files, server logs, and application executables.

Forensics, or forensic science, is the application of science to questions that are of interest to the legal system. As such, digital forensics is the analysis of computers and other types of digital media to determine if (it) they have been used for illegal or unauthorized activities, or are the “victims” of illegal attacks. Business and industry use digital forensics to gather information within their own businesses regarding intellectual property theft, fraud, network and computer intrusions, and unauthorized use of computers and other digital media including fax machines, answering machines, personal data assistance, cell phones, etc., for employee removal, and both civil and criminal litigation. Law enforcement agencies use digital forensics to gather digital evidence for a variety of crimes including child pornography, fraud, terrorism, extortion, cyberstalking, money laundering, forgery, and identity theft. The military and

government intelligence agencies use digital forensics to gather intelligence information from computers captured during military actions.

Problem Statement

Technologies that allow justive and public service organizations in different jurisdictions to share crime-related information facilitate fighting crime. Information sharing among jurisdictions requires a common, structure “language” for representing this information. Unfortunately, there exists no common language to share digital evidence-related crime information.

The goal of this research was to develop a representational scheme for digital evidence that can be used as the basis for information sharing among multiple agencies and jurisdictions. We call this schema the digital evidence markup language (DEML). DEML will serve as a plug-in to Global JXDM (which is now converging with the National Information Exchange Model, NIEM). Global JXDM is a data reference model for the exchange of information within the law enforcement and justice communities, and is a product of the Global Justice Information Sharing Initiative's Infrastructure and Standards Working Group (NIJ, 2004).

DEML is an XML-based schema providing a standardized means of representing of computer crime-related materials, i.e., digital evidence. An XML schema, using the National Information Exchange format, allows our prototype model to be extensible and flexible, a desirable property for models based on real world artifacts. Technology changes will require continual changes in the representational scheme to appropriately model changes in the technologies used in computer-related crime. For instance, since we first began this research, crimes have been committed with computer technology

that, until then, had not been used in such a manner (e.g., game consoles), as well as newer technology that did not exist when we started this research (e.g., plug computers). Consequently, it is clear that any model must be able to be easily extended through the addition of new technology and its associated properties.

Existing Literature

At the time this research was performed there was no published ‘research’ on a ‘common language’ for describing and disseminating information related to digital evidence. Therefore this is a new area of research, at least with respect to digital evidence. The personnel working on this research have diverse educational and research backgrounds, including psychology, computer science, engineering, computer forensics, information technology, and law enforcement. For this research we borrowed concepts from each of these fields in order to develop our prototype DEML model.

The best literature regarding digital evidence was produced by the Scientific Working Group on Digital Evidence (www.swgde.org). SWGDE is an organization composed of law enforcement agencies whose focus is on the practice of digital evidence forensics primarily in the laboratory setting (Pollitt, 2003). The original composition of SWGDE included Federal crime lab directors. Later membership included many agencies from state and local law enforcement. SWGDE’s definition of digital evidence encompasses, what we call “digital artifacts” only, that is, the bits and bytes stored on optical or magnetic media that define what we typically think of as ‘files’ or ‘software.’ By definition this excludes certain computer crime-related “objects” that might be important to law enforcement for use in arrests and subsequent prosecutions. Although these objects are used to create, store, and process digital artifacts, they do

not fall under the definition of digital evidence as proposed by SWGDE. For instance, the hardware a criminal uses in the execution of a crime is often seized at the time of arrest and used as evidence in court against the suspect; however, the hardware itself is not encompassed by SWGDEs definition of digital evidence. It is crucial that any representational scheme used to model digital evidence should be able to model any form of information that may be used by law enforcement for arrest or prosecution purposes. For this reason our model will include not only those artifacts that fall under SWGDEs definition of digital evidence, but also any other objects or processes that may be of value to law enforcement. For the purposes of this paper our definition of digital evidence will no only include digital artifacts (files, software) but also any hardware or procedures used in the creation, storage, or transmission of these digital artifacts.

Method

Object-Oriented Modeling: An Overview

Object-orienting modeling (OOM) is a concept commonly employed in computer science as a means of representing real-world artifacts and processes in programming code, typically used by software engineers in the design of code and code modules. We selected an object-oriented representation as the basis for modeling digital evidence for two reasons. The first is that we are modeling real-world artifacts and processes that are essentially composed of real-world *artifacts* (workstations, printers, cables, files, etc.). In OOM these objects are called ‘classes,’ which are abstract types. In turn, classes can be composed of other classes or abstract types. For instance, workstations are composed of objects -- motherboards, add-on cards, RAM, storage devices, human

interface devices, etc. -- each of which is composed of other classes. An object-oriented representation will allow us to use the powerful concepts of composition and inheritance to represent both hardware and digital artifacts in a flexible and extensible manner.

Classes have properties that are inherited by its subclasses. For example, the “Workstation” class has as properties (as a simple illustration):

```
Class Workstation
  Superclass: Computer
  Property: Serial Number: Numeric
  Property: Manufacturer: AlphaNumeric
  Property: Has-DVD?: Boolean
  Property: Has-NIC?: Boolean
  Property: RAM: Numeric
  Property: #-HDs: Numeric
  Property: HD-size:Numeric
```

In turn, subclasses are classes that inherit properties from a superclass. For example, the computer on which I’m typing is an Apple iMac, which is a subclass of Workstation.

```
Class Apple
  Superclass: Workstation
```

Note that properties are not listed under the subclass `Macintosh` because it is a subclass of `Workstation`, and therefore it inherits its superclass’s properties. Only properties that are unique to the subclass would be included in that subclass.

In object-oriented nomenclature, an *object* is an instance that represents a real, tangible entity (in our work). For example, the computer on which this report is typed would be modeled as:

```
Object: Philip’s Computer
      Superclass:      Apple
```

Digital Evidence Markup Language (DEML)

```
Version:                iMac
Serial Number:          QP8181HPPT0KM
Property: Has-DVD? :    Y
Property: Has-NIC?:    Y
Property: RAM:          4GB
Property: #-HDs:        1
Property: HD-size:      1TB
```

An object-oriented representation using UML allows us to use a common, mature methodology to model real-world objects in a way that is very straightforward, not to mention that there are numerous tools to facilitate model creation.

The second reason for an object-oriented representation is the need to develop and maintain an extensible and flexible schema. New technologies will be developed, and the diversity of technologies will increase. A schema built upon an object-oriented representation will support the modeling of new and diverse technologies by simply developing new classes (for diverse technologies) or inheritance (inclusion of new technologies built upon old technologies).

In OOM it is important to model the real-world objects, but it is also important that the representation reflects our subject matter experts (in this case, law enforcement) perceptions of digital evidence. Thus, our design is at least partially guided by members from the U.S. Secret Service as well as the U.S. Secret Services “Best Practices for Seizing Electronic Evidence” (Volume 2), by the tools law enforcement uses, as well as perceptions from select individuals from law enforcement.

The Unified Modeling Language

An object-oriented model requires some form of graphical modeling tool in order to display the relationships between different elements of the model, for instance, i.e., how does one represent the relationship between a computer, network interface card,

an Ethernet cable, and an IP address (all of which may be important evidence in a crime)? We have chosen to use UML 2.0 (Unified Modeling Language: OMG Group, www.omg.org) to visually represent our model because of the flexibility of UML for modeling, and because of our experience in working and teaching UML to computer science students. Before discussing UML, we first describe the components of an OO model.

Classes and Objects

A *class* is a construct that is used as an abstract template. An example of a class is *computer*. The class *computer* is an abstract concept that has certain properties, such as static storage, dynamic memory, a processor, and input/output capabilities (among others). Classes can have subclasses, which are more specific (yet abstract) instances of their super classes. For instance, *PCs*, *Macintoshes*[™], *smart phones*, *PDA*s, and *game consoles* are sub classes of the class *Computer*. We sub divide classes because some of have different attributes and properties than others. These more specific sub divided classes are called ‘subclasses,’ and they inherit the properties of their superclass. Inheritance of properties is described below.

An object is an *instance*, or instantiation, of a class. For example, a MacPro[™] laptop (Class:Macintosh), iPhone[™](Class:Smart_Phone), Palm V[™] (Class:PDA), Wii[™] console, (Class:Game_console) or Dell Optiplex[™] (Class:PC) workstation are tangible objects, each of which inherits properties from its associated sub classes listed above. Note that objects inherit properties of all their superset class, i.e., all instances of a class (all objects) belonging to the class of computer have storage, processor, I/O, etc.

A class diagram allows us to display the relationships between different classes in a visual manner. To illustrate a class diagram, our initial two top-tier objects consisted of hardware and digital artifacts (see Figure 2 below).

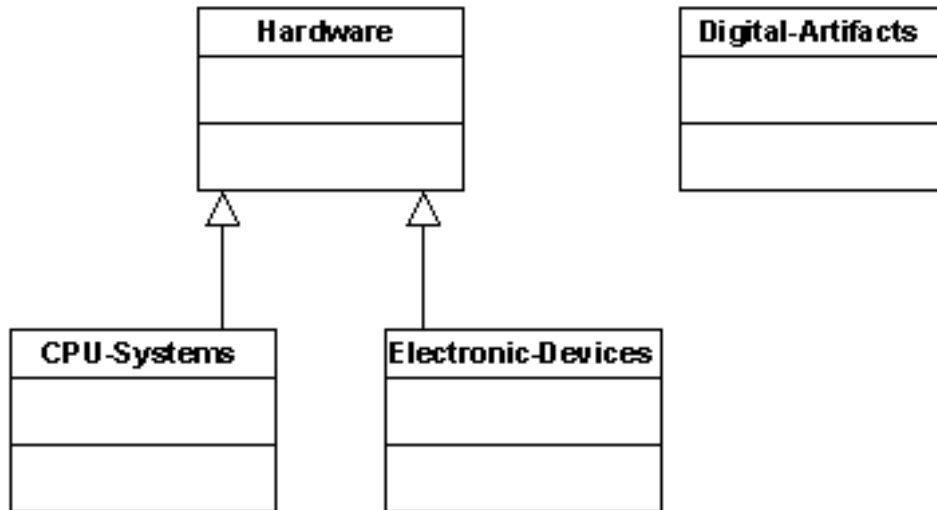


Figure 2. Superclasses for DEML Objects

Figure 2 visually indicates that hardware is composed of two subclasses: CPU-systems and electronic devices. Although it could be argued that this distinction is artificial, we based our decision to separate the two on the *US Secret Services Search and Seizure Guidelines, version 2* (which was up-to-date at the time of this research. Version 3 is now available).

The second super class, as defined in SWGDE’s definition of digital evidence, is the *digital artifact*. A digital artifact is composed of the bits and bytes that constitute what we normally think of as files stored on optical or magnetic media. A digital artifact can be partitioned into two subclasses: `Files` and `slack space` (see Figure 3). The class `Files` can also be partitioned into those that found in `allocated space`, and those in `unallocated space`. Craiger (2005) defined these as:

1. Allocated space is composed of clusters allocated to a file and that are tracked by the file system.

2. Unallocated space is composed of clusters not in use by a file. Unallocated space may contain residual information, e.g., from deleted files.

3. Slack space “is the space left over between the end of the data and the end of the last cluster or block” (Kruse & Heiser, p. 75, 2002). Slack space may contain residual information, e.g., from files previously deleted but which have been partially overwritten.

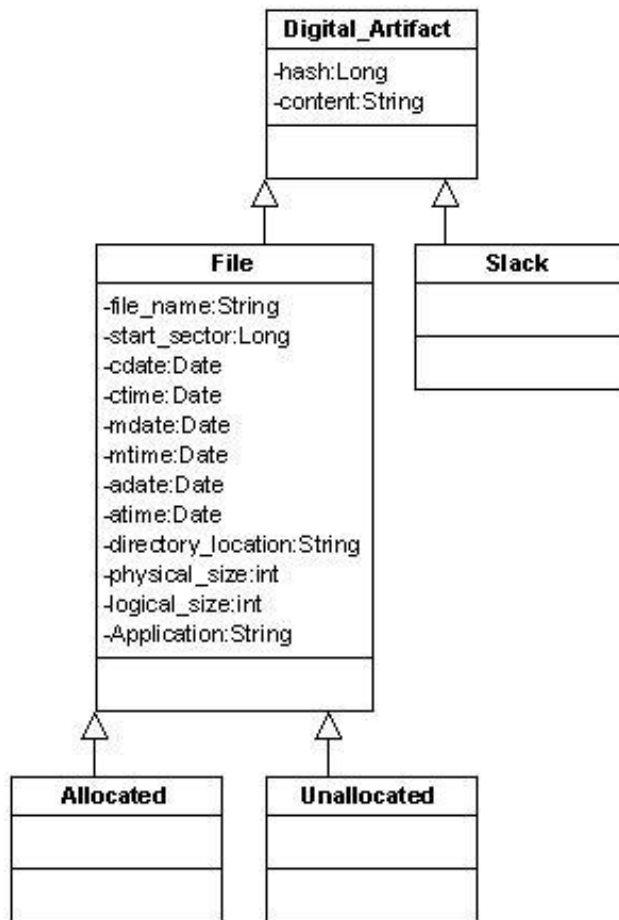


Figure 3. Class Diagram Showing Inheritance Relationships for Digital Artifacts

We can create a class diagram with inheritance links to indicate super and subclass relationships. Figure 4 is a draft example class diagram for our DEML.

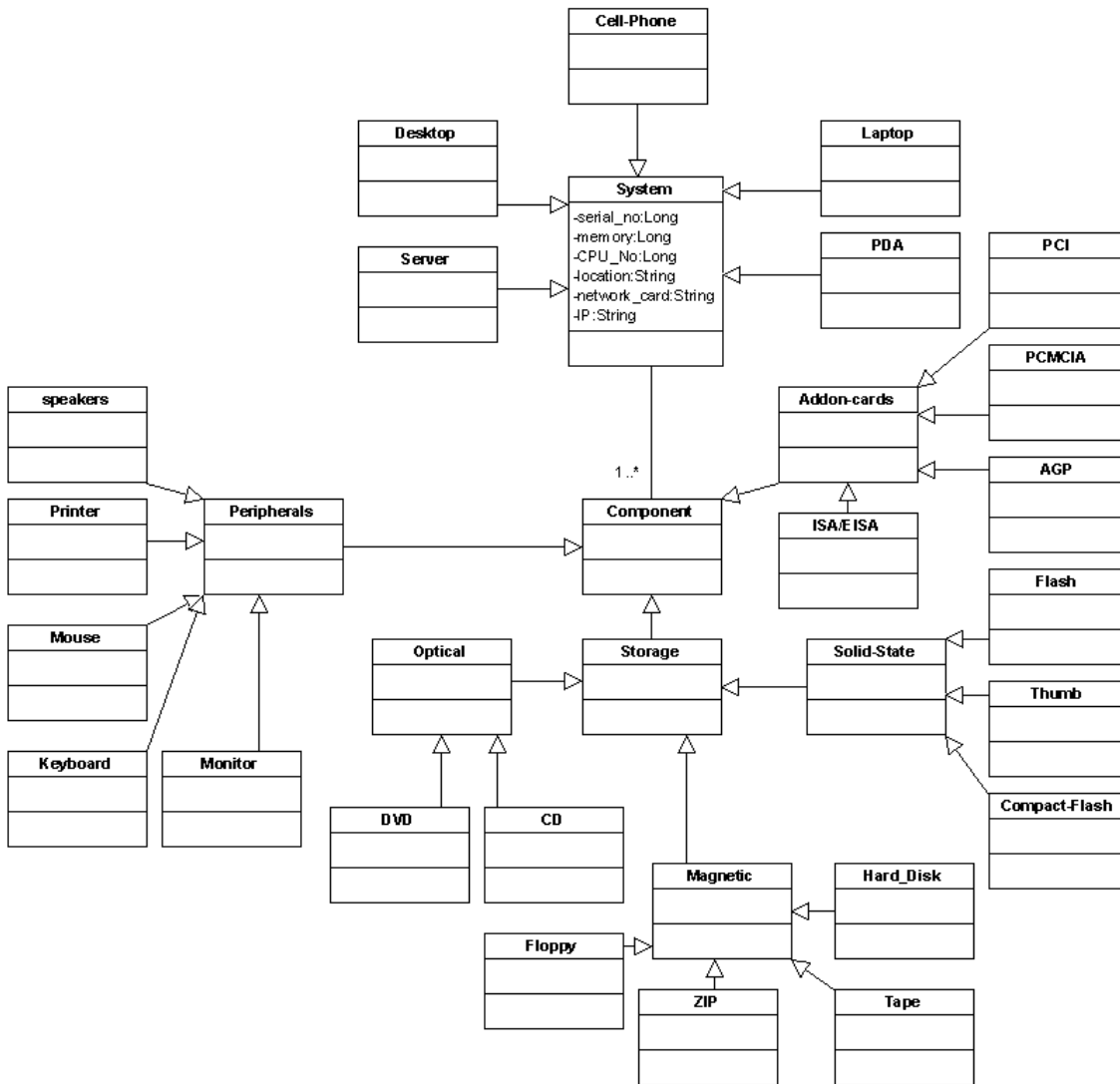


Figure 4. Class Diagram Showing Inheritance Links (Early version)

In this class diagram, the “System” is the superclass of subclasses `Server`, `PDA`, `Workstation`, `Laptop`, etc. Inheritance is indicated by a one sided arrow. In turn, the class `System` is composed of multiple components (as indicated by the line with no arrows). In turn, the “Component” class is the superclass of `Peripherals`,

Digital Evidence Markup Language (DEML)

Storage, Magnetic_Media, and so on. In this example, only the superclass `System` is shown to have properties (for simplicities sake).

Results

Statement of Results

Below we describe the results of our OO modeling. We describe how we identified class and properties, including sources used for the identification of relevant classes. Due to the extensive nature of the results (the model is quite large), we include a class diagram that depicts a global view of the model, followed by the XML code that represents our results at a detailed level, essentially our entire model in XML. The detail information includes the classes composing the model, class properties, and class associations. We also list the universal set of class properties we reviewed as extracted from over 24 digital forensic tools (commercial and open source).

Sources for Class and Properties

An important part of the modeling process is selection of classes and properties that compose the model. With the goal of developing a practical model (versus a theoretical/academic model), we selected sources commonly used by forensic examiners for the class/property information. For physical classes we used the U.S. Secret Service's *Best Practices of Seizing Electronic Evidence, Version 2*, which contains extensive information on possible sources of digital evidence (multitude of computer/electronic devices, numerous types of physical media, etc.). We supplemented this information, particularly on properties, through our own experts in information technology and computer science.

For data files and their associated properties we identified several popular commercial forensic tool suites and as well as open source tools and extracted

information on the data properties identified in these tools. Based on our survey we recently conducted for a separate research project, we found that the most common forensic tool suites indicated by forensic examiners completing the survey were Guidance Software's Encase and AccessData's Forensic Tool Kit. Based on our survey and previous experience/training we are secure in our decision that universe of properties is fairly well represented in the tools included in this research.

The tools we selected for an initial review including the following:

- Commercial Tools
 - EnCase Forensic edition ver. 5.x
 - EnCase Forensic edition ver. 6.x
 - AccessData FTK ver. 1.62.1 build 06.06.27
 - AccessData Password Recovery Toolkit 6, v6.2 Build 06.05.01
 - AccessData Registry Viewer, v1.4a
- Open Source Tools
 - Autopsy ver. 2.06 (TSK ver. 2.03)
 - 2Hash
 - bMap ver. 1.0.20
 - MAC_Grab.pl
 - Helix ver. 1.7 - Windows Live Preview Interface
 - WFT ver 2.0.00
 - FRED v1.4 for Helix
 - SecReport v3.02.10
 - Root Kit Revealer v1.7, SysInternals
 - MessenPass v1.04, NirSoft
 - Protected Storage PassView v1.62, NirSoft
 - RegScanner v1.20, NirSoft
 - IEHistoryView v1.30, NirSoft
 - IECookiesView v1.70, NirSoft

Digital Evidence Markup Language (DEML)

- Mail PassView v1.32, NirSoft
- Network Password Recovery v1.02, NirSoft
- Asterisk Logger v1.02, NirSoft
- MozillaCookiesView v1.11, NirSoft
- Adepto 1.0

We subsequently selected a subset of the universe of data file properties based upon several factors, including how often they were included in the various tools, and personal experience. We then used the resulting classes and properties to create a class diagram in UML, as depicted in Figure 5 below.

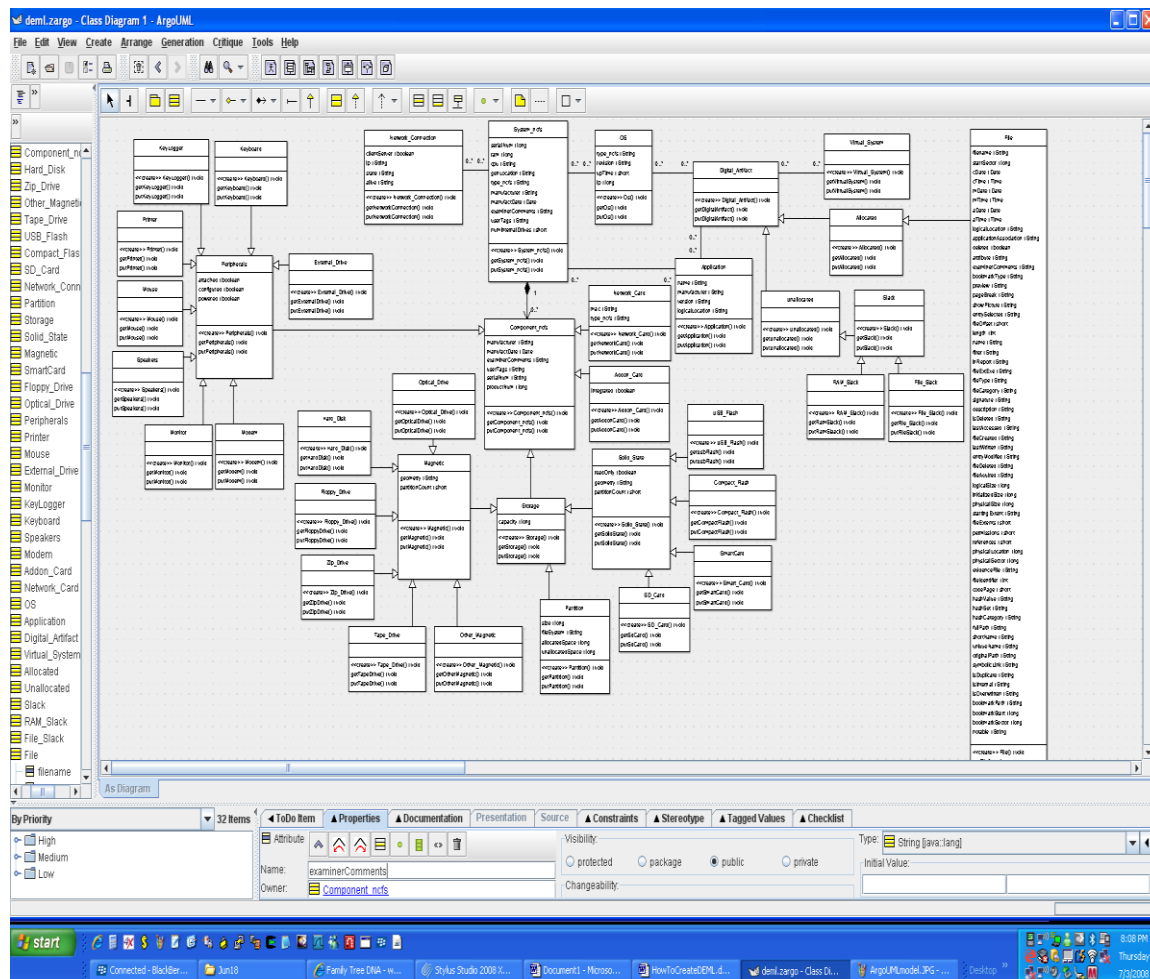


Figure 5. DEML in UML

The class diagram is so large that it's difficult to view it in its entirety, while still being able to view each class's properties. The best means of viewing the model is through viewing the XML code that is generated by the UML tool used to create the class diagram. You will find this code in its entirety below.

A Note about Class Properties

As described above, we identified class properties for model inclusion by reviewing the data file properties used in several commercial and open source tools, as well as through our personal experience. It was important to consider tools used for both Windows and Linux operating systems (technically, Linux is a kernel only) as their file systems each contain unique information not contained in the other. For instance, Linux-based files systems (EXT 2/3/4, ReiserFS, UFS, HFS+, etc.) and Windows-based file systems (e.g., FAT, NTFS) represent files somewhat differently, and therefore may have unique properties that do not overlap with other file systems. It is important to include multiple representations in our model.

We took this universal set of properties and selected those that appeared across multiple tools, or those that we deemed as relevant based on our experience. The universal set of class properties, along with the forensic tools from which they were extracted, appears below in Table 1. Note that we include information on the tool, the fields (what will become class and object properties in our model), as well as the "type" (as used in Computer Science) of the property (string, alphanumeric, numeric, Boolean, etc.).

ver. 6.x

File fields

Comment	AlphaNumerical
Bookmark Type	AlphaNumerical
Preview	AlphaNumerical
Comment	AlphaNumerical
Page Break	AlphaNumerical
Show Picture	AlphaNumerical
Entry Selected	AlphaNumerical
File Offset	Numerical
Length	Numerical
Name	AlphaNumerical
Filter	AlphaNumerical
In Report	AlphaNumerical
File Ext exe	AlphaNumerical
File Type	AlphaNumerical
File Category	AlphaNumerical
Signature	AlphaNumerical
Description	AlphaNumerical
Is Deleted	AlphaNumerical
Last Accessed	AlphaNumerical
File Created	AlphaNumerical
Last Written	AlphaNumerical
Entry Modified	AlphaNumerical
File Deleted	AlphaNumerical
File Acquired	AlphaNumerical
Logical Size	Numerical
Initialized Size	Numerical
Physical Size	Numerical
Starting Extent	AlphaNumerical

Digital Evidence Markup Language (DEML)

File Extents	Numerical
Permissions	Numerical
References	Numerical
Physical Location	Numerical
Physical Sector	Numerical
Evidence File	AlphaNumerical
File Identifier	Numerical
Code Page	Numerical
Hash Value	AlphaNumerical
Hash Set	AlphaNumerical
Hash Category	AlphaNumerical
Full Path	AlphaNumerical
Short Name	AlphaNumerical
Unique Name	AlphaNumerical
Original Path	AlphaNumerical
Symbolic Link	AlphaNumerical
Is Duplicate	AlphaNumerical
Is Internal	AlphaNumerical
Is Overwritten	AlphaNumerical
Bookmark Path	AlphaNumerical
Bookmark Start	Numerical
Bookmark Sector	Numerical
Notable	AlphaNumerical
File Extents	
Start Sectors	Numerical
Sectors	Numerical
Start Byte	Numerical
bytes	Numerical
Start Cluster	Numerical
Clusters	Numerical

Digital Evidence Markup Language (DEML)

Permissions

Name	AlphaNumerical
Id	AlphaNumerical
Property	Alpha
Permissions	AlphaNumerical

References

Name	AlphaNumerical
Path	AlphaNumerical

EnCase Forensic edition
ver. 5.x

File fields

Comment	AlphaNumerical
Bookmark Type	AlphaNumerical
Preview	AlphaNumerical
Comment	AlphaNumerical
Page Break	AlphaNumerical
Show Picture	AlphaNumerical
Entry Selected	AlphaNumerical
File Offset	Numerical
Length	Numerical
Name	AlphaNumerical
Filter	AlphaNumerical
In Report	AlphaNumerical
File Ext exe	AlphaNumerical
File Type	AlphaNumerical
File Category	AlphaNumerical
Signature	AlphaNumerical
Description	AlphaNumerical
Is Deleted	AlphaNumerical
Last Accessed	AlphaNumerical

Digital Evidence Markup Language (DEML)

File Created	AlphaNumerical
Last Written	AlphaNumerical
Entry Modified	AlphaNumerical
File Deleted	AlphaNumerical
File Acquired	AlphaNumerical
Logical Size	Numerical
Physical Size	Numerical
Starting Extent	AlphaNumerical
File Extents	Numerical
Permissions	Numerical
References	Numerical
Physical Location	Numerical
Physical Sector	Numerical
Evidence File	AlphaNumerical
File Identifier	Numerical
Hash Value	AlphaNumerical
Hash Set	AlphaNumerical
Hash Category	AlphaNumerical
Full Path	AlphaNumerical
Short Name	AlphaNumerical
Unique Name	AlphaNumerical
Original Path	AlphaNumerical
Symbolic Link	AlphaNumerical
Is Duplicate	AlphaNumerical
Bookmark Path	AlphaNumerical
Bookmark Start	Numerical
Bookmark Sector	Numerical
Excluded	AlphaNumerical
Hit Deleted	AlphaNumerical
Notable	AlphaNumerical

Digital Evidence Markup Language (DEML)

File Extents

Start Sectors	Numerical
Sectors	Numerical
Start Byte	Numerical
bytes	Numerical
Start Cluster	Numerical
Clusters	Numerical

Permissions

Name	AlphaNumerical
Id	AlphaNumerical
Property	Alpha
Permissions	AlphaNumerical

References

Name	AlphaNumerical
Path	AlphaNumerical

AccessData FTK ver. 1.62.1 build 06.06.27

Date

FTK Version Number	AlphaNumerical
Case Number	AlphaNumerical
Case Location	AlphaNumerical
Case Description	AlphaNumerical
Report Created	AlphaNumerical
Forensic Examiner	AlphaNumerical
Agency Address	AlphaNumerical
Phone	AlphaNumerical
Fax	AlphaNumerical
E-Mail	AlphaNumerical
Comments	AlphaNumerical
Investigator	AlphaNumerical
Agency	AlphaNumerical

Digital Evidence Markup Language (DEML)

Address	AlphaNumerical
Phone	AlphaNumerical
Fax	AlphaNumerical
E-Mail	AlphaNumerical
Comments	AlphaNumerical
Date	
Evidence Items	
Evidence Items	Numerical
File Items	
Total File Items	Numerical
Flagged Thumbnails	Numerical
Other Thumbnails	Numerical
File Status	
KFF Alert Files	Numerical
Bookmarked Items	Numerical
Bad Extension	Numerical
Encrypted Files	Numerical
From E-Mail	Numerical
Deleted Files	Numerical
From Recycle Bin	Numerical
Duplicate Items	Numerical
OLE subitems	Numerical
Flagged Ignore	Numerical
KFF Ignorable	Numerical
Data Carved Files	Numerical
File Category	
Documents	Numerical
Spreadsheets	Numerical
Databases	Numerical
Graphics	Numerical

Digital Evidence Markup Language (DEML)

E-Mail Messages	Numerical
Executables	Numerical
Archives	Numerical
Folders	Numerical
Slack/Free Space	Numerical
Other Known Type	Numerical
Unknown Type	Numerical
Date	
Display Name	AlphaNumerical
Evidence File Name	AlphaNumerical
Evidence Path	AlphaNumerical
Identification Name/Number	AlphaNumerical
Evidence Type	AlphaNumerical
Added	AlphaNumerical
Children	Numerical
Descendants	Numerical
Comment	AlphaNumerical
<Actual Files Listed>	
Case Log	
<Various settings>	
All Items	
<Tree Structure of Evidence>	
File Listing database	
<AccessDatabase.mdb>	
All Items	
Date	
Report file timezone	AlphaNumerical
File	AlphaNumerical
Full Path	AlphaNumerical
Alias	AlphaNumerical

Digital Evidence Markup Language (DEML)

Extension	AlphaNumerical
File Type	AlphaNumerical
Category	AlphaNumerical
Subject	AlphaNumerical
Created	Short Date and Time
Modified	Short Date and Time
Accessed	Short Date and Time
Logical Size	Numerical
Physical Size	Numerical
Children	Numerical
Descendants	Numerical
Encrypted	?
Deleted	Boolean-Alpha
Recycled	?
Carved	?
Indexed	AlphaNumerical
Sector	Numerical
Cluster	Numerical
Alternate Name	?
Duplicate	?
Read Only	?
System	?
Hidden	?
Item Number	Numerical
Compressed	?
KFF	AlphaNumerical
Bad Extension	?
Emailed	?
Header	AlphaNumerical
MD5	AlphaNumerical

Digital Evidence Markup Language (DEML)

SHA1	AlphaNumerical
Hash Set	AlphaNumerical
Email Date	?
From	?
To	?
CC	?
Attachment Info	?
Exported as	AlphaNumerical

Contents

<Actual bookmark name>

Date	
Report file timezone	AlphaNumerical
Name	AlphaNumerical
Comment	AlphaNumerical
File Count	Numerical
Selected Text	AlphaNumerical

<File Properties>

Date	
<Actual graphic image with actual evidence path>	

AccessData Password Recovery Toolkit 6, v6.2 Build 06.05.01

	Numerical
	Short Date and Time, 24hr
	AlphaNumerical
	AlphaNumerical
<Full path and file>	AlphaNumerical
Job Information	
Attack Type	AlphaNumerical
Module	AlphaNumerical
Profile	AlphaNumerical

Digital Evidence Markup Language (DEML)

Status	AlphaNumerical
Difficulty	AlphaNumerical
Begin Time	Short Date and Time, 24hr
End Time	Short Date and Time, 24hr
Decryptable	AlphaNumerical
Result Type	AlphaNumerical
Results	AlphaNumerical
Comments	AlphaNumerical

File Information

Filename	AlphaNumerical
Type	AlphaNumerical
Version	Numerical
Size	Numerical
MD5	AlphaNumerical
SHA-1	AlphaNumerical
Created	Short Date and Time, 24hr
Modified	Short Date and Time, 24hr

AccessData Registry Viewer, v1.4a

Key Name	AlphaNumerical
Name	AlphaNumerical
Type	AlphaNumerical
Data	AlphaNumerical
Key Name	AlphaNumerical
Name	AlphaNumerical
Type	AlphaNumerical
Data	AlphaNumerical
Key	AlphaNumerical

Digital Evidence Markup Language (DEML)

Name	
Name	AlphaNumerical
Type	AlphaNumerical
Data	AlphaNumerical

Autopsy ver. 2.06 (TSK ver. 2.03)

File	AlphaNumerical
MD5	AlphaNumerical
SHA-1	AlphaNumerical
Image	AlphaNumerical
Offset	AlphaNumerical
File System Type	AlphaNumerical
Date Generated	Short Date and Time
Investigator	AlphaNumerical
Directory Entry	Numerical
Allocated	Boolean
File Attributes	AlphaNumerical
Size	Numerical
Name	AlphaNumerical
Directory Entry Times/Written	Short Date and Time
Directory Entry Times/Accessed	Short Date and Time
Directory Entry Times/Created	Short Date and Time
Sectors	Numerical
File Type	Short Date and Time
<Actual Content>	AlphaNumerical
Autopsy Version	Numerical
The Sleuth Kit Version	Numerical
File	AlphaNumerical
MD5 of file	AlphaNumerical
SHA-1 of file	AlphaNumerical
MD5 of string	AlphaNumerical

Digital Evidence Markup Language (DEML)

SHA-1 of string	AlphaNumerical
Image	AlphaNumerical
Offset	AlphaNumerical
File System Type	AlphaNumerical
Date Generated	Short Date and Time
Investigator	AlphaNumerical
Directory Entry	Numerical
Allocated	Boolean
File Attributes	AlphaNumerical
Size	Numerical
Name	AlphaNumerical
Directory Entry Times/Written	Short Date and Time
Directory Entry Times/Accessed	Short Date and Time
Directory Entry Times/Created	Short Date and Time
Sectors	Numerical
File Type	Short Date and Time
<Actual Content>	AlphaNumerical
Autopsy Version	Numerical
The Sleuth Kit Version	Numerical
File System Type	AlphaNumerical
OEM Name	AlphaNumerical
Volume ID	AlphaNumerical
Volume Label (Boot Sector)	
Volume Label (Root Directory)	
File System Type Label	AlphaNumerical
Sectors before file system	Numerical
File System Layout (in sectors)	
Total Range	Numerical
Reserved	Numerical

Digital Evidence Markup Language (DEML)

Boot Sector	Numerical
FAT 0	Numerical
FAT 1	Numerical
Data Area	Numerical
Root Directory	Numerical
Cluster Area	Numerical
Range	Numerical
Root Directory	Numerical
Sector Size	Numerical
Cluster Size	Numerical
Total Cluster Range	Numerical
<Actual Sector ranges>	AlphaNumerical
<Numbers with an Allocated status>	Numerical
File Type	AlphaNumerical
MD5 of content	AlphaNumerical
SHA-1 of content	AlphaNumerical
Directory Entry	Numerical
Allocated	AlphaNumerical
File Attributes	AlphaNumerical
Size	Numerical
Name	AlphaNumerical
Directory Entry Times/Written	Short Date and Time
Directory Entry Times/Accessed	Short Date and Time
Directory Entry Times/Created	Short Date and Time
Sectors	Numerical

WFT ver
2.0.00

System Information

System Name	AlphaNumerical
Operating System	AlphaNumerical

Digital Evidence Markup Language (DEML)

	User Name	AlphaNumerical
	Windows	AlphaNumerical
	Directory	AlphaNumerical
	System Directory	AlphaNumerical
	System Date/Time	Short Date and Time
File		
	File Name	AlphaNumerical
	File Hash with Hash Identifier	AlphaNumerical
	<Actual file contents>	AlphaNumerical
	Time	Time
	Executable	AlphaNumerical
	<Status>	Alpha
	File Hash with Hash Identifier	AlphaNumerical
File		
	File Name	AlphaNumerical
	File Hash with Hash Identifier	AlphaNumerical
	<Actual file contents>	AlphaNumerical
	Action	Alpha
	Executable	AlphaNumerical
	MD5Checksum	AlphaNumerical
	Command	AlphaNumerical
	Output	AlphaNumerical
	Menu	AlphaNumerical
	Description	AlphaNumerical
Command		
	<Status>	Alpha
	File Hash with Hash Identifier	AlphaNumerical
	<Actual command executed>	AlphaNumerical
Description		

Digital Evidence Markup Language (DEML)

Command	AlphaNumerical
Description	AlphaNumerical
File	
File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical
Short formal date and time in 24h	AlphaNumerical
(Same format as above)	
(Output from DD.exe Physical memory dump)	
(Same format as above)	
(Output from Strings.exe)	
(Same format as above)	
(Output from mem.exe /p)	
Address	Numerical
Name	AlphaNumerical
Size	Numerical
Type	AlphaNumerical
(Same format as above)	
(Output from mem.exe /d)	
Address	Numerical
Name	AlphaNumerical
Size	Numerical
Type	AlphaNumerical
Command	
File Hash with Hash Identifier	AlphaNumerical
<Actual command executed>	AlphaNumerical
Description	
Command	AlphaNumerical
Description	AlphaNumerical

Digital Evidence Markup Language (DEML)

File

File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical
Date	Short Date
Time	Time
Dir Indicator	AlphaNumerical
Size	Numerical
Name	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C dir c:\ /S /OD /TC)

Date	Short Date
Time	Time
Dir Indicator	AlphaNumerical
Size	Numerical
Name	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C dir c:\ /S /OD /TW)

Date	Short Date
Time	Time
Dir Indicator	AlphaNumerical
Size	Numerical
Name	AlphaNumerical

Command

<Status>	Alpha
File Hash with Hash Identifier	AlphaNumerical
<Actual command executed>	AlphaNumerical

Description

Command	AlphaNumerical
Description	AlphaNumerical

Digital Evidence Markup Language (DEML)

File

File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical

(Same format as above)

(Output from Psinfo.exe -d -s -h)

<Parameter>	AlphaNumerical
<Value>	AlphaNumerical
Volume	AlphaNumerical
Type	AlphaNumerical
Format	AlphaNumerical
Label	AlphaNumerical
Size	AlphaNumerical
Free	Numerical
Free	Numerical
Installed	Short Date
Hotfix	AlphaNumerical
Applications	AlphaNumerical

(Same format as above)

(Output from hostname.exe)

<Actual Computer Name>	AlphaNumerical
------------------------	----------------

(Same format as above)

(Output from uname.exe -a)

<Actual values>	AlphaNumerical
-----------------	----------------

Command

File Hash with Hash Identifier	AlphaNumerical
<Actual command executed>	AlphaNumerical

Description

Command	AlphaNumerical
---------	----------------

Digital Evidence Markup Language (DEML)

File	Description	AlphaNumerical
	File Name	AlphaNumerical
	File Hash with Hash Identifier	AlphaNumerical
	<Actual file contents>	AlphaNumerical
	<Actual Computer Version values>	AlphaNumerical
(Same format as above)		
(Output from cmd.exe /C set)		
	<Parameter>	AlphaNumerical
	<Value>	AlphaNumerical
Command	<Status>	Alpha
	File Hash with Hash Identifier	AlphaNumerical
	<Actual command executed>	AlphaNumerical
Description	Command	AlphaNumerical
	Description	AlphaNumerical
File	File Name	AlphaNumerical
	File Hash with Hash Identifier	AlphaNumerical
	<Actual file contents>	AlphaNumerical
(Same format as above)		
(Output from uptime.exe /a)		
	<Various Information>	AlphaNumerical
	Date	Short Date
	Time	Time
	Event	AlphaNumerical
	Comment	AlphaNumerical

Digital Evidence Markup Language (DEML)

(Same format as above)

(Output from psuptime.exe)

<Actual values> AlphaNumerical

(Same format as above)

(Output from whoami.exe)

<Actual values> AlphaNumerical

(Same format as above)

(Output from net.exe config rdr)

<Actual values> AlphaNumerical

 <Parameter> AlphaNumerical

 <Value> AlphaNumerical

(Same format as above)

(Output from net.exe user)

<Actual values> AlphaNumerical

(Same format as above)

(Output from net.exe group)

<Actual values> AlphaNumerical

(Same format as above)

(Output from net.exe localgroup)

<Actual values> AlphaNumerical

(Same format as above)

(Output from net.exe accounts)

<Actual values> AlphaNumerical

 <Parameter> AlphaNumerical

 <Value> AlphaNumerical

(Same format as above)

(Output from net.exe accounts /domain)

<Actual values> AlphaNumerical

 <Parameter> AlphaNumerical

Digital Evidence Markup Language (DEML)

<Value> AlphaNumerical

(Same format as above)

(Output from auditpol.exe)

<Actual values> AlphaNumerical

<Parameter> AlphaNumerical

<Value> AlphaNumerical

(Same format as above)

(Output from pclip.exe)

<Actual values> AlphaNumerical

(Same format as above)

(Output from mem.exe /d)

Address Numerical

Name AlphaNumerical

Size Numerical

Type AlphaNumerical

<Various Information> AlphaNumerical

(Same format as above)

(Output from pslist.exe)

<Various Information> AlphaNumerical

Name AlphaNumerical

Pid Numerical

Pri Numerical

Thd Numerical

Hnd Numerical

Priv Numerical

CPU Time Numerical

Elapsed Time Numerical

<Various Information> AlphaNumerical

(Same format as above)

Digital Evidence Markup Language (DEML)

(Output from ps.exe -eaW)

Pid	Numerical
Ppid	Numerical
Pgid	Numerical
WinPid	Numerical
TTY	AlphaNumerical
UID	Numerical
Stime	Numerical
Command	AlphaNumerical

(Same format as above)

(Output from listdlls.exe)

<Various Information>	AlphaNumerical
Base	AlphaNumerical
Size	AlphaNumerical
Version	Numerical
Path	AlphaNumerical

(Same format as above)

(Output from pstat.exe)

<Various Information>	AlphaNumerical
User Time	Numerical
Kernel Time	Numerical
Ws	Numerical
Faults	Numerical
Commit	Numerical
Pri	Numerical
Hnd	Numerical
Thd	Numerical
Pid	Numerical
Name	AlphaNumerical

Digital Evidence Markup Language (DEML)

(Same format as above)

(Output from tlist.exe -v)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from tlist.exe -s)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from tlist.exe -c)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from cmdline.exe)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from handle.exe -a)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from psservice.exe)

<Actual values>	AlphaNumerical
Service_Name	AlphaNumerical

Digital Evidence Markup Language (DEML)

Display_Name	AlphaNumerical
Description	AlphaNumerical
Type	AlphaNumerical
State	AlphaNumerical
Win32_Exit_Code	AlphaNumerical
Service_Exit_Code	AlphaNumerical
CheckPoint	AlphaNumerical
Wait_Hint	AlphaNumerical

(Same format as above)

(Output from sc.exe queryex)

<Actual values>	AlphaNumerical
Service_Name	AlphaNumerical
Display_Name	AlphaNumerical
Type	AlphaNumerical
State	AlphaNumerical
Win32_Exit_Code	AlphaNumerical
Service_Exit_Code	AlphaNumerical
CheckPoint	AlphaNumerical
Wait_Hint	AlphaNumerical
Pid	Numerical
Flags	AlphaNumerical

(Same format as above)

(Output from net.exe start)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from servicelist.exe \\127.0.0.1)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from drivers.exe)

Digital Evidence Markup Language (DEML)

<Actual values>	AlphaNumerical
ModuleName	AlphaNumerical
Code	Numerical
Data	Numerical
Bss	Numerical
Paged	Numerical
Init	Numerical
LinkDate	AlphaNumerical

(Same format as above)

(Output from ipconfig.exe /all)

<Actual values>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from ipconfig.exe /all)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
#	Numerical
Address	Numerical
Broadcast	Numerical
Netmask	Numerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from arp.exe -a)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Internet Address	Numerical
Physical Address	AlphaNumerical

Digital Evidence Markup Language (DEML)

Type	AlphaNumerical
(Same format as above)	
(Output from route.exe print)	
<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Network Destination	Numerical
Netmask	Numerical
Gateway	Numerical
Interface	Numerical
Metric	Numerical
(Same format as above)	
(Output from netstat.exe -an)	
<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Proto	AlphaNumerical
Local Address	Numerical
Foreign Address	Numerical
State	AlphaNumerical
(Same format as above)	
(Output from fport.exe)	
<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Pid	Numerical
Process	AlphaNumerical
Port	Numerical
Proto	AlphaNumerical
Path	AlphaNumerical
(Same format as above)	

Digital Evidence Markup Language (DEML)

(Output from openports.exe -path -fport)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Pid	Numerical
Process	AlphaNumerical
Port	Numerical
Proto	AlphaNumerical
Path	AlphaNumerical

(Same format as above)

(Output from ipxroute.exe config)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from nbtstat.exe -n)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Name	AlphaNumerical
Type	AlphaNumerical
Status	AlphaNumerical

(Same format as above)

(Output from nbtstat.exe -c)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Name	AlphaNumerical
Type	AlphaNumerical
Host Address	Numerical
Life	Numerical

Digital Evidence Markup Language (DEML)

(Same format as above)

(Output from nbtstat.exe -s)

<Actual values> AlphaNumerical

(Same format as above)

(Output from hunt.exe \\127.0.0.1)

<Actual values> AlphaNumerical

<Parameter> AlphaNumerical

<Value> AlphaNumerical

(Same format as above)

(Output from net.exe share)

<Actual values> AlphaNumerical

<Various
Information> AlphaNumerical

Share Name AlphaNumerical

Resource AlphaNumerical

Remark AlphaNumerical

<Various
Information> AlphaNumerical

(Same format as above)

(Output from net.exe use)

<Actual values> AlphaNumerical

<Various
Information> AlphaNumerical

Status AlphaNumerical

Local AlphaNumerical

Remote AlphaNumerical

Network AlphaNumerical

<Various
Information> AlphaNumerical

(Same format as above)

(Output from net.exe view)

<Actual values> AlphaNumerical

Digital Evidence Markup Language (DEML)

<Various Information>	AlphaNumerical
Server Name	AlphaNumerical
Remark	AlphaNumerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from net.exe session)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
Computer	AlphaNumerical
User Name	AlphaNumerical
Client Type	AlphaNumerical
Opens	Numerical
Idle Time	Numerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from sniffer.exe)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from promiscdetect.exe)

<Actual values>	AlphaNumerical
-----------------	----------------

(Output from psloggedon.exe)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<Date>	Numerical
<Time>	AlphaNumerical
<System\username>	AlphaNumerical
<Various	AlphaNumerical

Digital Evidence Markup Language (DEML)

Information>

(Same format as above)

(Output from netusers.exe /local)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<System\username>	AlphaNumerical
<Formal username>	AlphaNumerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from netusers.exe /local /history)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<System\username>	AlphaNumerical
<Formal username>	AlphaNumerical
Last Logon	Date/Time
<Various Information>	AlphaNumerical

(Output from ntlast.exe -v -s)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from ntlast.exe -v -f)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from ntlast.exe -v -i)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from ntlast.exe -v -r)

<Actual values>	AlphaNumerical
-----------------	----------------

Digital Evidence Markup Language (DEML)

(Same format as above)

(Output from `dumpel.exe -t -l system -f <output.txt>`)

<Actual values>	AlphaNumerical
<Date>	Numerical
<Time>	AlphaNumerical
<?>	Numerical
<?>	Numerical
<MS Event ID#>	Numerical
<Service>	AlphaNumerical
<?>	AlphaNumerical
<Computer name>	AlphaNumerical
<Description>	AlphaNumerical

(Same format as above)

(Output from `dumpel.exe -t -l application -f <output.txt>`)

<Actual values>	AlphaNumerical
<Date>	Numerical
<Time>	AlphaNumerical
<?>	Numerical
<?>	Numerical
<MS Event ID#>	Numerical
<Service>	AlphaNumerical
<?>	AlphaNumerical
<Computer name>	AlphaNumerical
<Description>	AlphaNumerical

(Output from `dumpel.exe -t -l security -f <output.txt>`)

<Actual values>	AlphaNumerical
<Date>	Numerical
<Time>	AlphaNumerical
<?>	Numerical

Digital Evidence Markup Language (DEML)

<?>	Numerical
<MS Event ID#>	Numerical
<Service>	AlphaNumerical
<?>	AlphaNumerical
<Computer name>	AlphaNumerical
<Description>	AlphaNumerical

(Same format as above)

(Output from psloglist.exe)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<Unique sequence id#>	Numerical
<Service name>	AlphaNumerical
Type	AlphaNumerical
Computer	AlphaNumerical
Time	Date/Time
ID	Numerical
User	AlphaNumerical
<Description>	AlphaNumerical

(Output from psloglist.exe -s system)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<Unique sequence id#>	Numerical
<Log type>	AlphaNumerical
<Service name>	AlphaNumerical
<Type>	AlphaNumerical
<Computer>	AlphaNumerical
<Time>	Date/Time
<ID>	Numerical

Digital Evidence Markup Language (DEML)

<User> AlphaNumerical

<Description> AlphaNumerical

(Same format as above)

(Output from psloglist.exe -s application)

<Actual values> AlphaNumerical

<Various
Information> AlphaNumerical

<Unique sequence
id#> Numerical

<Log type> AlphaNumerical

<Service name> AlphaNumerical

<Type> AlphaNumerical

<Computer> AlphaNumerical

<Time> Date/Time

<ID> Numerical

<User> AlphaNumerical

<Description> AlphaNumerical

(Same format as above)

(Output from psloglist.exe -s security)

<Actual values> AlphaNumerical

<Various
Information> AlphaNumerical

<Unique sequence
id#> Numerical

<Log type> AlphaNumerical

<Service name> AlphaNumerical

<Type> AlphaNumerical

<Computer> AlphaNumerical

<Time> Date/Time

<ID> Numerical

<User> AlphaNumerical

<Description> AlphaNumerical

Digital Evidence Markup Language (DEML)

(Same format as above)

(Output from ntfsinfo.exe C)

<Actual values> AlphaNumerical

(Same format as above)

(Output from psfile.exe)

<Actual values> AlphaNumerical

(Same format as above)

(Output from net.exe file)

<Actual values> AlphaNumerical

(Same format as above)

(Output from cmd.exe /C tree c:\ /F /A)

<Actual values> AlphaNumerical

(Same format as above)

(Output from hfind.exe c:\)

<Actual values> AlphaNumerical

<Various Information> AlphaNumerical

<Directory or File> AlphaNumerical

<Date Time> AlphaNumerical

<Various Information> AlphaNumerical

File Hash with Hash Identifier AlphaNumerical

<Actual command executed> AlphaNumerical

Description

Command AlphaNumerical

Description AlphaNumerical

File

File Name AlphaNumerical

File Hash with Hash Identifier AlphaNumerical

<Actual file contents> AlphaNumerical

Digital Evidence Markup Language (DEML)

	<Various Information>	AlphaNumerical
	<Date>	Short Date
	<Time>	Time
	<Dir Indicator>	AlphaNumerical
	<Size>	Numerical
	<Name>	AlphaNumerical
	<Various Information>	AlphaNumerical
Command		
	<Status>	Alpha
	File Hash with Hash Identifier	AlphaNumerical
	<Actual command executed>	AlphaNumerical
Description		
	Command	AlphaNumerical
	Description	AlphaNumerical
File		
	File Name	AlphaNumerical
	File Hash with Hash Identifier	AlphaNumerical
	<Actual file contents>	AlphaNumerical
 (Same format as above)		
 (Output from efsinfo.exe /S: C:\ /U /R /C)		
	<Actual values>	AlphaNumerical
	<Directory or File>	AlphaNumerical
	<Encrypted or not>	AlphaNumerical
Command		
	File Hash with Hash Identifier	AlphaNumerical
	<Actual command executed>	AlphaNumerical
Description		
	Command	AlphaNumerical

Digital Evidence Markup Language (DEML)

Description	AlphaNumerical
File	
File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C type %SystemRoot%\win.ini)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C type %SystemRoot%\system.ini)

<Actual values>	AlphaNumerical
<Various Information>	AlphaNumerical
<Parameter>	AlphaNumerical
<Value>	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C type %SystemRoot%\winstart.bat)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from cmd.exe /C type %SystemRoot%\wininit.bat)

<Actual values>	AlphaNumerical
-----------------	----------------

Command

File Hash with Hash Identifier	AlphaNumerical
<Actual command executed>	AlphaNumerical

Digital Evidence Markup Language (DEML)

Description

Command	AlphaNumerical
Description	AlphaNumerical

File

File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical
<Various Information>	AlphaNumerical
<Date>	Short Date
<Time>	Time
<Dir Indicator>	AlphaNumerical
<Size>	Numerical
<Name>	AlphaNumerical
<Various Information>	AlphaNumerical

(Same format as above)

(Output from cmd.exe /C dir "%UserProfile%\Start Menu\Programs\Startup")

Command

<Status>	Alpha
File Hash with Hash Identifier	AlphaNumerical
<Actual command executed>	AlphaNumerical

Description

Command	AlphaNumerical
Description	AlphaNumerical

File

File Name	AlphaNumerical
File Hash with Hash Identifier	AlphaNumerical
<Actual file contents>	AlphaNumerical
<Registry Path>	AlphaNumerical
<Registry Key	AlphaNumerical

Digital Evidence Markup Language (DEML)

Type>

<Registry Key
Name> AlphaNumerical

<Registry Key
Value> AlphaNumerical

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad\ /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Policies\Microsoft\Windows\System\Scripts /S)

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\Run\ /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce /S)

(Same format as above)

Digital Evidence Markup Language (DEML)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Policies\Microsoft\Windows\System\Scripts /S)

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run\ /S)

(Same format as above)

(Output from autorunsc.exe -a -d -e -s -w)

<Actual values>	AlphaNumerical	
<Various Information>	AlphaNumerical	
<Registry Path>	AlphaNumerical	
<Registry Path Target Name>	AlphaNumerical	
<Registry Key Value>	AlphaNumerical	
<Registry Key Value>	AlphaNumerical	<Author>
<Registry Key Value>	AlphaNumerical	

(Same format as above)

(Output from reg.exe query "HKCU\Software\Microsoft\Internet Explorer\Explorer BarsS)

(Same format as above)

(Output from reg.exe query "HKCU\Software\Microsoft\Internet Explorer\TypedURLs" /S)

<Registry Path>	AlphaNumerical
<Registry Key Type>	AlphaNumerical
<Registry Key Name>	AlphaNumerical
<Registry Key Value>	AlphaNumerical

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU /S)

<Registry Path>	AlphaNumerical
-----------------	----------------

Digital Evidence Markup Language (DEML)

<Registry Key Type>	AlphaNumerical	REG_SZ
<Registry Key Name>	AlphaNumerical	b
<Registry Key Value>	AlphaNumerical	explorer\1

(Same format as above)

(Output from reg.exe query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\

<Registry Path>	AlphaNumerical
<Registry Key Type>	AlphaNumerical
<Registry Key Name>	AlphaNumerical
<Registry Key Value>	AlphaNumerical

(Same format as above)

(Output from reg.exe query HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall /S)

<Registry Path>	AlphaNumerical
<Registry Key Type>	AlphaNumerical
<Registry Key Name>	AlphaNumerical
<Registry Key Value>	AlphaNumerical

(Same format as above)

(Output from regdmp.exe)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from mdmchk.exe)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

(Output from mdmchk.exe)

<Actual values>	AlphaNumerical
-----------------	----------------

(Same format as above)

Digital Evidence Markup Language (DEML)

(Output from now.exe)

<Actual file contents>

Short formal date
and time in 24h

AlphaNumerical

FRED v1.4
for Helix

<MD5 Hash> with preceding backslash

AlphaNumerical

<Report path> with preceding asterisk

AlphaNumerical

<Various Information>

AlphaNumerical

Start Time

Time and Date

AlphaNumerical

PSINFO

<Various Information>

AlphaNumerical

Uptime

Time

Kernel version

AlphaNumerical

Product Type

Alpha

Product Version

Numerical

Service Pack

Numerical

Kernel Build Number

Numerical

Registered Organization

AlphaNumerical

Registered Owner

AlphaNumerical

Install Date

Date and Time

Activation status

Alpha

IE version

Numerical

System root

AlphaNumerical

Processors

Numerical

Processor speed

AlphaNumerical

Processor type

AlphaNumerical

Physical memory

AlphaNumerical

Video driver

AlphaNumerical

Digital Evidence Markup Language (DEML)

NET ACCOUNTS

Force user logoff...	AlphaNumerical	
Min password age, days	Numerical	
Max password age , days	Numerical	
Min password length	Numerical	
Length of password history	AlphaNumerical	
Lockout threshold	AlphaNumerical	
Lockout duration, min	Numerical	
Lockout observation window, min	Numerical	
Computer role	Alpha	
<Various Information>	AlphaNumerical	Footer info

NET FILE

{No data available}

NET SESSION

{No data available}

NET SHARE

<Various Information>	AlphaNumerical	
<Share Name>	AlphaNumerical	
<Resource>	AlphaNumerical	
<Remark>	AlphaNumerical	
<Various Information>	AlphaNumerical	

NET START

<Various Information>	AlphaNumerical	
<Started Services>	AlphaNumerical	
<Various Information>	AlphaNumerical	

NET USE

<Various Information>	AlphaNumerical	
<Status>	AlphaNumerical	
<Local>	AlphaNumerical	
<Remote>	AlphaNumerical	

Digital Evidence Markup Language (DEML)

<Network>	AlphaNumerical
<Various Information>	AlphaNumerical
NET USER	
<Various Information>	AlphaNumerical
<User accounts>	AlphaNumerical
<Various Information>	AlphaNumerical
NET VIEW	
{No data available}	
ARP (arp -a)	
{No data available}	
NETSTAT (netstat -an)	
<Various Information>	AlphaNumerical
<Proto>	AlphaNumerical
<Local Address>	AlphaNumerical
<Foreign Address>	AlphaNumerical
<State>	AlphaNumerical
LOGGED ON	
<Various Information>	AlphaNumerical
<Date and Time>	Date and Time
<Domain and User>	AlphaNumerical
<Various Information>	AlphaNumerical
Proclnterrogate	
<Various Information>	AlphaNumerical
<Full process file path and file (Process ID Number with label)>	
<Various Information>	AlphaNumerical
<Entry Point>	AlphaNumerical
<Base>	AlphaNumerical
<Size>	AlphaNumerical
<Module>	AlphaNumerical

Digital Evidence Markup Language (DEML)

FPORT (fport /p)

<Various Information>	AlphaNumerical
<PID>	Numerical
<Process>	AlphaNumerical
<Port>	Numerical
<Proto>	AlphaNumerical
<Path>	AlphaNumerical

PSLIST (pslist -x)

<Various Information>	AlphaNumerical
<Name>	AlphaNumerical
<PID>	Numerical
<Pri>	Numerical
<Thd>	Numerical
<Hnd>	Numerical
<Priv>	Numerical
<CPU Time>	Time, long
<Elapsed Time>	Time, long
<VM>	Numerical
<WS>	Numerical
<Priv>	Numerical
<Priv Pk>	Numerical
<Faults>	Numerical
<NonP>	Numerical
<Page>	Numerical
	Numerical
<Tid>	
<Pri>	Numerical
<Cswitch>	Numerical
<State>	AlphaNumerical

Digital Evidence Markup Language (DEML)

<User Time>	Time, long
<Kernel Time>	Time, long
<Elapsed Time>	Time, long
NBTSTAT	
<Various Information>	AlphaNumerical
{No data available}	
HIDDEN FILES (dir /s /a:h /t:a c: d:)	
<Various Information>	AlphaNumerical
Date	Short Date
Time	Time
Dir Indicator	AlphaNumerical
Size	Numerical
Name	AlphaNumerical
MD5SUMS	
{No data available}	
AT Scheduler list	
<Various Information>	AlphaNumerical
{No data available}	
END TIME	
Time and Date	AlphaNumerical

**SecReport
v3.02.10**

NIC Brand and Model	AlphaNumerical
IP Address	Numerical
Subnet Mask	Numerical
MAC Address	AlphaNumerical
Account Logon	Alpha
Account Management	Alpha
Directory Service Access	Alpha
Logon	Alpha

Digital Evidence Markup Language (DEML)

Object Access	Alpha
Policy Change	Alpha
Privilege Use	Alpha
Process Tracking	Alpha
System	Alpha
<Log Name>	AlphaNumerical
<Max Size>	Numerical
<Overwrite Old Events>	Numerical
<Overwrite Policy>	AlphaNumerical
<Various Information>	AlphaNumerical
<Service>	AlphaNumerical
<Start Type>	AlphaNumerical
<Status>	AlphaNumerical
<Service Full Name>	AlphaNumerical
<Account>	AlphaNumerical
<Various Information>	AlphaNumerical
<Application and version number>	AlphaNumerical
<Various Information>	AlphaNumerical
{No data available}	
<Various Information>	AlphaNumerical
<Port>	Numerical
<Protocol>	AlphaNumerical
<PID>	Numerical
<Program short name>	AlphaNumerical
<Program long name>	AlphaNumerical
Computer System	
Brand	AlphaNumerical
Model	AlphaNumerical
Serial No.	AlphaNumerical
Number of Processors	Numerical

Digital Evidence Markup Language (DEML)

BIOS version	AlphaNumerical	
BIOS Date	AlphaNumerical	
RAM size, Mbytes	Numerical	
Processors		
<CPU ID>	AlphaNumerical	
<Manufacturer>	AlphaNumerical	
<Name>	AlphaNumerical	
<Max Speed, MHz>	Numerical	
<L2 Cache, KB>	Numerical	
<ExtClock, MHz>	Numerical	
Fixed Disks		
<Drive Letter>	Alpha	
<FileSystem>	AlphaNumerical	
<Total Size, MB>	Numerical	
<Free Space, MB>	Numerical	
<Serial No.>	Numerical	
Recovery Console Installed	AlphaNumerical	
Norton Antivirus signature date	AlphaNumerical	
Root Kit Revealer v1.7, SysInternals		
	AlphaNumerical	c:\myDir\myFile.txt
	AlphaNumerical	Short Date and 12hr time
	AlphaNumerical	10KB
	AlphaNumerical	
MessenPass v1.04, NirSoft		
	AlphaNumerical	Trillian
	AlphaNumerical	MSN Messenger
	AlphaNumerical	dude123
	AlphaNumerical	pass123

Digital Evidence Markup Language (DEML)

Protected Storage PassView v1.62, NirSoft

AlphaNumerical	https://www.myfakepage.com/Login.asp'
AlphaNumerical	AutoComplete Passwords
AlphaNumerical	test
AlphaNumerical	blahblahblah

RegScanner v1.20, NirSoft

AlphaNumerical	HKCU\AppEvents\EventLabels\Close
AlphaNumerical	DispFileName
AlphaNumerical	REG_SZ
AlphaNumerical	Close Program
AlphaNumerical	4/3/2006 11:57:15AM
Numerical	14

IEHistoryView v1.30, NirSoft

AlphaNumerical	file:///d:/temp/myFile.csv
AlphaNumerical	
AlphaNumerical	2
AlphaNumerical	12/26/2006 3:12:04PM
AlphaNumerical	1/21/2007 3:12:10PM
AlphaNumerical	testaccount

IECookiesView v1.70, NirSoft

AlphaNumerical	www.yahoo.com
Numerical	16
AlphaNumerical	11/2/2006 3:15:08 PM
AlphaNumerical	9/6/2006 3:37:37 PM
AlphaNumerical	9/6/2006 3:37:37 PM
Numerical	68
AlphaNumerical	testaccount
AlphaNumerical	testaccount@www.yahoo[2].txt

Digital Evidence Markup Language (DEML)

AlphaNumerical	Active
AlphaNumerical	Unknown
AlphaNumerical	yahoo.com
Numerical	8
AlphaNumerical	FPS
AlphaNumerical	ds
AlphaNumerical	www.yahoo.com

Mail PassView v1.32,
NirSoft

Boolean

AlphaNumerical	8/19/2015 11:00:00 PM
AlphaNumerical	9/6/2006 3:37:37 PM
AlphaNumerical	Client
AlphaNumerical	192.168.10.10
AlphaNumerical	POP3
AlphaNumerical	test
AlphaNumerical	BigDog86

Network Password Recovery v1.02, NirSoft

AlphaNumerical	192.168.3.35
AlphaNumerical	Domain Password
AlphaNumerical	srv\admin1
AlphaNumerical	hyyu7TRF5
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	Boolean

Asterisk Logger v1.02,
NirSoft

AlphaNumerical	password2
AlphaNumerical	Short Data long time, 24hr
AlphaNumerical	CuteFTP

Digital Evidence Markup Language (DEML)

AlphaNumerical F:\Program Files\CuteFTP\CuteFTP.exe

Adepto 1.0

	AlphaNumerical	Me
	AlphaNumerical	12345
	AlphaNumerical	had
	AlphaNumerical	Quantum
	AlphaNumerical	FireBallP
	AlphaNumerical	123456
	AlphaNumerical	20.4 GB
	Numerical	123456
	Numerical	123456
	AlphaNumerical	IDE Primary Master
Source Device	AlphaNumerical	
Image Name	AlphaNumerical	
Image Notes	AlphaNumerical	
Destination	AlphaNumerical	
Mount Point	AlphaNumerical	
DD Type	AlphaNumerical	
Hash Type	AlphaNumerical	
Segment Size (MB)	AlphaNumerical	
Use Advanced Options	Boolean	
Advanced		
	Input BS	Numerical
	Output BS	Numerical
	Count	Numerical
	Seek	Numerical
	Skip	Numerical
	Conv	AlphaNumerical

Digital Evidence Markup Language (DEML)

Choose the first image in an Image set (.000)	AlphaNumerical
Destination Device	AlphaNumerical
Destination File	AlphaNumerical
Source Device	AlphaNumerical
Destination Device	AlphaNumerical
<Log entries in free form> (Selected entries in the log)	AlphaNumerical
System Name	AlphaNumerical
Description	AlphaNumerical
Product	AlphaNumerical
Vendor	AlphaNumerical
Serial	AlphaNumerical
Width	AlphaNumerical
Capabilities	AlphaNumerical
Configuration	AlphaNumerical
Core	
Description	AlphaNumerical
Product	AlphaNumerical
Vendor	AlphaNumerical
Physical ID	AlphaNumerical
Firmware	
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical
	AlphaNumerical

CPU

Digital Evidence Markup Language (DEML)

AlphaNumerical	CPU
AlphaNumerical	Pentium III (Coppermine)
AlphaNumerical	Intel Corp.
AlphaNumerical	400
AlphaNumerical	cpu@0
AlphaNumerical	6.8.1
AlphaNumerical	Microprocessor
AlphaNumerical	533MHz
AlphaNumerical	1GHz
AlphaNumerical	32 Bits
AlphaNumerical	L1 Cache
AlphaNumerical	
AlphaNumerical	32KB
AlphaNumerical	32KB
AlphaNumerical	Internal varies unified
Numerical	
AlphaNumerical	L2 Cache
AlphaNumerical	
AlphaNumerical	256KB
AlphaNumerical	256KB
AlphaNumerical	Internal varies unified
AlphaNumerical	
AlphaNumerical	512MB
Numerical	

Digital Evidence Markup Language (DEML)

AlphaNumerical	DIMM SDRAM Synchronous 100MHz (10.0 ns)
AlphaNumerical	
AlphaNumerical	DIMM_A
AlphaNumerical	128MB
AlphaNumerical	64 bits
AlphaNumerical	100MHz (10ns)
AlphaNumerical	DIMM SDRAM
AlphaNumerical	DIMM_B
AlphaNumerical	128MB
AlphaNumerical	64 bits
AlphaNumerical	100MHz (10ns)
PCI	
AlphaNumerical	Host Bridge
AlphaNumerical	Intel Corporation
AlphaNumerical	
AlphaNumerical	pci@00:00.0
AlphaNumerical	
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	VGA
AlphaNumerical	82810E DC-133 CGC [Chipset Graphics Controller]
AlphaNumerical	Intel Corporation
AlphaNumerical	pci@00:01.0
AlphaNumerical	64MB
AlphaNumerical	32 bits
AlphaNumerical	66 MHz
AlphaNumerical	vga bus master cap list
AlphaNumerical	PCI Bridge
AlphaNumerical	82801AA PCI Bridge

Digital Evidence Markup Language (DEML)

AlphaNumerical	Intel Corporation
AlphaNumerical	1e
AlphaNumerical	pci@00:0e.0
	AlphaNumerical
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	pci normal_decode bus_master
AlphaNumerical	Multimedia audio controller
AlphaNumerical	ES1371 [AudioPCI-97]
AlphaNumerical	Ensoniq
AlphaNumerical	
AlphaNumerical	pci@01:07.0
AlphaNumerical	
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	bus_master cap_list
AlphaNumerical	driver=ENS1371
AlphaNumerical	ioport:ecc0-ecff irq:9
AlphaNumerical	Ethernet interface
AlphaNumerical	3c9050-TX/TX-M [Tornado]
AlphaNumerical	3Com Corporation
AlphaNumerical	c
AlphaNumerical	pci@01:0c.0
AlphaNumerical	eth0
AlphaNumerical	
AlphaNumerical	00:b0:d0:12:34:55
AlphaNumerical	10MB/s
AlphaNumerical	100MB/s
AlphaNumerical	32 bits
AlphaNumerical	33MHz

Digital Evidence Markup Language (DEML)

AlphaNumerical	bus_master cap_list ethernet physical tp mii 10bt 10bt-fd 100bt 100bt-fd autonegociation
AlphaNumerical	autonegociation=on broadcast=yes driver=3c59x driverversion=LK1.1.19 duplex=half link=no multicast=yes port=MII speed=10MB/s
AlphaNumerical	ioport:ec00-ec7f iomemory:fdffc00- fdffc7f irq:5
	UNCLAIMED
AlphaNumerical	ISA Bridge
AlphaNumerical	82801AA ISA Bridge (LPC)
AlphaNumerical	Intel Corporation
AlphaNumerical	1f
AlphaNumerical	pci@00:1f.0
AlphaNumerical	
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	isa bus_master
AlphaNumerical	IDE interface
AlphaNumerical	82801AA IDE
AlphaNumerical	Intel Corporation
AlphaNumerical	1f.1
AlphaNumerical	pci@00:1f.1
AlphaNumerical	2
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	ide bus_master
AlphaNumerical	driver=PIIX_IDE

Digital Evidence Markup Language (DEML)

AlphaNumerical	ioport:ffa0-ffaf
AlphaNumerical	0
AlphaNumerical	IDE Channel 0
AlphaNumerical	0
AlphaNumerical	ide@0
AlphaNumerical	ide0
AlphaNumerical	33MHz
	AlphaNumerical
Description	AlphaNumerical
Physical ID	AlphaNumerical
Bus Info	AlphaNumerical
Logical Name	AlphaNumerical
Capacity	AlphaNumerical
Capabilities	AlphaNumerical
	AlphaNumerical
Description	AlphaNumerical
Bus Info	AlphaNumerical
Logical Name	AlphaNumerical
Capacity	AlphaNumerical
Capabilities	AlphaNumerical
	AlphaNumerical
Description	AlphaNumerical
Physical ID	AlphaNumerical
Bus Info	AlphaNumerical
Logical Name	AlphaNumerical
Capacity	AlphaNumerical
Capabilities	AlphaNumerical
AlphaNumerical	IDE Channel 1

Digital Evidence Markup Language (DEML)

AlphaNumerical

1

AlphaNumerical ide@1

AlphaNumerical ide1

AlphaNumerical 33MHz

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

Physical ID

Logical Name

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

AlphaNumerical

Digital Evidence Markup Language (DEML)

AlphaNumerical	
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	uhci bus_master
AlphaNumerical	driver=uhci_hcd
AlphaNumerical	ioport:ff80-ff9f irq:12
AlphaNumerical	UHCI Host Controller
AlphaNumerical	Linux 2.6.14-kanotix-9 uhci_hcd
AlphaNumerical	1
AlphaNumerical	usb@1
AlphaNumerical	usb1
AlphaNumerical	
AlphaNumerical	usb-1.10
AlphaNumerical	driver=hub maxpower=0mA slots=2 speed=12.0MB/s
AlphaNumerical	SMBus
AlphaNumerical	82801AA SMBus
AlphaNumerical	Intel Corporation
AlphaNumerical	1f.3
AlphaNumerical	pci@00:1f.3
AlphaNumerical	2
AlphaNumerical	32 bits
AlphaNumerical	33MHz
AlphaNumerical	driver=i801_smbus
AlphaNumerical	ioport:dcd0-dcdf irq:10

DEML NIEM Formatted XML Code

The XML code below is our DEML (NIEM formatted) prototype model.

```

<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:element name="SystemNcfs">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="serialNum"/>
        <xs:element ref="ram"/>
        <xs:element ref="cpu"/>
        <xs:element ref="genLocation"/>
        <xs:element ref="typeNcfs"/>
        <xs:element ref="manufacturer"/>
        <xs:element ref="manufactDate"/>
        <xs:element ref="examinerComments"/>
        <xs:element ref="userTags"/>
        <xs:element ref="numInternalDrives"/>
        <xs:element ref="ComponentNcfs"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="ram" type="xs:long"/>
  <xs:element name="cpu" type="xs:string"/>
  <xs:element name="genLocation" type="xs:string"/>
  <xs:element name="numInternalDrives" type="xs:short"/>
  <xs:element name="ComponentNcfs">
    <xs:complexType>
      <xs:sequence>
        <xs:element ref="manufacturer"/>
        <xs:element ref="manufactDate"/>
        <xs:element ref="examinerComments"/>
        <xs:element ref="userTags"/>
        <xs:element ref="serialNum"/>
        <xs:element ref="productNum"/>
        <xs:element ref="Peripherals"/>
        <xs:element ref="Storage"/>
        <xs:element ref="NetworkCard"/>
        <xs:element ref="AddonCard"/>
        <xs:element ref="Application"/>
        <xs:element ref="NetworkConnection"/>
        <xs:element ref="OS"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="productNum" type="xs:long"/>
  <xs:element name="Peripherals">
    <xs:complexType>

```

```

<xs:sequence>
  <xs:element ref="attached"/>
  <xs:element ref="configured"/>
  <xs:element ref="powered"/>
  <xs:element ref="KeyLogger"/>
  <xs:element ref="KeyBoard"/>
  <xs:element ref="Printer"/>
  <xs:element ref="Mouse"/>
  <xs:element ref="Speakers"/>
  <xs:element ref="Monitor"/>
  <xs:element ref="Modem"/>
  <xs:element ref="ExternalDrive"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="KeyLogger">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="KeyBoard">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Printer">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Mouse">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

    <xs:element ref="configured"/>
    <xs:element ref="powered"/>
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Speakers">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Monitor">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Modem">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ExternalDrive">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="attached"/>
      <xs:element ref="configured"/>
      <xs:element ref="powered"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Storage">
  <xs:complexType>
    <xs:complexContent>
      <xs:extension base="integrated">
        <xs:sequence>

```

```

    <xs:element ref="Partition"/>
    <xs:element ref="SolidState"/>
    <xs:element ref="Magnetic"/>
  </xs:sequence>
</xs:extension>
</xs:complexContent>
</xs:complexType>
</xs:element>
<xs:element name="Partition">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="size"/>
      <xs:element ref="fileSystem"/>
      <xs:element ref="allocatedSpace"/>
      <xs:element ref="unallocatedSpace"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="size" type="xs:long"/>
<xs:element name="fileSystem" type="xs:string"/>
<xs:element name="allocatedSpace" type="xs:long"/>
<xs:element name="unallocatedSpace" type="xs:long"/>
<xs:element name="SolidState">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="readOnly"/>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
      <xs:element ref="UsbFlash"/>
      <xs:element ref="CompactFlash"/>
      <xs:element ref="SmartCard"/>
      <xs:element ref="SdCard"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="UsbFlash">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="readOnly"/>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="CompactFlash">
  <xs:complexType>

```

```

<xs:sequence>
  <xs:element ref="readOnly"/>
  <xs:element ref="geometry"/>
  <xs:element ref="partitionCount"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="SmartCard">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="readOnly"/>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="SdCard">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="readOnly"/>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Magnetic">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
      <xs:element ref="OpticalDrive"/>
      <xs:element ref="HardDisk"/>
      <xs:element ref="FloppyDrive"/>
      <xs:element ref="ZipDrive"/>
      <xs:element ref="TapeDrive"/>
      <xs:element ref="OtherMagnetic"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="OpticalDrive">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>

```

```

</xs:element>
<xs:element name="HardDisk">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="FloppyDrive">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ZipDrive">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="TapeDrive">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="OtherMagnetic">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="geometry"/>
      <xs:element ref="partitionCount"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="NetworkCard">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="mac"/>
      <xs:element ref="typeNcfs"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="mac" type="xs:string"/>
<xs:element name="AddonCard" type="xs:string"/>
<xs:element name="Application">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="name"/>
      <xs:element ref="manufacturer"/>
      <xs:element ref="version"/>
      <xs:element ref="logicalLocation"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="version" type="xs:string"/>
<xs:element name="NetworkConnection">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="clientServer"/>
      <xs:element ref="ip"/>
      <xs:element ref="state"/>
      <xs:element ref="alive"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="clientServer" type="xs:boolean"/>
<xs:element name="state" type="xs:string"/>
<xs:element name="alive" type="xs:string"/>
<xs:element name="OS">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
      <xs:element ref="ip"/>
      <xs:element ref="DigitalArtifact"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="DigitalArtifact">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

<xs:element ref="ip"/>
<xs:element ref="VirtualSystem"/>
<xs:element ref="Allocated"/>
<xs:element ref="Unallocated"/>
<xs:element ref="Slack"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="VirtualSystem">
<xs:complexType>
<xs:sequence>
<xs:element ref="typeNcfs"/>
<xs:element ref="revision"/>
<xs:element ref="upTime"/>
<xs:element ref="ip"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Allocated">
<xs:complexType>
<xs:sequence>
<xs:element ref="typeNcfs"/>
<xs:element ref="revision"/>
<xs:element ref="upTime"/>
<xs:element ref="ip"/>
<xs:element ref="File"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="File">
<xs:complexType>
<xs:sequence>
<xs:element ref="filename"/>
<xs:element ref="startSector"/>
<xs:element ref="cDate"/>
<xs:element ref="cTime"/>
<xs:element ref="mDate"/>
<xs:element ref="mTime"/>
<xs:element ref="aDate"/>
<xs:element ref="aTime"/>
<xs:element ref="logicalLocation"/>
<xs:element ref="applicationAssociation"/>
<xs:element ref="deleted"/>
<xs:element ref="attribute"/>
<xs:element ref="examinerComments"/>
<xs:element ref="bookmarkType"/>

```

```
<xs:element ref="preview"/>
<xs:element ref="pageBreak"/>
<xs:element ref="showPicture"/>
<xs:element ref="entrySelected"/>
<xs:element ref="fileOffset"/>
<xs:element ref="length"/>
<xs:element ref="name"/>
<xs:element ref="filter"/>
<xs:element ref="inReport"/>
<xs:element ref="fileExtExe"/>
<xs:element ref="fileType"/>
<xs:element ref="fileCategory"/>
<xs:element ref="signature"/>
<xs:element ref="description"/>
<xs:element ref="isDeleted"/>
<xs:element ref="lastAccessed"/>
<xs:element ref="fileCreated"/>
<xs:element ref="lastWritten"/>
<xs:element ref="entryModified"/>
<xs:element ref="fileDeleted"/>
<xs:element ref="fileAquired"/>
<xs:element ref="logicalSize"/>
<xs:element ref="initializedSize"/>
<xs:element ref="startingExtent"/>
<xs:element ref="fileExtents"/>
<xs:element ref="permissions"/>
<xs:element ref="references"/>
<xs:element ref="physicalLocation"/>
<xs:element ref="physicalSector"/>
<xs:element ref="evidenceFile"/>
<xs:element ref="fileIdentifier"/>
<xs:element ref="codePage"/>
<xs:element ref="hashValue"/>
<xs:element ref="hashSet"/>
<xs:element ref="hashCategory"/>
<xs:element ref="fullPath"/>
<xs:element ref="shortName"/>
<xs:element ref="uniqueName"/>
<xs:element ref="symbolicLink"/>
<xs:element ref="isDuplicate"/>
<xs:element ref="isInternal"/>
<xs:element ref="isOverwritten"/>
<xs:element ref="bookmarkPath"/>
<xs:element ref="bookmarkStart"/>
<xs:element ref="bookmarkSector"/>
<xs:element ref="notable"/>
```

```

</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="filename" type="xs:string"/>
<xs:element name="startSector" type="xs:long"/>
<xs:element name="cDate" type="xs:date"/>
<xs:element name="cTime" type="xs:time"/>
<xs:element name="mDate" type="xs:date"/>
<xs:element name="mTime" type="xs:time"/>
<xs:element name="aDate" type="xs:date"/>
<xs:element name="aTime" type="xs:time"/>
<xs:element name="applicationAssociation" type="xs:string"/>
<xs:element name="deleted" type="xs:boolean"/>
<xs:element name="attribute" type="xs:string"/>
<xs:element name="bookmarkType" type="xs:string"/>
<xs:element name="preview" type="xs:string"/>
<xs:element name="pageBreak" type="xs:string"/>
<xs:element name="showPicture" type="xs:string"/>
<xs:element name="entrySelected" type="xs:string"/>
<xs:element name="fileOffset" type="xs:short"/>
<xs:element name="length" type="xs:int"/>
<xs:element name="filter" type="xs:string"/>
<xs:element name="inReport" type="xs:string"/>
<xs:element name="fileExtExe" type="xs:string"/>
<xs:element name="fileType" type="xs:string"/>
<xs:element name="fileCategory" type="xs:string"/>
<xs:element name="signature" type="xs:string"/>
<xs:element name="description" type="xs:string"/>
<xs:element name="isDeleted" type="xs:string"/>
<xs:element name="lastAccessed" type="xs:string"/>
<xs:element name="fileCreated" type="xs:string"/>
<xs:element name="lastWritten" type="xs:string"/>
<xs:element name="entryModified" type="xs:string"/>
<xs:element name="fileDeleted" type="xs:string"/>
<xs:element name="fileAquired" type="xs:string"/>
<xs:element name="logicalSize" type="xs:long"/>
<xs:element name="initializedSize" type="xs:long"/>
<xs:element name="startingExtent" type="xs:string"/>
<xs:element name="fileExtents" type="xs:short"/>
<xs:element name="permissions" type="xs:short"/>
<xs:element name="references" type="xs:short"/>
<xs:element name="physicalLocation" type="xs:long"/>
<xs:element name="physicalSector" type="xs:long"/>
<xs:element name="evidenceFile" type="xs:string"/>
<xs:element name="fileIdentifier" type="xs:int"/>
<xs:element name="codePage" type="xs:short"/>

```

```

<xs:element name="hashValue" type="xs:string"/>
<xs:element name="hashSet" type="xs:string"/>
<xs:element name="hashCategory" type="xs:string"/>
<xs:element name="fullPath" type="xs:string"/>
<xs:element name="shortName" type="xs:string"/>
<xs:element name="uniqueName" type="xs:string"/>
<xs:element name="symbolicLink" type="xs:string"/>
<xs:element name="isDuplicate" type="xs:string"/>
<xs:element name="isInternal" type="xs:string"/>
<xs:element name="isOverwritten" type="xs:string"/>
<xs:element name="bookmarkPath" type="xs:string"/>
<xs:element name="bookmarkStart" type="xs:long"/>
<xs:element name="bookmarkSector" type="xs:long"/>
<xs:element name="notable" type="xs:string"/>
<xs:element name="Unallocated">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
      <xs:element ref="ip"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Slack">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
      <xs:element ref="ip"/>
      <xs:element ref="RamSlack"/>
      <xs:element ref="FileSlack"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="RamSlack">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
      <xs:element ref="ip"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

<xs:element name="FileSlack">
  <xs:complexType>
    <xs:sequence>
      <xs:element ref="typeNcfs"/>
      <xs:element ref="revision"/>
      <xs:element ref="upTime"/>
      <xs:element ref="ip"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="serialNum" type="xs:long"/>
<xs:element name="typeNcfs" type="xs:string"/>
<xs:element name="manufacturer" type="xs:string"/>
<xs:element name="manufactDate" type="xs:date"/>
<xs:element name="examinerComments" type="xs:string"/>
<xs:element name="userTags" type="xs:string"/>
<xs:element name="attached" type="xs:boolean"/>
<xs:element name="configured" type="xs:boolean"/>
<xs:element name="powered" type="xs:boolean"/>
<xs:complexType name="integrated">
  <xs:sequence>
    <xs:element ref="integrated"/>
  </xs:sequence>
</xs:complexType>
<xs:element name="integrated" type="xs:boolean"/>
<xs:element name="readOnly" type="xs:boolean"/>
<xs:element name="geometry" type="xs:string"/>
<xs:element name="partitionCount" type="xs:short"/>
<xs:element name="name" type="xs:string"/>
<xs:element name="logicalLocation" type="xs:string"/>
<xs:element name="ip" type="xs:long"/>
<xs:element name="revision" type="xs:string"/>
<xs:element name="upTime" type="xs:short"/>
</xs:schema>

```

View the XML

This is the XML document that will be filled out by the user, validated against the schema, and used to actually update the database. Note that in addition class and properties, each property has a data type, typically alphanumeric (or string), numerical, Boolean (e.g., Y/N or T/F), or some structured data format.

```

<?xml version="1.0"?>
<SystemNcfs xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="file:///c:/Documents%20and%20Settings/Dennis%20Wood/
Desktop/June18/deml.xsd">
  <serialNum>-9223372036854775808</serialNum>
  <ram>-9223372036854775808</ram>
  <cpu>string</cpu>
  <genLocation>string</genLocation>
  <typeNcfs>string</typeNcfs>
  <manufacturer>string</manufacturer>
  <manufactDate>1999-01-21</manufactDate>
  <examinerComments>string</examinerComments>
  <userTags>string</userTags>
  <numInternalDrives>-32768</numInternalDrives>
  <ComponentNcfs>
    <manufacturer>string</manufacturer>
    <manufactDate>1999-01-21</manufactDate>
    <examinerComments>string</examinerComments>
    <userTags>string</userTags>
    <serialNum>-9223372036854775808</serialNum>
    <productNum>-9223372036854775808</productNum>
    <Peripherals>
      <attached>true</attached>
      <configured>true</configured>
      <powered>true</powered>
      <KeyLogger>
        <attached>true</attached>
        <configured>true</configured>
        <powered>true</powered>
      </KeyLogger>
      <KeyBoard>
        <attached>true</attached>
        <configured>true</configured>
        <powered>true</powered>
      </KeyBoard>
      <Printer>
        <attached>true</attached>
        <configured>true</configured>
        <powered>true</powered>
      </Printer>
      <Mouse>
        <attached>true</attached>
        <configured>true</configured>
        <powered>true</powered>
      </Mouse>
    </Peripherals>
  </ComponentNcfs>
</SystemNcfs>

```

```

<Speakers>
  <attached>true</attached>
  <configured>true</configured>
  <powered>true</powered>
</Speakers>
<Monitor>
  <attached>true</attached>
  <configured>true</configured>
  <powered>true</powered>
</Monitor>
<Modem>
  <attached>true</attached>
  <configured>true</configured>
  <powered>true</powered>
</Modem>
<ExternalDrive>
  <attached>true</attached>
  <configured>true</configured>
  <powered>true</powered>
</ExternalDrive>
</Peripherals>
<Storage>
  <integrated>true</integrated>
  <Partition>
    <size>-9223372036854775808</size>
    <fileSystem>string</fileSystem>
    <allocatedSpace>-9223372036854775808</allocatedSpace>
    <unallocatedSpace>-9223372036854775808</unallocatedSpace>
  </Partition>
  <SolidState>
    <readOnly>true</readOnly>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
    <UsbFlash>
      <readOnly>true</readOnly>
      <geometry>string</geometry>
      <partitionCount>-32768</partitionCount>
    </UsbFlash>
    <CompactFlash>
      <readOnly>true</readOnly>
      <geometry>string</geometry>
      <partitionCount>-32768</partitionCount>
    </CompactFlash>
    <SmartCard>
      <readOnly>true</readOnly>
      <geometry>string</geometry>

```

```

    <partitionCount>-32768</partitionCount>
  </SmartCard>
  <SdCard>
    <readOnly>>true</readOnly>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </SdCard>
</SolidState>
<Magnetic>
  <geometry>string</geometry>
  <partitionCount>-32768</partitionCount>
  <OpticalDrive>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </OpticalDrive>
  <HardDisk>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </HardDisk>
  <FloppyDrive>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </FloppyDrive>
  <ZipDrive>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </ZipDrive>
  <TapeDrive>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </TapeDrive>
  <OtherMagnetic>
    <geometry>string</geometry>
    <partitionCount>-32768</partitionCount>
  </OtherMagnetic>
</Magnetic>
</Storage>
<NetworkCard>
  <mac>string</mac>
  <typeNcfs>string</typeNcfs>
</NetworkCard>
<AddonCard>string</AddonCard>
<Application>
  <name>string</name>
  <manufacturer>string</manufacturer>
  <version>string</version>

```

```

    <logicalLocation>string</logicalLocation>
</Application>
<NetworkConnection>
  <clientServer>true</clientServer>
  <ip>-9223372036854775808</ip>
  <state>string</state>
  <alive>string</alive>
</NetworkConnection>
<OS>
  <typeNcfs>string</typeNcfs>
  <revision>string</revision>
  <upTime>-32768</upTime>
  <ip>-9223372036854775808</ip>
  <DigitalArtifact>
    <typeNcfs>string</typeNcfs>
    <revision>string</revision>
    <upTime>-32768</upTime>
    <ip>-9223372036854775808</ip>
    <VirtualSystem>
      <typeNcfs>string</typeNcfs>
      <revision>string</revision>
      <upTime>-32768</upTime>
      <ip>-9223372036854775808</ip>
    </VirtualSystem>
  </Allocated>
    <typeNcfs>string</typeNcfs>
    <revision>string</revision>
    <upTime>-32768</upTime>
    <ip>-9223372036854775808</ip>
  <File>
    <filename>string</filename>
    <startSector>-9223372036854775808</startSector>
    <cDate>1999-01-21</cDate>
    <cTime>13:20:00-05:00</cTime>
    <mDate>1999-01-21</mDate>
    <mTime>13:20:00-05:00</mTime>
    <aDate>1999-01-21</aDate>
    <aTime>13:20:00-05:00</aTime>
    <logicalLocation>string</logicalLocation>
    <applicationAssociation>string</applicationAssociation>
    <deleted>true</deleted>
    <attribute>string</attribute>
    <examinerComments>string</examinerComments>
    <bookmarkType>string</bookmarkType>
    <preview>string</preview>
    <pageBreak>string</pageBreak>

```

```
<showPicture>string</showPicture>
<entrySelected>string</entrySelected>
<fileOffset>-32768</fileOffset>
<length>-2147483648</length>
<name>string</name>
<filter>string</filter>
<inReport>string</inReport>
<fileExtExe>string</fileExtExe>
<fileType>string</fileType>
<fileCategory>string</fileCategory>
<signature>string</signature>
<description>string</description>
<isDeleted>string</isDeleted>
<lastAccessed>string</lastAccessed>
<fileCreated>string</fileCreated>
<lastWritten>string</lastWritten>
<entryModified>string</entryModified>
<fileDeleted>string</fileDeleted>
<fileAcquired>string</fileAcquired>
<logicalSize>-9223372036854775808</logicalSize>
<initializedSize>-9223372036854775808</initializedSize>
<startingExtent>string</startingExtent>
<fileExtents>-32768</fileExtents>
<permissions>-32768</permissions>
<references>-32768</references>
<physicalLocation>-9223372036854775808</physicalLocation>
<physicalSector>-9223372036854775808</physicalSector>
<evidenceFile>string</evidenceFile>
<fileIdentifier>-2147483648</fileIdentifier>
<codePage>-32768</codePage>
<hashValue>string</hashValue>
<hashSet>string</hashSet>
<hashCategory>string</hashCategory>
<fullPath>string</fullPath>
<shortName>string</shortName>
<uniqueName>string</uniqueName>
<symbolicLink>string</symbolicLink>
<isDuplicate>string</isDuplicate>
<isInternal>string</isInternal>
<isOverwritten>string</isOverwritten>
<bookmarkPath>string</bookmarkPath>
<bookmarkStart>-9223372036854775808</bookmarkStart>
<bookmarkSector>-9223372036854775808</bookmarkSector>
<notable>string</notable>
</File>
</Allocated>
```

```
<Unallocated>
  <typeNcfs>string</typeNcfs>
  <revision>string</revision>
  <upTime>-32768</upTime>
  <ip>-9223372036854775808</ip>
</Unallocated>
<Slack>
  <typeNcfs>string</typeNcfs>
  <revision>string</revision>
  <upTime>-32768</upTime>
  <ip>-9223372036854775808</ip>
<RamSlack>
  <typeNcfs>string</typeNcfs>
  <revision>string</revision>
  <upTime>-32768</upTime>
  <ip>-9223372036854775808</ip>
</RamSlack>
<FileSlack>
  <typeNcfs>string</typeNcfs>
  <revision>string</revision>
  <upTime>-32768</upTime>
  <ip>-9223372036854775808</ip>
</FileSlack>
</Slack>
</DigitalArtifact>
</OS>
</ComponentNcfs>
</SystemNcfs>
```

Conclusions

The result of our work is a prototype of a DEML model that can be used by the justice and public service communities (or any interested parties) to model and share information related to computer-related crimes. This OO model includes hardware, component, and data artifact related classes. The ultimate goal of our research is exemplified in our XML model. Note that we also developed an XML front end (using the NIEM website) that allows users to access our model. Below we discuss our findings and future research directions.

Discussion of Findings

Our prototype model is a schema based on XML that supports the standardization of digital evidence-related artifacts. We developed our using an object-oriented representation of digital evidence and associated media and technology, relying upon existing and accepted sources (e.g., *Best Practices of Seizing Electronic Evidence, U.S. Secret Service, Volume 2*, several forensic tool suites, and law enforcement forensic examiners) to identify classes and class properties. We employed the Unified Modeling Language as a basis for a graphic representation of our model. UML supports the creation of class diagrams, which are hierarchical representations of classes, along with associations between classes, their objects, and associated properties. We translated the class diagrams into an XML representation to serve as an extensible plug-in to GJXDM. This prototypes XML code is hosted on National Information Exchange Model (NIEM) website.

Because the one of the charters of NIJ is to assist local and state law enforcement, we developed our prototype model with practicality in mind, i.e., a model that is easily understood by local and state law enforcement (rather than a purely academic/theoretical perspective), and is therefore more likely to be employed by forensics examiners, law enforcement, and the courts, as a means to identify and describe digital evidence.

Implications for Policy and Practice

Justice and public service communities are cognizant of the need to share information across agency boundaries to increase efficiency in fighting crime. The problem is not lack of recognition, but **how** to share information. In a similar fashion, one of the biggest problems in information technology for any large company is sharing information across departmental/corporate boundaries. This is much easier for companies because they typically have larger IT budgets, and have a common corporate information culture (through a common CIO or CTO). The same cannot be said of the typical law enforcement agency, which must decide between spending money on squad car maintenance, more officers on the street, or computer technology.

There are several examples of successful information sharing projects across law enforcement agencies. The FBI's CODIS (Combined DNA Index System) is a database composed of DNA profiles, and is accessible to most law enforcement agencies. Hundreds of law enforcement agencies have used CODIS to identify perpetrators of crimes. Agencies can upload new DNA profiles and search through the database of millions of profiles seeking a match. One of the reasons behind CODIS's success is it uses a common, structured, language for representing DNA profiles.

Another successful information sharing project is FINDER. First deployed in 2004, Finder was created by professors from the University of Central Florida and local law enforcement, and uses a similar XML schema (based on GJXDM) to share information about pawn shop purchases. Similar to CODIS, FINDER allows law enforcement agencies to upload, search, and share information about pawn shop sales and purchases across agency boundaries. FINDER has proven successful in assisting law enforcement agencies to identify stolen property attempting to be sold to pawn shops, as well as identifying individuals on parole or probation who were outside their court ordered restricted space (usually a nearby county).

As more law enforcement agencies become more technically savvy (e.g., by hiring younger personnel who grew up on computers), there will be a more urgent call for information sharing. DEML is one small step in providing a common language that can be employed in place, or better yet, included in other model or implementations (like FINDER) as a way of expanding information sharing capabilities.

Implications for Future Research

Future development on information sharing should include extensions of our DEML to cover new technologies as well as the addition of new technologies not covered in our model. As suggested in the section above, DEML should be used as an extension of existing information sharing models, such as the FINDER model as means of creating a more encompassing means of capturing and sharing information possibly related to a crime.

Acknowledgements

We would like to thank Mark Pollitt (FBI, retired), Officer Eric Walton (Florida Electronic Crimes Task Force), Chris Marberry (ManTech), and Paul Burke (MIT Lincoln Labs) for feedback and input in the early stages of this research.

References and Additional Readings

- J. Bosworth and M.E. Kabay (Eds.). Computer Security Handbook. New York: Wiley.
- M. Caloyannides. (2002). Computer Forensics and Privacy. Artech House Computer
- M. Caloyannides. (2003). Desktop Witness. Artech House Computer Security Series.
- E. Casey. (2001). Digital Evidence and Computer Crime. Academic Press.
- E. Casey. (2002). Handbook of Computer Crime Investigation: Forensic Tools and Technology. Academic Press.
- E. Casey, T. Larson, & T. Long. (2002). Network analysis. In E. Casey (Ed.), Handbook of Computer Crime Investigation. Academic Press.
- Computer Security Incident Handling Guide. NIST: Gaithersburg, MD.
- P. Craiger. (May 2004). Linux: Portable forensics Toolkit. Presentation accepted for the 26th Annual Department of Energy Computer Security Training Conference. St. Louis, MO.
- P. Burke and P. Craiger. Xbox forensics. Journal of Digital Forensics Practice, New York, Taylor & Francis, 4, pp. 275-282, 2007.
- C. Marberry and P. Craiger. CD-R acquisition hashes affected by write options. Journal of Digital Forensics Practice, New York, Taylor & Francis, 4, pp. 1-10. 2007.
- S. Conrad, G. Dorn, and P. Craiger. Forensic analysis of PlayStation 3 Game Console. In G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics VI, Springer, New York. To appear.
- P. Craiger, Digital Evidence. In H. Bigdoli (Ed.), Handbook of Technology Management. Vol 2. New York: John Wiley & Sons, pp. 921-930, 2010.
- G. Dorn, C. Marberry, S. Conrad, and P. Craiger. Forensic analysis of virtual machines impact on host machine. In G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics V, Springer, New York. pp. 69-82. 2009.
- S. Conrad, C. Rodriguez, C. Marberry, and P. Craiger. Forensic analysis of the Sony Playstation Portable. In G. Peterson and S. Shenoi (Eds.), Advances in Digital Forensics V, Springer, New York. pp. 119-132. 2009.
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), Handbook of Digital and Multimedia Evidence. Humana Press, pp. 11-22. 2008

- P. Burke and P. Craiger, Forensic Analysis of Xbox Consoles. In P. Craiger and S. Sheno (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 269-280. 2008.
- C. Maryberry and P. Craiger, Burn Options Affect Cryptographic One-way Hashes of CD-R Media. In P. Craiger and S. Sheno (Eds.), *Advances in Digital Forensics III*, Springer, New York. pp. 149-161. 2008.
- P. Craiger, Training and Education in Digital Forensics. In J. Barbara (Ed.), *Handbook of Digital and Multimedia Evidence*. Humana Press, pp. 11-20. 2008.
- P. Craiger and P. Burke, Mac OS X Forensics. In M. Olivier and S. Sheno (Eds.), *Advances in Digital Forensics II*, Springer, New York, 159-170, 2006.
- P. Burke and P. Craiger, Trace evidence of secure delete programs. In M. Olivier and S. Sheno (Eds.), *Advances in Digital Forensics II*. Springer, New York, 185-198, 2006.
- P. Craiger, Computer forensics methods and procedures In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 736-755, 2006.
- P. Craiger, M. Pollitt and J. Swauger, Digital Evidence and law enforcement In H Bigdoli, (Ed), *Handbook of Information Security*, New York, John Wiley and Sons, 2, pp. 739-777, 2006.
- P. Craiger, Recovering digital evidence from Linux systems, In S. Sheno and M. Pollitt (Eds), *Advances in Digital Forensics*, New York, Springer, pp. 233-243, 2006.
- P. Craiger, J. Swauger, and C. Marberry. Digital forensic software tool validation. In P. Kanellis (Ed) *Digital Crime and Forensic Science in Cyberspace* Idea Group, 91-108, 2006.
- P. Craiger, P. Burke, and C. Marberry. Forensics Analysis of Phishing Cases Using Open Source and Free Tools. *Anti-phishing and Online Fraud. Journal of Digital Forensics Practice*, New York, Taylor & Francis, 223-230, 2007.
- P. Craiger. (Sept, 2002). An applied course in network forensics. Presentation for the Workshop for Dependable and Secure Systems. University of Idaho, Moscow, Idaho, Sept 23-35.
- P. Craiger, & M. Pollitt (to appear). Computer forensics and law enforcement. In H. Bigdoli (Ed.), *Handbook of Information Security*. John Wiley & Sons. Dartmouth Institute for Security Technology Studies. (2002). Law Enforcement Tools And

- Department of Energy. (2002). First Responders Guide. Department of Energy
Computer
- Dittrich, D. (2001). Basic Steps in Forensic Analysis of Unix Systems.
- D. Farmer, & W. Venema. (April, 2001). Being prepared for intrusion. Dr. Dobb's Jour-
- D. Farmer, & W. Venema. (Sept., 2000). Forensic computer analysis: An introduction. Forensic Laboratory.
- S. Furnell. (2002). Cybercrime: Vandalizing the Information Society. Upper Saddle River, NJ: Prentice-Hall.
- T. Grance, K. Kent, & B. Kim. (2004). National Institute of Standards and Technology
- B. Grundy. (2002). The Law Enforcement Introduction to Linux: A Beginner's Guide.
- K. Hardy & S. Kreston. (2001). Using Analogy to Explain Computer Forensics: Techniques used to explain computer jargon to courtroom juries. National District Attorney's Association. www.ndaa.org. Last visited 12/28/03.
- K. Jones, M. Shema & B. Johnson. (2002). Anti-hacker Toolkit. San Francisco: Keeney, M. et al. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. Carnegie Mellon SEI, May 2005.
- E. Kowalski, et al. Insider Threat Study: Illicit Cyber Activity in the Government Sector Carnegie Mellon SEI, January 2008.
- E. Kowalski, et al. Insider Threat Study: Illicit Cyber Activity in the Government Sector Carnegie Mellon SEI, January 2008.
- E. Kowalski, et al. Insider Threat Study: Illicit Cyber Activity in the Information Technology and telecommunications Sector. Carnegie Mellon SEI, January 2008.
- W. Kruse III & J. Heiser. (2001). Computer Forensics: Incident Response Essen-
- T. Larson. (2002). The other side of civil discovery. In E. Casey (Ed.), Handbook of Computer Crime Investigation. Academic Press.
- J. Lucas, & B. Moeller. (2004). The Effective Incident Response Team. Boston, MA: Addison-Wesley.
- A Marcella Jr., & R. Greenfield. (2002). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes.
- National Information Exchange Model. www.niem.gov.

Unified Modeling Language. www.uml.org.

J. Morris. (February 11, 2003). Forensics on the Windows Platform, Part Two. [www
http://computersight.com/software/forensic-analysis-of-a-windows-system-part-two/](http://computersight.com/software/forensic-analysis-of-a-windows-system-part-two/).

J. Morris. (January 28, 2003). Forensics on the Windows Platform, Part One.
www.securityfocus.com/printable/infocus/1661

S. Mueller. (2003). Upgrading and repairing PCs. New York: Que.

B. Nelson, A. Phillips, F. Enfinger, & C. Steuart. (2004). Guide to Computer Forensics.

U.S. Department of Justice. (July, 2002.) Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Computer Crime and Intellectual Property Section. Criminal Division, United States Department of Justice.

U.S. Secret Service. (2002). Best Practices Guide to Seizing Electronic Evidence, Version 2. <http://www.cio.com/securitytools/BPGv2.pdf> Last visited: December 29, 2003.

Dissemination of Findings

Our model was developed and uploaded to the National Information Exchange website (www.niem.gov). The model may be viewed and downloaded from that site.

Recall that one of the desirable outcomes of this research was to create a model that extensible. This means that it is quite simple to create additional components of the model, and to link them with existing model components. This is achievable because the NIEM XML format allows individual users (at least those who understand NIEM, XML and/or OO modeling and UML) to create their own class diagrams, export that to XML, and then upload this model to NIEM, thereby creating an extension of XML. This is important as technology evolves, it will be important to update the model. However, it is not necessary to create a new DEML or to replace it, as our model serves as a foundation for the description of digital evidence. Our prototype model

Digital Evidence Markup Language (DEML)

serves as a common foundation for all new technology changes that weren't included in the original model.