UDC 004.822:004.056
Preliminary Communication Article

An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence

Jasmin Ćosić *jascosic@bih.net.ba*
Ministry of the Interior of Una-sana canton
IT Section of Police Administration, Bihać,B&H

Zoran Ćosić *zoran.cosic@statheros.hr*
"STATHEROS",d.o.o.
Kaštel Stari, Split, Croatia

Miroslav Bača *miroslav.baca@foi.hr*
University of Zagreb
Faculty of Organization and Informatics Varaždin, Croatia

Abstract

Chain of custody of digital evidence in digital forensic field are today essential part of digital investigation process. In order the evidence to be accepted by the court as valid, chain of custody for digital evidence must be kept, or it must be known who exactly, when, where, why and how came into contact with evidence in each stage of the digital investigations process. This paper deals with digital evidence and chain of custody of digital evidence. Authors define taxonomy and use an ontological approach to manage chain of custody of digital evidence. The aim of this paper was to develop ontology to provide a new approach to study and better understand chain of custody of digital evidence . Additionally, developed ontology can be used as a method to further develop a set of standard and procedures for secure management with digital evidence.

Keywords: ontology, digital evidence, chain of custody of digital evidence, chain of evidence, digital forensic

1. Introduction

In today's world, digital forensic field relies on knowledge and knowledge management system as an important resource. The reason for this relies in fact that changes in digital technologies are in everyday occurrence and knowledge and knowledge management enable to create appropriate standards and procedures. Therefore is necessary to form new concepts and ideas from the existing information acquired from the existing knowledge. Ontology play an important role in creating a common definition among the domains of information in a particular area.

According to Gruber [9] ontology is explicit specification of a conceptualization process. The term is borrowed from philosophy, where Ontology is a systematic accounting of existence. There are two types of ontology. One starts with "O" and the other starts with "o" [10]. Accordingly [19] an important distinction should be made between an ontology written with "O" as compared that with "o". The "ontology" with lower case "o" describes situation in which knowledge is acquired for the purposes of organization or classification [1].

The ideas presented in this paper is to use a lower case "o" for presenting a ontology of digital evidence and chain of custody of digital evidence. Digital forensic and ontology are two normally unrelated topics. Ontology congruent to this paper is method that will help to better understanding and defining terms of digital forensic either digital evidence and chain of custody of digital evidence. Main goal is to define a taxonomy diagram of chain of custody of digital evidence that will be a central point for further work on this research.

There are many reasons for the presentation of this ontology. Digital evidence has experienced drastic changes over the last few years, particularly from the aspect of their existence and retrieval. At the beginning of digital forensics (25 years ago) digital evidence could be found on computers, then the external data carriers (CD,FDD, JAZZ, etc.), creation of networks and the Internet have moved them to the "clouds" and they are now found in almost all "embedded" systems (mobile phones, book readers, PDAs, MP3/MP4 players, smart phones, etc.). Therefore, this evidence is harder and harder to find. Another reason for establishing this ontology is the integrity of digital evidence - preservation of "chain of custody", which has become almost impossible today, because of easy modification and destruction this kind of evidence. The authors have also addressed these issues.

2. Related work on ontology in digital forensic field

There is a lack of scientific paper about using domain ontology in digital forensic field. Reasons for this is a multidisciplinary field of digital forensics, because knowledge of the technical aspects are not enough, it is necessary to know the law - legal aspects and implications of the process of presenting digital evidence in court. Some authors in scientific papers tried to present the groundwork for the "ontology of cyber forensics, digital forensics" and "ontology of small-scale devices”. The aim was to define the basic concepts and create a new approach to the study of the scientific field.

Heum Park et al. [17] in Cyber forensic ontology for cyber criminal investigation develop Cyber Forensic Ontology for the cyber investigation in cyber space. Cyber crime is classified into two classes - cyber terror and general cyber crime. Those two classes are connected with each other. Investigation of cyber terror requires high technology, system environment and experts. General cyber crime is connected with general crime by evidence (digital evidence). Authors defined the concepts and relations among crime types, evidence collection, criminals and crime case and law. The limitation of this ontological model is that it is less based on digital evidence and other phases that are important in the process of digital investigation and it is related to dealing with digital evidence. The only stage in the process of dealing with digital evidence, which authors mention is "collection", while they ignored all other phases (identification, searching, transporting, storing, examination, analysis and presentation).

David Christopher Harrill and Richard P. Mislan [11] presented small scale digital device forensics ontology in 2007, in order to develop an ontological to provide law enforcement with the appropriate knowledge regarding the devices found in the SSDD (Small Scale Digital Devices) domain. The paper categorized SSDDs according to certain criteria and gave detailed description of each of them. The purpose of this paper was to provide a guiding framework in which to place small scale digital devices. According to authors this ontology can be used as a method to further develop a set of standard and procedures at which to approach SSDD.

Ashley Brinson et al.[2] in 2007 developed the cyber forensic ontology for the purpose of finding the correct layer for specialization, certification and education within the cyber forensic domain. Topic of cyber forensic consisted of two subtopics: technology and profession. Technology subtopic is broken down into hardware and software. Profession side is broken down into law, academia, military and private sector. Hardware section of his model is broken up five different parts: large scale digital devices, small scale digital devices, computers, storage devices and obscure devices. The software section of his model contains three categories: analysis tools, operating system and file system. The law section focuses on law enforcement and courts and legal aspects of cyber forensic. Profession academia is broken down in research and education, while a military categories focuses on what cyber forensic duties military personnel perform. Military section can be defensive and offensive. Private sector was broken down into consulting and industry. This ontological model can be utilized for the purpose of curriculum development.

DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge by Kahvedzic and Kechadi [14] provides a general, application independent vocabulary that can be used to describe an investigation at different level of detail. His framework is defined to encapsulate all concepts of the digital forensic field and the relationship between them. Presented model encapsulates the knowledge associated with digital investigation cases. Paper and presented ontology are based on modeling the Windows registry and registry structure and authors limit the scope of this paper to the encoding of forensics knowledge associated with the Windows Registry.

3. Definition of basic concept related to this paper

There are so many definitions of digital forensic and digital evidence. One of many definitions is „digital forensic can be defined as the application of science and engineering to the legal problem of digital evidence“ [13].

According to Pollit and Whiteledge [18] „digital forensic is the science of collecting, preserving, examining, analyzing and presenting relevant digital evidence for use in judicial proceedings“. Digital forensics is no longer associated only to a laboratory in police and security agencies, but it is also used outside that area. Some areas where digital forensic play important role are: insurance companies, banks and corporates [6].

Digital evidence is defined as any data stored or transmitted using a computer that support of refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi [3]. The definition proposed by the Standard Working Group on Digital Evidence (SWGDE) is any information of probative value that is either stored or transmitted in a digital form [23]. Another definition proposed by the International Organization of Computer Evidence - IOCE is „...information stored or transmitted in binary form that may be relied upon in court“ [12].

In all phases of forensic investigation, digital evidence is susceptible to external influences and coming into contact with many factors. Legal admissibility of digital evidence is the ability of that evidence to be accepted as evidence in a court of law. The evidential weight of digital evidence can only be safeguarded if it can be proven that the records are accurate i.e. by whom they were created and when and that no alteration has occurred. In order for the evidence to be accepted by the court as valid, chain of custody for digital evidence must be kept, or it must be *known who exactly, when and where* came into contact with evidence in each stage of the investigation [8].

For the purposes of this paper "chain of custody" and "chain of evidence" would be considered like synonyms. The phrase “chain of custody” or “chain of evidence” refers to the accurate auditing control of original evidence material that could potentially be used for legal purposes. Some authors use a term „chain of evidence „instead of chain of custody .The purpose of testimony concerning chain of custody is to prove that evidence has not been altered or changed through all phases, and must include documentation on how evidence is gathered, how was transported, analyzed and presented. Knowing the current location of original evidence, is not enough for court, there must be accurate logs tracking evidence material at all time. Access to the evidence must be controlled and audited.

To prove the chain of custody, we must know all the details on how the evidence was handled every step of the way. The old formula used by police, journalists and researchers - Who, What, When, Where, Why, and How - "Five Ws" (and one H) can be applied to help in digital forensic investigation [5].

For the better understand this problem, here is one example of chain of custody of digital evidence:

SUBJECT is a owner of one IMAGINARY company. SUBJECT gave his laptop to an employee to take it to COMPUTER REPAIR COMPANY for display problems. Upon *repairing the laptop, COMPUTER REPAIR COMPANY started the laptop to ensure it had been fixed. A standard procedure of COMPUTER REPAIR COMPANY was to go to the Recent Items menu on the Start button of Windows® systems and select files for viewing. COMPUTER REPAIR COMPANY was presented with what appeared to be an image of a young child depicted in a sexually explicit manner. COMPUTER REPAIR COMPANY telephone the local police station. A police officer responded and observed the image and confirmed it to be a violation of a Low. The laptop was seized because it contained images of child pornography. The laptop was entered into evidence according to agency policy, and a search warrant was obtained for the examination of the computer. The computer was submitted for examination. At this time (before the investigation began) access to the lap-top has a owner-SUBJECT, two employee from COMPUTER REPAIR COMPANY, police officer from local police station and two random bystanders. In the process of digital investigations access to the lap-top and files on lap-top will have forensic investigators, court expert witness, prosecution, defense, court and other law enforcement personnel. That will be about 10-15 different personnel that can violate chain of custody of digital evidence. The court will interest what, who, when, where, how and why access to the lap-top and files on lap-top?*

Integrity of digital evidence is most important part of chain of custody. According to Vanstone [15], digital integrity is “the property whereby digital data has not been altered in an unauthorized manner since the time it was created, transmitted, or stored by an authorized source”. Scientific Working Group of Imaging Technology define that “The integrity of digital evidence ensures that the information presented is complete and unaltered from the time of acquiring until its final disposition”.

There are several adapted methods for digital signing an evidence in order to (im)prove its integrity:

- CRC (Cyclic Redundancy Check)
- Hash function
- Digital signature
- Timestamp
- Encryption
- Watermarking

Today most forensic tools and applications implement some type of checksum or hashing algorithm to allow investigators later to verify the disk or image integrity. A cryptographic hashing function or algorithm has the following technical characteristics [Table 1]. These functions are the most common ways to ensure integrity of digital evidence.

Method	Length	Description	Advantages	Disadvantages
Cyclic redundancy checks: CRC 16 CRC 32 CRC 64	16 bit 32 bit 64 bit	Circular Redundancy Check – CRC often used in file transfer to verify that the data transfer was successful.	Very simple to use Very fast Small data in output	Non secure hash function Problem with *message analysis* It is easy to generate other *messages* that result in the same CRC
Cryptographic hash function: MD2 MD4 MD5 SHA1 SHA224/256 SHA384/512	128 bit 128 bit 128 bit 160 bit 224/256 bit 384/512 bit	Hashing function – establishing mathematical calculation that generates a numerical value based on the input data. This numerical value is referred to as the hash value.	It is easy to compute the hash value for any given message Secure hash function Cryptographic hash function	Collision and Preimage attack , except SHA 224/256 and SHA 384/512 [5]

Digital signature	Depending on the used hash function	The resulting hash (process used in a hash) is encrypted with a specific private key. File integrity can be verified using hash value and the public key.	Binding identity to the integrity	Very slow Very complex to implement
Time stamp	Depending on the used hash function	Time stamps are typically used for logging events, in which case each event in a log is marked with a time stamp. In file systems, time stamp may refer to the stored date/time of the file creation or modification. Trusted time stamping is the process of securely keeping track of the creation and modification time of a document.	Bind date and time with integrity	Very complex to implement Dependence on the “third party”
Encryption	Depending on the used algorithm.	Encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as the key. The result of the process is encrypted information. Encryption itself can protect the confidentiality of messages.	Very secure	Very slow Complex to implement and maintain
Watermarking	Depending on the used algorithm.	Watermarking is the process of embedding information into another object/signal. It combines aspects of data hashing and digital watermarking.[6]	Very secure and simple to use	User cannot significantly alter some files without sacrificing the quality or utility of the data.

Table 1 Methods for digitally signing a evidence [4]

Every function has a advantage and disadvantage, and can be used in combination [4]. At any time, we must have an answer, when we are asked by the court or lawyer, when the contact with evidence happens?

Investigator or other personnel, who will eventually present his/her investigation hypothesis to the court, must be able to accurately describe not only those who handle the evidence, but *when* and *where*, and *what* happened regarding this. If he/she is not able to explain and prove that, the court will not accept evidence and the whole investigation is in vain.

4. Ontological approach to study chain of custody of digital evidence

As we already mentioned in the earlier part of the paper ontology is the explicit specification of a conceptualization of the real word. Ontology is word borrowed by computing for the explicit description of the conceptualization of a domain:

- concepts
- properties and attributes of concepts
- constraints on properties and attributes
- individuals (often, but not always)

Ontology defines

- a common vocabulary
- a shared understanding

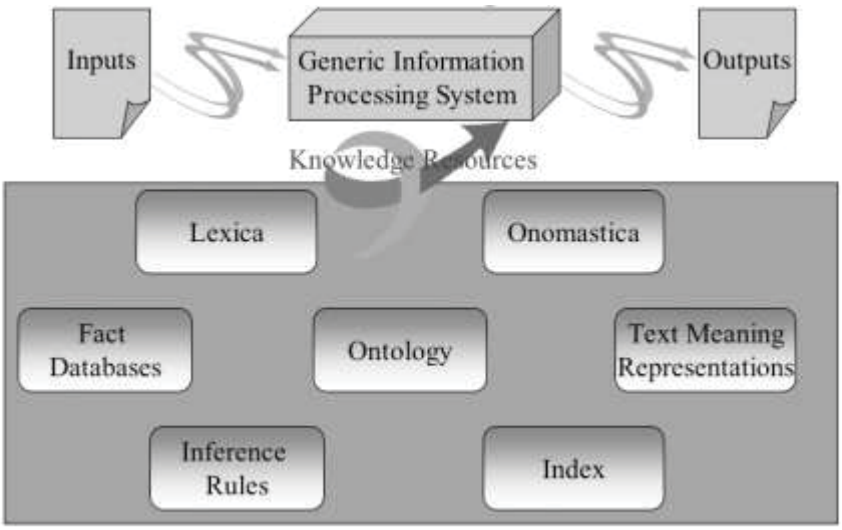


Figure 1 Application of the Ontological Paradigm to a Domain [20]

Figure 1 above shows a generic scheme of interaction of the ontological resources applied to a conceptual domain, such as information security. This scheme also can be used for digital forensic domain.

There is a lot of reason why we develop this ontology. Some of them are:

- To share common understanding of the structure of descriptive information
  - among people
  - among software agents
  - between people and software
- To enable reuse of domain knowledge
- To make domain assumptions explicit
- To separate domain knowledge from the operational knowledge
- To manage the combinatorial explosion
  - to avoid "re-inventing the wheel"
  - to introduce standards to allow interoperability [21]

Ontology includes machine-interpretable basic concepts definition in the domain and relations among them [16].

In this paper we define taxonomy and use an ontological approach to manage chain of custody of digital evidence. It was necessary to use some software tools for this purpose. We use a Protégé[1] [19]. Protégé is a free, open-source platform that provides a growing user community with a suite of tools to construct domain models and knowledge-based applications with ontology. Protégé was developed by Stanford Center for Biomedical Informatics Research at the Stanford University School of Medicine. Protégé, exists already

[1] CO-ODE Project - http://www.co-ode.org/.

about 20 years and today is widely used. It is made in Java, it's free and open source. It was originally developed to support knowledge acquisition for specialized medical expert systems, but today it has many plug-ins for various features, from making constraints on attribute values to exporting ontology in different formats (CLIPS, OWL, RDF, RDF Schema and HTML are delivered in standard distribution) and importing concepts from other tools into Protégé. It can be used as a basis for KBS development [22].

Figure 2,3 present an ontology graph – taxonomy diagram of digital chain of custody concepts. We use this classification schemes to make things easier to find and to add value to a group of objects. By adding value we mean that a classification (describing a group) may provide more information about the members of that group that is obvious from an analysis of a member. The ontology graph displays a domain ontology that matches concepts to help users determine their current problem. The ontology graph depicts hierarchical relations as arrows. The proposed DCoDeOn model (see Fig 2.3.) consists of few layers. There are five most important things in a chain of custody of digital evidence process on the top of hierarchy:

- *Characteristics*
- *Dynamics*
- *Factors*
- *Institutions*
- *Integrity*

This hierarchical structure is top-down based.

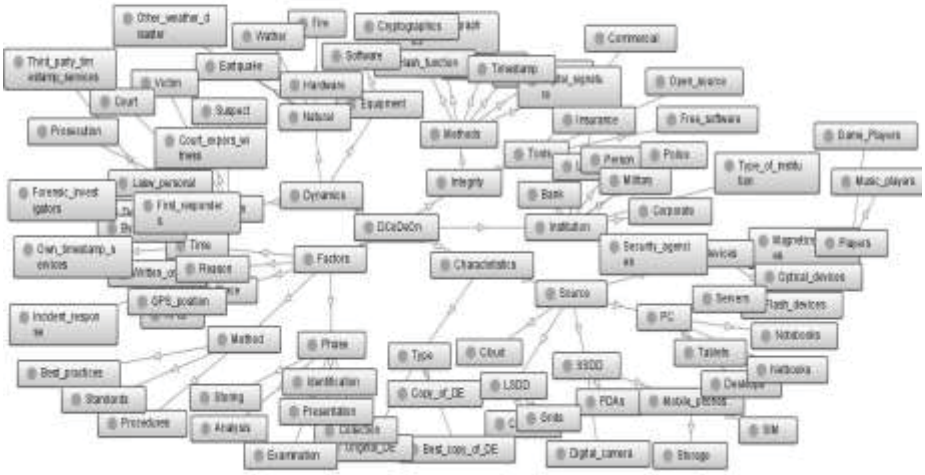


Figure 2 Ontology implementation and components (OntoGraph of CoDEOn)

A First section - C*haracteristic* is broken into S*ource* and T*ype*. *Source* can be a:

- *LSDD (Large Scale Digital Devices)*
- *SSDD (Small Scale Digital Devices)*
- *PC*
- *Devices*
- *Cloud*

and *Type* can be a:

- *Original_DE*
- *Best_copy_DE*
- *Working_copy_DE*

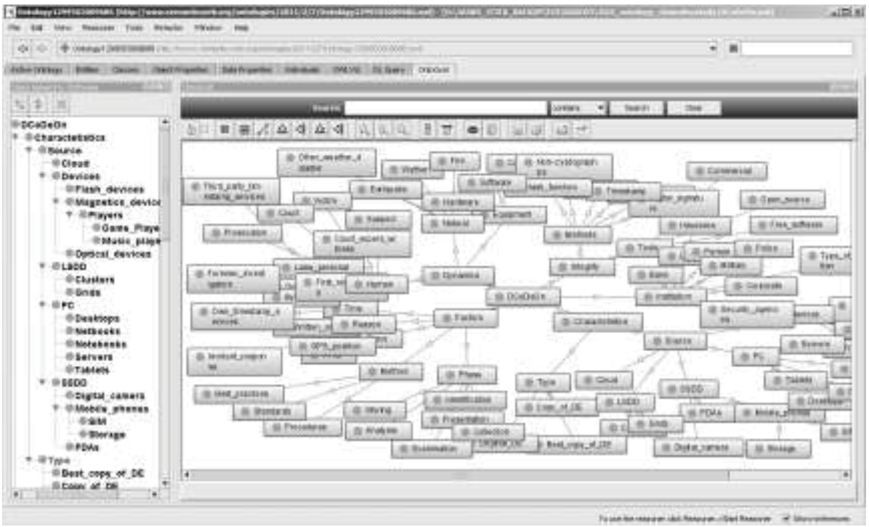


Figure 3 Ontology implementation (taxonomy diagram) of Digital Chain of Custody Concept (DCoDeOn) with Protégé

Large Scale Digital Devices (LSDD) is still broken into *Clusters* and *Grids*. *Small Scale Digital Devices* is broken into:

- *Digital_camera*
- *Mobile_phones (SIM,Storage)*
- *PDAs*
- *Players (Music_players, Game_players)*

Personal Computer (PC) is broken down into:

- *Tablets*
- *Netbooks*
- *Notebooks*
- *Desktop*
- *Servers*

A *cloud* can be any virtual space – internet, intranet, extranet etc. *Devices* can be:

- *Magnetic_devices*
- *Flash_devices*
- *Optical_devices*

Second section - *Dynamics* is broken down into *Equipment* (hardware and software) , *Human and Natural dynamics*.

Human dynamics can be:

- *First_responders*
- *Forensic_investigations*
- *Court_expert_witness*
- *Law_personal*
- *Prosecution*
- *Defense*
- *Court*
- *Suspect*
- *Victim*

- *Bystanders*

Natural dynamics is broken down into:

- *Earthquake*
- *Fire*
- *Wather*
- *Other_weather_disasters*

Third section *Factors* is very important because digital evidence management is broken into few factors that may answer on Five Ws [24] question . Five Ws (and One H) must provide an answer to key question:

- What is the digital evidence
- Where are the digital evidence
- Who manage (make contact) with digital evidence
- Why (reason) to do it
- When digital evidence is handled
- How is handled with digital evidence

Chain of Digital evidence (CoDe) can be presented like a function of secure management that consists of few factors:

- Fingerprint of digital evidence
- Biometrics characteristics
- Time stamp
- GPS locations of person who handles evidence
- Write order or incident response - reason (Why) and
- Standards, set of procedures and best practices.

This function can be presented as:

```
CoDe = f {  fingerprint _of _file,              //what
            biometrics_characteristic,          //who
            time_stamp,                         //when
            gps_location,                       //where        [1]
            reason,                             //why
            set_of_procedures};                 //how
```

With this concept we ensure security of a chain of custody. We propose use of biometrics characteristic for digital signing (Who), timestamp for adding a time (When), use some of web services (Google map example, GPS coordinate) or some RFID device for geo location (Where) and hashing and asymmetric encryption for securing digital evidence. Reason can be a write order or incident response. All the time it must be used a standards, procedures and best practices.

Use of all these factors provide safe and secure chain of custody, to ensure that digital evidence will be accepted by the court.

Methods that must be complied in digital investigation process are:

- *Standards*
- *Procedures*
- *Best_practices*

There are few *Phase* in digital investigation process (management with digital evidence):

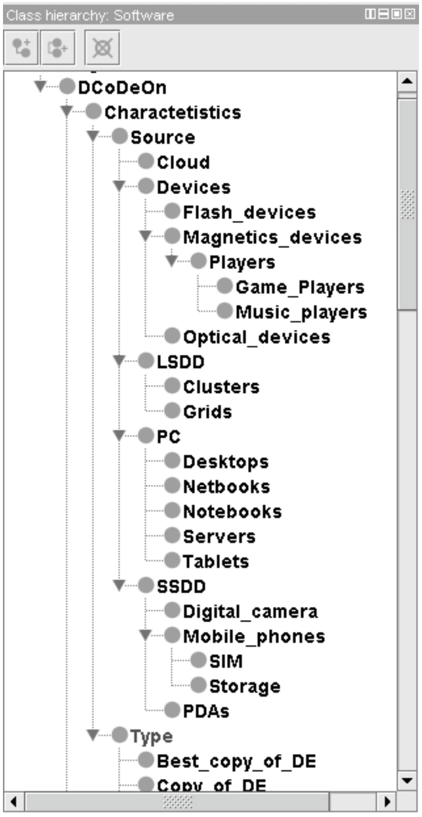
- *Analysis*
- *Collection*

- *Examination*
- *Identification*
- *Presentation*
- *Storing*

Each of these phases is equally important for chain of custody of digital evidence. *Place* can be identified by *GPS_location* or some of *RFID* devices. *Reason* can be *incident_response* or *written_order*.
Time of access to digital evidence (*When*) can be recorded with *timestamp_services* , that can be *own-service* and *third_party_services*. Answer to question *Who* made contact with digital evidence is a *Human_DE* and this is broken down in *biometrics_characteristics* (signature, fingerprint, iris etc…) or *non_biometrics_characteristics* (username, PID, etc…) of a person.

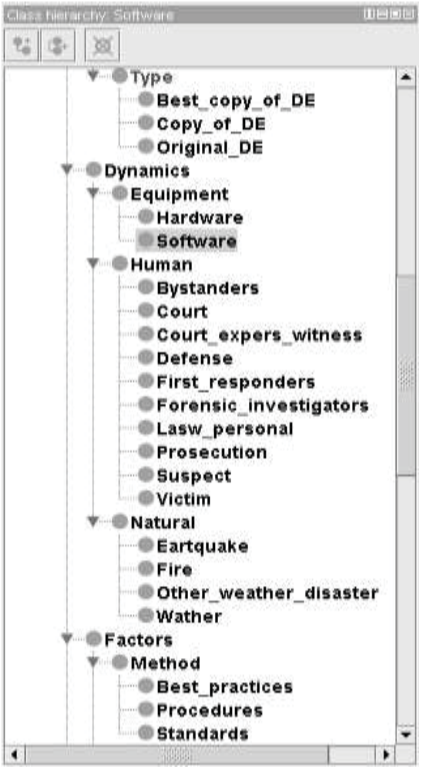
Section *Institution* is broken into:

- Bank
- Corporate
- Insurance
- Law
- Military
- Person
- Police
- Security_agencies



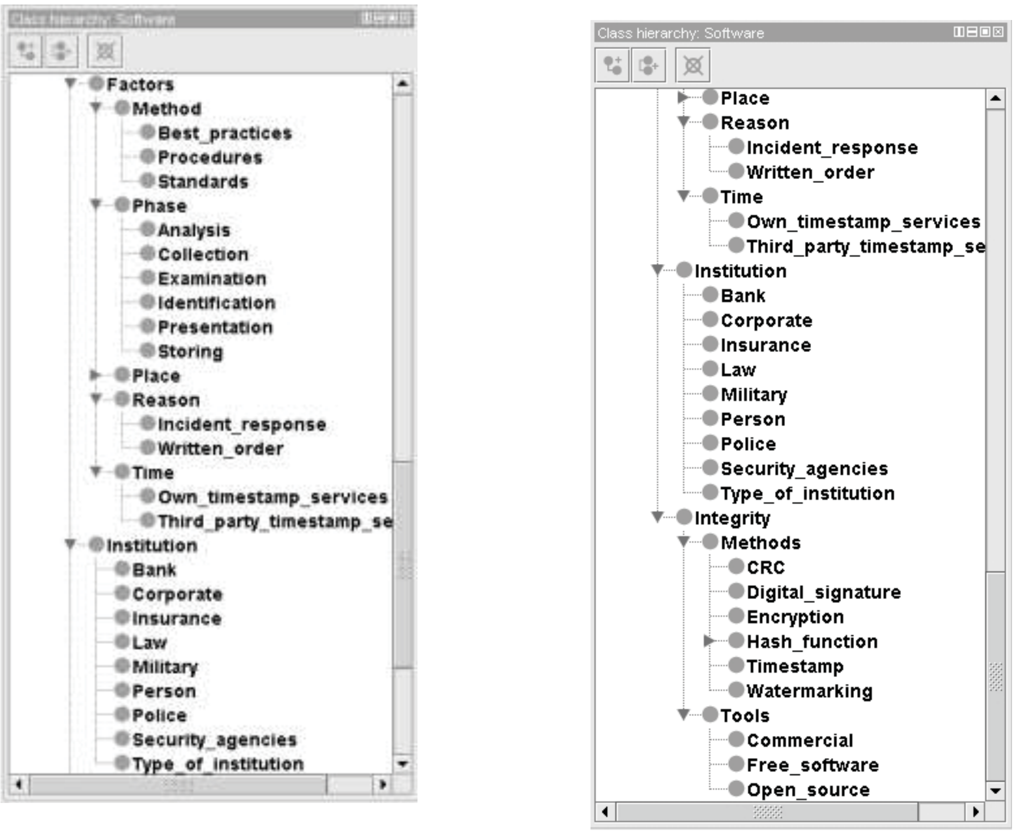
Class hierarchy: Software

```
DCoDeOn
  Charactetistics
    Source
      Cloud
      Devices
        Flash_devices
        Magnetics_devices
          Players
            Game_Players
            Music_players
        Optical_devices
      LSDD
        Clusters
        Grids
      PC
        Desktops
        Netbooks
        Notebooks
        Servers
        Tablets
      SSDD
        Digital_camera
        Mobile_phones
          SIM
          Storage
        PDAs
    Type
      Best_copy_of_DE
      Copy_of_DE
```



Class hierarchy: Software

```
    Type
      Best_copy_of_DE
      Copy_of_DE
      Original_DE
  Dynamics
    Equipment
      Hardware
      Software
    Human
      Bystanders
      Court
      Court_expers_witness
      Defense
      First_responders
      Forensic_investigators
      Lasw_personal
      Prosecution
      Suspect
      Victim
    Natural
      Eartquake
      Fire
      Other_weather_disaster
      Wather
  Factors
    Method
      Best_practices
      Procedures
      Standards
```



```
Factors
  Method
    Best_practices
    Procedures
    Standards
  Phase
    Analysis
    Collection
    Examination
    Identification
    Presentation
    Storing
  Place
  Reason
    Incident_response
    Written_order
  Time
    Own_timestamp_services
    Third_party_timestamp_se
Institution
  Bank
  Corporate
  Insurance
  Law
  Military
  Person
  Police
  Security_agencies
  Type_of_institution
```

```
  Place
  Reason
    Incident_response
    Written_order
  Time
    Own_timestamp_services
    Third_party_timestamp_se
Institution
  Bank
  Corporate
  Insurance
  Law
  Military
  Person
  Police
  Security_agencies
  Type_of_institution
Integrity
  Methods
    CRC
    Digital_signature
    Encryption
    Hash_function
    Timestamp
    Watermarking
  Tools
    Commercial
    Free_software
    Open_source
```

Figure 4 The different level of the DCoDEOn

Finally, the last , five section Integrity, which is also very important is divide into *Methods* and *Tools*. *Methods* for ensure integrity of digital evidence are:

- *CRC (Checksum redundancy check)*
- *Digital_signature*
- *Encryption*
- *Hash_function (cryptographic and non-cryptographic)*
- *Timestamp*
- *Watermarking [Table 1]*

Tools can be:

- *Commercial*
- *Freeware*
- *Open_source*

Figure 4 present a class hierarchy structure and different level of the DCoDEOn described in this paper. This structure is modeled top-down and presented in Protégé. The DCoDeOn (Digital Chain of Custody Digital Evidence Ontology) is designed in a way to simple insert new class (section). Slots (properties) can be defined in a class definition, property constraints, common facets (cardinality, value type etc.).

5. Summary

In this research authors deals with taxonomy (classification) of terms “chain of custody of digital evidence”. It is important because today chain of custody is essential and most vulnerable part of digital investigation process. Proposed taxonomy is modeled top-down;

most specific concepts were first defined and specialized afterwards. It was done a framework for developing ontology for chain of custody of digital evidence on the concepts of openness and modularity, so each new entity could be added in the future and described with attributes that are missing. With this ontology we can share common understanding of the structure of this domain (digital forensic) among forensic investigators and other personal that has to do with digital evidence, among software agents and between forensic investigator and software. It can also enable reuse of knowledge in digital investigation process.

The DCoDeOn (Digital Chain of Custody Digital Evidence Ontology) is designed in a way to simple insert new class (section). Slots (properties) can be defined in a class definition, property constraints, common facets (cardinality, value type etc.).

Acknowledgements

The presented research and results came out form the research supported by the Center for biometrics - Faculty of Organization and Information Science Varazdin, University of Zagreb.

References

[1] Brinson, A; Robinson, A; Rogers, M. A cyber forensic ontology: Creating a new approach to studying cyber forensic [Journal] // Digital investigation 3S. - 2006. - pp. 37-43.

[2] Brinson, A; Robinson, A; Rogers, M. A cyber forensic ontology: Creating a new approach to studying cyber forensic [Book Section] // Digital investigation 3S. - [s.l.] : Elsevier, 2006.

[3] Chisum, J. Crime Reconstruction and Evidence Dynamics [Conference] // Academy of Behaviour Profiling Annual Meeting. - Monterey, CA : [s.n.], 1999.

[4] Ćosić, J; Bača, M. (Im)proving chain of custody and digital evidence integrity with timestamp [Conference] // MIPRO, 33rd International Convention on Information and Communication Technology, Electronics and Microelectronics. - Opatija : [s.n.], 2010. - pp. 171-175.

[5] Ćosić, J; Bača, M. A Framework to (Im)Prove „Chain of Custody“ in Digital Investigation Process [Conference] // Proceeding of CECIIS 2010. - Varaždin, Croatia : [s.n.], 2010.

[6] Ćosić, J; Bača, M. Computer forensic-broad aspects of its application [Conference] // INFOTEH-JAHORINA,B&H. - Jahorina-Sarajevo : [s.n.], 2010. - pp. 857-860.

[7] Ćosić, J; Bača, M. Computer forensic-broad aspects of its application [Conference] // INFOTEH-JAHORINA,B&H. - Jahorina-Sarajevo : [s.n.], 2010. - pp. 857-860.

[8] Ćosić, J; Bača, M. Do we have a full control over integrity in digital evidence life cycle [Conference] // Proceedings of ITI- 32nd International Conference on Information Technology Interfaces. - Dubrovnik/Cavtat : [s.n.], 2010. - pp. 429-434.

[9] Gruber, T. A translation approach to portable ontology specifications, Knowledge Acquisition, An International Journal of Knowledge Acquisition for Knowledge-Based Systems, Volume 5, Number 2, pp. 199-220, 1993.

[10] Guarino, N. Formal Ontology and Information System [Conference] // Proceeding of FOIS98. - Trento-Italy : IOS Press - Amsterdam , 1998. - pp. 3-15.

[11] Harrill, D.C; Mislan, R.P. A Small Scale Digital Device Forensic ontology [Journal]. - [s.l.] : SMALL SCALE DIGITAL DEVICE FORENSIC JOURNAL , 2007. - Vol. VOL. 1.

[12] International Organization on Computer Evidence [Online]. - 02 06, 2011. - http://www.ioce.org/core.php?ID=1.

[13] Jenkinsen, B; Sammes, T. Forensic Computing A Practitioners Guide [Conference]. - New York : Springer, 2000.

[14] Kahvedzic, D; Kechadi, T. DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge [Journal]. - [s.l.] : ELSEVIER-Digital investigation, 2009. - Vols. V6 p23-33.

[15] Menezes, A. J; Oorschot,P.C; Vanstone, S.A. Handbook of Applied Criptografy [Book]. - [s.l.] : CRC Press, 1997.

[16] Nogueira, J.H.M; Vasconcelos, W.P Wamberto Ontology for Complex Mission Scenarios in Forensic Computing [Journal]. - [s.l.] : The Internationa Journal of Forensic Computer Science , 2008. - 1 : Vol. 2008(1).

[17] Park, H; Cho, S.H; Kwon,H.C. Forensic in Telecommunication, Information and Multimedia, e-Forensic [Conference]. - Adelaine, Australia : SpringerLink, 2009. - DOI:10.1007/978-3-642-02312-5.

[18] Pollit, M; Whitledge, A. Exploring big Haystacks. Data Mining and Knowledge Management [Conference] // IFIP Advances in Information and Communication Technology. - [s.l.] : SpringerLink, 2006. - pp. 67-76.

[19] Pretorius, J. Ontologies-Intruduction and Overview [Journal]. - 2004.
Protege Project [Online] // http://protege.stanford.edu/. - mart 01, 2011. - http://protege.stanford.edu/.

[20] Raskin, V. [et al.] Ontology in Information Security: A Useful Theoretical Foundation and Methodological Tool [Conference]. - New Mexico : ACM-NSPW, 2002.

[21] Rector, A. [et al.] Ontology Design Patterns and Problems: Practical Ontology Engineering using Protege-OWL [Journal]. - University of Manchester and Stanford Unviversity : [s.n.], 2005.

[22] Lovrenčić, S. [et al.] Formal Modelling Of Business Rules: What Kind Of Tool, Journal of Information and Organizational Science, JIOS [Journal]. - Varaždin, Croatia : Faculty of Organization and Informatics,, 2006. - No.2 : Vol. Vol.30¸

[23] Science Working Group on Digital Evidence [Online] // Science Working Group on Digital Evidence. - 02 06, 2011. - http://www.swgde.org/.

[24] The Five Ws (and One H) in Cyberspace [Online]. - 2 27, 2011. - http://www.media-awareness.ca/english/resources/special_initiatives/wa_resources/wa_shared/tipsheets/5Ws_of_cyberspace.cfm.