Significance of Semantic Reconciliation in Digital Forensics

Nickson M. Karie
[1]Department of Computer Science, University of Pretoria,
Private Bag X20, Hatfield 0028, Pretoria, South Africa
[2]Department of Computer Science, Kabarak University,
Private Bag - 20157, Kabarak, Kenya
menza06@hotmail.com

H.S. Venter
[1]Department of Computer Science, University of Pretoria,
Private Bag X20, Hatfield 0028, Pretoria, South Africa
hventer@cs.up.ac.za

ABSTRACT

Digital forensics (DF) is a growing field that is gaining popularity among many computer professionals, law enforcement agencies and other stakeholders who must always cooperate in this profession. Unfortunately, this has created an environment replete with semantic disparities within the domain that needs to be resolved and/or eliminated. For the purpose of this study, semantic disparity refers to disagreements about the meaning, interpretation, descriptions and the intended use of the same or related data and terminologies. If semantic disparity is not detected and resolved, it may lead to misunderstandings. Even worse, since the people involved may not be from the same neighbourhood, they may not be aware of the existence of the semantic disparities, and probably might not easily realize it.

The aim of this paper, therefore, is to discuss semantic disparity in DF and further elaborates on how to manage it. In addition, this paper also presents the significance of semantic reconciliation in DF. Semantic reconciliation refers to reconciling the meaning (including the interpretations and descriptions) of terminologies and data used in digital forensics. Managing semantic disparities and the significance of semantic reconciliation in digital forensics constitutes the main contributions of this paper.

Keywords: Digital forensics, semantic disparity, managing semantic disparity, semantic reconciliation, significance of semantic reconciliation

1. INTRODUCTION

Digital forensics plays a very important role in both incident detection and digital investigations. However, the investigation process in most cases demands cooperation between the computer professionals, law enforcement agencies and other forensic practitioners. Unfortunately, this has created an environment replete with semantic disparity within the domain that needs to be resolve and/or eliminated. Semantic disparity as defined by Xu and Lee (2002) refers to disagreements about the meaning, interpretation, description and the intended use of the same or related data. Moreover, according to Oxford Dictionaries (2013), disparity refers to the state of being different (lack of uniformity). If semantic disparity is not detected and resolved in digital forensics, it may lead to misunderstandings. In addition, semantic disparity may become a serious problem, for example, when trying to harmonise data/information from different sources (Piasecki, 2008).

Moreover, in the case of a digital forensic investigation process, the cooperation between the computer professionals, law enforcement agencies and other forensic practitioners presupposes the reconciliation of semantic disparities that are bound to occur in the domain. Unfortunately, DF lacks comprehensive methodologies, specifications and ontologies that can assist in resolving the semantic disparities that exist between the different digital forensic practitioners.

In this paper, therefore, we discuss semantic disparities in DF and further elaborate on how to manage it. In addition, this paper also presents the significance of semantic reconciliation in digital forensics. Furthermore, the presentation in this paper is a novel contribution that offers a simplified comprehension of semantic disparities in digital forensics. Moreover, this paper is also meant to spark further discussions on the development of methodologies and specifications for resolving semantic disparities in DF.

As for the remaining part of this paper, section 2 presents background concepts of semantic disparity while section 3 elaborates on how to manage semantic disparities in digital forensics. The significance of semantic reconciliation in digital forensics is handled in section 4. Finally, conclusions and future research work are considered in section 5.

2. BACKGROUND

In this section of the paper, the authors present background concepts on semantic disparities. Note that, semantic disparity as discussed in this paper is sometimes addressed as semantic heterogeneity in other previous research works (Xu and Lee, 2002; Sheth and Larse, 1990; Wang and Liu, 2009). However, for the purpose of this paper we adopt the use of the term semantic disparity in place of semantic heterogeneity.

To begin with, Sheth and Larsen (1990) argue that, semantic disparity is a problem that is not well understood in many domains and in the case of this paper digital forensics as well. There is not even an agreement regarding a clear definition of this problem (Xu and Lee, 2002; Sheth and Larse, 1990). However, different researchers have identified different forms of semantic disparity that are worth mentioning. A majority of these semantic disparities, however, focus more into the field of databases while others focus on distributed systems.

According to Lin et al. (2006), the problem of semantic disparity is extremely critical in situations of extensive cooperation and interoperation between distributed systems across different enterprises. In the case of digital forensics, for example, such a situation would make it difficult to manipulate distributed data/information in a centralized manner. This is because; the contextual requirements and the purpose of the information across the different systems may not be homogeneous.

Another effort by Colomb (1997) presented the case for structural semantic disparity (structural semantics define the relationships between the meanings of terminologies). Bishr (1998) on the other hand, elaborates on schematic disparity. The major problem as presented by Colomb (1997) lies in what can be called the fundamental conceptual disparity. Fundamental conceptual disparity occur when the terms used in two different ontologies, for example, have meanings that are similar, yet not quite the same (Xu and Lee, 2002). Schematic disparity, on the other hand, arises when information that is represented as data in one schema, is represented within the schema (as metadata) in another (Bishr, 1998; Miller, 1998).

Although the database perspective on semantic disparity is good and offers insights (Xu and Lee, 2002), it limits the understanding of semantic disparity and how to manage it in other domains. In the section that follows, therefore, we elaborate on how to manage semantic disparities focusing on the digital forensic domain.

3. MANAGING SEMANTIC DISPARITIES IN DIGITAL FORENSICS

Managing semantic disparities in a growing field like digital forensics can be a daunting task. This is because; the technological trends in DF are ever-changing; new terminologies are constantly introduced into the domain and new meanings assigned to existing terms (Karie and Venter, 2012). Therefore, methodologies and specifications need to be developed in digital forensics with the ability to effectively assist in managing semantic disparities that may crop up as a result of technological change or domain evolution. Such methodologies will further assist in establishing an efficient semantic reconciliation process in the domain. Furthermore, the requirement for semantic reconciliation methodologies and specifications in digital forensics is exceptionally important both for the advancement of the field as well as for the effective use of different domain terminologies and the representation of domain information.

Therefore, understanding the different potential circumstances and conflicts under which semantic disparity may arise in digital forensics can be of great significance in establishing a meaningful semantic reconciliation process.

3.1. Potential Conflicts that can Cause Semantic Disparity in Digital Forensics

Semantic disparity may occur in digital forensics, for example, when the communicating parties (computer professionals, law enforcement agencies, forensic practitioners, etc.) use different meanings, interpretations, descriptions and representations of the same or related domain terminologies and data. This causes variations in the understanding of domain information and how it is specified and structured in different components. This also implies that, perfect communication between the sender and the receiver of the information will be scanty. Having the ability to identify and avoid semantic disparities in digital forensics can assist investigators, for example, in decision making.

In the sub-sections that follow, therefore, we survey and present (based on our review of the literature) various conflicts (including examples where applicable) that can cause disparities in DF. Note that the conflicts discussed in this section only serves as common examples to facilitate this study and should not be treated as an exhaustive list.

3.1.1. Semantic Conflicts

Semantic conflicts occur when different people involved in the same domain do not perceive exactly the same set of real world objects, but instead they visualize overlapping sets (Bishr, 1998). As a result, disagreement about the meaning, interpretation and the descriptions of the same or related data and terminologies occur. Table 1 shows examples of the semantic conflicts (descriptions and interpretation of terminologies) in digital forensics.

DF Terminology	Descriptions
• First response	Include the first response to the detected incident (Valjarevic and Venter, 2012).
• Initial response	Perform an initial investigation, recording the basic details surrounding the incident, assembling the incident response team, and notifying the individuals who need to know about the incident (Mandia et al., 2003).
• Incident response	Consists of the detection and initial, pre-investigation response to a suspected computer crime related incident, such as a breach of computer security. The purpose of Incident response is also to detect, validate, assess, and determine a response strategy for the suspected security incident (Beebe and Clark, 2005).

Table 1: Semantic Conflicts in Digital Forensic Terminologies.

3.1.2. Descriptive Conflicts

Descriptive conflicts include naming conflicts due to homonyms and synonyms, as well as conflicts on attribute domain, scale, cardinalities, constraints, operations etc. (Bishr, 1998; Sheth and Gala, 1989; Larson et al. 1989). In the case of digital forensics, descriptive conflicts can occur, for example, when two terminologies representing related ideas of the domain concepts are described using different sets of properties. Table 2 present some of the descriptive conflicts identified in the digital forensic domain. Note that the terminologies in Table 1 and Table 2 are only selected examples to facilitate this study and by no means an exhaustive list.

DF Terminology	Descriptions
• Analysis	Determine significance, reconstruct fragments of data and draw conclusions based on evidence found. The distinction of analysis is that it may not require high technical skills to perform and thus more people can work on this case (Reith et al., 2002).
• Analysis	Analysis involves the use of a large number of techniques to identify digital evidence, reconstruct the evidence if needed and interpret it, in order to make hypothesis on how the incident occurred, what its exact characteristics are and who is to be held responsible (Valjarevic and Venter, 2012).
• Analysis	The use of different forensic tools and techniques to make sense of the collected evidence (Sibiya et al., 2012).
• Examination	Examination is an in-depth analysis of the digital evidence and is the application of digital forensic tools and techniques that are used to gather evidence (Lalla and Flowerday, 2010).
• Examination	An in-depth systematic search of evidence relating to the suspected crime. This focuses on identifying and locating potential evidence, possibly within unconventional locations. Construct detailed documentation for analysis (Reith et al., 2002).

Table 2: Descriptive Conflicts in Digital Forensic Terminologies.

The authors found that the terminologies in Table 1 and 2 are mostly used by digital forensic investigators and the law enforcement agencies during and after a digital forensic investigation process, hence the motivation for this study.

3.1.3. Structural Conflicts

Structural conflicts occur when two or more people use the same model, but choose different constructs to represent common real-world objects (Lee and Ling, 1995). In the context of digital forensics structural conflicts can occur, for example, when different domain members use the same digital forensic investigation process model but choose different constructs to present their results/findings. Note that, the term constructs, is used to mean ideas or theories containing various conceptual elements, and considered to be subjective but not based on any empirical evidence (Houts and Baldwin, 2004).

After attending several sessions of expert testimony (potential evidence presentation) in court and civil proceedings the authors found that different constructs are used by different digital forensic experts to convince the court that the potential digital evidence presented is worthy of inclusion into the criminal process. However, the constructs used during potential evidence presentation were based on experience rather than standardised guidelines or digital forensic logics. This is backed up by the fact that, there are

currently no standardised guidelines for even presenting the most common representations of potential digital forensic evidence in court or civil proceedings (Cohen, 2011). In the sub-section that follows, we explain different approaches that can assist in managing semantic disparity in DF.

3.2. Different Approaches to Manage Semantic Disparity

There exist different approaches that can assist in resolving semantic disparities in digital forensics (Farshad and Andreas, 2001). However, as with other examples explained earlier, the list discussed in this section present only selected examples and therefore should not be treated as an exhaustive list.

3.2.1. Building Ontologies

Ontologies can help deal with the problem of semantic disparity by providing formal, explicit definitions of data and reasoning over related concepts. Moreover, ontologies in most cases capture the conceptualization of experts in a particular domain of interest (Falbo et al., 1998). Ontology mapping can also be employed to find semantic correspondences between similar elements of different ontologies, thus allowing people to agree on terms that can be used when communicating (Noy, 2004).

In digital forensics, building a proper domain ontology in terms of its explication and its accordance with the conceptualization of domain experts can help in managing the semantic disparity that occurs in the domain. However, according to Kajan (2013), considering that anyone can design ontologies according to his/her own conceptual view of the world, care must be observed during the process of designing ontologies because, ontological disparity among different parties can become an inherent characteristic.

3.2.2. Representation of Ontologies and Reasoning Based on these Ontologies

According to Farshad and Andreas (2001), the representation of ontologies and reasoning based on these ontologies makes it possible to capture and represent ontological definitions and the important features that can be used in representing ontologies for reasoning. In the case of digital forensics such an approach would help create clear definitions of the different terminologies used in the domain. Moreover, this approach can also assist in managing semantic disparity in DF because the relationships that hold among domain terminologies can be realized and structured. For more information in this regard we refer the reader to (Palmer, 2001; Caloyannides, 2004 & Crouch, 2010) respectively.

3.2.3. Semantics Integration

Semantics integration deals with the process of interrelating information from diverse sources to create a homogeneous and uniform semantic of use (Noy, 2004). In the case of digital forensics, this can make communication easier by providing precise concepts that can be used to construct domain information. Furthermore, semantic integration can facilitate or even automate communication between different systems thus offering the ability to automatically link different ontologies (Gardner, 2005).

3.2.4. Explicit use of common shared semantics

The explicit and formal definitions of semantics of terms have always guided many researchers to apply formal ontologies (Guarino, 1998) as a potential solution of semantic disparity. A formal ontology usually consists of logical axioms that convey the meaning of terms for a particular domain (Bishr et al, 1999; Kottman, 1999). Furthermore, formal ontologies are usually concerned with the understanding of the members of the domain and help to reduce ambiguity in communication (Farshad and Andreas, 2001), understanding, representation and interpretations of information.

In the next section, we present the significance of semantic reconciliation in digital forensics.

4. SIGNIFICANCE OF SEMANTIC RECONCILIATION IN DIGITAL FORENSICS

While there are a lot of research activities in digital forensics even at the time of this study very little have been towards semantic reconciliation. The authors believe that, semantic disparity in any domain can alter the context as well as the purpose of any information delivered by an individual and thus should be avoided. In digital forensics, methodologies and specifications need to be developed that can effectively assist in semantic reconciliation. Furthermore, such methodologies and specifications can also be used, for example, as fundamental building blocks in resolving the present and future semantic disparities in the domain. Semantic reconciliation, in the authors' opinion, is a promising conception towards resolving semantic disparities in digital forensics. The sub-sections that follow will explain in more details some of the significances of semantic reconciliation in digital forensics.

4.1 Perfect Communication

Semantic disparities can be a serious barrier to perfect communication in any domain. Semantic reconciliation, on the other hand, can be used to bridge the semantic gap between different communicating parties thus bringing with it perfect communication in the domain (Parsons and Wand, 2003). This also implies that, information between the different digital forensic stakeholders (computer professionals, law enforcement agencies and other digital forensic practitioners) can be interpreted in such a way that the sender's desired effect is achieved. Moreover, after a security incident has occurred, for example, if the communication, interpretation and representation of information are done correctly, it is much easier and useful in apprehending the attacker, and stands a much greater chance of being admissible in the event of a prosecution (Brezinski and Killalea, 2002). Wrong interpretation and representation of evidence information, on the other hand, might create loopholes for intruders to escape and thus making it had to convict and prosecute them. Therefore, semantic reconciliation in digital forensics is inevitable if perfect communication is to be achieved.

4.2 Common Understanding

Semantic disparities may arise in digital forensics as a result of different representation or interpretation of terminologies and data; this may include the use of different alternatives or definitions to describe the same domain information. However, with semantic reconciliation the different digital forensic experts can achieve common understanding by reconciling the meaning of terms thus having common representation or interpretation of domain terminologies (Parsons and Wand, 2003). This also implies that, the meaning of information as interpreted by the receiver will align with the meaning intended by the sender (Anon, 2013). In the case of court or civil proceedings common understanding will also help different stakeholders treat queries conveniently and at the same time maintaining consistency in their understanding of the various digital forensic terminologies and data used during such proceedings.

4.3 Correct Interpretation

When two or more independent digital forensic practitioners with varying professional backgrounds are to cooperate during an investigation process, semantic conflicts may occur. It is, therefore, very important and critical that semantic disparities be resolved and/or eliminated to facilitate correct interpretation of domain information. Semantic reconciliation is one of the ways that can improve on correct interpretation through detecting the semantic similarities between the different terminologies and data used by the independent practitioners to describe or represent domain information (Parsons and Wand, 2003).

4.4 High-levels of collaboration

Many organisations are increasingly promoting collaborations as an important feature in organisation management (Tschannen-Moran, 2001). However, effective collaborations demands reasoning as well as effective communication. Therefore, semantic reconciliation in digital forensics can lead to high-levels of collaborations between the computer professionals, law enforcement agencies and other digital forensic

practitioners. Furthermore, semantic reconciliation can also help create uniformity in the use of both terminologies and data in the digital forensic domain thus easing cooperation.

4.5 Uniform Representation of Domain Information.

In the case of potential evidence presentation in any court of law, information conveyed with very many semantic variances can be semantically unreliable. Therefore, semantic reconciliation can help create uniform representation of domain information. This is backed up by the fact that, semantic reconciliation can also make interpretation and representation of domain information much easier and more accurate (Wang et al., 2005).

4.6 Faster Harmonisation of Information from Different Sources

Efficient information management and processing have become more and more important within enterprises or when enterprises are merging together (Ubbo et al. 2002). Moreover, to achieve semantic interoperability across information system using different terminologies, the meaning of the information that is interchanged has to be harmonised across the systems (Ubbo et al. 2002). However, semantic disparity may arise whenever two contexts do not use uniform interpretation of the same information. Therefore, the use of semantic reconciliation for the explication of implicit and hidden knowledge is a promising approach to overcome the problem of semantic disparity in digital forensics and can assist in faster harmonisation of information from different sources.

4.7 Less Errors during Analysis of Potential Digital Evidence Information

Errors in analysis and interpretation of digital evidence, in the case of an investigation process, are more likely where there are semantic disparities. Even more where there are no standardised procedures or formal representation of domain information (Chaikin, 2006). Semantic reconciliation, on the other hand, will enable computer professionals, law enforcement agencies and practitioners in digital forensics to agree on terminologies or keywords to be used in representing certain key information in the case of an investigation and also establish keyword structures so that their relationship to each other are easily known. This will enhance the analysis of potential digital evidence information in the domain.

5. CONCLUSION AND FUTURE WORK

The problem addressed in this paper was that of semantic disparity in digital forensics. Different approaches to manage semantic disparities in digital forensics have also been explained. Moreover, the paper has also elaborated on the significance of semantic reconciliation in the digital forensic domain. The presentation in this paper is a new contribution in digital forensics and is meant to spark further discussion on the development of methodologies and specifications for sematic reconciliation in the domain. As part of the future work, the authors are now engaged in a research project to try and develop specification and/or ontologies that will create a unified formal representation of the digital forensic domain knowledge and information. In addition, the authors also aim at developing a digital forensic semantic reconciliatory model as a way towards resolving the semantic disparities that occur in digital forensics. However, there is still much research to be carried out so as to provide directions on how to address semantic disparities in the digital forensic domain. More research also needs to be conducted in order to add on the work discussed in this paper.

REFERENCES

Anon, (2013), A Communication Model. Available at: http://www.worldtrans.org/TP/TP1/TP1-17.HTML [Accessed April 25, 2013].

Beebe, N.L., and Clark, J.G., (2005), "A Hierarchical,Objectives-Based Framework for the Digital Investigations Process". Published in Digital Investigation 2(2). pp 146-16

Bishr Y.A., (1998). Overcoming the Semantics and Other Barriers to GIS Interoperability. *International Journal of Geographic Information Science*, Vol. 12, No. 4, pp299-314

Bishr, Y. A.; Pundt, H.; Kuhn, W., and Radwan, M. (1999). Probing the concept of information communities- a first step toward semantic interoperability. *Interoperating Geographic Information Systems*, Kluwer Academic

Brezinski, D. and Killalea, T, (2002), Guidelines for Evidence Collection and Archiving. Available at: http://tools.ietf.org/html/rfc3227 [Accessed April 25, 2013].

Caloyannides, M.A., (2004). Privacy Protection and Computer Forensics. Second Edition, Artech House, 2004.

Chaikin, D., (2006), "Network investigationis of cyber attacks: the limits of digital evidence", Crime Law Soc. Change, vol. 46, pp. 239-256.

Cohen, F., (2011), Digital Forensic Evidence Examination. 3RD Edition. Published by fred cohen & Associates. ISBN # 1-878109-46-4

Colomb R.M. (1997). Impact of Semantic Heterogeneity on Federating Databases, *The Computer Journal*, Vol. 40, No. 5 p235-244.

Crouch, J.-Ed (2010). NSCI - An Introduction to Computer Forensics, Available at: http://www.nsci-va.org/WhitePapers/2010-12-16-Computer%20Forensics-Crouch-final.pdf [Accessed March 5, 2012].

Falbo, R.A., Menezes, C.S. and Rocha, A.R., (1998) A Systematic Approach for Building Ontologies. Proceeding of the 6th Ibero-American Conference on AI: Progress in Artificial Intelligence. pp. 349-360

Farshad H. and Andreas G, (2001) Resolving Semantic Heterogeneity in Schema Integration: an Ontology Based Approach, University of Zurich. *International Conference on Formal Ontology in Information Systems (FOIS)*, Ogunquit, Maine, USA.

Gardner, S.P. (2005), Ontologies and semantic data integration. DDT, Vol.10, No 14, pp. 1001-1007

Guarino, N., (1998). "Formal Ontology in Information Systems," *Proceedings of FOIS'98*, Trento, Italy.

Houts, A.C. and Baldwin, S., (2004), Constructs, operational definition, and operational analysis. Applied & Preventive Psychology, Vol.11, pp. 45–46

Kajan, E., (2013). Electronic Business Interoperability: Concepts, Opportunities and Challenges - Google Books. Available at: http://books.google.co.za/books?id=fNh2Frjj7oUC&pg=PA287&lpg=PA287&dq=Even+if+two+ontologies+use+the+same+name+for+a+concept,+the+associated+properties+and+the+relationships+with+other+concepts+are+most+likely+to+be+different&source=bl&ots=NQ74gKNzP-&sig=yxThC1hAO27mIwqhAkoJUlPAOUI&hl=en&sa=X&ei=gNUwUeiuMI-LhQfdloDYBQ&ved=0CDYQ6AEwAg#v=onepage&q=Even%20if%20two%20ontologies%20use%20the%20same%20name%20for%20a%20concept%2C%20the%20associated%20properties%20and%20the%20relationships%20with%20other%20concepts%20are%20most%20likely%20to%20be%20different&f=false [Accessed March 1, 2013].

Karie, N.M. and Venter, H.S., (2012) Measuring Semantic Similarity Between Digital Forensics Terminologies Using Web Search Engines. In the Proceedings of the 12th Annual Information Security for South Africa Conference. Johannesburg, South Africa. Published online by IEEE Xplore®.

Kottman, C., (1999). Semantics and Information Communities, the OpenGIS Abstract Specification Topic 14. Ver. 4. *OpenGIS Consortium*, OpenGIS™ Project Document Number 99-114.doc.

Lalla, H., and Flowerday, S.V., (2010), Towards a Standardised Digital Forensic Process: E-mail Forensics. In proceeding of the Information Security South Africa Conference. Sandton, South Africa

Larson, J.A., Navathe, S.B. and Elmasri, R., (1989), "A Theory of Attribute Equivalence in Databases with Application to Schema Integration", IEEE Transactions On Software Engineering, Vol. SE-15, No. 4.

Lee, M.L. and Ling, T.W., (1995), Resolving Structural Conflicts in the Integration of Entity-Relationship Schemas. Object-Oriented and Entity-Relationship Modeling Vol. 1021, pp. 424-433

Lin, Y., Strasunskas, D., Hakkarainen, S., Krogstie, J., and Solvberg, A., (2006), "Sematic Annotation Framework to Manage Semantic Heterogeneity of Process Models", *Proceedings of the 18th international conference on Advanced Information Systems Engineering*, pp. 433-446

Mandia,K., Prosise, C., and Pepe, M., (2003), "Incident Response & Computer Forensics" (Second Ed.), McGraw-Hill/Osborne, Emeryville.

Miller, R.J., (1998), "Using schematically heterogeneous structures", *Proceedings of the 1998 ACM SIGMOD international conference on Management of data*, pp. 189-200

Noy, N.F. (2004). "Semantic Integration: A Survey of Ontology- based Approaches", *SIGMOD Record*, Vol. 33, No. 4, pp65-70

Oxford Dictionaries, (2013), Definition of disparity in Oxford Dictionaries (British & World English). Available at: http://oxforddictionaries.com/definition/english/disparity [Accessed April 12, 2013].

Palmer, G., (2001). A Road Map for Digital Forensic Research, DFRWS Technical Report. DTR - T001-01 FINAL. *Report from the First Digital Forensic Research Workshop* (DFRWS).

Parsons, J. and Wand, Y., (2003), Attribute-Based Semantic Reconciliation of Multiple Data Sources. Journal on Data Semantics I, Vol. 2800, pp 21-47

Piasecki, M., (2008). "HydroTagger: A Tool for Semantic Mapping of Hydrologic Terms". *AAAI Spring Symposium: Semantic Scientific Knowledge Integration*, page 77-80.

Reith, M., Carr, C., and Gunsch, G., (2002), An Examination of Digital Forensic Models. International Journal of Digital Evidence. Vol.1, No.3

Sheth A.P. and Larse, J., (1990). Federated database systems for managing distributed, heterogeneous, and autonomous databases. *ACM Computing Surveys (CSUR) - Special issue on heterogeneous databases Surveys*. Vol. 22 No. 3, pp.183 – 236

Sheth, A.P. and Gala, S.K. (1989), "Attribute Relationships: An Impediment in Automating Schema Integration", Proceddings of theWorkshop on Heterogeneous Database Systems, Chicago

Sibiya, G., Venter, H.S., Ngobeni, S., and Fogwill, T., (2012), Guidelines for Procedures of a Harmonised Digital Forensic Process in Network Forensics. In proceeding of the Information Security South Africa Conference. Sandton, South Africa

Tschannen-Moran, M. (2001). Collaboration and the need for Trust, Journal of Education Administaration Vol. 39, No. , pp. 308-331

Ubbo, V., Stuckenschmidt, H., Schlieder, C., Wache, H., Timm, I., (2002),Terminology Integration for the Management of distributed Information Resources. Künstliche Intelligenz, Vol. 16, pp. 31–34

Valjarevic, A. and Venter, H.S., (2012), Harmonised Digital Forensic Investigation Process Model. In proceeding of the Information Security South Africa Conference. Sandton, South Africa

Wang, H. and Liu, J.N.K., (2009), Analysis of Semantic Heterogeneity Using a new Ontological Structure Based on Description Logics. Sixth International Conference on Fuzzy Systems and Knowledge Discovery

Wang, X., Ausdal, S.V. and Zhou, J., (2005), Managing the Life Cycle of Business Semantics. Available at: http://xtensible.net.s60489.gridserver.com/wp-content/uploads/managing-the-life-cycle-of-business-semantics.pdf [Accessed April 25, 2013].

Xu, Z., and Lee, Y.C. (2002). Semantic Heterogeneity of Geo Data, *Symposium on Geospatial Theory, Processing and Applications*, Ottawa.