Future Internet **2014**, *6*, 584-596; doi:10.3390/fi6030584

OPEN ACCESS

future internet

ISSN 1999-5903

www.mdpi.com/journal/futureinternet

Article

Digital Forensics to Intelligent Forensics

Alastair Irons [1,]* and Harjinder Singh Lallie [2]

[1] The University of Sunderland, David Goldman Informatics Centre, St Peters Campus,
Sunderland SR6 0DD, UK

[2] University of Warwick (WMG), Coventry CV4 7AL, UK; E-Mail: h.s.lallie@warwick.ac.uk

* Author to whom correspondence should be addressed; E-Mail: alastair.irons@sunderland.ac.uk;
Tel.: +44-191-515-2053; Fax: +44-191-515-2809.

Received: 1 April 2014; in revised form: 22 August 2014 / Accepted: 2 September 2014 / Published: 12 September 2014

Abstract: In this paper we posit that current investigative techniques—particularly as deployed by law enforcement, are becoming unsuitable for most types of crime investigation. The growth in cybercrime and the complexities of the types of the cybercrime coupled with the limitations in time and resources, both computational and human, in addressing cybercrime put an increasing strain on the ability of digital investigators to apply the processes of digital forensics and digital investigations to obtain timely results. In order to combat the problems, there is a need to enhance the use of the resources available and move beyond the capabilities and constraints of the forensic tools that are in current use. We argue that more intelligent techniques are necessary and should be used proactively. The paper makes the case for the need for such tools and techniques, and investigates and discusses the opportunities afforded by applying principles and procedures of artificial intelligence to digital forensics intelligence and to intelligent forensics and suggests that by applying new techniques to digital investigations there is the opportunity to address the challenges of the larger and more complex domains in which cybercrimes are taking place.

Keywords: digital forensics; intelligent forensics; digital intelligence; large data; social network analysis; artificial intelligence

1. Introduction

There is a growing concern that the technology, processes, and procedures used in digital investigations are not keeping abreast with the technology that criminals are using to perpetrate crime. This is generally due to a continual growth in cybercrime, increasing magnitudes of storage, a multitude of data evidence sources and continual increases in computational power. For these reasons, there exists a phenomenon, which we refer to as the "large data problem in digital forensics", which contributes to the increase in the "backlog" in of digital devices waiting to be digitally investigated. Various attempts have been made to identify the scale of the backlog, but estimates suggest between 6–12 months in 2004 [1] and rising to between 18–24 months in 2010 [2]. Similar patterns are reported in the US [3]. It should be noted that the backlog is only in part due to the increasing dataset sizes, part of the problem exists because of the increasing number of investigations coupled with too few investigators to investigate them.

One of the major pragmatic problems facing digital investigators is that at the outset of an investigation it is not apparent where digital evidence will be located, if the evidence is successfully located, it is often difficult to ascertain which evidence source will be relevant to an investigation. This leads to a situation where an investigator has to image all potential sources of digital evidence and indeed every device that has been included as part of a seizure.

The "range" of data sources increases considerably when an investigation involves social media and increases further still where numerous participants are involved. Added to this problem of an increasing multitude of data sources is the rapidly increasing storage sizes (and decreasing costs) available for purchase—typical hard disk capacities have increased from 10 Gb in the early 1980s to over a Tb in the 2010s.

The advent and adoption of "secure" technologies threatens to render current approaches to digital forensic investigation more complex and problematic. Technologies, such as the growth in encryption, which now encompasses full disk encryption; secure network communication; secure processors; and anonymous routing potentially make the time taken to undertake digital investigations longer.

Given this array of problems, we propose that it is necessary to review the ways in which digital investigations consider issues and we discuss the introduction of intelligent techniques in the investigative process. In this paper, we propose that there is a need to re-examine standard digital forensic processes and procedures, as well as the uses of investigative technology to adapt to advances in the criminal use of technology—this is done in the paper by consideration of intelligent forensics. A number of the key recent technological advances, which present particular challenges to law enforcement agencies, are analysed herein. We explore the concepts of *intelligence* and propose that *digital forensic intelligence* and *intelligent forensics* can add significant value to investigations.

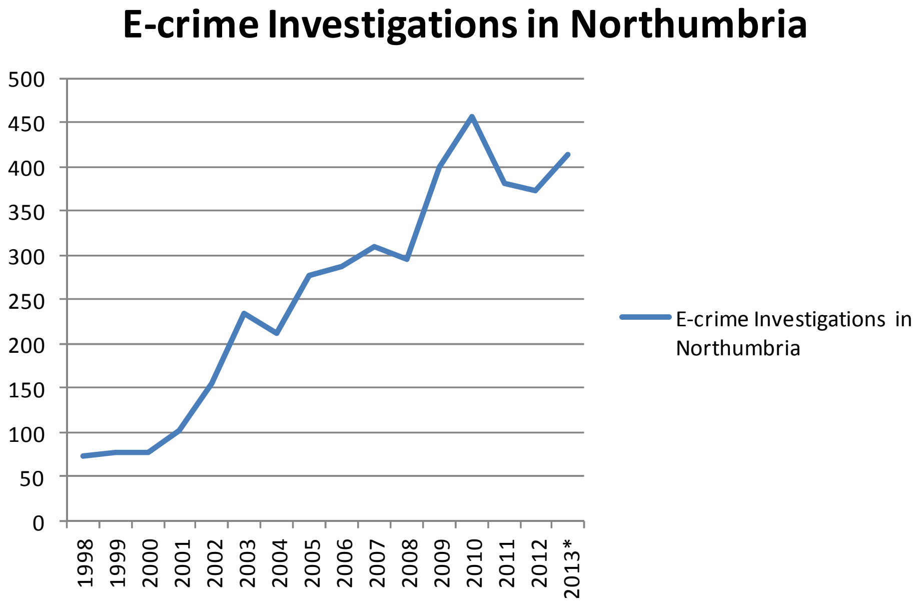
2. Digital Forensic Trends

As the number of digital devices proliferate, there continues to be an annual growth in cyber-crime and the perpetration of crime which involves the use of digital devices. This is demonstrated by annual data published by the FBI (Federal Bureau of Investigation), which shows a year-on-year growth in the number of forensic investigations, the amount of data being investigated and the amount of data being investigated per case (Table 1). The growth in cyber-crime can also be illustrated at the micro level. The following table (Figure 1) shows the growth in cyber crime investigations, using the Northumbria Police e-crime unit data as a local (to one of the authors) example. Whilst this is only one example it illustrates the pattern of growth of investigations—a pattern replicated throughout other police forces in the UK.

Table 1. The number of forensic examinations and amount of data processed by the FBI from 2007 to 2011 [3–7].

Year	**2007**	**2008**	**2009**	**2010**	**2011**
Number of Forensic Examinations	4634	4524	6016	6564	7629
Terabytes of Data Processed	1228	1756	2334	3086	4263
Terabyte per Forensic Examination	0.26	0.39	0.39	0.47	0.56

Figure 1. Ecrime Investigations in Northumbria Police region 1998–2013. Please note 2013 data only available for first three quarters and shown figure has been adjusted to reflect all year anticipated investigations (310 reported ecrimes to end September).



In 2012, the Computer Analysis Response Team, (CART—a department that provides assistance to the FBI in the search and seizure of digital evidence) supported around 14,000 investigations, conducted more than 133,000 digital investigations, and analysed more than 10,500 Terabytes of data [1].

Whilst this data illustrates the size of data investigated collectively by an agency, the problem is further evidenced by a number of recent individual investigations which have involved the analysis of very large data sources for instance, in July 2012, the FBI was ordered to copy 150 terabytes of data held on the *MegaUploads* server by Kim Dotcom [2].

One of the most well-known complex digital investigations centred around the investigation and enquiries that followed the Enron collapse in 2001. The US Securities and Exchange Commission (SEC) and the Federal Energy Regulatory Commission (FERC) conducted two separate independent enquiries into the collapse, and analysed very large email and accounting datasets, as well as a plethora of paperwork. The investigation drew expertise from across numerous domains, including the law enforcement agencies, forensic accountants, and digital investigators.

2.1. Network Forensics

When an investigation spans into the domain of network forensics, the problem becomes complicated by very large log files, such as those associated with firewall, IDS, or web servers. A typical organisational subdomain with 150 IP addresses may generate 60,000–70,000 IP entries in the firewall log per hour. Extend this to the whole network over the time period of a week and this can easily reach more than 150 million entries.

The potential dataset is increased further in the context of a criminal investigation if the data logs available from ISPs and the amount of data available in social network data are considered through for example: Facebook (indicating relationships, friendships, places, *etc.*), Flickr (containing metadata name/place tags), and YouTube (videos containing tags).

This phenomena also leads to the problem of log time correlation—a problem that has been explored by a number of authors including Abad *et al.* [8] who analysed the problem from an intrusion detection system viewpoint, Al-Hammadi and Aickelin [9], who considered the complex problem of botnet detection through log correlation, and Herrerias and Gome [10] to name a few.

2.2. Cloud Investigations

The area of cloud investigation has not received the research interest that it deserves, Beebe [11] and ENISA (European Network and Information Security Agency) [12] highlighted the need to prioritise further research into cloud investigation and in particular evidence gathering mechanisms.

Birk explored some of the complexities of investigating various cloud platforms and presents a very useful insight into the problems encountered in investigating SaaS, PaaS, and IaaS [13]. Lallie and Pimlott [14], Reilly *et.al.* [15], and Taylor et.al., [16] highlighted the problems encountered in attempting to apply guidelines in a cloud investigation and outlined some of the complexities of the acquisition process where data is in the cloud. Grispos *et al.* [17] concluded that current methods and guidelines for digital investigation could be insufficient for conducting a cloud investigation.

In addition to this, cloud investigations lead to jurisprudence/jurisdictional problems related to the ownership of the cloud storage and geographic location (highlighted by Taylor *et al.* [16] and Lallie and Pimlott [14]), and, also, the different methods of acquiring data from different cloud system deployment models.

Possibly one of the biggest problems in investigating the cloud is that of identifying and then subsequently imaging the data sources. A public cloud storage infrastructure may consist of dozens of server farms/data stores located at different geographic locations against which the data may be dynamically routed and stored [18]. The investigator has to identify the precise location of the data before being able to image the data. This, in of itself, presents a distinct forensics challenge for investigator and is a problem hitherto no explored well if at all. Imaging such large datasets requires a new approach to the technology and systems used by investigators to capture large data stores. Time-lining is quite fundamental to a digital investigation, however the uncertainties surrounding the location of data make it more difficult to timeline. File metadata does not store information relating to its movement and an investigator may struggle to chart the movement of data over any given period.

2.3. *Big* vs. *Large Data*

Are these examples of investigative problems—examples of big data? The term *big data* refers generally to the problems of processing very large datasets often collected to finite detail and which require elaborate and sometimes complex techniques to process the data. The definition is contextually contemporaneous and relative, what constitutes as big data today will not be big data in years to come. For instance, in the 1980s, the 100 GB hard disk enclosed in the IBM 3850 MSS (Mass Storage System)—used to provide researchers with instant access to the 1980 U.S. Census database, was considered to be a *big data* problem [19].

Generally, for an analytical problem to be a big data problem, it has to pass the 'test' of volume, velocity and/or variety. This implies that the dataset to be processed is too large (either or both in terms of number of items or size) to be processed effectively and efficiently (volume), it takes too long to extract meaningful data from the dataset (velocity) and/or the dataset comprises of numerous complex structures of data and includes for instance: computer access logs, imagery, financial transactions, and website navigation trees (variety). In all cases the most important point is that the processing of the dataset requires cutting edge technology.

We argue that the examples given herein are "large data" problems and not necessarily big data problems. Whilst there is the potential for digital investigations to face challenges in handling large data the current problems of volume, velocity and/or variety are different to other big data domains. The size of the data analysis problem in digital forensics cannot be compared with other big data problems such as those of analysing the CardioDX data or the Large Hadron Collider. The size of the digital investigative problem is significant, difficult to manage, but not unmanageable. We posit that this argument stands true until such a time as the digital forensics community is presented with such a problem which: involves either such a large dataset, takes too long to arrive at meaningful results and/or contains such a variety of data formats that current investigative tools and techniques cannot process it.

3. Digital Intelligence and Intelligent Forensics

The discussion, hitherto, has focused on the problem of complex/large digital investigations, we proceed to consider how an investigation can be extended to incorporate a range of techniques that can provide further insights into the case and possibly make the investigation more efficient. We posit that the digital forensics community has to extend its range of tools and techniques and find more efficient ways of analysing data and particularly to extract "intelligence" from evidence sources so as to give insights into user behaviour, as well as insights into the incident being investigated. This problem has received some attention from other authors, for instance, Lai *et al.* [20] proposed a conceptual framework useful in profiling Internet pirates and Ieong [21] proposes the FORZA (FORensics ZAchman) framework which considers investigations at multiple layers within an organisation in an effort to combine and apply multiple forensic techniques to solve complex problems. This research demonstrates a growing interest in examining digital forensic practice to solve complex problems. The Center for Information Security and Cryptography (CISC) [22] conducted a 15-month project into understanding the key behavioural characteristics and profiles of cyber criminals who conduct Internet piracy, cyberstalking, and online auction site fraud.

Intelligence plays a key part in criminal investigations and is the subject of numerous research papers and debates. Furthermore forensic intelligence is also a well-researched area, Ribaux for instance has written extensively on the use of forensic intelligence in crime analysis [23–25]

Within the context of criminal investigation, it is important to distinguish *intelligence* from *evidence*. Evidence is "*the available body of facts or information indicating whether a belief or proposition is true or valid*" [26] and intelligence is: "*the ability to acquire and apply knowledge and skills*" or "*the collection of information of military or political value*" [27]. The two definitions of intelligence are quite interesting, the former refers to the "ability to acquire" which tallies with Mithas' definition of digital intelligence whilst the second refers to the acquisition "for a purpose" which tallies with Stanhope's definition. Whilst the second definition refers specifically to military and political values of intelligence, this can of course be extended to other domains, such as business and law enforcement.

In the present context, intelligence is, therefore, relevant knowledge, which may or may not be evidence in a stated or as yet unstated crime or scenario. Clearly, it has certain qualities, for instance it has to have a value and for that to happen, it has to be—as Ribaux puts it, timely, accurate and usable [23].

The term *digital intelligence* seems to convey a number of meanings. Mithas [28] advocates that business managers can gain a significant advantage by having the intelligence to understand, analyse and use digital technology so as to provide competitive benefit and advantage, something that he refers to as *digital intelligence*.

Stanhope's view however is somewhat different and he proposes that digital intelligence is:

> *The capture, management, and analysis of data to provide a holistic view of the digital customer experience that drives the measurement, optimization, and execution of marketing tactics and business strategies.* [29]

Stanhope's definition is business-customer centric and the approach recognises the importance of digital intelligence to enable the analysis and understanding of complex consumer data. In his model, the various data types collected are the input to his digital intelligence architecture wherein ratings, comments, email, display advertising, transactions, and social networks are amongst a number of factors that act as digital data and business inputs which are processed and warehoused before analysis and action on the part of the business (Figure 2).

3.1. Digital Forensic Intelligence

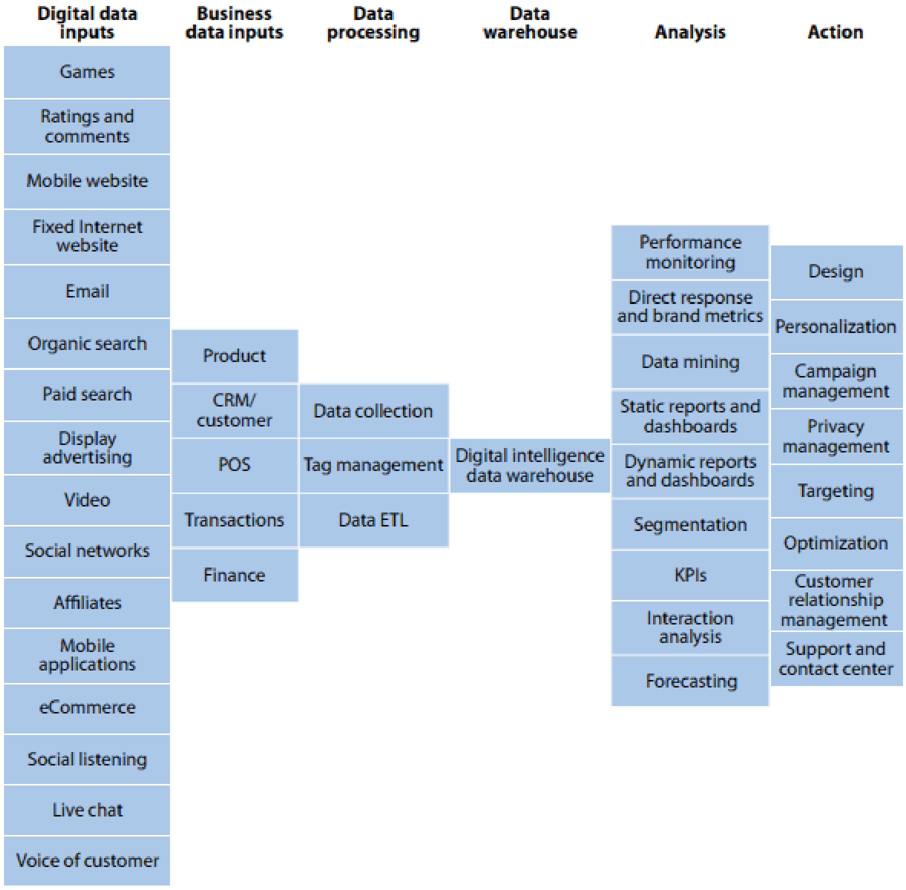
The two terms can be combined to posit a definition of *digital forensic intelligence* as:

> *Knowledge which has a value to law enforcement or other investigative agencies and which has been gathered through the forensic analysis and processing of digital storage systems.*

Digital forensic intelligence can be drawn from intelligence led activities, as well as through routine investigations quite often, the intelligence drawn thereof is stored in databases.

There are a number of examples of such intelligence databases within the forensic science domain, for instance the *UK National DNA Database* (NDNAD), the UK *National Fingerprint Database* (IDENT1) and the USA *Integrated Automated Fingerprint Identification System (IAFIS)*. These databases exemplify the difference between intelligence and evidence. The databases do not contain evidence but do contribute to the more efficient solving of crimes, which had not been known of at the time that relevant entries were added to the database.

Figure 2. Stanhope's "Digital Intelligence Architecture".



The gathering of intelligence has been described in various models, the one that most agencies around the world accepts seems to be the one developed by Metropolitan Police [30], which defines intelligence gathering as consisting of five stages: collection, evaluation, collation, analysis and dissemination.

3.2. Intelligent Forensics

Intelligent forensics is an inter-disciplinary approach, which makes use of technological advances and applies resource in a more intelligent way to solve an investigation. Intelligent forensics encompasses a range of tools and techniques from artificial intelligence, computational modelling and social network analysis in order to focus digital investigations and reduce the amount of time spent looking for digital evidence.

We posit that intelligent forensics is an approach that can be adopted to investigate particularly complex incidents.

Intelligent forensics can be applied proactively—before an incident occurs, and reactively—after an incident has taken place. The proactive use of intelligent forensics seeks to identify threats in advance of an incident taking place. This is applied currently in intelligence seeking situations by the secret/military services and law enforcement agencies (particularly in the UK/USA/Europe) and is beyond the scope of our discussions.

The reactive use of intelligent forensics techniques can be used as part of a standard investigation to provide more intelligence, which can guide the full analysis of the data sources. A number of techniques can be used at this juncture, such as social network analysis (SNA) and artificial intelligence (AI). We proceed to give a very brief overview of the value of these techniques in a digital investigation.

There are a number of potential intelligent forensic solutions in addressing the complexities of big data sources of digital evidence. The solutions focus on either cutting down the size of the investigation (for example using hashing to eliminate stable or non-changed data sources) or speeding up the tools for investigation or using intelligent forensics. Intelligent forensics makes use of enhanced processes and approaches. Traditionally digital forensics uses queries to find data. Whilst intelligent forensics would continue to use this approach in addition intelligent forensics uses approaches that enable data to find queries, data to find data and queries to find queries

3.2.1. Social Network Analysis

Social Network Analysis (SNA) draws on graph theory and other mathematical techniques to allow for the analysis of networks—in this case, networks of people. SNA can provide numerous insights into the network structure and highlight a series of metrics, such as degree centrality, which refers loosely to the centrality of a person in a network.

The value of SNA in investigations has been demonstrated most particularly in the abundance of research conducted into the Enron email dataset which contains around half a million emails generated over three and a half years. On the release of the dataset in 2002 into the public domain [31], researchers were able to:

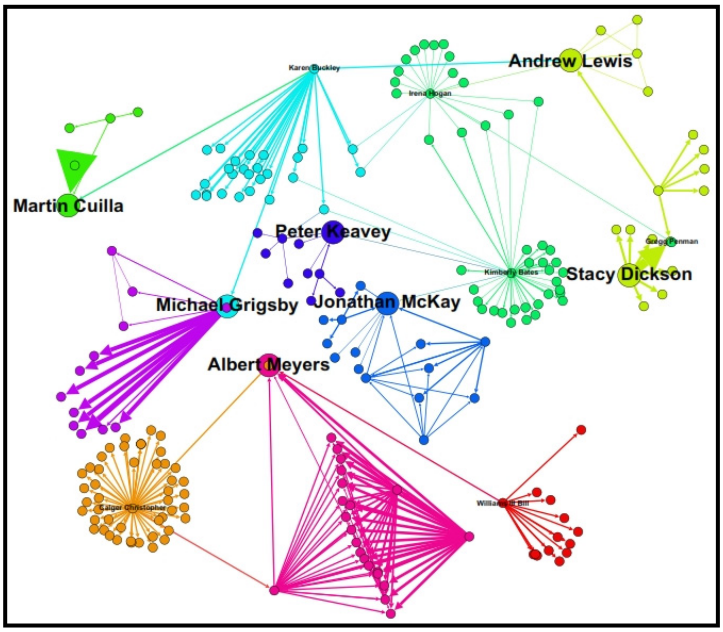
- Discover hidden groups, *i.e.*, “a group of individuals planning an activity over a communication medium without announcing their intentions” [32];
- Discovering organizational structure [33];
- Demonstrate how networks of people change during an emerging situation. In the Enron case for instance, the executives formed a tighter clique and information distribution became less coordinated during the collapse (Figure 3) [34].

How changes in word usage over time can demonstrate key players and individual influence [35].

SNA techniques allow the investigator to determine the density of communications, the strength of connections between two nodes or people and the “influencing power” of a person in a network. The same techniques can help to identify people who may not have been part of the original investigation thereby giving a greater “intelligent” insight into the investigation.

Whilst such a visual analysis is useful in identifying patterns, the real science behind such systems is the graph based mathematical analysis that allows an investigator to identify patterns in group behavior and in particular, identify key parts of the network—such as nodes that are the most influential in a network. A number of open source tools and solutions exist to enable this analysis such as NetworkX [36], Pajek [37], and Gephi [38], as well as industrial solutions, such as i2 analyser [39].

Figure 3. A reduced social network depicting email flow from group leaders in a number of groups in Enron.



3.3. Artificial Intelligence and Computer Forensics

In this section the opportunities to apply artificial intelligence to computer forensics are identified with the focus of the discussion examining the ways in which the application of artificial intelligence can enhance computer forensics investigations. It is not the purpose in this paper to enter the debate as to what constitutes artificial intelligence, except to say that within the context of this paper artificial intelligence is taken to be a computer system which models some degree of intelligence. The application of intelligence in computer forensics investigations takes on a number of components at various stages of the investigation life cycle—the gathering of digital evidence, the preservation of digital evidence (evidential integrity and evidential continuity), the analysis of digital evidence and the presentation of that evidence. In each of these stages the skill and knowledge of the computer forensics investigator is fundamental to the success of any investigation. However, it is hoped that the application of artificial intelligence to digital forensic investigations will provide a useful set of tools to the investigator to address complexity issues and more importantly will address the issues associated with speed and volume (size of data being investigated rather than backlog of cases which is a separate issue) of digital investigation cases, by identifying the most relevant areas for investigation and excluding areas where results are less likely. This approach has been used previously to a certain extent by the application of hash algorithms to eliminate dormant files and "static" systems files form digital investigations.

If the assumption is made that the knowledge that a digital investigator applies to an investigation can be formally structured then it can be used to form knowledge representation (digital forensic information to reason about). Similarly, if the knowledge is structured in such a way as to allow reasoning then the artificial intelligence concept of ontology (the formal structure of that representation so that reasoning can be applied) can be applied.

One of the significant challenges in applying artificial intelligence to computer forensics is the clarity in explaining artificial intelligence algorithm use in the computer forensics the reasoning process. This can be ameliorated by considering the application of artificial intelligence in computer forensics as essentially concerned with anomaly detection. There are two aspects to this: legal and computational. Legal anomalies consist of acts that transgress the law of a given jurisdiction, such as under-age drinking or driving. Computational anomalies consist of abnormal states of the computing machine, e.g., a sector which contains data in an abnormal part of disc; abnormally formatted data packets, data out of normal bounds whether in a data stream or held in static data storage; personal relational data which point to unusual relationships.

The detection of such anomalies involves the whole range of artificial intelligence techniques. Knowledge based systems can be built to capture a legal expert's understanding of the principles of the law and be able to signal unusual behaviour. Neural networks can also be trained to categorise in/appropriate behaviour and are even able to model the behaviour of different users so that it would be possible to signal unusual use patterns for the currently logged in user. Data mining and machine techniques can be used to discover patterns of behaviour and flag exceptions. Along with big data analytics and high performance computing platforms, it is possible to develop systems, which continuously learn and improve system performance in order to keep up with changing trends in the computer forensics arena.

Such techniques could be used to automate aspects of the identification, gathering, preservation and analysis of evidence both *post hoc* and proactively.

4. Summary

The trends of recent years indicate that the environment for cybercrime and for the application of digital forensics in digital investigations is changing and growing in scale. In order to be able cope with the management of cybercrime—in identifying, collecting, recovering, analysing, and documenting, there is a need to consider more effective and efficient processes and procedures in digital investigations. The development of new technologies and environments for potential cybercrime, such as advances in high performance computing and the cloud and prevalence of social media and the ubiquitous use of mobile technologies mean that there is a need to consider the tools and techniques open to a digital forensics investigator.

In this paper we have suggested that, in order to combat the current and future challenges of cybercrime, there is a need to enhance the use of the resources available and move beyond the capabilities and constraints of the forensic tools that are in current use. We argue that the use of intelligent techniques could be applied to digital investigations in order to enhance the investigations in terms of time and efficiency.

This paper has identified the potential opportunities afforded by applying principles and procedures of artificial intelligence to digital forensics intelligence and to intelligent forensics and that as a result of applying intelligent techniques to digital investigations there is the opportunity to address the challenges of the larger and more complex domains in which cybercrimes are taking place.

Author Contribution

This paper represents a collaboration between the two authors and each section has been put together based on shared experiences and expertise. Irons has taken a lead on sections 2.1 and 3.2 and Lallie has taken a lead on sections 2.2, 2.3 and 3.1.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. EURIM-ippr. (2004). EURIM—IPPR E-Crime Study: Partnership Policing for the Information Society. Third Discussion Paper. Available online: http://www.eurim.org/consult/e-crime/may_04/ECS_DP3_Skills_040505_web.htm (accessed on 31 December 2013).
2. European Information Society Group (EURIM). *Separating Myth from Reality and Snake-Oil from Practicality*; Partnership Policing for the Information Society, European Information Society Group (EURIM): London, UK, 2010. Available online: http://www.eurim.org.uk/activities/e-crime/partpolicing.php (accessed on 10 January 2014).
3. Gogolin, G. The Digital Crime Tsunami. In *Digital Investigation*; Elvisier: Amsterdam, Holland, 2010; Volume 7, pp. 3–8.
4. Federal Bureau of Investigation (FBI). 2013, Piecing Together Digital Evidence—The Computer Analysis Response Team. Available online: http://www.fbi.gov/news/stories/2013/january/piecing-together-digital-evidence/piecing-together-digital-evidence (accessed on 10 January 2014).
5. Otago Daily Times. FBI ordered to copy seized Dotcom data. Available online: http://www.odt.co.nz/news/national/213394/fbi-ordered-copy-seized-dotcom-data (accessed on 20 January 2012).
6. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). *Annual Report for Fiscal Year 2007*; RCFL: Virginia, Maryland, USA, 2007.
7. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). *Annual Report for Fiscal Year 2008*; RCFL: Virginia, Maryland, USA, 2008.
8. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). *Annual Report for Fiscal Year 2009*; RCFL: Virginia, Maryland, USA, 2009.
9. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). *Annual Report for Fiscal Year 2010*; RCFL: Virginia, Maryland, USA, 2010.
10. U.S. Department of Justice, Regional Computer Forensics Laboratory (RCFL). *Annual Report for Fiscal Year 2011*; RCFL: Virginia, Maryland, USA, 2011.
11. Abad, C.; Taylor, J.; Sengul, C.; Yurcik, W.; Zhou, Y.; Rowe, K. Log Correlation for Intrusion Detection: A Proof of Concept. In Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, NV, USA, 2003; pp. 255–264.
12. Al-Hammadi, Y.; Aickelin, U. Detecting botnets through log correlation. *arXiv preprint arXiv:1001.2665,* 2010. Avaialble online: http://arivx.org/ftp/arxw/papers/1001/1001.2665.pdf (accessed on 10 January 2014)

13. Herrerias, J.; Gomez, R. A Log Correlation Model to Support the Evidence Search Process in a Forensic Investigation. In Proceedings of the Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2007). 10–12 April 2007; pp. 31–42.
14. Beebe, N. Digital forensic research: The good, the bad and the unaddressed. *Adv. Digit. Forensics* **2009**, *V*, 17–36.
15. European Union Agency for Network and Information Security (ENISA). Cloud Computing. Benefits, Risks and Recommendations for Information Security. Available online: http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (accessed on 30 March 2014).
16. Birk, D. Technical Challenges of Forensic Investigations in Cloud Computing Environments. In Proceedings of the 6th International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 26 May 2011.
17. Lallie, H.S.; Pimlott, L. Applying the ACPO principles to Cloud forensic investigations. *J. Digit. Forensics Secur. Law* **2012**, *7*, 71–86.
18. Reilly, D.; Wren, C.; Berry, T. Cloud computing: Pros and cons for computer forensic Investigations. *Int. J. Multimedia Image Process. (IJMIP)* **2011**, *1*, 26–34.
19. Taylor, M.; Haggerty, J.; Gresty, D.; Lamb, D. Forensic investigation of cloud computing systems. *Netw. Secur.* **2011**, *2011*, 4–10.
20. Grispos, G.; Storer, T.; Glisson, W.B. Calm before the storm: the challenges of cloud computing in digital forensics. *Int. J. Digit. Crime Forensics (IJDCF)* **2012**, *4*, 28–48.
21. Qureshi, A. Plugging into Energy Market Diversity. In Proceedings of the 7th ACM Workshop on Hot Topics in Networks, Calgary, AB, Canada, 6–7 October, 2008.
22. Jacobs, A. The pathologies of big data. *Commun. ACM* **2009**, *52*, 36–44.
23. Lai, P.; Chow, K.-P.; Fan, X.-X.; Chan, V. An Empirical Study Profiling Internet Pirates. In *Advances in Digital Forensics IX*; Springer: New York, NY, USA, 2013; pp. 257–272.
24. Ieong, R.S. FORZA—Digital forensics investigation framework that incorporate legal issues. *Digital Investigation.* **2006**, *3*, 29–36.
25. Ribaux, O. *Forensics, Intelligence by the Trace*, PUR Presses Polytechnique: Lausanne, Switzerland, 2007.
26. Ribaux, O.; Girod, A.; Walsh, S.; Margot, P.; Mizrahi, S.; Clivaz, V. Forensic intelligence and crime analysis. *Law Probab. Risk* **2003**, *2*, 47–60.
27. Ribaux, O.; Walsh, S.J.; Margot, P. The contribution of forensic science to crime analysis and investigation: Forensic intelligence. *Forensic Sci. Int.* **2006**, *156*, 171–181.
28. Ribaux, O.; Baylon, A.; Roux, C.; Delémont, O.; Lock, E.; Zingg, C.; Margot, P. Intelligence-led crime scene processing. Part I: Forensic intelligence. *Forensic Sci. Int.* **2010**, *195*, 10–16.
29. Oxford University Press. *Evidence*. Available: http://oxforddictionaries.com/definition/evidence?q=evidence (accessed on 18 May 2012)
30. Oxford University Press. *Intelligence*. Available: http://oxforddictionaries.com/definition/intelligence?q=intelligence (accessed on 28 May 2012).
31. Mithas, S. *Digital Intelligence: What every Smart Manager Must Have for Success in an Information Age*; FinerPlanet: North Potomac, MD, USA, 2012.

32. Stanhope, J. Welcome to the Era of Digital Intelligence. Available online: http://www.xplusone.com/uploads/case_studies/Welcome_To_The_Era_Of_Dig.pdf (accessed on 30 March 2014).
33. Sparrow, M.K. The application of network analysis to criminal intelligence: An assessment of the prospects. *Soc. Netw.* **1991**, *13*, 251–274.
34. Diesner, J.; Frantz, T.L.; Carley, K.M. Communication networks from the Enron email corpus "It's always about the people. Enron is no different". *Comput. Math. Organ. Theory* **2005**, *11*, 201–228.
35. Baumes, J.; Goldberg, M.; Hayvanovych, M.; Magdon-Ismail, M.; Wallace, W.; Zaki, M. Finding hidden group structure in a stream of communications. *Intell. Secur. Infor.* **2006**, *3975*, 201–212.
36. Zhou, D.; Song, Y.; Zha, H.; Zhang, Y. Towards Discovering Organizational Structure from Email Corpus. In Proceedings of the 4th IEEE International Conference on Machine Learning and Applications, Los Angeles, CA, USA, 2005; p. 6.
37. Diesner, J.; Carley, K.M. Exploration of Communication Networks from the Enron Email Corpus. In Proceedings of the Workshop on Link Analysis, Counterterrorism and Security, SIAM International Conference on Data Mining, Newport Beach, CA, USA, 2005; pp. 21–23.
38. Keila, P.S.; Skillicorn, D. Structure in the Enron email dataset. *Comput. Math. Organ. Theory* **2005**, *11*, 183–199.
39. NetworkX. Available online: http://networkx.github.com/ (accessed on 28 January 2013).
40. Vlado, A. Pajek Wiki. Available online: http://pajek.imfm.si/doku.php (accessed on 28 January 2008).
41. Gephi. Available online: https://gephi.org/ (accessed on 28 January 2013).
42. IBM. i2 Intelligence Analysis Platform. Available online: http://www-03.ibm.com/software/products/en/intelligence-analysis-platform (accessed on 4 July 2014).